Micro Focus Security ArcSight Connectors

SmartConnector Parser Update Release Notes

7.9.1.8098.0

July 23, 2018

Micro Focus Security ArcSight
SmartConnector Parser Update Release Notes

7.9.1.8098.0

July 23, 2018

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical SupportPage: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation

Contents

SmartConnector Parser Release 7.9.1.8098.0 4
To Verify Your Upgrade Files 4
Supported SmartConnector Version 4
Obtain Parser Release AUP File 4
ArcSight Marketplace 4
MICRO FOCUS PROTECT 7/24 4
New Component or Version 4
Fixed Issues 5
Enhancements 5
Connector End-of-Life Notices 6
SmartConnector Support Ending Soon 6
SmartConnectors Support Recently Ended 6
Support Ended 4/28/2018 6
Support Ended 11/15/2017 6
Support Ended 10/17/2017 6
Support Ended 08/15/2017 6
Support Ended 06/15/2017 6
Updated Configuration Guides 7
Verify Your Upgrade Files Obtained from SSO 7
Upgrading to the 7.9.1.8098.0 Parser Release 7
Upgrade Locally to this Parser Release 7
Upgrade Remotely to this Parser Release Using ArcMC 8
From Marketplace Directly 8
From SSO or Marketplace, then Apply from the ArcMC Repository 9
Roll Back to a Previous Version 9
Verify the Parser Version AUP in Use 9
In ArcMC 9
In the Agent Logs 9

SmartConnector Parser Release 7.9.1.8098.0

These notes list SmartConnectors for which parser changes have been made and describe how to apply this latest ArcSight SmartConnector parser release.

To 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.
Visit the following site for information and instructions:
https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do

Note: If a Parser Override was provided, see if 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 may test the upgrade in a STAGE (staging) environment to make sure it works as expected prior to upgrading it in PROD (production).

Supported SmartConnector Version

This parser update has been certified with SmartConnector Framework release 7.9.0.8084.0. Use of this update with earlier framework releases is not supported.

Obtain Parser Release AUP File

ArcSight Marketplace

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

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

MICRO FOCUS PROTECT 7/24

The monthly ArcSight SmartConnector parser update releases are also posted to Protect 7/24 (https://community.softwaregrp.com/t5/Protect724/ct-p/Protect724).

New Component or Version

SmartConnector for	Number	Description
MS Windows Event Log Native	CON-19814	Added support for Windows 2008 R2 EventID 1074.
Microsoft Exchange MailBox Store	CON-20260	New support for Exchange 2010.

Fixed Issues

SmartConnector for	Number	Description
Snort Multiple File Connector	CON-18789	Some events were not being parsed.
NetApp Filer Syslog	CON-18612	Some events were not being parsed.
McAfee Network Security Manager Syslog	CON-19900	Some events were not being parsed.
Symantec Endpoint Protection DB Config	CON-20507	Some events were not being parsed.
IBM AIX Syslog	CON-20677	Some events were not being parsed.
Microsoft DNS Multiple Server File	CON-19055	Some events were not being parsed.

Enhancements

SmartConnector for	Number	Description
Linux Audit Syslog	CON-19758 CON-19746 CON-20081	Mappings were updated.
Fortinet FortiGate Syslog	CON-20168	Mappings were updated.
MS Office 365	CON-20101 CON-20725	Mappings were updated.
Checkpoint Syslog	CON-20078 CON-19923 CON-20502	Added support for: Connectra, Anti Virus, Security Gateway/Management, Linux OS, Syslog, Threat Emulation, Anti Bot and Anti Virus.
Symantec Endpoint Protection DB Config	CON-18790	Added "Source Process Id" and "Device Action" to common mappings.
MS SQL Server Audit Win Event Log Native Config	CON-20511	Mappings were updated.

Connector End-of-Life Notices

SmartConnector Support Ending Soon

SmartConnectors Support Recently Ended

Support Ended 4/28/2018

Support ending for all 32-bit SmartConnectors – Use 64-bit SmartConnectors.

Support Ended 11/15/2017

Lumension PatchLink Scanner DB – Product no longer available.

Support Ended 10/17/2017

Apache HTTP Server Access File (Legacy) – Use the SmartConnector for Apache HTTP Server Access Multiple File.

Cisco Content Services Switch Syslog (Legacy) – Support ended due to end of support by vendor.

Cisco Firewall Services Module Syslog (Legacy) – Support ended due to end of support by vendor.

Cisco Router non-IOS Syslog (Legacy) – Use the SmartConnector for Cisco IOS Syslog.

Cisco VPN Syslog (Legacy) – Use the SmartConnector for Cisco ASA Syslog.

eEye REM Security Management Console DB (Legacy) – Support ended due to end of support by vendor.

IBM Lotus Domino DB (Legacy) – Support ended due to lack of ODBC support with Java 8.

IBM Tivoli Access Manager File (Legacy) – Support ended due to end of support by vendor. For future product support, use the SmartConnector for IBM Security Access Manager Syslog.

IBM Tivoli Access Manager XML File (Legacy) – Support ended due to end of support by vendor. For future product support, use the SmartConnector for IBM Security Access Manager Syslog.

QoSient ARGUS (Legacy) – Support ended due to lack of customer demand.

RSA Identity Management Service SNMP (Legacy) – Use the SmartConnector for SNMP Unified.

Sun ONE Web Access Server File (Legacy) – Use the SmartConnector for Sun ONE Web Access Server Multiple File.

VMware ESXi Syslog – Support ended for vCenter versions 2.5, 3.5, 4.0, and 5.0 and ESX/ESXi servers 3.0, 4.0, and 5.0 due to end of support by vendor.

Support Ended 08/15/2017

VMware Web Services – Support ended for vCenter versions 2.5, 3.5, 4.0, and 5.0 and ESX/ESXi servers 3.0, 4.0, and 5.0 due to end of support by vendor.

Support Ended 06/15/2017

Rapid7 NeXpose XML File – Support ended for versions 4.0 through 4.12 due to end of support by vendor.

Updated Configuration Guides

SmartConnector configuration guides for the following devices have been updated for this release and are posted to the ArcSight Connector Documentation page on MICRO FOCUS Software Community at:

https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation

NetApp Filer Syslog
McAfee Network Security Manager Syslog
IBM AIX Syslog
MSWindowsEventLogNativeConfig
MicrosoftExchangeMailBox StoreWinEvtLogNativeConfig
UNIX Login/Logout File
Linux Audit Syslog Config
Fortinet FortiGate Syslog
MS Office 365
SymantecEndpointProtectionDB
MSSQLServerAuditWinEvtLogNativeConfig
Checkpoint Syslog

Verify Your Upgrade Files Obtained from SSO

After you obtain the parser release file from SSO, and before you upgrade, Micro Focus provides a digital public key for you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party. Visit the following site for information and instructions:
https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do

Upgrading to the 7.9.1.8098.0 Parser Release

The following sections document the multiple options for upgrading to this parser release:

- Upgrade Locally to this Parser Release
- Upgrade Remotely

Upgrade Locally to this Parser Release

Before starting this procedure, verify that you are running the SmartConnector framework version 7.7.0.8036.0. Applying this parser AUP release update to any SmartConnector release earlier that 7.7.0.8036.0 is not supported by Micro Focus ArcSight.

To upgrade locally to this parser release:

1. Download the appropriate parser release upgrade AUP file from the ArcSight Marketplace site (https://marketplace.microfocus.com/arcsight) at **Categories > SmartConnectors** or from SSO (https://softwaresupport.softwaregrp.com/).
2. Stop the SmartConnector.
3. To perform the parser upgrade, run the command:
   arcsight parseraupupgradelocal [your_upgrade_to_parser].aup [your_ignore_warning_flag]

Where:

[your_upgrade_to_parser].aup is the full path of the upgrade to parser AUP file (the file downloaded in step 1.) This file will be moved by the upgrade script. Verify that no other process is holding this file. Verify that the logged in user has both execute and write permissions for the selected directory.

[your_ignore_warning_flag] is the true/false flag indicating whether you want to ignore the "Parser AUP has later version than the connector" warning

4. The connector will be started automatically after upgrade has completed.

Upgrade Remotely to this Parser Release Using ArcMC

Before upgrading, have the latest version of the *Micro Focus Security ArcSight Management Center Administrator's Guide* available for any questions.

Note: Updating the parser AUP with ArcMC requires ArcMC version 2.5 or later.

You can upgrade to the new parser release from ArcMC either directly from Marketplace using ArcMC or from your ArcMC repository. See the following sections for details:

- From Marketplace Directly
- From SSO or Marketplace, then Apply from the ArcMC Repository

From Marketplace Directly

Before starting this procedure, connector must be running. If you have not already done so, create your administrative account on the ArcSight Marketplace.

To upgrade directly from Marketplace:

5. Click **Node Management** in ArcMC.
6. In the navigation tree, navigate to the host on which the container resides.
7. Select the container to be upgraded.
8. Click the **Upgrade** button.
9. (If not logged into Marketplace) On the upgrade page, click on "Save ArcSight Marketplace User" to enter your Marketplace credentials. This is a one-time task, unless you need to update your credentials.
10. Under **Select Upgrade Type**, choose **Parser upgrade**.
11. From the **Select Upgrade Version** down-down list, select the **7.9.1.8098.0** (Latest) parser upgrade AUP file.
12. Click **Upgrade**.
13. Verify in the Details column, under "Parser upgrade file push status", that the file was successfully pushed to the container. It signifies that the parser upgrade file was automatically downloaded to your repository. Status will show "Successful."
14. Wait while connectors restart automatically.
15. Use the Verify the Parser Version AUP in Use procedure to determine the parser AUP file in use.

From SSO or Marketplace, then Apply from the ArcMC Repository

Prior to performing an upgrade of a container, you will need a connector AUP file of the new parser version in your ArcMC repository.

This is a two-part process:

- Uploading the parser release AUP file to the repository from Marketplace or SSO
- Applying the parser upgrade to all connectors in a container

Note: If the new parser release AUP file (**7.9.1.8098.0**) already exists the repository, go to the next procedure to apply the parser upgrade.

To upload the new parser release AUP file to your repository:

1. Download the parser release upgrade AUP file for the connector from the ArcSight Marketplace (https://marketplace.microfocus.com/arcsight) by selecting **Categories > SmartConnectors** or go to SSO (https://softwaresupport.softwaregrp.com/).
2. Log in to the ArcMC browser-based interface.
3. Go to **Administration > Repositories**.
4. In the navigation tree, pick **Upgrade Files.**
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier. Click **Open**.
7. Click **Submit.** The file is uploaded.

You can now use the AUP upgrade file in the repository when you are ready to upgrade a container or containers to a specific version using the procedure.

To apply the parser upgrade AUP file to all connectors in a container:

1. Click Node Management.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the Containers tab.
4. On the Containers tab, select one or more containers to upgrade.
5. Click Upgrade.
6. On the upgrade page, under Select Upgrade Type, choose Parser upgrade.
7. Under Select Upgrade Version, from the drop-down list, choose the parser release AUP file version to which you want to use to upgrade the selected containers.
8. Click Upgrade. The upgrade is performed on all containers.

See “Upgrading All Connectors in a Container” in the *Micro Focus Security ArcSight Management Center Administrator’s Guide* for complete upgrade instructions.

Roll Back to a Previous Version

Users can roll back to a previous version by using any of three methods suggested for upgrading:

1. Apply the previous version of parser AUP locally.
2. Apply the previous version of parser AUP directly from Marketplace
3. Upload the previous version of the parser AUP to the ArcMC repository from SSO or Marketplace, then apply from ArcMC repository.

Verify the Parser Version AUP in Use

The parser upgrade file in use can be verified in ArcMC or in the agent logs.

In ArcMC

1. Go to Node Management > View All Nodes.
2. In the navigation tree, navigate to the host on which the container resides.
3. Verify that value in the Parser Version column matches the version number of the recent upgrade.

In the Agent Logs

1. Find the agent.log file at: /ArcSight_Home/current/logs
2. Search for the latest occurrence of the line in the log file that contains “ArcSight Parser Version.”
    a. Example:

```
<CODE MAP: '7.9.0.8084.0'>
```

<ArcSight Connector Version: 7.9.0.8084.0>
<ArcSight Parser Version: 7.9.1.8098.0 >