RiskIQ PassiveTotal Splunk App Installation and Configuration Guide

Document Details

Document Version	Date	Owners	Comments
1.0.0	27 May 2020	Crest Data Systems	Initial Draft
1.1.0	4th Sept 2020	Crest Data Systems	● Removed API Limit error message feature across dashboards. ● Added Cookies and Services tab in dashboards. ● Added Pull Indicators dashboard. ● Added data collection for HostAttribute Cookies.and Services. ● Added custom command rptcookies. rptservices and rptpullindicators.

Introduction

The RiskIQ PassiveTotal App for Splunk has a Search History Dashboard to visualize Search History (Personal and Team Search History), Live Investigation Dashboard and Local Investigation Dashboard to match experience similar to RiskIQ PassiveTotal Community UI where events are coming live from RiskIQ PassiveTotal API and from Splunk index on which bulk enriched data is collected by Add-on respectively. All dashboards will use various custom commands from Add-on to populate data.

The RiskIQ PassiveTotal Add-on for Splunk is useful for Bulk Enrichment of uploaded indicators (IP/Domain) provided in CSV files. It also has various useful custom commands, including each for a tab shown in RiskIQ PassiveTotal Community UI.

Compatibility Matrix

Browser	Google Chrome, Mozilla Firefox
OS	CentOS Linux, Windows
Splunk Enterprise Version	8.0.x, 7.3.x, 7.2.x
Supported Splunk Version	Splunk Cloud, Single-instance and Distributed Deployment
RiskIQ PassiveTotal API Version	2

System Requirement

The basic system requirements for the RiskIQ PassiveTotal Splunk integration App and Add-on are the same as the basic requirements of Splunk deployment. Please refer to this (Reference) to find the hardware and software details

- Intel x86 64-bit chip architecture
- 12 CPU cores at 2Ghz or greater speed per core
- 12GB RAM
- Standard 1Gb Ethernet NIC, optional second NIC for a management network
- Standard 64-bit Linux or Windows distribution

Installation of RiskIQ PassiveTotal App and Add-on for Splunk

The Add-on and App can be installed in three different ways:

- Go to **Apps > Manage Apps > Browse more apps**. Search for “RiskIQ PassiveTotal” and from the list select “RiskIQ PassiveTotal App for Splunk” and “RiskIQ PassiveTotal Add-on for Splunk”. The Splunk VM requires internet access for this way of App installation.
- Download the App and Add-on from Splunkbase. The App and Add-on can be installed either:
    - Through the Splunk user interface from **Apps > Manage Apps > Install the app from file**. Upload the downloaded file.
    - By extracting the compressed file (TA-riskiq-passivetotal-xx-x.x.x-x.tar.gz) and (passivetotal-xx-x.x.x-x.tar.gz) into the $SPLUNK_HOME$/etc/apps folder.

Note: Splunk restart is required after App and Add-on installation.

Standalone Splunk Deployment

If you have a standalone Splunk deployment, you can install the App and Add-on on a single Splunk instance (Reference). If you are going to install the RiskIQ PassiveTotal App for Splunk, it is mandatory to have the Add-on installed as well because the App fully depends on Add-on for its all functionality.

Distributed/Cluster Splunk Deployment

If you are deploying RiskIQ PassiveTotal App for Splunk on a distributed setup, the following are the changes needed on each type of node: (Reference)

	Add-On	**App**
Heavy Forwarder	Yes	-
Indexer/Indexer Cluster	-	-
Search Head/Search Head Cluster	Yes	Yes

Note: Configure Add-on on Search Head Deployer and then push it on Search Head Cluster. This step is required only for Live Investigation Dashboard and Search History Dashboard in App.

Splunk Cloud

Reference

Upgrade

Follow the below steps when upgrading from RiskSense App for Splunk.

- From the UI navigate to **Apps > Manage Apps**.
- In the top right corner select the **Install app from file**.
- Select **Choose File** and select the App package.
- Check the upgrade option.
- Select **Upload** and follow the prompts.
- Remove default.xml from $SPLUNK_HOME/etc/apps/passivetotal/local/data/ui/nav, if found from the backend.
- Restart Splunk.

Configuration of RiskIQ PassiveTotal Add-on for Splunk

The configuration pages for RiskIQ PassiveTotal Add-on for Splunk are only accessible by the user with admin_all_objects capability. In Splunk by default, the user having the admin role will have admin_all_objects capability.

Configure Account

Note: This Add-on supports HTTPS connection and SSL check for communication between Splunk and RiskIQ PassiveTotal out of the box. To configure the RiskIQ PassiveTotal details, please follow the below steps:

To Add/Update Account:

1. Go to **RiskIQ PassiveTotal Add-on for Splunk > Configuration > PassiveTotal Account**
2. Add/Update following PassiveTotal Account Credentials.

Parameters	Type	Description
Username/Email	Textbox	Username/Email of PassiveTotal Account.
API Key	Textbox	API key of PassiveTotal Account.

3. **Save** it.

Proxy Page

A user can configure proxy settings for RiskIQ PassiveTotal Add-on through this page.

1. Go to **RiskIQ PassiveTotal Add-on for Splunk > Configuration > Proxy**.
2. Add the **Proxy Type, Host, Port, Username,** and **Password.** Select the **Enable** checkbox and **Save** the details.

Logging Page

A user can configure the logging level for RiskIQ PassiveTotal Add-on through this page.

1. Go to **RiskIQ PassiveTotal Add-on for Splunk > Configuration > Logging**.
2. Select the **Log Level** from the drop-down and **Save** it.

Upload Indicator Page

For Bulk Enrichment of indicators (IP/Domain), follow below steps:

Sample CSV Format
Note: The header of the CSV file will be ignored, so it could be anything.

Indicators
abc.com
1.x.x.1
pqr.com
2.x.x.2

- To upload Indicators, go to the Upload Indicators page. Click Choose File and select CSV file from the local system. Click on Upload, It will save file and will automatically create modular input in disabled mode with the same name as CSV File.

- Users can enable/disable/edit/delete Modular Input by selecting specific Action on Inputs Section.

Inputs Page

NOTE: If the user has successfully uploaded a CSV file in the **Upload Indicators** page, then a Modular Input with the same name as CSV has been created automatically and should appear here.

Users can enable/disable/edit/delete Modular Input by selecting specific Action.

Configure Inputs

A user can see and configure inputs through **RiskIQ PassiveTotal Add-on for Splunk > Inputs**.

To Edit an Input

1. Find the Input (Input name will be the same as the CSV you uploaded) you want to edit from the list of configured inputs.
2. Click on **Action > Edit**
3. Update the following parameters in the dialog box.
4. Click on Save.

Parameters	Type	Description
Interval	Textbox	Modular Input invocation in Seconds or Cron
Index	Textbox	The index in which bulk enriched data will be collected
Dataset	Multi-valued Dropdown	Type of Datasets to collect out of Passive DNS, Whois, Certificates, Subdomains, Trackers, Components, Hostpairs Cookies, Services, OSINT, Hashes, or Tags.

To Enable an Input

1. Find the input you want to **Enable** from the list of inputs.
2. Click on **Action > Enable**

To Disable an Input

3. Find the input you want to **Disable** from the list of inputs.
4. Click on **Action > Disable**

To Delete an Input

5. Find the input you want to **Delete** from the list of inputs.
6. Click on **Action > Delete**

Note: If you are collecting data in a custom index, then follow the steps shown in the Troubleshooting Section, to set the custom index to a default one.

Configuration of RiskIQ PassiveTotal App for Splunk

The App does not require any specific configuration, but in case of the customized configuration of the RiskIQ PassiveTotal Add-on for Splunk, the role of all users should be updated. Refer.

Data Retention Policy

To control the amount of data in particular index, use below settings in $SPLUNK_HOME/etc/apps/TA-riskiq-passivetotal/local/indexes.conf for your index.

- **frozenTimePeriodInSecs = Time in seconds for which data should remain in index**
- **maxDataSize = 750**
- **maxHotBuckets = 1**

Ex. Use below settings for keeping 1 day data in index `my_test_index`

[my_test_index]

frozenTimePeriodInSecs = 86400

maxDataSize = 750

maxHotBuckets = 1

RiskIQ PassiveTotal Splunk Integration Architecture

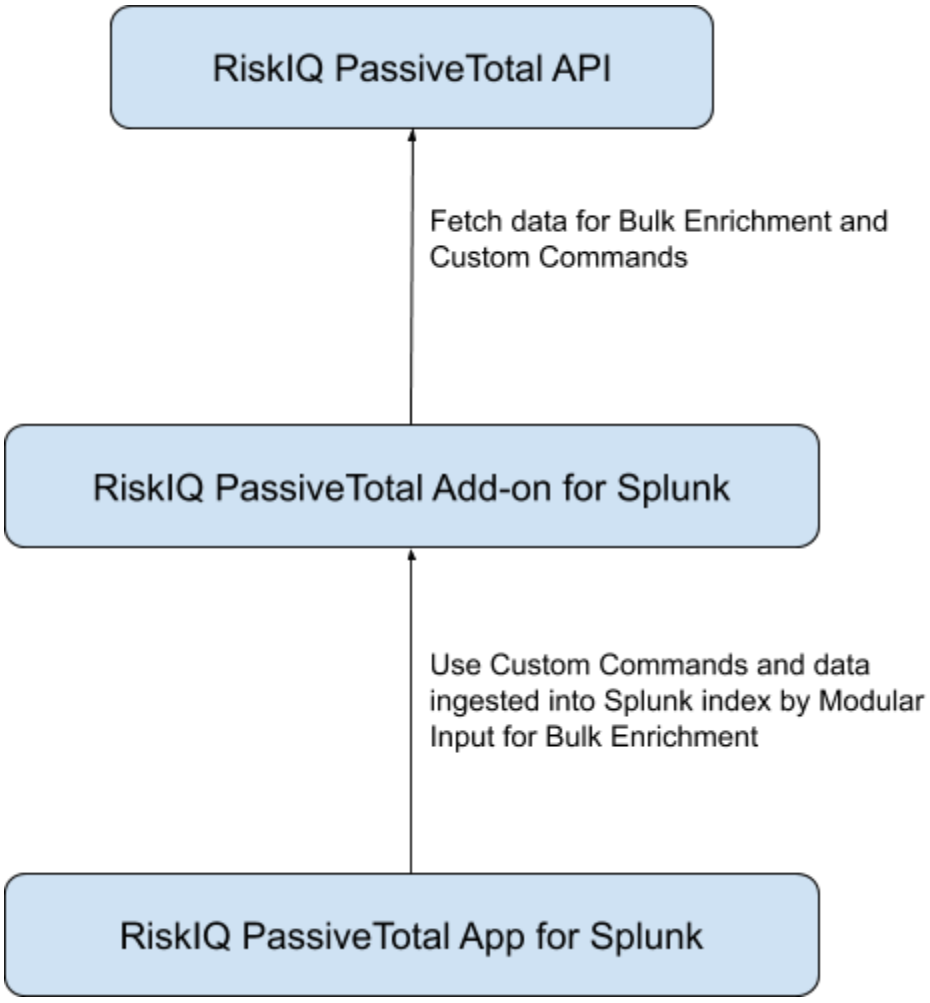
The diagram below demonstrates how Splunk integration for RiskIQ PassiveTotal works. The Splunk integration is divided into two standard parts: Add-on and App.

1. **RiskIQ PassiveTotal Add-on for Splunk**

The RiskIQ PassiveTotal Add-on collects the data from the RiskIQ PassiveTotal platform to ingest into Splunk for bulk enrichment of uploaded indicators and also for custom commands.

2. **RiskIQ PassiveTotal App for Splunk**

The RiskIQ PassiveTotal App contains ready to use dashboards which are built on the basis of the data collected by the RiskIQ PassiveTotal Add-on for Splunk.



Uninstalling RiskIQ PassiveTotal App and Add-on for Splunk

The RiskIQ PassiveTotal App and Add-on can be either disabled or completely uninstalled based on the requirement.

Disabling the App and Add-on

To disable the App and Add-on, you must be logged in to Splunk as an Administrator and follow the steps below.

1. Click the App name in the title bar, and then click Manage Apps.
2. In the search box, type the name of the app, and then click Search. In the Status column, next to both the App and Add-on, click Disable.

Uninstalling the App and Add-on

Follow these instructions based on your environment.

Uninstalling from a Standalone Environment

1. Disable the App and Add-on from Splunk user interface as detailed above.
2. Log in to the Splunk machine from the backend and delete the App and Add-on folders. The app and its directory are typically located in $SPLUNK_HOME/etc/apps/<appname>.
3. Verify that no local configuration files related to RiskIQ PassiveTotal App/Add-on are available in the $SPLUNK_HOME/etc/system and $SPLUNK_HOME/etc/users folders. If the local folder is present, remove it as well.
4. Restart Splunk.

Uninstall from a distributed or clustered environment

In a cluster or distributed environment, the RiskIQ PassiveTotal App is installed on all the Search Heads and the RiskIQ PassiveTotal Add-on is installed on Search Heads and Forwarders.

The steps to uninstall the App and Add-on are the same as for Standalone.

1. To perform any installation or uninstallation step on all the search nodes of a distributed environment, use a deployer manager.
2. From the deployer machine, go to $SPLUNK_HOME$/etc/shcluster/apps and remove the App and Add-on folders and execute cluster bundle command. Refer

Splunk Knowledge Objects

Sourcetypes

The RiskIQ PassiveTotal Add-on for Splunk provides the search-time knowledge for RiskIQ PassiveTotal data in the following formats:

Sourcetype	Endpoint	Description
riskiq:passivetotal:passivedns	/dns/passive	Passive DNS - Get Passive DNS data for the specified query
riskiq:passivetotal:whois	/whois	Retrieves the WHOIS data for the specified query
riskiq:passivetotal:certificates	/ssl-certificate/history	Retrieves the SSL certificate history for a given certificate SHA-1 hash or IP address.
riskiq:passivetotal:subdomains	/enrichment/subdomains	Get subdomains data for the specified query
riskiq:passivetotal:trackers	/host-attributes/trackers	Retrieves the host attribute trackers data for the specified query
riskiq:passivetotal:components	/host-attributes/components	Retrieves the host attribute components data for the specified query
riskiq:passivetotal:hostpairs	/host-attributes/pairs	Retrieves the host attribute pairs data for the specified query
riskiq:passivetotal:cookies	/host-attributes/cookies	Retrieves cookie data for a particular domain/IP
riskiq:passivetotal:services	/services	Retrieves all services for a particular IP
riskiq:passivetotal:tags	/actions/tags	Retrieves tags data for a given artifact.
riskiq:passivetotal:hashes	/enrichment/malware	Retrieves the Hashes data for the specified query
riskiq:passivetotal:osint	enrichment/osint	Get osint data for a specified query

Custom Commands

The RiskIQ PassiveTotal Add-on for Splunk provides the following Custom commands which will fetch live data from PassiveTotal Platform using it's REST API.

Note: Non-admin users are not allowed to run custom commands.

Custom Command	**Parameters**	**Description**
rptresolutions	query=<IPAddress/ Hostname>	Executes a Resolutions DNS query.
rptwhoissearch	field=<domain/organization/email/phone/address/nameserver/name>	Executes a WHOIS query on a given field.
	query=<IPAddress/ Hostname>	
rptwhois	query=<IPAddress/ Hostname>	Executes WHOIS query.
rptcertificates	field=<field on which to search (default: name)>	Executes a Certificates query on a given field.
	query=<IPAddress/ Hostname>	
rptsubdomains	query=<IPAddress/ Hostname>	Executes a Subdomains query.
rpttrackers	query=<IPAddress/ Hostname>	Executes a Trackers query.
rpttrackerssearch	type=<Type of tracker>	Executes a Trackers query with give type.
	query=<IPAddress/ Hostname>	
rptcomponents	query=<IPAddress/ Hostname>	Executes a Components query.

rpthostpairs	direction=<children/ parents/pairs (default: pairs)>	Executes a Host Pairs query.
	query=<IPAddress/ Hostname>	
rptcookies	query=<IPAddress/ Hostname>	Executes a cookie query.
rptservices	query=<IPAddress>	Executes a services query.
rptosint	query=<IPAddress/ Hostname>	Executes a OSINT query.
rpthashes	query=<IPAddress/ Hostname>	Executes a Hashes query.
rptdns	query=<IPAddress/ Hostname>	Executes a passive DNS query.
rpthistory	-	Executes a search history.
rptteamstream	-	Executes a team search history.
rptpullindicators	field="field1,field2" type="<endpoint>"	Fetches data for the fields mentioned from the given endpoint

Following Custom commands are for Backward Compatibility:

Custom Command	**Parameters**	**Description**
ptpdns	query=<IPAddress/ Hostname>	Executes a passive DNS query.
	earliest=<epoch time>	
	latest=<epoch time>	
ptupdns	query=<IPAddress/ Hostname>	Executes a passive DNS query for unique resolutions.
	earliest=<epoch time>	

	latest=<epoch time>	
ptssl	query=<IPAddress/ Hostname>	Executes a passive SSL query.
ptwhois	query=<IPAddress/ Hostname>	Executes a WHOIS query.
ptenrich	query=<IPAddress/ Hostname>	Executes an Enrichment query.
pttrackers	query=<IPAddress/ Hostname>	Executes a Trackers query.
pthostpairs	query, direction	Executes a Host Pairs query.
ptcomponents	query=<IPAddress/ Hostname>	Executes a Components query.
pthistory	query=<IPAddress/ Hostname>	Executes a History query.

Troubleshooting

App Configuration Issues

Local Investigation Dashboard is showing no results, even though custom commands show results when running directly on Splunk Search.

If you are collecting bulk enrichment data in the custom index, then Local Investigation Dashboard won't show any results, as it only searches in default indexes. To make the custom index a default one, follow the below steps:

1. Go to Splunk's Settings → Roles (USERS AND AUTHENTICATIONS)
2. Edit the specific role that the user has
3. In Indexes section, add the custom index into default indexes
4. Save it

Note: In a Distributed Environment, if you are using a custom index in Add-on to collect data for Bulk Enrichment, then the same custom index needs to be created on Search Heads as well and then add it into default indexes of Search Heads as shown above. In the case of Search Head Cluster, you can perform this step on one of the Search Heads.

Add-on Configuration Issues

Splunk search showing empty results (blank events)

- The number of events displayed in the Splunk search timeline is configurable by a parameter called `max_events_per_bucket`.
- Setting this parameter to higher value, will show more events in the timeline. The default value is 1000.
- To change this parameter follow below steps:
- Open/Create limits.conf under `$SPLUNK_HOME/etc/system/local/` folder.
- Create a stanza `[search]` if not already present.
- Add `max_events_per_bucket=<some higher number>` in `[search]` stanza.
- Save the file and restart Splunk.

The input or configuration page is not loading.

- Check log file for possible errors/warnings: $SPLUNK_HOME/var/log/splunk/splunkd.log

Data is not getting collected in Splunk for Bulk Enrichment

- Verify that such events exist on the RiskIQ PassiveTotal platform.
- Check the log file related to Bulk Enrichment that is generated under $SPLUNK_HOME/var/log/splunk/ta_riskiq_passivetotal_indicators.log.
- To get the detailed logs, in the Splunk UI, navigate to RiskIQ PassiveTotal Add-on For Splunk. Click on Configuration and go to the Logging tab. Select the Log level to DEBUG.
- Check the logs. They will be more verbose and will give the user insights on data collection.
- Disable/Enable the input to restart the enrichment process.

Splunk Monitoring Console

- Check the Monitoring Console (>=v6.5) for errors

If the Splunk Instance is behind a proxy, Configure Proxy settings by navigating to RiskIQ PassiveTotal Add-on for Splunk → Configuration → Proxy

Field Extraction Issues

1. Verify that the add-on is installed properly in the Splunk environment.
2. Verify that the source & sourcetype of the data is according to the list of sourcetype mentioned.
3. Check the data is being collected by the RiskIQ PassiveTotal Add-on for Splunk in the Specified index.