IT S
specialist

ITS INVENTORY

Inventory for QRadar
User Guide

1. Introduction

ITS Inventory for QRadar is a full-featured application that provides structured, enriched, relevant information about IT assets configuration. The application extends configuration data in the built-in QRadar Asset DB with information from Network Hierarchy, Log Sources, Reference Data, Active Directory/LDAP, DNS. As a result, you get all available assets configuration parameters in one place: name, IPs, MAC, network group, accounts, linked log sources status, security groups, etc.

The functionality implemented in Inventory Light gives security analytics and administrators a comprehensive toolbox to address cybersecurity asset management challenges.

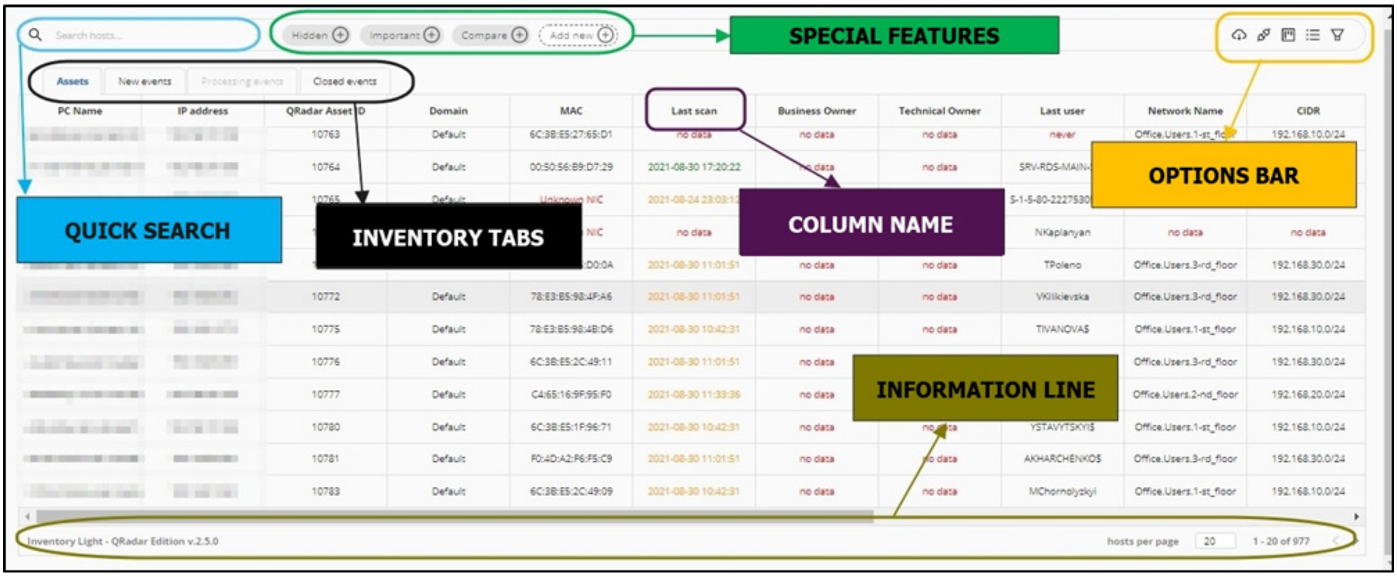
Base usage scenarios:

- searching, filtering assets by configuration parameters
- review asset details card with the most relevant and consolidated information
- detect assets not covered by security tools and policies
- use Inventory assets properties in SIEM context (correlation rules, searches, reporting)
- identify SIEM's configuration issues
- use quick access (in one console) to assets parameters during offense or incident analysis

ITS Inventory for QRadar is delivered through IBM AppExchange and absolutely free.
This guide provides detailed instructions for installing and initializing ITS Inventory application in QRadar.

2. Overview

A table consists of columns, rows, and cells. It is possible to work with each element of the table both individually and in combination with others. There are a quick search bar and special features at the top of the table, the options bar with icons for export, customizer panel, templates menu, filters menu and application activity are located in the right upper corner. An information line showing hints for special features is located below the table. The general structure of the table is shown in Figure 1.



PC Name	IP address	QRadar Asset ID	Domain	MAC	Last scan	Business Owner	Technical Owner	Last user	Network Name	CIDR
[redacted]	[redacted]	10763	Default	6C:3B:E5:27:65:D1	no data	no data	no data	never	Office.Users.1-st_flo	192.168.10.0/24
[redacted]	[redacted]	10764	Default	00:50:56:B9:D7:29	2021-08-30 17:20:22	no data	no data	SRV-RDS-MAIN-		
		10765	Default	Unknown NIC	2021-08-24 23:08:12			S-1-5-80-2227530		
				NIC	no data			NKaplanyan	no data	no data
[redacted]	[redacted]			:D0:0A	2021-08-30 11:01:51	no data	no data	TPoleno	Office.Users.3-rd_floor	192.168.30.0/24
[redacted]	[redacted]	10772	Default	78:E3:B5:98:4F:A6	2021-08-30 11:01:51	no data	no data	VKilikievska	Office.Users.3-rd_floor	192.168.30.0/24
[redacted]	[redacted]	10775	Default	78:E3:B5:98:4B:D6	2021-08-30 10:42:31	no data	no data	TIVANOVA$	Office.Users.1-st_floor	192.168.10.0/24
[redacted]	[redacted]	10776	Default	6C:3B:E5:2C:49:11	2021-08-30 11:01:51	no data			Office.Users.3-rd_floor	192.168.30.0/24
[redacted]	[redacted]	10777	Default	C4:65:16:9F:95:F0	2021-08-30 11:33:36	no data			Office.Users.2-nd_floor	192.168.20.0/24
[redacted]	[redacted]	10780	Default	6C:3B:E5:1F:96:71	2021-08-30 10:42:31	no data	no data	YSTAVYTSKYI$	Office.Users.1-st_floor	192.168.10.0/24
[redacted]	[redacted]	10781	Default	F0:4D:A2:F6:F5:C9	2021-08-30 11:01:51	no data	no data	AKHARCHENKO$	Office.Users.3-rd_floor	192.168.30.0/24
[redacted]	[redacted]	10783	Default	6C:3B:E5:2C:49:09	2021-08-30 10:42:31	no data	no data	MChornolyzkyi	Office.Users.1-st_floor	192.168.10.0/24

Inventory Light - QRadar Edition v.2.5.0

hosts per page 20 1 - 20 of 977

Figure 1

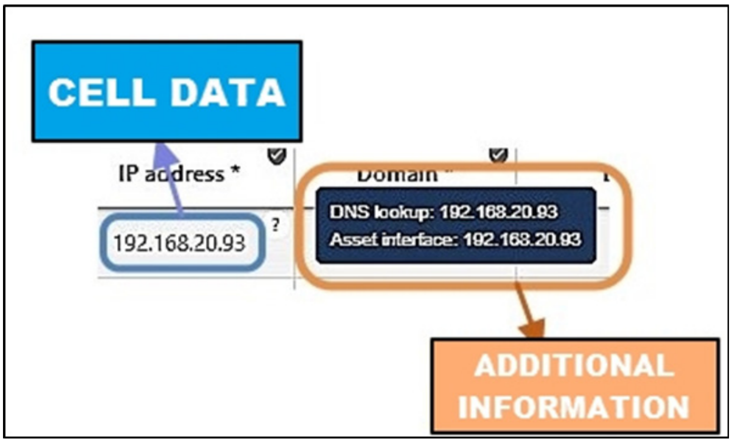
2.1 Cells

Table **cells** contain information. An empty cell indicates that the corresponding resource is not yet connected to the system. There are also separate markings inside the cell:

? **(question mark)** - additional data sources or additional information. Hovering over the cell displays detailed information.

! **(exclamation mark)** - is displayed if data from different sources do not match. This sign is displayed in red without hovering over the cell. Mouse pointing over the exclamation mark displays detailed information.

The general structure of the cell is shown on Figure 2.



IP address *

Domain *

192.168.20.93 ?

DNS lookup: 192.168.20.93
Asset interface: 192.168.20.93

Figure 2

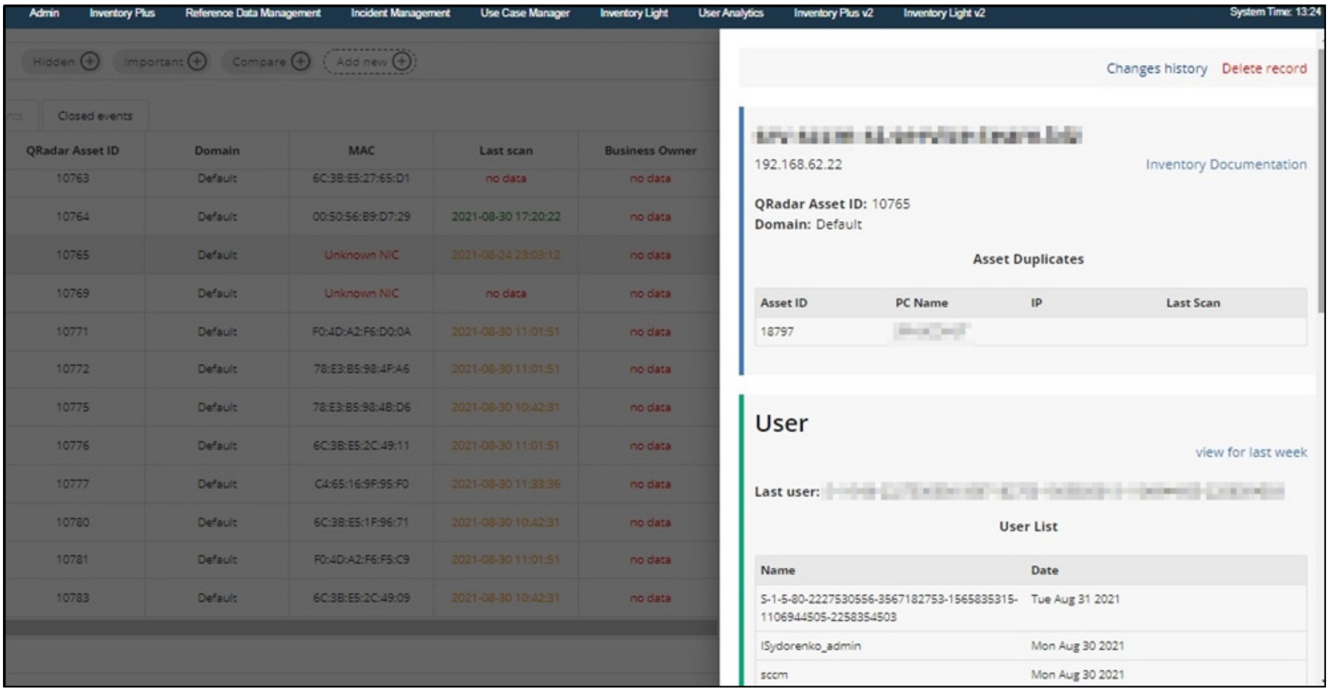
Data in cells

The information in the cells of the table can be of several types. Types are listed in Table 1.

Data	Display	Data type	Additional information
Text	t.service-team.biz	*string*	combination of letters and numbers is considered as string
Number	1570	*integer*	can be also a set of numbers
Date and time	21.05.2019, 11:34:14	*date and time*	hours are displayed in the 24-hour time zone
No data Not resolved Is not asset Never Empty cell		*NULL*	no data is not asset never not resolved

Table 1

Double-clicking on a cell opens a panel with details of all fields of the table (Figure 3). It is also possible to open these data in the summary table in the Assets tab in QRadar by clicking on **OPEN IN ASSETS TAB** in the upper right corner of the cell details panel.



QRadar Asset ID	Domain	MAC	Last scan	Business Owner
10763	Default	6C:3B:E5:27:65:D1	no data	no data
10764	Default	00:50:56:B9:D7:29	2021-08-30 17:20:22	no data
10765	Default	Unknown NIC	2021-08-24 23:03:12	no data
10769	Default	Unknown NIC	no data	no data
10771	Default	F0:4D:A2:F6:D0:0A	2021-08-30 11:01:51	no data
10772	Default	78:E3:B5:98:4F:A6	2021-08-30 11:01:51	no data
10775	Default	78:E3:B5:98:4B:D6	2021-08-30 10:42:31	no data
10776	Default	6C:3B:E5:2C:49:11	2021-08-30 11:01:51	no data
10777	Default	C4:65:16:9F:95:F0	2021-08-30 11:33:36	no data
10780	Default	6C:3B:E5:1F:96:71	2021-08-30 10:42:31	no data
10781	Default	F0:4D:A2:F6:F5:C9	2021-08-30 11:01:51	no data
10783	Default	6C:3B:E5:2C:49:09	2021-08-30 10:42:31	no data

Changes history Delete record

[redacted]

192.168.62.22

Inventory Documentation

QRadar Asset ID: 10765
Domain: Default

Asset Duplicates

Asset ID	PC Name	IP	Last Scan
18797	[redacted]		

User

view for last week

Last user: [redacted]

User List

Name	Date
S-1-5-80-2227530556-3567182753-1565835315-1106944505-2258354503	Tue Aug 31 2021
ISydorenko_admin	Mon Aug 30 2021
sccm	Mon Aug 30 2021

Figure 3

Important: details in Inventory could be different than in Assets tab.

The history of changes in Asset card could be seen on **CHANGES HISTORY** in the right upper corner. Deleting the data from the card is possible be pressing on **DELETE RECORD** in the right upper corner.

2.2 Information Line

Below the table there is an information line that contains hints and page views. The left part of the information bar gives you hints on performing some of the special features related operations.

On the right side of the information line there is the number of currently displayed rows and pages and the total number of pages for the selected configuration. It is possible to change the number of rows displayed and to go to the next or previous page using the chairs to the right of the total pages button. The structure of the rows and pages is shown in the Figure 4.

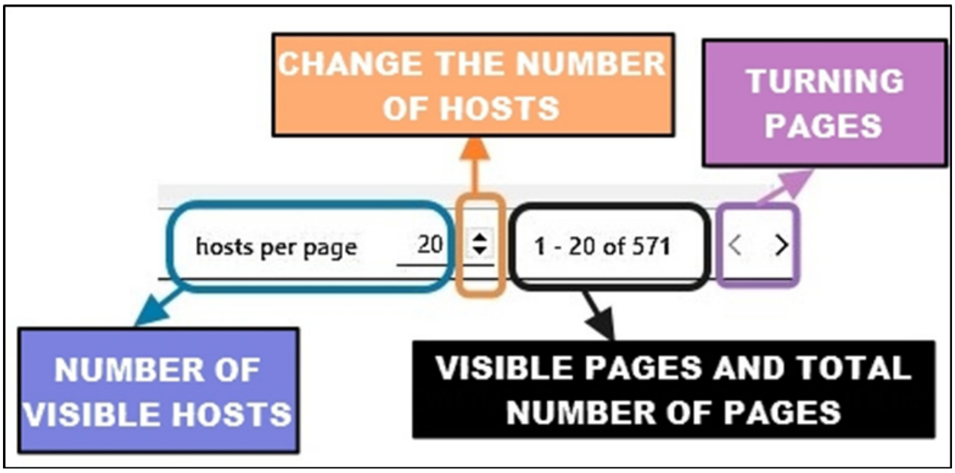

CHANGE THE NUMBER OF HOSTS
TURNING PAGES
hosts per page
20
1 - 20 of 571
NUMBER OF VISIBLE HOSTS
VISIBLE PAGES AND TOTAL NUMBER OF PAGES

Figure 4

2.3 Columns

Column is a vertical field that contains a title and consists of rows with information related to the element in the title. There are many columns in the table that could be customized using templates. The structure of the table column is shown in the Figure 5.

Rows in columns can be sorted in ascending order (ASC, where the empty cells are displayed last) or in descending order (DESC, where the empty cells are displayed first).

To change the sorting method click the column name once. It is possible to see the current ordering to the left of the special features above the table: Order to ASC. The ordering is done only for the selected column.

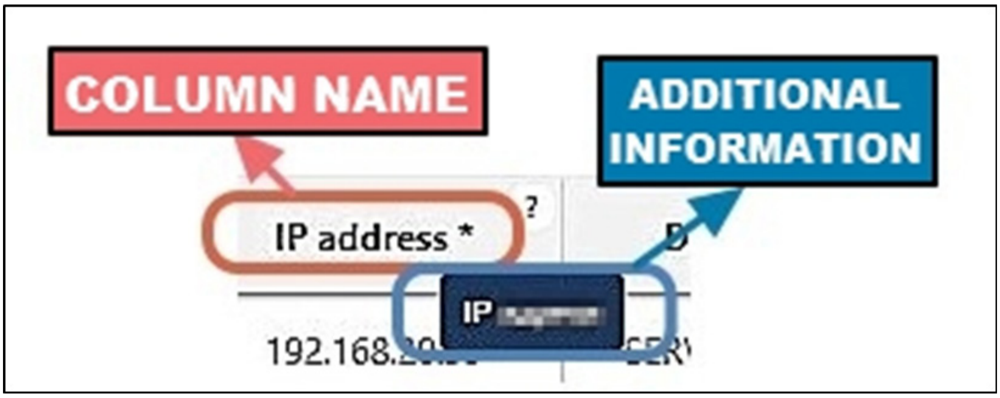
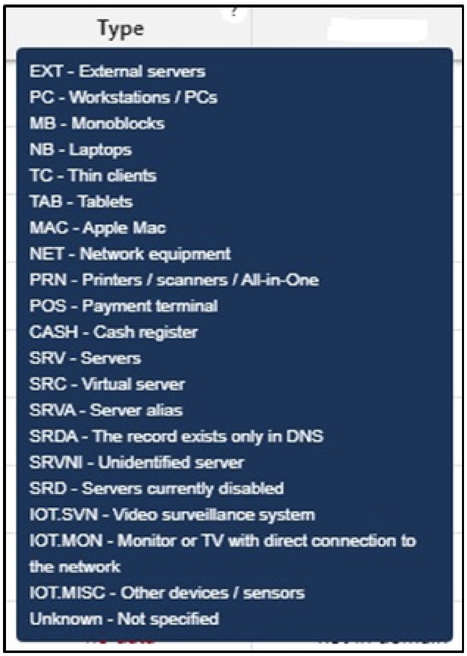


Figure 5

While hovering over the column name a question mark will appear in the upper right corner of the cell ? .

While hovering over it a pop-up window will show what information is covered in this column, what kind of information the name include and what are the abbreviations in the cell.

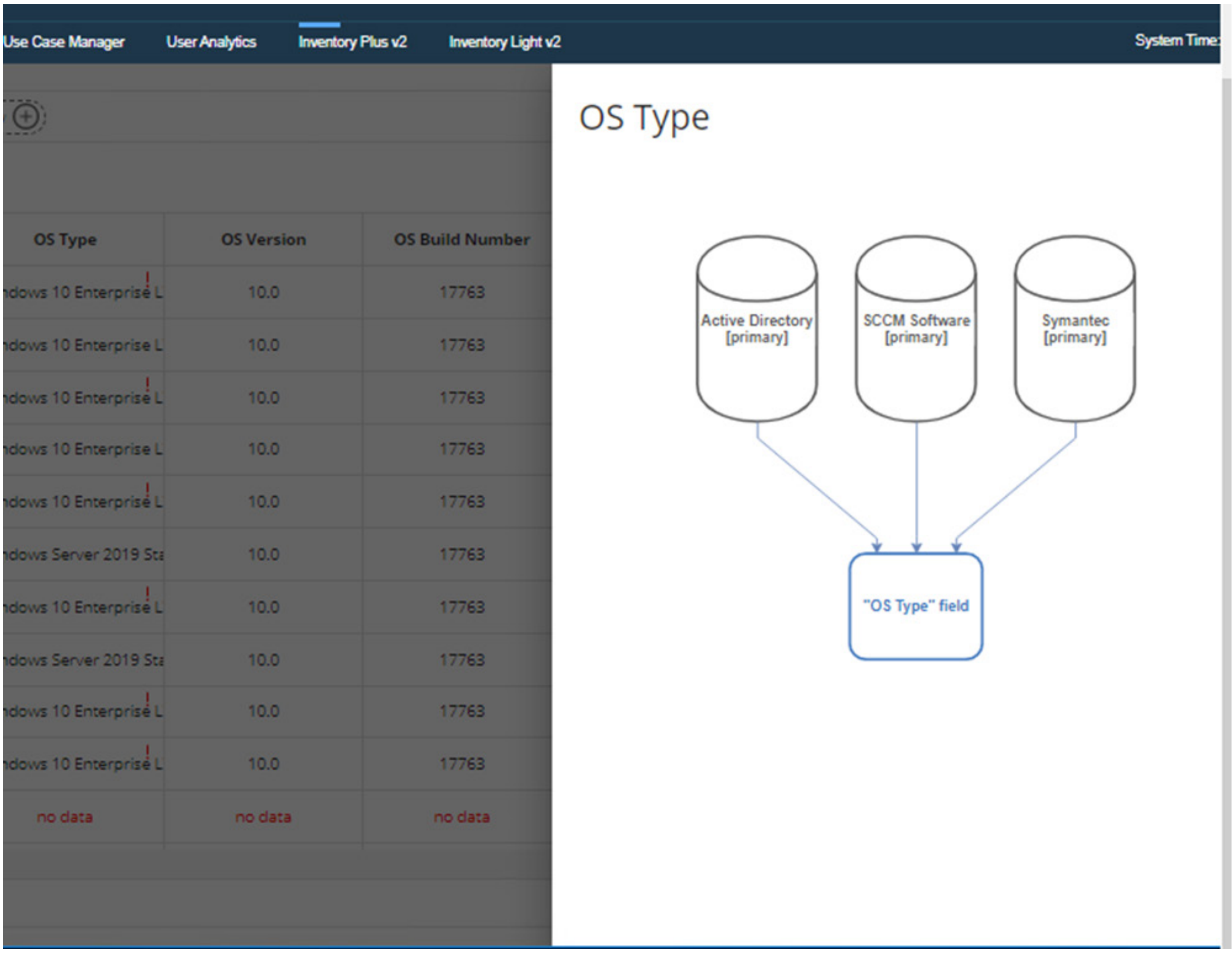

Type

EXT - External servers
PC - Workstations / PCs
MB - Monoblocks
NB - Laptops
TC - Thin clients
TAB - Tablets
MAC - Apple Mac
NET - Network equipment
PRN - Printers / scanners / All-in-One
POS - Payment terminal
CASH - Cash register
SRV - Servers
SRC - Virtual server
SRVA - Server alias
SRDA - The record exists only in DNS
SRVNI - Unidentified server
SRD - Servers currently disabled
IOT.SVN - Video surveillance system
IOT.MON - Monitor or TV with direct connection to the network
IOT.MISC - Other devices / sensors
Unknown - Not specified

Figure 6

The Type column contains the types of devices indicated in the table by abbreviated names. In the Quick Search bar it is possible to search not only shortened names, but also full device type names. What types of devices and shortened names are listed in the Type column is shown in the Figure 6.

Clicking on the icon ⤢ in the upper right corner with the name of the column opens a scheme of the sources of information from which the data the cells of the column is taken. The schemes are generated automatically from the application configuration An example of a scheme of the sources of the Type column is shown in Figure 7.



OS Type	OS Version	OS Build Number
ndows 10 Enterprise L	10.0	17763
ndows 10 Enterprise L	10.0	17763
ndows 10 Enterprise L	10.0	17763
ndows 10 Enterprise L	10.0	17763
ndows 10 Enterprise L	10.0	17763
ndows Server 2019 Sta	10.0	17763
ndows 10 Enterprise L	10.0	17763
ndows Server 2019 Sta	10.0	17763
ndows 10 Enterprise L	10.0	17763
ndows 10 Enterprise L	10.0	17763
no data	no data	no data

OS Type

Figure 7

2.4 Rows

Row is a bunch of cells that contains information corresponding to the column header to which they relate. The row does not have its own name or title. The row contains information pertaining to one system object. The rows can be sorted, selected and grouped. The cell search is performed in the quick search bar or by using the filter function. It is possible to customize the display of rows according to accessibility with special features. Important lines are highlighted in red always and appear first in the list.

2.5 Options Bar

There is an **options bar** in the upper right corner (Figure 8). It contains 6 icons, which can open the next panels:

- Export table data
- Customizer
- Activity
- Templates
- Filters

Each panel can be opened by clicking on the icon. The menu is displayed on the right side of the screen (the popup window for download options is opened next to the icon). The menu could be closed by clicking on any place outside the open panel (to close the popup window for download options it is possible by pressing Esc on the keyboard). The principle of using templates and filters is described in the sections Templates and Filters. Importing and exporting options are described in the section Data Export.

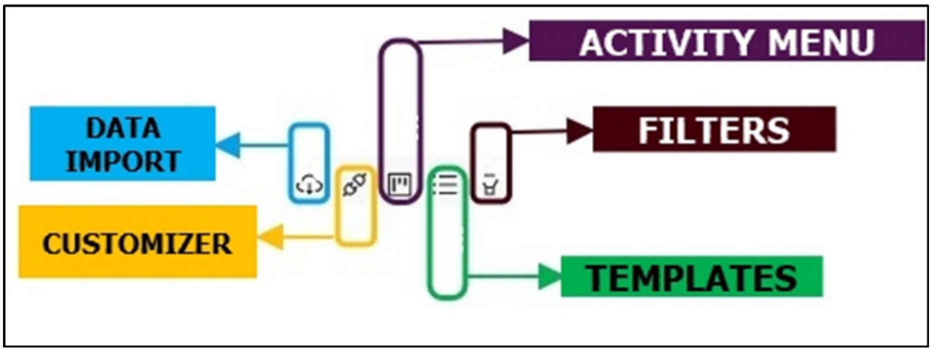


Figure 8

2.6 Search

To provide a search type the needed data in the search bar and press Enter. More detailed search procedure is described in the section Quick Search.

2.7 Filter

There are two ways to set the filter for the Inventory table.

1. Quick filter
   a. Right-click on the necessary **cell**
   b. Select the needed **logic operator** from the popup list
2. Advanced Filter
   a. Open the **filters menu**
   b. Select the **column**, where to apply the filter
   c. Select the **Logic Operator**
   d. Enter the **search value**
   e. Press **ADD FILTER**

2.8 Template

To create a template do the following steps:

1. Open the **template menu**
2. **Add** or **remove** the needed columns (fields) by choosing the v-mark on the left of the column name
3. **Move** the selected field to the needed place by the own columns order
4. Press **LOAD TEMPLATE**
5. Check the table in the tab Assets

For more information about the work with templates go to section Templates.

2.9 Data Export

To download data in JSON of CSV format provide the following steps:

1. Click on the **Export Data Table** menu
2. Choose the **format** to export data to the PC
3. The file is saved to the folder "Downloads"

For more information about exporting data go to the section Data Export.

3. Quick Search

Quick Search allows to look for the needed information in a table without using advanced filters. The quick search bar is located at the upper left corner of the screen and looks like as following 🔍 Search host... . A quick search is performed on a given parameter (words, numbers or dates) in the indexed fields, if a specific column is not selected. Search supports regular expressions. It is needed to press Enter to search. If the combination of letters or numbers does not exist in the table, the search result will be an empty table. If some rows or columns were hidden by the "hidden" special feature, these rows will not appear in search results. If the searched columns do not appear in the current table configuration (according to the applied filters and templates), the application will not display those columns in the search results.

The search can also be performed on additional data sources and not only on the displayed data in the cell. If a cell is marked with an exclamation mark !, both the data displayed in the cell and the data displayed in the popup window will appear in the search results. A more sophisticated and accurate search could be performed using the filter function. There is an option to perform a search with more parameters.

4. Filters

Filters function is placed under the icon ▽ on the options bar in the top right corner of the table. Advanced filters is a complex search with defined parameters, selecting specific items and sorted by specific criteria. This function allows not only finding the needed data, but also hiding unwanted or unnecessary information in the final result.

Compared to the templates function that touches columns, the advanced filters function is primarily used for rows. The advanced filter function can be applied to any template (currently opened, Default Template, All Fields or custom template). When a filter is applied to the table, the application shows, which particular filter is being used (currently activated) in the Activated Filter section. Filters can be saved with templates to a file and downloaded from a saved file.

4.1 Logic Operators

There are several Logic operators in the filter menu that are used to create advanced filters and setting options to find the data in the table. These operators are logical commands for creating search rules. How the Logic operator bar looks like is shown on Figure 9.

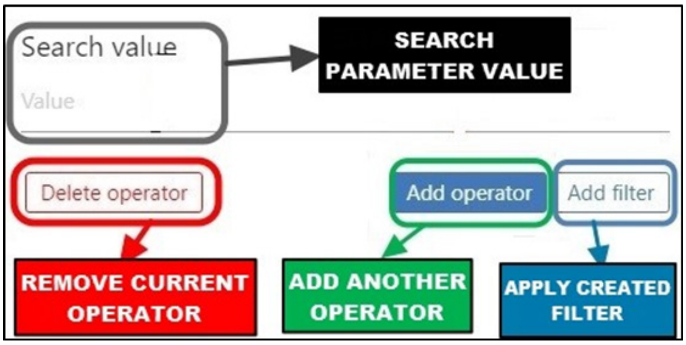
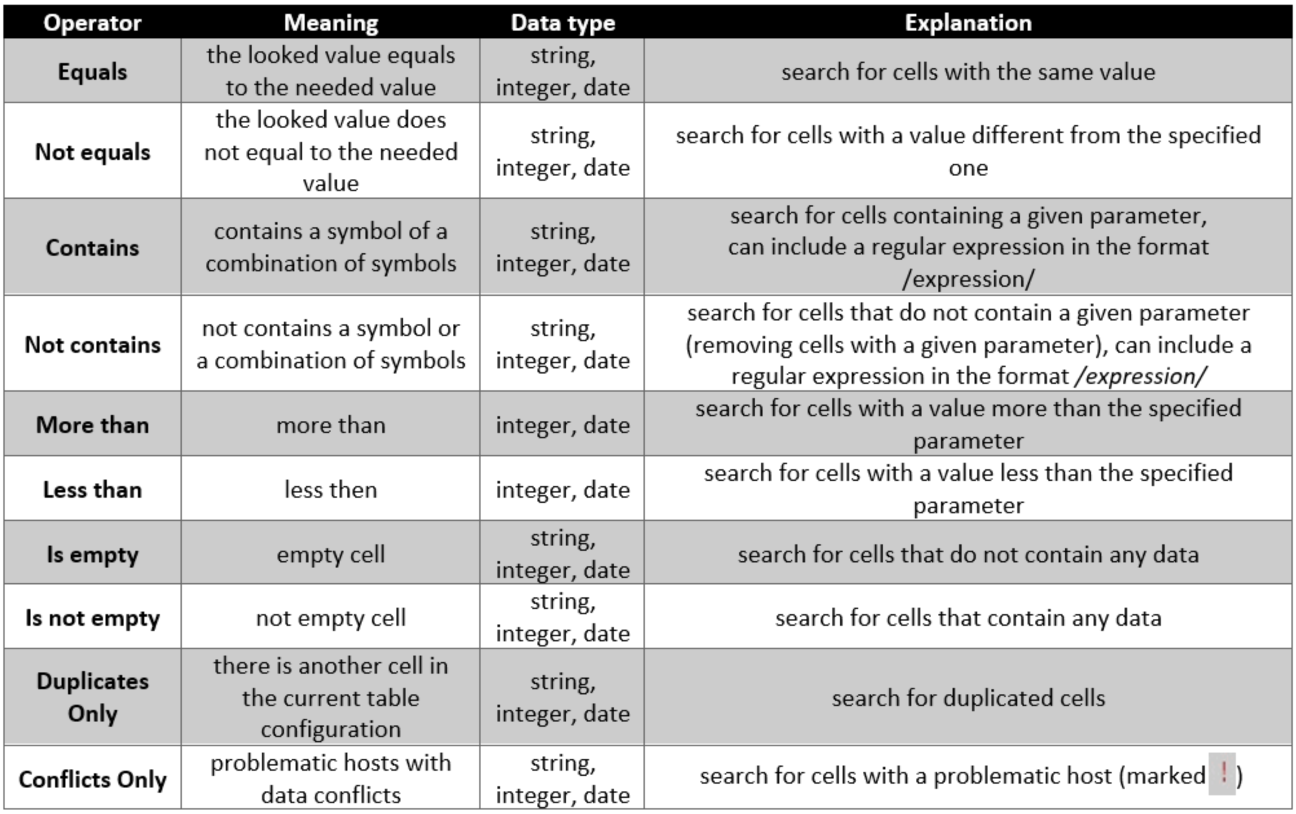


Figure 9

It is possible to add a logical operator through the filter menu when creating your own filter. Parameters are added to the **Search value bar** (for «Duplicates Only», «Conflicts Only», «Is empty» and «Is not empty» operators this field is not displayed). If the user has started adding a logical operator, but wants to cancel the addition, it is possible to use the red button **DELETE OPERATOR** below the line of the specified parameter. In the same way it is possible to delete the added statement in an existing filter while editing. After adding one or more logical operators click on **ADD FILTER** to apply the created filter. Meaning, explanation and usage of Logic operators is explained in Table 2.



Operator	Meaning	Data type	Explanation
Equals	the looked value equals to the needed value	string, integer, date	search for cells with the same value
Not equals	the looked value does not equal to the needed value	string, integer, date	search for cells with a value different from the specified one
Contains	contains a symbol of a combination of symbols	string, integer, date	search for cells containing a given parameter, can include a regular expression in the format /expression/
Not contains	not contains a symbol or a combination of symbols	string, integer, date	search for cells that do not contain a given parameter (removing cells with a given parameter), can include a regular expression in the format */expression/*
More than	more than	integer, date	search for cells with a value more than the specified parameter
Less than	less then	integer, date	search for cells with a value less than the specified parameter
Is empty	empty cell	string, integer, date	search for cells that do not contain any data
Is not empty	not empty cell	string, integer, date	search for cells that contain any data
Duplicates Only	there is another cell in the current table configuration	string, integer, date	search for duplicated cells
Conflicts Only	problematic hosts with data conflicts	string, integer, date	search for cells with a problematic host (marked !)

Table 2

4.2 Activated Filters

Activated Filters section can be found below the quick search bar or in the filter menu. It displays a list of all the filters currently applied to the current table configuration. The list of activated filters includes the name of the column that the filter is applied to, the Logic operator used, the search options and the button **DELETE** for deleting the filter. The structure of Activated Filters section is shown on Figure 10.

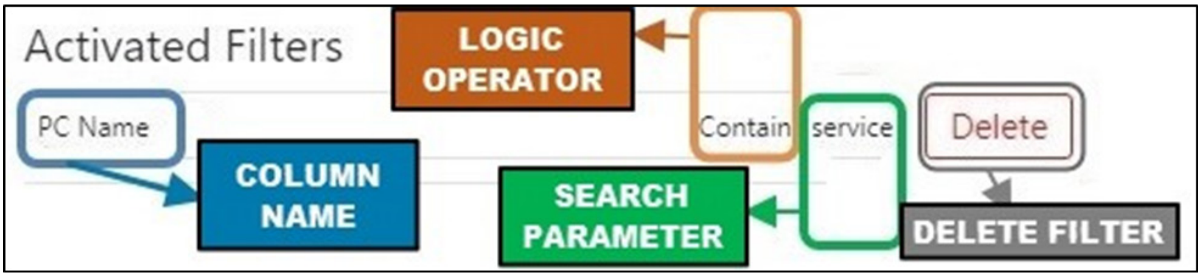


Figure 10

Activated Filters could be **edited**. To edit the activated filter click on the filter in the Activated Filters section in the template menu or directly in the table. After that the settings of the selected filter will be opened. Providing changes is done according to the algorithm of creating custom filter.

4.3 Quick Filters

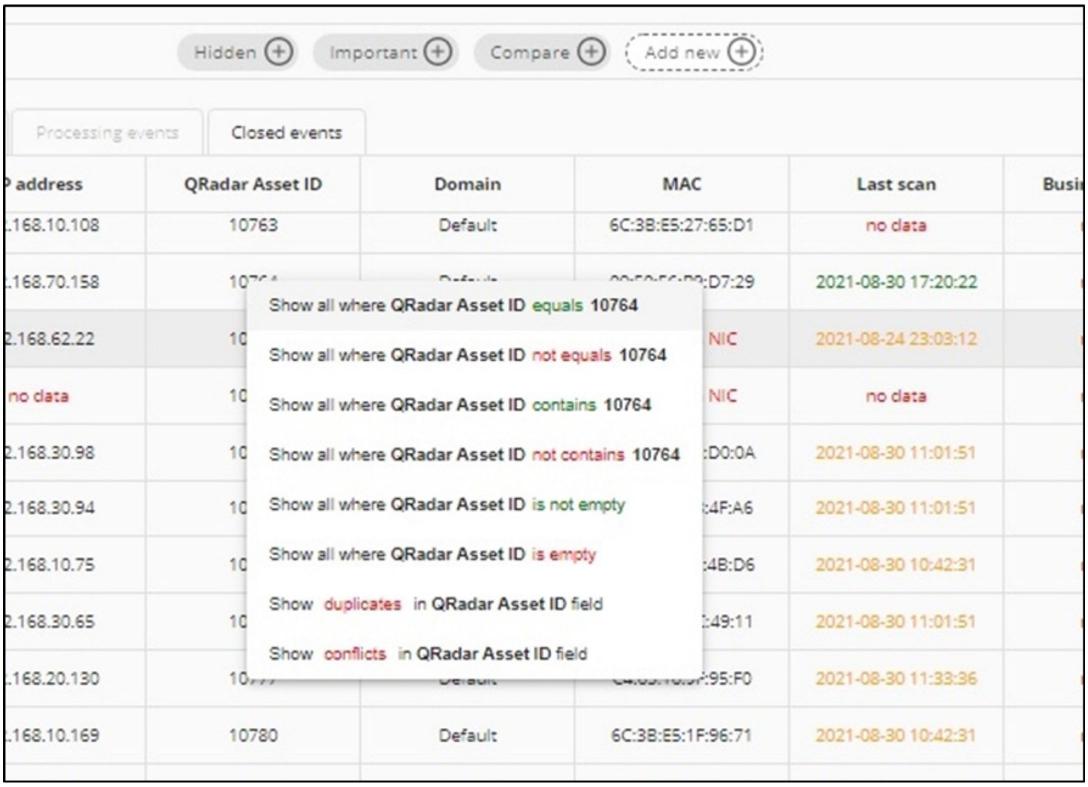
Inventory allows searching information by parameters. To create more complex filters there is a filter menu, but 6 simple filters can be applied directly in the table without opening a menu. To apply quick filter perform right-click on the cell with needed information. A popup window will appear with a list of filters, logic operators and search parameters available for the column that the selected cell belongs to.

There are 8 **quick filters** available:

- **Equals**
- **Not equals**
- **Contains**
- **Not contains**
- **Is not empty**
- **Is empty**
- **Duplicates**
- **Conflicts**

If the selected cell does not contain any information, only three filters ("is empty", "is not empty" and "conflicts") will be available. For some fields a quick duplicates filter cannot be applied. After selecting a quick filter it will appear in the activated filters block. After applying a quick filter it will appear in the activated filters section and could be modified and deleted.

Example of popup window for a quick filter for the column **PC Name** is shown on Figure 11.



P address	QRadar Asset ID	Domain	MAC	Last scan	Busi
.168.10.108	10763	Default	6C:3B:E5:27:65:D1	no data	
.168.70.158	107		:D7:29	2021-08-30 17:20:22	
2.168.62.22	10		NIC	2021-08-24 23:03:12	
no data	10		NIC	no data	
2.168.30.98	10		:D0:0A	2021-08-30 11:01:51	
2.168.30.94	10		:4F:A6	2021-08-30 11:01:51	
2.168.10.75	10		:4B:D6	2021-08-30 10:42:31	
2.168.30.65	10		:49:11	2021-08-30 11:01:51	
.168.20.130	10		:95:F0	2021-08-30 11:33:36	
.168.10.169	10780	Default	6C:3B:E5:1F:96:71	2021-08-30 10:42:31	

Show all where QRadar Asset ID equals 10764
Show all where QRadar Asset ID not equals 10764
Show all where QRadar Asset ID contains 10764
Show all where QRadar Asset ID not contains 10764
Show all where QRadar Asset ID is not empty
Show all where QRadar Asset ID is empty
Show duplicates in QRadar Asset ID field
Show conflicts in QRadar Asset ID field

Figure 11

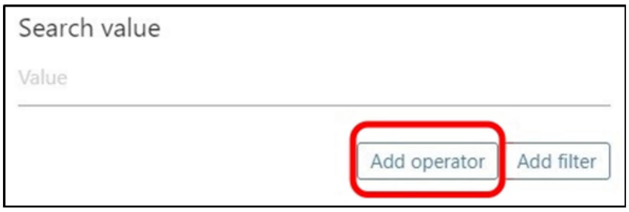
4.4 Custom Filter

Custom Filter is created on basis of saved filters and allows to search needed information and to exclude the unnecessary. It is also possible to create multiple filters for multiple columns of a template and apply them simultaneously. Created filter could be renamed to custom name and will appear next to default saved filters. Creating a custom filter goes as following:

1. Open the **filters menu**
2. Select the needed **column** from the list of Search field
3. Select the **Logic Operators**
4. Set the **search parameters** value in Search value section (search parameter for Date and Time has certain form and tips are listed below the Search Value bar)
5. Click **ADD FILTER** (filter as applied automatically for the opened table configuration and will appear in the section of activated filters)
6. **Add** more filters if needed
7. Select the **template** to which is needed to apply the filter
8. Click **SAVE**

4.5 Multiply Parameters Filter

When a user needs to find specific information that may contain related keywords (e.g. select all rows with the word «server» but exclude rows with «server-nt»), there is an option to use **Multiply Parameters Filter.**



To create such filter it is necessary to create custom filter and to add several Logic operators by clicking the button **ADD OPERATOR** (Figure 12). The second and every next Logic operator is added with the button **ADD OPERATOR**. To apply the filter click **ADD FILTER**.

5. Templates

Templates function is located in the top right corner under the icon ☰ in the options bar. Clicking on this icon opens the template menu. This function sorts and selects columns, disables columns view or displays all columns in a table. Each template with user preferences can be saved and downloaded to a file as well as to be opened previously saved template from a file. The template is applied by clicking on the **LOAD TEMPLATE** button in the bottom right corner below the list of columns in the templates menu.

5.1 Templates Menu

The templates menu consists of several sections and buttons. Each section contains a list of table columns and a view indication. The following sections are available in the template menu:
- **Templates** – all available templates (default and custom)
- **Table View Editor** – displaying of columns
- **New fields** – list of all columns, which are not displayed at the moment

Buttons in the menu are used to work with columns and templates:
- **Import** – downloading from a file
- **Add new fields** – adding and removing columns

☑ – column is displayed be default (impossible to hide)
☑ – column is displayed (possible to hide)
☐ – column is not displayed
■ – non-active column
- **Back** – return to the previous section list
- **Save as** – saving the selected configuration of custom template and adding the name of the template
- **Save** – saving the selected custom template configuration with the name
- **Load template** – display selected columns or creating a custom template
- **Download** – downloading the table to a file

Icon ⠿ means that the column can be moved. In the New Fields section is possible to search for the needed column by name (Figure 13). The search bar is located under the heading New Fields and is operated on the principle of a quick search bar.

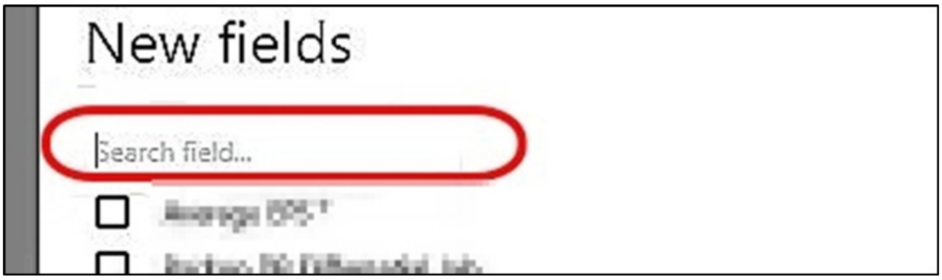


Figure 13

5.2 Saved Templates

There are two saved templates in the application that are used most often and can become the basis for creating custom template. All of them are available to open in the templates section from the template menu.

The algorithm of using saved templates is shown in Table 3.

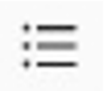
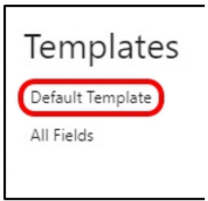
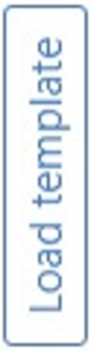
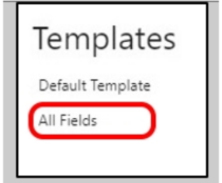
		Algorithm			
Template	**Selected Columns**	Open the templates menu	Select the template	Apply	**Usage**
Default Template	Columns by default				Default template contains the basic set of columns. Could serve as basic template for creating custom templates
All fields	All columns of the table				Choosing all the columns of the table

Table 3

5.3 Custom Template

The user can create, save or export own template if the needed columns in the Default Template selection are not displayed or there are too many columns in the All Fields selection. It is necessary to open the template menu and select one of the saved templates, which will be used as basis to create a custom template.

5.3.1 Create

The procedure of custom template creation goes as following:
1. Open **templates menu**
2. Select one of the existing templates
3. **Add** (New fields section) or **remove** needed columns (added column will move to the list of included columns, removed column will remain in the list of included columns)
4. **Change** the columns order if needed (click and hold the needed column and move it to the needed position)
5. Click **SAVE AS**
6. Enter the **name of the custom template** (the line with the name of chosen as basic template in the bottom part)
7. Click **SAVE**

Custom template is created, saved and available in templates menu. To return to the templates menu is possible by clicking **BACK** in the bottom area of templates section.

5.3.2 Edit

The procedure of custom template goes as following:
1. Open the **templates menu**
2. Click the **name the template**
3. **Remove** unnecessary columns from the section of custom template
4. **Add** needed columns from New fields section
5. **Arrange** the columns in the needed order
6. Click **SAVE AS**
7. Click **SAVE**

Remark: the application has no indication about saving templates, so it is needed to check if the template is saved and applied before completing the procedure.

5.3.3 Delete

The procedure of custom template deleting goes as following:
1. Open the **templates menu**
2. Click the **name of the template**
3. Click **DELETE** below the New Fields section

Remark: he application does not provide any warnings before deleting custom template and it is not possible to restore a deleted template if it has not been saved to a file, so it is recommended to save important custom templates to the file and be careful and confident when deleting.

5.3.4 Export template to file

Downloading a template to a file from the templates menu goes as following:
1. Open the **templates menu**
2. Select the **template**
3. **Change** the file name if needed
4. Press **DOWNLOAD** under the template name
5. Select the **folder** on the PC
6. Press **OK** to download (the template will be downloaded in .json format)

5.3.5 Import template from File

To import a table template from a previously saved .json file is needed to open the templates menu, click **IMPORT**, find the needed file on the PC and open it. Below the Default Template and All Fields templates the custom template will appear.

If the custom template's name is identical to the one, that already exists in the user's table configuration, two templates with the same name will appear in the list of templates. It means, that two templates with the name Default Template could be listed, where one templates will be Saved Templates and the other one with the same name will be custom template. The only difference is, that the custom template could be deleted by clicking **DELETE** button. How to import a table from a downloaded file is shown on Figure 14.

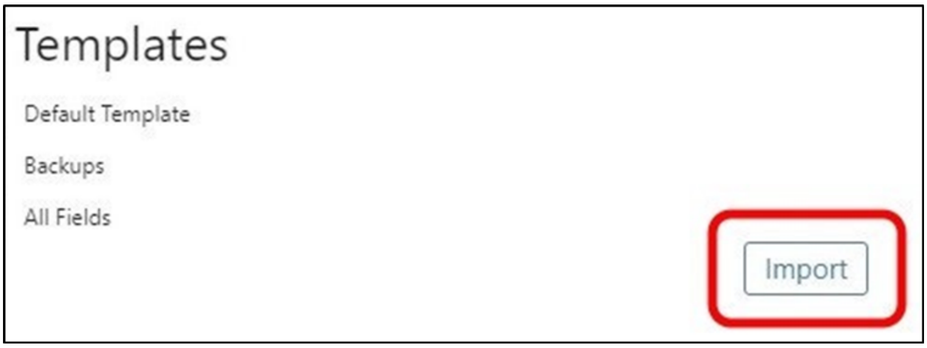
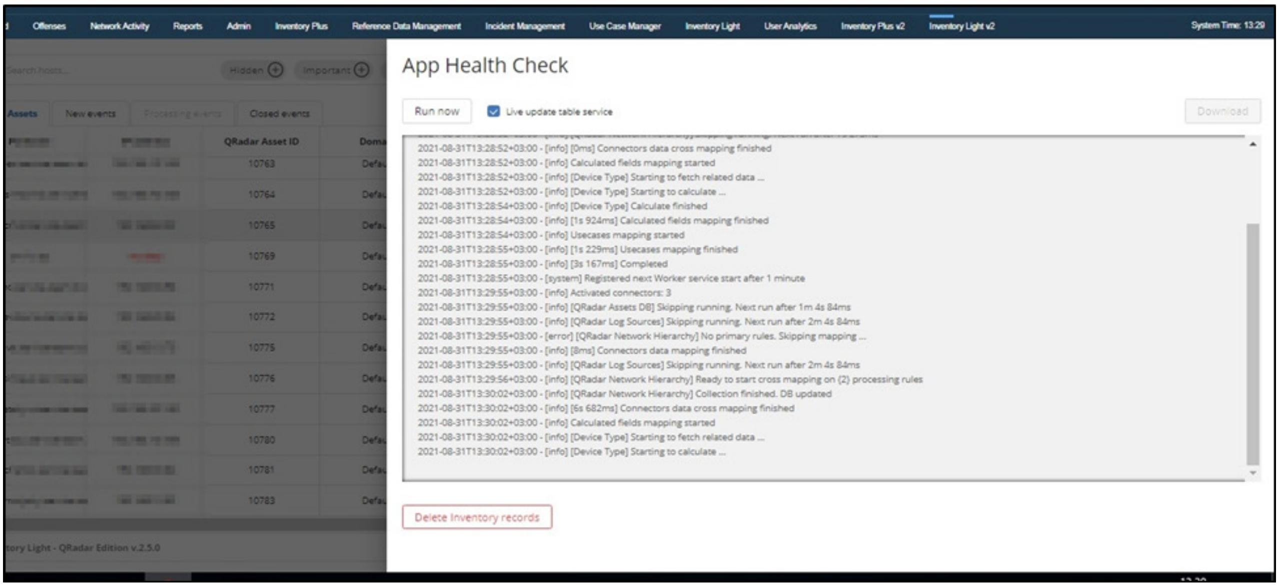


Figure 14

6. Activity Menu

The Activity Menu is located in the settings bar below the icon ▣ and contains the information about the current state of the Inventory, the activity log, and the on and off functions (Figure 15). Below the function field is the Inventory history log, which displays what happened in the application. **The Live update table service** check box means that the data aggregator is running. If unchecked, Inventory will not receive data from external sources.



☑ Live update table service

```
2021-08-31T13:28:52+03:00 - [info] [0ms] Connectors data cross mapping finished
2021-08-31T13:28:52+03:00 - [info] Calculated fields mapping started
2021-08-31T13:28:52+03:00 - [info] [Device Type] Starting to fetch related data ...
2021-08-31T13:28:52+03:00 - [info] [Device Type] Starting to calculate ...
2021-08-31T13:28:54+03:00 - [info] [Device Type] Calculate finished
2021-08-31T13:28:54+03:00 - [info] [1s 924ms] Calculated fields mapping finished
2021-08-31T13:28:54+03:00 - [info] Usecases mapping started
2021-08-31T13:28:55+03:00 - [info] [1s 229ms] Usecases mapping finished
2021-08-31T13:28:55+03:00 - [info] [3s 167ms] Completed
2021-08-31T13:28:55+03:00 - [system] Registered next Worker service start after 1 minute
2021-08-31T13:29:55+03:00 - [info] Activated connectors: 3
2021-08-31T13:29:55+03:00 - [info] [QRadar Assets DB] Skipping running. Next run after 1m 4s 84ms
2021-08-31T13:29:55+03:00 - [info] [QRadar Log Sources] Skipping running. Next run after 2m 4s 84ms
2021-08-31T13:29:55+03:00 - [error] [QRadar Network Hierarchy] No primary rules. Skipping mapping ...
2021-08-31T13:29:55+03:00 - [info] [8ms] Connectors data mapping finished
2021-08-31T13:29:55+03:00 - [info] [QRadar Log Sources] Skipping running. Next run after 2m 4s 84ms
2021-08-31T13:29:56+03:00 - [info] [QRadar Network Hierarchy] Ready to start cross mapping on (2) processing rules
2021-08-31T13:30:02+03:00 - [info] [QRadar Network Hierarchy] Collection finished. DB updated
2021-08-31T13:30:02+03:00 - [info] [6s 682ms] Connectors data cross mapping finished
2021-08-31T13:30:02+03:00 - [info] Calculated fields mapping started
2021-08-31T13:30:02+03:00 - [info] [Device Type] Starting to fetch related data ...
2021-08-31T13:30:02+03:00 - [info] [Device Type] Starting to calculate ...
```

Figure 15

7. Data Export

There is an option for export table data to a separate file. Table is saved and download in formats JSON or CSV and could be opened any time from the saved file.

Export option could be done in formats JSON and CSV from the options bar above the table in right upper corner under the icon ☁ . In order to do this click on the icon and select the desired file format in the popup window (Figure 16). The saved table includes the fields of search results, filters and templates applied. Name of the files consists of the word "Inventory" and date and time of download (e.g. **INVENTORY 06.08.2019, 08_37_38**).

For saving data appropriately in CSV format open the file in MS Excel, select the first column, click "Text to Columns" in the section "Data" and divide the text by commas. It is also possible to download the map of the field name and its ID in the API by clicking Export fields map under the download icon.

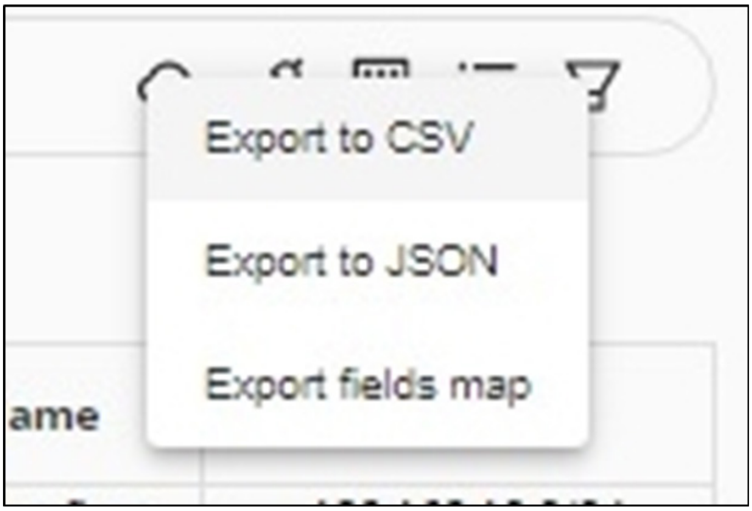


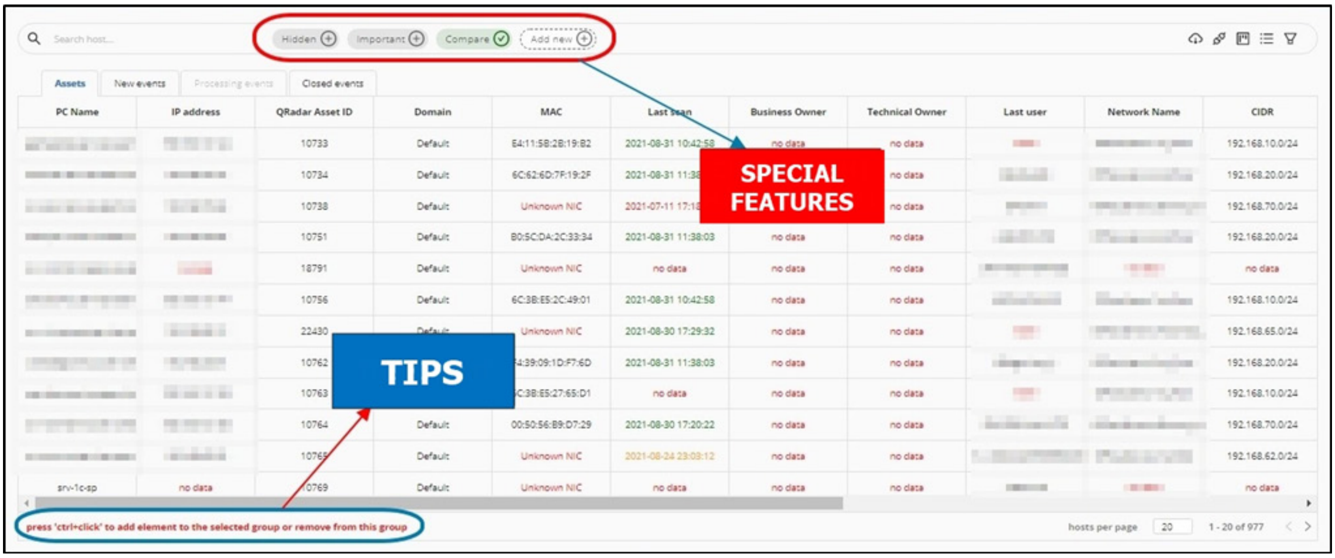
Figure 16

8. Special Features

Special Features are located in the center above the table and aimed to emphasize and hide selected rows of the table. There are three special features options: "Hidden", "Important" and "Compare". When the feature is inactive, it is displayed in black. When a user activates a special feature, that feature is marked in its color. When a user selects a function, the bottom information line gives a hint in red on how to select the desired row and save changes. When a special feature is colored, each selected row will be added to that selected special feature.

Marked with special feature option rows are saved to a separate file with the selected template. Therefore, another user will also see marked or hidden rows when opening a submitted file.

Special features and the information line view is shown on Figure 17.

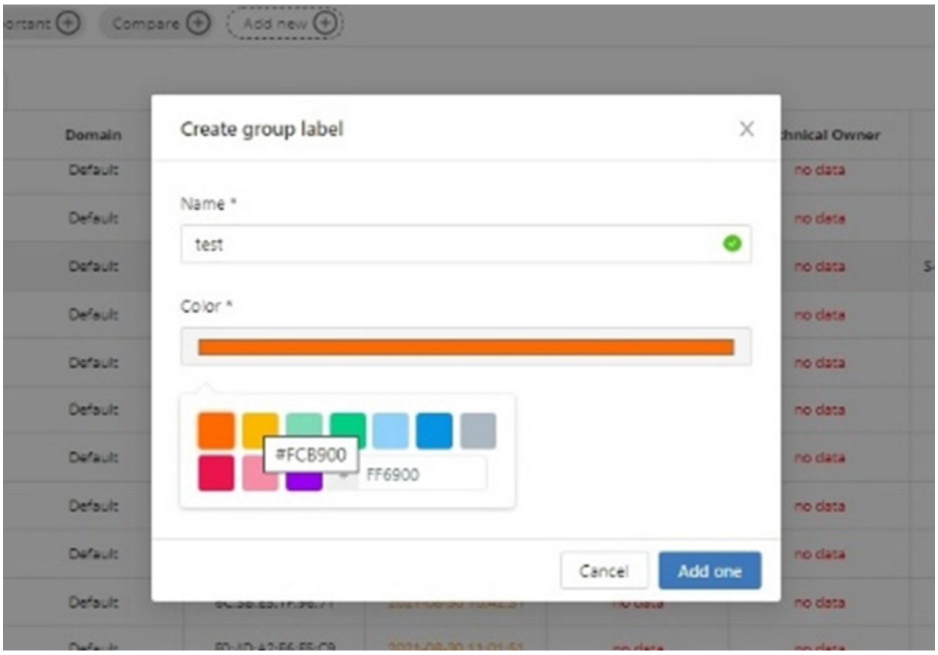


PC Name	IP address	QRadar Asset ID	Domain	MAC	Last scan	Business Owner	Technical Owner	Last user	Network Name	CIDR
[redacted]	[redacted]	10733	Default	E4:11:5B:2B:19:B2	2021-08-31 10:42:58	no data	no data	[redacted]	[redacted]	192.168.10.0/24
[redacted]	[redacted]	10734	Default	6C:62:6D:7F:19:2F	2021-08-31 11:38		no data	[redacted]	[redacted]	192.168.20.0/24
[redacted]	[redacted]	10738	Default	Unknown NIC	2021-07-11 17:18		no data	[redacted]	[redacted]	192.168.70.0/24
[redacted]	[redacted]	10751	Default	B0:5C:DA:2C:33:34	2021-08-31 11:38:03	no data	no data	[redacted]	[redacted]	192.168.20.0/24
[redacted]	[redacted]	18791	Default	Unknown NIC	no data	no data	no data	[redacted]	[redacted]	no data
[redacted]	[redacted]	10756	Default	6C:3B:E5:2C:49:01	2021-08-31 10:42:58	no data	no data	[redacted]	[redacted]	192.168.10.0/24
[redacted]	[redacted]	22430	Default	Unknown NIC	2021-08-30 17:29:32	no data	no data	[redacted]	[redacted]	192.168.65.0/24
[redacted]	[redacted]	10762		4:39:09:1D:F7:6D	2021-08-31 11:38:03	no data	no data	[redacted]	[redacted]	192.168.20.0/24
[redacted]	[redacted]	10763		C:3B:E5:27:65:D1	no data	no data	no data	[redacted]	[redacted]	192.168.10.0/24
[redacted]	[redacted]	10764	Default	00:50:56:B9:D7:29	2021-08-30 17:20:22	no data	no data	[redacted]	[redacted]	192.168.70.0/24
[redacted]	[redacted]	10765	Default	Unknown NIC	2021-08-24 23:03:12	no data	no data	[redacted]	[redacted]	192.168.62.0/24
srv-1c-sp	no data	10769	Default	Unknown NIC	no data	no data	no data	[redacted]	[redacted]	no data

press 'ctrl+click' to add element to the selected group or remove from this group

Figure 17

The application has the ability to create own selection of any color chosen. To create own selection button click on **ADD NEW**, adjust the settings and press **ADD ONE** (Figure 18).



Create group label

Name *

test

Color *

FF6900

Figure 18

It is impossible to mark a row with two special features at the same time. In order to execute this, select one feature, save the selection and then select the other.

The special features and the algorithm for their usage are given in Table 4.

Special Feature	Usage	Color	Algorithm			
			Choose the function	Choose the row	Save	Result (*below the table*)
Hidden	Hiding rows	-	Hidden ⊕	click *CTRL+click* to select or remove the row	Hidden ✓	Changes saved
Important	Marking rows as important *(red-marked rows are displayed first in the current configuration of the table)*	Red	Important ⊕		Important ✓	
Compare	Marking rows to paying attention	Green	Compare ⊕		Compare ✓	
Custom	Own marking	Own color	Add new ⊕		Own color	

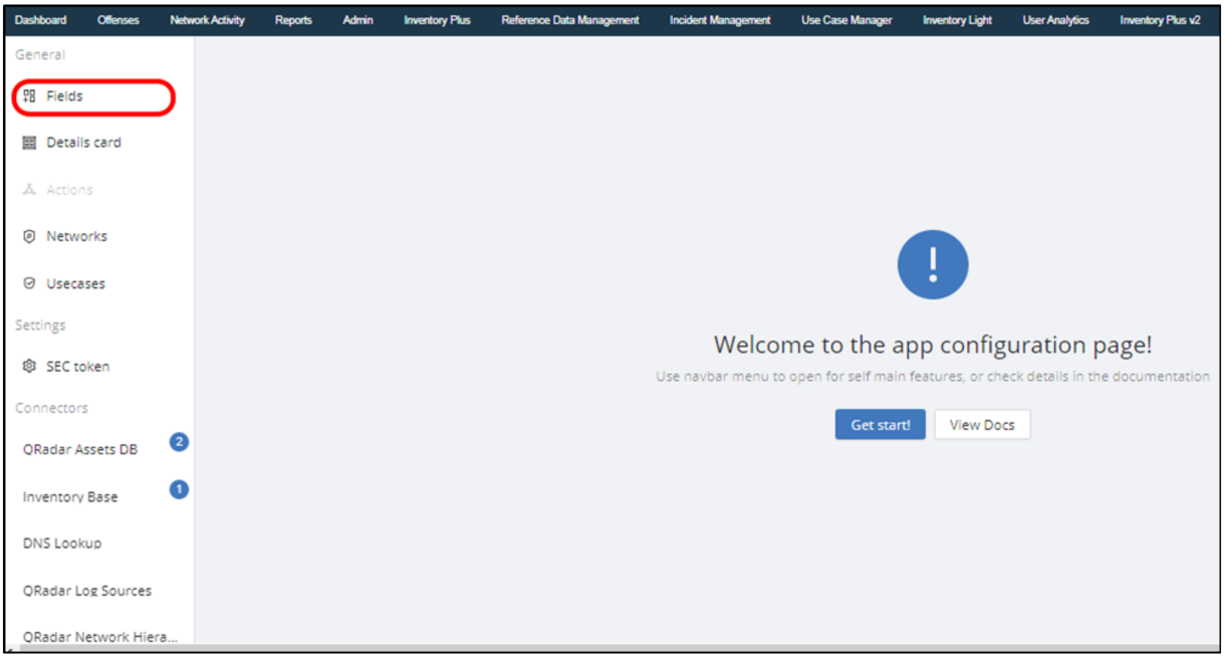
Table 4

9. Administration and Customization

To administrate the application it is needed to log in to the Customizer panel under the icon 🔧. The panel is available to users with Admin and Security Administrator rights and Security Profile: Admin. In the panel it is possible to register fields, configure a detailed view card, configure mechanisms for scanning and identification of network assets, implement Inventory Usecases and configure connectors and field mapping.

9.1 Field Registration

To register new fields and edit existing ones select the item **FIELDS** in the side menu (Figure 19).

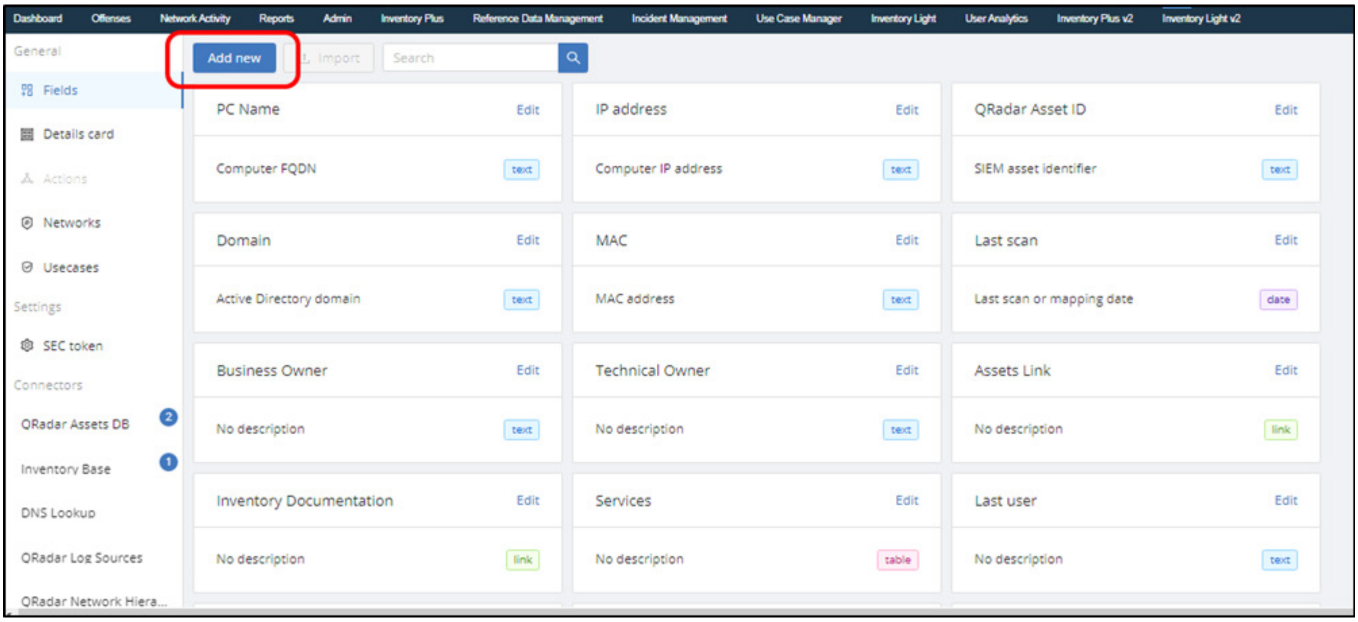


Welcome to the app configuration page!

Use navbar menu to open for self main features, or check details in the documentation

Figure 19

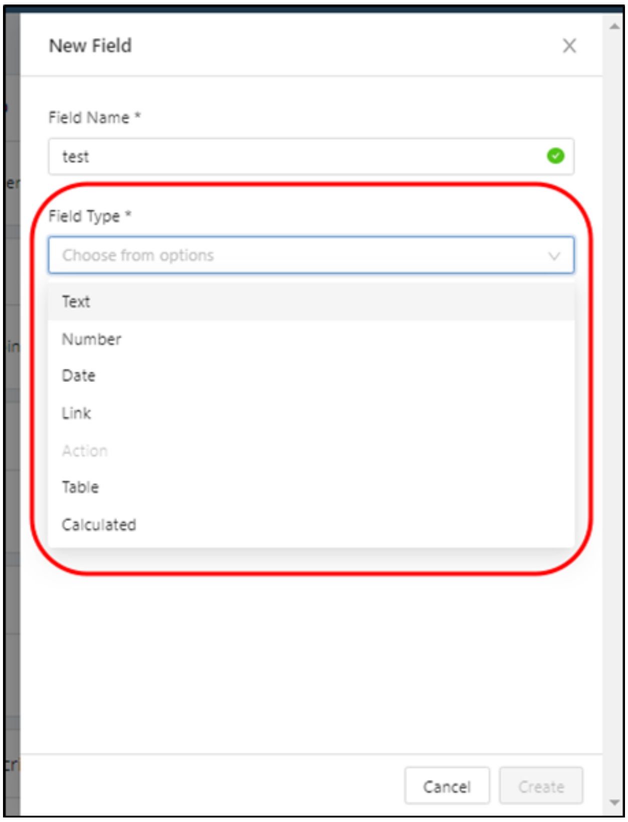
A list of fields already registered in the application will be available on the opening dashboard. Each field has a label that displays its type, as well as a button to edit the interface. Import controls are available at the top of the panel, which allows to import a ready-made field map and search for registered fields. In order to register a new field press **ADD NEW** (Figure 20).



PC Name	Edit	IP address	Edit	QRadar Asset ID	Edit
Computer FQDN	text	Computer IP address	text	SIEM asset identifier	text
Domain	Edit	MAC	Edit	Last scan	Edit
Active Directory domain	text	MAC address	text	Last scan or mapping date	date
Business Owner	Edit	Technical Owner	Edit	Assets Link	Edit
No description	text	No description	text	No description	link
Inventory Documentation	Edit	Services	Edit	Last user	Edit
No description	link	No description	table	No description	text

Figure 20

This will open the interface for creating a new Inventory field in the sidebar. Field Name and Field Type are required (Figure 21). Press CREATE to create a new field.


New Field

Field Name *

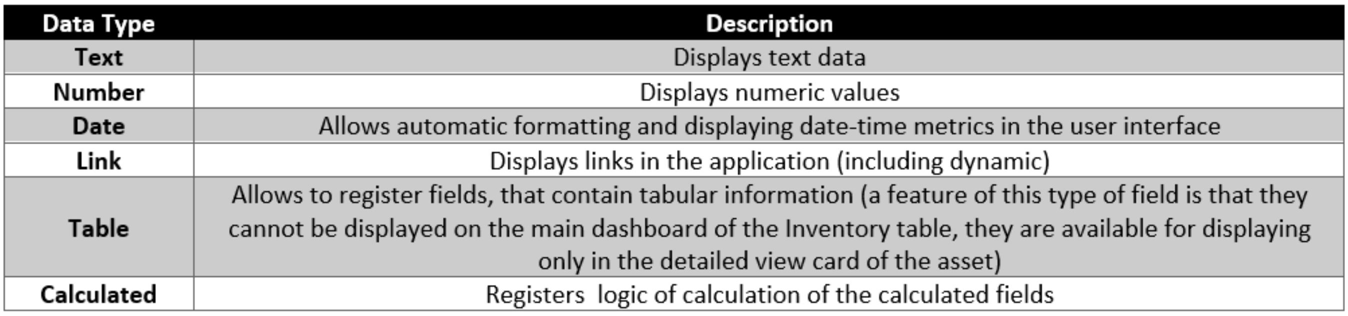
test

Field Type *

Choose from options

Figure 21

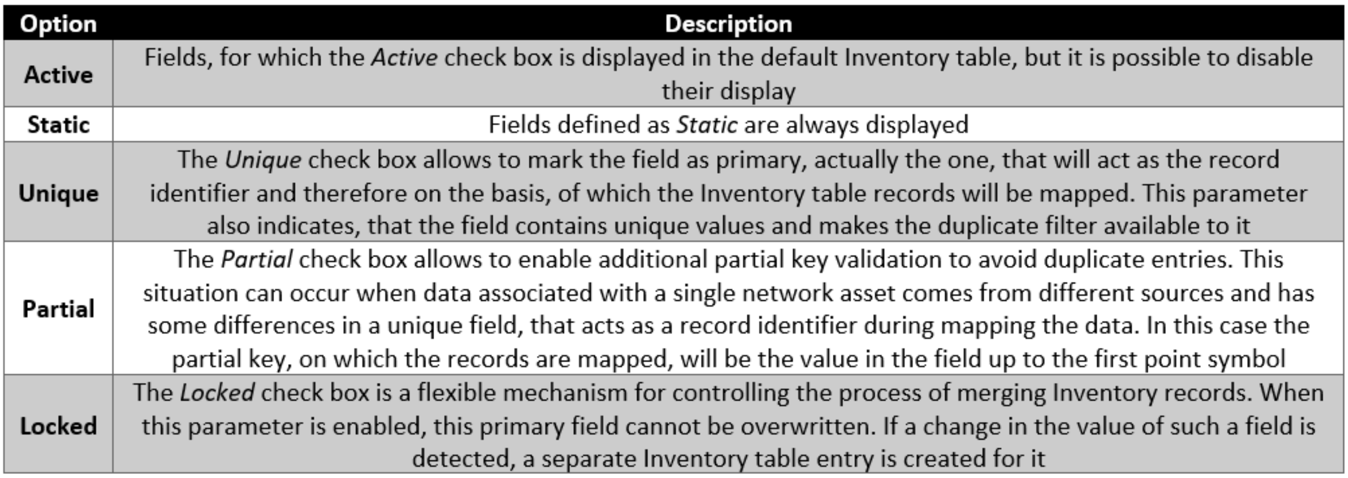
7 types of data are available in the application. Data types and their purpose are described in Table 5.



Data Type	Description
Text	Displays text data
Number	Displays numeric values
Date	Allows automatic formatting and displaying date-time metrics in the user interface
Link	Displays links in the application (including dynamic)
Table	Allows to register fields, that contain tabular information (a feature of this type of field is that they cannot be displayed on the main dashboard of the Inventory table, they are available for displaying only in the detailed view card of the asset)
Calculated	Registers logic of calculation of the calculated fields

Table 5

Additional field configuration options and their descriptions are listed in Table 6.

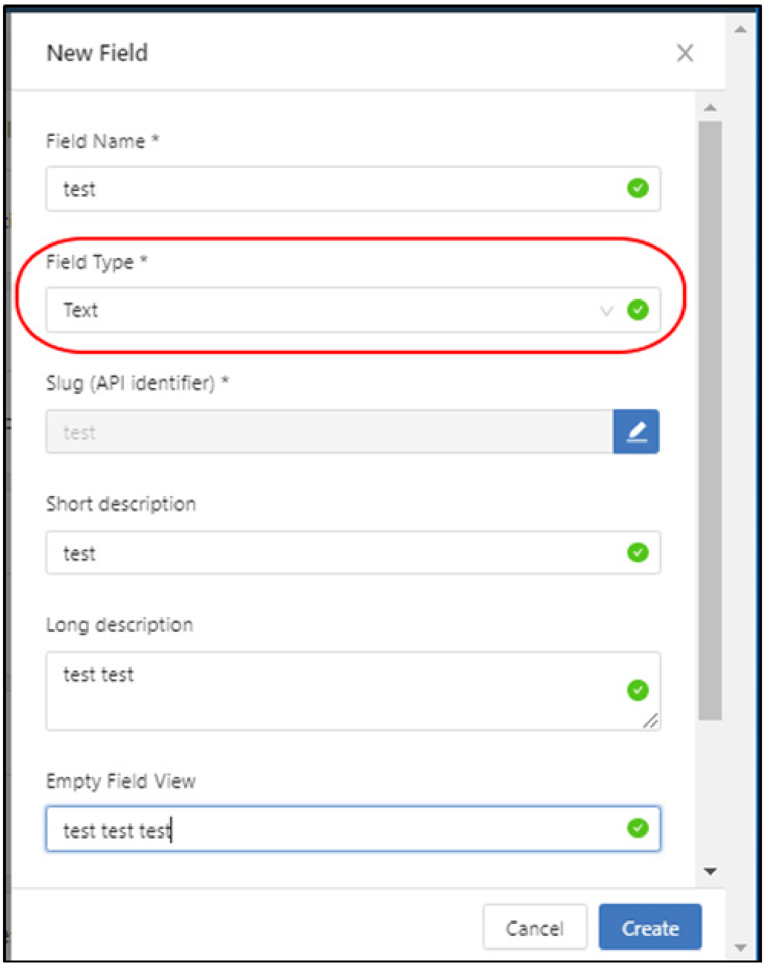


Option	Description
Active	Fields, for which the *Active* check box is displayed in the default Inventory table, but it is possible to disable their display
Static	Fields defined as *Static* are always displayed
Unique	The *Unique* check box allows to mark the field as primary, actually the one, that will act as the record identifier and therefore on the basis, of which the Inventory table records will be mapped. This parameter also indicates, that the field contains unique values and makes the duplicate filter available to it
Partial	The *Partial* check box allows to enable additional partial key validation to avoid duplicate entries. This situation can occur when data associated with a single network asset comes from different sources and has some differences in a unique field, that acts as a record identifier during mapping the data. In this case the partial key, on which the records are mapped, will be the value in the field up to the first point symbol
Locked	The *Locked* check box is a flexible mechanism for controlling the process of merging Inventory records. When this parameter is enabled, this primary field cannot be overwritten. If a change in the value of such a field is detected, a separate Inventory table entry is created for it

Table 6

9.1.1 Data Types Text, Number, Date

For the data types **Text**, **Number** and **Date** among the must-fill parameters is slug – a unique API field identifier (by default, it is generated automatically based on the field name, but can be adjusted if needed). The sidebar and configuration options for the Text, Number, and Date data types are shown on Figure 22.



New Field

Field Name *: test

Field Type *: Text

Slug (API identifier) *: test

Short description: test

Long description: test test

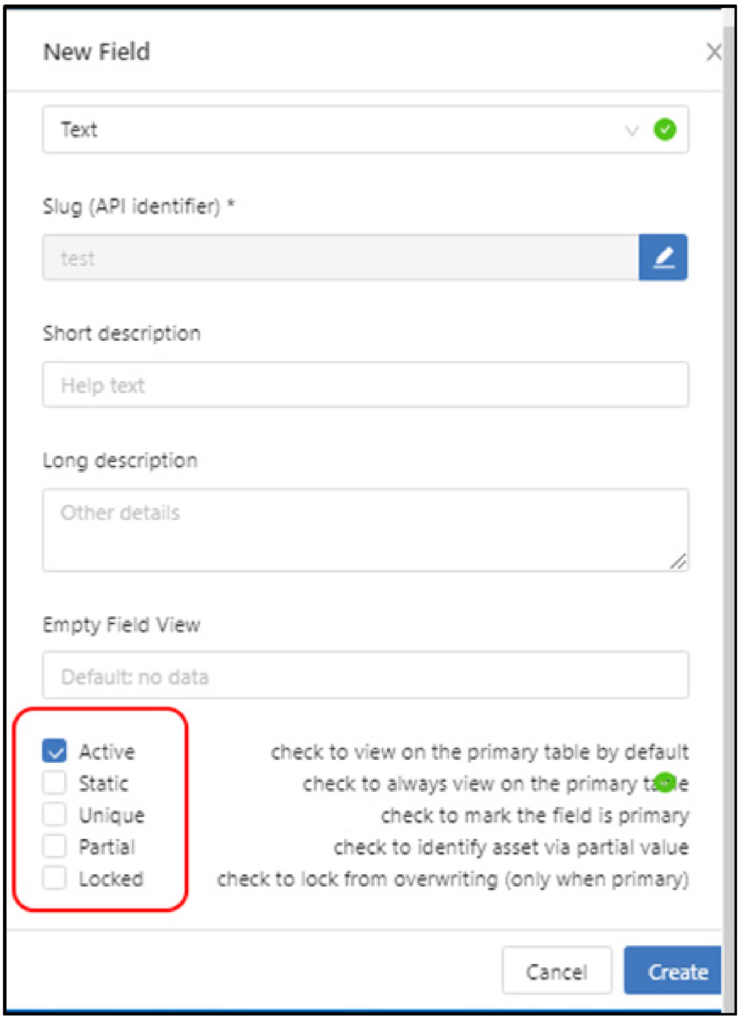
Empty Field View: test test test

Figure 22

Parameters to fill in:

- **Data Type** (necessarily) – a data type with strict typification during the calculation of its value
- **Short description** (optional) – a brief description displayed in the interface assistants
- **Long description** (optional) – detailed specification
- **Empty Field View** (optional) – automatic placeholder displayed when there is no data for the current field in a specific record (default value is no data)

A number of additional options are also available when setting up the field (Figure 23).



New Field

Text

Slug (API identifier) *

test

Short description

Help text

Long description

Other details

Empty Field View

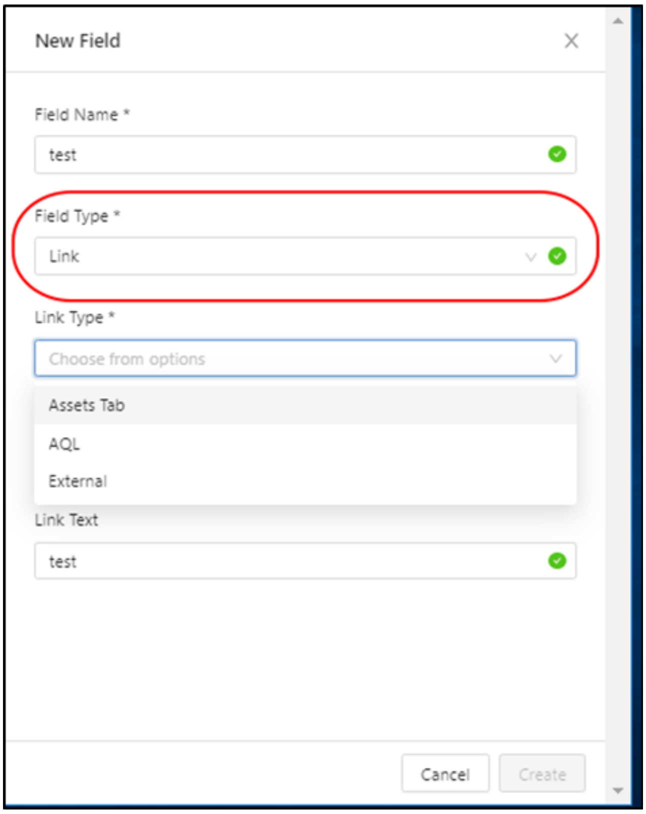
Default: no data

☑ Active — check to view on the primary table by default
□ Static — check to always view on the primary table
□ Unique — check to mark the field is primary
□ Partial — check to identify asset via partial value
□ Locked — check to lock from overwriting (only when primary)

Figure 23

9.1.2 Data Type Link

The Link data type is intended to display links in the application (Figure 24).



New Field

Field Name *: test

Field Type *: Link

Link Type *: Choose from options

Assets Tab
AQL
External

Link Text: test

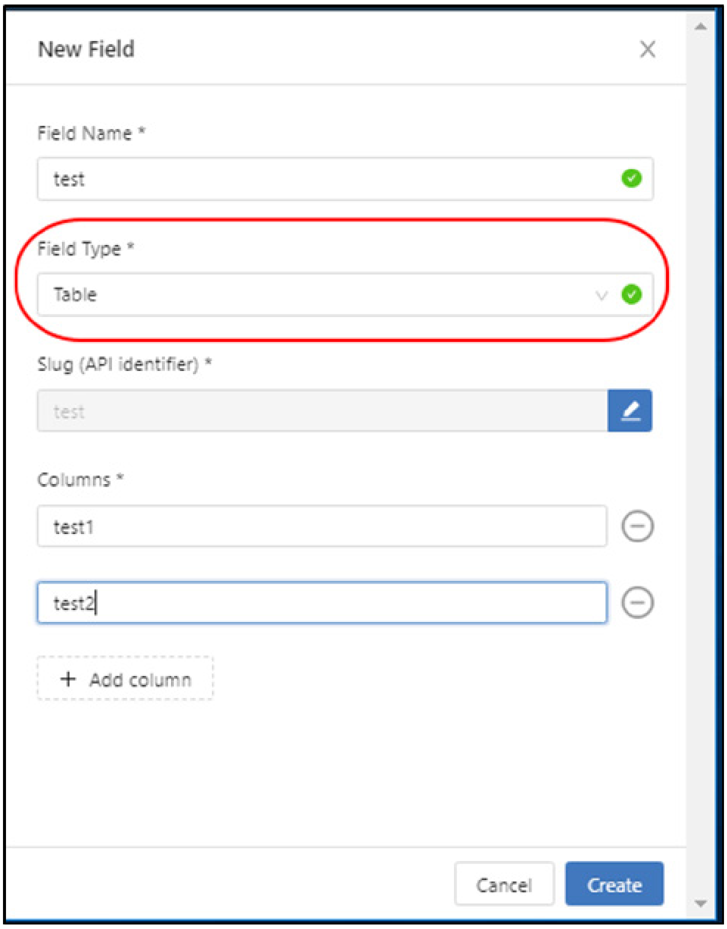
Figure 24

3 types of links are available by default:
- **Assets tab** (allows immediate switch to the Asset tab in the QRadar system)
- **AQL link** (allows executing an AQL query directly from the application and immediately open its result in the Log Activity tab)
- **External** (external URL allows to specify a link to any external resource)

Parameters to fill in:
- **Link Text** (optional) – a text to be displayed on the link (field name is displayed by default)
- **Link Value** (necessarily) – link payload (in case of an External link the full resource URL is specified. In case of AQL link the field specifies an AQL query is displayed where the possibility of dynamic templates is supported)

9.1.3 Data Type Table

The Table data type allows to create fields, that contain tabular information. At registration it is necessary to specify slug (unique API field identifier) and also to define in the constructor a column of the table which will be displayed in the user interface. The Table data type configuration panel is shown on Figure 25.



New Field

Field Name *
test

Field Type *
Table

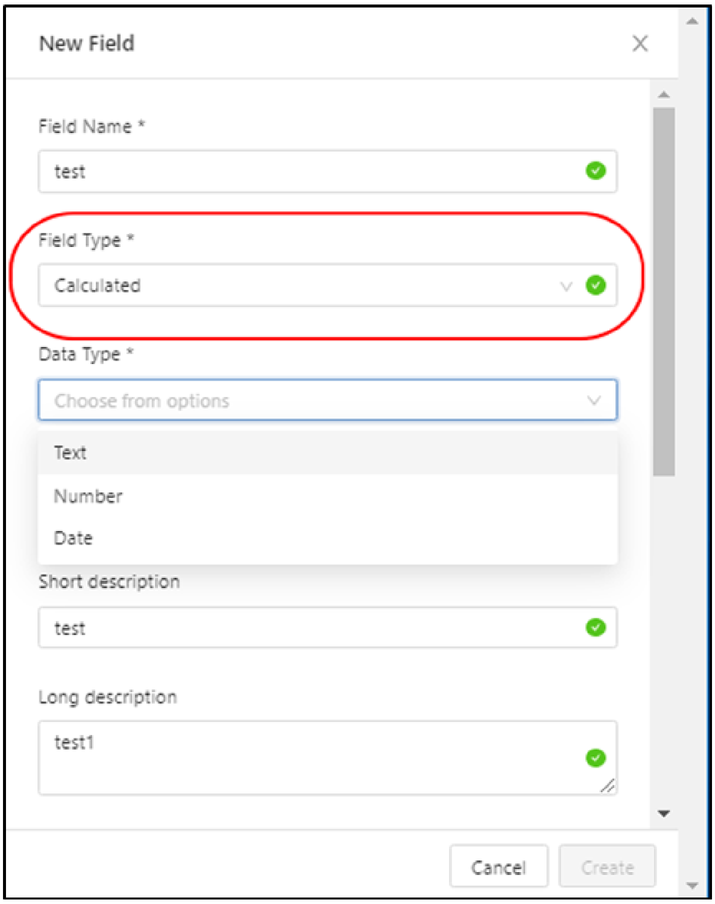
Slug (API identifier) *
test

Columns *
test1
test2

Figure 25

9.1.4 Data Type Calculated

The most interesting from the point of view of flexibility of adjustment are fields with data type Calculated (Figure 26).



New Field

Field Name *: test

Field Type *: Calculated

Data Type *: Choose from options

Short description: test

Long description: test1

Figure 26

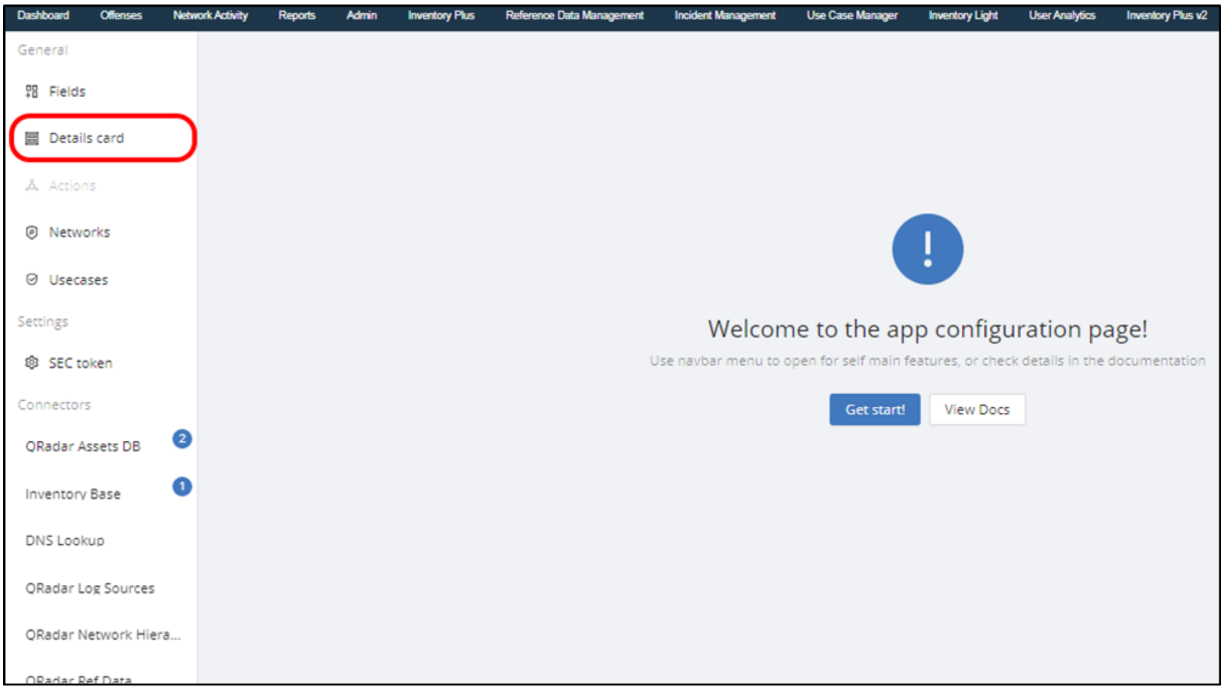
This type of data is intended to register and specify the logic of calculation of calculated fields. It is needed to enter a slug – a unique API field identifier (filled in automatically but can be adjusted if necessary).

Parameters to fill in:
- **Data Type** (necessarily) – a data type with strict typification during the calculation of its value
- **Short description** (optional) – a brief description displayed in the interface assistants
- **Long description** (optional) – detailed specification
- **Empty Field View** (optional) – automatic placeholder displayed when there is no data for the current field in a specific record (default value is no data)
- **Calculation logic** (all fields selected in the Fields parameter are presented as arguments to the input of this calculation function and can be used to calculate the final value of the current field)

The function template is formed automatically. It is needed to specify the logic for calculating the value, that will be returned by the function after the return command. The description of instructions is performed in the JavaScript programming language. This allows the declaration and use of any external functions as well as third-party npm modules pre-imported into the application through the import functionality in the Connectors block, which is described in **6.5 Connectors and Mapping.**

9.2 Detailed View Card

Not all registered fields are available for display in the main Inventory table in the form of columns. Data types such as links and tables are available only in the panel **Detailed View Card**. In order to go to the constructor of the detailed view card it is needed to open the admin panel of the application and press the tab **DETAILS CARD** in General section (Figure 27).



Welcome to the app configuration page!

Use navbar menu to open for self main features, or check details in the documentation

Figure 27

A detailed preview card constructor will be available on the opening dashboard, which allows to configure the output of various information and group it into logical blocks (Figure 28).

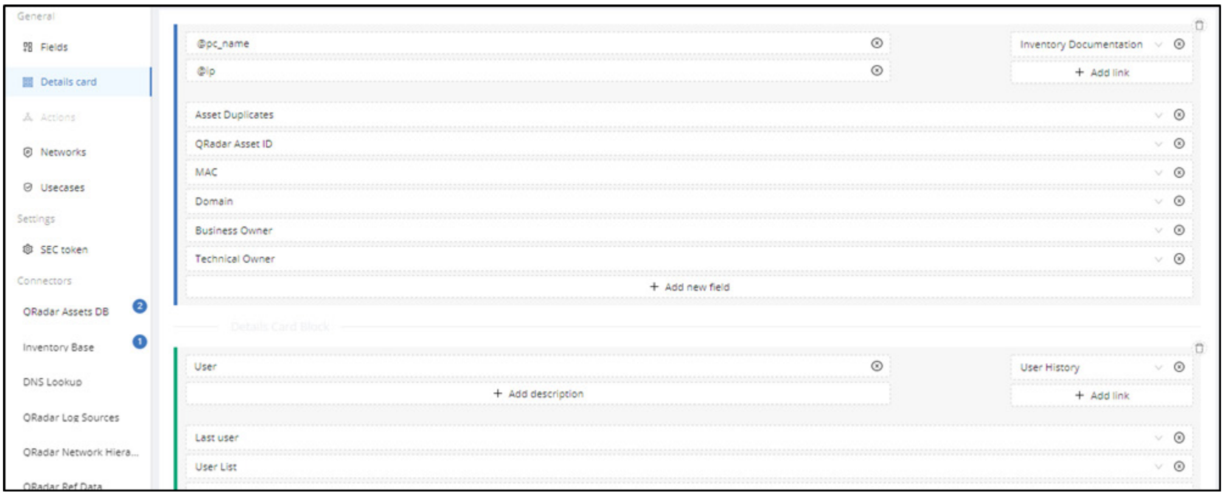


Figure 28

To add a new block click the control at the bottom of the panel. It is possible to specify a block name and a brief description while supporting the ability to render dynamic templates. To insert a dynamic parameter enter the @ symbol. The application will automatically pull up the recommended list of all available fields. In the right part of the block there is an area for displaying links. The area below allows to add an unlimited number of fields to display in the current block including those with a tabular type.

It is possible to use the controls to delete an unnecessary field or block. To save the detailed view tab settings click the Save button at the bottom of the panel. Going to the main dashboard of the application and opening the detail view panel for any of the inventory table entries, it is possible to see, that all the necessary information is rendered for the current asset according to the structure of the scheme built in the detailed menu constructor. links and tabular fields.

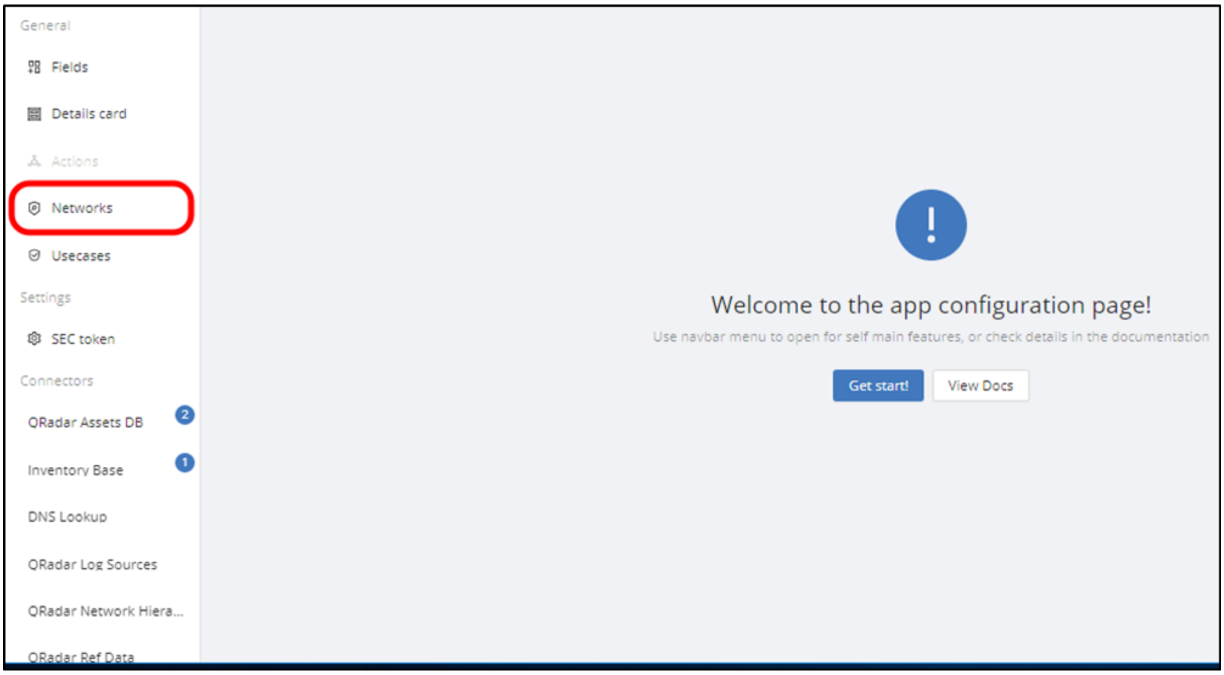
To create a detailed view card after its configuration click **CREATE**.

9.3 Scanning and Identification of Network Assets

One of the advantages of Inventory is the presence of built-in and accessible «out of the box» network scanning mechanisms and active discovery tools, which allows to scan individual endpoints and subnets and combine data on all detected network assets immediately after installing the application without having to wait for third-party connectors and configuration field mapping. Thus, immediately after installing the application, it is possible to add several subnets for scanning and even at this stage to get the initial entries in the Inventory table for network assets, which were identified during the scanning process. The toolkit is used as a scanning module in the application **NMap**.

To open the scan panel open the admin panel of the application and press on the tab **NETWORKS** of the General section (Figure 29).

This functionality is available **in a full version only** (Inventory Plus). In Inventory for QRadar editing of configured scan profiles is available.

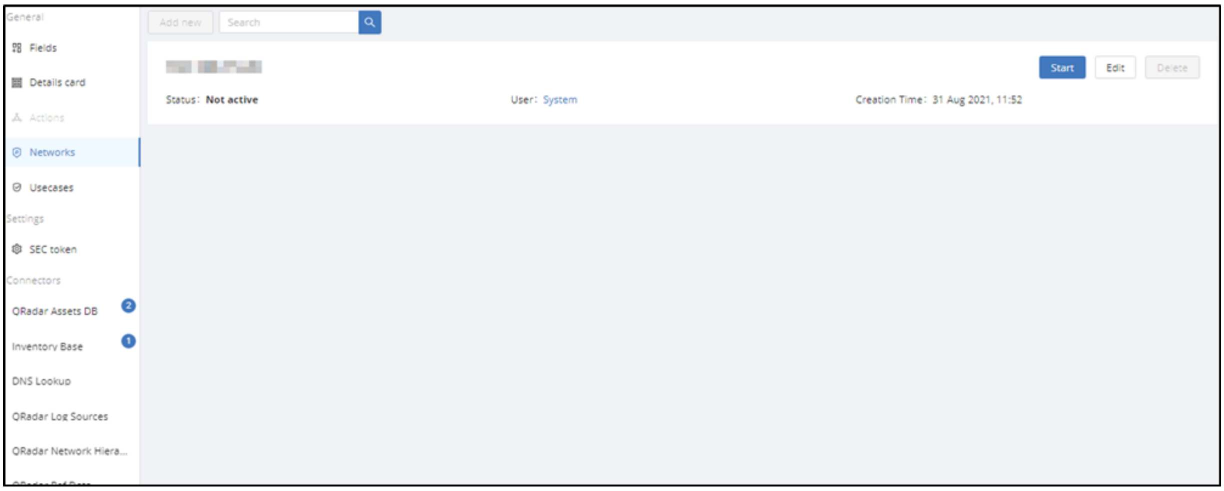


Welcome to the app configuration page!

Use navbar menu to open for self main features, or check details in the documentation

Figure 29

At the top of the panel search controls for registered scan profiles and adding a new one are available (Figure 30).

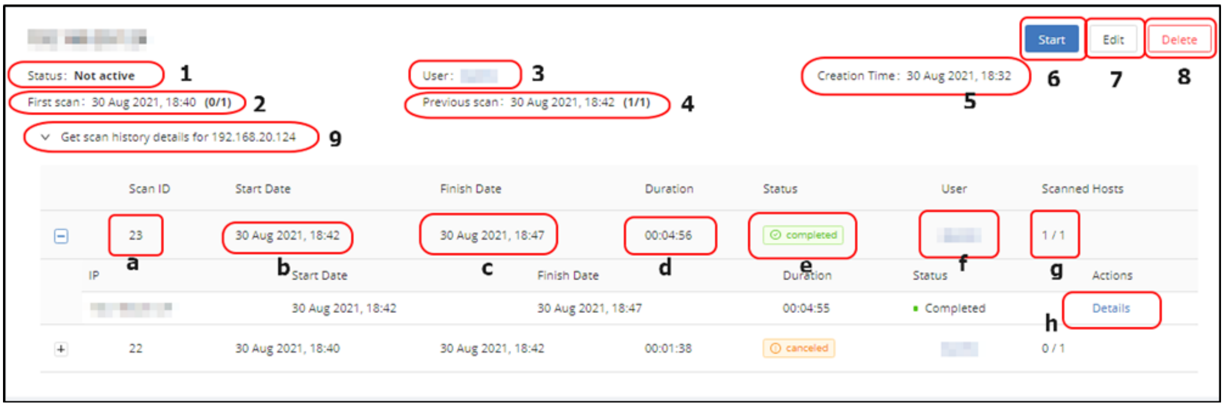


[redacted]

Status: **Not active**   User: System   Creation Time: 31 Aug 2021, 11:52

Figure 30

The scan profile panels and its fields are shown on Figure 31 and detailed below.



[redacted]

Status: **Not active**   User: [redacted]   Creation Time: 30 Aug 2021, 18:32

First scan: 30 Aug 2021, 18:40 **(0/1)**   Previous scan: 30 Aug 2021, 18:42 **(1/1)**

Get scan history details for 192.168.20.124

	Scan ID	Start Date	Finish Date	Duration	Status	User	Scanned Hosts
⊟	23	30 Aug 2021, 18:42	30 Aug 2021, 18:47	00:04:56	completed	[redacted]	1 / 1
+	22	30 Aug 2021, 18:40	30 Aug 2021, 18:42	00:01:38	canceled	[redacted]	0 / 1

IP	Start Date	Finish Date	Duration	Status	Actions
[redacted]	30 Aug 2021, 18:42	30 Aug 2021, 18:47	00:04:55	● Completed	Details

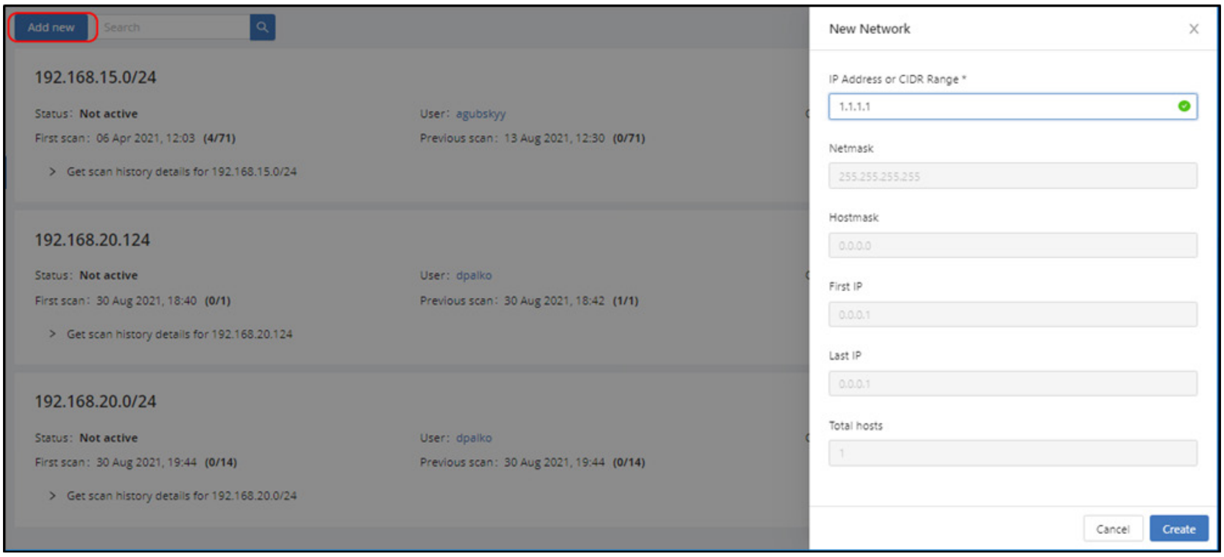
Figure 31

1. Current status
2. Date and time of the first scan with the number of scanned hosts
3. User, who performed the operation
4. Date and time of the last scan with the number of scanned hosts
5. Date and time of the last scan profile modification
6. Start scanning
7. Edit the configuration of scan profile
8. Delete the scan profile
9. Scan history (detailed information about the scanning)
    a. Scan ID
    b. Scan start date
    c. Scan finish date
    d. Scan duration
    e. Current status
    f. User, who started the scan
    g. Number of scanned hosts

h. Details about scanning
    i. Information about all scanned hosts
    ii. Current status of scan task
    iii. View of results for a completed scan, where it is possible to get basic information about the host and identified services.

All the information is available and updated in real time. The scanning process is optimized and does not create a load on system resources. Even during the scanning of large networks with a large number of identified hosts scan tasks are registered and queued. The scanning module processes them alternately in small groups with a limit on the number of active scanning tasks, which provides optimal speed and optimization of the use of system resources. If necessary it is possible to stop scan tasks or cancel the entire scan completely.

To register a new profile click **ADD NEW** and enter a subnet with the specified mask or a separate endpoint for scanning (Figure 32).



192.168.15.0/24

Status: **Not active**
User: agubskyy
First scan: 06 Apr 2021, 12:03 **(4/71)**
Previous scan: 13 Aug 2021, 12:30 **(0/71)**
> Get scan history details for 192.168.15.0/24

192.168.20.124

Status: **Not active**
User: dpalko
First scan: 30 Aug 2021, 18:40 **(0/1)**
Previous scan: 30 Aug 2021, 18:42 **(1/1)**
> Get scan history details for 192.168.20.124

192.168.20.0/24

Status: **Not active**
User: dpalko
First scan: 30 Aug 2021, 19:44 **(0/14)**
Previous scan: 30 Aug 2021, 19:44 **(0/14)**
> Get scan history details for 192.168.20.0/24

New Network

IP Address or CIDR Range *: 1.1.1.1
Netmask: 255.255.255.255
Hostmask: 0.0.0.0
First IP: 0.0.0.1
Last IP: 0.0.0.1
Total hosts: 1

Figure 32

To add a scan profile after configuration press **CREATE**.

It should also be noted, that the application contains a built-in connector for processing the results of scans called **Inventory Base**. It does not require additional parameters for configuration and allows immediate obtaining all identified as a result of the scanning module unique records of network assets. The process of configuring this connector is not different from others and is reduced to mapping the fields of identified hosts to the fields of the Inventory table. For more information on how to configure connectors see the section 6.5 Connectors and Mapping.

9.4 Inventory Usecases

An Inventory usecase (INV UC) is a control (i.e., status check) that is based only on configuration information on assets, that are loaded into the Inventory from external sources. Control status is calculated each time data is updated in Inventory for each Inventory table entry. This functionality is available in a **full version only** (Inventory Plus). In Inventory for QRadar editing of Inventory usecases is available.

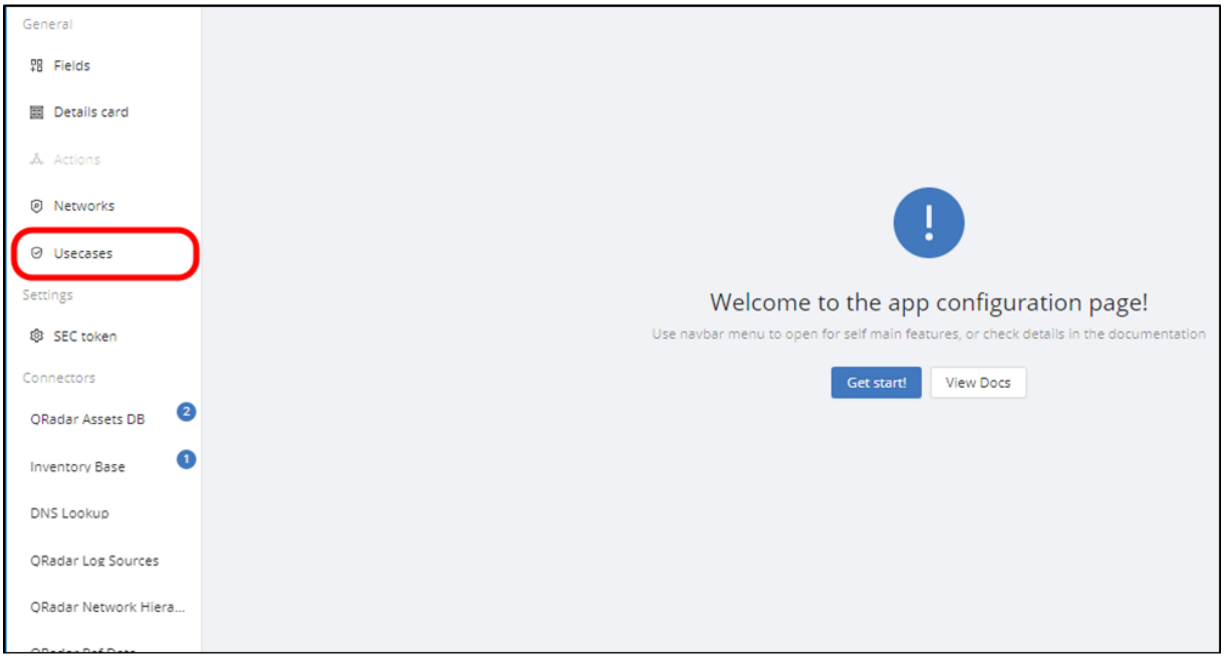
If the record falls under the logic of the detection rules described in the Inventory usecase, a new event is formed for it or the detection is recorded in an existing one if there is an active event at the moment of this asset.

Inventory for QRadar usage scenarios are in fact inventory usecase, that detect violation and anomalies in network objects based on Inventory data. It is possible to create inventory usecase for each infrastructure as needed, but there are several basic scenarios, that are relevant for each infrastructure. Basic inventory cases are listed and described in Table 7.

Usecase Name	Description	Severity	Logic
INV-UC-01 Network is not defined	This rule detects assets that haven't a network assigned from the QRadar Network Hierarchy	Low	• IP Address is not empty • CIDR is empty
INV-UC-02 Log Source does not exist	This rule detects assets that have no one an attached log source	Medium	• QRadar Asset ID is not empty • Last Event is empty
INV-UC-03 Log Source status is ERROR	This rule detects assets that have no events for a certain time range and their status is ERROR	High	• Log Source Status equals ERROR
INV-UC-04 PC Name Duplicates	This rule detects assets that have the same PC Name value. Additionally, the Inventory Light has its own policies to detect and merge duplicate assets, but in some cases, this rule can be useful	Low	• PC duplicates only
INV-UC-05 IP Duplicates	This rule detects assets that have the same IP address	Low	• IP Address duplicates only
INV-UC-06 MAC Duplicates	This rule detects assets that have the same MAC address	Low	• MAC duplicates only

Table 7

In order to go to the registration panel of Inventory usecases to open the admin panel of the application and press on the tab **USECASES** of the General section (Figure 33).

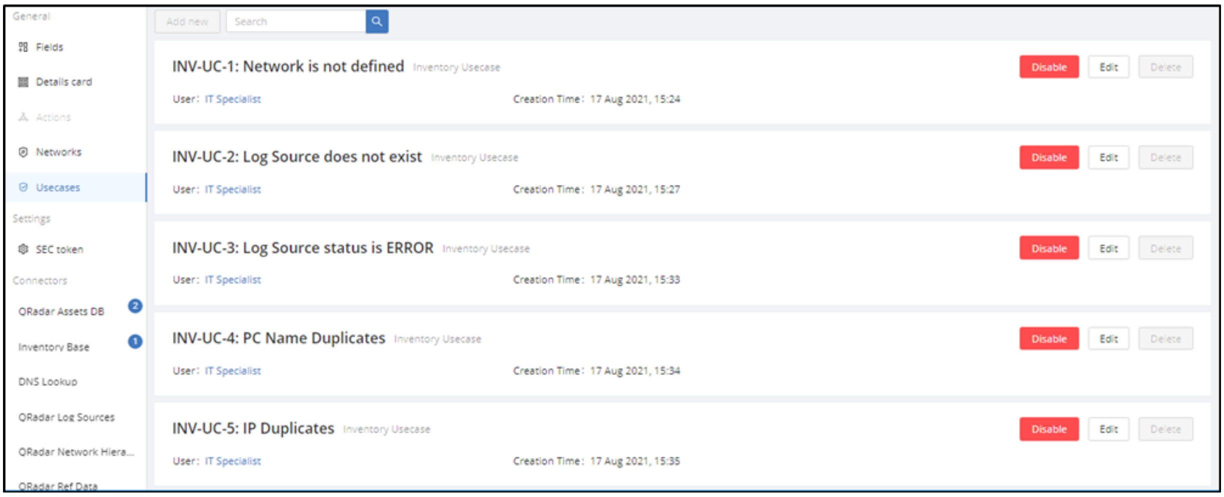


Welcome to the app configuration page!

Use navbar menu to open for self main features, or check details in the documentation

Figure 33

At the top of the panel it is possible to search for registered usecases and add new ones (Figure 34).



INV-UC-1: Network is not defined Inventory Usecase
User: IT Specialist Creation Time: 17 Aug 2021, 15:24

INV-UC-2: Log Source does not exist Inventory Usecase
User: IT Specialist Creation Time: 17 Aug 2021, 15:27

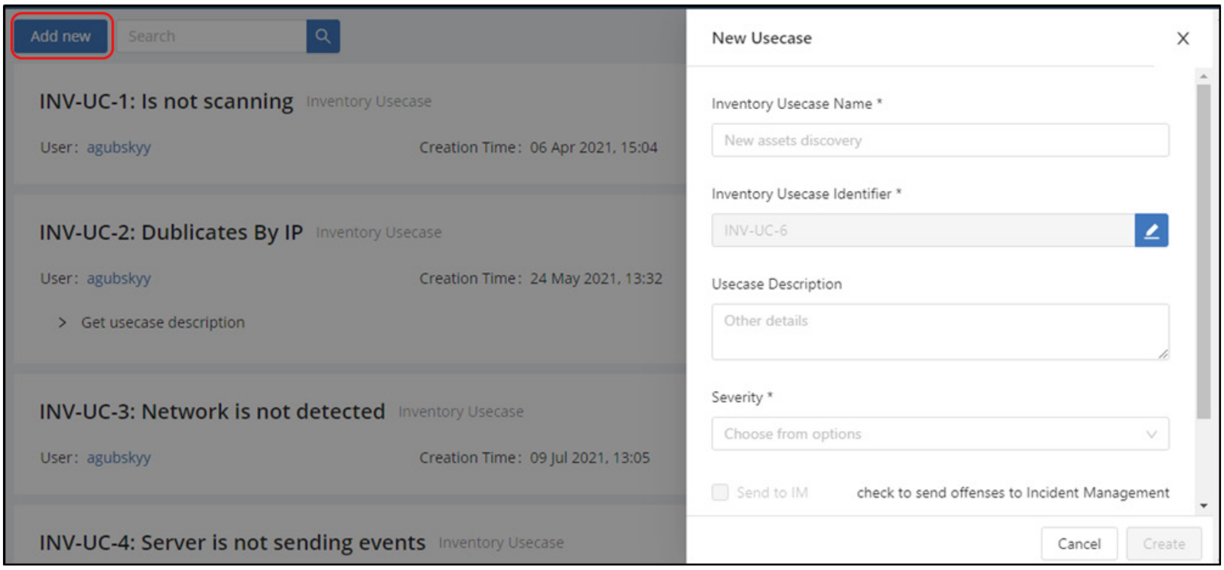
INV-UC-3: Log Source status is ERROR Inventory Usecase
User: IT Specialist Creation Time: 17 Aug 2021, 15:33

INV-UC-4: PC Name Duplicates Inventory Usecase
User: IT Specialist Creation Time: 17 Aug 2021, 15:34

INV-UC-5: IP Duplicates Inventory Usecase
User: IT Specialist Creation Time: 17 Aug 2021, 15:35

Figure 34

To register a new Inventory usecase press ADD NEW and fill in the required information (Figure 35).



INV-UC-1: Is not scanning Inventory Usecase
User: agubskyy Creation Time: 06 Apr 2021, 15:04

INV-UC-2: Dublicates By IP Inventory Usecase
User: agubskyy Creation Time: 24 May 2021, 13:32

INV-UC-3: Network is not detected Inventory Usecase
User: agubskyy Creation Time: 09 Jul 2021, 13:05

INV-UC-4: Server is not sending events Inventory Usecase

New Usecase ×

Inventory Usecase Name *
New assets discovery

Inventory Usecase Identifier *
INV-UC-6

Usecase Description
Other details

Severity *
Choose from options

□ Send to IM check to send offenses to Incident Management

Figure 35

Parameters to fill in:

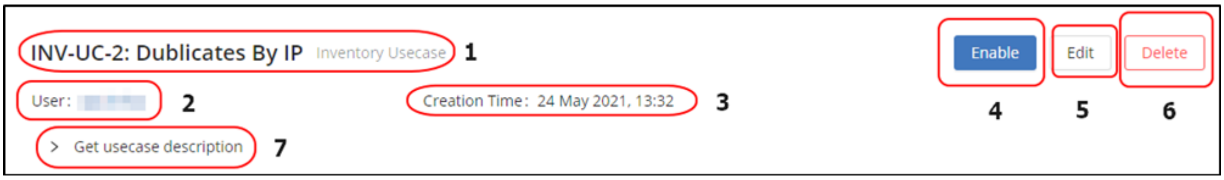
- **Inventory Usecase Name** (necessarily) – usecase name
- **Inventory Usecase Identifier** (necessarily) – unique identifier (assigned automatically incrementally, but it is possible to make adjustments if necessary)
- **Severity** (necessarily) – criticality level
- **Usecase Description** (optional) – description of Inventory usecase

The description of the detecting rules for the usecase is not different from creating custom filter and built on the similar concept. Meaning: it is possible to select the required Inventory field, specify a logical operator and, if available, determine the value. After pressing **ADD RULE** the rule will be added to the list of configures correlation rules.

To implement more complex scenarios related to complex logic and more complex calculations it is possible to register additional calculated fields.

As already mentioned, the offense status of registered usecases for each asset is calculated automatically at each iteration of the application data update. Thus, if a certain network asset has any problems or anomalies, that are detected on the basis of the registered rules of Inventory usecases, an event will be generated for it, which will be periodically saturated with new discoveries until the problem with this asset is resolved.

The main dashboard of the Usecases panel contains cards of registered usecases, where the data specified on Figure 36 and detailed below.



INV-UC-2: Dublicates By IP Inventory Usecase

User: [redacted]

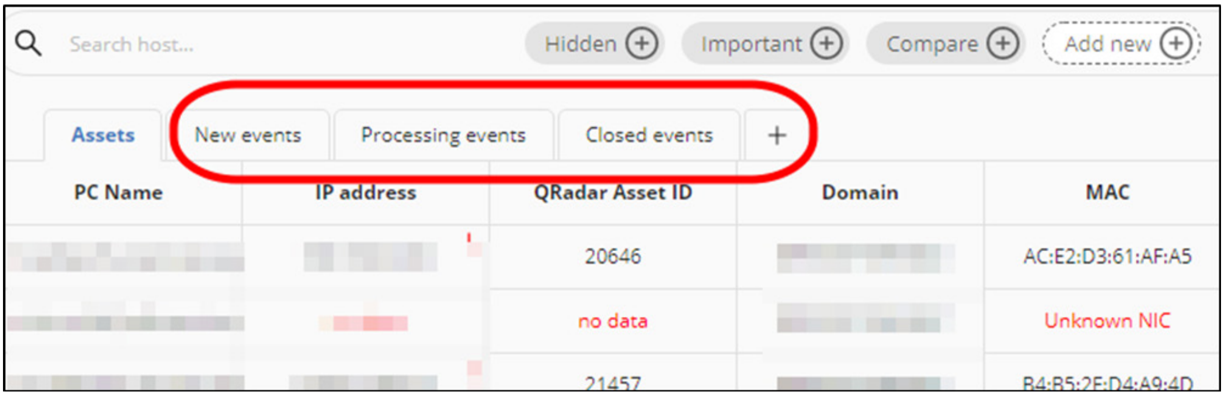
Creation Time: 24 May 2021, 13:32

Figure 36

1. **Usecase name**
2. **User** – user, who created the usecase
3. **Creation date** – date and time of creating
4. **Enable/Disable** – temporary disabling usecase without deleting (in this case detection by this rule will be disabled), and enable the disabled usecase
5. **Edit** – making changes to logic (adding logic based on several logical operators)
6. **Delete** – deleting usecase
7. **Usecase description** – detailed usecase description

To view the list of events go to the main dashboard of the application. There are 3 navigation tabs at the top (Figure 37):

- **New events** – panel with the new offenses
- **Processed events** – events that are already at the stage of analysis and resolution
- **Closed events** – resolved events

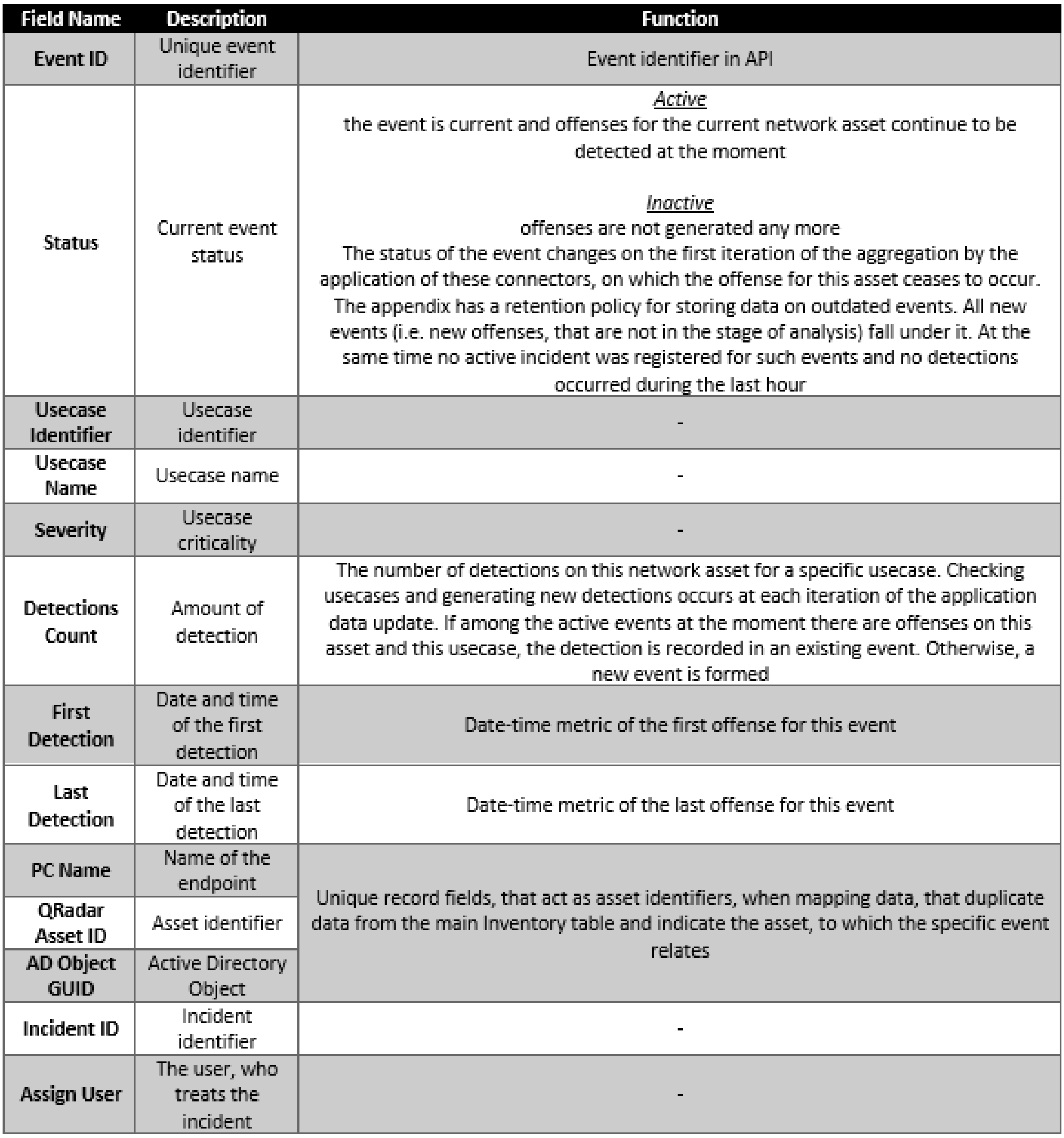


PC Name	IP address	QRadar Asset ID	Domain	MAC
[redacted]	[redacted]	20646	[redacted]	AC:E2:D3:61:AF:A5
[redacted]	[redacted]	no data	[redacted]	Unknown NIC
[redacted]	[redacted]	21457	[redacted]	B4:B5:2F:D4:A9:4D

Figure 37

All registered events appear on the first dashboard **New events**. After the incident on this event is registered it changes its status accordingly and is automatically transferred to the next dashboard **Processing events.** At this stage of the life cycle the event is being processed. Once the problem is resolved it is needed to close the event manually from the Inventory panel. After closing the event receives the status closed and is automatically transferred to the dashboard **Closed events**. Each of the dashboards looks similar to the main Inventory table, but as records here are registered events that reflect anomalies in the Inventory assets based on registered usecases.

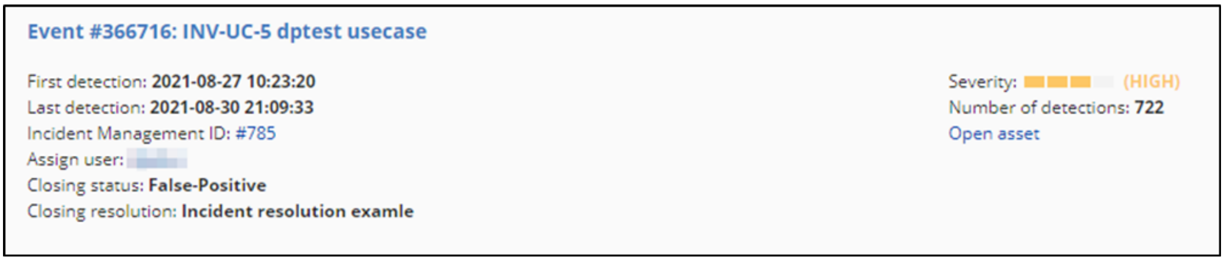
Fields of event dashboards, their names, description and purpose are specified in Table 8.



Field Name	Description	Function
Event ID	Unique event identifier	Event identifier in API
Status	Current event status	*Active* the event is current and offenses for the current network asset continue to be detected at the moment *Inactive* offenses are not generated any more The status of the event changes on the first iteration of the aggregation by the application of these connectors, on which the offense for this asset ceases to occur. The appendix has a retention policy for storing data on outdated events. All new events (i.e. new offenses, that are not in the stage of analysis) fall under it. At the same time no active incident was registered for such events and no detections occurred during the last hour
Usecase Identifier	Usecase identifier	-
Usecase Name	Usecase name	-
Severity	Usecase criticality	-
Detections Count	Amount of detection	The number of detections on this network asset for a specific usecase. Checking usecases and generating new detections occurs at each iteration of the application data update. If among the active events at the moment there are offenses on this asset and this usecase, the detection is recorded in an existing event. Otherwise, a new event is formed
First Detection	Date and time of the first detection	Date-time metric of the first offense for this event
Last Detection	Date and time of the last detection	Date-time metric of the last offense for this event
PC Name	Name of the endpoint	Unique record fields, that act as asset identifiers, when mapping data, that duplicate data from the main Inventory table and indicate the asset, to which the specific event relates
QRadar Asset ID	Asset identifier	
AD Object GUID	Active Directory Object	
Incident ID	Incident identifier	-
Assign User	The user, who treats the incident	-

Table 8

A detailed preview card is available for events on each of the dashboards, which opens in additional tabs on the navigation bar (Figure 38). To open the detailed view tab double-click on the row of the table with the needed event.



Event #366716: INV-UC-5 dptest usecase

First detection: **2021-08-27 10:23:20**
Last detection: **2021-08-30 21:09:33**
Incident Management ID: #785
Assign user: [redacted]
Closing status: **False-Positive**
Closing resolution: **Incident resolution examle**

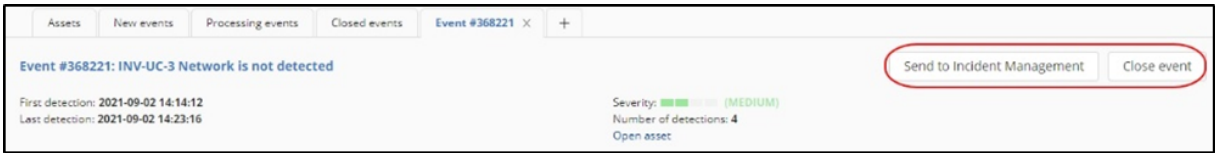
Severity: ■■■ (HIGH)
Number of detections: **722**
Open asset

Figure 38

The detailed card contains the following information of the event:

- **Event #** – event unique identifier
- **Usecase name** (clicking on it will open the appropriate Inventory usecase in the Usecases section to modify it or view the logic)
- **First detection** – date and time of the first detection
- **Last detection** – date and time of the last detecting
- **Incident management ID** – incident identifier
- **Assign user** – the user, who treats the incident
- **Closing status** (for closed events) – stage of closing
- **Closing resolution** (for closed events) – reason of closing
- **Severity** – incident criticality
- **Number of detections**
- **Open asset** – current asset, for which the event was generated (it is possible to go to the asset card by clicking)

In the upper right corner of the panel a dynamic bar with control controls placed (Figure 39).



Event #368221: INV-UC-3 Network is not detected

First detection: **2021-09-02 14:14:12**
Last detection: **2021-09-02 14:23:16**

Severity: ■■ (MEDIUM)
Number of detections: **4**
Open asset

Figure 39

Usecase incident procedure stage are described in Table 9.

Control	Description	Stage
Send to Incident Management	Incident registration, which will immediately transfer the incident to the Incident Management application and automatically fill in all the data in the form of a new incident	New events Processed events
Close	Closing the incident, which allows to close the current event	Processed events

Table 9

Remark: it is possible to combine multiple events into a single incident and register it as a single incident in the Incident Management application. Updating information in Inventory, when the incident status is updated, will be performed automatically for all events contained in it.

9.5 Connectors and Mapping

The process of data aggregation by an application from external sources is quite complex and requires consideration of many factors. Software modules, that allow to saturate the Inventory table with information from specific external sources, are called connectors. The purpose of the connector includes obtaining data according to a certain protocol, their pre-processing and reduction to the desired format and subsequent mapping of values to certain fields Inventory. The application implements the plugin extensible concept of management of installed connectors. Thus, each connector to an external source is supplied as a separate package containing the software module of the connector. The necessary connectors can be downloaded through the admin panel and perform further configuration.

Currently, for the application is implemented a significant number of different integration connectors for the most popular services and systems. Among the list of connectors currently available the following general connectors can be found:

- Universal HTTP connector
- Active Directory connector
- Universal connector for QRadar Reference Data
- Connectors for QRadar Assets DB, QRadar Group Policies, QRadar Log Sources, QRadar QVM Assets and QRadar Network Hierarchy
- Transportation connectors (IMAP, SSH)
- Connectors-parsers (XLSX Parser, CSV Parser)
- Connectors to a number of relational and non-relational databases (MySQL, PostgreSQL. MongoDB, MSSQL)
- Connectors for a wide range of popular services and systems (Defender ATP, McAfee, Symantec, Cisco Prime, SCCM, Tenable SC, vCenter)

The application has a wide range of integrations for uploading and aggregating data from external systems. It should be noted, that transportation connectors can only act as an unloading mechanism and support the creation of processing chains from multiple connectors as they have a separate configuration parameter called Additional parser, which allows to select a connector for the next pipeline processing. Scenarios can be implemented, when data, such as a daily report, is retrieved through a transportation connector and passed to the input of the next connector, which can be one of the parser connectors. Thus, the processing chain from several connectors is formed.

The process of creating a new connector is simple and comes down to writing a simple script to fetch data and describe a metadata file. Python and JavaScript are supported.

Connectors are divided the returned data into 2 types: those, that provide direct mapping, and those, that operate in cross-mapping mode and operate processing rules in data aggregation.

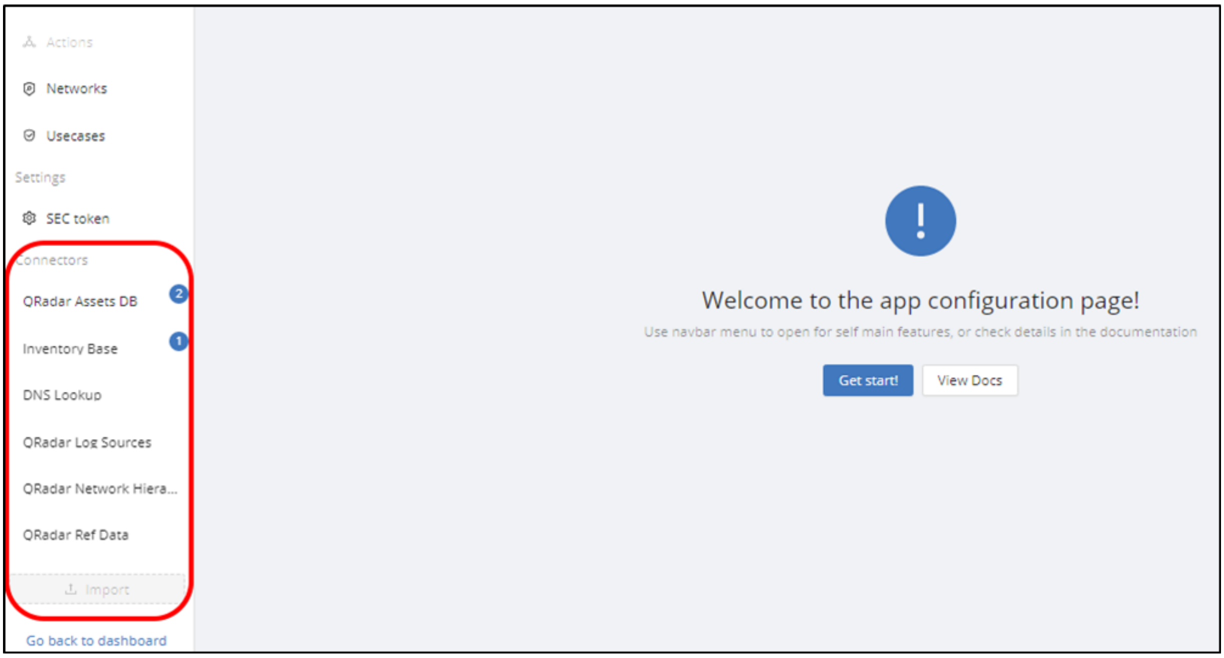
Direct mapping occurs, when the connector returns a set of data, that conceptually corresponds to the essence of the Inventory table record. Inventory combines data from different sources, so information about the same network assets may be repeated, so to avoid duplication each entry from the connector must be mapped to the corresponding Inventory entry based on a unique key (or several keys). Within the application this concept is implemented on the basis of the primary fields of the Inventory table.

So during the registration of a new field the checkbox is immediately indicating, that this field has the role of a unique identifier during mapping. Thus, in the process of obtaining connector data each record is checked for the presence of a corresponding record for this asset in the Inventory table. If this condition is met, the existing record is supplemented with information based on certain field mapping rules, otherwise a new record is created.

Another type of connectors are connectors that work in cross-mapping mode. They return individual data collections, that are conceptually related to individual entities and do not related to the assets defined in Inventory. The logic of processing the rules can be different and their number is not limited to one. Thus, connectors operating in cross-mapping mode allow to supplement Inventory records with information from third-party data collections based on certain rules with the logic of comparison.

Conceptually the process of data aggregation by the application is an iterative multi-stage process consisting of several main stages:
1. Launch connectors with direct mappings, that can be used at the moment according to their schedule and frequency. If no primary mapping field is defined for any of the connectors or a failure occurs, when trying to upload data from an external source, the mapping for that connector is skipped on the current iteration of the aggregation process.
2. Complement information with cross-mapping connectors
3. Calculation of calculated fields. At this point all external source data in the current iteration has already been pulled up and mapped to the Inventory fields. At this stage the calculation logic based on the dependent fields can already be performed
4. Start the process of calculating of Inventory usecases on the basis of registered rules. Records are analyzed for anomalies and inconsistencies, new events are formed or detections are added to existing ones.

Because the Inventory table data must be up-to-date and must not contain outdated information, the process of starting data aggregation is iterative and is performed automatically at regular intervals. In this case for each connector it is possible to specify the interval, at which it will be activated. Thus, the Inventory table data is dynamic and constantly updated and the refresh rate for different sources can be adjusted and the connectors, that run on each of the iterations, may be different..
A separate block of the admin panel is responsible for controlling the connectors installed in the application. This block is called **CONNECTORS** (Figure 40). This functionality is available in a **full version only** (Inventory Plus). In Inventory for QRadar editing of connectors is available.



Welcome to the app configuration page!

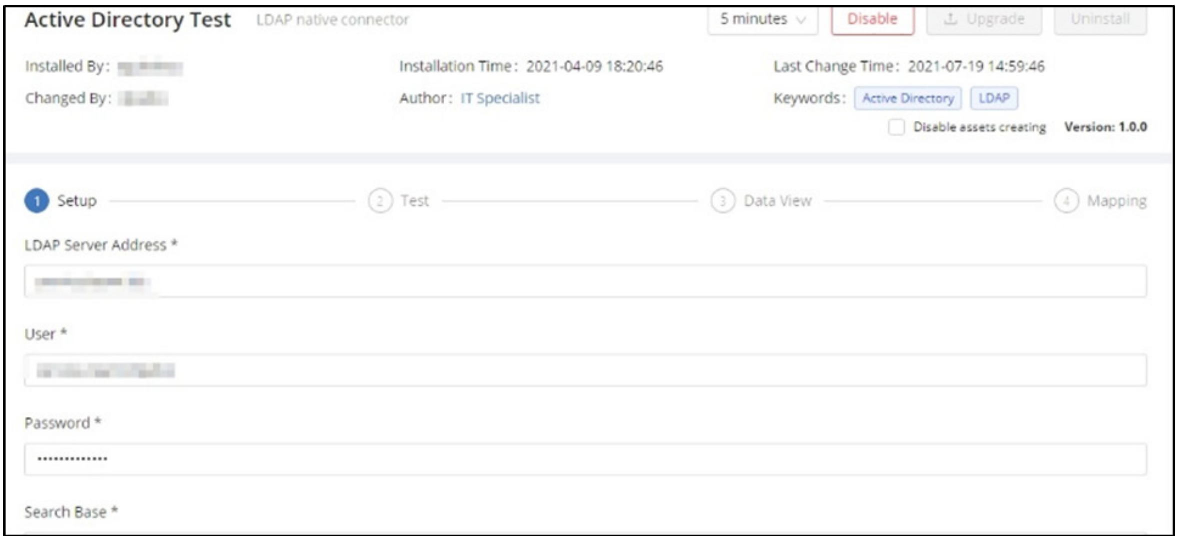
Use navbar menu to open for self main features, or check details in the documentation

Figure 40

The currently installed connectors in the application are displayed here. The blue label provides information about the number of mapped primary fields for this connector (i.e. the fields, that act as the record ID and therefore on the basis, of which the Inventory table records are mapped).

At the bottom of this section is the Import button is placed, which allows to download and install a new connector in the application or import an external NPM-module for use in post-processing functions and calculated fields.

Open the settings of each of the connectors by clicking on the appropriate menu section. The Active Directory test connector settings are shown on Figure 41.



Active Directory Test LDAP native connector

Installed By: [redacted]
Installation Time: 2021-04-09 18:20:46
Last Change Time: 2021-07-19 14:59:46
Changed By: [redacted]
Author: IT Specialist
Keywords: Active Directory LDAP
□ Disable assets creating
Version: 1.0.0

1 Setup
2 Test
3 Data View
4 Mapping

LDAP Server Address *
[redacted]

User *
[redacted]

Password *
•••••••••••••

Search Base *

Figure 41

- Installed By – users, who installed the connector
- Changed By – user, who modified the connector
- Installation Time – date and time, when the connector was installed
- Author – the author of the connector
- Last Change Time – date and time of last modification of the connector
- Keywords – key tag words
- Disable assets creating – disable the creation of new Inventory table entries for this connector (useful in the case of connectors, that should work in the mode of supplementing information only)
- Version – current connector version

In the upper right corner of the panel there are the managing controls, which include the following functions:

- Update time for the current source
- Enable/Disable – switching the connector on or off (in this case it will not be involved in the data aggregation process)
- Upgrade – installing an updated version on the current connector
- Delete – deleting the connector

9.5.1 Connector Configuration

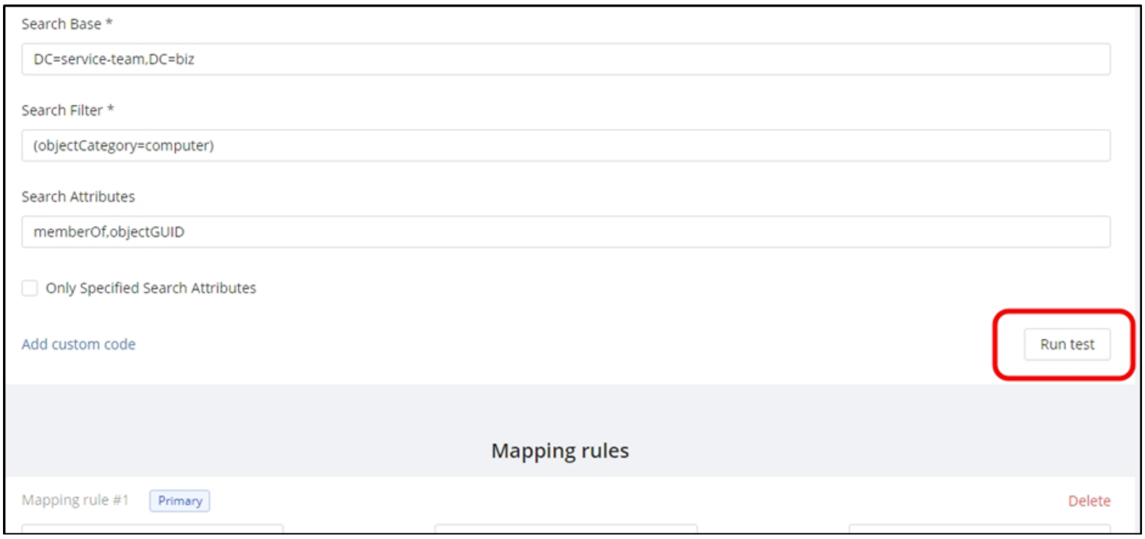
Step 1. Setup: Specify configuration information and authorization data for the connector Configuration parameters differ for each type of connector and depend on its type.

For example, in case of **ACTIVE DIRECTORY** connector is necessary to enter the following details:

- **LDAP Server Address** (necessarily) – server IP-address
- **User, Password** (necessarily) – user login and password for authentication on this server
- **Search Base, Search Filter** (necessarily) – search parameters
- **Search Attributes** (optional) – additional search attributes (the default set of standard attributes will be returned)
- **Only Specified Search Attributes** – measure the returned data to the specified attributes only

At the bottom of this panel there is a control **Add custom code**, that allows to describe the custom post-processing function of the connector data, if necessary. Instructions are described in the JavaScript.

After configuring the data press **RUN TEST** (Figure 42).



Search Base *
DC=service-team,DC=biz

Search Filter *
(objectCategory=computer)

Search Attributes
memberOf,objectGUID

□ Only Specified Search Attributes

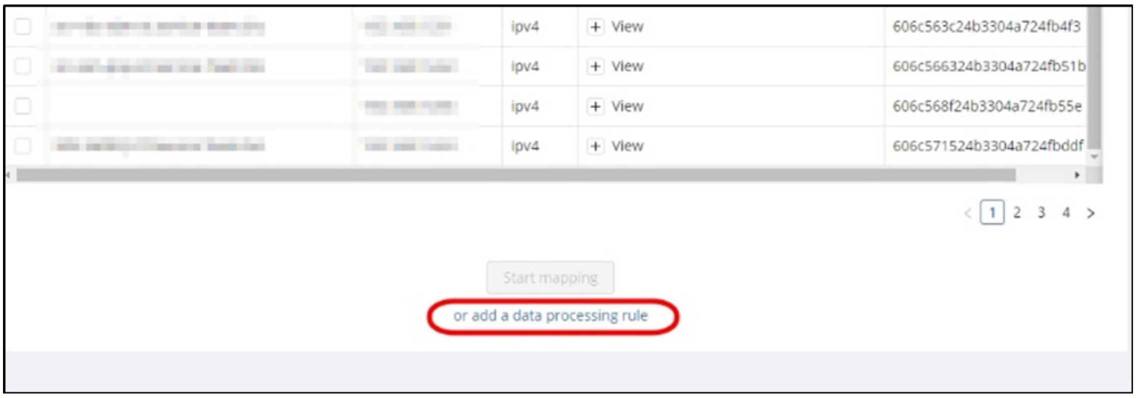
Figure 42

Step 2. Test: Test the connection and verify, that the entered configuration data is working

If the test is successful, the connector will download the test data from the current source and allow to view them in tabular form. It is possible to select multiple test data samples and start field mapping. For direct mapping connectors select the field name from the source and specify the Inventory field, in which the value mapping needed. Based on the field type the application can automatically format values to the required standard.

Step 3. Data view

After testing the results will appear. Additionally it is possible to apply the post-processing function to this particular field. To do so press **ADD A DATA PROCESSING RULE** and select the registered rule (Figure 42). It is also possible t create a new rule and describe its logic in the built-in editor. When describing the post-processing function, use external libraries and pre-loaded modules into the application through the import functionality.

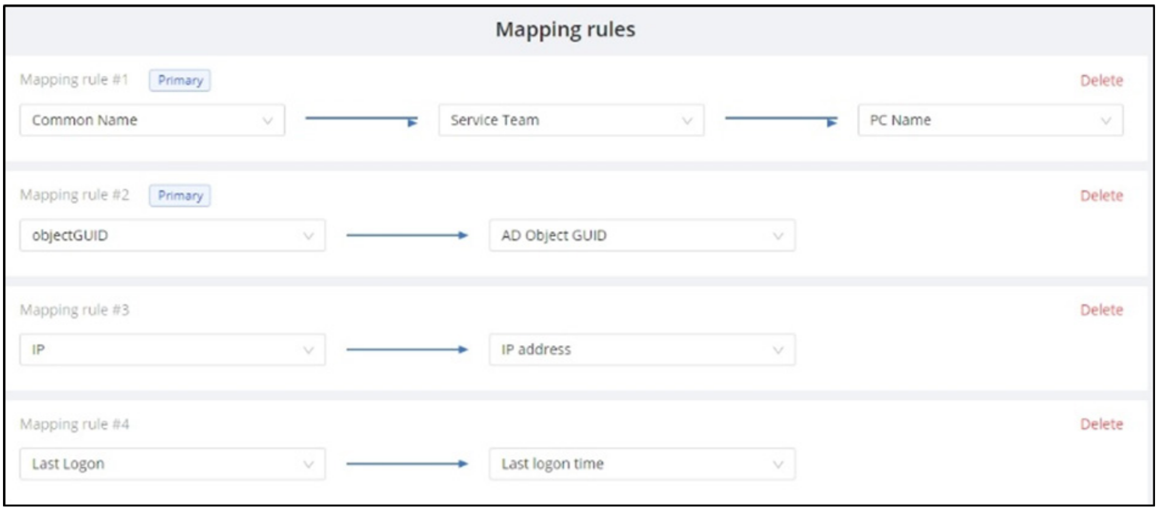


□	[redacted]	[redacted]	ipv4	+ View	606c563c24b3304a724fb4f3
□	[redacted]	[redacted]	ipv4	+ View	606c566324b3304a724fb51b
□		[redacted]	ipv4	+ View	606c568f24b3304a724fb55e
□	[redacted]	[redacted]	ipv4	+ View	606c571524b3304a724fbddf

Figure 43

After pressing **SAVE** the rule will be added to the list of mapping rules for the current connector.

Step 4. Mapping. Applying of mapping new fields
The mapping list of all fields is displayed in the section Mapping rules (Figure 44).



Mapping rules

Mapping rule #1 Primary — Delete
Common Name → Service Team → PC Name

Mapping rule #2 Primary — Delete
objectGUID → AD Object GUID

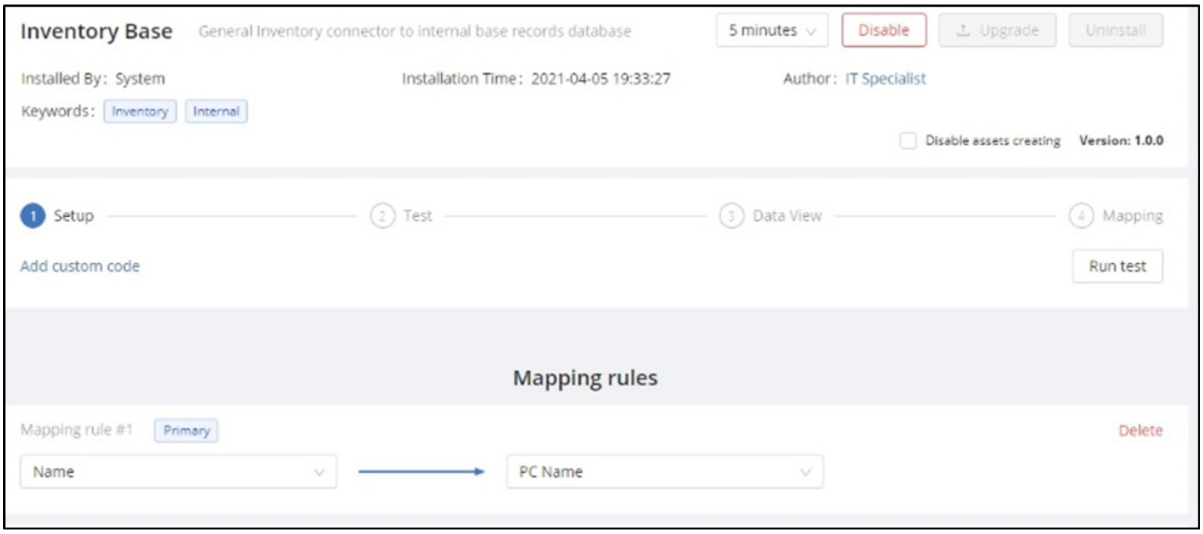
Mapping rule #3 — Delete
IP → IP address

Mapping rule #4 — Delete
Last Logon → Last logon time

Figure 44

It is possible to change or delete the rule logic. For rules, that use application fields, when mapping Primary, an additional label is displayed, which indicates, that this rule is primary, and therefore based on it will be mapping the records of the current connector.

One of the connectors is built into the application and does not require installation. It is called Inventory Base (Figure 45) and is intended to process the results of the network scanning Inventory module and does not require additional parameters for configuration.



Inventory Base General Inventory connector to internal base records database

Installed By: System
Installation Time: 2021-04-05 19:33:27
Author: IT Specialist
Keywords: Inventory Internal

□ Disable assets creating **Version: 1.0.0**

Mapping rules

Mapping rule #1 Primary

Name → PC Name

Figure 45