kaspersky_app Documentation

Release 2019

Diogo Silva

Oct 14, 2019

Contents:

1 Release Notes 1

2 Requirements 3

3 Installation 5

4 Support 7

5 Indices and tables 9

CHAPTER 1

Release Notes

1.1 v1.1.0 - October 2019

- Small fixes
- Dashboard improvements

1.2 v1.0.0 - August 2019

- Public release to Splunkbase

CHAPTER 2

Requirements

- Kaspersky Security Center 10 or newer
- Splunk 7.0 or newer
- Kaspersky Add-on for Splunk

CHAPTER 3

Installation

3.1 Install the Kaspersky App for Splunk

- Get the Kaspersky App for Splunk by downloading it from Splunkbase or browsing to it using the app browser within Splunk Web.
- Determine where and how to install this add-on in your deployment, using the tables on this page.
- Perform any prerequisite steps before installing, if required and specified in the tables below.
- Complete your installation.

3.1.1 Distributed deployments

Reference the tables below to determine where and how to install this app in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the app, you may need to install the app in multiple places.

Where to install this app

Unless otherwise noted, all supported apps can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in Splunk Add-ons for more information.

This table provides a reference for installing this specific app to a distributed deployment of Splunk Enterprise.

Splunk platform component	Supported	Required	Comments
Search Heads	Yes	Yes	Install this app to all search heads.
Indexers	No	No	
Heavy Forwarders	No	No	
Universal Forwarders	No	No	

Distributed deployment compatibility

This table provides a quick reference for the compatibility of this app with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this app on a search head cluster for all search-time functionality.
Indexer Clusters	No	
Deployment Server	Yes	Supported for deploying via Deployment server

3.1.2 Installation walkthroughs

The Splunk Add-Ons manual includes an Installing add-ons guide that helps you successfully install any add-on to your Splunk platform. For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

CHAPTER 4

Support

4.1 Bugs & Support Issues

You can file bug reports on our GitHub issue tracker, and they will be addressed as soon as possible. **Support is a volunteer effort**, and there is no guaranteed response time.

CHAPTER 5

Indices and tables

- genindex
- modindex
- search