

YSOFT SAFEQ 6 DOCUMENTATION

**THE SETUP, SERVICE, AND FUNCTIONS
OF YSOFT SAFEQ 6**

CONTENT

1	Executive Summary	3
2	Right to be Forgotten	4
2.1	Execution	4
2.2	Out of Scope	4
3	Right to Access	5
4	Right to Restriction of Processing	6
5	Right to Access - rta.exe	7
5.1	Name	7
5.2	Synopsis	7
5.3	Description	7
5.4	Options	7
6	Right to be Forgotten - rtbf.exe	9
6.1	Name	9
6.2	Synopsis	9
6.3	Description	9
6.4	Options	10
6.4.1	Running in unattended mode	10
7	Right to Restriction of Processing - rtr.exe	11
7.1	Name	11
7.2	Synopsis	11
7.3	Description	11
7.4	Options	12

1 EXECUTIVE SUMMARY

The General Data Protection Regulation has been thoroughly written about and explained in white papers and periodicals that give it the attention it deserves. The intent of this article is to provide the reader with an understanding on how the included GDPR executables can help an administrator execute upon a Data Subject's rights. In particular, Y Soft has developed three executables, each with a specific purpose:

- **rtbf.exe**: Allows an administrator to execute a Data Subject's Right to be Forgotten within YSoft SafeQ
- **rta.exe**: Allows an administrator to execute a Data Subject's Right to Access of Data within YSoft SafeQ
- **rtr.exe**: Allows an administrator to execute a Data Subject's Right to Restriction of Processing withing YSoft SafeQ, or to later re-identify a user whose request has expired.

For the purpose of this document, the following distinctions will be made:

- **Structured Data** includes data contained within YSoft SafeQ that has intentional, strictly defined purposes. This includes, for example, network usernames, names, surnames, email addresses, and home directories. Structured Data is intended to store only personal data, not sensitive data, unless the source of the data (e.g., Active Directory) was poorly defined or managed.
- **Unstructured Data** includes data contained within YSoft SafeQ that is not well defined or structured. This includes, for example, print jobs submitted by the Data Subject, along with metadata such as job titles, job origin, or file names. There is no simple way to filter this information to ensure it does not contain sensitive personal data, and thus the user is at their discretion to ensure that they understand this when submitting print jobs to YSoft SafeQ.

The scripts provided here are compatible with YSoft SafeQ 6 MU17 or later. For customers who have upgraded from much older versions of YSoft SafeQ 6, verify that the following lines are present and have appropriate values in the Management folder's **safeq.properties** file, located in the conf directory. Older releases only had the line **database.global.management.username**. The below code block is only a sample, and will not work in production environments.

```
# Database
...
database.global.management.domain =
database.global.management.username.without.domain =
database.global.management.username = ${database.global.management.username.without.domain}
...
```

2 RIGHT TO BE FORGOTTEN

The executable **rtbf.exe** is a simple command-line application that can be used in interactive or non-interactive mode to remove references to a Data Subject or fields that may contain a Data Subject's personal or sensitive data. This includes references to all **Structured Data** containing user data, but also unstructured data in the form of print job metadata.

The application works by fully anonymizing details that could be attributed back to an individual. To ensure that the data is still useful for reporting purposes, the username is still unique, however an administrator is unable to attribute this information back to a specific Data Subject.

2.1 EXECUTION

When running in interactive mode, you will be prompted to provide a user's login to remove. You will then be prompted with the extent of data that will be removed, with a request to proceed. Once this is done, the application will then prepare a series of queries, but will not commit the transaction until the very end. If the transaction fails for any reason, there is no need to worry about only partially deleted records.

```
User to remove: odaikuji
Be sure to remove the user from directory services before proceeding. The following data will be anonymized:
- Personal data (name, surname, email, etc.)
- User cards
- User aliases
- Roles explicitly assigned to the user
- Print Job Names
- Terminal access records
- Print jobs marked as favorite by the user will also be unfavorited.
User 'odaikuji' with ID 101 will be updated in the system. THIS OPERATION CANNOT BE UNDONE. Proceed (y/n):
```

The application can be run in non-interactive mode by supplying the parameters **-u <username> --no-prompt** where <username> is the login of the user.

2.2 OUT OF SCOPE

Information within the main databases of SafeQ are affected when this application is run. It does not modify system logs, archives of reports that an administrator or manager may have created, or print data files residing on YSoft SafeQ servers.

The following versions are not supported:

- YSoft SafeQ 4, any SR
- YSoft SafeQ 5, any MU

Support has not been tested for versions of YSoft SafeQ 6 prior to MU17. The solution only supports the first tenant in multi-tenant installations.

3 RIGHT TO ACCESS

rta.exe provides a human-readable document containing all of a Data Subject's information collected. For completeness, this report includes details on all available print jobs, user details, statistics from the data warehouse web reporting, as well as information from the DataMart, if enabled. The report can be quite large, especially if the user is a heavy printers. Note that print job titles are included, as users may print personal documents with sensitive titles.

The output is a simple HTML document with minimal CSS styling for better readability. Also note that an explanation of the data is included at the head of the document.



YSoft SafeQ Right to Access Request

Prepared for: Oda, Ikuji

Prepared on: 2018-05-17 14:27:23

Table of Contents

- [Disclaimer](#)
- [Basic User Details](#)
- [Authentication and Access History](#)
- [Recent Print Jobs](#)
- [Recently Accounted Jobs](#)
- [Cumulative Job Statistics](#)
- [Full Job Statistics for Recent Jobs](#)
- [Details Collected From the DataMart](#)

Disclaimer

This report fulfills a request filed by the Data Subject **Oda, Ikuji** to access records that were collected and processed on their behalf, with regard to YSoft SafeQ. YSoft SafeQ collects and manages personal data under the European Union's General Data Protection Regulation. While some of this information may be considered sensitive information under the law, this report discloses sensitive information about them.

The collected information is split into eight different sections. **Basic User Details** contains basic attributes about the data subject, including their network login ID, given and family name, user authenticated to a multifunction printer, network printer, or 3D printer monitored by YSoft SafeQ, to protect company proprietary data, only the id of the printer is included. **Recent Print Jobs** contains the estimated number of pages may not match the actual number of pages printed, but is included for completeness. Similarly, **Recently Accounted Jobs** contains the accounting types associated with the same print job. As an example, a print job may contain the following accounting types:

YSoft SafeQ also maintains a separate database called the data warehouse. The purpose of this database are for long-term statistics, and to provide an interface to allow customers to view their print statistics and **Full Job Statistics for Recent Jobs** aggregate statistics for built-in web reporting. For third-party applications, an administrator or reporting specialist will instead refer to the **DataMart** is formatted to show any records that are both confirmed to contain personal information, as well as additional fields that may or may not contain personal information.

Not all fields will contain particularly useful information. Fields may be marked as unknown, (empty), or similar values when the column doesn't correspond to the associated job title. For example, the **3D Print Jobs** section doesn't make sense with 3D Print jobs.

Basic User Details

User Attribute	Value
Login	odaikuji
Name	Ikuji
Surname	Oda

4 RIGHT TO RESTRICTION OF PROCESSING

The executable **rtr.exe** is also a simple command-line application that can be used in interactive or non-interactive mode. This application requires configuration in advance by setting up a separate, restricted database that the system can use to store data about a user to preserve the information and to keep it from being processed further. It then creates a pseudonym in YSoft SafeQ's systems for the user and redacts all other references to a Data Subject, including file names. Once a request has expired, or there is a need to re-identify the user, the -R flag will allow the administrator to reverse the process.

5 RIGHT TO ACCESS - RTA.EXE

5.1 NAME

rta - YSoft SafeQ 6 GDPR Right to Access CLI

5.2 SYNOPSIS

```
rta [-u login] [-o outputDir] [-V] [-l logFileName] [--log-file-trace logFileName] [--log-file-debug logFileName] [--log-file-info logFileName] [--log-file-warning logFileName] [--log-file-error logFileName] [--log-file-critical logFileName] [--version]
```

5.3 DESCRIPTION

YSoft SafeQ 6 - GDPR Right to Access CLI. Allows an administrator to execute a Data Subject's right to access. The program works by retrieving all references to structured and unstructured data within the YSoft SafeQ 6 databases related to the user, and exporting them to a single Hypertext Markup Language (HTML) file. The application must be run on one of the YSoft SafeQ 6 Management servers, as it references the configuration files to connect to the database.

The following information is stored in the HTML file:

- User: The contents of the row that specifies the user
- Aliases: All known aliases of the user
- Terminal Accesses: List of times the user was identified accessing a Terminal
- Job Details: Detailed record of print job metadata collected related to the user, including file names and job titles
- Job Accounting: List of print, copy, scan and faxing accounting data associated with the user
- Data Warehouse: List of information related to the user stored in the Data Warehouse and DataMart

The template for the HTML file is located in the same directory as the application. Minor modifications, such as changing the CSS Stylesheet formatting or the verbiage explaining the data, can be performed by anyone familiar with HTML, however it is not recommended to modify any section containing reserved name placeholders (words in all capital letters, with an ampersand at the beginning and end). Records in log files on YSoft SafeQ servers will not be provided.

5.4 OPTIONS

-u, --user <login> User to remove from the system

-o, --outputDir <directory> Output directory for the report to be delivered to

-r, --random-retries <Number> The number of times to generate a random number until failure.
Default 1000

-V, -VV, -VVV Increase logging level to (-V) INFO, (-VV) DEBUG, or (-VVV) TRACE

-l, --log <logFileName> Specify the log file where output will be sent

--log-file-trace <logFileName> Specify the log file where trace level logging will be sent

--log-file-debug <logFileName> Specify the log file where debug level logging will be sent

--log-file-info <logFileName> Specify the log file where info level logging will be sent

--log-file-warning <logFileName> Specify the log file where warning level logging will be sent

--log-file-error <logFileName> Specify the log file where error level logging will be sent

--log-file-critical <logFileName> Specify the log file where critical level logging will be sent

--version Print version and exit

6 RIGHT TO BE FORGOTTEN - RTBF.EXE

6.1 NAME

rtbf - SafeQ 6 GDPR Right to be Forgotten CLI

6.2 SYNOPSIS

```
rtbf [-u login] [-n] [-r] [-V] [-l logFileName] [--log-file-trace logFileName] [--log-file-debug logFileName] [--log-file-info logFileName] [--log-file-warning logFileName] [--log-file-error logFileName] [--log-file-critical logFileName] [--version]
```

6.3 DESCRIPTION

SafeQ 6 - GDPR Right to be Forgotten CLI. Allows an administrator to execute a Data Subject's right to be forgotten. The program works by anonymizing all references to structured and unstructured data within the YSoft SafeQ 6 databases related to the user. The application must be run on one of the SafeQ 6 Management servers, as it references the configuration files to connect to the database.

Tables impacted include:

- Print Jobs: Job titles, file names, and origins will be changed to <DELETED>. Favorited jobs will be un-favorited.
- Cards: Cards and PINs associated with the Data Subject will be removed.
- Aliases: Any aliases will be removed.
- PIN History: If PIN history is enabled, all records of a Data Subject's PIN history will be removed.
- Roles: If the Data Subject has any roles specifically associated with them, they will be disassociated from them
- Terminal Accesses: Any records of accessing terminals will be removed.
- Email Stats: Any scheduled statistics and counter reports to be sent to the data subject will be removed.
- Data Warehouse: References to the Data Subject in the Data Warehouse and the DataMart will be anonymized
- User: Name, surname, home directory, email, password (if relevant), extended ID, and notes will be cleared out. The login will be anonymized, and the source

The Data Subject's user login is anonymized, but still unique. All anonymized users will have a login of "DELETED_" followed by a large random number.. Due to the uniqueness of each customer environment and identity management systems, it may still be possible to identify a Data Subject using knowledge aggregated from systems outside of YSoft SafeQ. As an example, a user may be the only member of a Cost Center, or may have been known to be the only person to print at a specific time.

Records in log files on SafeQ servers will not be anonymized. However, the logs will be rotated out and the user will eventually have their data removed. Any previously exported reports will also not be anonymized.

6.4 OPTIONS

-n, --no-prompt Do not prompt for confirmation

-u, --user <login> User to remove from the system

-r, --random-retries <Number> The number of times to generate a random number until failure. Default 1000.

-v, -vv, -vvv Increase logging level to (-v) INFO, (-vv) DEBUG, or (-vvv) TRACE.

-l, --log <logFileName> Specify the log file where output will be sent

--log-file-trace <logFileName> Specify the log file where trace level logging will be sent

--log-file-debug <logFileName> Specify the log file where debug level logging will be sent

--log-file-info <logFileName> Specify the log file where info level logging will be sent

--log-file-warning <logFileName> Specify the log file where warning level logging will be sent

--log-file-error <logFileName> Specify the log file where error level logging will be sent

--log-file-critical <logFileName> Specify the log file where critical level logging will be sent

--version Print version and exit

6.4.1 RUNNING IN UNATTENDED MODE

rtbf -n -u <login>

If a batch of requests need to be processed, the above statement will not require any prompt to complete the action, and will supply the name. Specifying a log file will allow an Administrator to check on the success or failure of each individual request by using the -l <logFileName> attribute.

7 RIGHT TO RESTRICTION OF PROCESSING - RTR.EXE

7.1 NAME

rtr - SafeQ 6 GDPR Right to Restriction CLI

7.2 SYNOPSIS

```
rta [-u login] [-n] [-R] [-r numRetries] [-V] [-l logFileName] [--log-file-trace logFileName] [--log-file-debug logFileName] [--log-file-info logFileName] [--log-file-warning logFileName] [--log-file-error logFileName] [--log-file-critical logFileName] [--version]
```

7.3 DESCRIPTION

SafeQ 6 - GDPR Right to Restriction of Processing CLI. An Administrator can restrict further processing of a Data Subject in SafeQ by replacing the user's login and personal data with a pseudonym. Note that doing so will prevent the user from continuing to use the solution, and should only be used if the user is not expected to interact with YSoft SafeQ while their data is restricted.

A separate database must be created and properly configured so that the application can store mapping tables between the Pseudonym and the actual Data Subject. The restricted database can be either PGSQL or MSSQL, A companion configuration file, rtr-db.conf, must be modified by the database administrator with the proper connection information. The password can be encoded using the widget on the Management server's dashboard. The first time the application is run with a successful connection to the restricted database, the user will be asked to create the schema. Consult with your company's legal team on ensuring the database is isolated and properly protected from processing by unauthorized third parties.

Tables impacted include:

- Print Jobs: Job titles, file names, and origins will be changed to RESTRICTED. Favorited jobs will be un-favorited.
- Cards: Cards and PINs associated with the Data Subject will be removed.
- Aliases: Any aliases will be removed.
- Terminal Accesses: Any records of accessing terminals will be removed.
- Data Warehouse: References to the Data Subject in the Data Warehouse and the DataMart will be changed to RESTRICTED
- User: Name, surname, home directory, email, password (if relevant), extended ID, and notes will set to RESTRICTED or cleared out. The login will be changed to a pseudonym.

- Mobile Terminal Tokens and Codes will be completely removed. Users will need to be issued new tokens or codes.

The Data Subject's user login is pseudonymized, and still unique. All pseudonymized users will have a login of "restricted_" followed by a large random number.. Due to the uniqueness of each customer environment and identity management systems, it may still be possible to identify a Data Subject using knowledge aggregated from systems outside of YSoft SafeQ. As an example, a user may be the only member of a Cost Center, or may have been known to be the only person to print at a specific time.

Records in log files on SafeQ servers will not be pseudonymized. However, the logs will be rotated out and the user will eventually have their data removed. Any previously exported reports will also not be pseudonymized.

7.4 OPTIONS

- u, --user <login>** User to remove from the system
- n, --no-prompt** Do not prompt for confirmation
- o, --outputDir <directory>** Output directory for the report to be delivered to
- R** Lift the restriction of processing on the user
- r, --random-retries <Number>** The number of times to generate a random number until failure. Default 1000.
- V, -VV, -VVV** Increase logging level to (-V) INFO, (-VV) DEBUG, or (-VVV) TRACE.
- l, --log <logFileName>** Specify the log file where output will be sent
- log-file-trace <logFileName>** Specify the log file where trace level logging will be sent
- log-file-debug <logFileName>** Specify the log file where debug level logging will be sent
- log-file-info <logFileName>** Specify the log file where info level logging will be sent
- log-file-warning <logFileName>** Specify the log file where warning level logging will be sent
- log-file-error <logFileName>** Specify the log file where error level logging will be sent
- log-file-critical <logFileName>** Specify the log file where critical level logging will be sent
- version** Print version and exit