Micro Focus Security ArcSight SOAR

Software Version: 3.1

ArcSight SOAR Release Notes

Document Release Date: May 2021
Software Release Date: May 2021

Legal Notices

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

https://www.microfocus.com

Copyright Notice

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 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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

ArcSight SOAR 3.1 Release Notes

This release introduces ArcSight SOAR 3.1.

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. We want to hear your comments and suggestions about the documentation available with this product. If you have suggestions for documentation improvements, click comment on this topic at the bottom of any page in the HTML version of the documentation posted at the SOAR Documentation page.

About ArcSight SOAR

The ArcSight SOAR is a Security Orchestration, Automation and Response (SOAR) platform. SOAR provides a single unified pane of glass for automation of recurrent security events.

SOAR ensures end-to-end mapping of all cyber security incidents of the organization, thereby increasing the agility and responsiveness of the teams in addressing these issues. The ArcSight SOAR also provides the flexibility to modify existing or add customized security tools as per the requirement and provide a robust security shield for your organization.

SOAR deploys within the **ArcSight Platform**. For more information about the other products available within the suite, see the ArcSight Platform Technical Requirements Guide.

Closed Issues

This release resolves the following issues:

Key	Description
100039	ESM Alert Source integration is not working if CEF version 1.0 is selected in the Forwarding Connector setup.
139695	SOAR fails to redeploy and displays the database connection error.
160062	ArcSight ESM listener does not workif TLS is configured in Forwarding Connector setup.
162004	If there is no scope item for a given condition, then case consolidation adds unrelated alerts.
162007	Autocomplete does not work in code editor on some Windows clients.
162113	Default Analyst (Incident Operator in the earlier version of the product) Role’s permissions are broken.
162123	ArcSight ESM cases are not created when base event enrichment fails.
166048	ESM Alert source severity mapping is not aligned with ESM event severities.
171389	Custom fields are not visible when editing after case creation.

What's New?

The following sections outline the key features and functions provided in this release. For more information about these enhancements, see the specific product documentation.

- SOAR Licensing
- Out Of the Box Playbooks
- FIPS Support
- MISP Threat Sharing Integration Capabilities
- MITRE ATT&CK
- Online Documentation

SOAR Licensing

In addition to **ESM** and **Recon** users, **ArcSight Intelligence** users are now entitled to use SOAR without an extra license.

ArcSight SOAR also supports non-autopass ESM licenses. Customers using ESM version 6.11 and later can also use the SOAR capability.

Out of the Box Playbooks

ArcSight SOAR provides out of the box playbook library which can be used as templates. Customers can customize and use playbooks prepared by Micro Focus experts.

FIPS Support

As part of the ArcSight Platform, all SOAR sub-components now support Federal Information Processing Standard (FIPS) and SOAR runs in FIPS-enabled mode by default.

MISP Threat Sharing Integration Capabilities

ArcSight SOAR is integrated with MISP Threat Sharing and provides both threat intelligence sharing and enrichment for artifacts capabilities.

MITRE ATT&CK

In alignment with the ArcSight MITRE ATT&CK content, SOAR now has the capability to understand the MITRE ATT&CK Technique ID set by layered analytics and displays the attack details in SOAR case. You can also run playbooks based on MITRE ATT&CK Technique ID.

Online Documentation

All ArcSight SOAR documents are removed from the SOAR application and has been moved to ArcSight Documentation.

Known Issues

The following issues are currently being researched for ArcSight SOAR 3.1.

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 , then select the appropriate product category.

FortiManager Integration Does Not Work With FortiManager Version 6

Issue: FortiManager integration does not work with FortiManager version 6.2.3.

Workaround: There is no workaround at this time.

Analysts Get Assigned to Super User Role During Initial Login

Issue: The analyst logging in to the ArcSight SOAR platform for the first time, gets assigned to the role of **Super User**.

Workaround: User roles and permissions are not synchronized with the ArcSight platform's role and permissions. Please update the analyst permissions from "**Configuration - Roles**" and "**Configuration - Users**".

Action History Page Filters Have Multiple Entry With Same Name

Issue: Integration capabilities with the same name are listed multiple-times in **Action History** page filters.

Workaround: There is no workaround at this time.

SSL-Certificate Related Error During Bluecoat Proxy SG Integration

Issue: Bluecoat Proxy SG integration displays SSL-certificate related error while updating URL database.

Workaround: In order to retrieve the blocked URL database, the Bluecoat Proxy SG connects to SOAR through HTTPS. If the SSL certificate used on CDF environment is not trusted by Bluecoat Proxy SG, then such error occurs. Use a valid SSL certificate or disable **Verify Peer** option for default device profile on Bluecoat Proxy SG device.

No Entries Displayed for Failed Enrichment Activities on Incident Timeline

Issue: Incident timeline does not show entries for failed enrichment activities.

Workaround: There is no workaround at this time.

Scope Item Property Does Not Get Updated Due to Caching

Issue: The value of **Scope item** property does not get updated, if the cached enrichment result is used for a scope item that is a part of another incident.

Workaround: Disabling cache while performing enrichments prevents the occurrence of such issues.

ArcSight Intelligence Alert Source and Enrichment are not Supported at this Time

Issue: The ArcSight Intelligence integration has issues related with supporting root tenants within SOAR.

Workaround: There is no workaround at this time.

Technical Requirements

For more information about the software and hardware requirements for your deployment and a tuned performance, see the ArcSight Platform Technical Requirements Guide.

Upgrading From SOAR 3.0

You must complete following steps before upgrading from SOAR 3.0 to any higher release:

1. **Clear the SOAR messages queue**: Navigate to **Configuration** > **Parameters** on ArcSight SOAR and set *ArcSightListnerEnabled* to **False**. This debars SOAR from receiving any new alert. Thus SOAR does not generate any new message, but consumes all the queued ones.
2. **Monitor SOAR messages**: You can monitor the status of SOAR messages at `# TYPE jms_queue_size` gauge of https://${fusionhost}/soar/api/manage/prometheus (to access this URL, you must have enabled SOAR in ESM). After SOAR consumes all the message, you can proceed with the upgrade procedure.

> Note: The above procedure must be followed to upgrade from SOAR 3.0 only.

Licensing Information

ArcSight SOAR capabilities are license locked and require either the ESM , Intelligence or Recon license key to be present in the CDF cluster autopass license server. For information about activating a new license, see the ArcSight Platform Administrator's 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 ArcSight SOAR Release Notes (SOAR 3.1)

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!