opentext™

ArcSight Platform

Software Version: CE 24.1.1

ArcSight Platform CE Release Notes

Document Release Date: February 2024
Software Release Date: February 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 24.1.1

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	24.1.1 (7.7.0)
ArcSight Intelligence	24.1.1 (6.4.11)
ArcSight Recon	24.1.1 (1.5.7)
Transformation Hub	24.1.1 (3.7.3)
ArcMC	24.1.1 (3.2.3)

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

The 24.1.1 release is a suite patch to address a critical vulnerability in ArcSight Platform (CVE-2024-1811).

Technical Requirements

To upgrade to this release, you must have version 24.1.0 of ArcSight Platform installed in your environment.

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 the ArcSight Platform Patch Upgrade Files

Before you apply this release, you must have version 24.1.0 of the ArcSight Platform installed in your environment.

You can download upgrade packages for the products in the ArcSight Platform from the OpenText Downloads website. The upgrade 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. For more information about deploying products, see the *Administrator's Guide for ArcSight Platform*.

- "Understanding the Files to Download" below
- "Downloading and Verifying the Upgrade Files" on page 13

Understanding the Files to Download

Download the file 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	Transformation Hub
All Deployments – Metadata				
arcsight-suite-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		✔	✔	✔

The files are described below.

File Type	File Name	Description
All Deployments - Metadata	arcsight-suite-metadata-24.1.1-11.tar	Contains metadata for deployment of the OMT Management Portal
All Deployments - Images	esm-1.5.0-2.tar	Contains the images for deploying ArcSight ESM Web App
	fusion-1.9.1-11.tar and Arcsight-Fusion-24.1-v1.9.0-Bundle-License.txt	Contains the images for deploying the Fusion capability
	intelligence-6.4.11-2.tar and Intelligence-24.1-v6.4.11-Bundle-License.txt	Contains the images for deploying the Intelligence capability
	layered-analytics-1.3.5-2.tar	Contains the images for deploying the Layered Analytics capability.
	recon-1.5.7-2.tar	Contains the images for deploying the Recon capability
	transformationhub-3.7.3-2.tar	Contains the images for deploying the Transformation Hub capability
All Deployments - Dashboard Widgets	widget-sdk-3.2.23.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-24.1-2.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-24.1-2.zip	Contains the installation files for deploying capabilities to Amazon Web Services, Azure and Google Cloud

Downloading and Verifying the Upgrade Files

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to upgrade deployed capabilities.
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.
4. Begin the suite upgrade. For more information about the upgrade process for your particular environment, see the section of *Administrator's Guide for ArcSight Platform* corresponding to your deployment type:

- Upgrading Deployed Capabilities
- Upgrading Deployed Capabilities in AWS
- For Azure: Upgrading the ArcSight Suite
- Upgrading Deployed Capabilities in Google Cloud

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

736019 — Selecting a value for ArcMC Container Memory Limit throws 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 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.

- 614042 — Daylight Savings Time
- 613048 — Repartition Percentage Threshold
- 614047 — Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container
- 614048 — Certificate Warnings in Logstash Logs
- 613050 — Installer Does Not Validate the Value You Specify for Elasticsearch Data Retention Period
- 614049 — Uninstalling Intelligence Does Not Delete All Files
- 613051 — Unable to Retrieve Indices When Elasticsearch Cluster is Unstable

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.

606124 — 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**.

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`.

613042 — 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 616036) in order to be taken to the intended page.

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>
```

378083 - 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.

614050 - 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.

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
```

614048 - 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.

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.

879004 — After 24.1.1 Upgrade, ArcSight Product Version Number is Not Updated in UI

After an upgrade from 24.1 to 24.1.1, the About Products box and other UI elements will incorrectly show the product version as 24.1 instead of 24.1.1.

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.

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. 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
```

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

779004 — VPM Conditions/Triggers are not Being Applied for Scheduled Dashboards

Issue: For Virtual Private Models (VPM), Scheduled "Dashboards" will not return any data.

Workaround: Run the "Dashboard" through the reporting web portal instead.

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

Issue: If a custom report is **not** based on one of the OpenText Standard Content "Data Worksheets", then the date range prompt will be ignored and the default date range will always be used.

Workaround: Add or implement your own Date Range prompt to your custom reports.

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.

566085 — 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. OpenText recommends that you do not use the Network chart 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.

171158 — 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.

Known Issues Related to Search

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.

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.

616090 — For System Search Queries, #SSH Authentication Throws an Error

Issue: #SSH Authentication throws the following error when a system query is executed: "Fix error in query first: Cannot use free-form text after "and" or "where" operators."

Workaround: Expand the out of the box system query and correct the syntax before executing the search.

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 details.

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.

608098 — 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 list of auto-suggested options that are displayed as you enter the query. This applies to any field the user is not able to type in.

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

Issues Related to SOAR

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

- 719017 — Proxy Option Missing in SMTP Mail Server Integration Configuration
- 591118 — In Enrichment History, the Sort By Capability and Status Functionality Does Not Sort by alphabetical Order
- 655004 — SOAR FortiAnalyzer Plugin Should Accept Dynamic Ports
- 724037 — SOAR Does Not Reflect Changes made in User's Email Address and Username.
- 591117 — INetSoft Reports Load with an Error
- 598065 — SOAR Productivity widget does not show velocity graph

719017— Proxy Option Missing in SMTP Mail Server Integration Configuration

Issue: When configuring SMTP Mail Server integration, the proxy option is missing from the configuration settings.

Workaround: There is no workaround at this time.

591118 — In Enrichment History, the Sort By Capability and Status Functionality Does Not Sort by alphabetical Order

Issue: The Sort By Capability and Status Functionality does not sort by alphabetical order.

Workaround: There is no workaround at this time.

655004 — SOAR FortiAnalyzer Plugin Should Accept Dynamic Ports

Issue: SOAR FortiAnalyzer plugin does not accept dynamic ports

Workaround: There is no workaround at this time.

724037 — SOAR Does Not Reflect Changes made in User's Email Address and Username.

Issue: SOAR does not reflect changes made in User's email address.

Workaound: There is no workaround at this time.

591117 — INetSoft Reports Load with an Error

Issue: INetSoft reports load with an error listing about 3,000,000 row limit.

Workaround: There is no workaround at this time.

598065 — SOAR Productivity widget does not show velocity graph

Issue: SOAR productivity widget does not display velocity graph

Workaround: There is no workaround at this time.

Known Issues Related to Transformation Hub

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 may 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.

241208—If Cluster Has Firewall Enabled, Kafka Consumer IPs Shown as Cluster Internal IPs in CMAK

On a cluster whose nodes have a firewall enabled, Kafka consumer IP addresses are shown as cluster internal IP addresses on the Kafka consumers list in CMAK.

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 Documentation

609183 — Using the COPY option for a command includes extra tags if text in the command is highlighted from a search

A code fix resolved the issue where the text being searched for affects the copy command.

Resolved Issues Related to Intelligence

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

494001 — 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/

A code change addressed this issue.

Resolved Issues Related to Platform

752115— Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Installation no Longer Times out when IPv6 is Disabled on the Host Node

A code fix was applied to resolve the issue where the ArcSight Platform Installation timed out with IPv6 disabled on the host node.

736005—Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Upgrade from 23.1 to 23.2 or 23.3 no Longer Fails when IPv6 is Disabled on the Host Node

A code fix was applied to resolve the issue where the ArcSight Platform Upgrade failed with IPv6 disabled on the host node.

Issues Related to Reporting

162021 — Removing X/Y Fields from a Graph is Resolved

Previously in the chart editor, when you removed an X or Y field, the Reports Portal intermittently displayed an error message. A code update resolved this issue.

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.

610160 — Field "Id" is Available to Use With the top, bottom, rename, eval, and wheresql Operators

A software update now allows queries that use the search operators **top**, **bottom**, **rename**, **eval**, and **wheresql** to properly recognize the "Id" field as a column, regardless of the Fieldset used.

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.

776014 — SOAR shows Page unresponsive error when clicked from Reports > SOAR > Open Cases

Now SOAR page is responsive when clicked from Reports > SOAR > Open Cases.

775003 — For analyst user Configuration is Navigating to Cases Page When Clicked From RESPOND->CASES->CONFIGURATION

Now User Configuration is navigating to Cases page.

735021— Clickable Items Should Have Clickable Cursor Icon

Now Clicable Items have the clicable curson icon.

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.
- *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 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: