Micro Focus Security ArcSight SmartConnector Parsers

Software Version: 8.3.0

ArcSight Customer Support - Help with SmartConnector and Parser Updates

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 home page of this Help 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

ArcSight Customer Support - Help with SmartConnector and Parser Updates

About SmartConnectors and Event Parsers

The integration of device event-feeds in to ArcSight relies on the availability of a suitable SmartConnector (or FlexConnector) to both acquire and parse/normalize the raw device events in to the ArcSight schema. ArcSight SmartConnectors exist for the most common source devices and will have been tested, certified and documented against a given range of device versions. The SmartConnector release process follows a split monthly/quarterly cycle, whereby updates to parsing of many connectors are released each month and new features or support for completely new source devices requiring code-changes occur within the quarterly release.

As new versions of each device become available, existing parsing support might:

- Work perfectly well due to little or no change in the event format itself (even though not yet formally certified)
- Prove incomplete or suboptimal, possibly matched against an incorrect parser for a different source device
- Fail entirely to match the new format of the source events, resulting in 'unparsed event' alerts being generated
- Require a new mechanism entirely to acquire the events ready for parsing, resulting in no events being retrieved at all

Furthermore, parsing support even for device versions already certified by ArcSight may not prove optimal for all use-cases and would also require update to the associated connector parser to better meet a specific customer requirement.

Supporting Minor Parser Updates and Overrides

The majority of parsing requirements fall into the category of 'device version-updates' and typically require only minor changes to reinstate proper normalization. In order to streamline and hasten the update of the connectors, we have initiated a revised process via our Support organization who will now accept requests for connector device version-updates and, dependent upon the scope of work required as well as the availability of sample raw device events, may be able to devise and provide a 'parser override' before the next monthly or quarterly release. Previously, such requests fell under the 'Enhancement Request' process that is driven instead through the ArcSight Idea Exchange portal.

Thus, where sub-optimal or failed parsing is observed for either an existing certified device version, or else an updated version of an existing supported device, do the following:

- Check the available documentation to determine whether a more recent SmartConnector release is expected to support your device/version and upgrade the connector version accordingly. Otherwise,
- Raise a case with Support requesting a parser update
- State to Support the precise name, sub-component (where relevant) and version of the device that is no longer being parsed as expected.
- Acquire and provide Support with a set of sample events (wherever possible), that no longer parse correctly – highlighting the parsing deficiencies where not already self-evident
- Provide any relevant context, such as device version that last parsed correctly or other relevant data that may assist the triage process.

Once the prerequisite data points have been captured, Support will first attempt to reproduce the reported parsing behavior, before then engaging our development team to determine the scope of work required to correct or enhance the current parsing. Support will keep you informed of progress through the support-case and, where a parser override can be devised before the next release cycle, will share that with you for validation within your environment. Once validated, the parser changes will be automatically rolled-up in to the next parser AUP release.

Supporting Device Version Updates

Where the changes instead require more significant investigation, it may not be possible to provide an interim parser override. In this case, a formal request will be raised internally on your behalf and targeted for a future release. Support will let you know the outcome.

ArcSight recommends that our customers to work closely with their IT Ops team to preempt the upgrade of any source devices that feed ArcSight and review the latest SmartConnector Configuration Guide for each device to check whether or not the new device version has already been certified by ArcSight and thus avoid or mitigate any delay before updated parsing support can be made available. Given sufficient time before the roll-out of a new device version, it would therefore be appropriate to post a new 'idea' on the ArcSight Idea Exchange portal for triage by our Product Management team and potential inclusion in to the usual release-cycle. However, we understand that this preemptive approach is not always possible and hence have introduced the revised process described above to help our customers restore full visibility of their security events as soon as practicable.

Supporting Un-Obfuscated Parsers

Should you decide to develop an updated parser or override the out-of-the-box provided parser, we are pleased to announce that, as of the v8.0 SmartConnector release (July 2020), each release will include an unobfuscated/plaintext copy of the entire set of ArcSight parser files, which will provide a valuable starting-point for further parser development.

Supporting New Device Connectors

Finally, the ArcSight Idea Exchange portal remains the appropriate route for support requests for devices for which no SmartConnector is yet available. Please do not forget our FlexConnector SDK – available as part of your ArcSight entitlement – should you have the ability in-house to devise your own custom parsers, or to engage our Professional Services organization for more substantial parser development.

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 ArcSight Customer Support - Help with SmartConnector and Parser Updates (SmartConnector Parsers 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!