Micro Focus Security ArcSight Connectors

Software Version: 8.0.1.8336.0

Micro Focus SmartConnector Release Notes

Document Release Date: August 20, 2020
Software Release Date: August 20, 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 list SmartConnectors for which parser changes have been made and describe how to apply this latest ArcSight SmartConnector parser release 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.

Supported SmartConnector Version

This parser update has been certified with SmartConnector Framework release 8.0.0.8322. Use of this update with earlier framework releases is not supported.

Obtain Parser Release AUP File

ArcSight Marketplace

The monthly ArcSight SmartConnector parser update releases are posted to the ArcSight Marketplace. ArcSight Marketplace is an app store that enables rapid provisioning of your ArcSight SIEM deployment with content updates and trusted security content packages.

An ArcSight Marketplace administrative account is required to download and install the monthly connector parser updates. Browse to the Marketplace at https://marketplace.microfocus.com/arcsight to set up your administrative account.

MICRO FOCUS SECURITY COMMNUNITY

The monthly ArcSight SmartConnector parser update releases are also posted on the Micro Focus Security Community.

What's New in this Release

SmartConnector 8.0.1.8336.0 includes the following capabilities:

New SmartConnector

None at this time.

New Device, Component, or OS Version Support

SmartConnector for	Number	New Device, Component, or OS Version
Cisco Secure ACS Syslog	CON-21801	Added support for some new events of CSCOacs_ Passed_Authentications version 5.8
McAfee ePolicy Orchestrator DB	CON-22659	Added support to MOVE with ePO 5.10.
Microsoft Windows Event Log Native	CON-23622	Added support for Windows Server 2019 events.
Bro IDS NG File	CON-24197	Added support to the following Zeek 3.1.3 modules: -Conn, Dns, files,Http, ssl, weird, and x509.Added mappings for Support for Ja3 and Hash MD5 Hashes.

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
Amazon Web Services S3	CON-24364	Added support for Cisco Umbrella (version 3 and 4) - DNS Logs.
Microsoft Windows Event Log Native	CON-22898	Added support for Microsoft Antimalware on the Microsoft Security Essential Suite.
	CON-24254	Added support for event Id 23 and Microsoft Sysmon version 11.
Symantec Endpoint Protection DB	CON-24313	Updated Agent Behavior event mappings, Alerts Mappings v14.2, and Alerts Mappings v14.x. to fix performance issue.

Closed Issues

SmartConnector for	Number	Description
All SmartConnectors	CON-22160	Some events were not being parsed correctly.
	CON-24400	Updated Sysmon event Id 3 mappings.
Arbor Networks Peakflow Syslog	CON-24322	Some events were not being parsed correctly.
Blue Coat Proxy SG Multiple Server File	CON-24288	Updated Blue Coat Proxy SG SSL event mappings.
Cisco ISE Syslog	CON-24342	Updated Radius Accounting event type.
Juniper JUNOS Syslog	CON-24320	Updated device severity and agent severity mapping files.
Linux Audit Syslog	CON-24327	Added support for Snoopy Logger.
Pulse Secure Pulse Connect Secure Syslog	CON-18017	Some events were being unparsed in version 8.2R3.1.
Fortinet Fortigate Syslog	CON-19241	Some events were not being parsed correctly.
Proofpoint Enterprise Protection and Enterprise Privacy Syslog	CON-19322	Some events were not being parsed correctly.
ISC BIND Syslog	CON-19484	Some events were being unparsed in version 9.5.
Cisco IronPort Web Security Appliance File Cisco IronPort Web Security Appliance Syslog	CON-19646	Cisco Ironport was showing "Incomplete event" in the message field.
Oracle WebLogic Server File	CON-19688	Added support for a new Timestamp.
IBM SiteProtector DB	CON-21510	Updated IBM Site Protector Mappings. Added new field: Old File Hash.
OVAL Vulnerability Scanner	CON-23518	Some SQL_bind were not being parsed with the CRUD statments in Oracle XML file.
Oracle Audit Syslog	CON-23942	Updated parser file to fix a token DBID parsing issue.
Cisco NX-OS Syslog	CON-23945	Some events were not being parsed.

SmartConnector for	Number	Description
Microsoft Windows Event Log Native	CON-23960	Added support for the Microsoft OAlerts.
	CON-23971	Updated mappings for event Id 800.
	CON-24062	Updated mappings for event Id 4673.
	CON-24142	Added support for AppLocker events on Windows 10.
	CON-24207	Added support for Client DNS events on Windows 10.
Juniper Network and Security Manager Syslog	CON-24244	Some events were not being parsed.
	CON-8960	
	CON-9298	
Bro IDS NG File	CON-24385	Added support for Bro/Zeek events.

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/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 8.0.0.8322.

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 8.0.0.8322.

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 8.0.1.8336.0

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 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 Micro Focus SmartConnector Release Notes (Connectors 8.0.1.8336.0)

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!