Strażnik

podręcznik użytkownika

Strażnik: podręcznik użytkownika

data wydania środa, 17. maj 2017 Version 2.8.0

Spis treści

1 Informacje o tej dokumentacji 5

2 Do czego służy aplikacja Strażnik? 7

3 Korzystanie z aplikacji Strażnik 9

3.1 Konfiguracja aplikacji *Strażnik* 10

3.2 Szyfrowanie konwersacji e-mail 11
3.2.1 Odczytywanie zaszyfrowanych konwersacji e-mail 11
3.2.2 Szyfrowanie przychodzących wiadomości e-mail 12
3.2.3 Wysyłanie zaszyfrowanych wiadomości e-mail 12
3.2.4 Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail? 14

3.3 Szyfrowanie plików 15
3.3.1 Szyfrowanie plików 15
3.3.2 Tworzenie nowych zaszyfrowanych plików 16
3.3.3 Otwieranie zaszyfrowanych plików 16
3.3.4 Pobieranie zaszyfrowanych plików 17
3.3.5 Odszyfrowywanie plików 17

3.4 Szyfrowanie dokumentów pakietu Office 18
3.4.1 Tworzenie nowych zaszyfrowanych plików 19
3.4.2 Zapisywanie wybranych dokumentów w zaszyfrowanym formacie 19
3.4.3 Otwieranie zaszyfrowanego dokumentu 20

3.5 Wyloguj się z aplikacji Strażnik 21

3.6 Ustawienia aplikacji Strażnik 22
3.6.1 ustawienia zabezpieczeń aplikacji Strażnik 23
3.6.2 Ustawienia szyfrowania PGP 23
3.6.3 Zarządzanie kluczami 25

Indeks 29

1 Informacje o tej dokumentacji

Poniższe informacje pozwolą sprawniej posługiwać się tą dokumentacją.

- Jaka jest grupa docelowa niniejszej dokumentacji?
- Jaka jest zawartość niniejszej dokumentacji?
- Dodatkowa pomoc

Jaka jest grupa docelowa niniejszej dokumentacji?

Niniejsza dokumentacja jest skierowana do użytkowników, którzy chcą szyfrować komunikację e-mail i pliki, chroniąc je przed nieuprawnionym dostępem.

Jaka jest zawartość niniejszej dokumentacji?

Niniejsza dokumentacja zawiera następujące informacje:

- W sekcji *Do czego służy aplikacja Strażnik?* znajduje się opis aplikacji Strażnik.
- . W sekcji *Korzystanie z aplikacji Strażnik* znajdują się informacje dotyczące usługi Strażnik

. Niniejsza dokumentacja przedstawia mechanizmy pracy z typową instalacją i konfiguracją oprogramowania do pracy grupowej. Wersja, której używasz, może różnić się od przedstawionej w tym dokumencie.

Dodatkowa pomoc

Pełna dokumentacja oprogramowania do pracy grupowej znajduje się w podręczniku użytkownika programu Oprogramowanie do pracy grupowej.

2 Do czego służy aplikacja Strażnik?

Strażnik jest składnikiem zabezpieczeń oprogramowania do pracy grupowej umożliwiającym szyfrowanie wiadomości e-mail i plików.

- Szyfruj korespondencję e-mail prowadzoną z innym użytkownikami lub partnerami zewnętrznymi.
- Zaszyfruj pojedynczy plik i podziel się zaszyfrowanymi danymi z innymi użytkownikami.
- Określaj poziom szyfrowania za pomocą opcji zabezpieczeń.
- Szyfrowane dane są chronione hasłem. Aby uchronić się przed skutkami utraty hasła, korzystaj z funkcji resetowania go.

3 Korzystanie z aplikacji Strażnik

Dowiedz się, jak pracować z aplikacją *Strażnik*.

- Stosowanie ustawień podstawowych
- Szyfrowanie korespondencji e-mail
- Szyfrowanie plików
- Szyfrowanie dokumentów pakietu Office
- Stosowanie ustawień zabezpieczeń

3.1 Konfiguracja aplikacji *Strażnik*

Przed użyciem aplikacji *Strażnik* należy wprowadzić kilka ustawień podstawowych.

- Najpierw należy podać hasło zabezpieczające aplikacji Strażnik, które posłuży do szyfrowania danych oraz ich otwierania.
- Wpisz dodatkowy adres e-mail który przyda Ci się, gdy zapomnisz hasła do aplikacjiStrażnik. Dzięki niemu będziesz mieć możliwość zresetowania hasła zabezpieczającego aplikacji Strażnik i otrzymania nowego. Dlatego zalecamy wpisanie dodatkowego adresu e-mail. W przeciwnym razie nowe hasło zostanie wysłane na główny adres e-mail.

Podstawowe ustawienia można wprowadzić na dwa sposoby:

- Zdefiniuj podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania.
- Zdefiniuj podstawowe ustawienia na stronie ustawień oprogramowania do pracy grupowej przed pierwszym użyciem funkcji szyfrowania.

Jak zdefiniować podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania:

1. Włącz funkcję szyfrowania podczas tworzenia wiadomości e-mail, szyfrowania pliku lub przesyłania nowego pliku, klikając ikonę **Szyfrowanie** dostępną w drzewie folderów obok nazwy folderu.
2. Następnie pojawi się prośba o wpisanie hasła do aplikacji Strażnik oraz dodatkowego adresu e-mail. Wpisz potrzebne informacje.

Jak zdefiniować podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym polecenie **Zabezpieczenia Strażnik**.

   Po pierwszym uruchomieniu ustawień bezpieczeństwa aplikacji Strażnik pojawi się okno *Utwórz klucze zabezpieczeń Strażnik* .
3. W polu **Hasło** wprowadź hasło, którego chcesz używać do szyfrowania danych.

   Potwierdź hasło, wprowadzając je ponownie w polu **Zweryfikuj**.
4. W polu **Wpisz nowy dodatkowy adres e-mail** wpisz adres, na który otrzymasz hasło tymczasowe pozwalające na zresetowanie hasła zabezpieczającego aplikacji Strażnik.
5. Kliknij przycisk **OK**.

3.2 Szyfrowanie konwersacji e-mail

Dostępne są następujące możliwości:

- Odczytywanie zaszyfrowanych konwersacji e-mail
- Szyfrowanie przychodzących wiadomości e-mail
- Wysyłanie zaszyfrowanych wiadomości e-mail
- Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail?

3.2.1 Odczytywanie zaszyfrowanych konwersacji e-mail

Aby móc odczytać zaszyfrowaną wiadomość e-mail, należy podać co najmniej hasło zabezpieczające aplikacjiStrażnik. Nadawca szyfrowanej wiadomości może ją dodatkowo zabezpieczyć jeszcze jednym hasłem.

Jak przeczytać zaszyfrowaną wiadomość e-mail:

1. Wybierz wiadomość e-mail z ikoną *Szyfrowanie*. W widoku szczegółów pojawi się powiadomienie *Zabezpieczona wiadomość e-mail. Wpisz hasło aplikacji Guard Security.*

   Uwaga: Jeśli przy ostatnim użyciu aplikacji Strażnik the ustawiono zapamiętywanie hasła bezpieczeństwa w aplikacji Strażnik wiadomość e-mail wyświetli się natychmiast.

2. Wpisz hasło zabezpieczające aplikacji Strażnik.

   Można ustawić czas pamiętania hasła przez aplikację Strażnik. Aby to zrobić, wybierz opcję Nie wylogowuj mnie z aplikacji **Strażnik** i wybierz zakres czasu z listy.

   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.

3. Kliknij przycisk **OK**. Zawartość pojawi się w formacie zwykłego tekstu.

   Jeśli wiadomość e-mail ma załączniki, pojawią się funkcje obsługi załączników w formie zaszyfrowanej lub odszyfrowanej.

Uwaga: w przypadku korzystania z szyfrowanej korespondencji e-mail można tylko odpowiedzieć na tę wiadomość lub przesłać ją dalej.

Zobacz też

Szyfrowanie przychodzących wiadomości e-mail (p. 12)
Wysyłanie zaszyfrowanych wiadomości e-mail (p. 12)
Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail? (p. 14)

3.2.2 Szyfrowanie przychodzących wiadomości e-mail

Możesz ustawić automatyczne szyfrowanie wszystkich przychodzących wiadomości e-mail.

Jak szyfrować wszystkie wiadomości przychodzące:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Zabezpieczenia aplikacji Strażnik**. Kliknij pozycję **Ustawienia zaawansowane**.
3. Pamiętaj, aby włączyć funkcję **Włącz zaawansowane funkcje PGP**.
   Włącz opcję **Szyfruj wszystkie wiadomości przychodzące**.

Zobacz też

Odczytywanie zaszyfrowanych konwersacji e-mail (p. 11)
Wysyłanie zaszyfrowanych wiadomości e-mail (p. 12)
Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail? (p. 14)

3.2.3 Wysyłanie zaszyfrowanych wiadomości e-mail

Dostępne są następujące możliwości:

- Wysyłanie zaszyfrowanych wiadomości e-mail. Treść wiadomości e-mail będzie dostępna tylko dla nadawcy i odbiorcy wiadomości.
  Ostrzeżenie: w przypadku wysyłania wersji roboczej szyfrowanej wiadomości e-mail wysłana wersja robocza zostanie usunięta z folderu *Wersje robocze*.
- Wysyłanie wiadomości e-mail z podpisem. Podpis upewnia adresata, że wiadomość e-mail nie została zmodyfikowana po drodze.
- Wysyłanie zaszyfrowanych wiadomości e-mail z podpisem.

Jak wysłać zaszyfrowaną wiadomość e-mail:

1. Napisz wiadomość e-mail w aplikacji *E-mail* tak jak to zwykle robisz.
   Na stronie *Nowa wiadomość* kliknij widoczną w prawym górnym rogu ikonę **Szyfruj**
   Możesz też kliknąć pozycję **Zabezpieczenia** pod tematem. Wybierz opcję **Zaszyfruj**.
   Ikony wyświetlane obok odbiorców wskazują, czy możliwe jest zaszyfrowanie tej wiadomości u tego odbiorcy. Po ustawieniu kursora nad ikoną pojawi się odpowiedni opis.
2. Aby wyświetlić dodatkowe opcje, kliknij pozycję **Zabezpieczenia**. Możesz aktywować niżej wymienione opcje.
   Aby dodatkowo podpisać wiadomość e-mail, włącz opcję **Podpisz**.
   Jeśli klient poczty e-mail adresata nie obsługuje standardu PGP, a mimo to wiadomość powinna być czytelna, włącz opcję **PGP Inline**. Po włączeniu tego ustawienia nie będzie można wysyłać wiadomości e-mail w formacie HTML.
   Aby umożliwić odbiorcy e-mail wysłanie zaszyfrowanej odpowiedzi, odbiorca musi mieć Twój klucz publiczny. Możesz go wysłać jako załącznik. Aby to zrobić, kliknij polecenie **Dołącz mój klucz**.
3. Kliknij polecenie **Wyślij zaszyfrowane**.
   W przypadku wysyłania wiadomości do adresatów zewnętrznych pojawi się okno umożliwiające wysłanie im uwag dotyczących otwarcia zaszyfrowanej wiadomości e-mail [14].
   Odbiorca zaszyfrowanej wiadomości e-mail, z którym wcześniej nie prowadzono korespondencji, otrzyma załącznik z Twoim kluczem publicznym.

Zobacz też

Odczytywanie zaszyfrowanych konwersacji e-mail (p. 11)
Szyfrowanie przychodzących wiadomości e-mail (p. 12)
Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail? (p. 14)

3.2.4 Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail?

Zaszyfrowane wiadomości e-mail można także wysyłać do odbiorców zewnętrznych, którzy nie są użytkownikami oprogramowania do pracy grupowej. Po dodaniu odbiorcy zewnętrznego aplikacja Guard sprawdzi, czy oferuje on klucz publiczny. Dalsze postępowanie zależy od wyniku tej kontroli.

- Jeśli odbiorca oferuje klucz publiczny:
  - Wiadomość zostanie zaszyfrowana za pomocą tego klucza. Odbiorca może ją odczytać za pomocą klucza prywatnego.
  - Aby umożliwić odbiorcy wysłanie zaszyfrowanej odpowiedzi, Twój klucz publiczny zostanie wysłany jako załącznik o nazwie public.asc. Odbiorca może go następnie zaimportować do używanego klienta poczty e-mail.
- Jeśli odbiorca nie oferuje klucza publicznego:
  - Użytkownik zewnętrzny, który ma już konto gościa, razem z wiadomością e-mail otrzyma odnośnik do strony logowania na to konto. Użycie go i zalogowanie się pozwoli na odczytanie zaszyfrowanej wiadomości e-mail i ewentualne przesłanie odpowiedzi.
  - Jeśli dany użytkownik nie ma jeszcze takiego konta, zostanie ono założone. Następnie do użytkownika zewnętrznego zostanie wysłana wiadomość z automatycznie wygenerowanym hasłem i odnośnikiem do strony logowania na konto gościa. Po zalogowaniu się będzie możliwe nadanie własnego hasła.
    W zależności od konfiguracji automatycznie utworzone hasło i link do strony zostaną wysłane w osobnych e-mailach.
  - Konta dla gości (do odczytu szyfrowanych wiadomości e-mail) są kasowane po pewnej liczbie dni wprowadzonej w konfiguracji oprogramowania do pracy grupowej. Aby zachować ich dostępność są one także przesyłane w zaszyfrowanej formie jako załączniki do wiadomości z odnośnikiem o nazwie encypted.asc. Taki załącznik można przesłać na stronę konta gościa, odszyfrować i odczytać.

Zobacz też

Odczytywanie zaszyfrowanych konwersacji e-mail (p. 11)
Szyfrowanie przychodzących wiadomości e-mail (p. 12)
Wysyłanie zaszyfrowanych wiadomości e-mail (p. 12)

3.3 Szyfrowanie plików

Dostępne są następujące możliwości:

- Szyfrowanie plików
- Tworzenie nowych zaszyfrowanych plików
- Otwieranie zaszyfrowanych plików
- Pobieranie zaszyfrowanych plików
- Odszyfrowywanie plików

3.3.1 Szyfrowanie plików

W przypadku szyfrowania plików zostaną zaszyfrowane tylko ich ostatnie wersje. Wszystkie inne wersje zostaną usunięte.

Jak zaszyfrować plik:

Ostrzeżenie: w przypadku szyfrowania pliku zostaną usunięte wszystkie jego wersje — oprócz bieżącej. Aby zachować starszą wersję, należy ją zapisać przed zaszyfrowaniem pliku.

1. Wybierz dowolną liczbę plików w aplikacji *Pliki*. Kliknij widoczną na pasku narzędzi ikonę **Działania** ☰▾. W menu kliknij pozycję **Zaszyfruj**.

   Możesz także kliknąć ikonę **Działania** ☰. Kliknij pozycję menu **Szyfruj**.

2. Jeśli plik zawiera wiele wersji, pojawi się okno *Szyfrowanie plików*. Potwierdź, że chcesz zaszyfrować plik i usunąć wszystkie poprzednie wersje, klikając przycisk **OK**.

   Jeśli plik ma tylko jedną wersję, zostanie zaszyfrowany bez dalszych monitów.

Zobacz też

Tworzenie nowych zaszyfrowanych plików (p. 16)
Otwieranie zaszyfrowanych plików (p. 16)
Pobieranie zaszyfrowanych plików (p. 17)
Odszyfrowywanie plików (p. 17)

3.3.2 Tworzenie nowych zaszyfrowanych plików

Nowy zaszyfrowany plik możesz utworzyć, przesyłając plik lokalny z szyfrowaniem.

Jak utworzyć nowy zaszyfrowany plik:

1. Wybierz folder w drzewie folderów w aplikacji *Pliki*.
   Uwaga: otwórz folder, w przypadku którego masz uprawnienia do tworzenia obiektów.
2. Kliknij dostępną na pasku narzędzi ikonę **Nowe**. Kliknij pozycję **Dodaj i zaszyfruj plik lokalny**.
3. Wybierz dowolną liczbę plików w oknie *Prześlij plik*.
   Kliknij przycisk **Otwórz**. W obszarze wyświetlania będzie pokazywany bieżący status postępu.
   Aby anulować postęp, kliknij pozycję **Szczegóły pliku** z prawej strony u dołu obszaru wyświetlania. Kliknij pozycję **Anuluj** obok nazwy pliku w oknie *Postęp przesyłania*.

Wskazówka: nowy zaszyfrowany plik możesz także utworzyć, przeciągając go z pulpitu systemu operacyjnego do okna aplikacji *Pliki* i upuszczając w górnej części okna.

Zobacz też

Szyfrowanie plików (p. 15)
Otwieranie zaszyfrowanych plików (p. 16)
Pobieranie zaszyfrowanych plików (p. 17)
Odszyfrowywanie plików (p. 17)

3.3.3 Otwieranie zaszyfrowanych plików

Zaszyfrowany plik możesz otworzyć i przeczytać. Plik będzie nadal zapisany na serwerze w zaszyfrowanej postaci.

Jak otworzyć zaszyfrowany plik:

1. W obszarze wyświetlania w aplikacji *Pliki* wybierz zaszyfrowany plik. Kliknij widoczną na pasku narzędzi ikonę **Widok** .
2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Strażnik* . Wpisz hasło zabezpieczające aplikacji Strażnik.
   Można ustawić długość pamiętania hasła przez aplikację Strażnik. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.
   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.
   Kliknij przycisk **OK**.

Zobacz też

Szyfrowanie plików (p. 15)
Tworzenie nowych zaszyfrowanych plików (p. 16)
Pobieranie zaszyfrowanych plików (p. 17)
Odszyfrowywanie plików (p. 17)

3.3.4 Pobieranie zaszyfrowanych plików

Zaszyfrowany plik możesz pobrać, aby go lokalnie przeczytać lub zmodyfikować. Plik będzie nadal zapisany na serwerze w zaszyfrowanej postaci.

Jak pobrać zaszyfrowany plik:

1. W obszarze wyświetlania w aplikacji *Pliki* wybierz zaszyfrowany plik. Kliknij widoczną na pasku narzędzi ikonę **Widok** .

   Uwaga: Jeśli w okienku wyskakującym klikniesz polecenie **Pobierz**, pobrany plik pozostanie zaszyfrowany.

2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Strażnik* . Wpisz hasło zabezpieczające aplikacji Strażnik.

   Można ustawić długość pamiętania hasła przez aplikację Strażnik. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.

   Kliknij przycisk **OK**.

3. Kliknij ikonę **Działania** w przeglądarce. Kliknij polecenie **Pobierz odszyfrowane**.

Zobacz też

Szyfrowanie plików (p. 15)
Tworzenie nowych zaszyfrowanych plików (p. 16)
Otwieranie zaszyfrowanych plików (p. 16)
Odszyfrowywanie plików (p. 17)

3.3.5 Odszyfrowywanie plików

Aby usunąć szyfrowanie z pliku, należy go odszyfrować.

Jak odszyfrować plik:

1. W aplikacji *Pliki* wybierz zaszyfrowany plik w obszarze wyświetlania. Kliknij widoczną na pasku narzędzi ikonę **Działania** . W menu kliknij pozycję **Usuń szyfrowanie**.

2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Strażnik* . Wpisz hasło zabezpieczające aplikacji Strażnik.

   Można ustawić długość ważności hasła w aplikacji Strażnik. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.

   Kliknij przycisk **OK**.

Zobacz też

Szyfrowanie plików (p. 15)
Tworzenie nowych zaszyfrowanych plików (p. 16)
Otwieranie zaszyfrowanych plików (p. 16)
Pobieranie zaszyfrowanych plików (p. 17)

3.4 Szyfrowanie dokumentów pakietu Office

Istnieją następujące opcje:

- Tworzenie nowych zaszyfrowanych plików
- Zapisywanie wybranych dokumentów w zaszyfrowanym formacie
- Otwieranie zaszyfrowanego dokumentu

Dodatkowe funkcje są dostępne w aplikacji *Pliki*.

- szyfrowanie istniejących dokumentów
- odszyfrowywanie dokumentów

3.4.1 Tworzenie nowych zaszyfrowanych plików

Podczas tworzenia nowego dokumentu dostępne są opcje, które pozwolą go zapisać z szyfrowaniem.

Jak utworzyć nowy zaszyfrowany dokument:

1. W zależności od tego, czy chcesz utworzyć zaszyfrowany dokument tekstowy, arkusz kalkulacyjny lub prezentację, wybierz jedną z aplikacji *Tekst*, *Arkusz* lub *Prezentacja*..
2. Na pasku menu pakietu Office kliknij jeden z odpowiednich przycisków: **Nowy dokument tekstowy (szyfrowany)**, **Nowy arkusz kalkulacyjny (szyfrowany)**, **Nowa prezentacja (szyfrowana)**.
3. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Strażnik* . Wpisz hasło zabezpieczające aplikacji Strażnik.

   Można ustawić długość pamiętania hasła przez aplikację Strażnik. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.

   Kliknij przycisk **OK**.

Zobacz też

Zapisywanie wybranych dokumentów w zaszyfrowanym formacie (p. 19)
Otwieranie zaszyfrowanego dokumentu (p. 20)
Szyfrowanie plików (p. 15)

3.4.2 Zapisywanie wybranych dokumentów w zaszyfrowanym formacie

Po otwarciu dokumentu tekstowego, arkusza kalkulacyjnego lub prezentacji można zapisać dokument w formacie zaszyfrowanym.

Jak zapisać wybrany dokument w zaszyfrowanym formacie:

1. Otwórz dokument w aplikacji *Tekst*, *Arkusz* lub *Prezentacja*.
2. Na pasku narzędzi **Plik** kliknij pozycję **Zapisz w aplikacji Drive**. Wybierz opcję **Zapisz jako (zaszyfrowane)**.

   Pojawi się okno *Zapisz jako (zaszyfrowane)*. Wybierz folder i wpisz nazwę pliku. Kliknij przycisk **OK**.
3. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Strażnik* . Wpisz hasło zabezpieczające aplikacji Strażnik.

   Można ustawić długość pamiętania hasła przez aplikację Strażnik. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.

   Kliknij przycisk **OK**.

Zobacz też

Tworzenie nowych zaszyfrowanych plików (p. 19)
Otwieranie zaszyfrowanego dokumentu (p. 20)
Szyfrowanie plików (p. 15)

3.4.3 Otwieranie zaszyfrowanego dokumentu

Aby otworzyć zaszyfrowany dokument, wykonaj jedną z następujących czynności:

- odczytanie lub edycja dokumentu
- pobranie dokumentu w zaszyfrowanym formacie
- wydrukowanie dokumentu w formacie odszyfrowanego pliku pdf

Dokument na serwerze pozostaje zaszyfrowany.

Jak otworzyć zaszyfrowany dokument:

1. Otwórz dokument w aplikacji *Tekst*, *Arkusz* lub *Prezentacja*.
2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Strażnik* . Wpisz hasło zabezpieczające aplikacji Strażnik.

   Można ustawić długość pamiętania hasła przez aplikację Strażnik. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   W ustawieniach szyfrowania PGP możesz zdefiniować wartość domyślną zakresu czasu.

   Kliknij przycisk **OK**.
3. Możesz skorzystać z następujących funkcji:
   - Edycja dokumentu. Informacje na ten temat można znaleźć w podręczniku użytkownika aplikacji *Documents* .
   - Aby pobrać dokument w odszyfrowanym formacie, kliknij na pasku narzędzi polecenie **Pobierz** .
   - Aby zapisać dokument w formacie pdf w formacie odszyfrowanym, kliknij ikonę **Zapisz jako PDF** .

Zobacz też

Tworzenie nowych zaszyfrowanych plików (p. 19)
Zapisywanie wybranych dokumentów w zaszyfrowanym formacie (p. 19)
Szyfrowanie plików (p. 15)

3.5 Wyloguj się z aplikacji Strażnik

Z aplikacji Strażnik możesz się wylogować bez zamykania oprogramowania do pracy grupowej. Aby potem otworzyć zaszyfrowane wiadomości e-mail, pliki lub foldery, musisz ponownie wpisać hasło zabezpieczające aplikacji Strażnik.
Uwaga: Ta funkcja jest dostępna wyłącznie po włączeniu funkcji **Pamiętaj hasło** przy otwieraniu zaszyfrowanej wiadomości e-mail lub zaszyfrowanego pliku.

Jak się wylogować z aplikacji Strażnik:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu.
2. Wybierz z menu polecenie **Wyloguj się z aplikacji Strażnik**

3.6 Ustawienia aplikacji Strażnik

Dostępne są następujące możliwości:

- Aby zmienić ustawienia hasła zabezpieczającego aplikacji Strażnik, użyj opcji Ustawienia zabezpieczeń aplikacji Strażnik.
- Aby zmienić domyślne ustawienia wysyłania zabezpieczonych wiadomości e-mail, użyj opcji Ustawienia szyfrowania PGP.
- Możesz także wykonać czynności administracyjne dla kluczy PGP.

3.6.1 ustawienia zabezpieczeń aplikacji Strażnik

Dostępne są następujące możliwości:

- zmiana hasła zabezpieczającego aplikacji Strażnik
- Jeśli zapomnisz hasła aplikacji Strażnik, możesz poprosić przesłanie tymczasowego hasła zabezpieczającego aplikacji Strażnik, resetując hasło zabezpieczające aplikacji Strażnik.
- Zmiana zapasowego adresu e-mail.

Jak zmienić hasło zabezpieczające aplikacji Strażnik

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Strażnik Zabezpieczenia**.
3. W polu **Wprowadź bieżące hasło zabezpieczające aplikacji Strażnik** widocznym poniżej pola *Hasło* wpisz hasło, które do tej pory było używane do szyfrowania danych.

   W polu **Wprowadź nowe hasło zabezpieczające aplikacji Strażnik** wpisz hasło, którego od teraz chcesz używać do szyfrowania danych.

   Potwierdź nowe hasło, wpisując je ponownie do pola **Potwierdź nowe hasło zabezpieczające aplikacji Strażnik**.
4. Kliknij polecenie **Zmień hasło zabezpieczające aplikacji Strażnik**.

Jak zresetować hasło zabezpieczające aplikacji Strażnik:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Strażnik Zabezpieczenia**.
3. Kliknij polecenie **Zresetuj hasło zabezpieczające aplikacji Strażnik**. Na wpisany dodatkowy adres e-mail zostanie wysłane nowe hasło.

   Jeśli nie został wprowadzony zapasowy adres e-mail, nowe hasło zostanie wysłane na podstawowy adres e-mail.
4. Nowe hasło od razu zostanie bieżącym hasłem zabezpieczającym aplikacji Strażnik. Należy je natychmiast zmienić.

Jak zmienić zapasowy adres e-mail na potrzeby resetowania hasła do szyfrowania:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Strażnik Zabezpieczenia**.
3. Wpisz hasło służące do szyfrowania danych do pola **Wprowadź bieżące hasło zabezpieczające aplikacji Strażnik** widocznego poniżej pola *Dodatkowy adres e-mail*

   W polu **Wpisz nowy dodatkowy adres e-mail** wpisz adres, na który otrzymasz hasło tymczasowe pozwalające na zresetowanie hasła zabezpieczającego aplikacji Strażnik.

   Kliknij polecenie **Zmień adres e-mail**.

Zobacz też

Ustawienia szyfrowania PGP (p. 23)
Zarządzanie kluczami (p. 25)

3.6.2 Ustawienia szyfrowania PGP

Ustawienia szyfrowania PGP określają gotowe ustawienia wprowadzane podczas tworzenia wiadomości e-mail. Możesz je zmienić przed wysłaniem wiadomości.

Jak zmienić ustawienia szyfrowania PGP:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Zabezpieczenia aplikacji Strażnik**. Kliknij pozycję **Ustawienia zaawansowane**.
3. Wybierz jedną z opcji pod nagłówkiem *Ustawienia szyfrowania PGP*.

Dostępne są następujące ustawienia.

Zapamiętaj ustawienia domyślne hasła

Określa domyślny zakres czasowy pamiętania hasła do aplikacji Strażnik. Możesz zmienić to ustawienie domyślne, gdy pojawi się monit w aplikacji Strażnik.

Domyślnie podczas tworzenia wiadomości do wysłania w formie zaszyfrowanej

Umożliwia określenie, czy nowa wiadomość e-mail ma być domyślnie szyfrowana za pomocą PGP.

Domyślne dodawanie podpisu do wychodzących wiadomości e-mail

Umożliwia określenie, czy nowa wiadomość e-mail ma być domyślnie szyfrowana za pomocą PGP.

Włącz zaawansowane funkcje PGP

Określa, czy widoczne mają być wszystkie funkcje PGP.

Szyfruj wszystkie wiadomości przychodzące

Umożliwia określenie, czy domyślnie za pomocą PGP szyfrowane mają być wszystkie odbierane wiadomości.

Ustaw domyślnie w nowych wiadomościach PGP w tekście

Wskazuje, że szyfrowanie PGP ma być realizowane w tekście. Użyj tej opcji, jeśli wiadomość powinna być czytelna mimo tego, że klient e-mail odbiorcy nie obsługuje szyfrowania PGP. Po włączeniu tego ustawienia nie będzie możliwe wysyłanie wiadomości e-mail w formacie HTML.

Zobacz też

ustawienia zabezpieczeń aplikacji Strażnik (p. 23)
Zarządzanie kluczami (p. 25)

3.6.3 Zarządzanie kluczami

Do wysyłania i otrzymywania zaszyfrowanych wiadomości funkcje zarządzania kluczami przeważnie nie są potrzebne. Można ich użyć do następujących zadań:

- Chcesz użyć klucza PGP z aplikacji Strażnik w innych klientach e-mail, np. uruchamianych lokalnie.
- Masz klucze PGP z innych aplikacji. Chcesz ich użyć w aplikacji Strażnik.
- Chcesz wprowadzić klucz publiczny partnera zewnętrznego do aplikacji Strażnik, aby móc odczytywać zaszyfrowane wiadomości od niego.
- Chcesz przekazać klucz publiczny adresatowi, aby umożliwić mu odczytywanie Twoich zaszyfrowanych wiadomości bez uzyskiwania dostępu do serwera kluczy.

Jak otworzyć stronę do zarządzania kluczami:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Zabezpieczenia aplikacji Strażnik**. Kliknij pozycję **Ustawienia zaawansowane**.

   Włącz opcję **Włącz zaawansowane funkcje PGP**

Strona zawiera niżej wymienione elementy.

- Opcje pozwalające na dopasowywanie domyślnych ustawień aplikacji Strażnik.
- Sekcja *Twoje klucze* zawierająca funkcje do zarządzania prywatnymi i publicznymi kluczami PGP. Istniejące klucze zostaną wyświetlone poniżej pozycji *Lista Twoich kluczy*. Znajdują się na niej dwie pozycje:
  - Klucz główny służący między innymi do szyfrowania wiadomości e-mail.
  - Klucz zależny służący do szyfrowania i odszyfrowywania wiadomości e-mail oraz plików.

  Różnica między kluczem głównym i zależnym polega na jednej z funkcji technologii PGP. Każdy klucz główny i zależny zawiera klucz prywatny i publiczny. Przy odpowiedniej konfiguracji program Strażnik użyje automatycznie odpowiedniego klucza.
- Sekcja *Klucze publiczne* zawierające klucze publiczne współużytkowane przez Ciebie lub innych użytkowników. Jeśli na liście znajduje się klucz publiczny użytkownika, możesz założyć, że może on odszyfrowywać wiadomości e-mail.
- Klucze, które wygasły, są wyświetlane na czerwono.

Dostępne są następujące funkcje:

- Pobranie klucza publicznego
- Wysłanie klucza publicznego pocztą e-mail
- dodawanie nowych kluczy do istniejących przez przesłanie kluczy lokalnych lub utworzenie nowych kluczy w aplikacji Strażnik
- Zmiana klucza w klucz bieżący
- Pokazanie szczegółów klucza
- Usunięcie klucza
- Pobranie klucza prywatnego
- Dodanie kolejnego konta e-mail do klucza
- Przesłanie klucza publicznego partnera zewnętrznego

Jak pobrać klucz publiczny:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij polecenie **Pobierz klucz publiczny PGP** dostępne pod pozycją *Twoje klucze*.

Jak wysłać klucz publiczny pocztą e-mail:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij przycisk **Wyślij e-mailem swój klucz publiczny PGP** widoczny pod pozycją *Twoje klucze*.

Jak dodać nowe klucze:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Dodaj** + widoczną obok elementu *Lista Twoich kluczy* w sekcji *Twoje klucze*. Pojawi się okno *Dodawanie kluczy*.
3. Dostępne są następujące możliwości:
   - Aby dodać klucz prywatny, kliknij przycisk **Prześlij prywatny klucz**. Wybierz plik z kluczem prywatnym. Pojawi się okno *Prześlij prywatne klucze*.
     Aby przesłać nowy klucz, wpisz hasło zabezpieczające aplikacji Strażnik. Wpisz nowe hasło do nowego klucza.
   - Aby dodać klucz publiczny, kliknij przycisk **Prześlij tylko klucz publiczny**. Wybierz plik z kluczem publicznym.
   - Aby utworzyć nową parę kluczy, kliknij polecenie **Utwórz nowe klucze**. Pojawi się okno *Utwórz nowe klucze aplikacji Strażnik*.
     Wpisz hasło do nowego klucza i potwierdź je.
     Nowy klucz składa się z klucza głównego i odpowiedniego klucza zależnego.

   Nowy klucz zostanie umieszczony na górze listy kluczy i stanie się automatycznie kluczem bieżącym.

Jak ustawić klucz jako bieżący:

Możesz użyć tej funkcji, jeśli lista kluczy ma zawierać więcej niż jeden klucz główny i zależny. Od teraz szyfrowanie będzie realizowane za pomocą klucza bieżącego.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij pole wyboru poniżej *Listy Twoich kluczy* z opisem **Bieżący**. Po ustawieniu klucza głównego jako bieżącego odpowiedni klucz zależny zostanie także ustawiony jako bieżący — i na odwrót.

Jak wyświetlić szczegóły klucza:

Istnieje możliwość wyświetlenia szczegółów klucza. To szczególnie przydatne dla użytkowników rozumiejących technologię PGP.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Szczegóły** 🔍. Otworzy się okno *Szczegóły klucza*. Aby wyświetlić podpisy danego klucza, kliknij pozycję **Podpisy**.

Jak usunąć klucz:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Usuń** 🗑. Pojawi się okno *Usuń klucz prywatny*.
3. Dostępne są następujące opcje:
   - Aby wycofać klucz prywatny, kliknij polecenie **Odwołaj**.
     Wpisz hasło do klucza prywatnego i ewentualnie wybierz powód odwołania klucza.
     Kliknij polecenie **Odwołaj**.
   - Aby usunąć klucz prywatny, kliknij polecenie **Usuń**.
     Wpisz hasło do klucza prywatnego.
     Kliknij polecenie **Usuń**.

   Po usunięciu klucza głównego zostanie także usunięty odpowiedni klucz zależny.

Jak pobrać klucz prywatny:

Uwaga: Pobranie klucza prywatnego na komputer lokalny może stanowić zagrożenie bezpieczeństwa. Pamiętaj, aby zadbać o prywatność klucza prywatnego.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Pobierz** widoczną obok klucza na liście kluczy prywatnych w sekcji *Twoje klucze*.

Jak dodać kolejne konto e-mail do klucza:

Przy dodawaniu kolejnych identyfikatorów użytkownika do klucza możesz go wprowadzić do wielu kont e-mail.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Edytuj** . Otworzy się okno *Dodaj ID użytkownika*.
3. Wpisz nazwę identyfikatora użytkownika i adres e-mail, którego chcesz użyć w tym kluczu.
   Wpisz hasło do danego klucza.
   Kliknij przycisk **OK**.

Jak przesłać klucz publiczny partnera zewnętrznego:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Dodaj** widoczną obok +. Wybierz plik z kluczem publicznym.

Zobacz też

ustawienia zabezpieczeń aplikacji Strażnik (p. 23)
Ustawienia szyfrowania PGP (p. 23)

Indeks

D

Dokumentacja, 5

O

odszyfrowywanie plików, 17
Otwieranie zaszyfrowanych dokumentów, 20
otwieranie zaszyfrowanych plików, 16

P

pobieranie zaszyfrowanych plików, 17

R

resetowanie hasła, 23

S

Strażnik, 7, 9
  konfiguracja, 10
  ustawienia, 22
  Ustawienia szyfrowania PGP, 23
  ustawienia zabezpieczeń, 23
  wyloguj, 21
  zarządzanie kluczami, 25
szyfrowanie
  konwersacja e-mail, 11
  Pliki, 15
  szyfrowanie dokumentów pakietu Office, 18
  tworzenie nowych zaszyfrowanych plików, 19
  utwórz nowy zaszyfrowany plik, 16
  Zapisywanie wybranych dokumentów w zaszyfrowanym formacie, 19
Szyfrowanie dokumentów pakietu Office, 18
szyfrowanie konwersacji e-mail, 11
szyfrowanie plików, 15

T

tworzenie nowych zaszyfrowanych plików, 16
Tworzenie nowych zaszyfrowanych plików, 19

U

Ustawienia aplikacji Strażnik
  resetowanie hasła, 23
  zmiana hasła, 23
Ustawienia PGP w aplikacji Strażnik
  Domyślne dodawanie podpisu do wychodzących wiadomości e-mail, 24
  Domyślnie podczas tworzenia wiadomości do wysłania w formie zaszyfrowanej, 24
  Szyfruj wszystkie wiadomości przychodzące, 24
  Ustaw domyślnie w nowych wiadomościach PGP w tekście, 24
  Włącz zaawansowane funkcje PGP, 24
  Zapamiętaj ustawienia domyślne hasła, 24

W

Wyloguj
  zmiana hasła, 21

Z

Zapisywanie wybranych dokumentów w zaszyfrowanym formacie, 19
Zaszyfrowane dokumenty
  otwieranie, 20
zaszyfrowane pliki
  odszyfrowywanie, 17
  otwieranie, 16
  pobierz, 17
zaszyfrowane wiadomości e-mail
  blokowanie, 12
  czytanie, 11
  dostęp dla adresatów zewnętrznych, 14
  szyfrowanie przychodzących, 12
  wysyłanie, 12
Zmień hasło, 23