Micro Focus Security ArcSight Connectors

SmartConnector for Cisco Meraki Syslog

Configuration Guide

September 17, 2020

Configuration Guide

SmartConnector for Cisco Meraki Syslog

September 17, 2020

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

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://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
04/30/2020	First edition of this guide. Added support to model MR52

SmartConnector for Cisco Meraki Syslog

This guide provides information for installing the SmartConnector for Cisco Meraki Syslog and configuring the IOS device for syslog event collection. This connector supports Cisco Meraki model MR52.

Product Overview

Cisco Meraki Software is a complete 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

Configure 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. To begin setting up a Syslog server on the Meraki dashboard, first, navigate to Network-Wide > Configure > General.
2. Here you will see a section for Reporting, with the option for Syslog server configurations. Click on the Add a syslog server link to define a new server.
3. Configure an 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 to 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. As such, note that it may be necessary to create a Site-to-site firewall rule to allow the syslog traffic through. This is done from 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.

Enable 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
```

Enable 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
```

Set 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.

Limit the Error Message Severity Level

You can limit the number of messages by specifying the severity level of the error message. To do so, 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

Keyword	Level	Description	Syslog Def
debugging	7	Debugging messages	LOG_DEBUG

Define the UNIX System Logging Facility

You can log messages produced by UNIX system utilities. To do this, 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
```

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

Syslog Daemon
Syslog Pipe
Syslog File

The Syslog Daemon SmartConnector

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

If you are using SmartConnector for Syslog Daemon, add the following statement in the `rsyslog.conf` file to forward Oracle Audit events so that Syslog Daemon will start receiving events: `*.* @@(remote/local-host-IP):514`

Sample example: `local1.warning @@10.0.0.1:514`

> You can either use *.* to read all Syslog events or you can filter specific events by replacing regex with the specific event name. For example: `*.* @@(remote/local-host-IP):514` and `local1.warning @@10.0.0.1:514`

> Use @@ to send events over a TCP connection and use @ to send events over an UDP connection.

If you are running SmartConnector for Syslog Daemon on the same machine as the Oracle 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 may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

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

Configure the Syslog Pipe or File SmartConnector

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

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

For syslog pipe:

1. Create a pipe by executing the following command:

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

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

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

   or

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

   depending on your operating system.

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

On RedHat Linux, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

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

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

For syslog file:

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

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

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

Install the SmartConnector

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

Syslog Installation

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

Syslog Daemon
Syslog Pipe
Syslog File

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

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

Prepare to Install Connector

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

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

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

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

Install Core Software

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

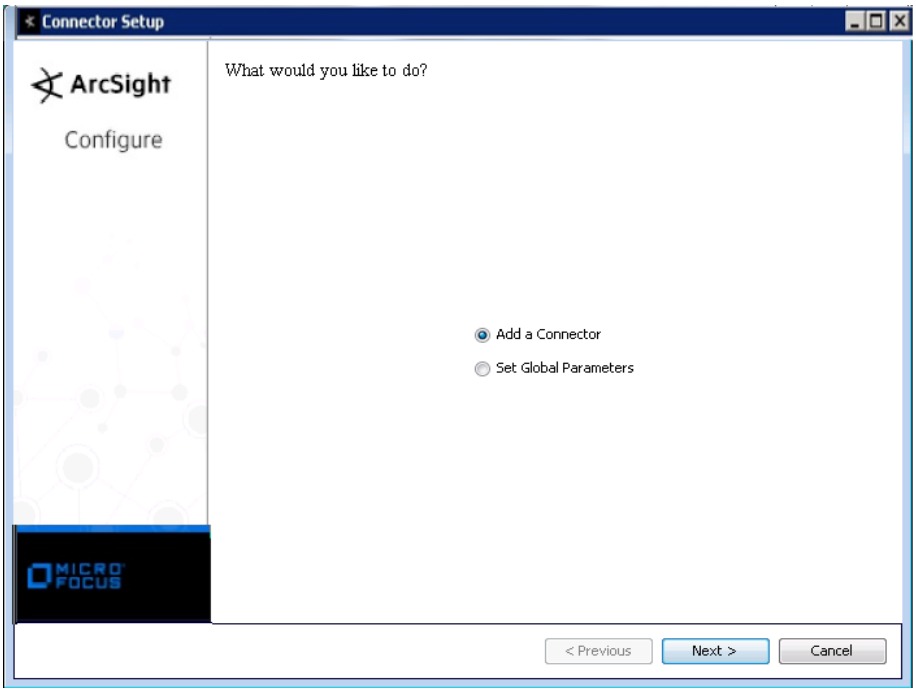
1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

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

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

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

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



Set Global Parameters (optional)

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

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

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

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.

Parameter	Setting
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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

Select Connector and Add Parameter Information

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

Syslog Daemon Parameters	*Network port*	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
Syslog File Parameters	*File Absolute Path Name*	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux). A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation. For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example: `filename'yyyy-MM-dd'.log;`

	For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: `filename'%d,1,99,true'.log;` Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.
Reading Events Real Time or Batch	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
Action Upon Reaching EOF	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
File Extension If Rename Action	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

Select a Destination

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

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

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

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

Complete Installation and Configuration

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

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

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for

Service Internal Name and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

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

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

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

Run the SmartConnector

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

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

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

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

Device Event Mapping to ArcSight Fields

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

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'

ArcSight ESM Field	Device-Specific Field
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
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
Device Custom Number 3	aid
Device Custom Number 3 Label	Association ID

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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