

---

# Micro Focus Security ArcSight SmartConnector

Software Version: 8.3.0

## Configuration Guide for Snort 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

© Copyright 2022 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## 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: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

### 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.

## Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to [ArcSight Product Documentation Community on the Micro Focus Security Community](#).

### Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

# Contents

Configuration Guide for Snort Syslog SmartConnector .....	6
Product Overview .....	7
Configuration .....	8
Configuring the Syslog SmartConnectors .....	8
Installing the SmartConnector .....	11
Preparing to Install Connector .....	11
Installing and Configuring the SmartConnector .....	11
Device Event Mapping to ArcSight Fields .....	15
SnortS Syslog Mappings to ArcSight ESM Fields .....	15
Snort Key Value Event Mappings to ArcSight ESM Fields .....	15
Send Documentation Feedback .....	17

# Configuration Guide for Snort Syslog SmartConnector

This guide provides information for installing the SmartConnector for Snort Syslog and configuring the Snort 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](mailto:Documentation-Feedback@microfocus.com).

For specific product issues, contact [Micro Focus Customer Care](#).

# Product Overview

Snort open source network-based intrusion detection system (NIDS) performs real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

# Configuration

To configure the device:

1. Locate and open the main Snort configuration file to edit:  
`<Snort_home>/etc/snort.conf`
2. Locate the `# syslog` section.
3. In the following line, replace `<hostipaddress>` with your own host IP address:  
`output alert_syslog: host=<hostipaddress>:514, LOG_AUTH LOG_ALERT`  
where, `<hostipaddress>` is the IP address of your syslog host.
4. Start Snort with the `-s` option; for example:  
`C:\Snort>bin\snort -c etc\snort.conf -s`

See the *Snort Users Guide*, `alert.syslog` section for more details on configuring syslog output.

## Configuring 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 Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

### 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 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 Connector

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**, then specify the following parameters:

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 <b>None</b> , <b>Rename</b> , or <b>Delete</b> 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 <b>None</b> .

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

a. Click **Next**, then specify the following parameters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> .
File Absolute Path Name	<p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none"> <li>• <b>Solaris:</b> <code>\var\adm\messages</code></li> <li>• <b>Linux:</b> <code>\var\log\messages</code></li> </ul> <p>You can use a wildcard pattern in the file name.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• <b>Date format log rotation:</b> The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. 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 <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code></li> <li>• <b>Index log rotation:</b> The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, 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: <code>filename '%d,1,99,true'.log</code>;</li> </ul> <p>Specifying <code>true</code> 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 <code>true</code> is optional.</p>
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 <b>None</b> , <b>Rename</b> , or <b>Delete</b> 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 <b>None</b> .
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 <b>Rename</b> . The default value is <b>Processed</b> , which adds a <code>.processed</code> 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.

### SnortS Syslog Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 1; Medium = 2; Low = 3
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 1	Revision
Device Custom String 2	SnortPrefix
Device Event Class ID	All of(GeneratorID,SnortID)
Device Product	'Snort'
Device Vendor	'Snort'
Message	Message

### Snort Key Value Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	ApplicationProtocol
Bytes In	InitiatorBytes
Bytes Out	ResponderBytes
Destination Address	DstIP
Destination Port	DstPort
Destination Process Name	AccessControlRuleName
Device Action	AccessControlRuleAction
Device Custom Number 1	InitiatorPackets
Device Custom Number 2	ResponderPackets
Device Custom String 1	DE

## Configuration Guide for Snort Syslog Smartconnector

### Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Revision
Device Custom String 3	OriginalClientIP
Device Custom String 4	Policy
Device Custom String 5	GID
Device Custom String 6	SID
Device Event Category	Classification
Device Event Class Id	'SFIMS Information'
Device Inbound Interface	IngressInterface
Device Outbound Interface	EgressInterface
Device Severity	One Of(Priority,'3')
File Type	All of('WebApplication: ',WebApplication)
Message	Message
Name	One Of(Message,'SFIMS info')
Old File Permission	All of('URLReputation: ',URLReputation)
Old File Type	All of('URLCategory: ',URLCategory)
Request Client Application	Client
Request Cookies	All of('Sinkhole: ',Sinkhole)
Request Method	ConnectType
Source Address	SrcIP
Source Port	SrcPort
Source User Name	one Of(Username,User)
Transport Protocol	Protocol



# 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 Snort Syslog Smartconnector (SmartConnector 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](mailto:Documentation-Feedback@microfocus.com).

We appreciate your feedback!