
Levono IMM Add-on for Splunk Documentation

Release 0.1.0

Diogo Silva

Sep 27, 2019

Contents:

1	Introduction	1
2	Requirements	3
3	Installation	5
4	Configuration	7
5	Troubleshooting	9
6	Support	11
7	Indices and tables	13

CHAPTER 1

Introduction

CHAPTER 2

Requirements

- Splunk 7.0 or newer
- Lenovo IMM

3.1 Install the Lenovo IMM Add-on for Splunk

- Get the Lenovo IMM Add-on 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 add-on 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 add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons 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 add-on to a distributed deployment of Splunk Enterprise.

Splunk platform component	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads.
Indexers	Yes	Optional	Required for the parsing operations (e.g. fixing timestamp) if the data is not coming from a heavy forwarder.
Heavy Forwarders	Yes	Yes	Required for the parsing operations (e.g. fixing timestamp).
Universal Forwarders	No	No	This add-on requires either a heavy forwarder or an indexer for the parsing operations (e.g. fixing timestamp).

Distributed deployment compatibility

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

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality.
Indexer Clusters	Yes	You can install this add-on on a indexer cluster for all index-time functionality.
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](#)

4.1 Splunk

- Configure a new index (e.g. imm) for the new logs

4.1.1 Receiving syslogs on Splunk

NOTE: Its recommended to use a separate and dedicated syslog solution (e.g. rsyslog, syslog-ng, etc) - Configure new UDP port (e.g. 514) pointing to the new index using the “lenovo:imm” sourcetype

4.1.2 Monitoring log files

- Configure a new file monitor input pointing to the new index using the “lenovo:imm” sourcetype

4.2 Lenovo IMM

- Configure syslog outputs

For more information please refer to the [Lenovo IMM documentation](#) or [Lenovo IMM user guide](#).

CHAPTER 5

Troubleshooting

6.1 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 7

Indices and tables

- `genindex`
- `modindex`
- `search`