H+H Software GmbH

Hidden Automatic Navigator

Version 4.5

Datenschutz-Administration

H+H Software GmbH
Maschmühlenweg 8-10
37073 Göttingen
Telefon: +49 (0)551 52208-0
Telefax: +49 (0)551 52208-25
E-Mail: hh@hh-software.com
Internet: www.hh-software.com

H+H vCard:

Inhalt

Einleitung

Dieses Handbuch erklärt Ihnen die Datenschutzfunktionen der Software Hidden Automatic Navigator. Es gibt Ihnen dabei Hilfestellung, Ihren gesetzlichen Pflichten bezüglich des Datenschutzes nachzukommen.

Der erste Start

Nach der Installation von Hidden Automatic Navigator gilt es, Ihr System und vor allem Ihre Daten vor unberechtigtem Zugriff zu schützen.

- **Anonyme Protokollierung:** HAN anonymisiert oder pseudonymisiert die Daten von Benutzern und Computern im Aufrufprotokoll. Dies vereinfacht Ihre Datenverarbeitung insofern, als dass Sie anonymisierte Protokolldaten frei statistisch auswerten können, ohne sich um den Personenbezug sorgen zu müssen. Die Einstellungen der Anonymisierungsfunktion sind durch einen Passwortschutz nach dem Vier-Augen-Prinzip geschützt. Das heißt, sie können zwei Passwörter an zwei Mitarbeiter vergeben und die Einstellung kann nur geändert werden, wenn beide Mitarbeiter jeweils ihr Passwort eingeben. Wie Sie diesen Passwortschutz konfigurieren, lesen Sie im Kapitel „*Anonyme Protokollierung schützen* 5".


Die HAN Pseudonymisierung ersetzt den Klarnamen durch ein Pseudonym. Die ersetzte Zeichenkette wird unwiederbringlich gelöscht. Insofern ist die HAN Pseudonymisierung ähnlich sicher wie der Anonymisierungsmechanismus. Garantiert frei von jeglichem Personenbezug sind die Daten jedoch nur, wenn die Anonymisierung verwendet wurde!

Datenschutzpraxis

- **Daten berichtigen, sperren, löschen:** Bei der Verarbeitung personenbezogener Daten sind Sie verpflichtet, die Daten aktuell zu halten. Hieraus ergibt sich die Pflicht, veraltete oder falsche Daten umgehend zu korrigieren. Außerdem sind Sie verpflichtet, Daten von Personen, die nicht länger am Verfahren Hidden Automatic Navigator teilnehmen, umgehend zu löschen. In Streitfällen oder bei schwebenden juristischen Verfahren kann eine Sperrung der Daten erforderlich werden. Wie Sie Daten berichtigen, sperren oder löschen, lesen Sie im Kapitel „*Berichtigen, Sperren, Löschen* 6".
- **Datenauskunft erstellen:** Laut Datenschutzgesetz sind Sie nach Antrag zu einer Datenauskunft verpflichtet, wenn ein von Datenverarbeitung durch Ihre Stelle Betroffener dies verlangt. Wie Sie eine Datenauskunft in der Software realisieren, lesen Sie im Kapitel „*Datenauskunft erstellen*".

Systemüberwachung

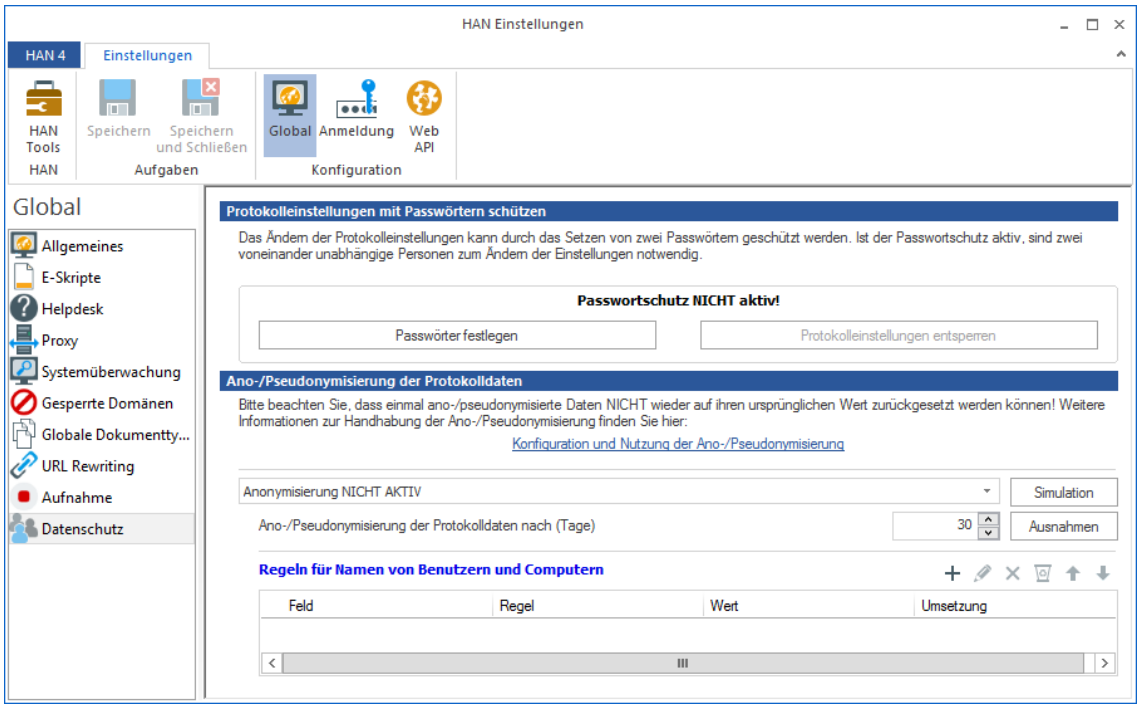
Beim Betrieb von HAN wachsen die Datenbanken. Dies führt dazu, dass mit der Zeit mehr Festplattenplatz benötigt wird, als direkt nach der Installation. Sollte der verfügbare Festplattenplatz einen kritischen Wert unterschreiten, wird Ihr HAN System stehen bleiben und keine weiteren Anfragen mehr annehmen. Um dieses Szenario zu vermeiden, kontrolliert HAN kontinuierlich den noch verfügbaren Festplattenplatz. Die Einstellungen dieser Systemüberwachung sind nach Ihren Bedürfnissen konfigurierbar. Zusätzlich verfügt die Systemüberwachung über eine Meldefunktion:

Beim Unterschreiten der von Ihnen als kritisch definierten Grenze wird eine E-Mail versendet. Den Empfänger dieser Mail definieren Sie frei. An dieser Stelle finden sich also in den HAN Einstellungen personenbezogene Daten. Wie Sie die Systemüberwachung konfigurieren, lesen Sie im HAN Handbuch, im Kapitel „Konfiguration/Festplattenplatz überwachen".

Richtig konfiguriert, unterstützt Sie die HAN Systemüberwachung bei der Umsetzung des Sicherstellen der Belastbarkeit der Systeme und Dienste auf Dauer.

Anonyme Protokollierung schützen

Eine Kernfunktion von Hidden Automatic Navigator ist die Protokollierung von Programmaufrufen und damit zusammenhängenden Daten. Das Wissen, wer wann wie lange mit einer E-Ressource gearbeitet hat und ob er auf eine freie Lizenz warten musste (Warteschlange), gibt wichtige Informationen, z.B. über die Auslastung Ihrer Produktlizenzen. Allerdings ist die Protokollierung personenbezogener Daten für die Statistik nicht ohne Risiko. Widerspräche ein von der Datenverarbeitung Betroffener im Nachhinein der Verwendung seiner persönlichen Daten, müssten Sie theoretisch Ihre gesamte statistische Datenbank löschen, da die Daten im Nachhinein nicht mehr von den restlichen Daten getrennt werden können. Deshalb protokolliert HAN standardmäßig Nutzungsdaten ohne Angabe von Benutzer oder Computer. Diesen Anonymisierungsmechanismus konfigurieren Sie in den HAN Einstellungen, in der Sektion **Global**, auf der Seite **Datenschutz**:



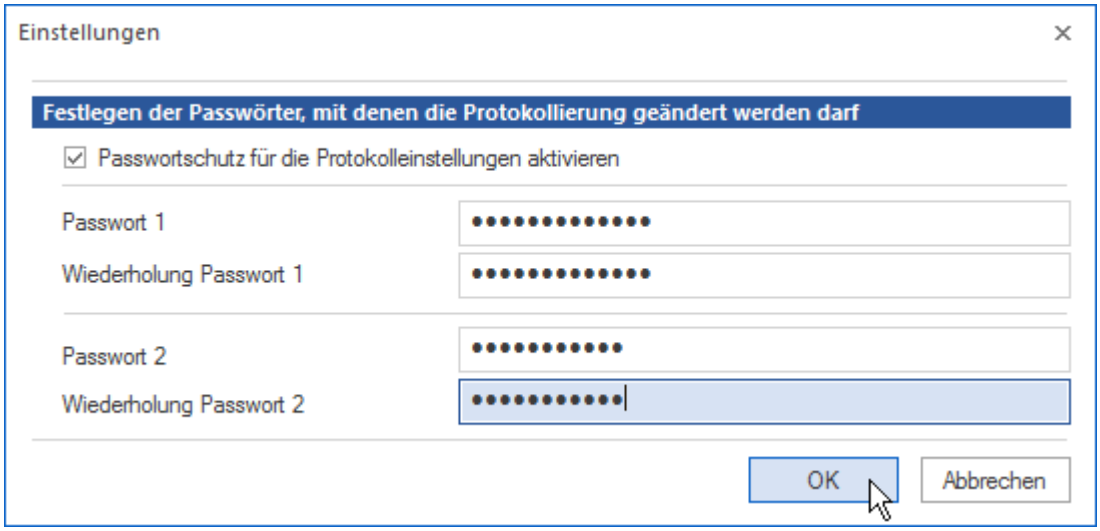
Der obige Screenshot zeigt den Zustand nach der Installation: Die Protokollierung von Stations- und Benutzernamen (**Ano-/Pseudonymisierung der Protokolldaten/Anonymisierung NICHT AKTIV**) ist abgeschaltet. Diese Einstellung müssen Sie vor unberechtigtem Zugriff schützen, indem Sie den Zugriff beschränken. HAN bietet hierfür einen Passwortschutz nach dem Vier-Augen-Prinzip. Sie definieren zwei Passwörter und vergeben diese an zwei unterschiedliche Personen. Dies erhöht die Sicherheit enorm, denn es reicht nun nicht mehr, in den Besitz eines Passwort zu gelangen.

Das H+H Installationsteam wird Sie vor der Abnahme der Installation auf das Thema Datenschutz ansprechen und die Einstellungen nach Ihren Wünschen konfigurieren.

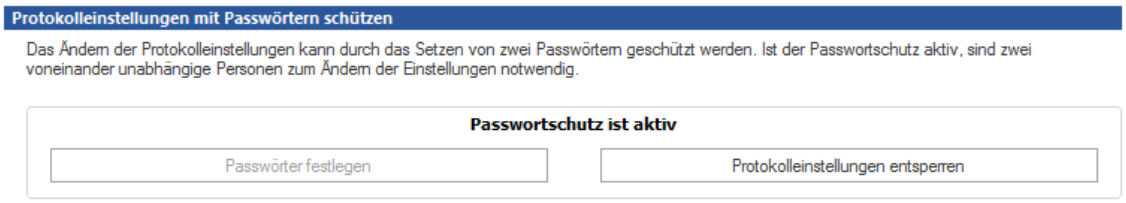
Passwörter festlegen

1. Klicken Sie die Schaltfläche Passwörter festlegen.

2. Im Dialog **Festlegen der Passwörter, mit denen die Protokollierung geändert werden darf** geben Sie zwei Passwörter ein und bestätigen über OK:



3. Klicken Sie im Menüband Speichern. Die Protokollierungseinstellungen sind nun gesperrt:



Zum Entsperren und Ändern der Protokollierung müssen Sie beide Passwörter eingeben.

Eine detaillierte Beschreibung der Anonymisierungs-/Pseudonymisierungsfunktion lesen Sie im HAN Handbuch, im Kapitel „*Anonymisierung/Pseudonymisierung von Protokolldaten*".

Berichtigen, Sperren, Löschen

Dieses Kapitel zeigt Ihnen, wie Sie personenbezogene Daten in Hidden Automatic Navigator berichtigen, sperren und löschen.

Berichtigen von Daten

Erfahren Sie von einem Fehler in personenbezogenen Daten, sind Sie dazu verpflichtet, diesen Fehler sofort zu korrigieren. Dies geschieht am besten über die HAN Programme. Sie benötigen entweder selbst entsprechende Zugriffsrechte oder die Assistenz eines Administrators.

Weitere Informationen lesen Sie in folgenden Kapiteln:

- „*Datenspeicherorte* 7" zeigt, wo in HAN personenbezogene Daten gespeichert sein können.
- Wie Sie personenbezogene Daten sperren, lesen Sie im Kapitel „*Sperren von Daten* 8".
- Wie Sie personenbezogene Daten löschen, bzw. wann personenbezogene Daten in HAN automatisch gelöscht werden, lesen Sie im Kapitel „*Löschfristen/Daten löschen* 9".

Datenspeicherorte

Um personenbezogene Daten in Hidden Automatic Navigator zu berichtigen, zu sperren oder zu löschen, müssen Sie zunächst wissen, wo Sie welche personenbezogenen Daten in der Software finden:

Alle Daten werden in der zentralen HAN Datenbank gespeichert. Die Datenbank ist passwortgeschützt und der Zugriff über das HAN Rollenkonzept begrenzt. Statt dem direkten Zugriff auf die Datenbank ist jedoch der Zugriff über die HAN Programme zu empfehlen, da dieser die Daten in den entsprechenden Zusammenhang stellt.

Datenspeicherorte in Hidden Automatic Navigator

System:

- HAN E-Skriptverwaltung: Windows-Benutzername des aktuell angemeldeten Benutzers – HAN zeigt im Programmmenü der E-Skriptverwaltung den aktuell angemeldeten Benutzer. Diese Information wird aus dem Environment des Betriebssystems ausgelesen und nicht gespeichert.
- E-Skripteigenschaften: Benutzername, Passwort – Auf der Seite **Anmeldung** werden skriptspezifische Anmeldedaten hinterlegt. Diese Anmeldedaten können – müssen aber nicht – personenbezogene Daten enthalten.
- Skripteditor: Benutzernamen, Passwörter – In E-Skripten, die einen Anmeldevorgang abbilden, können Anmeldedaten einen Personenbezug aufweisen, falls keine Variablen verwendet werden. Diese Daten sind in dem jeweiligen E-Skript gespeichert.
- Dateneditor: Stationskennungen, Benutzernamen, IP-Adressen, ggf. Variablen, LDAP-Benutzernamen, AD-Benutzernamen – In Berechtigungsobjekten und in Datengruppen können personenbezogene Daten enthalten sein.
- HAN Einstellungen: In den Einstellungen können auf mehreren Seiten in unterschiedlichen Kontexten personenbezogene Daten gespeichert sein:
  - Seite **Proxy**: Benutzername, Passwort
  - Seite **Systemüberwachung**: ggf. Absender, E-Mailadresse, Benutzername, Passwort – Diese Daten betreffen alle die E-Mail im Fehlerfall.
  - Seite **Authentifizierung** (Konfiguration der Authentifizierungsdienste): IP-Adressen, Benutzer-IDs, Passwörter – Die meisten Authentifizierungsdienste arbeiten mit den externen Datenbanken und speichern keine Daten. Eine Ausnahme ist z.B. der IP-Authentifizierungsdienst, der, je nach Konfiguration, Rückschluss auf natürliche Personen ermöglichen kann.
  - Seite **LDAP**: Benutzername, Passwort
  - Seite **EZB**: Benutzername
- Benutzerveraltung: Benutzernamen, Passwörter, HAN Rollen

Monitoring:

- Ereignisanzeige: Level, Code, Modul, Nachricht, Datum, Benutzer, Computer

- Webserver-Zugriffsprotokolle: IP-Adressen, Benutzernamen, Stationsnamen
- Webserver-Fehlerprotokolle (Fehlerprotokoll, SSL-Protokoll): IP-Adressen
- Lizenzmonitor: IP-Adresse, Benutzer, Letzter Zugriff, Sitzung: Start - Ende

Statistische Auswertung:

- Detailliertes Protokoll: Protokoll-ID, Größe der heruntergeladenen Datei, Datum, Benutzer, Computer, Status des Druckauftrags, URL
- Summiertes Protokoll: Protokoll-ID, Größe, Benötigte Zeit, Datum, Benutzer, Computer
- Statistik: Protokoll ID, Nutzung, Aufrufe, Startzeit, Endzeit, Benutzer, Station, Bytes, Attribut, Dokumenttypen, Kostenstelle, Gruppierte Protokoll-IDs, Gruppierte Benutzer, Gruppierte Stationen

 Für die statistische Auswertung ist in HAN eine Anonymisierung oder Pseudonymisierung der personenbezogenen Daten verfügbar. Falls Sie diese verwenden, werden diese Daten nach einem von Ihnen festgelegten Intervall mit einem Pseudonym überschrieben oder leer gesetzt.

Daten sperren

Benutzerdaten in HAN können zurzeit nicht gesperrt werden. Um einen Benutzer zu sperren, sperren Sie ihn in Ihrem Benutzersystem. Sobald der Benutzer keine Zugriffe mehr über HAN ausführt, werden auch keine weiteren Daten von ihm in Monitoring- oder Analysewerkzeugen von HAN verarbeitet. Was die Daten von Mitarbeitern an Speicherorten wie der Benutzerverwaltung angeht, empfehlen wir, diese Benutzer zu löschen und später ggf. wieder anzulegen.

Löschfristen/Daten löschen

In Hidden Automatic Navigator werden Nutzungsdaten, das für die statistische Auswertung der Nutzung des Systems unabdingbar ist, anonymisiert erhoben, um auch eine spätere statistische Auswertung möglich zu machen. Die Ereignis- und Fehlerprotokolle erheben und speichern jedoch auch Angaben zu Station und Benutzer. Ohne diese Daten wäre keine Analyse im Fehlerfall möglich.

Für diese Daten wurde entweder ein automatischer Löschmechanismus oder eine manuelle Löschfunktion implementiert. Lesen Sie im Folgenden, in welchen Protokollen personenbezogene Daten erhoben und gespeichert werden und wie sie gelöscht werden:

Modul	Löschart	Löschmethode
Ereignisanzeige	Automatisch	Capped; wird bei Erreichen einer bestimmten Dateigröße automatisch überschrieben
Detailliertes Protokoll	Automatisch	Nach gewähltem Intervall in der Datenbankwartung
Summiertes Protokoll	Nie/nur Anonymisierung	Gemäß Anonymisierungsintervall
Statistik	Gemäß zugrundeliegendem Protokoll	Nach gewähltem Intervall in der Datenbankwartung; Ausnahme: Dokumenttypen werden nicht gelöscht.
Webserver-Zugriffsprotokolle	Automatisch/manuell	Automatisch gemäß Anonymisierungsintervall, ansonsten manuell in den Systemeinstellungen
Webserver-Fehlerprotokolle (Fehlerprotokoll, SSL-Protokoll)	Manuell	In den Systemeinstellungen

Index

A

B

D

E

L

P

S

V