ArcSight Recon 1.0 Release Notes

July 2020

This release introduces ArcSight Recon 1.0 (Recon).

We designed this product 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.

About ArcSight Recon

Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database. The **Search** feature helps you investigate security issues by viewing search results and identifying outlier events. The **Reports** feature, including MITRE ATT&CK content, enables you to **hunt** for undetected threats as well as create charts and dashboard to visualize filtered data with tables, charts, and gauges. With the Outlier Analytics feature you can identify anomalous behavior by comparing incoming event values to typical values for your environment. When specifying a time range, you can enter dynamic value without using the calendar to pick dates, such as a start time 12 days ago (`$Now - 12d`).

Recon deploys within the **ArcSight Platform**. For more information about the other products available within the suite, see the *Release Notes for ArcSight Platform 2.3.0*.

Introducing the Widget SDK

This release introduces the **Widget Software Development Kit** (the Widget SDK), which enables you to build new widgets for the Dashboard or modify existing widgets for deployed solutions. The entitlement for your deployed product also grants you access to the Dashboard and to the Widget SDK. You can download the Widget SDK to your local production or test environment to start creating custom widgets.

- "Using the Widget SDK" on page 2
- "Considerations for Updating the Widget Store" on page 2

Using the Widget SDK

Once you unpack the Widget SDK, you have access to its documentation.

1. Extract the contents of the `widget-sdk-n.n.n.tgz` file.
2. Follow the steps in the **Getting Started** section of the included *ReadMe*.
3. After you compile the new or modified widget, add it to the widget store for use in the Dashboard.

Considerations for Updating the Widget Store

Review the following considerations before modifying or creating new widgets:

- Widgets provided with a deployed application are included in the default widget store directory: `/opt/NFS_Volume/arcsight-vol/fusion/widget-store`.
- Each new widget must have a unique name.
- You cannot edit an out-of-the-box widget. To prevent your custom widgets from being erased or overwritten by a product upgrade, do not name them the same as an out-of-the-box widget.

Known Issues

The following issues are currently being researched for Recon 1.0.

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.

- "Malware Scan Might Report a False Positive" on page 3
- "Install and Upgrade Fails Due to Comma Character in Admin Password" on page 3
- "Failure to Re-install after an Upgrade" on page 3
- "Admin Password Change Fails to Update Registry Admin" on page 4
- "Cannot Import Users from Enterprise Security Manager" on page 4
- "Opening Multiple Tabs for Recon Might Create an Authentication Error" on page 4
- "Saved Searches Page Continues to Display a Deleted Search" on page 4
- "Lookup List Field in a Fieldset Must be Joined to a Query" on page 4
- "Search Fails if String Operator Ends with a $" on page 4
- "Recon Accepts CSV File with Invalid Data, Creates Empty Lookup Table" on page 5
- "Inconsistent Results when Query Includes Multiple Comparison Values" on page 5

Malware Scan Might Report a False Positive

Issue: When scanning the `cdf-2020.05.00100-2.3.0.7.zip` file or an installer `*.tar` file that contains this file, certain malware detection programs might report a false positive in a subroutine called `updateRoleId`. This subroutine is within `/cdf/images/cdf-master-images.tgz` file.

Workaround: None needed. We validated that the code is not malware. We have verified that the package was built and compiled in a secure and trusted fashion. In an coming release, we will modify the packaging to avoid this false positive.

Install and Upgrade Fails Due to Comma Character in Admin Password

Issue: If the password for the administrative user for the CDF Management Portal that you use during an installation or upgrade process includes a comma (,) character, the following issues will occur:

- The CDF upgrade will fail when upgrading to CDF 2020.02 or CDF 2020.05.
- A new installation of CDF 2020.02 or CDF 2020.05 will fail during the image upload phase.

Workaround: Use the `/opt/arcsight/kubernetes/scripts/updateLocalRegistryInfo.sh` script to change the password to new one that does not include the restricted character. (`INST-2464`)

Failure to Re-install after an Upgrade

Issue: If you attempt to re-install the product after performing an upgrade, the installation might fail. This issue occurs when the installer cannot find the images required for installation. (`INST-2545`)

Workaround: To workaround this issue and find the required images, enter the following:

```
cd */cdf-2020.05.00100-2.3.0.7/cdf/images
/opt/arcsight/kubernetes/scripts/uploadimages.sh -F /opt/cdf_files/cdf-
  2020.05.00100-2.3.0.7/cdf/images/cdf-master-images.tgz -u register-user -p
  Arst@dm1n -y -c 2
/opt/arcsight/kubernetes/scripts/uploadimages.sh -F /opt/cdf_files/cdf-
  2020.05.00100-2.3.0.7/cdf/images/cdf-common-images.tgz -u register-user -p
  Arst@dm1n -y -c 2
/opt/arcsight/kubernetes/scripts/uploadimages.sh -F /opt/cdf_files/cdf-
  2020.05.00100-2.3.0.7/cdf/images/cdf-phase2-images.tgz -u register-user -p
  Arst@dm1n -y -c 2
```

Admin Password Change Fails to Update Registry Admin

Issue: Changing the password for the adminstrative user of the CDF Management Portal does not automatically change the password for the registry-admin user used to access the local docker registry.

Workaround: After changing the admin password, run the `/opt/arcsight/kubernetes/scripts/updateLocalRegistryInfo.sh` script to update password for registry-admin. (`INST-2464`)

Cannot Import Users from Enterprise Security Manager

Issue: When you attempt to import users from ArcSight Enterprise Security Manager, you will receive a 406 HTTPS Error if one of the following conditions is true:

- You attempt to import the users by using the IP address of the ESM server
- If you enter the FQDN (fully qualified domain name) for the ESM server but either the port or admin credentials are incorrect

Workaround: For the ESM server, specify a valid FQDN, as well as the correct port and admin credentials. (`HERC-9941`)

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.

Inconsistent Results when Query Includes Multiple Comparison Values

Issue: Search might return erroneous results when the search operator in the query is a comparison operator and includes three or more values. This issue occurs inconsistently. (`HERC-9662`)

For example, the following query might return erroneous results:

```
| eval abs_alias = abs (10 < 40 < 50 )
```

Workaround: When using a comparison operator, include no more than two values. For example:

```
| eval abs_alias = abs (10 < 40 )
```

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.

Issue with Pasting Content from Excel into a Search Query in Firefox

Issue: When pasting a query from an Excel document, the new lines are not visible in Search input. This issue occurs in the Firefox browser.

When pasting content into Search input, Search retains new line symbols in the pasted text if they do not stand between query language constructs. Search renders the new lines characters invisible. 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-2631`)

Workaround: When pasting a URL that contains special characters from another application, place quotes around the URL.

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.

Issues with Starting the Web Service Pod during an Upgrade

Issue: When you upgrade to Transformation Hub 3.3, you might observe an intermittent issue with starting the web service pod. This issue correlates with a slow network and/or slow VM response. When this issue occurs, the pod startup gets blocked or delayed, leading to various issues, such as failing to create new topics and/or registering the new latest avro schema version. In the web service log file, you might see the following message: `Thread Thread[vert.x-eventloop-thread-0,5,main] has been blocked for 5715 ms, time limit is 2000.` (EB-3061, EB-3062)

Workaround: Restart the web service pod.

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.

Technical Requirements

For more information about the software and hardware requirements for your deployment and a tuned performance, see the *Technical Requirements for ArcSight Recon 1.0*.

Downloading Recon

Before you begin installing Recon, you must download and unzip Recon and all 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.

You can download the following installation packages:

Files	Description

`recon-installer-1.0.0.7.tar.gz`
◆ `installers`
  ◆ `cdf-2020.05.00100-2.3.0.7.zip`
  ◆ `db-installer_3.2.0-4.tar.gz`
◆ `suite_images`
  ◆ `recon-1.0.0.7.tar`
  ◆ `transformationhub-3.2.0.29.tar`
  ◆ `fusion-1.1.0.29.tar`
  ◆ `arcsight-installer-metadata-2.3.0.29.tar.gz`
◆ Single-node installer scripts
	Contains the files for installing and deploying Recon:
	◆ Contains the following installer files:
	  ◆ CDF installer
	  ◆ Database installer
	  ◆ Recon installer
	◆ Contains the following image files:
	  ◆ Transformation Hub image
	  ◆ Recon offline image
	  ◆ Fusion image
	  ◆ CDF core image
	◆ Single-node installer scripts

(Conditional) `arcsight-installer-metadata-2.3.0.29.tar`	Installation files for all products that can be deployed in the ArcSight Platform
`ArcSight-ArcMC-2.9.2.2188.0.bin` (Optional)	Installation file for ArcSight Management Center (ArcMC)

To download and verify the signature of the downloaded files:

1. Log in to the computer where you want to install Recon.

2. Change to the directory where you want to download the installer files:

   ```
   cd <download_directory>
   ```

   For example:

   ```
   cd /opt
   ```

   NOTE: If you are planning to install Recon by using scripts, use `/opt` as the download location.

3. Download all the necessary product installer files from the Micro Focus Downloads website.
4. To verify the signature of the downloaded files, enter the following command:

   Syntax: `sha256sum <file_name>; cat <file_name>.sha256`

   Example: `sha256sum recon-x.x.x.x.zip; cat recon-x.x.x.x.sha256`

   The output from each set of compressed installation packages should match their corresponding SHA-256 signatures. If they do not match, download the files again and verify the signature. If the checksum does not match even with the new files, contact Micro Focus Customer Support.
5. To unzip the downloaded files, enter the following commands:

   For tar file: `tar xvfz <file_name>.tar.gz`

   For zip file: `unzip <file_name>.zip`

Installing Recon

Micro Focus provides several options for deploying your Recon environment. For more information, see the *Administrator Guide for ArcSight Recon 1.0* provided at the Recon Documentation site.

Before installing, please review the following considerations:

- "Add Report Permissions to Recon Roles" on page 8

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 Guide for ArcSight Recon 1.0* 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/

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

© Copyright 2020 Micro Focus or one of its affiliates.