Micro Focus Security ArcSight Release Notes

Software Version: 1.0 Patch 1

CyberRes Galaxy Threat Acceleration Program Release Notes

Document Release Date: June 2022
Software Release Date: June 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

© Copyright 2020 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.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S.Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

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

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

Galaxy Threat Acceleration Program Connector Release Notes

CyberRes Galaxy is an immersive cyberthreat experience that provides actionable and business-centric threat intelligence for security executives. CyberRes Galaxy enables cyber professionals to quickly gain visibility into the most pressing threats to their business and helps organizations secure their value chains so they can focus on driving business growth.

CyberRes Galaxy Threat Acceleration Program Connector connects the ArcSight ecosystem* to the CyberRes Galaxy Threat Feed server, synchronizing the data multiple times daily.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

You can access the additional documents from the CyberRes Galaxy Threat Acceleration Program site.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

What's New

June 2022

GTAP Connector Version 1.0 Patch 1

The following libraries were upgraded:

- Apache Tomcat to 9.0.62
- Zulu OpenJDK to 8u332
- Apache Log4j to 2.17.2

May 2022

Threat Intelligence Platform 3.7.0.0

Threat Intelligence Platform 3.7.0.0 is an ESM out of the box content package, that contains default content to monitor the GTAP connector. You can download Threat Intelligence Platform 3.7.0.0 from the Market Place.

This release contains three new rules and a new dashboard to help you monitor the health of the GTAP Connector installed in Basic and Plus modes:

- The new GTAP SmartConnector Status dashboard displays the health status of the GTAP Connector.

  To access the dashboard, select **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **GTAP SmartConnector Status**.

- An alert is triggered when error messages are received from the GTAP Connector.

  To set the rule, select **All Rules** > **ArcSight Foundation** > **Threat Intelligence Platform** > **GTAP SmartConnector Health/Error in GTAP SmartConnector Service Message**

- An alert is triggered, if data feeds from the GTAP Connector do not get updated during the specified period. The default time frame is two hours.

  To set the rule, select **All Rules** > **ArcSight Foundation** > **Threat Intelligence Platform** > **GTAP SmartConnector Health/No Update from GTAP SmartConnector**

- To monitor the health status of GTAP connector, select **All Rules** > **ArcSight Foundation** > **Threat Intelligence Platform** > **GTAP SmartConnector Health/Track GTAP SmartConnector Service Message**

GTAP Connector Version 1.0

New Galaxy Threat Acceleration Program Connector is released.

Known Issues

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.

Installing the Connector and Patches

Installing the Connector

For detailed instructions about installing the connector, see the Administration Guide for Galaxy Threat Acceleration Program Connector.

Release Contents

File Name	Description
ArcSight-8.3.0.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	Installer for Linux 64-bit systems
ArcSight-8.3.0.xxxx-GalaxyThreatAccelerationConnector-Win64.exe	Installer for Windows 64-bit systems

Downloading and Applying Patches

To download and apply this Connector patch, 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.

For detailed instructions about installing the connector, see the Administration Guide for Galaxy Threat Acceleration Program Connector.

To upgrade the Connector, follow the steps mentioned in the Upgrading Connectors Locally section of *ArcSight SmartConnector Installation Guide*.

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 CyberRes Galaxy Threat Acceleration Program Release Notes (Release Notes 1.0 Patch 1)

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!