

# ArcSight ArcSight Platform

Software Version: 23.2.1

## ArcSight Platform Release Notes

Document Release Date: March 2024

Software Release Date: March 2024

## **Legal Notices**

Open Text Corporation

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

### **Copyright Notice**

Copyright 2001 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### **Trademark Notices**

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

# What's New

This suite patch addresses a critical vulnerability in ArcSight Platform (CVE-2024-1811).

# Technical Requirements

To upgrade to this release, you must have version 23.2.0 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. For more information about installing or upgrading to ArcSight Platform 23.2.0, see the [ArcSight Platform 23.2 Release Notes](#).



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 Files

Before you apply this release, you must have version 23.2.0 of the ArcSight Platform installed in your environment.

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. For more information about deploying products, see the [Administrator's Guide for ArcSight Platform](#).

- ["Understanding the Files to Download" below](#)
- ["Downloading and Verifying the Files" on page 8](#)



**Note:** If you have ArcSight Intelligence installed, please contact [OpenText Support](#) for an Intelligence hotfix before you install this patch.

## Understanding the Files to Download

Download the 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 are deployed.

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

	ESM Command Center	Intelligence	Recon	Transformation Hub
<b>All Deployments – Metadata</b>				
arcsight-suite-metadata-n.n.n.n.tar	✓	✓	✓	✓
<b>All Deployments – Images</b>				
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		✓	✓	✓
<b>All Deployments – Dashboard Widgets</b>				
widget-sdk-n.n.n.n.tgz <i>(optional)</i>	✓	✓	✓	
<b>On-premises Deployments</b>				
arcsight-platform-installer-n.n.n.n.zip	✓	✓	✓	✓
<b>Cloud Deployments</b>				
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-23.2.1-4.tar	Contains metadata for deployment of the OMT Management Portal
All Deployments - Images	esm-7.6.5.4.tar	Contains the images for deploying ESM Command Center
	fusion-1.7.3.4.tar and arcsight-fusion-1.7.2-bundle-license.txt	Contains the images for deploying the Fusion capability
	intelligence-6.4.7.4.tar and intelligence-6.4.7-bundle-license.txt	Contains the images for deploying the Intelligence capability
	layered-analytics-1.3.3.4.tar	Contains the images for deploying the Layered Analytics capability
	recon-1.5.4.4.tar	Contains the images for deploying the Recon capability
	transformationhub-3.7.1.4.tar	Contains the images for deploying the Transformation Hub capability
	All Deployments - Dashboard Widgets	widget-sdk-3.2.22.tgz
On-premises Deployments	arcsight-platform-installer-23.2.0.3.zip	<p>Contains files for installing the infrastructure where you want to deploy capabilities, including the following content:</p> <ul style="list-style-type: none"> <li>• OMT installer</li> <li>• ArcSight Database installer - db-installer_x.x.x.x.tar.gz</li> <li>• Configuration files for the <a href="#">Installer</a> (on-premises only) and its example scripts</li> </ul> <p>You can find this file under Transformation Hub on the Software Downloads page</p>
Cloud Deployments	arcsight-platform-cloud-installer-23.2.0.3.zip	Contains the installation files for deploying capabilities to Amazon Web Services and Azure

## Downloading and Verifying the 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 files.
3. Download all the necessary 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 following topics in the *Administrator's Guide for ArcSight Platform*:

- [Upgrading Deployed Capabilities](#)
- [Upgrading Deployed Capabilities in AWS](#)

# Known Issues Related to Upgrade

These issues apply to upgrading to this release.

- ["865171 - Upgrade Process Might Cause Data Loss by Changing Retention Value to One Month" below](#)

## 865171 - Upgrade Process Might Cause Data Loss by Changing Retention Value to One Month

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

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

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

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

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



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

# 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.

- [Issues Related to Documentation](#)
- ["Issues Related to Database Upgrade" on the next page](#)
- ["Issues Related to Platform" on page 12](#)
- ["Issues Related to Reports Portal" on page 16](#)
- ["Issues Related to ArcSight Management Center" on page 19](#)
- [Issues Related to Intelligence](#)
- ["Issues Related to Search" on page 37](#)
- ["Issues Related to SOAR" on page 40](#)
- ["Issues Related to Transformation Hub" on page 43](#)
- ["Issues Related to Database Upgrade" on the next page](#)
- ["Issues Related to Recon" on page 46](#)

## Issues Related to Documentation

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

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

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

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

[https://www.microfocus.com/documentation/arcsight/arcsight-platform-23.2/arcsight-admin-guide-23.2/#deployment\\_manual/database\\_setup.htm?Highlight=vault\\_pod](https://www.microfocus.com/documentation/arcsight/arcsight-platform-23.2/arcsight-admin-guide-23.2/#deployment_manual/database_setup.htm?Highlight=vault_pod)

## Issues Related to Database Upgrade

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

### OCTCR33I611095 — Issues Related to FIPS-enabled Database Node Fails

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

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

```
resume=$(grep swap /etc/fstab | awk '{ print $1 }')  
boot=$(grep '/boot' /etc/fstab | awk '{ print $1 }')  
sed -i "s/ resume=UUID / resume=$resume /g" /etc/default/grub  
sed -i "s/ boot=UUID / boot=$boot /g" /etc/default/grub  
  
grub2-mkconfig -o /boot/grub2/grub.cfg
```

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

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

```
create scheduler under: default_secops_adm_scheduler  
scheduler: create target topic
```

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

Rolling back scheduler creation...

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

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

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

See [Using ArcSight Platform Installer for an Automated On-Premises Installation](#) in the Administrator's Guide to ArcSight Platform 23.2.1 for more installation information.

## Issues Related to Platform

- ["OCTCR33I112042 — Pods Might Not Run During Fusion Reinstall"](#) below
- ["OCTCR33I411123 — Event Integrity Query Indicates Insufficient Disk Space \(AWS/Azure\)" on the next page](#)
- ["OCTCR33I470057 — Left Navigation Menu Items Do Not Reliably Display When Pods Restart or are Unresponsive" on the next page](#)
- ["OCTCR33I534015 — Autopass container crashing with exception: relation "mysequence" already exists" on the next page](#)
- ["OCTCR33I712038 — Error Message Returned on Single-Node Rocky Linux Environments" on page 14](#)
- [OCTCR33I736005—Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Upgrade from 23.1 to 23.2 when IPv6 is Disabled on the Host Node](#)
- ["OCTCR33I744020 — Upgrade from 23.1 Fails and Rerun Upgrade Also Fails" on page 15](#)
- [OCTCR33I752115— Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Installation Times out when IPv6 is Disabled on the Host Node](#)

### OCTCR33I112042 — Pods Might Not Run During Fusion Reinstall

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

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

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

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

**Workaround:** See [View Event Integrity Check Results](#) to help troubleshoot this issue.

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

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

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

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

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

```
starting DB with 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-xxxxxxxx-xxxxx -c itom-  
postgresql -- bash
```

```
# get_secret ITOM_DB_DEFAULT_PASSWORD_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
```

## OCTCR33I712038 — Error Message Returned on Single-Node Rocky Linux Environments

Rocky Linux is supported by OMT but not by the ArcSight Database. Accordingly, on single node Rocky Linux environments, users may encounter an error message that says "Checking Required OS..... [FAIL]" when running the pre-install. In order to deploy a single node environment, users must use a supported version of RHEL instead of Rocky Linux.

## OCTCR33I736005—Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Upgrade from 23.1 to 23.2 when IPv6 is Disabled on the Host Node

**Issue:** When ArcSight Platform 23.1 is installed on premises with IPv6 disabled on the nodes, if the cluster is attempted to be upgraded to Platform 23.2 this can result in the portal-ingress-controller pod failing with a CrashLoopBackOff status. The message "Address family not supported by protocol" is reported in the nginx-ingress-lb or stunnel container logs.

**Workaround:** Contact [OpenText Support](#) to obtain a hotfix with instructions to resolve the issue in either of the following scenarios:

- Before upgrade to prevent a failure
- After upgrade to recover from the failure

## OCTCR33I744020 — Upgrade from 23.1 Fails and Rerun Upgrade Also Fails

When upgrading a cluster from 23.1 to 23.1 using `arcsight-install` or `autoUpgrade` or `upgrade.sh`, and it fails on the step returning `** Start to upgrade Apphub chart ...` (Step 4/5), the attempt to re-run the upgrade also fails with this message `Failed to upgrade apphub chart.Error: UPGRADE FAILED: execution error at (apphub/templates/cdf-cm.yaml:3:30): ERROR: Unsupported usage scenario. CDF apiserver cannot use external database when `global.database.internal` flag is true.`

This issue occurs because the position of the chart capabilities info stored in helm values are moved during upgrade. When you rerun the upgrade, the script tries to get the values from the original place.

**Workaround:** To resolve this issue, do the following:

1. Run this command to get the current helm values:

```
helm get values apphub -n $CDF_NAMESPACE -o yaml > /tmp/apphub.yaml
```

2. Run this command to back up the current values:

```
cp /tmp/apphub.yaml /tmp/apphub.yaml.bak
```

3. Run these commands to edit the helm values:

```
yq -i e '.tags=.global.services' /tmp/apphub.yaml  
yq -i e 'del(.global.services)' /tmp/apphub.yaml
```

4. Run the command to apply the changes:

```
source $CDF_HOME/properties/images/charts.properties  
helm upgrade apphub -n $CDF_NAMESPACE -f /tmp/apphub.yaml ${CDF_  
HOME}/charts/${CHART_ITOM_APPHUB}
```

5. Run the upgrade again.

## OCTCR33I752115— Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Installation Times out when IPv6 is Disabled on the Host Node

**Issue:** ArcSight Platform 23.2 installation times out at the AppHub phase with the ITOM-CDF-Deployer Pod in an 'Error' state and the Postgres-Ingress-Controller pod in a CrashLoopBackOff status. The message "Address family not supported by protocol" is reported in the nginx-ingress-lb or stunnel container logs.

**Workaround:** Attempt the ArcSight Platform 23.2 installation in either of the following ways:

1. Enable IPv6 on all cluster nodes and re-run the installation:
  - a. Run "-cmd uninstall" first and then the installation
2. When unable to enable IPv6, install the ArcSight Platform manually with monitoring capabilities disabled as under:
  - a. Uninstall the failed node
  - b. Run a manual install to bootstrap OMT:

```
/install -m <path_to_a_metadata_file> --cdf-home <path_to_installation_directory> --nfs-server <your_nfs_server_FQDN or IP Address> --nfs-folder <itom_volume_folder> --capabilities ClusterManagement=true,DeploymentManagement=true,LogCollection=true,Monitoring=false,MonitoringContent=false,Tools=true
```

- c. Execute the following command:

```
helm upgrade apphub -n core /opt/arcsight/kubernetes/charts/apphub-mini-1.23.0+20230500.182.tgz --reuse-values --set portalIngress.nginx.service.external.sslClientCertCAscm=""
```

- d. Proceed to the Management Portal at port 3000. Set up the cluster and deploy the ArcSight Platform.

## Issues Related to Reports Portal

- ["OCTCR33I134098 — Edit Wizard Preview is Unavailable" on the next page](#)
- ["OCTCR33I162021 — Cannot Remove X/Y Fields from a Graph" on the next page](#)
- ["OCTCR33I186007 — An Exported Report Might Have Format Issues" on the next page](#)

- ["OCTCR33I331194 — Reports and Dashboards Use UTC Time Zone"](#) below
- ["OCTCR33I336023 — Operations Performed on an Open Admin Tab Do Not Complete After You Log Out From Another Capability \(Recon or Reporting\) Tab"](#) on the next page
- ["OCTCR33I372067 — Contract & Usage Page Throws an Ingress Router Error and Does Not Load"](#) on the next page
- ["OCTCR33I409268 — Reporting Shows an Error When Single Sign On Secrets are Changed \(Azure\)"](#) on the next page
- ["OCTCR33I566085 — Network Chart Data Presented in Portions and Cut"](#) on the next page
- ["OCTCR33I589121— Brush Option Does Not Highlight Parabox Charts"](#) on page 19
- ["OCTCR33I71158 — Scheduled Tasks Do Not Allow Default Printer Selection"](#) on page 19

## **OCTCR33I134098 — Edit Wizard Preview is Unavailable**

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

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

## **OCTCR33I162021 — Cannot Remove X/Y Fields from a Graph**

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

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

## **OCTCR33I186007 — An Exported Report Might Have Format Issues**

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

**Workaround:** Manually change the formatting for the exported report.

## **OCTCR33I331194 — Reports and Dashboards Use UTC Time Zone**

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

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

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

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

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

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

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

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

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

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

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

## **OCTCR33I566085 — Network Chart Data Presented in Portions and Cut**

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

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

## **OCTCR33I589121— Brush Option Does Not Highlight Parabox Charts**

**Issue:** The brush option does not highlight parabox charts.

**Workaround:** There is no workaround at this time.

## **OCTCR33I71158 — Scheduled Tasks Do Not Allow Default Printer Selection**

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

## **Issues Related to ArcSight Management Center**

- ["OCTCR33I612094 — Fusion ArcMC Throws 503 Error After Restoring Configuration Data \(AWS, Azure and On-premises\)" on the next page](#)
- [" OCTCR33I408195 — Importing a Host File on Fusion ArcMC Points to a Different Log Folder " on the next page](#)
- ["OCTCR33I408194 — Fusion ArcMC Session License Expiration" on the next page](#)
- ["OCT33I359190 -- On G10 Appliance, ArcMC Does Not Validate IP Addresses for NIC Ports" on page 21](#)
- ["OCT33I363017 -- On G10 Appliance, IP Address Not Correctly Configured After Restore" on page 21](#)
- ["OCT33I363022 -- On G10 Appliance, Gateway Not Correctly Configured After Restore" on page 21](#)
- ["OCT33I425040 -- In Deployment/Topology View, Logger or ESM Destination for TH Shows Unknown IP Address" on page 21](#)
- ["OCT33I698065 -- On Azure, Intermittent Login Errors " on page 22](#)
- ["OCT33I736019 -- Selecting a value for ArcMC Container Memory Limit throws an unformatted screen error" on page 22](#)

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

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

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

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

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

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

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

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

**Workaround:** No known workaround for this release.

## OCTCR33I408194 — Fusion ArcMC Session License Expiration

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

**Workaround:** No known workaround for this release.

## **OCT33I359190 -- 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.

## **OCT33I363017 -- 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".

## **OCT33I363022 -- 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".

## **OCT33I425040 -- 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.

## OCT33I698065 -- 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.

## OCT33I736019 -- 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.

## Issues Related to Intelligence

- [OCTCR33I729040 — SearchManager Pods Fail Due to the Absence of Spacing in the Elasticsearch Data Retention Period Value](#)

- ["OCTCR33I494001 — Analytics Does Not Detect the Custom SQL Loader Scripts After the Intelligence Upgrade"](#) on the next page
- ["OCTCR33I606124 — Multi-step Upgrade From 21.1.x to 23.1.x Fails on Suite Upgrade to 23.1 \(a Non-Cloud Release\)"](#) on page 26
- ["OCTCR33I611096 — Analytics Fails to Load Data Sources Except for AD and Proxy"](#) on page 26
- ["OCTCR33I613042 — Intelligence Sharing URL Functionality Does Not Work if the User Does Not Have an Active Session"](#) on page 27
- [OCTCR33I616036 — If Not Already Logged into Fusion, the First Attempt to Log Directly Into Intelligence Dashboard Will Fail](#)
- [OCTCR33I400584 - Either the Intelligence Search API or Login to the Intelligence UI or both Fail with a Timeout Error \(IOException: Listener Timeout\) for Large Data Sets in the Database](#)
- [OCTCR33I399297 - Intelligence Search API Fails with a Timeout Error \(esSocketTimeout exception\) for Large Data Sets in the Database](#)
- [OCTCR33I401232 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Space or Special Character](#)
- [OCTCR33I399665 - Elasticsearch and Logstash Pods Fail in an AWS Deployment Because of Permission Issues](#)
- [OCTCR33I604032 - Elasticsearch and Logstash Pods Fail in an Azure Deployment Because of Permission Issues](#)
- [OCTCR33I614051 - Logstash Pod Fails on Data Ingestion in AWS Deployment When Using Self-signed Certificates](#)
- [OCTCR33I378083 - Erroneous Warning about Recon License](#)
- [OCTCR33I614050 - Special Characters for Database Credentials](#)
- [OCTCR33I616054 - Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects](#)
- [OCTCR33I614042 - Daylight Savings Time](#)
- [OCTCR33I613048 - Repartition Percentage Threshold](#)
- [OCTCR33I614047 - Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container](#)
- [OCTCR33I614048 - Certificate Warnings in Logstash Logs](#)
- [OCTCR33I613050 - Installer Does Not Validate the Value You Specify for Elasticsearch Data Retention Period](#)
- [OCTCR33I614049 - Uninstalling Intelligence Does Not Delete All Files](#)
- [OCTCR33I613051 - Unable to Retrieve Indices When Elasticsearch Cluster is Unstable](#)

- [OCTCR33I399647 - HTTP Status 400 - Bad Request](#)

## OCTCR33I729040 — 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.

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

**Issue:** For AWS and Azure deployments, after the Intelligence upgrade from 22.1.0 to 23.1, analytics does not detect the custom SQL loader scripts of the previous version of Intelligence. Instead, it proceeds with the default SQL loader scripts present in <arcsight\_nfs\_vol\_path>/interset/analytics/vertica\_loader\_sql/0/1.12.4.27/

**Workaround:** Follow the steps below:

### Step 1: Perform the following steps before the upgrade:

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

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

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

```
mkdir 1.1.9.1.9
```

4. Navigate to the following directory:

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

- Execute the following command to move the SQL loader scripts from <arcsight\_nfs\_vol\_path>/interset/analytics/vertica\_loader\_sql/0 to <arcsight\_nfs\_vol\_path>/interset/analytics/vertica\_loader\_sql/0/1.1.9.1.9:

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

- Execute the following command to grant permissions to the 1.1.9.1.9 directory:

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

## Step 2: Upgrade the Intelligence capability.

For more information, see [Upgrading your Environment](#) in the [Administrator's Guide for ArcSight Platform](#).

## Step 3: Perform the following steps after the upgrade:

- Run Analytics to start the next analytics run. For more information, see [Running Analytics on Demand](#) in the [Administrator's Guide for ArcSight Platform](#).
- During the analytics run, the 1.12.4.27 folder is created in the following directory with the default SQL loader scripts:

```
cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.12.4.27
```

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

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

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

```
cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.12.4.27
```

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

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

```
cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.1.9.1.9
```

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

```
cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.1.9.2.9
```

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

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

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

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

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

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

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

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

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

1. Open a certified web browser.
2. Specify the following URL to log in to the 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`.

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

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

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

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

**Issue:** Logging in to Intelligence dashboard `https://<hostname>/interaset` 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>/interaset` will be successful.

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

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

**Workaround:** Perform the following steps:

1. Open a certified web browser.
2. Log in to the 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
```

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

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

**Workaround:** Perform the following steps:

1. Open a certified web browser.
2. Log in to the 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
```

## OCTCR33I401549 - 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.

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

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

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

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

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

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

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

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

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

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

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

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

```
df -h
```

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

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

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

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

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

**Issue:** In an AWS deployment of Intelligence, when data is ingested, the Logstash pod enters into a CrashLoopBackOff state from a Running state. This issue occurs if you have configured 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>
```

## OCTCR33I378083 - Erroneous Warning about Recon License

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

**Workaround:** There is no workaround for this issue.

## OCTCR33I614050 - Special Characters for the Database Credentials

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

- Whitespace
- Single quotes

**Workaround:** There is no workaround at this time.

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

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

**Workaround:** There is no workaround at this time.

## **OCTCR33I614042 - Daylight Savings Time**

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

**Workaround:** There is no workaround needed.

## **OCTCR33I613048 - Repartition Percentage Threshold**

**Issue:** In the **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.

## **OCTCR33I614047 - 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
```

## OCTCR33I614048 - Certificate Warnings in Logstash Logs

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

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

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

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

**Issue:** In the **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.

## **OCTCR33I614049 - Uninstalling Intelligence Does Not Delete All Files**

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

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

## **OCTCR33I613051 - Unable to Retrieve Indices When Elasticsearch Cluster is Unstable**

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

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

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

## OCTCR33I399647 - HTTP Status 400 - Bad Request

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

**Workaround:** Perform the following steps:

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

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

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

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

OR

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

11. Log in to Intelligence or other application user interfaces available for this domain such as the OMT Management Portal or the Fusion dashboard.
12. Using the **Developer tools** option in your browser, ensure that the **INTERSET\_SESSION** cookie is only available to request with `/interset` in the path.



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

## Issues Related to Search

- ["HERC-9865 — Fieldset Fails to Revert to its Original Setting"](#) below
- ["OCTCR33I113040 — CSV File Export Fails after You Change the Date and Time Format"](#) below
- ["OCTCR33I179782 — Scheduled Search Appends Erroneous Values to the Run Interval"](#) on the next page
- ["OCTCR33I608098 — Certain top/bottom Queries Refresh When the User Presses the Space Bar While Entering the Query"](#) on the next page
- ["OCTCR33I608115 — Vulnerabilities: System Query is Duplicated With Two Different Names"](#) on page 39
- ["OCTCR33I609036 — Upgrade Issues: Searches That Use the "All Fields" Fieldset and the "All Time" Time Range Do Not Complete"](#) on page 39
- ["OCTCR33I610160 — Unable to Use the Field "Id" With the top, bottom, rename, eval, and wheresql Operators"](#) on page 39
- ["OCTCR33I610161 and OCTCR33I615024 — Incorrect Search Results Occur When Filtering With the "Id" Field"](#) on page 40
- ["OCTCR33I616090 — For System Search Queries, #SSH Authentication Throws an Error"](#) on page 40

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

**Issue:** If you change a fieldset after running a search, then leave the **Search** web page or navigate to a different feature, Search fails to revert the fieldset to the original setting. For example, you choose the *Base Event Fields* fieldset and run the search, then change the fieldset to *All Fields*. Next you navigate to the **Saved Searches** page. When you return to the **Search** page, the fieldset is still *All Fields* rather than reverting to *Base Event Fields* as it should.

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

### OCTCR33I113040 — CSV File Export Fails after You Change the Date and Time Format

**Issue:** After modifying the date and time format in preferences, the CSV export function for saved searches runs before the preference change fails.

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

## **OCTCR33I179782 — Scheduled Search Appends Erroneous Values to the Run Interval**

**Issue:** When creating a scheduled search, if you select Every 2 hours in the **Pattern** section, the search runs every two hours, at every even hour, such as 0, 2, 4, 6, etc and appending the minutes setting in **Starting From** value. The system ignores the hour setting in **Starting From**.

For example, you might select **Every 2** hours and choose **Starting From** at 01:15 am. Search will run every 2 hours at 2:15 am, 4:15 am, 6:15 am, and so on.

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

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

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

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

- | top Device Receipt Time
- | top Device Event Class ID
- | top Device Event Category

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

- | top Source Address
- | top Agent Severity

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

#Vulnerabilities | top Device Event Class ID

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

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

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

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

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

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

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

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

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

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

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

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

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

## OCTCR33I616090 — 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.

## Issues Related to SOAR

- [OCTCR33I548027 — Trend Micro Apex Central Integration Fails.](#)
- [OCTCR33I567004 — SOAR Widgets Display Problems with Duplicate Widgets.](#)
- [OCTCR33I567003 - For soar case timeline widget, the data is not displayed properly](#)
- [OCTCR33I567004 - For Soar Timeline widget,the data is not getting displayed properly.](#)
- [OCTCR33I657003 - Proxy Option Missing in Microsoft Exchange EWS Integration Configuration](#)
- [OCTCR33I192790 - The Or condition in Workflow does not work when used with "Alert source Equals".](#)
- [OCTCR33I711107 - SOAR case links in Inetsoft reports do not redirect to the correct case.](#)
- [OCTCR33I724048 - SOAR INetSoft Reports Fail If CA Certificates Are Updated](#)

### **OCTCR33I567003 - For SOAR case timeline widget, the data is not displayed properly**

**Issue:** For SOAR case timeline widget, the timeline chart shall be either plotted or display "no data" if the data is not present for selected timerange.

**Workaround:** There is no workaround at this time.

### **OCTCR33I567004 - For SOAR Timeline widget, the data is not getting displayed properly.**

**Issue:** For SOAR timeline widget, when multiple widgets are present in dashboard, data is displayed for only widget.

**Workaround:** There is no workaround at this time.

### **OCTCR33I657003 - Proxy Option Missing in Microsoft Exchange EWS Integration Configuration**

**Issue:** While configuring Microsoft Exchange EWS integration, the proxy option is missing from the configuration settings.

**Workaround:** There is no workaround at this time.

### **OCTCR33I548027 — Trend Micro Apex Central Integration Fails**

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

**Workaround:** There is no workaround at this time.

## **OCTCR33I567004 — SOAR Widgets Display Problems with Duplicate Widgets**

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

**Workaround:** There is no workaround at this time.

## **OCTCR33I192790 - The Or condition in Workflow does not work when used with "Alert source Equals".**

**Issue:** In SOAR Workflow Or conditions do not work when used with Alert source Equals.

**Workaround:** There is no workaround at this time.

## **OCTCR33I711107 - SOAR case links in Inetsoft reports do not redirect to the correct case.**

**Issue:** Links to cases in Inetsoft reports do not display the correct case.

**Workaround:** There is no workaround at this time.

## **OCTCR33I724048 - SOAR INetSoft Reports Fail If CA Certificates Are Updated**

**Issue:** SOAR INetSoft Reports fail if CA certificates are updated.

**Workaround:**

1. Log in to ArcSight and Navigate to **Reports > Portal > Data > Data Source > Edit soar\_data\_source**.
2. Update the connection URL **DefaultJavaSSLFactory** with **NonValidatingFactory**.

## Issues Related to Transformation Hub

- [OCTCR33I377141 — Event Integrity Enablement Stops Enrichment Stream Processor Pods](#)
- [OCTCR33I409228 — Schema Instances May Be Allocated to Single Worker Node](#)
- [OCTCR33I609151 — CEF Routing Rule with Less Than Condition May Result in Unintended Events in Destination Topic](#)
- [OCTCR33I609152 — CEF Routing Rule with Numeric Test May Result in Unintended Events in Destination Topic](#)

### OCTCR33I377141 — 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.

### OCTCR33I409228 — Schema 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.

- 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).

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

```
topic="_schemas"
```

- 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'
```

- 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
```

- 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' $assignfile
sed -i -r "s/(,replicas:\s*([\d-9,]+)/\1$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 >
$selectfile
kubectl cp $selectfile $namespace/th-kafka-0:$selectfile
rm -f "$selectfile"
kubectl exec -n $namespace th-kafka-0 -- kafka-leader-election --bootstrap-
server th-kafka-svc:9092 --election-type preferred --path-to-json-file
$selectfile
```

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/^\s*(ReplicationFactor:\s*\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.

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

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

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

When routing CEF events, if a routing rule tests a numeric field, a CEF event that has a value in that field may be routed in an unintended way. Numbers are compared as strings instead of numerically.

The result is that destination topics for affected CEF rules may not receive intended events, or may receive unintended events.

## **Issues Related to Recon**

- ["OCTCR33I715058 — Changing the time zone at Logger causes event migration failures" on the next page](#)

## **OCTCR33I715058 — Changing the time zone at Logger causes event migration failures**

**Issue:** A Logger with a time zone different than the one set in Recon will cause the event starting time stamps to be misidentified, causing a failure to migrate Logger event files.

**Workaround:** There is no workaround at this time.

# Resolved Issues

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

- ["Security Fixes in Previously Released Patches" below](#)
- ["Issues Related to Platform" below](#)
- ["Issues Related to Reporting" on page 50](#)
- ["Issues Related to ArcMC" on page 52](#)
- ["Issues Related to Search" on page 52](#)
- ["Issues Related to SOAR" on page 57](#)
- ["Issues Related to Transformation Hub" on page 63](#)

## Security Fixes in Previously Released Patches

This release includes the security fixes previously available with ArcSight Platform 23.1. For more information about these security fixes, see the [Release Notes for ArcSight Platform 23.1](#).

## Issues Related to Platform

- ["OCTCR33I242328 – On Node Management, the Filtering Option Does Not Work Correctly in Some Columns" on the next page](#)
- ["OCTCR33I276138 – Data Timeseries Chart Fails to Update after Changing Categories" on the next page](#)
- ["OCTCR33I349068 – Exported Tables No Longer Show Squeezed Columns" on the next page](#)
- ["OCTCR33I409215 – Database in 22.1 Release Will Not Support FIPS" on the next page](#)
- ["OCTCR33I414022 – Event Integrity Query for Large Time Range No Longer Indicates Insufficient Disk Space \(AWS/Azure\)" on the next page](#)
- ["OCTCR33I491108 – Pods Might Not Run During Fusion Reinstall" on page 50](#)
- ["OCTCR33I500006 – The Insights Tab Disappears From the Fusion Dashboard After the License Expires" on page 50](#)
- ["OCTCR33I592057 – Logout Issues With SAML2 Have Been Resolved" on page 50](#)

- ["OCTCR33I610053 — Event Integrity: The Check Progress Percentage Might Exceed 100%" on the next page](#)

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

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

## **OCTCR33I276138 – Data Timeseries Chart Fails to Update after Changing Categories**

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

## **OCTCR33I349068 – Exported Tables No Longer Show Squeezed Columns**

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

## **OCTCR33I409215 – Database in 22.1 Release Will Not Support FIPS**

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

## **OCTCR33I414022 — Event Integrity Query for Large Time Range No Longer Indicates Insufficient Disk Space (AWS/Azure)**

A code change resolved the problem where when a large time range was selected (e.g., 1/31-2/22), there was an intermittent error of "Other" when running an Event Integrity query in an Amazon Web Service (AWS) or Azure environment.

## **OCTCR33I491108 – Pods Might Not Run During Fusion Reinstall**

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

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

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

## **OCTCR33I592057 — Logout Issues With SAML2 Have Been Resolved**

After a code update, the logout process now work properly when the product is configured to use an external SAML provider

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

A code change resolved two cases where the check progress percentage might be misleading. They are:

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

## **Issues Related to Reporting**

- ["OCTCR33I160009 – Reporting - Chart Wizard Now Correctly Displays the Convert to Measure Button" on the next page](#)

- ["OCTCR33I161014 — Reporting - Dashboard Wizard Now Loads All Data" below](#)
- ["OCTCR33I162021 – X/Y Fields Can Now be Removed From a Graph" below](#)
- ["OCTCR33I566085 – Issues Resolved for Network Chart Data Being Presented in Portions and Cut Out of the Display" below](#)

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

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

## **OCTCR33I161014 — Reporting - Dashboard Wizard Now Loads All Data**

A software fix resolved the a problem where using the Dashboard wizard, the chart intermittently failed to load. This was because the same type of data had been selected at the same time.

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

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

## **OCTCR33I566085 – Issues Resolved for Network Chart Data Being Presented in Portions and Cut Out of the Display**

Before implementing a software fix, the Network chart tended to truncate data, such as IP addresses, to the point where the displayed content was not useful. These display problems have now been addressed.

## Issues Related to ArcMC

- ["OCT33I659040 -- Error Communicating to Web Server Error" below](#)
- ["OCT33I348119 -- Error message while deploying connector on a Virtual CHA and selecting S3 bucket as destination" below](#)

### **OCT33I659040 -- Error Communicating to Web Server Error**

This error message `Error Communicating to Web Server` indicates that the `net-tools` package must be installed in order to install ArcMC. `net-tools` has been added as a prerequisite to install ArcMC.

### **OCT33I348119 -- Error message while deploying connector on a Virtual CHA and selecting S3 bucket as destination**

In some cases, when deploying a connector on a Virtual CHA and selecting S3 as a destination, an error message would be displayed. This issue has been resolved.

## Issues Related to Search

- ["OCTCR33I167004 – Scheduled Tasks are Now Prevented From Being Saved After the User Closed the Dialog Box" on the next page](#)
- ["OCTCR33I161014 — Reporting - Dashboard Wizard Now Loads All Data" on the previous page](#)
- ["OCTCR33I178795 – Fieldsets No Longer Default to Base Event Fields After an Upgrade" on page 54](#)
- ["OCTCR33I324035 – Search Query No Longer Returns Incorrect Results if the Query is not Explicitly Stated" on page 54](#)
- ["OCTCR33I341227 – You May Now Use Search Operators in the Name of a Saved Query or Criteria" on page 54](#)
- ["OCTCR33I369029 — Load Modal Now Loads Search Criteria When the Fieldset is Deleted" on page 54](#)
- ["OCTCR33I408155 – Backup Failures in S3 While Deleting Obsolete Files From S3 Has Been Resolved" on page 55](#)

- ["OCTCR33I549163 and OCTCR33I592116 – Searches With no Changes Since the Last Run No Longer Appear to be Stuck"](#) on page 55
- ["OCTCR33I500006 – The Insights Tab Disappears From the Fusion Dashboard After the License Expires"](#) on page 50
- ["OCTCR33I576073 – Switching Tabs While Saving Searches No Longer Causes an Error"](#) on page 55
- ["OCTCR33I549163 and OCTCR33I592116 – Searches With no Changes Since the Last Run No Longer Appear to be Stuck"](#) on page 55
- ["OCTCR33I160009 – Reporting - Chart Wizard Now Correctly Displays the Convert to Measure Button"](#) on page 51
- ["OCTCR33I341227 – You May Now Use Search Operators in the Name of a Saved Query or Criteria"](#) on the next page
- ["OCTCR33I592116 – Re-executing Searches No Longer Prompts an Error Message or Prevents the Search Grid From Displaying"](#) on page 56
- ["OCTCR33I603036 – The Application No Longer Displays an Error When You Try to Save Search Criteria"](#) on page 57
- ["OCTCR33I162021 – X/Y Fields Can Now be Removed From a Graph"](#) on page 51
- ["OCTCR33I615024 – Searching for a "global event id" Field Does Not Yield Incorrect Results Anymore"](#) on page 57

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

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

## **OCTCR33I174130 – Scheduled Searches No Longer Fail to Export to CSV**

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

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

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

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

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

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

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

## **OCTCR33I369029 — Load Modal Now Loads Search Criteria When the Fieldset is Deleted**

A software fix resolved the problem where search criteria was not load under the circumstances described below.

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

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

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

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

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

## **OCTCR33I566082 — Scheduled Searches: Problems Related to Switching the Field “Search Expires in” in User Preferences Have Been Resolved**

Previously, if you created a scheduled search that contained an expiration option, such as “Search expires in” = 7 days, then changed the value in User Preferences to “Search expires in” = 10 weeks, the scheduled search failed to complete and showed an incorrect setting (“Search expires in” = 7 weeks). The issue also occurred if you switched the settings from weeks to days, weeks to “Never Expire,” even with a fresh install. A code change resolved the issue.

## **OCTCR33I576073 — Switching Tabs While Saving Searches No Longer Causes an Error**

A code fix resolved the problem caused by switching tabs while saving a search. Previously, the system threw an error that stated "Results do not match the specified serach query."

## **OCTCR33I576083 — Outlier Detection: Outlier History Display Has Been Corrected When No Score Exists**

Previously in **Outlier Detection**, when no score existed, **Top Anomalous Hosts** and **Outlier History** posted zeros (0) and displayed empty charts.

Additionally, if you clicked a zero score in **Top Anomalous Hosts**, then **Selected Anomalous IP** and **Selected Anomaly Host** also displayed empty charts. A code updated resolved this problem.

## **OCTCR33I585053 — Inability to Add a Field from Event Inspector to an Active Search if the Field is Not Available in the Fieldset Has Been Resolved**

The problem created if you added a field from the Event Inspector to an active search when the field was not available in the fieldset of the active search has been resolved. Before the fix, a red line displayed under any field in the search query that was not in the active fieldset. Additionally, hovering your cursor over the field would display the following error message: Columns only from fieldset are permitted.

## **OCTCR33I587006 — Search No Longer Fails When the "where condition" Operator Has Any <...> and Contains a Filter for Field Groups**

Previously, the following field groups were not supported because they were not string data. If a user wanted to include a non-string datatype field group in a | where any...contains query, the field datatype needed to be converted to string (using eval to string). Otherwise, the software might display an error alerting you about non-applicable field groups, such as custom float, float, ip, ip6, mac, port, path, timestamp, or url. This problem has been resolved.

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

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

## **OCTCR33I603036 — The Application No Longer Displays an Error When You Try to Save Search Criteria**

A code update resolved the problem where the user encountered an error when they tried to save specific search criteria before running a query, even if the user entered correct syntax and parameters.

## **OCTCR33I608090 — The Search Tab is No Longer Intermittently Visible After Installation,**

A code update resolved the issue of the Search tab displaying intermittently following an installation..

## **OCTCR33I615024 — Searching for a "global event id" Field Does Not Yield Incorrect Results Anymore**

Before adding a code fix, queries that filtered specific "id" or "Global Event Id" field values did not return correct results . For example: id = "123456789" or id != "123456789"

### **Issues Related to SOAR**

- ["OCTCR33I421034 – A Wrong Protocol Name in the Arcsight Listener Protocol Parameter Makes SOAR Crash Upon Restart" on the next page](#)
- ["OCTCR33I427039 – Action History Page Filters Have Multiple Entry With Same Name" on page 59](#)
- ["OCTCR33I428078 – No Entries Displayed for Failed Enrichment Activities on Cases Timeline" on page 59](#)
- ["OCTCR33I430016 – Unable to Delete the Column that was Added First to the List" on page 59](#)
- ["OCTCR33I454142 – WinRM Logoff User Capability Does Not Get Username From Scope" on page 59](#)
- ["OCTCR33I467084 – Unable to Add File to Case Scope in Automation" on page 59](#)
- ["OCTCR33I478040 – Error While Adding Comment to a Case" on page 60](#)

- ["OCTCR33I485001 – Error While Deleting a Case in Open Status" on page 60](#)
- ["OCTCR33I504024 – Large Java Stack Trace is Found When Dispatching Case to a UserGroup" on page 60](#)
- ["OCTCR33I512001 – Unable to Add a Second Item to Cisco Firepower Management Center Block IP and Block URL Capabilities" on page 60](#)
- ["OCTCR33I514042 – IP Country Information is Always Unknown" on page 60](#)
- ["OCTCR33I530023 – SOAR MISP Integration Fetches all the Events For Device Connectivity" on page 61](#)
- ["OCTCR33I553001 – Username Query is Missing in Parameter Definition" on page 61](#)
- ["OCTCR33I554001 – Liquibase Migration Error " on page 61](#)
- ["OCTCR33I554081 – Unable to Save Playbooks With Alert Source as the Starting Condition" on page 61](#)
- ["OCTCR33I555096 – New Notifications are Not Displayed Properly" on page 61](#)
- ["OCTCR33I569001 – Scope Item Property List – Paging is Broken" on page 61](#)
- [OCTCR33I605095 FTP Action plugin is failing on action rollback if the remote.file.filename.appenduid=true](#)
- [OCTCR33I620081 Exchange EWS Integration - OAuth2 should be the default authentication method](#)
- [OCTCR33I638001 - SOAR allows to execute Quarantine Computer action capability with empty / null parameters](#)
- [OCTCR33I661021 - Base Event Download Doesn't Work Properly](#)
- [OCTCR33I680023 - Enhancement to have the ability to specify primarily custom Active Lists when enriching a case](#)
- [OCTCR33I659020 - UI displays "duplicate or empty name" error when Active List Names from ESM](#)
- [OCTCR33I612130 — SOAR Message Broker Pod Backup File Cannot be Created Automatically](#)
- [OCTCR33I720001 - SOAR About Button Does Not Work.](#)

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

SOAR crashes while restarting if protocol name provided for Arcsight Listener Protocol Parameter is wrong. If a wrong protocol name is specified for the ArcSight Listener Protocol an error message is displayed, but the name gets saved. However, while restarting the soar-web-

app crashes with an error message. Resolution: A code fix was applied to resolve the issue. A code fix was applied to resolve the issue.

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

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

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

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

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

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

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

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

### **OCTCR33I467084 – Unable to Add File to Case Scope in Automation**

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

## **OCTCR33I478040 – Error While Adding Comment to a Case**

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

## **OCTCR33I485001 – Error While Deleting a Case in Open Status**

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

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

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

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

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

## **OCTCR33I514042 – IP Country Information is Always Unknown**

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

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

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

## **OCTCR33I553001 – Username Query is Missing in Parameter Definition**

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

## **OCTCR33I554001 – Liquibase Migration Error**

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

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

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

## **OCTCR33I555096 – New Notifications are Not Displayed Properly**

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

## **OCTCR33I569001 – Scope Item Property List – Paging is Broken**

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

### **OCTCR33I605095 FTP Action plugin fails on action rollback if the remote.file.filename.appenduuid=true**

Now FTP Action plugin works as expected when remote.file.filename.appenduuid=true.

### **OCTCR33I620081 Exchange EWS Integration - OAuth2 should be the default authentication method**

In Exchange EWS Integration , OAuth2 has been set as the default authentication method.

### **OCTCR33I638001 - SOAR allows to execute Quarantine Computer action capability with empty / null parameters**

Now SOAR does not accept to take action with null / empty values.

### **OCTCR33I661021 - Base Event Download Doesn't Work Properly**

Now base event csv includes base event data.

### **OCTCR33I680023 - Enhancement to have the ability to specify primarily custom Active Lists when enriching a case**

Now you can select custom Active List at the top of dropdown box.

### **OCTCR33I659020 - UI displays "duplicate or empty name" error when Active List Names from ESM**

Now Active List Path/Name can display lists from ESM .

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

Now SOAR message broker pod backup file can be created automatically.

## **OCTCR33I720001 - SOAR About Button Does Not Work**

The SOAR About button now displays the required information.

## **Issues Related to Transformation Hub**

- [OCTCR33I404035 – Upgraded Schema Registry Pods Fail](#)
- [OCTCR33I713070 – Fusion ArcMC Displays "No Data Returned At This Time" After TH Upgrade](#)
- [OCTCR33I713079 – Kafka Manager Fails to Show Consumers or Metrics After TH Upgrade](#)

## **OCTCR33I404035 – Upgraded Schema Registry Pods Fail**

The issue of upgraded EKS worker nodes causing Schema Registry pods to fail no longer occurs.

## **OCTCR33I713070 – Fusion ArcMC Displays "No Data Returned At This Time" After TH Upgrade**

In some cases, the Event Parsing Error, Stream Processing EPS, and Stream Processing Lag fields in Fusion ArcMc might display 'No data returned at this time' after a TH upgrade. This issue no longer occurs.

## **OCTCR33I713079 – Kafka Manager Fails to Show Consumers or Metrics After TH Upgrade**

After upgrading from 21.1.x to 22.2 or higher, Kafka Manager may fail to show Kafka consumers or metrics, and the Kafka Manager log may contain warnings that a broker may not

be available. This happens when Kafka Manager starts before the Kafka brokers after the upgrade; timing allows Kafka Manager to connect to pre-upgrade brokers before they exit. This issue no longer exists after upgrading to 23.2.0.

## Support

### Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://www.microfocus.com/documentation/argsight/">https://www.microfocus.com/documentation/argsight/</a>

# Contents

What's New .....	3
Technical Requirements .....	4
Downloading the Files .....	5
Understanding the Files to Download .....	5
Downloading and Verifying the Files .....	8
Known Issues Related to Upgrade .....	9
865171 - Upgrade Process Might Cause Data Loss by Changing Retention Value to One Month .....	9
Known Issues .....	10
Issues Related to Database Upgrade .....	11
OCTCR33I611095 — Issues Related to FIPS-enabled Database Node Fails .....	11
OCTCR33I617102 — Post-installation, You Might See an Error About Creating the Scheduler's Target Topic .....	11
Issues Related to Platform .....	12
OCTCR33I112042 — Pods Might Not Run During Fusion Reinstall .....	12
OCTCR33I411123 — Event Integrity Query Indicates Insufficient Disk Space (AWS/Azure) .....	13
OCTCR33I470057 — Left Navigation Menu Items Do Not Reliably Display When Pods Restart or are Unresponsive .....	13
OCTCR33I534015 — Autopass container crashing with exception: relation "mysequence" already exists .....	13
OCTCR33I712038 — Error Message Returned on Single-Node Rocky Linux Environments .....	14
OCTCR33I736005—Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Upgrade from 23.1 to 23.2 when IPv6 is Disabled on the Host Node ..	14
OCTCR33I744020 — Upgrade from 23.1 Fails and Rerun Upgrade Also Fails .....	15
OCTCR33I752115— Portal-Ingress-Controller Pod in CrashLoopBackOff State after ArcSight Platform Installation Times out when IPv6 is Disabled on the Host Node .....	16

Issues Related to Reports Portal .....	16
OCTCR33I134098 — Edit Wizard Preview is Unavailable .....	17
OCTCR33I162021 — Cannot Remove X/Y Fields from a Graph .....	17
OCTCR33I186007 — An Exported Report Might Have Format Issues .....	17
OCTCR33I331194 — Reports and Dashboards Use UTC Time Zone .....	17
OCTCR33I336023 — Operations Performed on an Open Admin Tab Do Not Complete After You Log Out From Another Capability (Recon or Reporting) Tab .....	18
OCTCR33I372067 — Contract & Usage Page Throws an Ingress Router Error and Does Not Load .....	18
OCTCR33I409268 — Reporting Shows an Error When Single Sign On Secrets are Changed (Azure) .....	18
OCTCR33I566085 — Network Chart Data Presented in Portions and Cut .....	18
OCTCR33I589121— Brush Option Does Not Highlight Parabox Charts .....	19
OCTCR33I71158 — Scheduled Tasks Do Not Allow Default Printer Selection .....	19
Issues Related to ArcSight Management Center .....	19
OCTCR33I612094 — Fusion ArcMC Throws 503 Error After Restoring Configuration Data (AWS, Azure and On-premises) .....	20
OCTCR33I408195 — Importing a Host File on Fusion ArcMC Points to a Different Log Folder .....	20
OCTCR33I408194 — Fusion ArcMC Session License Expiration .....	20
OCT33I359190 -- On G10 Appliance, ArcMC Does Not Validate IP Addresses for NIC Ports .....	21
OCT33I363017 -- On G10 Appliance, IP Address Not Correctly Configured After Restore	21
OCT33I363022 -- On G10 Appliance, Gateway Not Correctly Configured After Restore ..	21
OCT33I425040 -- In Deployment/Topology View, Logger or ESM Destination for TH Shows Unknown IP Address .....	21
OCT33I698065 -- On Azure, Intermittent Login Errors .....	22
OCT33I736019 -- Selecting a value for ArcMC Container Memory Limit throws an unformatted screen error .....	22
Issues Related to Intelligence .....	22
OCTCR33I729040 — SearchManager Pods Fail Due to the Absence of Spacing in the Elasticsearch Data Retention Period Value .....	24

OCTCR33I494001 — Analytics Does Not Detect the Custom SQL Loader Scripts After the Intelligence Upgrade .....	24
OCTCR33I606124 — Multi-step Upgrade From 21.1.x to 23.1.x Fails on Suite Upgrade to 23.1 (a Non-Cloud Release) .....	26
OCTCR33I611096 — Analytics Fails to Load Data Sources Except for AD and Proxy .....	26
OCTCR33I613042 — Intelligence Sharing URL Functionality Does Not Work if the User Does Not Have an Active Session .....	27
OCTCR33I616036 — If Not Already Logged into Fusion, the First Attempt to Log Directly Into Intelligence Dashboard Will Fail .....	27
OCTCR33I400584 - Either the Intelligence Search API or Login to the Intelligence UI or both Fail with a Timeout Error (IOException: Listener Timeout) for Large Data Sets in the Database .....	28
OCTCR33I399297 - Intelligence Search API Fails with a Timeout Error (esSocketTimeout exception) for Large Data Sets in the Database .....	29
OCTCR33I401549 - Most Pods Enter into the CrashLoopBackOff State if the KeyStore Password Starts with a Space or a Special Character .....	30
OCTCR33I399665 - Elasticsearch and Logstash Pods Fail in an AWS Deployment Because of Permission Issues .....	30
OCTCR33I604032 - Elasticsearch and Logstash Pods Fail in an Azure Deployment Because of Permission Issues .....	30
OCTCR33I614051 - Logstash Pod Fails on Data Ingestion in AWS Deployment When Using Self-Signed Certificates .....	31
OCTCR33I378083 - Erroneous Warning about Recon License .....	32
OCTCR33I614050 - Special Characters for the Database Credentials .....	32
OCTCR33I616054 - Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects .....	33
OCTCR33I614042 - Daylight Savings Time .....	33
OCTCR33I613048 - Repartition Percentage Threshold .....	33
OCTCR33I614047 - Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container .....	33
OCTCR33I614048 - Certificate Warnings in Logstash Logs .....	34
OCTCR33I613050 - Installer Does Not Validate the Value You Specify for Elasticsearch Data Retention Period .....	35
OCTCR33I614049 - Uninstalling Intelligence Does Not Delete All Files .....	35

OCTCR33I613051 - Unable to Retrieve Indices When Elasticsearch Cluster is Unstable	35
OCTCR33I399647 - HTTP Status 400 - Bad Request	36
Issues Related to Search	37
HERC-9865 — Fieldset Fails to Revert to its Original Setting	37
OCTCR33I113040 — CSV File Export Fails after You Change the Date and Time Format	37
OCTCR33I179782 — Scheduled Search Appends Erroneous Values to the Run Interval	38
OCTCR33I608098 — Certain top/bottom Queries Refresh When the User Presses the Space Bar While Entering the Query	38
OCTCR33I608115 — Vulnerabilities: System Query is Duplicated With Two Different Names	39
OCTCR33I609036 — Upgrade Issues: Searches That Use the "All Fields" Fieldset and the "All Time" Time Range Do Not Complete	39
OCTCR33I610160 — Unable to Use the Field "Id" With the top, bottom, rename, eval, and wheresql Operators	39
OCTCR33I610161 and OCTCR33I615024 — Incorrect Search Results Occur When Filtering With the "Id" Field	40
OCTCR33I616090 — For System Search Queries, #SSH Authentication Throws an Error	40
OCTCR33I567003 - For SOAR case timeline widget, the data is not displayed properly	41
OCTCR33I567004 - For SOAR Timeline widget, the data is not getting displayed properly.	41
OCTCR33I657003 - Proxy Option Missing in Microsoft Exchange EWS Integration Configuration	41
OCTCR33I548027 — Trend Micro Apex Central Integration Fails	41
OCTCR33I567004 — SOAR Widgets Display Problems with Duplicate Widgets	42
OCTCR33I192790 - The Or condition in Workflow does not work when used with "Alert source Equals".	42
OCTCR33I711107 - SOAR case links in Inetsoft reports do not redirect to the correct case.	42
OCTCR33I724048 - SOAR INetSoft Reports Fail If CA Certificates Are Updated	42
Issues Related to Transformation Hub	43
OCTCR33I377141 — Event Integrity Enablement Stops Enrichment Stream Processor Pods	43
OCTCR33I409228 — Schema Instances May Be Allocated to Single Worker Node	43

OCTCR33I609151— CEF Routing Rule with Less Than Condition May Result in Unintended Events in Destination Topic .....	46
OCTCR33I609152— CEF Routing Rule with Numeric Test May Result in Unintended Events in Destination Topic .....	46
Issues Related to Recon .....	46
OCTCR33I715058 — Changing the time zone at Logger causes event migration failures	47
Resolved Issues .....	48
Security Fixes in Previously Released Patches .....	48
Issues Related to Platform .....	48
OCTCR33I242328 – On Node Management, the Filtering Option Does Not Work Correctly in Some Columns .....	49
OCTCR33I276138 – Data Timeseries Chart Fails to Update after Changing Categories .....	49
OCTCR33I349068 – Exported Tables No Longer Show Squeezed Columns .....	49
OCTCR33I409215 – Database in 22.1 Release Will Not Support FIPS .....	49
OCTCR33I414022 — Event Integrity Query for Large Time Range No Longer Indicates Insufficient Disk Space (AWS/Azure) .....	49
OCTCR33I491108 – Pods Might Not Run During Fusion Reinstall .....	50
OCTCR33I500006 – The Insights Tab Disappears From the Fusion Dashboard After the License Expires .....	50
OCTCR33I592057 — Logout Issues With SAML2 Have Been Resolved .....	50
OCTCR33I610053 — Event Integrity: The Check Progress Percentage Might Exceed 100% .....	50
Issues Related to Reporting .....	50
OCTCR33I160009 – Reporting - Chart Wizard Now Correctly Displays the Convert to Measure Button .....	51
OCTCR33I161014 — Reporting - Dashboard Wizard Now Loads All Data .....	51
OCTCR33I162021 – X/Y Fields Can Now be Removed From a Graph .....	51
OCTCR33I566085 – Issues Resolved for Network Chart Data Being Presented in Portions and Cut Out of the Display .....	51
Issues Related to ArcMC .....	52
OCT33I348119 -- Error message while deploying connector on a Virtual CHA and selecting S3 bucket as destination .....	52

Issues Related to Search .....	52
OCTCR331167004 – Scheduled Tasks are Now Prevented From Being Saved After the User Closed the Dialog Box .....	53
OCTCR331174130 – Scheduled Searches No Longer Fail to Export to CSV .....	53
OCTCR331178795 – Fieldsets No Longer Default to Base Event Fields After an Upgrade .....	54
OCTCR331324035 – Search Query No Longer Returns Incorrect Results if the Query is not Explicitly Stated .....	54
OCTCR331341227 – You May Now Use Search Operators in the Name of a Saved Query or Criteria .....	54
OCTCR331369029 – Load Modal Now Loads Search Criteria When the Fieldset is Deleted .....	54
OCTCR331408155 – Backup Failures in S3 While Deleting Obsolete Files From S3 Has Been Resolved .....	55
OCTCR331549163 and OCTCR331592116 – Searches With no Changes Since the Last Run No Longer Appear to be Stuck .....	55
OCTCR331566082 – Scheduled Searches: Problems Related to Switching the Field “Search Expires in” in User Preferences Have Been Resolved .....	55
OCTCR331576073 – Switching Tabs While Saving Searches No Longer Causes an Error .....	55
OCTCR331576083 – Outlier Detection: Outlier History Display Has Been Corrected When No Score Exists .....	56
OCTCR331585053 – Inability to Add a Field from Event Inspector to an Active Search if the Field is Not Available in the Fieldset Has Been Resolved .....	56
OCTCR331587006 – Search No Longer Fails When the "where condition" Operator Has Any <...> and Contains a Filter for Field Groups .....	56
OCTCR331592116 – Re-executing Searches No Longer Prompts an Error Message or Prevents the Search Grid From Displaying .....	56
OCTCR331603036 – The Application No Longer Displays an Error When You Try to Save Search Criteria .....	57
OCTCR331608090 – The Search Tab is No Longer Intermittently Visible After Installation, .....	57
OCTCR331615024 – Searching for a "global event id" Field Does Not Yield Incorrect Results Anymore .....	57
Issues Related to SOAR .....	57

OCTCR33I421034 – A Wrong Protocol Name in the Arcsight Listener Protocol Parameter Makes SOAR Crash Upon Restart .....	58
OCTCR33I427039 – Action History Page Filters Have Multiple Entry With Same Name .....	59
OCTCR33I428078 – No Entries Displayed for Failed Enrichment Activities on Cases Timeline .....	59
OCTCR33I430016 – Unable to Delete the Column that was Added First to the List .....	59
OCTCR33I454142 – WinRM Logoff User Capability Does Not Get Username From Scope	59
OCTCR33I467084 – Unable to Add File to Case Scope in Automation .....	59
OCTCR33I478040 – Error While Adding Comment to a Case .....	60
OCTCR33I485001 – Error While Deleting a Case in Open Status .....	60
OCTCR33I504024 – Large Java Stack Trace is Found When Dispatching Case to a UserGroup .....	60
OCTCR33I512001 – Unable to Add a Second Item to Cisco Firepower Management Center Block IP and Block URL Capabilities .....	60
OCTCR33I514042 – IP Country Information is Always Unknown .....	60
OCTCR33I530023 – SOAR MISP Integration Fetches all the Events For Device Connectivity .....	61
OCTCR33I553001 – Username Query is Missing in Parameter Definition .....	61
OCTCR33I554001 – Liquibase Migration Error .....	61
OCTCR33I554081 – Unable to Save Playbooks With Alert Source as the Starting Condition .....	61
OCTCR33I555096 – New Notifications are Not Displayed Properly .....	61
OCTCR33I569001 – Scope Item Property List – Paging is Broken .....	61
OCTCR33I605095 FTP Action plugin fails on action rollback if the remote.file.filename.appenduid=true .....	62
OCTCR33I620081 Exchange EWS Integration - OAuth2 should be the default authentication method .....	62
OCTCR33I638001 - SOAR allows to execute Quarantine Computer action capability with empty / null parameters .....	62
OCTCR33I661021 - Base Event Download Doesn't Work Properly .....	62
OCTCR33I680023 - Enhancement to have the ability to specify primarily custom Active Lists when enriching a case .....	62

OCTCR33I659020 - UI displays "duplicate or empty name" error when Active List Names from ESM .....	62
OCTCR33I612130 — SOAR Message Broker Pod Backup File Cannot be Created Automatically .....	63
OCTCR33I720001 - SOAR About Button Does Not Work .....	63
Issues Related to Transformation Hub .....	63
OCTCR33I404035 – Upgraded Schema Registry Pods Fail .....	63
OCTCR33I713070 – Fusion ArcMC Displays "No Data Returned At This Time" After TH Upgrade .....	63
OCTCR33I713079 – Kafka Manager Fails to Show Consumers or Metrics After TH Upgrade .....	63
Send Documentation Feedback .....	73

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on ArcSight Platform Release Notes (ArcSight Platform 23.2.1)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [MFI-Documentation-Feedback@opentext.com](mailto:MFI-Documentation-Feedback@opentext.com).

We appreciate your feedback!