



# **Micro Focus Security**

## **ArcSight SmartConnector**

Software Version: 8.2.2

### **Release Notes**

Document Release Date: October 2021

Software Release Date: October 2021

## Legal Notices

Micro Focus  
The Lawn  
22-30 Old Bath Road  
Newbury, Berkshire RG14 1QN  
UK

<https://www.microfocus.com>

## Copyright Notice

© Copyright 2010 - 2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

## 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.

## 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

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

# Contents

- Overview ..... 5
  - Supported SmartConnector Version ..... 5
  - Obtaining Parser Release AUP File ..... 5
- SmartConnector Enhancements ..... 6
- Support for New Devices or OS Versions ..... 6
- Closed Issues ..... 7
- Known Limitations ..... 8
- System Requirements ..... 15
- To Apply this Release ..... 15
- Upgrading to 8.2.2 ..... 16
  - Upgrading Locally ..... 16
  - Upgrading Remotely ..... 17
    - From Marketplace Directly ..... 17
    - From SLD or Marketplace ..... 18
  - Rolling Back to a Previous Version ..... 19
  - Verifying the Parser Version AUP in Use ..... 19
- Connector End-of-Life Notices ..... 20
  - SmartConnector Support Ending Soon ..... 20
  - SmartConnector Support Recently Ended ..... 20
- Send Documentation Feedback ..... 21

# Overview

This Release Notes document lists SmartConnectors for which parser changes have been made. It also describes the procedure to apply the latest ArcSight SmartConnector parser release and provides other information about recent changes and open and closed issues (generated by various vendor devices) to the ArcSight ESM Manager, Logger, Transformation Hub, Recon, and other destinations.



**Important:** The 8.2.0 patch overwrites parser updates. If you want to install the latest patch, then you must install it before you install the parser updates.

## Supported SmartConnector Version

Parser 8.2.2 update has been certified with SmartConnector Framework release 8.2.0. Use of this update with earlier framework releases is not supported.

## Obtaining Parser Release AUP File

The 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.

It is mandatory to set up an [ArcSight Marketplace](#) administrative account to download and install the monthly connector parser updates.

# SmartConnector Enhancements

In each SmartConnector release, various security fixes, feature updates, and bug fixes are made to the field mappings for individual SmartConnectors.



**Important:** If you use any of the SmartConnectors listed in [Closed Issues](#), be aware that installing the updated SmartConnector can impact your created content.

SmartConnector for	Description
Amazon S3	<p>Added support for AWS CloudFront Real-time logs.</p> <p>Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.</p> <ul style="list-style-type: none"><li>• If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.</li><li>• If the content is not in that edge location, CloudFront retrieves it from an origin that you've defined—such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.</li></ul>
Cisco IOS Syslog	Updated Cisco IOS version to 16.6.4.

## Support for New Devices or OS Versions

SmartConnector for	Description
Linux Audit File	Added platform or version support for RHEL 8.4
Linux Audit Syslog	Added platform or version support for RHEL 8.4
UNIX Login/Logout File	Added platform or version support for RHEL 8.4
UNIX OS Syslog	Added platform or version support for RHEL 8.3

## Closed Issues

SmartConnector for	Description
Cisco NX-OS Syslog	<p>Events from the following modules were not being parsed: nfs, vxdmp, hwmgmt, atd, systemd-modules-load, and pmlogger.</p> <p><b>Fix:</b> The capability of these modules have been improved to parse events.</p>
Citrix NetScaler Syslog	<p>Events from the following modules were not being parsed: SSLVPN LOGIN, AAATM LOGIN, EVENT DEVICEDOWN, EVENT MONITORDOWN, EVENT MONITORUP, and EVENT DEVICEOFS.</p> <p><b>Fix:</b> Following changes were made to improve the parsing capability:</p> <ul style="list-style-type: none"> <li>• Added the destinationServiceName field in the following modules: SSLVPN LOGIN, AAATM LOGIN, EVENT MONITORDOWN, and EVENT MONITORUP.</li> <li>• Added the destinationHostName and destinationPort fields in the EVENT DEVICEDOWN module.</li> <li>• Added the following fields in the EVENT DEVICEOFS module: destinationAddress, destinationHostName and destinationPort.</li> </ul>
McAfee Network Security Manager Syslog	<p>The following events were not being parsed: requestMethod, requestUrl, reason, destinationServiceName, requestContext, and requestClientApplication.</p> <p><b>Fix:</b> This issue is fixed.</p>
Microsoft Windows Event Log – Native: Active Directory	<p>The event 2889 mappings of the deviceProduct and name fields were not being parsed correctly.</p> <p><b>Fix:</b> The parsing capability has been improved.</p>
Oracle Audit Syslog	<p>The events from type module were not being parsed.</p> <p><b>Fix:</b> Added support to parse events from the type module.</p>
Symantec Endpoint Protection DB	<p>The <b>requestUrl</b> field was not parsing URLs correctly.</p> <p><b>Fix:</b> This issue is fixed.</p>
Symantec Endpoint Protection Syslog	<p>The following events were not being parsed: admin logins, client registration, group additions, and policy updates.</p> <p><b>Fix:</b> This issue is fixed.</p>
UNIX OS Syslog	<p>Events from the following modules were not parsing correctly: SSHD, CRON, SENDMAIL, XNTPD, IN.ROUTED, NFS, JAVA, VXDMP, and HWMGMTD.</p> <p><b>Fix:</b> Added regex and mapping support for these modules to improve the parsing capability.</p>

## Known Limitations

### Fortinet Fortigate Syslog

A wrong variable is creating a parsing error.

#### Workaround:

- **For CEF 0.1 and CEF 0.1 on Logger:** If the value of the fields **sent** and **rcvd** from the raw events are higher than the maximum integer number( $2^{31}-1$ ), they are rounded to the maximum integer number 2,147,483,647.
- **For CEF 1.0 and CEF 1.0 on Logger:** If the raw event fields **sent** and **rcvd** are more than 32 bits, they fit into the bytesIn/bytesOut variable.
- **For ESM:** Add the bytesInBytesOut.scaling.divider.=10 property in the server and decipher it based on the divider set for **bytesIn/bytesOut**.  
If the values are higher than the maximum integer number( $2^{31}-1$ ), they are rounded to the maximum integer number, 2,147,483,647.

[CON-25642]

### 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"
```

```
ctrl+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 must be 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 "[All SmartConnectors or Collectors](#) " on the previous page.

[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:

Make sure that you install the following 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](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:

- yum install -y unzip
- 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]

## System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to the [Technical Requirements for SmartConnector](#) guide.

## To Apply this Release

Download the appropriate executable for your platform from the [Software Licenses and Downloads \(SLD\)](#).

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.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides available on the [Micro Focus Product Documentation website](#).

To apply this patch for the ArcSight FlexConnector REST and ArcSight Common Event Format REST connectors, see [Upgrading SmartConnectors](#).

# Upgrading to 8.2.2

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

- [Upgrading Locally](#)
- [Upgrading Remotely](#)
  - [From Marketplace Directly](#)
  - [From SLD or Marketplace](#)

Micro Focus provides a digital public key 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, visit the [Micro Focus Partner Portal](#) site.



**Note:** If a Parser Override was provided, determine whether the Bug or Feature Request number is included in the [Closed Issues](#) or [SmartConnector Enhancements](#) section. If the number is not listed, do not upgrade the Connector. You can test the upgrade in a STAGE (staging) to ensure it works as expected before you upgrade your PROD (production) environment.

## Upgrading Locally

Before starting this procedure, verify that you are running the SmartConnector framework version 8.2.0. Applying this parser AUP release update to any SmartConnector release earlier than 8.2.0 is not supported by Micro Focus.

### To upgrade locally:

1. Download the appropriate parser release upgrade AUP file in one of the following methods:
  - Go to **Categories > SmartConnectors** in the [ArcSight Marketplace](#)
  - [Software Licenses and Downloads \(SLD\)](#)

2. Stop the SmartConnector.

3. Run the following 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 downloaded in [step 1](#). This file will be moved by the upgrade script. Verify that no other

process is using 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. After the upgrade completes, connector starts automatically.

## Upgrading Remotely

You can upgrade to the new parser release from ArcMC either directly from Marketplace using ArcMC or from your ArcMC repository.

Before upgrading, have the latest version of the [ArcSight Management Center Administrator’s Guide](#) available for any questions.



**Note:** Updating the parser AUP with ArcMC requires ArcMC version 2.7 or later.

### 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 the Marketplace:

1. Click **Node Management** in ArcMC.
2. In the navigation tree, navigate to the host on which the container resides.
3. Select the container to be upgraded.
4. Click the **Upgrade** button.
5. (Optional) If you have not logged in to Marketplace, on the upgrade page, click **Save ArcSight Marketplace User** to enter your Marketplace credentials. This is a one-time task, unless you need to update your credentials.
6. From **Upgrade Type**, choose **Parser upgrade**.
7. From the **Select Upgrade Version** drop-down list, select the 8.2.2 (Latest) parser upgrade AUP file.
8. Click **Upgrade**.
9. In the **Details** column, under **Parser upgrade file push status**, verify that the status is displayed as **Successful**, to indicate that the file was successfully pushed to the container. It signifies that the parser upgrade file was automatically downloaded to your repository.
10. Wait while connectors restart automatically.
11. To determine the parser AUP file in use, see [Verifying the Parser Version AUP in Use](#).

## From SLD or Marketplace

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

**To upgrade from SLD or Marketplace and then to apply it from the ArcMC Repository, complete the following process:**

1. Upload the parser release AUP file to the repository from Marketplace or SLD.
2. Apply the parser upgrade to all connectors in a container.



**Note:** If the new parser release AUP file (8.2.1) 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 appropriate parser release upgrade AUP file in one of the following methods:
  - Go to **Categories > SmartConnectors** in the [ArcSight Marketplace](#).
  - [Software Licenses and Downloads \(SLD\)](#)
2. Log in to the ArcMC browser-based interface.
3. Go to **Administration > Repositories**.
4. In the navigation tree, select **Upgrade Files**.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Open**.
8. 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. Select one or more containers to upgrade.
5. Click **Upgrade**.
6. From **Select Upgrade Type**, choose **Parser upgrade**.

7. From the **Select Upgrade Version** drop-down list, select the parser release AUP file version to which you want to upgrade the selected containers.
8. Click **Upgrade**. The upgrade is performed on all containers.

For complete upgrade instructions, see [Upgrading All Connectors in a Container](#) in the [ArcSight Management Center Administrator's Guide](#).

## Rolling Back to a Previous Version

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

- Apply the previous version of parser AUP locally.
- Apply the previous version of parser AUP directly from Marketplace.
- Upload the previous version of the parser AUP to the ArcMC repository from SLD or Marketplace, then apply from ArcMC repository.

## Verifying the Parser Version AUP in Use

You can verify the parser upgrade file in use either 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 the 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".

Example:

```
<CODE MAP: '8.2.0.xxxx.0>  
<ArcSight Connector Version: 8.2.0.xxxx.0>  
<ArcSight Parser Version: 8.2.1>
```



**Note:** You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your PROD (production) environment.

## 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]
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. [CON-25726]
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 Release Notes (SmartConnector 8.2.2)**

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](mailto:Documentation-Feedback@microfocus.com).

We appreciate your feedback!