Splunk® Enterprise Security REST API Reference 6.6.0

The Splunk Enterprise Security API

Generated: 7/23/2021 11:44 am

The Splunk Enterprise Security API

Splunk Enterprise Security offers a set of REST API endpoints that you can use to interact with the Splunk Enterprise Security frameworks programmatically or from Splunk search. These API endpoints are for Splunk Enterprise Security admins and for developers who are building integration applications for use with Splunk Enterprise Security.

The Splunk Enterprise Security REST API provides methods for accessing selected features in the Enterprise Security framework. The API follows the principles of Representational State Transfer (REST).

There are REST API access and usage differences between Splunk Cloud Platform and Splunk Enterprise. If you are using Splunk Cloud Platform, see Using the REST API with Splunk Cloud Platform in *REST API Tutorials*.

Navigate to specific endpoints and review available REST operations.

URI	Summary	GET	PUT	POST	DEL
Threat Intelligence endpoints					
/data/threat_intel/upload	Upload a threat intelligence file in STIX, IOC, or CSV format.				
/services/data/threat_intel/item/{threat_intel_collection}	Create or list rows in a threat intelligence collection.				
/services/data/threat_intel/item/{threat_intel_collection} /{item_key}	List, update, or delete a row in a threat intelligence collection.				
Notable Event endpoints					
/services/notable_update	Modify notable events.				
Analytic Story endpoints					
/services/analyticstories/configs/{stanza_type}	Acts as a proxy to configs/conf-analyticstories, with validation.				
/services/analyticstories/configs/{stanza_type}/{name}	Acts as a proxy to configs/conf-analyticstories/{stanza_name}.				
/services/analyticstories/configs/{stanza_type}/{name}/acl	Returns ACL information.				
/services/analyticstories/configs/{stanza_type}/{name}/move	Moves stanzas to other apps.				
/services/analyticstories/configs/_reload	Reloads data for the endpoint.				
/services/analyticstories/schemas/{version}	Reloads data for the endpoint.				
/services/analyticstories/batch	Takes a JSON array conforming to the analytic story JSON schema and saves it in proper format into analyticstories.conf.				