

# Micro Focus Security SOAR

Software Version: 3.0.0

## ArcSight SOAR Release Notes

Document Release Date: December 2020

Software Release Date: December 2020

### Legal Notices

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

<https://www.microfocus.com>

### Copyright Notice

© Copyright 2020 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 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:

[ArcSight Product Documentation on the Micro Focus Security Community](#)

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

# ArcSight SOAR 3.0.0 Release Notes

This release introduces ArcSight SOAR 3.0.0.

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](#)
- [What's New?](#)
- [Known Issues](#)
- [Technical Requirements](#)
- [Installing SOAR](#)
- [Licensing Information](#)
- [Contacting Micro Focus](#)
- [Legal Notice](#)

# 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](#).

# What's New?

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

- ["Deployment on CDF Platform" below](#)
- ["SOAR Licensing" below](#)
- ["Fusion UI Integration " below](#)
- ["Improved Plugin Development Environment" below](#)
- ["New Integration Plugin Upload" on the next page](#)

## Deployment on CDF Platform

With this release, the ArcSight SOAR will now run on ArcSight Platform (CDF). The deployment of SOAR on ArcSight Platform enables an easy and quick installation and configuration of ArcSight SOAR with containerization.

## SOAR Licensing

All **ESM** and **Recon** users are now entitled to use SOAR without an extra license. There is no license charge associated with SOAR capabilities now.

## Fusion UI Integration

In order to complement the integration to ArcSight Platform, SOAR is now accessible within the Fusion UI with a single sign-on. All capabilities of ArcSight Platform can now be accessed in Fusion User Interface.

## Improved Plugin Development Environment

The ArcSight SOAR now provides you with an environment to develop new plugins for easier automation. This can be achieved using the remote debugging and auto complete feature of code editor.

## New Integration Plugin Upload

With the new plugin upload interface, you can upload your own plugin to SOAR. The SOAR capability can guide the new plugins through the required configuration.

# Known Issues

The following issues are currently being researched for ArcSight SOAR 3.0.0.

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" below](#)
- ["Analysts Get Assigned to Super User Role During Initial Login" below](#)
- ["Action History Page Filters Have Multiple Entry With Same Name" on the next page](#)
- ["SSL-Certificate Related Error During URL Database update at Bluecoat Proxy SG Integration" on the next page](#)
- ["No Entries Displayed for Failed Enrichment Activities on Incident Timeline " on the next page](#)
- ["Plugin Script Used By Integration Gets Deleted From Customization Library" on the next page](#)
- ["Scope Item Property Does Not Get Updated Due to Caching" on page 9](#)
- ["SOAR-WEB-APP Container Crashes After SOAR Capability Redeployment" on page 9](#)

## FortiManager Integration Does Not Work With FortiManager Version 6

**Issue:** FortiManager integration is not working 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 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 URL Database update at 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 occur. 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.

## Plugin Script Used By Integration Gets Deleted From Customization Library

**Issue:** Plugin script used by integration gets deleted from Customization Library.

**Workaround:** There is no workaround at this time. Restarting SOAR service re-creates the plugin script.



## 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.

## SOAR-WEB-APP Container Crashes After SOAR Capability Redeployment

**Issue:** After redeployment of SOAR capability soar-web-app container crashes with the following log message:


**FATAL: password authentication failed for user soar**

**Workaround:** Perform following actions:

 Warning: Performing these steps will delete all data created by SOAR users.

1. Get into shell of the running itom-postgresql-default pod:

```
kubectl exec -it -n core itom-postgresql-default-xxxxxxxx-xxxxx -c itom-postgresql-default -- bash
```

 Note: The alphanumeric value in the name of the pod will vary. Look for "kubectl get pods -n core".

2. Move postgres configuration file to backup and create a new one for temporal use:

```
mv $PGDATA/pg_hba.conf $PGDATA/pg_hba.org
tee $PGDATA/pg_hba.conf <<-'EOF'
> local all postgres trust
> host all postgres 0.0.0.0/0 md5
> EOF
```

3. Restart the postgres with temporal configuration:

```
gosu postgres pg_ctl reload -D "$PGDATA"
```

4. Log in to postgres:

```
psql --dbname=defaultdb --username=postgres
```

5. Run the following queries to delete user and schema.

```
DROP DATABASE soar;
```

```
DROP USER soar;
```

6. Exit the postgres with \q.

7. Overwrite temp configuration with original conf file:

```
mv $PGDATA/pg_hba.org $PGDATA/pg_hba.conf
```

8. Restart postgres with original data:

```
gosu postgres pg_ctl reload -D "$PGDATA"
```

9. Exit itom-postgresql-default container with **exit** command.

Wait for soar-web-app pod to crash and restart again for the database to get automatically populated.

# 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](#).





# Licensing Information

ArcSight SOAR capabilities are license locked and require either the ESM 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 3.0.0)**

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 [arcsight\\_doc@microfocus.com](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!