Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Check Point Syslog

Configuration Guide

April 15, 2017

Configuration Guide

SmartConnector for Check Point Syslog

April 15, 2017

Copyright © 2016 – 2017 Hewlett Packard Enterprise Development LP

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
05/15/2017	Updated configuration information.
02/15/2017	Updated versions supported paragraph. Added remote system logging configuration information.
12/15/2016	Added information clarifying supported events.
11/30/2016	Updated installation procedure for setting preferred IP address mode. Added troubleshooting information.
02/15/2016	First release of SmartConnector documentation.

Contents

SmartConnector for Check Point Syslog

This guide provides information for installing the SmartConnector for Check Point Syslog and for configuring the device for syslog event collection. Check Point with Gaia Operating System R77.30 is supported. The Check Point Syslog connector supports the same events as the Check Point OPSEC NG connector as well as Provider-1 (now known as Multi-Domain Management) events. See table below for supported modules.

Product Overview

Check Point Endpoint Security protects PCs and eliminates the need to deploy and manage multiple agents by combining firewall, anti-virus, anti-spyware, full disk encryption, media encryption with port protection, network access control, program control, and VPN.

The following table indicates the modules supported by the connector for the initially supported R77.30 version:

Module	R77.30
Anti-bot	X
Anti-spam	X
Anti-virus	X
Application Control	X
Data Loss Prevention	X
Email Security	X
Firewall and VPN	X
Identity Awareness	X
IPS	X
URL Filtering	X

Configuration

Check Point's Long Term Evolution (LTE) feature adds support for sending Check Point Logs to a Syslog Server. LTE is supported on Gaia Security Gateways of R77.30 and higher, and requires the R77.30 Add-On (see sk105412 http://supportcontent.checkpoint.com/solutions?id=sk105412) on the Security Management Server or Multi-Domain Server.

Information in the configuration section of this guide has been derived from the *Check Point Firewall R77 Versions Administration Guide*. See that document for complete configuration information.

Enable System Logging on Gaia Portal

1 In the Gaia portal, go to **System Management > System Logging**.

2 In the **System Logging** section, select the following options:

Send audit logs to management server upon successful configuration
Send audit logs to syslog upon successful configuration

3 Save your changes before exiting the portal.

Send Check Point Logs to a Syslog Server

You can configure gateways to send logs directly to syslog servers by first defining syslog servers, then updating the logging properties of the gateways. Note that IPv6 and software blade logs are not supported.

Define a Syslog Server

To define a syslog server:

1 In SmartDashboard, click the **Firewall** tab.

2 In the **Servers and OPSEC Applications** object tree, right-click **Servers > New > Syslog**.

3 In the **Syslog Properties** window, enter or select values for the following:

Name
Optional comment
Host
Port (Default = 514)
Version (BSD Protocol or Syslog Protocol)

Configure a Gateway to Send Logs to Syslog Servers

You can configure a gateway to send logs to multiple syslog servers. Make sure the syslog servers are the same type: BSD Protocol or Syslog Protocol.

To send the logs from a gateway to syslog servers:

1 In SmartDashboard, go to **Gateway Properties > Logs**.

2 In the **Send logs and alerts to these log servers** table, click the green button to add syslog servers.

3 Click **OK**.

4 Install policy.

Remote System Logging

Configure the settings for the system logs, including sending them to a remote server. Make sure to configure the remote server to receive the system logs.

Configure Remote System Logging – WebUI

This section includes procedures for configuring system logging to remote servers using the WebUI.

To send system logs using the WebUI:

1 In the tree view, click **System Management > System Logging**.

2 Click **Add**. The **Add Remote Server Logging Entry** window opens.

3 In **IP Address**, enter the IP address of the remote server.

4 In **Priority**, select the severity level of the logs that are sent to the remote server.

5 Click **OK**.

Configure Remote System Logging - CLI (syslog)

To send system logs to a remote server:

```
add syslog log-remote-address <remote ip> level <severity>
```

To stop sending system logs to a remote server:

```
delete syslog log-remote-address <remote ip> level <severity>
```

To configure the file name of the system log:

```
set syslog filename <file>
```

To show the system logging settings:

```
show syslog all
            filename
            log-remote-addresses
```

Parameter	Description
syslog	Configures the system logging.
log-remote-access	Configures remote IP address for system logging.
level	Filters a severity level for the system logging.
filename	Configures or shows the file name of the system log.

Parameter Value	Description
<remote ip>	IP address of remote computer.
<severity>	Syslog event severity level: emerg, alert, crit, err, warning, notice, info, debug, or all.
<file>	System log file name.

Example:

```
add syslog log-remote-address 111.0.2.1 level all
set syslog filename system_logs
show syslog filename
```

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

Syslog Daemon
Syslog Pipe
Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.

Messages longer than 1024 bytes may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file (`rsyslog.conf`) can be added to write the events to either a ***file*** or a system ***pipe*** and the ArcSight SmartConnector can be configured to read the events from it. **In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon.**

The **Syslog Pipe** SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The **Syslog File** SmartConnector is similar to the Pipe SmartConnector; however, this SmartConnector monitors events written to a syslog file (such as `messages.log`) rather than to a system pipe.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the **/etc/rsyslog.conf** file, which contains specific details about which events to write to files, write to pipes, or send to another host. First, create a pipe or a file; then modify the **/etc/rsyslog.conf** file to send events to it.

For syslog pipe:

1 Create a pipe by executing the following command:

```
mkfifo /var/tmp/syspipe
```

2 Add the following line to your **/etc/rsyslog.conf** file:

```
*.debug  /var/tmp/syspipe
```

or

```
*.debug  |/var/tmp/syspipe
```

depending on your operating system.

3 After you have modified the file, restart the syslog daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.

On RedHat Linux, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

```
kill -HUP `cat /var/run/syslog.pid´
```

This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

Syslog Daemon
Syslog Pipe
Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file

connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

1 Download the SmartConnector executable for your operating system from the HPE SSO site.

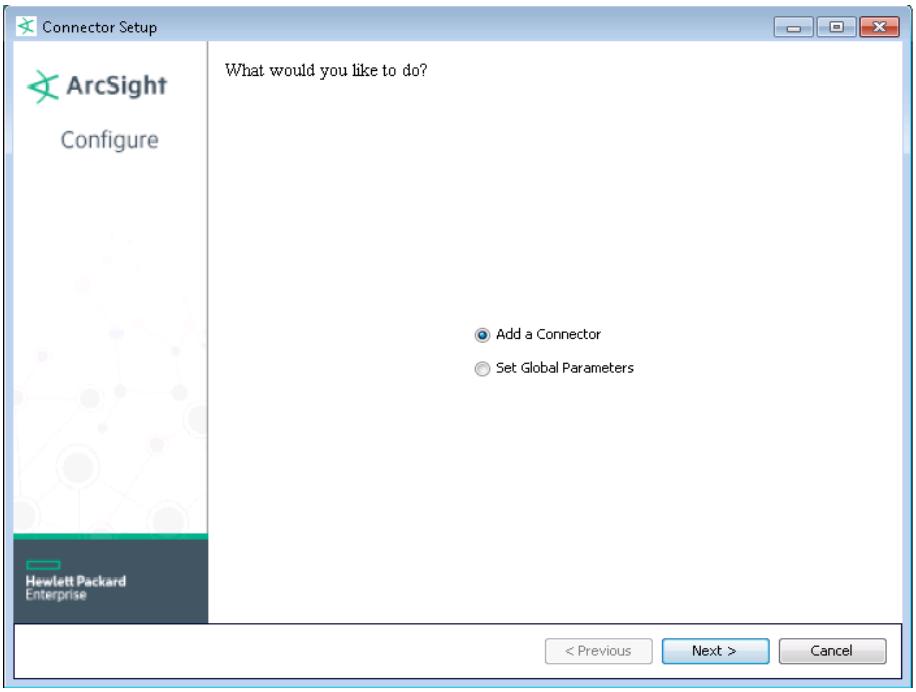
2 Start the SmartConnector installation and configuration wizard by running the executable.

When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	If both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is IPv4.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2. Select **Syslog Daemon, Pipe, or File** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Syslog Daemon Parameters	*Network port*	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe

Syslog File Parameters	*File Absolute Path Name*	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux).
		A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation.
		For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example:
		`filename'yyyy-MM-dd'.log;`
		For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:
		`filename'%d,1,99,true'.log;`
		Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.

	Reading Events Real Time or Batch	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
	Action Upon Reaching EOF	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
	File Extension If Rename Action	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

Check Point may obfuscate some confidential fields, showing some like '***Confidential***'. To see these fields without obfuscation, contact Check Point Support for the CPLogToSyslog hot fix and apply the hotfix to the management server. There is also a Multi-Domain Management CPLogToSyslog hotfix available from Check Point.

Check Point Common Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	dst
Destination Service Name	One of (service_id, service)
Device Action	Action
Device Address	deviceAddress
Device Custom String 3	message
Device Event Category	'SecurityLog'
Device Event Class ID	One of (Action, event_name, malware_action, auth_status, one of (scan direction, all of (product, 'Event') 'Scan Summary'))
Device External ID	deviceID
Device Facility	product_family
Device Product	One of (message, 'product=')
Device Receipt Time	datetime
Device Vendor	'Check Point'
Name	One of (Action, event_name, malware_action, auth_status, one of (scan direction, all of (product, 'Event') 'Scan Summary'))
Source Address	src
Source Port	s_port
Transport Protocol	One of (proto, Proto)

Check Point Anti-bot (Anti Malware) Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination Host Name	dst_machine_name
Destination User Name	dst_user_name
Device Custom String 1	malware_rule_name
Device Custom String 2	protection_id
Device Custom String 3	Protection Type
Device Custom String 4	Protection name
Device Custom String 5	Source OS
Device Custom String 6	scan direction
Device Severity	severity
Message	reason
Reason	reason
Request Client Application	web_client_type
Request URL	resource

ArcSight ESM Field	Device-Specific Field
Source Host Name	src_machine_name
Source User Name	One of (src_user_name, user)

Check Point Anti-Spam Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	dst_machine_name
Destination User Name	dst_user_name
Device Custom Number 1	Recipients Number
Device Custom String 1	email_id
Device Custom String 2	email_message_id
Device Custom String 3	email_spool_id
Device Custom String 4	email_control
Device Custom String 5	email_session_id
Device Event Category	email_spam_category
Message	One of (reason, email_control_analysis)
Source Host Name	src_machine_name
Source User Name	src_user_name

Check Point Anti-Virus Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination DNS Domain	Destination DNS Hostname
Device Custom String 1	malware_rule_name
Device Custom String 2	protection_id
Device Custom String 3	Protection Type
Device Custom String 4	Protection name
Device Custom String 5	Source OS
Device Severity	severity
File Name	file name
File Type	file_type
Message	One of (description, information)
Request Client Application	web_client_type
Request URL	resource
Source Host Name	src_machine_name
Source User Name	One of (src_user_name, user)

Check Point Application Control Event Mapppings

ArcSight ESM Field	Device-Specific Field
Bytes In	received_bytes
Bytes Out	sent_bytes

ArcSight ESM Field	Device-Specific Field
Destination Host Name	des_machine_name
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (dst_user_name, UserCheck)
Device Custom String 1	app_rule_name
Device Custom String 3	app_rule_id
Device Custom String 4	user_status
Device Custom String 5	UserCheck_Configuration_Level
Device Custom String 6	frequency
Device Event Category	app_category
Device Outbound Interface	UserCheck_Interaction_name
Event Outcome	Update Status
File ID	snid
File Size	bytes
Message	portal_message
Reason	reason
Request Client Application	web_client_type
Request URL	resource
Source Host Name	src_machine_name

Check Point Audit Event Mappings

ArcSight ESM Field	Device-Specific Field
Category Outcome	Audit Status (Success, Failure)
Destination Host Name	Machine
Destination User Name	Administrator
Device Action	Action
Device Custom String 2	Subject
Device Custom String 3	ObjectTable
Device Custom String 4	Operation Number
Device Custom String 5	ObjectName
Device Custom String 6	PolicyName
Device Event Category	'AuditLog'
Device Event Class ID	One of (Operation, 'AuditLog')
Device Facility	product_family
External ID	Uid
Message	One of (all of (one of (TCP packet out of state, tcp_flags, FieldsChanged, Additional Info)
Name	One of (Operation, 'AuditLog')
Source Address	client_ip

Check Point DLP Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	dlp_transport
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (dlp_recipients, UserCheck)
Device Custom String 1	dlp_rule_name
Device Custom String 2	rule
Device Custom String 3	incident_extension
Device Custom String 4	user_status
Device Custom String 5	UserCheck_Confirmation_Level
Device Custom String 6	scan direction
Device Event Category	dlp_categories
Device Outbound Interface	UserCheck_Interaction_name
Device Severity	severity
External ID	dlp_fule_uid
File Name	dlp_file_name
File Size	message_size
Message	One of (information, portal_message, dlp_violation_description, dlp_action_reason)
Source NT Domain	from

Check Point Email Security (imap, pop-3, smtp, ldap) Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	dst_machine_name
Destination Translated Address	xlatedst
Destination User Name	dst_user_name
Device Custom Number 1	email_recipients_num
Device Custom String 1	eamil_id
Device Custom String 2	email_message_id
Device Custom String 3	email_spool_id
Device Custom String 4	email_control
Device Custom String 5	email_session_id
Message	email_control_analysis
Source Host Name	src_machine_name
Source User Name	src_user_name

Check Point Identity Awareness Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	connectivity_state
Device Custom String 2	identity_src
Device Custom String 3	identity_type
Device Custom String 4	termination_reason

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	auth_method
Device Custom String 6	src_user_group
Device Event Category	ctrl_category
Device Version	client_version
File ID	snid
File Path	src_machine_group
Message	description
Request Client Application	client_name
Request Context	origin_sic_name
Source Host Name	src_machine_name
Source NT Domain	domain_name
Source User Name	One of (src_user_name, user)
Source User Privileges	roles

Check Point SmartDefense Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	dst_machine_name
Destination User Name	dst_user_name
Device Custom Number 1	during_sec
Device Custom Number 2	fragments_dropped
Device Custom Number 3	Update Version
Device Custom String 1	voip_log_type
Device Custom String 2	Protection Type
Device Custom String 3	protection_id
Device Custom String 4	TCP flags
Device Custom String 5	content_type
Device Custom String 6	Protection Name
Device Severity	Severity
File ID	snid
Message	One of (message, attack, Attack Info, description)
Request Client Application	web_client_type
Request URL	resource
Source Host Name	src_machine_name
Source User Name	One of (src_user_name, user)

Check Point URL Filtering Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination Host Name	dst_machine_name
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (dst_user_name, UserCheck)

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	limit_requested
Device Custom Number 2	limit_applied
Device Custom String 1	app_rule_name
Device Custom String 3	app_rule_id
Device Custom String 4	user_status
Device Custom String 5	Update Status
Device Custom String 6	UserCheck_Confirmation_Level
Device Event Category	app_category
Device Outbound Interface	UserCheck_Interaction_name
Event Outcome	update status
File ID	snid
Message	portal_message
Request Client Application	web_client_type
Request URL	resource
Source Host Name	src_machine_name
Source User Name	One of (src_user_name, user)

Check Point VPN-1 and FireWall-1 Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination Host Name	dst_machine_name
Destination Translated Address	xlatedst
Destination Translated Port	xlatesport
Destination User Name	dst_user_name
Device Custom String 1	rule
Device Custom String 2	policy
Device Custom String 3	ICMP
Device Custom String 4	ICMP Code
Device Custom String 5	ICMP Type
Device Inbound Interface	inzone
Device Outbound Interface	outzone
File ID	snid
File Size	bytes
Message	One of (sys_message:, default device message, message_info)
Reason	reason
Source Host Name	src_machine_name
Source NT Domain	domain
Source Translated Address	xlatesrc
Source User Name	One of (src_user_name, user, User)
Start Time	event_start_time

Troubleshooting

Why do some fields show '*Confidential***'?**

Check Point may obfuscate some confidential fields, showing some like '***Confidential***'. To see these fields without obfuscation, contact Check Point Support for the CPLogToSyslog hot fix and apply the hotfix to the management server. There is also a Multi-Domain Management CPLogToSyslog hotfix available from Check Point.