



Guard

podręcznik użytkownika

Guard: podręcznik użytkownika

data wydania środa, 23. marzec 2016 Version 2.4.0

Copyright © 2016-2016 OX Software GmbH , Niniejszy dokument stanowi własność intelektualną firmy OX Software GmbH

Niniejszy dokument może być kopiowany w całości lub części pod warunkiem umieszczenia w każdej kopii niniejszej informacji o prawach autorskich. Informacje zawarte w tym podręczniku zostały zebrane z zachowaniem najwyższej staranności. Nie jest jednak możliwe całkowite wykluczenie błędów. Firma OX Software GmbH, autorzy i tłumacze nie odpowiadają za ewentualne błędy i ich konsekwencje. Używane w niniejszym podręczniku nazwy programów i urządzeń mogą być zastrzeżonymi znakami towarowymi i są wykorzystywane bez udzielania gwarancji możliwości ich darmowego wykorzystywania. Firma OX Software GmbH z reguły przestrzega zasad pisowni ustalonych przez producentów. Reprodukacja nazw marek, nazw handlowych, logo itd. w niniejszym podręczniku (nawet bez specjalnego oznaczenia) nie oznacza, że te nazwy mogą zostać uznane za darmowe (w rozumieniu prawa dotyczącego znaków towarowych i nazw marek).

Spis treści

1	Informacje o tej dokumentacji	5
2	Do czego służy aplikacja Guard?	7
3	Korzystanie z aplikacji Guard	9
3.1	Konfiguracja aplikacji <i>Guard</i>	10
3.2	Szyfrowanie konwersacji e-mail	11
3.2.1	Odczytywanie zaszyfrowanych konwersacji e-mail	11
3.2.2	Wysyłanie zaszyfrowanych wiadomości e-mail	11
3.2.3	Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail?	12
3.3	Szyfrowanie plików	13
3.3.1	Szyfrowanie plików	13
3.3.2	Tworzenie nowych zaszyfrowanych plików	13
3.3.3	Otwieranie zaszyfrowanych plików	13
3.3.4	Pobieranie zaszyfrowanych plików	14
3.3.5	Odszyfrowywanie plików	14
3.4	Wylogowywanie się z aplikacji Guard	15
3.5	Ustawienia aplikacji Guard	16
3.5.1	Ustawienia zabezpieczeń aplikacji Guard	16
3.5.2	Ustawienia domyślne aplikacji Guard	17
3.5.3	Zarządzanie kluczami	18
Indeks	21

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 Guard?* znajduje się opis aplikacji Guard.
 - . W sekcji *Korzystanie z aplikacji Guard* znajdują się informacje dotyczące usługi Guard
- . 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 Guard?

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

- Szyfruj korespondencję e-mail prowadzoną z innymi użytkownikami lub partnerami zewnętrznymi.
- Zszyfruj 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 Guard

Dowiedz się, jak pracować z aplikacją *Guard*.

- [Stosowanie](#) ustawień podstawowych
- Szyfrowanie [korespondencji e-mail](#)
- Szyfrowanie [plików](#)
- [Stosowanie](#) ustawień zabezpieczeń

3.1 Konfiguracja aplikacji *Guard*


Przed użyciem aplikacji *Guard* trzeba skonfigurować kilka ustawień podstawowych.

- Przed wszystkim należy wprowadzić hasło aplikacji Guard Security służące do szyfrowania danych oraz uzyskiwania dostępu do nich.
- Wpisz zapasowy adres e-mail, który będzie przydatny w sytuacji, gdy zapomnisz hasła aplikacji Guard Security. Pozwoli to na użycie funkcji jego resetowania i wysłanie do Ciebie nowego hasła. Z powodów bezpieczeństwa zdecydowanie zalecamy skonfigurowanie tej funkcji. W przeciwnym razie nowe hasło zostanie wysłane na główne konto e-mail.


Istnieją dwa sposoby wprowadzania ustawień podstawowych:

- 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. Pojawi się monit o wpisanie hasła aplikacji Guard Security oraz zapasowego adres e-mail. Wpisz odpowiednie dane.

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 pozycję **Guard Security** na pasku bocznym.
W przypadku wybrania ustawień aplikacji Guard Security po raz pierwszy pojawi się okno *Utwórz klucze aplikacji Guard Security*.
3. W polu **Hasło** wprowadź hasło, którego chcesz używać do szyfrowania danych.
Potwierdź hasło, wprowadzając je ponownie w polu **Zweryfikuj**.
4. W polu **Wprowadź nowy zapasowy adres e-mail** wprowadź adres e-mail umożliwiający odebranie hasła tymczasowego podczas resetowania hasła aplikacji Guard Security.
5. Kliknij przycisk **OK**.

3.2 Szyfrowanie konwersacji e-mail


Dostępne są następujące możliwości:

- [Odczytywanie zaszyfrowanych konwersacji 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 przeczytać zaszyfrowaną wiadomość e-mail, trzeba znać co najmniej hasło aplikacji Guard Security. Nadawca zaszyfrowanej wiadomości e-mail może ją zabezpieczyć dodatkowym 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 podczas ostatniego używania aplikacji Guard zostało skonfigurowane zapamiętanie hasła zabezpieczeń przez tę aplikację, wiadomość e-mail zostanie wyświetlona od razu, zależnie od tego ustawienia.
2. Wprowadź hasło aplikacji Guard Security.
Można ustawić długość pamiętania hasła. Aby to zrobić, wybierz opcję **Nie wylogowuj mnie z aplikacji Guard**. Wybierz z listy odpowiednią wartość.
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.

3.2.2 Wysyłanie zaszyfrowanych wiadomości e-mail

Dostępne są następujące możliwości:

- Wysyłanie zaszyfrowanych wiadomości e-mail. Treść wiadomości e-mail będzie dostępna tylko dla nadawcy i adresata 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 e-mail* kliknij widoczną z prawej strony u góry ikonę **Zaszyfruj** .
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 wysłać wiadomości e-mail w formacie HTML.
3. Kliknij pozycję **Wyślij bezpieczną**.
W przypadku wysyłania wiadomości do adresatów zewnętrznych pojawi się okno umożliwiające wysłanie im [uwag dotyczących otwarcia zaszyfrowanej wiadomości e-mail \[12\]](#).
Odbiorca zaszyfrowanej wiadomości e-mail, z którym wcześniej nie prowadzono korespondencji, otrzyma załącznik z Twoim kluczem publicznym.

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

Zaszyfrowane wiadomości e-mail można także wysłać 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 zostaną wysłane wiadomości z kilkoma informacjami, automatycznie wygenerowanym hasłem i odnośnikiem do strony logowania na konto gościa. Po wpisaniu otrzymanego hasła automatycznego będzie możliwe wprowadzenie własnego hasła.
 - 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 `encrypted.asc`. Taki załącznik można przesłać na stronę konta gościa, odszyfrować i odczytać.

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.

3.3.2 Tworzenie nowych zaszyfrowanych plików

Nowy zaszyfrowany plik możesz utworzyć, przysyłając 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. W oknie *Prześlij plik* wybierz dowolną liczbę plików.
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.

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. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security. Można ustawić długość pamiętania hasła. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość. Kliknij przycisk **OK**.

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 zamiast tego w wyskakującym okienku klikniesz polecenie **Pobierz**, pobrany plik pozostanie zaszyfrowany.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security. Można ustawić długość pamiętania hasła. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość. Kliknij przycisk **OK**.
3. Kliknij ikonę **Działania**  w przeglądarce. Kliknij polecenie **Pobierz odszyfrowane**.

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. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security. Można ustawić długość pamiętania hasła aplikacji Guard Security. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość. Kliknij przycisk **OK**.

3.4 Wylogowywanie się z aplikacji Guard

Z aplikacji Guard możesz się wylogować bez zamykania oprogramowania do pracy grupowej. Aby potem otworzyć zaszyfrowane wiadomości e-mail, pliki lub foldery, musisz ponownie wpisać hasło aplikacji Guard Security.

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 Guard Security:

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

3.5 Ustawienia aplikacji Guard

Dostępne są następujące możliwości:


- Aby zmienić ustawienia hasła aplikacji Guard Security, użyj opcji [Ustawienia zabezpieczeń aplikacji Guard](#).
- Aby zmienić domyślne ustawienia wysyłania zabezpieczonych wiadomości e-mail, użyj opcji [Ustawienia domyślne aplikacji Guard](#).
- Możesz także wykonać czynności [administracyjne dla kluczy PGP](#).

3.5.1 Ustawienia zabezpieczeń aplikacji Guard


Dostępne są następujące możliwości:

- [Zmiana](#) hasła aplikacji Guard Security.
- Jeśli zapomnisz hasła aplikacji Guard Security, możesz je [zresetować](#), żądając wysłania hasła tymczasowego na dodatkowy adres e-mail.
- [Zmiana](#) zapasowego adresu e-mail.


Jak zmienić hasło aplikacji Guard Security:

1. Kliknij ikonę **menu systemowego**  widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij pozycję **Guard Security** na pasku bocznym.
3. W polu **Wprowadź bieżące hasło aplikacji Guard Security** w obszarze *Hasło* wprowadź hasło służące dotychczas do szyfrowania danych.
W polu **Wprowadź nowe hasło aplikacji Guard Security** wprowadź hasło, którego chcesz używać do szyfrowania danych od tej pory.
Potwierdź hasło, wprowadzając je ponownie w polu **Zweryfikuj nowe hasło aplikacji Guard Security**.
4. Kliknij pozycję **Zmień hasło aplikacji Guard Security**.

Jak zresetować hasło aplikacji Guard Security:

1. Kliknij ikonę **menu systemowego**  widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij pozycję **Guard Security** na pasku bocznym.
3. Kliknij pozycję **Zresetuj hasło aplikacji Guard Security**. Na Twój zapasowy 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 aplikacji Guard Security. 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 pozycję **Guard Security** na pasku bocznym.
3. W polu **Wprowadź bieżące hasło aplikacji Guard Security** w obszarze *Zapasowy adres e-mail* wprowadź hasło służące do szyfrowania danych.
W polu **Wprowadź nowy zapasowy adres e-mail** wprowadź adres e-mail umożliwiający odebranie hasła tymczasowego podczas resetowania hasła aplikacji Guard Security.
Kliknij polecenie **Zmień adres e-mail**.

3.5.2 Ustawienia domyślne aplikacji Guard

Ustawienia domyślne oznaczają gotowe ustawienia wprowadzane podczas tworzenia wiadomości e-mail. Możesz je zmienić przed wysłaniem wiadomości.

Jak zmienić ustawienia domyślne:

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

Dostępne są następujące ustawienia.

Domyślnie podczas tworzenia wiadomości do wysłania w formie zaszyfrowanej

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

Domyślne dodawanie podpisu do wychodzących wiadomości e-mail

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

Domyślne ustawienie PGP zapewniające użycie PGP Inline ze względu na zgodność


Umożliwia określenie, 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.

3.5.3 Zarządzanie kluczami

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

- Chcesz użyć kluczy PGP aplikacji Guard w innych klientach poczty e-mail, np. lokalnych.
- Masz klucze PGP z innych aplikacji PGP i chcesz je wprowadzić do aplikacji Guard.
- Chcesz wprowadzić klucz publiczny partnera zewnętrznego do aplikacji Guard, aby 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. Wybierz pozycję **Guard Security** na pasku bocznym. Kliknij pozycję **Ustawienia PGP aplikacji Guard**.

Strona zawiera niżej wymienione elementy.

- Opcje pozwalające na dopasowywanie [domyślnych ustawień aplikacji Guard](#)
- 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 Guard 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.

Dostępne są następujące funkcje:

- [Pobranie](#) klucza publicznego
- [Wysłanie klucza publicznego pocztą e-mail](#)
- [Dodanie nowych kluczy](#) do istniejących przez przesłanie kluczy lokalnych lub utworzenie nowych kluczy w aplikacji Guard
- [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 +**. 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 aplikacji Guard Security. 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 klucze aplikacji Guard Security*.
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**  obok klucza na *Liście Twoich kluczy*. 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**  na *Liście Twoich kluczy* obok elementu *Twoje klucze*. 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. Dopilnuj, aby nikt inny nie miał do niego dostępu.

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**  widoczną *Listy Twoich kluczy* poniżej elementu *Twoje klucze*. Pojawi 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 **+** polecenia *Lista kluczy publicznych PGP* poniżej sekcji *Klucze publiczne*. Wybierz plik z kluczem publicznym.

Indeks

D

Dokumentacja, 5

G

Guard, 7, 9

- konfiguracja, 10
- ustawienia, 16
- ustawienia domyślne, 17
- ustawienia zabezpieczeń, 16
- wylogowywanie się, 15
- zarządzanie kluczami, 18

O

odszyfrowywanie plików, 14
otwieranie zaszyfrowanych plików, 13

P

pobieranie zaszyfrowanych plików, 14

R

resetowanie hasła, 16

S

szyfrowanie

- konwersacja e-mail, 11
- pliki, 13
- tworzenie nowych zaszyfrowanych plików, 13

szyfrowanie konwersacji e-mail, 11
szyfrowanie plików, 13

T

tworzenie nowych zaszyfrowanych plików, 13

U

ustawienia aplikacji Guard

- resetowanie hasła, 16
- Zmiana hasła, 16

ustawienia PGP aplikacji Guard

- Domyślne dodawanie podpisu do wychodzących wiadomości e-mail, 17
- Domyślne ustawienie PGP zapewniające użycie PGP Inline ze względu na zgodność, 17
- Domyślnie podczas tworzenia wiadomości do wysłania w formie zaszyfrowanej, 17

W

wylogowywanie się

- Zmiana hasła, 15

Z

zaszyfrowane pliki

- odszyfrowywanie, 14

otwieranie, 13
pobieranie, 14
zaszyfrowane wiadomości e-mail

- blokowanie, 11
- czytanie, 11
- dostęp dla adresatów zewnętrznych, 12
- wysyłanie, 11

zmiana hasła, 16

