Micro Focus Security ArcSight Smart Connectors

Software Version: 7.15.0.8295.0

Release Notes

Document Release Date: April 30, 2020
Software Release Date: April 30, 2020

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:

ArcSight Product Documentation on the Micro Focus Security Community

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

Overview 5

What's New in this Release 6

New SmartConnector 6

New Device, Component, or OS Version Support 7

SmartConnector Enhancements 9

Closed Issues 10

System Requirements 13

Hardware Requirements 13

Known Limitations 14

Upgrading to 7.15.0.8295.0. 18

To Apply this Release 19

Connector End-of-Life Notices 20

SmartConnector Support Ending Soon 20

SmartConnector Support Recently Ended 20

Support Ended 11/22/2019 20

Support Ended 8/21/2019 20

Support Ended 4/28/2018 20

Support Ended 02/21/2018 20

Send Documentation Feedback 21

Overview

These notes describe how to apply this latest release of ArcSight SmartConnectors, as well as providing other information about recent changes and open and closed issues (generated by various vendor devices) to the ArcSight ESM Manager, Logger, or other destinations.

A connector is an application that collects raw events from security devices, processes them into ArcSight security events, and transports them to destination devices. Connectors are the interface between the Manager and the network devices that generate ESM-relevant data on your network.

Connectors collect event data from network devices, then normalize it in two ways. First, they normalize values (such as severity, priority, and time zone) into a common format. Also, they normalize the data structure into a common schema. Connectors can filter and aggregate the events to reduce the volume sent to the Manager, ArcSight Logger, or other destinations, which increases ArcSight's efficiency and reduces event processing time.

Note: The device versions currently documented in individual SmartConnector configuration guides are versions that have been tested by ArcSight Quality Assurance. These are generally referred to as versions certified. For minor device versions that fall in between certified versions, it has been our experience that vendors typically do not make major changes to the event generation mechanism in minor versions therefore, we consider these versions to be supported. Minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.0 have been certified; Dragon Export Tool version 7.5 is considered to be supported.

In brief, connectors:

- Collect all the data you need from a source device, eliminating the need to return to the device during an investigation or audit.
- Parse individual events and normalize event values (such as severity, priority and time zone) into a common schema (format) for use by the ESM Manager.
- Filter out data you know is not needed for analysis, thus saving network bandwidth and storage space (optional).
- Aggregate events to reduce the quantity of events sent to the ESM Manager, increasing ArcSight's efficiency and reducing event processing time (optional).
- Categorize events using a common, human-readable format, saving you time and making it easier to use those event categories to build filters, rules, reports, and data monitors.
- Pass processed events to the ESM Manager.

Depending upon the network device, some connectors can issue commands to devices. These actions can be executed manually or through automated actions from rules and some data monitors.

Integrated into this release

Parser update releases 7.14.1.8253.0, 7.14.2.8258.0, and 7.14.3.8270.0 have been integrated into this framework release. These releases contain version updates, fixed issues, and enhancements for a number of SmartConnectors. For details, see the corresponding release notes on the Micro Focus Security Community.

- 7.14.3.8270.0 Release Notes
- 7.14.2.8258.0 Release Notes
- 7.14.1.8253.0 Release Notes

What's New in this Release

SmartConnector 7.15.0 includes the following capabilities:

New SmartConnector

SmartConnector for	Number	New Device, Component, or OS Version
Cisco Meraki Syslog	CON-22647	Added support for model MR52
MS Office 365: Microsoft Exchange Online Message Tracking	CON-19977	Added support for Microsoft Exchange Online Message Tracking

New Device, Component, or OS Version Support

SmartConnector for	Number	New Device, Component, or OS Version
All SmartConnectors	CON-23473	CentOS 8.1 is now supported.
	CON-23460	SLES 15 & SLES 15.1 are now supported.
	CON-23459	RHEL 8.1 is now supported.
	CON-17259	An allocation failure message is being displayed in some logs. This is normal GC (Allocation Failure) behavior. Unfortunately, it was the wording chosen by the vendor while generating young Eden Garbage Collection
	CON-23531	This framework release includes event categorization updates up to the release of February R2 2020. Later AUP Packages can be downloaded from SSO and ESM and will take Micro Focus SmartConnectors 7.15.0.8295.0 precedence over them.
MS Office 365:	CON-20005 CON-21256 CON-21257 CON-22046 CON-23157 CON-23339	Added support for Sway events, PowerBIAudit events, CRM events, Yammer events, SkypeForBusiness events, Discovery events, Microsoft Team events, Advanced Threat Protection events, Advanced eDiscovery events, Project events, Security and Compliance Center events, and Power Apps events.
ArcSight FlexConnector	CON-22907	Added new operation "scientificNotationToStringOperation" to ArcSight Operators. Currently, none of the fields in ESM show “double” data type. Therefore, it is recommended to map it as a string field. **To apply the fix:** Create new parameter “parsedoubleasstring”: • Default value: false • If users set this parameter to true, the token with data type “double”, will not be converted to the scientific notation.

SmartConnector for	Number	New Device, Component, or OS Version
Amazon Web Services CloudWatch	CON-23158	The SmartConnector installation prerequisites have been modified so that high privileges are no longer a requirement.
	CON-23159	Users can now use "existing" log groups.
	CON-22783	Added support for Amazon Cloud HSM Audit Logs.

SmartConnector Enhancements

In each SmartConnector release, various security fixes, feature updates, and bug fixes are made to the field mappings for individual SmartConnectors. If you use any of the SmartConnectors listed in the "Closed Issues" section of these release notes, be aware that installing the updated SmartConnector can impact your created content.

SmartConnector for	Number	Description
All SmartConnectors	CON-16788	From the ESM Console, users can now detect when events / files are dropped from the agent queue.
	CON-23833	The minimum acceptable DH key size has been increased to 2048 bits.
	CON-23245	The performance of connector has been improved, when sending events to Logger as a destination.
Syslog NG Daemon	CON-19056	Added tokens available for Syslog NG Daemon only. Some additional header information needed to be parsed and mapped to ESM fields.
	CON-14606	Syslog NG now supports events with multiple structure data (RFC5424).
Microsoft Azure Monitor Event Hub	CON-23134	Added support for: AzureFirewallApplicationRule and AzureFirewallNetworkRule
	CON-23465 .	PowerShell scripts are now signed in Azure Event Hub SmartConnectors. This allows users to run them in security-enabled environments with an execution policy set to either RemoteSigned or AllSigned.
	CON-23758	The new Powershell script removes all the old version files before upgrading.

Closed Issues

SmartConnector for	Number	Description
Microsoft DNS Trace Log Multiple Server File	CON-21642	The event stream stopped without displaying an error message.
Check Point Syslog	CON-22449	Additional data fields were not being mapped correctly.
	CON-22973	Some Checkpoint Firewall R80.10 Syslog events were not being parsed correctly. Fix: Updated R77 Common Security Event Mappings and R77 VPN-1 and FireWall-1 Event Mappings.
Rapid7 NeXpose XML File	CON-22852	A performance issue has been fixed.
ArcSight FlexConnector	CON-22781	JSON parsers were not providing additionaldata, unlike, other FlexConnectors. A new parameter was added to JSON parsers, so that users can enable the feature and auto tokenize all JSON nodes. **To apply the fix**. Include the line "autotokenize.enable=true" in the parser. **Caution**: Enabling this feature might affect the connector performance. . **Note**: If you define a token using a JSON node, but the token name and the node name are different, two tokens will be created.
	CON-22752	`Bro_ng_file_http` logs were not being parsed properly. Fix: Request URL information is now properly populated.
Amazon Web Services CloudWatch	CON-23040	Some route53 events were not being parsed correctly. Fix: The regex has been modified. **Note**: Due to a regex issue, values coming in as "-", are not supported.
	CON-23903	Updated the regex of cloudhsm.map and it now recognizes some CloudHSM Audit Log events.

SmartConnector for	Number	Description
Microsoft Windows Event Log Native	CON-23404	A password encryption issue was fixed by updating access parameters.
	CON-23626	Events were not getting forwarded to ESM.
	CON-23649	A warning message was displayed while installing the connector.
	CON-23652	Multiple Microsoft Windows Event Log – Native instances can now run on the same machine.
	CON-23862	From ArcMC 2.9.2 or later versions, the One-Click feature was failing when deploying the connector.
All SmartConnectors	CON-23494	When creating an HTTP connection object on a location different from jetty libraries, it was not calling the REST API service. Collectors (version 7.14.0) are now loading properly into ArMC.
	CON-23612	The connectors were not working in conapp mode.
	CON-23666	The installer screen of the UI was displaying unaligned text.
	CON-23750	The starting panel of Install Anywhere was displaying content that belonged to a different screen.
	CON-23809	TLS 1.0 and TLS 1.1 protocols have been disabled.
Amazon Web Services CloudTrail	CON-22199	Connector latency in 'processLog' and 'processSource'. The connector was consuming SQS messages very slowly with 1000 messages waiting in the SQS queue. Fix: The EPS has been increased, improving the performance of event parallel processing. The event time field has been mapped to the device recipient time field which were previously displaying the wrong date in the end time. Two new parameters have been added to `agent.properties`: "awsthreadcount": default value is 10. "awsfilterevent": default value is false. The requirement can now be customized but it is not recommended to increase the number of threads.
	CON-22890	Added support for Amazon Lambda.

SmartConnector for	Number	Description
Oracle Audit Vault DB	CON-23535	The wrong parser was being picked by the connector. For oracle audit vault version 12.2.x, the message "Database version [12.2.x] detected" is displayed now properly.
Malware Information Sharing Platform Model Import Connector	CON-23687	The port field was not mapped correctly.
	CON-23819	Added new parameter "Enforce Warning list".
	CON-23867	The port was not mapped correctly.
All SmartConnectors running on Solaris	CON-23589	SmartConnectors 7.11 and higher versions were not bundling Jre in Solaris platform. Steps to change the JRE: 1. Set `ARCSIGHT_DEV` environment variable to 0 export `ARCSIGHT_DEV=0.` 2. Set `JAVA_HOME` environment variable to the java path export `JAVA_HOME=<custom_java_path>`. 3. Set `JAVA_HOME` in the PATH environment variable without disturbing the existing PATH export `PATH=$JAVA_HOME/bin:$PATH`. 4. Start the `connector/agent`.

All IBM DB2 SmartConnectors	CON-23603	DB2 drivers are no longer provided in the connector installation due to licensing requirements. Later versions of DB2 drivers can be found here, but users require IBM login credentials.
		Also, IBM now requires a license jar to be added to the connector in order to connect to the database.
		Fix:
		To connect to an IBM DB2 database:
		1. Copy the following files from IBM DB installation location, for example,
		`C:\ProgramFiles\IBM\SQLLIB\java`
		`db2jcc4.jar`
		`db2jcc_license_cu.jar`
		2. Add them to the current\user\agent\lib directory of each connector that needs to connect to a DB2 instance.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to the ArcSight Security Open Data Platform (SODP) Support Matrix guide available on the Micro Focus Software Community page.

Hardware Requirements

- CPU: 2 CPU X 4 Cores each (2 x Intel E5620, quad core, 2.4 Ghz or better)
- RAM: 16 GB
- Disk: 60 GB
- Number of network interfaces—1 Dedicated Gig Ethernet interface

Note: To achieve better performance, use a server with higher system specifications.

Known Limitations

ArcMC Managed SmartConnectors

One-Click installation is failing on RHEL 8.1 and CentOS 8.1 through ArcMC 2.9.4.

Workaround:

Pre-requisites for instant connector/ collector deployment for 8.1 O:

- Python2
- Libselinux-python

Unlike Linux 6.x and 7.x, the prerequisites above are not integrated by default in Linux 8.x. If you are installing/ have installed ArcMC in a RHEL/CentOS 8.1 machine, perform the following steps. Also, apply these changes to the target Linux hot (the VM where the connector/ collector will be deployed):

1. Install python2:

   ```
   sudo yum install -y python2
   ```
2. Create a symlink:

   ```
   sudo ln -s /usr/bin/python2 /usr/bin/pythonPer
   ```
3. Install the `libselinux-python` package:

   ```
   sudo yum install -y libselinux-python
   ```

   Note: Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: `http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`

[CON-23909]

IBM Big Fix REST API

While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file:

`"E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties`". When the client properties file is auto populated incorrectly, the connector installation fails.

Workaround.

Manually set the correct path, which is: `$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties`

[CON-23907]

Malware Information Sharing Platform Model Import Connector

When running the MISP connector in FIPS mode, the following error is displayed on the console:

```
java.security.KeyManagementException: FIPS mode: only SunJSSE TrustManagers
may be used

at sun.security.ssl.SSLContextImpl.chooseTrustManager
(SSLContextImpl.java:120)

at sun.security.ssl.SSLContextImpl.engineInit(SSLContextImpl.java:83)

at javax.net.ssl.SSLContext.init(SSLContext.java:282)

at org.apache.http.conn.ssl.SSLContextBuilder.build
(SSLContextBuilder.java:164)

at org.apache.http.conn.ssl.SSLSocketFactory.<init>
(SSLSocketFactory.java:303)

at com.arcsight.agent.dm.f.b.q(b.java:581)

at com.arcsight.agent.dm.f.b.r(b.java:555)

at com.arcsight.agent.dm.f.b.d(b.java:173)

at com.arcsight.agent.Agent.a(Agent.java:674)

at com.arcsight.agent.Agent.a(Agent.java:1171)

at com.arcsight.agent.Agent.e(Agent.java:948)

at com.arcsight.agent.Agent.main(Agent.java:1960)
```

Workaround:

This message can be ignored. It does not affect the functionality.

[CON-23875

Microsoft Windows Event Log (WiSC)

WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. We have experienced the following issues:

• Issue #1: High CPU utilization on the monitored Windows host (log endpoint)

High CPU utilization has been detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average).

• Issue #2: WinRM inherent EPS limitations

Given the circumstances with WinRM, the event rate has a limit of around 140 EPS (sustained). Therefore, we do not recommend the use of the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates.

Workaround: To mitigate these issues, we recommend using the Windows Native Connector (WiNC) SmartConnector.

[CON-21601]

For more information, see the Technical Note on WinRM-related Issues.

Microsoft Azure Monitor Event Hub

The Azure Event Hub Debug Mode for function apps should not be enabled during normal operation, only for support purposes. Enabling it, may cause parsing and mapping errors.

Workaround:

To change this setting:

1. Go to the Azure portal < Function app < Configuration.

2. Set the "DebugMode" application value to False.

3. Restart the Function App.

[CON-22784]

After deploying the connector, events are duplicated or out of order

[CON-22809]

All Windows Event Log Connectors, both Native and Unified

If the connector cannot process events fast enough and the internal queue fills up, it might stop processing.

Workaround:

None at this time. You can re-configure the MQ parameters in agent.properties to prevent the queue from filling up.

[CON-19425]

All SmartConnectors

You might not be able to install your connector because of some missing packages.

Workaround:

Ensure that the following packages are installed:

1. yum install -y unzip

2. yum install -y fontconfig \ dejavu-sans-fonts

[CON-22085]

All SmartConnectors installed on Solaris

When upgrading SmartConnectors on Solaris, a timeout error is displayed. Follow the applicable workaround:

If the Solaris connector is already installed as a standalone, locally upgrade to 7.15.0.8295.0.

If the Solaris Connector is installed as a service:

1. Stop the service.

2. Go to HOME/current/bin and execute. /runagentsetup.

3. Uninstall the service in Global Parameters and exit the wizard.

4. Perform a local upgrade to 7.15.0.8295.0.

5. Install the Connector as a service and exit the wizard.

6. Start the service.

[CON-22080]

All SmartConnectors

Connector logs show Fatal Exception error: Unable to find requested property `'transport.cefkafka.extra.prod.props'`. This message does not impact the performance or the functionalities of the Connector.

If you are using a map file with an expression set in the `<connector_install_location>\current\user\agent\map location`, and the connector runs out of memory, add the following property to `agent.properties` as a workaround:
`parser.operation.result.cache.enabled=false`
If this problem happens with Windows Event Log Native, and if the above work-around does not completely solve the problem, reduce the value of the Native connector parameter 'eventprocessorthreadcount'. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:

```
agents[0].eventprocessorthreadcount=5 or agents
[0].eventprocessorthreadcount=1, etc..
```

where 0 is the index of the WiNC connector in the container. [CON-19234, CON-18977]

Upgrading to 7.15.0.8295.0.

Micro Focus provides a digital public key for you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:
https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do

Note: If a Parser Override was provided, determine whether the Bug or Feature Request number is included in the Fixed or Enhancements section. If the number is not listed, do not upgrade the Connector. You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your environment PROD (production)

To Apply this Release

Download the appropriate executable for your platform and the "SmartConnector Configuration Guides .Zip" file from the Support Web Site.

When downloading the documentation zip file, create a folder for documentation (such as `C:\ArcSight\Docs`) and unzip in that folder. Then double-click **`index.html`** in the **`agentdocinstall`** directory to access the individual configuration guides.

The 64-bit executable is available for download for Windows and Linux platforms. Only the 64-bit executable is available for Solaris platforms. Users should move to the Solaris 64-bit platform. There is no upgrade path from the Solaris 32-bit image to the Solaris 64-bit image.

All SmartConnectors are currently supported on 64-bit platforms other than those listed as exceptions in the "SmartConnectors with 64-Bit Support" document. This document is available on the Micro Focus Security Community as well as in the SmartConnector Configuration Guide zip file available for download from the Support Web Site.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

None at this time.

SmartConnector Support Recently Ended

Support Ended 11/22/2019

Solsoft Policy Server – Support ended due to lack of customer demand.

[CON-22478]

Support Ended 8/21/2019

Support ended for Oracle Audit DB v9 – end of support by vendor.

[CON-22834]

Support Ended 4/28/2018

Support ending for all 32-bit SmartConnectors – Use 64-bit SmartConnectors.

Support Ended 02/21/2018

Symantec Endpoint Protection DB – SEP version 11 support ended by vendor.

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 Release Notes (Smart Connectors 7.15.0.8295.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!