Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Cisco Secure ACS Syslog SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

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

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for Cisco Secure ACS Syslog SmartConnector

Configuration Guide for Cisco Secure ACS Syslog SmartConnector

This guide provides information for installing the SmartConnector for Cisco Secure ACS Syslog and configuring the device for 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 Secure Access Control Server (ACS) for Windows is a major component of Cisco trust and identity networking security solutions. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework.

Configuration

Configure Cisco ACS Syslog Logging

This section provides configuration information for alarm syslog targets, remote log targets, and global logging categories.

Log Message Severity Levels

Log messages can have the following severity levels:

ACS Severity Level	Description	Syslog Severity Level
Fatal	Emergency. ACS is not functioning and immediate action must be taken.	1
Error	Critical or error conditions exist.	3
Warn	Normal, but significant condition.	4
Notice	Audit and accounting messages. Messages of severity NOTICE are always sent to the configured log targets and are not filtered, regardless of the specified severity threshold.	5
Info	Diagnostic informational message.	6
Debug	Diagnostic message.	7

Syslog Message Header Format

Syslog messages are sent to remote syslog servers with this syslog message header format:

```
  <pri_num> <YYYY Mmm DD hh:mm:ss> <xx:xx:xx:xx/host_name> <cat_name>
<msg_id> <total_seg> <seg_num>
```

Where the content of the header is described thusly:

- pri_num - The priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. The facility code values are:

  - Local0 (Code=16)
  - Local1 (Code=17)
  - Local2 (Code=18)
  - Local3 (Code=19)
  - Local4 (Code=20)
  - Local5 (Code=21)
  - Local6 (Code=22, the default)
  - Local7 (Code=23)
- YYYY Mmm DD hh:mm:ss - Date of message generation, based on the local clock of the originating ACS.
  - YYYY - Numeric representation of the year.
  - Mmm - Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
  - DD - Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number.
  - hh - The hour of the day—00 to 23.
  - mm - The minute of the hour—00 to 59.
  - ss - The second of the minute—00 to 59.

Some devices send messages that specify a time zone in the format -/+hhmm, where - and + identify the directional offset from the ACS server's time zone. hh is the number of offset hours and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on an ACS node that is two hours ahead of the ACS server's time zone.

- xx:xx:xx:xx/host_name - The IP address of the originating ACS, or the hostname.
- cat_name - The logging category name preceded by the CSCOacs string.
- msg_id - The unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.
- total_seg - Total number of segments in a log message. Long messages are divided into more than one segment.
- seg_num - The segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

Create Alarm Syslog Targets

The Monitoring and Report Viewer sends alarm notifications as syslog messages. To receive the syslog messages, a syslog server must be configured with alarm syslog targets.

To configure a syslog server:

1 Navigate to **Monitoring Configuration** > **System Configuration** > **Alarm Syslog Targets**. The Alarm Syslog Targets page displays.

2 Click **Create**.

3 Enter values for the following fields:

- Option Identification: Name - The name of the alarm syslog target. The maximum length is 255 characters.
- Option Identification: Description - (Optional) A brief description of the alarm to be created. The maximum length is 255 characters.
- Configuration: IP Address - IP address of the machine where the syslog server runs.
- Use Advanced Syslog Options: Port - Port to which the syslog server listens. The default is 514. The value can be from 1 to 65535.
- Use Advanced Syslog Options: Facility Code - Remote syslog server targets are identified by the facility code. The value can be Local0 through Local7.

4 Click **Submit.**

Configure Remote Log Targets

Logging messages for a specific logging category can be sent to remote log targets residing on a syslog server.

To create a remote log target:

1 Navigate to **System Administration** > **Configuration** > **Log Configuration** > **Remote Log Targets**. The Remote Log Targets page displays.

2 Perform one of the following options:

- Click **Create**. The **Remote Log Targets > Create** page displays.
- Click the check box next to the remote log target that you want to duplicate and click **Duplicate**. The Remote Log Targets > Duplicate page displays.

- Click the check box next to the remote log target that you want to modify and click **Edit**. The Remote Log Targets > Edit page displays.

3 Enter values for the following fields:

- General: Name - The name of the remote log target. The maximum length is 32 characters.
- General: Description - The description of the remote log target. The maximum length is 1024 characters.
- General: Type - The type of the remote log target. Syslog is the only option.
- Target Configuration: IP Address - IP address of the remote log target, in the format x.x.x.x.
- Target Configuration (v5.6 only): Target Type - Select UDP Syslog, TCP Syslog, or Secure TCP Syslog to define the type of connection used to send logg messages.
- Target Configuration: Use Advanced Syslog Options - Click to enable the advanced syslog options - port number, facility code, and maximum length.
- Target Configuration: Port - The port number of the remote log target used as the communication channel between the ACS and the remote log target. The default is 514.
- Target Configuration: Facility Code - Remote syslog server targets are identified by the facility code. The value can be one of the following: Local0 (Code=16), Local1 (Code=17), Local2 (Code=18), Local3 (Code=19), Local4 (Code=20), Local5 (Code=21), Local6 (Code=22, the default), Local7 (Code=23).
- Target Configuration: Maximum Length - The maximum length of the remote log target messages. Values can be from 200 to 1024.

4 Click **Submit.** The Remote Log Targets page displays with the new remote log target.

Configuring Global Logging Categories

Select and configure global logging categories for local targets and remote syslog targets. A logging category contains message codes that describe a function of ACS, a flow, or a use case. Categories are arranged in a hierarchical structure and used for logging configuration.

- Name - a descriptive name
- Type - Audit, Accounting, or Diagnostics
- Attribute List - a list of attributes that can be logged with messages associated with a category

To select and configure a global logging category:

1. Navigate to **System Administration** > **Configuration** > **Log Configuration** > **Logging Categories** > **Global**. The Logging Categories page is displayed
2. Click the name of the logging category you want to configure or, click the radio button next to the name of the logging category you want to configure and click **Edit**.
3. Enter values for General: Log Severity.
   - FATAL: Emergency. ACS is not usable and you must take action immediately.
   - ERROR: Critical or error condition.
   - WARN: Normal, but significant condition. (Default)
   - INFO: Informational message.
   - DEBUG: Diagnostic bug message.

   For diagnostic logging categories, use the drop-down list box to select the severity level. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.)
4. Configure Local Settings for Category.

   Target Configuration: Log to Local Target - Check to enable logging to the local target. (For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled.)
5. Configure Logged Attributes.

   Display only. All attributes are logged to the local target.
6. To configure a remote syslog target, click the **Remote Syslog Target** and select targets:
   - Available Targets: Select the targets you want for your configuration and move them to the Selected Targets list.
   - Selected Targets: This list has the targets you want included in your configuration. You can move unwanted targets to the Available Targets list.
7. Click **Submit.** The Remote Log Targets page displays with the new remote log target.

Format of Syslog Messages in ACS Reports

Syslog messages included in ACS reports have the following format:

<n> *mmm dd hh:mm:ss XX:XX:XX:XX TAG msg_id total_seg seg# A1=V1*

The elements of the message are:

- *n* – The Priority value of the message; it is a combination of facility and severity of the syslog message.
- *mmm dd hh:mm:ss* – Date and time of the message.
- *XX:XX:XX:XX* – IP address of the machine generating this syslog message.
- *TAG* – One of the following values, depending upon the application name.
- CisACS_01_PassedAuth–Cisco ACS passed authentications.
- CisACS_02_FailedAuth–Cisco ACS failed attempts.
- CisACS_03_RADIUSAcc–Cisco ACS RADIUS accounting.
- CisACS_04_TACACSAcc–Cisco ACS TACACS+ accounting.
- CisACS_05_TACACSAdmin–Cisco ACS TACACS+ administration.
- CisACS_06_VoIPAcc–Cisco ACS VoIP accounting.
- CisACS_11_BackRestore–ACS backup and restore log messages.
- CisACS_12_Replication–ACS database replication log messages.
- CisACS_13_AdminAudit–ACS administration audit log messages.
- CisACS_14_PassChanges–ACS user password changes log messages.
- CisACS_15_ServiceMon–ACS service monitoring log messages.
- CisACS_16_ApplAdmin–ACS appliance administration audit log messages.
- L*msg_id* – Unique message ID. All segments of one message share the same message ID.
- *total_seg* – Total number of segments in this message.
- *seg#* – Segment sequence number within this message segmentation.
- *A1=V1* – Attribute-value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Facility Codes

ACS syslog messages use the following facility values:

- **4:** Security and authorization messages. This value is used for all AAA related messaged (failed attempts, passed attempts, accounting, and so on).
- **13:** Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (informational). For example, if the facility value is 13 and the severity value is 6, the Priority value is 110 ((8 x 13) + 6). The Priority value appears according to the syslog server setu7p, and might appear as one of the following:

- **System3.Info**
- **<110>**

You cannot configure the format of the syslog facility and severity on ACS.

The following sample syslog message shows how the facility code and other information might look in a ACS-generated syslog message:

```
  <110> Oct 16 08:58:07 64.103.114.149 CisACS_!#_AdminAudit 18729fp11 1 0
AAA Server=tfurman-w2k,admin-username-local_login,browser4-
ip=127.0.0.1,text-message=Administration session finished,
```

In this example, <110> represents the calculated value when the facility code is 13 (the log audit facility code).

Message Length Restrictions

When an ACS message exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- If all attribute-value elements fit into one segment, no segmentation is performed.
- If the message does not fit into one segment, the message is split between attribute-value pairs, keeping an attribute-value pair complete within the segment.
- In rare cases when one attribute-value pair is too long to fit in one segment all by itself, the value is segmented between sequenced segments of the message. Such segmentation might occur if an attribute value contains several hundreds of characters. In general, ACS attribute values are designed to avoid such length.

All segments of one message have exactly the same header. The `<msg_id>` and `<total_seg>` values are shared between all components. The `<seg#>` is set according to the number of segments and the relative part of the content that follows.

Use the following message length restrictions:

- To send messages to a standard syslog server, the maximum message length must be 1024 bytes.
- To send messages to Cisco Security Monitoring, Analysis, and Response System (MARS), the maximum message length must be 500 bytes.
- Message segmentation must be used when the original message, including header and data, exceeds length limitations.

ACS Syslog Messages with More Than Two Segments

When an ACS syslog message has more than two segments, the parser processes the first segment and appends additional key/value pairs from the segments that follow to merge them all into one event.

Configuring for 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: • **Solaris:** `\var\adm\messages` • **Linux:** `\var\log\messages` You can use a wildcard pattern in the file name. In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation: • **Date format log rotation:** The device creates a new log at a specified time in the with the naming convention `filename.timestamp.log`. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new `filename.timestamp.log` and begins processing that file. To enable this log rotation, specify timestap in `yyyy-MM-dd` date format. For example, `filename.yyyy-MM-dd.log` • **Index log rotation:** The device writes to indexed files in the following format: `filename.log.001, filename.log.002, filename.log.003`, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:`filename'%d,1,99,true'.log;` Specifying `true` indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of `true` is optional.
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

b. Click **Next.**

5. Select a destination and configure parameters.
6. Specify a name for the connector.
7. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

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

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Device Vendor and Device Product fields may sometimes show UNIX rather than the actual vendor and product names.

Cisco Secure ACS General Mappings

ArcSight ESM Field	Device-Specific Field
Connector (Agent) Severity	Very High = FATAL, High = ERROR, Medium = WARN, Low = INFO, DEBUG, NOTICE, Unknown
Device Custom Number 1	ConfigVersionId
Device Event Category	msg
Device Event Class Id	tag
Device Host Name	address
Device Product	'Cisco Secure ACS'
Device Receipt Time	timestamp
Device Severity	One of (severity, mergedevent.deviceSeverity, "Unknown")
Device Vendor	'CISCO'
Device Version	ACSVersion
External ID	msgid
Message	message
Name	msg

Cisco Secure ACS Administrative and Operational Audit Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	AdminIPAddress
Destination Service Name	AdminInterface
Destination User Name	AdminName
Device Custom String 1	AdminSession
Device Custom String 4	AuthenticationMethod
Device Custom String 5	SelectedAccessService
Reason	Response
Source Address	AdministratorClientIP
Source User Name	UserName

Cisco Secure ACS Failed Attempts

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Destination Address	Device IP Address
Destination NT Domain	ADDomain
Destination Port	Device port
Destination Service Name	Service
Destination User Name	User
Device Address	DestinationIPAddress
Device Custom String 1	AcsSessionID
Device Custom String 2	Port
Device Custom String 3	AuthorizationPolicyMatchedRule
Device Custom String 4	Authen-Method
Device Custom String 5	Type
Device Custom String 6	NetworkDeviceGroups

ArcSight ESM Field	Device-Specific Field
Event Outcome	Response one of (Pass=Success, Fail=Failure)
Reason	oneOf(Response,FailureReason)
Source Host Name	Remote-Address
Source User Name	UserName

Cisco Secure ACS Passed Authentications

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Destination Address	oneOfAddress(DestinationIPAddress,Device IP Address)
Destination Address	DestinationIPAddress
Destination DNS Domain	AD-Domain
Destination Mac Address	Called-Station-ID
Destination NT Domain	ADDomain
Destination Port	Destination Port
Destination Service Name	Service
Destination Translated Address	NAS-IP-Address
Destination Translated Port	NAS-Port
Destination User Name	User
Device Address	Device IP Address
Device Custom Number 2	Privilege Level
Device Custom String 1	AcsSessionID
Device Custom String 2	Port
Device Custom String 3	AuthorizationPolicyMatchedRule
Device Custom String 4	ExternalGroups
Device Custom String 5	Type
Device Custom String 5	Type or Service-Type
Device Custom String 6	NetworkDeviceGroups
Event Outcome	Response one of (Pass=Success, Fail=Failure)

ArcSight ESM Field	Device-Specific Field
File Hash	SelectedCommandSet
File Id	NAS-Port-Id
File Type	NAS-Port-Type
FileName	NetworkDeviceName
Old File Hash	MatchedCommandSet
Old File Id	AD-Host-Candidate-Identities
Old File Type	AD-Host-Resolved-Identities
Request Context	CmdSet
Request Method	AuthenticationMethod
Source Address	Calling-Station-ID
Source DNS Domain	AD-Host-DNS-Domain
Source Host Name	Remote-Address
Source Mac Address	Calling-Station-ID
Source User Name	UserName

Cisco Secure ACS TACACS Accounting

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Remote-Address
Destination Service Name	Service
Destination User Name	User
Device Action	AcctRequest-Flags
Device Custom String 1	AcsSessionID
Device Custom String 2	Port
Device Custom String 4	Authen-Method
Device Custom String 5	Type
Device Custom String 6	NetworkDeviceGroups

Cisco Secure ACS TACACS Diagnostics

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Remote-Address
Destination Service name	Service
Destination User Name	User
Device Custom Number 2	SessionId
Device Custom String 1	AcsSessionID
Device Custom String 3	Device Port
Device Custom String 5	Type
Event Outcome	Response one of (Pass=Success, Fail=Failure)

Cisco Secure ACS Policy Diagnostics

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Device Custom String 1	AcsSessionID
Device Receipt Time	Time and Date
Source User Name	UserName

Cisco Secure ACS RADIUS Diagnostics

ArcSight ESM Field	Device-Specific Field
Destination Address	NAS-IP-Address
Destination Host Name	Called-Station-ID
Destination Mac Address	Called-Station-ID
Destination Port	DestinationPort
Destination User Name	User-Name
Device Custom Sring 5	Service-Type
Device Custom String 1	AcsSessionID

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	NAS-Port
Device Custom String 3	Device Port
Source Mac Address	Calling-Station-ID

Cisco Secure ACS System Statistics

ArcSight ESM Field	Device-Specific Field
Additional data	SysStatsUtilizationNetwork
Device Custom String 1	role (Role Name)

Cisco Secure ACS Authentication Flow Diagnostics

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	AcsSessionID
Source User Name	UserName

Cisco Secure ACS Administrator Authentication and Authorization

ArcSight ESM Field	Device-Specific Field
Source User Name	UserName

Cisco Secure ACS Identity Stores Diagnostics

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Device Custom String 1	AcsSessionID
Source User Name	UserName

Cisco Secure ACS RADIUS Accounting

ArcSight ESM Field	Device-Specific Field
Destination Address	Device IP Address
Destination User Name	User-Name
Device Address	Destination IP Address
Device Custom String 1	AcsSessionID
Device Custom String 2	NAS-Port
Device Custom String 5	Service-Type
Device Custom String 6	NetworkDeviceGroup
Source Address	Framed-IP-Address

Note: If a truncate error related to UNIX events pops, add the following parameter in "agent.properties":

size.validation.fields = rawEvent,message

size.validation.sizes = 7000,7000

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 Secure ACS 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!