renkforce

CE

(PL) **Instrukcja użytkowania**

Menedżer haseł RF-PM-01

Nr zam. 1593964

Zastosowanie zgodne z przeznaczeniem

Menedżer haseł renkforce służy do bezpiecznego przechowywania i obsługi nazw użytkowników i haseł nawet do 100 stron internetowych. Nowoczesne algorytmy kodowania (AES25, SEED 256, ARIA) chronią każdy rejestr przed nieautoryzowanym dostępem (od strony sprzętowej). Zabezpieczone przez nadrzędne „hasło główne" (6-120 znaków) dane dostępu do zapisanych stron internetowych mogą być wprowadzane automatycznie, bez przesyłania do schowka.

Aby zabezpieczyć dane użytkownika, przechowywana zawartość - dane dostępowe - jest automatycznie usuwana po sześciu nieprawidłowych wpisach z rzędu i nie może zostać przywrócona. Ochrona produktu przed niewłaściwym użyciem i możliwość przywrócenia utraconych danych dostępu.

Nazwa użytkownika może mieć maksymalnie 300 znaków, a hasło maksymalnie 120 znaków. Dodatkowo można zapisać krótkie notatki (maksymalnie 150 znaków) dotyczące każdej strony internetowej. Produkt jest dostosowany do obsługiwania jedno- i dwupoziomowych okien logowania (por. Logowanie Google).

Aby móc korzystać z produktu, należy uruchomić na komputerze program. Jest on dołączony do zestawu i znajduje się w menedżerze haseł USB - przechowywany lokalnie. Należy się upewnić, że użytkownik posiada wymagane uprawnienia do komputera, z którego korzysta. Dzięki funkcji Plug-and-Play instalacja nie jest wymagana. Wystarczy uruchomienie. Obsługiwane są systemy operacyjne Windows 7 i nowsze. Następujące przeglądarki pozwalają na automatyczne logowanie przy użyciu tego produktu: IE, Chrome, Opera, QQ, 360safe, Sogou, Firefox

Korzyści płynące z menedżera haseł: Można używać różnych danych dostępu dla różnych stron internetowych z bezpiecznymi - ale często trudnymi do zapamiętania - zwrotami. Użytkownik pozostaje przy tym niezależny, tzn. nie jest połączony z żadnym konkretnym urządzeniem ani kontem użytkownika. Produkt powinien być bezpiecznie przechowywany, stanowi bezpośrednie zagrożenie dla właściciela w przypadku niepożądanego dostępu lub publicznego ujawnienia stronom trzecim. Przekazywanie produktu z powiązanym hasłem głównym umożliwia łatwe przejęcie danych dostępowych do wielu stron internetowych. Produkt jest w szczególności przeznaczony dla osób o wysokiej potrzebie bezpieczeństwa cyfrowego, działów w firmach lub do prostego zarządzania dziedzictwem cyfrowym.

Zawartość zestawu

- Menedżer haseł
- Pokrywa interfejsu USB
- Instrukcja użytkowania

Aktualne instrukcje użytkowania

Pobierz aktualne instrukcje użytkowania za pomocą łącza www.conrad.com/downloads lub przeskanuj widoczny kod QR. Należy przestrzegać instrukcji przedstawionych na stronie internetowej.

Wyjaśnienie symboli

Symbol z wykrzyknikiem w trójkącie oznacza ważne zalecenia tej instrukcji, których należy bezwzględnie przestrzegać.

⟶ Symbol strzałki pojawia się w miejscach, w których znajdują się dokładne wskazówki i porady dotyczące eksploatacji.

Zasady bezpieczeństwa

Należy dokładnie przeczytać instrukcję użytkowania produktu i rozpocząć jego użytkowanie dopiero po zrozumieniu instrukcji. Pendrive jest gotowy do użycia po 30 s - 5 min (w zależności od komputera) od momentu podłączenia do komputera (z systemem Windows). Urządzenie jest częściowo rozpoznawane jako „wadliwa pamięć USB". Nie oznacza to błędu. Urządzenie nie jest typowym nośnikiem pamięci masowej i nie funkcjonuje jako taki nośnik. Jeżeli menedżer haseł nie zostanie rozpoznany przez komputer, należy na krótko odłączyć urządzenie i podłączyć je ponownie. Nigdy nie należy odłączać produktu podczas procedury zapisywania lub instalacji. Funkcjonalność dla maszyn wirtualnych (VM) nie jest gwarantowana. Należy ostrożnie obchodzić się z produktem i nie dopuścić do jego kontaktu z płynami.

Należy wybrać bezpieczne i znane tylko użytkownikowi hasło główne. Powinno być to nowe, niestosowane wcześniej hasło. Powinno się ono również znacznie różnić od innych (znanych) haseł. Przykłady złych haseł:

MojePierwszeHaslo -> MojeDrugie Haslo | Haslo123456 -> 123456Haslo

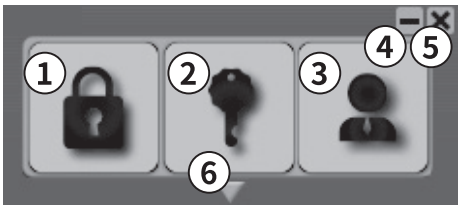
Należy zapoznać się z zasadami tworzenia bezpiecznych haseł. Z biegiem czasu ulegają one zmianie. Należy często aktualizować swoje hasła. Nie zmieniać przy tym tylko hasła głównego menedżera haseł. Również hasła do stron internetowych stają się mniej bezpieczne w miarę rozwoju technologii.

Starsze witryny mogą nie obsługiwać „przekierowania", gdzie wprowadzony adres internetowy jest przekierowywany na właściwą stronę.
Przykład: https://conrad.com —> https://www.conrad.com

Stosowanie produktu

Należy podłączyć menedżer haseł do odpowiedniego komputera. Urządzenie zostanie rozpoznane jako napęd. Należy uruchomić (przez dwukrotne kliknięcie) program „Menedżer haseł" w „Eksploratorze Windows". Otworzy się okno programu. Należy wybrać język oraz podać bezpieczne hasło główne. Należy powtórzyć hasło główne, aby uniknąć literówek.

Okno programu składa się z następujących przycisków:



1 „Login" Automatyczne logowanie (z zapisanymi danymi dostępu) do aktualnej strony internetowej.

2 „Password" Wstawianie hasło strony internetowej.

3 „Manager" Otwarcie okna administracyjnego.

4 Minimalizacja okna na pasku zadań

5 Zamknięcie programu

6 Przegląd ulubionych (strzałka przy dolnej krawędzi): wyświetlanie zapisanych stron internetowych. Przy więcej niż 8 stronach internetowych można przewinąć cała listę.

a) Zapisywanie danych dostępu w menedżerze haseł

1 Należy uruchomić menedżer haseł. Należy kliknąć maskę wprowadzania strony internetowej, dla której mają zostać zapisane dane dostępu. Jeśli na przykład konto zostało już zarejestrowane w witrynie Google, należy kliknąć „Dodaj konto", aby zapisać dane dostępu do innego konta Google.

2 Gdy dane dostępu zostaną zapisane, należy nacisnąć lewym przyciskiem myszy przycisk „Login" w menedżerze haseł.

3 Pojawi się okno „dodaj konto internetowe". Nazwa strony i adres internetowy zostaną automatycznie wypełnione. W razie potrzeby można je poprawić.

4 Należy potwierdzić konto za pośrednictwem przycisku „rejestracja". Dane dostępu do innych witryn można utworzyć zgodnie z powyższym opisem.

5 Jeżeli ma być dodane kolejne konto do tej samej witryny, należy kliknąć myszką w maskę wprowadzania danych na stronie internetowej. Następnie w menedżerze haseł należy kliknąć prawym przyciskiem myszy na „Login".

6 Okno „dodaj konto internetowe". Należy postępować zgodnie z opisem w punkcie 3 i 4.

7 Po naciśnięciu lewym przyciskiem myszy w „Login" pojawi się lista ze wszystkimi powiązanymi kontami.

⟶ **Zamiast adresu URL można również podać bezpośredni adres IP.**

b) Dostęp do zapisanych stron (logowanie jednopoziomowe)

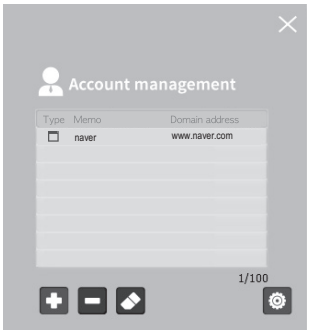
- Logowanie jednopoziomowe charakteryzuje się tym, że w tym samym oknie można podać hasło i identyfikator logowania.
- Należy kliknąć myszką w najwyższą maskę logowania zarejestrowanej strony (kursor powinien migać w masce logowania).
- W menedżerze haseł należy kliknąć lewym przyciskiem myszy na „Login".
- Dane dostępu do strony internetowej zostaną wypełnione automatycznie [Identyfikator logowania -> „Tab" -> Hasło -> „Enter"].

⟶ Alternatywne układy klawiatury / zmiany układów mogą zmieniać wprowadzone dane i powodować błędy logowania.

c) Dostęp do zapisanych stron (logowanie wielopoziomowe)

- Logowanie wielopoziomowe charakteryzuje się tym, że wszystkie wymagane informacje logowania są wprowadzane oddzielnie, jedna po drugiej. Nie ma możliwości podania wszystkich informacji logowania w jednym kroku.
- Należy kliknąć myszką w (jedyną) maskę logowania zarejestrowanej strony (kursor powinien migać w masce logowania).
- Należy kliknąć i przytrzymać przycisk „Logowanie" prawym przyciskiem myszy przez co najmniej 1 sekundę. Wpisany zostaje tylko identyfikator logowania, nawet jeśli przechowywane są identyfikator logowania i hasło.
- Po automatycznym wprowadzeniu hasła należy kliknąć odpowiedni przycisk (np. Następny / Dalej / OK) na stronie internetowej, aby przejść do następnej maski wprowadzania.
- Należy kliknąć myszką w (jedyną) maskę logowania strony (kursor powinien migać w masce logowania).
- Należy kliknąć i przytrzymać przycisk (2) „Hasło" lewym przyciskiem myszy przez co najmniej 1 sekundę. Zostaje wpisane hasło powiązane z identyfikatorem logowania, po którym następuje „Enter". Samo kliknięcie bez przytrzymania powoduje wprowadzenie jedynie hasła.

d) Usuwanie bądź edycja danych dostępu i menu ustawień



- Należy kliknąć przycisk Manager (3) lub po prawej stronie paska zadań „Manager" w menu programu Menedżer haseł, aby uzyskać dostęp do przeglądu wszystkich zapisanych haseł.
- Kliknięcie w kwadrat przed danym wpisem powoduje przełączenie na odpowiednią stronę w standardowej przeglądarce. Jeżeli do jednej strony internetowej zapisanych jest kilka danych logowania, można wybrać żądane logowanie do strony internetowej, klikając w wybraną witrynę na tej liście. Krzyż w kwadracie przed danym wpisem wskazuje na kilka zapisanych danych logowania.
- Za pomocą przycisku + można dodać nowy wpis lub usunąć wybrany wpis za pomocą przycisku -. Ikona gumki otwiera okno wprowadzania zmian do wpisu witryny. Jeśli pozycja ma zostać zmieniona tylko częściowo (np. ma zostać zachowane hasło), nie należy zmieniać ani wprowadzać wpisów. Jeżeli istnieje więcej kont, należy wybrać jedno, aby wprowadzić w nim zmiany lub je usunąć.
- Kliknięcie przycisku w prawym górnym rogu powoduje zamknięcie okna menedżera.

Ustawienia

Należy wybrać z okna administracji symbol koła zębatego, aby wykonać niektóre z poniższych funkcji:

1 Zamknąć

Kliknięcie przycisku w prawym górnym rogu powoduje zamknięcie okna programu.

2 Automatyczne LOGOWANIE

Aby automatycznie zarejestrować menedżera haseł za pomocą hasła głównego, należy aktywować tę funkcję, a następnie podać hasło główne. Potwierdzić przyciskiem „OK".

→ Nie można jednocześnie włączyć funkcji automatycznego logowania i automatycznego wylogowania. Aktywacja tej funkcji powoduje trwałe zapisanie hasła głównego na komputerze użytkownika, tym samym ograniczając maksymalne bezpieczeństwo, które można osiągnąć.

3 Automatyczne WYLOGOWANIE

Aktywowanie automatycznego wylogowania (możliwy przedział czasowy od 1 min do 8 h) powoduje wyświetlenie okna informacyjnego po upływie ustalonego czasu. Menedżer haseł zostaje automatycznie wylogowany po potwierdzeniu („OK") lub upłynięciu czasu. Po naciśnięciu przycisku „NIE" odliczanie zostanie zresetowane.

Nie można jednocześnie włączyć funkcji automatycznego logowania i automatycznego wylogowania. Dezaktywacja trwa od 1 do 3 s ze względu na sprzęt. Wyrejestrowanie zalogowanych stron internetowych nie jest automatyczne. Blokowana jest możliwość ponownego logowania za pomocą zapisanych informacji konta.

4 Zmiana hasła głównego

Aby zmienić hasło główne menedżera haseł, należy nacisnąć „Change PW", wprowadzić bieżące hasło główne, podać nowe hasło główne, a następnie spróbować ponownie. Należy zatwierdzić zmianę.

5 Tworzenie PLIKU KOPII ZAPASOWEJ

Należy zapisać zaszyfrowany plik odzyskiwania (x.POP) na swoim urządzeniu. Należy przy tym nacisnąć przycisk „Backup", podać bezpieczne hasło szyfrowania i folder docelowy na komputerze. Dzięki temu plikowi zawartość może zostać przeniesiona do nowego menedżera haseł.

Bez hasła szyfrowania nie można przywrócić menedżera haseł. Nie należy używać tego samego hasła jako hasła głównego i hasła szyfrowania.

6 Przywracanie menedżera haseł

Należy przywrócić stan kopii zapasowej w menedżerze haseł, klikając „Restore". Należy wybrać żądaną kopię zapasową (rozszerzenie pliku .POP), wprowadzić odpowiednie hasło i kliknąć „Przywróć".

Ten proces spowoduje nadpisanie odpowiedniej zawartości menedżera hasła.

7 Automatyczne włączenie

Ta funkcja minimalizuje okno menu po logowaniu poprzez kliknięcie w przycisk menu „Password Manager"

8 Ustawienia języka

Można wybrać język spośród D/GB/F/NL/I/PL za pośrednictwem pozycji „Select Language" w menu.

→ Wybór języka nie zmienia układu klawiatury.

9 Informacje na temat wersji

Omawia bieżącą wersję (firmware, oprogramowanie i numer seryjny) urządzenia.

Aktualizacja

Przed rozpoczęciem aktualizacji należy zamknąć menedżer haseł na komputerze. Nigdy nie należy odłączać sprzętu podczas aktualizacji. Przed rozpoczęciem aktualizacji należy stworzyć kopię zapasową.

Należy pobrać bieżącą aktualizację (pod:) i ją uruchomić (dwukrotne kliknięcie). Należy przeczytać ostrzeżenie (patrz wyżej) i potwierdzić za pomocą OK. Należy podać hasło główne i stworzyć kopię zapasową, jeżeli w menedżerze zadań przechowywane są ważne dane. Należy podać hasło kopii zapasowej i wybrać docelowy folder dla kopii zapasowej. Po udanej identyfikacji produktu oraz weryfikacji na menedżerze haseł zapisany zostaje nowy system operacyjny. Udaną aktualizację należy potwierdzić przyciskiem OK, wyjąć urządzenie i ponownie je podłączyć. Po aktualizacji urządzenie uruchamia się dodatkową minutę dłużej.

Komunikaty o błędach

Typowe komunikaty o błędach to:

- Zainstalowana wersja oprogramowania jest bardziej aktualna od wersji wybranej aktualizacji.
- Urządzenie nie rozpoznaje menedżera haseł. Należy podłączyć odpowiednie urządzenie.
- Nie można rozpocząć aktualizacji. Należy ponownie uruchomić komputer, poprawnie podłączyć urządzenie i upewnić się, że użytkownik posiada odpowiednie prawa dostępu do aktualizacji.
- Wersja oprogramowania zainstalowanego programu nie mogła zostać rozpoznana. Należy ponownie uruchomić komputer, poprawnie podłączyć urządzenie i upewnić się, że użytkownik posiada odpowiednie prawa dostępu do aktualizacji.
- Błąd File Write (FW): Błąd komunikacji podczas aktualizacji. Należy powtórzyć procedurę. Należy ponownie uruchomić komputer, poprawnie podłączyć urządzenie i upewnić się, że użytkownik posiada odpowiednie prawa dostępu do aktualizacji.

→ Ostatecznie błąd w języku angielskim zostanie oznaczony jako „Error".

Utylizacja

Urządzenia elektroniczne zawierają surowce wtórne; pozbywanie się ich wraz z odpadami domowymi nie jest dozwolone. Po zakończeniu eksploatacji produktu należy go zutylizować zgodnie z obowiązującymi przepisami prawnymi.

Dane techniczne

Wersja oprogramowania	1.7 (na podstawie niniejszej instrukcji)
Napięcie robocze	DC 5 V
Zużycie energii	0,5 W
Interfejs	USB 2.0 High Speed (kompatybilny wstecz)
Wskaźniki robocze	wielokolorowe diody LED
Algorytmy szyfrowania	AES256, SEED 256, ARIA sprzętowy układ zabezpieczający
Grupa urządzeń	komputer
System operacyjny	Windows 7, Windows 8, Windows 10
Obsługiwane przeglądarki	Internet Explorer (IE), Chrome, Opera, QQ, 360safe, Sogou, Firefox
Wymiary produktu	26 x 79 x 14 mm
Ciężar	0,013 kg
Temperatura robocza	od 0 do 45 °C
Temperatura przechowywania	od -20 do 70 °C

To publikacja została opublikowana przez Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92240 Hirschau, Niemcy (www.conrad.com).