Micro Focus Security ArcSight ArcSight SIEM as a Service

23.6.1

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

What's New 7

Improves the SOAR Capability 7

SOAR Fusion Role and Permissions 8

Import/Export of SOAR Triggers 8

New Integration Plugins for SOAR 8

Event Integrity Check Now Supports MD5 and SHA-1 Algorithms 8

Dashboards for the Built-in Foundation Security Content 9

Technical Requirements 9

Downloading and Installing the Data Ingestion Components 10

Known Issues 10

Issues Related to Fusion User Management 10

OCTCR33I326061 — When Selecting Manage Credentials, Advanced Authentication Services Requires You to Log Out 11

OCTCR33I336023 — Operations Performed on an Open Admin Tab Do Not Complete After You Log Out From Another Capability (Recon or Reporting) Tab 11

Issues Related to Reporting 11

OCTCR33I134098 — Edit Wizard Preview is Unavailable 12

OCTCR33I186007 — An Exported Report Might Have Format Issues 12

OCTCR33I331194 — Reports and Dashboards Use UTC Time Zone 12

OCTCR33I409268 — HTTP STATUS 500 Error When Clicking the Portal 12

OCTCR33I466062 — Report Queries All Events if You Do Not Specify Values for Start and End Times 12

OCTCR33I589121 — Brush Option Does Not Highlight Parabox Charts 13

Issues Related to Search 13

OCTCR33I676036 - Search Fails to Add a Field Specified in an Eval Operator 13

OCTCR33I179782 — Scheduled Search Appends Erroneous Values to the Run Interval 14

OCTCR33I549094 — Intermittent Failure of .csv File Containing Scheduled Search Results 14

OCTCR33I608098 — Certain top/bottom Queries Refresh When the User Presses the Space Bar While Entering the Query 14

OCTCR33I610161 — Incorrect Search Results Occur When Filtering With a Specific "Id" Field 15

OCTCR33I616090 — For System Search Queries, #SSH Authentication Throws an Error 15

Issues Related to SOAR 15
OCTCR33I567003 - SOAR Case Timeline Widget Displays No Data 16
OCTCR33I567004 - Using Multiple SOAR Timeline Widgets Causes Incorrect Data to Display 16
OCTCR33I657003 - Proxy Option Missing in Microsoft Exchange EWS Integration Configuration 16
OCTCR33I660018 - SaaS - Detect is Added as an Alert Source in SOAR without Detect Deployment 17
OCTCR33I705007 - Process Queues Do Not Show Data/Empty Columns 17
OCTCR33I192790 - Workflow OR Condition Does Not Work When Used with "Alert source = Internal" 17
OCTCR33I711107 - SOAR Case Links in Inetsoft Reports Do Not Redirect to the Correct Case 17
OCTCR33I698088 - Additional Real Time Detection Alert Sources Cause Event Consumption Issues 17
OCTCR33I722021 - Respond Option Redirects Users with No SOAR Permissions 18
Issues related to Real-time Threat Detection 18
OCTCR33I703013 - Session Timeout Results in an Error During Login 20
OCTCR33I685008 - Mismatch Between Console and Manager Causes an Error 20
OCTCR33I231646 – Some Resources are Unavailable After Uninstalling the Security Monitoring - Base Package 20
OCTCR33I233578 – Conditions Do Not Support Multiple Operators at the Parent Level 21
OCTCR33I233579 – Disabled Rule Continues to Fire 21
OCTCR33I235130 – Attributes in a Drill-Down Definition Not Visible When Using a Query Viewer 21
OCTCR33I370003 – Retrieving Rules Returns a Bad Request 21
OCTCR33I386094 – Services Do Not Recognize the jmx.rmi.enabled Property Value 22
OCTCR33I386148 – Columns in Audit Event Channels Incorrectly Refer to Event Broker 22
OCTCR33I579036 – Send Email Notification to Email Option Does Not Work 22
OCTCR33I585013 – SaaS Login Screen for ACC from Fusion Should not Display Even if the Persistor is Busy or if a Persistor is Down 22
OCTCR33I591010 – Extended Attribute on Installer File Causes Error on macOS 23
OCTCR33I616038 — Degradation of Event Ingestion 23
NGS-12407 – Annotation Flag Not Set When Forwarding Events 23
NGS-14041 – UPPER or LOWER Built-in String Functions Return Incorrect Results in Russian Locale 23
NGS-14477 – System Does Not Immediately Recognize Increase in Space 24

NGS-19880 – Maximizing Console on Linux Might Cause Mouse to Not Respond Properly 24
NGS-21831 – InSubnet Condition Strictly Enforces Wildcard Asterisk 24
NGS-21986 – JavaScript Unresponsive Error Occurs When Viewing the Last N Events Data Monitor 24
NGS-22568 – LengthOf Function Might Display Incorrect Values in Traditional Chinese Environment 25
NGS-22583 – Creating a Drilldown Based on an Active Channel Results in Display Errors 25
NGS-22600 – Top Value Count Dashboard is Missing Some Values in Traditional Chinese Environment 25
NGS-22659 – Exiting or Closing Console in Dark Theme Results in Prompt to Save Changes Even If You Made No Changes 25
NGS-22669 – Payload Information Cannot be Retrieved 26
NGS-22991 – Display Hangs When Viewing a Data Monitor in Tile Format in Simplified and Traditional Chinese Environments 26
NGS-23214 – ArcSight Console Might Not Run Properly If Properties File Contains Encrypted and Unencrypted Entries 26
NGS-23437 – Dashboard Background Image Does Not Carry Over from Console to Command Center 26
NGS-23444 – Dark Theme Renders Some Onscreen Instructions Illegible 27
NGS-23489 – Multiple Consoles on Same Linux Machine Causes Upgrade to Fail 27
NGS-24957 – GetSessionData Function Might Display an Incorrect Result 27
NGS-26357 – Charts Might Appear Small in ArcSight Command Center 27
NGS-26380 – Override Status and Remove Entry Options Do Not Work Correctly 28
NGS-26720 – Generated Correlation Events Display the Wrong URI 28
NGS-26915 – Analyze Channel Option Might be Disabled 28
NGS-27091 – Issue With Drill Down From Stacked Bar Charts 28
NGS-29487 – Issue with Font Rendering on Windows and Linux Operating Systems 29
NGS-32858 – MITRE Activity Dashboard Might be Blank 29
Resolved Issues 29
Issues Related to Reporting 29
OCTCR33I161014 — Dashboard Wizard No Longer Fails to Load All Data 30
Issues Related to Search 30
OCTCR33I576073 — Switching Tabs While Saving Searches No Longer Causes an Error 30
OCTCR33I619035 — Fieldset and Time Stamp Selections are Now Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass 30

OCTCR33I643057 — When You Are Viewing Raw Events in the Search Results Table, The Scrolling Action No Longer Becomes Stuck 31
OCTCR33I615073 — Query No Longer Exceeds Database Limits When a Long Operator Chain is Used With the "All Fields" Fieldset 31
OCTCR33I619045 — The Database Installer Now Limits the Maximum Query Size for the Available Memory 31
Issues Related to SOAR 31
OCTCR33I638001 — SOAR Allows to Execute Quarantine Computer Action Capability with Empty /Null Parameters 32
OCTCR33I605095 FTP Action plugin fails on action rollback if the remote.file.filename.appenduuid=true 32
OCTCR33I620081 Exchange EWS Integration - OAuth2 should be the default authentication method 32
OCTCR33I658007 Real Time Detection Pretty Printer is missing 32
OCTCR33I693038 Submitter is shown as Null for Detect Base Event enrichment in enrichment history 32
OCTCR33I697019 - SOAR Real-time Threat Detection Base Event Enrichment Might Fail 32
Contacting Micro Focus 33
Publication Status 33
Send Documentation Feedback 34

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 9
- "Downloading and Installing the Data Ingestion Components" on page 10
- "Known Issues" on page 10
- "Resolved Issues" on page 29
- "Contacting Micro Focus" on page 33

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.

Improves the SOAR Capability

This release provides the following enhancements to the SOAR capability:

- SOAR Fusion Role and Permissions
- Import/Export of SOAR Triggers
- "New Integration Plugins for SOAR " below

SOAR Fusion Role and Permissions

With this release, SOAR role and permissions have been integrated into Fusion. This enables simplifying SOAR user permissions so that it can be more manageable and easily mapped to user-personas.

Import/Export of SOAR Triggers

With this release, users will be able to import/export a trigger which is similar to playbook import/export feature.

New Integration Plugins for SOAR

New Integration Plugins:

- **BMC Helix ITSM Integration**

  This integration plugin has the following action and enrichment capabilities: Create Incident, Update Incident, Get an Incident, Close Incident, Add Work Note to Incident.
- **Cisco Umbrella Integration**

  This integration plugin has the following action and enrichment capabilities: Get Domain Status, Get Security Score Information, Get Risk Score, Get WHOIS Domain, Get Related Domain, Get Co-occurrences, Get Passive DNS Record.
- **Microsoft Teams Integration**

  This integration plugin has the following action and enrichment capabilities: List Teams, List Channels, Create Team, Create Channel, List Team Members, Add Team Member, Delete Member, Send Message, Retrieve Message, Archive Team, Unarchive Team.

Event Integrity Check Now Supports MD5 and SHA-1 Algorithms

To run Event Integrity Checks on raw events, you can configure a SmartConnector to use the MD5, SHA-1, or SHA-256 algorithms. Previously, you had to use the SHA-256 algorithm.

The Event Integrity Check validates that the event information in your database matches the content sent from the SmartConnectors. For more information about running an Event

Integrity Check, see the Help. You must have the Log Management and Compliance service to use this feature.

Dashboards for the Built-in Foundation Security Content

This release includes three new and one improved dashboards under Foundation content to help you monitor security issues.

- **Vulnerability Overview**

  Updated with new charts and widgets to better display vulnerabilities affecting your environment.
- **User Profile Overview**

  Displays information about a specific user's actions in your environment. This is a drill-down dashboard that can be opened with a specific user from another dashboard, table, bar, chart, or entered in the dashboard search bar. The dashboard requires a valid user to show information.
- **SSH Attacks Activity Overview**

  Displays a overview of SSH protocol usage so that you can monitor threats and see vulnerabilities in your environment.
- **Web Application Attacks**

  Displays information from web-based attacks on your environment.

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
- Issues Related to Reporting
- Issues Related to Search
- Issues Related to SOAR
- 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" on the next page
- "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" on the next page
- "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.

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

- OCTCR33I676036 - Search Fails to Add a Field Specified in an Eval Operator
- "OCTCR33I179782 — Scheduled Search Appends Erroneous Values to the Run Interval" on the next page
- "OCTCR33I549094 — Intermittent Failure of .csv File Containing Scheduled Search Results" 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 15
- "OCTCR33I616090 — For System Search Queries, #SSH Authentication Throws an Error" on page 15

OCTCR33I676036 - Search Fails to Add a Field Specified in an Eval Operator

Issue: If you run a search, then add an eval operator to the query to filter the results, it's possible that Search fails to add the field specified in the operator phrase to the results table. For example, you ran the query `Device Event Class ID = FAILED`. Then you want to change the device vendor field to upper case, naming the new field Vendor. So you add `|` *`eval Vendor = upper (Device Vendor)`* to the query. You click Search, and the system executes the modified query. However, the results table fails to include the Vendor field as requested.

Workaround: If this issue occurs, open a new Search tab and then copy the query, including the eval phrase, to the new tab. Run the search.

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.

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.

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.

OCTCR33I616090 — For System Search Queries, #SSH Authentication Throws an Error

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

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

Issues Related to SOAR

- "OCTCR33I567003 - SOAR Case Timeline Widget Displays No Data" on the next page
- "OCTCR33I567004 - Using Multiple SOAR Timeline Widgets Causes Incorrect Data to Display" on the next page
- "OCTCR33I657003 - Proxy Option Missing in Microsoft Exchange EWS Integration Configuration" on the next page
- "OCTCR33I660018 - SaaS - Detect is Added as an Alert Source in SOAR without Detect Deployment" on page 17

- "OCTCR33I705007 - Process Queues Do Not Show Data/Empty Columns" on the next page
- "OCTCR33I192790 - Workflow OR Condition Does Not Work When Used with "Alert source = Internal"" on the next page
- "OCTCR33I711107 - SOAR Case Links in Inetsoft Reports Do Not Redirect to the Correct Case" on the next page
- "OCTCR33I698088 - Additional Real Time Detection Alert Sources Cause Event Consumption Issues" on the next page
- "OCTCR33I722021 - Respond Option Redirects Users with No SOAR Permissions" on page 18

OCTCR33I567003 - SOAR Case Timeline Widget Displays No Data

Issue: Even if data is present for the selected time range, the SOAR case timeline widget displays no data.

Workaround: There is no workaround at this time.

OCTCR33I567004 - Using Multiple SOAR Timeline Widgets Causes Incorrect Data to Display

Issue: If multiple SOAR timeline widgets are present on a dashboard, the data is displayed for only one widget. For example, if the selected time range is between September 17 and 20, the displayed data might be for September 2.

Workaround: There is no workaround at this time.

OCTCR33I657003 - Proxy Option Missing in Microsoft Exchange EWS Integration Configuration

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

Workaround: There is no workaround at this time.

OCTCR33I660018 - SaaS - Detect is Added as an Alert Source in SOAR without Detect Deployment

Issue: Detect is added automatically as an alert source in SOAR without Detect being deployed.

Workaround: There is no workaround at this time.

OCTCR33I705007 - Process Queues Do Not Show Data/Empty Columns

Issue: Process queues do not display data as expected.

Workaround: There is no workaround at this time.

OCTCR33I192790 - Workflow OR Condition Does Not Work When Used with "Alert source = Internal"

Issue: When you create an incident with an internal alert source ("Alert source = Internal"), the OR condition does not evaluate correctly.

Workaround: There is no workaround at this time.

OCTCR33I711107 - SOAR Case Links in Inetsoft Reports Do Not Redirect to the Correct Case

Issue: Links to cases in Inetsoft reports do not redirect to the correct URL. The case URL resets, choosing the case at the top of the list. This occurs with both System Admin and minimum permission roles.

Workaround: There is no workaround at this time.

OCTCR33I698088 - Additional Real Time Detection Alert Sources Cause Event Consumption Issues

Issue: Multiple Real Time Detection Alert Sources cause event consumption issues. If one already exists, SOAR allows a new one to be created instead of declining it.

Workaround: There is no workaround at this time.

OCTCR33I722021 - Respond Option Redirects Users with No SOAR Permissions

Issue: If you have no SOAR permissions and click **Respond** in the navigation pane, you will be taken to the /mgmt/my-profile/account page.

Workaround: There is no workaround at this time.

Issues related to Real-time Threat Detection

- "OCTCR33I703013 - Session Timeout Results in an Error During Login" on page 20
- "OCTCR33I685008 - Mismatch Between Console and Manager Causes an Error" on page 20
- "OCTCR33I231646 – Some Resources are Unavailable After Uninstalling the Security Monitoring - Base Package" on page 20
- "OCTCR33I233578 – Conditions Do Not Support Multiple Operators at the Parent Level" on page 21
- "OCTCR33I233579 – Disabled Rule Continues to Fire" on page 21
- "OCTCR33I235130 – Attributes in a Drill-Down Definition Not Visible When Using a Query Viewer" on page 21
- "OCTCR33I370003 – Retrieving Rules Returns a Bad Request" on page 21
- "OCTCR33I386094 – Services Do Not Recognize the jmx.rmi.enabled Property Value" on page 22
- "OCTCR33I386148 – Columns in Audit Event Channels Incorrectly Refer to Event Broker" on page 22
- "OCTCR33I579036 – Send Email Notification to Email Option Does Not Work" on page 22
- "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 22
- "OCTCR33I591010 – Extended Attribute on Installer File Causes Error on macOS" on page 23
- "OCTCR33I616038 — Degradation of Event Ingestion" on page 23
- "NGS-12407 – Annotation Flag Not Set When Forwarding Events" on page 23
- "NGS-14041 – UPPER or LOWER Built-in String Functions Return Incorrect Results in Russian Locale" on page 23
- "NGS-14477 – System Does Not Immediately Recognize Increase in Space" on page 24

- "NGS-19880 – Maximizing Console on Linux Might Cause Mouse to Not Respond Properly" on page 24
- "NGS-21831 – InSubnet Condition Strictly Enforces Wildcard Asterisk" on page 24
- "NGS-21986 – JavaScript Unresponsive Error Occurs When Viewing the Last N Events Data Monitor" on page 24
- "NGS-22568 – LengthOf Function Might Display Incorrect Values in Traditional Chinese Environment" on page 25
- "NGS-22583 – Creating a Drilldown Based on an Active Channel Results in Display Errors" on page 25
- "NGS-22600 – Top Value Count Dashboard is Missing Some Values in Traditional Chinese Environment" on page 25
- "NGS-22659 – Exiting or Closing Console in Dark Theme Results in Prompt to Save Changes Even If You Made No Changes" on page 25
- "NGS-22669 – Payload Information Cannot be Retrieved" on page 26
- "NGS-22991 – Display Hangs When Viewing a Data Monitor in Tile Format in Simplified and Traditional Chinese Environments" on page 26
- "NGS-23214 – ArcSight Console Might Not Run Properly If Properties File Contains Encrypted and Unencrypted Entries" on page 26
- "NGS-23437 – Dashboard Background Image Does Not Carry Over from Console to Command Center" on page 26
- "NGS-23444 – Dark Theme Renders Some Onscreen Instructions Illegible" on page 27
- "NGS-23489 – Multiple Consoles on Same Linux Machine Causes Upgrade to Fail" on page 27
- "NGS-24957 – GetSessionData Function Might Display an Incorrect Result" on page 27
- "NGS-26357 – Charts Might Appear Small in ArcSight Command Center" on page 27
- "NGS-26380 – Override Status and Remove Entry Options Do Not Work Correctly" on page 28
- "NGS-26720 – Generated Correlation Events Display the Wrong URI" on page 28
- "NGS-26915 – Analyze Channel Option Might be Disabled" on page 28
- "NGS-27091 – Issue With Drill Down From Stacked Bar Charts" on page 28
- "NGS-29487 – Issue with Font Rendering on Windows and Linux Operating Systems" on page 29
- "NGS-32858 – MITRE Activity Dashboard Might be Blank" on page 29

OCTCR33I703013 - Session Timeout Results in an Error During Login

Issue: If your session has timed out and you attempt to log in, the following error occurs: `Manager license not valid`.

Workaround: Start the Console with the following command:

```
<CONSOLE_HOME>/bin/arcsight console -m <tenantname>
```

OCTCR33I685008 - Mismatch Between Console and Manager Causes an Error

Issue: When you start the Console, if the Console version does not match the Manager version, you might receive one of the following error messages:

- `Failed to authenticate user via OSP`
- `Not setup for OSP. Run 'managersetup'`

Workaround: To fix the error, download and install the matching Console version from the Console download bucket location specified in your welcome email. For example: `<account>-<region>-detect-console-download-bucket`.

To verify the version required by the Manager:

1. Log in to the Fusion Dashboard.
2. Navigate to DETECT > Command Center.
3. Click Help > About.
4. Note the version number listed for Command Center, such as 8.0.1.2777.0.

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 Reporting" below
- "Issues Related to Search" on the next page
- "Issues Related to SOAR" on page 31

Issues Related to Reporting

- "OCTCR33I161014 — Dashboard Wizard No Longer Fails to Load All Data" on the next page

OCTCR33I161014 — Dashboard Wizard No Longer Fails to Load All Data

When using the Dashboard wizard, the chart no longer fails to load if the same type of data has been selected at the same time.

Issues Related to Search

- "OCTCR33I576073 — Switching Tabs While Saving Searches No Longer Causes an Error" below
- "OCTCR33I619035 — Fieldset and Time Stamp Selections are Now Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass" below
- "OCTCR33I643057 — When You Are Viewing Raw Events in the Search Results Table, The Scrolling Action No Longer Becomes Stuck " on the next page
- "OCTCR33I615073 — Query No Longer Exceeds Database Limits When a Long Operator Chain is Used With the "All Fields" Fieldset" on the next page
- "OCTCR33I619045 — The Database Installer Now Limits the Maximum Query Size for the Available Memory" on the next page

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

Issue: After applying a code change, the application no longer throws an error ("Results do not match the specified search query") when you switch tabs while saving a search.

OCTCR33I619035 — Fieldset and Time Stamp Selections are Now Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass

Issue: A code fix now preserves search criteria fieldset and time stamp selections (such as "Max results" and "Session search expires") when you load them using the **Mange Search** Search icon (the magnifying glass) or type them into the Search field.

OCTCR33I643057 — When You Are Viewing Raw Events in the Search Results Table, The Scrolling Action No Longer Becomes Stuck

Issue: A code update resolved the issue of the scrolling action becoming stuck if you are performing infinite scrolling while viewing raw event data in the Search Results Table..

OCTCR33I615073 — Query No Longer Exceeds Database Limits When a Long Operator Chain is Used With the "All Fields" Fieldset

When you use a long operator chain with "All Fields" fieldset, the resulting query no longer exceeds the database limits and fail. **Field summary** no longer fails to open.

OCTCR33I619045 — The Database Installer Now Limits the Maximum Query Size for the Available Memory

When you use a long operator chain with the "All Fields" fieldset, the database installer now correctly limits the maximum query size. When you reach the query limit, searches will execute properly, but field summary load performance might be affected.

Issues Related to SOAR

- "OCTCR33I638001 — SOAR Allows to Execute Quarantine Computer Action Capability with Empty /Null Parameters" on the next page
- OCTCR33I605095 — FTP Action plugin is failing on action rollback if the remote.file.filename.appenduuid=true
- OCTCR33I620081 — Exchange EWS Integration - OAuth2 should be the default authentication method
- OCTCR33I658007 — Real Time Detection Pretty Printer is missing
- OCTCR33I693038 — Submitter is shown as Null for Detect Base Event enrichment in enrichment history
- OCTCR33I697019 - SOAR Real-time Threat Detection Base Event Enrichment Might Fail

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

SOAR no longer allows you 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

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

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

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

OCTCR33I658007 Real Time Detection Pretty Printer is missing

Real time Detection now displays the pretty printer content.

OCTCR33I693038 Submitter is shown as Null for Detect Base Event enrichment in enrichment history

In Enrichment history, the submitter for Real-time Threat Detection Base Events enrichment is shown as ArcSIght SOAR

OCTCR33I697019 - SOAR Real-time Threat Detection Base Event Enrichment Might Fail

SOAR Real-time Threat Detection base event enrichment used to fail if correlation events reached SOAR before they could be persisted in the database.

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

Publication Status

Released: July 14, 2023

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 23.6.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!