SoftWatch

Data Security

and

Data Privacy Protection

Guidelines

Table of Contents

Version Changes

#	Change Description	Pages	Changed by	Date	Version
1.	New Document	All	Yariv M.	June 19th, 2017	V1.0
2.	Filter Machines: Typo correction	9	Yariv M.	Aug. 31st, 2017	V2.0
3.	Update	1	Reut R.	Aug. 06th, 2018	V2.0

Purpose

Data Security and Personal Data Protection have become a widespread practice worldwide. New EU regulations entered into force in May 2016 and were applied as of May 2018, forcing all EU member countries to adopt them as a standard. SoftWatch operates in both NA and Europe, in compliance with these new standards, as will be presenting in this document.

Data Security

a. Hosting

SoftWatch backend servers are hosted by Amazon Web Services (AWS)* in two locations:

- NA - AWS East (North Virginia and Ohio) for companies that are based in the Americas.
- Europe (Frankfurt) for companies that are based in Europe.

b. **Security**

By using the AWS platform, which complies with the highest security standards that are available on the market today, SoftWatch adopts these standards as well. SoftWatch incorporates into its solution additional security layers:

- AV software that is installed on its development machines, protecting from viruses, malware, phishing etc.
- Connection to the SoftWatch GUI is made over a secured connection (https).
- SoftWatch's traffic between the CollectIT agent and backend server is encrypted.

c. Data Access

Access to customer data is limited:

- Access to the data is allowed only via the SoftWatch GUI
- SoftWatch uses users access control, allowing each customer to decide who is the personnel authorized to access the software GUI. The users list is maintained by the customer's appointed administrator. Since each customer's data is stored in separate tables, it is impossible to mistakenly view other customer's data.
- SoftWatch may access the data with the customer's consent.

d. Account Expiration and Data Disposal

Once the account expiration date has been reached, a customer may ask SoftWatch to delete all his data from SoftWatch servers and data deletion will be performed within a few days. Since all data resides on AWS virtual environment, there is no need to shred any physical hardware or take any additional precautions in order to ensure that there are no data "leftovers" after the deletion.

*** Additional information about AWS solution can be found under the following link:**
https://aws.amazon.com/about-aws/global-infrastructure/

Personal Data Protection

In addition to ensuring data security as demonstrated above, SoftWatch keeps strict Personal Data Protection guidelines:

a. **Hosting**

European-based companies' data is kept on AWS servers located in Frankfurt, therefore it is ensured that all data, including personal data, is **kept within the EU.**

NA-based companies data is kept on AWS servers located either in North Virginia or Ohio.

b. **Passwords Policies**

Since the users lists and passwords are maintained by the customer's appointed administrator, passwords can be set according to the different customers' policies. There is no limitation to any password policy.

c. **Additional Encryption**

SoftWatch allows using two types of CollectIT agents – "non-encrypted" (default) and "encrypted".

In both cases, the traffic between the agent and the backend servers is SSL encrypted. The "encrypted" agent allows additional MD5 encryption of the User Name/Machine Name/Domain Name. Consequently, by using the encrypted agent, the User Name, Machine Name and Domain Name will appear as meaningless strings in the SoftWatch GUI and will not reveal the real names behind them. The MD5 encryption is unidirectional, therefore it can only be decrypted by the customer.

Please refer to **Appendix A** for additional information.

d. **The Right to be Forgotten**

To allow customers to comply with this principle, SoftWatch provides the option of excluding specific users from the SoftWatch data collection (Opt-Out). The Opt-Out process can be implemented in several levels:

- Specific machines' traffic can be blocked on the SoftWatch backend Servers side.
- Specific users can be blocked on the SoftWatch backend servers side.
- Specific users can be blocked on the SoftWatch CollectIT agent side.
- The CollectIT agent can be removed from specific machines, by the customer's IT department.

In addition, SoftWatch allows deleting user and machine data from the system, even if data has already been collected for them.

Please refer to **Appendix B** for screen captures.

e. Account Expiration and Data Disposal

Once an account expires and SoftWatch is requested to delete all the account information, SoftWatch will delete all the information, including personal data (user names etc.) that has been collected or imported to the system during the usage period. SoftWatch does not keep any information or record once an account has been deleted.

f. Data Usage Authorization

SoftWatch will never use the data collected for any purpose other than the one for which license have been purchased and as agreed between the customer and SoftWatch. SoftWatch will never share any data with any 3rd party, unless requested and authorized by the customer or agreed between the customer and SoftWatch. Any such request, authorization or agreement shall be made in writing.

Appendix A: CollectIT Agent Data Encryption

a) **Data Encryption in Use by SoftWatch**

SSL encryption is always used to secure the data in transit between the Agent and the Web platform.
In addition, SoftWatch offers optional MD5 encryption for data at rest. Each customer can decide whether to use this option or not.

b) **MD5 Encryption Method Description**

To encrypt the data - username, machine name, domain name - we:

- capitalize the data (e.g. User and UsEr == USER)
- MD5 the capitalized string and send that data from the Agent to the Web platform. As a result, instead of having the username / machine name / domain name shown on the Web user interface, we will have an encrypted string. There will be no option for anyone to decrypt this string back to username / machine name / domain name.
- All data is encrypted before it leaves the agent.

c) **In order to make sense of the data the Admin user should:**

create a spreadsheet with a list of usernames (uppercase only) in column A and another column with its matching MD5 hashing. The data from our web UI should be downloaded to a spreadsheet.
A Vlookup function should be used to cross-match data based on the MD5 strings that should be identical in both Spreadsheets.

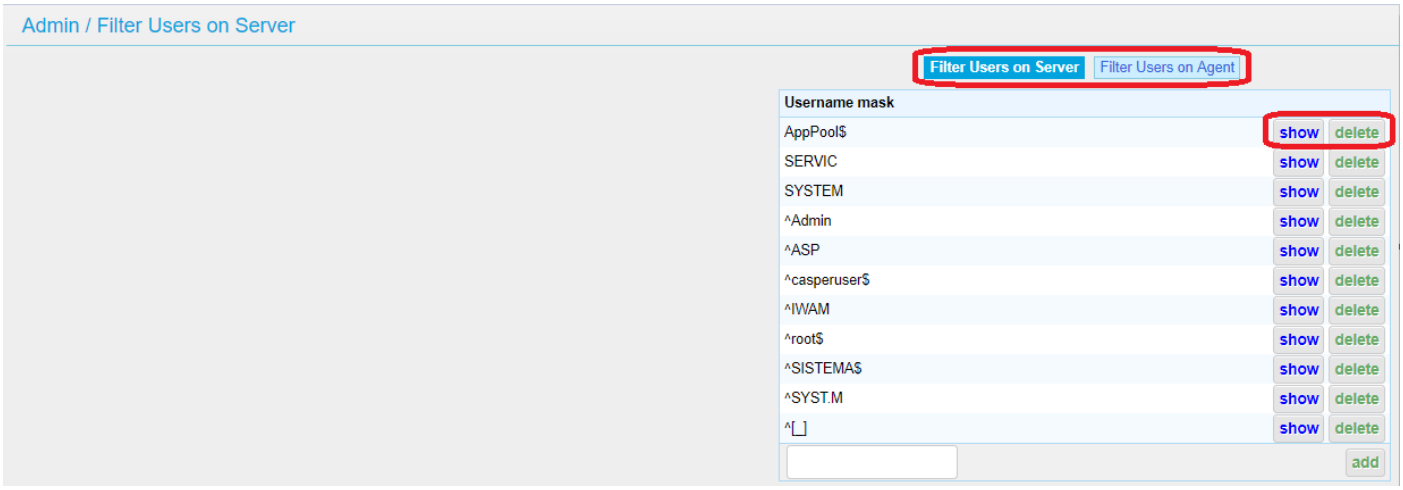
d) **Example:**

Assuming that a user name is Danny, MD5 hashing will be performed for “DANNY” and its result is:
username_hash = md5(strtoupper("Danny")) = md5("DANNY") = "e3981fbbff99da7bdbff05410c9e1637"

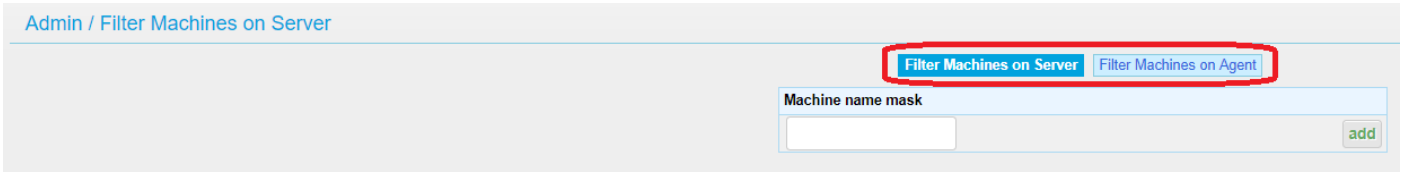
"e3981fbbff99da7bdbff05410c9e1637" is the string that is stored on our system for username “Danny” and should be used as the lookup value for the spreadsheets cross-match.

Appendix B: Users and Machines Opt-Out

Filter Users on Server / Agent



Filter Machines on Server / Agent



Delete Existing Users / Machines