


# Reference Data Management

- Reference Data Management
  - Create new data
  - Display data
    - Reference Sets
      - Add Entry
      - Bulk Add
      - Import CSV
      - Export CSV
      - Delete Entry
      - Clear Data
      - Delete Set
    - Reference Maps
      - Bulk Add
      - Import CSV
    - Reference Map of Sets
      - Bulk Add
      - Import CSV
    - Reference Tables
      - Bulk Add
      - Import CSV
  - Dependencies
  - Named Service
  - Additional information and known issues
    - Dates
    - Searching
    - Import large files
    - Reference Map of Sets with sparse keys and dense values
    - Errors
      - Errors after Updating the App

The app allows the creation, deletion and visualization of all types of Reference Data in QRadar. Most supported operations on the different data types can be performed from within the app, for instance bulk insertion of new data into a Reference Map. The different data types and available operations are described below.

The view consists of two sections.


In the left side of the view, all the defined reference data entries are shown. The entries are ordered alphabetically by type (set, map, map of set, table).

 Search

Reference Set	▼
Reference Map	▼
Reference Map of Sets	▼
Reference Table	▼

## Create new data

By clicking on the `Create New` button below a reference data type, a new reference data entry of the specific type can be created:

 Search

Reference Set ^

Create New

For the different types, different kinds of data need to be specified. For instance, for a set, the `name` , `element type` are required, the `time to live` is optional and can be specified as a numeric value + an element of {mons,days,hours,minutes,seconds} from the dropdown menu.

Add new Reference Set to Database

Reference Set Name ⓘ

Element Type ⓘ

ALN

Timeout Type ⓘ

FIRST\_SEEN

Time to Live ⓘ

days ▼

Create

Reference Maps and Map of Sets are created similarly. An additional detail on tables: A number of "inner keys" can be specified to define the table structure. Each inner key consists of a `name` and a `type` which can be chosen from the dropdown at the right. Inner keys can be added via the "Add Inner Key" button and deleted via the "Trash" Icon to the right of the key.

Add new Reference Table to Database

Reference Table Name ⓘ

Timeout Type ⓘ

FIRST\_SEEN

Time to Live ⓘ

seconds

Key Label ⓘ

Outer Key Label

Key Type ⓘ

ALN

Inner Keys ⓘ

ALNInner Key 1

ALNInner Key 2

Add Inner Key

Create

# Display data

Clicking on one of the entries will display the contents of the specified entry.

Critical Assets ⓘ

Delete Set

Clear Data

Number of Elements: 22

Creation Time: 27/Aug/2015, 07:15:40 PM

Timeout Type: FIRST\_SEEN

Time To Live: Forever

Value Type: IP

3.0.0.0

Add Entry | Bulk Add | Import from File | Export to File

<input type="checkbox"/>	Value	First Seen	Last Seen	Source
<input type="checkbox"/>	13.0.0.0	04/Mar/2020, 10:47:55 AM	04/Mar/2020, 10:47:55 AM	reference data api
<input type="checkbox"/>	3.0.0.0	04/Mar/2020, 10:47:55 AM	04/Mar/2020, 10:47:55 AM	reference data api
<input type="checkbox"/>	123.0.0.0	06/Mar/2020, 09:07:33 AM	06/Mar/2020, 09:07:33 AM	xxxx

Items per page 10

1-3 of 3 items

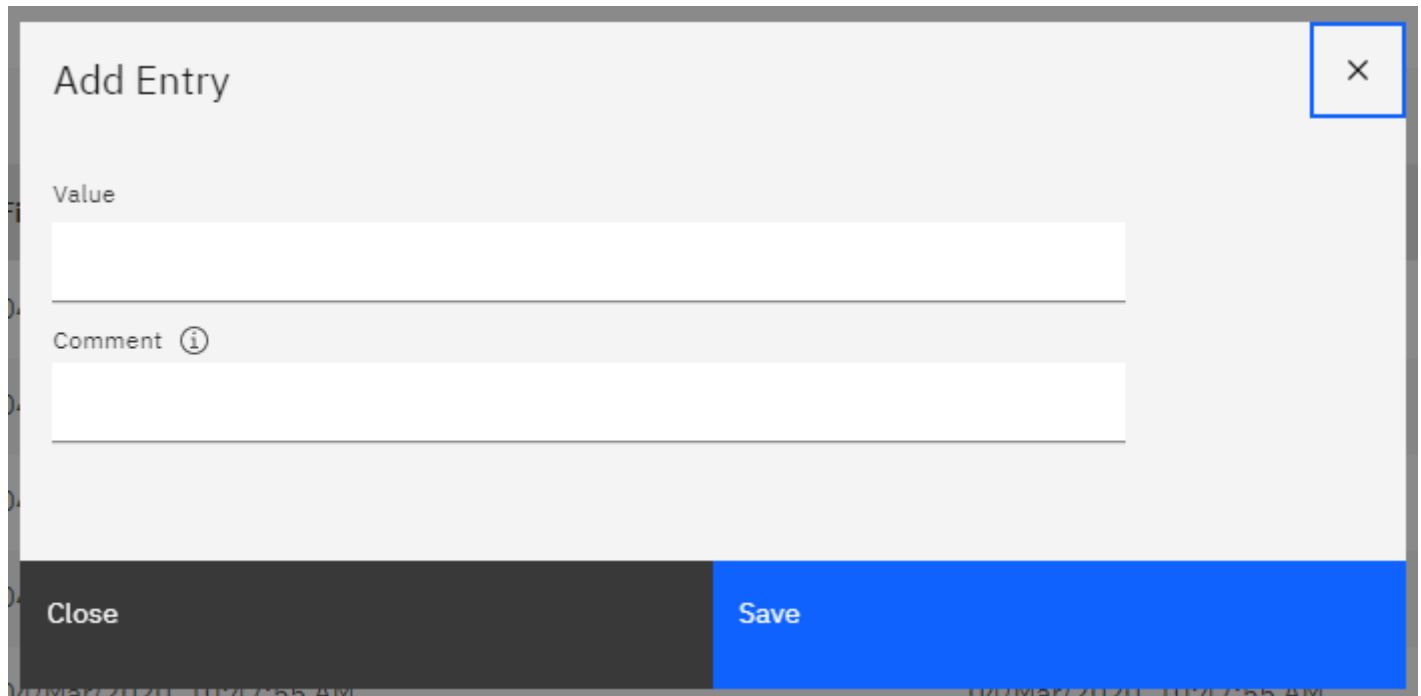
1 of 1 pages

It should be noted, that for large reference data entries, loading will be done in chunks but the data will only be displayed when all entries have been loaded. That the loading is ongoing can be verified by checking if the `number of elements` , displayed on the top of the view changes periodically.

## Reference Sets

### Add Entry

Add a single entry to the reference set. A value must be specified. Additionally, a comment can be added which will be stored in the `source` property for the entry. This can be convenient for tracking changes.

A screenshot of a web application dialog box titled "Add Entry". The dialog has a light gray background and a dark gray border. In the top right corner, there is a small square button with a blue border and a black "X" icon. Below the title, there are two input fields. The first is labeled "Value" and is a simple white text box. The second is labeled "Comment" followed by a small circular icon containing an "i". This is also a white text box. At the bottom of the dialog, there are two buttons: "Close" on the left and "Save" on the right. The "Close" button is dark gray, and the "Save" button is blue. The dialog is overlaid on a blurred background of the application interface.

### Bulk Add

Add multiple entries at the same time. A separator needs to be specified which can be used to split the entries. Additionally, a new line can be used to separate entries, as new lines will be implicitly used as separator character.

### Import CSV

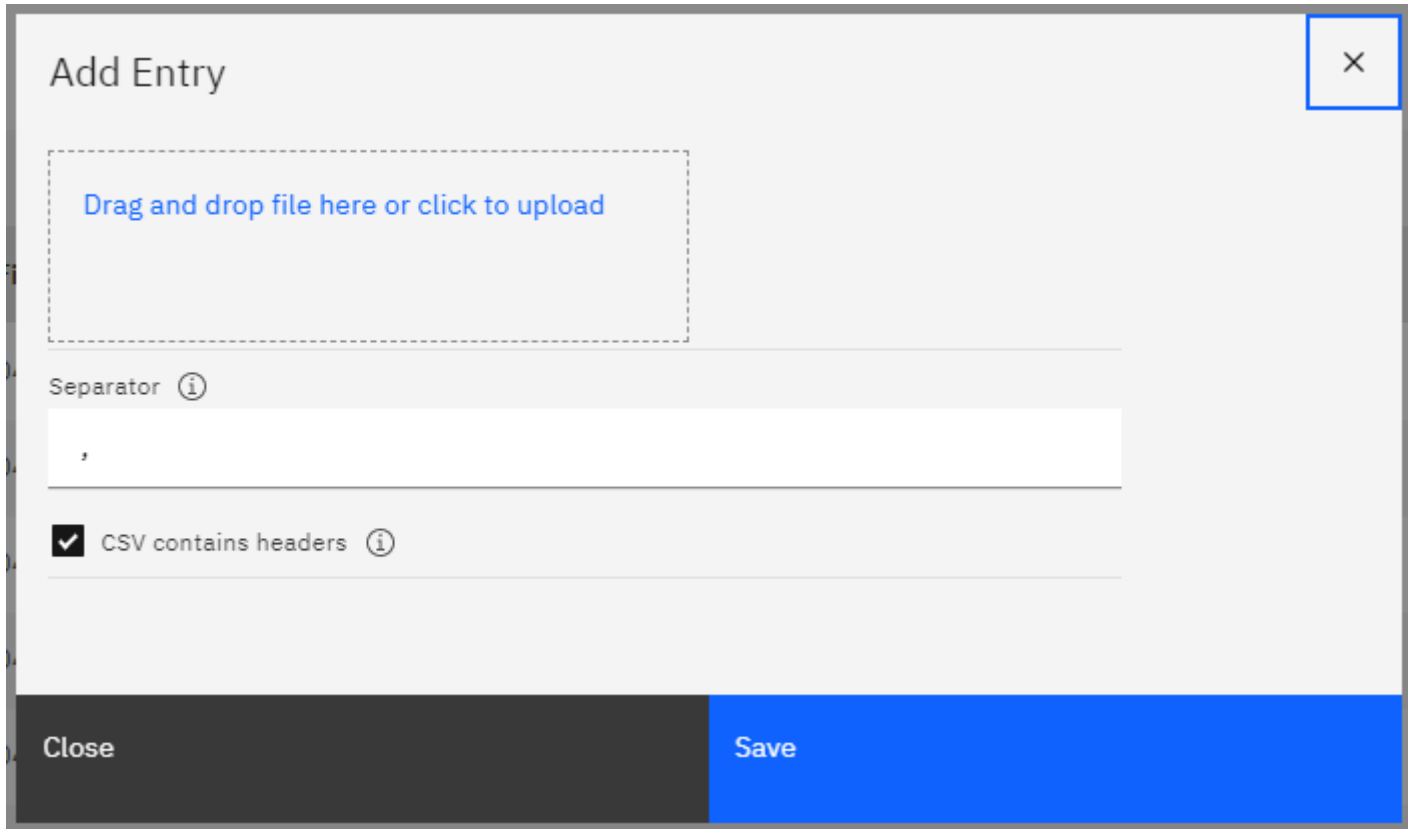
Similiarly to the `Bulk Add` functionality, instead of pasting the contents in the bulk add text area, a file can be specified which contains the data to be added. Each entry is separated by a new line. The expected format is either

```
value1
value2
value3
```

or

```
values,other,headers  
value1,some,data  
value2,other,data2
```

However, all list entries besides the first column are ignored during the upload. This is only added to be able to directly reimport data that has been exported via the app before.



Add Entry

Drag and drop file here or click to upload

Separator ⓘ

,

☒ CSV contains headers ⓘ




Close Save

## Export CSV

The data can be exported easily into a file in CSV format where each entry is separated by a new line. CSV is allowed because it is possible to directly reimport data that has been exported via the App. Fields like `last_seen` are simply ignored by the upload function.


## Delete Entry

One or multiple entries can be selected by clicking on them in the table. Clicking on `Delete Entry` afterwards, will attempt to delete the selected entries from the reference data.

2 items selected					Delete 	Cancel
	Value		First Seen	Last Seen	Source	
<input checked="" type="checkbox"/>	0.0.0.0		04/Mar/2020, 10:47:55 AM	04/Mar/2020, 10:47:55 AM	reference data api	
<input checked="" type="checkbox"/>	1.0.0.0		04/Mar/2020, 10:47:55 AM	04/Mar/2020, 10:47:55 AM	reference data api	
<input type="checkbox"/>	10.0.0.0		04/Mar/2020, 10:47:55 AM	04/Mar/2020, 10:47:55 AM	reference data api	
<input type="checkbox"/>	11.0.0.0		04/Mar/2020, 10:47:55 AM	04/Mar/2020, 10:47:55 AM	reference data api	

## Clear Data

There are two buttons on the upper right side for each Reference Data Entry.

Critical Assets		Delete Set
Number of Elements: 22		Clear Data
Creation Time: 27/Aug/2015, 07:15:40 PM		

Clicking this button will purge all data for this reference data entry. This might be helpful to get rid of all content while keeping the reference data entry existant (e.g. if it cannot be deleted due to dependencies).

## Delete Set

If the reference data entry has no dependencies, it can be deleted by clicking `Delete Set`. Attempting to delete an reference data entry will ask for confirmation before performing any action.

Dependencies are displayed below the table with reference data contents.

## Reference Maps

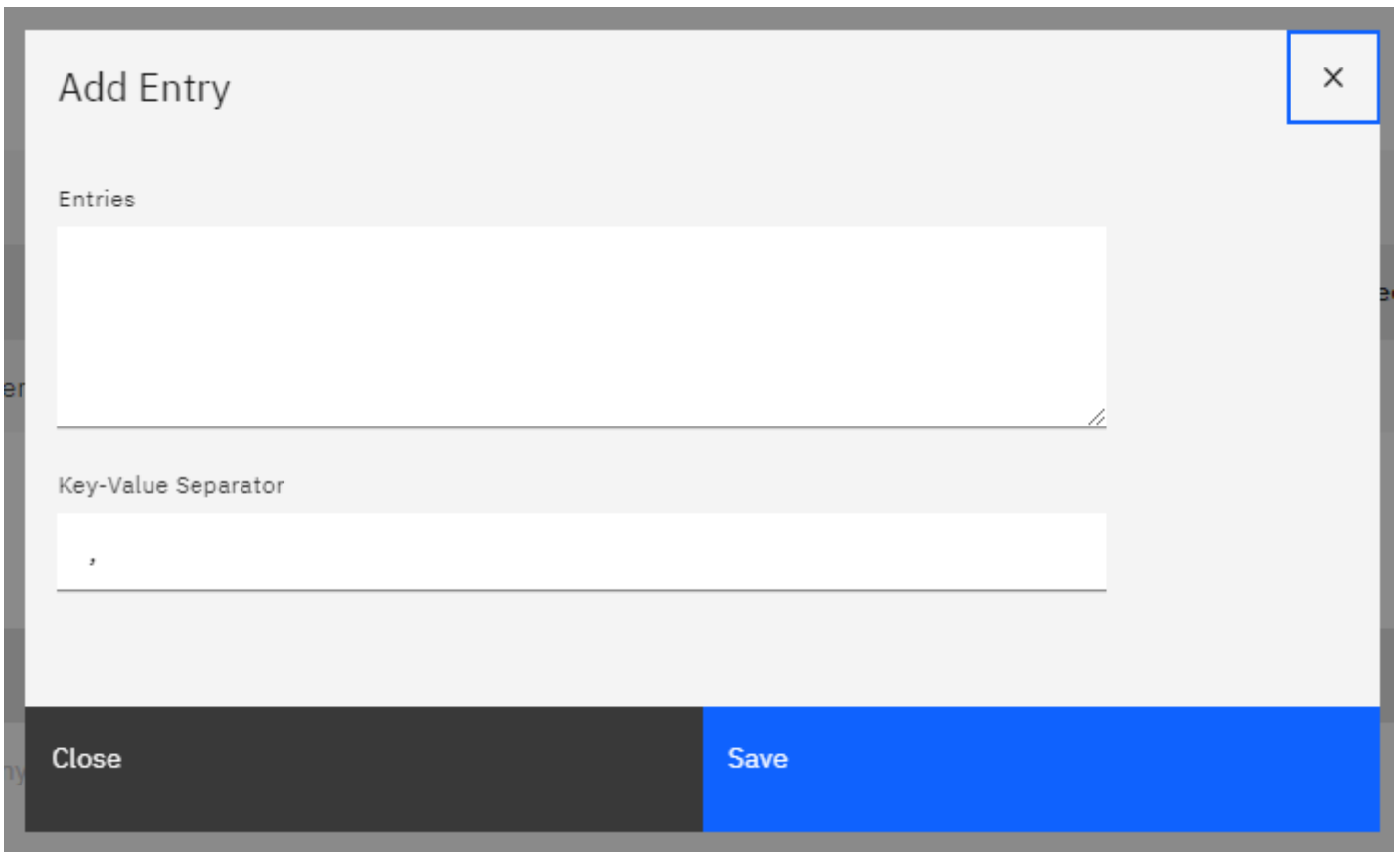
Reference Maps support essentially the same operations as reference sets.

## Bulk Add

The expected format for bulk adding data is:

```
key,value
key2,value2
key3,value3...
```

where the separator between two entries can be specified as Key-Value-Separator

A dialog box titled "Add Entry" with a close button (X) in the top right corner. It contains two input fields: "Entries" and "Key-Value Separator". The "Entries" field is a large text area with a small icon in the bottom right corner. The "Key-Value Separator" field is a smaller text input containing a comma. At the bottom, there are two buttons: "Close" and "Save".

Add Entry

Entries

Key-Value Separator

Close Save

## Import CSV

The expected format for importing data is:

```
key,value,optional,headers...  
key1,value1,..  
key2,value2,..
```

Only the two first columns are relevant for importing, the rest is ignored

## Reference Map of Sets

CorrelatedAttackMap

Number of Elements: 5

Creation Time: 09/May/2014, 08:16:42 PM

Timeout Type: UNKNOWN

Time To Live: Forever

Value Type: ALN

Delete Map of Sets

Clear Data

Q

Add Entry | Bulk Add | Import from File | Export to File

☐Key

^ ☐TestKey

☐

Value

First Seen

Last Seen

Source

☐TestValue1

03/Apr/2020, 12:51:45 PM

03/Apr/2020, 12:51:45 PM

reference data api

☐TestValue2

03/Apr/2020, 12:51:45 PM

03/Apr/2020, 12:51:45 PM

reference data api

☐TestValue3

03/Apr/2020, 12:51:45 PM

03/Apr/2020, 12:51:45 PM

reference data api

Items per page 10 1-3 of 3 items

1 1 of 1 pages

☐TestKey2

Items per page 10 1-2 of 2 items

1 1 of 1 pages

When opening a Reference Map of Sets, only the outer keys are displayed. The inner values for a specific outer key can be displayed by clicking the **v** at the left side of the key.

It should be noted, that searching will always search in the keys AND the values of a data entry, e.g. searching for `smss.exe` will display all keys that match this expression as well as all keys that have some value, matching this expression.

Q Value3

Add Entry | Bulk Add | Import from File | Export to File

☐Key

^ ☐TestKey

☐

Value

First Seen

Last Seen

Source

☐TestValue1

03/Apr/2020, 12:53:00 PM

03/Apr/2020, 12:53:00 PM

reference data api

☐TestValue2

03/Apr/2020, 12:53:00 PM

03/Apr/2020, 12:53:00 PM

reference data api

☐TestValue3

03/Apr/2020, 12:53:00 PM

03/Apr/2020, 12:53:00 PM

reference data api

Items per page 10 1-3 of 3 items

1 1 of 1 pages

☐TestKey2

Items per page 10 1-1 of 1 items

1 1 of 1 pages

## Bulk Add

The expected format for bulk adding data is:



```
key,value
key,valueX
key,valueY
key2,value2
key2,value2X...
```

## Import CSV

The expected format for importing data is:

```
key,value,optional,headers...
key,value1,..
key,value2,..
```

Only the two first columns are relevant for importing, the rest is ignored

## Reference Tables

Reference Tables are a more restricted version of Map of Maps where a predefined number of key=value pairs can be specified for an outer key.

<b>IOCrackingTable</b>	<a href="#">Delete Table</a>
Number of Elements: 6068	<a href="#">Clear Data</a>
Creation Time: 28/Nov/2018, 07:37:07 PM	
Timeout Type: LAST_SEEN	
Time To Live: 1 years	
Key Types: ALN (requester), ALNIC (mail), ALNIC (iocType), ALNIC (response), ALN (origin), ALN (info),	
Value Type: ALN	

(10){?}(4)

[Add Entry](#) | [Bulk Add](#) | [Import from File](#) | [Export to File](#)

☐ Key

☐ 10.10.10.10

<input type="checkbox"/>	Inner Key	Value	First Seen	Last Seen	Source
<input type="checkbox"/>	Info	internal IP	26/Mar/2020, 10:06:02 AM	26/Mar/2020, 10:06:02 AM	reference data api
<input type="checkbox"/>	iocType	ip	26/Mar/2020, 10:06:02 AM	26/Mar/2020, 10:06:02 AM	reference data api
<input type="checkbox"/>	mail	-	26/Mar/2020, 10:06:02 AM	26/Mar/2020, 10:06:02 AM	reference data api
<input type="checkbox"/>	origin	Internal_IPs	26/Mar/2020, 10:06:02 AM	26/Mar/2020, 10:06:02 AM	reference data api
<input type="checkbox"/>	requester	admin	26/Mar/2020, 10:06:02 AM	26/Mar/2020, 10:06:02 AM	reference data api
<input type="checkbox"/>	response	info	26/Mar/2020, 10:06:02 AM	26/Mar/2020, 10:06:02 AM	reference data api

Items per page 10 ▾ 1-6 of 6 items

1 ▾ of 1 pages < >

Items per page 10 ▾ 1-1 of 1 items

1 ▾ of 1 pages < >

## Bulk Add

The expected format for bulk adding data is:

```
outerkey,innerkey,value
outerkey,innerkey2,value2
outerkey,innerkey3,value3
outerkey2,innerkey,value
outerkey2,innerkey2,value2...
```

## Import CSV

The expected format for importing data is:

```
outerkey,innerkey,value,optional,headers...
outerkey,innerkey,value
outerkey,innerkey2,value2
outerkey,innerkey3,value3
outerkey2,innerkey,value
outerkey2,innerkey2,value2...
```

Only the two first columns are relevant for importing, the rest is ignored

## Dependencies

When opening a reference data entry, a dependency check is performed. Rule and BB dependencies can be opened directly in a popup window for editing. Those dependencies can easily be identified by their blue text color:

### Dependencies

(CRE\_RULE) AssetExclusion: Exclude NetBIOS Name By DNS Name

(CRE\_RULE) AssetExclusion: Exclude NetBIOS Name By IP

(CRE\_RULE) AssetExclusion: Exclude NetBIOS Name By MAC Address

## Named Service

The app supports accessing individual Reference Data via a named service interface.

Accessing a specific reference data entry can be achieved by calling:

```
https://{qradar_url}/console/plugins/{app_id}/app_proxy/#/data/view/{type}/{name}
```

a new entry can be created by calling

```
https://{qradar_url}/console/plugins/{app_id}/app_proxy/#/data/create/{type}
```

where type is one of ["sets", "maps", "tables", "map\_of\_sets"]

This can be done via code by using the QRadar JS SDK doing a request similar to this:

```

QRadar.rest({
  httpMethod: "GET",
  path: "/api/gui_app_framework/named_services",
  onComplete: function() {
    let services = JSON.parse(this.responseText);
    let service = QRadar.getNamedService(services, 'reference_data_service', 1);
    let endpoint = QRadar.getNamedServiceEndpoint(service, 'data');
    restArgs = QRadar.buildNamedServiceEndpointRestArgs({}, endpoint, {'type':'sets','name':'early_wa
    window.openWindow(restArgs.path)
  }
})

```

## Additonal information and known issues


### Dates

Dates in DATE Ref Data is represented as timestamp (UNIX epoch). The same is true for 'last seen' or 'first seen' which leads to potentially surprising values like '1.54393E+12' when exported to CSV and opened in a program like MS Excel. They need to be converted to a date, which, in MS Excel may be done with a formula like

```
=((((A1/1000)/60)/60)/24)+DATE(1970,1,1)
```

### Searching

Most search fields are regex fields, i.e. one can input a javascript regular expression that will be evaluated against the search text.

 Search

If data contains 'subdata' which is not shown in the tables directly (e.g. reference table inner key/values), this data is usually also searched for the search expression.

Important: Only keys/values are searched. It is currently not possible to search for things like 'source', 'last seen' or 'first seen'.

### Import large files

It has been observed, that the app hangs when importing large files (e.g. Reference Sets with > 100k entries). Usually, the file is still uploaded correctly, so after a page refresh, it should be displayed as expected.

# Reference Map of Sets with sparse keys and dense values

Attempting to load a Map of Set that contains only a small number of keys but an extraordinarily large number of values for each key (e.g. 5 keys with 100k values each). Loading that data might fail. Adding data, purging data and deleting the reference data entry are still possible. There is currently no workaround available.

## Errors

Most errors are handled either silently or by displaying an error message at the top of the currently displayed screen. For instance, the below error occurred when the user attempted to delete a reference set with dependents.

Error

Conflict: The Reference Data has dependents that rely on it. Delete cancelled.

×

Delete Set

Clear Data

Asset Reconciliation DNS Blacklist

↻

Number of Elements: 0

Creation Time: 06/Jan/2014, 08:20:57 PM

Timeout Type: LAST\_SEEN

Time To Live: 7 days

Value Type: ALNIC

## Errors after Updating the App

Some users reported duplicate tabs after updating the app from Version 2.0.0 to a newer version. This can be fixed by uninstalling both applications via the API and performing a clean reinstall.

- 1.) Uninstall the App via the Extension Management (Admin -> Extension Management)
- 2.) Find the old App ID for the other version (most easily via `docker ps` on the console or App Host)
- 3.) Remove the old App from QRadar (most easily via the API  
`DELETE /gui_app_framework/applications/{application_id} )`
- 4.) Do a fresh installation (most easily via the App Extension GUI)