Micro Focus Security ArcSight ArcSight Platform

Software Version: 22.1.1

ArcSight Platform Release Notes

Document Release Date: May 2022
Software Release Date: May 2022

Legal Notices

Copyright Notice

© Copyright 2001 - 2022 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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

Support

Contact Information

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

Contents

Release Notes for the ArcSight Platform 22.1.2

Thursday, August 25, 2022

This release provides updates for and resolves previous issues in ArcSight Platform 22.1.0, including security fixes available in ArcSight Platform 22.1.1.

> For more information about installing or upgrading to the 22.1.0 release, see the *Release Notes for ArcSight Platform 22.1.0.*

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

- "Software Fixes in this Release" on page 7
- "Technical Requirements" on page 8
- "Downloading the Files" on page 9
- "Known Issues" on page 11
- "Contacting Micro Focus" on page 27

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

Component	Version
ArcSight Command Center for Enterprise Security Manager	7.6.0
Fusion	1.5.2
ArcSight Intelligence	6.4.1
ArcSight Recon	1.4.2
Transformation Hub	3.6.1
Layered Analytics	1.3.1

The documentation for this product is available on the documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment** or **support** on this topic at the bottom of any page in the HTML version of the documentation posted at the ArcSight Platform Documentation page or the documentation pages for the included products.

Software Fixes in this Release

This release includes the following software enhancement and fixes:

- "Enhancement: Migrating Data to ArcSight Recon from ArcSight Logger" below
- "Security Fixes in AcSight Platform 22.1.1" below

Enhancement: Migrating Data to ArcSight Recon from ArcSight Logger

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

The migration process also includes the following enhancements:

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

Security Fixes in AcSight Platform 22.1.1

This release includes the security fixes previously available with ArcSight Platform 22.1.1. For more information about these security fixes, see the Release Notes for ArcSight Platform 22.1.1.

Technical Requirements

To upgrade to this release, you must have one of the following versions of ArcSight Platform installed in your environment:

- 22.1.1
- 22.1.0

For more information about the software and hardware requirements required for a successful deployment, see the *Technical Requirements for ArcSight Platform*. These *Technical Requirements* include guidance for the size of your environment based on expected workload. Micro Focus recommends the tested platforms listed in this document. For more information about installing or upgrading to ArcSight Platform 22.1.0, see the *Release Notes for ArcSight Platform 22.1.0*.

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

Downloading the Files

Before applying the patches in this release, ensure that you have an appropriate version of ArcSight Platform installed in your environment.

- "Understanding the Files to Download" below
- "Downloading the Files" below

Understanding the Files to Download

Download the following patch files for the associated components deployed in your environment.

If you are upgrading from 22.1.1, then download only the files listed for ArcSight Platform and Recon.

Product.	To download these files...	Description
ArcSight Platform	arcsight-installer-metadata-22.1.2.x.tar fusion-1.5.2.x.tar db-installer_3.5.2-x.tar.gz	Contains the images for updating the common services for the ArcSight Database
Transformation Hub	transformationhub-3.6.1.x.tar	Contains the images for updating Transformation Hub
ESM Command Center	esm-7.6.0.x.tar layered-analytics-1.3.1.x.tar	Contains the images for updating the ESM Command Center capability and Layered Analytics
Intelligence	intelligence-6.4.1.x.tar layered-analytics-1.3.1.x.tar	Contains the images for updating the Intelligence capability and Layered Analytics
Recon	recon-1.4.2.x.tar	Contains the images for updating the Recon capability

Downloading the Files

To download the patch files, do the following:

1. Follow the link to the product name in the table's **Product** column.

2. Download the listed patch files. Ensure that you also download the signature files (.sig) associated with each patch file.

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

3. Upgrade to 22.1.2.

   For more information, see "Upgrading to 22.1.2" in the *Administrator's Guide for ArcSight Platform*.

Known Issues

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

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.

- OCTCR33I500006 - The Insights Tab Disappears From the Fusion Dashboard After the License Expires
- "OCTCR33I489104 - After successful upgrade from 22.1.0->22.1.1->22.1.2 CDF portal shows older version as available update" on the next page
- "OCTCR33I470057 - Left navigation menu items do not reliably display when pods restart or are unresponsive" on the next page
- "OCTCR33I444011 - Database Installer not compatible with S3v4 API" on page 13
- "OCTCR33I428177 - Custom vbr system path is not honored during database backup configuration" on page 13
- "OCTCR33I414022 - Event Integrity Query for Large Time Range Indicates Insufficient Disk Space (AWS/Azure)" on page 13
- "OCTCR33I411123 - Event Integrity Query Indicates Insufficient Disk Space (AWS/Azure) " on page 13
- "OCTCR33I408155 - Backup Failures in S3 While Deleting Obsolete Files" on page 14
- "OCTCR33I378083 - Displays an Erroneous Warning about a Recon License" on page 14
- "OCTCR33I372067 - Contract & Usage Page Throws an Ingress Router Error and Does Not Load" on page 14
- "OCTCR33I339016 - Specified Sizes for Dashboard Table Cells do not Work in a SaaS Environment" on page 15
- "OCTCR33I167004 - Schedule task | If the user closes the dialog box, the software saves the task anyway" on page 15
- "OCTCR33I112042 - Pods Might Not Run During Fusion Reinstall" on page 15
- " OCTCR33I494001 - Analytics Does Not Detect the Custom SQL Loader Scripts After the Intelligence Upgrade" on page 15

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

Issue: The **Insights** tab disappears from the Fusion dashboard after the licenses for the Arcsight Intelligence and Transformation Hub capabilities expire. Even after activating new licenses for the two capabilities, the licenses are not validated and the **Insights** tab remains unavailable in the Fusion dashboard.

Workaround: Restart the `intelligence-arcsightconnector-api-xxxxxxxxxx-xxxxx` pod in your Arcsight deployment for the **Insights** tab to appear again in the Fusion dashboard.

OCTCR33I489104 - After successful upgrade from 22.1.0->22.1.1->22.1.2 CDF portal shows older version as available update

Issue: After completing a successful upgrade from 22.1.0->22.1.1->22.1.2, the CDF portal shows an older version as the available update. The CDF portal should not display any updates because the latest one has been upgraded.

Workaround : Delete the metadata file that says there is an available update from CDF portal (Deployment->metadata) if customers do not remove older metadata, future upgrades might fail because of version conflicts.

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.

OCTCR33I444011 - Database Installer not compatible with S3v4 API

Issue: The installer needs to be compatible with the S3v4 so that it works in all AWS regions and also with S3 emulators like NetApp. This defect requires a code fixes in the DB installer and in other admin tools.

OCTCR33I428177 - Custom vbr system path is not honored during database backup configuration

Issue: While configuring or re-configuring a database backup using the **db_backup.sh** script, a custom path is not being honored if you select the **vbr system** path to a **custom path** instead of the **default path**. Customers might lose all the backup logs and data if they do not notice the **/tmp** directory contains a backup configuration.

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

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

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

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.

OCTCR33I408155 - Backup Failures in S3 While Deleting Obsolete Files

Issue: Part of the backup operation is clearing obsolete backup files that are older than the backup retention configuration setting. Due to this issue, the cleanup of obsolete files might not completed successfully and some obsolete files might remain, resulting in higher than necessary backup storage utilization.

Workaround: A patch will be released to fix this issue so that the cleanup operation reliably completes. However, if you need to resolve this issue sooner than the patch release, contact Technical Support to obtain a modified `/opt/vertica/bin/vbr.py` file that contains a fix that can be applied immediately. Also, edit the `config/backup_restore_cloud_storage_base.ini` file by uncommenting and setting `cloud_storage_concurrency_delete = 1`.

OCTCR33I378083 - Displays an Erroneous Warning about a 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.

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.

OCTCR33I339016 - Specified Sizes for Dashboard Table Cells do not Work in a SaaS Environment

Issue: On your dashboard, when you manually change a table cell size, the emerging window does not show the values you entered in the fields, and the table cells cannot be resized. (This issue only affects SaaS environments.)

Workaround:Even though the values are not visible, you can still modify them inside the fields and use them as intended. One way to do this is to use the shortcut **Ctrl + A** to select values in the field and then copy or replace them, as needed.

OCTCR33I167004 - Schedule task | If the user closes the dialog box, the software saves the task anyway

Issue: When clicking the close button during the scheduler task creation process, the modal is being closed, but the task is being saved as well.

Workaround: If the task was not intended to be saved in the scheduler table, proceed to select such task and delete it.

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.

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 22.1.2, 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/0/1.9.2.9/

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 1.9.1.9 directory:

```
mkdir 1.9.1.9
```

4. Navigate to the following directory:

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

5. Execute the following command to move the SQL loader scripts from <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0 to <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_sql/0/1.9.1.9:

```
mv *.md5 *.sql 1.9.1.9
```

6. Execute the following command to grant permissions to the 1.9.1.9 directory:

```
chown -R 1999:1999 1.9.1.9
```

Step 2: Upgrade the Intelligence capability.

For more information, see Upgrading to 22.1.2 in the Administrator's Guide for ArcSight Platform.

Step 3: Perform the following steps after the upgrade:

1. Run Analytics to start the next analytics run. For more information, see Running Analytics on Demand in the Administrator's Guide for ArcSight Platform.
2. During the analytics run, the 1.9.2.9 folder is created in the following directory with the default SQL loader scripts:

```
cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
sql/0/1.9.2.9
```

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

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

   ```
   kubectl logs -f interset-analytics-xxx -n arcsight-installer-xxx -c
   interset-analytics
   ```

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

   ```
   cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
   sql/0/1.9.2.9
   ```

   c. Update the md5 files with the md5 sums corresponding to the modified SQL loader scripts in the following directory:

   ```
   cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
   sql/0/1.9.1.9
   ```

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

On Multi-master Non-root Install, itom-cdf-keepalived Pod Restarting and Suite Fails to Deploy

Issue: If sudo installing a multi-master cluster through the arcsight-install tool, you will notice all capability pods are marked as pending, and `itom-cdf-keepalived` pod is existing only in single replica and crashing. In addition, the `kubectl get nodes` command returns all of your worker nodes in a NotReady stats. If the sudo installation for multi-master was executed manually via install.sh, you will notice only the `itom-cdf-keepalived` pod in single replica count and crashing, even before you try to deploy the capabilities.

Workaround: Use `kubectl edit ds/itom-cdf-keepalived -n kube-system` to edit the daemonset definition of `cdf-keepalived`. Locate the "nodeSelector" section and change its value (make sure to honor the spacing) to master: "true". Save and exit as a normal vi session. Make sure `command kubectl get ds/itom-cdf-keepalived -n kube-system` returns now the current/desired replica count of 3.

After an Upgrade from the Patch Release, Error Returned: "Failed to upgrade. Internal Server Error."

Issue: After upgrading to 22.1 from the 21.1, in some cases, the error message might be returned in the upgrade's final stages: "Failed to Upgrade. Internal Server Error." The issue can also be detected in logs if some resources are not upgraded.

Workaround: If you encounter this problem, please delete the old upgrade pod and then run the following command:

```
kubectl delete deployment suite-upgrade-pod-arcsight-installer -n `kubectl get
namespaces | grep arcsight-installer | awk ' {print $1}
```

Run the upgrade again.

Accessing the CDF Management Portal Reconfigure Page

Issue: At times, you might not be able to access the CDF Management Portal Reconfigure page. For example, this issue might occur when you are trying to perform an upgrade.

Workaround: Follow these steps:

1. Verify the status of the nginx-ingress-controller DaemonSet :

   ```
   NS=$(kubectl get namespaces | awk '/arcsight/{print $1}');kubectl get
   daemonset nginx-ingress-controller -n $NS
   ```

2. Create a new nginx-ingress-controller.yaml file:

   ```
   cd ${K8S_HOME};kubectl get daemonset nginx-ingress-controller -n `kubectl
   get namespaces | grep arcsight-installer | awk '{print $1}'` -o yaml > \
   nginx-ingress-controller.yaml
   ```

3. Ensure that the saved nginx-ingress-controller.yaml file exist in the ${K8S_HOME}home directory (/opt/arcsight/kubernetes) and contains definitions in yaml format.

4. Delete the current nginx-ingress-controller configuration:

   ```
   kubectl delete -f ./nginx-ingress-controller.yaml
   ```

5. Apply the new nginx-ingress-controller configuration:

   ```
   kubectl apply -f ./nginx-ingress-controller.yaml
   ```

6. Wait until the nginx-ingress-controller pods are up and running:

```
kubectl get pods -n $NS --watch | grep nginx-ingress-controller
```

7. Verify the nginx-ingress-controller controller daemonset status:

```
kubectl get daemonset nginx-ingress-controller -n $NS
```

8. To continue to upgrade deployed capabilities, see "Accepting the Certificate" in the *Administrator's Guide for ArcSight Platform*.

Issues Related to Reports Portal

- "OCTCR33I409268 - Reporting Shows an Error When Single Sign On Secrets are Changed (Azure)" below
- "OCTCR33I349068 - Some Exported Tables Show Squeezed Columns" below
- "OCTCR33I331194 - Reports and Dashboards Use UTC Time Zone" on the next page
- "OCTCR33I186200 - My Reports Folder Cannot Be Used for Exporting" on the next page
- "OCTCR33I186011 - After Hours Access Activity on GDPR Systems Summary Report Fails to Run" on the next page
- "OCTCR33I186007 - An Exported Report Might Have Format Issues" on the next page
- "OCTCR33I162021 - Cannot Remove X/Y Fields from a Graph" on page 21
- "OCTCR33I161014 - Dashboard Wizard Fails to Load all Data" on page 21
- "OCTCR33I134098 - Edit Wizard Preview is Unavailable" on page 21

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.

OCTCR33I349068 - Some Exported Tables Show Squeezed Columns

Issue: Some dashboard table columns display squeezed columns when they are exported using specific formats like HTML.

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.

OCTCR33I186200 - My Reports Folder Cannot Be Used for Exporting

Issue: You cannot export content from the **My Reports** folder.

Workaround: Contact Support for help with this issue.

OCTCR33I186011 - *After Hours Access Activity on GDPR Systems Summary* Report Fails to Run

Issue: When you specify a long time range for the *After Hours Access Activity on GDPR Systems Summary* report, the report fails to run.

Workaround: You must remove the Day of the Week variable. Complete the following steps:

1. Right-click the report.
2. Select **Edit Table**.
3. Right-click the dayOfWeek variable.
4. Select **Remove**.

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.

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.

OCTCR33I161014 - Dashboard Wizard Fails to Load all Data

Issue: If you create a dashboard using the Dashboard Wizard, when the chart is not loading, there is data that cannot be selected at the same time. This issue occurs intermittently.

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

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.

Issues Related to Search

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.

OCTCR33I411211 - Time Range Loads Incorrectly When Selecting the Default Option "DD/MM/YY hh:mm:ss:ms"

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

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

OCTCR33I385042 and OCTCR33I174130 - Search Fails to Load All Saved Search Criteria Settings

Issue: If you load a saved search Criteria from the Search page, the system fails to load the saved fieldset or time range.

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

1. Select **Search > Criteria**.

2. Click the box next to the search criteria that you want to load.

3. Click **Load**

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

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

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

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

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

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

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

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

1. The customer creates his or her own fieldset.

2. The customer creates a search criteria and assigns his or her custom fieldset to it.

3. The customer deletes the fieldset that was just created.

4. The search criteria fieldset returns to the one set in the user preferences.

5. The customer tries to load the Search Criteria from the Feature Table, but it will not load and displays a red "Failed to load search list" error message.

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

OCTCR33I341227 - Cannot Use Search Operators in the Name of a Saved Query or Criteria

Issue: If you include a search operator in the name of a saved query or criteria, Search includes that part of the saved name in the query. For example, you save a query with the name `Users and Devices`. When you load that query, Search adds "and Devices" to the query field. This occurs because "and" is also a search operator.

Workaround: Avoid the following terms in the name of a saved search query or criteria:

Term to Avoid	Workaround
&	No workaround
|	No workaround
and	Use without spaces before or after the term. For example: `UsersAndDevices`
or	Use without spaces before or after the term. For example: `UsersORdevices`

OCTCR33I324035 - Search Query Might Return Incorrect Results if the Query is not Explicitly Stated

Issue: The Search field should return the correct results from a search. If you do not get the results you expect, you might need to restate the query. For example, if your query is written with spaces, only the first word is shown in the results.

Workaround: State the query using explicit phrasing without any spaces.

OCTCR33I181059 - Fieldsets Display Database Names

Issue: When you create a fieldset, Search displays the coding-style name for the fields instead of the human-readable names that you see when creating a search query. For example, in a query you can enter or select Agent `Address`. However, in the fieldsets selection, this same field appears as agent `AddressBin`.

This issue also occurs when you're adding queries to a report.

Workaround: To identify the coding-style names, see "Mapping Database Names to their Appropriate Search Fields" in the Help or the *User Guide for ArcSight Recon*.

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.

OCTCR33I178795 - Fieldsets Default to Base Event Fields After an Upgrade

Issue: After upgrading to this release, the **Public Default Fieldset** defaults to *Base Event Fields*.

Workaround: In User Preferences, specify the fieldset that you want and set it as default again.

OCTCR33I174130 - Scheduled Searches Sometimes Fail to Export to CSV

Issue: On occasion, when you export a completed run of a scheduled search, the CSV file fails to display any data.

Workaround: If this issue occurs, view the results of the run. Then, from the Events table, export the data to a CSV file.

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

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

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

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.

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

Issue: If you change the 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.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos.
- The Micro Focus Community pages.

Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- *Administrator's Guide for ArcSight Platform*, which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.
- *Technical Requirements for ArcSight Platform*, which provides information about the hardware and software requirements and tuning guidelines for the ArcSight Platform and the deployed capabilities.
- *User's Guide for Fusion 1.5 in the ArcSight Platform*, which is embedded in the product to provide both context-sensitive Help and conceptual information.
- Product Support Lifecycle Policy, which provides information on product support policies.

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 22.1.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!