
Micro Focus Security ArcSight Intelligence

Software Version: 2021.11.1

ArcSight Intelligence SaaS 2021.11.1 Release Notes

Document Release Date: 11/19/2021

Software Release Date: 11/19/2021



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 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 home page of this Help 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

Email	cyberressupport@microfocus.com
Support Web Site	https://support.cyberreshelp.com

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 Intelligence SaaS 2021.11.1 Release Notes (Intelligence 2021.11.1)

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 cyberressuport@microfocus.com.

We appreciate your feedback!

Introduction

This release introduces ArcSight Intelligence SaaS 2021.11.1.

- [System Requirements](#)
- [What's New?](#)
- [Known Issues](#)

System Requirements

ArcSight Intelligence SaaS supports the following Web browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

What's New?

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

- ["Entity Risk Calculation Enhancements "](#) below
- ["Schema Enhancements"](#) below
- ["Performance Enhancements"](#) below

Entity Risk Calculation Enhancements

The way Intelligence calculates entity risk based on anomalies encountered has been enhanced. These enhancements allow changes in entity risk to be traced back more effectively to individual anomalies and yield improved analytics results.

Schema Enhancements

A unified schema has been implemented that encompasses all fields used by our analytics as well as certain informational fields. This simplifies the mapping process while providing greater coverage and flexibility with data sources. Improvements have been made to the mapping of authentication domain events, leading to higher quality anomalies.

Performance Enhancements

Context value calculation has now been streamlined. These enhancements have resulted in shorter analytics runtimes, reduced search disk space usage, reduced search load, faster index times, and faster search query times.

Known Issues

Micro Focus 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 Micro Focus Customer Support at cyberressuport@microfocus.com.

- [Single sensor event slips through filter](#)
- [Tag Management displaying wrong entity count](#)
- [Event search doesn't maintain horizontal scroll position on when filtering](#)
- [Events tab loses horizontal scroll bar in Chrome](#)
- [Column filtering type ahead not working for single character](#)
- [Events column filter limits at 100 values](#)
- [Unable to filter column by special characters](#)
- [PDF Report formatting issues](#)
- [Jump to search not working for anomalies related to UNKNOWN_USERNAME](#)

Single sensor event slips through filter

Issue: On the Events Page, if a user filters for violations utilizing the "interaset_data_source[0]" field, a single instance of a sensor event may be included in the search.

Workaround: There is no workaround at this time.

[344190]

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]

Event search doesn't maintain horizontal scroll position when filtering

Issue: When applying a filter to a column on the Events page, the horizontal scroll position is sometimes reset.

Workaround: There is no workaround at this time.

[344073]

Events page loses horizontal scrollbar in Chrome

Issue: When navigating to the Events page from the Overall Risk page, if the user applies a "Zoom to" filter, the horizontal scrollbar may disappear.

Workaround: Reset the columns or refresh the page.

[345046]

Column filtering type ahead not working for single character

Issue: When utilizing a column filter on the Events page, if a single character is filtered, non-matches may also be returned to the user.

Workaround: There is no workaround at this time.

[348264]

Events column filter limits at 100 values

Issue: When utilizing a column filter on the Events page, only a 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]

PDF Report formatting issues

Issue: Generated PDF reports may contain incorrectly rendered graphics and/or not match what is seen in the UI.

Workaround: There is no workaround at this time.

[331209]

Jump to search not working for anomalies related to UNKNOWN_USERNAME

Issue: J2S not returning events for UNKNOWN_USERNAME user.

Workaround: There is no workaround at this time.

[375039]

Known Limitations

Search

Search currently has limitation where it requires at least 2 characters after a hyphen split in order 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.

Comment and Tag Mapping

This release contains changes and improvements that affect the normalization, ingest, and analytics processes. Due to the nature of these changes and the current upgrade process, any previously applied anomaly tags or comments will not be present after the post-upgrade analytics run is complete.