Micro Focus
ArcSight Release Notes

Software Version: 2.0.1

ArcSight Threat Acceleration Program Release Notes

Document Release Date: April 2023
Software Release Date: April 2023

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

ArcSight Threat Acceleration Program Release Notes

ArcSight is an immersive cyberthreat experience that provides actionable and business-centric threat intelligence for security executives. ArcSight 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.

ArcSight Threat Acceleration Program Connector connects the ArcSight ecosystem to the ArcSight 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 ArcSightThreat Acceleration Program documentation 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 in Version 2.0.1

- **Integration with Virus Total:** As part of ATAP Connector 2.0.1 release, ArcSight Threat Intelligence/Research solution got enlisted as a security vendor in the security vendor list of VirusTotal, for "threat detection through malicious IIndicator of Compromise (IoC)". VirusTotal, part of Google Cloud, provides threat context and reputation data to help analyze suspicious files, URLs, domains, and IP addresses to detect cybersecurity threats.

  ArcSight Threat Intelligence feed (previously known as Galaxy GTAP Plus) - powered by OpenText Threat Research (previously known as CyberRes Galaxy) will periodically provide the following IoC types for VirusTotal users: IP addresses, domain names, and URLs. This will further enrich/enhance VirusTotal users' experience, as unique/high fidelity threat research, powered by OpenText Threat Research will be available to all VirusTotal users.

  This is a win-win solution for the security industry, as security practitioners will have less blind spots, thanks to ArcSight Threat Intelligence. When an IoC is found to be malicious according to ArcSight Threat Intelligence, further details will be provided, along with a link to cyberresgalaxy.com portal, for up-to-date security threat bulletin details.
- **Default Content Version 4.1:** The Default Content version 4.1 contains rules with very high confidence and low false positive rate.

Known Issues

Connector is Unable to Receive Any Events After Installation

The connector is unable to receive any event after installation, if you have installed the latest version of ATAP Plus connector on a machine where MISP Model Import Connector was previously installed.

Workaround: Clear cache from the `user/agent/agentdata` folder, then restart the connector. The connector will now be able to receive events and send events to destination.

Unable to Download Certificate From Microsoft Edge Browser

If the Microsoft Edge Browser is used to connect to the TI server, then the users are unable to download certificates to enable FIPS mode.

Workaround: Use a different browser such as Chrome.

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 and Upgrading Default Packages

For a fresh installation of Content Package 4.1, see Installing Default Content Package.

If you already have 3.x version of default content, you cannot directly upgrade the package to 4.x. For more information, see Upgrading Default Content Package From Version 3.x to Version 4.x.

You can however, upgrade from 4.0 to 4.1.

Installing and Upgrading the ATAP Connector

Installing the Connector

For detailed instructions about installing the connector, see the Installing the ATAP Connector.

Upgrading the Connector

For detailed instructions about upgrading the connector, see the Upgrading the ATAP Connector.

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 ArcSight Threat Acceleration Program Release Notes (Release Notes 2.0.1)

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!