Micro Focus Security ArcSight Platform

Software Version: 23.1

ArcSight Platform Release Notes

Legal Notices

Copyright Notice

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.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S.Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

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://www.microfocus.com/documentation/arcsight/

Contents

Release Notes for the ArcSight Platform 23.1

This release provides updates for and resolves previous issues in ArcSight Platform 22.1.x.

ArcSight Platform enables you to deploy a combination of security, user, and entity solutions into a single cluster within the OPTIC Management Toolkit (OMT) environment. The core services for this OMT environment, including the Dashboard and user management, are provided by a common layer called Fusion.

This release includes the following versions of the ArcSight Platform's primary components:

Component	Version
ArcSight Command Center for Enterprise Security Manager	7.6.4
Fusion	1.6.1
ArcSight Intelligence	6.4.4
ArcSight Recon	1.5.1
Transformation Hub	3.7.0
Layered Analytics	1.3.2

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.

What's New

This release includes the following enhancements:

Enhances the Search Capability

This release enhances the existing Search functionality and introduces several new functions that give you the power and flexibility to create robust searches of your data.

- "Inspect, Filter, and Display Events" below
- "Event Histogram to View Search Results" on the next page
- "Event Inspector for Viewing Event Details" on the next page
- "Home Tab – Your Overview of Search" on page 13
- "New Operators for Queries" on page 13
- "Operator Chaining for Powerful Queries" on page 14
- "Import and Export Search Queries or Criteria" on page 14
- "Upgrading to the New Search Capability" on page 15

Inspect, Filter, and Display Events

Search enhances how you can view and filter events.

- **Data histogram** – events-per-time segmented data graph that allows a Linear or Log scale data display. Additionally, clicking on a histogram bar or zooming in on a data range generates a list of matching events that are contained in that time period.
- **Event drill down** – clicking on a histogram bar generates a list of the matching events contained in the time period represented by that bar.
- **“Search expires in”** setting can be overridden for a particular session or saved search: the time duration can be extended to up to 120 hours from the 24 default.
- **Search result filter capability** – the Field Summary icon allows further filtering of a search result by selecting specific values from the actual results, weeding out results not containing that chosen value.
- **Event Inspector** – right-clicking an event in the Event Table allows users to open the Event Inspector. The Event Inspector provides additional details on an event for research purposes and additional functionality, such as the capability to export events and copy event URLs.

Event Histogram to View Search Results

The **Event Histogram** displays data in an events-per-time segmented data graph. The histogram lets you switch the display between a Linear Scale or a Log Scale. As you hover your pointer over the histogram, the bar color directly below the pointer changes and displays a tooltip of the day/date/time of that event range. Click a bar to view that event's information for a specific time range. Click again to deselect the bar.

Event Inspector for Viewing Event Details

The **Event Inspector** displays additional details on any event selected from the Search Results table. The Event Inspector opens in a panel and groups the event details by category, such as **Agent** and **Source**. In addition, the Event Inspector provides tools that allow you to control the data in the event details. Some options include: copying and sharing the event details via a URL, exporting the details to PDF or CSV, and applying an event detail to a current or new search. Use the Event Inspector to research further into events to help you find possible threats.

- When viewing event details in the Event Inspector, you can copy and share the Event Inspector URL. The URL will direct users to the event details page of the selected event. The Event Inspector URL contains the event's ID in the database (id) and global event ID (geid). See the table below for examples of the Event Inspector URL format. Use these formats to create the URL.

> The Event Inspector URL must contain the geid. If not, an error will display preventing you from accessing the event details.

URL Type	Example
Event Inspector URL	/rec/fusionSearch/eventsInspector/?eventsTable=Recon&id=5139791690&geid=3009625190352082178
Event Inspector URL (geid and id only)	/rec/fusionSearch/eventsInspector/?id=5139791690&geid=3009625190352082178
Event Inspector URL (geid only)	/rec/fusionSearch/eventsInspector/?geid=3009625190352082178

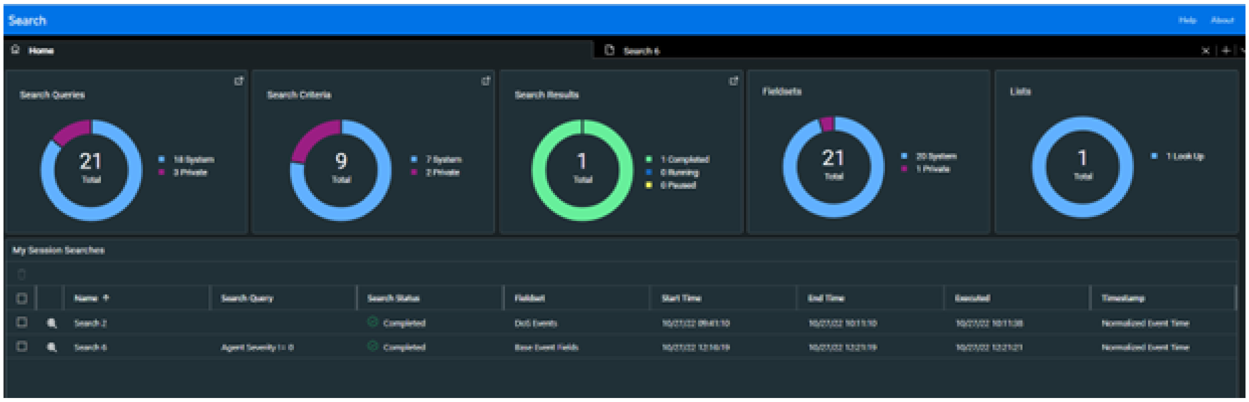
Home Tab – Your Overview of Search

The Search **Home** tab provides a high-level of your Search activity while also giving you immediate access to search features.

- A list of all your session (non-saved) searches
- Widgets that show the state of saved search queries, saved search criteria, saved search results, fieldsets, and lookup lists. (**Note**: You now need to access these items through the **Home** tab; they have been removed from the left navigation menu in the application.)

You can click ↗ in a widget to access that feature. For more information about using the **Home** tab, see the **Help** or "Viewing and Managing Your Searches" in the User's Guide to Fusion 1.6.1

Figure 1. Screenshot of the Search Home Tab



My Session Searches

□		Name ↑	Search Query	Search Status	Fieldset	Start Time	End Time	Executed	Timestamp
□	🔍	Search 2		Completed	DoS Events	10/27/22 09:41:10	10/27/22 10:11:10	10/27/22 10:11:38	Normalized Event Time
□	🔍	Search 6	Agent Severity != 0	Completed	Base Event Fields	10/27/22 12:16:19	10/27/22 12:21:19	10/27/22 12:21:21	Normalized Event Time

New Operators for Queries

You can use the following operators in your search queries:

- **chart (stats)** – a collection of aggregation (avg, sum, count, etc.) and span functions. Aggregation functions, such as avg, sum, count, etc., display the results of an aggregation operation in a results table. The span function lets you group events by a time field (such as Normalized Event Time) and a time bucket (such as 1 h, 5 m, and 30 s).
- **eval** – You can now use the following new eval functions:
  - **concat** – an eval function that lets you create a new string field that concatenates (or links together) strings from other fields
  - **if and case** – eval functions that expect a specified condition be met. An If() statement returns a value when a condition is True, or another value if it is False. A case expression runs through a set of given conditions and returns a value when the first condition is True then the software stops searching for other conditions.

    - **replace** – lets you replace the content (expressed as string) of a column and to return the value in a new column
    - **tonumber** – lets you convert string columns into floating point numbers so that the data can be applied to additional calculations
    - **tostring** – lets you convert columns into string values
- **rename** – assigns a new name to specified column in the fieldset
- **top and bottom** – lists the search results of the most common values for the specified field in a tabular form from the highest count value to the lowest (or vice versa)
- **where (filter)** – acts as a filter to display only results that fulfill a particular condition.
- **wheresql** – is similar to the 'where' clause, except that the filter clause is specified in SQL language. This gives you the advantage of using many of the database's native analytic functions, data-type-specific functions, aggregate functions, etc., to drilldown to just the data that complies with the conditions.

Operator Chaining for Powerful Queries

Construct complex searches by chaining together multiple search operators into a single query. During operator chaining, the search takes a set of results from one operation and uses them as input for the next operation. It gives you the flexibility to “slice and dice” data to extract and analyze it on a highly granular level.

Operator chaining works with pipeline search operators, such as **rename,eval**, **where (filter)**, **wheresql**, **top**, **bottom (rare)**, and **chart (stats)**.

Import and Export Search Queries or Criteria

You can import and export saved search queries and criteria by using a compressed JSON file. The saved search queries contain only the specified query expression, ready for you to load into a new search at any time. Saved search criteria combine a query expression and other Search elements such as fieldsets and the time range of the data that you want to retrieve. Note that the file must contain either queries or criteria, rather than both and cannot exceed 100 MB.

To support this enhancement, we added two permissions that you can assign to user roles:

- Import and Export Search Criteria
- Import and Export Search Queries

For more information about assigning permissions and managing roles, see the Help or see "Managing Users" in the User Guide for Fusion 1.6.1.

Upgrading to the New Search Capability

After you upgrade to the new Search capability, you might encounter minor issues with saved scheduled searches. The general workaround to prevent these issues is to save your previous results **before** the upgrade and recreate them for new search runs. Issues you might see include:

- For completed scheduled searches before and after an upgrade, the "number of results" column may not match actual search results or equal zero. But, you can still view the actual results by opening the completed scheduled searches.
- The results of scheduled searches that contain the **eval** operator may not load properly if you are loading them in a search results tab that is already open.

Introducing the Data Processing Monitoring Dashboard

The ArcSight Administrator now has an out of the box **Data Processing Monitoring** dashboard that contains a *Database Event Ingestion Timeline* widget useful for monitoring the rate of event ingestion into the database. This widget can also be used in custom dashboards by other users who are in a role that has the *Access Database Monitoring Overview* permission.

Changes to the Access Database Monitoring Permission

The earlier *Access Database Monitoring* permission is now split into the following two permissions:

1. **Access Database Monitoring Overview** - Grants users the ability to view the rate of event ingestion into the database.
2. **Access Database Monitoring Details** - Grants users the ability to view details about the high-level, summary information about the workload and health of the database.

> Roles that previously had the *Access Database Monitoring* permission will now have the *Access Database Monitoring Details* permission.

Updates for Fusion

This release includes security updates and enhancements for third-party components.

- "Component Updates" on the next page
- "Log4j Replaced in Fusion ArcMC" on the next page

Component Updates

This release updates the following third-party components to ensure that your system is secure from potential security vulnerabilities and attacks. These enhancements might also improve performance and stability or add features that enhance the development process.

Apache HTTP

Fixes vulnerabilities discovered in the previous version of the program. Apache HTTP is widely used in web servers and applications, and it is an important component of many IT infrastructures. Vulnerabilities in Apache HTTP can expose security threats, thus it is critical to remain up to speed on software upgrades and resolve any reported vulnerabilities as soon as possible.

Apache Tomcat

Provides critical security updates and bug fixes, ensuring that your system is secure from potential security vulnerabilities and attacks. This new version of Apache Tomcat also improves the performance and stability of your web applications, making it a more reliable and efficient platform for running critical web-based services.

Java

Provides critical security updates and bug fixes to the Java Runtime Environment (JRE) and Java Development Kit (JDK), ensuring that your system is secure from potential security vulnerabilities and attacks. This version of Java also improves performance, stability and adds new features which enhance the development process.

OpenSSL

Includes critical security updates and patches for known vulnerabilities, ensuring that your system is secure from potential threats and attacks. This new version also improves the performance and stability of your system, making it a more reliable and efficient platform for running critical applications and services.

PostgreSQL JDBC Driver

Provides critical bug fixes and new features to the Java application, ensuring that your system is stable and efficient. This new version of the PostgreSQL JDBC driver provides better performance and stability, enabling Java applications to connect with the PostgreSQL database seamlessly. The new version also improves the security of your database by providing critical security patches and fixes, protecting your database from potential security vulnerabilities and attacks.

Log4j Replaced in Fusion ArcMC

In this release, we replaced **Log4j 1.x** with **Reload4J** as it provides better performance, reliability, and security to the logging system of your application. Reload4J offers an enhanced logging system that addresses the vulnerabilities associated with Log4j.

For information about improvements in ArcMC, see the *ArcSight Management Center 3.2 Release Notes*.

Introduces Tamper-resistant Event Storage

The ArcSight Database now enforces the immutability of events once they are received from data sources, thus ensuring that not even the most privileged database administrator can modify or delete an event. This is achieved through a new database-native capability that rejects commands to modify or delete events for all users. This capability is built in such a way that it does not interfere with your configured retention policies.

Combined with the existing Event Integrity Check capability, the solution provides an end-to-end, long-term solution for ensure that events in the database will be exactly as reported by the device where the activity was observed.

Improves the Process for Migrating Data to the ArcSight Database from ArcSight Logger

This release improves the process that you follow to migrate data to the ArcSight Database from Logger. As part of this improved process, the database can decompress, read, and parse the data files that you migrate. This change moves most of the migration process to the database and Recon, rather than relying on your performing steps in Logger.

The migration process also includes the following enhancements:

- Enables you to initiate data migration after you have migrated all metadata
- Allows you to restore an incomplete migration from the last chunk of data obtained
- Eliminates failed searches that contain no events

New Dashboards for the Built-in Foundation Security Dashboards and Reports

This release includes two new dashboards under Foundation content to help you monitor security issues.

- Attacks and Suspicious Activity Overview
- Login Activity Overview

Adds Support for SmartConnector 8.4

This release adds support for SmartConnector 8.4. If you are using a previous version of SmartConnector, it is recommended that you upgrade to SmartConnector 8.4 to take advantage of security and other defect fixes. However, the ArcSight Platform continues to be compatible with older versions of the SmartConnector as specified at Technical Requirements for ArcSight Platform.

For more information about the most recent changes, enhancements, known limitations, and software fixes, see *Release Notes for ArcSight SmartConnector 8.4*.

Improves the SOAR Capability

This release includes the following enhancements to the SOAR capability.

- "New Integration Plug-ins for SOAR" below
- "New Reports and Widgets in SOAR" on the next page
- Enhancements

New Integration Plug-ins for SOAR

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

Integration Plug-in	Description
AWS Network Firewall	Integration plugin that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs)
Azure Network Security Groups	Integration plugin that is used to filter network traffic to and from Azure resources in an Azure virtual networks.
Crowdstrike Falcon	Integration plugin that allows organizations to leverage its lightweight agent.
CyberRes Galaxy Threat Accelerator	CyberRes Galaxy Threat Accelerator Program (GTAP) Plus is a Threat Intelligence feed, available as a subscription service from Micro Focus CyberRes.
FraudGuard.io	Integration plugin designed to provide an easy way to validate usage by continuously collecting and analyzing real-time internet traffic.
Intezer	Integration plugin that automates alert triage, incident response and threat hunting.
Microsoft Defender for Endpoint	Integration plugin designed to help enterprise networks prevent , detect, investigate, and respond to advanced threats.

New Reports and Widgets in SOAR

The following new reports and widgets are added to SOAR:

Widgets	Description
Analyst Performance Report	Analyst Performance reports on Inetsoft for selected analyst/analysts in a given time-frame.
Analyst Task Summary Report	The guideline/low fidelity mockups are attached. Layout, colours and fonts should be aligned with platform guidelines and other reports.
Case Load Widget	The widget shows the data for total open, assigned cases for the selected analysts (up to five) or top 5 members of a selected user group based on their average number of cases per week.
Productivity widget	The Productivity widget incorporates several elements related to SOC productivity such as Case Closure Velocity, Highest Velocity,Productivity by Analyst Groups

Enhancements

The following Enhancements are added to SOAR:

Enhancements	Description
Copy Scope Item value to Clipboard	An icon is added next to Scope Item value, to copy the value to clipboard.
Support for OAuth2 in SMTP/IMAP Authentication and Exchange EWS Integration	Supporting OAuth2 as an authentication mechanism in SMTP Integration (for both SMTP Auth and IMAP Auth) and also Exchange EWS Integration.

Updates for ArcSight Transformation Hub

This release includes the following updates for Transformation Hub:

- OpenSSL updated to address CVE vulnerabilities, a version of Log4j was replaced with Reload4j, the JRE has been updated, and the Spring expression library has been updated.
- Confluent Platform was updated.
- Resolved miscellaneous customer issues.

Technical Requirements

For more information about the software and hardware requirements required for a successful deployment, see the *Technical Requirements for ArcSight Platform*. These *Technical Requirements* include guidance for the size of your environment based on expected workload. Micro Focus recommends the tested platforms listed in this document.

> ⚠ Customers running on platforms not provided in the Technical Requirements or with untested configurations will be supported until the point Micro Focus determines the root cause is the untested platform or configuration. According to the standard defect-handling policies, Micro Focus will prioritize and fix issues we can reproduce on the tested platforms.

Downloading the ArcSight Platform Installation Files

You can download installation packages for the products in the ArcSight Platform from the Micro Focus Downloads website. The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

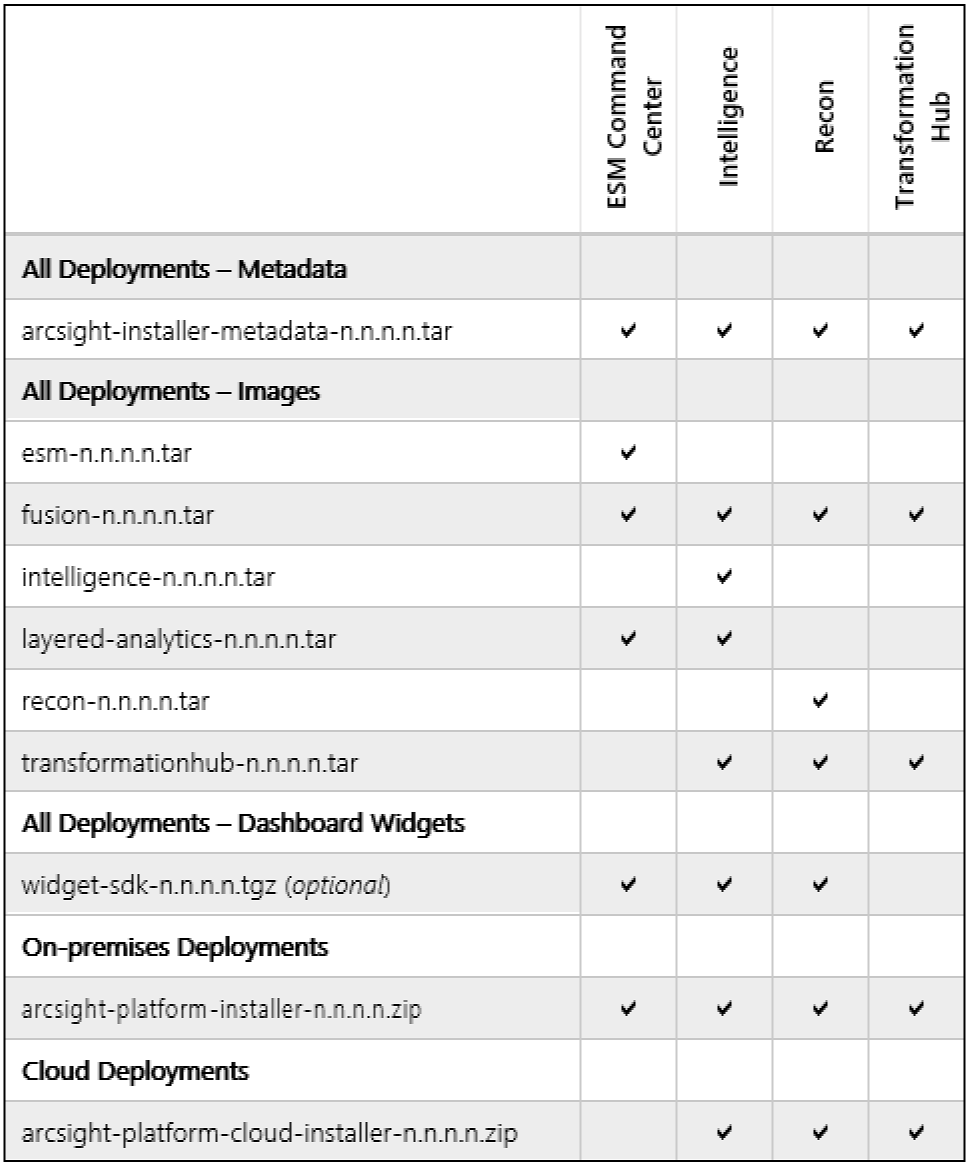
Micro Focus provides several options for deploying products in your environment. For more information about deploying a product, see the *Administrator’s Guide for ArcSight Platform*.

- "Understanding the Files to Download" below
- "Downloading the Installation Files" on page 24

> ⚠ Azure deployments can be upgraded to this version of the ArcSight Platform. However, to perform an Azure upgrade, it is necessary to contact Micro Focus Support before you begin.

Understanding the Files to Download

Download the installation packages described below. You only need one copy of each file, regardless of the products that you intend to deploy. For example, the Transformation Hub-based files are available with the ESM, Intelligence, and Recon software downloads, but you only need to download the files once. The Transformation Hub file set includes the packages for the OMT (OPTIC Management Toolkit) installer, the ArcSight Platform Installer, and the ArcSight database.



	ESM Command Center	Intelligence	Recon	Transformation Hub
All Deployments – Metadata				
arcsight-installer-metadata-n.n.n.n.tar	✓	✓	✓	✓
All Deployments – Images				
esm-n.n.n.n.tar	✓			
fusion-n.n.n.n.tar	✓	✓	✓	✓
intelligence-n.n.n.n.tar		✓		
layered-analytics-n.n.n.n.tar	✓	✓		
recon-n.n.n.n.tar			✓	
transformationhub-n.n.n.n.tar		✓	✓	✓
All Deployments – Dashboard Widgets				
widget-sdk-n.n.n.n.tgz (*optional*)	✓	✓	✓	
On-premises Deployments				
arcsight-platform-installer-n.n.n.n.zip	✓	✓	✓	✓
Cloud Deployments				
arcsight-platform-cloud-installer-n.n.n.n.zip		✓	✓	✓

To understand the files that you might need for your ArcSight Platform deployment, review the descriptions in the following table:

File Type	File Name	Description
All Deployments - Metadata	arcsight-suite-metadata-23.1.0.6.tar	Contains metadata for deployment of the OMT Management Portal
All Deployments - Images	esm-7.6.4.6.tar	Contains the images for deploying ESM Command Center
	fusion-1.6.1.6.tar and arcsight-fusion-1.6.1.6-license.txt	Contains the images for deploying the Fusion capability
	intelligence-6.4.4.6.tar and intelligence-6.4.4.6-License.txt	Contains the images for deploying the Intelligence capability
	layered-analytics-1.3.2.6.tar	Contains the images for deploying the Layered Analytics capability
	recon-1.5.1.6.tar	Contains the images for deploying the Recon capability
	transformationhub-3.7.0.6.tar	Contains the images for deploying the Transformation Hub capability
All Deployments - Dashboard Widgets	widget-sdk-3.2.14.tgz	(Optional) Provides the Widget Software Development Kit (the Widget SDK) that enables you to build new widgets or modify existing widgets for deployed applications such as ESM and Intelligence
On-premises Deployments	arcsight-platform-installer-23.1.0.8.zip	Contains files for installing the infrastructure where you want to deploy capabilities, including the following content: • OMT installer • ArcSight Database installer - db-installer_x.x.x.x.tar.gz • Configuration files for the Installer (on-premises only) and its example scripts You can find this file under Transformation Hub on the Software Downloads page
Cloud Deployments	arcsight-platform-cloud-installer-23.1.0.8.zip	Contains the installation files for deploying capabilities to Amazon Web Services and Azure

Downloading the Installation Files

To download and verify the signature of the downloaded files:

1. Log in to the computer where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the Micro Focus Downloads website along with their associated signature files (.sig).

   Micro Focus provides a digital public key that is used to verify that the software you downloaded from the Micro Focus software entitlement site is indeed from Micro Focus and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the Micro Focus Code Signing site. If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact Micro Focus Customer Support.
4. Begin the installation.

   For more information about the installation process for your particular environment, see the following topics in the *Administrator's Guide for ArcSight Platform*:

   - Checklist: Planning to Deploy the Platform
   - Checklist: Creating an On-premises Deployment
   - Checklist: Creating an AWS Deployment
   - Checklist: Creating an Azure Deployment

Connectors in Transformation Hub (CTH) and Collectors Now Deprecated

The Connectors in Transformation Hub (CTH) and Collectors are supported for the ArcSight Platform 23.1 release and are now deprecated. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024. CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Platform 23.1 release.

Known Issues

These issues apply to common or several components in your ArcSight Platform deploy. For more information about issues related to a specific product, please see that product's release notes.

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.

- Issues Related to Documentation
- "Issues Related to Database Upgrade" on the next page
- "Issues Related to Platform" on page 28
- "Issues Related to Reports Portal" on page 33
- "Issues Related to Arcsight Management Center" on page 36
- Issues Related to Intelligence
- "Issues Related to Search" on page 51
- "Issues Related to SOAR" on page 59
- "Issues Related to Transformation Hub" on page 60
- "Issues Related to Database Upgrade" on the next page

Issues Related to Documentation

OCTCR33I609183 — Using the COPY option for a command includes extra tags if text in the command is highlighted from a search

In documentation, performing a text search and then using the COPY button to copy highlighted search results will result in invalid commands if the text is pasted.

Workaround: If the command block you want to copy includes highlighted text, you must remove the highlights before copying. At the end of the URL, remove everything after the .htm text. Then click **Copy** to correctly copy the code in the gray box.

For example, if you searched for the text `vault_pod,` remove `?Highlight=vault_pod` from the URL (highlighted in example below):

https://wwwtest.microfocus.com/documentation/arcsight/arcsight-platform-23.1/arcsight-admin-guide-23.1/#deployment_manual/database_setup.htm?Highlight=vault_pod

Issues Related to Database Upgrade

- "OCTCR33I611095 — Issues Related to FIPS-enabled Database Node Fails" below
- "OCTCR33I617102 — Post-installation, You Might See an Error About Creating the Scheduler's Target Topic" below

OCTCR33I611095 — Issues Related to FIPS-enabled Database Node Fails

Issue: The FIPS-enabled database node fails to reboot, pre-install, handle installing prerequisites, and update. It is a problem with /etc/default/grub

Workaround: After running the ./arcsight-install --cmd preinstall, execute these commands on all database nodes:

```
resume=$(grep swap /etc/fstab | awk '{ print $1 }')

boot=$(grep '/boot' /etc/fstab | awk '{ print $1 }')

sed -i "s/ resume=UUID / resume=$resume /g" /etc/default/grub

sed -i "s/ boot=UUID / boot=$boot /g" /etc/default/grub


grub2-mkconfig -o /boot/grub2/grub.cfg
```

OCTCR33I617102 — Post-installation, You Might See an Error About Creating the Scheduler's Target Topic

Issue: After running the command to perform post-installation configurations, you might see the following error:

```
create scheduler under: default_secops_adm_scheduler

scheduler: create target topic

ERROR. Failed to create scheduler's target topic. For more details, please check log file.

Rolling back scheduler creation...
```

Workaround: Kill the pod "fusion-db-adm-schema-mgmt", example command:

```
kubectl delete pod -n <arcsight-installer-namespace> fusion-db-adm-schema-mgmt-xxxx
```

Wait for the pod to be completely running and then re-run the post-install again.

See Using ArcSight Platform Installer for an Automated On-Premises Installation in the Administrator's Guide to ArcSight Platform 23.1 for more installation information.

Issues Related to Platform

- "OCTCR33I112042 — Pods Might Not Run During Fusion Reinstall" below
- "OCTCR33I411123 — Event Integrity Query Indicates Insufficient Disk Space (AWS/Azure)" on the next page
- "OCTCR33I414022 — Event Integrity Query for Large Time Range Indicates Insufficient Disk Space (AWS/Azure)" on the next page
- "OCTCR33I470057 — Left Navigation Menu Items Do Not Reliably Display When Pods Restart or are Unresponsive" on the next page
- "OCTCR33I592057 — Logout Issues With SAML2" on the next page
- "OCTCR33I610053 — Event Integrity: The Check Progress Percentage Might Exceed 100%" on page 30
- "OCTCR33I534015 — Autopass container crashing with exception: relation "mysequence" already exists" on page 30
- "OCTCR33I736073 — Platform (OMT) Upgrade From 22.1 to 23.1 Failing During Uploading Images When Internal Certificate Was Renewed" on page 31
- "OCTCR33I751100 — fluentbit pod on some worker nodes may experience crashes" on page 32

OCTCR33I112042 — Pods Might Not Run During Fusion Reinstall

Issue: After you undeploy the Fusion capability and then redeploy Fusion into the same cluster, pods might remain in CrashLoopBackOff or PodInitializing status. The root cause of the issue is that the redeploy causes the system to forget the password for the rethinkdb database.

Workaround: Delete all of the files in the NFS folder before redeploying Fusion: arcsight-nfs/arcsight-volume/investigate/search/rethinkdb/hercules-rethinkdb-0. This will cause the rethinkdb database to be automatically recreated when Fusion is redeployed.

OCTCR33I411123 — Event Integrity Query Indicates Insufficient Disk Space (AWS/Azure)

Issue: There is an intermittent error of "insufficient disk space" when running an Event Integrity query in an Amazon Web Service (AWS) or Azure environment. There is a related issue for insufficient disk space.

Workaround: See View Event Integrity Check Results to help troubleshoot this issue.

OCTCR33I414022 — Event Integrity Query for Large Time Range Indicates Insufficient Disk Space (AWS/Azure)

Issue: If a large time range is selected (e.g., 1/31-2/22), there is an intermittent error of "Other" when running an Event Integrity query in an Amazon Web Service (AWS) or Azure environment. Known Issue OCTCR33I411123 is related issue for insufficient disk space behavior.)

Workaround: We recommend to select one day for event integrity check.

OCTCR33I470057 — Left Navigation Menu Items Do Not Reliably Display When Pods Restart or are Unresponsive

Issue: This defect tracks issues that affect the left navigation menu display until there is a proper fix. A related defect (OCTCR33I465016) for the Event Integrity User Interface features becoming disabled as a result of installing the 22.1.1 patch had only a temporary solution to the problem. For now, we intend to perform a periodic menu registration in the containers that register their menu items for nodejs containers and java containers and to revert certain files.

OCTCR33I592057 — Logout Issues With SAML2

Issue: Logout does not work properly when the product is configured to use an external SAML provider.

Workaround: Access the product UI (prior to login) using a private/incognito browser tab and, after logout, close all private browser tabs. This will ensure the session created at login is cleared from the browser.

OCTCR33I610053 — Event Integrity: The Check Progress Percentage Might Exceed 100%

Issue: Two cases where the check progress percentage might be misleading are:

1. If there are duplicate verification events, the check progress percentage might exceed 100% (because those events are often counted as duplicates).
2. When the search engine is restarted and new verification events are being ingested during the down time, the progress of checking verification events can be shown as 100% (even though the process is still running).

Workaround: If the status is "In Progress" with a percentage of 100% or greater, wait until the status shows as "Completed".

OCTCR33I534015 — Autopass container crashing with exception: `relation "mysequence" already exists`

Issue: Due to a race condition in a resource constrained cluster node, your autopass pod may crash with the following error:

```
kubectl logs -n arcsight-installer-xxxxx autopass-lm-xxxxxxxx-xxxx -c
autopass-lm -p
```

```
starting DB with paramaters
```

```
.. <> ...
```

```
org.postgresql.util.PSQLException: ERROR: relation "mysequence" already
exists
```

Workaround: If this occurs, use this procedure as a workaround.

1. Log into the `cdfapiserver` database pod to recover the password, and then log in with the password into the itom-default database as follows:

```
kubectl exec -it -n core cdfapiserver-postgresql-xxxxxxxxxx-xxxxx -c itom-
postgresql -- bash
```

```
# get_secret ITOM_DB_DEFAULT_PASSWD_KEY | cut -d "=" -f2-
# psql --host=itom-postgresql --dbname=defaultdbapsdb --username=postgres
```

2. List the relations to see the flag, remove it and exit the psql with "\q" and ssh pod with "exit"

```
defaultdbapsdb=# \ds public.*
```

```
drop sequence public.mysequence;
```

3. Restart the autopass pod using `kubectl delete pod`, and then make sure the container starts correctly with 2/2 Ready status.

```
kubectl delete pod -n arcsight-installer-xxxxx autopass-lm-xxxxxxxx-xxxx
```

OCTCR33I736073 — Platform (OMT) Upgrade From 22.1 to 23.1 Failing During Uploading Images When Internal Certificate Was Renewed

Platform (OMT) Upgrade from 22.1 to 23.1 may fail during uploading images when the internal certificate was renewed. The process may end with this error:

```
** Upgrade Infrastructure components ... (Step 8/10)
```

```
Update Apphub components images successfully.
```

```
Pushing apphub images ...
```

```
Failed to push apphub images...
```

Workaround: Use the following procedure.

1. Go to unpacked arcsight installer script subfolder.

```
cd <arcsight installer package>/installers/cdf/cdf/scripts/
```

2. Renew the certificates. In the below command, replace the <days> value with your own value in days. (Minimal value of one year, 365 days, recemented 3 years)

```
./renewCert --renew -t internal -V <days> -n core
```

3. Go to the charts folder. (Your command may differ if you do not use default values.)

```
cd /opt/arcsight/kubernetes/charts/
```

4. Store the renewed certificate and the key in variables.

```
cert=$(kubectl get secret kube-registry-cert -n core -o json|jq '.data."kube-registry.crt"' -r)
```

```
key=$(kubectl get secret kube-registry-cert -n core -o json|jq '.data."kube-registry.key"' -r)
```

5. Get the chart name with version and store it in a variable.

```
chart=$(helm list -n core -o json|jq -c -r '.[] | select( .name == "kube-registry" )'.chart)
```

6. Set the new certificate and key in chart.

```
helm upgrade kube-registry ${chart}.tgz -n core --set tls.cert=${cert} --set tls.key=${key} --reuse-values
```

7. Apply your changes.

```
kubectl rollout restart deployment kube-registry -n core
```

8. Wait until the cluster is healthy (and all pods are running).

```
kubectl get pods -A
```

> If some PODs are not running more then 30 minutes after applying the fix, you may delete them using `kubectl delete pod -n <namespace> <pod name>`

9. Run the upgrade again (it will continue where it failed).

```
cd <arcsignt installer package>/
```

```
arcsight-install --cmd upgrade
```

OCTCR33I751100 — fluentbit pod on some worker nodes may experience crashes

Issue: On some nodes due to higher pod count fluentbit may experience increased load and constantly crash with out of memory (OOM) condition, due to a strict default memory limit.

Workaround: This behavior is not affecting log collection and may be considered normal. The restart of a container after memory consumption threshold is reached is controlled by Kubernetes in a timely fashion and log collection activity is experiencing minimal downtime. No action is necessary by the user.

Issues Related to Reports Portal

OCTCR33I134098 — Edit Wizard Preview is Unavailable

Issue: When you edit an asset using the Edit Wizard option, you cannot preview the report or dashboard.

Workaround: To preview your changes, select the metadata option from the Edit Wizard.

OCTCR33I161014 — Dashboard Wizard Fails to Load All Data

Issue: When using the Dashboard wizard, the chart intermittently fails to load because the same type of data has been selected at the same time.

Workaround: When this issue occurs, select one event data from the left panel and use the **Full Editor** (located in top right corner) to continue creating the dashboard.

OCTCR33I162021 — Cannot Remove X/Y Fields from a Graph

Issue: In the chart editor, when you remove an X or Y field, the Reports Portal display an error message. This issue occurs intermittently.

Workaround: When this issue occurs, try again or avoid removing fields from the Axis.

OCTCR33I186007 — An Exported Report Might Have Format Issues

Issue: When using the Export Asset feature, the formatting for the reports might have issues such as dark backgrounds, dark fonts, and dark table cells.

Workaround: Manually change the formatting for the exported report.

OCTCR33I331194 — Reports and Dashboards Use UTC Time Zone

Issue: The start and end times for your reports and dashboards use UTC time instead of your local time zone.

Workaround : When you run a report or dashboard and pick start and end times, ensure they use the UTC time zone format.

OCTCR33I336023 — Operations Performed on an Open Admin Tab Do Not Complete After You Log Out From Another Capability (Recon or Reporting) Tab

Issue: Open two browser tabs, one with **Admin** or **Fusion User Management** (FUM) and another with any other capability (Reporting or Recon). If you log out from the capability tab, any subsequent operation performed on the **Admin** tab does not complete.)

Workaround: Refresh the browser to complete the log out process.

OCTCR33I372067 — Contract & Usage Page Throws an Ingress Router Error and Does Not Load

Issue: When the user tries to navigate from My Profile to Contract & Usage, the page throws an ingress router error message as follows and does not load:

```
The Route You Reach Does not Exist
Please check your router configuration and the path in your address bar.
```

Workaround: Refresh the page to load the Contract & Usage page.

OCTCR33I409268 — Reporting Shows an Error When Single Sign On Secrets are Changed (Azure)

Issue: Reporting runs into an Open id or HTTP 500 error when single sign on secrets are changed. The reporting app can take a few minutes to fully start, so this error does not happen right after applying the change.

OCTCR33I566085 — Network Chart Data Presented in Portions and Cut

Issue: The Network chart tends to truncate data, such as IP addresses, to the point where the displayed content is not useful.

Workaround: There is no workaround. Micro Focus recommends that you do not use the Network chart at this time.

OCTCR33I589121— Brush Option Does Not Highlight Parabox Charts

Issue: The brush option does not highlight parabox charts.

Workaround: There is no workaround at this time.

OCTCR33I71158 — Scheduled Tasks Do Not Allow Default Printer Selection

Issue: The default printer field is a textbox that allows any value instead of being a list of valid entries.

Issues Related to Arcsight Management Center

- "OCTCR33I612094 — Fusion ArcMC Throws 503 Error After Restoring Configuration Data (AWS, Azure and On-premises)" below
- " OCTCR33I408195 — Importing a Host File on Fusion ArcMC Points to a Different Log Folder " below
- "OCTCR33I408194 — Fusion ArcMC Session License Expiration" on the next page

OCTCR33I612094 — Fusion ArcMC Throws 503 Error After Restoring Configuration Data (AWS, Azure and On-premises)

Issue: After following the configuration data restoration process, opening Fusion ArcMC from the Fusion dashboard produces a **503 Service temporarily unavailable** error.

Workaround: Correct the permissions of the ArcMC folder by executing the following commands:

```
cd /mnt/efs/<nfs_folder>/
```

```
$ sudo chown -R 1999:1999 arcsight-volume/arcmc
```

```
$ kubectl delete pods -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)  $(kubectl get pods -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1) | grep arcmc | cut -d ' ' -f1)
```

OCTCR33I408195 — Importing a Host File on Fusion ArcMC Points to a Different Log Folder

Issue: When a user attempts to import a hosts file into Fusion ArcMC, they may encounter an issue where the log folder being pointed to does not match the Fusion ArcMC NFS. This mismatch can occur for a variety of reasons and can lead to confusion and difficulties for the user in accessing and interpreting the log data.

Workaround: No known workaround for this release.

OCTCR33I408194 — Fusion ArcMC Session License Expiration

Issue: When the Fusion license expires during a session, a spurious error message will be displayed: "Unable to retrieve CSRF token. Got status code:0". Click OK to dismiss this error.

Workaround: No known workaround for this release.

Issues Related to Intelligence

- "OCTCR33I494001 — Analytics Does Not Detect the Custom SQL Loader Scripts After the Intelligence Upgrade" on the next page
- "OCTCR33I606124 — Multi-step Upgrade From 21.1.x to 23.1.x Fails on Suite Upgrade to 23.1 (a Non-Cloud Release)" on page 40
- "OCTCR33I611096 — Analytics Fails to Load Data Sources Except for AD and Proxy" on page 40
- "OCTCR33I613042 — Intelligence Sharing URL Functionality Does Not Work if the User Does Not Have an Active Session" on page 41
- OCTCR33I616036 — If Not Already Logged into Fusion, the First Attempt to Log Directly Into Intelligence Dashboard Will Fail
- OCTCR33I400584 - Either the Intelligence Search API or Login to the Intelligence UI or both Fail with a Timeout Error (IOException: Listener Timeout) for Large Data Sets in the Database
- OCTCR33I399297 - Intelligence Search API Fails with a Timeout Error (esSocketTimeout exception) for Large Data Sets in the Database
- OCTCR33I401232 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Space Character
- OCTCR33I399665 - Elasticsearch and Logstash Pods Fail in an AWS Deployment Because of Permission Issues
- OCTCR33I604032 - Elasticsearch and Logstash Pods Fail in an Azure Deployment Because of Permission Issues
- OCTCR33I614051 - Logstash Pod Fails on Data Ingestion in AWS Deployment When Using Self-signed Certificates

- OCTCR33I378083 - Erroneous Warning about Recon License
- OCTCR33I614050 - Special Characters for Database Credentials
- OCTCR33I616054 - Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects
- OCTCR33I614042 - Daylight Savings Time
- OCTCR33I613048 - Repartition Percentage Threshold
- OCTCR33I614047 - Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container
- OCTCR33I614048 - Certificate Warnings in Logstash Logs
- OCTCR33I613050 - Installer Does Not Validate the Value You Specify for Elasticsearch Data Retention Period
- OCTCR33I614049 - Uninstalling Intelligence Does Not Delete All Files
- OCTCR33I613051 - Unable to Retrieve Indices When Elasticsearch Cluster is Unstable
- OCTCR33I401549 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Special Character
- OCTCR33I399647 - HTTP Status 400 - Bad Request

OCTCR33I494001 — Analytics Does Not Detect the Custom SQL Loader Scripts After the Intelligence Upgrade

Issue: For AWS and Azure deployments, after the Intelligence upgrade from 22.1.0 to 23.1, analytics does not detect the custom SQL loader scripts of the previous version of Intelligence. Instead, it proceeds with the default SQL loader scripts present in <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.12.4.27/

Workaround: Follow the steps below:

Step 1: Perform the following steps before the upgrade:

1. Launch a terminal session and as a root user, log in to the node where NFS is present.
2. Navigate to the following directory:

   ```
   cd /<arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/
   ```

3. Execute the following command to create the 1.1.9.1.9 directory:

   ```
   mkdir 1.1.9.1.9
   ```

4. Navigate to the following directory:

   ```
   cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0
   ```

5. Execute the following command to move the SQL loader scripts from <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0 to <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.1.9.1.9:

   ```
   mv *.md5 *.sql 1.1.9.1.9
   ```

6. Execute the following command to grant permissions to the 1.1.9.1.9 directory:

   ```
   chown -R 1999:1999 1.1.9.1.9
   ```

Step 2: Upgrade the Intelligence capability.

For more information, see Upgrading your Environment in the Administrator’s Guide for ArcSight Platform.

Step 3: Perform the following steps after the upgrade:

1. Run Analytics to start the next analytics run. For more information, see Running Analytics on Demand in the Administrator’s Guide for ArcSight Platform.
2. During the analytics run, the 1.12.4.27 folder is created in the following directory with the default SQL loader scripts:

   ```
   cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
   sql/0/1.12.4.27
   ```

3. (Conditional) If you have been using custom SQL loader scripts in 22.1.0, then the SQL loader scripts with inconsistent md5 sums between the current and previous versions are displayed in the Analytics logs. Perform the following steps to review and modify the SQL loader scripts:

   a. Execute the following command to check the logs of the analytics pod:

      ```
      export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
      pn=$(kubectl get pods -n $NS | grep -e 'interset-analytics' | awk '
      {print $1}')
      kubectl logs -f $pn -n $NS -c interset-analytics
      ```

   b. Review and add the necessary modifications to the new SQL loader scripts present in the following directory:

      ```
      cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
      sql/0/1.12.4.27
      ```

c. Update the md5 files with the md5 sums corresponding to the modified SQL loader scripts.

   - If you are upgrading from 22.1.0 to 23.1, execute the following command:

     ```
     cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
     sql/0/1.1.9.1.9
     ```

   - If you are upgrading from 22.1.2 to 23.1, execute the following command:

     ```
     cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
     sql/0/1.1.9.2.9
     ```

   Analytics is triggered automatically after all the SQL loader scripts with inconsistent md5 sums are updated.

OCTCR33I606124 — Multi-step Upgrade From 21.1.x to 23.1.x Fails on Suite Upgrade to 23.1 (a Non-Cloud Release)

Issue: When running a suite upgrade to 23.1.x, if you see the pop-up message "System error, please contact system administrator" do the following. Keep the log tailing by running "**kubectl logs -n core cdf-apiserver-xxxxxxxxx-xxxxx -c cdf-apiserver --follow | grep RuntimeException**" and re-try the Suite upgrade. It should return the line "**java.lang.RuntimeException: Failed apply suite config pod**" after you see the pop-up error message on the UI.

Workaround: Delete the suite-conf service by running "**kubectl delete svc -n core suite-conf-svc-arcsight-installer**" and re-try the upgrade using the **Deployments** panel in the **OMT Management Portal**.

OCTCR33I611096 — Analytics Fails to Load Data Sources Except for AD and Proxy

Issue: If the configuration for the data sources is set to "all" and the input data contains data from AD, Proxy, and other supported data sources, analytics loads only the AD and Proxy data sources and displays the following error message:

```
Exception in thread "main" java.lang.IllegalArgumentException: Config
validation failed: Missing option --action
```

As a result, analytics is unable to load the other data sources, such as Resource, Share, VPN, and Repository.

Workaround: Perform the following steps to specify each data source for the data source configuration:

1. Open a certified web browser.
2. Specify the following URL to log in to the CDF Management Portal: `https://<cdf_masternode_hostname_or_virtual_ip_hostname>:5443`.
3. Select **Deployment** > **Deployments**.
4. Click ... (Browse) on the far right and choose Reconfigure. A new screen will be opened in a separate tab.
5. Click **Intelligence**.
6. In the **Analytics Configuration - Database** section, modify **Database Loader Data Sources** field's value to `ad,pxy,res,sh,vpn,repo`.

OCTCR33I613042 — Intelligence Sharing URL Functionality Does Not Work if the User Does Not Have an Active Session

Issue: Intelligence Sharing URL functionality does not work if user does not have an active session. If a user is not logged in, then after a successful sign in, the shared URL lands on the default interset landing page instead of the shared page.

Workaround: When sharing a link using the Share Short URL functionality in Intelligence, the recipient needs to be logged into an active session (as described in Known Issue OCTCR33I616036) in order to be taken to the intended page.

OCTCR33I616036 — If Not Already Logged into Fusion, the First Attempt to Log Directly Into Intelligence Dashboard Will Fail

Issue: Logging in to Intelligence dashboard `https://<hostname>/interset` by using a web browser fails in the first attempt.

Workaround: Perform the following steps:

1. Log in to Fusion dashboard `https://<hostname>/dashboard`.
2. Navigate to **Insights** > **Entities at Risk**. It will redirect you to the Intelligence dashboard.

After performing the above steps, subsequent attempts to log in to the Intelligence dashboard `https://<hostname>/interset` will be successful.

OCTCR33I400584 - Either the Intelligence Search API or Login to the Intelligence UI or both Fail with a Timeout Error (IOException: Listener Timeout) for Large Data Sets in the Database

Issue: Either the Intelligence Search API or login to the Intelligence UI or both fail with the IOException: Listener Timeout after waiting for 30 seconds while querying a large data set (approximately 2 billion records) in the database.

Workaround: Perform the following steps:

1. Open a certified web browser.
2. Log in to the CDF Management portal as the administrator.

   `https://<virtual_FQDN>:5443`
3. Click **CLUSTER** > **Dashboard**. You are redirected to the **Kubernetes Dashboard**.
4. In **Namespace**, search and select the `arcsight-installer-xxxx` namespace.
5. In **Config and Storage**, click **Config Maps**.
6. Click the filter icon, then search for `investigator-default-yaml`.
7. In the **db-elasticsearch** section of the YAML tab, modify the **esListenerTimeout** value based on the data size.

   For example, if the Intelligence search API takes 150 seconds to retrieve data from the database, then ensure that you set the **esListenerTimeout** value to more than 150 seconds to avoid the exception.

   > **Note:** Ensure that you set the **esListenerTimeout** value in milliseconds.
8. Click **Update**.
9. Restart the interset-api pods:
   a. Launch a terminal session and log in to the master or worker node.
   b. Execute the following command to retrieve the namespace:

   ```
   export NS=$(kubectl get namespaces | grep arcsight|cut -d ' ' -f1)
   ```

   c. Execute the following commands to restart the interset-api pods:

   ```
   kubectl -n $NS scale deployment interset-api --replicas=0
   ```

   ```
   kubectl -n $NS scale deployment interset-api --replicas=2
   ```

OCTCR33I399297 - Intelligence Search API Fails with a Timeout Error (esSocketTimeout exception) for Large Data Sets in the Database

Issue: Intelligence Search API fails with the esSocketTimeout exception while querying a large data set (approximately 4 billion records) in the database, along with ingestion and analytics running simultaneously.

Workaround: Perform the following steps:

1. Open a certified web browser.
2. Log in to the CDF Management portal as the administrator.

   `https://<virtual_FQDN>:5443`
3. Click **CLUSTER** > **Dashboard**. You are redirected to the **Kubernetes Dashboard**.
4. In **Namespace**, search and select the `arcsight-installer-xxxx` namespace.
5. In **Config and Storage**, click **Config Maps**.
6. Click the filter icon, then search for `investigator-default-yaml`.
7. In the **db-elasticsearch** section of the YAML tab, modify the **esSocketTimeout** value based on the data size.

   For example, if the Intelligence search API takes 150 seconds to retrieve data from the database, then ensure that you set the **esSocketTimeout** value to more than 150 seconds to avoid the exception.

   > **Note:** Ensure that you set the **esSocketTimeout** value in milliseconds.
8. Click **Update**.
9. Restart the interset-api pods:
   a. Launch a terminal session and log in to the master or worker node.
   b. Execute the following command to retrieve the namespace:

   ```
   export NS=$(kubectl get namespaces | grep arcsight|cut -d ' ' -f1)
   ```

   c. Execute the following commands to restart the interset-api pods:

   ```
   kubectl -n $NS scale deployment interset-api --replicas=0
   ```

   ```
   kubectl -n $NS scale deployment interset-api --replicas=2
   ```

OCTCR33I401232 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Space Character

Issue: In the **CDF Management Portal** > **Configure/Deploy** page > **Intelligence** > **KeyStores** section > **KeyStore Password** field, if you specify a password that starts with a space character, most pods enter into the CrashLoopBackOff state.

Workaround: For the **KeyStore Password** field, do not specify a password that starts with a space character.

OCTCR33I399665 - Elasticsearch and Logstash Pods Fail in an AWS Deployment Because of Permission Issues

Issue: When configuring the EFS for deploying Intelligence in AWS, even after setting the permissions in the arcsight-volume folder to 1999:1999, the Elasticsearch and Logstash pods enter into a CrashLoopBackOff state from a Running state.

Workaround: If the pods enter into the CrashLoopBackOff state, perform the following steps:

1. Log in to the bastion host.
2. Navigate to the following directory and set the permissions to 1999:1999 again:

   ```
   cd /mnt/efs/<parent_folder_name>
   chown -R 1999:1999 arcsight-volume
   ```

3. Wait for the Elasticsearch and Logstash pods to come up.
4. If the pods enter into a Running state and then into a CrashLoopBackOff state, keep repeating steps 2 and 3 till the pods are stable, that is, they do not move from the Running state to the CrashLoopBackOff state.

OCTCR33I604032 - Elasticsearch and Logstash Pods Fail in an Azure Deployment Because of Permission Issues

Issue: When preparing the NFS server for deploying Intelligence in Azure, even after setting the permissions in the arcsight-volume folder to 1999:1999, the Elasticsearch and Logstash pods enter into a CrashLoopBackOff state from a Running state.

Workaround: If the pods enter into the CrashLoopBackOff state, perform the following steps:

1. (Conditional) If the NFS server is not the Azure NetApp Files server, do the following:
   a. From your jump host, SSH to the NFS VM using its private IP address.
   b. Log in to the NFS VM.
   c. Become root.
   d. Navigate to the following directory and set the permissions to 1999:1999 again:

```
cd /nfs
chown -R 1999:1999 arcsight-volume
```

2. (Conditional) If the NFS server is the Azure NetApp Files server, do the following:
   a. From your jump host, become root.
   b. Execute the following command to retrieve the directory on which the Azure NetApp Files server is mounted:

```
df -h
```

   The directory corresponding to <IP address of the NetApp Files server>/volume is the directory on which the Azure NetApp Files server is mounted.

   c. Navigate to the directory retrieved in the previous step and set the permissions to 1999:1999 again:

```
cd /<Azure NetApp Files server directory>
chown -R 1999:1999 arcsight-volume
```

3. Wait for the Elasticsearch and Logstash pods to come up.
4. If the pods enter into a Running state and then into a CrashLoopBackOff state, keep repeating steps 4 and 5 till the pods are stable, that is, they do not move from the Running state to the CrashLoopBackOff state.

OCTCR33I614051 - Logstash Pod Fails on Data Ingestion in AWS Deployment When Using Self-Signed Certificates

Issue: In an AWS deployment of Intelligence, when data is ingested, the Logstash pod enters into a CrashLoopBackOff state from a Running state. This issue occurs if you have configured CDF in the cloud (AWS) environment with self-signed certificates.

Workaround: Perform the following steps:

1. Connect to the bastion.
2. Execute the following command to scale down the Logstash nodes:

   ```
   kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
   scale statefulset interset-logstash --replicas=0
   ```

3. Execute the following command to modify the logstash-config-pipeline configmap:

   ```
   kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
   edit configmaps logstash-config-pipeline
   ```

4. Update the value of the **verify_mode** field from "verify_peer" to "verify_none".
5. Save the configmap.
6. Execute the following command to scale up the Logstash nodes:

   ```
   kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
   scale statefulset interset-logstash --replicas=<number_of_replicas>
   ```

OCTCR33I378083 - Erroneous Warning about Recon License

Issue: In an ArcSight Platform deployment that has Intelligence with an MSSP license, you will receive the usual notifications that the licenses are about to expire. However, if the MSSP license expires, the Platform erroneously displays a warning that the Recon license has expired even though Recon is not deployed. This issue does not occur when Recon is deployed, with or without the MSSP license.

Workaround: There is no workaround for this issue.

OCTCR33I614050 - Special Characters for the Database Credentials

Issue: The following characters are not supported for the database credentials:

- Whitespace
- Single quotes

Workaround: There is no workaround at this time.

OCTCR33I616054 - Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects

Issue: When anomalies are identified because few users access a specific project, and one or more of the users are flagged as bots, changing the BOT users to NOTBOT users — and therefore increasing the number of non-bot users accessing the project — will not impact the project's identification as 'inactive'. Anomalies will therefore continue to be identified when the project is accessed, even though more non-bot users are now regularly accessing the project.

Workaround: There is no workaround at this time.

OCTCR33I614042 - Daylight Savings Time

Issue: During the weeks immediately following Daylight Savings Time (DST) clock changes, you may observe an increase in reported Normal Working Hours anomalies. These anomalies, which are due to automatic software clock changes, will usually have risk scores of zero (0), and are reflective of the perceived Normal Working Hours pattern shift.

Workaround: There is no workaround needed.

OCTCR33I613048 - Repartition Percentage Threshold

Issue: In the **CDF Management Portal>Configure/Deploy** page **>Intelligence**, when you specify a value for the **Repartition Percentage Threshold** field, the installer does not validate the value. However, Intelligence Analytics fails if the value is not set between 0.7 and 1.0 as stated in the tooltip.

Workaround: Ensure that you set a value between 0.7 and 1.0.

OCTCR33I614047 - Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container

Issue: In the **CDF Management Portal>Configure/Deploy** page **>Intelligence**, when you change the value of the **HDFS NameNode** field to deploy the HDFS NameNode container on another worker node, the older instance of the HDFS NameNode container goes into a pending state instead of being terminated.

Workaround: Perform the following steps after changing the value in the field:

1. In the CDF Management Portal, click **Cluster>Nodes**.
2. Click the [-] icon for the **intelligence-namenode:yes** label present on the worker node.
3. From **Predefined Labels**, drag and drop the **intelligence-namenode:yes** label to the worker node to which you want to add it. Ensure the worker node matches the new value you specified in the **HDFS NameNode** field.
4. Configure the database with HDFS. For more information, see the "Configuring the Database with HDFS for Intelligence" section in the Administrator's Guide for ArcSight Platform.
5. Restart the HDFS DataNodes. Do the following:

   a. Launch a terminal session and log in to a worker node where an HDFS DataNode is deployed.

   b. Execute the following commands:

   ```
   NAMESPACE=$(kubectl get namespaces | grep arcsight-installer | awk '{
   print $1}')
   ```

   ```

   kubectl get pods -n $NAMESPACE | grep -e 'hdfs\|interset-analytics' |
   awk '{print $1}' | xargs kubectl delete pod -n $NAMESPACE --force --
   grace-period=0
   ```

OCTCR33I614048 - Certificate Warnings in Logstash Logs

Issue: When you view the Logstash logs, you might come across the following warnings:

- ** WARNING ** Detected UNSAFE options in elasticsearch output configuration!
- ** WARNING ** You have enabled encryption but disabled certificate verification.
- ** WARNING ** To make sure your data is secure change :ssl_certificate_vertification to true

Workaround: There is no workaround needed. You can ignore these warnings as there is no impact in the functionality.

OCTCR33I613050 - Installer Does Not Validate the Value You Specify for Elasticsearch Data Retention Period

Issue: In the **CDF Management Portal** > **Configure/Deploy** page > **Intelligence** > **Elasticsearch Configuration** section, the installer does not validate the value you specify for the **Elasticsearch Data Retention Period** field. The tool-tip for the **Elasticsearch Data Retention Period** field suggests that you should specify a value greater than 30 for indices retention. However, there is no validation preventing you from entering a value that is less than 30. If you specify a value that is less than 30, the value for **Elasticsearch Data Retention Period** will be set to the minimum default value of 30 days.

Workaround: There is no workaround at this time.

OCTCR33I614049 - Uninstalling Intelligence Does Not Delete All Files

Issue: When you uninstall Intelligence, some files are not deleted from the `/opt/arcsight/k8s-hostpath-volume/interset` directory of all the worker nodes. Therefore, when you install Intelligence again, the intelligence pods stay in Init state.

Workaround: Before installing Intelligence again, manually delete the remaining files from the `/opt/arcsight/k8s-hostpath-volume/interset` directory of all the worker nodes. If you have modified the value of the **Elasticsearch Node Data Path** field in the **Intelligence** tab of the CDF Management Portal, check and manually delete the remaining files from the directory you have specified for the **Elasticsearch Node Data Path** field for all the worker nodes.

OCTCR33I613051 - Unable to Retrieve Indices When Elasticsearch Cluster is Unstable

Issue: When your Elasticsearch Cluster is not stable and you run the reindex jobs, the jobs run successfully but display the following error message in the job details:

```
Error occurred while getting all ES indices: Request cannot be executed; I/O
reactor status: STOPPED
```

Workaround: You must restart the Elasticsearch cluster to refresh the Elasticsearch environment.

OCTCR33I401549 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Special Character

Issue: In the **CDF Management Portal** > **Configure/Deploy** page > **Intelligence** > **KeyStores** section > **KeyStore Password** field, if you specify a password that starts with a special character, most pods enter into the CrashLoopBackOff state.

Workaround: For the **KeyStore Password** field, do not specify a password that starts with a special character.

OCTCR33I399647 - HTTP Status 400 - Bad Request

Issue: If the cookie request size exceeds the cookie size limit, your screen displays a **HTTP Status 400 - Bad Request** message when you try to open the CDF Management Portal.

Workaround: Perform the following steps:

1. Open a certified web browser.
2. Login to the Management portal as the administrator.
   `https://<virtual_FQDN>:5443`
3. Click **CLUSTER** > **Dashboard**. You will be redirected to the **Kubernetes Dashboard**.
4. Under **Namespace**, search and select the `arcsight-installer-xxxx` namespace.
5. Under **Config and Storage**, click **Config Maps**.
6. Click the filter icon, and search for `investigator-default-yaml`.
7. Click the three dot icon and select **Edit**.
8. In the **YAML** tab, under the `interset-cookie` section, add the following:

   ```
   path: /interset;SameSite=Lax
   ```

9. Click **Update**.
10. To apply the changes, restart the `interset-api` pods by either deleting the `interset-api` pods or scaling down the `interset-api` deployments using the following commands:

    ```
    kubectl delete pods -n <arcsight-installer-namespace> <interset-api-pod-
    1> <interset-api-pod-2>
    ```

    OR

```
kubectl scale deployment -n <arcsight-installer-namespace> interset-api -
-replicas=0
kubectl scale deployment -n <arcsight-installer-namespace> interset-api -
-replicas=2
```

11. Log in to Intelligence or other application user interfaces available for this domain such as the CDF Management Portal or the Fusion dashboard.

12. Using the **Developer tools** option in your browser, ensure that the **INTERSET_SESSION** cookie is only available to request with **/interset** in the path.

> To verify the information about cookies passed in each request, in the **Developer tools** option of your browser, click **Network** > **Cookies**.

Issues Related to Search

HERC-9865 — Fieldset Fails to Revert to its Original Setting

Issue: If you change a fieldset after running a search, then leave the **Search** web page or navigate to a different feature, Search fails to revert the fieldset to the original setting. For example, you choose the *Base Event Fields* fieldset 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.

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

OCTCR33I113040 — 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.

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

OCTCR33I167004 — Scheduled Tasks Can be Saved Even if the User Closes the Dialog Box

Issue: When you click the **Close** button during the scheduler task creation process, the modal dialog box closes, but the task is still being saved.

Workaround: If you do not intend to save the task in the scheduler table, select the task and manually delete it.

OCTCR33I179782 — 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**.

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: To run the Search at a selected hour and minutes, specify a specific hour for the **Starting From** setting.

OCTCR33I369029 — Load Modal Does Not Load Search Criteria When the Fieldset is Deleted

Issue: Search criteria does not load under the circumstances described below.

1. The customer creates his or her own fieldset.
2. The customer creates a search criteria and assigns his or her custom fieldset to it.
3. The customer deletes the fieldset that was just created.
4. The search criteria fieldset returns to the one set in the user preferences.
5. The customer tries to load the Search Criteria from the Feature Table, but it will not load and displays a red "Failed to load search list" error message.

Workaround: Load the search criteria from the **Load** modal dialog box in the main search page.

OCTCR33I369158 — Saved Query or Criteria Can Overwrite the Query in a Saved Results that Has the Same Name

Issue: If you save a Query or Criteria and use the same name as a previously saved search Results, the system overwrites the query in that saved search results rather than saving a new Query or Criteria with the specified name. For example, you execute a search and save the results as `Checking Log4J Vulnerabilities`. If you create and save a new search Query or Criteria with that same name, you have changed the query in the saved Results. The next time that you run `Checking Log4J Vulnerabilities`, Search will use the newly saved query instead of your original query.

Workaround: Before saving a new Query or Criteria, review the existing saved Results to ensure that you do not use the same name.

OCTCR33I379056 — Cannot Change the Start or End Date While a Notification Banner is Present

Issue: If the application currently displays a notification banner, Search fails to accept a change to the **Start time** or **End time** for a custom date range.

Workaround: Clear the notifications, then change the date range.

OCTCR33I385042 — Issues Loading a Saved Search Criteria Using # in the Search Input Box

Issue: If you load a saved search criteria in the search input box using #, the system fails to load the saved fieldset or time range.

Workaround: Load the saved criteria from the Saved Search Criteria page:

1. Select **Search > Criteria**.
2. Click the box next to the search criteria that you want to load.
3. Click **Load**

OCTCR33I411211 — Time Range Loads Incorrectly When Selecting the Default Option “DD/MM/YY hh:mm:ss:ms”

Issue: When the User sets `DD/MM/YY hh:mm:ss:ms` in user preferences and loads a search criteria, the time range is reported incorrectly.

Workaround: Manually change the time range that was set in the search criteria.

OCTCR33I549094 — Intermittent Failure of .csv File Containing Scheduled Search Results

Issue: Exporting the results of a Scheduled search from the Completed tab might intermittently result in an empty .csv file.

Workaround: If this happens, export the data to a .csv file again from the **Events** table.

OCTCR33I566082 — Scheduled Searches: Problems Related to Switching the Field “Search Expires in” in User Preferences

Issue: If you create a scheduled search that contains an expiration option, such as “Search expires in” = 7 days, then change the value in User Preferences to “Search expires in” = 10 weeks, the scheduled search fails to complete and shows an incorrect setting (“Search expires in” = 7 weeks). The issue also occurs if you switch the settings from weeks to days, weeks to “Never Expire,” even with a fresh install.

OCTCR33I576073 — Switching Tabs While Saving Searches Causes an Error

Issue: If you switch tabs while saving a search, the system throws an arror that states "Results do not match the specified serach query."

Workaround: Refresh the browser.

OCTCR33I576083 — Outlier Detection: Outlier History Display is Incorrect When No Score Exists

Issue: In **Outlier Detection**, when no score exists, **Top Anomalous Hosts** and **Outlier History** post zeros (0) and display empty charts.

Additionally, if you click a zero score in **Top Anomalous Hosts**, then **Selected Anomalous IP** and **Selected Anomaly Host** also display empty charts.

OCTCR33I585053 — Cannot Add a Field from Event Inspector to Active Search if the Field is Not Available in the Fieldset

Issue: If you add a field from the Event Inspector to an active search, and the field is not available in the fieldset of the active search, an error will occur. A red line will display under any field in the search query that's not in the active fieldset. Hover your cursor over the field to display the following error message: Columns only from fieldset are permitted.

Workaround: Either add the field to the active fieldset or choose a fieldset that includes the field you wish to add to the active search.

OCTCR33I587006 — Search Fails When the "where condition" Operator Has Any <...> and Contains a Filter for Field Groups

Issue: The following field groups are not supported because they are not string data. If a user wants to include a non-string datatype field group in a | where any...contains query, the field datatype needs to be converted to string (using eval to string). Otherwise, the software might display an error alerting you about non-applicable field groups, such as custom float, float, ip, ip6, mac, port, path, timestamp, or url.

OCTCR33I603036 — The Application Displays an Error When You Try to Save Search Criteria

Issue: The user encounters an error when they try to save specific search criteria prior to running a query, even though they have entered correct syntax and parameters.

OCTCR33I608090 — After Installation, the Search Tab is Intermittently Visible

Issue: After you perform an installation of the application, the Search tab may become intermittently visible.

Workaround: Follow the process described below.

1. Perform a fresh install the application.
2. Login as an administrator or system administrator.
3. If the Search tab does not display, do the following:

   On Moba/terminal, execute the following commands to shut down these 2 pods:

   kubectl scale deploy -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1) fusion-search-web-app --replicas=0

   kubectl scale deploy -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1) fusion-ui-services --replicas=0

OCTCR33I608098 — Certain top/bottom Queries Refresh When the User Presses the Space Bar While Entering the Query

Issue: Queries that use the **top/bottom** search operator along with fields that begin with "Device" may fail completely or partially.

Cases that fail all the time contain fields that begin with "Device" and use the other fields listed below.

| top Device Receipt Time

| top Device Event Class ID

| top Device Event Category

Cases that fail intermittently also use another pipe operator or fail when the user keeps typing words not present in the fields, such as below:

| top Source Address

| top Agent Severity

Example: Begin entering the query below. Anything after the word "Device" clears out after you press the space bar.

#Vulnerabilities | top Device Event Class ID

Workaround: To avoid this behavior, select the field from the drop-down options for that query while you are entering it. This applies to any field the user is not able to type in.

OCTCR33I608115 — Vulnerabilities: System Query is Duplicated With Two Different Names

Issue: You can run into a search error when using "All Fields" fieldset and using more than 5 pipe operations.

OCTCR33I609036 — Upgrade Issues: Searches That Use the "All Fields" Fieldset and the "All Time" Time Range Do Not Complete

Issue: Migrations or upgrade issues from the 22.1.x releases may cause searches that use the Fieldset "All Fields" and Time Range = "All Time" to become disabled. The **Search** button may also become disabled. Additionally, if the user clicks the **Play/Continue** button, the search will not complete.

Workaround: Post-migration, create a new search that uses the same details.

OCTCR33I610160 — Unable to Use the Field "Id" With the top, bottom, rename, eval, and wheresql Operators

Issue: Queries that use the search operators **top**, **bottom**, **rename**, **eval**, and **wheresql** do not recognize the "Id" field as a column, regardless of the Fieldset used.

- For the **eval** search operator, the search will execute but "Id" will be treated as a string.
- For **top**, **bottom**, **rename**, and **wheresql** search operators, the search execution will fail and you see the error message "Fix error in query first: Unknown column "Id."
- For the **wheresql** search operator, the error message "An error occurred while executing the search. Execution could not complete" displays.

Workaround: Although there is no workaround, we recommend removing the use of the "Id" field from the query to avoid a search execution failure.

OCTCR33I610161 and OCTCR33I615024 — Incorrect Search Results Occur When Filtering With the "Id" Field

Issue: Queries that filter specific "id" field values will not return correct results . For example: id = "123456789" or id != "123456789"

Workaround: Although there is no workaround, we suggest you do not use the "Id" field in queries to avoid getting incorrect results because of the issue.

Issues Related to SOAR

- OCTCR33I548027 — Trend Micro Apex Central Integration Fails
- OCTCR33I567004 — SOAR Widgets Display Problems with Duplicate Widgets
- OCTCR33I612130 — SOAR message broker pod backup file cannot be created automatically.

OCTCR33I548027 — Trend Micro Apex Central Integration Fails

Issue: Due to a known issue related to authentication, the integration with Trend Micro Apex Central fails.

Workaround: There is no workaround at this time.

OCTCR33I567004 — SOAR Widgets Display Problems with Duplicate Widgets

Issue: If multiple SOAR timeline widgets are present in a dashboard, then data is displayed for only one widget.

Workaround: There is no workaround at this time.

OCTCR33I612130 — SOAR Message Broker Pod Backup File Cannot be Created Automatically

Issue: SOAR message broker pod backup file cannot be created automatically.

Workaround: Complete the following procedure to create the message broker pod backup file manually:

1. Enter the following Kubernetes command in your terminal:

   ```
   kubectl edit cm soar-artemis-pod-tools-cm -n <arcsight-installer-namespace>
   ```

2. Replace the line `/usr/sbin/cron start` with `/usr/sbin/crond start`.
3. Replace the line `folder_to_be_deleted=$(ls -dt $source_directory/backup/*/ | sed -e '1,24d' | xargs)` with `folder_to_be_deleted=$(echo $(ls -dt $source_directory/backup/*/ | sed -e '1,24d'))`
4. Replace the line `files_to_be_deleted=$(ls -dt $source_directory/backup-logs/* | sed -e '1,120d' | xargs)` with `files_to_be_deleted=$(echo $(ls -dt $source_directory/backup-logs/* | sed -e '1,120d'))`
5. Replace the line `source_restore_root_dir=$(find "$source_directory/restore" -mindepth 1 -maxdepth 1 -type d -print0 | xargs -I {} echo "{}")` with `source_restore_root_dir=$(ls -d $source_directory/restore/*/ | awk '{print substr($1, 1, length($1)-1)}')`
6. Replace the line `rsync -avrHAXS $source_directory/restore/* $source_directory/ with rsync -avrHAXS $source_restore_root_dir/* $source_directory/`
7. Enter the following command to save and exit:

   ```
   esc + :wq + enter.
   ```

8. Enter the following command to restart the pod:

   ```
   kubectl delete pod <soar-message-broker-pod-name> -n <arcsight-installer-namespace>
   ```

Issues Related to Transformation Hub

- "OCTCR33I377141— If Event Integrity is Enabled, Enrichment Stream Processor Pods Stop Working" on the next page
- "OCTCR33I408161— After Upgrade to 3.6, Some ArcMC Fields No Longer Display Event Data" on the next page
- "OCTCR33I409142 — After Upgrade to 3.6, Kafka Manager May Fail to Show Metrics " on the next page

- "OCTCR33I409228 — In Multi-Node Scenario, Schema Registry Instances May Be Allocated to a Single Node" on the next page
- "OCTCR33I609151 — CEF Routing Rule with Less Than Condition May Result in Unintended Events in Destination Topic" on page 65
- "OCTCR33I609152 — CEF Routing Rule with Numeric Test May Result in Unintended Events in Destination Topic" on page 65

OCTCR33I377141— If Event Integrity is Enabled, Enrichment Stream Processor Pods Stop Working

If the Event Integrity feature is enabled, and then the Enrichment Stream Processor (SP) source topic number of partitions is changed, the Enrichment SP pods will stop working.

Workaround: In Kafka Manager change the Event integrity changelog internal topic, named with the following format and pattern: com.arcsight.th.AVRO_ENRICHMENT_1-integrityMessageStore-changelog number of partitions to match the source topic number of partitions. Then, restart the Enrichment pods.

OCTCR33I408161— After Upgrade to 3.6, Some ArcMC Fields No Longer Display Event Data

After upgrading TH to 3.6, in some cases the following ArcMC fields will no longer display any data: Event Parsing Error, Stream Processing EPS, Stream Processing Lag showing the message 'No data returned at this time'.

Workaround: Restart TH WebServices pod after the upgrade running the following commands:

```
namespace=$( kubectl get namespaces | awk '/^arcsight-installer-/{print $1}'
)
pod=$( kubectl -n $namespace get pods | awk '/^th-web-service-/{print $1}' )
kubectl -n $namespace delete pod $pod
```

OCTCR33I409142 — After Upgrade to 3.6, Kafka Manager May Fail to Show Metrics

After upgrading to Transformation Hub 3.6, Kafka Manager may fail to show Kafka consumers or metrics, and the Kafka Manager log may contain warnings that a broker may not be available. This happens when Kafka Manager starts before the Kafka brokers after the upgrade; timing allows Kafka Manager to connect to pre-upgrade brokers before they exit.

Workaround: The solution is to restart the Kafka Manager management pod. Perform these steps on the master node to restart Kafka Manager:

```
namespace=$( kubectl get namespaces | awk '/^arcsight-installer-/{print $1}'
)
pod=$( kubectl -n $namespace get pods | awk '/^th-kafka-manager-/{print $1}'
)
kubectl -n $namespace delete pod $pod
```

OCTCR33I409228 — In Multi-Node Scenario, Schema Registry Instances May Be Allocated to a Single Node

This issue applies to deployments where Transformation Hub is deployed in a multi-node scenario. After deploying Transformation Hub in a multi-node scenario, Schema Registry instances may get allocated to a single worker node. Instances should be distributed across worker nodes to ensure that failover will provide high availability. Please check the distribution of Schema Registry instances across worker nodes to make sure instances run on more than one node using the following procedure:

1. Identify the worker nodes that are running Schema Registry instances by running the following commands on the master node:

```
namespace=$( kubectl get namespaces | awk '/^arcsight-installer-/{print $1}'
)
fmt="custom-
columns=NODE:.spec.nodeName,NAME:.metadata.name,STATUS:.status.phase"
kubectl -n $namespace get pods -o "$fmt" --sort-by=".spec.nodeName" | grep -E
"NODE|th-schemaregistry"
```

2. If the output shows all instances are running on the same worker node, do the following:
   2a. Restart Schema Registry using this command in order to spread the instances across worker nodes:

```
kubectl -n $namespace rollout restart deployment th-schemaregistry
```

2b. Verify restart has completed by waiting until all Schema Registry pods have a status of "Running" and a small "AGE" value of the minutes or seconds since you performed the restart by running this command.

```
kubectl -n $namespace get pods | grep -E "STATUS|schemaregistry"
```

2c. After the restart completes, verify that the instances are now running on different worker nodes by running this command:

```
kubectl -n $namespace get pods -o "$fmt" --sort-by=".spec.nodeName" | grep -E
"NODE|th-schemaregistry"
```

In a multi-node scenario, a topic used internally by Schema Registry may get configured with too few replicas, which reduces reliability and can make the registry fail during failover. Check the topic's configuration to verify it has the proper replica count (replication factor) using the following procedures on the master node.

3. Set the topic to be used in later commands:

```
topic="_schemas"
```

4. Print the replication factor for the topic, as follows:

```
topicinfo=$( kubectl -n $namespace exec th-kafka-0 -- kafka-topics --
bootstrap-server th-kafka-svc:9092 --describe --topic $topic )
echo "$topicinfo" | sed -n -re '/ReplicationFactor:/s/^.*
(ReplicationFactor:\s*\S+)\s.*/\1/p'
```

5. If the replication factor is not equal to 3, perform the following steps (5a-5f) to change the configuration. If it equals 3, skip to Step 6.

   5a. Get the list of brokers to set as replicas, including the topic's partition leader. If the cluster has more than three brokers, limit the replicas to three using the following commands.

```
leader=$(  echo "$topicinfo" | sed -n -re '/Leader:/s/^.*Leader:\s*
(\S+)\s.*/\1/p' )
allbrokerids=$( kubectl exec -n $namespace th-zookeeper-0 -- zookeeper-shell
th-zook-svc:2181 ls /brokers/ids | grep -E '^[[][0-9]+' | tr -d '[ ]' )
n=1; blist=$leader; for b in ${allbrokerids//,/ } ; do if [[ $n -lt 3 && !
$blist =~ $b ]]; then n=$((++n)); blist="$blist,$b"; fi; done
```

5b. Generate a replica configuration file, as follows:

```
topicfile=/tmp/topic.json
assignfile=/tmp/assign.json
printf '{"topics": [{"topic": "%s"}], "version":1}' $topic > $topicfile
kubectl cp $topicfile $namespace/th-kafka-0:$topicfile
kubectl -n $namespace exec th-kafka-0 -- kafka-reassign-partitions --broker-
list "$allbrokerids" --bootstrap-server th-kafka-svc:9092 --generate --
topics-to-move-json-file $topicfile > $assignfile
sed -i '1,/Proposed partition reassignment/d' $assignfile
sed -i -r "s/(,.replicas.:\[)([0-9,]+)/\1$blist/" $assignfile
sed -i 's/,\s*"log_dirs"\s*:\s*[[][^]]*[]]//' $assignfile
kubectl cp $assignfile $namespace/th-kafka-0:$assignfile
rm -f "$assignfile" "$topicfile"
```

5c. Use the file to add the replica configuration with this command:

```
kubectl -n $namespace exec th-kafka-0 -- kafka-reassign-partitions --
bootstrap-server th-kafka-svc:9092 --reassignment-json-file $assignfile --
execute |& grep -v "Save this to use"
```

The output should end with this message:

```
Successfully started reassignment of partitions.
```

5d. Verify that the reassignment completes by running a verification command with the same input file, as follows:

```
kubectl -n $namespace exec th-kafka-0 -- kafka-reassign-partitions --
bootstrap-server th-kafka-svc:9092 --reassignment-json-file $assignfile --
verify
```

When reassignment has completed, the output will show the following:

```
Reassignment of partition _schemas-0 completed successfully.
```

5e. Since the replicas have changed, run a preferred leader election for the topic's partition with the following commands:

```
electfile=/tmp/election.json
printf '{"partitions": [{"topic": "%s","partition":0}]}\n' $topic >
$electfile
kubectl cp $electfile $namespace/th-kafka-0:$electfile
rm -f "$electfile"
kubectl exec -n $namespace th-kafka-0 -- kafka-leader-election --bootstrap-
server th-kafka-svc:9092 --election-type preferred --path-to-json-file
$electfile
```

5f. Verify that the topic now has three replicas by running this command:

```
kubectl -n $namespace exec th-kafka-0 -- kafka-topics --bootstrap-server th-
kafka-svc:9092 --describe --topic $topic | sed -n -re
'/ReplicationFactor:/s/^.*(ReplicationFactor:\s*\S+)\s.*/\1/p'
```

Also in a multi-node scenario, an internal ArcSight topic may get configured with too few replicas, which reduces reliability of Stream Processor metrics and can prevent ArcMC from displaying the metrics. Check the topic's configuration to verify it has the proper replica count. Perform the following procedures on the master node.

6. Set the topic to be used in later commands:

```
topic=th-arcsight-avro-sp_metrics
```

7. Repeat Steps 4 and 5 above to check the topic and then modify it if needed. The topic needs to have the same replica count as the previous topic: 3.

OCTCR33I609151 — CEF Routing Rule with Less Than Condition May Result in Unintended Events in Destination Topic

When routing CEF events, if a routing rule tests a numeric field with a "less than" condition, ("<" or "<="), a CEF event that does not contain that field will match the condition and will be routed to the destination topic. The result is that the destination topic may contain unintended CEF events.

OCTCR33I609152 — CEF Routing Rule with Numeric Test May Result in Unintended Events in Destination Topic

When routing CEF events, if a routing rule tests a numeric field, a CEF event that has a value in that field may be routed in an unintended way. Numbers are compared as strings instead of numerically. The result is that destination topics for affected CEF rules may not receive intended events, or may receive unintended events.

Known Issues Related to Upgrade

These issues apply to upgrading to this release.

- "OCTCR33I865171 - Upgrade Process Might Cause Data Loss by Changing Retention Value to One Month" below

OCTCR33I865171 - Upgrade Process Might Cause Data Loss by Changing Retention Value to One Month

Issue: When you upgrade to this release, it's possible that the process might reset the data retention value for storage groups to the default of one month. If this occurs, the system could erroneously purge data that you want to retain. The data purge job runs at midnight on the first day of each month.

This issue occurs when the autopass pod is down but the fusion-search-web-app and fusion-search-and-storage-web-app pods are running. The autopass pod tells the system whether you have a license that allows more than one month of storage, such as the ArcSight Recon license. For more information about pods that run on the worker nodes, see Understanding Labels and Pods in the *Administrator's Guide to the Arcsight Platform*.

Workaround: Immediately after upgrading to this release, complete the following steps:

1. Log in to ArcSight Platform with an account that has the *Manage Storage Groups* permission.
2. Select **Configuration** > **Storage**.
3. Select the storage group that you want to check.
4. Reset the value for **Delete Data Older Than** to your preferred settings, such as 12 months.

   For more information about data retention, see "Delete Old Data from the Storage Groups" in the ArcSight Platform Help and Configuring the Policy for Retaining Data in the *Administrator's Guide to the Arcsight Platform*.

> To avoid any inadvertent changes to storage group retention, we recommend that you regularly monitor the autopass pod to ensure that it stays up.

Resolved Issues

These issues apply to common or several components in your ArcSight Platform deploy. For more information about issues related to a specific product, please see that product's release notes, as applicable.

Security Fixes in Previously Released Patches

This release includes the security fixes previously available with ArcSight Platform 23.1. For more information about these security fixes, see the Release Notes for ArcSight Platform 22.1.2.

OCTCR33I160009 – Reporting - Chart Wizard Now Correctly Displays the Convert to Measure Button

The **Convert to Measure** button occasionally became unavailable if you tried to create a chart using the **Chart Wizard** after you changed from "convert" to "dimension."

OCTCR33I162021 – X/Y Fields Can Now be Removed From a Graph

Issue: In the chart editor, when you remove an X or Y field, the Reports Portal display an error message. This intermittent issue was resolved by a software fix.

OCTCR33I242328 – On Node Management, the Filtering Option Does Not Work Correctly in Some Columns

On Node Management page under the *Container* tab, the columns: **Name** and **Parser Ver** are not filtering. A code fix was applied to resolve the issue.

OCTCR33I276138 – Data Timeseries Chart Fails to Update after Changing Categories

A software fix resolved the issue where, when viewing the Data Timeseries Chart in the Data Quality dashboard, the stacked area chart failed to automatically update as soon as you selected an event category, such as Future Events, Past Events, or Active Events.

OCTCR33I349068 – Exported Tables No Longer Show Squeezed Columns

Issue: A code change resolved the problem where some dashboard table columns displayed squeezed columns when they were exported using specific formats like HTML

OCTCR33I409215 – Database in 22.1 Release Will Not Support FIPS

A code fix resolved the issue where the database did not support FIPS mode due to a defect.

OCTCR33I491108 – Pods Might Not Run During Fusion Reinstall

After you undeploy the Fusion capability and then redeploy Fusion into the same cluster, pods might remain in CrashLoopBackOff or PodInitializing status. The root cause of the issue is that the redeploy causes the system to forget the password for the rethinkdb database. A software change fixed this issue.

OCTCR33I500006 – The Insights Tab Disappears From the Fusion Dashboard After the License Expires

A code fix was applied to resolve the issue related to the Insights tab disappearing from the dashboard due to an expired license.

Issue Related to ArcMC

- "OCTCR33I242397 – Storage of Log Files History Generated Over Years Are Occupying a Sizable Amount of Space" below
- "OCTCR33I409212 – Pre-upgrade CTH is Not Displayed in ArcMC After the Upgrade is Executed" on the next page
- "OCTCR33I409274 – ArcMC Online Help is Presenting Installation Information That is Only Required on the Admin Guide" on the next page
- "OCTCR33I511149 – When the Restoration Script is Run With the -o Option, ArcMC Fails to Restore the Backup" on the next page
- "OCTCR33I511150 – The ArcMC Postgres Database Was Not Automatically Registered With the Itom pg-backup Service" on the next page
- "OCTCR33I555046 – The Backup Directory in Fusion ArcMC is Growing Rapidly in Size" on page 71

OCTCR33I242397 – Storage of Log Files History Generated Over Years Are Occupying a Sizable Amount of Space

Previously, storage of log files history from /opt/arcsight/arcmc/userdata/logs/tomcat/ were occupying sizable amount of space. A software fix resolved this issue.

OCTCR33I409212 – Pre-upgrade CTH is Not Displayed in ArcMC After the Upgrade is Executed

The issue of the pre-upgrade CTH not being displayed in ArcMC after the upgrade has been executed is caused by the loss of information or data during the upgrade process. The upgrade process may have overwritten or altered the data that was stored in the pre-upgrade CTH, causing it to not be displayed in ArcMC. A code fix was applied to resolve the issue.

OCTCR33I409274 – ArcMC Online Help is Presenting Installation Information That is Only Required on the Admin Guide

Information concerning installation that can only be found in the Admin Guide is displayed in the ArcMC Online help. A code fix was applied to resolve the issue.

OCTCR33I511149 – When the Restoration Script is Run With the -o Option, ArcMC Fails to Restore the Backup

Prior to a code change, ArcMC could experience backup restoration failures, as described below. A code fix resolved the issue.

ArcMC's backup restoration is crucial for protecting data and configurations. However, if the restore script is executed with the -o option, it may fail. The -o option specifies options during the restoration process, and its incorrect usage can cause the backup to not be properly restored.

OCTCR33I511150 – The ArcMC Postgres Database Was Not Automatically Registered With the Itom pg-backup Service

Prior to a code change, ArcMC postgres database experienced backup and restore issues, as described below:

The ArcMC postgres database is a critical component for storing and managing data within the Arcsight Management Center system. However, if the database is not automatically registered with the ITOM pg-backup service, it may not be properly backed up and protected. This can lead to potential data loss or corruption in the event of a system failure or other emergency.

OCTCR33I555046 – The Backup Directory in Fusion ArcMC is Growing Rapidly in Size

A software fix was applied to the following issue:

Logging (especially from the fusion-arcmc-web-app container) is quickly depleting disk space, these logs are in ArcMC backup directory within the arcsight-volume/ArcMC/backups directory. This increase in size can lead to several problems such as a lack of storage space, slow backups, and slow restore operations. Additionally, it can also make it difficult to manage the backup data and identify which backups are essential and which can be deleted.

Issues Related to Search

- "OCTCR33I167004 – Scheduled Tasks are Now Prevented From Being Saved After the User Closed the Dialog Box" below
- "OCTCR33I174130 – Scheduled Searches No Longer Fail to Export to CSV" on the next page
- "OCTCR33I178795 – Fieldsets No Longer Default to Base Event Fields After an Upgrade" on the next page
- "OCTCR33I324035 – Search Query No Longer Returns Incorrect Results if the Query is not Explicitly Stated" on the next page
- "OCTCR33I341227 – You May Now Use Search Operators in the Name of a Saved Query or Criteria" on the next page
- "OCTCR33I408155 – Backup Failures in S3 While Deleting Obsolete Files From S3 Has Been Resolved" on the next page
- "OCTCR33I549163 and OCTCR33I592116 – Searches With no Changes Since the Last Run No Longer Appear to be Stuck" on page 73
- "OCTCR33I592116 – Re-executing Searches No Longer Prompts an Error Message or Prevents the Search Grid From Displaying" on page 73

OCTCR33I167004 – Scheduled Tasks are Now Prevented From Being Saved After the User Closed the Dialog Box

A code change resolved the issue of a user being able to accidentally save a scheduled task after closing the dialog box (and intending to not save the work).

OCTCR33I174130 – Scheduled Searches No Longer Fail to Export to CSV

Issue: A software change resolved the occasional problem where the CSV file of an exported scheduled search failed to display any data.

OCTCR33I178795 – Fieldsets No Longer Default to Base Event Fields After an Upgrade

Issue: A code change addressed the problem of the Public Default Fieldset defaulting to Base Event Fields after you upgraded the software.

OCTCR33I324035 – Search Query No Longer Returns Incorrect Results if the Query is not Explicitly Stated

Issue: A code fix resolved the issue of the Search field returning incorrect search results due to a query not being written explicitly. You no longer have to be as careful about stating the query. For example, the query is more forgiving about the use of spaces.

OCTCR33I341227 – You May Now Use Search Operators in the Name of a Saved Query or Criteria

Issue: A code change now allows you to include a search operator in the name of a saved query or criteria. Search no longer erroneously includes that part of the saved name in the query. For example, if you save a query with the name Users and Devices, Search does not include "and Devices" in the query field. The code now recognizes the difference between "and" as a word and "and as a search operator.

OCTCR33I408155 – Backup Failures in S3 While Deleting Obsolete Files From S3 Has Been Resolved

Issue: Previously, an error occurred (SlowDown) when calling the DeleteObjects operation. Part of the backup operation was clearing obsolete backup files that were older than the backup retention configuration setting. Due to this issue, the cleanup of obsolete files did not complete successfully and some obsolete files remained, resulting in higher than necessary backup storage utilization.

OCTCR33I549163 and OCTCR33I592116 – Searches With no Changes Since the Last Run No Longer Appear to be Stuck

A code change resolved the issue where the user interface did not allow you to rerun custom time range searches that had no changes since the previous run.

OCTCR33I592116 – Re-executing Searches No Longer Prompts an Error Message or Prevents the Search Grid From Displaying

The UI no longer prevents triggering searches that do not have any changes since last run.

Issues Related to SOAR

- "OCTCR33I411072 – Broken Case Links in SOAR InetSoft Reports" on the next page
- "OCTCR33I421034 – A Wrong Protocol Name in the Arcsight Listener Protocol Parameter Makes SOAR Crash Upon Restart" on the next page
- "OCTCR33I427039 – Action History Page Filters Have Multiple Entry With Same Name" on the next page
- "OCTCR33I428078 – No Entries Displayed for Failed Enrichment Activities on Cases Timeline" on page 75
- "OCTCR33I430016 – Unable to Delete the Column that was Added First to the List" on page 75
- "OCTCR33I454142 – WinRM Logoff User Capability Does Not Get Username From Scope" on page 75
- "OCTCR33I467084 – Unable to Add File to Case Scope in Automation" on page 75
- "OCTCR33I478040 – Error While Adding Comment to a Case" on page 75
- "OCTCR33I485001 – Error While Deleting a Case in Open Status" on page 76
- "OCTCR33I504024 – Large Java Stack Trace is Found When Dispatching Case to a UserGroup" on page 76

OCTCR33I411072 – Broken Case Links in SOAR InetSoft Reports

In the InetSoft Reports the links are correctly forwarding to SOAR Case

OCTCR33I421034 – A Wrong Protocol Name in the Arcsight Listener Protocol Parameter Makes SOAR Crash Upon Restart

SOAR crashes while restarting if protocol name provided for Arcsight Listener Protocol Parameter is wrongIf a wrong protocol name is specified for the ArcSight Listener Protocol an error message is displayed, but the name gets saved. However, while restarting the soar-web-app crashes with an error message.Resolution: A code fix was applied to resolve the issue. A code fix was applied to resolve the issue.

OCTCR33I427039 – Action History Page Filters Have Multiple Entry With Same Name

Some action history integrations have same capability names. This results in the same capability name being displayed multiple times. A software fix addressed this issue.

OCTCR33I428078 – No Entries Displayed for Failed Enrichment Activities on Cases Timeline

After a failed enrichment, there is no related 'enrichment failed' entry on the activity timeline. The Cases timeline does not show entries for failed enrichment activities. A code fix resolved this issue.

OCTCR33I430016 – Unable to Delete the Column that was Added First to the List

A software fix allows you to delete the column that was added first to the list

OCTCR33I454142 – WinRM Logoff User Capability Does Not Get Username From Scope

A software fix allows the value for username to logoff parameter to be selected from the case scope items for WinRM plugin.

OCTCR33I467084 – Unable to Add File to Case Scope in Automation

When a file is added as a comment, it is automatically added to case scope. However, it is not possible to add the file in automation. A code fix was applied to resolve the issue.

OCTCR33I478040 – Error While Adding Comment to a Case

If you try adding a comment to a Case without adding a file, an error is displayed. A code fix was applied to resolve the issue.

OCTCR33I485001 – Error While Deleting a Case in Open Status

As a result of a code change, the replacement editor now displays when you try to delete a case in open status.

OCTCR33I504024 – Large Java Stack Trace is Found When Dispatching Case to a UserGroup

In SOAR, when creating a dispatch rule and assigning an alert to a UserGroup (Salesforce Case ID: 02337357) a large stack trace is noted in the 'soar-web-app' pod. A code fix was applied to resolve the issue.

OCTCR33I512001 – Unable to Add a Second Item to Cisco Firepower Management Center Block IP and Block URL Capabilities

A code fix resolved the problem of Cisco Firepower's API, returning data that is paginated and contains 25 records by default. Now all the records display.

OCTCR33I514042 – IP Country Information is Always Unknown

In SOAR, Country Scope item property for IP addresses are displayed as unknown. A code fix was applied to resolve the issue.

OCTCR33I530023 – SOAR MISP Integration Fetches all the Events For Device Connectivity

SOAR MISP Integration fetches all events for device connectivity. For the MISP server with lots of events, it takes minutes to complete the test. A code fix was applied to resolve the issue.

OCTCR33I553001 – Username Query is Missing in Parameter Definition

The parameter definition for username is missing in the username query. A code fix was applied to resolve the issue. With the changes, a new dropdown is displayed, which enables you to select usernames from the case scope.

OCTCR33I554001 – Liquibase Migration Error

Liquibase Migration Error is displayed because of syntax errors in the tag. A code fix was applied to resolve the issue.

OCTCR33I554081 – Unable to Save Playbooks With Alert Source as the Starting Condition

The alert source can now be chosen as a starting condition.

OCTCR33I555096 – New Notifications are Not Displayed Properly

When a new notification arrives, clicking on the notification bell shows just the company logo. A code fix was applied to resolve the issue.

OCTCR33I569001 – Scope Item Property List – Paging is Broken

The Scope Item Property List page now displays the actual count of items.

Issues Related to Transformation Hub

- "OCTCR33I360046 – Incorrect TH Hostnames Displayed on ArcMC in Cloud" on the next page
- "OCTCR33I376076 – Fusion Password with Backslash (\) Can Cause TH Web Services to Crash" on the next page

- "OCTCR33I410157 and OCTCR33I561027 – New Parameters Added to Prevent ArcMC-TH Timeout" below
- "OCTCR33I491188 – C2AV Processor Failed With Specific Events and Configuration" on the next page
- "OCTCR33I498001 – CEF Routing Rule With "Contains," "Starts With," "Ends With" Can Stop Event Flow to Destination Topic" on the next page

OCTCR33I360046 – Incorrect TH Hostnames Displayed on ArcMC in Cloud

An issue has been resolved where incorrect Transformation Hub hostnames and CPU/memory values (0) were presented on ArcMC in AWS and Azure in ArcSight suite deployments which include the Intelligence capability.

OCTCR33I376076 – Fusion Password with Backslash (\) Can Cause TH Web Services to Crash

On the pre-deployment/Reconfigure page for Fusion Single Sign-on Configuration, entering a Fusion password (Client Secret) that includes a backslash character (\) could cause Transformation Hub web services to crash and not restart. This issue has been resolved.

OCTCR33I410157 and OCTCR33I561027 – New Parameters Added to Prevent ArcMC-TH Timeout

Previously, the `ARCMC_CONNECTION_TIMEOUT_MS` property value was hardcoded and not configurable, which could cause TH-to-ArcMC communication timeouts.

For more flexibility, the following new environment variables have been defined.

`WS_AUTH_ARCMC_CONNECTION_TIMEOUT`	30000	The amount of time (milliseconds) before a request to connect to ArcMC is retried due to ArcMC timeout.
`WS_AUTH_ARCMC_CONNECTION_NUM_RETRIES`	2	The number of times that TH retries to connect ArcMC due to ArcMC timeout.

Adjust the values of these parameters by creating or editing the file arcsight-env-override.properties under the folder <NFS_root_DIRECTORY>/transformationhub/config in a text editor. Prefix the names of these properties with *arcsight.th.web-service*. to create an override. Then, restart the Web Services Pod. For more information, see Overriding Application Properties.

OCTCR33I491188 – C2AV Processor Failed With Specific Events and Configuration

The C2AV Stream Processor was failing when processing some specific Powershell events provided by the customer with the field truncation flag as true. The failure caused Stream Threads to terminate, ultimately causing the entire C2AV processor to fail and restart.

A code change fixed the issue, and now the stream processing threads are no longer failing when processing the specific problematic events when the truncation flag is enabled.

OCTCR33I498001 – CEF Routing Rule With "Contains," "Starts With," "Ends With" Can Stop Event Flow to Destination Topic

When routing events between CEF topics, event flow to a destination topic would stop if the route's rule tested a field with the operators "contains", "starts with" or "ends with", and the source topic received an event that had no value for the field. This issue has been resolved and event flow to the destination will not stop.

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.
- *Technical Requirements for ArcSight Platform*, which provides information about the hardware and software requirements and tuning guidelines for the ArcSight Platform and the deployed capabilities.
- *User’s Guide for Fusion 1.6.1 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.

Publication Status

Released: March 22, 2023

Updated: Monday, March 18, 2024

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 Platform Release Notes (ArcSight Platform 23.1)

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!