Splunk® Supported Add-ons Splunk Add-on for Check Point OPSEC LEA released

Generated: 12/16/2018 12:02 am
# Table of Contents

**Overview**
- About the Splunk Add-on for Check Point OPSEC LEA ........................................ 1
- Source types for the Splunk Add-on for Check Point OPSEC LEA ............................ 1
- Release notes for the Splunk Add-on for Check Point OPSEC LEA ....................... 2
- Release history for the Splunk Add-on for Check Point OPSEC LEA ....................... 5
- Hardware and software requirements for the Splunk Add-on for Check Point OPSEC LEA .......................................................... 21
- Installation and configuration overview for the Splunk Add-on for Check Point OPSEC LEA .......................................................... 22

**Installation**
- Install the Splunk Add-on for Check Point OPSEC LEA ....................................... 23

**Configuration**
- Configure OPSEC LEA to send data to the Splunk platform .................................. 26
- Configure the Splunk Add-on for Check Point OPSEC LEA through the UI ............. 27
- Configure the Splunk Add-on for Check Point OPSEC LEA using the command line and configuration files ........................................ 31

**Troubleshooting**
- Troubleshoot the Splunk Add-on for Check Point OPSEC LEA .............................. 36

**Reference**
- Lookups for the Splunk Add-on for Check Point OPSEC LEA ............................ 42
Overview

The Check Point App for Splunk has replaced the Splunk Add-on for OPSEC LEA for data collection.

About the Splunk Add-on for Check Point OPSEC LEA

<table>
<thead>
<tr>
<th>Version</th>
<th>4.3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Products</td>
<td>Check Point OPSEC LEA R77, R80</td>
</tr>
<tr>
<td>Visible</td>
<td>Yes. This add-on contains views for configuration.</td>
</tr>
</tbody>
</table>

The Splunk Add-on for Check Point OPSEC LEA allows a Splunk software administrator to collect and analyze firewall, VPN, Anti-Virus, Anti-Bot, SmartDefense (IPS), Threat Emulation, and audit logs from Check Point standalone FW-1 firewalls, standard Multi-Domain Security Management (Provider-1) environments, and Provider-1 environments using the Multi-Domain Log Module (MLM). After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on.

This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Download the Splunk Add-on for Check Point OPSEC LEA from Splunkbase at http://splunkbase.splunk.com/app/3197.

Discuss the Splunk Add-on for Check Point OPSEC LEA on Splunk Answers at http://answers.splunk.com/answers/app/3197.

Source types for the Splunk Add-on for Check Point OPSEC LEA

The Splunk Add-on for Check Point OPSEC LEA collects data from the following sources via a modular input using the OPSEC LEA SDK and provides the following source types and CIM compatibility.
<table>
<thead>
<tr>
<th><strong>Collection method</strong></th>
<th><strong>CIM data models</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall or VPN</td>
<td>opsec</td>
</tr>
<tr>
<td>VPN</td>
<td>opsec:vpn</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>opsec:anti_virus</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>opsec:anti_malware</td>
</tr>
<tr>
<td>IPS Software Blade/SmartDefense</td>
<td>opsec:smartdefense</td>
</tr>
<tr>
<td>Threat Emulation</td>
<td>opsec:threat_emulation</td>
</tr>
<tr>
<td>Audit</td>
<td>opsec:audit</td>
</tr>
</tbody>
</table>

The Check Point App for Splunk has replaced the Splunk Add-on for OPSEC LEA for data collection.

**Release notes for the Splunk Add-on for Check Point OPSEC LEA**

Version 4.3.1 of the Splunk Add-on for Check Point OPSEC LEA was released on May 9, 2018.

**About this release**

Version 4.3.1 of the Splunk Add-on for Check Point OPSEC LEA is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.5.x, 6.6.x, 7.0.x, 7.1.x, 7.2.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.11</td>
</tr>
<tr>
<td>Platforms</td>
<td>Linux (RHEL/CentOS 5.x, 6.x, 7.x) for forwarders</td>
</tr>
<tr>
<td></td>
<td>Linux kernel version 2.6.32 or later (x86_64)</td>
</tr>
</tbody>
</table>
Platform independent for search heads and indexers

Vendor Products | Check Point OPSEC LEA R77, R80

Upgrade instructions

There are no upgrade issues if you are upgrading from version 4.3.0 to 4.3.1.

New and updated features

There are no new features in the Splunk Add-on for Check Point OPSEC LEA version 4.3.1.

Fixed issues

Version 4.3.1 of the Splunk Add-on for Check Point OPSEC LEA contains the following fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-05-01</td>
<td>ADDON-17338</td>
<td>Unable to Forward Firewall Logs Check Point OPSEC LEA HF</td>
</tr>
<tr>
<td>2018-04-24</td>
<td>ADDON-17021</td>
<td>Splunk process starts lea_loggrabber, spawns many processes but does not exit properly, making the system inaccessible.</td>
</tr>
</tbody>
</table>

Known issues

Version 4.3.1 of the Splunk Add-on for Check Point OPSEC LEA has the following known issues.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-09-11</td>
<td>ADDON-19506</td>
<td>New connections fail with &quot;REST API ERROR 400&quot; or &quot;Fatal error: glibc detected an invalid stdin handle&quot; on Linux with a glibc version higher than 2.17-196</td>
</tr>
</tbody>
</table>

Workaround:
1. Download [1]
2. replace $SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/bin/opsec-tools binaries with the updated versions.
<table>
<thead>
<tr>
<th>Date</th>
<th>ADDON-XXXXX</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-05-14</td>
<td>ADDON-18066</td>
<td>3. After you update the two binaries, you must reset the one time password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64bit systems: Unable to establish SIC due to Glibc errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workaround: We consider the syslog approach a better strategy than the current</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LEA add-on given the current limitations of this 3rd party tool regarding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>versions of RHEL/CentOS. It should be rather straight forward to get the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>export utility installed, open the needed ports and configure the input.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After that, we need to verify if they have normalization ready yet but, we will</td>
</tr>
<tr>
<td></td>
<td></td>
<td>look into that further.</td>
</tr>
<tr>
<td>2017-03-26</td>
<td>ADDON-14240</td>
<td>The 'product' field is missing in some firewall events related to environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operations (example: logswitch, policy install/uninstall)</td>
</tr>
<tr>
<td>2017-03-21</td>
<td>ADDON-14201</td>
<td>Several products are not covered in loggrabber product filter logic</td>
</tr>
<tr>
<td>2017-03-19</td>
<td>ADDON-14171</td>
<td>Server name is not supported as orig filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workaround: Use IP address for orig values</td>
</tr>
<tr>
<td>2017-03-19</td>
<td>ADDON-14170</td>
<td>&quot;Non-Audit&quot; and &quot;Firewall Audit&quot; Events with no products won't be indexed when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOT IN product list is provided</td>
</tr>
<tr>
<td>2016-09-09</td>
<td>ADDON-11246</td>
<td>SHA1 is not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workaround: File a ticket with Splunk support to request version 3.1 of the add-on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>has SHA1 support.</td>
</tr>
<tr>
<td>2016-09-09</td>
<td>ADDON-10038,</td>
<td>Enabled input will block app upgrade</td>
</tr>
<tr>
<td></td>
<td>ADDON-13450</td>
<td>Workaround: Disable this add-on before upgrading and enable it after upgrading</td>
</tr>
<tr>
<td>2016-05-31</td>
<td>ADDON-9779</td>
<td>Error message occurs in log files when TA is installed without a configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connection</td>
</tr>
<tr>
<td>2016-05-27</td>
<td>ADDON-9728</td>
<td>Conflict &quot;action&quot; field value for eventtype &quot;opsec_audit_authentication&quot; mapped</td>
</tr>
<tr>
<td></td>
<td></td>
<td>both to CIM: Authentication and Change Analysis</td>
</tr>
<tr>
<td>2016-05-24</td>
<td>ADDON-9680</td>
<td>Some vendor_action values are not in the lookup table &quot;checkpoint_opsec_actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>csv&quot; for eventtype &quot;opsec_communicate&quot;</td>
</tr>
<tr>
<td>2015-10-13</td>
<td>ADDON-8017</td>
<td>Numeric value misinterpreted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workaround: Convert bytes related values to INT_MAX(2147483647) if they're near</td>
</tr>
</tbody>
</table>
Third-party software attributions

Version 4.3.1 of the Splunk Add-on for Check Point OPSEC LEA incorporates the following third-party libraries:

- Httplib2 Python library
- SortedContainers
- Bootstrap
- select2
- Remote PDB
- pythonfutures
- fw1-loggrabber

Release history for the Splunk Add-on for Check Point OPSEC LEA

Latest release

The latest version of the Splunk Add-on for Check Point OPSEC LEA is version 4.3.1. See Release notes for the Splunk Add-on for Check Point OPSEC Lea for the release notes of this latest version.

Version 4.3.0

Version 4.3.0 of the Splunk Add-on for Check Point OPSEC LEA is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.5 or later</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.4 or later</td>
</tr>
<tr>
<td>Platforms</td>
<td>Linux (RHEL/CentOS 5.x, 6.x, 7.x) for forwarders</td>
</tr>
<tr>
<td></td>
<td>Platform independent for search heads and indexers</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>Check Point OPSEC LEA R77, R80</td>
</tr>
</tbody>
</table>
Upgrade instructions

If you are upgrading the Splunk Add-on for Check Point OPSEC LEA from 4.2.0 to 4.3.0, you will need to do one of the following.

Configure the Splunk Add-on for Check Point OPSEC LEA in the UI

If you have configured the Splunk Add-on for Check Point OPSEC LEA through the UI with excluded fields included, then there are no upgrade issues from version 4.2.0 to 4.3.0.

If you have configured the Splunk Add-on for Check Point OPSEC LEA through the UI without excluding fields, you may see additional fields in your events. To remove those fields, do the following steps.

1. Navigate to the Inputs Page in the Splunk Add-on for Checkpoint OPSEC LEA.
2. Select the Data input you would like to edit.
3. Clear the Fetch all fields option and in the selection boxes that appear beneath the option, move unwanted fields from the Selected fields box to the Excluded fields box.
4. Click Update.

Configure the Splunk Add-on for Check Point OPSEC LEA with the configuration files

Add the following inputs to upgrade from version 4.2.0 to 4.3.0.

1. Modify the configuration to remove the fields property (list of fields to consider as whitelist).
2. Add the new field_black_list property in each stanza with the list of fields that should be blacklisted.
   For example, if you would like to blacklist the sent_bytes and short_desc fields, update the stanza to replace the fields line with:

   <![input-name>]
   field_black_list = sent_bytes,short_desc

   For an example, see Create an input in the Configure inputs topic.

New and updated features

Version 4.3.0 of the Splunk Add-on for Check Point OPSEC LEA contains the following new features:
- Upgraded the lealoggrabber utility from 1.11.1 to 2.1.
- Added support of authentication type `sslca_clear` for data collection.

**Fixed issues**

Version 4.3.0 of the Splunk Add-on for Check Point OPSEC LEA contains the following fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-01-15</td>
<td>ADDON-12958</td>
<td>Corrupted checkpoints breaks ingestion</td>
</tr>
</tbody>
</table>

**Known issues**

Version 4.3.0 of the Splunk Add-on for Check Point OPSEC LEA has the following known issues.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2018-09-11 | ADDON-19506  | New connections fail with "REST API ERROR 400" or "Fatal error: glibc detected an invalid stdio handle" on Linux with a glibc version higher than 2.17-196
| 2018-09-11 | ADDON-19506  | Workaround:
1. Download [1]
2. replace $SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/bin/opsec-tools binaries with the updated versions.
3. After you update the two binaries, you must reset the one time password. |
| 2018-03-06 | ADDON-17338  | Unable to Forward Firewall Logs Check Point OPSEC LEA HF
| 2018-03-06 | ADDON-17338  | Workaround:
Temporary workaround was to restart the forwarder every hour. This NO LONGER works. |
| 2018-02-11 | ADDON-17021  | Splunk process starts lea_loggrabber, spawns many processes but does not exit properly, making the system inaccessible.
| 2018-02-11 | ADDON-17021  | Workaround:
- Reboot system. |
<p>| 2017-03-26 | ADDON-14240  | The 'product' field is missing in some firewall events related to environment operations (example: logswitch, policy install/uninstall) |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>ADDON-ID</th>
<th>Issue</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-21</td>
<td>ADDON-14201</td>
<td>Several products are not covered in loggrabber product filter logic</td>
<td></td>
</tr>
<tr>
<td>2017-03-19</td>
<td>ADDON-14171</td>
<td>Server name is not supported as orig filter</td>
<td>Use IP address for orig values</td>
</tr>
<tr>
<td>2017-03-19</td>
<td>ADDON-14170</td>
<td>&quot;Non-Audit&quot; and &quot;Firewall Audit&quot; Events with no products won't be indexed when NOT IN product list is provided</td>
<td></td>
</tr>
<tr>
<td>2016-09-09</td>
<td>ADDON-11246</td>
<td>SHA1 is not supported</td>
<td>File a ticket with Splunk support to request version 3.1 of the add-on which has SHA1 support.</td>
</tr>
<tr>
<td>2016-06-05</td>
<td>ADDON-10038, ADDON-13450</td>
<td>Enabled input will block app upgrade</td>
<td>Disable this add-on before upgrading and enable it after upgrading done.</td>
</tr>
<tr>
<td>2016-05-31</td>
<td>ADDON-9779</td>
<td>Error message occurs in log files when TA is installed without a configured connection</td>
<td></td>
</tr>
<tr>
<td>2016-05-27</td>
<td>ADDON-9728</td>
<td>Conflict &quot;action&quot; field value for eventtype &quot;opsec_audit_authentication&quot; mapped both to CIM: Authentication and Change Analysis</td>
<td></td>
</tr>
<tr>
<td>2016-05-24</td>
<td>ADDON-9680</td>
<td>Some vendor_action values are not in the lookup table &quot;checkpoint_opsec_actions.csv&quot; for eventtype &quot;opsec_communicate&quot;</td>
<td></td>
</tr>
<tr>
<td>2015-10-13</td>
<td>ADDON-8017</td>
<td>Numeric value misinterpreted</td>
<td>Convert bytes related values to INT_MAX(2147483647) if they're negative by EVAL. If you extract the field, the negative value will switch to the positive value.</td>
</tr>
</tbody>
</table>

**Third-party software attributions**

Version 4.3.0 of the Splunk Add-on for Check Point OPSEC LEA incorporates the following third-party libraries:

- Httplib2 Python library
- SortedContainers
- Bootstrap
- select2
- Remote PDB
pythonfutures
fw1-loggrabber

**Version 4.2.0**

Version 4.2.0 of the Splunk Add-on for Check Point OPSEC LEA is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.4 or later</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.4 or later</td>
</tr>
<tr>
<td>Platforms</td>
<td>Linux (RHEL/CentOS 5.x, 6.x, 7.x) for forwarders</td>
</tr>
<tr>
<td></td>
<td>Platform independent for search heads and indexers</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>Check Point OPSEC LEA R76, R77, R80</td>
</tr>
</tbody>
</table>

**Upgrade instructions**

There are no upgrade issues if you are upgrading from version 4.1.0 to 4.2.0.

**New and updated features**

Version 4.2.0 of the Splunk Add-on for Check Point OPSEC LEA lets you reduce indexed data volume by configuring the following new settings when creating inputs:

- Specify only the log fields you are interested in to collect data from
- Filter events by common log fields - product and orig

**Fixed issues**

Version 4.2.0 of the Splunk Add-on for Check Point OPSEC LEA contains the following fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-31</td>
<td>ADDON-14305</td>
<td>'dest', 'dvc_nt_host' field for eventtype &quot;opsec_audit&quot; is wrong</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>ADDON-13253</td>
<td>value of field &quot;dest&quot;, &quot;src&quot; in sourcetype &quot;opsec:anti_virus&quot; and &quot;opsec:anti_malware&quot; should be exchanged</td>
</tr>
<tr>
<td>2017-03-27</td>
<td>ADDON-12657</td>
<td>OPSEC Add-on calculated field does not</td>
</tr>
</tbody>
</table>
include 'icmp' values for 'transport' field

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-24</td>
<td>ADDON-14221</td>
<td>Data channel select and timestamp setting can not work at the same time</td>
</tr>
<tr>
<td>2017-03-22</td>
<td>ADDON-13276</td>
<td>Unable to collect data on search head</td>
</tr>
<tr>
<td>2017-03-20</td>
<td>ADDON-14168</td>
<td>Splunk start error message after connection is configured</td>
</tr>
<tr>
<td>2017-03-20</td>
<td>ADDON-14089, ADDON-11454</td>
<td>Input cannot work and be displayed when input number exceeds 30</td>
</tr>
</tbody>
</table>

**Known issues**

Version 4.2.0 of the Splunk Add-on for Check Point OPSEC LEA has the following known issues:

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2018-09-11 | ADDON-19506  | New connections fail with "REST API ERROR 400" or "Fatal error: glibc detected an invalid stdio handle" on Linux with a glibc version higher than 2.17-196  

**Workaround:**  
1. Download [2]  
2. replace  
   `$SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/bin/opsec-tools`  
   binaries with the updated versions.  
3. After you update the two binaries, you must reset the one time password. |
| 2018-01-08 | ADDON-16520  | Excluded field still showing up in a left side panel |
| 2017-06-29 | ADDON-15195, ADDON-16372 | OPSEC App with hyphen in the name breaks integration |
| 2017-03-26 | ADDON-14240  | The 'product' field is missing in some firewall events related to environment operations (example: logswitch, policy install/uninstall) |
| 2017-03-21 | ADDON-14201  | Several products are not covered in loggrabber product filter logic |
| 2017-03-19 | ADDON-14171  | Server name is not supported as orig filter  

**Workaround:**  
Use Ip address for orig values |
<p>| 2017-03-19 | ADDON-14170  | &quot;Non-Audit&quot; and &quot;Firewall Audit&quot; Events with no products won't be indexed when NOT IN product list is provided |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>ADDON-XXXXX</th>
<th>Issue</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-01-30</td>
<td>ADDON-13450, ADDON-10038</td>
<td>Enabled input will block app upgrade</td>
<td>Disable TA before upgrade, then enable it after upgrade is done</td>
</tr>
<tr>
<td>2016-09-09</td>
<td>ADDON-11246</td>
<td>SHA1 is not supported</td>
<td>File a ticket with Splunk support to request version 3.1 of the add-on that has SHA1 support.</td>
</tr>
<tr>
<td>2016-05-31</td>
<td>ADDON-9779</td>
<td>Error message occurs in log files when TA is installed without a configured connection</td>
<td></td>
</tr>
<tr>
<td>2016-05-27</td>
<td>ADDON-9728</td>
<td>Conflict &quot;action&quot; field value for eventtype &quot;opsec_audit_authentication&quot; mapped both to CIM: Authentication and Change Analysis</td>
<td></td>
</tr>
<tr>
<td>2016-05-24</td>
<td>ADDON-9680</td>
<td>Some vendor_action values are not in the lookup table &quot;checkpoint_opsec_actions.csv&quot; for eventtype &quot;opsec_communicate&quot;</td>
<td></td>
</tr>
<tr>
<td>2015-10-13</td>
<td>ADDON-8017</td>
<td>Numeric value misinterpreted</td>
<td>Convert bytes related values to INT_MAX(2147483647) if they're needed using EVAL. If you extract the field, the negative value will switch to the positive value.</td>
</tr>
</tbody>
</table>

**Third-party software attributions**

Version 4.2.0 of the Splunk Add-on for Check Point OPSEC LEA incorporates the following third-party libraries:

- Httplib2 Python library
- SortedContainers
- Bootstrap
- select2
- Remote PDB
- pythonfutures
- fw1-loggrabber

**Version 4.1.0**

Version 4.1.0 of the Splunk Add-on for Check Point OPSEC LEA is compatible with the following software, CIM versions, and platforms.
Splunk platform versions: 6.3 or later
CIM: 4.4 or later
Platforms: Linux (RHEL/CentOS 5.x, 6.x, 7.x) for forwarders
Platform independent for search heads and indexers
Vendor Products: Check Point OPSEC LEA R76, R77, R80

**Upgrade instructions**

There are no upgrade issues if you are upgrading from version 4.0.0 to 4.1.0.

**New and updated features**

Version 4.1.0 of the Splunk Add-on for Check Point OPSEC LEA has the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-23</td>
<td>ADDON-11399</td>
<td>Updated configuration UI and opseclea_connection.conf to support SIC certificate sharing or reuse among multiple connections.</td>
</tr>
<tr>
<td>2016-09-19</td>
<td>ADDON-10799, ADDON-9688</td>
<td>Added support for Splunk platform 6.5.0</td>
</tr>
</tbody>
</table>

**Fixed issues**

Version 4.1.0 of the Splunk Add-on for Check Point OPSEC LEA contains the following fixed issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-21</td>
<td>ADDON-11401</td>
<td>Failed to ingest non-utf8 data</td>
</tr>
</tbody>
</table>

**Known issues**

Version 4.1.0 of the Splunk Add-on for Check Point OPSEC LEA has the following known issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-09</td>
<td>ADDON-11246</td>
<td>SHA1 is not supported. <strong>Workaround:</strong> File a ticket with Splunk support to request version 3.1 of the add-on, which has SHA1 support.</td>
</tr>
<tr>
<td>2016-06-02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ADDON-10011</td>
<td>If a forwarder is stopped while collecting data from OPSEC LEA, events can be lost, particularly if the inputs use online mode. <strong>Workaround:</strong> If you need to stop a forwarder for any reason, first disable the Splunk Add-on for Check Point OPSEC LEA, since it might be collecting data, and wait for 10 seconds before stopping the forwarder.</td>
<td></td>
</tr>
<tr>
<td>SPL-122152</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-06-01 ADDON-9779</td>
<td>Error messages, including &quot;Failed to send rest request&quot;, occur in log files after the add-on has been installed when no connection is configured. When Splunk is shutting down, the REST service may be terminated before the modular input, so the REST call initiated by the modular input will return an error.</td>
<td></td>
</tr>
<tr>
<td>2016-05-27 ADDON-9728</td>
<td>Event type &quot;opsec_audit_authentication&quot; mapped to both Authentication and Change Analysis CIM models resulting in conflicting &quot;action&quot; field value.</td>
<td></td>
</tr>
<tr>
<td>2016-05-24 ADDON-9680</td>
<td>Some vendor_action values are not in lookup table checkpoint_opsec_actions.csv for event type &quot;opsec_communicate&quot;.</td>
<td></td>
</tr>
<tr>
<td>2015-10-13 ADDON-8017</td>
<td>Due to an OPSEC SDK limitation, some bytes values are beyond the range of the integer type. To work around this issue, bytes related values (e.g., bytes, send_bytes, client_inbound_bytes) that have a negative value as a result of EVAL will be converted to INT_MAX (2147483647) at search time.</td>
<td></td>
</tr>
<tr>
<td>2015-08-17 OPSEC-398/ADDON-8053</td>
<td>When FIPs is enabled in a distributed Splunk Enterprise environment, the Manage Connections page cannot be accessed on the search head, even after restarting the Splunk platform.</td>
<td></td>
</tr>
<tr>
<td>2015-05-13 OPSEC-333/ADDON-8012</td>
<td>lea_loggrabber does not support the --nofieldnames option. This limits firewall log data ingestion to key value pairs and prevents log data ingestion from CSV files.</td>
<td></td>
</tr>
</tbody>
</table>
**Third-party software attributions**

Version 4.1.0 of the Splunk Add-on for Check Point OPSEC LEA incorporates the following third-party libraries:

- Httplib2 Python library
- SortedContainers
- Bootstrap
- select2
- Remote PDB
- pythonfutures
- fw1-loggrabber

**Version 4.0.0**

Version 4.0.0 of the Splunk Add-on for Check Point OPSEC LEA was released on June 20, 2016. Version 4.0.0 of the Splunk Add-on for Check Point OPSEC LEA is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.3 or later</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.4 or later</td>
</tr>
<tr>
<td>Platforms</td>
<td>Linux (RHEL/CentOS 5.x, 6.x, 7.x) for forwarders</td>
</tr>
<tr>
<td></td>
<td>Platform independent for search heads and indexers</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>Check Point OPSEC LEA R76, R77, R80</td>
</tr>
</tbody>
</table>

**Migration guide**

The Splunk Add-on for Check Point OPSEC LEA 4.0.0 replaces the Splunk Add-on for Check Point OPSEC LEA 3.1.0.

Some features of the Splunk Add-on for Check Point OPSEC LEA 3.1.0 are not available in this add-on:

- Support for Solaris has been removed.
- Support for remote connections has been removed.
- Support for OPSEC versions without vendor support has been removed.
- The fw1-loggrabber.conf file has been removed as direct configuration of lea_loggrabber is no longer supported.

The Splunk Add-on for Check Point OPSEC LEA 4.0.0 add-on folder name is different than previous versions of the Splunk Add-on for Check Point OPSEC
LEA, thus installing version 4.0.0 will not overwrite a previous version. You cannot upgrade from a previous version of the add-on. You must remove the previous version of the add-on before installing the new version.

All events indexed by previous versions are supported by this version. However, configurations in previous versions are not transferable to the new version. You must recreate your configurations in the Splunk Add-on for Check Point OPSEC LEA 4.0.0 using either the GUI or the configuration files.

You can choose to re-use the certificate files you used to connect to your OPSEC LEA servers in a previous version of the add-on if you create connections in the .conf file or you can pull the certificates again. If you pull the certificates again you will need to perform reconfiguration in OPSEC LEA.

To prevent duplicate events from being indexed, use the Start Time field when configuring the input using Splunk Web or in the .conf files.

**New and removed features**

Version 4.0.0 of the Splunk Add-on for Check Point OPSEC LEA has the following new features. Some features from the previous release have also been removed in this release.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-05-20</td>
<td>ADDON-8448</td>
<td>Re-build the Splunk Add-on for Check Point OPSEC LEA to bring it into line with current standards for Splunk built add-ons, including standardizing logging and updating the UI, and add support for the 64bit/SHA2 opsec_pull_cert utility.</td>
</tr>
<tr>
<td>2016-05-05</td>
<td>ADDON-8447</td>
<td>Add support for R80.</td>
</tr>
<tr>
<td>2016-06-01</td>
<td>ADDON-8462</td>
<td>Add prebuilt panels.</td>
</tr>
<tr>
<td>2016-05-06</td>
<td>ADDON-8594</td>
<td>Support .conf file based configuration.</td>
</tr>
<tr>
<td>2016-05-09</td>
<td>ADDON-8029</td>
<td>Remove support for Solaris.</td>
</tr>
<tr>
<td>2016-05-05</td>
<td>ADDON-8588</td>
<td>Remove support for remote connections.</td>
</tr>
<tr>
<td>2016-05-05</td>
<td>ADDON-8446</td>
<td>Remove support for OPSEC versions without vendor support.</td>
</tr>
<tr>
<td>2016-06-02</td>
<td>ADDON-8992</td>
<td>Remove support for direct configuration of lea_loggrabber. fw1-loggrabber.conf has been</td>
</tr>
</tbody>
</table>
Fixed issues

Version 4.0.0 of the Splunk Add-on for Check Point OPSEC LEA fixes the following issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-05-20</td>
<td>ADDON-8448</td>
<td>Splunk Add-on for Check Point OPSEC LEA does not support the 6.4 release of the Splunk platform. The add-on requires version 6.3.</td>
</tr>
<tr>
<td>2016-05-05</td>
<td>ADDON-8447</td>
<td>Splunk Add-on for Check Point OPSEC LEA does not support the R80 release of Check Point. The add-on requires 77.3 or earlier.</td>
</tr>
<tr>
<td>2016-05-08</td>
<td>ADDON-8275</td>
<td>Splunk Add-on for Check Point OPSEC LEA does not support the SHA256 certificate. The add-on requires the SHA1 certificate.</td>
</tr>
<tr>
<td>2016-05-31</td>
<td>ADDON-9743</td>
<td>Incorrect &quot;action&quot; field value for event type &quot;opsec_audit_authentication&quot; mapped to Authentication CIM model.</td>
</tr>
<tr>
<td>2016-05-31</td>
<td>ADDON-9736</td>
<td>Incorrect &quot;action&quot; value for event type &quot;opsec_audit_change&quot;.</td>
</tr>
<tr>
<td>2016-05-30</td>
<td>ADDON-9742</td>
<td>Incorrect &quot;change_type&quot; value for event type &quot;opsec_audit&quot;.</td>
</tr>
<tr>
<td>2016-05-30</td>
<td>ADDON-9737</td>
<td>Update &quot;action&quot; value for event type &quot;opsec_communicate&quot; from &quot;blocked&quot; to &quot;dropped&quot;.</td>
</tr>
<tr>
<td>2016-05-30</td>
<td>ADDON-9729</td>
<td>Update event type &quot;opsec_audit_authentication&quot; definition to <code>search = sourcetype=opsec:audit (Operation=&quot;Log In&quot; OR Operation=&quot;Log Out&quot; OR Operation=&quot;Force Log Out&quot;)</code>.</td>
</tr>
<tr>
<td>2016-05-30</td>
<td>ADDON-9660</td>
<td>Wrong &quot;transport&quot; field value for event type &quot;opsec_communicate&quot;.</td>
</tr>
<tr>
<td>2016-05-26</td>
<td>ADDON-9661</td>
<td>Use &quot;rule_id&quot; instead of &quot;rule&quot; when it is an integer.</td>
</tr>
<tr>
<td>2016-05-25</td>
<td>ADDON-9681</td>
<td>Source type &quot;opsec:vpn&quot; is not in lookup table.</td>
</tr>
<tr>
<td>Date</td>
<td>Ticket Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2016-05-25</td>
<td>ADDON-9674</td>
<td>Some &quot;te_action&quot; values are not in lookup table for source type &quot;opsec:smartdefense&quot;.</td>
</tr>
<tr>
<td>2016-05-25</td>
<td>ADDON-9664</td>
<td>Some &quot;src_port&quot; field values are not integers.</td>
</tr>
<tr>
<td>2016-05-25</td>
<td>ADDON-9658</td>
<td>&quot;service&quot; is not always a port value in source types &quot;opsec&quot; and &quot;opsec:vpn&quot;.</td>
</tr>
<tr>
<td>2016-05-24</td>
<td>ADDON-9659</td>
<td>&quot;dvc_ip&quot; should be IP address.</td>
</tr>
<tr>
<td>2016-05-24</td>
<td>ADDON-9656</td>
<td>Add &quot;db_tag_for_opsec&quot; stanza to other source types.</td>
</tr>
<tr>
<td>2016-05-23</td>
<td>ADDON-9599</td>
<td>Some fields with &quot;:&quot; in the value are not extracted by DELIMS.</td>
</tr>
<tr>
<td>2016-05-23</td>
<td>ADDON-9597</td>
<td>Wrong &quot;host&quot; field value. The host value is the Splunk instance hostname instead of the physical device.</td>
</tr>
<tr>
<td>2016-05-18</td>
<td>ADDON-9420</td>
<td>The &quot;src&quot; field is overwritten by the &quot;origin&quot; field.</td>
</tr>
<tr>
<td>2016-05-18</td>
<td>ADDON-8018</td>
<td>Action values &quot;drop&quot; and &quot;accept&quot; are incorrect values for Network Traffic data in the CIM.</td>
</tr>
<tr>
<td>2016-05-09</td>
<td>ADDON-8019</td>
<td>Informational message should appear when no certificates are available.</td>
</tr>
<tr>
<td>2016-05-08</td>
<td>ADDON-8275</td>
<td>OPSEC LEA fails to connect after changing certificate to SHA256.</td>
</tr>
<tr>
<td>2016-05-06</td>
<td>ADDON-8198</td>
<td>Include spec files to describe the configuration options offered.</td>
</tr>
<tr>
<td>2016-05-06</td>
<td>ADDON-8020</td>
<td>Checkpoint add-on does not alias &quot;src&quot; and &quot;dest zones&quot;.</td>
</tr>
<tr>
<td>2016-05-05</td>
<td>OPSEC-402 /ADDON-8014</td>
<td>Making the Splunk Add-on for Check Point OPSEC LEA global can cause namespace conflicts with other apps and add-ons. On forwarders, use local to prevent conflict. On search heads, keep the add-on global to enable knowledge sharing, but disable the UI.</td>
</tr>
<tr>
<td>2104-04-07</td>
<td>OPSEC-208 /ADDON-8044</td>
<td>When migrating from 2.0.x, enabling <strong>Online mode</strong> immediately after upgrade might cause gaps in your data. This occurs because online</td>
</tr>
</tbody>
</table>
mode collects new incoming logs only. It does not perform log look back. Therefore any data stored during the upgrade process will not be pulled into Splunk. We recommend that you do not enable online mode until after all log data generated during the upgrade period is indexed. This can also affect users who are editing connections while online mode is enabled. In the period between when the new configuration is reloaded and a new watchdog is started, some logs may be dropped. Note that this behavior can also occur when moving online connections.

**Known issues**

Version 4.0.0 of the Splunk Add-on for Check Point OPSEC LEA has the following known issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-09</td>
<td>ADDON-11246</td>
<td>SHA1 is not supported. <strong>Workaround:</strong> File a ticket with Splunk support to request version 3.1 of the add-on, which has SHA1 support.</td>
</tr>
<tr>
<td>2016-07-12</td>
<td>ADDON-10514</td>
<td>Authentication fails on dedicated server. <strong>Workaround:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Create a single object in SmartDashboard for the LEA connection and initialize SIC with a one time password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In Splunk UI, go to the OPSEC add-on and create a connection to the primary management server, using the one-time password to initialize the connection, and store the certificate file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. cd to the opsec TA local directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Open the opsec_connection.conf file, make a copy of the working stanza and give it a new name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Change the IP address to IP of the dedicated server, set lea_server_type=dedicated, and change the first section of the opsec_entity_sic_name field (CN name) to the name of the OPSEC LEA connection object.</td>
</tr>
<tr>
<td>Date</td>
<td>ADDON-XXXXX</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
7. Go back into the configuration UI for this add-on and create an input for that connection.  
If a forwarder is stopped while collecting data from OPSEC LEA, events can be lost, particularly if the inputs use online mode. **Workaround:** If you need to stop a forwarder for any reason, first disable the Splunk Add-on for Check Point OPSEC LEA, since it might be collecting data, and wait for 10 seconds before stopping the forwarder. |
<p>| 2106-06-01 | ADDON-9779 | Error messages, including &quot;Failed to send rest request&quot;, occur in log files after the add-on has been installed when no connection is configured. When Splunk is shutting down, the REST service may be terminated before the modular input, so the REST call initiated by the modular input will return an error. |
| 2106-05-30 | ADDON-9758 | You may not see the latest events when searching the index for data gathered by inputs that use online mode. When using online mode, the add-on caches the fetched events in memory until the buffer is full. There can be latency if there are not enough new incoming events from Check Point as the last events will be held in buffer until enough new ones come in. However, the data is not lost. |
| 2106-05-30 | ADDON-9756 | The data input page for the Splunk Add-on for Check Point OPSEC LEA should be disabled or hidden. You cannot configure inputs using the <strong>Settings &gt; Data inputs &gt; Splunk Add-on for Check Point OPSEC LEA</strong> page. You must use the add-on configuration page accessed by selecting <strong>Splunk Add-on for Check Point OPSEC LEA</strong> in the left side menu or by selecting <strong>Apps &gt; Launch app</strong> next to Splunk Add-on for Check Point OPSEC LEA. |
| 2106-05-27 | ADDON-9728 | Event type &quot;opsec_audit_authentication&quot; mapped to both Authentication and Change Analysis CIM models resulting in conflicting &quot;action&quot; field value. |
| 2106-05-24 | ADDON-9680 | Event type &quot;opsec_audit_authentication&quot; mapped to both Authentication and Change Analysis CIM models resulting in conflicting &quot;action&quot; field value. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-05-23</td>
<td>ADDON-9634</td>
<td>Some vendor_action values are not in lookup table checkpoint_opsec_actions.csv for event type &quot;opsec_communicate&quot;.</td>
</tr>
<tr>
<td>2015-10-13</td>
<td>ADDON-8017</td>
<td>Errors about pam.i686 when pam.x86_64 is already installed on Linux 64-bit machine. See the workaround in the Troubleshooting section.</td>
</tr>
<tr>
<td>2015-08-17</td>
<td>OPSEC-398/ADDON-8053</td>
<td>Due to an OPSEC SDK limitation, some bytes values are beyond the range of the integer type. To work around this issue, bytes related values (e.g., bytes, send_bytes, client_inbound_bytes) that have a negative value as a result of EVAL will be converted to INT_MAX (2147483647) at search time.</td>
</tr>
<tr>
<td>2015-05-13</td>
<td>OPSEC-333/ADDON-8012</td>
<td>When FIPs is enabled in a distributed Splunk Enterprise environment, the Manage Connections page cannot be accessed on the search head, even after restarting the Splunk platform.</td>
</tr>
<tr>
<td>2015-05-13</td>
<td>OPSEC-198</td>
<td>lea_loggrabber does not support the --nofieldnames option. This limits firewall log data ingestion to key value pairs and prevents log data ingestion from CSV files.</td>
</tr>
<tr>
<td>2004-03-18</td>
<td>OPSEC-198</td>
<td>In Check Point version R77.10, Log Server stops forwarding logs to LEA clients. This occurs when switching the active log to new one (log switch) and the Log Server does not notify the LEA client about the new log file. Fix: Install hotfix on Check Point Multi-Domain Security Management Server/Log Server machine.</td>
</tr>
</tbody>
</table>

**Third-party software attributions**

Version 4.0.0 of the Splunk Add-on for Check Point OPSEC LEA incorporates the following third-party libraries:

- Httplib2 Python library
- SortedContainers
- Bootstrap
- select2
- Remote PDB
- pythonfutures
- fw1-loggrabber
Hardware and software requirements for the Splunk Add-on for Check Point OPSEC LEA

Operating system requirements for the Splunk Add-on for Check Point OPSEC LEA

These operating system requirements apply to Splunk forwarders only. Search heads and indexers can be hosted on any Splunk supported platform.

- Linux (RHEL/CentOS)
- Linux kernel version 2.6.32 or later (x86_64)
- Bash, version 3 or later.
- GNU C library (glibc.i686 32-bit). For example, install using `yum install glibc.i686`
- PAM shared libraries (pam.i686 32-bit). For example, install using `yum install pam.i686`

Check Point OPSEC LEA setup requirements

For Check Point server authentication to work, the $HOME directory must be writable by the Linux account that Splunk is running as.

Make sure ports 18184 and 18210 are open to Splunk. 18184/tcp: is used to retrieve FW/AUDIT logs from the Check Point API and 18210/tcp: is used for a one time connection to pull the certificate.

Sizing guidelines

It is important that your Splunk Add-on for Check Point OPSEC LEA deployment includes sufficient heavy forwarder and indexer capacity to handle the incoming load. An insufficient number of heavy forwarders or indexers can negatively impact performance.

A heavy forwarder can handle up to 13,000 events per second (EPS). If you are collecting more than 13,000 EPS from your OPSEC LEA connections, you can add additional heavy forwarders and spread the inputs across the heavy forwarders. If you use indexer clustering, you can use light forwarders for data collection and spread the parsing and indexing tasks among the indexers in your cluster.

See Where to install this add-on for information about which Splunk tiers to install the add-on to.
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 plan to run this add-on entirely in Splunk Cloud, there are no additional Splunk platform requirements.
- For Splunk Light system requirements: see System Requirements in the Splunk Light 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.

Installation and configuration overview for the Splunk Add-on for Check Point OPSEC LEA

Complete the following steps to install and configure this add-on.

1. Install the Splunk Add-on for Check Point OPSEC LEA.
2. Configure OPSEC LEA to send data to the Splunk platform.
3. Configure the Splunk Add-on for Check Point OPSEC LEA through the UI.

To pull data from dedicated log servers or standby management servers, most customers will find it easier to configure steps 2 and 3 through the Web UI, and then clone the actual connection stanza via configuration files (opsec_configuration.conf) as detailed in Configure the Splunk Add-on for Check Point OPSEC LEA using the command line and configuration files.
Installation

Install the Splunk Add-on for Check Point OPSEC LEA

1. Get the Splunk Add-on for Check Point OPSEC LEA by downloading it from https://splunkbase.splunk.com/app/3197 or browsing to it using the app browser within Splunk Web.
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.

Distributed deployments

Use 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.

Note: Linux (RHEL/CentOS 5.x, 6.x, or 7.x) is required for forwarders but search heads and indexers are platform independent.

<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Heads</td>
<td>Yes</td>
<td>Yes</td>
<td>Install this add-on to all search heads where Check Point OPSEC LEA</td>
</tr>
</tbody>
</table>
knowledge management is required. Splunk recommends that you turn the Visible setting off for the add-on on your search heads to prevent data duplication errors that can result from running inputs on your search heads instead of (or in addition to) your data collection node.

<table>
<thead>
<tr>
<th>Indexers</th>
<th>Yes</th>
<th>Conditional</th>
<th>This add-on does not need to be installed on indexers if it is installed on a heavy forwarder.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavy Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>Install this add-on on either a heavy or light forwarder for data collection. Because this add-on retains state and checkpoint locally on the data ingestion node, the forwarder needs to be backed up.</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>No</td>
<td>No</td>
<td>The universal forwarder is not supported because this add-on requires Python.</td>
</tr>
<tr>
<td>Light Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>Install this add-on on either a heavy or light forwarder for data collection. If installed on a light forwarder, the add-on must also be installed on your indexers. Because this add-on retains state and checkpoint locally on the data ingestion node, the forwarder needs to be backed up.</td>
</tr>
</tbody>
</table>

**Distributed deployment feature compatibility**

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

<table>
<thead>
<tr>
<th>Distributed deployment feature</th>
<th>Supported</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Head Clusters</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Indexer Clusters</td>
<td>Yes</td>
<td>Before installing this add-on to an Indexer cluster, remove the <code>eventgen.conf</code> file and all files in the</td>
</tr>
</tbody>
</table>
This add-on does not support installation or configuration via Deployment Server. This add-on retains state and checkpoint locally on the data ingestion node. For this reason, you cannot use a deployment server because of potential for duplication by running on multiple forwarders.

### 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:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light
Configuration

Configure OPSEC LEA to send data to the Splunk platform

You need to perform configuration in Check Point OPSEC LEA before you can collect OPSEC LEA data with the Splunk Add-on for Check Point OPSEC LEA.

Create the Splunk OPSEC application

Create the Splunk OPSEC application using the Check Point SmartDashboard or the desired CMA/Domain on Provider-1. Name the new OPSEC application SplunkLEA. (You can use any name but SplunkLEA is recommended by convention.) When configuring the host, select or create the Splunk host on which the Splunk Add-on for Check Point OPSEC LEA is being installed for data collection, usually a forwarder. Consult the Check Point documentation for more information about creating an OPSEC application.

Do not use hyphens in OPSEC App name. See certificate authority not found error.

Create the OPSEC application certificate

Create an OPSEC application certificate in the Check Point SmartDashboard. Be sure to take note of the one-time password you enter. You will need this one-time password when you create an OPSEC LEA connection in the add-on. Note that the password must not include any of the following special characters: exclamation (!), circumflex accent (^), tilde (~), grave accent (¨), quotation ("), or apostrophe (’).

After initialization, note the opsec_sic_name that is generated. You will need this opsec_sic_name if you are configuring the add-on using the configuration files. Consult the Check Point documentation for more information about creating an application certificate.

Add firewall rules

If there are firewalls between the Splunk instance performing the data collection and the Management Server, you need to add firewall rules using the SmartDashboard application. Verify that the FW1_lea and FW1_ica_pull rule
settings are correct. Action should be set to **accept** for both rules. Consult the Check Point documentation for more information about firewall rules.

### Install the database

The last configuration step for OPSEC LEA is to install the database. In the SmartDashboard, under **Policy**, install the database for your Management Server. Consult the Check Point documentation for more information.

### Configure the Splunk Add-on for Check Point OPSEC LEA through the UI

You can configure the Splunk Add-on for Check Point OPSEC LEA using the configuration files or Splunk Web. This section describes how to configure the Splunk Add-on for Check Point OPSEC LEA using Splunk Web. When you create a connection using the Splunk Add-on for Check Point OPSEC LEA configuration page, the add-on pulls the OPSEC application certificate for you.

You will need to have admin permissions to configure this add-on.

### Create an OPSEC LEA connection

If you have a standard Check Point Provider-1 environment, you must configure an OPSEC LEA connection for each Customer Management Add-on (CMA) connected to the Multi-Domain Management Server (MDS). The CMA acts as both Log Server (handling log file collection) and Management Server (issuing the OPSEC application certificate). If your Provider-1 environment includes the optional Multi-Domain Log Module (MLM), you must configure an OPSEC LEA connection for each Customer Log Module (CLM) connected to the Multi-Domain Log Module (MLM). In this case, the CLM acts as the Log Server, while the CMA acts as the Management Server.

**Prerequisite:**

Before you begin, make sure port 18210 is open to your management server as this port is blocked on many firewalls and the pull-cert.sh script pulls the certificate on port 18210. Also make sure that the log server port (default 18184) is open to your log servers.

**Steps:**
1. Access Splunk Web on the node responsible for data collection.
2. Go to the Splunk Add-on for Check Point OPSEC LEA configuration page, either by clicking on the name of the add-on on the left navigation banner on the home page or by going to Manage Apps, then clicking Launch app in the row for Splunk Add-on for Check Point OPSEC LEA.
3. Click the Configuration menu.
4. In the Connection tab, click Add Connection.
5. In the Add Connection dialog, type a name for the connection in the Name field. This name must be unique for each connection.
6. Type the Log Server IP address.
   - For standard MDS (Multi-Domain Server) environments, the Log Server IP is the CMA IP address.
   - For standalone environments, the Log Server IP is the Management Server IP address.
7. Accept the default Log Server Port number, 18184, unless your local environment uses a different port.
8. From the Major Version list, select the version of your Check Point deployment.
9. From the Log Server Type list, select the type of Check Point deployment you have.
10. If you selected log server type Secondary Management Server or Dedicated Server in the previous step, the Log Server Object Name field appears. This is the name of the Secondary Management Server or Dedicated Server. (Example name for a Secondary Management Server: manager_server2.) You do not need to specify the full SIC name (for example, CN=cp_mgmt_manager_server2). The full SIC name will be generated automatically by the add-on.
11. In the SIC Certificate field, select one of these options:
   - Pull New SIC Certificate: Fill in the following fields that appear.
     - Management Server IP: The IP address of the Management Server.
     - OPSEC App Name: The name of the application you created for Splunk in Check Point OPSEC LEA, for example, SplunkLEA.
     - One-Time Password: The password you used when you created the OPSEC application certificate.
   - Reuse Existing SIC Certificate: Choose an already configured SIC certificate, if any, from the list.
12. Click Add. The connection will be saved and will be displayed on the Connection tab. The pulled certificate will be saved as <Connection Name>_<random number>.p12 in $SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/certs. For example: test1234_517533425.p12.
Note: If you receive an error message, this might be because you have not installed glibc.i686 and pam.i686, you are using an invalid password or IP address, the connection to the server is down, or port 18210 is blocked by your firewall. For error details, see $SPLUNK_HOME/var/log/splunk/web_service.log. See the Troubleshooting section for troubleshooting tips. Please note that port 18210 will not be listening on a Log Server (CLM/MLM), and you must configure the SIC initialization to the CMA IP instead. Then you can configure additional CLMs via the opsec_configuration.conf file.

You can edit, delete, or clone a connection by clicking the Action link for the connection in the Actions column.

Note: You cannot delete a connection sharing an SIC certificate with another connection through certificate reuse.

Set logging level

1. Click the Logging tab on the Splunk Add-on for Check Point OPSEC LEA configuration page.
2. The default Log Level is INFO. Change this to DEBUG or ERROR as needed.
3. Click Save.

Create a new input

1. From the Splunk Add-on for Check Point OPSEC LEA configuration page, click Inputs at the top and click Create New Input.
2. Type an unique name for the input.
3. Choose a Connection from the connections that have been previously configured.
4. Choose Offline Mode or Online Mode. Online mode enables Check Point's real-time mode. This keeps a single Check Point process running, and prevents the Check Point process from being closed when no new log data is available on the Check Point server. This might help improve performance in cases where data flow is intermittent.
5. (optional) Check No-Resolve Mode if you want to specify the loggrabber --no-resolve argument to turn object name resolution off.
6. From the Data list, select the data you want to collect with the input.
   ♦ Non-Audit: Collects all event types except audit events.
   ♦ Firewall Events: Collects firewall events only.
   ♦ Firewall Audit: Collects audit events only.
   ♦ SmartDefense: Collects Smart Defense events only.
   ♦ VPN (Virtual Private Network): Collects VPN events only.
7. Set the interval with which to collect data with this input in seconds. The default is 3600 seconds.
8. Select an index to use other than default if desired. This is the index to which Check Point events will be sent.
9. (optional) In the Host field, provide the value you would like to use for the Host field in Splunk events.
10. (optional) Specify a Start Time to begin collecting events in this format: YYYY-MM-DDThh:mm:ssTZD. For example: 2016-06-01T00:00:00+08:00. If you are upgrading from a previous version of the Splunk Add-on for Check Point OPSEC LEA, use this field to specify when to begin collecting events in order to prevent re-indexing events that have already been indexed by the Splunk platform. Note that collection starts at the time specified here from the currently active log file if there is more than one log file.
11. By default, the add-on collects all log data with an input. You can limit data collection to only the log fields you are interested in to decrease indexed data volume.
   To exclude fields from data collection, clear the Fetch all fields option and in the selection boxes that appear beneath the option, move unwanted fields from the Selected fields box to the Excluded fields box. Only common log fields are listed in the Selected Fields box. By default, all possible fields will be included in the event. Click the plus sign (+) at the top the box to include fields that are not there. Enter the field name in the text box and click Enter to add fields in the Selected Fields box. To exclude any field, add fields in the Excluded fields box.
   ♦ Note: You can verify the field name by using the following query.

        index=<index-name> sourcetype=<source-type> | table _raw

   Run the above query and find the field from the raw event that you want to blacklist. Refer to the LEA Fields to verify the fields.
12. Optionally, filter events by common log fields - product and org. The org filter rule is only available for non-audit and firewall audit metrics. When setting the org filter rule, enter valid IP address in IPV4 format and delimit multiple IP addresses using comma (,).
13. Click Add to create the input. The input will now be listed on the Inputs page.

You can edit, delete, disable, or clone an input by clicking the Action link for the input in the Actions column.
Upgrade instructions

If you have configured the Splunk Add-on for Check Point OPSEC LEA through the UI with excluded fields included, then there are no upgrade issues from version 4.2.0 to 4.3.1.

If you have configured the Splunk Add-on for Check Point OPSEC LEA through the UI without excluding fields, you may see additional fields in your events. To remove those fields, do the following steps.

1. Navigate to the **Inputs Page** in the Splunk Add-on for Checkpoint OPSEC LEA.
2. Select the **Data input** you would like to edit.
3. Clear the **Fetch all fields** option and in the selection boxes that appear beneath the option, move unwanted fields from the **Selected fields** box to the **Excluded fields** box.
4. Click **Update**.

Configure the Splunk Add-on for Check Point OPSEC LEA using the command line and configuration files

You can configure the Splunk Add-on for Check Point OPSEC LEA using the command line and configuration files or Splunk web. This section describes how to perform the configuration using the command line and configuration files.

To configure the add-on manually, perform the following four steps:

1. Pull the OPSEC application certificate.
2. Create an OPSEC LEA connection.
3. Set the logging level.
4. Create an input.

Pull the OPSEC application certificate

**Prerequisite:**

- Port 18210 must be open. The pull-cert.sh script pulls the certificate on port 18210.
Steps

1. At the command line on the Splunk node responsible for data collection, go to `$SPLUNK_HOME/etc/apps/Splunk_TACheckpoint-opseclea/bin`.
2. Run the `pull-cert.sh` script to pull the certificate from the Management Server:
   ```bash
   /pull-cert.sh <CMA_IP> <OPSEC_app_name> <password> <outputFileName>.p12
   ```
   For example:
   ```bash
   /pull-cert.sh 10.160.27.253 SplunkLEA password test1234_517533425.p12
   ```
   Parameters:
   - `<CMA_IP>` is the CMA IP address.
   - `<OPSEC_app_name>` is the OPSEC Application name (for example, SplunkLEA).
   - `<password>` is the one-time password (activation key) obtained when you created the OPSEC application certificate. Note: The password must not include any of the following special characters: exclamation (!), circumflex accent (^), tilde (~), grave accent (\'), and quotation ('').
   - `<outputFileName>` is the output file (*.p12) containing the application DN name as defined in the Management Server.

   The command returns an opsec_sic_name, for example:
   ```bash
   [CN=SplunkLEA, O=opsec-p1-R7540-demo_Management_Server...3tvqd0]
   ```

   Important: Save the opsec_sic_name because you will need to provide it when you edit the opseclea_connection.conf configuration file.

3. View the `$SPLUNK_HOME/etc/apps/Splunk_TACheckpoint-opseclea/certs` directory to confirm that `<outputFileName>.p12` has been created as specified in the command line.

Create an OPSEC LEA connection

If you have a standard Check Point Provider-1 environment, you must configure an OPSEC LEA connection for each Customer Management Add-on (CMA) connected to the Multi-Domain Management Server (MDS). The CMA acts as both Log Server (handling log file collection) and Management Server (issuing the OPSEC application certificate). If your Provider-1 environment includes the optional Multi-Domain Log Module (MLM), you must configure an OPSEC LEA connection for each Customer Log Module (CLM) connected to the Multi-Domain Log Module (MLM). In this case, the CLM acts as the Log Server, while the the CMA acts as the Management Server.

Steps

1. Create a file called `opseclea_connection.conf` in
   `$SPLUNK_HOME/etc/apps/Splunk_TACheckpoint-opseclea/local`.
2. Create a connection stanza using the example below, specifying the values necessary for your environment and your needs:

```plaintext
[<connection name>]
cert_name = <cert name pulled using pull-cert.sh script, example: outputFileName.p12>
certificate = <connection name from which SIC certificate is reused>
fw_version = <version of OPSEC LEA: R76, R77 or R80>
lea_app_name = <application name created on OPSEC LEA Smart Dashboard, example: SplunkLEA>
lea_server_auth_port = <OPSEC LEA server port, default value is 18184>
lea_server_auth_type = <sslca or sslca_clear>
lea_server_ip = <OPSEC LEA server IP address>
lea_server_type = <OPSEC LEA server type: primary, secondary or dedicated>
lea_object_name = <name of Secondary Management Server or Dedicated Server if lea_server_type is secondary or dedicated. Example: manager_server2>
opsec_entity_sic_name = <example: CN=cp_mgmt,O=r7730-domain1_Management_Server_Management_Server..gtruxt>
opsec_sic_name = <example: CN=SplunkLEA,O=r7730-domain1_Management_Server_Management_Server..gtruxt>
```

**Note:** Both the `opsec_entity_sic_name` and `opsec_sic_name` are case sensitive.

**Note:** For `opsec_sic_name` use the `opsec_sic_name` that was generated when you ran the pull-cert.sh script.

**Note:** The `opsec_entity_sic_name` is the Entity SIC Name of the stand-alone Check Point Manager, Provider-1 Customer Log Module (CLM), or Provider-1 Customer Management Add-on (CMA). The Entity SIC Name can be created from the CN part of the SIC Name.

- ♦ If the Log Server is activated on the Primary Management Server, replace the value of CN with `cp_mgmt`.
- ♦ If the Log Server is activated on the Secondary Management Server, replace the value of CN with `cp_mgmt_<object_name>` where `<object_name>` is the name of the Log Server object.
- ♦ If the Log Server is activated on a Dedicated Server, replace the value of CN with `<object_name>`, where `<object_name>` is the name of the Log Server object.

Alternatively, you can use the Check Point Database tool, GuiDBedit, to locate the Entity SIC Name.

3. Add a stanza with a unique name for each connection you would like to create and save the file.
Set logging level

The default Log Level is INFO. Change this setting to DEBUG or ERROR if desired.

1. Create a file called opseclea_settings.conf in
   $SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/local.
2. Add the following stanza and specify a log level - INFO, DEBUG, OR ERROR.
   ```
   [logging]
   level = DEBUG
   ```
3. Save the file.

Create an input

1. Create a file called opseclea_inputs.conf in
   $SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/local.
2. Create an input stanza using the example below, specifying the values necessary for your environment and your needs:
   ```
   [<input name>]
   connection = <connection name from opseclea_connection.conf>
   data = <Data to fetch: non_audit (Non-Audit), fw (Firewall Events), audit (Firewall Audit), smartdefense (SmartDefense), or vpn (VPN)>
   index = <index to use for the fetched data>
   interval = <input interval in seconds>
   mode = <input mode: offline or online>
   disabled = <0 = enabled; 1 = disabled>
   host = <value to use for Host field in Splunk events (optional)>
   starttime = <start time to fetch data in format YYYY-MM-DDThh:mm:ssTZD (optional). Example: 2016-06-01T00:00:00+08:00>
   noresolve = <0 = off; 1 = on. Loggrabber --no-resolve argument which prevents object name resolution>
   filter = product=New Anti Virus,Policy Server,Linux OS;orig!=123.22.22.22,124.34.234.2
   ```
3. Add a stanza with a unique name for each input you would like to create and save the file.

**Note:** You can verify the field name by using the following query.

```
index=<index-name> sourcetype=<source-type> | table _raw
```
Run the above query and find the field from the raw event that you want to blacklist. Refer to the LEA Fields to verify the fields.

**Upgrade instructions**

Add the following inputs to upgrade from version 4.2.0 to 4.3.0.

1. Modify the configuration to remove the fields property (list of fields to consider as whitelist).
2. Add the new `field_black_list` property in each stanza with the list of fields that should be blacklisted.
   - For example, if you would like to blacklist the `sent_bytes` and `short_desc` fields, update the stanza to replace the `fields` line with:

   ```
   [<input-name>]
   field_black_list = sent_bytes, short_desc
   ```
Troubleshooting

Troubleshoot the Splunk Add-on for Check Point OPSEC LEA

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in Splunk Add-ons. For additional resources, see Support and resource links for add-ons in Splunk Add-ons.

Splunk Add-on for Check Point OPSEC LEA logs

This add-on has 3 logs that are located at $SPLUNK_HOME/var/log/splunk:

- splunk_ta_checkpoint-opseclea_modinput.log
- splunk_ta_checkpoint-opseclea_ucc_lib.log
- splunk_ta_checkpoint-opseclea_util.log

To check for errors in the internal logs for this add-on, you can perform this search:

index=_internal source=*ta_checkpoint-opseclea*

You can configure the logging verbosity on the configuration page for the add-on. Supported log levels are INFO, DEBUG, and ERROR.

A large amount of debug information is provided by the Check Point OPSEC SDK if the log level is set to DEBUG. This will have an impact on performance, especially if the data volume is large.

Online mode inputs limitation

Inputs are executed in a thread pool which can handle between 4 and 128 tasks. However, because online mode tasks never finish, each online mode task always occupies one thread in the thread pool. The add-on can support 120 online mode tasks at the most. If there are more than 120 online mode tasks, the data collection process will exit and the following error message will be logged: "There are too many online mode inputs. The count is <int> which should be less than 1".
Use this search to check if you are encountering this limitation.

index="_internal" sourcetype="opseclea:log:modinput" "too many online mode inputs"

To resolve this error, deploy rest inputs on another heavy forwarder.

**32-bit run time environment errors**

This add-on requires a 32-bit run time environment. If the latest i686 packages are not the same version as the currently installed x86_64 packages on the machine, errors like the following can occur:

Error: Protected multilib versions: libgcc-4.4.7-3.el6.i686 != libgcc-4.4.6-4.el6.x86_64
Error: Protected multilib versions: pam-1.1.1-13.el6.i686 != pam-1.1.1-10.el6_2.1.x86_64

To resolve this type of error, you need to upgrade the x86_64 packages first and then install the i686 packages.

For example:

```
> yum upgrade libgcc.x86_64 pam.x86_64
> yum install pam.i686 glibc.i686 libgcc.i686
```

**SIC errors**

You can use the following search to determine if SIC errors are occurring.

index="_internal" sourcetype="opseclea:log:modinput" "SIC ERROR"

Follow these steps to troubleshoot SIC errors:

1. Check that the Log Server Type (lea_server_type) is configured correctly. The valid options are primary, secondary, and dedicated. Different log server types have different entity sic names.
2. Check that the opsec_entity_sic_name and opsec_sic_name are correct. The opsec_sic_name uses this format: CN=<Splunk OPSEC application name>,O=<host information>..<a string>. For opsec_entity_sic_name, use the following guidelines: The Entity SIC Name of the Log Server object can be created from the CN in the SIC Name.
If the Log Server is activated on the Primary Management Server, replace it with `?cp_mgmt?` as in this example:

```
CN=cp_mgmt,O=CP-hero1-take-195.checkpoint.com.fsd9kx
```

If the Log Server is activated on the Secondary Management Server, replace it with `?cp_mgmt_<OBJECT_NAME>?` as in this example:

```
CN=cp_mgmt_<OBJECT_NAME>,O=CP-hero1-take-195.checkpoint.com.fsd9kx
```

where `<OBJECT_NAME>` is the name of the Log Server object.

If the Log Server is activated on dedicated server, replace it with `?OBJECT_NAME?` as in this example:

```
CN=<OBJECT_NAME>,O=CP-hero1-take-195.checkpoint.com.fsd9kx
```

where `<OBJECT_NAME>` is the name of the Log Server object.

3. If you receive the following error message in the logs: "Invalid arg: file %s doesn't exist", check that a file with the extension `.p12` exists in the `$SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/certs` directory. If not, pull a cert down by running `pull-cert.sh` or delete the connection and add a new one on the add-on configuration page.

4. If other SIC errors are present in the log, see the Check Point documentation at http://dl3.checkpoint.com/paid/20/How-To-Troubleshoot-SIC-related-Issues.pdf?HashKey=1463490738_979d1a6f694300a70576eecfe9d55b85&xtn=.pdf.

**lea_loggrabber errors**

If you are seeing lea_loggrabber errors such as "COMM_FAILURE" in the add-on logs, check the following:

- The machine running this add-on can access the Check Point machine.
- The Check Point machine is running and healthy.

**Time configuration**

If you configured your OPSEC LEA connections and inputs in the configuration files and you receive the error "Required syntax: 'starttime=YYYY-MM-DDThh:mm:ssTZD", you need to configure the time using ISO-8601 format.

**Historic log fetching limitation**

There are limits to the add-on's ability to collect historic log data when more than one log file exists on Check Point. When using the "Start Time" parameter, data collection will start at the specified time from the currently active log file. The start
time does not apply to other log files.

**Events lost when forwarder stopped**

If a forwarder is stopped during data collection from OPSEC LEA, events can be lost. If you need to stop a forwarder for any reason, disable the Splunk Add-on for Check Point OPSEC LEA first, and wait 10 seconds before stopping the forwarder.

**Log Server stops forwarding logs to LEA clients in Check Point version R77.10**

In Check Point version R77.10, the Log Server may stop forwarding logs to LEA clients. This occurs when switching the active log to a new one (log switch) and the Log Server does not notify the LEA client about the new log file.

**Fix:** Install hotfix on Check Point Multi-Domain Security Management Server/Log Server machine.

**Integer overflow for bytes values**

Due to an OPSEC SDK limitation, some bytes values are beyond the range of the integer type. To work around this issue, bytes related values that have a negative value as a result of EVAL (e.g., bytes, send_bytes, client_inbound_bytes, client_outbound_bytes, server_inbound_bytes and server_outbound_bytes) will be converted to INT_MAX (2147483647) at search time. The raw data will contain the negative value, but in the extracted field, the negative value will be converted to 2147483647.

**Missing OPSEC fields**

While configuring or modifying input, if some fields are added to **Excluded Fields** and the **Fetch all fields** option is selected, the fields added to **Excluded Fields** are filtered out. To ensure all OPSEC fields are indexed, select **Fetch all fields** and make sure that no fields are added to the **Excluded Fields** section.

**Certificate authority not found error**

If you are seeing this error `Opsec error. rc=-1 err=-93 The referred entity does not exist in the Certificate Authority`, reset the one-time password from the OPSEC configuration to pull the certificate again. This is commonly a result of using a hyphen in the OPSEC app name.
Extra fields in your Splunk events

If you are upgrading the Splunk Add-on for Check Point OPSEC LEA from 4.2.0 to 4.3.0, you may see more fields in your Splunk events that are not present in the Selected Field lists. Manually add those fields into the Excluded Fields box to exclude them.

- See Upgrade instructions using the UI or

Upgrade instructions using the command line and configuration files.

Checkpoint errors

When two or more data inputs are configured for the same product (e.g. non_audit, firewall) and follow similar naming convention (e.g input/9, input/19, etc), there is a possibility of race condition as all these inputs refer to the same checkpoint file.

You will see the following warning message: Unable to get a lock or parse the checkpoint file <Name of the checkpoint file>. Will retry on next run.

Your error will be logged in splunk_ta_checkpoint-opseclea_modinput.log and Splunk software will stop indexing data for that particular data input.

Data collection errors persist after upgrading to version 4.3.1

If data collection errors persist after upgrading the Splunk Add-on for Check Point OPSEC LEA from 4.3.0 to 4.3.1, create a new data input with a new OPSEC application object and enter the last event index time in the Start time input field.

1. Disable the inputs.
2. If the Data input field is set to audit, enter the following search query and make a note of the last event index time:

```
index=<index_name> sourcetype=opsec:audit | head 1 | eval latest_timestamp=strftime(time, "%Y-%m-%dT%H:%M:%STZD") | table latest_timestamp
```

Replace TZD with the local timezone.
3. If the Data input field is set to non-audit, enter the following search query and make a note of the last event index time:
index=<index_name> sourcetype!=opsec:audit | head 1 | eval latest_timestamp=strftime(time, "%Y-%m-%dT%H:%M:%STZD") | table latest_timestamp

Replace TZD with the local timezone.
4. Upgrade the Splunk Add-on for Check Point OPSEC LEA.
5. Create a new data input with a new OPSEC application object, and enter the last event index time value in the Start Time input field.
6. Restart Splunk.
Reference

Lookups for the Splunk Add-on for Check Point OPSEC LEA

The Splunk Add-on for Check Point OPSEC LEA has 5 lookups. The lookup files map fields from OPSEC LEA systems to CIM-compliant values in the Splunk platform. The lookup files are located in:

$SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint-opseclea/lookups.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkpoint_actions_te.csv</td>
<td>Maps the te_action field value for the opsec:smartdefense, opsec:threat_emulation, opsec:anti_virus source types to action field in CIM models.</td>
</tr>
<tr>
<td>checkpoint_audit_actions.csv</td>
<td>Maps the vendor operation field for opsec:audit to action field in CIM models.</td>
</tr>
<tr>
<td>checkpoint_ids_severity.csv</td>
<td>Maps vendor severity to severity field in CIM models for source type opsec:threat_emulation.</td>
</tr>
<tr>
<td>checkpoint_opsec_actions.csv</td>
<td>Maps the vendor_action field for OPSEC to action field in CIM models for source types opsec and opsec:vpn.</td>
</tr>
<tr>
<td>checkpoint_vendor_info.csv</td>
<td>Maps source type to add vendor product information.</td>
</tr>
</tbody>
</table>