OpenText
ArcSight Intelligence SaaS

Software Version: 6.4.8

Release Notes

Document Release Date: July 2023
Software Release Date: July 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

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

Contents

Introduction

The release notes document for ArcSight Intelligence SaaS includes the following:

System Requirements

ArcSight Intelligence SaaS supports the following web browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

What's New?

The following sections outline the key features and the issues resolved in this release:

- Support for Microsoft Defender for Endpoint as a Data Source
- New Entity Type for Cloud Application Data
- Support for Audit Logging Service

Support for Microsoft Defender for Endpoint as a Data Source

ArcSight Intelligence SaaS now supports the ingestion and analysis of endpoint data from Microsoft Defender for Endpoint. Defender for Endpoint needs to be configured to forward data to Azure Event Hubs. The data in the Azure Event Hubs is then retrieved by Intelligence and processed further.

Note: Only the following event types of Defender for Endpoint are supported by Intelligence for analytics: DeviceEvents, DeviceLogonEvents, DeviceNetworkEvents, DeviceProcessEvents, DeviceFileEvents

New Entity Type for Cloud Application Data

In the previous versions of ArcSight Intelligence SaaS, incoming data from cloud applications were treated as data of the **Share** entity type and anomalies were also displayed as **Share** entity type anomalies in the UI. However, in the latest version, data from cloud applications are mapped to a separate entity type called **Cloud Apps**, and their anomalies are also now displayed as **Cloud Apps** entity type anomalies in the UI.

Support for Audit Logging Service

This release introduces an Audit Logging service that allows the system administrators and auditors to gain insights into the user activities. The service logs the requests made to the endpoints of Intelligence, and then sends the logs to AWS Cloudwatch. System administrators and auditors can then use the REST APIs to access the audit logs.

Known Issues

OpenText strives to ensure that our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, contact Open Text Support for Micro Focus products.

Delay in the display of the crowdstrike_LogDomain field values in the Query Editor

Issue: For a list of events in the **Events** page, when you click **Type to filter raw events** to create queries through the **Query Editor** and type or select the **crowdstrike_LogDomain** field, it takes more than 30 seconds to display the values corresponding to the field instead of a much lesser time. While the delay occurs regularly for the **crowdstrike_LogDomain** field, the issue is sporadic for other fields.

Workaround: There is no workaround at this time.

[613004]

Sum total of count of each value of column does not equal event count

Issue: For a list of events in the **Events** page, when you click the filter symbol of any column and add the count of each of its values, the sum total does not equal the number of events displayed.

Workaround: There is no workaround at this time.

[413014]

Tag Management displaying wrong entity count

Issue: When a tag is selected in the Tag Management modal, the wrong number of "Total entities tagged" is displayed.

Workaround: There is no workaround at this time.

[346007]

Events column filter limits at 100 values

Issue: When utilizing a column filter on the **Events** page, only 100 values are displayed.

Workaround: There is no workaround at this time.

[350180]

Unable to filter column using special characters

Issue: On the **Events** page, column filters are unable to utilize special characters.

Workaround: There is no workaround at this time.

[366021]

Known Limitations

The following item provide a summary of any known limitations with this release of Intelligence:

Search

A Search limitation requires that at least 2 characters be entered after a hyphen split to be able to successfully search events. For example, a search for a workstation named "mac-5" may not produce any results, but a search for a workstation named "mac-45" will produce search results as intended.

Publication Status

Released: Wednesday, October 25, 2023

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/

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 (Intelligence SaaS 6.4.8)

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!