Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Fortinet FortiGate Syslog SmartConnector

Document Release Date: February 2022
Software Release Date: February 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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for Fortinet FortiGate Syslog SmartConnector

Configuration Guide for Fortinet FortiGate Syslog SmartConnector

This guide provides information for installing the SmartConnector for Fortinet FortiGate Syslog and 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 provide information about configuring SmartConnectorss 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

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 through 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.
2. 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
```

3. Enter 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
```

4. Enter 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 the following 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
```

Configuring the Syslog SmartConnectors

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

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 your selected 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

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

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)
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
Destination User Name	user
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	One of(status,sync_status)
Device Custom String 5	policyid
Device Custom String 6	group
Device Direction	One of (trandisp, tran_disp), 'snat=outbound', 'dnat=inbound'

ArcSight ESM Field	Device-Specific Field
Device Event Category	Both (type, subtype)
Device Event Class ID	One of (logid, log_id)
Device External ID	One of (devid, device_id)
Device Facility	type
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
File Size	One of (rcvdbyte, rcvd) (when the values are greater than 2147483647)
Message	msg
Name	IfThenElse(service,,concatenate(subtype," ",one Of (status,msg)),concatenate(type,": ",service," ",status))
Old File Path	cfgpath
Old File Size	One of (sentbyte, sent) (when the values are greater than 2147483647)
Reason	One of(reason,hbdn_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

ArcSight ESM Field	Device-Specific Field
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
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 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)
Old File Name	countapp (Number Of Application Control Logs)
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)

ArcSight ESM Field	Device-Specific Field
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

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 Fortinet FortiGate Syslog SmartConnector (SmartConnectors 8.3.0)

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!