Micro Focus Security ArcSight Connectors

SmartConnector for Check Point Syslog

Configuration Guide

August 24, 2019

Configuration Guide

SmartConnector for Check Point Syslog

August 24, 2019

Copyright © 2016 – 2019 Copyright 2019 Micro Focus or one of its affiliates.

Legal Notices

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice. The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus. Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms. U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
08/24/2019	Added new mappings to R77 Anti-bot (Anti Malware) Event Mappings table
08/24/2019	Added new mappings to R80 VPN-1 and FireWall-1 Event Mappings table
08/24/2019	Added support for CheckPoint R80.20 version
08/24/2019	Added and updated R80 Anti-Malware Event Mappings
08/24/2019	Updated R80 New Anti-Virus Event Mappings table

Date	Description
08/24/2019	Updated R80 Application Control Event Mappings
08/24/2019	Updated R80 Identity Awareness Event Mappings
08/24/2019	Updated R80 URL Filtering Event Mappings
08/24/2019	Updated R80 SmartDefense Event Mappings
08/24/2019	Updated R80 FG Event Mappings
08/24/2019	Updated R80 Common Audit Event Mappings
08/24/2019	Added R80 HTTPS Inspection Event Mappings table
08/24/2019	Added R80 SmartEvent Client Event Mappings table
08/24/2019	Added R80 Syslog Event Mappings table
08/24/2019	Added R80 System Monitor Event Mappings table
08/24/2019	Added R80 Connectra Event Mappings table
08/24/2019	Added R80 Application Control URL Filtering Event Mappings table
08/24/2019	Added R80 Security Gateway/Management Event Mappings table
08/24/2019	Added R80 VPN-1 and FireWall-1(+)FG Event Mappings table
08/24/2019	Updated R80 VPN-1 and FireWall-1 Event Mappings table
08/24/2019	Added R80 SmartView Monitor Event Mappings table
08/24/2019	Added R80 SmartView Tracker Event Mappings table
08/24/2019	Added R80 Logs Indexer Event Mappings table
08/24/2019	Added R80 Query-database Event Mappings table
08/24/2019	Added R80 Web-UI Event Mappings table
08/24/2019	Added R80 SmartConsole Event Mappings table
08/24/2019	Added R77 Application Control(+)URL Filtering Event Mappings table
08/24/2019	Added R77 HTTPS Inspection Event Mappings Event Mappings table
08/24/2019	Added R77 FG Event Mappings table
08/24/2019	Added R80 FG(+)VPN-1 and FireWall-1 Event Mappings table
07/24/2019	Updated R80 Common Audit Event Mappings and R80 CLI Event Mappings
06/19/2019	Added support for R80 CLI module
06/19/2019	Added R80 CLI Event Mappings table
06/19/2019	Updated R80 Common Audit Event Mappings table
12/17/2018	Updated Common Syslog Event Mappings
11/19/2018	Added "Device Host Name" to R80 and R77 Common Syslog Event Mappings.
10/24/2018	Added support for R80 FG Event Mappings. Added "Device Host Name" for R80 and R77 Common Syslog Event Mappings. Updated mappings for R80 VPN-1 and FireWall-1, R80 Application Control, R80 Identity Awareness, R80 URL Filtering, R80 Log Update and R80 VPN-1
08/20/2018	Added support for VPN-1 and Log Update Modules. Updated R80 VPN-1 and R80 Log Update Event Mappings. Updated R77 Threat Emulation Event Mappings.
07/18/2018	Added support for: Connectra, Anti Virus, Security Gateway/Management, Linux OS, Syslog, Threat Emulation, Anti Bot and Anti Virus. Added "Source Process Id", "Name", "Device Event Class Id" and "Device Action" to common mappings. Updated R77 VPN-1 and FireWall-1 Event Mappings
05/16/2018	Updated in R77 VPN-1 and FireWall-1 Event Mappings
10/20/2017	Added support for R80.10
10/17/2017	Added encryption parameters to Global Parameters. Added time zone mapping to common event mappings
09/15/2017	Added support for the following modules: ESOD, Eventia Analyzer Server, Identity Logging, and VPN-1 Edge
08/15/2017	Added "Destination Port" to common mappings.
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

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode. Added troubleshooting information
02/15/2016	First release of SmartConnector documentation

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 and R80.10 are 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 R77.30, R80.10, and R80.20 versions:

R77.30 Modules	R80.10 Modules	R80.20 Modules
Anti-bot (Anti-Malware)	Anti-Malware	Anti-Malware
Anti-Spam	Anti-Spam	Antivirus
Anti-Virus	New Anti-Virus	HTTPS Inspection
Application Control	Application Control	SmartEvent Client
Audit	Audit	Syslog
DLP (Data Loss Prevention)	DLP (Data Loss Prevention)	System Monitor
Email Security	Email Security	Connectra
ESOD	ESOD	Application Control URL Filtering
Eventia Analyzer Server	Identity Awareness	Security Gateway/Management
Identity Awareness	Identity Logging	VPN-1 and FireWall-1(+)FG
Identity Logging	SmartDefense	SmartView Monitor
SmartDefense	SmartDashboard	SmartView Tracker
URL Filtering	SmartUpdate	Logs Indexer
VPN-1 and Firewall-1	URL Filtering	Query-database
VPN-1 Edge	VPN-1 and Firewall-1	Web-UI
Connectra	Log Update	SmartConsole
Anti Virus	VPN-1	FG(+)VPN-1 and FireWall-1
Security Gateway/Management	FG	
Linux OS		
Syslog		
Threat Emulation		
Anti Bot and Anti Virus		

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.

Parameter	Description
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 Micro Focus SSO and Protect 724 sites.

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

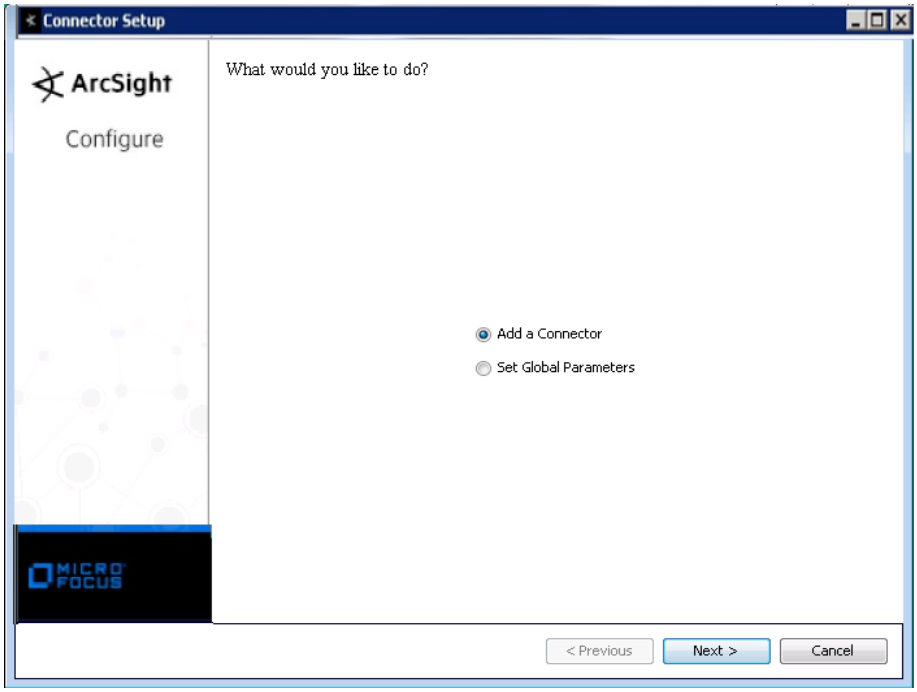
2. Start the SmartConnector installation and configuration wizard by running the executable.

> 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:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.
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	When 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. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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 proceed with "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.

R80 and R77 Common Syslog Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
Device Address	One of (deviceAddress, address)
Device Custom String 1	One of (product, blade_name)
Device Custom String 4	One of (message, message2)
Device Event Class Id	action
Device External ID	device ID
Device Host Name	host
Device Product	One of (ProductName, product, blade_name)
Device Receipt Time	one of ('UTC', datetime)
Device Time Zone	one of ('Zulu', timezone)
Device Vendor	'Check Point'
Name	action
Source Process Id	id

R80 Common Audit Event Mappings

ArcSight ESM Field	Device-Specific Field
Category Outcome	Audit Status (Success = /Success, Failure = /Failure)
Destination Host Name	__oneOf(Machine,machine)
Destination User Name	__oneOf(Administrator,administrator)
Device Action	One of (Action,action)
Device Custom String 1	'null'
Device Custom String 2	__oneOf(Subject,subject)
Device Custom String 3	One of (ObjectTable,objecttable)
Device Custom String 4	One of (Operation Number,operation_number)
Device Custom String 5	__oneOf(ObjectName,objectname)
Device Custom String 6	All of (One Of(policy_id_tag),One of (Additional Info,additional_info),One of (ObjectType,objecttype),One of (Operation,operation),One of (ObjectName,objectname))
Device Event Category	'AuditLog'
Device Event Class ID	__oneOf(Operation,operation)
Device Facility	product_family
Event Name	__oneOf(Operation,operation) (example: One of (One of (Operation,operation), 'AuditLog'))
External ID	Uid
Message	One of (all of ('TCP packet out of state:', TCP packet out of state,';', ' tcp_flags:', tcp_flags,";"), One of (FieldsChanges,fieldsChanges), One of(Additional Info,additional_info))
Name	One of (Operation,operation)
Source Address	client_ip

R80 Common Security Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	dst
Destination Port	One of (d_port, service)
Destination Service Name	One of (service_id, service)
Device Action	One of (action,Action)
Device Custom String 1	'null'
Device Event Category	'SecurityLog'
Device Event Class ID	One of (action, Action, event_name, malware_action, auth_status short_desc, description, message_info, activity, scan directin, all of (one of (ProductName, product), 'l', One of (subscription_stat, 'Event')), 'Scan Summary')
Device Facility	product_family
Name	One of (action, Action, event_name, malware_action, auth_status short_desc, description, message_info, activity, scan direction, all of (one of (ProductName, product), 'l', One of(subscription_stat, 'Event')), 'Scan Summary')
Source Address	src
Source Port	s_port
Transport Protocol	One of (proto, Proto)

R80 Anti-Malware Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	One of (Suppressed logs,suppressed_logs)
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination Custom String 5	Source OS
Destination Translated Address	scope
Destination User Name	aba_customer
Device Custom Date 1	time
Device Custom Date 2	subs_exp
Device Custom Floating Point 2	One of (Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Custom Number 3	Confidence Level
Device Custom String 1	malware_rule_name
Device Custom String 2	Protection Type
Device Custom String 3	protection_id
Device Custom String 4	Protection name
Device Direction	ifdir
Device Facility	malware_family
Device Host Name	One of (Origin,origin)
Device Severity	One of (Severity, severity)
End Time	LastUpdateTime
Event Outcome	Update Status
File Hash	malware_rule_id
File ID	log_id
File Name	packet_capture_name

ArcSight ESM Field	Device-Specific Field
File Path	packet_capture_unique_id
File Type	log_type
Message	One of (description, long_desc, next_update_desc, short_desc, subscription_stat_desc)
Old File ID	session_id
Old File Path	ifname
Old File Type	type
Reason	reason
Request Client Application	web_client_type
Request Context	One of (OriginSicName,origin_sic_name)
Request URL	resource
Source Host Name	src_machine_name
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User Name	One of (src_user_name, user)

R80 Anti-Spam Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	aba_customer
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	Recipients Number
Device Custom Number 2	ContentVersion
Device Custom String 1	Both (rule, rule_name)
Device Custom String 3	email_control
Device Custom String 5	email_session_id
Device Event Category	email_spam_category
Device Host Name	Origin
File ID	LogId
File Type	log_type
Old File Type	type
Request Context	OriginSicName
Source Port	sport_svc
Source Process ID	is_first_for_luuid

R80 Application Control Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	Suppressed logs
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (UserCheck, aba_customer)

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point 2	One of (Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Floating Point1	app_id
Device Custom Floating Point4	flags
Device Custom Number 1	ContentVersion
Device Custom Number 3	app_risk
Device Custom String 1	app_rule_name
Device Custom String 3	app_rule_id
Device Custom String 4	app_properties
Device Custom String 6	UserCheck_Confirmation_Level
Device Custom String5	ifname
Device Direction	ifdir
Device Event Category	One of (app_category, matched_category)
Device Host Name	One of(Origin,origin)
Device Severity	Severity
End Time	LastUpdateTime
Event Outcome	Update Status
File ID	snid
File Size	bytes
File Type	log_type
Message	One of (app_desc, portal_message)
Old File ID	log_id
Old File Name	appi_name
Old File Type	type
Reason	description
Request Client Application	web_client_type
Request Context	One of(OriginSicName,origin_sic_name)
Request URL	resource
Source Host Name	src_machine_name
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User Name	One of (src_user_name, user)

R80 DLP Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	dlp_transport
Destination Process Name	dlp_data_type_name
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (dlp_recipients, UserCheck, aba_customer)
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Custom String 1	dlp_file_name

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	rule
Device Custom String 3	incident_extension
Device Custom String 4	rule_uid
Device Custom String 5	user_status
Device Custom String 6	UserCheck_Confirmation_Level
Device Event Category	dlp_categories
Device Host Name	Origin
Device Severity	severity
End Time	LastUpdateTime
External ID	dlp_rule_uid
File ID	log_id
File Name	dlp_file_name
File Size	message_size
File Type	log_type
Message	One of (portal_message, dlp_violation_description)
Old File ID	dlp_type_uid
Old File Type	type
Reason	dlp_action_reason
Request Context	OriginSicName
Request URL	outgoing_url
Source NT Domain	from
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User Name	One of (src_user_name, user)

R80 CLI Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Custom Floating Point 3	sequencenum
Device Custom Number 1	version
Device Direction	ifdir
Device Host Name	origin
File ID	loguid
Request Context	originsicname

R80 Email Security Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	dst_machine_name
Destination Translated Address	xlatedst
Destination Translated Port	xlatedport_svc
Destination User Name	One of (dst_user_name, aba_customer)

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	email_recipients_num
Device Custom Number 2	ContentVersion
Device Custom String 1	Both (rule, rule_name)
Device Custom String 4	email_control
Device Custom String 5	email_session_id
Device Host Name	Origin
Device Inbound Interface	inzone
Device Outbound Interface	outzone
End Time	LastUpdateTime
File ID	snid
File Type	log_type
Message	message_info
Old File ID	LogId
Old File Type	type
Request Context	OriginSicName
Source Host Name	src_machine_name
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	xlatesrc
Source Translated Port	xlatesport_svc
Source User Name	One of (src_user_name, user)

R80 ESOD Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	aba_customer
Device Custom Date 2	subs_exp
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Custom String 3	sig_ver
Device Custom String 4	update_src
Device Event Class Id	One of(All of(One of(product,blade_name),'|','Event'), All of(activity,'|',Update Status))
Device Host Name	Origin
Event Outcome	Update Status
File ID	LogId
File Type	log_type
Message	activity
Name	One of(All of(One of(product,blade_name),'|','Event'), All of(activity,'|',Update Status))
Old File Type	type
Reason	reason
Request Context	OriginSicName

ArcSight ESM Field	Device-Specific Field
Source Process ID	is_first_for_luuid

R80 Identity Awareness Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	aba_customer
Device Address	endpoint_ip
Device Custom Floating Point 2	One of (Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Floating Point4	flags
Device Custom Number 1	ContentVersion
Device Custom String 1	connectivity_state
Device Custom String 2	identity_src
Device Custom String 3	identity_type
Device Custom String 4	auth_status
Device Custom String 5	auth_method
Device Custom String 6	src_user_group
Device Direction	ifdir
Device Domain	domain_name
Device Event Category	ctrl_category
Device External Id	device_identification
Device Host Name	One of(Origin,origin)
Device Version	client_version
End Time	LastUpdateTime
File Hash	logid
File ID	snid
File Type	log_type
Message	description
Old File Id	loguid
Old File Type	type
Reason	termination_reason
Request Client Application	client_name
Request Context	One of(OriginSicName,origin_sic_name)
Source Mac Address	macsourceaddress
Source Process ID	is_first_for_luuid
Source User Name	One of (src_user_name, user)
Source User Privileges	src_user_group

R80 Identity Logging Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	aba_customer
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion

ArcSight ESM Field	Device-Specific Field
Device Host Name	Origin
File ID	LogId
File Type	log_type
Message	description
Old File Type	type
Request Context	OriginSicName
Source Address	Src
Source Host Name	src_machine_name
Source Process ID	is_first_for_luuid
Source User Name	One of (src_user_name, user)

R80 New Anti-Virus Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	One of(Suppressed logs,suppressed_logs)
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination DNS Domain	One of(Destination DNS Hostname,destination_dns_hostname)
Destination Translated Address	scope
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (UserCheck, aba_customer)
Device Custom Date 1	time
Device Custom Date 2	subs_exp
Device Custom Floating Point 2	One of(Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Custom Number 3	One of(Confidence Level,confidence_level)
Device Custom String 1	malware_rule_name
Device Custom String 2	One of(Protection Type,protection_type)
Device Custom String 3	protection_id
Device Custom String 4	One of(Protection name,protection_name)
Device Custom String 5	Source OS
Device Custom String 6	UserCheck_Confirmation_Level
Device Direction	ifdir
Device Facility	malware_family
Device Host Name	One of(Origin,origin)
Device Severity	One of (Severity, severity)
End Time	LastUpdateTime
Event Outcome	Update Status
File Hash	session_id
File ID	snid
File Name	One of(file name,packet_capture_name)
File Path	packet_capture_unique_id
File Permission	user_status
File Type	file_type

ArcSight ESM Field	Device-Specific Field
Message	One of (description, next_update_desc, subscription_stat_desc)
Old File Hash	ticket_id
Old File ID	log_id
Old File Name	packet_capture_name
Old File Permission	malware_rule_id
Old File Type	type
Reason	reason
Request Client Application	web_client_type
Request Context	One of(OriginSicName,origin_sic_name)
Request URL	resource
Source Host Name	src_machine_name
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User Name	One of (src_user_name, user)

R80 SmartDefense Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	Suppressed logs
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination User Name	aba_customer
Device Custom Date 1	time
Device Custom Date 2	policy_time
Device Custom Floating Point 1	Update Version
Device Custom Floating Point 2	One of (Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Floating Point 4	sequencenum
Device Custom Number 1	ContentVersion
Device Custom Number 2	One of (Flags,flags)
Device Custom Number 3	fragments_dropped
Device Custom String 1	Both (rule, rule_name)
Device Custom String 2	One of (Protection Type,protection_type)
Device Custom String 3	protection_id
Device Custom String 4	One of (Protection name,protection_name)
Device Custom String 5	One of (SmartDefense profile, SmartDefense Profile,smartdefense_profile)
Device Custom String 6	malware_rule_name
Device Direction	ifdir
Device Facility	source_os
Device Host Name	Origin
Device Severity	One of (Severity,severity)
File Hash	One of(description_url,industry_reference)
File ID	snid
File Name	session_id

ArcSight ESM Field	Device-Specific Field
File Path	ifname
File Permission	sub_policy_name
File Type	log_type
Message	One of ((message,Attack Info,attack_info,attack,Error,precise_error,description)
Name	attack
Old File Hash	loguid
Old File ID	log_id
Old File Name	layer_name
Old File Path	more_sources
Old File Permission	policy
Old File Type	type
Reason	reason
Request Client Application	web_client_type
Request Context	One of (OriginSicName,originsicname)
Request URL	resource
Source Host Name	src_machine_name
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User Name	One of (src_user_name, user,source)

R80 SmartDashboard Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	aba_customer
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Host Name	Origin
File ID	LogId
File Type	log_type
Old File Type	type
Request Context	OriginSicName
Source Process ID	is_first_for_luuid

R80 SmartUpdate Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	aba_customer
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Host Name	Origin
File ID	LogId

ArcSight ESM Field	Device-Specific Field
File Type	log_type
Old File Type	type
Request Context	OrigiinSicName
Source Process ID	is_first_for_luuid

R80 URL Filtering Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	Suppressed logs
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (UserCheck, aba_customer)
Device Custom Floating Point 1	app_id
Device Custom Floating Point 2	One of (Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Floating Point4	flags
Device Custom Number 1	ContentVersion
Device Custom Number 3	app_risk
Device Custom String 1	app_rule_name
Device Custom String 3	app_rule_id
Device Custom String 4	app_properties
Device Custom String 6	UserCheck_Confirmation_Level
Device Custom String5	ifname
Device Direction	ifdir
Device Event Category	One of (app_category, matched_category)
Device Host Name	One of(Origin,origin)
Device Severity	Severity
End Time	LastUpdateTime
Event Outcome	Update Status
File ID	snid
File Size	bytes
File Type	log_type
Message	One of (description, app_desc, portal_message)
Old File ID	log_id
Old File Name	appi_name
Old File Type	type
Request Client Application	web_client_type
Request Context	One of(OriginSicName,origin_sic_name)
Request URL	resource
Source Host Name	src_machine_name
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User Name	One of (src_user_name, user)

R80 VPN-1 and FireWall-1 Event Mappings

ArcSight ESM Field	Device-Specific Field
Application protocol	protocol
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination Host Name	cu_detected_by
Destination Translated Address	xlatedst
Destination Translated Port	xlatedport_svc
Destination User Name	aba_customer
Device Custom Date 1	cu_detection_time
Device Custom Date 2	Policy Date
Device Custom Floating Point 1	hit
Device Custom Floating Point 2	One of(Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Floating Point4	flags
Device Custom Number 1	ContentVersion
Device Custom Number 2	ICMP Type
Device Custom Number 3	ICMP Code
Device Custom String 1	Both (rule, rule_name)
Device Custom String 2	policy
Device Custom String 3	ICMP
Device Custom String 4	rule_uid
Device Custom String5	ifname
Device Custom String6	sig_id
Device Direction	ifdir
Device Dns Domain	Connection Direction
Device Host Name	One of(Origin,origin)
Device Inbound Interface	inzone
Device Outbound Interface	outzone
Device Severity	Severity
Event Outcome	Update Status
External ID	seqencenum
File Hash	layer_uuid
File ID	snid
File Modification Time	last_hit_time
File Name	layer_name
File Size	bytes
File Type	log_type
Message	One of (default device message, description, fw_message, information, log_sys_message, message_info, sys_message, TCP packet out of state, sys_message:)
Old File Hash	match_table.layer_uuid
Old File ID	log_id
Old File Name	match_table.layer_name
Old File Path	src_user_dn
Old File Permission	blade_name

ArcSight ESM Field	Device-Specific Field
Old File Type	type
Reason	action_reason
Request Context	One of(OriginSicName,originsicname)
Source Host Name	src_machine_name
Source NT Domain	domain
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	xlatesrc
Source Translated Port	xlatesport_svc
Source User Name	One of (src_user_name, user)
Start Time	event_start_time

R80 HTTPS Inspection Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point2	flags
Device Custom Floating Point3	sequencenum
Device Custom String 2	All of (app_category,app_properties)
Device Custom String 3	All of (https_inspection_action,https_inspection_rule_id,https_validation,https_inspection_rule_name)
Device Custom String 4	status
Device Custom String 5	ifname
Device Direction	ifdir
Device Host Name	origin
Device Severity	severity
File Id	snid
Message	description
Old File Id	failure_impact
Reason	reason
Request Context	origin_sic_name
Source User Name	One Of (src_user_name,user)

R80 SmartEvent Client Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point2	flags
Device Custom Floating Point3	sequencenum
Device Custom Number 1	update_service
Device Custom String 4	status
Device Custom String 5	failure_impact
Device Direction	ifdir
Device Host Name	origin
Device Severity	severity

ArcSight ESM Field	Device-Specific Field
Message	description
Reason	reason

R80 Syslog Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Date 2	syslog_date
Device Custom Floating Point2	flags
Device Custom Floating Point3	sequencenum
Device Custom String 5	ifname
Device Direction	ifdir
Device Facility	facility
Device Host Name	origin
Device Severity	syslog_severity
Message	default_device_message
Source User Name	user

R80 Syslog Monitor Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point2	flags
Device Custom String 2	All of (event,parameter,alert,condition,current_value)
Device Custom String 4	system_alert_message
Device Custom String 5	ifname
Device Direction	ifdir
Device Host Name	origin
Message	sys_message:
oldFileId	loguid

R80 Connectra Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	office_mode_ip
Destination Host Name	hostname
Destination Mac Address	mac_address
Destination NtDomain	domain_name
Device Custom Date 1	time
Device Custom Floating Point2	flags
Device Custom String 1	tunnel_protocol
Device Custom String 4	methods
Device Custom String 5	auth_encryption_methods
Device Direction	ifdir
Device Host Name	origin

ArcSight ESM Field	Device-Specific Field
Old File Id	loguid
Request Context	origin_sic_name

R80 Application Control URL Filtering Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point2	flags
Device Custom String 4	update_status
Device Direction	ifdir
Device Host Name	origin
Device Severity	severity
Old File Id	loguid
Request Context	origin_sic_name

R80 Security Gateway/Management Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	status
Device Custom Date 1	time
Device Custom Floating Point2	flags
Device Custom Number 2	update_service
Device Custom String 2	failure_impact
Device Custom String 3	comment
Device Direction	ifdir
Device Host Name	origin
Device Severity	severity
Message	description
Old File Id	loguid
Reason	reason

R80 VPN-1 and FireWall-1(+)FG Event Mappings

ArcSight ESM Field	Device-Specific Field
bytesIn	c_in_bytes
bytesOut	c_out_bytes
Device Custom Date 1	Both (date,hour)
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	ContentVersion
Device Custom String 1	Both (rule,rule_name)
Device Custom String 2	All of (s_in_total_drops,s_in_exceed_drops,c_out_total_drops,c_out_exceed_drops)
Device Custom String 4	All of (s_in_bytes,s_out_bytes)
Device Custom String 5	One of(InterfaceName,Interface)

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	All of (client_inbound_packets,client_outbound_packets,server_inbound_packets, server_outbound_packets,client_inbound_bytes,client_outbound_bytes, server_inbound_bytes,server_outbound_bytes,client_inbound_interface, client_outbound_interface,server_inbound_interface,server_outbound_interface)
Device CustomFloating Point 2	Flags
Device Direction	IfDir
Device Host Name	Origin
DeviceCustomString3	All of (fg-1_client_in_rule_name,fg-1_client_out_rule_name,fg-1_server_in_rule_name,fg-1_server_out_rule_name)
File Id	LogId
File Size	bytes
File Type	log_type
Old File Type	type
Request Context	OriginSicName
Source Port	sport_svc
Source Process Id	is_first_for_luuid
Start Time	start_time

R80 FG(+)VPN-1 and FireWall-1 Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	received_bytes
Destination User Name	aba_customer
Device Custom Date1	Both (date," ",hour)
Device Custom Floating Point2	Flags
Device Custom Floating Point3	SequenceNum
Device Custom Number 1	ContentVersion
Device Custom Number 2	NAT_addtnl_rulenum
Device Custom Number 3	NAT_rulenum
Device Custom String 1	Both (rule,rule_name)
Device Custom String 2	community
Device Custom String 3	fw_subproduct
Device Custom String 4	scheme,methods
Device Custom String 5	One of (InterfaceName,Interface)
Device Custom String 6	vpn_feature_name
Device Direction	IfDir
Device Host Name	One of (Origin,origin)
Device Inbound Interface	inzone
Device Outbound Interface	outzone
End Time	LastUpdateTime
File Hash	peer gateway
File Id	LogId
File Type	log_type
Old File Type	type
Request Context	One of (OriginSicName,originsicname)
Source Port	sport_svc

ArcSight ESM Field	Device-Specific Field
Source Process ID	is_first_for_luuid
Source Translated Address	xlatesrc
Source Translated Port	xlatesport_svc

R80 SmartConsole Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	ip_address
Device Action	action
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Custom Floating Point 3	sequencenum
Device Direction	ifdir
Device Host Name	origin
Event Outcome	audit_status
File ID	logic_changes
File Name	session_name
File Type	session_uid
Old File ID	loguid
Old File Type	uid
Request Context	origin_sic_name

R80 SmartView Monitor Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Direction	ifdir
Device Host Name	origin
Old File ID	loguid
Request Context	origin_sic_name

R80 SmartView Tracker Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Direction	ifdir
Device Host Name	origin
Old File ID	loguid
Request Context	origin_sic_name

R80 Logs Indexer Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Direction	ifdir
Device Host Name	origin
Old File ID	loguid
Request Context	origin_sic_name

R80 Query-database Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Direction	ifdir
Device Host Name	origin
Old File ID	loguid
Request Context	origin_sic_name

R80 Line-editor Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Direction	ifdir
Device Host Name	origin
Old File ID	loguid
Request Context	origin_sic_name

R80 Web-UI Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Direction	ifdir
Device Host Name	origin
Old File ID	loguid

R77 Common 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

ArcSight ESM Field	Device-Specific Field
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 ('TCP packet out of state:',TCP packet out of state,';','tcp_flags:',tcp_flags,";"), FieldsChanges, Additional Info)
Name	One of (Operation, 'AuditLog')
Source Address	client_ip

R77 Common Security Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	dst
Destination Port	One of (d_port, service)
Destination Service Name	One of (service_id, service)
Device Action	Action
Device Custom String 1	'null'
Device Event Category	'SecurityLog'
Device Event Class ID	One of (Action, event_name, malware_action, auth_status, one of (all of (one of (product, blade_name), One of(subscription_stat, 'Event')) 'Scan Summary'))
Device Facility	product_family
Name	One of (Action, event_name, malware_action, auth_status, one of (all of (one of (product, blade_name), One of(subscription_stat, 'Event')) 'Scan Summary'))
Source Address	src
Source Port	s_port
Transport Protocol	One of (proto, Proto)

R77 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 Floating Point 1	unique_detected_hour
Device Custom Floating Point 2	unique_detected_day
Device Custom Floating Point 3	unique_detected_week
Device Custom Floating Point 4	unique_detected_mail
Device Custom Number 1	scan_hosts_hour
Device Custom Number 2	scan_hosts_day
Device Custom Number 3	scan_hosts_week
Device Custom String 1	malware_rule_name

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

R77 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

R77 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

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

R77 Application Control 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)
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_Confirmation_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
Source User Name	One of (src_user_name, user)

R77 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_rule_uid

ArcSight ESM Field	Device-Specific Field
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

R77 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	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
Message	email_control_analysis
Source Host Name	src_machine_name
Source User Name	src_user_name

R77 ESOD Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	activity
Device Custom Date 1	subs_exp (Subs Exp)
Device Custom String 3	sig_ver (Sig Version)
Device Custom String 4	update_src (Update Src)
Device Event Class Id	One of(All of(One of(product,blade_name),'|','Event'), All of(activity,'|',Update Status))
Event Outcome	Update Status
Name	One of(All of(One of(product,blade_name),'|','Event'), All of(activity,'|',Update Status))
Reason	reason

R77 Eventia Analyzer Server Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Machine
Destination User Name	Administrator
Device Custom Number 1	Operation Number
Device Custom String 1	session_id (Session ID)
Device Custom String 2	Subject
Device Custom String 3	Additional Info
Name	Operation

ArcSight ESM Field	Device-Specific Field
Source Address	client_ip

R77 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
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

R77 Identity Logging Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point 1	information (Minutes)
Device Custom String 1	One of (src_user_name, user)(Email Information)
Message	information
Source Address	Src
Source Host Name	src_machine_name
Source User Name	One of (src_user_name, user)

R77 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

ArcSight ESM Field	Device-Specific Field
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)

R77 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)
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)

R77 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 User Name	dst_user_name
Device Custom Date 1	All of (date,' ',hour)
Device Custom Number 1	rule

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	NAT_addtnl_rulenum
Device Custom Number 3	NAT_rulenum
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 Custom String 6	Interface
Device Inbound Interface	inzone
Device Outbound Interface	outzone
File ID	One of (snid, all of ('rule_uid: ',rule_uid))
File Size	bytes
File Type	type
Message	One of (sys_message:, default device message, message_info, TCP packet out of state)
Reason	reason
Source Host Name	src_machine_name
Source NT Domain	domain
Source Translated Address	xlatesrc
Source Translated Port	xlatesport
Source User Name	One of (src_user_name, user, User)
Start Time	event_start_time

R77 VPN-1 Edge Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	dst
Device Custom String 1	rule
Device Custom String 3	peer gateway
Device Custom String 6	scan direction
Message	msg
Source Address	src

R77 Connectra Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Translated Address	assigned_IP:
Device Custom Number1	client_build
Device Custom String 1	All of ('compliance_check: ',compliance_check,'|','compliance_name: ',compliance_name)
Device Custom String 2	reject_id
Device Custom String 5	auth_encryption_methods
Device Custom String 6	host_ip
Device Version	client_version
Event Outcome	status
File Hash	All of ('office_mode_ip: ',office_mode_ip)

ArcSight ESM Field	Device-Specific Field
File Id	All of ('Device_identification: ',Device_identification)
File Path	All of ('access_status: ',access_status)
Message	All of ('OM: ',OM:,'|','description: ',description)
Old File Hash	All of ('methods: ',methods)
Old File Id	All of ('session_uid: ',session_uid)
Reason	reason
Request Client Application	browser
Source Host Name	Hostname
Source Mac Address	mac_address
Source NT Domain	domain_name
Source Translated Address	old_IP:
Source User Name	All of ('User: ',User,'|','user_dn: ',user_dn,'|','user: ',user)
Source User Privileges	user_group
Start Time	login_timestamp

R77 Anti Virus Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Severity	severity
Event Outcome	update status
Message	description
Reason	reason

R77 Security Gateway/Management Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	status
Device Custom String 3	version
Device Custom String 4	update_service
Device Event Class Id	One of (All of (One of(product,blade_name),"|","Event"),All of(description,"|",status))
Device Severity	severity
Message	All of ('comment: ',comment,'|','description: ',description,'|','failure_impact: ',failure_impact)
Name	One of (All of (One of (product,blade_name),"|","Event"),All of(description,"|",status))
Reason	reason

R77 Linux OS Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Facility	facility
Device Severity	syslog_severity
Event Outcome	login_status
Message	default_Device_message
Source Address	Src

ArcSight ESM Field	Device-Specific Field
Source Process Name	Application
Source User Name	User

R77 Syslog Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	syslog_date
Device Facility	facility
Device Severity	syslog_severity
Message	default_Device_message
Source User Name	User

R77 Threat Emulation Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	dst_machine_name
Destination User Name	dst_user_name
DestinationTranslatedAddress	scope
Device Custom String 1	UUid
Device Custom String 2	Protection Type
Device Custom String 3	to
Device Custom String 4	from
Device Custom String 6	malware_rule_id
Device Severity	severity
File Hash	All of ('file_md5: ',file_md5)
File Id	snid
File Name	file_name
File Size	file_size
File Type	file_type
Message	All of ('description: ',description,'|','blade_description: ',blade_description,'|','update_description: ',update_description,'|','subscription_description: ',subscription_description)
Old File Hash	All of ('file_sha1: ',file_sha1)
Old File Id	All of('session_id: ',session_id)
Old File Name	All of ('file_sha256: ',file_sha256)
Old File Type	All of('log_id: ',log_id)
Reason	Errors
Requested URL	resource
Source Host Name	src_machine_name
Source Translated Address	proxy_src_ip
Source User Name	All of ('src_user_name: ',src_user_name,'|','user: ',user)

R77 Application Control(+)URL Filtering Event Mappings

ArcSight ESM Field	Device-Specific Field

ArcSight ESM Field	Device-Specific Field
Device Action	Update Status
Device Severity	Severity
Message	description

R77 HTTPS Inspection Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	All of (app_category,app_properties)
Device Custom String 3	All of (https_inspection_action,HTTPS_inspection_rule_id,https_validation,HTTPS_inspection_rule_name)
File ID	snid
Message	description
Reason	reason
Requested URL	resource
Source Host Name	src_machine_name
Source User Name	One of (src_user_name,user)

R77 FG Event Mappings

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

R80 VPN-1 Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	peer_gateway
Device Custom Floating Point2	Flags
Device Custom Floating Point3	sequencenum
Device Custom Number1	Time
Device Custom Number2	Version
Device Custom String3	ifname
Device Custom String6	VPN Feature Name
Device HostName	origin
DeviceDirection	ifdir
File Id	loguid
Message	ike
Reason	Concatenate(encryption_failure,reject_category)
Request Context	originsicname

R80 Log Update Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point2	Flags

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point3	sequencenum
Device Custom Number1	time
Device Custom Number2	version
Device Custom Number3	packets
Device Custom String3	ifname
Device Host Name	origin
DeviceDirection	ifdir
File Id	All of ('loguid: ',loguid)
File Size	bytes
Old File Id	All of ('logid: ',logid)
Request Context	originsicname

R80 FG Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	c_in_bytes
Bytes Out	c_out_bytes
DestinationUserName	aba_customer
Device Custom Floating Point2	One of (Flags,flags)
Device Custom Floating Point3	SequenceNum
Device Custom Floating Point4	flags
Device Custom Number 1	ContentVersion
Device Custom Number3	packets
Device Custom String5	One of(ifname,IfName)
Device Host Name	One of(Origin,origin)
DeviceDirection	One of(IfDir,ifdir)
File Id	One of(logid,LogId)
File Size	bytes
fileType	log_type
Old File Id	logid
oldFileType	type
Request Context	One of (OriginSicName,originsicname)
SourcePort	sport_svc
sourceProcessId	is_first_for_luuid

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.