Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.1

Configuration Guide for Check Point Syslog SmartConnector

Document Release Date: May 2022
Software Release Date: May 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Revision History

Date	Description
07/09/2021	Added support for CheckPoint R80.30.
06/18/2020	Added support for R80 FDE, R80 MEPP, and R80 Endpoint Security Console.
05/21/2020	Added support for R80 Application Control, R80 Email Security, R80 Identity Logging, R80 SmartDefense, R80 VPN-1 and FireWall-1, R80 Anti Malware, R80 New Anti Virus, R80 Identity Awareness, R80 URL Filtering, R80 DLP, R80 HTTPS Inspection, R80 Syslog and "Unknown Product" Product mappings.
04/30/2020	Updated R77 Common Security Event Mappings and R77 VPN-1 and FireWall-1 Event Mappings.
03/19/2020	Added new mappings for Checkpoint Audit Syslog R80 Database Tool and for Checkpoint Audit Syslog R80 Unknown.
08/24/2019	Added new mappings to R77 Anti-bot (Anti Malware) Event Mappings.
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.
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.

Date	Description
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.

Date	Description
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

Configuration Guide for Check Point Syslog SmartConnector

Configuration Guide for Check Point Syslog SmartConnector

This guide provides information for installing the SmartConnector for Check Point Syslog and for configuring the device for syslog event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

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.

Supported versions for Check Point with Gaia Operating System are:

R77.30, R80.10, R80.20, and R80.30

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.

The following table indicates the supported modules:

R77.30 Modules (Limited Support) [1]	**R80.10 Modules**	**R80.20 Modules**	**R80.30 Modules**
Anti-bot (Anti-Malware)	Anti-Malware	Anti-Malware	AntiMalware
Anti-Spam	Anti-Spam	Antivirus	AntiSpam
Anti-Virus	New Anti-Virus	HTTPS Inspection	ApplicationControl
Application Control	Application Control	SmartEvent Client	ApplicationControl_URLFiltering
Audit	Audit	Syslog	CLI
DLP (Data Loss Prevention)	DLP (Data Loss Prevention)	System Monitor	Connectra
Email Security	Email Security	Connectra	DLP
ESOD	ESOD	Application Control URL Filtering	EndpointSecurityConsole
Eventia Analyzer Server	Identity Awareness	Security Gateway/Management	ESOD
Identity Awareness	Identity Logging	VPN-1 and FireWall-1 (+)FG	FG
Identity Logging	SmartDefense	SmartView Monitor	HTTPSInspection
SmartDefense	SmartDashboard	SmartView Tracker	IdentityAwareness
URL Filtering	SmartUpdate	Logs Indexer	IdentityLogging
VPN-1 and Firewall-1	URL Filtering	Query-database	MEPP

[1]The vendor no longer supports version R77.30. Therefore, we offer limited support.

R77.30 Modules (Limited Support) [1]	R80.10 Modules	R80.20 Modules	R80.30 Modules
VPN-1 Edge	VPN-1 and Firewall-1	Web-UI	NewAntiVirus
Connectra	Log Update	SmartConsole	QueryDatabase
Anti Virus	VPN-1	FG(+)VPN-1 and FireWall-1	SecurityGatewayManagement
Security Gateway/Management	FG	MEPP	SmartConsole
Linux OS		DFE	SmartDashboard
Syslog			SmartDefense
Threat Emulation			SmartEventClient
Anti Bot and Anti Virus			SmartViewMonitor
			Syslog
			SystemMonitor
			URLFiltering
			VPN1FireWall1
			WebUI

[1]The vendor no longer supports version R77.30. Therefore, we offer limited support.

Configuration

Check Point's Long Term Evolution (LTE) feature adds support for sending Check Point Logs to a Syslog Server. The LTE is supported on all the versions of Gaia Security Gateways. The Add-On is required on the Security Management Server or Multi-Domain Server.

Information in the following section of this guide has been derived from the *Check Point Firewall R77 Versions Administration Guide*. For a different version, see the particular Check Point version Administration Guide for complete configuration information.

Enabling 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.

Sending 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.

Defining 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)

Configuring 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.

Configuring 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.

Configuring 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**.

Configuring 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
```

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Deamon, Syslog Deamon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Deamon 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 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: `local1.warning @@10.0.0.1:514`

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

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

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 additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

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.

Using the SmartConnector for Syslog Pipe or File

This section provides information 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.

For Syslog Pipe:

1. Execute the following command to create a pipe:

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

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

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

   or

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

3. Restart the syslog daemon in one of the following methods:
   Enter the following commands:

   ```
   /etc/init.d/syslogd stop
   /etc/init.d/syslogd start
   ```

   or

   Execute the following command to send a configuration restart signal:

   On RedHat Linux:

   ```
   service syslog restart
   ```

   On Solaris:

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

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

   The syslog daemon is forced to reload the configuration and start writing to the pipe.
3. Restart the syslog daemon in one of the following methods:
   a. Restart the syslog daemon in one of the following methods:
      Enter the following commands:

      ```
      /etc/init.d/syslogd stop
      /etc/init.d/syslogd start
      ```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

Installing the SmartConnector

The following sections provide instructions for installing and configuring the Check Point Syslog SmartConnector.

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Check Point Syslog Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
  a. Click **Next**, the specify the following paramenters:

Parameters	Description
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, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.

  b. **Click Next.**
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, the specify the following paramenters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: `/var/tmp/syspipe`.
File Absolute Path Name	Specify the full path name for the file from which this connector will read events. The following are default values: • **Solaris:** `\var\adm\messages` • **Linux:** `\var\log\messages` You can use a wildcard pattern in the file name. In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation: • **Date format log rotation:** The device creates a new log at a specified time in the with the naming convention `filename.timestamp.log`. The connector detects the new log and terminates the reader thread to the previous log after the 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, specify timestap in `yyyy-MM-dd` date format. For example, `filename.yyyy-MM-dd.log` • **Index log rotation:** The device writes to indexed files in the following format: `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 the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of `true` is optional.
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

b. Click **Next.**

5. Select a destination and configure parameters.

6. Specify a name for the connector.
7. 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.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

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

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.

R81 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 Date 1	Package date
Device Custom Date 2	Subs Expire
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	Scan 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
Device Custom String 2	Protection Type
Device Custom String 3	Protection ID
Device Custom String 4	Protection Name
Device Custom String 5	Source OS
Device Custom String 6	Scan Direction
Device Facility	malware_family
Device Severity	One of (severity,Severity)
Event Outcome	One of (status,Status,Update Status)

ArcSight ESM Field	Device-Specific Field
File ID	log_id
Message	One of (description,long_desc,next_update_desc,short_desc,subscription_stat_desc)
Reason	reason
Request Client Application	web_client_type
Request Url	resource
Source Host Name	src_machine_name
Source Translated Address	One of (proxy_src_ip)
Source User Name	One of (src_user_name,user)
Source Port	sport_svc

R81 Application Control Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	protocol
Base Event Count	One of (Suppressed logs,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 Action	https_inspection_action
Device Custom Date 2	Subs Expire
Device Custom Number 3	Application Risk
Device Custom String 1	Application Rule Name
Device Custom String 2	Application Rule ID
Device Custom String 3	Application Properties
Device Custom String 4	User Status
Device Custom String 5	User Check Confirmation Level
Device Event Category	One of (app_category,matched_category)
Device Host Name	One of (Origin,origin)
Device Severity	Severity

ArcSight ESM Field	Device-Specific Field
End Time	LastUpdateTime
Event Outcome	Update Status
File ID	log_id
File Type	log_type
Message	One of (app_desc,portal_message)
Old File ID	snid
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 Method	method
Request Url	resource
Source Host Name	src_machine_name
Source Port	sport_svc)
Source Translated Address	One of (proxy_src_ip)
Source User Name	One of (user,src_user_name)
Destination Dns Domain	dst_user_dn
Old File Name	One of (appi_name,layer_name)
Old File Hash	layer_uuid
Source Dns Domain	src_user_dn

R81 System Monitor Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	event parameter alert:condition to current_value
Device Custom String 4	System alert message
Device Host Name	One of (Origin,origin)
Message	sys_message:
Old File Id	loguid
File Path	sensor_alert_module

R81 VPN-1 & FireWall-1 Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes Out	sent_bytes
Destination Host Name	dst_machine_name
Destination Service Name	service_id
Destination User Name	dst_user_name
Device Custom Date 2	Expire Time
Device Custom String 1	Rule & Rule Name
Device Custom String 2	TCP packet out of state
Device Custom String 3	TCP Flags
Device Custom String 4	Rule UID
Device Inbound Interface	inzone
Device Outbound Interface	outzone
Device Severity	Severity
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	layer_uuid
Old File ID	snid
Old File Name	layer_name
Old File Path	src_user_dn
Source Host Name	src_machine_name
Source Port	sport_svc
Source User Name	One of (src_user_name,user)
Application Protocol	protocol
Device Custom String 5	sig_id
Device Custom String 5 Label	Signature Id

R81 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 ID	One of (src_user_name,user)
Source User Name	One Of (src_user_name,user)

R81 Security Gateway/Management

ArcSight ESM Field	Device-Specific Field
Device Action	status
Device Custom Floating Point 1	Version
Device Custom Number 1	Update Service
Device Custom String 2	Failure Impact
Device Custom String 3	Comment
Device Host Name	One of (Origin,origin)
Device Severity	Severity

ArcSight ESM Field	Device-Specific Field
Message	description
Old File ID	loguid
Reason	reason

R81 Smart Console Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Severity	Severity
End Time	event_end_time
File Create Time	cu_detection_time
File Hash	cu_rule_id
File ID	log_id
File Modification Time	cu_last_update_time
File Name	Session name
File Type	Session UID
Old File Hash	cu_rule_category
Old File ID	Logic Changes
Source Nt Domain	domain
Source User Name	Customer_Name
Start Time	event_start_time

R81 Smart Defense Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	Suppressed logs
Bytes In	received_bytes
Bytes Out	sent_bytes
Device Custom Date 2	Policy Time
Device Custom Floating Point 1	Update Version
Device Custom Floating Point 3	Sequence Number
Device Custom Number 1	Content Version

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	During Second
Device Custom Number 3	Fragments Dropped
Device Custom String 1	Rule & Rule Name
Device Custom String 2	Protection Type
Device Custom String 3	Protection ID
Device Custom String 4	Protection Name
Device Custom String 5	SmartDefense Profile
Device Custom String 6	Malware Rule Name
Device Facility	Source_OS
Device Host Name	One of (Origin,origin)
Device Severity	One of (Severity,severity)
File Hash	__concatenate(Description URL,Industry Reference)
File ID	log_id
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 ID	loguid
Old File Name	layer_name
Old File Path	more_sources
Old File Permission	policy
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 Translated Address	proxy_src_ip
Source User Name	One of (src_user_name,user,source)

R81 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

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

R80.30 Common Audit Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	One of (Machine,machine)
Destination User Name	One of (Administrator,administrator)
Device Action	One of (Action,action)
Device Custom String 2	Subject
Device Custom String 3	Object Table
Device Custom String 4	Operation Number
Device Custom String 5	Object Name
Device Custom String 6	Policy Name
Device Event Category	" AuditLog"
Device Event Class ID	One of (event_name,One of (Operation,operation),"AuditLog")
Device Facility	ProductFamily
Event Outcome	Audit Status
External ID	Uid
Message	One of (__concatenate(TCP packet out of state,,""))
Name	One of (event_name,One of (Operation,operation),"AuditLog")
Source Address	client_ip

R80.30 Common Security Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	One of (dst,dst_ip)
Destination Port	One of (d_port,service,d_port)
Destination Service Name	One of (service_id,service,svc)
Device Event Category	"SecurityLog"
Device Event Class ID	One of (action,Action,event_name,malware_action,auth_status,short_ desc,description,message_info,activity,subscription_stat_desc,contract_ name,rule_name,event_type,, scan direction, all of (one of (ProductName, product), '|', One of(subscription_stat, 'Event')), 'Scan Summary')
Device Facility	ProductFamily
Name	One of (action,Action,event_name,malware_action,auth_status,short_ desc,description,message_info,activity,subscription_stat_desc,contract_ name,rule_name,event_type,, scan direction, all of (one of (ProductName, product), '|', One of(subscription_stat, 'Event')), 'Scan Summary')
Source Address	One of (src,src_ip,scope)
Source Port	s_port
Transport Protocol	One of (proto,Proto)

R80.30 CLI Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	Time
Device Custom Number 1	Version
Device Direction	ifdir
Device Host Name	origin
File ID	loguid
Request Context	One of (originsicname,origin_sic_name)

R80.30 query-database Event Mappings

ArcSight ESM Field	Device-Specific Field
File ID	admin_level
File Name	CMA_Name
Old File ID	session_id
Old File Name	MDS_Name
Source User Name	Customer_Name

R80.30 SmartConsole Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Severity	Severity
End Time	event_end_time
File Create Time	cu_detection_time
File Hash	cu_rule_id
File ID	log_id
File Modification Time	cu_last_update_time
File Name	Session name
File Type	Session UID
Old File Hash	cu_rule_category
Old File ID	Logic Changes
Source Nt Domain	domain
Source User Name	Customer_Name
Start Time	event_start_time

R80.30 SmartDashboard Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Severity	Severity
File Create Time	cu_detection_time

ArcSight ESM Field	Device-Specific Field
File Hash	cu_rule_id
File ID	log_id
File Modification Time	cu_last_update_time
File Name	CMA_Name
Old File Hash	cu_rule_category
Source Host Name	hostname
Source Nt Domain	domain
Source User Name	Customer_Name
Start Time	event_start_time

R80.30 SmartView Monitor Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Severity	Severity
File Create Time	cu_detection_time
File Hash	cu_rule_id
File ID	log_id
File Modification Time	cu_last_update_time
File Name	CMA_Name
Old File Hash	cu_rule_category
Source Nt Domain	domain
Start Time	event_start_time

R80.30 Endpoint Security Console Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Version
Device Host Name	origin
File Hash	cu_rule_id
File ID	log_id
File Modification Time	cu_last_update_time

ArcSight ESM Field	Device-Specific Field
File Name	CMA_Name
Old File Hash	cu_rule_category
Old File ID	admin_level
Old File Name	MDS_Name
Request Context	One of (originsicname,origin_sic_name)
Source Nt Domain	domain
Source User Name	Customer_Name
Start Time	event_start_time

R80.30 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 Date 1	Package date
Device Custom Date 2	Subs Expire
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	Scan 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
Device Custom String 2	Protection Type
Device Custom String 3	Protection ID
Device Custom String 4	Protection Name
Device Custom String 5	Source OS
Device Custom String 6	Scan Direction

ArcSight ESM Field	Device-Specific Field
Device Facility	malware_family
Device Severity	One of (severity,Severity)
Event Outcome	One of (status,Status,Update Status)
File ID	log_id
Message	One of (description,long_desc,next_update_desc,short_desc,subscription_stat_desc)
Reason	reason
Request Client Application	web_client_type
Request Url	resource
Source Host Name	src_machine_name
Source Translated Address	One of (proxy_src_ip)
Source User Name	One of (src_user_name,user)

R80.30 Anti Spam Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	to
Destination User Name	Recipients
Device Custom Number 1	Email Recipients Number
Device Custom String 1	Rule & Rule Name
Device Custom String 2	Recipients
Device Custom String 3	Email Control
Device Custom String 4	Sender IP & Sender Address
Device Custom String 5	Email Session ID
Device Event Category	email_spam_category
Device Host Name	One of (Origin,origin)
File ID	log_id
File Type	log_type
Old File Type	type
Reason	reason
Request Context	One of (originsicname,origin_sic_name)

ArcSight ESM Field	Device-Specific Field
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source User ID	from

R80.30 Application Control Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	protocol
Base Event Count	One of (Suppressed logs,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 Action	https_inspection_action
Device Custom Date 2	Subs Expire
Device Custom Number 3	Application Risk
Device Custom String 1	Application Rule Name
Device Custom String 2	Application Rule ID
Device Custom String 3	Application Properties
Device Custom String 4	User Status
Device Custom String 5	User Check Confirmation Level
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	log_id
File Type	log_type
Message	One of (app_desc,portal_message)
Old File ID	snid
Old File Name	appi_name

ArcSight ESM Field	Device-Specific Field
Old File Type	type
Reason	description
Request Client Application	web_client_type
Request Context	One of (originsicname,origin_sic_name)
Request Method	method
Request Url	resource
Source Host Name	src_machine_name
Source Port	sport_svc)
Source Translated Address	One of (proxy_src_ip)
Source User Name	One of (user,src_user_name)

R80.30 MEPP Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	usercheck_incident_uid
Device Custom Date 1	Time
Device Custom Floating Point 3	Sequence Number
Device Custom Number 1	Media Authorized
Device Custom Number 2	Organization Host
Device Custom Number 3	Is Target Encrypted Storage
Device Custom String 1	Reading Data Access
Device Custom String 2	Connectivity State
Device Custom String 3	Installed Products
Device Custom String 4	Writing Data Access
Device Custom String 5	Host Type
Device Custom String 6	Media Type
Device External ID	machine_guid
Device Host Name	One of (Origin,origin)
Device Process Name	process
Device Severity	One of (severity,Severity)
Device Version	client_version

ArcSight ESM Field	Device-Specific Field
File Hash	media_class_id
File ID	media_manufacturer
File Name	file_name
File Path	os_name
File Permission	file_operation
File Size	file_size
File Type	event_type
Message	description
Old File Hash	media_encrypted
Old File ID	loguid
Old File Name	os_version
Old File Path	destination_path
Old File Permission	media_description
Old File Type	data_type
Source Dns Domain	user_name
Source Host Name	src_machine_name
Source Service Name	client_name
Source User ID	user_sid
Source User Name	One of (src_user_name,user_name)

R80.30 Security Gateway/Management Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	status
Device Custom Floating Point 1	Version
Device Custom Number 1	Update Service
Device Custom String 2	Failure Impact
Device Custom String 3	Comment
Device Host Name	One of (Origin,origin)
Device Severity	Severity

ArcSight ESM Field	Device-Specific Field
Message	description
Old File ID	loguid
Reason	reason

R80.30 Syslog Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point 3	Sequence Number
Device Facility	facility
Device Host Name	One of (Origin,origin)
Device Severity	syslog_severity
Message	default_device_message
Source Address	Src
Source User Name	user

R80.30 System Monitor Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	event parameter alert:condition to current_value
Device Custom String 4	System alert message
Device Host Name	One of (Origin,origin)
Message	sys_message:
Old File Id	loguid

R80.30 Application Control(+)URL Filtering Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	protocol
Device Custom Date 1	Creation Time
Device Custom Date 2	Last Hit Time

ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	Packets
Device Custom String 5	Signature ID
Device Custom String 6	Server|Client Inbound|Outbound Packets|Bytes
Device Severity	Severity
File Size	bytes
Message	description

R80.30 Connectra Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	One of (Suppressed_Logs,suppressed_logs))
Destination Address	office_mode_ip
Destination Nt Domain	domain_name
Destination Translated Address	assigned_IP:
Device Custom Number 1	Client Build
Device Custom String 1	Tunnel_protocol
Device Custom String 2	Reject ID
Device Custom String 4	Methods
Device Custom String 5	Auth Encryption Methods
Device Custom String 6	Host IP
Device Event Category	cvpn_category
Device Host Name	One of (Origin,origin)
Device Version	client_version
Event Outcome	status
File Create Time	login_timestamp
File Hash	device_identification
File ID	log_id
File Path	os_name
File Type	event_type
Old File ID	session_uid
Reason	reason

ArcSight ESM Field	Device-Specific Field
Request Client Application	browser
Request Context	One of (originsicname,origin_sic_name)
Source Host Name	Hostname
Source Mac Address	mac_address
Source Nt Domain	user_dn
Source Service Name	client_name
Source Translated Address	proxy_src_ip
Source User Name	User,user
Source User Privileges	user_group
Start Time	event_start_time

R80.30 DLP Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	dlp_transport
Bytes In	received_bytes
Bytes Out	sent_bytes
Destination Process Name	dlp_data_type_name
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (dlp_recipients,UserCheck,aba_customer)
Device Action	https_inspection_action
Device Custom Number 1	Content Version
Device Custom String 1	DLP Rule Name
Device Custom String 2	Rule
Device Custom String 3	Incident Extension
Device Custom String 4	Rule UID
Device Custom String 5	Scan Direction
Device Custom String 6	User Check Confirmation Level
Device Event Category	dlp_categories
Device Host Name	One of (Origin,origin)
Device Outbound Interface	UserCheck_Interaction_name

ArcSight ESM Field	Device-Specific Field
Device Severity	severity
End Time	event_end_time
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 (information,portal_message,dlp_violation_description,dlp_action_reason)
Old File ID	dlp_data_type_uid
Old File Type	type
Reason	dlp_action_reason
Request Context	One of (originsicname,origin_sic_name)
Request Url	outgoing_url
Source Nt Domain	from
Source Port	sport_svc
Source Translated Address	proxy_src_ip
Source User Name	One of (user,src_user_name)
Start Time	event_start_time

R80.30 New Anti Virus Event Mappings

ArcSight ESM Field	Device-Specific Field
File ID	log_id
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	One of (scope)
Destination User ID	UserCheck_incident_uid
Destination User Name	One of (UserCheck,aba_customer)
Device Custom Date 2	Subs Expire

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Content Version
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 Custom String 5	Source OS
Device Custom String 6	User Check Confirmation Level
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 Name	One of (file name,packet_capture_name)
File Path	packet_capture_unique_id
File Size	bytes
File Type	file_type
Message	One of (description,next_update_desc,subscription_stat_desc)
Old File Hash	ticket_id
Old File ID	snid
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 Nt Domain	domain

ArcSight ESM Field	Device-Specific Field
Source Port	sport_svc
Source Translated Address	One of (proxy_src_ip)
Source User Name	One of (src_user_name,user)

R80.30 SmartDefense Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	Suppressed logs
Bytes In	received_bytes
Bytes Out	sent_bytes
Device Custom Date 2	Policy Time
Device Custom Floating Point 1	Update Version
Device Custom Floating Point 3	Sequence Number
Device Custom Number 1	Content Version
Device Custom Number 2	During Second
Device Custom Number 3	Fragments Dropped
Device Custom String 1	Rule & Rule Name
Device Custom String 2	Protection Type
Device Custom String 3	Protection ID
Device Custom String 4	Protection Name
Device Custom String 5	SmartDefense Profile
Device Custom String 6	Malware Rule Name
Device Facility	Source_OS
Device Host Name	One of (Origin,origin)
Device Severity	One of (Severity,severity)
File Hash	__concatenate(Description URL,Industry Reference)
File ID	log_id
File Permission	sub_policy_name
File Type	log_type
Message	One of (message,Attack Info,attack_info,attack,Error,precise_error,description)
Name	attack

ArcSight ESM Field	Device-Specific Field
Old File ID	loguid
Old File Name	layer_name
Old File Path	more_sources
Old File Permission	policy
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 Translated Address	proxy_src_ip
Source User Name	One of (src_user_name,user,source)

R80.30 SmartEvent Client Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Update Service
Device Custom String 3	Comment
Device Custom String 4	Status
Device Custom String 5	Version
Message	description

R80.30 URL Filtering Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	Suppressed logs
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 Date 2	Subs Expire
Device Custom Floating Point 1	Application ID
Device Custom Number 3	Application Risk
Device Custom String 1	Application Rule Name
Device Custom String 3	Application Rule ID
Device Custom String 4	Application Properties
Device Custom String 6	User Check Confirmation Level
Device Event Category	One of (app_category,matched_category)
Device Severity	Severity
Event Outcome	Update Status
File ID	log_id
File SIze	bytes
File Type	log_type
Message	One of (description,app_desc,portal_message)
Old File ID	snid
Old File Name	appi_name
Request Client Application	web_client_type
Request Url	resource
Source Host Name	src_machine_name
Source Nt Domain	domain
Source Port	sport_svc
Source Translated Address	proxy_src_ip
Source User Name	One of (user,src_user_name,User)
Start Time	event_start_time

R80.30 VPN-1 & FireWall-1 Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes Out	sent_bytes
Destination Host Name	dst_machine_name
Destination Service Name	service_id

ArcSight ESM Field	Device-Specific Field
Destination User Name	dst_user_name
Device Custom Date 2	Expire Time
Device Custom String 1	Rule & Rule Name
Device Custom String 2	TCP packet out of state
Device Custom String 3	TCP Flags
Device Custom String 4	Rule UID
Device Inbound Interface	inzone
Device Outbound Interface	outzone
Device Severity	Severity
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	layer_uuid
Old File ID	snid
Old File Name	layer_name
Old File Path	src_user_dn
Source Host Name	src_machine_name
Source Port	sport_svc
Source User Name	One of (src_user_name,user)

R80.30 ESOD Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 2	Subs Expire
Device Custom Number 1	Content Version
Device Custom String 3	Signature Version
Device Custom String 4	Update Source
Event Outcome	Update Status
File ID	log_id
File Type	log_type
Message	activity
Old File Type	type
Reason	reason

R80.30 FG Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Content Version
Device Custom Number 3	Packets
Device Custom String 3	FG-1 Client and Server Rule Name
File ID	log_id
File Type	log_type
Message	sys_message:
Old File ID	loguid
Old File Type	type
Source Port	sport_svc

R80.30 HTTPS Inspection Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point 1	Version
Device Custom Floating Point 3	Sequence Number
Device Custom Number 1	Update Service
Device Custom String 2	App Category & App Properties
Device Custom String 3	Comment
Device Custom String 4	Status
Device Custom String 5	HTTPS Info
Device Severity	severity
File ID	failure_impact
Message	description
Old File ID	snid
Reason	reason
Request Context	One of (originsicname,origin_sic_name)

R80.30 Identity Awareness Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Nt Domain	domain_name
Device Address	One of (endpoint_ip)
Device Custom Number 1	Client Build
Device Custom String 1	Connectivity State
Device Custom String 2	Identity Source
Device Custom String 3	Identity Type
Device Custom String 4	Authentication Status
Device Custom String 5	Authentication Method
Device Custom String 6	Roles
Device Event Category	ctrl_category
Device External ID	device_identification
Device Severity	severity
Device Host Name	One of (Origin,origin)
Device Version	client_version
End Time	LastUpdateTime
File ID	logid
File Path	os_name
File Type	log_type
Message	One of (description ,description,Authentication trial)
Old File ID	snid
Old File Name	os_version
Old File Type	type
Reason	termination_reason
Request Client Application	browser
Source Service Name	client_name
Request Context	One of (originsicname,origin_sic_name)
Source Host Name	src_machine_name

ArcSight ESM Field	Device-Specific Field
Source Mac Address	macsourceaddress
Source User Name	One of (src_user_name,user)
Source User Privileges	src_user_group

R80.30 Identity Logging Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Host Name	One of (Origin,origin)
File ID	logid
File Type	log_type
Message	One of (description,information)
Old File Type	type
Request Context	One of (originsicname,origin_sic_name)
Source Address	src
Source Host Name	src_machine_name
Source User Name	One of (src_user_name,user)

Checkpoint Audit Syslog R80 Database Tool

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
Message	additional_info
Old File Id	loguid

Checkpoint Audit Syslog R80 Unknown

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
Message	additional_info
Old File Id	loguid

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)

ArcSight ESM Field	Device-Specific Field
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), '|', 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), '|', 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

ArcSight ESM Field	Device-Specific Field
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
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 ID	One of (src_user_name,user)
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)
Device Custom Floating Point 2	One of (Flags,flags)
Device Custom Floating Point 3	SequenceNum
Device Custom Floating Point1	app_id

ArcSight ESM Field	Device-Specific Field
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 ID	One of (src_user_name,user)
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
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

ArcSight ESM Field	Device-Specific Field
Source NT Domain	from
Source Port	sport_svc
Source Process ID	is_first_for_luuid
Source Translated Address	proxy_src_ip
Source User ID	One of (src_user_name,user)
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 Id	One of (dst_user_name,aba_customer)
Destination User Name	One of (dst_user_name, aba_customer)
Device Custom Floating Point 2	Flags
Device Custom Floating Point 3	SequenceNum
Device Custom Number 1	email_recipients_num
Device Custom Number 2	ContentVersion

ArcSight ESM Field	Device-Specific Field
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 ID	One of (src_user_name,user)
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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 ID	One of (src_user_name,user)
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
Device Host Name	Origin
File ID	LogId

ArcSight ESM Field	Device-Specific Field
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 ID	One of (src_user_name,user)
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)

ArcSight ESM Field	Device-Specific Field
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
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 ID	One of (src_user_name,user)
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
File Path	ifname
File Permission	sub_policy_name

ArcSight ESM Field	Device-Specific Field
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 ID	One of (src_user_name,user)
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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 ID	One of (src_user_name,user)
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

ArcSight ESM Field	Device-Specific Field
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
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 ID	One of (src_user_name,user)
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 ID	One of (src_user_name,user)
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

ArcSight ESM Field	Device-Specific Field
Device Direction	ifdir
Device Host Name	origin
Device Severity	severity
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 ID	user
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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)

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	All of (s_in_bytes,s_out_bytes)
Device Custom String 5	One of(InterfaceName,Interface)
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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

R80 FDE Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	time
Device Custom Date 2	policy_date
Device Custom Floating Point 2	flags
Device Custom Floating Point 3	sequencenum
Device Custom Number 2	version
Device Custom Number 3	policy_type
Device Custom String 1	fde_details
Device Custom String 3	installed_products
Device Custom String 4	os_version
Device Custom String 5	host_type
Device Custom String 6	policy_name
Device Direction	ifdir
Device Host Name	origin
Device Severity	severity
Device Version	client_version
Event Outcome	regexTokenNoWarning(description,".*?(successfully).*")
File Hash	fde_account_guid
File Id	policy_guid
File Name	fde_account

ArcSight ESM Field	Device-Specific Field
File Path	os_name
File Type	event_type
Message	descriptionlue
Old File Hash	fde_rh_guid
Old File Id	loguid
Old File Name	policy_version
Source DNS Domain	user_name
Source Host Name	src_machine_name
Source Service Name	client_name
Source User ID	user_sid
Source User Name	oneOf(src_user_name,user_name)

R80 MEPP Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Id	usercheck_incident_uid
Device Custom Date 1	time
Device Custom Floating Point 2	flags
Device Custom Floating Point 3	sequencenum
Device Custom Number 1	media_authorized
Device Custom Number 2	is_organization_host
Device Custom Number 3	is_target_encrypted_storage
Device Custom String 1	reading_data_access
Device Custom String 2	connectivity_state
Device Custom String 3	installed_products
Device Custom String 4	writing_data_access
Device Custom String 5	host_type
Device Custom String 6	media_type
Device Direction	ifdir
Device Host Name	origin

ArcSight ESM Field	Device-Specific Field
Device Process Name	process
Device Severity	severity
Device Version	client_version
File Hash	media_class_id
File Id	media_manufacturer
File Name	file_name
File Path	os_name
File Permission	file_operation
File Size	file_size
File Type	event_type
Message	description
Old File Hash	media_encrypted
Old File Id	loguid
Old File Name	policy_version
Old File Path	destination_path
Old File Permission	media_description
old File Type	data_type
Source DNS Domain	user_name
Source Host Name	src_machine_name
Source Service Name	client_name
Source User ID	user_sid
Source User Name	oneOf(src_user_name,user_name)

R80 Endpoint Security Console 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

ArcSight ESM Field	Device-Specific Field
Device Direction	ifdir
Device Host Name	origin
Old File Id	loguid
Request Context	originsicname
Source User ID	uid

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
Device Custom Floating Point3	sequencenum
Device Custom Number1	time
Device Custom Number2	version

ArcSight ESM Field	Device-Specific Field
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

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
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	oneOf(service_id,service,svc)
Device Action	oneOf(Action,action)
Device Custom String 1	'null'
Device Event Category	'SecurityLog'
Device Event Class ID	oneOf(product,blade_name,ProductName)

ArcSight ESM Field	Device-Specific Field
Device Facility	product_family
Name	oneOf(product,blade_name,ProductName)
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
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

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 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

ArcSight ESM Field	Device-Specific Field
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)

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

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 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
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
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

ArcSight ESM Field	Device-Specific Field
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
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)

ArcSight ESM Field	Device-Specific Field
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
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	HighLevelLogKey
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
Request Context	OriginSicName
Source Host Name	src_machine_name
Source NT Domain	domain
Source Port	sport_svc
Source Translated Address	xlatesrc

ArcSight ESM Field	Device-Specific Field
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)
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)

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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
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)

Unknown Product Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	cu_detected_by
Device Custom Date 1	cu_detection_time
Device Custom Floating Point2	flags
Device Custom Floating Point3	sequencenum
Device Custom Number 1	cu_log_count
Device Custom Number 2	time_interval
Device Custom Number 3	version
Device Custom String 5	ifname

ArcSight ESM Field	Device-Specific Field
Device Direction	ifdir
Device Event Class Id	one Of(concatenate (alert,description),"Unknown|Event")
Device Host Name	origin
Device Product	"Unknown Product"
Device Severity	severity
Device Version	version
End Time	event_end_time
File Id	logid
Message	description
Name	one Of(concatenate (alert,description),"Unknown|Event")
Old File Id	loguid
Reason	reason
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.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Check Point Syslog SmartConnector (SmartConnectors 8.3.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!