ArcSight Recon 1.3 Release Notes

ArcSight as a Service

September 2021

This release introduces ArcSight as a Service (ArcSight SaaS), which enables you to use a combination of security, user, and entity solutions in a SaaS environment. The core services for ArcSight aaS, including the Dashboard and user management, are provided by a common layer called Fusion.

This release also includes Recon capabilities. Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database. Recon deploys within the **ArcSight Platform**. For more information about the other products available within the suite, see the *Release Notes for ArcSight Containerized Platform 21.1*.

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website, well as context-sensitive user guides within the product. If you have suggestions for documentation improvements, click Send Us Feedback at the bottom of the page in the HTML version of the documentation posted at the Recon Documentation page.

What's New

This release includes the following features and enhancements:

- "Introducing ArcSight Platform as a Service" below
- "Checking the Integrity of Event Data" below

Introducing ArcSight Platform as a Service

This release introduces ArcSight as a Service (SaaS). SaaS is a software licensing model that allows you to subscribe and access software on external servers in the cloud and not in premises. This service is deployed, configured, and maintained by Micro Focus. Your log in is authenticated using the Micro Focus Advanced Authentication as a Service solution.

For an outline of the process, see the *ArcSight Platform as a Service Quick Start Guide for Administrators*.

Checking the Integrity of Event Data

This release introduces the Event Integrity feature. This feature searches the database for verification events received within the specified date range, then runs a series of checks to compare content in the database with information supplied by the verification event.

Known Issues

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support, and then select the appropriate product category.

- "Search Permissions Include a Non-functional Permission" below
- "Storage Groups Push Changes Fail on Lock Exception" on the next page
- "Search" on the next page
- "Fieldsets" on page 4
- "Outlier Model" on page 5
- "Cannot Import Users from Enterprise Security Manager" on page 5
- "Data Quality Dashboard - Data Timeseries Chart Fails to Update after Changing Categories" on page 6

Search Permissions Include a Non-functional Permission

This release includes functionality designed to support checking the integrity of events for a future release. Some artifacts for that future functionality are exposed in the interface, such as the *Perform Event Integrity Check* permission listed in the **Searches** section of the **Roles** page. Although you can add this permission to a role, currently there are no rights associated with the permission.

Storage Groups Push Changes Fail on Lock Exception

Issue: Sometimes when you have ingestion going on, pushing storage groups changes to the system fails as it's unable to acquire lock on events table. (OCTCR33I180085)

Workaround: Stop Ingestion (scheduler) and apply changes to the system and then start the ingestion again.

Search

The following issues affect your use of the Search feature:

- "Scheduled Searches Sometimes Fail to Export to CSV" below
- "CSV File Export Fails after You Change the Date and Time Format" below
- "Search Fails to Revert the Fieldset to its Original Setting" below
- "Issue with Default Time Setting" on the next page
- "Scheduled Search Appends Erroneous Values to the Run Interval" on the next page
- "Known Issues" on the previous page
- "Search Join Fails when Lookup List has ‘User’ as a Value" on the next page

Scheduled Searches Sometimes Fail to Export to CSV

Issue: On occasion, when you export a completed run of a scheduled search, the CSV file fails to display any data. (OCTCR33I174130)

Workaround: If this issue occurs, view the results of the run. Then, from the Events table, export the data to a CSV file.

CSV File Export Fails after You Change the Date and Time Format

Issue: After modifying the date and time format in preferences, the CSV export function for saved searches runs before the preference change fails. (OCTCR33I113040)

Workaround: Run the scheduled search again, then save it. Select the CSV icon to download the file.

Search Fails to Revert the Fieldset to its Original Setting

Issue: If you change the fieldset after running a search, then leave the **Search** page or move out of the Search section, Search fails to reset the fieldset to the original setting. For example, you choose the *Base Event Fields* field set and run the search, then change the fieldset to *All Fields*. Next you navigate to the Saved Searches page. When you return to the **Search** page, the fieldset is still *All Fields* rather than reverting to *Base Event Fields* as it should. (HERC-9865)

Workaround: To revert the fieldset to its original setting, press **F5** while viewing the Search.

Issue with Default Time Setting

Issue: In User Preferences, if your preferred **Default Time Setting** is Static, you cannot use the date picker to quickly change the time range for the search. (OCTCR33I174128)

Workaround: Manually enter the date and time values. Alternatively, change your preferred **Default Time Setting** to Dynamic or Preset. For more information about configuring your user preferences, see the *User's Guide for Fusion*.

Scheduled Search Appends Erroneous Values to the Run Interval

Issue: When creating a scheduled search, if you select Every 2 hours in the Pattern section, the search runs every two hours, at every even hour, such as 0, 2, 4, 6, etc and appending the minutes setting in Starting From value. The system ignores the hour setting in Starting From value. (OCTCR33I179782)

For example, you might select Every 2 hours and choose Starting From at 01:15 am. Search will run every 2 hours at 2:15 am, 4:15 am, 6:15 am, and so on.

Workaround: Use the Specific Hour setting to run the Search at a selected hour and minutes specified in the Starting From field.

Search Join Fails when Lookup List has 'User' as a Value

Issue: Search displays an error and fails to apply a join if an associated lookup list includes the word "user" for a data value. (HERC-8283)

Workaround: Contact support for help with this issue.

Fieldsets

The following issues affect your use of the fieldsets function:

- "Issue with Fieldsets after Upgrading to this Version" below
- "Fieldsets Display Database Names" below

Issue with Fieldsets after Upgrading to this Version

Issue: After upgrading, the Public Default Fieldset defaults to Base Event Fields. (OCTCR33I178795)

Workaround: In User Preferences, specify the fieldset that you want and set it as default again.

Fieldsets Display Database Names

Issue: When you create a fieldset, Search displays the coding-style name for the fields instead of the human-readable names that you see when creating a search query. For example, in a query you can enter or select Agent Address. However, in the fieldsets selection, this same field appears as agentAddressBin.

This issue also occurs when you’re adding queries to a report. (OCTCR33I181059)

Workaround: Refer to “Mapping Database Names to their Appropriate Search Fields” in the Help or the *User Guide for ArcSight Recon*.

Outlier Model

The following issues affect your use of the outlier model function:

- "Fails to Display after you Change the Timestamp Format" below
- "Erroneously Implies the Date is an Error" below

Fails to Display after you Change the Timestamp Format

Issue: When you apply a timestamp format to an outlier model, and then change the timestamp format, the model fails to appear in **Available Models**.

For example, you create a model in Configuration > Outlier with the **Device Receipt Time** of 12/31/19. You then change the timestamp format in My Profile > Preferences > Date/Time Format to YYYY/MM/DD hh:mm:ss:ms. When you access Configuration > Outlier, Recon no longer displays the model with the modified timestamp. (OCTCR33I113036)

Workaround: In My Profile > User Preferences > Date/Time Format, select the original timestamp format for the model. Recon displays the model in **Available Models**.

Erroneously Implies the Date is an Error

Issue: When you copy a search query to create the filter for an outlier model and the query includes a timestamp, Recon erroneously highlights the specified date as if the date or its format were invalid.

For example, you copy a search query that includes the phrase Normalized Event Time = 29/05/20 16:20:39:288. In Configuration > Outlier, you paste the copied query in the filter field for a new model. The query field underlines the timestamp in red, which is the usual indication that the value is invalid. (OCTCR33I112031)

Workaround: Ignore the highlight that indicates that the copied timestamp value is invalid.

Cannot Import Users from Enterprise Security Manager

Issue: When you attempt to import users from ArcSight Enterprise Security Manager, you will receive a 406 HTTPS Error if one of the following conditions is true you attempt to import the users by using the IP address of the ESM server or if you enter the FQDN (fully qualified domain name) for the ESM server but either the port or admin credentials are incorrect. (HERC-9941)

Workaround: For the ESM server, specify a valid FQDN, as well as the correct port and admin credentials.

Event Integrity Status Displays Incorrectly

Issue: When you run an Event Integrity Check and no data is available, the status field displays Failed (OCTCR33I276038).

Workaround: The status field should display No Data.

Data Quality Dashboard - Data Timeseries Chart Fails to Update after Changing Categories

Issue: When viewing the Data Timeseries Chart in the Data Quality dashboard, the stacked area chart should automatically update as soon as you select an event category, such as Future Events, Past Events, or Active Events. However, when you select an event category, the stacked area chart fails to update automatically. (OCTCR33I276138)

Workaround: To refresh the Data Timeseries Chart, clear all the event categories and select them again in this order: Future Events, Past Events, and Active Events.

Technical Requirements

For more information about the software and hardware requirements required for a successful deployment, see the *Technical Requirements for ArcSight Platform*.

Downloading Recon

Before you begin installing Recon, you must download necessary product installation packages. The installation package also includes the respective signature file, for validating that the downloaded software is authentic and not tampered by a third party.

To review the list of the files and versions to download for this release, see the *Release Notes for ArcSight Platform*.

Installing Recon

Micro Focus provides several options for deploying your Recon environment. For more information,see the *Administrator's Guide for ArcSight Platform* provided at the Recon Documentation site.

Add Report Permissions to Recon Roles

When you deploy Recon, the default roles common in the ArcSight Platform all receive the permissions to conduct searches. However, these roles do not receive any of the Report-based permissions. Only the *Report User* role, specific to Recon, has permission to perform all the reporting actions, including the reporting admin actions.

To ensure that Recon users can access both the Search and Report features, either add one or more of the Report permissions to the default roles or create new roles with the permissions. Ensure that any user assigned a reporting permission also has a Search or Admin permission. For more information about assigning roles and permissions, see the Help in the product.

> Reports do not function appropriately if a user's role has only Report-based permissions. For example, the default Report user role must have at least one Search- or Admin-based permission. (HERC-10003)

Licensing Information

For information about activating a new license, see the *Administrator's Guide for ArcSight Platform* provided at the Recon Documentation site.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos.
- The Micro Focus Community pages.

Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- *Administrator's Guide for ArcSight Platform*, which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.
- *User's Guide for Fusion 1.3 in the ArcSight Platform*, which is embedded in the product to provide both context-sensitive Help and conceptual information.
- Product Support Lifecycle Policy, which provides information on product support policies.

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment** or **support** on this topic at the bottom of any page in the HTML version of the documentation posted at the ArcSight Platform Documentation page or the documentation pages for the included products.

Legal Notices

© Copyright 2001 - 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.