Micro Focus Security ArcSight Investigate

Software Version: 3.1.0

Release Notes

Document Release Date: April, 2020
Software Release Date: April, 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Supported Platforms and Browsers

For details on browser support, refer to the Investigate Deployment Guide.

What's New in this Release

- New search functions:
  - EVAL: Calculates an expression provided by the user as part of a search. Several mathematical and logical functions are provided as part of this feature allowing users to create complex expressions using data returned from search.
  - RENAME: Allows renaming of fields returned from search.
- Data Quality Dashboard: Displays detailed information about the gap between an event's Device Receipt Time at the SmartConnector and Persist Time within Investigate. The dashboard helps to identify log sources that have wide variances between the two timestamps so that time at source can be corrected.
- Single Sign On: Allows users to log in with a single ID and password. This feature is shared across ArcSight containerized applications.

Fixed Issues

This release addresses the following issues:

Issue	Description
HERC-9016	This release resolves an issue where admin users were unable to create another user with the same admin role.
HERC-9015	This release resolves an issue where the warning message about roles hierarchy and assignment was not being displayed when creating a new user with the same Admin Role.
HERC-8678	This release resolves an issue where online help requested login credentials twice when using Edge browser.
HERC-8047	This release resolves an issue where empty/null IP/MAC address field values were not being displayed as (Null).
HERC-7851	This release resolves an issue where Lookup Upload would hang if the CSV file had more data columns than header columns.
HERC-7125	This release resolves an issue where charts with a time X-axis and a categorical Y axis only displayed the year in X-axis labels while omitting month, day, hour and minute time parts. An example of such a chart is Login by Destination Address Over Time.
HERC-5844	This release resolves an issue where search results could not be exported to a PDF file within MS Edge browser.

Open Issues

This release contains the following open issues:

Issue	Description
HERC-9296	When the Single Source Chart is in zoom mode and you switch to another Data Category, the Reset Axes option on the chart might not work properly. Workaround: Double click on the chart to zoom out to its original view.
HERC-9393	Search operators tolower & toupper continue to load when using negative numbers. Workaround: Do not use negative numbers with the tolower & toupper search operators.
HERC-9348	Investigate 3.1.0 does not support ' " ' (Double Quotes) & '.' (Period) as a part of alias names.(e.g. 1) | eval tes"t = abs (10) 2) | eval tes.t = abs (10)). Workaround: Do not use ' " ' (Double Quotes) & '.' (Period) as a part of alias names.
HERC-9327	Investigate 3.1.0 does not support ' " ' (Double Quotes) & '.' (Period) as a part of alias names.(e.g. 1) | eval tes"t = abs (10) 2) | eval tes.t = abs (10)). Workaround: Do not use ' " ' (Double Quotes) & '.' (Period) as a part of alias names.
HERC-9296	When the Single Source Chart is in zoom mode and you switch to another Data Category, the Reset Axes option on the chart might not work properly. Workaround: There is another way to reset chart's view is to double click on the chart. It will zoom out to its original view.
HERC-8682	When filtering out an IP in Outliers (right click on the first IP from the Top Anomalous Host table > Filter out that IP > Apply) a warning message "Could not refresh widgets" might be displayed and there will be no data shown on the graph when using the filter menu. Workaround: Click Detect and try again.
HERC-8645	Modifying the fieldset and then restoring it creates a new search after clicking play. Workaround: Search time range and query can be restored by navigating to another section as Dashboard and coming back to the search.
HERC-8553	Search cannot be resumed after changing the time range and then setting it back to the original time. Workaround: Navigate to another section such as Dashboard and come back to the search, this will restore Search time range and query.
HERC-8283	When a lookup list has the word "user" it will cause search join to fail. Workaround: None available at this time.
HERC-8220	A search with selected lookup list fields needs the lookup list to be part of a join in the search query. Workaround: Unselect the lookup fields from fieldset or use the lookup list in the search query.
HERC-7827	Deleted saved search remains displayed in 'Saved Results' UI. Workaround: Refresh the browser page.

Issue	Description
HERC-7597	IP or MAC addresses fields may increase field size when imported, this may impact the upper limit of the CSV file size and number of records when loading a lookup list. Workaround: Limit the CSV file size to approximately 50MB or limit the number of total IP/MAC addresses in the file to 1 million.
HERC-7129	If you create a lookup list using a CSV file with invalid data, Investigate ignores the invalid data and creates the lookup list, but does not notify the user that the CSV file contains invalid data. Workaround None available at this time.
HERC-3241	For an ESM search, you cannot search for the Name field using complex special characters without receiving the error, "Fix query first" Workaround: When invoking Investigate from ESM with values that contain both single and double quotes, truncate the value in Investigate Search Input after the second quote symbol, e.g. if you ESM value of the Name field is: my_esm_value'with"single'and"double_quotes and it got inserted into Investigate as: Name = 'my_esm_value'with"single'and"double_quotes truncate it after the single quote: Name= 'my_esm_value' and replace = with 'starts with': Name starts with 'my_esm_value' After invoking Investigate, remove text starting from the first quote inside the value (the text starting from the second red highlighting in the control). e.g. for the following example: 19@\Aaction@=accept@\Aorig@=167798303@\Ai/f_dir@=outbound@\Ahas_accounting@=0@\Aproduct@=FWM@\AObjectName@=firewall_properties@\AObjectType@=firewall_properties@\AObjectTable@=properties@\AOperation@=Modify Object@\AUid@= Unknown macro: {97AEB653-9AEA-11D5-BD16-0090272CCB30} @\AAdministrator@=Security Management Server@\AMachine@=localhost@\AFieldsChanges@=cluster_id_counter: changed from '0' to '4239' ;@\ASubject@=Object Manipulation@\AOperation Number@=1,-9223372036854775808,-2147483648,-2147483648,"","","","","","","" 1) leave: Name = '19@\Aaction@=accept@\Aorig@=167798303@\Ai/f_dir@=outbound@\Ahas_accounting@=0@\Aproduct@=FWM@\AObjectName@=firewall_properties@\AObjectType@=firewall_properties@\AObjectTable@=properties@\AOperation@=Modify Object@\AUid@= Unknown macro: {97AEB653-9AEA-11D5-BD16-0090272CCB30} @\AAdministrator@=Security Management Server@\AMachine@=localhost@\AFieldsChanges@=cluster_id_counter: changed from ' 2) replace '=' with starts with: Name starts with '19@\Aaction@=accept@\Aorig@=167798303@\Ai/f_dir@=outbound@\Ahas_accounting@=0@\Aproduct@=FWM@\AObjectName@=firewall_properties@\AObjectType@=firewall_properties@\AObjectTable@=properties@\AOperation@=Modify Object@\AUid@= Unknown macro: {97AEB653-9AEA-11D5-BD16-0090272CCB30} @\AAdministrator@=Security Management Server@\AMachine@=localhost@\AFieldsChanges@=cluster_id_counter: changed from '
HERC-2631	When pasting a query from an Excel document in Firefox, the new lines are not visible in Search input. Workaround: When pasting a URL that contains special characters from another application, place quotes around the URL. When pasting into Search input, new line symbols are be retained in the pasted text if they do not stand between query language constructs. New lines characters are rendered invisible in Search Input. Thus, you will not be able to see them but they will be taken into account when matching column names and column values, and recognizing other query language constructs.

Known Issues

HERC-7125	For horizontal visualizations that include a category (for example, Login by Destination Address Over Time), Investigate only displays the year on the Y axis and does not include the minute, hour, day, and month details. Workaround: To view detailed time information, hover over a value in a bar or zoom in to the cluster.
HERC-5737	Issue: When screen resolution is below 1920x1080, visual elements may not render as expected. Workaround: Set the resolution to 1920x1080 or greater.
HERC-2631	Issue: When pasting a query from an Excel document in Firefox, the new lines are not visible in Search input. Workaround: When pasting a URL that contains special characters from another application, place quotes around the URL. When pasting into Search input, new line symbols are be retained in the pasted text if they do not stand between query language constructs. New lines characters are rendered invisible in Search Input. Thus, you will not be able to see them but they will be taken into account when matching column names and column values, and recognizing other query language constructs.
HERC-8318	Some customers may observe that ingestion of events from the Transformation Hub into Investigate/Vertica occasionally pauses. Such a situation can occur where source devices run with incorrect system clocks or when they produce timestamps (device receipt times) that cannot be parsed correctly and which may have gone unnoticed before the deployment of Investigate. The duration and frequency of the ingestion pauses is dependent upon the extent to which such timestamps deviate more than +/- 2 days from real-time. Extreme cases (event timestamps spanning many days before or after the actual date) could result in a backlog of events beyond the available/configured retention of the TH Avro Topic that feeds Investigate. In such a case, there is a risk that some events may be purged from TH before Investigate/Vertica automatically resumes its ingestion; any events purged from TH will never be consumed in to Investigate. Should such behavior be observed, please contact Micro Focus Support to first validate the cause. While the most effective remediation is to correct such timestamp anomalies at source (this is also needed for effective security event-monitoring), Micro Focus is researching methods to mitigate the effect on Investigate ingestion for a future release.

For information regarding Transformation Hub known issues, refer to the Transformation Hub Release Notes available from the Micro Focus Community.

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 Release Notes (Investigate 3.1.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!