



**CENTRUM
CYBERBEZPIECZEŃSTWA**

Wiedza, wsparcie, zaufanie

SECUREBOX


INSTRUKCJA OBSŁUGI




1.	Słownik pojęć	3
2.	Proces obsługi Aplikacji	5
2.1.	Czynności początkowe	5
2.2.	Uproszczona obsługa urządzenia – procesu skanowania i kopiowania plików	6
2.3.	Poszczególne kroki procesu skanowania plików	9
2.4.	Poszczególne kroki procesu kopiowania plików	12
2.5.	Czynności końcowe	14
2.6.	Oczekiwany rezultat	14
3.	Wyciąg kluczowych informacji z warunków gwarancji	15

SecureBox to urządzenie oraz aplikacja, które wspomagają ochronę organizacji klienta przed zagrożeniami przenoszonymi na nośnikach danych USB oraz płytach CD/DVD. Aplikacja analizuje pliki pochodzące z nośników zewnętrznych oznaczonych jako USB RED (potencjalnie niebezpieczne), a następnie kopiuje jedynie te pliki, które są niezainfekowane, na nośnik organizacji klienta oznaczony jako USB BLUE (bezpieczny). Dzięki ekranowi dotykowemu, przejrzystemu interfejsowi użytkownika oraz dostępowi do sprawdzonych silników antywirusowych, urządzenie zapewnia łatwą obsługę i bezpieczeństwo dla organizacji.

USB RED lub CD/DVD RED   – Nośnik pamięci USB lub płyta CD/DVD, które mogą zawierać zainfekowane pliki. Z tego nośnika będą kopiowane pliki na nośnik USB BLUE (bezpieczny).

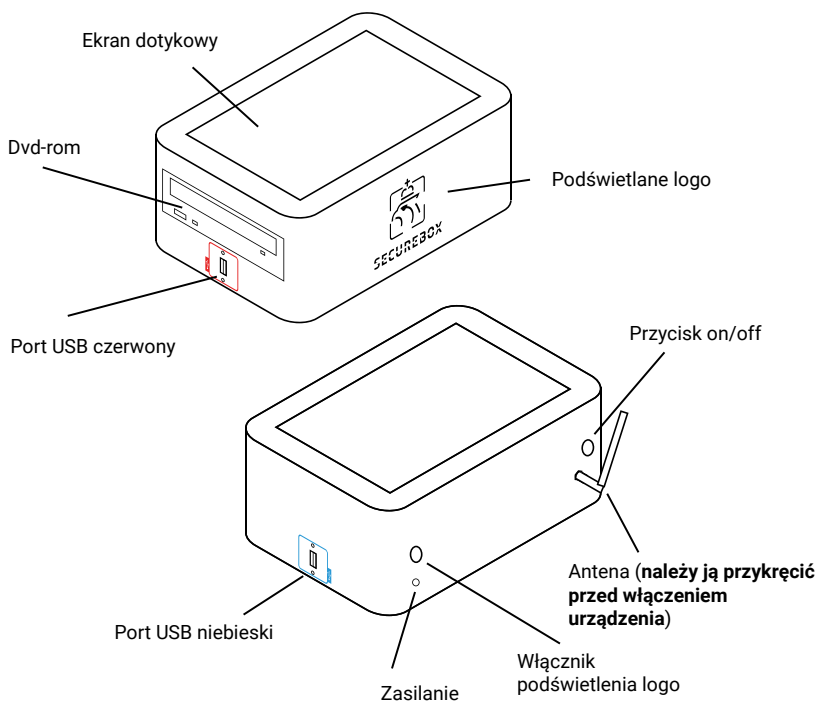
USB BLUE  – Nośnik pamięci USB, który zawiera wyłącznie niezainfekowane pliki. Na ten nośnik będą kopiowane niezainfekowane pliki, tak aby można było podłączyć go do innych komputerów organizacji.

Plik Nieprzeskanowany  – Plik, który nie został jeszcze przeskanowany przez silniki antywirusowe aplikacji.

Plik Bezpieczny **Bezpieczny** – Plik, w którym podczas skanowania przez silnik antywirusowy, nie wykryto wirusa.

Plik Niebezpieczny **Niebezpieczny** – Plik, w którym podczas skanowania przez silnik antywirusowy, wykryto wirusa.

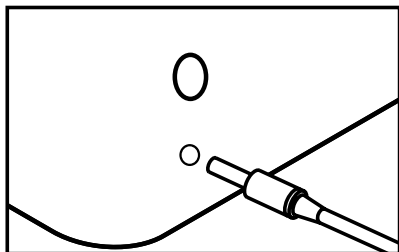
Plik Skopiowany **Skopiowany** – Plik bezpieczny (wcześniej przeskanowany i oznaczony jako „Bezpieczny”), który został skopiowany na nośnik organizacji (USB BLUE).



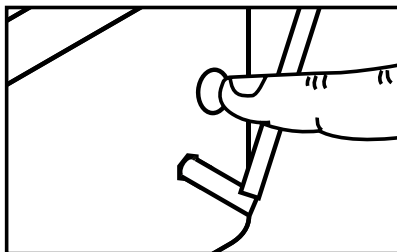
2.1 Czynności początkowe

1. Dostęp do urządzenia SecureBox.
2. Dostęp do aktualnej wersji Aplikacji.
3. Na płycie CD/DVD RED, szyfrowanym nośniku pamięci USB RED lub nośniku pamięci USB RED, istnieją pliki, które mogą być potencjalnie zagrożone obecnością wirusów.
4. Na nieszyfrowany lub szyfrowany nośnik pamięci USB BLUE należy przekopiować pliki wolne od wirusów.

2.2. Uproszczona obsługa urządzenia – procesu skanowania i kopiowania plików



1. Podłącz zasilacz do Secure-Box.



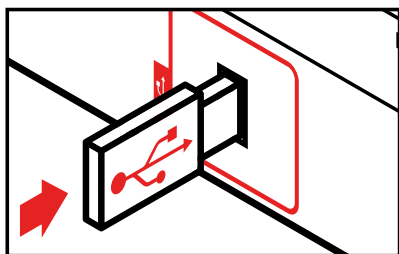
2. Włącz SecureBox przyciskiem on/off.



3. Pojawi się ekran uruchamiania aplikacji, poczekaj kilka chwil.



4. Pojawi się polecenie, aby podłączyć USB RED lub CD/DVD RED.



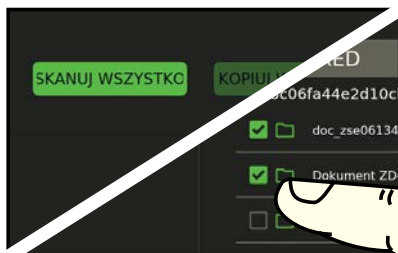
5. Podłącz USB RED do czerwonego portu po lewej stronie urządzenia.



6. Jeżeli USB RED jest zaszyfrowane wprowadź hasło i naciśnij przycisk <Enter>.



7. Pojawi się ekran główny aplikacji.



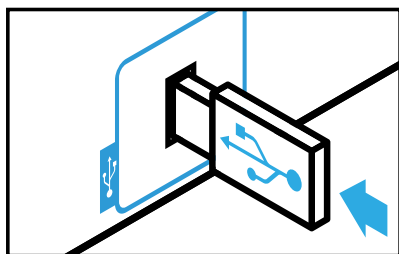
8. Kliknij przycisk <Skanuj wszystko> lub wybierz foldery lub pojedyncze pliki do skanowania, a następnie kliknij przycisk <Skanuj>.



9. Pojawi się ekran skanowania. Poczekaj aż pliki zostaną przeskanowane i wyświetli się raport skanowania. Następnie kliknij przycisk <Rozumiem>.



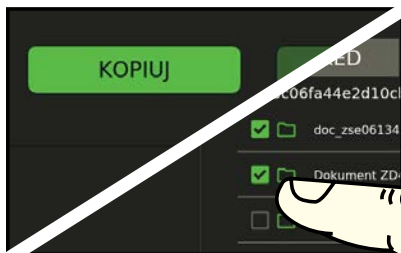
10. Po zakończeniu skanowania wyświetli się ekran główny, a przeskanowane pliki będą miały status: „Bezpieczny” lub „Niebezpieczny”.



11. Aby skopiować pliki oznaczone jako „Bezpieczne” na USB BLUE, włóż USB BLUE do niebieskiego portu po prawej stronie urządzenia.



12. Pojawi się ekran USB BLUE (z informacjami nt. nośnika USB BLUE), przełącz się na zakładkę USB BLUE (po lewej stronie u góry ekranu).



13. Kliknij przycisk „Kopiuj”, aby skopiować Bezpieczne pliki na USB BLUE lub wybierz pliki, które nie zostały jeszcze przeskanowane, a następnie kliknij przycisk <Skanuj> (patrz kroki 9-10).



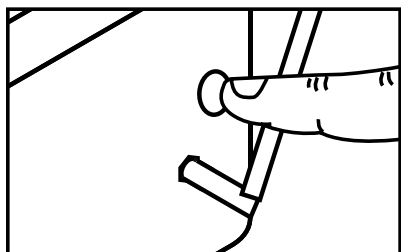
14. Po kliknięciu przycisku <Kopiuj> pojawi się ekran kopiowania, poczekaj aż pliki zostaną przekopiowane i wyświetli się raport kopiowania. Następnie kliknij przycisk <Rozumiem>.



15. Po zakończeniu kopiowania wyświetli się ekran główny, a skopiowane pliki będą miały status „Skopiowany” zarówno w zakładce USB RED jak i USB BLUE. Gratulacje! Pliki zostały sprawdzone i skopiowane na USB BLUE.



16. Po odłączeniu nośnika USB RED aplikacja powróci do ekranu startowego



17. W celu wyłączenia urządzenia należy przytrzymać kilka sekund przycisk on/off.

2.3. Poszczególne kroki procesu skanowania plików

1. Włączyć urządzenie SecureBox.



il. 1

2. Pojawi się ekran ładowania aplikacji z informacją: „Poczekaj na załadowanie się aplikacji” (*il. 1*)



il. 2

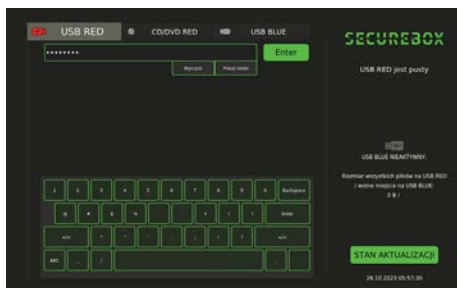
3. Po kilkunastu sekundach pojawi się komunikat: Podepnij pendrive do USB RED lub włóż płytę CD/DVD (*il. 2*). Do urządzenia do portu oznaczonego kolorem czerwonym należy podłączyć nośnik pamięci USB RED lub włożyć płytę CD/DVD.



il. 3

Aplikacja wyświetli pliki znajdujące się na nośniku pamięci USB RED lub płycie CD/DVD. Przycisk <Skanuj wszystko> jest aktywny. (*il. 3*)

Jeśli podłączasz zaszyfrowany nośnik pamięci USB RED, zostanie wyświetlony ekran umożliwiający



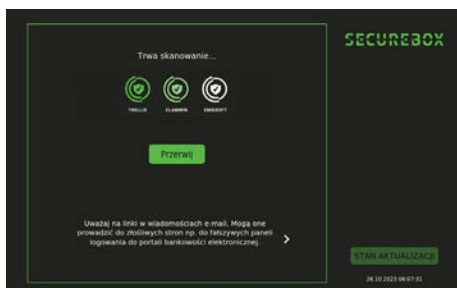
il. 4

odszyfrowanie nośnika poprzez wprowadzenie hasła (il. 4). Wprowadź hasło i kliknij przycisk <Enter>. Po poprawnym odszyfrowaniu nośnika pamięci USB RED, aplikacja wyświetli ekran, jak na **ilustracji 3**.

4. Należy użyć przycisku <Skanuj wszystko> aby aplikacja rozpoczęła skanowanie całej zawartości USB RED lub wybrać ręcznie poszczególne pliki (lub foldery) i kliknąć przycisk <Skanuj>.

Jeśli wybrane pliki do skanowania przekroczą 120 MB, aplikacja wyświetli informację o możliwości długiego trwania procesu skanowania.

5. Aplikacja wyświetli ekran skanowania plików (il. 5). W tym momencie Aplikacja skanuje pliki silnikami antywirusowymi w celu wykrycia plików zagrożonych wirusami. Podczas procesu skanowania Aplikacja na bieżąco wyświetla wskazówki dla Użytkowników.



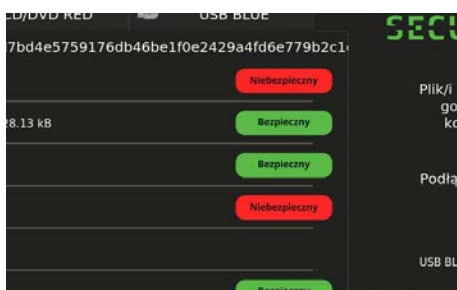
il. 5

Aplikacja skanuje pliki silnikami antywirusowymi w celu wykrycia plików zagrożonych wirusami. Podczas procesu skanowania Aplikacja na bieżąco wyświetla wskazówki dla Użytkowników.

6. Po zakończeniu skanowania wyświetla się raport skanowania (il. 6) informujący o efektach skanowania: ilość przeskanowanych plików i ilość



il. 6



il. 7

wykrytych zagrożeń. Należy wcisnąć przycisk <Rozumiem>.

7. Następuje powrót do ekranu głównego Aplikacji. Przeskanowane pliki mają status „Bezpieczny” lub „Niebezpieczny” (*il. 7*). Użytkownik ma możliwość wyboru kolejnych plików Nieprzeskanowanych (o ile takie zostały) lub przejścia do etapu kopiowania plików.

2.4. Poszczególne kroki procesu kopiowania plików

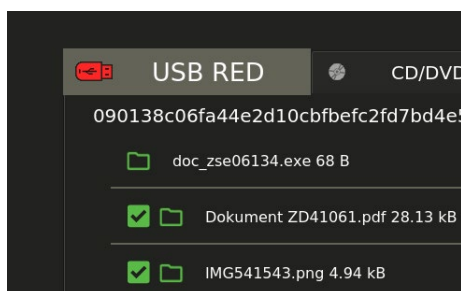
1. Do urządzenia do portu oznaczonego kolorem niebieskim należy podłączyć nośnik pamięci USB BLUE. Aplikacja wyświetli ekran z zakładką USB BLUE, zawierającą informacje o plikach i dostępnym miejscu na nośniku pamięci USB BLUE (*il. 8 i il. 9*)



il. 8



il. 9



il. 10

Jeśli podłączasz zaszyfrowany nośnik pamięci USB BLUE, zostanie wyświetlony ekran umożliwiający odszyfrowanie nośnika poprzez wprowadzenie hasła (*il. 4*). Wprowadź hasło i kliknij przycisk <Enter>. Po poprawnym odszyfrowaniu nośnika pamięci USB BLUE, aplikacja wyświetli ekran, jak przedstawiono na *ilustracji 8*.

2. Przejdź do zakładki USB RED (*il. 10 i il. 11*) i użyj przycisku <Kopiuj>, aby aplikacja rozpoczęła kopiowanie przeskanowanych Bezpiecznych



il. 11

plików lub wybierz ręcznie pojedyncze pliki (lub foldery) Bezpieczne i kliknij przycisk <Kopiuj>. Aplikacja informuje o wielkości zaznaczonych plików na USB RED i dostępnym miejscu na USB BLUE (**il.12**).



il. 12

3. Aplikacja wyświetli ekran kopiowania plików. Po zakończeniu kopiowania wyświetli się raport kopiowania informujący o ilości skopiowanych plików. Naciśnij przycisk <Rozumiem> (**il. 13**)



il. 13

4. Następuje powrót do ekranu głównego aplikacji. Skopiowane pliki mają status „Skopiowany” zarówno w zakładce USB RED, jak i USB BLUE.

2.5. Czynności końcowe

Odłączyć nośnik pamięci USB RED oraz nośnik pamięci USB BLUE od urządzenia.

2.6. Oczekiwany rezultat

Aplikacja wykryła podłączony do urządzenia portu oznaczonego kolorem czerwonym nośnik pamięci USB RED, płytę CD/DVD RED lub szyfrowany nośnik pamięci USB RED i wyświetliła pliki znajdujące się na tym nośniku. Aplikacja wykryła podpięty do urządzenia do portu oznaczonego kolorem niebieskim nośnik pamięci USB BLUE i poinformowała o tym użytkownika wyświetlając informację na ekranie głównym. Użytkownik dokonał wyboru plików znajdujących się na nośniku pamięci USB RED. Aplikacja przeskanowała pliki silnikami antywirusowymi i skopiowała pliki niezainfekowane na nośnik pamięci USB BLUE. Aplikacja wyświetliła raporty ze skanowania i kopiowania plików, w których znalazły się informacje o ilości plików przeskanowanych, zainfekowanych oraz skopiowanych.



3. WYCIĄG KLUCZOWYCH INFORMACJI Z WARUNKÓW GWARANCJI

1. Centrum Cyberbezpieczeństwa udziela gwarancji na cały okres obowiązywania Zlecenia na terenie Polski.
2. W ramach udzielonej gwarancji Centrum Cyberbezpieczeństwa zobowiązuje się do reagowania na zgłoszenia serwisowe dotyczące awarii i błędów Systemu Securebox oraz awarii urządzenia. Zgłoszenia należy kierować na adres email: securebox@cc.gov.pl
3. Gwarancja nie obejmuje uszkodzeń wynikłych z niewłaściwego, niezgodnego z przeznaczeniem użytkowania urządzenia, w tym stłuczenia ekranu dotykowego.
4. Dane kontaktowe Gwaranta (Centrum Cyberbezpieczeństwa):
Centrum Cyberbezpieczeństwa ul. Rynek Solny 1 lok. 6, 6A, 7
22-400 Zamość
5. Pozostałe warunki gwarancji znajdują się w umowie zawartej pomiędzy Centrum Cyberbezpieczeństwa a Ministerstwem Sprawiedliwości Biuro Cyberbezpieczeństwa.



**CENTRUM
CYBERBEZPIECZEŃSTWA**

cc.gov.pl



SECUREBOX

cc.gov.pl/securebox

© 2023 Wszelkie prawa zastrzeżone Centrum Cyberbezpieczeństwa

Jesteś zainteresowany naszą ofertą?

Napisz do nas lub zadzwoń

securebox@cc.gov.pl

+48 570 353 545