Micro Focus Security ArcSight SmartConnectors

Software Version: 8.4

SmartConnector Release Notes

Document Release Date: November 2022
Software Release Date: November 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

Release Highlights

The SmartConnector 8.4 release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Significant performance and stability Improvements for Microsoft Windows Event log – Native (WiNC)
- Support for Microsoft Windows Server 2022 in WiNC
- Support for the new Graph API in Microsoft 365 Defender
- Support for VMware ESXi 7.0 Server Syslog
- Support for Security Command Center (SCC) service logs in Google Cloud Platform (GCP)
- Support for AWS log sources

For detailed information, see the "What's New" on the next page section of this guide.

The Connector Team have worked tirelessly, and in a few cases, have enjoyed the benefits of some of our customers partnering with us to overcome some of these issues. We appreciate the extra effort from our customer success and support teams, and especially our customers, to help us understand and reproduce some difficult situations so that we can improve our SmartConnectors.

Additionally, we will be updating affected entries in ArcSight Idea Exchange portal, and continue to monitor it to help us prioritize and plan new features for our next release.

What's New

SmartConnector 8.4 incorporates the following SmartConnector 8.3 patch releases, and content and categorization updates:

- SmartConnector 8.3 Patch 1
- SmartConnector 8.3 Patch 2
- SmartConnector 8.3 Patch 3
- SmartConnector 8.3.1
- SmartConnector 8.3.2
- SmartConnector 8.3.3
- Event Content-Categorization updates from February 2022 R1 to September 2022 R1

For more information, see the corresponding release notes in the ArcSight SmartConnectors 8.3 Documentation website.

New SmartConnectors and Modules

New SmartConnectors/ Application Module	Description
Check Point Syslog	Added support for the following modules of Check Point R81: • Anti-Malware, Application Control • System Monitor, VPN-1 & FireWall-1 • HTTPS Inspection, Security Gateway/ Management • Smart Console, Smart Defense • URL Filtering • Threat Emulation • New Anti Virus • Threat Extraction • Anti-Bot • Content Awareness • Identity Awareness • DLP, and Forensics
Check Point Syslog	Added support for the following modules of Check Point R80.40: • Application Control Content Awareness • Application Control URL Filtering Content Awareness • CloudGuard IaaS, Content Awareness • SmartDefense VPN-1 & FireWall-1 • URL Filtering Content Awareness • URL Filtering VPN-1 & FireWall-1 • VPN-1 & FireWall-1 Application Control • VPN-1 & FireWall-1 Content Awareness • VPN-1 & FireWall-1 URL Filtering • WEB_API
Microsoft Windows Event log – Native (WiNC): Windows Server 2022 – BITS Client	Added additional fields support for Event ID 61.

New SmartConnectors/ Application Module	Description
Microsoft Windows Event log – Native (WiNC): Windows Server 2022 – Remote Access	Added support for the following events: • 600 • 608 • 635 • 653 • 654 • 670 • 671 • 672 • 700 • 827 • 848 • 20019 • 20084 • 20085
Microsoft Windows Event log – Native (WiNC): Windows Server 2022 – Windows Defender AntiVirus	Added support for the following events: • 1010 • 2003 • 2031 • 2041 • 3007 • 5009 • 5011 • 5013

New SmartConnectors/ Application Module	Description
Microsoft Windows Event log – Native (WiNC): Windows Server 2022 – NTDS Database	Added support for the following events: • 1009 • 1013 • 1133 • 1166 • 1167 • 1197 • 1257 • 1258 • 1260 • 1261 • 1481 • 1515 • 1516 • 1517 • 1518 • 1544 • 1585 • 1904
Microsoft Windows Event log – Native (WiNC): Windows Server 2022	Added support for the following modules: • Microsoft-Windows-Security-Auditing • Service Control • NPS

New SmartConnectors/ Application Module	Description
VMware ESXi Server Syslog	Added support for the following VMWare ESX 7.0 modules: • sensord • Vsansystem • hostd-probe • Rhttpproxy • Clomd, nsx-opsagent • kmxa, vmkernel • apiForwarder • cfgAgent • esxtokend • fdm, hostd • kmxa, localcli • nestdb-server • nsxavim • nsx-exporter • nsx-opsagent • nsx-proxy • nsx-sfhc • nsx-sha • osfsd • smartd • vmkwarning • Vpxa • VSANMGMTSVC For more information, see Configuration Guide for VMware ESXi Syslog SmartConnector

New Cloud Support

Application Module	Description
Amazon S3	The following parsers have been added to our growing list of Amazon S3 SmartConnector supported log sources: • AWS CloudTrail • Blue Coat Proxy SG Multiple Server File • Box • CA SiteMinder Single Sign-On File • CEF Format • Check Point OPSEC NG • Cisco Secure IPS SDEE • Cisco Sourcefire Defense Center eStreamer • Dell EMC Isilon/PowerScale Unity and VNXe Storage • Google Cloud Platform • HPE OM i Web Services • HPE OM Incident Web Service • HPE OpenVMS File • HPE UX Audit File • IBM BigFix REST API • IBM NVAS for z/OS File • IBM NVAS Session for z/OS File • IBM SDSF for z/OS File • IBM System Log for z/OS File • IBM WebSphere File • IP Flow Information Export (IPFIX) • IP Flow (Netflow/J-Flow) • Juniper Steel-Belted Radius File • Microsoft 365 Defender • Microsoft DHCP File • Microsoft DNS DGA Trace Log Multiple Server File • Microsoft Exchange PowerShell • Microsoft Forefront Threat Management Gateway File • Microsoft IIS File • Microsoft IIS Multiple Site File • Microsoft Network Policy Server File • Microsoft Office 365 Management Activity • NetApp ONTAP XML File • NMap XML File • Okta • IDMEF XML File • OVAL XML File • sFlow Devices • Snort Multiple File • TCPdump • Qualys QualysGuard File • Rapid7 NeXpose XML File • SAINT Vulnerability Scanner • Sun ONE Direct Server/Multi Server File • Tenable Nessus .nessus File • Tenable SecurityCenter XML File • Tripwire IP360 File • Tripwire Manager File • UNIX Login/Logout File • VMware Web Services • Zeek IDS NG File For more information about the complete list of log sources supported through the Amazon S3 SmartConnector, see Configuration Guide for Amazon S3 SmartConnector.

Application Module	Description
AWS Security Hub	Added support for the following services: • IAM Access Analyzer Service • Macie Services
Google Cloud Platform (GCP)	Added support for the following Security Command Center (SCC) service logs: • API key vulnerability findings • Compute image vulnerability findings • Compute instance vulnerability findings • Container vulnerability findings • Dataset vulnerability findings • DNS vulnerability findings • Firewall vulnerability findings • IAM vulnerability findings • KMS vulnerability findings • Monitoring vulnerability findings • Multi-factor authentication findings • Network vulnerability findings • Pub/Sub vulnerability findings • SQL vulnerability findings • Storage vulnerability findings • Subnetwork vulnerability findings • VM Manager findings • Web Security Scanner findings • Event Threat Detection rules

Application Module	Description
Microsoft 365 Defender	Added support for the **Graph API** alert type to fetch events through Microsoft 365 Defender APIs in Microsoft Graph. For more information, see parameter details in the Configuration Guide for SmartConnector for Microsoft 365 Defender.
Microsoft Azure Monitor Event Hub	• The Microsoft product name **Azure Security Center** has now been rebranded as **Microsoft Defender for Cloud**. For more information, see Configuration Guide for Microsoft Azure Monitor Event Hub. • The upgrade scenario has been enhanced by modifying the PowerShell script. For more information, see *Step 7* of the Upgrading the Connector section in *Configuration Guide for Microsoft Azure Monitor Event Hub*. • The deployment script has been enhanced to verify that the key properties exist and contain appropriate values before proceeding on deployment • All Microsoft support and development for the Azure Active Directory Authentication Library (ADAL), including security fixes, ends in December, 2022. The authorization functionality has now been migrated to Microsoft Authentication Library (MSAL) for token retrieval and authentication in the Azure Monitor Function application.

Security Updates

SmartConnector Security Updates Application Module	Description
All DB Connectors (using PostgreSQL JDBC Driver)	Upgraded PostgreSQL JDBC version to 42.4.1.
All SmartConnectors and Load Balancer	• Upgraded Tomcat version to 9.0.65. • Upgraded JRE version to 8u342.
All SmartConnectors, all Cloud Native connectors, and Load Balancer	Upgraded Apache Log4j library version to 2.18.0.

Version Updates

Application Module Version Updates	Description
All SmartConnectors	Upgraded JRE timezone database version to 2022a.
Linux Audit Syslog Linux Audit File	Added support for Red Hat Enterprise Linux Server (RHEL) 8.5 and 8.6.
UNIX Login/Logout File UNIX OS Syslog	Added support for Red Hat Enterprise Linux Server (RHEL) 8.5 and 8.6.

Platform Support

Application Module Platform Support	Description
All SmartConnectors	Added support for Red Hat Enterprise Linux Server (RHEL) 8.5 and 8.6.

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

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	Added support for the new destination called "ArcSight SaaS". If SmartConnectors are configured to use Arcsight SaaS as a destination, SmartConnectors ingest events into the Amazon Managed Streaming for Apache Kafka (Amazon MSK) server. For more information about the parameters to be selected during a connector's installation, see ArcSight SaaS in *Installation Guide for ArcSight SmartConnectors*.
FlexConnector for REST	Added a new property to explicitly set the vendor time zone as an enhancement.
Microsoft Windows Event log - Native (WiNC)	Added support for the **Source User ID** field in the Event ID 4624.
Okta Connector	Added support for the **API Token** grant type to authenticate requests to Okta APIs. For more information, see Configuration Guide for SmartConnector for Okta. **Important**: It is recommended to use the **API Token** grant type, because the **Authorization Code** and **Password** grant types will be deprecated from the ArcSight 23.1 release, the first release of 2023.

Software Fixes

The following issues are fixed in the 8.4 release:

Application Modules Software Fixes	Description
All Connectors (configured with Amazon S3 Destination)	The Connector was unable to upload AVRO files to S3 bucket, even though the Connector service was up and running. **Fix**: The Connector is now able to upload AVRO files to S3 bucket.
All Connectors with CEF inputs	The connector was unable to process CEF events because of malformed events. **Fix**: Added additional error handling in place to address this issue.
All SmartConnectors	The SmartConnectors were using port 8080 unnecessarily because of the regression in SmartConnector 8.3 Patch 3. **Fix**: The fixes have been implemented in the connector not to use port 8080 anymore.
ArcSight FlexConnector JSON Multiple Folder Follower	The JSON events were not being parsed and sent to a destination. **Fix**: Now, the events are getting parsed and sent to the destination correctly.
Cisco IOS Syslog	Events for the IOSXE-6-PLATFORM module were not being parsed. **Fix**: The new sub-message has been provided to handle unparsed events for the IOSXE-6-PLATFORM module.
Cisco IronPort Email Security Appliance File	The mapping details for **Device Custom String 6** were missing. **Fix**: Modified the regex to handle the mapping details.
Cisco Wireless LAN Controller Syslog	Some of the events were not being parsed for Cisco Wireless LAN Controller. **Fix**: Added new sub-message and regex to handle the unparsed events.
Citrix NetScaler Syslog	The Citrix NetScalar 12.1 events were not being parsed. **Fix**: The regex has been modified for the unparsed events.
F5 BIG-IP Syslog	The F5 BIG-IP Syslog logs were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.
Fortinet Fortigate Syslog	The Fortinet Fortigate Syslog event keys were not being parsed. **Fix**: The regex associated with **additionaldata.ui** has been modified to handle the unparsed events.
IBM AIX Audit Syslog	The IBM AIX 7.2 logs were not being parsed. **Fix**: Added new sub-message regex to handle the unparsed events.

Application Modules Software Fixes	Description
Infoblox NIOS Syslog	The Infoblox 8.4 events for Infoblox NIOS Syslog were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.

Application Modules Software Fixes	Description
Intersect Alliance SNARE Syslog	Some of the events were not being parsed for Windows Snare 4.0. **Fix**: Provided support for the following events: • 1 • 3 • 6 • 12 • 13 • 14 • 15 • 16 • 18 • 20 • 25 • 27 • 32 • 35 • 44 • 55 • 98 • 109 • 139 • 143 • 144 • 153 • 172 • 1074 • 4200 • 5211 • 6006 • 6038 • 7026 • 10016 • 10148 • 10149 • 14531 • 14533 • 15300

Application Modules Software Fixes	Description
	• 15301 • 16962 • 16977 • 16983 • 36871 • 50036 • 50037 • 51046 • 51047
Linux Audit File	The RHEL 8.3 auditd events were not being parsed. **Fix**: The new sub-message has been provided to handle unparsed events.
Load Balancer	Load Balancer was unable to share the load with the connector, because it misinterpreted that the connector was busy. **Fix**: Error handling for invalid load statistics has now been improved.
Microsoft 365 Defender	The **mitreTechnique** field was not mapped correctly. **Fix**: The **mitreTechnique** mapping has been modified to **Device Custom String 6**.
Microsoft Azure Monitor Event Hub	The Azure Monitor Function application was unable to start or stop the Cloud Function application. **Fix**: The Azure Monitor Function application requires the Contributor role on the resource group to start or stop the Cloud Function application. To assign the Contributor role, ensure that the user deploying the cloud Connector has the Owner role on the resource group. For more information, see the Setting User Permissions in Azure section in *Configuration Guide for Microsoft Azure Monitor Event Hub*.
Microsoft DNS DGA Trace Log Multiple Server File	Some of the events for Microsoft DNS DGA Trace Log Multiple Server File were unable to handle time stamp. **Fix**: Added a new regex to handle the time stamp.
Microsoft Office 365 Management Activity	The **Source Username** and **Destination Username** fields were missing under Active Directory for the event **Change User Password**. **Fix**: Added the **Source Username** and **Destination Username** mappings to these fields.

Application Modules Software Fixes	Description
Microsoft Office 365 Management Activity	Some of the events for Microsoft Office 365 Management Activity were unable to parse a few additional fields. **Fix**: Added token and mapping support for the additional fields to improve the parsing capability.
Microsoft Windows Event log - Native (WiNC)	The connector was facing an MQ full issue while transferring the events. **Fix**: The WiNC connector now uses fewer resources and runs at higher event per second rates when compared to SmartConnector version 8.3, because of the architectural changes.
Microsoft Windows Event log - Native (WiNC)	TLS protocol was not supported during the communication between winc-agent (.NET component) and the SmartConnector (Java component). **Fix**: TLS protocol is now supported during the communication between winc-agent (.NET component) and the SmartConnector (Java component) that are installed on Windows Servers - 2016, 2019, and 2022. If SmartConnector 8.4 is installed on Windows Server 2012 R2, then TLS is not supported because of the cipher suite support limitations in Microsoft Windows. The SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol by changing the parameter value from **agents[0].communicationprotocol=TLS to agents [0].communicationprotocol=Raw TCP** **Note**: If you have installed the SmartConnector on the Win 2012 and Win 2012 R2 (with the latest security updates) and you want to use TLS, then perform the following steps: 1. Stop the connector 2. Add the following cipher information in the **agent.properties** file: **syslogng.ssl.cipher.suites=TLS_ DHE_ RSA_WITH_AES_128_GCM_SHA256** 3. Restart the connector.

Application Modules Software Fixes	Description

Microsoft Windows Event log - Native (WiNC)	The connector was unable to receive events from the hosts when one or more hosts were down.
	
	Fix: To fix this issue, the following properties have been added in the **agent.default.properties** file:
	
	`winc.winc-agent.checkHostStatusViaWmi=`
	
	`winc.winc-agent.checkHostStatusViaPing=false`
	
	`winc.winc-agent.endpointReconnectInterval=300000`
	
	`winc.winc-agent.OStoCheckHostAlive=Windows Server 2019 Standard`
	
	For more information, see the Troubleshooting section in the Configuration Guide for Microsoft Windows Event Log - Native SmartConnector.

Microsoft Windows Event log - Native (WiNC)	The authorization error was displayed and the Windows account was getting locked out when the incorrect password was entered multiple times. **Fix**: The issue has been fixed.
Microsoft Windows Event log - Native (WiNC)	The **Event ID: 403** for Microsoft ADFS was not being parsed. **Fix**: The parsing capability for the **destinationPort** and **oldFileId** fields have been improved for Event ID: 403 to handle unparsed event.
Pulse Secure Pulse Connect Secure Syslog	Some of the events were not being parsed for Pulse Secure device. **Fix**: Added new sub-message and mapping details to handle the unparsed events.
Pulse Secure Pulse Connect Secure Syslog	The Pulse secure events were not being parsed. **Fix**: Modified the sub-message regex to handle the unparsed events.
Pulse Secure Pulse Connect Secure Syslog	The Pulse Secure Pulse Connect Secure Syslog events were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.

Application Modules Software Fixes	Description
Symantec Endpoint Protection DB	All the Symantec Endpoint Protection DB events were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.
Syslog NG Daemon	When the Linux Auditd event merging is enabled and the **Generate Unparsed Events** parameter is set to **Yes**, the Linux Auditd events were sent as unparsed events along with the parsed merged events. **Fix**: The unparsed events are no longer sent with the parsed merged events.
UNIX OS Syslog	The Solaris events for UNIX OS Syslog were not being parsed. **Fix**: Added new sub-messages to handle the unparsed events.

Event Categorization Updates

This release contains the event content-categorization updates made to the following data sources between February 2022 R1 and September 2022 R1 releases:

- Amazon Security Hub
- Check Point:
  - Content Awareness
  - Anti-Bot
  - Firewall-1
  - VPN-1 & FireWall-1 Application Control
  - VPN-1 & FireWall-1 Content Awareness
  - VPN-1 & FireWall-1 URL Filtering
  - Gaia
  - Threat Extraction
  - Application Control Content Awareness
  - Application Control URL Filtering Content Awareness
  - Cloudguard IaaS
  - URL Filtering Content Awareness
- Cisco:
  - CiscoRouter 15.4
  - NX-OS 15.1

    - Wireless LAN Controller 7.6
    - Cisco ISE 1
- F5 Big IP
- Fortinet:
    - Fortigate 5.2 Content 3.086
    - Fortigate-1801F
    - Fortigate -200E
    - Fortigate-3000D
    - Fortigate-400E
    - Fortigate-601E
    - Fortigate-80E
    - Fortigate-VM64
    - FortiManager-VM
- Infoblox NIOS
- ISS:
    - RealSecure Network Sensor
    - RealSecure OS Sensor
- Juniper:
    - IDP 3526
    - Netscreen VPN SSL 1000
- McAfee Host Intrusion Prevention 7.0/8.0 content version 12336
- McAfee Network Security Manager 10.9.37.3
- Microsoft:
    - Microsoft Windows
    - Microsoft Windows WindowsUpdateClient
    - Windows Remote Management
    - Forefront Protection
- Palo Alto Networks PAN OS 10.0.0.8
- Snort:
    - Snort 3.0
    - Sourcefire SEU 31350
- Sun Solaris 10
- Symantec:

    - Endpoint Protection 11
    - Network Security 7100 1445
- Unix
- VMmware ESX 7.6
- Tippingpoint SMS IPS DV9711
- Pulse Secure Connect Secure
- Google Cloud Security Command Center
- IBM X-Force XPU 4208.18170

For more information, see Release Notes for ArcSight Content-Categorization Updates 2022.

Updated Support Policy

Inline with the documents ArcSight Customer Support - Help with SmartConnector and Parser Updates, Technical Requirements for SmartConnectors, the note at the top of the SmartConnector Grand List (A-Z) documentation page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the SmartConnector Grand List (A-Z) documentation page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see ArcSight Customer Support - Help with SmartConnector and Parser Updates.

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 8.4 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-CONNECTORUNOBFUSCATEDPARSERS-8.4.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight8.4.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.

ArcSight-8.4.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-8.4.xxxx.0-MispModelConnector-Linux64.bin	This is the installer file for MISP Connector support for Linux.
ArcSight-8.4.xxxx.0-MispModelConnector-Win64.exe	This is the installer file for MISP Connector support for Windows.
ArcSight-AWS-CloudWatch-Connector-8.4.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for CyberRes Galaxy Threat Acceleration Program Connector support for Linux.
ArcSight-8.4.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for CyberRes Galaxy Threat Acceleration Program Connector support for Windows.

Upgrading to 8.4

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 8.4

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 8.4

For information about upgrading Load Balancer to 8.4, see Upgrading Load Balancer.

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 SmartConnectors	**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 Connector	**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 Windows Event log - Native (WiNC)	**WiNC SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2** The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS. **Workaround**: Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol. To use 'Raw TCP', perform the following steps after installing the SmartConnector: 1. Open the `<ARCSIGHT HOME>/current/user/agent/agent.properties` file. 2. Change the parameter value from **agents[0].communicationprotocol=TLS** to **agents [0].communicationprotocol=Raw TCP** 3. Restart the SmartConnector.
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.

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 23.2 release, the second 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 Connector.

SmartConnector Support Recently Ended

SmartConnector	End of Support Date	Reason
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - CyberRes Galaxy Threat Acceleration Program Connector, which has enhanced threat intelligence capabilities.
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 8.4)

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!