Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Fortinet FortiGate Syslog

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Fortinet FortiGate Syslog

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
06/15/2017	Updated Event mappings and UTM mappings.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Added support for FortiGate OS version 5.2. Removed support for versions 3.0 and 4.0 due to end of support by the vendor.
11/17/2015	Updated mappings.
05/15/2015	Added new parameters for Syslog File.
06/28/2013	Added support for Fortinet OS v5.0 and IPv6 mappings.
05/15/2012	Added new installation procedure.
06/30/2011	End of life for FortiGate OS version 2.8.

Contents

SmartConnector for Fortinet FortiGate Syslog

This guide provides information for installing the SmartConnector for Fortinet FortiGate Syslog and configuring the device for syslog event collection. OS versions 5.0, and 5.2 are supported.

Product Overview

The FortiGate appliance provides security monitoring and intrusion protection services. FortiGate closes the vulnerability window by stopping viruses and worms before they enter the network, and stops attacks that evade conventional antivirus products with realtime response to fast-spreading threats.

Configuration

FortiGate OS Versions 5.0 and 5.2 Configuration

For information enabling and configuring logging for Fortinet FortiGate, see "Logging and Reporting for FortiOS 5.2" at the following URL:

http://docs.fortinet.com/uploaded/files/2180/fortigate-loggingreporting-52.pdf

Enabling Logging

To enable logging (web configuration):

1. Log in to the Web Configuration interface.
2. Select **Log&Report**, then **Log Config**.
3. Click the **Event Log** tab.
4. Select **Enable**.
5. Select the logs you want recorded.
6. Click **Apply**.

Configuring Logging

1. Log in to the Web Configuration interface.
2. Select **Log&Report**, then **Log Config**; the **Log Setting** tab is displayed.
3. Make sure **Syslog** is selected.
4. Enter the IP address of the remote computer running syslog server software.
5. Enter the port number of the syslog server.

6 Select the severity level for which you want to record log messages. The FortiGate appliance will log all levels of severity down to but not lower than the level you select. For example, if you want to record emergency, alert, critical, and error messages, select **Error**.

7 Select the **Facility** to be used from the drop-down list or accept the default value.

8 Click **Apply**.

Configuring Logging via the CLI

To configure FortiGate using the CLI, enter the following:

```
config log syslogd setting
     set facility alert
     set port <port_integer>
     set server <server_ip_address>
     set status enable
end
config log syslogd filter
     set severity debug
end
```

where `<server_ip_address>` is the IP address and `<port_integer>` is the Port on which the syslog server is running.

To enable logging to multiple Syslog servers using the CLI, enter the following:

1 Log in to the CLI.

Enter the following commands to configure the first syslog server:

```
config log syslogd setting
     set csv {disable | enable}
     set facility <facility_name>
     set port <port_integer>
     set reliable {disable | enable}
     set server <ip_address>
     set status {disable | enable}
end
```

2 The following commands configure the second syslog server:

```
config log syslogd2 setting
     set csv {disable | enable}
     set facility <facility_name>
     set port <port_integer>
     set reliable {disable | enable}
     set server <ip_address>
```

```
        set status {disable | enable}
    end
```

3 The following commands configure the third syslog server:

```
    config log syslogd3 setting
        set csv {disable | enable}
        set facility <facility_name>
        set port <port_integer>
        set reliable {disable | enable}
        set server <ip_address>
        set status {disable | enable}
    end
```

By default, most FortiGate features are enabled for logging. Refer to this example to disable the FortiGate features you do not want the Syslog server to record:

```
    config log syslogd filter
        set traffic {enable | disable}
        set web {enable | disable}
        set url-filter {enable | disable}
    end
```

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

Syslog Daemon
Syslog Pipe
Syslog File

The Syslog Daemon SmartConnector

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

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

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

The Syslog Pipe and File SmartConnectors

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

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

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

Configure the Syslog Pipe or File SmartConnector

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

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

For syslog pipe:

1. Create a pipe by executing the following command:

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

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

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

   or

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

   depending on your operating system.

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

   On RedHat Linux, you would execute:

   ```
   service syslog restart
   ```

   On Solaris, you would execute:

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

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

For syslog file:

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

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

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

Install the SmartConnector

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

Syslog Installation

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

Syslog Daemon
Syslog Pipe
Syslog File

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

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

Prepare to Install Connector

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

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

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

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

Install Core Software

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

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

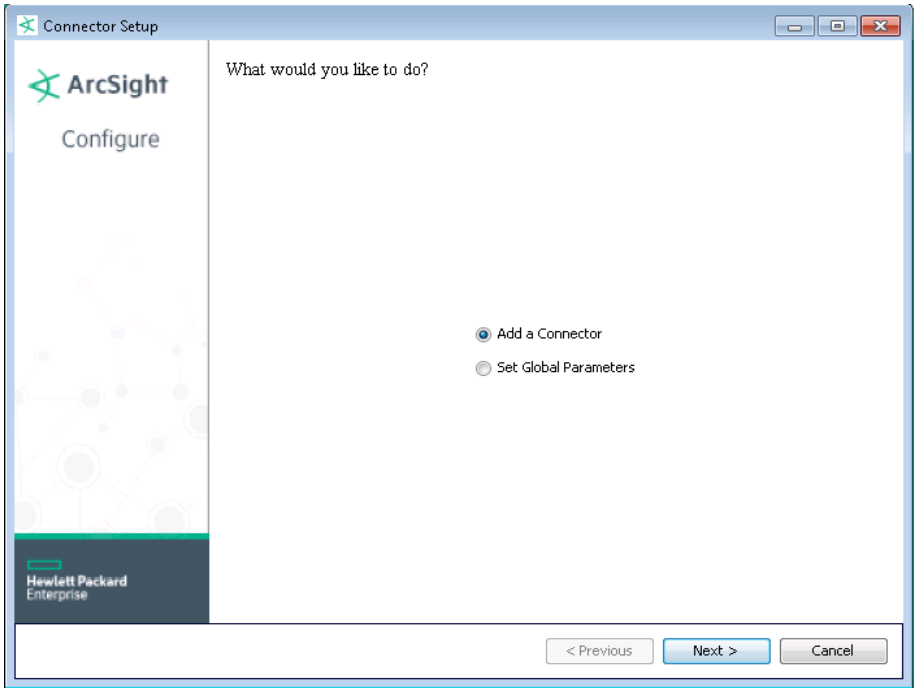
2 Start the SmartConnector installation and configuration wizard by running the executable.

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

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

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

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



Set Global Parameters (optional)

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

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.

Parameter	Setting
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

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

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

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

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Syslog Daemon, File, or Pipe** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

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

Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe

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

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

Select a Destination

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

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

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

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

Complete Installation and Configuration

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

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

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

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

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

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

Run the SmartConnector

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

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

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

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

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Fortigate Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = emergency; High = critical, alert, high, elevated; Medium = warning, error, medium; Low = notice, information, notification, debugging, low
Bytes In	One of (rcvdbyte, rcvd)

ArcSight ESM Field	Device-Specific Field
Bytes Out	One of (sentbyte, sent)
Destination Host Name	One of (dstname, dst_name, hostname)
Destination Port	One of (dstport, dst_port, locport, loc_port, dport)
Destination service Name	service
Device Action	One of (action, status)
Device Custom IPv6 Address 2	srcip (Source IPv6 Address)
Device Custom IPv6 Address 3	dstip (Destination IPv6 Address)
Device Custom Number 1	duration
Device Custom Number 2	One of (sentpkt, sent_pkt) (Packets Sent)
Device Custom Number 3	One of (rcvdpkt, rcvd_pkt) (Packets Received)
Device Custom String 1	rule
Device Custom String 2	One of (msg, ref) (Reference)
Device Custom String 3	vpn
Device Custom String 4	status
Device Custom String 5	policyid
Device Custom String 6	group
Device Direction	One of (trandisp, tran_disp), 'snat=outbound', 'dnat=inbound'
Device Event Category	Both (type, subtype)
Device Event Class ID	One of (logid, log_id)
Device External ID	One of (devid, device_id)
Device Host Name	One of (devname, _SYSLOG_SENDER)
Device Inbound Interface	One of (intf, interface, srcintf, src_int, sintf)
Device Outbound Interface	One of (dstintf, dst_int, out_if, dintf)
Device Product	'Fortigate'
Device Receipt Time	date, time
Device Severity	One of (level, pri)
Device Vendor	'Fortinet'
Event Outcome	status (success|failure|failed)
External ID	One of (SN, sn)
File Name	One of (file, msg)
File Path	msg
Message	msg
Name	One of (service, both (subtype, status), all of (type, service, status))
Reason	reason
Request Context	One of (catdesc, cat_desc)
Request Cookies	cookies
Request URL	One of (arg, url)
Source Host Name	One of (srcname, src_name)
Source Port	One of (srcport, src_port, remport, rem_port, sport)
Source Service Name	One of (role, msg)
Source User Name	One of (user, from, to)
Transport Protocol	proto

FortiGate Additional Data Mappings

ArcSight ESM Field	Device-Specific Field
act	act
app	app
app_list	One of (applist, app_list)
app_type	One of (apptype, app_type)
attack_id	One of (attackid, attack_id)
aven	aven
BlockedFrom	from
BlockedTo	to
carrier_ep	One of (carrierep, carrier_ep)
cat	cat
count	count
dec_spi	One of (decspi, dec_spi)
enc_spi	One of (encspi, enc_spi)
esp_auth	One of (espauth, esp_auth)
esp_transform	One of (esptransform, esp_transform)
fcni	fcni
fdni	fdni
field	field
ftp	ftp
fwver	fwver
icmp_code	(One of (icmpcode, icmp_code)
icmp_id	One of (icmpid, icmp_id)
icmp_type	One of (icmptype, icmp_type)
idsdb	idsdb
idsmn	idsmn
idssn	idssn
imap	imap
InboundSPI	One of (in_spi, spi)
init	init
interface	interface
libav	libav
method	method
mode	mode
next_stat	One of (nextstat, next_stat)
out_intf	One of (outintf, out_intf)
OutboundSPI	One of (out_spi, spi)
phase2_name	phase2_name
pop3	pop3
rbldb	rbldb
result	result
schd	schd
serial	serial
smtp	smtp

ArcSight ESM Field	Device-Specific Field
stage	stage
Submodule	submodule
tunnel	tunnel
tunnel_id	One of (tunnelid, tunnel_id)
tunnel_ip	One of (tunnelip, tunnel_ip)
tunnel_type	One of (tunneltype, tunnel_type)
ui	ui
vd	vd
virdb	virdb
virus	virus
VpnTunnel	One of (vpntunnel, vpn_tunnel)
xauth_group	One of (xauthgroup, xauth_group)
xauth_user	One of (xauthuser, xauth_user)

FortiGate IDS, IPS Mappings

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	One of (attackid, attack_id)

FortiGate Event Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	Bandwidth (as Integer)
Bytes Out	Bandwidth (as Integer)
Destination User Priviliges	new
Device Custom Date 1	datarange (Start Time For Report)
Device Custom Date 2	datarange (End Time For Report)
Device Custom Number 1	limit (Data Limit For Quarantine)
Device Custom Number 2	used (Data Used For Quarantine)
Device Custom Number 3	totalsession ("Total Session")
Device Custom String 1	cfgattr (Configuration Attribute)
Device Custom String 2	processtime (Process Time For Report)
Device Custom String 3	reporttype (Report Type)
Device Custom String 4	submodule (Submodule Name)
Device Custom String 5	fazlograte (The FortiAnalyzer Log Rate)
Device Custom String 6	profile (The Profile)
Event Outcome	state
File Name	filename
File Size	filesize
Message	One of (logdesc, error)
Old File Type	peer_notif
Source Address	server
Source Process Name	One of (ui, module)
Source User Privileges	old

FortiGate Traffic Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	One of (action, One of(craction, utmaction, appact))
Device Custom Number 1	countapp (Number Of Application Control Logs)
Device Custom Number 2	sessionid (Session ID)
Device Custom Number 3	countweb (Number Of Web Filter Logs)
Device Custom String 1	poluuid (UUID Of The Firewall Policy)
Device Custom String 3	crscore (Client Reputation Score)
Device Custom String 4	countav (Number Of AV Logs)
Device Custom String 6	appcat (Application Category)
Device Severity	apprisk
Name	Both type and one of (status, subtype)
Source User ID	appid
Source User Privileges	crlevel

FortiGate UTM Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	voip_proto
Device Custom Number 2	One of (sessionid, session_id) (Session ID)
Device Custom Number 3	policy_id (Policy ID)
Device Custom String 1	dtype (Data Type)
Device Custom String 2	eventtype (Event Type)
Device Custom String 3	analyticscksum (The Checksum Of The File Submitted)
Device Custom String 4	quarskip (Quarantine Skip Explanation)
Device Custom String 5	profile (Profile)
Device Custom String 6	appcat (Application Category Name)
Device External ID	One of (virusid, event_id)
Device Inbound Interface	direction (incoming=inbound)
Device Outbound Interface	direction (outgoing=outbound)
Device Severity	apprisk
Event Outcome	analyticssubmit
Message	error
Name	Both (type, subtype)
Old File ID	call_id
Request Client Application	agent
Request Method	One of (reqtype, kind)
Source User ID	appid