opentext™

ArcSight SIEM as a Service

Software Version: 23.9.1

ArcSight SIEM as a Service Release Notes

Document Release Date: September 2023
Software Release Date: September 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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.

This release includes the following services:

Service	Version
Log Management & Compliance	1.5.5
Real-time Threat Detection	8.1.0

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.

Documentation Changes

Renaming the User Guide for Fusion

In this release, we have renamed the User Guide for Fusion to User Guide for ArcSight Platform and ArcSight SIEM as a Service (ArcSight SaaS). This change reflects the fact that the guide provides concepts and use cases for many of the features in ArcSight Platform and ArcSight

SaaS, beyond just the common layer of services. This guide also provides context-sensitive help for most features when you are logged into the product.

The version of the guide now matches the release version instead a version associated with a particular deployed capability or service. For example, the current guide includes 23.9.1 for ArcSight SaaS.

For the Real-time Threat Detection Service

This release includes the following changes to the Real-time Threat Detection service:

- Introduces the Option to Run Real-time Searches
- Real-time Threat Detection Geographical Information Update
- Real-time Threat Detection Vulnerability Update

Introduces the Option to Run Real-time Searches

You have the flexibility to obtain search results based on a fixed date and time or to stream events in real time.

The new **real-time search** option constantly updates the results of your query, starting from a beginning range (such as the last 30 minutes). As long as there is data to satisfy the query, the data continues to build in the histogram and events table.

Real-time search requires the Real-time Threat Detection service in the ArcSight SaaS environment.

Real-time Threat Detection Geographical Information Update

This version of SIEM as a ServiceReal-time Threat Detection includes an update to the geographical information used in graphic displays. The version is GeoIP-532_2023089.

Real-time Threat Detection Vulnerability Updates

This release includes recent vulnerability mappings from the August 2023 Update:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3622 updated CVE
- McAfee Intrushield 11.10.8.1 updated CVE
- TippingPoint UnityOne DV9814 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE
- McAfee Group Shield Enterprise 7.0 updated CVE

Improves the SOAR Capability

This release provides the following enhancements to the SOAR capability:

- Context sensitive help
- SOAR action approval enhancements
- "New Integration Plugins for SOAR " below

Context sensitive help

With this release, a help button has been added.

SOAR action approval enhancements

With this release, SOAR will accept static email address for external approvers.

New Integration Plugins for SOAR

New Integration Plugins:

- **Amazon GuardDuty Integration**

  This integration plugin has the following action and enrichment capabilities: List Detectors, Get Detector Details, Create Trusted IP List, Delete Trusted IP List, List Trusted IP List, Get Trusted IP List Detail, Add to trusted IP List, Remove from trusted IP List, Create Threat Intel List, Delete Threat Intel List, List Threat Intel List, Get Threat Intel List Details, Add to Threat Intel List, Remove from Threat Intel List, List Findings, Get Finding Detail, Archive Finding, Unarchive Finding, Update Finding Feedback.

- **Netskope Integration**

  This integration plugin has the following action and enrichment capabilities: List Quarantined Files, Allow Quarantined File, Block Quarantined File.

- **SentinelOne Integration**

  This integration plugin has the following action and enrichment capabilities: Disconnect from Network: Connect to Network,Get Agent Status/ Get Endpoint Details, List Installed Applications, List Events for Endpoint, List Groups, Get Group Details, Get Hash Reputation, Move Agent to Group, Add to Blacklist, Delete from Blacklist, Get Blacklist, List Threats, Get Threat Details, Update Threat, Add to Exclusion List,Remove from Exclusion List, Scan (Full Disk Scan).

- **EnCase Endpoint Security**

This integration plugin has the following action and enrichment capabilities: List Investigations, Find Hosts with IOCs, Standard Agent Timeline (Snapshot), Collect Memory, Create Snapshot, Find Hosts with Items of Interest, Get Investigation Job Status, Get Event Status, Collect Data - Pre Defined Filter, Collect Data -Custom Filter, Isolate, Reconnect, Create Event, Remediate.

Revokes *Execute Search* Permission from Reports Permissions

This release revokes the *Execute Search* permission from the Reports permissions:

- *Report Admin*
- *Design Reports*
- *Schedule Reports*
- *View Reports*

If you have created roles that include these Reports permissions and those roles also need to run searches, you should add the *Execute Search* permission to the roles.

For more information about assigning and available permissions, see Assigning Permissions to Roles in the Help.

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. OpenText 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 OpenText determines the root cause is the untested platform or configuration. According to the standard defect-handling policies, OpenText 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. OpenText strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit OpenText Support for Micro Focus products, then select the appropriate product category.

All issues listed in this section belong to the OCTCR33I repository, unless otherwise noted.

- "Issues Related to the Base Platform Service" below
- "Issues Related to User Management" on the next page
- Issues Related to Reporting
- Issues Related to Search
- Issues Related to SOAR
- Issues Related to Real-time Threat Detection

Issues Related to the Base Platform Service

750053 — Import Logger Status Does not Update Correctly

Issue: The status does not update properly when a user tries to import Logger Archives. After the migration initiates, the status changes to "Pending Import," but it remains in that state until the migration has completed. Additionally, the status does not update and remains in the "Not Started" state when you try to import metadata.

Workaround: Refresh the page.

Issues Related to User Management

- "326061 — When Selecting Manage Credentials, Advanced Authentication Services Requires You to Log Out" below
- "336023 — Operations Performed on an Open Admin Tab Do Not Complete After You Log Out From Another Capability (Recon or Reporting) Tab" below

326061 — 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, the service will allow you to enter your credentials to log in.

336023 — 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

- "186007 — An Exported Report Might Have Format Issues" below
- "331194 — Reports and Dashboards Use UTC Time Zone" below
- "409268 — HTTP STATUS 500 Error When Clicking the Portal" below
- "466062 — Report Queries All Events if You Do Not Specify Values for Start and End Times" on the next page
- "589121 — Brush Option Does Not Highlight Parabox Charts" on the next page
- "773027 — Cannot Specify Time Ranges for Custom Reports and Dashboards Because the Enter Parameters Modal is not Displayed" on the next page
- "779004 — VPM Conditions/Triggers are not Being Applied for Scheduled Dashboards" on the next page

186007 — 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.

331194 — 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.

409268 — 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.

466062 — 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.

589121 — Brush Option Does Not Highlight Parabox Charts

Issue: The brush option does not highlight parabox charts.

Workaround: There is no workaround for this issue.

773027 — Cannot Specify Time Ranges for Custom Reports and Dashboards Because the Enter Parameters Modal is not Displayed

Issue: If a custom report is **not** based on one of the OpenText Standard Content "Data Worksheets", then the user will not be prompted for a date range and the default date range will always be used.

Workaround: Add/implement your own Date Range prompt to your custom reports.

779004 — VPM Conditions/Triggers are not Being Applied for Scheduled Dashboards

Issue: For Virtual Private Models (VPM), Scheduled "Dashboards" will not return any data.

Workaround: Run the "Dashboard" through the reporting web portal instead.

Issues Related to Search

179782 — 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 selected hours and minutes, specify specific hours from the option **Specific Hour** and minutes from the **Starting From** setting.

608098 — 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 list of auto-suggested options that are displayed as you enter the query. This applies to any field the user is not able to type in.

616090 — 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.

676036 - 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.

692029 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.

733209 — Scheduled Searches: An Error Indicating You Cannot Retrieve Fields Displays When You Try to Load a Field Summary on a Completed Run

Issue: For scheduled searches, when you try to load a field summary on completed runs that contain aggregation operators, the following error is displayed: "Cannot retrieve the summary number of events per field. Please reload the search." and field summary dialog box closes itself.

Workaround: There is no workaround for this issue. The error prevents user from properly loading field summary on a completed run from scheduled searches.

For non-aggregation operators, the error is displayed, but field summary dialog box does not close.

757008 — Incorrect Number is Shown for Amount of Results When Saving Real-time Search Results

Issue: After saving the search results of a Real-time Search, an issue causes an incorrect number to be shown for the amount of results in the Manage Search > Search Results page.

Workaround: The problem is only on the Search Results page. If you click on the saved Search Results to open them in a new tab, you will see the correct results amount on the Search tab. After that, if you reload / refresh the Search Results page, the latest data will be retrieved, and the correct amount of search results will be shown.

766026 — User Preferences Drop-down Menus are Closed if You Click in the Scrollbar

Issue: The user preferences drop-down menus closes if the user clicks in scrollbar. This issue only affects the preferences page.

Workaround: You can scroll down using mouse wheel or by using the keyboard.

Issues Related to SOAR

- "719017 – Proxy Option Missing in SMTP Mail Server Integration Configuration" below
- "735021 – Clickable Items Should Have Clickable Cursor Icon" below
- "769041 – Source Column Is Empty for Detect Events" on the next page
- "775003 – For Analyst User, Configuration is Navigating to Cases Page when Clicked from Respond->Cases->Configuration " on the next page
- "776014 — SOAR shows Page unresponsive error when clicked from Reports > SOAR > Open Cases" on the next page

719017 – Proxy Option Missing in SMTP Mail Server Integration Configuration

Issue: When configuring SMTP Mail Server integration, the proxy option is missing from the configuration settings.

Workaround: There is no workaround at this time.

735021 – Clickable Items Should Have Clickable Cursor Icon

Issue: Clickable items do not display the clickable cursor icon.

Workaround: There is no workaround at this time.

769041 – Source Column Is Empty for Detect Events

Issue: Source column is empty from alerts that are received for Detect.

Workaround: There is no workaround at this time.

775003 – For Analyst User, Configuration is Navigating to Cases Page when Clicked from Respond->Cases->Configuration

Issue: For analyst user left navigation in SOAR - Configuration page is navigating to cases page when clicked from Respond->Cases->Configuration.

Workaround: Click Dashboard -> Respond -> Configuration to view Configuration page.

776014 — SOAR shows Page unresponsive error when clicked from Reports > SOAR > Open Cases

Issue: SOAR UI shows "Page unresponsive" error when clicked from Reports > SOAR > Open Cases if there are more than 80,000 cases.

Workaround: There is no workaround at this time.

Issues related to Real-time Threat Detection

- "231646 – Some Resources are Unavailable After Uninstalling the Security Monitoring - Base Package" on page 22
- "233578 – Conditions Do Not Support Multiple Operators at the Parent Level" on page 22
- "233579 – Disabled Rule Continues to Fire" on page 22
- "235130 – Attributes in a Drill-Down Definition Not Visible When Using a Query Viewer" on page 22
- "370003 – Retrieving Rules Returns a Bad Request" on page 23
- "585013 – SaaS Login Screen for ACC from Fusion Should not Display Even if the Persistor is Busy or if a Persistor is Down" on page 23
- "591010 – Extended Attribute on Installer File Causes Error on macOS" on page 23

- "NGS-29487 – Issue with Font Rendering on Windows and Linux Operating Systems" on page 29

231646 – 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.

233578 – 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.

233579 – 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.

235130 – 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.

370003 – 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.

585013 – 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.

591010 – 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
  ```

752015 – 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.

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-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.

All issues listed in this section belong to the OCTCR33I repository, unless otherwise noted.

- "Issues Related to Search" below
- "Issues Related to SOAR" on page 31
- "Issues Related to Real-time Threat Detection" on page 33

Issues Related to Search

- "549094 — Intermittent Failure of .csv File Containing Scheduled Search Results Has Been Fixed" on the next page
- "576073 — Switching Tabs While Saving Searches No Longer Causes an Error" on the next page
- "619035 — Fieldset and Time Stamp Selections are now Preserved When Loading Search Criteria Using the Manage Search > Magnifying Glass" on the next page
- "643057 — Scrolling No Longer Sticks When You View Raw Events in the Search Results Table" on the next page

- "733144 — Search Results Now Clean Up Properly When Executing Different "Pipe" Queries Using the Same Tab" on the next page

549094 — 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.

576073 — 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."

619035 — 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.

643057 — 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.

733144 — Search Results Now Clean Up Properly When Executing Different "Pipe" Queries Using the Same Tab

Previously, in a SaaS environment, when you searched using different "pipe" operator queries in the same Search tab, the search results did not completely clean up previous searches. This was especially true when you ran an aggregation search and then ran a non-aggregation search. A software fix has resolved this issue.

Issues Related to SOAR

- "192790 - Workflow OR Condition Does Not Work When Used with "Alert source = Internal"" below
- "567003 - SOAR Case Timeline Widget Displays No Data" below
- "567004 - Using Multiple SOAR Timeline Widgets Causes Incorrect Data to Display" on the next page
- "643164 - SOAR Approval List on Cases Page should display as offline data" on the next page
- "698088 - Additional Real Time Detection Alert Sources Cause Event Consumption Issues" on the next page
- "705007 - Process Queues Do Not Show Data/Empty Columns" on the next page
- "711107 - SOAR Case Links in Inetsoft Reports Do Not Redirect to the Correct Case" on the next page
- "718001 - RESPOND Left Menu Item Should Be Hidden If The User Does Not Have SOAR Permission" on the next page
- "722038 - SOAR_WebUI: WebUI keeps timing out too early and the Re-login pop-up appears repeatedly" on page 33
- "732005 - Multiple SOAR Case Status Widget Do Not Show Right Data" on page 33
- "734065 - Access Denied Error Appears When Adding/Removing Watcher using the Star Icon" on page 33
- "734078 - Fixing soar-jython for unsupported libraries" on page 33
- "735062 - SOAR ESM Case Creation Should Not Be Stopped Even if There Are Invalid Scope Items" on page 33

192790 - Workflow OR Condition Does Not Work When Used with "Alert source = Internal"

Issue: A code fix now allows you to create an incident with an internal alert source ("Alert source = Internal").

567003 - SOAR Case Timeline Widget Displays No Data

Issue: A code fix has now resolved this issue where SOAR Case Tamerlane Widget displayed no data

567004 - Using Multiple SOAR Timeline Widgets Causes Incorrect Data to Display

Issue: A code fix has now resolved this issue where SOAR Timeline Widget displayed incorrect data

643164 - SOAR Approval List on Cases Page should display as offline data

Issue: A code fix has now resolved the issue where SOAR Approval list displayed long data.

698088 - Additional Real Time Detection Alert Sources Cause Event Consumption Issues

Issue: A code fix has now resolved the issue where multiple Real Time Detection Alert Sources cause event consumption issues.

705007 - Process Queues Do Not Show Data/Empty Columns

Issue: Now process queues display data as expected.

711107 - SOAR Case Links in Inetsoft Reports Do Not Redirect to the Correct Case

Issue: A code fix has now resolved the issue when you click SOAR Case Links it used to redirect to incorrect data.

718001 - RESPOND Left Menu Item Should Be Hidden If The User Does Not Have SOAR Permission

Issue: A code fix has now resolved the issue where RESPOND left menu was not hidden if user did not have SOAR Permission.

722038 - SOAR_WebUI: WebUI keeps timing out too early and the Re-login pop-up appears repeatedly

Issue: A code fix has now resolved the issue where the WebUI used to time out too early and the logging pop-up appeared repeatedly.

732005 - Multiple SOAR Case Status Widget Do Not Show Right Data

Issue: A code fix has now resolved the issue where SOAR Case Status widget displayed incorrect data.

734065 - Access Denied Error Appears When Adding/Removing Watcher using the Star Icon

Issue: A code fix has now resolved the issue where access was denied while adding/removing watcher using the star icon.

734078 - Fixing soar-jython for unsupported libraries

Issue: A code fix has now resolved the issue where soar-jython is fixed for unsupported libraries.

735062 - SOAR ESM Case Creation Should Not Be Stopped Even if There Are Invalid Scope Items

Issue: A code fix has now resolved the issue where SOAR ESM Case creation was stopped when there were invalid scope items.

Issues Related to Real-time Threat Detection

- "579036 – Send Email Notification to Email Option Now Works Correctly" on the next page
- "580041 – Unrecognized App Warning No Longer Occurs During Console Installation" on the next page
- "586008 – Import Users & Groups from ESM Option Has Been Hidden in a SaaS Environment" below
- "613001 — Login to ACC Using OSP is No Longer Case Sensitive" below
- "616038 — Degradation of Event Ingestion" on the next page
- "685008 - Mismatch Between Console and Manager No Longer Causes an Error" on the next page
- "703013 - Session Timeout No Longer Results in an Error During Login" on the next page

579036 – 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.

580041 – 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**.

586008 – 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.

613001 — 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.

616038 — Degradation of Event Ingestion

Real-time Threat Detection is scaled to an EPS limit. Previously, sending EPS above the deployed limit for extended periods of time might result in degradation of event ingestion into MSK. This issue has been resolved.

685008 - 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'`

703013 - 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`.

Contacting OpenText

For specific product issues, contact OpenText SaaS Customer Success Support team or email us at Documentation-Feedback@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
- OpenText Community pages for Micro Focus products

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 (SIEM as a Service 23.9.1)

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!