Archer® Suite

Version 6.9.2

Security Events Report API

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

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.

License Agreement.

This software and the associated documentation are proprietary and confidential to R SA Security LLC or its affiliates 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 RSA.

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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 -2021 RSA Security LLC or its affiliates. All Rights Reserved.

© 2020 -2021 RSA Security LLC or its affiliates. All Rights Reserved.

July 2021

Contents

Security Events Report API

The Security Events Report API returns a set of up to 50,000 security events for the date specified in the request.

Usage

Privileges. This API requires read privileges to the Security Events Report, which can be found under the Access Control Reports.

URL. localhost/Archer/api/core/system/AccessControlReports/SecurityEvents

Method. POST

Resources.

The resource information for the API is described in the following table.

Resource	Description
Response Format	JSON
Requires Authentication	Yes

Request body parameters.

The required request body parameters for the API are described in the following table.

Parameter	Data Type	Description
eventType	String	A valid eventType that the Security Events Report API supports. For more information, see Supported eventTypes.
eventsForDate	String	A valid date that the Security Events Report API generates events for, in the format YYYY-MM-DD. The selected date can range from six days to one day before the selected date. For example, if today is 2021-01-06 (January 6, 2021), then the range of acceptable dates is between 2021-01-05 (January 5, 2021) and 2021-01-01 (January 1, 2021).
instanceName	String	A valid instance name, which the IIS logs use to track the API request.

Supported eventTypes

The Security Events API supports the following eventTypes:

- All Events
- Access Role Created
- Access Role Deleted
- Access Role Modified
- Account Status Modified
- Configuration Administrator Added
- Configuration Administrator Deleted
- Content Administrator Added
- Content Administrator Deleted
- Content Decrypted In Bulk
- Content Encrypted In Bulk
- Failed User Login
- Full Application Content Delete
- Global Report Permission Granted
- Global Report Permission Removed
- LDAP Configuration Delete Started
- LDAP Configuration Delete Completed
- Maximum Login Retries Exceeded
- Offline Access Sync Requested-Download
- Offline Access Sync Requested-Upload
- Password Changed by Administrator
- Password Changed by User
- PIN Request Failed
- PIN Request Successful
- Reset Password Requested
- Role Assigned to User
- Role Removed from User
- Security Events Started
- Security Events Stopped
- Security Parameter Assignment Modified
- Security Parameter Created
- Security Parameter Deleted
- Security Parameter Modified
- Sub-Form Configuration Administrator Added
- Sub-Form Configuration Administrator Deleted
- Translation Export Requested
- Translation Import Requested
- User Account Added
- User Account Deleted
- User Account Modified
- User Added to Group
- User Full Name Modified
- User Login
- User Login Name Modified
- User Account Modified
- User Logout
- User Removed from Group

Headers.

The required headers for the API are described in the following table.

Parameter	Data Type	Value
Content-Type	String	`application/json`
Authorization	String	`Archer session-id=sessionToken` `sessionToken` is a valid session token ID for the API user login.
X-HTTP-Method-Override	String	`GET`

Output.

This response returns Strings. If the request is successful, the response returns the Event, the user that started the event, the event timestamp, and the event details. The API also returns the HTTP Status code 200.

If the request fails, the API issues an exception and returns other HTTP Status Codes.

If the request exceeds 50,000 events, the API returns an error.

Example

The following example is a Security Events API request and response, which includes examples of both successful and failed responses. Replace the placeholders below with actual values.

Request Header

Content-Type: `application/json;odata.metadata=none`

Authorization: `Archer session-id="session token ID from login"`

Accept:
`application/json,text/html,application/xhtml+xml,application/xml;q=.9,*/*;q=0.8`

X-Http-Method-Override: `GET`

Request Body Example

```
{
      "InstanceName":"Archer",
      "EventType": "all events",
      "EventsForDate": "2021-06-17"
}
```

Response Examples

Security Events Report API successful response


```
{
      "Links": [],
      "RequestedObject": [
            {
                  "Event": "User Login",
                  "InitiatingUser": "Administrator, System ",
                  "Timestamp": "2021-06-17T01:36:46.023",
                  "EventDetails": "Account: Administrator, System "
            },
            {
                  "Event": "User Login",
                  "InitiatingUser": "Administrator, System ",
                  "Timestamp": "2021-06-17T01:59:54.73",
                  "EventDetails": "Account: Administrator, System "
            },
            {
                  "Event": "User Login",
                  "InitiatingUser": "Administrator, System ",
                  "Timestamp": "2021-06-17T10:46:42.333",
                  "EventDetails": "Account: Administrator, System "
            }
      ],
      "IsSuccessful": true,
      "ValidationMessages": []
}
```


Security Events Report API failure response

This API request failed due to an invalid parameter, All vents, where Events is misspelled.


```
{
      "Links": [],
      "RequestedObject": null,
      "IsSuccessful": false,
      "ValidationMessages": [
            {
                  "Reason": "",
                  "Severity": 3,
                  "MessageKey": "InvalidRequestPage:InvalidRequest",
                  "Description": "The request contains invalid
parameter value: All vents",
                  "Location": -1,
                  "ErroredValue": null,
                  "Validator": "Validation",
                  "XmlData": null,
```

```
                "ResourcedMessage": "Invalid Request"
            }
        ]
}
```