Guard

podręcznik użytkownika

Guard: podręcznik użytkownika

data wydania wtorek, 13. styczeń 2015 Version 1.2

Spis treści

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 OX App Suite.

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 innym użytkownikami lub partnerami zewnętrznymi.
- Encrypt single files. Share the encrypted data with other users.
- Określaj poziom szyfrowania za pomocą opcji zabezpieczeń.
- Wyznaczaj datę lub godzinę wygaśnięcia szyfrowanych danych.
- 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
- encrypt files
- Stosowanie ustawień zabezpieczeń

3.1 Konfiguracja aplikacji *Guard*

Prior to be able to use *Guard*, you have to apply some basic settings.

- First of all you have to enter a Guard security password that is used to encrypt data and to access encrypted data.
- Enter a secondary E-Mail address that is used if you forget your Guard security password. In this case, use the function for resetting the Guard security password. A new password will then be sent to you. For security reasons, it is highly recommended to enter a secondary E-Mail address for this purpose. Otherwise the new password is sent to your primary E-Mail account.

There are two options for making the basic settings:

- Define the basic settings while initially using an encryption function.
- Define the basic settings in the groupware settings page before using the encryption function.

How to define the basic settings when initially using an encryption function:

1. Enable the encryption function when composing an E-Mail, encrypting a file or uploading a new file by clicking on the **Encrypt** icon .
2. You consecutively will be asked to enter a Guard security password and a secondary E-Mail address. Enter the data.

How to define the basic settings before initially using an encryption:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Kliknij pozycję **Ustawienia aplikacji 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 korespondencji e-mail

Dostępne są następujące możliwości:

- Czytanie zaszyfrowanych wiadomości e-mail
- Wysyłanie zaszyfrowanych wiadomości e-mail
- Dostęp dla odbiorców zewnętrznych

3.2.1 Czytanie zaszyfrowanych wiadomości 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. Select an E-Mail with the *Encrypted* icon . In the detail view, the notification *Secure E-Mail, enter your Guard security password.* is displayed.
2. Wprowadź hasło aplikacji Guard Security.

   You can define how long the security password should be remembered. To do so, enable **Keep me logged into Guard**. Select a value from the list.

   Nadawca mógł zabezpieczyć wiadomość e-mail dodatkowym hasłem. W takim przypadku pojawi się jeszcze jedno pole wejściowe, w którym należy wprowadzić dodatkowe hasło.
3. Kliknij przycisk **OK**.

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:

- send an encrypted E-Mail

  Warning: When sending an encrypted E-Mail draft, the draft will be deleted when being sent from the *Drafts* folder.
- to increase the security level, you can use further functions
- retract a sent encrypted E-Mail by blocking it.

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 ikonę **Szyfruj** widoczną z prawej strony u góry.

   You can also click on **Security options** on the left. Activate **Enable Guard**.
2. Aby jeszcze bardziej zwiększyć bezpieczeństwo, możesz skorzystać z dodatkowych funkcji: ustawić datę lub godzinę wygaśnięcia, a także użyć dodatkowego hasła.
3. Kliknij pozycję **Wyślij bezpieczną**.

   W przypadku wysyłania wiadomości do odbiorców zewnętrznych pojawi się okno umożliwiające wysłanie im uwag dotyczących otwarcia zaszyfrowanej wiadomości e-mail [12].

Jak używać dodatkowych funkcji szyfrowania podczas wysyłania wiadomości e-mail:

Warunek: jest wybrana strona *Nowa wiadomość e-mail*.

1. Na stronie *Nowa wiadomość e-mail* kliknij pozycję **Opcje zabezpieczeń** widoczną z lewej strony.
2. Aby jeszcze bardziej wzmocnić ochronę szyfrowanej wiadomości e-mail dodatkowym hasłem, włącz opcję **Wymagaj dodatkowego hasła**. Pojawi się okno *Dodatkowe hasło*.

   Wprowadź dodatkowe hasło w polach **Hasło** i **Potwierdź**. Kliknij przycisk **OK**.
3. Aby określić datę wygaśnięcia widoczności zaszyfrowanej wiadomości e-mail, wybierz pozycję w polu **Wycofaj za**.

Jak zablokować zaszyfrowaną wiadomość e-mail:

1. Otwórz folder **Wysłane obiekty**. Wybierz wysłaną zaszyfrowaną wiadomość e-mail.
2. If being prompted for, enter the Guard security password.

   You can define how long the security password should be remembered. To do so, enable **Keep me logged into Guard**. Select a value from the list.

   Nadawca mógł zabezpieczyć wiadomość e-mail dodatkowym hasłem. W takim przypadku pojawi się jeszcze jedno pole wejściowe, w którym należy wprowadzić dodatkowe hasło.
3. Click the **More** icon ≡▾ in the detail view. Click the **Retract** menu item. The E-Mail can no longer be read by the recipients.

3.2.3 Dostęp dla odbiorców zewnętrznych

Zaszyfrowane wiadomości e-mail można też wysyłać do odbiorców zewnętrznych, którzy nie korzystają z oprogramowania do pracy grupowej. W takiej sytuacji:

- Automatycznie zostaje utworzone specjalne konto dla odbiorcy zewnętrznego.
- Określ, czy odbiorca zewnętrzny otrzyma automatycznie utworzone powiadomienie o zaszyfrowanej wiadomości e-mail czy powiadomienie niestandardowe.
- Odbiorca zewnętrzny otrzymuje wiadomość e-mail z powiadomieniem oraz automatycznie utworzonym hasłem.

  Depending on the groupware configuration, you can transfer a 4 digit pin to the recipient to secure the automatically created password.
- Odbiorca zewnętrzny otrzymuje wiadomość e-mail z łączem do strony umożliwiającej mu zalogowanie się na specjalnym koncie.
- Następnie odbiorca zewnętrzny musi wprowadzić swój adres e-mail oraz automatycznie utworzone hasło.
- Po pierwszym zalogowaniu się na tym koncie odbiorca zewnętrzny jest proszony o zmianę automatycznie utworzonego hasła. Jest wyświetlana zaszyfrowana wiadomość e-mail.
- Odbiorca zewnętrzny może wysłać zaszyfrowaną odpowiedź na tę wiadomość.

3.3 Szyfrowanie plików

Dostępne są następujące możliwości:

- Szyfrowanie plików
- Creating new encrypted files
- Opening encrypted files
- Downloading encrypted files
- Decrypting files

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. In the *Pliki* app, click on a file in the detail view. In the pop-up, click the **More** icon . Click on **Encrypt** in the menu.
   You can also select a file. Click the **More** icon in the toolbar. Click on **Encrypt** in the menu.
2. Pojawi się okno *Szyfruj pliki*. Potwierdź chęć zaszyfrowania pliku i usunięcia wszystkich starszych wersji, klikając przycisk **OK**.

3.3.2 Creating new encrypted files

You can create a new encrypted file by uploading a local file with encryption.

How to create a new encrypted file:

1. Open a folder in the folder tree.
   Note: Open a folder for which you have the appropriate permissions to create objects.
2. Click on **New** in the toolbar. Click on **Upload new file**.
3. In the *Upload new files* window, click on **Select file**. Select one or several files.
   Click the **Encrypt** icon on the upper right part.
4. You can enter file information in the *Description* field.
5. Click on **Encrypt** in the menu.

Tip: You can also create a new encrypted file by dragging a file from your operating system's desktop to the *Pliki* app window and drop it in the upper part.

3.3.3 Opening encrypted files

You can open and read an encrypted file. The file remains encrypted on the server.

Jak otworzyć zaszyfrowany plik:

1. In the *Pliki* app, click on a file in the detail view. In the pop-up, click on **Decrypt and Open**.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security.
   You can define how long the security password should be remembered. To do so, enable **Remember Password**. Select a value from the list.
   Kliknij przycisk **OK**.

3.3.4 Downloading encrypted files

You can download an encrypted file to locally read or edit it. The file remains encrypted on the server.

How to download an encrypted file:

1. In the *Pliki* app, click on a file in the detail view. In the pop-up, click the **More** icon . Click on **Download Decrypted**.
   Note: If you click on **Download** in the pop-up instead, the downloaded file remains encrypted.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security.
   Kliknij przycisk **OK**.

3.3.5 Decrypting files

You can remove a file's encryption by decrypting the file.

How to decrypt a file:

1. In the *Pliki* app, click on an encrypted file in the detail view. In the pop-up, click the **More** icon Click on **Remove Encryption** in the menu.
   You can also select a file. Click the **More** icon in the toolbar. Click on **Remove Encryption** in the menu.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security.
   You can define how long the Guard security password should be valid. To do so, enable **Remember Passwort**. Select a value from the list.
   Kliknij przycisk **OK**.

3.4 Wylogowywanie się z aplikacji Guard

You can sign out from Guard without closing the groupware. To open an encrypted E-Mail, file or folder afterwards, you again have to enter the Guard security password.
Note: This function is only available if you enable **Remember Password** when opening an encrypted E-Mail or file.

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 zabezpieczeń aplikacji Guard

Dostępne są następujące możliwości:

- customize the Guard default settings
- Zmiana hasła aplikacji Guard Security
- If you forgot your Guard security password, you can request a temporary Guard security password to be emailed to you by resetting the Guard security password.
- change the secondary E-Mail address

How to change the Guard default settings:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Kliknij pozycję **Ustawienia aplikacji Guard Security** na pasku bocznym.
3. Change a setting below *Defaults*.

The following settings are available.

Use Guard when composing a new email

Defines whether a new E-Mail is encrypted per default. Regardless of this preset option, you can define for each E-Mail whether it should be sent encrypted or decrypted.

Jak zmienić hasło aplikacji Guard Security:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij w menu pozycję **Ustawienia**.
2. Kliknij pozycję **Ustawienia aplikacji 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. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Kliknij pozycję **Ustawienia aplikacji Guard Security** na pasku bocznym.
3. Kliknij pozycję **Zresetuj hasło aplikacji Guard Security**. Na Twój zapasowy adres e-mail zostanie wysłane nowe hasło.

   If not having entered a secondary E-Mail address, the new password will be sent to your primary E-Mail address.
4. To nowe hasło będzie aktualnym hasłem aplikacji Guard Security. Należy je niezwłocznie zmienić.

How to change your secondary E-Mail address for resetting the encryption password:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Kliknij pozycję **Ustawienia aplikacji 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 pozycję **Zmień adres e-mail**.

Indeks