# Splunk® Supported Add-ons
# Splunk Add-on for McAfee ePO Syslog released

Generated: 11/05/2022 11:55 am

# Table of Contents

# Overview

## Splunk Add-on for McAfee ePO Syslog

| | |
|---|---|
| Version | 1.1.0 |
| Vendor Products | • McAfee Endpoint ePO v5.10<br>• McAfee Endpoint Security<br>♦ v10.6.0<br>♦ v10.6.1<br>♦ v10.6.1.1607<br>♦ v10.7.0<br>♦ v10.7.0.1285<br>♦ v10.7.0.3255 |
| Visible in Splunk Web | No. This add-on does not contain any views. |

The Splunk Add-on for McAfee ePO Syslog lets a Splunk Enterprise administrator collect anti-virus information via Syslog. You can then directly analyze the data or use it as a contextual data feed to correlate with other security data in Splunk. This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk Enterprise apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Download the Splunk Add-on for McAfee ePO Syslog from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release Notes for the Splunk Add-on for McAfee ePO Syslog.

For information about installing and configuring the Splunk Add-on for McAfee, see Install the Splunk Add-on for McAfee ePO Syslog.

## Hardware and software requirements for the Splunk Add-on for McAfee ePO Syslog

### Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements, see System Requirements in the Splunk Enterprise *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

For information about installation locations and environments, see Install the Splunk Add-on for McAfee ePO Syslog.

# Installation

## Install the Splunk Add-on for McAfee ePO Syslog

1. Download the Splunk Add-on for McAfee ePO Syslog at Splunk Add-on for McAfee ePO Syslog from Splunkbase.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the tables below.
4. Complete your installation.

If you need step-by-step instructions on how to install an add-on in your specific deployment environment, see the installation walkthroughs section at the bottom of this page for links to installation instructions specific to Splunk Cloud, distributed deployment, or a single-instance deployment.

### Distributed deployment

Use the tables in this topic 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. 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***

In a distributed deployment, this add-on must be deployed to all tiers in order to use all functionality. 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 the Splunk platform.

| Splunk platform instance type | Supported | Required | Actions required / Comments |
|---|---|---|---|
| Search Heads | Yes | Yes | Install this add-on to all search heads where McAfee ePO Syslog knowledge management is required. |
| Indexers | Yes | No | The add-on must be installed on indexers if you use universal or light forwarders for data collection. |
| Heavy Forwarders | Yes | Yes | If you are using a Heavy forwarder, you must install McAfee ePO Syslog. |
| Universal Forwarders | Yes | See comments | Supported for syslog inputs only. |

***Distributed deployment feature compatibility***

This table describes the compatibility of this add-on with Splunk distributed deployment features.

| Distributed deployment feature | Supported | Actions required / Comments |
|---|---|---|
| Search Head Clusters | Yes | In a distributed deployment, this add-on must be deployed to these tiers in order for all functionality included in the add-on to work. |
| Indexer Clusters | Yes | In a distributed deployment, this add-on must be deployed to these tiers in order for all functionality included in the add-on to work. |
| Deployment Server | Yes | |

| Distributed deployment feature | Supported | Actions required / Comments |
|---|---|---|
| | | In a distributed deployment, this add-on must be deployed to these tiers in order for all functionality included in the add-on to work. |

## Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

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

# Configuration

## Configure inputs using TCP or UDP

Note the following:

- The source type for this add-on is `mcafee:epo:syslog`. See Source types for the Splunk Add-on for McAfee.
- The ports for the add-on must match the ports you specified when you configured the McAfee ePO system for logging. You must enable these inputs using either Splunk Web on your heavy forwarder or by manually editing the `inputs.conf` See How to edit a configurationfile.

To configure inputs using Splunk Connect For Syslog, see Configure Syslog Input

### Manually enable UDP and TCP inputs

To manually enable the UDP or TCP inputs in `inputs.conf`:

1. Create an `inputs.conf` file in the add-on local folder:
    - On *nix:

```
$SPLUNK_HOME/etc/apps/Splunk_TA_mcafee_epo_syslog/local
```

    - On Windows:

```
%SPLUNK_HOME%\etc\apps\Splunk_TA_mcafee_epo_syslog\local
```

2. Open the local `inputs.conf` file:
    - On *nix:

```
$SPLUNK_HOME/etc/apps/Splunk_TA_mcafee_epo_syslog/local/inputs.conf
```

    - On Windows:

```
%SPLUNK_HOME%\etc\apps\Splunk_TA_mcafee_epo_syslog\local\inputs.conf
```

3. To create a TCP input copy the following stanzas into your local `inputs.conf` file:

```
[tcp://9515] <Change the value to custom port numbers if you used different ports on your McAfee
server.>
disabled = false
connection_host=ip
sourcetype = mcafee:epo:syslog
```

4. To create a UDP input copy the following stanzas into your local `inputs.conf` file:

```
[udp://9514] <Change the value to custom port numbers if you used different ports on your McAfee
server.>
disabled = false
connection_host=ip
sourcetype = mcafee:epo:syslog
```

5. Restart the Splunk software.

### Enable UDP and TCP inputs using Splunk Web

1. Log into Splunk Web on your data collection node.
2. Navigate to **Settings** > **Data inputs**.
3. To collect data using TCP, click **TCP** then click **Enable** next to "TCP port 9515".
4. To collect data using UDP, click **UDP** then click **Enable** next to "UDP port 9514".
5. If you configured different port numbers on the McAfee ePO server, click **New** to add a custom port number.

You do not need to restart the Splunk software.

### Enable decryption of encrypted syslog streamsm

If you get events in Splunk in an unreadable format(encrypted logs), the certificate used for communication between McAfee ePO Server and the Syslog server is either not valid, not present, or not trusted.

To generate a self-signed certificate and add its path on the Splunk side, refer to the documentation for your syslog server if not sending syslog directly to splunk.

Generate a self-signed certificate for Windows by following the steps from here - https://support.jetglobal.com/hc/en-us/articles/235636308-How-To-Create-a-SHA-256-Self-Signed-Certificate

To incorporate the certificate:

1. After pasting the certificate in "Trusted Root Certification Authorities", double-click on the certificate, and navigate to "Details".
2. Click on the "Copy to file" option, and click "Next".
3. Select the "Yes, export the private key" option, and click "Next".
4. Check the "Include all certificates in the certification path if possible" option under the Personal Information Exchange section and click "Next".
5. Check the "Password" option and click "Next".
6. Select where you want to save the exported certificate by clicking on "Browse", provide the filename, and click on "Save".
7. Click "Next" and then click on Finish. A success message dialogue box should appear on the successful export of the certificate.
8. The downloaded certificate will be in ".pfx" file format, user will need to convert it to ".pem" file format using an online editor.
9. rovide this certificate path in $SPLUNK_HOME/etc/apps/search/local/inputs.conf.

   Below is the sample stanza for the same for Windows: [SSL] rootCA = $SPLUNK_HOME\etc\auth\cacert.pem serverCert = $SPLUNK_HOME\etc\newcert.pem sslPassword = <certificate password> Below is the sample stanza for *nix: [SSL] rootCA = $SPLUNK_HOME/etc/auth/cacert.pem serverCert = $SPLUNK_HOME/etc/newcert.pem sslPassword = <certificate password>/li>

10. Restart Splunk. Your new events should appear in a readable format

Reference and troubleshooting links:
https://community.splunk.com/t5/Getting-Data-In/how-to-configure-Mcafee-Epo-to-send-data-to-Splunk/m-p/532241

## Configure Syslog Input

To use Splunk Connect for Syslog to collect Syslog data, see the documentation at:

https://splunk.github.io/splunk-connect-for-syslog/main/

Splunk recommends using SC4S instead of configuring Splunk to listen for syslog messages directly. TLS is required for direct configuration.

# Reference

## Lookups for the Splunk Add-on for McAfee ePO Syslog

| Lookup filenames | Description |
|---|---|
| `mcafee_epo_action_v110.csv` | Maps the `vendor_action` field to the `action` field. |
| `mcafee_epo_severity.csv` | Maps the `severity_id` field with the `severity` field. |

## Source types for the Splunk Add-on for McAfee ePO Syslog

The Splunk Add-on for McAfee ePO Syslog provides the index-time and search-time knowledge for intrusion prevention and malware scan data from the following formats.

| Data format | Source Type | Description | CIM compliance |
|---|---|---|---|
| `syslog` | `mcafee:epo:syslog` | Contains McAfee ePO events collected via Syslog | Intrusion Detection, Malware |

## Troubleshooting

- If events appear in an unreadable format (encrypted logs), check to make sure the certificate used for communication between McAfee ePO Server and Syslog Server might be either present, valid, and trusted.

For more information, see, Configure inputs using TCP or UDP.

# Release Notes

## Release notes for the Splunk Add-on for McAfee ePO Syslog

Version 1.1.0 of the Splunk Add-on for McAfee ePO Syslog was released on August 22, 2022.

### Features

- Support for latest CIM v5.0.1
- Support for McAfee Endpoint Security 10.7.x & McAfee Agent 5.5.x
- Enhanced CIM field mappings and increased coverage

### Compatibility

Version 1.1.0 of the Splunk Add-on for McAfee ePO Syslog is compatible with the following versions, platforms, and products.

| | |
|---|---|
| Splunk platform versions | 8.1, 8.2, 9.0 |
| CIM | 5.0.1 |
| Platforms | Platform Independent |
| Vendor Products | • McAfee Endpoint ePO v5.10<br>• McAfee Endpoint Security<br>♦ v10.6.0<br>♦ v10.6.1<br>♦ v10.6.1.1607<br>♦ v10.7.0<br>♦ v10.7.0.1285<br>♦ v10.7.0.3255 |

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

### Known issues

Version 1.1.0 of the Splunk Add-on for McAfee ePO Syslog contains the following known issues.

If no issues appear below, no issues have yet been reported.

### Third-party software attributions

Version 1.1.0 of the Splunk Add-on for McAfee ePO Syslog does not incorporate any third-party software or libraries.