Micro Focus Security ArcSight ArcSight SIEM as a Service

23.4.1

ArcSight SIEM as a Service Release Notes

Legal Notices

Copyright 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.

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 ArcSight SIEM as a Service

This ArcSight SIEM as a Service (ArcSight or ArcSight SaaS) 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.

- "What's New" below
- "Technical Requirements" on page 12
- "Downloading and Installing the Data Ingestion Components" on page 12
- "Known Issues" on page 13
- "Resolved Issues" on page 30
- "Contacting Micro Focus" on page 40

For 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. Context-sensitive user guides also are available 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.

Introduces the Ability to Query ArcSight Logger Data in ArcSight SaaS

This release gives you the ability to import data currently in ArcSight Logger to ArcSight SaaS. You can import archived event data from all available Loggers, thus eliminating the need to continue managing Loggers in your environment. ArcSight SaaS stores the imported data in the ArcSight Database, making it available for Search and Reporting activities once the data import has completed successfully.

The import process has two phases. In Phase One, you will run a tool on your Loggers to connect them to ArcSight SaaS. In the tool, you can choose which archived data you want to import, thus creating a catalog of the metadata that defines the archived events and uploading that along with the Logger archives to temporary storage in an AWS S3 bucket. In Phase Two, you will log in to ArcSight SaaS and begin importing the event data that is associated with the archive catalogs in temporary storage to the ArcSight Database.

For data that has not been imported, the temporary files will be deleted from the bucket based on the ArcSight license purchased by your organization.

For more information about configuring data ingestion and importing Logger data, see "Checklist: Migrating Logger Data" in the *ArcSight SIEM as a Service - Quick Start for Administrators* and "Importing Logger Data to the ArcSight Database (SaaS)" in the product Help.

Please be aware that importing data from your Loggers is one method for ingesting event data from your environment. As a best practice, you should also configure your existing SmartConnectors to send events to ArcSight SaaS so that search queries will include the latest events in your environment. For more information, see "Getting Started" in the *ArcSight SIEM as a Service - Quick Start for Administrators*.

Improves the SOAR Capability

This release provides the following enhancements to the SOAR capability:

- Ability to use File Type Scope Items in Integration Plugins
- "New Integration Plugins for SOAR " on the next page

Use File-type Scope Items in Integration Plugins

SOAR now has the ability to use or call file type scope items in the integration plugins. This feature enables plugin authors to write enrichment or action plugins (for example, Intezer, Virustotal, etc.) that can directly use files for use cases such as submitting them to sandboxing solutions..

It also enables the SOC analyst to enrich files and not just hashes.

New Integration Plugins for SOAR

New Integration Plugins:

- **BMC Helix Remedyforce Integration**

  This integration plugin has the following action and enrichment capabilities: Add Client Note to Incident, Add Client Note to Service Request, Close Incident, Close Service Request, Create Incident, Create Service Request, Update Incident, Update Service Request, Get Incident Details, Get Service Request Details, List Request Definition Questions, List Request Definitions.

- **Domain Tools Integration**

  This integration plugin has the following action and enrichment capabilities: Get Domain Profile, Get Domain Reputation, Get Domain Risk, Domain Hosting History, Recent Domain, Reverse IP Lookup, Reverse IP Whois, Whois Lookup, Iris Investigate.

- **McAfee Web Gateway v2 Integration**

  This integration plugin has the following action and enrichment capabilities: Add Entry to List, Remove Entry from List, Get List Entries, Get List Entry Details, Get Lists.

- **Microsoft Azure Active Directory Integration**

  This integration plugin has the following action and enrichment capabilities: Add User to Group, Disable User, Enable User, Get User Details, Get User’s Manager, List Groups, List User’s Groups, List Users, Remove User from Group, Revoke Sessions, Create Group, Delete Group, List Delegated Permissions.

- **Microsoft Defender for CloudApps Integration**

  This integration plugin has the following action and enrichment capabilities: Close Alert as Benign, Close Alert as False Positive, Close Alert as True Positive, Get Alert by ID, Get Entity Details, List Activities, List Activities by IP, List Activities by User, List Activities by User Domain, List Alerts,List Alerts by IP, List Alerts by Severity, List Alerts by Status, List Entities, List IP Ranges, Mark Alert as Read, Mark Alert as Unread.

- **Sailpoint Integration**

  This integration plugin has the following action and enrichment capabilities: Disable Account, Enable Account, Get Account Activity, Get Account Details, Get Account Entitlements, Get Account IDs.

- **Slack Integration**

This integration plugin has the following action and enrichment capabilities: List Channels, Get Channel Info, Create Channel, Send Message to Channel, Archive Channel, Invite User to Channel.

Improves the Built-in Foundation Dashboards

This release changes some built-in dashboards in the Foundation category:

- **Account Management Overview**

  Improves usability and visualizations of account activity.
- **Malware Overview**

  Improves usability and visualizations of the types of malware attacking your environment, outcomes, and responses by anti-malware tools.
- **Attacks and Suspicious Activity**

  Improves usability and visualizations that displays suspicious activity in your environment. Moved from the Network Monitoring folder to the Malware Monitoring folder.
- **Login Activity Overview**

  Displays log-in activity and outcomes in your environment. This dashboard replaces Failed Logins Overview and Successful Login Overview dashboards.
- **Host Profile Overview**

  New dashboard that displays activity on a specified host.

Introduces ArcMC 3.2.0 for the vCHA

This release provides an upgrade for ArcMC in the vCHA and instructions about updating it to ArcMC 3.2.0. We recommend that you upgrade to ArcMC 3.2.0 in the vCHA to take advantage of the latest security fixes and resolved issues. However, ArcSight SaaS continues to be compatible with older versions of ArcMC.

This release also includes an update for the operating system in the vCHA. For more information about updating components of the vCHA, see "Upgrading the vCHA" and "Installing the Virtual CHA" in the *ArcSight SIEM as a Service - Quick Start for Administrators*.

For more information about the most recent updates, enhancements, known issues, and resolved software fixes in ArcMC, see the *Release Notes for ArcMC 3.2*.

Adds Support for SmartConnector 8.4 P1

This release adds support for SmartConnector 8.4 P1. If you are using a previous version of SmartConnector, we recommend you upgrade to this version to take advantage of security and other defect fixes. However, ArcSight SaaS continues to be compatible with older versions of the SmartConnector as specified in the "Technical Requirements for Data Ingestion."

For more information about the most recent changes, enhancements, known limitations, and software fixes, see Release Notes for ArcSight SmartConnector 8.4 P1.

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

Technical Requirements

For more information about the software and hardware requirements needed 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 19
- 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 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 16

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.

Workaround: There is no workaround for this issue.

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 for this issue.

Issues Related to Search

- "OCTCR33I179782 — Scheduled Search Appends Erroneous Values to the Run Interval" below
- "OCTCR33I411211 — Time Range Loads Incorrectly When Selecting the Default Option “DD/MM/YY hh:mm:ss:ms”" on the next page
- "OCTCR33I549094 — Intermittent Failure of .csv File Containing Scheduled Search Results" on the next page
- "OCTCR33I576073 — Switching Tabs While Saving Searches Causes an Error" 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
- "OCTCR33I610161 — Incorrect Search Results Occur When Filtering With a Specific "Id" Field" on page 18
- "OCTCR33I615073 — Query May Exceed Database Limits When a Long Operator Chain is Used With the "All Fields" Fieldset" on page 18
- "OCTCR33I619035 — Fieldset and Time Stamp Selections are not Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass" on page 19
- "OCTCR33I616090 — For System Search Queries, #SSH Authentication Throws an Error" on page 19
- "OCTCR33I643057 — When You Are Viewing Raw Events in the Search Results Table, Scrolling Might Become Stuck " on page 19

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.

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.

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.

OCTCR33I610161 — Incorrect Search Results Occur When Filtering With a Specific "Id" Field

Issue: Queries that filter specific "id" field values will not return correct results such as id = "123456789" or id != "123456789." This issue appeared after running a search using a custom time frame while searching for a specific "id" field value. A related issue, OCTCR33I615024, has been resolved.

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.

OCTCR33I615073 — Query May Exceed Database Limits When a Long Operator Chain is Used With the "All Fields" Fieldset

Issue: When you use a long operator chain with "All Fields" fieldset, the resulting query may exceed the database limits and fail. **Field summary** may also fail to open because of this problem.

Workaround: Narrow the fieldset to include only those listed in the Operator Chaining query.

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: When loading search criteria from the folder icon, the original search parameters (including the field set and timestamp) are preserved.

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.

OCTCR33I643057 — When You Are Viewing Raw Events in the Search Results Table, Scrolling Might Become Stuck

Issue: Doing infinite scrolling while viewing raw event data in the Search Results Table might cause the scrolling to become stuck.

Workaround: Close the Search tab and restart the search in a new Search tab.

Issues Related to SOAR

- OCTCR33I605095 — FTP Action Plugin Fails on Action Rollback if the remote.file.filename.appenduuid=true
- OCTCR33I638001 — SOAR Allows to Execute Quarantine Computer Action Capability with Empty /Null Parameters

OCTCR33I605095 — FTP Action Plugin Fails on Action Rollback if the remote.file.filename.appenduuid=true

Issue: FTP action rollback fails when remote.file.filename.appenduuid=true.

Workaround: There is no workaround at this time.

OCTCR33I638001 — SOAR Allows to Execute Quarantine Computer Action Capability with Empty /Null Parameters

Issue: SOAR allows to execute Quarantine Computer action capability with empty / null parameters.

Workaround: There is no workaround at this time.

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
- "OCTCR33I235130 – Attributes in a Drill-Down Definition Not Visible When Using a Query Viewer" on page 22
- "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 23
- "OCTCR33I579036 – Send Email Notification to Email Option Does Not Work" on page 23
- "OCTCR33I585013 – SaaS Login Screen for ACC from Fusion Should not Display Even if the Persistor is Busy or if a Persistor is Down" on page 24
- "OCTCR33I591010 – Extended Attribute on Installer File Causes Error on macOS" on page 24
- "OCTCR33I616038 — Degradation of Event Ingestion" on page 24

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

OCTCR33I585013 – SaaS Login Screen for ACC from Fusion Should not Display Even if the Persistor is Busy or if a Persistor is Down

Issue: The ACC login screen from Fusion might display instead of the Single Sign-on (SSO) login screen. This can happen If persisitor is busy or some services are not running.

Workaround: Watch for the persistor load to become less or make sure all Real-time Threat Detection services are running before logging into to ACC.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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-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.

Workaround: If you have old content that uses InSubnet without a supported format (for example, 2-address, or CIDR, or wildcard), update to 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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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

Issue: The ArcSight console might not run properly if the properties file contains both encrypted and unencrypted entries.

Workaround: 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 and ssl.keystore.password.encrypted

and likewise for ssl.truststore.password.

If you see this, remove the entry that is not encrypted. If you do not do this, then the ArcSight Console might not run properly.

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.

Workaround: There is no workaround for this issue.

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-24957 – GetSessionData Function Might Display an Incorrect Result

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

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

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.

Workaround: Try again. The option will be enabled on the second attempt.

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

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

Workaround: There is no workaround for this issue.

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-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" on the next page
- "Issues Related to Search" on page 32
- "Issues Related to SOAR" on page 37

Issues Related to Platform

- "OCTCR33I610053 — Event Integrity: The Check Progress Percentage Issue Has Been Corrected" on the next page

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" below
- "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" on the next page
- "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 expand 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
- "OCTCR33I339016 — Dashboard Creation: Setting a Cell Size in the Table Does Now Works in a SaaS Environment" on page 34
- "OCTCR33I369029 — Load Modal No Longer Loads Search Criteria When the Fieldset is Deleted" on page 34
- "OCTCR33I453265 – Event Grid No Longer Blinks When Loading Data" on page 34
- "OCTIM33I512017 – Search Settings for a Saved Search Criteria Now Display" on page 34
- "OCTCR33I549163 – Searches With No Changes Since the Last Run No Longer Appear Stuck" on page 35

- "OCTCR33I549165 and OCTCR33I566003 – Results of Saved Scheduled Search Results and Saved Searches Containing the Rename Operator Now Display Properly" on page 35
- "OCTCR33I549166 — Results of Saved Scheduled Searches Containing the Eval Operator Now Display Properly" on page 35
- "OCTCR33I561004 — Completed Runs of a Scheduled Search Containing the Rename Operator No Longer Return 0 Results" on page 35
- " OCTCR33I566020 – Search Histogram: The Histogram's Current Zoom and Pan State is Now Maintained if Users Switch Tabs" on page 36
- "OCTCR33I566082 — Scheduled Searches: Resolved Issues Related to Switching the Field "Search Expires in" in User Preferences" on page 36
- "OCTCR33I566223 — The Number of Results Column Now Reflects the Correct value for Scheduled Searches" on page 36
- "OCTCR33I576083 — Outlier Detection: Outlier History Displays Correctly When No Score Exists" on page 36
- "OCTCR33I576112 — Outlier Detection: Addressed Issue About Multiple Outlier Model Scoring at the Same Time" on page 37
- "OCTCR33I585053 — Can Now Add a Field from Event Inspector to Active Search Even if the Field is Not Available in the Fieldset" on page 37
- "OCTCR33I587006 – Search No Longer Fails When the "where condition" Operator has any <...> and Contains a Filter for Field Groups" on page 37
- "OCTCR33I615024 — Search Queries Now Show Correct Results When Filtering With the "Id" Field" on page 37

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.

OCTCR33I339016 — Dashboard Creation: Setting a Cell Size in the Table Does Now Works in a SaaS Environment

Previously, 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. After a code change, settings for table cell sizes now work in a SaaS environment.

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 the 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.

OCTCR33I615024 — Search Queries Now Show Correct Results When Filtering With the "Id" Field

After a software fix, queries that filter on specific "id" field values (for example, id = "123456789" or id != "123456789") now return correct results.

Issues Related to SOAR

- "OCTCR33I600192 — CyberRes Galaxy Plugin should ignore availability check errors after the initial setup" on the next page

OCTCR33I600192 — CyberRes Galaxy Plugin should ignore availability check errors after the initial setup

CyberRes Galaxy plugin now correctly ignores the availability check errors after initial setup.

OCTCR33I604014 — Deleting the First Column in List Does Not Work as Expected

The issue where deleting the first column in List did not work properly has been resolved.

OCTCR33I491060 — All Integrations and Status Filter Function Problem in Enrichment History

After a software update, if we select an integration from all integration dropdown, it displays the related data.

OCTCR33I606049 — FTP Action Plugin Fails on Action Rollback if Filename on FTP has been Filled

A code fix has resolved this issue.

OCTCR33I598089 — McAfee NSP Integration Blacklist MD5 Hash Action Failed for 10.1.7.40 version

A code fix has resolved this issue.

OCTCR33I605011 — Cannot Fetch MITRE Attacks when Proxy is set and ignoreSSL is checked

Now when proxy is set and ignoreSSL is checked you can fetch MITRE attacks.

OCTCR33I580005 — Multiple Authentication Failure Workflow Template Customization Field is not Saving Properly

Now you can save the multiple authentication failure workflow template customization field.

OCTCR33I593012 — Playbook Editor Dropdown Save Button should be blocked for Empty Parameters

A software update now prevents you from saving the playbook editor dropdown when the parameter is empty.

OCTCR33I605120 — SMTP — Send Email To Scope Item Recipients Capability Adds Duplicated Customization Parameters

A code fix has resolved this issue

OCTCR33I597052 — SOAR Case Load Widget shows Wrong Severity in Possibly Delayed Column

A code fix has now resolved this issue.

OCTCR33I597147 — SOAR — CyberRes Galaxy Enrichment Capabilities fetches Unnecessarily Huge Data

Now SOAR CyberRes Galaxy enrichment capabilities fetches only the required data.

OCTCR33I592041 — SOAR Widgets — Mean Time and Mean Response Selection are not displayed

Now you can view Mean Time and Mean Response in SOAR Widgets.

OCTCR33I603059 — Update SOAR Productivity Widget Number of Groups Criteria

SOAR Productivity widget **Number of Groups** criteria has now been changed to **Most Productive Number of Groups**.

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!