Micro Focus Security ArcSight SOAR

Software Version: 3.2

ArcSight SOAR Release Notes

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

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

https://www.microfocus.com

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

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 3.2 Release Notes

This release introduces ArcSight SOAR 3.2.

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
191780	Column name is not displayed if ESM Active list has only one column.
191811	The ArcSight Intelligence integration has issues related with supporting root tenants within SOAR.
241819	SOAR uses its own UI Sesion Time Out configuration instead of ArcSight Platform timeout value.
320003	Custom case field is not set if case is created by automation.
325044	Lock User capability in Active Directory integration must be Disable User.
326079	FortiManager integration does not work with FortiManager version 6.2.3 and later.
335018	UI corrections in Top Playbooks Executed, Case Timeline and Case Breakdown dashboard widgets.
350068	Listing tags in McAfee EPO integration gives error.
354018	Enrichment cache mechanism is not working
364152	Advanced Mail Send capability configuration throws exception in workflow editor.
371022	SOAR actions fail if there’s Unassigned active lists on ESM.

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.

Cloud Native Deployment

You can now deploy and configure SOAR in the following cloud environments:

- **Azure** - Leverages the capabilities of the Microsoft Azure cloud platform.
- **Amazon Web Services (AWS)** - Leverages its cloud-native services and capabilities.

For more information, see "Setting Up Your Azure Deployment Architecture" and "Setting Up Your Deployment Architecture (Amazon Web Services)" in the *Administrator's Guide for ArcSight Platform*.

New Integration Plug-ins

The following new integration plug-ins are added to ArcSight SOAR 3.2:

Integration Plug-in	Description
Fortinet Forti Manager v2	New Forti Manager integration plugin supports Forti Manager JSON-RPC API (version 6.x and 7.x) for managing firewall addresses and address groups.
Micro Focus IT Service Manager	Integration plugin for creating and managing incident records on Service Manager.

Integration Plug-in	Description
Micro Focus UCMDB	Integration plugin for enriching CI information from UCMDB.
Microsoft Azure Active Directory	Enrichment and action capabilities to leverage Microsoft's cloud-based IAM solution.
Microsoft Graph Security	Integration plugin for querying and updating alerts through Microsoft Graph Security API.
MxToolbox	Integration plugin for checking domain MX and blacklist status on MxToolbox service.
Trend Micro Vision One	Integration plugin for querying and responding attacks on Trend Micro Vision One threat defense platform.
Udger	Enrichment plugin for querying User-Agent data.

Out-of-the-Box Plug-ins

The following integration plug-ins published previously on the ArcSight Marketplace are now out-of-the-box plug-ins:

Integration Plug-in	Description
AbuseIPDB	IP enrichment capabilities with AbuseIPDB API.
APIVoid	Integration plugin for APIVoid API service for threat analysis and threat detection and prevention with IP, Domain, URL and Email enrichment capabilities.
Amazon S3	Integration plugin for Amazon S3 object storage service for bucket operations.
Cisco Firepower Management Center	Cisco Firepower Management Center Integration plugin for blocking IP addresses and URLs.
CyThreat Threat Intelligence	Integration plugin for enriching IP addresses, domains, and file hashes from CyThreat Threat Intelligence service.
EmailRep.io	Integration plugin for enriching email addresses on EmailRep.io web service.
Have I Been Pwned?	Enrichment capabilities for checking accounts and domains through data breach databases.
Ipinfo	IP Query enrichment capability using IPinfo web service.
Jira	Bi-directional integration with Jira for case/ticket operations.
Okta	Integration plugin for enrichments and actions on Okta IAM solution.
ServiceNow	Bi-directional integration with ServiceNow for case/ticket operations.
URLScan.io	Integration plugin for enriching URLs from URLScan.io web service.

Updated Integration Plug-ins

The following integration plug-ins are updated for this release:

Integration Plug-in	Description
Amazon IAM	New enrichment and action capabilities have been added for user & group enrichment and taking response actions for users.
MISP	More descriptive messages are shown when queried IP or event not found on MISP.
Virus Total	URL Scan capability has been improved to handle result returned by Virus Total for previously-unknown URLs.

Migrated Reports

This release provides migration of following reports to platform reporting:

- Open Cases
- Closed Cases
- Integration History
- Integration Summary

STIX Support

This release supports exporting and importing of the case scope items in STIX sharable format.

Allowed IP Address Field

The **Allowed IP address** field is now removed from the ArcSight ESM alert source configuration.

Default Email Notification Templates

This release enhances the **Default Email Notification Template**, in the **Configuration** < **Customization Library** tab of SOAR application, to cover a wide range of use cases.

Added New Default Case Status

SOAR now provides following new default case statuses for case configuration:

- Duplicate
- False Positive
- Resolved

Trigger Workflow Decision Element

The **Trigger Workflow Decision Element** now supports **Previous Severity** and **New Severity** conditions.

Known Issues

The following issues are currently being researched for ArcSight SOAR 3.2.

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.

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. You must 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.

ESM Does Not Forward the Correlated Events to SOAR in AWS Environment

Issue: The Application Load Balancer (ALB) does not forward the correlated events from ESM to SOAR on AWS environment.

Workaround: If the ArcSight Platform is installed on AWS and ESM on a different VPC, use a Network Load Balancer (NLB) instead of an Application Load Balancer (ALB) on AWS as the ALB does not support TCP communication channel required for sending correlated events from ESM to SOAR.

SOAR Case Links in INetSoft Reports are Not Working

Issue: SOAR Case links in INetSoft Report are not working as expected in the current release will be fixed in the next release.

Workaround: . we can manually copy a case id in report and search it in SOAR case page.

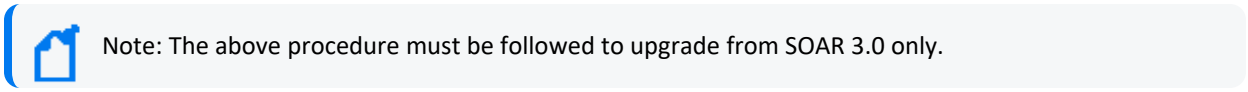
Technical Requirements

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.

Undeploying SOAR for Instaling and Upgrading to SOAR 3.2

SOAR is now moved under Fusion capability. Thus the resource definitions and patch command of SOAR related resources must be changed.

So, for the customers who already have SOAR pre-installed in their environments, they must undeploy SOAR first and then start the upgrade to create SOAR resources.

To undeploy SOAR:

1. Click **DEPLOYMENT**, and select **Deployments**.
2. Click the **Three Dots** (Browse) on the far right and select **Change**. A new screen is displayed in a separate tab.
3. Uncheck the boxes of Arcsight SOAR and click **NEXT** until you return to the **Deployment** page again.

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 3.2)

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!