

ⓓ Bedienungsanleitung

Passwort-Manager RF-PM-01

Best.-Nr. 1593964

Bestimmungsgemäße Verwendung

Der renkforce Passwort-Manager dient dem sicheren Speichern und Umgang mit Benutzernamen und Passwörtern für bis zu 100 Internetseiten. Moderne Verschlüsselungsalgorithmen (AES256, SEED 256, ARIA) schützen jegliche Eingaben vor unerlaubtem (Hardware-) zugriff. Geschützt durch ein übergeordnetes „Masterpasswort“ (6-120 Zeichen) können die Zugangsdaten für hinterlegte Webseiten automatisch eingegeben werden, ohne Übertrag in die Zwischenablage.

Zu Ihrer Datensicherheit wird der gespeicherte Inhalt - Ihre Zugangsdaten - nach sechs Fehleingaben in Folge automatisch gelöscht und kann nicht wieder hergestellt werden. Schützen Sie das Produkt vor Missbrauch und ermöglichen Sie sich die Wiederherstellung bei verloren gegangenen Zugangsdaten.

Es sind jeweils für Benutzername bis zu 300 Zeichen und Passwort maximal 120 Zeichen vorgesehen. Zusätzlich können kurze Notizen (max. 150 Zeichen) zu jeder Webseite abgespeichert werden. Das Produkt ist geeignet ein- und zweistufige Loginfenster (vergl. Google-Anmeldung) zu bedienen.

Um das Produkt nutzen zu können, muss auf dem Computer ein Programm ausgeführt werden. Dieses ist im Lieferumfang enthalten und befindet sich auf dem USB-Passwort-Manager — lokal gespeichert. Vergewissern Sie sich, dass Sie auf dem genutzten Computer über die nötigen Rechte verfügen. Durch die Plug-and-Play Funktionalität ist keine Installation nötig. Das Ausführen genügt. Es werden die Windows Betriebssysteme ab Windows 7 und neuer unterstützt. Über die folgenden Browser können Sie sich mit diesem Produkt automatisch anmelden: IE, Chrome, Opera, QQ, 360safe, Sogou, Firefox

Ihr Vorteil durch die Nutzung dieses Passwort-Managers: Sie können für verschiedene Webseiten unterschiedliche Zugangsdaten nutzen mit sicheren - aber oft schwierig zu merkenden Phrasen. Dabei sind Sie autark d.h. nicht an ein spezifisches Gerät oder einen verwaltenden Nutzeraccount gebunden. Das Produkt sollte sicher aufbewahrt werden, stellt jedoch bei unerwünschtem Zugriff oder öffentlichem Zugang durch Dritte keine unmittelbare Gefahr für den Eigentümer dar. Durch Weitergabe des Produktes mit dem zugehörigen Masterpasswort ermöglichen Sie eine einfache Übergabe von Zugangsdaten für eine Vielzahl an Webseiten. Besonders eignet sich das Produkt für Einzelpersonen mit hohem digitalen Sicherheitsanspruch, Abteilungen in Firmen oder zur einfachen Verwaltung des digitalen Erbes.

Lieferumfang

- Passwort-Manager
- USB-Schnittstellendeckel
- Betriebsanleitung



Aktuelle Bedienungsanleitungen

Laden Sie aktuelle Bedienungsanleitungen über den Link www.conrad.com/downloads herunter oder scannen Sie den abgebildeten QR-Code. Befolgen Sie die Anweisungen auf der Webseite.

Symbol-Erklärung



Das Symbol mit dem Ausrufezeichen im Dreieck weist auf wichtige Hinweise in dieser Bedienungsanleitung hin, die unbedingt zu beachten sind.



Das Pfeil-Symbol ist zu finden, wenn Ihnen besondere Tipps und Hinweise zur Bedienung gegeben werden sollen.

Sicherheitshinweise

Lesen Sie die Anleitung zu Ihrem Produkt vollständig und benutzen Sie das Produkt erst wenn Sie dessen Anwendung verstanden haben. Der Stick ist nach dem Verbinden mit einem (Windows-) Computer nach 30 s - 5 min einsatzbereit (abhängig von Ihrem Computer). Zum Teil wird das Gerät als „Defekter USB-Stick“ erkannt. Dies stellt keinen Fehler dar. Das Gerät ist kein klassischer Massenspeicher und reagiert auch nicht wie solch einer. Sollte der Passwort-Manager von Ihrem PC nicht erkannt werden, trennen Sie das Gerät kurzzeitig und verbinden Sie es erneut. Trennen Sie niemals das Produkt während eines Speicher- oder Initialisierungsvorgangs. Die Funktionalität kann für virtuelle Maschinen (VM) nicht garantiert werden. Behandeln Sie das Produkt sorgsam und setzen Sie es keinen Flüssigkeiten aus.

Wählen Sie ein sicheres, nur Ihnen bekanntes Masterpasswort. Dieses sollte zuvor nicht bereits von Ihnen anderweitig verwendet worden sein. Auch sollte sich dieses stark unterscheiden von Ihren anderen (bekannten) Passwörtern. Schlechte Passwortbeispiele sind z. B.:

MeinErstesPasswort -> MeinZweitesPasswort | Passwort123456 -> 123456Passwort

Informieren Sie sich über sichere Passwortempfehlungen. Diese ändern sich im Laufe der Zeit. Passen Sie Ihre verwendeten Passwörter regelmäßig an. Ändern Sie dabei nicht nur das Masterpasswort dieses Passwortmanagers. Auch Webseitenpasswörter werden mit verbesserter Technik unsicherer.

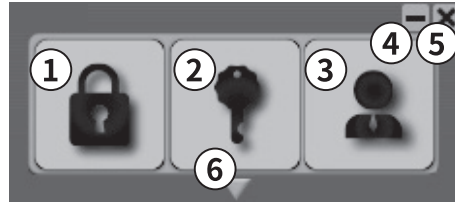
Ältere Webseiten unterstützen ggf. keine „redirection“, bei dem die eingegebene Webadresse auf die korrekte Seite weitergeleitet wird.

Beispiel: <https://conrad.com> —> <https://www.conrad.com>

Produktanwendung

Verbinden Sie den Passwort-Manager mit einem geeigneten Computer. Das Gerät wird als Laufwerk erkannt. Starten Sie (per Doppelklick) das Programm „Passwort Manager“ im „Windows Explorer“. Es öffnet sich ein Programmfenster. Wählen Sie Ihre bevorzugte Sprache aus und geben Sie ein sicheres Masterpasswort ein. Wiederholen Sie das Masterpasswort, um Tippfehler zu vermeiden.

Das Programmfenster besteht aus folgenden Bedienknöpfen:



- | | |
|--------------|--|
| 1 „Login“ | Meldet Sie automatisch (mit den gespeicherten Zugangsdaten) auf der aktuellen Webseite an. |
| 2 „Password“ | Fügt das Passwort der Webseite ein. |
| 3 „Manager“ | Öffnet ein Verwaltungsfenster. |
| 4 | Minimiert das Fenster auf die Taskleiste |
| 5 | Schließt das Programm |
| 6 | Favoritenübersicht (Pfeil am unteren Rand): zeigt die hinterlegten Webseiten an. Bei mehr als 8 Webseiten kann durch die gesamte Liste gelaufen (scroll) werden. |

a) Zugangsdaten im Passwort-Manager hinterlegen

- 1 Führen Sie den Passwort Manager aus. Klicken Sie auf die Eingabemaske der Website, für die Sie die Zugangsdaten hinterlegen wollen. Falls beispielsweise auf der Google Webseite bereits ein Account angemeldet ist, klicken Sie auf „Konto hinzufügen“ um Ihre Zugangsdaten für einen weiteren Google Account zu hinterlegen.
- 2 Sobald Sie Ihre Zugangsdaten hinterlegt haben, drücken Sie im Passwort Manager mit der linken Maustaste auf „Login“.
- 3 Das Fenster „Web Account hinzufügen“ erscheint. Die Websitebezeichnung und Internetadresse werden automatisch ausgefüllt. Nach bedarf können diese angepasst werden.
- 4 Bestätigen Sie den Account über „registrieren“. Die Zugangsdaten für weitere Websites können, wie in den Schritten zuvor beschrieben, erstellt werden.
- 5 Falls Sie für dieselbe Website einen weiteren Account hinterlegen wollen, klicken Sie mit der Maus auf die Eingabemaske der Website. Klicken Sie anschließend im Passwort Manager mit der rechten Maustaste auf „Login“.
- 6 Das Fenster „Web Account hinzufügen“. Gehen Sie wie in 3 und 4 vor.
- 7 Wenn Sie mit der linken Maustaste „Login“ drücken, erscheint eine Liste mit allen verfügbaren Accounts.

➔ Anstelle einer URL kann auch eine direkte IP-Adresse angegeben werden.

b) Zugang zu einer hinterlegten Webseite (Einstufiger Login)

- Einstufige Login sind dadurch gekennzeichnet, dass Sie im selben Fenster Passwort und Login-ID eingeben können.
- Klicken Sie mit der Maus in die oberste Eingabemaske einer registrierten Website (in der Eingabemaske sollte der Cursor blinken).
- Klicken Sie im Passwort Manager mit der linken Maustaste auf „Login“.
- Die Zugangsdaten für die Website werden automatisch ausgefüllt [Login-ID -> „Tab“ -> Passwort -> „Enter“].

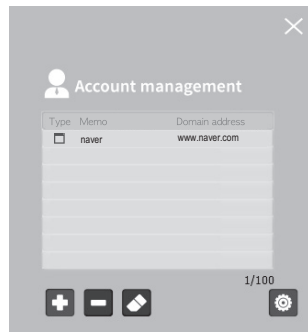
➔ Alternative Tastaturlayouts / Layoutwechsel können die eingegebenen Daten ändern und führen Login-Fehlschlägen.

c) Zugang zu einer hinterlegten Webseite (Mehrstufiger Login)

- Mehrstufige Login sind dadurch gekennzeichnet, dass alle benötigten Login Informationen getrennt nacheinander abgefragt werden. Es können nicht alle Login Informationen in einem Schritt eingegeben werden.
- Klicken Sie mit der Maus in die (einzige) Eingabemaske einer registrierten Website (in der Eingabemaske sollte der Cursor blinken).
- Klicken und halten Sie die Schaltfläche „Login“ mit der rechten Maustaste für mindestens 1 s. Es wird nur die Login-ID eingegeben, auch wenn Login-ID und Passwort hinterlegt sind.
- Klicken Sie nach der automatischen Passwordeingabe auf die entsprechende Schaltfläche (zb Next / Weiter / OK) auf der Webseite um zur nächsten Eingabemaske zu gelangen.
- Klicken Sie mit der Maus in die (einzige) Eingabemaske der Website (in der Eingabemaske sollte der Cursor blinken).
- Klicken und halten Sie die Schaltfläche (2) „Password“ mit der linken Maustaste für mindestens 1 s. Es wird das zur Login-ID zugehörige Passwort gefolgt von „Enter“ eingegeben. Ein Klicken ohne halten fügt nur das Passwort ein.

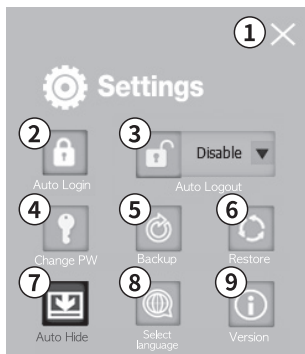
d) Löschen oder Anpassen von Zugangsdaten und Einstellungsmenu

- Klicken Sie auf die Schaltfläche Manager (3) oder Klicken sie rechts auf der Taskleiste im Menü des Passwort-Manager Programmes auf „Manager“ um in die Übersicht aller gespeicherten Passwörter zu gelangen.
- Mit Klick auf das Quadrat vor dem jeweiligen Eintrag wechseln Sie im Standardbrowser auf die entsprechende Webseite. Sind mehrere Login-Daten hinterlegt zu einer Webseite können Sie per Klick auf den Webseiteneintrag in dieser Liste das gewünschte Webseiten-Login auswählen. Dabei weist ein Kreuz in dem Quadrat vor einem Eintrag auf mehrere hinterlegte Logindaten hin.
- Mit dem Button + fügen Sie einen neuen Eintrag hinzu oder löschen den Gewählten mit dem Klick auf -. Das Radersymbol öffnet das Eingabefenster eines Webseiteneintrags für Änderungen. Möchten Sie einen Eintrag nur bedingt ändern (z. B. Passwort beibehalten) verändern Sie die jeweiligen Einträge nicht bzw machen Sie keinen Eintrag. Bei mehreren vorhandene Account wählen die den gewünschten aus für Änderungen oder Löschen.
- Per Klick auf das Kreuz in der rechten oberen Ecke schließen Sie das Managerfenster.



Einstellungen

Wechseln Sie aus dem Managementfenster per Zahnrad-Symbol in das folgende Fenster um eine der folgenden Funktionen auszuführen:



1 Schliessen

Mit Klick auf das Kreuzsymbol in der oberen rechten Ecke schließen Sie das Programmfenster.

2 Automatischer LOGIN

Wünschen Sie eine automatische Anmeldung des Passwort-Managers per Masterpasswort, aktivieren Sie diese Funktion und geben Sie anschließend Ihr Masterpasswort ein. Bestätigen Sie mit OK.

→ Sie können nicht gleichzeitig die Funktion automatischer Login und automatischer Logout aktivieren. Mit der Aktivierung dieser Funktion speichern Sie dauerhaft das Masterpasswort auf Ihrem Computer und schränken dadurch die maximal erreichbare Sicherheit ein.

3 Automatischer LOGOUT

Durch Aktivierung der automatischen Abmeldung (einstellbarer Zeitraum 1 min - 8 h) erscheint nach Ablauf der Zeit ein Informationsfenster. Mit dem Bestätigen („OK“) oder Versteichen der Zeit wird der Passwort-Manager automatisch abgemeldet. Durch betätigen des Knopfes „NO“ wird der Count-Down zurückgesetzt.



Sie können nicht gleichzeitig die Funktion automatischer Login und automatischer Logout aktivieren. Die Deaktivierung dauert Hardwarebedingt 1 -3 s. Eine Abmeldung von den eingeloggten Webseiten erfolgt nicht automatisch. Es wird eine Neuanmeldung mit den hinterlegten Accountinformationen verhindert.

4 Master-PASSWORT Ändern

Um das Masterpasswort des Passwort-Managers zu ändern, drücken Sie „Change PW“, geben Sie das aktuelle Masterpasswort ein, geben Sie ein neues Masterpasswort ein und wiederholen Sie dieses. Bestätigen Sie den Änderungswunsch.

5 BACKUP-FILE erstellen

Speichern Sie eine verschlüsselte Wiederherstellungsdatei (x.POP) auf Ihrem Gerät ab. Wählen Sie dazu die Schaltfläche „Backup“, geben Sie ein sicheres Verschlüsselungspasswort an und einen Speicherort auf Ihrem PC. Mit dieser Datei kann der Inhalt auf einen neuen Passwort-Manager übertragen werden.



Ohne das Verschlüsselungspasswort kann der Passwort-Manager nicht wieder hergestellt werden. Nutzen Sie nicht das selbe Passwort für Masterpasswort und Verschlüsselungspasswort.

6 Passwort-Manager Wiederherstellen

Stellen Sie den Backup-Zustand auf einem Passwort-Manager wieder her mit dem Klick auf „Restore“. Wählen Sie das gewünschte Backup (Dateiendung .POP), geben Sie das dazu passende Passwort ein und klicken Sie auf „Restore“.



Der aktuelle Inhalt des Passwort-Managers wird durch diesen Vorgang überschrieben.

7 Automatisches Einblenden

Diese Funktion Minimiert das Menüfenster nach einem Login per Klick auf den Menübutton „Password Manager“

8 Spracheinstellungen

Ändern Sie die Menüsprache zwischen D/GB/F/NL/I/PL mit dem Menüpunkt „Select Language“.



Die Sprachwahl ändert nicht das Tastaturlayout.

9 Versionsinformationen

Gibt die Aktuelle Version (Firmware, Software, und Seriennummer) Ihres Gerätes aus.

Update



Schließen Sie das Passwort-Managerprogramm auf dem Computer bevor die das Update durchführen. Entfernen Sie niemals die Hardware während des Updates. Erstellen Sie ein Backup vor dem Ausführen eines Updates.

Laden Sie sich das aktuelle Update (unter:) herunter und führen Sie dieses aus (Doppelklick). Beachten Sie die Warnung (siehe oben) und bestätigen Sie mit OK. Geben Sie das Masterpasswort ein und erstellen Sie im Folgenden ein Backup, falls wichtige Daten auf dem Passwort-Manager gespeichert sein sollten. Geben Sie ein Backuppasswort ein und wählen Sie einen Speicherort für das Backup. Nach erfolgreicher Produktidentifizierung und Verifizierung wird ein neues Betriebssystem auf den Passwort-Manager geschrieben. Nach erfolgreichem Update bestätigen Sie dieses mit OK, entfernen Sie das Gerät und verbinden Sie es erneut. Nach einem Update benötigt das Gerät zusätzlich bis zu einer Minute für die Initialisierung.

Fehlermeldungen

Typische Fehlermeldungen des Updates sind:

- Die Softwareversion des Programmes ist aktueller als die Version Ihres gewünschten Updateprogramms.
- Der Passwort-Manager konnte an Ihrem Gerät nicht erkannt werden. Schließen Sie das korrekt Gerät an.
- Update konnte nicht gestartet werden. Starten Sie Ihren Computer neu, schließen Sie das Produkt korrekt an und vergewissern Sie sich über die passenden Zugriffsrechte des Updates.
- Die Softwareversion des Installierten Programmes konnte nicht erkannt werden. Starten Sie Ihren Computer neu, schließen Sie das Produkt korrekt an und vergewissern Sie sich über die passenden Zugriffsrechte des Updates.
- File Write (FW) Fehler: Kommunikationsfehler während des Updates. Wiederholen sie den Vorgang. Starten Sie Ihren Computer neu, schließen Sie das Produkt korrekt an und vergewissern Sie sich über die passenden Zugriffsrechte des Updates.



Eventuell wird ein Fehler in englischer Sprache gekennzeichnet durch „Error“ ausgegeben.

Entsorgung



Elektronische Geräte sind Wertstoffe und gehören nicht in den Hausmüll. Entsorgen Sie das Produkt am Ende seiner Lebensdauer gemäß den geltenden gesetzlichen Bestimmungen.

Technische Daten

Softwareversion.....	1.7 (Basis dieser Anleitung)
Betriebsspannung.....	DC 5 V
Energieverbrauch	0.5 W
Schnittstelle	USB 2.0 High Speed (abwärtskompatibel)
Betriebsanzeige.....	Mehrfarbige LED
Verschlüsselungsalgorithmen.....	AES256, SEED 256, ARIA Hardwarebasierter Sicherheitschip
Gerätegruppe	Computer
Betriebssystem.....	Windows 7, Windows 8, Windows 10
Unterstützte Browser.....	Internet Explorer (IE), Chrome, Opera, QQ, 360safe, Sogou, Firefox
Produktabmessungen.....	26 x 79 x 14 mm
Gewicht.....	0,013 kg
Betriebstemperatur.....	0 bis 45 °C
Lagertemperatur.....	-20 bis 70 °C

Dies ist eine Publikation der Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92240 Hirschau (www.conrad.com).

Alle Rechte einschließlich Übersetzung vorbehalten. Reproduktionen jeder Art, z. B. Fotokopie, Mikroverfilmung, oder die Erfassung in elektronischen Datenverarbeitungsanlagen, bedürfen der schriftlichen Genehmigung des Herausgebers. Nachdruck, auch auszugsweise, verboten. Die Publikation entspricht dem technischen Stand bei Drucklegung.

© Copyright 2018 by Conrad Electronic SE.

1593964_V2_0118_02_VTP_m_de

Operating instructions

Password Manager RF-PM-01

Item no. 1593964

Intended use

The password manager renkforce is designed for safe storage and handling usernames and passwords for up to 100 websites. Modern encryption algorithms (AES256, SEED 256, ARIA) protect any entries from unauthorised (hardware) access. Protected by an overarching „master password“ (6-120 characters), access data for the introduced websites can be entered automatically without copying to clipboard.

To secure your data, the saved content - your access data - is deleted automatically after six erroneous entries in a row and cannot be restored again. Protect the product from misuse and enable the possibility of restoration in the event of the access data loss.

Up to 300 characters are reserved for usernames and maximum 120 characters for passwords. In addition, short notes (max. 150 characters) for every website can be saved. The product is suitable for one- and two-step login screens (compare Google login).

To be able to use the product, you must run a program on the computer. It is included in the scope of delivery and stored locally in the password manager on the USB drive. Make sure you have the necessary rights on the computer that you use. Due to the plug-and-play functionality, no installation is needed. It is enough just to launch it. The product is compatible with Windows operating systems starting with Windows 7 onwards. You can automatically login with this product using the following browsers: IE, Chrome, Opera, QQ, 360safe, Sogou, Firefox

Your advantage when using the password manager: You can apply varying access data for different websites using secure phrases that are often hard to memorise. While doing so, you are independent, i.e. linked to no specific device or managing account. The product should be stored safely, however, unwanted or public access by third parties does not pose an immediate danger to its owner. When handing over the product along with the respective master password, you enable simple transfer of access data for a variety of websites. The product is especially suitable for individuals with high requirements for digital security, for departments of companies or for digital heritage management.

Package contents

- Password manager
- USB port lid
- Operating instructions



Up-to-date operating instructions

Download the latest operating instructions via the link www.conrad.com/downloads or scan the QR code. Follow the instructions on the website.

Explanation of symbols



An exclamation mark in a triangle indicates important instructions in these operating instructions which absolutely have to be observed.



The arrow symbol indicates specific tips and advice on operation.

Safety instructions

Please read completely the operating instructions for your product and only use the product if you understand how to use it. The USB stick is ready for use within 30 s - 5 min. (depending on your computer) after connecting to the (Windows based) computer. In some cases, the device is detected as a „defective USB stick“. This is not an error. The device is not a classic bulk memory and does not respond like one. If your PC does not detect the password manager, briefly reconnect the device again. Never disconnect the product in the course of storage or initialisation procedure. Functionality for virtual machines (VM) cannot be guaranteed. Treat the product with care and do not expose it to any liquids.

Choose a secure master password that only you are aware of. You should not choose the one you have already used elsewhere before. It should also differ significantly from your other (known) passwords. Bad passwords are, for example:

MyFirstPassword -> MySecondPassword | Password123456 -> 123456Password

Find out about practices of secure password creating. These are changed over time. Regularly adjust the passwords that you use. In doing so, do not change just the master password of this password manager. The website passwords become less secure as technology improves.

Older sites do not support, where applicable, any redirection, when you are routed to correct site after the web address is entered.

Example: <https://conrad.com> -> <https://www.conrad.com>

Product use

Connect the password manager to a suitable computer. The device is recognised as a drive. Start (by a double click) the „Password Manager“ in the „Windows Explorer“. The program window opens. Select your preferred language and enter a secure master password. Repeat the master password to avoid any typos.

The program window contains the following control buttons:



- 1 „Login“ logs you in automatically (using the saved access data) to the current website.
- 2 „Password“ pastes the password for the website.
- 3 „Manager“ opens the administration window.
- 4 Minimises the window to the task bar
- 5 Closes the program
- 6 Favourites overview (an arrow at the bottom edge): shows the stored websites. If there are more than 8 websites, the entire list can be scrolled through.

a) Logging access data in the password manager

- 1 Launch the password manager. Click the entry form of the website, access data for which you wish to log. If e.g., an account is already registered on Google site, click „Add account“ to log access data for another Google account.
- 2 Once you have logged your access data, press „Login“ with the left mouse button in the password manager.
- 3 „Add web account“ window appears. The website name and Internet address are filled in automatically. These can be adjusted as needed.
- 4 Confirm the account through „register“. The access data for websites can be compiled as described in the above steps.
- 5 If you want to log another account for the same website, click the entry form of the website with the mouse. After that, click „Login“ in the password manager with the right button of the mouse.
- 6 „Add web account“ window appears. Proceed as described in steps 3 and 4.
- 7 When you click „Login“ with the left mouse button, a list of all available accounts appears.

→ You can also enter a direct IP address instead of a URL.

b) Accessing a logged website (one-step login)

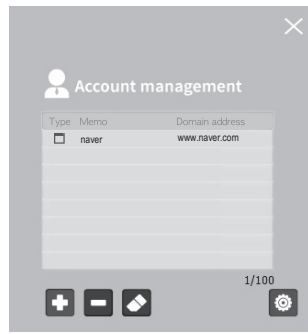
- One-step login is characterised by that you can introduce both password and login ID in the same window.
 - Click with the mouse the upper entry form of a registered website (the cursor in the entry form must be flashing).
 - Click „Login“ in the password manager with the left button of the mouse.
 - The access data for the website are filled in automatically [login ID -> „Tab“ -> password -> „Enter“].
- Alternative keyboard layouts / layout change may alter the entered data and lead to login failures.

c) Accessing a logged website (multi-step login)

- Multi-step login is characterised by that all necessary portions of login information is queried separately. Not all portions of login information can be introduced in a single step.
- Click with the mouse the (only) entry form of a registered website (the cursor in the entry form must be flashing).
- Click and hold the „Login“ switch area with the right mouse button for at least 1 s. Only the login ID is introduced even if login ID and password are already logged.
- After automatic password entry click the corresponding switch area (e.g., next / OK) on the website to proceed to the next entry form.
- Click with the mouse the (only) entry form of the website (the cursor in the entry form must be flashing).
- Click and hold the switch area (2) „Password“ with the left mouse button for at least 1 s. The password associated with the login ID is entered followed by „Enter“. A click without holding only inserts the password.

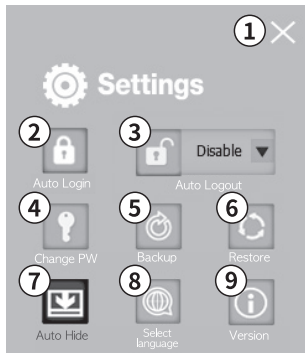
d) Deleting or adjusting access data and setting menu




- Click the Manager (3) switch area or „Manager“ on the right in the task bar of the password manager program menu to proceed to overview of all the saved passwords.
- Proceed in the standard browser to the respective website by clicking a square preceding relevant entry. If several login data have been logged for a website, you can choose the desired website login by clicking the website entry in this list. A cross in the square before an entry points out several login data sets logged.
- Add a new entry by the (+) button or delete the selected one by clicking (-). The eraser symbol opens the input field of a website entry for changes. If you wish to alter an entry only to a limited degree (e.g., retaining the password), do not change the respective entries or do not make an entry. In case of several accounts available, choose the ones you wish to change or to delete.
- Close the manager window by clicking the cross in the right upper corner.



Settings

Proceed from the management window by clicking the gear symbol to the next window to exercise the following functions:



- 1 Close**
Close the program window by clicking the cross in the right upper corner.
- 2 Automatic LOGIN**
If you choose automatic logon of the password manager with master password, enable this function and then enter your master password. Confirm by clicking OK.
→ You cannot enable the automatic logon and automatic logout functions at the same time. With this function enabled, you choose to continuously store the master password on your computer and thus restrict the maximum achievable security.
- 3 Automatic LOGOUT**
After the automatic logout (adjustable timeframe is 1 min to 8 h) is enabled, after expiration of the set period, an information window will appear. The password manager logs out automatically upon confirmation („OK“) or expiry of the period. Pressing the „NO“ button will reset the count-down.
 You cannot enable the automatic logon and automatic logout functions at the same time. Depending on the hardware, disabling occurs in 1 -3 s. Logout from the sites you are logged in does not occur automatically. New logon with the logged account-ing data is disabled.
- 4 Changing master password**
To change the master password of the password manager, press „Change PW“, enter the current master password, enter and then re-enter the new one. Confirm the change.
- 5 Creating BACKUP FILE**
Save an encrypted file (x.POP) on your device. To do that, choose the „Backup“ switch area, introduce a secure encryption password and specify the location on your PC. Using this file, you can transfer the content to a new password manager.
 It is impossible to recover the password manager without the encryption password. Do not use the same password as both master and encryption password.
- 6 Recovery of the password manager**
Recover the backed up status of a password manager by clicking „Restore“. Select the desired backup (with .POP extension), enter the matching password and click „Restore“.
 This procedure will overwrite the current contents of the password manager.

7 Automatic hiding

This function minimises the menu window after login by clicking the menu button „Password Manager“

8 Language settings

Toggle the menu language between D/GB/F/NL/I/PL using the menu item „Select Language“.

→ The language choice does not change the keyboard layout.

9 Version information

Displays the current version (firmware, software, and serial number) of your device.

Update



Shut the password manager program on your computer before performing updates. Never remove the hardware in the course of the updates. Before performing an update, create a backup.

Download the current update (at:) and launch it (double click). Observe the warning (see above) and confirm by clicking OK. Enter the master password and create a backup, if any important data must be saved in the password manager. Enter a backup password and choose a location for the backup. After successful product identification and verification, a new operating system is written to the password manager. After successful update, confirm this by clicking OK, remove the device and connect it again. After an update, the device additionally needs up to a minute to initialise.

Error messages

Typical error messages as regards updates are:

- The software version of the program is more up to date than the version of the desired update package.
- No password manager detected on your device. Connect the device properly.
- Update could not be started. Restart your computer, reconnect the product correctly and make sure you have proper permissions for the updates.
- The software version of the installed program not recognised. Restart your computer, reconnect the product correctly and make sure you have proper permissions for the updates.
- File write (FW) error: Communication error in the course of updates. Repeat the procedure. Restart your computer, reconnect the product correctly and make sure you have proper permissions for the updates.

→ It is possible that mistakes in English language will be recognised by error messages.

Disposal



Electronic devices are recyclable materials and do not belong in the household waste. At the end of its service life, dispose of the product according to the relevant statutory regulations.

Technical data

Software version	1.7 (basis for this manual)
Operating voltage	DC 5 V
Power consumption	0.5 W
Interface.....	high speed USB 2.0 (downward compatible)
Status indicator.....	multicolour LED
Encryption algorithms	AES256, SEED 256, ARIA hardware based security chip
Equipment group	computer
Operating system	Windows 7, Windows 8, Windows 10
Supported browsers	Internet Explorer (IE), Chrome, Opera, QQ, 360safe, Sogou, Firefox
Product dimensions	26 x 79 x 14 mm
Weight	0.013 kg
Operating temperature	0 to 45 °C
Storage temperature.....	-20 to 70 °C

Mode d'emploi

Gestionnaire de mot de passe RF-PM-01

N° de commande 1593964

Utilisation conforme

Le gestionnaire de mot de passe renkforce sert à la sauvegarde sûre et à la gestion du nom d'utilisateur et des mots de passe jusqu'à 100 pages internet. Les algorithmes de cryptage moderne (AES256, SEED 256, ARIA) protègent chaque donnée contre un accès non autorisé (logiciel). Sous la protection d'un « mot de passe principal » sécurisé (6-120 signes), les données d'accès pour des pages internet déposées sont insérées automatiquement, sans transfert dans le presse-papiers.

Pour la sécurité de vos données, le contenu sauvegardé - vos données d'accès - pour les pages internet déposées seront automatiquement éliminées et ne seront plus reproduites. Protégez votre produit des abus et permettez-vous la restauration en cas de données d'accès perdues.

Pour le nom d'utilisateur ainsi que pour le mot de passe, 120 signes sont respectivement prévus. En outre, de courtes notes (max. 150 signes) peuvent être sauvegardées pour chaque page internet. Le produit est adapté pour gérer la fenêtre de connexion en une ou deux étapes (comparable à une inscription sur Google).

Pour utiliser le produit, un programme doit être installé sur l'ordinateur. Celui-ci est contenu dans la livraison et se trouve sauvegardé localement sur le gestionnaire de mot de passe USB. Assurez-vous que vous avez des droits d'accès nécessaires sur l'ordinateur utilisé. Aucune installation n'est nécessaire avec la fonction Plug-and-Play. L'exécution est suffisante. Les systèmes d'exploitation Windows à partir de Windows 7 sont supportés. Vous pouvez vous inscrire automatiquement via les moteurs de recherche suivants : IE, Chrome, Opera, QQ, 360safe, Sogou, Firefox

Votre avantage avec l'utilisation de ce gestionnaire de mot de passe : Vous pouvez utiliser diverses données d'accès pour différentes pages internet avec des phrases sûres - mais souvent difficiles à mémoriser. Pour cela, vous êtes autonomes, c'est à dire que vous n'êtes reliés à aucun appareil spécifique ou compte d'utilisateur à gérer. Le produit doit être conservé de manière sûre, mais ne représente aucun danger immédiat pour le propriétaire en cas d'accès non désiré ou public via une tierce personne. En cas de transfert du produit avec le mot de passe principal, vous autorisez une simple transmission des données d'accès pour de nombreuses pages internet. Le produit est particulièrement adapté aux personnes individuelles avec des exigences de sécurité élevées, à des départements d'entreprises ou simplement à la gestion d'un héritage numérique.

Étendue de la livraison

- Gestionnaire de mot de passe
- Couvercle d'interface
- Mode d'emploi



Modes d'emploi actuels

Téléchargez les modes d'emplois actuels sur le lien www.conrad.com/downloads ou bien scannez le code QR représenté. Suivez les indications du site internet.

Explication des symboles



Le symbole avec le point d'exclamation dans un triangle signale des consignes importantes dans ce mode d'emploi qui doivent impérativement être respectées.



Le symbole de la flèche renvoie à des astuces et conseils d'utilisation spécifiques.

Consignes de sécurité

Lisez le mode d'emploi du produit en intégralité et n'utilisez le produit que lorsque vous avez compris son application. La clé est opérationnelle 30 s à 5 min après son raccordement avec un ordinateur (Windows) - selon votre ordinateur. L'appareil peut être reconnu comme « clé USB défectueuse ». Cela ne représente aucune erreur. L'appareil n'est pas une mémoire de masse classique et ne réagit pas comme telle. Si un gestionnaire de mot de passe n'est pas reconnu sur votre ordinateur, déconnectez brièvement l'appareil et raccordez-le à nouveau. Ne déconnectez jamais le produit pendant un processus de sauvegarde ou d'initialisation. La fonctionnalité ne peut être garantie pour les machines virtuelles (VM). Manipulez le produit avec soin et ne le mettez pas en contact avec un liquide.

Choisissez un mot de passe sécurisé et connu de vous seul. Celui-ci ne doit avoir jamais été utilisé nulle part ailleurs auparavant. De même, il doit se différencier fortement de vos autres mots de passe (connus). Des exemples de mauvais mots de passe sont :

Mon premier mot de passe -> mon deuxième mot de passe | Mot de passe123456 -> 123456 mot de passe

Informez-vous sur des recommandations plus sûres quant aux mots de passe. Celles-ci changent avec le temps. Réadaptez les mots de passe que vous utilisez régulièrement. Pour cela, ne modifiez pas seulement le mot de passe principal de ce gestionnaire de mot de passe. Les mots de passe de pages internet deviennent également vulnérables avec le perfectionnement de la technique.

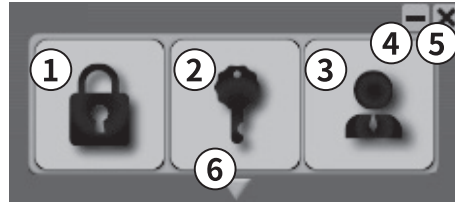
D'anciennes pages internet ne supportent le cas échéant aucune « redirection » lors que laquelle l'adresse internet saisie est redirigée vers la page internet correcte.

Exemple : <https://conrad.com> -> <https://www.conrad.com>

Utilisation du produit

Connectez le gestionnaire de mot de passe avec un ordinateur adapté. L'appareil est reconnu comme disque dur. Démarrez (avec un double clic) le programme « gestionnaire de mot de passe » dans « Windows Explorer ». Une fenêtre de programme s'ouvre. Choisissez votre langue de prédilection et saisissez un mot de passe principal sûr. Répétez le mot de passe principal en évitant des fautes de frappe.

La fenêtre de programme est composée des boutons de commande suivants :



- 1 « Login » vous inscrit automatiquement (avec les données d'accès sauvegardées) sur le site internet actuel.
- 2 « Mot de passe » C'est le mot de passe de la page internet.
- 3 « Gestionnaire » Ouvre la fenêtre d'administration.
- 4 Minimise la fenêtre sur la barre de menu
- 5 Ferme le programme
- 6 Aperçu des favoris (flèche sur le bord inférieur) : montre les pages internet déposées. À partir de 8 pages internet, la liste s'affiche avec un menu déroulant.

a) Déposer les données d'accès dans le gestionnaire de mot de passe

- 1 Exécutez le gestionnaire de mot de passe. Cliquez sur le masque de saisie de la page internet pour laquelle les données d'accès doivent être déposées. Si par exemple, un compte est déjà inscrit sur la page Google, cliquez sur « ajouter un compte » pour déposer vos données d'accès pour un autre compte Google.
- 2 Dès que vos données d'accès sont déposées, cliquez dans le gestionnaire de mot de passe avec le bouton **gauche** de la souris sur « Login ».
- 3 La fenêtre « Ajouter un compte web » apparaît. La dénomination et l'adresse internet de la page sont saisies automatiquement. Si besoin, vous pouvez les adapter.
- 4 Confirmez le compte via « Enregistrer ». Les données d'accès pour d'autres sites internet peuvent être créés en suivant les étapes décrites précédemment.
- 5 Si vous voulez déposer un autre compte pour le même site internet, cliquez avec la souris sur le masque de saisie du site internet. Cliquez ensuite dans le gestionnaire de mot de passe avec le bouton **droit** de la souris sur « Login ».
- 6 La fenêtre « Ajouter un compte web » apparaît. Procédez comme aux points 3 et 4.
- 7 Si vous cliquez sur « Login » avec le bouton **gauche** de la souris, une liste avec tous les comptes disponibles s'affiche.

→ Au lieu de l'URL vous pouvez saisir une adresse IP directe.

b) Accès à une page internet déposée (Connexion à une étape)

- Une connexion à une étape se caractérise par le fait que vous pouvez saisir le mot de passe et l'ID d'utilisateur dans la même fenêtre.
- Cliquez avec la souris sur le masque de saisie situé en haut du site internet enregistré (le curseur devrait clignoter dans le masque de saisie).
- Cliquez ensuite dans le gestionnaire de mot de passe avec le bouton **gauche** de la souris sur « Login ».
- Les données d'accès pour le site internet sont saisis automatiquement [Login-ID -> « Tab » -> Password -> „Enter”].

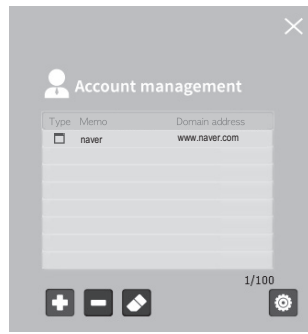
→ Une configuration alternative du clavier / changement de configuration peut provoquer une modification des données saisies et entraîner une erreur de connexion.

c) Accès à une page internet déposée (Connexion à plusieurs étapes)

- Une connexion à plusieurs étapes se caractérisent par le fait que toutes les informations de connexion sont requises l'une après l'autre de manière séparée. Il n'est pas possible de saisir toutes les informations de connexion en une seule fois.
- Cliquez avec la souris sur le (seul) masque de saisie du site internet enregistré (le curseur devrait clignoter dans le masque de saisie).
- Cliquez et maintenez la touche « Login » avec le bouton droit de la souris pendant au moins 1 s. Seul l'ID de connexion sera saisi, même si l'ID de connexion et le mot de passe ont été déposés.
- Après la saisie automatique du mot de passe, cliquez sur le bouton correspondant (par ex. prochain / continuer / OK) sur la page internet pour accéder au masque de saisie suivant.
- Cliquez avec la souris sur le (seul) masque de saisie du site internet enregistré (le curseur devrait clignoter dans le masque de saisie).
- Cliquez et maintenez la touche (2) « Mot de passe » avec le bouton gauche de la souris pendant au moins 1 s. Le mot de passe correspondant à l'ID de connexion sera saisi, suivi de « Enter ». Si vous cliquez sans maintenir la touche, seul le mot de passe sera saisi.

d) Élimination ou adaptation des données d'accès et des réglages du menu

- Cliquez sur le bouton du gestionnaire (3) ou bien cliquez à droite dans la barre de menu du programme de gestionnaire de mot de passe sur « Gestionnaire » pour accéder à l'aperçu de tous les mots de passe sauvegardés.
- En cliquant sur la case devant la saisie correspondante, vous passez dans le moteur de recherche sur le site internet correspondant. Si plusieurs données de connexion sont déposées pour un site internet, vous pouvez sélectionner la connexion souhaitées au site internet en cliquant sur le site internet saisi dans la liste. Une croix dans la case devant la saisie correspondante indique l'existence de plusieurs données de connexion.
- Le bouton + permet d'ajouter une nouvelle saisie ou d'éliminer les saisies sélectionnées en un clic. Le symbole de la gomme ouvre la fenêtre de saisie d'un site internet pour des modifications. Si vous voulez modifier une saisie seulement partiellement (par ex. maintenir le mot de passe), ne modifiez pas toutes les saisies et ne faites aucune saisie. En cas d'existence de plusieurs comptes, sélectionnez le compte souhaité à modifier ou à éliminer.
- En cliquant sur la croix dans le coin droit supérieur, vous pouvez fermer la fenêtre du gestionnaire.



Réglages

Dans le gestionnaire, le symbole de la roue dentée permet d'exécuter l'une des fonctions suivantes dans la fenêtre correspondante :



1 FERMER

En cliquant sur la croix dans le coin droit supérieur, vous pouvez fermer la fenêtre du programme.

2 CONNEXION automatique

Si vous souhaitez une connexion automatique du gestionnaire de mot de passe, activez cette fonction et saisissez le mot de passe principal. Confirmez en cliquant sur « OK ».

→ Vous pouvez activer simultanément la fonction de connexion et de déconnexion automatique. En activant cette fonction, vous sauvegardez de manière permanente le mot de passe principal sur votre ordinateur et restreignez ainsi au niveau de sécurité maximale accessible.

3 DÉCONNEXION automatique

En activant la déconnexion automatique (laps de temps réglable de 1 min à 8 h), l'écoulement du temps s'affiche dans une fenêtre d'information. La confirmation (« OK ») ou la fin du temps écoulé pré-réglé provoque la déconnexion automatique du gestionnaire de mot de passe. En appuyant sur la touche « NO », le compte à rebours est réinitialisé.



Vous pouvez activer simultanément la fonction de connexion et de déconnexion automatique. La désactivation dure selon le software de 1 à 3 s. Une déconnexion des sites internet connectés n'a pas lieu de manière automatique. Une nouvelle connexion avec les informations de compte déposées est empêchée.

4 Modification du MOT DE PASSE principal

Pour modifier le mot de passe principal du gestionnaire de mot de passe, appuyez sur « Change PW ». Saisissez le mot de passe actuel, saisissez un nouveau mot de passe et répétez ce dernier. Confirmez le souhait de modification.

5 Créer un UN FICHIER DE SAUVEGARDE

Sauvegardez des données de restauration cryptées (x.POP) sur votre appareil. Pour cela, choisissez le bouton « backup », saisissez une mot de passe de cryptage sécurisé et un fichier de sauvegarde sur votre ordinateur. Ces données permettent de transférer le contenu sur un nouveau gestionnaire de mot de passe.



Sans le mot de passe de cryptage, le gestionnaire de mot de passe ne peut pas être restauré. N'utilisez pas le même mot de passe pour le mot de passe principal et le mot de passe de cryptage.

6 Restauration du gestionnaire de mot de passe

Restaurer l'état de la sauvegarde d'un gestionnaire de mot de passe en cliquant sur « Restore ». Sélectionnez la sauvegarde souhaitée (Extension de donnée .POP), saisissez en plus le mot de passe correspondant et cliquez sur « Restore ».



Le contenu actuel du gestionnaire de mot de passe est écrasé.

7 Masquage automatique

Cette fonction minimise la fenêtre de menu après une connexion en cliquant sur le bouton du menu « gestionnaire de mot de passe »

8 Réglage des langues

Commutez la langue du menu entre D/GB/F/NL/I/PL à l'aide du point du menu « Select Language ».

→ Le choix de la langue ne modifie pas la configuration du clavier.

9 Informations sur les versions

Annonce la version actuelle (version du micro programme, logiciel et numéro de série) de votre appareil.

Mise à jour



Fermez le programme du gestionnaire de mot de passe sur votre ordinateur avant d'exécuter la mise à jour. Ne retirez jamais le matériel informatique pendant la mise à jour. Effectuez une sauvegarde avant l'exécution d'une mise à jour.

Téléchargez la version actuelle de la mise à jour (sur :) et exécutez celle-ci (double clic). Observez l'avertissement (voir plus haut) et confirmez avec OK. Saisissez le mot de passe principal et effectuez ensuite une sauvegarde, si des données importantes doivent être sauvegardées sur le gestionnaire de mot de passe. Saisissez un mot de passe de sauvegarde et choisissez un fichier de sauvegarde. Après la réussite de l'identification du produit et une vérification, un nouveau système d'exploitation sera inscrit dans le gestionnaire de mot de passe. Après la réussite de la mise à jour, confirmez celle-ci avec OK, déconnectez l'appareil et reconnectez-le. Après une mise à jour, l'appareil nécessite jusqu'à une minute pour se réinitialiser.

Messages d'erreurs

Les messages d'erreur typiques sont :

- La version du logiciel du programme est plus récente que la version de votre programme de mise à jour souhaité.
- Le gestionnaire de mot de passe n'est pas reconnu par votre appareil. Connectez l'appareil correctement.
- La mise à jour n'a pas pu démarrer. Redémarrez l'ordinateur, connectez le produit correctement et assurez-vous que les droits d'accès de la mise à jour soient corrects.
- La version du logiciel du programme installé n'est pas reconnue. Redémarrez l'ordinateur, connectez le produit correctement et assurez-vous que les droits d'accès de la mise à jour soient corrects.
- Erreur d'écriture du fichier (FW) : Erreur de communication pendant la mise à jour. Répétez le processus. Redémarrez l'ordinateur, connectez le produit correctement et assurez-vous que les droits d'accès de la mise à jour soient corrects.

→ Une erreur en langue anglaise sera éventuellement caractérisée par « Error ».

Élimination



Les appareils électroniques sont des objets recyclables et ils ne doivent pas être éliminés avec les ordures ménagères. Procédez à l'élimination du produit au terme de sa durée de vie conformément aux dispositions légales en vigueur.

Caractéristiques techniques

Version de logiciel.....	1.7 (Base de ce mode d'emploi)
Tension de service.....	CC 5 V
Consommation d'énergie.....	0.5 W
Interface.....	USB 2.0 High Speed (rétro compatible)
Voyant de fonctionnement.....	LED multicolore
Algorithmes de cryptage.....	AES256, SEED 256, ARIA puce sécurisée basée sur le matériel
Groupe d'appareil.....	Ordinateur
Systèmes d'exploitation.....	Windows 7, Windows 8, Windows 10
Moteurs de recherche supportée.....	Internet Explorer (IE), Chrome, Opera, QQ, 360safe, Sogou, Firefox
Dimensions du produit.....	26 x 79 x 14 mm
Poids.....	0,013 kg
Température de service.....	de 0 à + 45 °C
Température de stockage.....	de -20 à + 70 °C

Ceci est une publication de Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92240 Hirschau (www.conrad.com).

Tous droits réservés, y compris de traduction. Toute reproduction, quelle qu'elle soit (p. ex. photocopie, microfilm, saisie dans des installations de traitement de données) nécessite une autorisation écrite de l'éditeur. Il est interdit de le réimprimer, même par extraits. Cette publication correspond au niveau technique du moment de la mise sous presse.

© Copyright 2018 by Conrad Electronic SE.

1593964_V2_0118_02_VTP_m_fr

Gebruiksaanwijzing**Wachtwoord-manager RF-PM-01**

Bestelnr. 1593964

Beoogd gebruik

De renkforce wachtwoord-manager dient voor het veilig opslaan en beheren van gebruikersnamen en wachtwoorden voor tot 100 websites. Moderne versleutelingsalgorithmen (AES256, SEED 256, ARIA) tegen het invoeren van niet geoorloofde (hardware-) toegang. Bescherm door een overkoepelend "master-wachtwoord" (6-120 karakters) kunnen de toegangsgegevens voor geregistreerde websites automatisch worden ingegeven, zonder overdracht in het tussen-geheugen.

Voor de veiligheid van uw gegevens wordt de opgeslagen inhoud - uw toegangsgegevens - na zes foute ingaven op rij automatisch gewist en kan niet opnieuw worden hersteld. Bescherm het product tegen misbruik en maak het opnieuw herstellen van verloren gegane toegangsgegevens mogelijk.

Er zijn voor de gebruikersnaam tot 300 karakters en voor het wachtwoord maximaal 120 karakters voorzien. Er kunnen ook voor elke website een korte notitie (max. 150 karakters) worden opgeslagen. Het product is geschikt om een log-in-venster in een of twee stappen (vergi aanmelding bij Google) te bedienen.

Om het product te kunnen gebruiken, moet er op de computer een programma worden uitgevoerd. Dit is in de levering inbegrepen en bevindt zich lokaal opgeslagen op de USB-wachtwoord-manager. Controleer of u over voldoende rechten beschikt op de gebruikte computer. Door de plug-and-play-functie is er geen installatie nodig. Het uitvoeren volstaat. De Windows-besturingssystemen vanaf Windows 7 en nieuwer worden ondersteund. U kunt zich met dit product automatisch via de volgende browsers aanmelden: IE, Chrome, Opera, QQ, 360safe, Sogou, Firefox

Uw voordeel door het gebruik van deze wachtwoord-manager: U kunt voor verschillende websites verschillende toegangsgegevens gebruiken met veilige - maar vaak moeilijk te herinneren zinnen. Daarbij bent u autarkisch, d.w.z. U bent niet aan een specifiek apparaat of een vertegenwoordigende gebruikersaccount gebonden. Het product moet veilig worden bewaard maar er is geen onmiddellijk gevaar voor de eigenaar bij een ongewenste toegang of openbare toegang door derden. Door het doorgeven van het product met het bijhorende master-wachtwoord maakt u een eenvoudige overgave van de toegangsgegevens voor talrijke websites mogelijk. Het product is bijzonder geschikt voor personen met hoge digitale veiligheidseisen, afdelingen in bedrijven of voor het eenvoudig beheer van het digitaal patrimonium.

Omvang van de levering

- Wachtwoord-manager
- USB-interface-deksel
- Gebruiksaanwijzing

**Actuele gebruiksaanwijzingen**

Download de actuele gebruiksaanwijzingen via de link www.conrad.com/downloads of scan ze met behulp van de afgebeelde QR-code. Volg de aanwijzingen op de website.

Verklaring van de symbolen

Het pictogram met het uitroepteken in een driehoek wijst op belangrijke aanwijzingen in deze gebruiksaanwijzing die te allen tijde nageleefd moeten worden.

→ U treft het pijl-symbool aan bij bijzondere tips en instructies betreffende de bediening.

Veiligheidsinstructies

Lees de bij het product horende handleiding volledig en gebruik het product pas wanneer u het gebruik begrepen hebt. De stick is 30 s - 5 min na het verbinden met een computer gebruiksklaar. (Afhankelijk van uw computer). Het apparaat wordt gedeeltelijk als een "defecte USB-stick" herkend. Dit stelt geen fout voor. Het apparaat is geen klassiek massagegeheugen en reageert ook als dusdanig. Indien de wachtwoord-manager niet door uw PC wordt herkend, koppel het apparaat dan gedurende korte tijd los en verbind het opnieuw. Koppel het apparaat nooit los tijdens een opslag- of initialisatieproces. De functionaliteit kan niet gegarandeerd worden voor virtuele machines (VM). Behandel het product zorgzaam en plaats het niet in vloeistoffen.

Kies een veilig master-wachtwoord dat alleen door u gekend is. Dit mag voordien nog niet door u gebruikt zijn. Het moet ook sterk verschillend zijn van andere (gekende) wachtwoorden. Slechte wachtwoorden zijn bijv.:

Mijneerstewachtwoord > Mijntweedewachtwoord | Wachtwoord123456 -> 123456Wachtwoord
Informeert u over veilige wachtwoordanbevelingen. Deze veranderen in de loop van de tijd. Pas de door u gebruikte wachtwoorden regelmatig aan. Verander hierbij alleen het Master-wachtwoord van deze wachtwoord-manager. Ook website-wachtwoorden worden door de verbeterde techniek onveilig.

Oudere websites ondersteunen in bepaalde gevallen geen "redirection" waarbij het ingegeven webadres naar de correcte website wordt verdergeleid.

Voorbeeld: <https://conrad.com> → <https://www.conrad.com>

Productgebruik

Verbind de wachtwoord-manager met een geschikte computer. Het apparaat wordt als drive herkend. Start door dubbel te klikken het programma „Wachtwoord-manager“ in „Windows Explorer“. Er opent zich een programmavenster. Kies uw voorkeurtal en geef een veilig master-wachtwoord in. Herhaal het master-wachtwoord om tikfouten te voorkomen.

Het programmavenster bestaat uit de volgende bedieningsknoppen:



- 1 "Login" Meldt u automatisch (met de opgeslagen toegangsgegevens) op de actuele website aan.
- 2 "Password" voegt het wachtwoord van de website in.
- 3 "Manager" opent een beheervenster.
- 4 Minimaliseert het venster op de takenlijst
- 5 Sluit het programma
- 6 Favorietenoverzicht (Pijl aan de onderste rand) toont de geregistreerde websites. Bij meer dan 8 websites kan er door de volledige lijst worden gebladerd.

a) Toegangsgegevens in de wachtwoord-manager registreren

- 1 Voer de wachtwoord-manager uit. Klik in het invoerveld van de website waarvoor u de toegangsgegevens wilt registreren. Wanneer er bijv. op de Google-website reeds een account is aangemeld, klikt u op „Account toevoegen“ om uw toegangsgegevens voor een bijkomende Google-account te registreren.
- 2 Van zodra u uw toegangsgegevens heeft geregistreerd, drukt u in wachtwoord-manager met de linker muisknop op „log-in“.
- 3 Het venster „Webaccount toevoegen“ verschijnt. De naam van de website en het internet-adres worden automatisch ingevuld. Deze kunnen, indien gewenst, worden aangepast.
- 4 Bevestig de account via „Registreren“. De toegangsgegevens voor bijkomende websites kunnen gecreëerd zoals hierboven beschreven.
- 5 Indien u voor dezelfde website een bijkomende account wilt registreren, klikt u met de muis in het invoerveld van de website. Klik vervolgens in de wachtwoord-manager met de rechter muisknop op „log-in“.
- 6 Het venster „Webaccount toevoegen“. Ga te werk zoals in 3 en 4.
- 7 Wanneer u met de linker muisknop op „log-in“ klikt, verschijnt een lijst met alle beschikbare accounts.

→ In plaats van een URL kan ook een direct IP-adres worden ingegeven.

b) Toegang tot een geregistreerde website (log-in in een enkele stap)

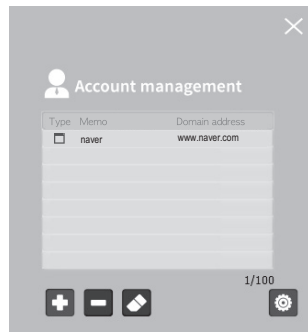
- Eenstaps-logins worden daardoor gekenmerkt dat u in hetzelfde venster zowel wachtwoord als log-in-ID kunt ingeven.
 - Klik met de muis in het bovenstaande invoerveld van een geregistreerde website (de cursor moet in het invoerveld knipperen).
 - Klik in de wachtwoord-manager met de linker muisknop op „log-in“.
 - De toegangsgegevens voor die website worden automatisch ingevuld [log-in-ID -> „Tab“ -> Wachtwoord -> „Enter“].
- Alternatieve toetsenbord-layout's/lay-out-wijzigingen kunnen de ingegeven gegevens wijzigen en leiden tot mislukte log-in's.

c) Toegang tot een geregistreerde website (log-in in meerdere stappen)

- Log-in's in meerdere stappen worden daardoor gekenmerkt dat alle nodige log-in-informatie apart van elkaar wordt opgevraagd. Niet alle log-in-informatie kan in een stap worden weergegeven.
- Klik met de muis in het (enige) invoerveld van een geregistreerde website (de cursor moet in het invoerveld knipperen).
- Hoe de toets „log-in“ tenminste 1 sec. ingedrukt. Er wordt alleen de log-in ingegeven, zelfs wanneer log-in-ID en wachtwoord geregistreerd zijn.
- Klik na de automatische wachtwoordinvoer vervolgens op de overeenstemmende toets (bijv. next/verder/OK) op de website om naar het volgende invoerveld te gaan.
- Klik met de muis in het (enige) invoerveld van de website (de cursor moet in het invoerveld knipperen).
- Hou de toets (2) „Wachtwoord“ ten minste voor 1 seconde met de linker muisknop ingedrukt. Het bij de log-in-ID horende wachtwoord wordt gevolgd door „Enter“ ingegeven. Klikken zonder ingedrukt houden voegt alleen het wachtwoord in.

d) Wissen of aanpassen van toegangsgegevens en instellingenmenu

- Klik op de toets „Manager” (3) of klik rechts op de takenlijst in het menu van het wachtwoord-manager-programma op „Manager” om naar het overzicht van alle opgeslagen wachtwoorden te gaan.
- Door op het vierkantje van de bijhorende invoer te klikken, gaat u in de standaard-browser daar de overeenstemmende website. Indien er meerdere log-in-gegevens voor een website zijn geregistreerd, kunnen u door op de website-invoer in deze lijst te klikken, de gewenste website selecteren. Daarbij wijst een kruisje in het vierkant voor een invoer op verschillende geregistreerde log-in-gegevens.
- Met de +-toets kunt u een nieuwe invoer toevoegen en door op - te klikken kunt u de selectie verwijderen. Het gom-symbool opent het invoervenster voor de invoer van een website voor wijzigingen. Indien u een invoer slechts gedeeltelijk wilt veranderen (bijv. Wachtwoord bewaren), dan verandert u de invoer niet of geeft u niets in. Indien er meerdere accounts beschikbaar zijn, selecteert u diegene die u wenste veranderen of te verwijderen.
- Door op het kruisje in de rechterbovenhoek te klikken, sluit u het „Manager”-venster.



Instellingen

Ga in het beheervenster via het tandwiel-symbool naar het volgende venster om de volgende functie uit te voeren:



1 Sluiten

Door op het kruisje in de rechterbovenhoek te klikken, sluit u het programmavenster.

2 Automatische LOG-IN

Indien u een automatische aanmelding van de wachtwoord-manager via het master-wachtwoord wenst, activeert u deze functie en geef vervolgens uw master-wachtwoord in. Met OK bevestigen.

→ U kunt de functie automatische log-in niet tegelijk met de functie automatische logout activeren. Met de activatie van deze functie slaat u het master-wachtwoord continu op uw computer op en beperkt u daardoor de maximaal bereikbare veiligheid.

3 Automatische LOG-OUT

Door de activatie van de automatische afmelding (instelbare tijd 1 min - 8 uur) verschijnt na het verstrijken van de tijd een informatievenster. Door de bevestiging („OK”) of het verstrijken van de tijd wordt de wachtwoord-manager automatisch afgemeld. Door de toets „NO” te activeren wordt de count-down teruggezet.



U kunt de functie automatische log-in niet tegelijk met de functie automatische logout activeren. Het uitschakelen duurt afhankelijk van de hardware tussen 1 en 3 seconden. Afmelden van ingelogde websites gebeurt niet automatisch. Een nieuwe aanmelding met de geregistreerde account-informatie wordt verhinderd.

4 Master-WACHTWOORD veranderen

Om het master-wachtwoord van de wachtwoord-manager te wijzigen, drukt u op „Change PW”, geeft u het actuele wachtwoord in, geeft u een nieuw master-wachtwoord in en herhaalt u dit. Bevestig uw wijzigingsaanvraag.

5 BACKUP-FILE creëren

Sla een versleuteld herstelbestand (x.POP) p uw apparaat op. Selecteer daarvoor de toets „Back-up” en geef een versleutelingswachtwoord in een opslagplaats op uw PC in. Met dit bestand kan de inhoud op een nieuwe wachtwoord-manager worden overgedragen.



Zonder het versleutelingswachtwoord kan de wachtwoord-manager niet hersteld worden. Gebruik niet hetzelfde wachtwoord als master-wachtwoord en als versleutelingswachtwoord.

6 Wachtwoord-manager opnieuw herstellen

Herstel de back-up-toestand op een wachtwoord-manager door op „Restore” te klikken. Kies de gewenste back up (bestandsexentie.POP), geef het bijhorende wachtwoord en klik op „Resore”.



De actuele inhoud van de wachtwoord-manager wordt door dit proces overschreven.

7 Automatisch verbergen

Deze functie minimaliseert het menu-venster na een log-in met een klik op de menu-toets „Wachtwoord-manager”

8 Taalinstellingen

Wijzig de menutaal tussen D/GB/F/NL/I/PL met het menu-item „Select language”.

→ De taalkeuze verandert de lay-out van het toetsenbord net.

9 Versie-informatie

Toont de actuele versie (Firmware, software en serienummer) van uw apparaat.

Update



Sluit wachtwoord-manager-programma op de computer af voor u de update uitvoert. De hardware nooit tijdens de update verwijderen. Maak een back-up voor het uitvoeren van een update.

Download de actuele update (onder:) en voer die uit (Dubbel klikken). Hou rekening met de waarschuwing (zie boven) en bevestig met OK. Geef het master-wachtwoord in en doe vervolgens een back-up voor het geval er belangrijke gegevens op de wachtwoord-manager zouden zijn opgeslagen. Geef een back-up-wachtwoord in en selecteer een plaats om de back-up op te slaan. Na een geslaagde productidentificatie en verificatie wordt een nieuw besturingssysteem op de wachtwoord-manager geschreven. Na een geslaagde update bevestigt u deze met OK, verwijdert u het apparaat en verbindt u het opnieuw. Na een update heeft het apparaat een minuut extra nodig voor de initialisatie.

Foutmeldingen

Typische foutmeldingen van de update zijn:

- De software-versie van het programma is actueler dan de versie van het door u gekozen update-programma.
- De wachtwoord-manager kon door uw apparaat niet herkennen. Sluit het correcte apparaat aan.
- De update kon niet worden gestart. Start uw computer opnieuw op, sluit het product correct aan controleer of u over de juiste toegangsrechten voor de update beschikt.
- De softwareversie van het geïnstalleerde programma kon niet herkend worden. Start uw computer opnieuw op, sluit het product correct aan controleer of u over de juiste toegangsrechten voor de update beschikt.
- File Write (FW) fout: Communicatiefout tijdens de update. Het proces herhalen. Start uw computer opnieuw op, sluit het product correct aan controleer of u over de juiste toegangsrechten voor de update beschikt.

→ Eventueel wordt een fout in het Engels als „Error” aangegeven.

Verwijdering



Elektronische toestellen bevatten waardevolle materialen en horen niet bij het huishoudelijk afval. Verwijder het product aan het einde van zijn levensduur conform de geldende wettelijke bepalingen.

Technische specificaties

Softwareversie.....	1.7 (Basis van deze handleiding)
Bedrijfsspanning.....	DC 5 V
Energieverbruik	0.5 W
Interface.....	USB 2.0 High Speed (naar beneden compatibel)
Werkingsweergave	Meerkleurige LED
Versleutelingsalgoritmes.....	AES256, SEED 256, ARIA Hardware-gebaseerde veiligheids-chip
Apparategroep.....	Computer
Besturingssysteem	Windows 7, Windows 8, Windows 10
Ondersteunde browser.....	Internet Explorer (IE), Chrome, Opera, QQ, 360safe, Sogou, Firefox
Productafmetingen	26 x 79 x 14 mm
Gewicht.....	0,013 kg
Bedrijfstemperatuur	0 tot 45 °C
Opslagtemperatuur.....	-20 tot 70 °C

Dit is een publicatie van Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92240 Hirschau (www.conrad.com).

Alle rechten, vertaling inbegrepen, voorbehouden. Reproducties van welke aard ook, bijvoorbeeld fotokopie, microverfilming of de registratie in elektronische gegevensverwerkingsapparatuur, vereisen de schriftelijke toestemming van de uitgever. Nadruk, ook van uittreksels, verboden. De publicatie voldoet aan de technische stand bij het in druk bezorgen.

© Copyright 2018 by Conrad Electronic SE.

1593964_V2_0118_02_VTP_m_nl