RiskIQ Security Intelligence Service Add-on Installation and Configuration Guide

May 2020

Document Details

Document Version	Date	Owners	Document Status	Comments
1.0.0	20 May 2020	Crest Data Systems	Draft - v1	Initial Draft

Document Details 2

Introduction 5

Compatibility Matrix 5

System Requirement 5

Download 5

Installation of RiskIQ Security Intelligence Service Add-on for Splunk 6
- Standalone Splunk Deployment 6
- Distributed/Cluster Splunk Deployment 6
- Splunk Cloud 6

Configuration of RiskIQ Security Intelligence Service Add-on for Splunk 7
- Configure Account 7
  - Pre-Flight Checks: 7
    - Data collection from RiskIQ-AWS S3 Buckets 7
  - To add Account: 7
  - To update a Account: 8
  - To remove a Account: 8
- Proxy Page 8
- Logging Page 8
- Inputs Page 9
- Configure Inputs 9
  - To Add an Input: 9
  - To Disable an Input: 10
  - To Enable an Input: 10
  - To Edit an Input: 10

Uninstalling RiskIQ Security Intelligence Service Add-on for Splunk 11
- Disabling the Add-on 11
- Uninstalling the Add-on 11
  - Uninstalling from a Standalone Environment 11
  - To uninstall from a distributed or clustered environment: 11

Splunk Knowledge Objects 12
- Index 12
- Sourcetypes 12
- Data Retention Policy 12
- Add Index To Role 13

Troubleshooting 13
  - Add-on Configuration Issues 13

The input or configuration page is not loading. 13
Account and Inputs are configured but data doesn't appear in Splunk search or Dashboard 13
Data is not getting collected in Splunk 13
Splunk Monitoring Console 14
If the Splunk Instance is behind a proxy, Configure Proxy settings by navigating to RiskIQ Security Intelligence Service Add-on for Splunk -> Configuration -> Proxy 14
Data Collection Monitoring Dashboard 14
Field Extraction Issues 14

Introduction

The RiskIQ Security Intelligence Service Add-on for Splunk is useful for data collection of Newly Observed Domain, Newly Observed Host, Malware Blacklist, Phishing Blacklist, Scam Blacklist and Content Blacklist data files from RiskIQ-AWS S3 Buckets. Add-on is also useful in transforming and parsing data. Add-on contains a Data Collection Monitoring dashboard which provides an overview of the data that has been collected.

Compatibility Matrix

Browser	Google Chrome, Mozilla Firefox
OS	CentOS Linux, Windows
Splunk Enterprise Version	8.0.x, 7.3.x, 7.2.x, 7.1.x
Supported Splunk Version	Splunk Cloud, Single-instance and Distributed Deployment

System Requirement

The basic system requirements for the RiskIQ Security Intelligence Service Add-on is the same as the basic requirements of Splunk deployment. Please refer to this (Reference) to find the hardware and software details to set up as per your requirements.

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

Download

You can download RiskIQ Security Intelligence Service Add-on For Splunk from Splunkbase.

Installation of RiskIQ Security Intelligence Service Add-on for Splunk

The Add-on can be installed via three different ways:

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

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

Standalone Splunk Deployment

If you have a standalone Splunk deployment, you can install the Add-on on a single Splunk instance. (Reference)

Distributed/Cluster Splunk Deployment

If you are deploying RiskIQ Security Intelligence Service Add-on for Splunk on a distributed setup, the following are the changes needed on each type of node: (Reference)

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

Splunk Cloud

Reference

Configuration of RiskIQ Security Intelligence Service Add-on for Splunk

The configuration pages for RiskIQ Security Intelligence Service 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

Pre-Flight Checks:

Data collection from RiskIQ-AWS S3 Buckets

Please note that This Add-on supports HTTPS connection and SSL check for communication between Splunk and RiskIQ-AWS S3 out of the box. To configure the RiskIQ-AWS S3 details, please follow the below steps:

To add Account:

1. Go to **RiskIQ Security Intelligence Service Add-on for Splunk > Configuration > Account**
2. Select **Add** from the top right corner.
3. Add a unique **Account Name**, provide the **RiskIQ-AWS AccessKeyId**, **RiskIQ-AWS SecretKey,** and Select **Data Types** from Multi-Valued Dropdown for which you want to collect data files from S3 Buckets.

Parameters	Type	Description
Account Name	Textbox	Unique name for the Account. This will be used for Splunk purpose to fetch the credentials from passwords.conf
RiskIQ-AWS AccessKeyId	Textbox	AccessKeyId of RiskIQ-AWS Account
RiskIQ-AWS SecretKey	Password Textbox	SecretKey of Provided AccessKeyID for RiskIQ-AWS Account
Data Types	Multi-valued Dropdown	Types of data files which need to be collected from RiskIQ-AWS S3 Buckets

4. **Add** the Account.

- Once The Account is added. The list of all the added Accounts is visible on the **Configurations** page.
- On successful configuration of Account, Modular Inputs will be created automatically for selected data types in **Disabled** mode under Inputs page.
- While configuring the Account, if the user has not access to the S3 buckets of selected data types then Access denied for <data types> message will be shown.

To update a Account:

1. Go to **RiskIQ Security Intelligence Service Add-on for Splunk > Configuration > Account**
2. Find the system you want to **Edit** from the list of configured accounts.
3. Click on **Action > Edit**
4. Update the required parameters in the dialog box.
5. Click on Save.

To remove a Account:

Note: Before removing the Account make sure none of the Inputs are using the account you want to remove.

1. Go to **RiskIQ Security Intelligence Service Add-on for Splunk > Configuration > Account**
2. Find the system you want to **Remove** from the list of configured accounts.
3. Click on **Action > Delete**.

Proxy Page

A user can configure proxy settings for RiskIQ Security Intelligence Service Add-on through this page.

1. Go to **RiskIQ Security Intelligence Service 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 Security Intelligence Service Add-on through this page.

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

Inputs Page

Below list of Inputs are available for data collection on the **Inputs** page for the newly created system.

1. RiskIQ Security Intelligence Service Input

NOTE: If the user has successfully performed the **Account Configuration** step, then Modular Inputs for selected Data Types has been created automatically and should appear here in **Disabled** Mode.

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

Users can manually create Modular Input by clicking on the **Create New Input button** provided on top right.

Configure Inputs

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

To Add an Input:

1. Go to **RiskIQ Security Intelligence Service Add-on for Splunk > Input**.
2. Select **Create New Input** from the top right corner.
3. Provide required parameters for Input Configuration and **Add** the Input

RiskIQ Security Intelligence Service Input

Parameters	Type	Description
Name	Textbox	Name of the input.
Interval	Textbox	Modular Input invocation in Seconds
Index	Dropdown	The index in which data will be collected
Data Type	Dropdown	Type of data which you want to collect
Collect Data For	Dropdown	How many days of data you want to collect for the first time.
RiskIQ-AWS Account	Dropdown	Account configured from “Accounts” Page

To Disable an Input:

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

To Enable an Input:

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

To Edit an Input:

1. Go to **RiskIQ Security Intelligence Service Add-on for Splunk > Inputs**
2. Find the Input you want to edit from the list of configured inputs.
3. Click on **Action > Edit**
4. Update the required(desired) parameters in the dialog box.
5. Click on Save.

Note: If you are collecting data in a custom index then follow below steps:

- Add a custom index to Role for Splunk default search. Reference

Uninstalling RiskIQ Security Intelligence Service Add-on for Splunk

The RiskIQ Security Intelligence Service Add-on can be either disabled or completely uninstalled based on the requirement.

Disabling the Add-on

To disable the Add-on, you must be logged into 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 the Add-on, click Disable.

Uninstalling the Add-on

Follow these instructions based on your environment.

Uninstalling from a Standalone Environment

1. Disable the Add-on from Splunk user interface as detailed above.
2. Log in to the Splunk machine from the backend and delete the Add-on folder. The Add-on and its directory are typically located in $SPLUNK_HOME/etc/apps/<appname>.
3. Verify that no local configuration files related to RiskIQ Security Intelligence Service 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.

To uninstall from a distributed or clustered environment:

In a cluster or distributed environment, the RiskIQ Security Intelligence Service Add-on is installed on Search Heads and Forwarders.

The steps to uninstall the 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 Add-on folders and execute cluster bundle command. Refer

Splunk Knowledge Objects

Index

The data gets indexed into the index, which was selected while configuring the input on Splunk. If User has configured data collection in a custom index, follow below steps

- Add a custom index to Role for Splunk default search. Reference

NOTE: You must create the index before starting the data collection.

Sourcetypes

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

Sourcetype	Bucket	Data File
riskiq:sis:domain	sis-new-observations	Newly Observed Domain
riskiq:sis:host	sis-new-observations	Newly Observed Host
riskiq:sis:malware	riq-sis-blacklist-malware	Malware Blacklist
riskiq:sis:phish	riq-sis-blacklist-phish	Phishing Blacklist
riskiq:sis:scam	riq-sis-blacklist-scam	Scam Blacklist
riskiq:sis:content	riq-sis-blacklist-content	Content Blacklist

Data Retention Policy

To control the amount of data in particular Index, use below settings in $SPLUNK_HOME/etc/apps/TA-riskiq-security-intelligence-service/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
```

Add Index To Role

To add your custom index to default search, navigate to

1. Settings -> Roles
2. Create/Select the role -> Click the indexes tab
3. Search for you custom index -> Check the Default checkbox
4. Save it

Troubleshooting

Add-on Configuration Issues

The input or configuration page is not loading.

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

Account and Inputs are configured but data doesn't appear in Splunk search or Dashboard

- One of the possible causes for this problem is when a user has selected a different index to collect data. Splunk by default searches inside the **main** index.
- To add your custom index to default search, navigate to Settings -> Roles -> Select the role -> Click the indexes tab -> Search for you custom index -> Check the Default checkbox -> Save

Data is not getting collected in Splunk

- Go to the Search tab. Hit the following query index=_internal sourcetype=tariskiqsecurityintelligenceservice:log and check the results.
- Verify the configured Modular Inputs are valid and such files exist in the Bucket.
- Check the log file related to data collection is generated under $SPLUNK_HOME/var/log/splunk/ta_riskiq_security_intelligence_service_*.log.

- To get the detailed logs, in the Splunk UI, navigate to RiskIQ Security Intelligence Service Add-on For Splunk. Click on Configuration and go to the Logging tab. Select the Log level to DEBUG. Reference
- Disable/Enable the input to recollect the data.
- Check the logs. They will be more verbose and will give the user insights on data collection.

Splunk Monitoring Console

- Check the Monitoring Console (>=v6.5) for errors
- Visit the Application Health dashboard

If the Splunk Instance is behind a proxy, Configure Proxy settings by navigating to RiskIQ Security Intelligence Service Add-on for Splunk -> Configuration -> Proxy

Data Collection Monitoring Dashboard

Users can use the Data Collection Monitoring dashboard to get the overview of the data that has been collected by the Add-on over time.
Below Panels are available in the RiskIQ Security Intelligence Service Add-on For Splunk -> Data Collection Monitoring Dashboard

- Data Collected By Type In MB
- Events Collected By Sourcetype
- Events Collected Over Time

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 Security Intelligence Service Add-on for Splunk in the Specified index.