Splunk® Supported Add-ons
Splunk Add-on for Check Point Log Exporter released

Generated: 11/05/2022 11:58 am

Table of Contents

Overview

About the Splunk Add-on for Check Point Log Exporter

Version	1.1.0
Vendor Products	Check Point Software R81 and R81.10, Check Point Endpoint client version E84.30 and E86.20, Check Point Management server version: R80.40, R81.10
Visible	No. This add-on does not contain any views.

The Splunk Add-on for Check Point Log Exporter allows a Splunk software administrator to collect data from Check Point Log Exporter over syslog.

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

Download the Splunk Add-on for Check Point Log Exporter from Splunkbase at http://splunkbase.splunk.com/app/5478.

Discuss the Splunk Add-on for Check Point Log Exporter on Splunk Answers at https://community.splunk.com/t5/Apps-and-Add-ons/ct-p/apps-add-ons.

Hardware and software requirements for the Splunk Add-on for Check Point Log Exporter

Review the following requirements before you install and configure the Splunk Add-on for Check Point Log Exporter.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply to the Splunk software 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.
- If you manage 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 Log Exporter

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

1. Install the Splunk Add-on for Check Point Log Exporter Log Exporter.
2. Configure Check Point Log Exporter to send data to the Splunk platform.

Installation

Install the Splunk Add-on for Check Point Log Exporter Log Exporter

1. Get the Splunk Add-on for Check Point Log Exporter by downloading it from https://splunkbase.splunk.com/app/xxxx 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.

Where to install this add-on

Unless otherwise noted, supported add-ons are installable to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

Use these tables to determine where and how to install this add-on in your environment. Depending on your environment, preferences, and add-on requirements, you may need to install the add-on in multiple places.

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

Splunk platform component type	Supported	Required	Actions required / Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Check Point Log Exporter knowledge management is required. As a best practice, turn add-on visibility off on your search heads to prevent data duplication errors resulting from running inputs on your search heads instead of or in addition to your data collection node.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data. It is required if you use universal forwarders to collect data.
Heavy Forwarders	Yes	No	This add-on supports forwarders of any type for data collection.
Universal Forwarders	Yes	No	

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

Migrate to Splunk Add-on for Check Point Log Exporter

Migrate from Splunk Add-on for Check Point OPSEC LEA

The Splunk Add-on from Check Point Log Exporter uses the log exporter in Check Point to push syslog data in Splunk.

If the Splunk Add-on for Check Point OPSEC LEA is installed on your deployment, disable the OPSEC LEA inputs before migrating to Splunk Add-on for Check Point Log Exporter. Ingesting data from both add-ons would lead to data duplication in the Splunk instance.

The Splunk add-on for Check Point Log Exporter uses new sourcetypes to ingest and extract information from the data. The existing data from Check Point OPSEC LEA are not available in the new add-on. However, the ingested data in the existing sourcetype would still be searchable in the sourcetype.

Follow the steps described in the Configure section to ingest syslog data from Check Point to Splunk.

Migrate from Splunk App for Check Point

The Splunk Add-on for Check Point Log Exporter uses the same sourcetypes for ingesting the data from the Splunk log format from the Check Point App for Splunk. After installing the Splunk add-on for Check Point Log Exporter, you might experience degraded performance because extractions from the add-on and the app would run on the same data. Significant CIM mapping changes are included in this release to adhere to the CIM standards, and existing content may not correctly include these events.

Configure Check Point Log Exporter to send correct Syslog RFC 5424 format data

This topic describes how to send logs in Syslog format to Splunk. Syslog is the recommended format of data collection and provides better performance than the Splunk log format.

1. Open the cp terminal
2. Enter the `expert` command to log in in expert mode.
3. Navigate to the configuration directory.
4. Execute `cp SyslogFormatDefinition.xml SyslogRecommendedFormatDefinition.xml`
5. Open `SyslogRecommendedFormatDefinition.xml` and edit the `start_message_body,fields_separatator,field_value_separatator` as follows:
   ```
   <start_message_body>[sc4s@2620 </start_message_body>
   <fields_separatator> </fields_separatator>
   <field_value_separatator>=</field_value_separatator>
   ```
   .
6. Copy `SyslogRecommendedFormatDefinition.xml` into `$EXPORTERDIR/targets//conf`.
7. Navigate to the configuration file `$EXPORTERDIR/targets//targetConfiguration.xml`.
8. Add the reference to the `SyslogRecommendedFormatDefinition.xml` under the key. For example, if `$EXPORTERDIR=/opt/CPrt-R81/log_exporter`, the absolute path will become `<formatHeaderFile>/opt/CPrt-R81/log_exporter/targets/<your_log_exporter>/conf /SyslogRecommendedFormatDefinition.xml</formatHeaderFile>` .
9. Restart `cp_log_exporter` by executing the command `cp_log_export restart name <your_log_exporter>`. Make sure if you migrate to a different format that the existing format is disabled, or else it would lead to data

duplication.

Configure Check Point Log Exporter to send Syslog data to Splunk

1. Enter the `expert` command in the Check Point server.

   ```
   expert .
   ```

2. Enter the expert password.
3. Execute the following command:

   ```
   cp_log_export add name exporter_splunk target-server <target-server> target-port  target-port
    protocol <tcp|udp> format <syslog|splunk> read-mode semi-unified
   ```

4. Start the export process on your Check Point Server:

   ```
   cp_log_export restart name exporter_splunk
   ```

Configuration

Configure inputs

Configure a syslog input using Splunk Connect for Syslog

Splunk recommends using Splunk Connect for Syslog to configure syslog inputs. To configure inputs using Splunk Connect for Syslog, see the documentation at https://splunk.github.io/splunk-connect-for-syslog/main/sources/vendor/Checkpoint/logexporter_5424/.

Configure a syslog input with Splunk Web

1. Configure a syslog input as described in Add a network input using Splunk Web.
2. Set the sourcetype as cp_log/cp_log:syslog.

Configure a syslog input via Backend

1. Open or create `$SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint_log_exporter/local/inputs.conf`.
2. If you are using TCP, copy and paste the following stanza into the file and select your configured sourcetype among the list:

   ```
   [tcp://514]
   sourcetype = <cp_log|cp_log:syslog>
   disabled = false
   ```
3. If you are using UDP, copy and paste the following stanza into the file.

   ```
   <pre>
   [udp://514]
   sourcetype =<cp_log|cp_log:syslog>
   disabled = false
   ```
4. If you are using forwarders, configure forwarding by defining tcp outputs and then enabling a receiver.
5. Restart the Splunk platform. If you have a distributed deployment, restart your forwarder and indexers.

Verify your input is working

If you have a distributed deployment, perform the following search on your Search head to check that the Splunk platform is indexing events from your Checkpoint Log Exporter logs:

```
index=* sourcetype=cp_log*
```

Troubleshooting

Troubleshoot

Keys not extracting due to large events

Splunk has a default limit of resources which are used to parse events. If events are too large the regex will stop parsing the keys value pairs in the events. If that happens, the resource limit needs to be increased so that the parsing continues. Increase the depth_limit in transforms.conf by following these steps: If your events are ingested in `cp_log` sourcetype, increase the depth_limit for the `kv_cp_log_format`

```
[kv_cp_log_format]
FORMAT = $1::$2
REGEX = ([a-zA-Z0-9_-]+):?=([^|]+)
MV_ADD = true
DEPTH_LIMIT = 200000
```

If your events are ingested in `cp_log:syslog` sourcetype, increase the depth_limit for the `kv_cp_log_format`

```
[kv_cp_syslog_log_format]
FORMAT = $1::$2
REGEX = ([a-zA-Z0-9_-]+):?="((?:[^"\\]|\\.)+)"
MV_ADD = true
DEPTH_LIMIT = 200000
```

Reference

Lookups for the Splunk Add-on for Check Point Log Exporter

The Splunk Add-on for Check Point Log Exporter has the following **lookups**. The lookup files map fields from Check Point Log Exporter to CIM-compliant values in the Splunk platform. The lookup files are located in: `$SPLUNK_HOME/etc/apps/Splunk_TA_checkpoint_log_exporter/lookups`.

Filename	Description
`checkpoint_service_app.csv`	Maps `transport_id` to `protocol` and `transport`.
`checkpoint_transport_protocols.csv`	Maps `service` port to `app`.

Source types for the Splunk Add-on for Check Point Log Exporter

The Splunk Add-on for Check Point Log Exporter provides the following source types and CIM compatibility.

Sourcetype	Event type	CIM compliance
`cp_log`	cp_tcp_attack	Intrusion Detection
	cp_network_communicate	Network Traffic
	cp_change	Change
	cp_change_audit	Change
	cp_logout_logs	Change
	cp_change_network	Change
	cp_alert	Alerts
	cp_malware_attack	Malware Attacks
	cp_ids_attack	Intrusion Detection
	cp_auth_logs	Authentication
	cp_endpoint_activity	Inventory
`cp_log:syslog`	cp_tcp_attack	Intrusion Detection
	cp_network_communicate	Network Traffic
	cp_change	Change
	cp_change_audit	Change
	cp_logout_logs	Change
	cp_change_network	Change
	cp_alert	Alerts
	cp_malware_attack	Malware Attacks
	cp_ids_attack	Intrusion Detection
	cp_auth_logs	Authentication

	Event type	CIM compliance
	cp_endpoint_activity	Inventory

Sourcetype

Release Notes

Release notes for the Splunk Add-on for Check Point Log Exporter

Version 1.1.0 of the Splunk Add-on for Check Point Log Exporter was released on April 21, 2022.

About this release

Version 1.1.0 of the Splunk Add-on for Check Point Log Exporter is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.1, 8.2
CIM	5.0.0
Platforms	Platform independent
Vendor Products	Check Point Software R81 and R81.10, Check Point Endpoint client version E84.30 and E86.20, Check Point Management server version: R80.40, R81.10

New Features

- Compatibility with CIM v5.0.0
- Added support for below new blades

Blade Source CLI checkpoint:audit Identity Awareness checkpoint:sessions Endpoint checkpoint:endpoint

- Enhanced existing CIM extractions
- Added support for 2 new DM: Inventory and Change Network
- Log out logs will be tagged with Change DM instead of Authentication DM
- Fixed extraction for file_path field of Malware DM
- Updated search query for cp_change and cp_change_audit event types for tracking accurate audit logs
- Fixed extraction for event_action=" Detect", previously action was blocked now it will be allowed.
- Enhanced extractions for bytes_in, bytes_out and packets_in, packets_out

Field changes

Sourcetype	Applicable events	Fields			v1
		Added Fields	Modified Fields	Removed Fields	
['cp_log:syslog']	product="Application Control" AND proto=*	session_id, event_src, packets_in, packets_out, bytes_out, direction, dvc_ip, bytes_in, dest_interface			
['cp_log:syslog']	product="Connectra" AND event_type="Login"	session_id, event_src, direction, dvc_ip,	tag, eventtype, tag::eventtype,		communicate,network, cp_network_communicate,

Sourcetype	Applicable events	Fields			v1
		protocol_version, authentication_method	app, action		communicate,network, https, Log In
['cp_log:syslog']	event_type="Logout"	result, object_category, tag, session_id, event_src, eventtype, tag::eventtype, object, direction, dvc_ip, object_id, change_type, status, object_attrs	action		Log Out
['cp_log:syslog']	product="Identity Awareness" AND identity_src="AD Query"	tag, app, event_src, eventtype, tag::eventtype, vendor_product, id, dest, authentication_method, dest_nt_domain, dvc, src_ip, dest_ip	action, src, source		Update, 10.160.174.195, checkpoint:cp_default
['cp_log:syslog']	product="SmartDefense"	event_src, file_path, bytes_out, direction, dvc_ip, bytes_in, src_interface, protocol_version			
['cp_log:syslog']	protection_type="URL reputation", protection_type="protection"	event_src, action, direction, dvc_ip, src_interface, protocol_version			
['cp_log:syslog']	session_name="IPS" AND fieldchanges=*	object_category, session_id, direction, dvc_ip, object_id, user_type, object_attrs	tag, eventtype, tag::eventtype		audit, cp_change_audit, audit
['cp_log:syslog']	internal_ca="VPN certificate created"	result, object_category, tag, eventtype, tag::eventtype, object, direction, dvc_ip, object_id, change_type, dest_interface, status	action		Key Install
['cp_log:syslog']	package_action="Install"	result, object_category, tag, action, eventtype, tag::eventtype, command, object, direction, dvc_ip, object_id, change_type, status, object_attrs			
['cp_log:syslog']	product="SmartConsole" AND operation="Delete Object"	tag, session_id, eventtype, tag::eventtype, direction, dvc_ip, object_id, user_type			
['cp_log:syslog']	product="DLP" AND reject_category="User '<user>' has failed to log into the portal"	tag, app, event_src, eventtype, tag::eventtype, direction, dvc_ip, dest, dest_ip	action		Reject

Sourcetype	Applicable events	Fields			v1
['cp_log:syslog']	subject="Object Manipulation" AND operation="Modify Object"	session_id, direction, dvc_ip, user_type, object_attrs	tag, eventtype, tag::eventtype, dest, dest_ip		audit, cp_change_audit, audit, 10.160.113.11, 10.160.113.11
['cp_log:syslog']	operation="Install Policy"	result_id, user_type, direction, dvc_ip	dest, src_ip, src, dest_ip		10.160.113.11, 10.160.0.11, 10.160.0.11, 10.160.113.11
['cp_log:syslog']	product="Identity Awareness" AND error_description="Identity information will be deleted"	app, type, body, vendor_product, id, dest, dvc, src_ip, description, src	source		checkpoint:cp_default
['cp_log:syslog']	event_type="Status Changed"	event_src, direction, dvc_ip, change_type, object_attrs	tag, eventtype, tag::eventtype		audit, cp_change_audit, audit
['cp_log:syslog']	subject="Endpoint Activity" AND objecttype="endpoint"	tag, endpoint_sam, endpoint_type, tag::eventtype, eventtype, endpoint_workgroup, endpoint_sid, description			
['cp_log:syslog']	subject="Object Manipulation" AND objecttype="PolicyUpdateTime"	result, object_category, status, user_name, vendor_product, dest, dvc, user, src_user, object_id, id, user_type, src_ip, src, command, src_user_name, object, change_type, date, object_attrs, dest_ip	tag, eventtype, tag::eventtype, action, source		audit, cp_change_audit, audit, Accept, checkpoint:cp_default
['cp_log:syslog']	product="Forensics"	event_src, direction, dvc_ip	file_path	url	c:\\users\\administrator\\downloads\\
['cp_log:syslog']	operation="Log In"	result_id, direction, dvc_ip, change_type, user_type, authentication_method	eventtype, dest, src_ip, src, dest_ip		, 10.160.113.11, 10.160.0.11, 10.160.0.11, 10.160.113.11
['cp_log:syslog']	protection_type="URL Filtering" AND action="Detect"	event_src, action, file_path, direction, dvc_ip, category, ids_type, signature			
['cp_log:syslog']	event_type="TE Info Event" AND reason="Valid_TE_License"	object_category, event_src, action, object, direction, dvc_ip, change_type, status, object_attrs	tag, eventtype, tag::eventtype		alert, cp_alert, alert
['cp_log:syslog']	product="Threat Emulation" AND action="Detect"	event_src, direction, dvc_ip, protocol_version, dest_interface	app, action		Threat Emulation, blocked
['cp_log:syslog']	product="Threat Extraction" AND failure_impact=*	tag, app, eventtype, tag::eventtype, direction, dvc_ip, signature	dest	dest_ip	10.160.0.11

Sourcetype	Applicable events	Fields			v1
['cp_log:syslog']	session_name="APPI Update"	object_category, session_id, direction, dvc_ip, object_id, user_type, object_attrs	tag, eventtype, tag::eventtype		audit, cp_change_audit, audit
['cp_log:syslog']	db_ver=* and update_status=*	dest_ip, change_type, direction, dvc_ip	tag, eventtype, tag::eventtype, object_attrs		audit, cp_change_audit, audit, database version
['cp_log:syslog']	operation="Log Out" AND product="WEB_API"	object_category, session_id, object, direction, dvc_ip, object_id, change_type, user_type, object_attrs	tag, eventtype, tag::eventtype, action		authentication, , authentication, success
['cp_log:syslog']	product="Threat Emulation" AND errors=*	event_src, direction, dvc_ip, protocol_version, signature			
['cp_log:syslog']	product="VPN-1 & FireWall-1"	src_interface, event_src, direction, dvc_ip			
['cp_log:syslog']	product="VPN-1 & FireWall-1" AND hll_key=*	session_id, event_src, packets_in, packets_out, bytes_out, direction, dvc_ip, bytes_in, src_interface, dest_interface			
['cp_log:syslog']	service_id="echo-request"	session_id, event_src, icmp_code, direction, dvc_ip, icmp_type, dest_interface			
['cp_log:syslog']	product="Connectra" AND action="Failed Log In"	session_id, event_src, direction, dvc_ip, protocol_version, authentication_method	tag, eventtype, tag::eventtype, app, action		communicate,network, cp_network_communicate, communicate,network, https, Failed Log In
['cp_log:syslog']	product="Connectra" AND action="Reject"	session_id, event_src, file_path, direction, dvc_ip, protocol_version	action		Reject
['cp_log:syslog']	product="Log Update" AND action="Accept"	event_src, packets_in, packets_out, bytes_out, direction, dvc_ip, bytes_in, src_interface, protocol_version, dest_interface	action		Accept

CIM changes

Source	Applicable Events	Previous CIM model	New CIM model
checkpoint:audit	auth_method="Password"	Network_Traffic	Authentication
checkpoint:audit	fieldschanges=* NOT audit_status=*	Change.Auditing_Changes	Change.All_Changes
checkpoint:sessions			Alerts

Source	Applicable Events	Previous CIM model	New CIM model
	error_description="Identity information will be deleted"		
checkpoint:firewall	new_status=*	Change.Auditing_Changes	Change.All_Changes
checkpoint:endpoint	objecttype="PolicyUpdateTime" AND operation="Modify Object"		Change.Auditing_Changes
checkpoint:ids_malware	product="Threat Emulation" AND reason="Valid_TE_License"	Alerts	Change.All_Changes
checkpoint:web	update_status=* AND db_ver=*	Change.Auditing_Changes	Change.All_Changes
checkpoint:audit	operation="Log Out"	Authentication	Change.All_Changes
checkpoint:audit	product="Connectra" AND event_type="Logout", product="System Monitor" AND package_action="Install", product="SmartConsole" AND operation="Delete Object"		Change.All_Changes
checkpoint:sessions	product="Identity Awareness" AND identity_src="AD Query"		Authentication
checkpoint:firewall	internal_ca="VPN certificate created"		Change.Network_Changes
checkpoint:firewall	product="DLP" AND reject_category="User '<user>' has failed to log into the portal"		Authentication
checkpoint:sessions	product="Identity Awareness" AND error_description="Identity information will be deleted"		Alerts
checkpoint:endpoint	subject="Endpoint Activity" AND objecttype="endpoint"		Inventory.All_Inventory.OS
checkpoint:endpoint	subject="Object Manipulation" AND objecttype="PolicyUpdateTime"		Change.All_Changes
checkpoint:ids_malware	product="Threat Extraction" AND failure_impact=*		Alerts

Fixed issues

Version 1.1.0 of the Splunk Add-on for Check Point Log Exporter contains the following fixed issues.

Known issues

Version 1.1.0 of the Splunk Add-on for Check Point Log Exporter has the following known issues.

Third-party software attributions

Version 1.1.0 of the Splunk Add-on for Check Point Log Exporter does not incorporate any third-party libraries.

Release history for Check Point Log Exporter

Version 1.1.0 of the Splunk Add-on for Check Point Log Exporter was released on April 19, 2022. See

Version 1.0.1

Version 1.0.1 of the Splunk Add-on for Check Point Log Exporter was released on August 13, 2021.

About this release

Version 1.0.1 of the Splunk Add-on for Check Point Log Exporter is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.0, 8.1, 8.2
CIM	4.19
Platforms	Platform independent
Vendor Products	Check Point Software R81, Checkpoint Endpoint client version E84.30, Checkpoint Management server version: R80.40

Fixed issues

Version 1.0.1 of the Splunk Add-on for Check Point Log Exporter contains the following fixed issues.

- The extractions for sender, recipient, subject have been updated.
- Updated the extraction for CIM field rule from policy field in the log-line.
- A new MV field remediated_file_list has been created to list the names of the remediated files from field remediated_files

Known issues

Version 1.0.1 of the Splunk Add-on for Check Point Log Exporter has the following known issues.

Third-party software attributions

Version 1.0.1 of the Splunk Add-on for Check Point Log Exporter does not incorporate any third-party libraries.

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Check Point Log Exporter was released on April 14, 2021.

About this release

Version 1.0.0 of the Splunk Add-on for Check Point Log Exporter is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.0, 8.1, 8.2
CIM	4.19
Platforms	Platform independent
Vendor Products	Check Point Software R81, Checkpoint Endpoint client version E84.30, Checkpoint Management server version: R80.40

New and updated features

The following are features provided by the new Splunk Add-on for Check Point Log Exporter version 1.0.0.

- Provides migration from the Checkpoint App for Splunk. The add-on contains the data collection and data extraction logic and CIM complaint mappings.
- If your Splunk environment has the Splunk Add-on for Checkpoint OPSEC LEA installed, then the event feed from that TA needs to be disabled to prevent data duplication in your Splunk environment. Refer to the Migrate section for further details.
- Support for Syslog data ingestion using the Log Exporter in the following formats and source types:
- Latest version of Check Point Gaia supported R81, Checkpoint Endpoint client version E84.30, Checkpoint Management server version: R80.40.
- Latest CIM version supported: 4.19
    - ♦ SC4S support for both splunk & syslog log format
    - ♦ Compatibility/Easy Migration from Checkpoint App

The following products are currently supported in the add-on. The mapping of the sources is based on the names of the products.

Product	Source
Scheduled system update	checkpoint:audit
WEB_API	checkpoint:audit
SmartDashboard	checkpoint:audit
System Monitor	checkpoint:audit
Log Update	checkpoint:audit
license-mgmt	checkpoint:audit
smart_event	checkpoint:audit
SmartConsole	checkpoint:audit
SmartEvent Client	checkpoint:audit
SmartUpdate	checkpoint:audit
WEB-UI	checkpoint:audit
SmartView	checkpoint:audit
Security Gateway/Management	checkpoint:audit

SmartDefense	checkpoint:audit
Smart Defense	checkpoint:audit
Web_API_internal	checkpoint:audit
Eventia Analyzer Client	checkpoint:audit
SmartProvisioning Connector	checkpoint:audit
SmartLSM Endpoint Security Console	checkpoint:audit
SmartLSM	checkpoint:audit
ROBO GUI	checkpoint:audit
Management Blade	checkpoint:audit
Connectra	checkpoint:audit
Check Point Security Management Server	checkpoint:audit
MTA	checkpoint:email
Anti-Spam	checkpoint:email
Anti Spam	checkpoint:email
Endpoint Management	checkpoint:endpoint
Core	checkpoint:endpoint
Endpoint Compliance	checkpoint:endpoint
MEPP	checkpoint:endpoint
Media Encryption & Port Protection	checkpoint:endpoint
Endpoint Security Console	checkpoint:endpoint
Firewall	checkpoint:firewall
DLP	checkpoint:firewall
Application Control	checkpoint:firewall
RAD	checkpoint:firewall
HTTPS Inspection	checkpoint:firewall
Compliance	checkpoint:firewall
Compliance Blade	checkpoint:firewall
VPN-1 & Firewall-1	checkpoint:firewall
Network Security	checkpoint:firewall
IPS	checkpoint:ids
WIFI	checkpoint:ids
Wifi	checkpoint:ids
Cellular	checkpoint:ids
Threat Emulation	checkpoint:ids_malware
New Anti Virus	checkpoint:ids_malware

Anti-Virus	checkpoint:ids_malware
Anti-Bot	checkpoint:ids_malware
Threat Extraction	checkpoint:ids_malware
Anti-Ransomware	checkpoint:ids_malware
Anti-Exploit	checkpoint:ids_malware
Forensics	checkpoint:ids_malware
OS Exploit	checkpoint:ids_malware
Application	checkpoint:ids_malware
Text Message	checkpoint:ids_malware
Network Access	checkpoint:ids_malware
Zero Phishing	checkpoint:ids_malware
Anti-Malware	checkpoint:ids_malware
Anti Malware New Anti Virus	checkpoint:ids_malware
IOS Profile	checkpoint:network
Device	checkpoint:network
Mobile Access	checkpoint:network
WIFI Network	checkpoint:network
VPN	checkpoint:sessions
Mobile App	checkpoint:sessions
Mobile	checkpoint:sessions
URL filtering	checkpoint:web

When Product is not available, and only the subproduct is present in the event, the source assignment is as follow:

subproduct	source
VPN	checkpoint:sessions
VPN-1	checkpoint:sessions

Fixed issues

Version 1.0.0 of the Splunk Add-on for Check Point Log Exporter contains the following fixed issues.

Known issues

Version 1.0.0 of the Splunk Add-on for Check Point Log Exporter has the following known issues.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for Check Point Log Exporter does not incorporate any third-party libraries.