Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide

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 Cisco ASA Syslog SmartConnector

This guide provides information for installing the SmartConnector for Cisco ASA 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 Cisco Adaptive Security Appliance (ASA) Series is a modular platform that provides firewall security monitoring and intrusion protection services for the complete security solution. These security appliances provide the next generation of security and VPN services.

If your appliance has Cisco IDS or Cisco IPS installed, those events are not collected as syslog events. Use the SmartConnector for Cisco Secure IPS SDEE for IPS event collection.

Cisco default syslog format is the only format supported by this SmartConnector.

Configuration

Configuring the Cisco Device to Send Events

To configure the Cisco device to send syslog events to a syslog server:

1. Telnet to your Cisco machine.
2. Within the console, enter enable mode by specifying the following command:
   `hostname(config)# enable` or `hostname(config)# en`.
3. Enter configuration mode by specifying the following command:
   `hostname(config)# configure terminal` or `hostname(config)# conf t`.
4. Enter the following lines:

```
hostname(config)# logging on
hostname(config)# logging timestamp
hostname(config)# no logging standby
hostname(config)# no logging console
hostname(config)# no logging monitor
hostname(config)# no logging buffered debugging
hostname(config)# logging trap debug
hostname(config)# no logging history
hostname(config)# logging facility <syslog server logging directory>
hostname(config)# logging queue 512
hostname(config)# logging host inside <syslog server ip address>
```

The **logging facility** can be one of the following:

16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

For example, to log to syslog facility local6, create the following entry on the device:

```
logging facility 22
```

For the **logging host**, replace `syslog server ip address` with the syslog server's IP address. You can use multiple logging host commands to specify additional servers.

For the **logging trap** severity level, the `debug` level is specified, which logs the following message types:

0–emergencies–System unusable messages
1–alert–Take immediate action
2–critical–Critical condition
3–error–Error message
4–warning–Warning message
5–notification–Normal but significant condition
6–informational–Information message
7–debugging–Debug messages and log FTP commands and WWW URLs

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 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 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

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms.

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

Updates to mappings include mapping the last user data to the additionaldata.externalAuthenticationUser. The idfw_user data is mapped to the destinationUserName or sourceUserName field. (The port and host name determine whether the username is source or destination.) These changes could affect your content.

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.

Cisco ASA Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 0, 1; High = 2, 3; Medium = 4, 5; Low = 6,7
Destination Host Name	IP
Destination User Name	User
Device Custom IPv6 Address 1	Device IPv6 Address
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	ICMP Type
Device Custom Number 2	ICMP Code
Device Custom Number 3	DurationInSeconds
Device Custom String 1	ACL/Policy Maps
Device Custom String 2	Unit
Device Custom String 3	TCP Flags
Device Custom String 4	Order
Device Custom String 5	Connection Type
Device Custom String 6	Duration
Device Event Category	MessageClass
Device Event Class Id	PixMessageId
Device Facility	_SYSLOG_FACILITY

ArcSight ESM Field	Device-Specific Field
Device Host Name	One of (DeviceHostName, _SYSLOG_SENDER)
Device Product	Product
Device Receipt Time	PixDate
Device Severity	PixSeverity (7 - 0)
Device Vendor	'CISCO'
Message	Reason, Message
Name	PixMessage
Transport Protocol	TCP/UDP/ICMP/IGMP/ARP/PPTP/PPP/PPPoE/TACACS+/ESMTP

Troubleshooting

What is the expected behavior from the connector for a typical teardown message from ASA?

For teardown messages, because the direction of the flow is not known from the syslog message, we do not know for certain what is the source and what is the destination. Based on the format of the syslog message (shown below) we map the **for/from** part to `source` and the **to** part to `destination`.

```
  Apr 20 17:54:51 151.174.6.33 Apr 20 2010 13:54:51: %ASA-6-302014:
Teardown TCP connection 227777586 for outside:98.136.152.54/80 to
inside:172.27.191.13/2710 duration 0:00:00 bytes 4699 TCP FINs
```

How to get the default value in the 'Destination Port' field of ESM for Cisco-ASA with the message ID 212006?

For the Cisco-ASA log with message id 212006, the **Destination Port** can have a different value than the ‘number’; however, it can also be snmp, ssh, ftp, etc. This results in an absence of **Destination Port** value because only the **Application Protocol** field can carry such data.

For example: The default SNMP port number is 161. Therefore, you can enable the port service mapping in the SmartConnector by performing the following steps:

1 While installing the SmartConnector, select **Continue**, and then click **Next**.

2 Select **Modify Connector** and click **Next**.

3 Select **Add, modify, or remove destinations** and click **Next**.

4 Select the **ESM Manager** and click **Next**.

5 Select **Modify destination settings** and click **Next**.

6 In the **Choose a group of destination settings to modify** window, select **Processing**, and then click **Next**.

7 Select **Yes** from the **Enable Port-Service Mapping** drop-down menu and click **Finish**.

8 Select **Done with editing destination settings** and click **Next**.

9 Select **Exit** and click **Next**.

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 (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!