MCAS REST API for Sentinel Playbooks

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

[Pending Review]

MCAS REST API for Sentinel Playbooks

Token

The authentication for MCAS REST API is handled via API tokens.

To use the API Token when making a request to the MCAS REST API, you need to an Authorization Header in this format,

KEY	VALUE
Authorization	Token <API Token>

URL

The URL provided by MCAS when creating an API Token gets re-directed when accessed. In Postman this redirection is handled seamlessly, but in a Azure Logic App it returns a HTTP 301 error. Removing the datacenter designation from the URL provides the actual URL that it is redirected to. For example, if MCAS provides the URL, https://<domainname>.eu2.portal.cloudappsecurity.com then from a Logic App the URL needs to be specified like this https://<domainname>.portal.cloudappsecurity.com

To GET alerts, the URL would therefore be,

- https://<domainname>.portal.cloudappsecurity.com/api/v1/alerts

It was also found that to resolve or dismiss alert, a "/" had to be added to the end of the URL. The URLs would therefore look like this,

- https://<domainname>.portal.cloudappsecurity.com/api/v1/alerts/resolve/
- https://<domainname>.portal.cloudappsecurity.com/api/v1/alerts/<alertid>/dismiss/

Useful Links

- Cloud App Security REST API
- HOWTO: Query REST API For Bulk Alert Resolve using Postman