Micro Focus Security ArcSight ArcSight SIEM as a Service

23.1.1

ArcSight SIEM as a Service Release Notes

Legal Notices

Copyright Notice

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 ArcSight SIEM as a Service

ArcSight SIEM as a Service (ArcSight) release lets you use a combination of security, user, and entity solutions in a SaaS environment. The core services for ArcSight, including the Dashboard and user management, are provided by a common layer called Fusion.

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

For more information about learning how to use ArcSight SIEM as a Service, see the *ArcSight SIEM as a Service Quick Start for Administrators*.

The documentation for this product is available on the documentation website, well as context-sensitive user guides within the product. 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 SaaS documentation page.

What's New

The following sections outline the key features and functions provided in this release.

Introducing ArcMC 3.2.0

This release provides an upgrade for your standalone instance of ArcMC, updating it to ArcMC 3.2.0. If you previously installed a standalone ArcMC, we recommend that you upgrade to v3.2.0 to take advantage of the latest security fixes and resolved issues. However, ArcSight SaaS continues to be compatible with older versions of ArcMC.

For more information about the most recent updates, enhancements, known issues, and resolved software fixes, see the *Release Notes for ArcMC 3.2*.
To upgrade a standalone instance of ArcMC, see "Upgrading ArcMC" in the *ArcSight SIEM as a Service - Quick Start for Administrators*. You can upgrade the standalone instance either locally or remotely.

> We will provide an update for ArcMC in the vCHA in a future release of ArcSight SaaS.

Introduces Real-time Threat Detection

This release introduces the Real-time Threat Detection functionality. **Real-time Threat Detection** is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. It consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

Technical Requirements

For more information about the software and hardware requirements required for a successful deployment, see "Understanding the Technical Requirements" of the *ArcSight SIEM as a Service - Quick Start for Administrators*.

These *Technical Requirements* include guidance for the size of your environment based on expected workload. Micro Focus recommends the tested platforms listed in this document.

> Customers running on platforms not provided in this document 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 and Installing the Data Ingestion Components

To download and install the data ingestion components locally, see "Setting Up Data Ingestion" in the *ArcSight SIEM as a Service - Quick Start for Administrators*.

> You might need to upgrade the SmartConnectors provided in the download package. Also, if a patch is required for the vCHA, standalone ArcMC, or SmartConnectors, you can download the files from your Amazon S3 bucket as described in the *Quick Start*.

Known Issues

These issues apply to common or several components in your ArcSight SIEM as a Service environment. 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.

- "Issues Related to Fusion User Management" below
- Issues Related to Reporting
- Issues Related to Search
- "Issues Related to SOAR" on page 18
- Issues Related to Real-time Threat Detection

Issues Related to Fusion User Management

- "OCTCR33I326061 — When Selecting Manage Credentials, Advanced Authentication Services Requires You to Log Out" 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

OCTCR33I326061 — When Selecting Manage Credentials, Advanced Authentication Services Requires You to Log Out

Issue: When you try to manage your credentials from your user profile, a new tab is opened for the Advanced Authentication (AA) service (where your credentials are managed). However, this service prompts you to log out of AA. The system is designed for single sign-on, so there should be no need to logout or login when selecting manage credentials from your user profile.

Workaround: When the Advanced Authentication service prompts you, complete the following steps:

1. At the prompt, click **Logout**.

2. Return to the **ArcSight as a Service** tab.
3. Select **Manage Credentials** (again).

This time, AA will allow you to enter your credentials to log in.

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.

Issues Related to Reporting

- "OCTCR33I134098 — Edit Wizard Preview is Unavailable" below
- "OCTCR33I161014 — Dashboard Wizard Fails to Load All Data" below
- "OCTCR33I186007 — An Exported Report Might Have Format Issues" on the next page
- "OCTCR33I331194 — Reports and Dashboards Use UTC Time Zone" on the next page
- "OCTCR33I409268 — HTTP STATUS 500 Error When Clicking the Portal" on the next page
- "OCTCR33I466062 — Report Queries All Events if You Do Not Specify Values for Start and End Times" on the next page
- "OCTCR33I589121 — Brush Option Does Not Highlight Parabox Charts" on page 13

OCTCR33I134098 — Edit Wizard Preview is Unavailable

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

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

OCTCR33I161014 — Dashboard Wizard Fails to Load All Data

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

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

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.

OCTCR33I409268 — HTTP STATUS 500 Error When Clicking the Portal

Issue: Reporting runs into an Open ID or HTTP 500 error when single sign-on secrets are changed. This error does not happen right after applying the change. Reporting session information needs time to expire.

OCTCR33I466062 — Report Queries All Events if You Do Not Specify Values for Start and End Times

Issue: When scheduling a report, the user interface does not indicate that **start_time** and **end_time** are required parameters. If a user does not specify a value for these parameters, the report will fall back to query all events with a maximum limit of 3 million. This can result in the report returning many more events than intended and place an unintended large load on the database.

Workaround: When scheduling a report, specify values for **start_time** and **end_time** even though the user interface does not require it.

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.

Issues Related to Search

- "OCTCR33I610161 and OCTCR33I615024 — Incorrect Search Results Occur When Filtering With the "Id" Field" on page 18
- "OCTCR33I619035 — Fieldset and Time Stamp Selections are not Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass" on page 18

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.

OCTCR33I339016 — Dashboard Creation: Setting a Cell Size in the Table Does Not Work in a SaaS Environment

Issue: When a user chooses to manually change the cell size of a table, the emerging window does not display the values entered in the fields, and the window cannot be resized.

Workaround: Even though the values are not visible, the user can still modify then inside the fields and use them as intended. Use shortcuts such as **Ctrl + A** to select the value entered in the field, then can copy the values or replace them, as desired.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OCTCR33I576073 — Switching Tabs While Saving Searches Causes an Error

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

Workaround: Refresh the browser.

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

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

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.

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.

OCTCR33I619035 — Fieldset and Time Stamp Selections are not Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass

Issue: Search criteria fieldset and time stamp selections are not being preserved when you load them using the **Mange Search** magnifying glass.

Workaround: Load search criteria from the folder icon to retain the original fieldset and time stamp search parameters.

Issues Related to SOAR

- "OCTCR33I567004 — Data is not Displayed Properly for SOAR Timeline Widget" on the next page

- "OCTCR33I612130 — SOAR Message Broker Pod Backup File Cannot Be Created Automatically" below

OCTCR33I567004 — Data is not Displayed Properly for SOAR Timeline Widget

Issue: Dashboard displays a single SOAR timeline widget even when multiple widgets are present.

Workaround : There is no workaround if user needs to see 3 items at the same time.

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

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

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

1. Enter the following Kubernetes command in your terminal:

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

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

7. Enter the following command to save and exit:

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

8. Enter the following command to restart the pod:

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

Issues Related to Real-time Threat Detection

- "OCTCR33I231646 – Some Resources are Unavailable After Uninstalling the Security Monitoring - Base Package" on page 22
- "OCTCR33I233578 – Conditions Do Not Support Multiple Operators at the Parent Level" on page 22
- "OCTCR33I233579 – Disabled Rule Continues to Fire" on page 22
- "OCTCR33I234098 – Peer Search Disregards Hit Count Limit" on page 22
- "OCTCR33I235042 – Connector Upgrade Process Fails" on page 23
- "OCTCR33I235091 – 45-Median Report Returns "No Results" Message" on page 23
- "OCTCR33I235130 – Attributes in a Drill-Down Definition Not Visible When Using a Query Viewer" on page 23
- "OCTCR33I370003 – Retrieving Rules Returns a Bad Request" on page 23
- "OCTCR33I386094 – Services Do Not Recognize the jmx.rmi.enabled Property Value" on page 23
- "OCTCR33I386148 – Columns in Audit Event Channels Incorrectly Refer to Event Broker" on page 24
- "OCTCR33I579036 – Send Email Notification to Email Option Does Not Work" on page 24
- "OCTCR33I591010 – Extended Attribute on Installer File Causes Error on macOS" on page 24
- "OCTCR33I616038 - Degradation of Event Ingestion" on page 24
- "NGS-12407 – Annotation Flag Not Set When Forwarding Events" on page 24
- "NGS-14041 – UPPER or LOWER Built-in String Functions Return Incorrect Results in Russian Locale" on page 25
- "NGS-14477 – System Does Not Immediately Recognize Increase in Space" on page 25
- "NGS-17387 – OK and Apply Buttons are Not Enabled Correctly in the Reports Editor" on page 25

- "NGS-19880 – Maximizing Console on Linux Might Cause Mouse to Not Respond Properly" on page 25
- "NGS-20458 – Search Parameter | regex "#" Causes Search Query to Fail" on page 25
- "NGS-21831 – InSubnet Condition Strictly Enforces Wildcard Asterisk" on page 26
- "NGS-21986 – JavaScript Unresponsive Error Occurs When Viewing the Last N Events Data Monitor" on page 26
- "NGS-22568 – LengthOf Function Might Display Incorrect Values in Traditional Chinese Environment" on page 26
- "NGS-22583 – Creating a Drilldown Based on an Active Channel Results in Display Errors" on page 26
- "NGS-22600 – Top Value Count Dashboard is Missing Some Values in Traditional Chinese Environment" on page 26
- "NGS-22659 – Exiting or Closing Console in Dark Theme Results in Prompt to Save Changes Even If You Made No Changes" on page 27
- "NGS-22669 – Payload Information Cannot be Retrieved" on page 27
- "NGS-22991 – Display Hangs When Viewing a Data Monitor in Tile Format in Simplified and Traditional Chinese Environments" on page 27
- "NGS-23004 – Importing a Case Package from an English Locale to a Simplified Chinese Locale Might Result in Incorrect Values" on page 27
- "NGS-23214 – ArcSight Console Might Not Run Properly If Properties File Contains Encrypted and Unencrypted Entries" on page 28
- "NGS-23429 – Report Output Does Not Includes HTML Reports" on page 28
- "NGS-23437 – Dashboard Background Image Does Not Carry Over from Console to Command Center" on page 28
- "NGS-23444 – Dark Theme Renders Some Onscreen Instructions Illegible" on page 29
- "NGS-23489 – Multiple Consoles on Same Linux Machine Causes Upgrade to Fail" on page 29
- "NGS-23554 – ArcSight Investigate 1.01 Displays No Data Results" on page 29
- "NGS-23639 – Search Fails When String-Based Fields Contain Leading or Trailing Spaces" on page 29
- "NGS-24957 – GetSessionData Function Might Display an Incorrect Result" on page 30
- "NGS-25631 – Package Push Operation Does Not Verify That a Package Exists on Subscribers" on page 30
- "NGS-26357 – Charts Might Appear Small in ArcSight Command Center" on page 30
- "NGS-26380 – Override Status and Remove Entry Options Do Not Work Correctly" on page 30

OCTCR33I231646 – Some Resources are Unavailable After Uninstalling the Security Monitoring - Base Package

Issue: If you uninstall the Security Monitoring - Base package, some resources will be unavailable, such as the variables related to MITRE ATT&CK.

Workaround: Uninstall the Security Monitoring - Base - Active List package, and then reinstall both packages.

OCTCR33I233578 – Conditions Do Not Support Multiple Operators at the Parent Level

Issue: When you create a condition in a channel or an Active List, if the AND and OR operators are at the parent level, the filter summary does not include the OR.

Workaround: Ensure there is only one operator at the parent level. You can then add other operators under the parent operator.

OCTCR33I233579 – Disabled Rule Continues to Fire

Issue: In distributed mode, when a user deletes a list that a rule references, the rule is disabled but continues to fire.

OCTCR33I234098 – Peer Search Disregards Hit Count Limit

Issue: When you run a peer search with a Real-time Threat Detection installation as a peer, Real-time Threat Detection disregards the hit count limit.

OCTCR33I235042 – Connector Upgrade Process Fails

Issue: The connector upgrade process fails the first time you try to run it from the Console.

Workaround: Please restart the Console, connect to Real-time Threat Detection, and start the connector upgrade process again. The upgrade will proceed without further error.

OCTCR33I235091 – 45-Median Report Returns "No Results" Message

If license usage data is corrupted, the 45-median report will state, "No results were returned from the server."

OCTCR33I235130 – Attributes in a Drill-Down Definition Not Visible When Using a Query Viewer

Issue: When you create a drill-down definition, you can base it on all available attributes. When viewing a query viewer in a chart, however, not all attributes are visible. Drill-down definitions that use attributes that are not part of a chart view are invalid.

Workaround: Use a table to view the query viewer.

OCTCR33I370003 – Retrieving Rules Returns a Bad Request

Issue: When using the Real-time Threat Detection API, if you delete a rule in a folder from the Real-time Threat Detection web application. retrieving rules from that folder returns a bad request.

Workaround: Retrieve the rule again, and then no error occurs.

OCTCR33I386094 – Services Do Not Recognize the jmx.rmi.enabled Property Value

Issue: Setting the `jmx.rmi.enabled` property value in the `esm.properties` file affects only the correlator and aggregator services. The repo and mbus services do not recognize it.

Workaround: To affect all services, use the `jmx.rmi.enabled` property value in the `esm.defaults.properties` file.

OCTCR33I386148 – Columns in Audit Event Channels Incorrectly Refer to Event Broker

Issue: In the default Transformation Hub audit events active channel, as well as any custom audit event channels, the Device Event Class ID and Device Event Category columns incorrectly refer to Event Broker instead of Transformation Hub. This does not affect functionality in any way.

OCTCR33I579036 – Send Email Notification to Email Option Does Not Work

Issue: When you configure the Send Notification rule action in a SaaS environment, the "send email notification to email" option does not work.

OCTCR33I591010 – Extended Attribute on Installer File Causes Error on macOS

Issue: When you use a browser to download the macOS installer file, the file has an extended attribute, `com.apple.quarantine`. This attribute causes the following error:

```
"ArcSightConsoleSaaS" is damaged and can't be opened. You should move it to
the Trash.
```

Workaround: Use curl to download the installer file.

OCTCR33I616038 - Degradation of Event Ingestion

Issue: Real-time Threat Detection is scaled to an EPS limit. Sending EPS above the deployed limit for extended periods of time might result in degradation of event ingestion into MSK.

NGS-12407 – Annotation Flag Not Set When Forwarding Events

Issue: Annotation flag indicating 'forwarded' may not get set when forwarding events from Real-time Threat Detection.

NGS-14041 – UPPER or LOWER Built-in String Functions Return Incorrect Results in Russian Locale

Issue: Database queries using the UPPER or LOWER built-in string functions in the Russian locale return incorrect results when filtering events. This applies especially to queries using the Ignore Case option, which rely on the UPPER function.

NGS-14477 – System Does Not Immediately Recognize Increase in Space

Issue: Space-based retention cleans up same day data, but even after increasing the space, the system does not recognize that the space has been increased until midnight.

NGS-17387 – OK and Apply Buttons are Not Enabled Correctly in the Reports Editor

Issue: There was an issue in the reports editor where after selecting another query, or modifying the current one for the given report, the OK/Apply buttons were not being enabled correctly when doing further modifications to the Fields Table cells on the Data tab of the Report Editor.

NGS-19880 – Maximizing Console on Linux Might Cause Mouse to Not Respond Properly

Issue: On Linux, mouse interaction with ArcSight Console after maximizing may not respond as expected.

Workaround: Instead of maximizing, drag corners of ArcSight Console to resize to fill desktop.

NGS-20458 – Search Parameter `| regex "#"` Causes Search Query to Fail

Issue: The search parameter `| regex "#"` will cause the search query to fail and will throw a 503 service request error. Once the page gets a 503 error, it does not leave this state.

Workaround: Refresh the page (press F5).

NGS-21831 – InSubnet Condition Strictly Enforces Wildcard Asterisk

Issue: The InSubnet condition strictly enforces the use of the wildcard asterisk "*". For example, a filter like 10.10. is invalid, and 10.10.*.* is valid.

Old content that uses inSubnet without a supported format (2-address, or CIDR, or wildcard) will need to use a supported format.

NGS-21986 – JavaScript Unresponsive Error Occurs When Viewing the Last N Events Data Monitor

Issue: Viewing the Last N events data monitor in the ArcSight Command Center which contains numerous variable fields (based on an overlapping Session List) may cause a JavaScript unresponsive error.

Workaround: Limit the data monitor to six variable fields with 10 rows, or split the fields by creating one or more data monitors.

NGS-22568 – LengthOf Function Might Display Incorrect Values in Traditional Chinese Environment

Issue: In Traditional Chinese the function LengthOf may display incorrect values and/or produce the wrong filter results.

NGS-22583 – Creating a Drilldown Based on an Active Channel Results in Display Errors

Issue: The Condition Summary is not formatted in color codes and also does not display the field Display Name when a drilldown is created based on Active Channel.

NGS-22600 – Top Value Count Dashboard is Missing Some Values in Traditional Chinese Environment

Issue: On a Traditional Chinese Installation, when you display the Top Value Count dashboard, the Stacking Area, Area,Scatter Plot, and Line options show no data. Data displays in the Bar, Pie, and Stacking Bar options.

NGS-22659 – Exiting or Closing Console in Dark Theme Results in Prompt to Save Changes Even If You Made No Changes

Issue: When you open two dashboards (All Monitored Devices and Critical Monitored Devices) while the Console is set to dark theme in /All Dashboards/ArcSight Administration/Devices/ and exit or close, you are prompted to save them even when no changes are made.

Workaround: Select Yes and save the dashboards. The next time you open and close these dashboards, you do not get the save prompt.

NGS-22669 – Payload Information Cannot be Retrieved

Issue: When events are sent to Real-time Threat Detection by Transformation Hub, payload information cannot be retrieved for the corresponding event.

NGS-22991 – Display Hangs When Viewing a Data Monitor in Tile Format in Simplified and Traditional Chinese Environments

Issue: In Simplified Chinese and Traditional Chinese, if you create a data monitor with the type HourlyCount and view it in tile format, its display will hang with no data displayed.

NGS-23004 – Importing a Case Package from an English Locale to a Simplified Chinese Locale Might Result in Incorrect Values

Issue: On a system with the Simplified Chinese locale, after the import of a case package created in English locale, the properties of the case may have default values instead of the entered values. This issue exists in both the ArcSight Command Center and the ArcSight Console.

NGS-23214 – ArcSight Console Might Not Run Properly If Properties File Contains Encrypted and Unencrypted Entries

Issue: In FIPS mode, if you have used changepassword to encrypt either ssl.keystore.password or ssl.truststore.password, and then you run consolesetup, check config/client.properties to make sure that you do not have entries for both

ssl.keystore.password

ssl.keystore.password.encrypted

and likewise for ssl.truststore.password. If you do, remove the entry that is not encrypted.

If you do not do this, then the ArcSight Console might not run properly.

NGS-23429 – Report Output Does Not Includes HTML Reports

Issue: Reports run in HTML format from ArcSight Command Center containing charts do not show up in the report output when the server is configured with the following properties, which save report output in database:

vfs.report.provider.scheme=db

vfs.report.provider.class=com.arcsight.common.vfs.database.ArcDatabaseFileProvider

vfs.report.provider.base=db://reports/archive

Workaround: Run the report in PDF format.

NGS-23437 – Dashboard Background Image Does Not Carry Over from Console to Command Center

Issue: If you set a background image to a dashboard in the ArcSight Console, this image is not set to the same dashboard when it is viewed in the ArcSight Command Center.

NGS-23444 – Dark Theme Renders Some Onscreen Instructions Illegible

Issue: When ArcSight Console is in dark theme and you run the "arcsight replayfilegen" command, you will have difficulty following instructions on the Wizard.

Workaround: Run the command when the ArcSight Console is in the default theme.

NGS-23489 – Multiple Consoles on Same Linux Machine Causes Upgrade to Fail

Issue: If two users each have a Console installed on the same Linux machine and they both try to upgrade, the first upgrade will succeed but the second will fail with the error /tmp/exportfile.pkcs12 (Permission denied).

Workaround: Delete the file "/tmp/exportfile.pkcs12" and re-run consolesetup for the second user to transfer settings again.

NGS-23554 – ArcSight Investigate 1.01 Displays No Data Results

Issue: If you launch the Arcsight Investigate integration command from a blank field (a field with an empty value) in either the ArcSight Console or the ArcSight Command Center, ArcSight Investigate 1.01 displays no data results.

Workaround: Change the search field value to one of the following:

- String value: `'',NONE`
- Integer value: `0,NONE`

NGS-23639 – Search Fails When String-Based Fields Contain Leading or Trailing Spaces

Issue: When you start ArcSight Investigate from Real-time Threat Detection on string based fields containing leading or trailing spaces, the search will fail.

Workaround: In such cases, manually fix the spaces before or after the value.

NGS-24957 – GetSessionData Function Might Display an Incorrect Result

Issue: The GetSessionData function that uses sessionlist with multiple keys might show an incorrect result.

NGS-25631 – Package Push Operation Does Not Verify That a Package Exists on Subscribers

Issue: Unlike the ArcSight Console, which prevents the import of packages that already exist in the system, the Package Push operation of the Content Management feature in the ArcSight Command Center does not verify that a package exists on Subscribers. In some cases, pushing a modified package can cause resource corruption.

NGS-26357 – Charts Might Appear Small in ArcSight Command Center

Issue: While viewing dashboards in the ArcSight Command Center, charts might appear small.

Workaround: Refresh the page for proper rendering.

NGS-26380 – Override Status and Remove Entry Options Do Not Work Correctly

Issue: In the Last State data monitor, the Override Status and Remove Entry options are not working correctly.

NGS-26720 – Generated Correlation Events Display the Wrong URI

Issue: If you move a rule group from the Real-time Rules folder to another folder (and delete from Real-time Rules), and then you schedule that new rule group, when rules in this new group are triggered, you will notice that the generated correlation events show the wrong information: the URI is still remembered as the old Real-time Rules folder instead of the new URI.

NGS-26915 – Analyze Channel Option Might be Disabled

Issue: The "Analyze Channel" option on the channel's right-click menu might be disabled sometimes on the bar chart or pie chart. On the second attempt, the option will be enabled.

NGS-27091 – Issue With Drill Down From Stacked Bar Charts

Issue: Drill down from stacked bar charts doesn't work as expected.

NGS-29487 – Issue with Font Rendering on Windows and Linux Operating Systems

Issue: An issue with font rendering on Windows and Linux operating systems can affect how the Console displays resource names containing one or more "." characters. For example, the resource name is clipped in the resource tree or a resource name might extend over a nearby component on the screen.

Workaround: Change the Console font to one that does not demonstrate this behavior, such as Arial.

To change the font for the Console, go to **Edit > Preferences**, and select **Global Options**. Change the font to Arial, and apply the changes.

NGS-29702 – Event Search Uses Local Time Instead of Server Time

Issue: If your local computer is in a different timezone than the Real-time Threat Detection server, any event search attempts to use the local time instead of the server time. For example, if you create an Active Channel that uses the Real-time Threat Detection server time, and then perform an event search, the event search uses the local time range. As a result, there is a mismatch and the event cannot be found.

Workaround: When you perform an event search, specify the time zone for the Real-time Threat Detection server.

NGS-32858 – MITRE Activity Dashboard Might be Blank

Issue: The MITRE Activity Dashboard might be blank, even if there is data in the Rules Triggered with Mitre ID Active List (/All Active Lists/ArcSight Foundation/MITRE ATT&CK/Rules Triggered).

Workaround: Delete the row with empty values or manually update the row with the correct data.

Resolved Issues

Issues reported in this section apply to common or several components in your ArcSight SIEM as a Service environment. For more information about issues related to a specific product, please see that product's release notes.

- "Issues Related to Platform" below
- "Issues Related to Reporting" below
- "Issues Related to Search" on page 34
- "Issues Related to SOAR" on page 38
- "Issues Related to Real-time Threat Detection" on page 40

Issues Related to Platform

- "OCTCR33I610053 — Event Integrity: The Check Progress Percentage Issue Has Been Corrected" below

OCTCR33I610053 — Event Integrity: The Check Progress Percentage Issue Has Been Corrected

A code fix has resovled an issue with check progress percentage. Previously, if the system encountered duplicate verification events, the check progress percentage sometimes exceeded 100%, and the events were counted multiple times.

Issues Related to Reporting

- "OCTCR33I160009 – Chart Wizard No Longer Fails to Display the Convert to Measure Button" on the next page

- "OCTCR33I162021 — Removing X/Y Fields From a Graph Display Issue is Resolved" below
- "OCTCR33I346022 – Issues Related to Exported Dashboard Failing to Include All Columns in Some Tables" below
- "OCTCR33I461037 – Display issues for Raw Event Information Have Been Resolved" on the next page
- "OCTCR33I566085 — Network Chart Truncated Data Display Has been Resolved" on the next page

OCTCR33I160009 – Chart Wizard No Longer Fails to Display the Convert to Measure Button

A software fix resolved the problem of the **Convert to Measure** button becoming unavailable if you tried to create a chart using the Chart wizard after you changed from "convert" to "dimension."

OCTCR33I162021 — Removing X/Y Fields From a Graph Display Issue is Resolved

A software update resolved a chart editor problem. Previously, when you removed an X or Y field, the Reports Portal intermittently displayed an error message.

OCTCR33I346022 – Issues Related to Exported Dashboard Failing to Include All Columns in Some Tables

An issue was identified where tables in a dashboard have several columns. If you export the dashboard, the right side of the table might become truncated, hiding some data from the exported visuals.

This is expected behavior. The expected behavior of the "expand components" option is to fully expend scrolling tables and scrolling charts.

OCTCR33I461037 – Display issues for Raw Event Information Have Been Resolved

A software fix has resolved the raw event information display problems for text alignment, scrolling, and tooltip information.

OCTCR33I566085 — Network Chart Truncated Data Display Has been Resolved

A code update resolved the issue where the network chart display truncated data, such as IP addresses, to the point where the displayed content is not useful.

Issues Related to Search

- "OCTCR33I167004 — Scheduled Tasks: If the User Closes the Dialog Box, the Task is No Longer Automatically Saved" on the next page
- "OCTCR33I610053 — Event Integrity: The Check Progress Percentage Issue Has Been Corrected" on page 32
- "OCTCR33I369029 — Load Modal No Longer Loads Search Criteria When the Fieldset is Deleted" on the next page
- "OCTIM33I512017 – Search Settings for a Saved Search Criteria Now Display" on page 36
- "OCTCR33I549163 – Searches With No Changes Since the Last Run No Longer Appear Stuck" on page 36
- "OCTCR33I549165 and OCTCR33I566003 – Results of Saved Scheduled Search Results and Saved Searches Containing the Rename Operator Now Display Properly" on page 36
- "OCTCR33I549166 — Results of Saved Scheduled Searches Containing the Eval Operator Now Display Properly" on page 36
- "OCTCR33I561004 — Completed Runs of a Scheduled Search Containing the Rename Operator No Longer Return 0 Results" on page 37
- " OCTCR33I566020 – Search Histogram: The Histogram’s Current Zoom and Pan State is Now Maintained if Users Switch Tabs" on page 37
- "OCTCR33I566082 — Scheduled Searches: Resolved Issues Related to Switching the Field “Search Expires in” in User Preferences" on page 37
- "OCTCR33I566223 — The Number of Results Column Now Reflects the Correct value for Scheduled Searches" on page 37

- "OCTCR33I566082 — Scheduled Searches: Resolved Issues Related to Switching the Field “Search Expires in” in User Preferences" on page 37
- "OCTCR33I346022 – Issues Related to Exported Dashboard Failing to Include All Columns in Some Tables" on page 33
- "OCTCR33I585053 — Can Now Add a Field from Event Inspector to Active Search Even if the Field is Not Available in the Fieldset" on page 38
- "OCTCR33I587006 – Search No Longer Fails When the "where condition" Operator has any <...> and Contains a Filter for Field Groups" on page 38

OCTCR33I167004 — Scheduled Tasks: If the User Closes the Dialog Box, the Task is No Longer Automatically Saved

A problem with saving while closing the dialog box has been resolved. Previously, when you clicked the **Close** button during the scheduler task creation process, the modal dialog box closed, but the task was still saved.

OCTCR33I369029 — Load Modal No Longer Loads Search Criteria When the Fieldset is Deleted

Search criteria does not load under the circumstances described below.

- The customer creates his or her own fieldset.
- The customer creates a search criteria and assigns his or her custom fieldset to it.
- The customer deletes the fieldset that was just created.
- The search criteria fieldset returns to the one set in the user preferences.
- 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.

OCTCR33I453265 – Event Grid No Longer Blinks When Loading Data

The issue where the grid appeared to blink while scrolling and simultaneously trying to load data from the server has been resolved. This was related to the API taking a long time to load the data.

OCTIM33I512017 – Search Settings for a Saved Search Criteria Now Display

An issue where Search failed to display appropriately after you selected saved search criteria has been resolved. Previously, you might have seen the following error messages:

- Failed to load search list
- Failed to initialize server state for user
- Failed to load all global metadata messages

OCTCR33I549163 – Searches With No Changes Since the Last Run No Longer Appear Stuck

A code fix resolved a problem where the user interface did not allow you to rerun custom time range searches that did not have any changes since the last run.

OCTCR33I549165 and OCTCR33I566003 – Results of Saved Scheduled Search Results and Saved Searches Containing the Rename Operator Now Display Properly

A code fix resolved display problems for saved scheduled search results and saved searches that contain the **rename** operator. Previously, the data would not load properly when the user opened the Search results tab, and the renamed columns did not appear in the grid. This has now been addressed.

OCTCR33I549166 — Results of Saved Scheduled Searches Containing the Eval Operator Now Display Properly

A code change resolved toe problem where the results of a saved Scheduled search containing the eval operator would not load properly when it was opened in the Search Results tab.

OCTCR33I561004 — Completed Runs of a Scheduled Search Containing the Rename Operator No Longer Return 0 Results

A code update addressed a problem with the rename operator. Previously, the results of a Scheduled search (canned query) containing the rename operator would reflect 0 results and an error would be displayed.

OCTCR33I566020 – Search Histogram: The Histogram’s Current Zoom and Pan State is Now Maintained if Users Switch Tabs

A code fix has resolved the problem that occurred where the zoom/pan state was not being maintained when a user zoomed or panned in the histogram or switched tabs, and then returned to the original tab.

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

A software fix resolved the problem where the search failed to complete and showed an incorrect setting. The user could encounter this issue if they 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 error revealed itself by giving a result of 7 weeks instead of 10 weeks. This issue also occurred if you switched the settings from weeks to days and weeks to “Never Expire,” even with a fresh install.

OCTCR33I566223 — The Number of Results Column Now Reflects the Correct value for Scheduled Searches

A code change resolved the issue. Previously, for Scheduled searches with the **where** operator, the # OF RESULTS column did not match actual search results stats.

OCTCR33I576083 — Outlier Detection: Outlier History Displays Correctly When No Score Exists

A software fix addressed a problem In **Outlier Detection**, where the **Top Anomalous Hosts** and **Outlier History** posted zeros (0) and displayed empty charts when no score exists,.

OCTCR33I576112 — Outlier Detection: Addressed Issue About Multiple Outlier Model Scoring at the Same Time

Scoring is done at regular intervals. If scoring fails during a certain period, then scoring will try again during the next period. A code update now prevents errors related to multiple outlier models scoring at the same time.

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

A code update resolved this issue. Previously, if you added a field from the Event Inspector to an active search, and the field was not available in the fieldset of the active search, an error occurred.

OCTCR33I587006 – Search No Longer Fails When the "where condition" Operator has any <...> and Contains a Filter for Field Groups

A software fix now lets you use non-string datatype fields in a **| where any...contains** query without having to convert the fields to string data. Previously you had to use eval to string in the query syntax.

Issues Related to SOAR

- "OCTCR33I467084 - Unable to Add File to Scope in Automation" on the next page
- "OCTCR33I514042 - SOAR - IP Country Information is Always Unknown" on the next page

OCTCR33I467084 - Unable to Add File to Scope in Automation

The problem where the files and the hash values were not getting added to case scope automatically is resolved.

OCTCR33I514042 - SOAR - IP Country Information is Always Unknown

The problem where the country scope item property for IP addresses were shown unknown, is fixed. This issue was caused due to configuration issues of Geo IP database.

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

This integration was fetching all the events for device connectivity, which was not required has been resolved.

OCTCR33I553001 - Username Query is Missing Parameter Definition

A software fix has resolved the missing parameter definition for username in username query. Now the username parameter will be searched in sourceUserName and destinationUserName fields.

OCTCR33I554081 – Workflow Playbook: Now Saves Playbooks with Alert Source as a Starting Condition

A code change fixed the issue that occurred when the alert source equals or not equals option is selected as the starting condition for a workflow playbook. The pre-saved condition now shows the chosen alert source and the playbook can be saved.

OCTCR33I568187 — Case Custom Field Value are Now Saved in Automation Bit

A code change resolved to issue of custom fields not saving values In automation bits.

Issues Related to Real-time Threat Detection

- "OCTCR33I234215 – Resolved Problem of the Connector Installation Program Returning a Handshake Error" below
- "OCTCR33I580041 – Unrecognized App Warning No Longer Occurs During Console Installation" below
- "OCTCR33I586008 – Import Users & Groups from ESM Option Now Work in SaaS Environment" on the next page
- " OCTCR33I566020 – Search Histogram: The Histogram's Current Zoom and Pan State is Now Maintained if Users Switch Tabs" on page 37

OCTCR33I234215 – Resolved Problem of the Connector Installation Program Returning a Handshake Error

Issue: When configuring Connector version 7.15 or older with Real-time Threat Detection, the installation program returned a handshake error. A software fix resolved this issue.

OCTCR33I580041 – Unrecognized App Warning No Longer Occurs During Console Installation

Issue: A code change resolved a problem when you installed the Real-time Threat Detection Console in a Windows 10 environment, an "unrecognized app" warning occurred. The previous solution was to click **Run Anyway**.

OCTCR33I586008 – Import Users & Groups from ESM Option Now Work in SaaS Environment

Issue: Previously, the Import Users & Groups from ESM functionality was not applicable in a SaaS environment, but the option is still visible in this release. This issue has been resolved.

OCTCR33I613001 - Login to ACC Using OSP is No Longer Case Sensitive

The Real-time Threat Detection User\External ID field is case sensitive. When adding users to Real-time Threat Detection, ensure that the External ID field value matches the email address, including case of the email provided to Fusion User Management.

Contacting Micro Focus

For specific product issues, contact CyberRes SaaS Customer Success Support team or email us at cyberressupport@microfocus.com. For outtages, call +1 (855) 982-2261 (US).

Additional technical information or advice is available from several sources:

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

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 SIEM as a Service Release Notes (ArcSight SIEM as a Service)

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!