ArcSight Recon 1.1 Release Notes

December 2020

ArcSight Recon 1.1 (Recon) includes new features, improves usability, and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input.

We hope you continue to help us ensure that our products meet all your needs. We want to hear your comments and suggestions about the documentation available with this product. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Recon Documentation page.

Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database.

Recon deploys within the **ArcSight Platform**. For more information about the other products available within the suite, see the *Release Notes for ArcSight Platform 20.11*.

What's New?

This release includes the following features, enhancements, and software fixes:

Search Function Enhancements

This release enhances the **Search** function. The **Search** function helps you investigate security issues by viewing search results and identifying outlier events.

Enhanced Event Details Panel

When users select an event in the Events table, Search opens the **Event Details** panel. This panel includes a unique URL for the event, which can be shared with colleagues or used to view the details in a separate browser tab.

Users can export the entire set of Event Details to a PDF or CSV file, or choose specific values within the details to export. Also when choosing specific values, users can add them to a search query or use with nsLookup and WhoIs.

Configure Preferences for Search Settings

To reduce the time needed to create and manage searches, users can configure their preferred Search settings. For example, users can specify a default fieldset, time range (including a dynamic time range), and a default view for Search results. The view can include raw data for events.

Set an Expiration Time for Searches

You can now specify how often you want searches to expire, and thus be removed from the system. This option enables you to reduce the amount of search results held in the database, thus enabling Search performance. The database purges expired searches at midnight.

Choose from Three Types of Timestamps

Search can display results based on the timestamp associated with each event. The database stores three different timestamps for each event: Database Receipt Time; Device Receipt Time; and Normalized Event Time. For peak performance, Search automatically uses the Normalized Event Time setting. Users can also choose to specify a timestamp as the default setting for all their searches.

Added Ability to Create Storage Groups

This release gives you the ability to create **storage groups**, which allows you to partition the incoming events data and provide different retention periods based on query filters. Because you can set data retention policies per storage group, you can retain certain high volume events for a short time period and other important events for longer time period.

The **query filter** enables you to associate a storage group with specific compliance requirements, business needs, or search activities. Recon uses the specified query filters to direct events to the correct storage group. For example, one group might have a filter for `categoryDeviceGroup =/ Firewall` and another for `severity >= 7`. If an event does not match any of the active filters, Recon sends the event to the *DefaultStorage* group. You cannot change the name, query, or rank of the *DefaultStorage* group.

Reporting Enhancements

This release leverages the Reports and Dashboards function previously available with ArcSight Logger only. This function includes MITRE ATT&CK content, enabling you to **hunt** for undetected threats as well as create charts and dashboard to visualize filtered data with tables, charts, and gauges. The Reporting content comes in the following categories.

Cloud-based Dashboards and Reports

Content based on the industry-wide standards set by the Cloud Security Alliance (CSA). This alliance has identified the most significant security threats to the shared, on-demand nature of cloud computing.

Foundational Dashboards and Reports

Content focused on entities, networks, firewalls, malware, and known vulnerabilities.

OWASP-based Dashboards and Reports

Content based on the industry-wide standards set by the Open Web Application Security Project® (https://owasp.org). OWASP has established a list of the Top 10 security risks to web applications, focusing on the most critical threats to the shared, on-demand nature of web-based applications.

Incorporate Content from Data Sources

If you have the Report Admin permission, you can configure Reporting to incorporate data from additional sources, such as a relational database or a REST data source containing XML- or JSON-formatted data.

Import and Export Content

If you have the Report Admin permission, you can add and remove Reporting content, also known as assets, for the reports and dashboards.

Resolved Issues

This release includes the following software fix that resolves a previous issue:

Failure to Re-install after an Upgrade

This release resolves the issue where you might experience a failure when attempting to re-install the product after performing an upgradel. This issue occurred because the installer failed to find the images required for installation. (`INST-2545`)

Known Issues

The following issues are currently being researched for Recon 1.2.

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/), and then select the appropriate product category.

Outlier Model - Erroneously Implies the Date is an Error

Issue: When you copy a Search query to create the filter for an outlier model and the query includes a timestamp, Recon erroneously highlights the specified date as if the date or its format were invalid.

For example, you copy a search query that includes the phrase `Normalized Event Time = 29/05/20 16:20:39:288`. In **Configuration** > **Outlier**, you paste the copied query in the filter field for a new model. The query field underlines the timestamp in red, which is the usual indication that the value is invalid. (`OCTCR33I112031`)

Workaround: Ignore the highlight that indicates that the copied timestamp value is invalid.

Outlier Model - Does Not Display After Changing the Timestamp Format

Issue: When you apply a timestamp format to an outlier model, and then change the timestamp format, Recon does not display the model in Available Models.

For example, you create a model in **Configuration** > **Outlier** with the Device Receipt Time = 12/31/19. You then change the timestamp format in **My Profile** > **User Preferences** > Date/Time Format to `YYYY/MM/DD hh:mm:ss:ms`. When you access **Configuration** > **Outlier**, Recon no longer displays the model with the modified timestamp. (`OCTCR33I113036`)

Workaround: In **My Profile** > **User Preferences** > Date/Time Format, select the original timestamp format for the model. Recon displays the model in Available Models.

Outlier Model - Issues with Custom Range Start and End Time

Issue: When you apply a Custom Range to an outlier model, the system automatically adds 1 hour to the Start Time and End Time. For example, if you enter 08/18/20 05, the system changes it to 08/18/20 06. (`OCTCR33I116004`)

Workaround: Enter 1 hour less than the desired time. Recon will automatically add 1 hour to the time. For example, enter 08/18/20 04 for 08/18/20 05.

Issue with Searches and Features and Timestamp

Issue: When you change the time format for existing searches and features, errors might occur. (OCTCR33I112038)

Workaround: You might need to correct the time format for the timestamp.

Issue with Time Zone Setting - Incorrect End Times

Issue: In **User Preferences**, when you set the Time Zone to Database time zone or Custom Time zone, and then Select Range to Yesterday, Week to Date, Month to Date, and so on, the start time is 6:00 instead of 0:00. Recon also displays the end time incorrectly. (OCTCR33I115040)

Workaround: In **My Profile** > **User Preferences** > Date/Time Format, set the Time Zone to Browser time zone.

Issue with Time Zone Setting - Performing a Search

Issue: In **User Preferences**, when you set the Time Zone to Database time zone, your ability to search might not work properly. (OCTCR33I115046)

Workaround: In My Profile > **User Preferences** > Date/Time Format, set the Time Zone to Browser time zone, and then perform the search again.

Users Can Create Storage Groups Using a Filter

Issue: When you create a storage group, Recon allows you to enter invalid data in the query filter, such as 12345. (OCTCR33I101043)

Workaround: Use a valid Query Filter. For example:

- Existing fields, such as 'categoryBehavior', 'name', 'agentAddressBin', 'destinationPort', etc.
- Use the correct SQL language. For more information, see the *Reference Manual SQL Lanaguge Elements*.

Saved Searches Remain Listed After Deletion by Expiration

Issue: When creating storage groups, you can enter a filter value such as 12345. The saved searches remain listed after deletion by expiration. (OCTCR33I113045)

Workaround: Reload the browser page to load searches displaying the correct items listed.

Issue with Default Time Setting Static

Issue: Recon fails to apply the default value of Last 30 Minutes when you set the Default Time Setting to Static. (OCTCR33I116009)

Workaround: None. If you want Last 30 Minutes as your default, use the Dynamic preference and select Last 30 Minutes. Otherwise, use Static and always specific a custom date range.

Issue with Reindexing Process in an Upgraded Recon Database

Issue: When Recon is reindexing, a script Re-creating text index completed displays; however, the process is still running and Recon is not ready for use. (OCTCR33I115036)

Workaround: Do not use the product immediately. Give Recon time to create indexes, and so on.

Opening Multiple Tabs for Recon Might Create an Authentication Error

Issue: Recon might redirect you to the login page but fail to let you enter credentials, when all of the following conditions are true:

- You have Recon open in a browser tab;
- You have at least three open tabs displaying content for the Reports feature; and
- You log out of Recon or wait for any of the tabs to time out.

When you attempt to log in again from any of the tabs, you might see an authentication error. (HERC-9758)

Workaround: If this issue occurs, enter the Recon URL, `https://hostname/re`, in a new tab.

Saved Searches Page Continues to Display a Deleted Search

Issue: After you delete a saved search, the **Saved Searches** page continues to display the deleted search. (HERC-7827)

Workaround: Refresh the browser page.

Lookup List Field in a Fieldset Must be Joined to a Query

Issue: When you add a Lookup List field to a fieldset without also adding the field to the query, Search fails to load. This issue occurs because Search expects the Lookup List field to be part of a join in the search query. (HERC-8220)

Workaround: Remove the lookup field(s) from the fieldset or use the Lookup List in the search query.

Search Fails if String Operator Ends with a $

Issue: Search fails to return results when you use string-based search operators and the string ends with `$`. Affected operators might include *trim*, *ltrim*, *rtrim*, *md5*, *lower*, *upper*, and *substr*. (HERC-9307)

For example, the following type of query will fail:

```
| eval md5_alias = md5(Hello$)
```

Workaround: Run the search without the `$` at the end of the string. For example:

```
| eval md5_alias = md5(Hello)
```

Recon Accepts CSV File with Invalid Data, Creates Empty Lookup Table

Issue: If the CSV file for your Lookup List contains invalid data, Recon will successfully create the lookup table. However, because Recon ignores the invalid data, the new lookup table will not have any data. Also, you will not receive a notification about the empty Lookup List. (HERC-7129)

Workaround: There is no workaround at this time.

Size or Contents of a CSV File Can Adversely Affect the Ability to Load a Lookup List

Issue: When you add a CSV containing IP or MAC address fields, the size of those fields can increase when imported as a Lookup List. As a result, the CSV file might exceed the file size limit or the maximum number of records allowed for loading a Lookup List. (HERC-7597)

Workaround: Limit the CSV file size to approximately 50 MB or limit the number of total IP and MAC addresses in the file to 1 million.

Data in the Events Timeline and Table are Out of Sync

Issue: If you narrow the range of time in the Events Timeline then execute a new search, the timeline and the Events table might become out of sync. When this occurs, the table displays a "No events to show" message. (HERC-9901)

Workaround: Perform one of the following actions:

- To prevent this issue from occurring, select **Disable Range Selector** in the Events Timeline *before* executing a new search. This action clears the narrowed time range selection.
- If this issue has already occurred, refresh the browser. The Events Timeline will update to display the previously selected time range. Then select **Disable Range Selector** in the Events Timeline. The Events table automatically reloads with data that matches the timeline.

Search Fails to Revert Fieldset to Original Setting

Issue: If you change the fieldset after running a search, then leave the Search page or move out of the Search section, Search fails to reset the fieldset to the original setting. For example, you choose the *Base Event Fields* field set and run the search, then change the fieldset to *All Fields*. Next you navigate to Saved Searches page. When you return to the Search page, the fieldset is still *All Fields* rather than reverting to *Base Event Fields* as it should. (HERC-9865)

Workaround: To revert the fieldset to its original setting, press **F5** while viewing the Search.

Data Quality Chart Fails to Update After Changing Time to a Dynamic Value

Issue: When you change a time setting for charts in the Data Quality dashboard, the charts automatically updates as soon as you pick the new value. However, if you change the **Start Time** or **End Time** to a dynamic value, the charts fail to update automatically. (HERC-9913)

Workaround: To refresh the charts, click outside the time selection that you just changed. For example, if you changed the **End Time** to a dynamic value, click either on a chart or on the **Start Time**.

Search Join Fails when Lookup List Has 'User' as a Value

Issue: Search displays an error and fails to apply a join if an associated lookup list includes the word "user" for a data value. (HERC-8283)

Workaround: None available at this time.

Script to Enable Reporting Fails to Work on a Single Node Machine

Issue: If you create users in Recon before running the script that enables Reporting, those users automatically get assigned the Report Admin role, which you cannot change.

When you only have a single permission for the reporting roles, Recon does not map the permission to InetSoft accurately because InetSoft expects Recon user permissions in an array. For example, in Recon, by default, the *Report User* role has only one permission that is *Report Admin*. So, in that case, you cannot use the *Report User* functionality. (`HERC-10045`)

Workaround: Use the *Reports* permissions (*Report Admin*, *Design Reports*, *Schedule Reports*, *View Reports*) with at least one other Recon permission. For example, to use the *Report User* functionality, you can modify the *Report User* role to include *Report Admin* and *Execute Search* permissions.

Multi-node Installation (Master, Worker, and Database Setup) Fails When `database ssl-enabled` is Specified as `False`

Issue: For a master, worker, and database setup, the multi-node installation fails when `database ssl-enabled` is Specified as `False`. (`INST-2796`)

Workaround: For a master, worker, and database setup, specify `database ssl-enabled` as `true`:

```
database ssl-enabled=true
```

Additional Documentation

For more information about using Recon, see the additional documentation below.

Applying Storage Group Settings to the Events Table

When applying a query filter to storage groups, you can use SQL language or an existing field:

- 'categoryBehavior'
- 'name'
- 'agentAddressBin'
- 'destinationPort'

For example: `categoryDeviceGroup='/Firewall' or categoryDeviceGroup='/IDS'`

For more information about the correct SQL language to use, see the *Reference Manual SQL Language Elements*.

The following are *incorrect* examples of a query filter:

- The query `categoryDeviceGroupX='/Firewall'` will fail because `categoryDeviceGroupX` does not exist) does not exist)
- The query `name != 'Outlier' and severity >= 7` will fail because there should be no spaces between the operators (`!=` or `>=`) and the values (`'Outlier'` or `7`).

Technical Requirements

For more information about the software and hardware requirements for your deployment and a tuned performance, see the *Technical Requirements for ArcSight Platform 20.11*.

Downloading Recon

Before you begin installing Recon, you must download necessary product installation packages. The installation package also includes the respective signature file, for validating that the downloaded software is authentic and not tampered by a third party.

To review the list of the files and versions to download for this release, see the *Release Notes for ArcSight Platform*.

Installing Recon

Micro Focus provides several options for deploying your Recon environment. For more information, see the *Administrator's Guide for ArcSight Platform* provided at the Recon Documentation site.

Before installing, please review the following considerations:

- "Add Report Permissions to Recon Roles" on page 9

Add Report Permissions to Recon Roles

When you deploy Recon, the default roles common in the ArcSight Platform all receive the permissions to conduct searches. However, these roles do not receive any of the Report-based permissions. Only the *Report User* role, specific to Recon, has permission to perform all the reporting actions, including the reporting admin actions.

To ensure that Recon users can access both the Search and Report features, either add one or more of the Report permissions to the default roles or create new roles with the permissions. Ensure that any user assigned a reporting permission also has a Search or Admin permission. For more information about assigning roles and permissions, see the Help in the product.

NOTE: Reports do not function appropriately if a user's role has only Report-based permissions. For example, the default *Report user* role must have at least one Search- or Admin-based permission. (`HERC-10003`)

Licensing Information

For information about activating a new license, see the *Administrator's Guide for ArcSight Platform* provided at the Recon Documentation site.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/