Micro Focus Security ArcSight Connectors

Software Version: 8.2.0

SmartConnector Release Notes

Document Release Date: May 2021
Software Release Date: May 2021

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Overview

SmartConnector

The SmartConnector (also known as 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 standard format. Also, they normalize the data structure into a standard schema. Connectors can filter and aggregate 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 significant 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 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 (Avro, CSV, and CEF format) for log consumers, including ArcSight ESM, ArcSight Logger, Transformation Hub, Amazon S3, 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 number of events sent to the log consumers, increasing ArcSight's efficiency, and reducing event processing time (optional).
- Categorize events using a standard, human-readable format. Save time and make it easier to use those event categories to build filters, rules, reports, and data monitors for various analytics, including real-time correlation, UEBA, machine learning, search and hunt scenarios.

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

Load Balancer

ArcSight SmartConnector Load Balancer provides a “connector-smart” load balancing mechanism by monitoring the status and load of SmartConnectors. Currently, it supports two types of event sources and SmartConnectors. One distributes the syslog input stream to syslog connectors using TLS, TCP, or UDP protocol and the other downloads files from a remote server and distributes them to the file-based connectors. Note that the TLS protocol is supported for the SmartConnector for Syslog NG Daemon only.

Load Balancer ensures efficiency by distributing the load to a pool of SmartConnectors. Load Balancer supports high availability configuration with active and standby nodes. It distributes the events received to one or more SmartConnectors predefined in the SmartConnector pool.

Load Balancer is aware of the following information for SmartConnectors defined as the SmartConnector pool:

- **Availability (up or down)** - Load Balancer monitors SmartConnectors for availability. Events are not forwarded to a SmartConnector if it is not running (down). Instead, events are forwarded to the next available SmartConnector in the pool per the defined load-balancing algorithm rules.
- **SmartConnector Load** - CPU usage, memory usage, and queue drop rate for events.

For more information about downloading, installing and configuring the Security ArcSight SmartConnector Load Balancer application for use with event collection for ArcSight products, refer to Configuration Guide for ArcSight SmartConnector.

Release Highlights

SmartConnector Updates

- **SmartConnector for Google Cloud**
  - Added support for Google's IAM and Publish/Subscribe log sources.
  - It enables certificate-based zero-trust connections between On-Premise and Google Cloud Platform (GCP).
- **Microsoft Azure Monitor Event Hub**

  The new Microsoft 365 Defender (M365D) SmartConnector supports aggregated Azure log sources.
- **AWS Cloud SmartConnectors**

  The AWS Cloud Front service is now supported in the Amazon Web Services S3 SmartConnector.

Documentation Improvements

- Much of the documentation has been moved online, in HTML format, and supplemented by PDFs. Remaining documentation will be moved online in future releases. The new online documentation is available here: ArcSight SmartConnectors Documentation.
- Online documentation can be searched for relevant materials (Event IDs, etc.) and all related topics are presented in a selection list for drill-in.
- All Windows and related Connectors have been consolidated into a single guide (WiNC, PowerShell, Sysmon, etc.)
- Cloud connector documentation (AWS, Azure, and GCP) has been improved to simplify and clarify connector configuration and deployment.

Detect Zero-Day Attacks

New Polyverse Zerotect FlexConnector now supports Polyverse's industry-leading polymorphic and Zero-Day detection capabilities.

- https://marketplace.microfocus.com/arcsight/content/zerotect
- https://marketplace.microfocus.com/arcsight/category/partner-integrations
- Zerotect now certified on Micro Focus ArcSight (polyverse.com)

Significant Performance and Stability Improvements

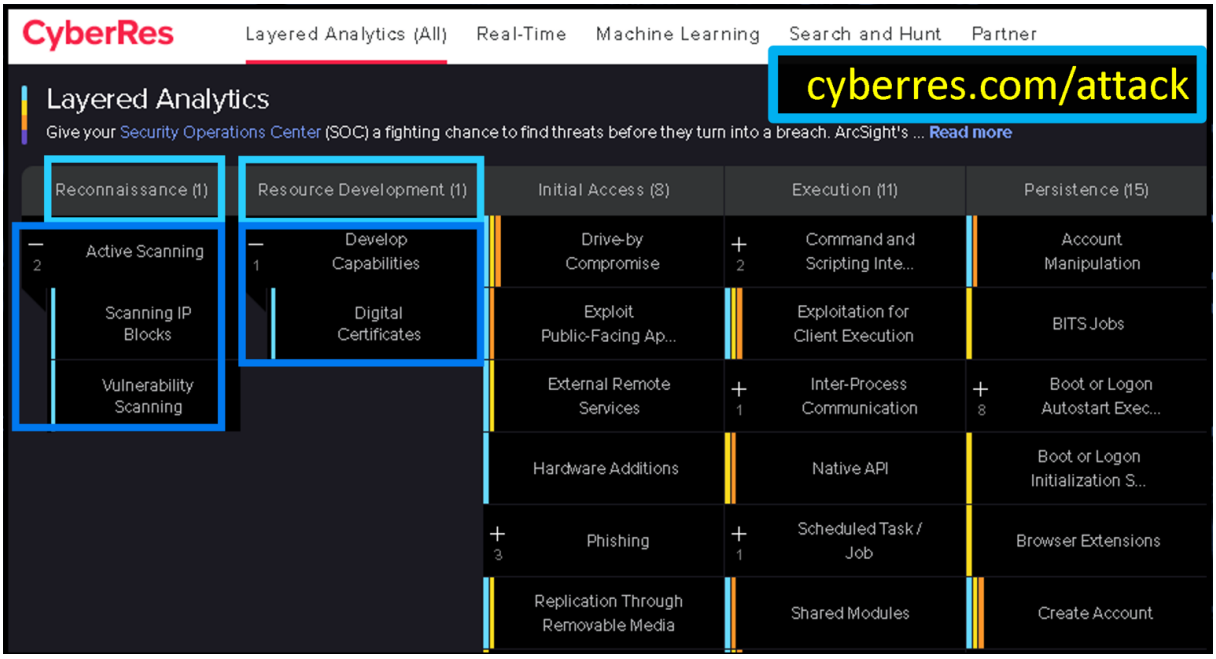
- Windows Native Connector (WiNC) performance has been improved 20% on a Gen10 CHA.
- Stability improvements to the ActiveMQ were addressed and now will dynamically adjust cache space sizes based on activity.
- Leader ACK(ON) performance when communicating with Transformation Hub now performs nearly equivalent to when ACK (OFF) is specified.

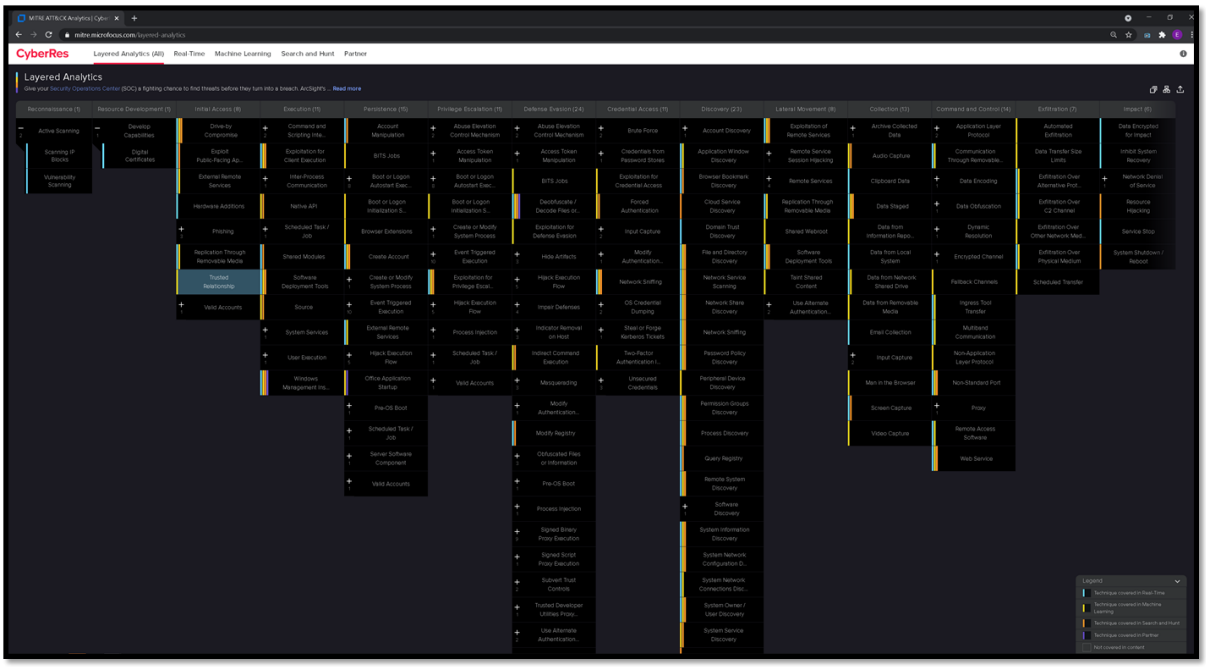
Content and Parser Improvements

Over 60 data sources with new signatures and categorizations, supporting popular devices from Cisco, Microsoft, Carbon Black, etc.

See the Categorizer AUP documentation for specific version support:

- New Tactics and Techniques
  - New ATT&CK tactics: Reconnaissance and Resource Development
  - New ATT&CK techniques: (Example: IP scanning blocks, etc.)
- New Best Practices guide: Kick-Start Your MITRE ATT&CK Journey with ArcSight
- New CyberRes MITRE ATT&CK Landing Page - cyberres.com/attack





- ArcSight Compliance Packs are getting refreshed in a phased approach, with each ArcSight release.
- Going forward, ArcSight Compliance Packs will apply to the entire ArcSight portfolio, represented by a single SKU.
- With this 2021.1 release, a brand-new package has also been developed.

  ArcSight Compliance Pack for GDPR(*) : A set of reports, dashboards and search & hunt queries focused on helping organizations in their GDPR compliance journey.
- PCI and IT Governance Compliance Insight Packs for Logger and ESM have been merged into the new/single packaging format, with no significant changes in their content. New content has been added for ArcSight Recon -ArcSight's Search and Hunt solution-.
  - **ArcSight Compliance Pack for PCI**
  - **ArcSight Compliance Pack for IT Governance**
- Micro Focus has released a dedicated package to help ArcSight customers and their incident response teams identify, remediate, and defend against attacks associated with the HAFNIUM-inspired global cyber attacks. See, HAFNIUM Targeting Microsoft Exchange Servers.
- Note that, this is content above and beyond the Zero-Day real-time coverage already provided by our Threat Intelligence Platform default content, which requires a one-time setup of our out-of-the-box MISP CIRCL Model Import Connector. For more details on how to implement this connector, please see the following whitepaper and video:
  - How To: Using MISP threat intelligence with ArcSight ESM
  - Video: Using MISP Threat Intelligence with ArcSight ESM

- ESM Default Content (*) v3.3 has been released, providing the following enhancements and fixes:

  ESM Default Content has been kept up-to-date with the latest MITRE ATT&CK matrix developments, by adding initial support for the 2x brand-new ATT&CK tactics: “Reconnaissance” and “Resource Development”.

  - T1595: Active Scanning
    - T1595.001: Scanning IP Blocks
    - T1595.002: Vulnerability Scanning
  - T1587: Develop Capabilities
    - T1587.003: Digital Certificates

(*) General Data Protection Regulation (GDPR) 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

Important: ESM Default Content is a constantly-updated package that is included as part of latest ArcSight ESM release. As this content may be updated more frequently than the ArcSight platform release cycle, a copy of that content is also provided here. This also helps our customers who may be on previous release of ArcSight ESM. This content is tested and certified to work with ArcSight ESM 6.9.1c or later versions.

What's New in this Release

SmartConnector

SmartConnector 8.2.0 includes the following capabilities:

- Support for Micro Focus SaaS - Recon

  SmartConnectors now support data integrity features required by Recon.

  It enables certificate-based zero-trust connections between On-Prem and AWS cloud.

  SmartConnector produced hash, which is calculated based on raw event data, now allows not to create a hash at every event level, but only at an aggregate level of 100 events (and so on). Note that the count 100 is also configurable for aggregation of number of events.

  The hash value is inserted into the Unified Data Store (UDS) to ensure that the event records are not tampered with post-insertion into the UDS.

  > **Note:** It is mandatory to specify a Unique Generator ID for the connector. If a value is not specified, events will not be processed for any destinations in certain configurations, such as **Amazon S3** as one of the destinations or the **Check Event Integrity Method** parameter is selected as **Recon** for any destination.

- Platform Currency and Security Updates

  Platform component version updates have been certified on RHEL 7.9 and 8.3, and CentOS 7.9 and 8.3 with the current releases of Azul Zulu Java runtime, Tomcat and the Confluent platform.

  Component libraries include current vulnerability compliance, ciphers are up-to-date. Static cipher suites have been removed.

- Connector Groups

  SmartConnectors can now be configured with a connector group name, enabling logical grouping of Connectors in ArcMC. This logical grouping is useful to customers to view and manage multiple connectors servicing a log source.

- Added support for the latest releases of Micro Focus Security, Risk and Governance products. Refer to the Support Matrix of each product for applicability.
- Miscellaneous bug fixes. Refer to the Release Notes for the specific defects addressed.

Load Balancer

Load Balancer 8.2.0 includes the following capabilities:

- Added support for Red Hat Enterprise Linux (RHEL) 7.9 and 8.3 as the Load Balancer installation platforms.
- Added support for CentOS Linux 7.9 and 8.3 as the Load Balancer installation platforms.
- Java Runtime Environment is upgraded to version 8U282.
- Security vulnerability fixes.

New SmartConnectors

SmartConnector for	Number	New Device, Component, or OS Version
Google Cloud	CON-25356 CON-25342	Added support for Google Cloud. Added support to the following events: • Pub/Sub • IAM In addition, this connector can process all other log sources with the generic parsing mechanism.
Microsoft 365 Defender	CON-25241	The new Microsoft 365 Defender (M365D) SmartConnector supports following Azure log sources: • Endpoints with Microsoft Defender for Endpoint • Email and collaboration with Microsoft Defender for Office 365 • Identities with Microsoft Defender for Identity and Azure AD Identity Protection • Applications with Microsoft Cloud App security
Trend Micro Apex Central Multiple DB	CON-25113	Added support for Trend Micro Apex Central Multiple DB Connector. The following Trend Micro Apex Central products are supported: • OfficeScan Client/Server Edition • InterScan Messaging Security Suite • ScanMail for Lotus Domino

New Device, Component, or OS Version Support

SmartConnector for	Number	New Device, Component, or OS Version
All SmartConnectors	CON-25259	Added support for RHEL/CentOS 7.9.
	CON-25385	Added support for RHEL/CentOS 8.3.
	CON-25608	This framework release includes event categorization updates up to the release of Feb R2 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 8.2.0 version takes precedence over other categorization packages.
Amazon Web Services S3	CON-23455	Added support for CloudFront Access Logs.
Microsoft Azure Event Hubs	CON-25340	Migrated Powershell scripts to Az cmdlets.
Microsoft Windows Event Log Native	CON-25063	Added support for ADFS Admin 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-25296	Removed the static cipher suits (TLS_RSA_WITH_AES_128_GCM_SHA256) from the connector code base.
	CON-25629	Removed support for TLS 1.0 and 1.1.
Box Connector	CON-25108	Removed NSS libraries, as FIPS is now being supported by BouncyCastle.
FlexConnectors		
McAfee ePolicy Orchestrator DB	CON-25702	WITH(NOLOCK) has been implemented for all the queries available for McAfee ePolicy Orchestrator DB connectors.

Closed Issues

SmartConnector

SmartConnector for	Number	Description
All SmartConnectors	CON-24613	Some events were not being parsed.
	CON-24994	Some security vulnerabilities were addressed in this release.
	CON-24945	
	CON-25223	1. The connector could not retrieve more than 1999 events in one single execution. This issue has been fixed. 2. When the events do not reach MessageTrace API event retrieval time interval, there is a new 24-hour window to retrieve the events that were not retrieved from the API.
	CON-25496	Upgraded zulu openjdk to 8u282.
	CON-25478	The **startTime** and **endTime** fields were being populated with deviceReceiptTime value if the source log or event data was left blank.
	CON-25549	While integrating Azure Sentinel alerts, a certificate error was displayed. **Fix**: Updated the troubleshooting section with the steps on how to enable SNI.
Apache HTTP Server Error File	CON-25472	Some events were not being parsed correctly.
Box	CON-23409	A refresh token was being rejected by the Box site because of the date time format. This issue has been fixed.
Actor Model Import Connector for Microsoft Active Directory	CON-24920	A time stamp error was being displayed in groups with "/" . This issue has been fixed.
	CON-25335	Removed other destination types except for ArcSight ESM from our Actor and Asset MIC SmartConnectors.
Microsoft DHCP File	CON-22058	The connector was throwing exceptions when the file was being rotated. The issue has been fixed.

SmartConnector for	Number	Description
Microsoft Windows Event Log Native	CON-25626	Added "Status" mappings for event 4625.
	CON-25627	Added "ObjectType" mappings for event 5145.
	CON-25290	Some events from the security channel were not parsing correctly. This issue has been fixed.
	CON-25647	The MQ persist storage space was running out of space, and the connector was not able to process events. This issue has been fixed.
Nortel Contivity Switch (VPN) Syslog	CON-25400	Some events were not being parsed correctly.
UNIX OS Syslog	CON-25422	Some events were not being parsed correctly.
Rapid7 NeXpose XML File	CON-25429	Event deserialization was failing whenever the connector tried sending large events to ESM, and the following error was displayed: "Error while parsing event (...) java.lang.IndexOutOfBoundsException" This issue has been fixed.

SmartConnector for	Number	Description
Rest FlexConnector	CON-25675	The Salesforce API might not be able to receive events, and instead, the following error is displayed: `[2021-03-06 10:36:22,507][FATAL] [com.arcsight.agent.loadable.agent._ FlexRestApiAgent] [refreshCredentials]There is no refresh token. Cannot refresh the access token. Please reconfigure the connector to have the user authenticated again.` The property `scope=full refresh_token` must be added. To add the property `scope=full refresh_token`: 1. From the **agent.properties** file, go to `agents [0].reauthenticate_onstartup=false`. 2. Change the property to **true**.
	CON-22491	REST FlexConnector stores the last time stamp before sending it to the destination flow, and when the connector gets restarted during the process of storing and sending the last time stamp, it results in the loss of events. **Fix**: The implementation has been changed for storing the time stamp after sending it to the destination. This prevents loss of events when you restart the connector.
FlexConnectors	CON-25041	The flexagent wizard was not mapping address type fields. This issue has been fixed.

Load Balancer

Key	Description
CONLB-513	Need to remove the **TLS_RSA_WITH_AES_128_GCM_SHA256** static cipher suite from the Load Balancer code base. **Fix**: The **TLS_RSA_WITH_AES_128_GCM_SHA256** static cipher suite has been removed as the default value for the **ssl.cipher.suites** parameter now. If you want to use ciphers other than those present in the code base, then specify the value for the **ssl.cipher.suites** parameter under global configuration in the **lbConfig.xml** file.

Integrated into this Release

Parser update releases 8.1.1.8412.0, 8.1.2.8416.0, and 8.1.3.8422.0 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.

- 8.1.1.8412.0 Release Notes
- 8.1.2.8416.0 Release Notes
- 8.1.3.8422.0 Release Notes

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to Technical Requirements for SmartConnectors 8.2.0.

SmartConnector Requirements

- SmartConnector 7.12.X or later
- SmartConnector for Syslog NG Daemon and file-based SmartConnectors

Software or Platform Requirements

- Supported: Red Hat Enterprise Linux (RHEL) 6.8, 6.9, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, and 8.3 (64-bit only)
- Certified: Red Hat Enterprise Linux (RHEL) 7.7, 7.9 , 8.1, 8.2, and 8.3 (64-bit only)
- Supported: CentOS Linux 6.8, 6.9, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, and 8.3 (64-bit only)
- Certified: CentOS Linux 7.6, 7.7 , 7.9, 8.1 ,8.2, and 8.3 (64-bit only)

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.

Downloading SmartConnector 8.2.0

SmartConnector

Download the appropriate executable for your platform and the **SmartConnector Configuration Guides .Zip** file from the Support website.

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 available on the Micro Focus Security Community and in the *SmartConnector Configuration Guide zip* file available for download from the Support website.

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

Load Balancer

Download the 64-bit executable "ArcSightSmartConnectorLoadBalancer-8.2.0.bin" file and the Micro Focus SmartConnector Load Balancer Configuration Guide from the Support website. When downloading the documentation zip file, create a folder for documentation (such as `C:\ArcSight\Docs`) and unzip the file in that folder.

For a successful Load Balancer installation, see Installation and Configuration.

Upgrading to 8.2.0

Verify 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, refer to Micro Focus GPG or RPM Signature Verification.

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 8.2.0

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

For information and instructions, see Upgrading Connectors.

Upgrading Load Balancer to 8.2.0

Perform the following steps to upgrade to Load Balancer 8.2.0:

1. Download Load Balancer 8.2.0 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 8.2.0 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 8.2.0:

- **For 8.0.0 users**: `cp -a 8.0.0/user current`
- **For 8.1.0 users**: `cp -a 8.1.0/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.

Known Limitations

SmartConnector

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
```

[CON-25361]

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.

[CON-25568]

All SmartConnectors or Collectors

SmartConnector or Collector remote connections fail due to low entropy.

All SmartConnector 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.

To ensure that the entropy value is at the desired level:

1. Install the `rng-tools` package by the following command:
   `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 by the following command:
   `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 by the following commands:
   `systemctl enable rngd.service`
   `systemctl start rngd.service`
6. Ensure that the `rngd` package is always running (even after a reboot) by the following command as `root` user:
   `chkconfig --level 345 rngd on`
7. Check the entropy availability in the system, after starting the `rngd` service by the following command:
   `cat /proc/sys/kernel/random/entropy_avail`

[CON-25177]

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 [CON-25177].

[CON-25133]

ArcMC Managed SmartConnectors

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`

[CON-23909] and [CON-23970]

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:

Set the following path manually:

```
$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. 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.

[CON-21601]

Microsoft Azure Monitor Event Hub

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 debug mode:

1. Go to **Azure portal** > **Function app** > **Configuration**.

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

3. Restart the Function App.

[CON-22784]

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.

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.

[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 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.

[CON-19234, CON-18977]

Load Balancer Known Limitations

Note: This table includes legacy issue from the ArcSight Installer.

Key	Description

CONLB-417	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 Soon

None at this time.

SmartConnector Support Recently Ended

Connector	End of Support Date	Reason
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. [CON-17404]
Solsoft Policy Serve	11/22/2019	Lack of customer demand. [CON-22478]
Oracle Audit DB version 9	8/21/2019	End of support by vendor. [CON-22834]
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. [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 SmartConnector Release Notes (Connectors 8.2.0)

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!