opentext™

ArcSight Platform

Software Version: CE 24.2

ArcSight Platform CE Release Notes

Document Release Date: June 2024
Software Release Date: June 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Contents

Release Notes for the ArcSight Platform CE 24.2

ArcSight Platform Cloud Edition (CE) 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, Search, and user management, are provided in the base platform.

This release includes the following versions (and technical versions) of the ArcSight Platform's primary components:

Component	Version
ArcSight Command Center for Enterprise Security Manager	24.2 (1.6.0)
ArcSight Intelligence	24.2 (6.4.13)
ArcSight Recon	24.2 (1.6.0)
ArcSight SOAR	24.2 (3.11.0)
Transformation Hub	24.2 (3.7.4)
ArcMC	24.2 (3.2.4)

The documentation for this product is available on the ArcSight 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 on the ArcSight Platform CE Documentation page or the documentation pages for the included products.

What's New

This release includes enhancements to the following capabilities, components, and features:

Introducing Multi-tenancy in the ArcSight Platform

This release introduces the following enhancement in the ArcSight Platform:

- "Introduces the Ability to Create a Multi-tenant Environment" below
- Benefits of Optics in a Multi-tenant Environment

Introduces the Ability to Create a Multi-tenant Environment

This release gives you the ability to create and manage multiple tenants in your environment. In a multi-tenant environment, a **provider** offers platform services to its tenants. A provider can be an enterprise that wants to create different tenants for different groups or regions within its organizational structure or an MSSP organization that offers subscription services to tenant organizations.

The following considerations apply for a multi-tenant environment:

- After you enable Multi-tenancy, you cannot disable it or revert to single-tenant mode.
- You cannot use the Multi-tenancy feature with the ArcSight Intelligence capability.
- You cannot assign the *Perform Event Integrity Check* permission to a tenant user. Only a provider user can run the checks.

For more information, review the following content:

The links below for the *Administrator's Guide for ArcSight Platform* direct you to the off-cloud deployment version of the guide. You can find the same topics in the guides corresponding to the following deployment environments:

- AWS
- Azure
- Google Cloud

- Planning for Multi-tenancy in the *Administrator's Guide for Arcsight Platform*
- Enabling Multi-tenancy in the *Administrator's Guide for Arcsight Platform*
- Setting Up Multi-tenancy in the *User's Guide for ArcSight Platform.*

Benefits of Optics in a Multi-tenant Environment

Optics help you gain insight into specific aspects of your environment by visualizing correlated events from ArcSight ESM, which you can filter and drill into. Depending on your permissions, you can view tenant-specific data or a rolled-up view of data across multiple tenants.

For example, a CISO might want a quick overview of alerts worldwide or review key security metrics based on alerts. A security analyst can quickly identify potential threats and take the necessary actions to mitigate risks.

Optics are available only when Multi-tenancy is enabled and ArcSight ESM integrated with the Platform.

For the ArcSight Platform Installer

This release has the following updates for the platform installer.

- Automated Off-Cloud Installation as a Non-Root User
- Modification to Preparatory Steps for a Manual Off-Cloud Installation as a Non-Root User
- "SSL Automatically Enabled" below
- Capability Name Changes
- Fusion is Now Named Core

Automated Off-Cloud Installation as a Non-Root User

A new procedure is provided for an automated off-cloud installation as a non-root user. For more information see section, Using ArcSight Platform Installer for an Automated Off-Cloud Installation in the *Administrator's Guide for the ArcSight Platform CE 24.2*

Modification to Preparatory Steps for a Manual Off-Cloud Installation as a Non-Root User

The procedure to prepare for a manual off-cloud installation as a non-root user has been completely revised. For more information see section, Preparing for Manual Off-Cloud Installation Using a Non-Root User, in the *Administrator's Guide for the ArcSight Platform CE 24.2*

SSL Automatically Enabled

Beginning with the 24.2 release, SSL is always enabled for connections to the ArcSight Platform.

Fusion is Now Named *Core*

The Fusion capability is now named *Core* and is a mandatory deployment. Layered Analytics has been moved to Core and is also a mandatory deployment. SOAR has been moved out of Core and is now a separate deployment.

Capability Name Changes

Capabilities in the ArcSight Platform are now named as shown below. This change is reflected in the Platform installer as well as the **About** box.

- ArcSight ESM Command Center
- ArcSight Intelligence
- ArcSight Recon
- ArcSight SOAR
- ArcSight Transformation Hub

For Common Features in the ArcSight Platform

For Documentation

With this release, the single *ArcSight Platform Administrator's Guide* has been divided into four guides, one corresponding to each deployment type: Off-Cloud, Azure, AWS, and GCP. Instructions in each guide apply only to installation and maintenance of the Platform on the specified deployment type. (The unified guide has been discontinued.)

The new guides are located here:
https://wwwtest.microfocus.com/documentation/arcsight/arcsight-platform-24.2/

For Search

This release includes the following enhancements and changes for the Search feature:

Export Search Results as a PDF

Beginning with 24.2, you can now export the entire search results table to a .pdf file. Previously, you could only export a single result as a .pdf or .csv file. Additionally, .csv was the only allowed file format to export search results for an entire table. Your data is exported,

based on the specified fieldset for the search. Please note the export process limits the file to one million event records.

For the Reports Portal

This release includes the following enhancements and changes for the Reports Portal:

Migration Tool to Bring ArcSight Logger Reports into the ArcSight Platform

Reporting is an essential tool for communicating the state of your network security to internal and external stakeholders. Logger reports (captured views or summaries of events encountered by your system) play an integral role in indicating the overall health of your organization's network.

To help you switch to the ArcSight Platform from ArcSight Logger, we now provide you with a tool to migrate your Logger reports.

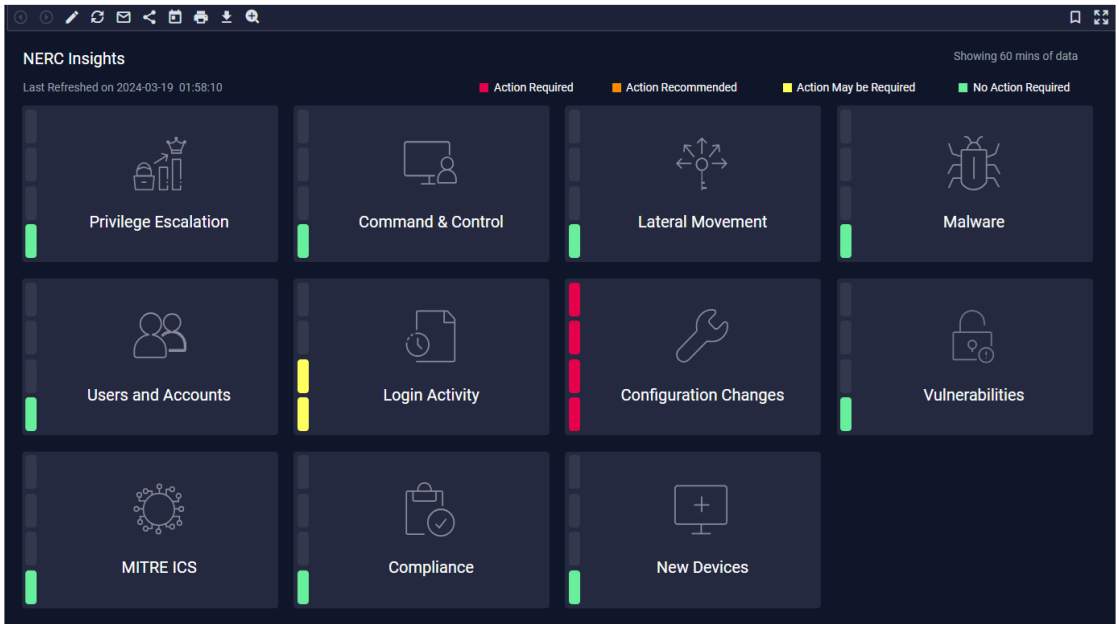
Introducing NERC Compliance Reporting for ArcSight Recon

This release introduces compliance reporting for NERC (North American Electric Reliability Corporation), which is essential for owners, operators, and users of bulk power systems in the United States and Canada who must comply with NERC standards. The **ArcSight Recon Compliance Pack for NERC** includes 16 dashboards that help you monitor the health of your bulk power system and ensure NERC compliance.

Three of these dashboards are overview dashboards that use ESM correlated events to provide a high-level perspective of your system's health and compliance. For example, the *NERC Insights* dashboard shown below enables you to quickly identify areas in need of action. You can drill into the different widgets, such as *Configuration Changes*, then determine which assets are out of compliance.

For more information, see Ensuring Compliance with NERC Standards in the *User's Guide to the ArcSight Platform CE 24.2*.

Note: Certain dashboards in this package require ArcSight ESM and ArcSight ESM Unified NERC CIP to populate.



Each of the dashboards below has been organized by their corresponding NERC control number, such as 005.

Category	Dashboard	Description
CIP Overview– Executive Summary	NERC Compliance Overview	Provides a color-coded status overview of NERC CIP-related alerts reported in the organization. Click each widget to view a drill-down dashboard with more information about alerts. NERC Compliance Overview refreshes every 5 minutes with real-time data from the ArcSight Forwarding Connector. **Note:** This dashboard requires ArcSight ESM Unified NERC CIP to populate.
	NERC Insights	The NERC Insights dashboard offers a snapshot of the health and compliance status of the organization's infrastructure. Each insight within the dashboard has color coded status to facilitate immediate action to high severity issues. This dashboard is updated every 5 minutes with data collected over the past hour. This dashboard requires correlation events forwarded from ESM to Recon. **Note:** This dashboard requires ArcSight ESM Unified NERC CIP to populate.

Category	Dashboard	Description
	Real-Time Alerts by CIP ID	Provides an overview of specific NERC CIPs based on ESM Alerts. To access this dashboard directly from the CIP Overview folder, you must select a specific CIP, such as CIP-010. Real-Time Alerts by CIP ID requires correlation events forwarded from ESM to Recon. **Note:** This dashboard requires ArcSight ESM Unified NERC CIP to populate.
CIP-002-6 Cyber Security: BES Cyber System Categorization	New Devices	Helps you track new device activity.
CIP-005-7 Cyber Security: Electronic Security Perimeter(s)	Traffic Anomaly	Helps you identify anomalies in network traffic.
CIP-007-6 Cyber Security: System Security Management	Login Activity Overview	Provides an overview of login activity. The table shows the details of the event, and each event will take you to the **Event Inspector**. You can also click **Open in Search** and it will take you to the search page and loads the categoryBehavior = /Authentication/Verify query with the same time that the dashboard was run.
	Malware Overview	Helps you track malware activity.
	User Activity Overview	Provides an overview of user activity.
	Users and Accounts Overview	Provides an overview of all the users created and deleted in the last hour.
CIP-008-6 Cyber Security: Incident Reporting and Response Planning	Attack and Suspicious Activity Overview	Displays an overall view of the attackers, their techniques, and targets.
	Command and Control Overview	Displays command and control events. You can drill down to this dashboard from the Insights dashboard.
	Lateral Movement Overview	Displays lateral movement events which represent the way an attack spreads from an entry point to the rest of the network. For example, by placing malware on a user's computer, a malicious user could attempt to move laterally to infect other computers on the network, to infect internal servers, and so on until they reach their final target. The Lateral Movement Overview dashboard is interactive, so clicking on a specific item on a chart will render the other charts accordingly.

Category	Dashboard	Description
	MITRE ATT&CK ICS Overview	Displays an overview of MITRE ATT&CK events including charts that sort events by MITRE ATT&CK technique, tactic, and frequency. This dashboard requires correlation events forwarded from ESM to Recon. **Note:** Requires ArcSight ESM to populate.
	Privilege Escalation Overview	Displays privilege escalation events. This is a drill-down dashboard that can be reached from the NERC Insights dashboard.
CIP-010-4 Cyber Security: Configuration Change Management and Vulnerability Assessments	Configuration Changes Overview	Provides an overview of configuration changes found on the organization.
	Vulnerability Overview	Provides information to help you track vulnerabilities reported in your enterprise.

For ArcSight Recon

This release includes the following enhancements and changes for ArcSight Recon:

- "Introduces Appliances for Recon" below
- "Introduces the Compliance Insight Pack for NERC" below

Introduces Appliances for Recon

The **R8000** and **R8100** appliances represent a robust, high performance appliance version of Recon that comprises all the original Recon features, built-in storage for the ArcSight Database (in Enterprise mode), fault-tolerant disk subsystem management, and compliance with Serial Attached SCSI (SAS) 3.0.

Introduces the Compliance Insight Pack for NERC

This release introduces compliance reporting for NERC (North American Electric Reliability Corporation), which is essential for owners, operators, and users of bulk power systems in the United States and Canada who must comply with NERC standards. The **ArcSight Recon Compliance Pack for NERC** includes 16 dashboards that help you monitor the health of your bulk power system and ensure NERC compliance.

For more information, see "Introducing NERC Compliance Reporting for ArcSight Recon" on page 13 and Ensuring Compliance with NERC Standards in the *User's Guide to the ArcSight Platform CE 24.2*.

For SOAR

This release includes the following enhancements and changes for SOAR functionality:

New Integration Plug-ins for SOAR

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

Integration Plug-in	Description
Amazon AWS CloudTrail	This integration plug-in has the following enrichment capabilities: • List Trails • Get Trail • Create Trail • Delete Trail • Start Logging • Stop Logging • Get Trail Status • Lookup Events • List Queries
Cisco SecureX	This integration plug-in has the following enrichment capabilities: • Get Observable Details • Get Observable Score • Get Event Details • Get Threat Context (Targets) • Respond observable
Cofense Triage	This integration plug-in has the following enrichment capabilities: • Get URL Details • Get Domain Details • Get Report Details • List Report Attachments • Download Attachment Payload • Get Reporter Details • Update Report Category • List Threat Indicators • Get Threat Indicator Details

Integration Plug-in	Description
New Team Cymru	This integration plug-in has the following enrichment capabilities: • Single Lookup Hash Query • Bulk Lookup Hash Query
OpenText Network Detection and Response	This integration plug-in has the following enrichment capabilities: • List Alerts • Get Alert Details • Get SmartPcap • List Meta Data Activity
ServiceNow CMDB	This integration plug-in has the following enrichment capabilities: • List Assets • Get Asset by ID • Update Asset Tag

Enhancements

- **Multi-Tenancy for MSSP-SOAR**

  With this release, ArcSight Platforms supports Multi-tenancy wherein, you can create and manage multiple tenants.

- **Installation Update for SOAR**

  Up to the previous releases, SOAR used to be bundled with Core and would be automatically installed when Core would be installed. With this release, SOAR is now an independent capability and has its own installation file. If you need SOAR in your environment, ensure that you download the installation package specified for SOAR in the Understanding the Files to Download section and proceed to install SOAR as a separate capability.

End of Support Announcements

OpenText strives to ensure that our products provide quality solutions for your enterprise software needs, ensuring continuity in features for our customers. However, there are times when new products or features replace existing functionality, or the maintenance of a feature is no longer viable. When such a situation occurs, we find that we must stop supporting the product or feature.

The following functions, features, or products are no longer be supported or will not be supported after the indicated date:

ArcSight Dashboard and Widget SDK

Last available release: ArcSight Platform 24.2

ArcSight Platform 24.2 will be the last release that includes the ArcSight Dashboard and the Widget Software Development Kit (Widget SDK).

In lieu of using the Dashboard, you can access built-in reports and dashboards in the Reports Portal. You also can create new reports and dashboards there. Moreover, with Multi-tenancy enabled, you have access to the new Optics that give you insight into alerts and global security status.

Collectors and Connectors in Transformation Hub (CTH)

As announced in the 23.1 release, the Collectors feature and the Connectors in Transformation Hub (CTH) feature have been deprecated, and from the ArcSight Platform 24.2 release on, only existing collectors and CTH deployments are supported. You can continue managing your collectors and CTHs in the platform, but you cannot create any new ones.

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. OpenText 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 OpenText determines the root cause is the untested platform or configuration. According to the standard defect- handling policies, OpenText will prioritize and fix issues we can reproduce on the tested platforms.

Downloading Files

You can download the required installation or content packages.

Download the Installation Files

You can download installation packages for the products in the ArcSight Platform from the OpenText 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.

OpenText provides several options for deploying products in your environment.

See the guide that corresponds to your deployment:

- Administrator's Guide for the ArcSight Platform CE 24.2 - AWS Deployment
- Administrator's Guide for the ArcSight Platform CE 24.2 - Azure Deployment
- Administrator's Guide for the ArcSight Platform CE 24.2 - Google Cloud Deployment
- Administrator's Guide for the ArcSight Platform CE 24.2 - Off-Cloud Deployment

Understanding the Files to Download

Download the installation packages indicated in the table below. A check mark indicates that the file is required for the product. You will only need one copy of each file, regardless of the products that you intend to deploy.

For example, if you are deploying both Recon and Intelligence, both require the file arcsight-installer-metadata.n.n.n.n.tar. However, you would only need a single copy of this file to support both deployments.

	ESM Command Center	Intelligence	Recon	SOAR	Transformation Hub
All Deployments – Metadata					
arcsight-suite-metadata-n.n.n.n.tar	✔	✔	✔	✔	✔
All Deployments – Images					
core-n.n.n.n.tar	✔	✔	✔	✔	✔
esm-n.n.n.n.tar	✔			✔	
intelligence-n.n.n.n.tar		✔			
recon-n.n.n.n.tar			✔		
soar-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		✔	✔	✔	✔

The files are described below.

File Type	File Name	Description
All Deployments - Metadata	arcsight-suite-metadata-24.2.0-5.tar	Contains metadata for deployment of the OMT Management Portal
All Deployments - Images	esm-1.6.0-5.tar	Contains the images for deploying ArcSight ESM Web App
	core-24.2.0-5.tar	Contains the images for deploying the Core functionality
	intelligence-6.4.13-5.tar and Intelligence-6.4.13-5-Bundle-License.txt	Contains the images for deploying the Intelligence capability
	recon-1.6.0-5.tar	Contains the images for deploying the Recon capability
	soar-3.11.0-5.tar	Contains the images for deploying the SOAR capability
	transformationhub-3.7.4-5.tar	Contains the images for deploying the Transformation Hub capability
All Deployments - Dashboard Widgets	widget-sdk-3.2.25.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-24.2.0-6.zip	Contains files for installing the infrastructure where you want to deploy capabilities, including the following content: • OMT installer • ArcSight Database installer - db-installer_n.n.n.n.tar.gz • Configuration files for the Installer (off-cloud only) and its example scripts You can find this file under Transformation Hub on the Software Downloads page
Cloud Deployments	arcsight-platform-cloud-installer-24.2.0-6.zip	Contains the installation files for deploying capabilities to Amazon Web Services, Azure and Google Cloud
Recon Appliance	RECON-R7615-R8X00-RH92-FIPS-STIG-24.2.0-1.iso	Contains the image to restore a Recon appliance to its factory settings

Downloading and Verifying the Installation Files

To download and verify the signature of your downloaded files:

1. Log in to the host 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 OpenText Downloads website along with their associated signature files (*.sig).

   Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the **Get the Public Keys** procedure).

   OpenText provides a digital public key that is used to verify that the software you downloaded from the OpenText software entitlement site is indeed from OpenText and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the OpenText 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 OpenText Customer Support.

   If Intelligence is deployed on the ArcSight Platform, there is no provision to enable multi-tenancy on the platform. Therefore, consider the following:
   • Do not download the Intelligence related files if you are installing the ArcSight Platform 24.2.
   • Download the Intelligence related files if you are upgrading Intelligence with the ArcSight Platform from 24.1 to 24.2 and you do not require the upgraded platform to be multi-tenant enabled. You can enable multi-tenancy on the upgraded platform at a later stage, wherein you must first uninstall Intelligence, and then enable multi-tenancy from the **Reconfigure** tab in the OMT portal.

4. Begin the installation.

   For more information about the installation process for your specific deployment, look for the **Planning to Deploy the Platform** and **Deployment** checklist.

   See the guide that corresponds to your deployment:

   - Administrator's Guide for the ArcSight Platform CE 24.2 - AWS Deployment
   - Administrator's Guide for the ArcSight Platform CE 24.2 - Azure Deployment
   - Administrator's Guide for the ArcSight Platform CE 24.2 - Google Cloud Deployment
   - Administrator's Guide for the ArcSight Platform CE 24.2 - Off-Cloud Deployment

Download Content Packages

If you enable Multi-tenancy and integrate with ArcSight ESM, you can ingest alerts and use the optics in ArcSight Platform. You will need the content package `ArcSight_Provider_Portal.arb`, which can be downloaded from Software Licenses and Downloads (SLD).

For more information, see Configuring Network and Zone Model in ArcSight ESM.

Certain content packages require paid licenses.

Known Issues

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

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

All issues listed in this section belong to the OCTCR33I repository, unless otherwise noted.

Known Issues Related to ArcMC

- "363017 — On G10 Appliance, IP Address Not Correctly Configured After Restore" on page 28
- "359190 — On G10 Appliance, ArcMC Does Not Validate IP Addresses for NIC Ports" on page 28

736019 — Selecting a value for ArcMC Container Memory Limit Returns an unformatted screen error

This error only happens under specific circumstances:

- When attempting to save the new memory limit or Fusion configuration before previous changes were saved (while the `fusion-arcmc-web-app` pod is restarting and stages are still updating)
- When the ITOM Management Portal session has timed out

Workaround: Perform the following steps:

1. Ensure that your session is active in the **ITOM Management Tool** and the **Reconfiguration** page. Login again if the session has timed out.
2. Execute the following command through `ssh`:

   ```
   kubectl get pods -A | grep "NAME\|arcmc-web-app"
   ```

   The output of the command should show a value of **4/4** (the pod's **READY** state) and of **Running** (the pod's **STATUS**) for the `fusion-arcmc-web-app` pod.
3. Go to the **ITOM Management portal** and click on the 3 dots menu. Select the **Reconfigure** option.
4. Go to **ArcMC Configuration** and select a value for **ArcMC Container Memory Limit** (4GB, 5GB, 6GB, 7GB or 8GB).
5. Click the **Save** button.

698065 — On Azure, Intermittent Login Errors

In some circumstances on Azure, there may be intermittent login and backend errors between Fusion, ArcMC and Kafka Manager.

Workaround: No known workaround for this release.

648050 — Routing Rules Character Limitations

Historically, ArcMC users could create Transformation Hub routing rules that test a string field's value against text entered by a user. For example, "agent == abc". To prevent browser problems, ArcMC was changed in a previous release to reject some non-alphanumeric characters when defining field value tests in a routing rule. Existing rules that used those characters still work, but new field value tests cannot use those characters. New field tests can only use alphanumeric characters and the five following five characters: underscore (_), hyphen (-), colon (:), space ( ), and period (.).

612094 — 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)
```

425040 — In Deployment/Topology View, Logger or ESM Destination for TH Shows Unknown IP Address

When in Deployment/Topology view, the IP address of a Logger or ESM destination for Transformation Hub shows as an unknown IP.

Workaround: No known workaround for this release.

408195 — 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.

408194 — 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.

363022 — On G10 Appliance, Gateway Not Correctly Configured After Restore

For G10 Appliances with a 10G NIC, after a restore, the gateway is not correctly configured.

Workaround: From the CLI, modify the IP address and gateway with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".

363017 — On G10 Appliance, IP Address Not Correctly Configured After Restore

For G10 Appliances with a 10G NIC, after a restore, the IP address is not correctly configured.

Workaround: From the CLI, modify the IP address with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".

359190 — On G10 Appliance, ArcMC Does Not Validate IP Addresses for NIC Ports

On G10 appliances, ArcMC does not validate when the user enters invalid IP values when trying to modify the "IP Address" or the "Subnet Mask" field from a network interface (or also called NIC port).

Workaround: No known workaround for this release.

Known Issues Related to ESM

These known issues apply to the ESM capability in your ArcSight Platform deployment. All the issues listed here belong to the OCTCR33I repository, unless otherwise noted.

896079 — ESM Web App Loads Indefinitely When ESM Host is Not Configured in OMT

Issue: If the ESM capability is enabled, and the ESM host has not been configured in the admin page, the ESM Web App gets stuck in loading status.

Workaround: Ensure that the ESM host has been configured in the admin page, and that the `OSP` configuration is set to integrate with ESM according to the instructions provided in the guide.

899136 — After upgrading OMT from 24.1 to 24.2, the ESM Web App might not restart properly on its own

Issue: The `ESM Web App` pod might not restart properly after the platform has been upgraded to 24.2, and the about box might still show the old version of the app.

Workaround: Restart the `ESM Web App` pod manually.

Known Issues Related to Intelligence

These known issues apply to the Intelligence capability in your ArcSight Platform deployment. All the issues listed here belong to the OCTCR33I repository, unless otherwise noted.

773025 — Changing the BOT_CLEANER_ENABLED Value Through Swagger UI Results in Internal Error

Issue: In the Intelligence **API Documentation** > **Tuning API** > **Parameters** > **PUT /{tid}/parameters/{name}**, changing the **BOT_CLEANER_ENABLED** parameter value from 0 to 1 results in an internal error and its value remains as 0.

Workaround: Execute the following query from a database node:

```
UPDATE default_secops_intelligence.PARAMETERS SET  val= '1.0' where
NAME='BOT_CLEANER_ENABLED';
```

729040 — SearchManager Pods Fail Due to the Absence of Spacing in the Elasticsearch Data Retention Period Value

Issue: In the **OMT Management Portal** > **Configure/Deploy** Page > **Intelligence** > **Elasticsearch Configuration** > **Elasticsearch Data Retention Period** field, if you specify a value without providing a space between the colon and the number of days, the SearchManager pods fail to start and instead enter into a CrashLoopBackOff state.

Workaround: Ensure that you include a space when specifying the value of the **Elasticsearch Data Retention Period** field. For example, a value of 0: 90 is valid, where 0 is the tenant ID, 90 is the number of days to retain the Elasticsearch Indices, and there is a space between : (colon) and 90. A value of 0:90 is invalid because there is no space between : (colon) and 90.

611096 — 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 OMT Management Portal: `https://<omt_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`.

616036 — 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.

400584 - 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 OMT 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
   ```

399297 - 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 OMT 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
   ```

401549 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Space or a Special Character

Issue: In the **OMT Management Portal** > **Configure/Deploy** page > **Intelligence** > **KeyStores** section > **KeyStore Password** field, if you specify a password that starts with a space or 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 space or a special character.

614051 - 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 OMT 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>
```

614042 - 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.

613048 - Repartition Percentage Threshold

Issue: In the **OMT 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.

614047 - Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container

Issue: In the **OMT 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 OMT 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
```

613050 - Installer Does Not Validate the Value You Specify for Elasticsearch Data Retention Period

Issue: In the **OMT 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.

614049 - 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 OMT 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.

613051 - 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.

Known Issues Related to Platform

These issues apply to the ArcSight Platform. For more information about issues related to a specific product, please see that product's release notes.

OpenText strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit OpenText Support, and then select the appropriate product category. All issues listed below belong to the OCTCR33I repository, unless otherwise noted.

900075 — Fails to Connect to a Logger in a FIPS-enabled Deployment

Issue: When you attempt to migrate data from a Logger and you have a FIPS-enabled environment, it's possible that the connection to the Logger will fail. This issue occurs when the ssh-keyscan fails in FIPS mode. You will see the following error:

`Error: Failed to create Logger connection` *`[logger_address]`*

Workaround: If this issue occurs, you should set up an SSH connection between the Logger and the database. This workaround applies to an off-cloud deployment of the ArcSight Database on a server running RHEL 9.2 as well as on an appliance for ArcSight Recon.

1. Log in to the database server:
   - *For an off-cloud deployment:* Log in to the primary ArcSight Database node as a `root` user.
   - *For a Recon appliance:* Log in as an ArcSight user.
2. If your login credentials do not have the database administrator permissions, change to a database admin user:
   - *For an off-cloud deployment:* `su - [dbadmin_username]`
   - *For a Recon appliance:* `sudo su - [dbadmin_username]`
3. To set up a SSH connection with the Logger, enter the following command:

   ```
   ssh -oUserKnownHostsFile=/home/[dbadmin_username]/known_loggers [host_username]@[IP_address_or_name_of_logger_host]
   ```

   where *[host_username]@[IP_address_or_name_of_logger_host]* represents the Logger.
4. Accept the `hostkey` when prompted.
5. Log out of the server.

6. To register the Logger:
   a. Log in to ArcSight Platform, then select **Configuration** > **Import Logger Data** > **Logger Metadata Import**.
   b. Follow the steps described in the Help for registering a Logger.
   c. When prompted, enter the IP address or host name that you specified in Step 3 above.

898339 — AWS Fresh Installation Fails on EKS Later Than 1.28.3

Issue: A fresh installation wil fail if you select an EKS version that is later than version 1.28.3.

Workaround: Select one with an earlier version number.

888044 — Kernel Crashing on DB Nodes in GCP

In order to use the ArcSight Database in a VM instance in GCP, the OS must be upgraded to RHEL 9.4. To upgrade a VM instance in GCP to RHEL 9.4, do the following:

1. Create a VM instance using the boot disk RHEL 9.
2. SSH to the new VM.
3. Upgrade the OS by running the command:
   `sudo yum upgrade`
4. To confirm the upgrade to RHEL 9.5, run the command:
   `cat /etc/redhat-release`

886046 — Erroneous Error Message in Database Installer Log

Issue: When you install the ArcSight Database in an AWS deployment, the `db-installer.log` file might list the following error:

```
 -bash: line 1: dbadmin: command not found
 ++++++ execute :  select cluster from default_secops_adm_scheduler.stream_
clusters
 ERROR 4650: Schema "default_secops_adm_scheduler" does not exist
```

This error has no effect on database functionality.

Workaround: You can safely disregard the error message.

863005 — Upgrade to ArcSight 24.2 may fail with errors related to cluster connectivity

Issue: While running the ArcSight 24.2 upgrade you may receive error messages indicating failures on specific cluster nodes, with wording such as:

```
Failed to pull image localhost:5000/arcsight/pause:3.9 and logs shows
connection refused.
```

```
One of the itom-cdf-keepalived, kube-registry, itom-prometheus-crds pods
shows ImagePullErr status and shows connection refused when pod is described
by kubectl.
```

Workaround:

1. Attempt to re-run the upgrade.
2. If re-running the upgrade does not solve the problem, run the following command on every node where the error occurs:

   ```
   <OMT_HOME>/bin/kube-restart.sh
   ```

   For example:

   ```
   /opt/arcsight/kubernetes/bin/kube-restart.sh
   ```

3. Run the upgrade again.

If you run the manual upgrade and the version of firewall is equal or greater than `0.9.0` (`firewall-cmd --version`) you might prevent upgrade failures by running the following commands on every node:

```
firewall-cmd --add-forward
firewall-cmd --add-forward --permanent
firewall-cmd --add-interface cni0
firewall-cmd --add-interface cni0 --permanent
```

These steps are included into the `arcsight-install --cmd upgrade` command, so they're not necessary with `arcsight-install` upgrades.

844085 — An Operation to Add a New Role or Group to a User Succeeds, But the UI Does Not Update to Reflect the Change

Issue: When you add a new role or group to a user, the operation succeeds but the UI does not update to display the just added role or group against the user in the UI.

Workaround: Refresh the browser to view the expected changes.

750053 — Import Logger Status Does Not Update Correctly

Issue: The status does not update properly when a user tries to import Logger Archives. After the migration initiates, the status changes to "Pending Import," but it remains in that state until the migration completes. Additionally, the status does not update and remains in the "Not Started" state when you try to import metadata.

Workaround: Refresh the page.

614050 - Special Characters for the Database Credentials

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

- Space character
- Single quotes

Workaround: There is no workaround at this time.

534015 — 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 parameters
```

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

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

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

1. To recover the password, log in to the `cdfapiserver` database pod.
2. Log in to the itom-default database with the password 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
```

3. 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;
```

4. 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
```

470057 — 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.

411123 — 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.

112042 — 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.

Known Issues Related to Reports Portal

898369 - Exceptions When Running Logger Report Converter Tool

Issue: You might encounter exceptions when running the Logger Report Converter Tool in a FIPS enabled environment. These exceptions may be ignored. Instead, refer to the final tool output to confirm whether or not the reports were converted successfully and are listed under "Converted files," or if any were not converted and are listed under the "Failed files" output.

Workaround: There is no workaround at this time.

898212 - InetSoft Logger Report Converter Tool Does Not Handle Custom Logger Report Formats

Issue: The 24.2 release represents Phase One for implementing the Logger Report Converter Tool. The tool has been tested to successfully convert all of the "Standard" Logger reports. But, as of 5/29/2024, there are some remaining issues related to converting "Custom" Logger report because the tool does not support all of the attributes that may exist in "Custom" reports.

Workaround: Run the tool against exported "Custom" Logger Reports. Depending on the attributes used, some custom reports might convert successfully, as determined by the tool output under the "Converted files" output.

898076 — Tenants Should Not Create Top-level Reporting Folders

Issue: Currently, tenant Reporting users are able to create top-level folders immediately beneath the "Repository" folder. The "Repository" folder is located in the left navigation panel of Dashboard & Reports (if Multi-tenancy is enabled).

Workaround: As a best practice, tenant Reporting users should not create any top-level folders directly beneath the "Repository" folder. Instead, they should only create additional folders under their own "Custom Content" folder or under their under their own private "My Reports" folder.

589121 — Brush Option Does Not Highlight Parabox Charts

Issue: The brush option does not highlight parabox charts.

Workaround: There is no workaround at this time.

409268 — 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.

Workaround: There is no workaround at this time.

372067 — 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.

336023 — 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.

331194 — 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.

186007 — 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.

162054 — Warning Message is Displayed: Query Plan Prevents Materialized View (MV) Sharing

Issue: A warning message displays when two dashboards are created under the same data worksheet.

Workaround: Ideally, the system should share Materialized Views (MVs), but if different parameters are needed, different worksheets should be used.

Known Issues Related to Search

898088 — Search Tab Has a Black Background and User Cannot Create a New Search if the Search is Canceled While it is Still Running

Issue: The problem is caused when the user creates a query using fields that are not part of the selected fieldset. When the user executes the search, they will see an error that asks them to add this field to the fieldset. This is expected behavior.

The user then adds the missing field to the current fieldset and reruns the search. If they cancel the search while it is still running, the Search page displays a black background.

Workaround: Reload the page. To prevent the issue, wait for search execution to finish, delete that search, and create a new one.

837049 — Delete Scheduled Search Dialog Box is Missing the OpenText Branding Design

Issue: The dialog box for deleting scheduled searches has not been updated to the new OpenText branding design.

Workaround: There is no workaround for this issue.

793025 — Scheduled Searches: Unable to Navigate Through Page Elements Using the Tab Key

Issue: While working with scheduled searches, users cannot navigate through the interface using the Tab key. The Tab key does not respond.

Workaround: There is no workaround for this issue.

774031 — Under Certain Rare Conditions, the fusion-db-search-engine Pod Can Run into High Memory and CPU Utilization, Causing System Instability

Issue: Under certain rare conditions, fusion-db-search-engine pod can run into high memory and cpu utilization causing system instability.

Workaround: The system creates two live aggregate projections - categoryFieldsLAP and deviceFieldsLAP to aid in values auto-suggestion feature in Search for the following fields - categoryDeviceGroup,categoryObject,categoryOutcome,categorySignificance,categoryTechniq ue and DeviceVendor,deviceProduct,deviceEventClassId. This auto-suggestion feature is intended for low cardinality fields. In rare scenarios if you have wrongly configured custom data sources or have lot of different data sources, it can result in high cardinality for these fields. If you are seeing high resource utilization for fusion-db-search-engine pod, run the following two queries to check the number of entries in the live aggregate projections -

select count(*) from default_secops_adm.categoryFieldsLAP;

select count(*) from default_secops_adm.deviceFieldsLAP;

If the count is >50K, it is going to be performant intensive to show so many in auto-suggest dropdown in UI. Drop that projection by running following command -

drop projection <projection_name> where projection_name can be default_secops_adm.categoryFieldsLAP or default_secops_adm.deviceFieldsLAP whose count is greater than 50K.

766026 — User Preferences Drop-down Menus are Closed if You Click in the Scrollbar

Issue: The user preferences drop-down menus closes if the user clicks in scrollbar. This issue only affects the preferences page.

Workaround: You can scroll down using mouse wheel or by using the keyboard.

757008 — Saving Real-time Searches as Fixed-time Searches: Incorrect Results Count Display on the Manage Search Tab after Auto-pausing by Selecting a Histogram Bar

Issue: After saving a Real-time Search as a Fixed-time Search, a wrong number displays for the amount of results in the **Manage Search** > **Search Results** page.

Workaround: The issue only occurs on the **Search Results** page. If you click on the saved search results to open them in a new tab, the correct amount of results displays on the **Search** tab. If you reload/refresh the Search Results page the latest data is retrieved and the correct amount of search results will be shown.

674039 — System Erroneously Clears All Search Data Instead of Refreshing the Search Results

Issue: When you attempt to refresh current search results, the system might erroneously clear all data from the Results Table and Events Histogram. This issue can occur if no new data is available and the search includes the following settings:

- Fixed-time search
- Query contains the *top*, *bottom*, *chart*, or *stats* operator

The system might also fail to inform you that no new data is available for the refresh.

Workaround: Run the search in a new tab.

609036 — 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 settings.

608115 — 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.

Workaround: There is no workaround at this time.

610161 — Incorrect search result when filtering with "id" field

Issue: Queries that filter specific "Id" field values will not return correct results. For example, results for the following are not correct: id = "123456789" or id != "123456789:

Workaround: There is no workaround at this time. We suggest not using the "Id" field directly in queries.

179782 — 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 selected hours and minutes, specify specific hours from the option **Specific Hour** and minutes from the **Starting From** setting.

113040 — 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

Known Issues Related to SOAR

These resolved issues apply to the SOAR capability in your ArcSight Platform deployment. Issues listed here belong to the OCTCR33I repository, unless otherwise noted.

598065 — SOAR Productivity Widget does not show Velocity Graph

Issue: Case closure velocity widget does not show velocity graph.

Workaround: There is no workaround for this issue.

900026 — CapabilityTypeRecordListener Error during Table Sort

Issue: While running the application for table sort, a CapabilityTypeRecordListener is diplayed.

Workaround: There is no workaround for this issue.

877030 — Postgres DB Backup/Restore Script Should Support Pre-Schema Restoration

Issue: Postgres DB backup/restore script does not support pre-schema restoration.

Workaround: There is no workaround for this issue.

895045 — SOAR Permissions and Respond in Left Navigation is Shown Even After Undeploying SOAR

Issue: SOAR permissions and respond shouldn't be displayed after undeploying SOAR

Workaround:Removing all Respond (SOAR) permissions..

900041 - SOAR Swagger UI is Not Accessible for MSSP Users

Issue: MSSP users won't be able to access the SOAR Swagger UI. Non-MSSP customers will be able to use the Swagger UI as normal. SOAR REST API works for both MSSP and Non-MSSP customers.

Workaround: YAML file can be accessed via <ArcSight Host>/soar-api/api/v1/openapi.yaml?tenant =<tenant-key> using the SOAR REST API Client Credentials.

Known Issues Related to Transformation Hub

891218— Multi-tenancy Does not Support Transformation Hub Compression Algorithm ZSTD

Issue: If Multi-tenancy is enabled, the Transformation Hub compression algorithm *zstd* is not supported.

Workaround: Ensure the Transformation Hub compression algorithm is set to the supported option, *gzip*.

609152— 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.

609151— 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 could contain unintended CEF events.

409228 — Schema Registry Instances May Be Allocated to Single Worker Node

Transformation Hub is often deployed as a multi-node service. 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 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.

Workaround: The following procedures should be run on the Transformation Hub master node.

1. Identify the worker nodes that are running Schema Registry instances:

```
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"
```

If the output shows all instances are running on the same worker node, Schema Registry must be restarted to spread the instances across worker nodes.

2. Restart Schema Registry.

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

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.

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

After the restart completes, verify the instances are now running on different worker nodes.

```
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).

3. In a multi-node deployment, identify the replica count for the topic "_schemas". Set the topic to be used in later commands.

   ```
   topic="_schemas"
   ```

4. Print the replication factor.

```
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 3, perform the following steps to change the configuration: 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.

```
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
```

6. Generate a replica configuration file.

```
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"
```

7. Use the file to add the replica configuration:

```
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.
```

8. Verify the reassignment completes by running a verify command with the same input file.

```
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 say this:

```
Reassignment of partition th-arcsight-avro-sp_metrics-0 completed successfully
```

9. Since the replicas have changed, run a preferred leader election for the topic's partition.

```
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
```

Verify the topic now has three replicas:

```
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. In a multi-node deployment, identify the replication factor for the topic "th-arcsight-avro-sp_metrics".

10. Set the topic to be used in later commands.

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

Repeat all of steps 4 and 5 above to check the topic and modify it if needed. The topic needs to have the same replica count as the previous topic: three.

377141 — Event Integrity Enablement Stops Enrichment Stream Processor Pods

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

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

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.

All issues listed in this section belong to the OCTCR33I repository, unless otherwise noted.

Resolved Issues Related to Upgrade

876045 — Upgrade Process Previously Could Cause Data Loss by Changing Retention Value to One Month

Previously, when you upgraded the database, the process could potentially reset the data retention value for storage groups to the default of one month. If this happened, the system

could erroneously purge data you wanted to retain. (This is because the data purge job runs at midnight on the first day of each month.)

This issue occurred when the autopass pod was down but the fusion-search-web-app and fusion-search-and-storage-web-app pods were 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.) A software update resolved the issue.

Resolved Issues Related to Intelligence

These resolved issues apply to the Intelligence capability in your ArcSight Platform deployment:

- "729040 — SearchManager Pods Fail Due to the Absence of Spacing in the Elasticsearch Data Retention Period Value" below
- "611096 — Analytics Fails to Load Data Sources Except for AD and Proxy" below

729040 — SearchManager Pods Fail Due to the Absence of Spacing in the Elasticsearch Data Retention Period Value

Issue: In the OMT Management Portal > Configure/Deploy Page > Intelligence > Elasticsearch Configuration > Elasticsearch Data Retention Period field, if you specify a value without providing a space between the colon and the number of days, the SearchManager pods fail to start and instead enter into a CrashLoopBackOff state.

Fix: This issue has been resolved now. You must specify a value without providing a space between the colon and the number of days. For example, 0:90.

611096 — 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 Resources, Share, VPN, and Repository.

Fix: This issue has been resolved now.

Resolved Issues Related to Reports Portal

779004 — VPM Conditions/Triggers are now Being Applied for Scheduled Dashboards

Previously, Virtual Private Models (VPM), Scheduled "Dashboards" would not return any data. A code change resolved this issue.

773027 — Restored Ability to Specify Time Ranges for Custom Reports and Dashboards Because the Enter Parameters Modal is not Displayed

A software fix now allows a custom report that is **not** based on one of the OpenText Standard Content "Data Worksheets" to successfully apply your specified date range.

566085 — Network Chart Data are No Longer Presented in Portions and Cut

A correction to the code now allows the Network chart to display data without truncating portions of it.

Resolved Issues Related to Search

733209 — Scheduled Searches no Longer Display an Error When You Try to Load a Field Summary on a Completed Run

A code fix resolved an issue for scheduled searches that occurred when you tried to load a field summary on completed runs that contained aggregation operators. Previously, you received the following error: "Cannot retrieve the summary number of events per field. Please reload the search." and field summary dialog box closes itself.

616090 — For System Search Queries, #SSH Authentication No Longer Generates an Error

A code fix resolved the issue where #SSH Authentication threw an error when a system query was executed. The error message stated: "Fix error in query first: Cannot use free-form text after "and" or "where" operators."

608098 — Certain top/bottom Queries and Fields that Begin With "Device" no Longer Fail

A code change resolved the problem where queries that use the **top/bottom** search operator along with fields that begin with "Device" would fail completely or partially.

Cases that previously failed all the time contained fields that began with "Device" and used the other fields listed below.

| top Device Receipt Time

| top Device Event Class ID

| top Device Event Category

Cases that failed intermittently also used another pipe operator or failed when the user kept 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

Resolved Issues Related to SOAR

These resolved issues apply for the SOAR capability in your ArcSight Platform deployment:

- 591118 - Enrichment History - Sort By Capability And Status Functionality Does not Sort By Alphabetical Order
- 655004 - SOAR FortiAnalyzer Plugin Should Accept Dynamic Ports
- 724037 - Enhancement - SOAR Should Support Updating User's Email Address and Username When Changed in FUM
- 719017 - Proxy Option Missing in SMTP Mail Server Integration Configuration
- 737015 - API Documentation soar-api/js-api-doc Search Does Not Work
- 8502032 - ''Access Denied'' Error During Action Rollback with Manage SOAR Integrations Permission
- 853043 - SOAR Response Headers Returning Only One Header Key Value Even When Multiple Keys Are Present
- 853078 - EWS Mail Receiver Should Get All Body Content
- 854004 - Case and Alerts Details Missing in Email Notification
- 857027 - Access is Denied when Creating a Search in SOAR cases including Alert Source Rule Name Condition
- 866085 - CreateTicketComment Method Does Not Work Properly
- 877024 - Missing Job ID Scope Item in EnCase Plugin
- 880090 - SOAR Performance Issue Due to Lack of Index for Ticket Table
- 190609 - Missing Type Parameter in Scope Action Parameter

591118 - Enrichment History - Sort By Capability And Status Functionality Does not Sort By Alphabetical Order

Now in Enrichment history, Sort By and Status functionality sorts in alphabetical order.

655004 - SOAR FortiAnalyzer Plugin Should Accept Dynamic Ports

Now SOAR FortiAnalyzer plugin accepts dynamic ports.

724037 - Enhancement - SOAR Should Support Updating User's Email Address and Username When Changed in FUM

Now SOAR supports updating users email address and username when changed in FUM.

719017 - Proxy Option Missing in SMTP Mail Server Integration Configuration

Now proxy option is available in SMTP mail server integration configuration.

737015 - API Documentation soar-api/js-api-doc Search Does Not Work

Now API documentation search works as expected.

8502032 - ''Access Denied'' Error During Action Rollback with Manage SOAR Integrations Permission

Now there is no error during action rollback with manage SOAR Integrations permission.

853043 - SOAR Response Headers Returning Only One Header Key Value Even When Multiple Keys Are Present

Now SOAR response headers return multiple header key value.

853078 - EWS Mail Receiver Should Get All Body Content

Now EWS mail receiver gets all body content.

854004 - Case and Alerts Details Missing in Email Notification

Now Case and Alerts details are mentioned in email notification.

857027 - Access is Denied when Creating a Search in SOAR cases including Alert Source Rule Name Condition

Now you can create a search in SOAR cases including alert soure rule name condition.

866085 - CreateTicketComment Method Does Not Work Properly

Now CreateTicketComment method works as expected.

877024 - Missing Job ID Scope Item in EnCase Plugin

Now Job ID scope item is visible in EnCase plugin.

880090 - SOAR Performance Issue Due to Lack of Index for Ticket Table

Now SOAR is able to query the status of cases.

190609 - Missing Type Parameter in Scope Action Parameter

Now type parameter is present in scope action parameter.

Resolved Issues Related to Transformation Hub

849027--Transformation Hub Routing rules now work correctly when using the NOT operator in multiple conditions.

Routing rules will now work correctly when the NOT operator is used for multiple conditions. Previously, if the NOT operator includes all conditions in a rule, this would cause a problem in the rule expression, resulting in the NOT condition being ignored and nothing being filtered.

Contacting OpenText

For specific product issues, contact OpenText Support.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos.
- The OpenText 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.

  See the guide that corresponds to your deployment:

  - Administrator's Guide for the ArcSight Platform CE 24.2 - AWS Deployment
  - Administrator's Guide for the ArcSight Platform CE 24.2 - Azure Deployment
  - Administrator's Guide for the ArcSight Platform CE 24.2 - Google Cloud Deployment
  - Administrator's Guide for the ArcSight Platform CE 24.2 - Off-Cloud Deployment
- *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 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: Wednesday, June 5, 2024

Updated: Tuesday, June 4, 2024