Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector Release Notes

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://www.microfocus.com/documentation/arcsight/

Contents

What's New

SmartConnector 8.2.0 Patch 1, Patch 2, Patch 3, 8.2.1, 8.2.2, and event categorization updates have been integrated into this framework release. For more information, see the corresponding release notes in the SmartConnector Documentation Website.

New SmartConnectors

SmartConnectors	Description
CyberRes Galaxy Threat Acceleration Program SmartConnector	The CyberRes Galaxy Threat Acceleration Program SmartConnector is a new generation MISP connector, which provides enhanced threat intelligence capabilities. The CyberRes Galaxy Threat Acceleration Program SmartConnector retrieves threat intelligence events and attribute data and uploads it to ESM Active Lists found under `/All Active Lists/ ArcSight Foundation/ Threat Intelligence Platform`. These entries include, IP addresses, domain names, emails, hash values, and URLs. The CyberRes Galaxy Threat Acceleration Program SmartConnector is available in the following variants: • **CyberRes Galaxy Threat Acceleration Program Plus:** This option is subscription based. After you have purchased the license, collect the API key license before you install the connector in this mode. The subscription is for a limited period, after which the license can be renewed. They can access premier content hosted on the GTAP server `threatfeed.cyberres.com` instance. • **CyberRes Galaxy Threat Acceleration Program Basic:** All customers with the ArcSight ESM license can use this version free of cost. They do not need any API key to access the content hosted on the GTAP server `threatfeed.cyberres.com` instance. • **Custom MISP Instance:** This option can be used if you already use a public or private instance of MISP server as per the need of the organization. This option does not require subscription. For more information, see Configuration Guide for CyberRes Galaxy Threat Acceleration Program SmartConnector.

Support for New Devices and Version Updates

Application Module	Description
All SmartConnectors	• Added support for Microsoft Windows Server 2022. • Upgraded Apache Log4j library version to 2.17.1.
All SmartConnectors	This framework release includes event categorization updates up to the release of Oct R1 2021. For more information about products currently supported, see the AUP Release Notes from SSO. ESM uses the latest version of Micro Focus SmartConnectors. Thus, the SmartConnectors 8.3.0 version takes precedence over other categorization packages.
All SmartConnectors and Load Balancer	• Upgraded Tomcat version to 9.0.54. • Upgraded Zulu OpenJDK to 8u312.
Amazon CloudWatch Connector	Added support for Python 3.8 in AWS Lambda.
Syslog Connectors	Added support for RHEL 8.4.

SmartConnector Enhancements

Application Module	Description
Amazon S3	• Amazon S3 now supports more than 100 log sources in addition with the existing log sources. For more information about the supported log sources by Amzon S3, see SmartConnectors for the Cloud. • The **CloudWatch Exported Logs** parameter is introduced. Set this parameter to **true**, if the logs are exported from CloudWatch to Amazon S3. The default value is **false**.
AWS Security Hub	• Added support for Amazon Inspector service. • Added support for AWS GovCloud region.

Application Module	Description

All SmartConnectors (configured with Amazon S3 Destination)	• The maximum limit for number of events that can be stored in each Avro file is now increased to 50,000.
	• Until 8.2.0 Patch1 release, connector had higher local storage requirement.
	Following changes are made to the storage requirement from the Patch 2 release:
	◦ Earlier, files that were successfully uploaded to Amazon S3 bucket were retained locally for 5 days, by default. From this release, the files that are successfully uploaded to Amazon S3 will not be retained locally, by default. To retain files, set the value for the following property in minutes in the **agent.properties** file:
	`transport.avroawss3.file.s3done.retention.minutes=0`
	If you set the retention period to higher than zero, then you must define the cleanup frequency in the following property:
	`transport.avroawss3.s3donefile.cleanup.interval.minutes=1`
	The retained files are cleared periodically as per the value specified for this property.
	◦ If a connector is unable to send the output to Amazon S3, for any reason, such files are cached locally for 6 hours, by default. To modify the default value, specify a different value in minutes for the following property in the **agent.properties** file:
	`transport.avroawss3.file.done.retention.minutes=360`
	To periodically clear the cache, specify a value in minutes for the following property:
	`transport.avroawss3.donefile.cleanup.interval.minutes=60`

Okta Connector	The **Grant Type** parameter is introduced to enable the Okta connector to support the password grant method. The **Grant Type** parameter options include: **Authorization Code** and **Password**. The default value is **Authorization Code**.
ArcSight FlexConnector for REST	• The **Grant Type** parameter is introduced to support different mechanisms that the application must use to get Access Tokens. The **Grant Type** parameter options include: **Authorization Code**, **Password**, and **Client Credentials**. The default value is **Authorization Code**. • Added the **fetcheventsonstartup** parameter in the `agent.properties` file. The default value for **fetcheventsonstartup** is **false**. When you set this value to **true**, the connector starts fetching events immediately after it starts, instead of waiting for the **queryfrequency** interval to fetch the events. For information about modifying the parameters, see Developer's Guide to FlexConnector for REST.

Application Module	Description
ArcSight FlexConnector for Kafka	Added support for the **AVRO** content type, for Security events getting ingested into the Connector. It is mandatory to specify a JSON configuration file name, if the **Content Type** parameter is selected as **AVRO** . Added a new parameter - **Avro Schema**, to provide a schema file path with an extension (such as `/opt/TestSchema.avsc`). This parameter is applicable only for the **Avro** content type.
Implementing ArcSight Common Event Format (CEF) - Version 26	Introduced 1.2 version of CEF specification for producers and consumers. For more information, see Implementing ArcSight Common Event Format (CEF) - Version 26 document.
• Sybase Adaptive Server Enterprise DB • ArcSight FlexConnector	Added password encryption support for Sybase 16.0 database. For information about the **Password Encryption Enabled** parameter, see Configuration Guide for Sybase Adaptive Server Enterprise DB.

Software Fixes

The following issues are fixed in the 8.3.0 release:

Application Modules	Description
All SmartConnectors	The Amazon S3 bucket owner was unable to read the events in Avro format, because the connector was configured with a user from an AWS account other than the owner of the Amazon S3 bucket. The Amazon S3 bucket has been now configured with the appropriate Access Control List (ACL).
All SmartConnectors	The `./arcsight agent tempca -i` command was failing with the following exception: `NullPointerException: arcsight agent tempca -i`
All SmartConnectors	The Syslog connectors configured with Amazon S3 destination had performance issue at higher EPS. Now, the performance of Syslog connectors configured with Amazon S3 destination has been improved.
All SmartConnectors	When configuring a connector with more than one destination of the same type, the silent installation of a connector was not running as expected, because the destination names were not matching. Now, the destination names are appearing correctly, and therefore the silent installation of a connector is running fine.
All SmartConnectors	Security vulnerability fixes.

Application Modules	Description
• ArcSight FlexConnector REST • ArcSight Common Event Format REST	The installation and upgrade of the ArcSight FlexConnector REST and ArcSight Common Event Format REST connectors fail with the following error: `Fatal Error: Parameter state is not registered. Agent has not been correctly initialized` The **state** parameter has been registered now.
Collector	Collector stopped working and started displaying a "Fatal Exception" when an invalid encoding value was provided. The **Encoding** property is now a drop-down menu that contains the following values supported by Transformation Hub (TH): **UTF-8** and **US-ASCII**. The default value is **UTF-8**. The **UTF-8** and **US-ASCII** encoding values are supported. If you provide an invalid encoding value, then the default value **UTF-8** is considered. You can check the error message that is displayed in **collector.log**. Example: `[2021-09-07 04:03:04,340][ERROR] [com.arcsight.collector.loadable.collector._SyslogDCollector] [initCharacterEncoding]Inside catch block Unable to recognize [UTF18], as a supported character set. Will use the default [UTF8] instead, please double check the property [encoding]`
Microsoft DHCP File	The Microsoft DHCP File connector was not detected automatically, when connection to remote file was restored after interruption. You must restart the connector after you complete the configuration, so that the connector can start processing events.
Model Import Connector for MISP (Open Source Threat Intelligence and Sharing Platform Solution)	In ArcSight Console, the **indicatorType** column was being displayed as **suspicious** for all indicators. This was happening because, in the latest version of MISP MIC, extra fields were getting added in tags. The additional fields are now handled in the tags. All the **indicatorTypes** values are appropriately populated now.
Model Import Connector for MISP (Open Source Threat Intelligence and Sharing Platform Solution)	MISP Connector was unable to start in FIPS Mode with Client Authentication.
Oracle Audit DB	When the connector failed to change the Oracle database password, the old and new passwords appeared in clear text. Now, the passwords are not visible.
Syslog NG Daemon Connector/Collector	The **TLS** protocol option was not appearing for the Syslog NG Daemon Connector and Collector, if the **UDP** or **Raw TCP** protocol option was selected in ArcMC.

Installing SmartConnectors

For information about installing SmartConnector, see the Installing SmartConnectors section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to Technical Requirements for SmartConnectors.

Downloading the SmartConnector 8.3.0 Installation Packages

You can download the SmartConnector installation packages for your platform from the Software Licenses and Downloads (SLD). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

File Name	Description
Arcsight-8.3.0.xxxx.0-aup_extractor.zip	The tool used to upgrade the parser updates for Cloud.
ArcSight-8.3.0.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.3.0.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight-8.3.0.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.3.0.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.3.0.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.3.0.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.3.0.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.3.0.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.

ArcSight-8.3.0.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.3.0.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for CyberRes Galaxy Threat Acceleration Program SmartConnector support for Linux.
ArcSight-8.3.0.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for CyberRes Galaxy Threat Acceleration Program SmartConnector support for Windows.
ArcSight-8.3.0.xxxx.0-MispModelConnector-Linux64.bin	This is the installer file for MISP Connector support for Linux.
ArcSight-8.3.0.xxxx.0-MispModelConnector-Win64.exe	This is the installer file for MISP Connector support for Windows.
ArcSight-AWS-CloudWatch-Connector-8.3.0.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.3.0.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.3.0.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.3.0.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSight_WiNC_Hosting_Appliance.8.3.0.xxxx.0.tgz	This contains the deployment scripts and dependencies required for hosting WiNC on connector hosting appliance (CHA).
ArcSight-ConnectorUnobfuscatedParsers-8.3.0.xxxx.0.zip	This contains unobfuscated parser files for various devices.

Upgrading to 8.3.0

Important: If you use any of the SmartConnectors listed in the Software Fixes section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

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.

For information and instructions, see Verifying Micro Focus Signatures with gpg or rpm.

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)

Upgrading SmartConnector to 8.3.0

You can upgrade a SmartConnector to implement the newly implemented features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see Upgrading SmartConnectors.

Upgrading Load Balancer to 8.3.0

Perform the following steps to upgrade to Load Balancer 8.3.0:

1. Download Load Balancer 8.3.0 from the Support website.
2. Stop Load Balancer. If running in High Availability (HA) mode, stop Load Balancer on both hosts.

   Note: Micro Focus does not support running mismatched versions of Load Balancer during the upgrade.
3. Install Load Balancer 8.3.0 in the same directory where you had the previous version installed. It will create a new directory for the current version.
4. Run the following command in the installation directory to move configuration and batch files to 8.3.0:
   - **For 8.1.0 users**: `cp -a 8.1.0/user current`
   - **For 8.2.0 users**: `cp -a 8.2.0/user current`
5. If Load Balancer is running in HA mode, repeat the installation steps on the other host.
6. Start Load Balancer. If running in HA mode, start the primary instance first.

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.

Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:

Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command: `cd Xxxxx/lib/agent`
3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
6. Run the following command: `cd Xxxxx/lib/agent/axis`
7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Open the `Xxxxx\lib\agent` folder.
3. Search for **log4j** and delete all the entries.

4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.
5. Search for **log4j** and delete all the entries.
6. Open the `Xxxxx\lib\agent\axis` folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm-rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
All SmartConnector	**Unable to Add Two Transformation Hub Destinations with Different Configurations** While configuring multiple destinations, you cannot add two Transformation Hub destinations with different configurations and content types such as Avro and CEF. This is a known limitation of SmartConnectors. **Workaround:** None.

	SmartConnector or Collector remote connections fail due to low entropy
	All SmartConnectors or Collectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector or Collector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.
	Workaround:
	To ensure that the entropy value is at the desired level:
	1. Install the `rng-tools` package:
	`sudo yum install -y rng-tools`
	2. Add the following line to the `/etc/sysconfig/rngd` file:
	`EXTRAOPTIONS="-r /dev/urandom"`
	3. Check the entropy availability in the system:
	`cat /proc/sys/kernel/random/entropy_avail`
	4. Start the `rngd` package as root user:
	`service rngd start`
	5. Enable the `rngd` service to start at the system start-up:
	`systemctl enable rngd.service`
	`systemctl start rngd.service`
	6. Ensure that the `rngd` package is always running (even after a reboot) as `root` user:
	`chkconfig --level 345 rngd on`
	7. Check the entropy availability in the system, after starting the `rngd` service:
	`cat /proc/sys/kernel/random/entropy_avail`

	Unable 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

All SmartConnectors installed on Solaris	**When upgrading SmartConnectors on Solaris, a timeout error is displayed.** **Workaround**: • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: a. Stop the service. b. Go to `HOME/current/bin` and execute `./runagentsetup`. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	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 functionality of the Connector. **Workaround:** 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 the above workaround does not completely solve the problem, reduce the value of the **eventprocessorthreadcount** Native connector parameter. 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.

All File SmartConnectors	**When adding a log into a log file using the vi text editor, events are not sent to ESM**
	Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.
	Workaround:
	Use the cat command to append data:
	`Syntax:`
	`cat >> log_file_name [ Enter ]`
	`"your logs"`
	`ctlr+c`

CyberRes Galaxy Threat Acceleration Program SmartConnector	**Possibility of Time Difference While Comparing ESM Lists Against Events from the MISP Instance** While comparing the `firstDetectTime` and `lastDetectTime` of ESM Threat Intelligence Platform lists against the event and attribute dates from the MISP Instance, you might notice time difference. This is because of the difference in timezone where the MISP Instance is hosted. **Workaround:** None.

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.

Google Cloud SmartConnector	**The Google SmartConnector cannot authenticate tokens with Google API** The following error is displayed when the connector is used from ArcMc with the One-Click feature: `{ “error” : “invalid_grant”, “error_description” : "Invalid JWT: Token mustbe a short-lived token (60 minutes) and in a reasonable timeframe. Check youriat and exp values in the JWT claim." }` **Workaround:** The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.

ArcMC Managed SmartConnectors	**SmartConnectors cannot be bulk-upgraded on a Linux server** **Workaround:** Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the `rng-tools` on the corresponding Linux OS. **Note**: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server. To install and configure the `rng-tools` package after a fresh install, follow the steps mentioned for SmartConnector or Collector remote connections fail due to low entropy.

	One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4
	This issue might occur in other ArcMC versions.
	Workaround:
	Pre-requisites for instant connector or collector deployment:
	• Python2
	• Libselinux-python
	Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.
	To manually install Python:
	Apply these changes to the target Linux host (the VM where the connector or collector will be deployed):
	1. Install python2 by the following command:
	`sudo yum install -y python2`
	2. Create a symlink by the following command:
	`sudo ln -s /usr/bin/python2 /usr/bin/python`
	3. Install the `libselinux-python` package by the following command:
	`sudo yum install -y libselinux-python`
	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`

IBM Big Fix REST API	**Connector installation fails when the client properties file is auto populated incorrectly** 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:** Set the following path manually: `$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties`
Microsoft Windows Event Log (WiSC)	**WiSC SmartConnector issues** WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. it has the following issues: • Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is 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 WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. **Workaround**: To mitigate these issues, use the Windows Native Connector (WiNC) SmartConnector. For more information, see the Technical Note on WinRM-related Issues.

Microsoft Azure Monitor Event Hub	**Azure Event Hub debug mode issue** Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors. **Workaround**: To configure the debug mode: 1. Go to **Azure portal** > **Function app** > **Configuration**. 2. Set the **DebugMode** application value to **False**. 3. Restart the Function App.
Microsoft Windows Event Log Native Connector	**Connector is unable to process events if the internal queue fills up** 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.

Load Balancer	**Load Balancer `arc_connlb` service does not start and displays an error message**
	
	When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer `arc_connlb` service does not start and displays an error message in the `lb.out.wrapper.log` even after you start the `arc_connlb` service manually.
	
	Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop. Perform the following steps to fix this issue:
	
	1. After you install Load Balancer as a service, before you upgrade, stop the `arc_connlb` service by using the following command:
	
	`# /etc/init.d/arc_connlb stop`
	
	or
	
	`service arc_connlb stop`
	
	2. After Load Balancer is successfully upgraded, start the `arc_connlb` service by using the following command:
	
	`# /etc/init.d/arc_connlb start`
	
	or
	
	`service arc_connlb start`

Connector End-of-Life Notices

SmartConnector Support Ending

Connector	End of Support Date	Reason
Model Import Connector for MISP (Malware Information Sharing Platform)	2023	The MISP Connector will be deprecated for the ArcSight 23.1 release, the first release of 2023. Customers using MISP today are strongly advised to migrate to the Galaxy Threat Acceleration Program (GTAP), which includes support for MISP and premium intelligence feeds. For more information, see the Configuration Guide for CyberRes Galaxy Threat Acceleration Program SmartConnector.

SmartConnector Support Recently Ended

SmartConnector	End of Support Date	Reason
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/14/2020	End of support by vendor.
Windows Server 2008 R2	01/14/2020	End of support by vendor.
Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/22/2019	Lack of customer demand.
Oracle Audit DB version 9	8/21/2019	End of support by vendor.

All 32-bit SmartConnectors	4/28/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/21/2018	End of support by vendor.
Solaris 10 Premier support	01/31/2018	End of support 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 SmartConnector Release Notes (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!