# Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

## Configuration Guide for Cisco Meraki 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 |

# 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 Cisco Meraki Syslog SmartConnector 7

Product Overview 8

Configuration 9

Configuring the Device to Store Messages 9

Additional Considerations for Syslog 9

Enabling Time-Stamps on Log Messages 9

Enabling System Message Logging 10

Setting the Syslog Destination 10

Limiting the Error Message Severity Level 10

Defining the UNIX System Logging Facility 11

Configuring the Syslog SmartConnectors 11

Installing the SmartConnector 14

Preparing to Install the SmartConnector 14

Installing and Configuring the SmartConnector 14

Device Event Mapping to ArcSight Fields 18

Common Mappings to ArcSight ESM Events 18

Cho event type flows, urls, ip_flow_start Mappings to ArcSight ESM Events 18

Type events & airmarshal_eventst Mappings to ArcSight ESM Events 19

Type events & airmarshal_eventst with type = 8021x_auth Mappings to ArcSight ESM Events 19

Type events & airmarshal_eventst with type = 8021x_eap_success Mappings to ArcSight ESM Events 20

Type events & airmarshal_eventst with type = association Mappings to ArcSight ESM Events 20

Type events & airmarshal_eventst with type = association_reject Mappings to ArcSight ESM Events 21

Type events & airmarshal_eventst with type = cli_set_rad_parms Mappings to ArcSight ESM Events 21

Type events & airmarshal_eventst with type = disassociation Mappings to ArcSight ESM Events 22

Type events & airmarshal_eventst with type = 8021x_deauth Mappings to ArcSight ESM Events ..... 23
Type events & airmarshal_eventst type with multiple_dhcp_servers_detected Mappings to ArcSight ESM Events ..... 23
Type events & airmarshal_eventst type = radius_mac_auth Mappings to ArcSight ESM Events ..... 24
Type events & airmarshal_eventst with type = rogue_ssid_detected Mappings to ArcSight ESM Events ..... 24
Type events & airmarshal_eventst with type = splash_auth Mappings to ArcSight ESM Events ..... 25
Type events & airmarshal_eventst with type = wpa_auth Mappings to ArcSight ESM Events ..... 25
Type events & airmarshal_eventst with type = wpa_deauth Mappings to ArcSight ESM Events ..... 26
Type events & airmarshal_eventst with type = ssid_spoofing_detected Mappings to ArcSight ESM Events ..... 26
Type events & airmarshal_eventst with type = device_packet_flood Mappings to ArcSight ESM Events ..... 27
Type events & airmarshal_eventst with type = 8021x_eap_failure Mappings to ArcSight ESM Events ..... 27

Send Documentation Feedback ..... 28

Configuration Guide for Cisco Meraki Syslog SmartConnector

# Configuration Guide for Cisco Meraki Syslog SmartConnector

This guide provides information for installing the SmartConnector for Cisco Meraki Syslog and configuring the IOS 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

Cisco Meraki Software is a cloud-managed networking solution with wireless, switching, security, WAN optimization, and MDM, centrally managed over the web, built from the ground up for cloud management. Cisco Meraki is the leader in cloud-managed networking and among Cisco's fastest-growing portfolios: over 100% annual growth and tens of millions of devices connected worldwide.

# Configuration

## Configuring the Device to Store Messages

To configure a Cisco Meraki device to store messages for reporting purposes from MX security appliances, MR access points, and MS switches:

1. From the Meraki dashboard, navigate to **Network-Wide** > **Configure** > **General**.
2. Go to **Reporting** > **Syslog server configurations**, then click the **Add a syslog server** link to define a new server.
3. Configure the IP address of your syslog server, the UDP port the server is listening on, and the roles you wish to be reported to the server.
4. If the Flows role is enabled for Meraki MX reporting, logging for individual firewall rules can be enabled/disabled on the **Security appliance** > **Configure** > **Firewall** page (Optional for Meraki MX reporting).

## Additional Considerations for Syslog

Syslog messages can take up a large amount of disk space, especially when collecting flows. When deciding on a host to run the syslog server, make sure that you have enough storage space on the host to hold the logs. Consult the syslog-ng man page for further information on only keeping logs for a certain amount of time.

If the environment has multiple MX devices using site-to-site VPN, and logging is done to a syslog server on the remote side of the VPN, that traffic will be subject to the site-to-site firewall.

Note that it might be necessary to create a Site-to-site firewall rule to allow the syslog traffic through. To do this, go to **Security appliance** > **Configure** > **Site-to-site VPN** > **Organization-wide settings** > **Add a rule**.

Follow the instructions in the following sections to enable timestamps and system message logging, and to set the syslog destination, severity level, and syslog facility.

## Enabling Time-Stamps on Log Messages

By default, log messages are not time-stamped. To enable time-stamping of log messages and debug messages, use the following commands in global configuration mode:

```
Router(Config)#service timestamps log datetime localtime
```

```
Router(Config)#service timestamps debug datetime localtime
```

# Enabling System Message Logging

System message logging is enabled by default. It must be enabled to send messages to any destination other than the console. To reenable message logging after it has been disabled, use the following command in global configuration mode:

```
Router(config)#logging on
```

# Setting the Syslog Destination

To identify the syslog server that is to receive logging messages, use the following command in global configuration mode:

```
Router(config)#logging host
```

The *host* argument is the name or IP address of the host. By issuing this command more than once, you build a list of syslog servers that receive logging messages. The `no logging` command deletes the syslog server with the specified address from the list of syslogs.

# Limiting the Error Message Severity Level

You can limit the number of messages by specifying the severity level of the error message. Use the following command in global configuration mode:

```
Router(config)#logging trap level
```

| Keyword | Level | Description | Syslog Def |
|---|---|---|---|
| emergencies | 0 | System unusable | LOG_EMERG |
| alerts | 1 | Immediate action needed | LOG_ALERT |
| critical | 2 | Critical conditions | LOG_CRIT |
| errors | 3 | Error conditions | LOG_ERR |
| warnings | 4 | Warning conditions | LOG_WARNING |
| notifications | 5 | Normal but significant condition | LOG_NOTICE |
| informational | 6 | Informational messages only | LOG_INFO |
| debugging | 7 | Debugging messages | LOG_DEBUG |

## Defining the UNIX System Logging Facility

You can log messages produced by UNIX system utilities. Enable this type of logging and define the UNIX system facility from which you want to log messages. Consult the operator manual for your UNIX operating system for more information about these UNIX system facilities.

To define UNIX system facility message logging, use the following command in global configuration mode:

`Router(config)#logging facility` *`facility-type`*

# 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 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

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:<br>• **Solaris:** `\var\adm\messages`<br>• **Linux:** `\var\log\messages`<br>You can use a wildcard pattern in the file name.<br>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:<br>• **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`<br>• **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;`<br>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.

## Common Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Action | Action |
| Device Custom Number 2 | eventType |
| Device Event Category | eventType |
| Device Event Class ID | __concatenate(eventType," ",_oneOf(action,extraAction)) |
| Device Host Name | deviceHostName |
| Device Product | Meraki Access Point |
| Device Receipt Time | __concatenate(time,second) |
| Device Vendor | 'CISCO' |
| Message | Message |
| Name | __concatenate(eventType," ",_oneOf(action,extraAction)) |
| Request Url | requestUrl |

## Cho event type flows, urls, ip_flow_start Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Address | dst |
| Destination Port | oneOf(dport,dst) |
| Destination Translated Address | translated_dst_ip |
| Destination Translated Port | translated_port |
| Device Custom Number 1 | type |
| Device Custom Number 1 Label | Type |

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Request Client Application | agent |
| Source Address | src |
| Source Mac Address | mac |
| Source Port | oneOf(sport,src) |
| Transport Protocol | protocol |

# Type events & airmarshal_eventst Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Address | dst |
| Destination Port | oneOf(dport,dst) |
| Destination Translated Address | translated_dst_ip |
| Destination Translated Port | translated_port |
| Device Custom Number 1 | type |
| Device Custom Number 1 Label | Type |
| Request Client Application | agent |
| Source Address | src |
| Source Mac Address | mac |
| Source Port | oneOf(sport,src) |
| Transport Protocol | protocol |

# Type events & airmarshal_eventst with type = 8021x_ auth Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |
| Source Address | client_ip |
| Source Mac Address | client_mac |
| Source User Name | identity |

# Type events & airmarshal_eventst with type = 8021x_eap_success Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |
| Source Address | client_ip |
| Source Mac Address | client_mac |
| Source User Name | identity |

# Type events & airmarshal_eventst with type = association Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom String 2 | channel |
| Device Custom String 2 Label | Channel |
| Device Custom String 3 | rssi |
| Device Custom String 3 Label | Received Signal Strength Indication |
| Source Address | client_ip |
| Source Mac Address | client_mac |

# Type events & airmarshal_eventst with type = association_reject Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Address | best_ap |
| Device Custom Number 1 | load |
| Device Custom Number 1 Label | Load |
| Device Custom Number 2 | best_ap_load |
| Device Custom Number 2 Label | Best Ap Load |
| Device Custom Number 3 | best_ap_rssi |
| Device Custom Number 3 Label | Best Ap Rssi |

# Type events & airmarshal_eventst with type = cli_set_ rad_parms Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | vlan |
| Device Custom Number 3 Label | Vlan |
| Device Custom String 3 | rtt |

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom String 3 Label | Round Trip Time |
| Device Custom String 4 | attr |
| Device Custom String 4 Label | Attribute |

# Type events & airmarshal_eventst with type = disassociation Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | vlan |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Vlan |
| Device Custom Number 3 Label | Association ID |
| Device Custom String 2 | channel |
| Device Custom String 2 Label | Channel |
| Device Custom String 4 | dns_server |
| Device Custom String 4 Label | DNS Server |
| Device Custom String 5 | concatenate("dhcp_ip: ",dhcp_ip,"\|dhcp_server: ",dhcp_server,"\|dhcp_server_mac: ",dhcp_server_mac) |
| Device Custom String 5 Label | DHCP Information |
| Reason | reason |
| Source Address | ip_src |
| Source Mac Address | client_mac |
| Source User Name | identity |

# Type events & airmarshal_eventst with type = 8021x_deauth Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |
| Source Address | client_ip |
| Source Mac Address | client_mac |
| Source User Name | identity |

# Type events & airmarshal_eventst type with multiple_dhcp_servers_detected Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Address | server_ip |
| Destination Mac Address | server_mac |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Source Address | original_server_ip |
| Source Mac Address | original_server_mac |

# Type events & airmarshal_eventst type = radius_mac_auth Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Event Outcome | resp |

# Type events & airmarshal_eventst with type = rogue_ssid_detected Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Mac Address | dst |
| Device Custom Number 1 | vlan_id |
| Device Custom Number 1 Label | Vlan ID |
| Device Custom Number 2 | fc_type |
| Device Custom Number 2 Label | FC Type |
| Device Custom Number 3 | fc_subtype |
| Device Custom Number 3 Label | FC SubType |
| Device Custom String 2 | channel |
| Device Custom String 2 Label | Channel |
| Device Custom String 3 | rssi |
| Device Custom String 3 Label | Received Signal Strength Indication |
| Device Custom String 4 | ssid |
| Device Custom String 4 Label | SSID |
| Device Custom String 5 | bssid |
| Device Custom String 5 Label | BSSID |

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom String 6 | wired_mac |
| Device Custom String 6 Label | Wired Mac |
| Source Mac Address | src |

# Type events & airmarshal_eventst with type = splash_ auth Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| bytesIn | download |
| bytesOut | upload |
| Device Custom Number 1 | duration |
| Device Custom Number 1 Label | Duration |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | wired_vlan |
| Device Custom Number 3 Label | Wired Vlan |
| Source Mac Address | mac |

# Type events & airmarshal_eventst with type = wpa_auth Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |
| Source Address | client_ip |
| Source Mac Address | client_mac |

# Type events & airmarshal_eventst with type = wpa_deauth Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |
| Source Address | client_ip |
| Source Mac Address | client_mac |

# Type events & airmarshal_eventst with type = ssid_spoofing_detected Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Mac Address | dst |
| Device Custom Number 2 | vap |
| Device Custom Number 2 | fc_type |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 2 Label | FC Type |
| Device Custom Number 3 | fc_subtype |
| Device Custom Number 3 Label | FC SubType |
| Device Custom String 2 | channel |
| Device Custom String 2 Label | Channel |
| Device Custom String 4 | ssid |
| Device Custom String 4 Label | SSID |
| Device Custom String 5 | bssid |
| Device Custom String 5 Label | BSSID |
| Source Mac Address | src |

# Type events & airmarshal_eventst with type = device_packet_flood Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Destination Mac Address | device |
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | alarm_id |
| Device Custom Number 2 Label | Alarm ID |
| Device Custom Number 3 | dos_count |
| Device Custom Number 3 Label | DOS Count |
| Device Custom String 3 | packet |
| Device Custom String 3 Label | Packet |
| Device Custom String 4 | state |
| Device Custom String 4 Label | State |
| Device Custom String 5 | inter_arrival |
| Device Custom String 5 Label | Inter Arrival |
| reason | reason |

# Type events & airmarshal_eventst with type = 8021x_eap_failure Mappings to ArcSight ESM Events

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Device Custom Number 1 | radio |
| Device Custom Number 1 Label | Radio |
| Device Custom Number 2 | vap |
| Device Custom Number 2 Label | Virtual Access Point |
| Device Custom Number 3 | aid |
| Device Custom Number 3 Label | Association ID |
| Source User Name | identity |

# 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 Cisco Meraki 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!