H+H Software

Hidden Automatic Navigator

Version 4.5

Data Protection Administration

H+H Software GmbH
Maschmuehlenweg 8-10
37073 Goettingen
Phone: 0049 (0)551 52208-0
Fax: 0049 (0)551 52208-25
E-mail: hh@hh-software.com
Internet: www.hh-software.com

H+H vCard:

Contents

Introduction

This manual explains the data protection features of the software Hidden Automatic Navigator. It will help you to comply with your legal obligations regarding data protection.

Initial Startup

After installing Hidden Automatic Navigator it is important to protect your system and especially your data from unauthorized access.

- **Anonymous logging:** HAN anonymizes the data of users and computers in the call log by default. This simplifies your data processing to the extent that you can evaluate anonymized log data statistically without having to worry about the personal reference. The settings of the anonymization function are protected by password protection according to the two-man rule. This means that you assign two passwords to two employees and the setting can only be changed if both employees enter their passwords. For details on configuring this password protection, see "*Protect Anonymous Logging* 5".


The HAN pseudonymization replaces the clear name with a pseudonym. The replaced string is irretrievably deleted. In this respect, the HAN pseudonymisation is as secure as the anonymisation mechanism. However, the data is only guaranteed to be free of any personal reference if anonymisation has been used!

Data protection practices

- **Rectification, Restriction of Processing, Erasure:** When processing personal data, you are obliged to keep the data up to date. This results in the obligation to correct outdated or incorrect data immediately. In addition, you are obliged to immediately erase data of persons who are no longer involved in the procedure Hidden Automatic Navigator. In the event of disputes or pending legal proceedings, it may be necessary to restrict the data from processing. How to correct, restrict or erase personal data is explained in the chapter entitled „*Rectification, Restriction of Processing, Erasure* 6".
- **Create information about processed data:** According to the Data Protection Act, you are obliged to provide information on data upon request if a person affected by data processing by your institution so requests. How to create information about processed data in the software is explained in the chapter entitled "*Create Information about Processed Data*".

Disk Space Monitoring

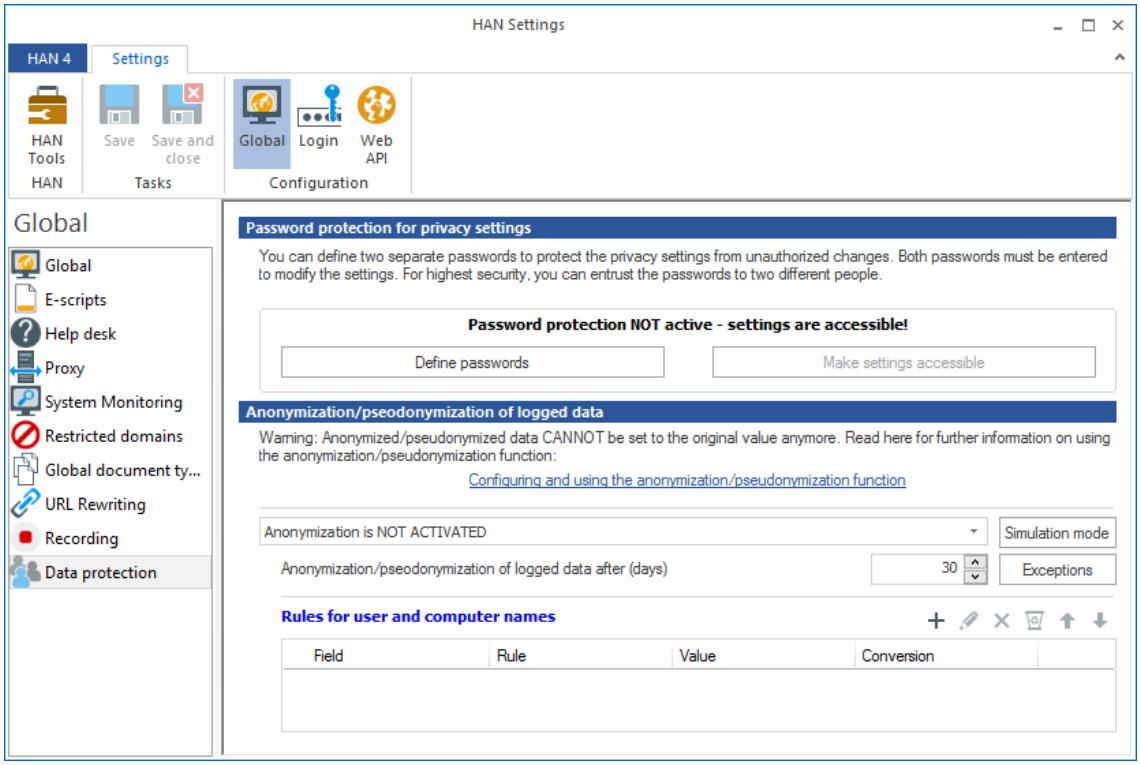
When operating HAN, the databases increase in size. This will result in more disk space being required over time than directly after installation. If the available disk space falls below a critical value, your HAN system will stop and not accept any further requests. To avoid this scenario, HAN continuously checks the available disk space. The settings of this system monitoring can be configured according to your requirements. In addition, the system monitoring has a notification function:

If the value falls below the limit you defined as critical, an e-mail will be sent. You freely define the recipient of this e-mail. So this is one of the locations of personal data in the HAN Settings program. How to configure the system monitoring is described in the HAN manual, chapter "*Configuration/Disk Space Monitoring*".

Correctly configured, the HAN system monitoring ensures the resilience of the system and services on a permanent basis.

Protect Anonymous Logging

The logging of program calls and related data is a core function of Hidden Automatic Navigator. Knowing who has worked with an e-resource for how long and when and whether they had to wait for a free license (queue) provides important information, e.g. about the utilization of your product licenses. However, logging personal data for statistical purposes is not without risk. If a data subject subsequently objects the use of his or her personal data, you would theoretically have to delete your entire statistical database, as specific data records can no longer be separated from the rest of the data afterwards. Therefore HAN logs usage data without logging the user or computer identifier. This anonymization mechanism is configured in the HAN settings, in the **Global** section, on the **Data Protection** page:



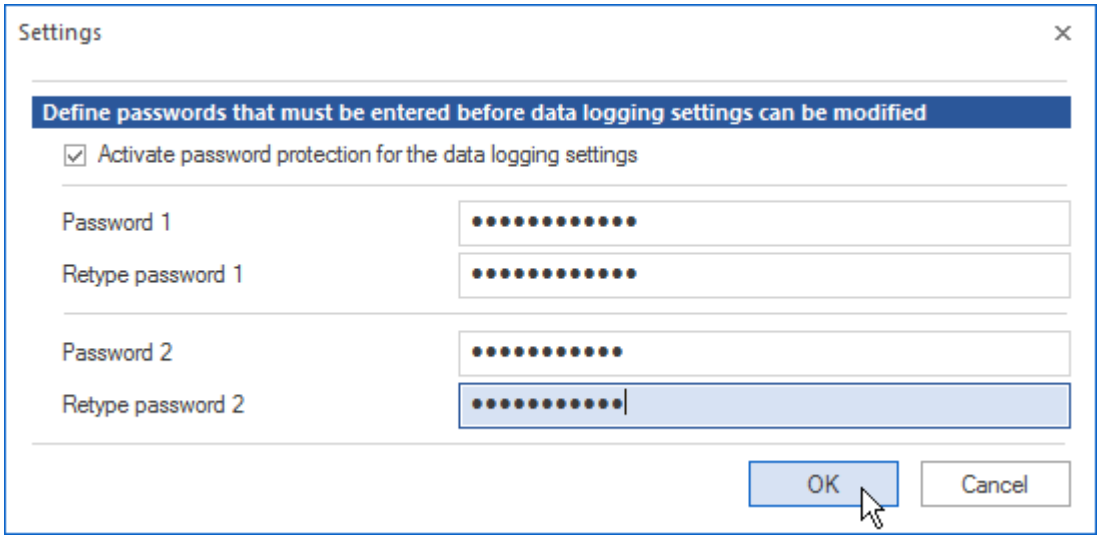
The screenshot above shows the state after installation: The logging of station and user names (**Anonymization/pseudonymization of logged data/Anonymization is NOT ACTIVATED**) is switched off. You have to protect this setting from unauthorized changes by restricting access. HAN offers password protection according to the two-man rule. You define two passwords and assign them to two different people. This increases security enormously, because it is no longer enough to acquire one of the passwords.

Before acceptance of the installation, the H+H installation team will address data protection measures and configure the settings according to your requirements.

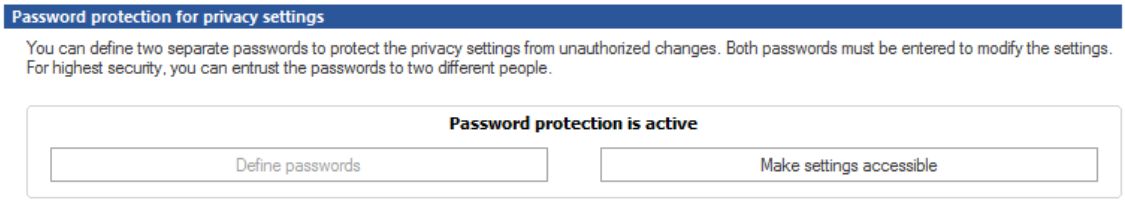
Set passwords

1. Click on the Define passwords button.

2. In the **Define passwords that must be entered before data logging settings can be changed** dialog enter two passwords and confirm with OK:



3. In the ribbon click on Save. The logging settings are now locked:



To unlock and change logging settings, you must enter both passwords.

A detailed description of the anonymization/pseudonymization function can be found in the HAN manual, in the chapter "*Anonymisation/Pseudonymisation of Record Data*".

Rectification, Restriction of Processing, Erasure

This chapter describes how to rectify, restrict and erase personal data in Hidden Automatic Navigator.

Rectifying data

If you learn of an error in personal data, you are obliged to correct (rectify) this error immediately. This is best done using the HAN programs. You need either access rights yourself or the assistance of an administrator.

For more information, see the following chapters:

- "*Data Locations* 7" describes where in HAN personal data may be stored.
- How to restrict personal data from processing is explained in the chapter entitled „*Restricting Personal Data from Processing* 8".
- How to erase personal data, or when personal data in HAN are erased automatically, is explained in the chapter entitled "*Erasure Periods/Erasing Data* 9".

Data Locations

To rectify, restrict or erase personal data in Hidden Automatic Navigator you need to know first where to find which personal data in the software:


All data are stored in the central HAN database. The database is password protected and access is limited using the HAN role concept. Instead of direct access to the database, however, we recommend you use the HAN programs, because they show the data in the appropriate context.

Data locations in Hidden Automatic Navigator

System:

- HAN E-Script Administration: Windows user name of the currently logged on user - HAN displays the currently logged on user in the program menu of the E-Script Administration. This information is read from the operating system environment and is not stored.
- E-Script Properties: user name, password—On the **Login** page script-specific login data is stored. These login data may - but do not have to - contain personal data.
- Script Editor: user names, passwords—In e-scripts that perform a login process, credentials may have a personal reference if no variables are used. This data is stored in the respective e-script.
- Data Editor: Station IDs, user names, IP addresses, variables if any, LDAP user names, AD user names - Permission objects and data groups may contain personal data.
- HAN Settings: In the HAN Settings program, personal data can be stored on several pages in different contexts:
  - **Proxy** page: user name, password
  - **System Monitoring** page: possibly sender, e-mail address, user name, password – This data belongs to the e-mail send in the event of an error.
  - **Authentication** page (authentication services configuration): IP addresses, user IDs, passwords—Most authentication services work with external databases and do not store any data. An exception is, for example, the IP authentication service, which, depending on the configuration, can allow conclusions to be drawn on natural persons.
  - **LDAP** page: user name, password
  - **EZB** page: user name
- User Administration: user names, passwords, HAN roles

Monitoring:

- Event Log: level, code, module, message, date, user, computer
- Web server access logs: IP addresses, user names, station names
- Web server error logs (error log, SSL log): IP addresses
- License Monitor: IP address, user, last access, session: start - end

Statistical analysis:

- Detailed access log: record ID, size of downloaded file, date, user, computer, status of print job, URL
- Summarized access log: record ID, size, time required, date, user, computer
- Statistics: record ID, usage, calls, start time, end time, user, station, bytes, attribute, document types, cost center, grouped record IDs, grouped users, grouped stations

 For statistical analysis, an anonymization or pseudonymization of personal data is available in HAN. If you use these, this data will be overwritten with a pseudonym or set empty after an interval you specify.

Restricting Personal Data from Processing

At this point, user data in HAN cannot be restricted from processing. To restrict a user, restrict him or her in your user system. As soon as the user no longer accesses HAN, no further data is processed of him in HAN monitoring or analysis tools. As far as the data of employees in storage locations such as HAN User Administration is concerned, we recommend that you delete these users and create them again later if necessary.

Erasure Periods/Erasing Data

In Hidden Automatic Navigator the data of the call log, which is indispensable for the statistical evaluation of the use of the system, are collected anonymously in order to enable a later statistical evaluation. However, the event and error logs also collect and store station and user information. Without this data, no analysis would be possible in the event of an error.

Either an automatic erasure mechanism or a manual erasure function has been implemented for this data. Please read below in which logs personal data are collected and stored and how they are erased:

Module	Erasing type	Erasing method
Event Log	Automatically	Capped; automatically overwritten when a certain file size is reached
Detailed access log	Automatically	According to selected interval in database maintenance
Summarized access log	Never/only anonymization	According to anonymization interval
Statistics	According to the underlying protocol	According to selected interval in database maintenance; exeption: Document types are not erased.
Web server access logs	Automatically/manually	Automatically according to anonymization interval, otherwise manually in the HAN System Settings program
Web server error logs (error log, SSL log)	Manually	In the HAN System Settings program

Index

A

D

E

I

P

R

T