Micro Focus Security ArcSight ArcSight SIEM as a Service

23.8.1

ArcSight SIEM as a Service Release Notes

Legal Notices

Copyright Notice

Support

Contact Information

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

Contents

Release Notes for ArcSight SIEM as a Service

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. ArcSight SaaS is built on a base platform that provides a set of core services, including the Dashboard, Search, and user management.

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

For 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.

Dashboards for the Built-in Foundation Security Content

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

- **DGA Overview**

  Updated with new charts and widgets that identify domain generated algorithms.
- **IDS Events Overview**

  A new dashboard that identifies IDS events.
- **Reconnaissance Activity**

  Updated with new charts and widgets to identify reconnaissance activity.
- **Traffic Anomaly Overview**

  Updated with new charts and widgets to identify traffic anomalies.

Adds Support for Session Lists in Real-time Threat Detection Service

This release includes support for session lists in the Real-time Threat Detection service. **Session lists** allow you to track traffic with IP addresses of interest. While you can manually update session lists, their real value comes when you author automatic, rule-driven lists with dynamic content.

Introduces ArcMC 3.2.1 for the vCHA and Standalone

This release provides an upgrade for both ArcMC in the vCHA and for your standalone instance of ArcMC, along with instructions about updating either to ArcMC 3.2.1. It is recommended that you upgrade to ArcMC 3.2.1 to take advantage of the latest security fixes and resolved issues. However, ArcSight SaaS continues to be compatible with older versions of ArcMC.

- To update components of the vCHA, see "Upgrading the vCHA" and "Installing the Virtual CHA" in the *ArcSight SIEM as a Service - Quick Start for Administrators*.
- To upgrade a standalone instance of ArcMC, see "Upgrading ArcMC" in the *ArcSight SIEM as a Service - Quick Start for Administrators*. You can upgrade the standalone instance either locally or remotely.

For more information about the most recent updates, enhancements, known issues, and resolved software fixes in ArcMC, see the *Release Notes for ArcMC 3.2.1*.

Adds Support for SmartConnector 8.4.2

This release adds support for SmartConnector 8.4.2. If you are using a previous version of SmartConnector, we recommend that 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 8.4.2.

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" in 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

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

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

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.

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.

OCTCR33I692029 Search Criteria — Expired Max Results and Session Search Selections are Displayed When Loading Search Criteria

Issue: Expired maximum search results and session search selections are being incorrectly displayed when you load search criteria.

By default, search criteria are sorted alphabetically by name. Maximum search results and date fields (such as search expiration) are stored as part of the search criteria, as indicated by a message from the application. They are displayed in the Manage Search table, where you can visualize saved the search criteria.

Workaround: Use the folder icon to load search criteria. This will preserve the original search parameters, including field set and timestamp information.

Issues Related to SOAR

- "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 the next page
- "OCTCR33I705007 - Process Queues Do Not Show Data/Empty Columns" on the next page
- "OCTCR33I698088 - Additional Real Time Detection Alert Sources Cause Event Consumption Issues" on page 17
- "OCTR33I718001 - Respond Option Redirects Users with No SOAR Permissions" on page 17

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.

OCTR33I718001 - 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. This issue will be resolved in version 23.9.1.

Issues related to Real-time Threat Detection

OCTCR33I752015 – Logging Out of Command Center Does Not Terminate ArcSight Session

Issue: If you log in to ArcSight in the Admin role and open the Real-time Threat Detection Command Center, logging out of Command Center does not log you out of ArcSight.

Workaround: Manually log out on the ArcSight tab or close the tab.

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.

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: You can work around this issue by doing one of the following:

- Use curl to download the installer file.
- Run this command from a Terminal window:

  ```
  sudo xattr -dr com.apple.quarantine
  /path/to/ArcSightConsoleSaaS.app
  ```

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.

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 Search" on the next page
- "Issues Related to SOAR" on page 29
- "Issues Related to Real-time Threat Detection" on page 29

Issues Related to Search

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

A software fix resolved the problem where exporting the results of a Scheduled search from the Completed tab intermittently resulted in an empty .csv file.

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

A code update resolved the problem where if you switched tabs while saving a search, the system generated an error that stated "Results do not match the specified search query."

OCTCR33I594059 — URL Paths for Search Have Changed

Issue: Associated with the improvements for search capability, some URL paths have changed to use "/search" in the path. Previously, the URL paths used "/fusionSearch" instead. Users should be aware of this change when they are creating, opening, or updating searches and when they are working with URLs related to the Event Inspector.

Workaround: If you encounter the outdated path, manually change it to use "/search".

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

After a software fix, Search criteria fieldset and time stamp selections (such as "Max results" and "Session search expires") are again preserved when you load them using the **Mange Search** Search icon (the magnifying glass) or type them into the Search field.

OCTCR33I643057 — Scrolling No Longer Sticks When You View Raw Events in the Search Results Table

Prior to a code update, doing infinite scrolling while viewing raw event data in the Search Results Table might cause the scrolling to become stuck.

Issues Related to SOAR

Issues Related to Real-time Threat Detection

OCTCR33I703013 - Session Timeout No Longer Results in an Error During Login

Issue: A code change resolved an issue where attempting to log in when your session has timed out caused the following error: `Manager license not valid`.

OCTCR33I685008 - Mismatch Between Console and Manager No Longer Causes an Error

Issue: When you start the Console, if the Console version does not match the Manager version, you no longer receive one of the following error messages:

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

OCTCR33I579036 – Send Email Notification to Email Option Now Works Correctly

Issue: When you configure the Send Notification rule action in a SaaS environment, the "send email notification to email" option now works correctly.

OCTCR33I580041 – Unrecognized App Warning No Longer Occurs During Console Installation

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

OCTCR33I586008 – Import Users & Groups from ESM Option Has Been Hidden in a SaaS Environment

Issue: Previously, the Import Users & Groups from ESM functionality was not applicable in a SaaS environment, but the option was still visible in this release. This functionality is now hidden for SaaS environments.

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

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

Contacting Micro Focus

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

Additional technical information or advice is available from several sources:

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

Send Documentation Feedback

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

Feedback on ArcSight SIEM as a Service Release Notes (ArcSight SIEM as a Service 23.8.1)

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!