Micro Focus Security ArcSight Smart Connectors

Software Version: 8.0.0.8322

Release Notes

Document Release Date: July 31, 2020
Software Release Date: July 31, 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

These notes describe how to apply this latest release of ArcSight SmartConnectors, as well as provide other information about recent changes and open and closed issues.

A connector is an application that collects raw events from security devices, processes them into ArcSight security events, and transports them to destination consumers.

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 ArcSight ESM, ArcSight Logger, or other destinations. This further 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, 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 into a common schema (CEF format) for use by the log consumers, including ArcSight ESM, ArcSight Logger or 3rd party destinations.
- 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 the log consumers, 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 for various analytics, including: realtime correlation, UEBA, machine learning, search and hunt scenarios.

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.

Release Highlights

SmartConnector Updates

- **New SmartConnectors: AWS Security Hub and AWS S3**

  This SmartConnector 8.0.0.8322 release has significant improvements and new support for AWS native cloud services, including new SmartConnectors for AWS S3 and AWS Security Hub log sources. Refer to the Release Notes that describe these new features.

  - **AWS Security Hub SmartConnector** supports AWS GuardDuty event processing in ASFF format.

    AWS Security Hub consumes, aggregates, organizes, and prioritizes findings from AWS security services and from third-party product integrations. Security Hub processes these findings using a standard finding format called the AWS Security Finding Format (ASFF), which eliminates the need of time-consuming data conversion efforts. Then, it correlates the ingested findings across products to prioritize the most important ones.
  - **AWS S3 SmartConnector** supports Cisco Umbrella DNS log processing.
- **New Support for Un-obfuscated Parsers**

  The un-obfuscated parsers are now available on the installation media, bypassing the need to work with customer support to get access to these parser definitions.
- **Windows Native SmartConnector (WiNC) on a Gen9 Connector Hosting Appliance (CHA)**

  The Windows Native SmartConnector (WiNC) can now run in a Windows 2019 Server VM, hosted on Gen9 ArcMC Connector Hosting Appliance (CHA). As a result, certain low-to-medium EPS environments, are no longer required to build a separate WiNC-hosting Windows VM, which would need its own IP address, on a physical host or a hypervisor. For more information, see the SmartConnector Microsoft Windows Event Log Native on CHA guide.

Content Updates

- **Coronavirus Themed Cyber Threats**

  With coronavirus-themed cyber-attacks skyrocketing, we are facing one of the largest cybersecurity challenges of our time. Opportunistic cyber criminals are seeking to take advantage of the chaos, with targeted COVID-19 attacks.

  To stay on top of these cyber threats, ArcSight has released blog posts, realtime-correlation rules, dashboards, search and hunt queries, Threat Intel based packages and our partner SOC Prime's package.

- **ESM Default Content**

  ESM Default Content is a set of content packages that provide immediate value, especially to those organizations starting their Next-Gen SIEM journey with ArcSight. ESM Default Content consists of 2 packages:

  - Threat Intelligence Platform -based on the CRCL MISP Malware Information Sharing Platform (MISP) and Threat Sharing Platform
  - Security Threat Monitoring

- **Updates since ArcSight 2020.1 release in April 2020**

  Since ArcSight 2020.1, we have updated ESM Default Content, and the latest version is v2.3.

  For v2.2 and v2.3 releases, the following MITRE Ids have been added to ArcSight's MITRE ATT&CK coverage:

  T1003, T1012, T1034, T1036, T1045, T1056, T1060, T1063,T1068,T1076,T1077, T1078, T1083, T1085, T1086, T1088, T1089, T1090, T1093,T1105,T1112,T1113, T1118, T1132, T1193, T1201, T1490, T1503, T1518.

- **MITRE ATT&CK Landing Page Refresh**

  Micro Focus' official MITRE ATT&CK framework landing page has undergone an exhaustive refresh, both functionally and cosmetically. As a result, customers looking to start their MITRE ATT&CK journey can simply download the latest ArcSight ESM Default Content package, in order to have real-time correlation rules, search queries, dashboards and other content for their Next-Gen SOC requirements.

  They can also export the JSON file of ArcSight's coverage in multiple analytics domains, to do a self-assessment of their SOC maturity level, based on their preferred

MITRE ATT&CK navigator layers.

- **ArcSight Recon – New Content for this New Product in the ArcSight Family**

  ArcSight Recon is a brand-new product geared towards Search and Hunt in Big Data environments. For the July 2020 release of Recon 1.0 (based on Vertica), we have an identified tactical content, based on MITRE ATT&CK's framework. The dashboards and reports provide you with valuable resources to aid you and your enterprise in the hunt for undetected threats. This product will also help you recognize patterns and trends in the MITRE ATT&CK events. MITRE ATT&CK Overview dashboards and otherMITRE ATT&CK related reports are available.

- **ArcSight Logger MITRE ATT&CK Package**

  ArcSight Logger has seen a significant content boost in the ArcSight 2020.2 release, all based on MITRE ATT&CK. 100+ Logger Searches will let you hunt MITRE ATT&CK related activity. Some examples include:

  - Bitcoin Activity originated from AWS EC2 cloud instance
  - Find Invoke Mimikatz PowerShell activity JavaScript Code Executed through rundll32
  - Malicious Control Panel File Detected
  - Malicious PowerShell Cmdlets
  - Metasploit Detected

- **Beaconing Detection**

  Beaconing Detection will be available as a freely-downloadable package for ArcSight Logger on ArcSight Marketplace at the end of July 2020. This is a Big Data use case

that helps hunt down those repetitive processes which are likely to communicate to the outside world and probably ex filtrate a large, encrypted ZIP file or wait for the next command to perform in the enterprise, etc. It is challenging to guess the right "event name", or the periodicity/ frequency as they can easily change, for example, using a DNS based ex filtration with a Domain Generation Algorithm is considered dated. As modern red team tools like Cobalt Strike which uses repetitive techniques to perform stealthy C2 activities, or other 0-day attacks, the detection is considered to be only possible with Beaconing Detection algorithms.

What's New in this Release

- We added a new SmartConnector to support **NetApp ONTAP version 9.3 patch 8**.
- Added support for the latest releases of Micro Focus Security, Risk and Governance products. Refer to the Support Matrix of each product for applicability.
- Security updates have been implemented to LoadBalancer.
- SmartConnectors now support ZSTD compression, which generally performs better than GZIP, when communicating with Transformation Hub.
- A memory profile can be applied to a SmartConnectorto start it with tailored memory allocations consistent with the SmartConnector’s role in a Logger ecosystem.
- Component libraries include current vulnerability compliance, and ciphers are up-to-date.
- Improvements to the WINC SmartConnector to support MITRE IDs: T1003, T1012, T1034, T1036, T1045, T1056, T1060, T1063, T1068, T1076, T1077, T1078, T1083, T1085, T1086, T1088, T1089, T1090, T1093, T1105, T1112, T1113, T1118, T1132, T1193, T1201, T1490, T1503, T1518
- Platform component version updates have been certified on RHEL 7.8, CentOS 7.8 and current releases of Azul Zulu Java runtime. Component libraries include current vulnerability compliance, and ciphers are up-to-date.
- Miscellaneous bug fixes. Refer to the Release Notes for the specific defects addressed.

LoadBalancer

This release contains a new version of LoadBalancer, for more information see: Links

Integrated into this release

Parser update releases 7.15.1.8305.0 and 7.15.2.8312.0 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.

- 7.15.1.8305.0 Release Notes
- 7.15.2.8312.0 Release Notes

New SmartConnector

SmartConnector for	Number	New Device, Component, or OS Version
NetApp ONTAP	CON-20639	Added support to version 9.3 patch 8.
Amazon Web Services S3	CON-21093 CON-23986	The new Smart Connector collects and processes Cisco Open DNS Umbrella events.
Amazon Web Services Security Hub	CON-24213 CON-24219 CON-24055	The new SmartConnector processes Guard Duty Events through EventBridge.

New Device, Component, or OS Version Support

All SmartConnectors	CON-23902	The Logger Download-able Connector (On board connector) can now send events to Transformation Hub.
	CON-24045	This framework release includes event categorization updates up to the release of February R2 2020. Later AUP Packages can be downloaded from SSO and the support platform and will take Micro Focus SmartConnectors 8.0 precedence over them. For more information, see the ArcSight SmartConnector User Guide 8.0.0
	CON-24110	Red Hat Enterprise Linux (RHEL) 7.8 is now supported.
	CON-24111	CentOS 7.8 is now supported.
	CON-23495	Un-obfuscated parsers are now part of each Framework or Parser Release package.
	CON-24021	Some security vulnerabilities have addressed for this release.
	CON-23796	Added Microsoft Azure Monitor Even Hub as a new destination for ArcMC on-board connectors.
	CON-23497	Added support for ZStandard Connector and Collector.
Microsoft Windows Event Log Native (WINC) on CHA	CON-23341 CON-23475	When being installed in a Connector Host Appliance (CHA), the WINC connector can now run in a Windows 2019 Server VM on Gen9 CHAs. For more information, see the SmartConnector Microsoft Windows Event Log Native on CHA guide.

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
REST API FlexConnector	CON-20102	This connector now supports TLS extension Server Name Indication (SNI). For more information, see the FlexConnector REST Developer's guide.
Model Import Connector for MISP	CON-23239	The connector can now collect up to 12 month-old events. For more information, see the Model Import Connector for MISP guide.

Closed Issues

SmartConnector for	Number	Description
All SmartConnectors	CON-23376	Removed the CBC cipher suites below: TLS_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA Added the following ECDHE cipher: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	CON-24164	The output file name format in the destination type CEFfile changed from yyyy-MM-dd-HH-mm-ss.done.cef to yyyy-MM-dd-HH-mm-ss.SSS.done.cef. Similarly to CSV.
	CON-24162	The Yukon Territory of Canada timezone was not setting its clocks back, correctly. A hotfix to address Canada Yokon timezone update is now available for ArcSight products. Contact Customer Support to obtain the fix.
Amazon Web Services CloudWatch	CON-23036	The "severity" field was showing as "unknown" in Route53 events
	CON-23695	Updated the DNS Resolved field from "device Custom String 5" to "Source Address".
Cisco ASA Syslog	CON-18288	The "Set host name only (lowercase)" functionality was not being considered. This functionality belongs to destination specific settings.
Microsoft Azure Monitor Event Hub	CON-23481	Updated the permissions to deploy and configure the connector. For more information, see the SmartConnector for Microsoft Azure Monitor Event Hub guide.
	CON-24034	An Audit Log issue was fixed.
	CON-21979	Added event mappings for group/ roles.

SmartConnector for	Number	Description
Microsoft Windows Event Log Native	CON-18904 CON-22976	Several values in the Properties field of Event Id 4662 were not being parsed. For more information, see the SmartConnector for MS Windows Event Log - Native SmartConnector (WiNC) guide.
Model Import Connector	CON-23908	The threat level has been translated to human-readable medium.
Syslog NG Daemon	CON-24136	The connector currently supports TLS 1.2. TLSv1 and TLSv1.1 are no longer supported.

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

All SmartConnectors

The connector upgrade fails with ESM in FIPS 140 mode.

To upgrade the connector in Linux (Standalone / Service):

1. Edit the `bashrc` file command: `"vi ~/.bashrc"`
2. In that file, write export `JAVA_TOOL_OPTIONS=-Dorg.bouncycastle.rsa.allow_multi_use=true`
3. Save the changes and run `"source ~/.bashrc"`.
4. Proceed with upgrade.

To upgrade the connector in Windows Standalone Mode:

1. Open the command prompt and write `setx JAVA_TOOL_OPTIONS "-Dorg.bouncycastle.rsa.allow_multi_use=true"`
2. Proceed with upgrade as needed.

To upgrade the connector in Windows Service Mode:

- Go to `current/user/agent/agent.wrapper.conf` and add the line `"wrapper.java.additional.12=-Dorg.bouncycastle.rsa.allow_multi_use=true"`

or

- Open the command prompt and write `` `setx JAVA_TOOL_OPTIONS "-Dorg.bouncycastle.rsa.allow_multi_use=true"` ``

or

- Stop the connector in service mode and start it in standalone.

Proceed with the upgrade, ESM will upgrade the connector and start it in service mode.

[CON-24281]

IO Exception Length Tag

While connecting 7.15.0 SmartConnectors with the latest ESM in Default non-FIPS SSL mode, an IO exception length tag is displayed.

Workaround

From ESM, configure the connector in default mode along with Client Authentication (CA) and add the line `"ssl.keystore.type=JKS"` in `$ARCSIGHT_HOME/user/agent/agent.properties` along with the other configuration prerequisites.

[CON-24260]

MS Windows Event Log (WISC)

If you try to "Modify connector parameters", after completing the installation with the "Enter Manually" option selected, an error was displayed.

Workaround

None at this time.

[CON-20759]

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:

- 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/python
   ```
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 8.0.0.8322

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 01/14/2020

Windows Server 2008 R2 - end of support by vendor.

[CON-17404]

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.

Support Ended 01/31/2018

Solaris 10 Premier support - end of support by vendor. [CON-17404]

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 8.0.0.8322)

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!