Micro Focus Security ArcSight Connectors

Software Version: 8.1.0

Micro Focus SmartConnector Release Notes

Document Release Date: December 3, 2020
Software Release Date: December 3, 2020

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:

ArcSight Product Documentation on the Micro Focus Security Community

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

These notes describe how to apply this latest release of ArcSight SmartConnectors and provide other information about recent changes and open and closed issues.

A 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 the 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 (CEF format) for log consumers, including ArcSight ESM, ArcSight Logger 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.

Release Highlights

SmartConnector Updates

- **Significant Performance and Stability Improvements**

  Performance improvements focused on code refactoring have achieved SmartConnector throughput improvements between 500% to 1,000% versus SmartConnectors v8.0.0 on an ArcSight Gen10 Connector Host Appliance. This release is also more stable and reliable. Throughput improvements apply to FlexConnectors and RepSM Plus as well.

  Load Balancer stability has improved to detect when a SmartConnector is not responding and gracefully reconnect to the connector.

- **New and improved SmartConnectors supporting popular event sources and vendor cloud services:**

  Amazon Web Services

  - Additional event sources supported in the AWS Security Hub cloud-native SmartConnector.
  - CEF, XML and XQuery log types are now supported by the AWS S3 cloud-native SmartConnector.
  - Non-CloudTrail messages can be deleted by the AWS CloudWatch Connector.

  Microsoft Azure

  - New Azure Security Center SmartConnector
  - Support added for SASL Plain Authentication in the Kafka FlexConnector enables the connector to ingest events from **Azure Event Hub** securely.

  Windows Native SmartConnector (WiNC) on a G10 C6700 Connector Hosting Appliance (CHA)

  - Windows Native SmartConnector (WiNC) can now run in a Windows 2019 Server VM, hosted on Gen10 ArcMC Connector Hosting Appliance (CHA). WiNC runs native Microsoft Windows code to ingest Windows event sources.

    For more information, see the SmartConnector Microsoft Windows Event Log Native on CHA guide.

  Okta Identity and Access Management

- This new SmartConnector supports Okta's industry-leading identity and access management solution.

Netscout Arbor Security Syslog

- The Netscout Syslog SmartConnector integrates Arbor Network Peakflow v8.4

- **Avro-Formatted Event Streams**

  ArcSight supports Avro-formatted event streams throughout its infrastructure. SmartConnectors can emit Avro-formatted events, which can be consumed by Transformation Hub. Avro is an industry-standard data format which provides flexibility in defining fields based on a Schema Registry. New fields can be added, and others changed while maintaining compatibility with prior and future schema releases.

- **New FlexConnectors**

  This new FlexConnector supports Microsoft 365 Defender -formerly Microsoft Threat Protector (MTP) – includes support for Microsoft Graph API and Advanced Thread Protection events.

Content and Parser Improvements

- **Changes in session interfaces for RepSM Plus that ensure compatibility with the backend Zvelo system content feeds**.
- **MITRE ATT&CK**

  We have improved the detection in the finance industry against specialized threat actors.
- **Parsers**
  - New version updates for McAfee ePO, Cisco Secure ACS, Zeek, Arbor Networks Peakflow, MS Active Directory, Linux Audit File, ClamAV, and Snoopy Logger
  - Parsing improvements for Juniper, MS Sysmon, Cisco NX, Blue Coat, Fortinet Fortigate, Oracle Audit Syslog, and Symantec EndPoint Protection
- Categorization
  - Improved categorizations for Office 365, Syslog messages, Cisco, Juniper, CheckPoint, and IBM related logs.
- Added support for the latest releases of Micro Focus Security, Risk and Governance products. Refer to the Support Matrix of each product for applicability.
- Platform component version updates have been certified on RHEL 8.2, CentOS 8.2 and current releases of Azul Zulu Java runtime and Apache Tomcat. Component libraries include current vulnerability compliance, and ciphers are up-to-date.
- Miscellaneous bug fixes. Refer to the Release Notes for the specific defects addressed.

What's New in this Release

SmartConnector 8.1.0.8371.0 includes the following capabilities:

- Our Kafka FlexConnector reads/sends events from/to Azure Event Hub via SASL Plain Authentication.
- Netscout Arbor Security Syslog supports Arbor Network Peakflow v8.4.
- Security updates have been implemented to LoadBalancer.
- Component libraries include current vulnerability compliance, and ciphers are up-to-date.
- Miscellaneous bug fixes. Refer to the Release Notes for the specific defects addressed.
- The SmartConnector for Microsoft Azure Monitor Event Hub now supports Azure Security Center events.
- SmartConnectors with TH as a destination can create outputs in the AVRO format.

Note: Note: From August 2020 and on, framework and parser releases will contain an unobfuscated file. This file includes the latest parser updates of the SmartConnectors currently supported.
The reference file name is **ArcSight-ConnectorUnobfuscatedParsers-8.1.0.8371.0.zip**. To obtain more information, go to softwaresupport.softwaregrp.com.

LoadBalancer

This release contains a new version of LoadBalancer, for more information see the SmartConnector Load Balancer 8.1.0.1090.0 Release Notes and the SmartConnector Load Balancer 8.1.0.1090.0 Configuration Guide.

New SmartConnector

SmartConnector for	Number	New Device, Component, or OS Version
Netscout Arbor Security Syslog	CON-21185	Added support for Netscout Arbor Security Syslog events. For more information, see the SmartConnector for Netscout Arbor Security Syslog configuration guide.
Okta FlexConnector	CON-24582	Added support for Okta events. For more information, see the ArcSight FlexConnector for Okta configuration guide.

New Device, Component, or OS Version Support

SmartConnector for	Number	New Device, Component, or OS Version
All SmartConnectors	CON-24435	Added support for CentOS 8.2.
	CON-24434	Added support for Red Hat Enterprise Linux (RHEL) 8.2.
	CON-24708	This framework release includes event categorization updates up to the release of October R1 2020. Later AUP Packages can be downloaded from SSO and the support platform and will take Micro Focus SmartConnectors 8.1.0 precedence over them. For more information, see the SmartConnector User Guide.
ArcSight FlexConnectors	CON-23528	Added support to the Kafka FlexConnector, it now reads events from Azure Event Hub via SASL Plain Authentication. For more information, see the ArcSight FlexConnector for Kafka configuration guide.
Microsoft Azure Monitor Event Hub	CON-24203	Added support for a new event type: Azure Security Center. For more information, see the SmartConnector for Microsoft Azure Monitor Event Hub configuration guide.
Microsoft Windows Event Log Native	CON-24958	Added support for NETLOGON events. For more information, see the SmartConnector for MS Win Event Log N-MS Netlogon Logs configuration guide

SmartConnector for	Number	New Device, Component, or OS Version
Microsoft Windows Event Log Native (WiNC) on CHA	CON-24640	Created a PowerShell for WinRM and firewall configuration on Windows.
	CON-24625	Modified the "WiNC_CHA_Installer.sh" script to automate the manual steps and install Windows Server 2019 on the KVM host . A VM is automatically created based on the details provided in the script. Added a new option to enable VNC access in the Enforcing mode of SE Linux on WiNC appliances.
	CON-24372	Added support for G10 C6700 Connector Hosting Appliances. For more information, see the SmartConnector Microsoft Windows Event Log Native on CHA guide.
SmartConnectors with Transformation Hub as a Destination	CON-24341 CON-24423 CON-24651	SmartConnectors with TH as a destination can create outputs in the AVRO format.
Zeek IDS NG File	CON-24408 CON-24463	Added support for the following log types: rdp and socks. For more information, see the Zeek IDS NG File configuration guide.

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
Oracle Audit DB	CON-23000	Separate parsers have been provided for Multi-tenant and Single tenant Oracle DB Auditing with each framework. For more information, see the SmartConnector for Oracle Audit DB configuration guide.
CEF Encrypted Syslog	CON-23661	AES-GCM is the new default encryption scheme for CEF Encrypted Syslog (UDP).
All Cloud SmartConnectors	CON-25095	A new utility has been provided to apply parser updates for Cloud SmartConnectors. For more information, see the configuration guides of our AWS and Microsoft Azure SmartConnectors.
All SmartConnectors	CON-23941	Updated Java to allow escape sequences when events are sent to a CSV destination.
	CON-24161	Updated the *Configuring the Connector* chapter on the SmartConnector User Guide with the topic "Updating TZ Data".
	CON-24337 CON-24338 CON-24352 CON-24453 CON-24455 CON-24464 CON-24514 CON-24724	Our SmartConnectors had performance improvements. The performance tool document will be published soon.

SmartConnector for	Number	Description
All SmartConnectors	CON-24731	Updated the bc-fips-1.0.0 jar to bc-1.0.2. This update resolves some FIPS mode fresh installation issues.
	CON-24829	Modified the content types and the content type labels on the Transformation Hub destination parameter. For more information, see the SmartConnector User Guide
Amazon Web Services S3	CON-24367	Added support for the following log types XML, XQuery and CEF. For more information, see the SmartConnector for Amazon Web Services S3 configuration guide.
Actor Model Import Connector for MS Active Directory	CON-24386	Added support for Active Directory on Microsoft Windows Server 2019.
	CON-24420	Added the support for Active Directory on Microsoft Windows Server 2016.

Closed Issues

SmartConnector for	Number	Description
All SmartConnectors	CON-23245	SmartConnectors' performance has been improved so that the process of sending events to Logger as a destination is now more efficient and stable.
	CON-22465	Updated source code to validate events, so that if they contain an invalid XML character, the events are dropped.
	CON-24432	Warning message removed from RHEL & CentOS 6.x, 7.x, 8.x platforms.
	CON-24466	Updated the JDK version to JDK 8U265.
	CON-24528	The MISP Connector failed to receive and send data to ESM Active lists after importing data for a few days. This issue had been fixed
	CON-24644	SmartConnectors installed on Windows servers consume a lot of disk space. The troubleshooting section of the SmartConnector User Guide has been updated with the workaround.
	CON-24796	The RepSM Plus connector stopped receiving reputation data. For more information, see the This issue had been fixed For more information, see the ESM RepSM Plus CIP Solutions Guide 1.70.0 and the ESM RepSM Plus CIP Release Notes 1.70.0
	CON-24333	An error message indicating "remove GC (Allocation Failure)" was being displayed on the console when the connector was running as a standalone. This issue has been fixed.
	CON-24339	When multiple commands were sent to the connector at the same time, each command was duplicated. This issue has been fixed.

SmartConnector for	Number	Description
All SmartConnectors	CON-22724	When the connector was installed in silent mode, the "Unique Generator ID" was being ignored. This issue has been fixed, for more information see the For more information, see the SmartConnector User Guide.
Amazon Web Services CloudTrail	CON-23804	Added a new property in the `agent.properties` file, which can be set to true / false and delete non-cloud trail messages. For more information, see the SmartConnector for Amazon Web Services CloudTrail configuration guide.
Amazon Web Services Security Hub	CON-25116	Added support to the newly-updated log format in GuardDuty events. For more information, see the SmartConnector for Amazon Web Services Security Hubl configuration guide.
ArcSight Common Event Format REST	CON-23764	The OAuth2 Client Properties file is now left in blank to proceed with basic authentication.
Blue Coat Proxy SG Multiple Server File	CON-22108	The SmartConnector kept reading corrupted GZ files, repeatedly. The issue has been fixed.
Microsoft Azure Monitor Event Hub	CON-24537 CON-24538	Updated deployment script options for fresh installations and upgrades. For more information, see the SmartConnector for Microsoft Azure Monitor Event Hub configuration guide.
Microsoft DNS Trace Log Multiple Server File	CON-23730	The SmartConnector attempted to read deleted log files. This issue has been fixed.
Microsoft Windows Event Log Native (WiNC)	CON-24328	The troubleshooting section has been updated with a new topic: Permission Issues with Obfuscationkey as non Administrator User. For more information, see the SmartConnector for MS Windows Event Log - Native SmartConnector (WiNC) configuration guide.

SmartConnector for	Number	Description
	CON-24997	Some event mappings were empty when being sent to ESM. Fix: Updated mappings for Event 4742.
Qualys Guard File	CON-20931 CON-21105	The SmartConnector was not able to generate open port events. Fix: Added support for version 10.3. For more information, see the SmartConnector for Qualys QualysGuard File configuration guide.
Zeek IDS NG File	CON-24837	Some events were not being sent to ESM by the connector. This issue has been fixed. For more information, see the Zeek IDS NG File configuration guide.

Integrated into this release

Parser update releases 8.0.1.8336.0, 8.0.2.8340.0 and 8.0.3.8356.0 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.

- 8.0.1.8336.0 Release Notes
- 8.0.2.8340.0 Release Notes
- 8.0.3.8356.0 Release Notes

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to the ArcSight Security Open Data Platform (SODP) Support Matrix guide available on the Micro Focus Software Community page.

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.

Known Limitations

ArcMC Managed SmartConnectors

SmartConnectors cannot be bulk-upgraded on a Linux server.

Workaround:

Before performing a SmartConnector bulk upgrade from ArcMC on a given Linux server (any 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 automatically start the `rng-tools` package after a fresh install (on a Linux server or an ArcMC appliance), follow these steps:

1. Add the following line to the `/etc/sysconfig/rngd` file:
   `EXTRAOPTIONS="-r /dev/urandom"`
2. Start the `rngd` package as root user:
   `service rngd start`
3. To ensure that the `rngd` package is always running (even after a reboot), run the following command as root user:
   `chkconfig --level 345 rngd on`

[CON-25133]

ArcMC Managed SmartConnectors

One-Click installation fails on RHEL 8.1 or later and CentOS 8.1 or later through ArcMC 2.9.4.

Workaround:

Pre-requisites for instant connector/ collector deployment for 8.1 0:

- Python2
- Libselinux-python

Unlike Linux 6.x and 7.x, the prerequisites above are not integrated by default in Linux 8.x. If you have installed or plan to install ArcMC in a RHEL/CentOS 8.1 machine, perform the following steps. Also, apply these changes to the target Linux host (the VM where the connector/ collector will be deployed):

1. Install python2:
   ```
   sudo yum install -y python2
   ```
2. Create a symlink:
   ```
   sudo ln -s /usr/bin/python2 /usr/bin/python
   ```
3. Install the `libselinux-python` package:
   ```
   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]

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:

Manually set the correct path, which is: `$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, which has experienced 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, we do not recommend the use of the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates.

Workaround:

To mitigate these issues, we recommend using the Windows Native Connector (WiNC) SmartConnector.

[CON-21601]

For more information, see the Technical Note on WinRM-related Issues.

Microsoft Azure Monitor Event Hub

Enable the Azure Event Hub Debug Mode for function apps only for support purposes. Enabling it for normal operation can cause parsing and mapping errors.

Workaround:

To change this setting:

1. Go to the 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 8.1.0.8371.0.
- If the Solaris Connector is installed as a service:

1. Stop the service.

2. Go to HOME/current/bin and execute. /runagentsetup.

3. Uninstall the service in Global Parameters and exit the wizard.

4. Perform a local upgrade to 8.1.0.8371.0.

5. Install the Connector as a service and exit the wizard.

6. 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 if the above work-around does not completely solve the problem, reduce the value of the Native connector parameter 'eventprocessorthreadcount'. 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]

Upgrading to 8.1.0.8371.0

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, 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)

To Apply this Release

Download the appropriate executable for your platform and the "SmartConnector Configuration Guides .Zip" file from the Support Web Site.

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. This document is available on the Micro Focus Security Community as well as in the SmartConnector Configuration Guide zip file available for download from the Support Web Site.

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

Connector End-of-Life Notices

SmartConnector Support Ending Soon

None at this time.

SmartConnector Support Recently Ended

Support Ended 01/14/2020

Windows Server 2008 R2 - end of support by vendor.

[CON-17404]

Support Ended 11/22/2019

Solsoft Policy Server – Support ended due to lack of customer demand.

[CON-22478]

Support Ended 8/21/2019

Support ended for Oracle Audit DB v9 – end of support by vendor.

[CON-22834]

Support Ended 4/28/2018

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

Support Ended 02/21/2018

Symantec Endpoint Protection DB – SEP version 11 support ended by vendor.

Support Ended 01/31/2018

Solaris 10 Premier support - 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 Micro Focus SmartConnector Release Notes (Connectors 8.1.0)

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!