kaspersky

Kaspersky VPN for Mac

© 2022 AO Kaspersky Lab

Spis treści

Pomoc Kaspersky VPN

Omówienie Kaspersky VPN

Najczęściej zadawane pytania

- Wymagania sprzętowe i programowe
- Instalowanie i dezinstalowanie aplikacji
- Nawiązywanie połączenia z My Kaspersky
- Wersje Kaspersky VPN
- Aktualizowanie do wersji Unlimited
- Chroń swoje połączenie z niezabezpieczoną siecią Wi-Fi
- Dlaczego nie można otworzyć strony internetowej przy włączonym Kaspersky VPN?

Subskrypcja i konto

- Wersje Kaspersky VPN
- Aktualizowanie do wersji Unlimited
- Przywracanie subskrypcji
- Zmiana konta My Kaspersky
- Informacje o subskrypcji
- Informacje o anonimowych subskrypcjach

Podawanie informacji

- Informacje o przekazywanych danych
- Zgodność z prawem Unii Europejskiej
- Zawartość plików śledzenia, plików zrzutów i plików ustawień

Zacznij pracę z aplikacją

- Wymagania sprzętowe i programowe
- Instalowanie i dezinstalowanie aplikacji
- Uruchamianie aplikacji po raz pierwszy
- Nawiązywanie połączenia z My Kaspersky
- Informacje o weryfikacji dwuetapowej

Wykonywanie podstawowych zadań

- Aktywowanie połączenia VPN
- Wybieranie serwera VPN
- Wyświetlanie ilości wykorzystanego i dostępnego ruchu sieciowego
- W jaki sposób konfigurować Dzielone tunelowanie
- Chroń swoje dane, jeśli Twoje bezpieczne połączenie zostało utracone
- Konfigurowanie ustawień VPN dla znanych sieci Wi-Fi
- Włączanie i wyłączanie wysyłania danych w celach marketingowych
- Włączanie śledzenia
- Chroń swoje połączenie z niezabezpieczoną siecią Wi-Fi
- Wybieranie działania, jakie Kaspersky VPN wykona po nawiązaniu połączenia z niezabezpieczoną siecią Wi-Fi

W jaki sposób uzyskać obsługę klienta

Znane problemy

Źródła informacji o aplikacji

Informacje prawne

- Przeglądanie warunków Umowy licencyjnej i Oświadczenia marketingowego
- Informacje o kodzie firm trzecich
- Informacje o znakach towarowych

Pomoc Kaspersky VPN

Witamy w Kaspersky VPN

- Omówienie Kaspersky VPN

Rozpoczęcie pracy

- Wymagania sprzętowe i programowe
- Zainstaluj Kaspersky VPN
- Wstępna konfiguracja

Wykonywanie podstawowych zadań

- Aktywowanie połączenia VPN
- Wybieranie serwera VPN
- Chroń swoje dane, jeśli Twoje bezpieczne połączenie zostało utracone
- Konfigurowanie ustawień VPN dla znanych sieci Wi-Fi
- W jaki sposób konfigurować Dzielone tunelowanie

Ochrona danych osobowych

- Informacje o przekazywanych danych
- Zgodność z prawem Unii Europejskiej
- Zawartość plików śledzenia, plików zrzutów i plików ustawień

Należy skontaktować się z obsługą klienta

- W jaki sposób skontaktować się z obsługą klienta

Omówienie Kaspersky VPN

Kaspersky VPN Secure Connection (zwany dalej - Kaspersky VPN) ukrywa Twoją rzeczywistą lokalizację i szyfruje wszystkie dane wysyłane i odbierane przez komputer Mac. Kaspersky VPN można zainstalować na komputerach stacjonarnych, laptopach i urządzeniach mobilnych z systemem Microsoft® Windows®, macOS, Android™ lub iOS™. Możesz używać programu Kaspersky VPN do różnych typów połączeń sieciowych, na przykład: Wi-Fi, lokalnych połączeń internetowych lub połączeń z modemem USB.

Uwaga: Możesz znaleźć informacje o funkcjach i udoskonaleniach bieżącej i poprzedniej wersji aplikacji w sklepie App Store.

Nie udostępniaj swojej prywatności

Publiczne sieci Wi-Fi mogą być niewystarczająco chronione, na przykład, jeśli sieć Wi-Fi korzysta z podatnego na ataki protokołu szyfrowania. Kaspersky VPN ustanawia bezpieczne połączenie szyfrowane z odwiedzanymi stronami internetowymi, dzięki czemu żaden haker nie może przechwycić zaszyfrowanych danych.

Wybierz optymalną trasę do odwiedzanych stron internetowych

Podczas korzystania z programu Kaspersky VPN można wybrać serwer VPN i być widocznym w internecie jako użytkownik z innego kraju. Możesz też przeglądać treści bez względu na ograniczenia regionalne.

Zezwól Kaspersky VPN na automatyczną ochronę niezabezpieczonych połączeń

Możesz skonfigurować aplikację tak, aby VPN było włączane automatycznie podczas nawiązywania połączenia z niezabezpieczonymi sieciami Wi-Fi.

Zezwalanie Kaspersky VPN na automatyczną ochronę połączenia

Możesz skonfigurować aplikację tak, aby VPN było włączane automatycznie po uruchomieniu komputera Mac.

Chroń swoje dane, jeśli Twoje bezpieczne połączenie zostało utracone

Możesz użyć Kill Switch, aby skonfigurować aplikację do automatycznego całkowitego zerwania połączenia z internetem, gdy spada połączenie VPN.

Najczęściej zadawane pytania

Wymagania sprzętowe i programowe

Kaspersky VPN posiada następujące wymagania sprzętowe i programowe:

- 1 GB pamięci (RAM)
- 320 MB wolnego miejsca na dysku
- System operacyjny macOS 11-13
- Połączenie internetowe
- Typ procesora: Intel, Apple Silicon

Instalowanie i dezinstalowanie aplikacji

Kaspersky VPN może zostać zainstalowany z poziomu sklepu App Store.

W celu zainstalowania aplikacji:

1. Otwórz aplikację App Store.
2. Odszukaj Kaspersky VPN i zainstaluj aplikację.
   Aplikacja App Store może wyświetlić pytanie o wprowadzenie danych uwierzytelniających Apple ID.

> **Uwaga:** Więcej informacji dotyczących korzystania z App Store i instalowania aplikacji można znaleźć w odpowiednich podręcznikach użytkownika dla posiadanego komputera Mac.

W celu odinstalowania aplikacji:

1. Odszukaj aplikację w Finderze.
2. Otwórz menu skrótu i wybierz **Przenieś do Kosza**.

> **Uwaga:** Więcej informacji na temat odinstalowywania aplikacji można znaleźć w odpowiednich podręcznikach użytkownika dla komputera Mac.

Nawiązywanie połączenia z My Kaspersky

Jeśli otwierasz program Kaspersky VPN, możesz zalogować się do My Kaspersky z użyciem konta My Kaspersky. Jeśli korzystałeś z innej aplikacji Kaspersky, na przykład, Kaspersky VPN dla innego urządzenia lub Kaspersky Internet Security, prawdopodobnie masz już konto My Kaspersky. Użyj go do zalogowania się. Jeśli nie masz konta, możesz je utworzyć.

Uwaga: Jeśli zalogowałeś się do My Kaspersky w innej aplikacji Kaspersky na komputerze Mac, po zainstalowaniu, aplikacja Kaspersky VPN wyświetli pytanie o zalogowanie się do My Kaspersky przy użyciu tego samego konta.

Logowanie do My Kaspersky przy użyciu istniejącego konta

1. Otwórz okno główne aplikacji i kliknij **Zaloguj**.

   Zostanie otwarte okno **Zaloguj się do My Kaspersky**.

2. Wykonaj jedną z następujących czynności:

   - Jeśli chcesz nawiązać połączenie z My Kaspersky za pośrednictwem konta Google, Facebook lub Apple, kliknij odpowiedni przycisk i postępuj zgodnie z instrukcjami. Więcej informacji znajduje się na stronie systemu pomocy My Kaspersky. Jeśli nie masz jeszcze konta My Kaspersky, aplikacja wyświetli pytanie o zarejestrowanie się na stronie My Kaspersky.

     Uwaga: Dostępność opcji logowania za pośrednictwem Facebooka zależy od regionu.

   - Jeśli masz login i hasło do swojego konta My Kaspersky, wprowadź swoje dane uwierzytelniające i kliknij **Zaloguj**.

     Uwaga: Jeśli kilka razy w krótkim czasie wprowadzisz błędne hasło, konieczne będzie wprowadzenie znaków z obrazka, by przejść pomyślnie kontrolę bezpieczeństwa.

     Uwaga: Jeśli włączono weryfikację dwuetapową dla Twojego konta My Kaspersky, konieczne będzie wprowadzenie kodu otrzymanego przez wiadomość SMS lub wygenerowanego w aplikacji uwierzytelniającej.

   Zostanie otwarte okno dialogowe z Oświadczeniem dotyczącym przetwarzania danych w celach korzystania z portalu internetowego (Oświadczenie dotyczące portalu internetowego).

3. Wykonaj jedną z następujących czynności:

   - Jeśli nie akceptujesz Oświadczenia dotyczącego portalu internetowego, kliknij **Nie akceptuję**.

     Uwaga: Nie możesz zalogować się do My Kaspersky lub utworzyć konta My Kaspersky bez zaakceptowania Oświadczenia dotyczącego portalu internetowego.

   - Jeśli akceptujesz Oświadczenie dotyczące portalu internetowego, kliknij przycisk **Akceptuję**, aby kontynuować.

   Kaspersky VPN zaloguje Cię na konto My Kaspersky.

Tworzenie konta My Kaspersky z poziomu interfejsu aplikacji

1. W oknie **Zaloguj się do My Kaspersky** kliknij **Utwórz konto**.

   Zostanie otwarte okno **Utwórz konto My Kaspersky**.

   Uwaga: Jeśli wprowadzisz adres e-mail, który jest już używany, niepoprawny adres e-mail lub zbyt popularne hasło kilka razy w krótkim przedziale czasu, będziesz musiał wprowadzić znaki z obrazka, aby przejść kontrolę bezpieczeństwa.

2. W polu do wprowadzenia adresu e-mail wpisz adres e-mail, który chcesz skojarzyć z nowym kontem My Kaspersky.

3. W polu do wprowadzenia hasła wpisz hasło do swojego konta My Kaspersky.

   Uwaga: Hasło musi zawierać minimum osiem znaków, w tym przynajmniej jedną cyfrę, jedną małą literę oraz jedną dużą literę. Hasło nie może zawierać spacji.

4. W polu potwierdzenia hasła ponownie wpisz hasło.

5. W menu wyskakującym wyboru kraju wybierz kraj.

   Uwaga: Kaspersky VPN automatycznie wyświetla Twój kraj w oparciu o region ustawiony w ustawieniach systemowych Język & Region. Ta opcja określa ustawienia regionalne dla Twojego konta My Kaspersky, na przykład, język wyświetlania i dostępne aplikacje firmy Kaspersky. Będziesz mógł zmienić region dla swojego konta My Kaspersky w późniejszym czasie tylko poprzez skontaktowanie się z działem obsługi klienta.

6. Kliknij odnośnik **Polityka prywatności**, aby przeczytać Politykę prywatności, która opisuje zarządzanie danymi.

   Zostanie otwarte okno przeglądarki wyświetlające Politykę prywatności.

7. Jeśli wyrażasz zgodę na warunki Polityki prywatności, zaznacz pole **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki Polityki prywatności opisującej zasady przetwarzania danych**.

   Uwaga: Przycisk **Utwórz** stanie się dostępny tylko wtedy, gdy potwierdzisz, że przeczytałeś, rozumiesz i akceptujesz Politykę prywatności.

8. Jeśli wyrażasz zgodę na udostępnienie swojego adresu e-mail, aby otrzymywać wiadomości e-mail z informacjami i ofertami promocyjnymi, zaznacz pole **Wyrażam zgodę na udostępnienie firmie Kaspersky mojego adresu e-mail w celu otrzymywania spersonalizowanych ofert marketingowych**.

9. Kliknij **Utwórz**.

   Zostanie otwarte okno dialogowe z Oświadczeniem dotyczącym przetwarzania danych w celach korzystania z portalu internetowego (Oświadczenie dotyczące portalu internetowego).

10. Wykonaj jedną z następujących czynności:

    - Jeśli nie akceptujesz Oświadczenia dotyczącego portalu internetowego, kliknij **Nie akceptuję**.

Uwaga: Nie możesz zalogować się do My Kaspersky lub utworzyć konta My Kaspersky bez zaakceptowania Oświadczenia dotyczącego portalu internetowego.

- Jeśli akceptujesz Oświadczenie dotyczące portalu internetowego, kliknij przycisk **Akceptuję**, aby kontynuować.

Kaspersky VPN nawiąże połączenie z My Kaspersky i utworzy konto użytkownika. Po utworzeniu konta zostanie otwarte okno główne aplikacji, a na adres e-mail, określony podczas rejestracji, zostanie wysłana wiadomość z instrukcjami dotyczącymi aktywacji konta.

Ważne: Aby możliwe było nawiązanie połączenia z My Kaspersky, konieczny jest dostęp do Internetu.

Wersje Kaspersky VPN

Kaspersky VPN jest dostępny w wersjach: bezpłatna i Unlimited.

Wersja bezpłatna:

- Darmowa.
- Zawsze dostępna.
- Ograniczona ilość bezpiecznego ruchu sieciowego na dzień.
- Nie możesz wybrać serwera VPN. Jest wybierana automatycznie.

Możesz przełączyć się z wersji bezpłatnej do wersji Unlimited, kupując subskrypcję.

Wersja Unlimited:

- Nieograniczony ruch sieciowy.
- Możesz wybrać serwer VPN.
- Kill Switch.
- Dostępna poprzez subskrypcję.
- Aplikacja może być zainstalowana na kilku urządzeniach (Mac, mobilne, tablet, PC) w obrębie jednej subskrypcji.

Więcej informacji na temat wersji Kaspersky VPN można znaleźć na stronie My Kaspersky.

Uwaga: Podczas korzystania z wersji Unlimited programu Kaspersky VPN aplikacja może powiadomić o dostępności innej subskrypcji. To powiadomienie pojawia się tylko wtedy, gdy odnaleziona subskrypcja dotyczy mniejszej liczby urządzeń niż bieżąca subskrypcja. Jeśli przejdziesz na tę subskrypcję, Kaspersky VPN zainstalowany na niektórych Twoich urządzeniach przełączy się do wersji bezpłatnej.

Aktualizowanie do wersji Unlimited

Jeśli potrzebujesz nieograniczonego zabezpieczonego ruchu sieciowego oraz chcesz wolnego wyboru serwerów VPN, możesz zaktualizować wersję Unlimited programu Kaspersky VPN. Jeśli korzystasz już z wersji Unlimited, a Twoja subskrypcja utraciła ważność lub rozpoczął się okres karencji, możesz ją odnowić.

Kup/odnów subskrypcję

1. Na zakładce ruchu sieciowego lub subskrypcji okna głównego aplikacji kliknij **Rozszerz** lub **Szczegóły**.

   Zostanie otwarte okno z bieżącym stanem subskrypcji.

2. Aby kupić lub odnowić subskrypcję, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

   Uwaga: Jeśli nie jesteś podłączony do My Kaspersky, Kaspersky VPN wyświetli Oświadczenie dotyczące przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie o zakupie) przed zakupem subskrypcji. Pamiętaj, że kupując subskrypcję, potwierdzasz, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Oświadczenie o zakupie.

Subskrypcję dla Kaspersky VPN możesz kupić także na stronie My Kaspersky lub na stronie internetowej Kaspersky:

- Jeśli kupisz subskrypcję na stronie My Kaspersky, subskrypcja zostanie aktywowana automatycznie po sfinalizowaniu zakupu.
- Jeśli kupisz subskrypcję na stronie internetowej Kaspersky, otrzymasz kod aktywacyjny w wiadomości e-mail wysłanej na podany adres e-mail. Aby aktywować subskrypcję, musisz dodać kod aktywacyjny do swojego konta My Kaspersky i podłączyć Kaspersky VPN do My Kaspersky. Więcej informacji na temat ręcznego dodawania kodu aktywacyjnego do swojego konta My Kaspersky można znaleźć w pomocy My Kaspersky.

Note: To learn about VPN availability in Russia, please read this article.

Chroń swoje połączenie z niezabezpieczoną siecią Wi-Fi

Podczas nawiązywania połączenia z dowolną siecią Wi-Fi, Kaspersky VPN sprawdza stan sieci Wi-Fi zgodnie z danymi z Kaspersky Security Network i inne kryteria, takie jak, czy używany jest protokół szyfrowania podatny na ataki lub popularna nazwa sieci (SSID). Korzystając z tych informacji, Kaspersky VPN określa, czy sieć Wi-Fi jest bezpieczna.

Jeśli już nawiązałeś połączenie z niezabezpieczoną siecią Wi-Fi, możesz chronić swoje połączenie przy użyciu Kaspersky VPN.

Chroń swoje połączenie z niezabezpieczoną siecią Wi-Fi

1. W oknie głównym aplikacji włącz VPN.
2. W otwartym oknie powiadomienia kliknij **Tak, włącz**, jeśli chcesz, żeby Kaspersky VPN włączał VPN automatycznie podczas nawiązywania połączenia z niezabezpieczoną siecią Wi-Fi.

Włącz wykrywanie niezabezpieczonych sieci Wi-Fi przy użyciu Kaspersky Security Network

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.
2. W zakładce **Niezabezpieczona sieć Wi-Fi** zaznacz pole **Włącz wykrywanie w chmurze za pomocą Kaspersky Security Network**.

   If you don't have Location Services enabled for Kaspersky VPN, a window with instructions opens.

   Uwaga: System macOS wymaga włączenia usług lokalizacji, aby Kaspersky VPN mógł uzyskać nazwę sieci Wi-Fi (BSSID). Kaspersky Security Network wykorzysta ją do wykrycia niezabezpieczonych sieci Wi-Fi. Nie będą one używane do określenia Twojej prawdziwej lokalizacji.

   Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

   A dialog with the Statement Regarding Data Processing For Purpose Of Providing Unsecured Wi-Fi Network Cloud Detection With Kaspersky Security Network Functionality (Unsecured Wi-Fi Network Cloud Detection Statement) opens.
3. Wykonaj jedną z następujących czynności:
   - If you don't accept the Unsecured Wi-Fi Network Cloud Detection Statement, click **Nie akceptuję**.
   - If you accept the Unsecured Wi-Fi Network Cloud Detection Statement, click **Akceptuję**.

     Note: You can revoke your acceptance by unselecting the **Włącz wykrywanie w chmurze za pomocą Kaspersky Security Network** checkbox at any time.

Aplikacja użyje Kaspersky Security Network do wykrywania niezabezpieczonych sieci Wi-Fi.

Dlaczego nie można otworzyć strony internetowej przy włączonym Kaspersky VPN?

Niektóre strony internetowe i usługi sieciowe odrzucają dostęp, jeśli próbujesz nawiązać z nimi połączenie poprzez VPN. Strony internetowe i usługi sieciowe mogą odrzucić dostęp poprzez VPN z następujących powodów:

- Właściciele stron internetowych chcą, aby licencjonowana zawartość, którą publikują, była dostępna tylko w określonym kraju, ponieważ dla różnych krajów istnieją różne oferty i ceny.
- Właściciele stron internetowych chcą, żeby strona internetowa była odwiedzana tylko w określonym regionie. Na przykład, loteria odbywa się tylko dla danego kraju, a więc dostęp z innych regionów jest zabroniony.

- Istnieją usługi sieciowe, które, z prawnych powodów, są dostępne w określonym regionie (na przykład, niektórzy dostawcy usług multimediów lub programy telewizyjne). Te usługi sieciowe stawiają opór anonimizerom i nie są dostępne, gdy używasz VPN (lub innego anonimizera), aby uzyskać do nich dostęp.

- Te usługi sieciowe nie tylko określają lokalizację klienta, ale także określają, czy klient używa anonimizera. Jeśli zostanie wykryta próba uzyskania dostępu do usługi sieciowej za pośrednictwem anonimizera, dostęp do usługi sieciowej zostanie zablokowany.

- Jeśli nie możesz uzyskać dostępu do określonej strony internetowej lub usługi sieciowej przy użyciu Kaspersky VPN, zalecamy skontaktowanie się z obsługą klienta. Zgłoś usługę sieciową, która jest niedostępna i z której lokalizacji. Firma Kaspersky zrobi wszystko, co w jej mocy, aby rozwiązać problem.

Wersje Kaspersky VPN

Kaspersky VPN jest dostępny w wersjach: bezpłatna i Unlimited.

Wersja bezpłatna:

- Darmowa.
- Zawsze dostępna.
- Ograniczona ilość bezpiecznego ruchu sieciowego na dzień.
- Nie możesz wybrać serwera VPN. Jest wybierana automatycznie.

Możesz przełączyć się z wersji bezpłatnej do wersji Unlimited, kupując subskrypcję.

Wersja Unlimited:

- Nieograniczony ruch sieciowy.
- Możesz wybrać serwer VPN.
- Kill Switch.
- Dostępna poprzez subskrypcję.
- Aplikacja może być zainstalowana na kilku urządzeniach (Mac, mobilne, tablet, PC) w obrębie jednej subskrypcji.

Więcej informacji na temat wersji Kaspersky VPN można znaleźć na stronie My Kaspersky.

Uwaga: Podczas korzystania z wersji Unlimited programu Kaspersky VPN aplikacja może powiadomić o dostępności innej subskrypcji. To powiadomienie pojawia się tylko wtedy, gdy odnaleziona subskrypcja dotyczy mniejszej liczby urządzeń niż bieżąca subskrypcja. Jeśli przejdziesz na tę subskrypcję, Kaspersky VPN zainstalowany na niektórych Twoich urządzeniach przełączy się do wersji bezpłatnej.

Aktualizowanie do wersji Unlimited

Jeśli potrzebujesz nieograniczonego zabezpieczonego ruchu sieciowego oraz chcesz wolnego wyboru serwerów VPN, możesz zaktualizować wersję Unlimited programu Kaspersky VPN. Jeśli korzystasz już z wersji Unlimited, a Twoja subskrypcja utraciła ważność lub rozpoczął się okres karencji, możesz ją odnowić.

Kup/odnów subskrypcję

1. Na zakładce ruchu sieciowego lub subskrypcji okna głównego aplikacji kliknij **Rozszerz** lub **Szczegóły**.

   Zostanie otwarte okno z bieżącym stanem subskrypcji.

2. Aby kupić lub odnowić subskrypcję, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

   Uwaga: Jeśli nie jesteś podłączony do My Kaspersky, Kaspersky VPN wyświetli Oświadczenie dotyczące przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie o zakupie) przed zakupem subskrypcji. Pamiętaj, że kupując subskrypcję, potwierdzasz, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Oświadczenie o zakupie.

Subskrypcję dla Kaspersky VPN możesz kupić także na stronie My Kaspersky lub na stronie internetowej Kaspersky:

- Jeśli kupisz subskrypcję na stronie My Kaspersky, subskrypcja zostanie aktywowana automatycznie po sfinalizowaniu zakupu.
- Jeśli kupisz subskrypcję na stronie internetowej Kaspersky, otrzymasz kod aktywacyjny w wiadomości e-mail wysłanej na podany adres e-mail. Aby aktywować subskrypcję, musisz dodać kod aktywacyjny do swojego konta My Kaspersky i podłączyć Kaspersky VPN do My Kaspersky. Więcej informacji na temat ręcznego dodawania kodu aktywacyjnego do swojego konta My Kaspersky można znaleźć w pomocy My Kaspersky.

Note: To learn about VPN availability in Russia, please read this article.

Przywracanie subskrypcji

Po zalogowaniu się do konta My Kaspersky szczegóły subskrypcji pojawią się automatycznie na stronie My Kaspersky. Jeśli chcesz zastosować tę subskrypcję do programu Kaspersky VPN, zainstalowanego na innym urządzeniu Mac, wystarczy zalogować się do My Kaspersky.

Jeśli nie zalogowałeś się do My Kaspersky i chcesz zastosować swoją subskrypcję do bezpłatnej wersji Kaspersky VPN na innym urządzeniu Mac, konieczne może być przywrócenie subskrypcji.

Przywracanie subskrypcji

1. Otwórz okno główne aplikacji na urządzeniu z zainstalowaną bezpłatną wersją Kaspersky VPN.
2. Na zakładce subskrypcji okna głównego aplikacji kliknij **Rozszerz**.
   Zostanie otwarte okno z bieżącym stanem subskrypcji.
3. Kliknij **Przywróć zakupy**.
   Zostanie wyświetlone okno dialogowe z Oświadczeniem o zakupie.

   Uwaga: Po kliknięciu **Przywróć zakupy**, może być konieczne ponowne uruchomienie aplikacji.
4. Kliknij **Akceptuję**.
5. W monicie o podanie poświadczeń App Store wprowadź swój login i hasło.

Twoja subskrypcja jest stosowana do Kaspersky VPN.

Zmiana konta My Kaspersky

Jeśli chcesz używać innego konta My Kaspersky, możesz wylogować się z bieżącego konta My Kaspersky z poziomu interfejsu aplikacji i zalogować się na inne konto My Kaspersky.

Zmiana konta My Kaspersky

1. W lewym dolnym rogu okna głównego aplikacji kliknij swój adres e-mail.
2. W otwartym oknie dialogowym kliknij **Wyloguj**.
3. W oknie dialogowym **Czy na pewno chcesz wylogować się z My Kaspersky?** kliknij przycisk **Wyloguj**, aby potwierdzić, że chcesz wylogować się z bieżącego konta My Kaspersky.
   Zostanie otwarte okno **Zaloguj się do My Kaspersky**.
4. Wprowadź poświadczenia innego konta My Kaspersky i kliknij przycisk **Zaloguj**.

Informacje o subskrypcji

Subskrypcja dla Kaspersky VPN stanowi zakup prawa do użytkowania aplikacji zgodnie z określonymi parametrami (na przykład, data ważności subskrypcji, liczba urządzeń). Subskrypcję dla aplikacji Kaspersky VPN możesz zamówić u dostawcy usług (np. Google Play lub App Store).

Subskrypcją możesz zarządzać za pośrednictwem osobistego konta na stronie internetowej dostawcy usług (np. przez konto Apple lub Google).

Przed zakupieniem subskrypcji możesz wypróbować wersję Unlimited Kaspersky VPN za darmo. Subskrypcja testowa Kaspersky VPN działa przez krótki okres testowy. Po zakończeniu okresu testowego, zostanie pobrana opłata za subskrypcję. Jeśli nie chcesz korzystać z Kaspersky VPN, musisz anulować subskrypcję przed zakończeniem okresu testowego.

Subskrypcję można odnawiać automatycznie lub ręcznie. Automatycznie odnawiana subskrypcja odnawia się automatycznie pod koniec każdego okresu subskrypcji do momentu jej anulowania. Ręcznie odnawiana subskrypcja musi zostać odnowiona pod koniec każdego okresu subskrypcji. Po wygaśnięciu subskrypcji dla Kaspersky VPN, może zostać zaoferowany okres karencji, podczas którego można korzystać z aplikacji bez ograniczeń. Jeśli przed upływem okresu karencji nie odnowisz subskrypcji, aplikacja przełączy się do wersji bezpłatnej. Aby wrócić do wersji Unlimited, kup nową subskrypcję.

Ważne: Zamówienie subskrypcji dla Kaspersky VPN nie prowadzi do anulowania innych subskrypcji obejmujących Kaspersky VPN. Aby uniknąć dodatkowych opłat, pamiętaj o anulowaniu lub wyłączeniu automatycznego odnawiania dla subskrypcji, których nie potrzebujesz.

Anuluj subskrypcję dla Kaspersky VPN lub przełącz na odnawianie ręczne:

1. Wejdź na stronę konta osobistego na stronie internetowej dostawcy usług.
2. Sprawdź, czy posiadasz aktywne subskrypcje obejmujące Kaspersky VPN.
3. Anuluj lub wyłącz automatyczne odnawianie dla subskrypcji, których nie potrzebujesz.

Informacje o anonimowych subskrypcjach

Twoja subskrypcja jest uznawana za „anonimową", jeśli kupiłeś subskrypcję dla wersji Unlimited programu Kaspersky VPN w sklepie App Store, gdy nie jesteś zalogowany na swoim koncie My Kaspersky lub gdy nie posiadasz konta My Kaspersky. Anonimowa subskrypcja jest powiązana z kontem App Store, ale nie z kontem My Kaspersky.

W każdej chwili możesz powiązać swoją anonimową subskrypcję z kontem My Kaspersky. Po zalogowaniu się do My Kaspersky na urządzeniu za pomocą wersji Unlimited programu Kaspersky VPN, Twoja subskrypcja jest automatycznie kojarzona z Twoim kontem My Kaspersky. Ten proces może trochę potrwać, a aktywne sesje VPN na Twoich urządzeniach mogą zostać zatrzymane. Następnie możesz używać My Kaspersky do zarządzania subskrypcją. Wszystkie urządzenia korzystające z tej subskrypcji zostaną automatycznie połączone z Twoim kontem My Kaspersky. Będziesz także mógł używać swojego konta My Kaspersky do zastosowania swojej subskrypcji do Kaspersky VPN na nowych urządzeniach (jeśli limit urządzeń nie został osiągnięty).

Po przywróceniu anonimowej subskrypcji z Kaspersky VPN po zalogowaniu się do konta My Kaspersky, Twoja subskrypcja jest również automatycznie kojarzona z Twoim kontem My Kaspersky. Wszystkie urządzenia korzystające z tej subskrypcji zostaną automatycznie z nią połączone.

Uwaga: Po powiązaniu subskrypcji z kontem My Kaspersky, musisz potwierdzić wszystkie automatycznie podłączone urządzenia na My Kaspersky.

Możesz odłączyć subskrypcję od My Kaspersky, kontaktując się z obsługą klienta.

Odłącz anonimową subskrypcję od urządzenia

1. Kliknij **Szczegóły subskrypcji**.

   Zostanie wyświetlone okno z aktualnymi szczegółami subskrypcji.

2. Kliknij **Odłącz od subskrypcji**.

3. Potwierdź czynność, klikając ponownie **Odłącz od subskrypcji**.

Twoja aplikacja przełączy się na wersję bezpłatną.

Informacje o przekazywanych danych

Przejrzyj informacje dotyczące danych przekazywanych firmie Kaspersky podczas korzystania z wcześniejszych wersji aplikacji

- Kaspersky VPN 3.0
- Kaspersky VPN 2.16
- Kaspersky VPN 2.15
- Kaspersky VPN 2.14
- Kaspersky VPN 2.13
- Kaspersky VPN 2.12
- Kaspersky VPN 2.11
- Kaspersky VPN 2.10
- Kaspersky VPN 2.9
- Kaspersky VPN 2.8
- Kaspersky VPN 2.7
- Kaspersky VPN 2.6
- Kaspersky Secure Connection 2.5
- Kaspersky Secure Connection 2.4
- Kaspersky Secure Connection 2.3
- Kaspersky Secure Connection 2.2
- Kaspersky Secure Connection 2.1
- Kaspersky Secure Connection 2.0
- Kaspersky Secure Connection 1.0

Dane przekazywane firmie Kaspersky przy użyciu Kaspersky VPN 3.1

Kaspersky chroni wszystkie otrzymane informacje zgodnie z prawem i zasadami Kaspersky. Dane są przekazywane za pośrednictwem bezpiecznego kanału.

Przekazywane dane osobiste

Wyrażasz zgodę na dostarczanie do Kaspersky danych osobistych poprzez zaakceptowanie Umowy licencyjnej, Polityki prywatności, Oświadczenia dotyczącego przetwarzania danych w celach marketingowych (Oświadczenie marketingowe), Oświadczenia dotyczącego przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie o zakupie) lub Oświadczenia dotyczącego przetwarzania danych w celach korzystania z portalu internetowego (Oświadczenie dotyczące portalu internetowego). Możesz przejrzeć listę danych przekazanych zgodnie z warunkami każdego dokumentu prawnego w odpowiadającym dokumencie prawnym.

Umowę licencyjną można przejrzeć w App Store.

Przeczytaj Oświadczenie marketingowe i wyłącz wysyłanie danych

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W sekcji **Ulepszona użyteczność** kliknij **Pokaż Oświadczenie marketingowe**, jeśli chcesz przeczytać warunki Oświadczenia marketingowego.

   Zostanie otwarte okno zawierające Oświadczenie marketingowe.

3. Jeśli chcesz wyłączyć wysyłanie danych, odznacz pole **Pomóż firmie Kaspersky ulepszać produkty wysyłając informacje dotyczące aplikacji i środowiska, w którym ona działa**.

Jeśli nie chcesz, aby Kaspersky odbierał i przetwarzał dane dostarczane zgodnie z Oświadczeniem o zakupie, możesz odwołać swoją akceptację, odłączając subskrypcję.

Odłącz anonimową subskrypcję od urządzenia

1. Na zakładce subskrypcji okna głównego aplikacji kliknij **Szczegóły**.

   Zostanie otwarte okno z bieżącym stanem subskrypcji.

2. Kliknij **Szczegóły subskrypcji**.

   Zostanie wyświetlone okno z aktualnymi szczegółami subskrypcji.

3. Kliknij **Odłącz od subskrypcji**.

4. Potwierdź czynność, klikając ponownie **Odłącz od subskrypcji**.

Twoja aplikacja przełączy się na wersję bezpłatną.

Ważne: Po odłączeniu Kaspersky VPN od subskrypcji, subskrypcja pozostaje aktywna. Aby uzyskać więcej informacji o warunkach subskrypcji, zobacz Informacje o subskrypcji.

Jeśli nie chcesz, aby Kaspersky odbierał dane dostarczane zgodnie z Oświadczeniem dotyczącym portalu internetowego, możesz odwołać swoją akceptację, wylogowując się z My Kaspersky.

Wylogowywanie się z My Kaspersky

1. W lewym dolnym rogu okna głównego aplikacji kliknij swój adres e-mail.
2. W otwartym oknie dialogowym kliknij **Wyloguj**.

Jeśli nie chcesz, aby firma Kaspersky przetwarzała te dane dostarczane zgodnie z Oświadczeniem dotyczącym portalu internetowego, musisz usunąć swoje konto My Kaspersky.

Usuń swoje konto My Kaspersky

1. W lewym dolnym rogu okna głównego aplikacji kliknij swój adres e-mail.
2. W otwartym oknie dialogowym kliknij **Usuń konto**.
   Otworzy się okno przeglądarki.
3. Postępuj zgodnie z instrukcjami wyświetlanymi w przeglądarce.

Więcej informacji o usuwaniu konta My Kaspersky znajduje się w pomocy My Kaspersky.

Ważne: Po wylogowaniu lub usunięciu konta My Kaspersky, Kaspersky VPN przełącza się do wersji bezpłatnej.

Przekazywane dane nieosobowe

Wyrażasz zgodę na dostarczanie do Kaspersky danych nieosobowych poprzez zaakceptowanie Umowy licencyjnej.

Dane nieosobowe są dostarczane do Kaspersky w następujących celach:

Zapewnianie podstawowej funkcji zakupionego Oprogramowania Posiadacza praw.

- Informacje o Oprogramowaniu Posiadacza Praw: pełna wersja Oprogramowania; ID Oprogramowania; wersja językowa Oprogramowania; grupa Oprogramowania; wynik działania Oprogramowania; kod błędu.
- Informacje o wykorzystaniu Kaspersky Security Network (KSN): identyfikator konfiguracji.
- ID tematu w pomocy do Oprogramowania; nazwa łącza.

Oprócz powyższych informacji, w przypadku zalogowania się w portalu internetowym przy użyciu konta Facebook lub Google, Posiadacz praw musi otrzymać z Twojego urządzenia i przetworzyć następujące dane nieosobowe:

- Informacje dotyczące uwierzytelniania: kod autoryzacyjny otrzymany od dostawcy tożsamości; token dostępu otrzymany od dostawcy tożsamości; typ danych wysłanych do dostawcy tożsamości; identyfikator Posiadacza praw w systemie dostawcy tożsamości; nazwa dostawcy tożsamości; URI, do którego wysłana jest odpowiedź dostawcy tożsamości; parametry wymagane od dostawcy tożsamości; identyfikator zasobu Posiadacza praw; typ tokena; wartość wygenerowana dla weryfikacji żądania.

Uwaga: Dostępność opcji logowania za pośrednictwem Facebooka zależy od regionu.

Poprawy jakości, wyglądu i skuteczności działania Oprogramowania, produktów, usług i infrastruktury Posiadacza praw poprzez analizę interakcji, doświadczenia i zadowolenia użytkowników.

- Informacje o Komputerze Użytkownika końcowego, na którym zainstalowano Oprogramowanie: model urządzenia; numer wersji systemu operacyjnego; rozszerzone informacje o wydaniu systemu operacyjnego; rodzinę systemu operacyjnego; wersja pakietu Service Pack dla systemu operacyjnego; wersja systemu operacyjnego zainstalowanego na komputerze użytkownika; wersja bitowa systemu operacyjnego; edycja systemu operacyjnego; typ urządzenia (laptop, komputer stacjonarny, tablet); typ systemu operacyjnego (serwer, stacja robocza, kontroler domeny); kod kraju.

- Informacje o Oprogramowaniu Posiadacza Praw: scenariusz przesłania statystyk; informacje o węzłach VPN; pełna wersja Oprogramowania; ID aktualizacji Oprogramowania; ID Oprogramowania; wersja językowa Oprogramowania; identyfikator rebrandingu Oprogramowania; typ zainstalowanego Oprogramowania; wynik działania Oprogramowania; kod błędu; stan instalacji/dezinstalacji Oprogramowania; kod błędu instalacji; flaga wskazująca, czy instalacja została przerwana przez użytkownika; czas trwania instalacji Oprogramowania w sekundach; typ instalacji (nowa instalacja, aktualizacja); tryb działania Kaspersky VPN Secure Connection; ID scenariusza uruchamiania połączenia VPN; stan ustawień klienta VPN; identyfikatory Oprogramowania w Firebase.

- Informacje o wykorzystaniu Kaspersky Security Network (KSN): protokół użyty do wymiany danych z KSN; ID usługi KSN, do której dostęp uzyskało Oprogramowanie; data i godzina zaprzestania otrzymywania statystyk; liczba połączeń z KSN wzięta z pamięci podręcznej; liczba żądań, dla których odpowiedź znaleziono w lokalnej bazie żądań; liczba nieudanych połączeń z KSN; liczba nieudanych transakcji KSN; tymczasowa dystrybucja anulowanych żądań wysłanych do KSN; tymczasowa dystrybucja nieudanych połączeń z KSN; tymczasowa dystrybucja nieudanych transakcji KSN; tymczasowa dystrybucja pomyślnych połączeń z KSN; tymczasowa dystrybucja pomyślnych transakcji KSN; tymczasowa dystrybucja pomyślnych żądań wysłanych do KSN; tymczasowa dystrybucja żądań wysłanych do KSN, które przekroczyły limit czasu oczekiwania; liczba nowych połączeń z KSN; liczba niepomyślnych żądań wysłanych do KSN spowodowanych przez błędy routingu; liczba niepomyślnych żądań spowodowanych przez wyłączenie usługi KSN w ustawieniach Oprogramowania; liczba niepomyślnych żądań wysłanych do KSN spowodowanych przez problemy z siecią; liczba pomyślnych połączeń z KSN; liczba udanych transakcji KSN; całkowita liczba żądań wysłanych do KSN; data i godzina rozpoczęcia otrzymywania statystyk.

- kod autoryzacyjny otrzymany od dostawcy tożsamości; token dostępu otrzymany od dostawcy tożsamości; typ danych wysłanych do dostawcy tożsamości; identyfikator Posiadacza praw w systemie dostawcy tożsamości; nazwa dostawcy tożsamości; URI, do którego wysłana jest odpowiedź dostawcy tożsamości; parametry wymagane od dostawcy tożsamości; treść komunikatu o błędzie; kod błędu systemu operacyjnego; czas trwania sesji VPN; metoda żądania http; identyfikator zasobu Posiadacza praw; typ tokena; token uwierzytelniania w usługach Posiadacza praw; TTL tokena; ścieżka do przetwarzanego obiektu; metoda używana do autoryzacji w Oprogramowaniu; wartość wygenerowana dla weryfikacji żądania; ID tematu w pomocy do Oprogramowania; informacje o implementacji przechwytywania dostępu do usługi sieciowej; unikatowy identyfikator żądania wysłanego do usług Posiadacza praw; nazwa łącza; numer wiersza pliku źródłowego w rejestratorze wyjątku; ID protokołu; całkowity czas przetwarzania żądania; typ błędu przetwarzania protokołu; kod kategorii błędu; adres DNS usługi sieciowej, do której uzyskano dostęp; czasu dostępu do serwera; zdalny port i adres IP usługi sieciowej, do której uzyskano dostęp; przetwarzany adres internetowy.

Zgodność z prawem Unii Europejskiej

W przypadku dystrybucji programu na terenie Unii Europejskiej, Kaspersky VPN spełnia warunki Rozporządzenia o Ochronie Danych Osobowych (RODO, ang. GDPR - General Data Protection Regulation).

Akceptując Umowę licencyjną, potwierdzasz, że masz odpowiedni wiek do zainstalowania Kaspersky VPN na terenie Unii Europejskiej. Po zainstalowaniu Kaspersky VPN, zostanie zaoferowane przeczytanie i zaakceptowanie warunków wymaganych do wstępnej konfiguracji i korzystania z Kaspersky VPN: Warunki dotyczące przetwarzania danych i Polityka prywatności oraz Oświadczenie dotyczące przetwarzania danych w celach marketingowych (Oświadczenie marketingowe).

Zostanie także zaoferowana możliwość przeczytania i zaakceptowania warunków wymaganych do korzystania z Kaspersky VPN: Oświadczenie dotyczące przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie o zakupie) i Oświadczenie dotyczące przetwarzania danych w celach korzystania z portalu internetowego (Oświadczenie dotyczące portalu internetowego).

Jeśli zdecydujesz się zaakceptować te oświadczenia, będziesz mógł je odrzucić w ustawieniach aplikacji w dowolnym momencie.

Ważne: Jeśli posiadasz wcześniejszą wersję Kaspersky VPN zainstalowaną na systemie OS X 10.11 (El Capitan) i planujesz korzystać z aplikacji na terenie Unii Europejskiej, powinieneś zaktualizować swój system operacyjny do macOS 10.14, a następnie zaktualizować Kaspersky VPN. Jeśli nie chcesz od razu zaktualizować systemu operacyjnego, usuń Kaspersky VPN z komputera.

Zawartość plików śledzenia, plików zrzutów i plików ustawień

Uwaga: Dostęp do wszystkich plików opisanych w tej sekcji może zostać uzyskany przez administratora systemu komputera i właściciela konta komputera z zainstalowanym programem Kaspersky VPN.

1. Pliki śladowe

Pliki śledzenia zawierają następujące informacje o zdarzeniach występujących podczas działania Kaspersky VPN. Pliki śledzenia są przechowywane lokalnie na komputerze w następujących folderach: ~/Library/Group Containers/2Y8XE5CQ94.com.kaspersky.ksec/Library/Application Support/KSEC/Logs/.

Ślady znajdują się w następujących plikach:

- ksec_agent_<znacznik czasu>.log
- ksec_app_<znacznik czasu>.log
- ksec_daemon_<znacznik czasu>_pid_<PID>.log
- ksec_networkextension_<znacznik czasu>.log

Pliki śledzenia mogą zawierać następujące informacje:

- Informacje o urządzeniu i systemie operacyjnym (unikatowy identyfikator urządzenia, typ urządzenia, adresy MAC urządzeń sieciowych, typ systemu operacyjnego, wersja systemu operacyjnego)
- Informacje o aplikacji załadowanej przez użytkownika (adres URL, atrybuty, rozmiar pliku, informacje o procesie, który załadował plik)
- Informacje o uruchomionych aplikacjach i ich modułach
- Informacje o działaniu aplikacji i jej modułach
- Informacje dotyczące błędów i wykorzystania interfejsu graficznego zainstalowanej aplikacji Kaspersky
- Informacje o połączeniach sieciowych i ustawieniach sieci: adres IP zdalnego komputera i komputera użytkownika, adres IP serwerów DNS, adres MAC punktu dostępowego, nazwa sieci, siła sygnału, numery portów

użytych do nawiązania połączenia, protokół sieciowy, stan połączenia w momencie wygenerowania pliku, reputacja sieci, ustawienia serwera proxy – suma kontrolna nazwy użytkownika/hasła

- Informacje dotyczące ustawień połączenia z serwerami Kaspersky
- Informacje o połączeniach z serwerami Pango
- Informacje o typie licencji (typ licencji, region)
- Informacje o pakietach sieciowych odebranych przez komputer i wysłanych z komputera przez sieć telekomunikacyjną
- Informacje o wysyłanych i odbieranych wiadomościach e-mail oraz wiadomościach komunikatorów
- Informacje o My Kaspersky: informacje o nazwach użytkowników i hasłach do stron internetowych oraz zawartość plików cookie
- Certyfikat publiczny serwera
- Informacje o ustawieniach regionalnych języka, ID oprogramowania, dostosowaniu oprogramowania, wersji oprogramowania, unikatowy ID instalacji oprogramowania, unikatowy ID komputera

Pliki śledzenia zawierają tylko informacje niezbędne do rozwiązania problemów z aplikacją. Kaspersky używa plików śledzenia do badania przypadków związanych z błędami pojawiającymi się podczas działania Kaspersky VPN.

Domyślnie, tworzenie plików śledzenia jest wyłączone. Generowanie plików śledzenia można włączyć w ustawieniach aplikacji.

Pliki śledzenia można wysyłać do Kaspersky tylko ręcznie. Kaspersky VPN nie wysyła plików śledzenia do Kaspersky automatycznie.

Możesz wybrać sposób wysłania plików śledzenia do Kaspersky.

Przed wysłaniem plików śledzenia do Kaspersky, sprawdź ich zawartość.

Ważne: Pliki śledzenia mogą zawierać informacje osobiste lub dane wrażliwe. Wysyłając pliki śledzenia do Kaspersky, wyrażasz zgodę na dostarczenie Kaspersky wszystkich danych znajdujących się w wysyłanych plikach śledzenia oraz zgadzasz się na metodę użytą do ich wysłania.

2. Pliki zrzutów

Pliki zrzutów zawierają wszystkie informacje o pamięci roboczej procesów aplikacji w momencie tworzenia zrzutu. Pliki zrzutów mogą zawierać poufne dane.

Pliki zrzutów są generowane przez system operacyjny i są wysyłane na serwery Apple tylko za Twoją zgodą. Przed wysłaniem pliku zrzutu, sprawdź jego zawartość.

3. Dodatkowe pliki

Kaspersky VPN tworzy także dodatkowe pliki ustawień, które są przechowywane na komputerze użytkownika. Te pliki mogą zawierać informacje niezbędne do działania Oprogramowania: ustawienia, wewnętrzne bazy danych, pliki konfiguracyjne.

Specjaliści z obsługi klienta mogą poprosić o dostarczenie dodatkowych plików w celu skrócenia czasu przetwarzania zgłoszeń związanych z błędami w Oprogramowaniu. Użytkownik wysyła te dane ręcznie na prośbę specjalisty z obsługi klienta.

Wysyłając dodatkowe pliki ustawień do obsługi klienta, wyrażasz zgodę na dostarczenie wszystkich danych znajdujących się w tych plikach oraz zgadzasz się na metodę użytą do ich wysłania. Przed wysłaniem tych plików, sprawdź ich zawartość.

Te dodatkowe pliki mogą zawierać następujące informacje:

- Ustawienia serwera proxy – sumę kontrolną nazwy użytkownika i hasła
- Dane uwierzytelniające do nawiązania połączenia z My Kaspersky
- Nazwy sieci Wi-Fi, dla których reguły włączania bezpiecznego połączenia są konfigurowane

Zacznij pracę z aplikacją

Wymagania sprzętowe i programowe

Kaspersky VPN posiada następujące wymagania sprzętowe i programowe:

- 1 GB pamięci (RAM)
- 320 MB wolnego miejsca na dysku
- System operacyjny macOS 11-13
- Połączenie internetowe
- Typ procesora: Intel, Apple Silicon

Instalowanie i dezinstalowanie aplikacji

Kaspersky VPN może zostać zainstalowany z poziomu sklepu App Store.

W celu zainstalowania aplikacji:

1. Otwórz aplikację App Store.
2. Odszukaj Kaspersky VPN i zainstaluj aplikację.
   Aplikacja App Store może wyświetlić pytanie o wprowadzenie danych uwierzytelniających Apple ID.

> **Uwaga:** Więcej informacji dotyczących korzystania z App Store i instalowania aplikacji można znaleźć w odpowiednich podręcznikach użytkownika dla posiadanego komputera Mac.

W celu odinstalowania aplikacji:

1. Odszukaj aplikację w Finderze.
2. Otwórz menu skrótu i wybierz **Przenieś do Kosza**.

> **Uwaga:** Więcej informacji na temat odinstalowywania aplikacji można znaleźć w odpowiednich podręcznikach użytkownika dla komputera Mac.

Uruchamianie aplikacji po raz pierwszy

Podczas pierwszego uruchomienia Kaspersky VPN na komputerze aplikacja wyświetla monit o zaakceptowanie warunków wymaganych do początkowej konfiguracji i korzystania z Kaspersky VPN.

Uruchamianie Kaspersky VPN po raz pierwszy

1. Kliknij ikonę Launchpada znajdującą się w Docku.

   Zostanie otwarte okno zawierające listę aplikacji.

2. Kliknij ikonę Kaspersky VPN.

3. W oknie **Zanim rozpoczniesz, zapoznaj się z Warunkami dotyczącymi przetwarzania danych i Polityką prywatności** przeczytaj treść Warunków dotyczących przetwarzania danych.

4. Kliknij odnośnik **Polityka prywatności**, aby przeczytać Politykę prywatności, która opisuje zarządzanie danymi.

   Zostanie otwarte okno przeglądarki wyświetlające Politykę prywatności.

5. Wykonaj jedną z następujących czynności:

   - Jeśli nie zgadzasz się z Warunkami dotyczącymi przetwarzania danych lub Polityką prywatności, zamknij okno aplikacji i nie korzystaj z aplikacji.

   - Jeśli zgadzasz się z Warunkami dotyczącymi przetwarzania danych i Polityką prywatności, potwierdź to, zaznaczając odpowiednie pola.

     Uwaga: Przycisk **Akceptuję** stanie się dostępny tylko wtedy, gdy potwierdzisz, że przeczytałeś, rozumiesz i akceptujesz Warunki dotyczące przetwarzania danych oraz Politykę prywatności.

6. Kliknij **Akceptuję**.

7. W oknie **Oświadczenie dotyczące przetwarzania danych w celach marketingowych** przeczytaj treść Oświadczenia marketingowego. Akceptując Oświadczenie marketingowe, zezwalasz Kaspersky na zaoferowanie dodatkowych korzyści.

8. Jeśli wyrażasz zgodę na warunki Oświadczenia dotyczącego przetwarzania danych w celach marketingowych, kliknij **Akceptuję**, a następnie, w wyświetlonym oknie potwierdzenia kliknij **Potwierdzam**.

   Uwaga: Możesz wycofać swoją akceptację w ustawieniach aplikacji w dowolnym momencie.

9. W następnym oknie możesz pobrać wersję Unlimited Kaspersky VPN. Wykonaj jedną z następujących czynności:

   - Jeśli chcesz rozpocząć 7-dniowy bezpłatny okres próbny lub zakupić subskrypcję, kliknij niebieski przycisk z odpowiednim tekstem.

     Klikając **Uruchom 7-dniową wersję testową** lub **Kup subskrypcję za <cena>/rok** lub **Kup subskrypcję za <cena>/miesiąc**, potwierdzasz, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Oświadczenia dotyczącego przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie zakupu) zazwyczaj wyświetlane po prawej stronie okna aplikacji.

   - Jeśli wcześniej zakupiłeś subskrypcję dla Kaspersky VPN i chcesz zastosować tę subskrypcję do tej kopii aplikacji, kliknij **Przywróć zakupy** w prawym górnym rogu okna aplikacji.

     Jeśli wcześniej nie zaakceptowałeś Oświadczenia dotyczącego przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie o zakupie), zapoznaj się z warunkami tego oświadczenia w otwartym oknie dialogowym i kliknij **Akceptuję**. Klikając **Akceptuję**, potwierdzasz, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Oświadczenie dotyczące przetwarzania danych w celach zakończenia procesu zakupu (Oświadczenie o zakupie).

Uwaga: Możesz pominąć ten krok, klikając **Pomiń**. Aplikacja zostanie przełączona do wersji bezpłatnej Kaspersky VPN. Możesz uzyskać wersję Unlimited aplikacji później, w dowolnym momencie.

Zostanie otwarte okno główne aplikacji.

Nawiązywanie połączenia z My Kaspersky

Jeśli otwierasz program Kaspersky VPN, możesz zalogować się do My Kaspersky z użyciem konta My Kaspersky. Jeśli korzystałeś z innej aplikacji Kaspersky, na przykład, Kaspersky VPN dla innego urządzenia lub Kaspersky Internet Security, prawdopodobnie masz już konto My Kaspersky. Użyj go do zalogowania się. Jeśli nie masz konta, możesz je utworzyć.

Uwaga: Jeśli zalogowałeś się do My Kaspersky w innej aplikacji Kaspersky na komputerze Mac, po zainstalowaniu, aplikacja Kaspersky VPN wyświetli pytanie o zalogowanie się do My Kaspersky przy użyciu tego samego konta.

Logowanie do My Kaspersky przy użyciu istniejącego konta

1. Otwórz okno główne aplikacji i kliknij **Zaloguj**.

   Zostanie otwarte okno **Zaloguj się do My Kaspersky**.

2. Wykonaj jedną z następujących czynności:

   - Jeśli chcesz nawiązać połączenie z My Kaspersky za pośrednictwem konta Google, Facebook lub Apple, kliknij odpowiedni przycisk i postępuj zgodnie z instrukcjami. Więcej informacji znajduje się na stronie systemu pomocy My Kaspersky. Jeśli nie masz jeszcze konta My Kaspersky, aplikacja wyświetli pytanie o zarejestrowanie się na stronie My Kaspersky.

     Uwaga: Dostępność opcji logowania za pośrednictwem Facebooka zależy od regionu.

   - Jeśli masz login i hasło do swojego konta My Kaspersky, wprowadź swoje dane uwierzytelniające i kliknij **Zaloguj**.

     Uwaga: Jeśli kilka razy w krótkim czasie wprowadzisz błędne hasło, konieczne będzie wprowadzenie znaków z obrazka, by przejść pomyślnie kontrolę bezpieczeństwa.

     Uwaga: Jeśli włączono weryfikację dwuetapową dla Twojego konta My Kaspersky, konieczne będzie wprowadzenie kodu otrzymanego przez wiadomość SMS lub wygenerowanego w aplikacji uwierzytelniającej.

   Zostanie otwarte okno dialogowe z Oświadczeniem dotyczącym przetwarzania danych w celach korzystania z portalu internetowego (Oświadczenie dotyczące portalu internetowego).

3. Wykonaj jedną z następujących czynności:

   - Jeśli nie akceptujesz Oświadczenia dotyczącego portalu internetowego, kliknij **Nie akceptuję**.

     Uwaga: Nie możesz zalogować się do My Kaspersky lub utworzyć konta My Kaspersky bez zaakceptowania Oświadczenia dotyczącego portalu internetowego.

   - Jeśli akceptujesz Oświadczenie dotyczące portalu internetowego, kliknij przycisk **Akceptuję**, aby kontynuować.

Kaspersky VPN zaloguje Cię na konto My Kaspersky.

Tworzenie konta My Kaspersky z poziomu interfejsu aplikacji

1. W oknie **Zaloguj się do My Kaspersky** kliknij **Utwórz konto**.

   Zostanie otwarte okno **Utwórz konto My Kaspersky**.

   Uwaga: Jeśli wprowadzisz adres e-mail, który jest już używany, niepoprawny adres e-mail lub zbyt popularne hasło kilka razy w krótkim przedziale czasu, będziesz musiał wprowadzić znaki z obrazka, aby przejść kontrolę bezpieczeństwa.

2. W polu do wprowadzenia adresu e-mail wpisz adres e-mail, który chcesz skojarzyć z nowym kontem My Kaspersky.

3. W polu do wprowadzenia hasła wpisz hasło do swojego konta My Kaspersky.

   Uwaga: Hasło musi zawierać minimum osiem znaków, w tym przynajmniej jedną cyfrę, jedną małą literę oraz jedną dużą literę. Hasło nie może zawierać spacji.

4. W polu potwierdzenia hasła ponownie wpisz hasło.

5. W menu wyskakującym wyboru kraju wybierz kraj.

   Uwaga: Kaspersky VPN automatycznie wyświetla Twój kraj w oparciu o region ustawiony w ustawieniach systemowych Język & Region. Ta opcja określa ustawienia regionalne dla Twojego konta My Kaspersky, na przykład, język wyświetlania i dostępne aplikacje firmy Kaspersky. Będziesz mógł zmienić region dla swojego konta My Kaspersky w późniejszym czasie tylko poprzez skontaktowanie się z działem obsługi klienta.

6. Kliknij odnośnik **Polityka prywatności**, aby przeczytać Politykę prywatności, która opisuje zarządzanie danymi.

   Zostanie otwarte okno przeglądarki wyświetlające Politykę prywatności.

7. Jeśli wyrażasz zgodę na warunki Polityki prywatności, zaznacz pole **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki Polityki prywatności opisującej zasady przetwarzania danych**.

   Uwaga: Przycisk **Utwórz** stanie się dostępny tylko wtedy, gdy potwierdzisz, że przeczytałeś, rozumiesz i akceptujesz Politykę prywatności.

8. Jeśli wyrażasz zgodę na udostępnienie swojego adresu e-mail, aby otrzymywać wiadomości e-mail z informacjami i ofertami promocyjnymi, zaznacz pole **Wyrażam zgodę na udostępnienie firmie Kaspersky mojego adresu e-mail w celu otrzymywania spersonalizowanych ofert marketingowych**.

9. Kliknij **Utwórz**.

   Zostanie otwarte okno dialogowe z Oświadczeniem dotyczącym przetwarzania danych w celach korzystania z portalu internetowego (Oświadczenie dotyczące portalu internetowego).

10. Wykonaj jedną z następujących czynności:

    - Jeśli nie akceptujesz Oświadczenia dotyczącego portalu internetowego, kliknij **Nie akceptuję**.

Uwaga: Nie możesz zalogować się do My Kaspersky lub utworzyć konta My Kaspersky bez zaakceptowania Oświadczenia dotyczącego portalu internetowego.

- Jeśli akceptujesz Oświadczenie dotyczące portalu internetowego, kliknij przycisk **Akceptuję**, aby kontynuować.

Kaspersky VPN nawiąże połączenie z My Kaspersky i utworzy konto użytkownika. Po utworzeniu konta zostanie otwarte okno główne aplikacji, a na adres e-mail, określony podczas rejestracji, zostanie wysłana wiadomość z instrukcjami dotyczącymi aktywacji konta.

Ważne: Aby możliwe było nawiązanie połączenia z My Kaspersky, konieczny jest dostęp do Internetu.

Informacje o weryfikacji dwuetapowej

Ważne: Weryfikacja dwuetapowa może być niedostępna w Twoim regionie. Więcej informacji znajduje się na stronie systemu pomocy My Kaspersky.

Weryfikacja dwuetapowa uniemożliwia ludziom ze złymi zamiarami zalogowanie się na Twoje konto My Kaspersky nawet wtedy, gdy znają Twoje hasło. W celu zweryfikowania Twojej tożsamości otrzymasz unikatowy kod zabezpieczający na jeden z następujących sposobów:

- Za pośrednictwem wiadomości SMS. Używamy numeru telefonu, który zapisałeś na My Kaspersky. Oznacza to, że do zalogowania się na Twoje konto potrzebne jest Twoje hasło oraz Twój telefon.
- Za pośrednictwem aplikacji uwierzytelniającej. W pierwszej kolejności należy skonfigurować weryfikację dwuetapową za pośrednictwem Twojego numeru telefonu komórkowego, aby funkcja aplikacji uwierzytelniającej była dostępna.

Weryfikację dwuetapową możesz włączyć na My Kaspersky. Jeśli zmienisz numer telefonu, możesz go zaktualizować na My Kaspersky. Jeśli już zalogowałeś się na swoje konto na urządzeniu, nic się nie zmieni dla Ciebie. Więcej informacji znajduje się na stronie systemu pomocy My Kaspersky.

Uwaga: Kod zabezpieczający jest ważny przez krótki czas. Jeśli wygaśnie, zażądaj innego kodu zabezpieczającego.

Jeśli nie otrzymałeś wiadomości SMS z kodem zabezpieczającym

1. Sprawdź, czy Twoje urządzenie mobilne jest włączone, a sieć mobilna jest dostępna.
2. Zaczekaj, aż przycisk **Zażądaj kodu ponownie** stanie się dostępny w aplikacji.
3. Kliknij **Zażądaj kodu ponownie**.

Jeśli problem wciąż się pojawia, skontaktuj się z działem obsługi klienta.

Aktywowanie połączenia VPN

Użyj jednej z następujących metod do aktywowania bezpiecznego połączenia w Kaspersky VPN:

1. Możesz włączyć/wyłączyć VPN z poziomu interfejsu aplikacji lub na pasku menu.

   Należy pamiętać, że po zakończeniu działania Kaspersky VPN aplikacja przestaje działać, a bezpieczne połączenie zostaje wyłączone.

   Włączanie VPN

   Wykonaj jedną z następujących czynności:

   - W oknie głównym aplikacji włącz VPN.
   - Na pasku menu kliknij ikonę aplikacji i wybierz **Włącz VPN**.

   Wyłączanie VPN

   Wykonaj jedną z następujących czynności:

   - W oknie głównym aplikacji wyłącz VPN.
   - Na pasku menu kliknij ikonę aplikacji i wybierz **Wyłącz VPN**.

2. Możesz zezwolić Kaspersky VPN na działanie w tle.

   Jeśli ta opcja jest włączona, aplikacja będzie zawsze monitorować połączenia Wi-Fi i ostrzegać, jeśli dołączysz do niezabezpieczonej sieci Wi-Fi. Możesz skonfigurować Kaspersky VPN tak, aby automatycznie włączał VPN po wykryciu niezabezpieczonej sieci. Zalecane jest używanie tej opcji.

   Jeśli chcesz zakończyć działanie aplikacji, możesz zrobić to ręcznie.

   Zezwalanie Kaspersky VPN na działanie w tle

   1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

      Zostanie otwarte okno ustawień aplikacji.

   2. W sekcji **Uruchom w tle** zaznacz pole **Pozwól Kaspersky VPN na działanie w tle (zalecane)**.

   Po zamknięciu Kaspersky VPN, aplikacja będzie działać w tle.

   Kończenie działania Kaspersky VPN z poziomu menu ikony aplikacji

   Na pasku menu kliknij ikonę aplikacji i wybierz **Zakończ** lub **Rozłącz i zakończ**, jeśli Kaspersky VPN działa w tle.

3. Aby zapewnić maksymalną ochronę, możesz skonfigurować Kaspersky VPN tak, aby automatycznie włączał VPN po uruchomieniu komputera Mac.

   Zezwalanie Kaspersky VPN na automatyczną ochronę połączenia

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W sekcji **Uruchom w tle** zaznacz pole **Pozwól Kaspersky VPN na działanie w tle (zalecane)**, a następnie zaznacz pole **Włącz VPN automatycznie po uruchomieniu komputera Mac**.

   Uwaga: Pole **Włącz VPN automatycznie po uruchomieniu komputera Mac** jest dostępne, jeśli pole **Pozwól Kaspersky VPN na działanie w tle (zalecane)** jest zaznaczone.

Uwaga: Bezpieczne połączenie może zostać utracone z powodu niestabilnego połączenia internetowego lub podczas przełączania się między sieciami. W takim przypadku przesyłane dane nie są chronione. Kaspersky VPN przywraca bezpieczne połączenie po ponownym połączeniu się z internetem. Jeśli nie można przywrócić bezpiecznego połączenia, Kaspersky VPN powiadomi o tym fakcie. Aby chronić swoje dane w przypadku zerwania bezpiecznego połączenia, możesz użyć Kill Switch. Całkowicie blokuje przesyłanie danych do czasu przywrócenia bezpiecznego połączenia.

Wybieranie serwera VPN

Jeśli chcesz ukryć swój adres IP i pojawić się w internecie jako użytkownik z innego miejsca, możesz zmienić lokalizację, wybierając inny serwer VPN. Obecnie Kaspersky VPN obsługuje następujące lokalizacje serwerów VPN.

Jeśli chcesz obejrzeć film lub serial w dniu jego światowej premiery, mimo że w twoim regionie premiera jest zaplanowana na późniejszy termin, wystarczy, że uruchomisz aplikację i wybierzesz region, w którym jest on dostępny. Zalecamy następujące serwery dla treści regionalnych.

Uwaga: Lokalizacje na liście są ustalane w oparciu o adres IP serwera VPN i niekoniecznie odpowiadają lokalizacji fizycznej serwera VPN.

Wybieranie serwera VPN

1. Na zakładce serwer VPN okna głównego aplikacji kliknij **Zmień**.

   Zostanie otwarta lista serwerów VPN.

2. Wybierz serwer VPN, z którego chcesz korzystać.

Kaspersky VPN od razu nawiąże połączenie z wybranym serwerem VPN.

Uwaga: Tylko wersja Unlimited aplikacji umożliwia wybranie serwera VPN, z którego chcesz korzystać. W wersji bezpłatnej program Kaspersky VPN automatycznie wybiera lokalizację bezpłatnego serwera VPN.

Wyświetlanie ilości wykorzystanego i dostępnego ruchu sieciowego

Kaspersky VPN wyświetla ilość zużytego i dostępnego ruchu sieciowego w bezpłatnej wersji aplikacji.

Jeśli korzystasz z bezpłatnej wersji Kaspersky VPN, korzystanie z bezpiecznego ruchu sieciowego jest ograniczone każdego dnia. Jeśli przekroczysz ograniczenie zabezpieczonego ruchu sieciowego, aplikacja wyświetli informację, że bezpieczne połączenie jest niedostępne. Od wyświetlenia powiadomienia do wyłączenia bezpiecznego połączenia może minąć kilka minut.

Możesz usunąć to ograniczenie, aktualizując aplikację do wersji Unlimited.

Wyświetlanie ilości wykorzystanego i dostępnego ruchu sieciowego

Otwórz okno główne aplikacji i sprawdź kartę ruchu sieciowego w prawym dolnym rogu.

Uwaga: Możesz także sprawdzić ilość zużytego i dostępnego ruchu sieciowego w menu **Połączenie** lub w menu ikony aplikacji.

Informacje o dostępnym i wykorzystanym ruchu sieciowym są aktualizowane nie częściej niż raz na minutę. Po wyłączeniu bezpiecznego połączenia, informacje o zużytym bezpiecznym ruchu sieciowym zostają zaktualizowane w ciągu 30 sekund.

W jaki sposób konfigurować Dzielone tunelowanie

Można skonfigurować włączenie połączenia VPN tylko dla wybranych aplikacji (Dzielone tunelowanie).

Uruchom VPN tylko dla wybranych aplikacji

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.
   Zostanie otwarte okno ustawień aplikacji.
2. W zakładce **Dzielone tunelowanie** zaznacz pole wyboru **Uruchom VPN tylko dla wybranych aplikacji**.
3. Wykonaj jedną z następujących czynności:
   - Aby dodać aplikację do listy, wpisz lub wybierz nazwę aplikacji w polu wyboru.
   - Aby usunąć aplikację z listy, zaznacz ją i kliknij .

Uwaga: Dzielone tunelowanie jest dostępne tylko w wersji Unlimited programu Kaspersky VPN.

Dzielone tunelowanie ma następujące ograniczenia:

- Ustawienia Dzielonego tunelowania można skonfigurować tylko dla aplikacji niesystemowych z folderu Aplikacje.

- Jeżeli Dzielone tunelowanie jest włączone i połączenie VPN zostanie przerwane, Kill Switch odetnie transfer danych przez Internet tylko dla aplikacji dodanych do listy Dzielone tunelowanie.

Chroń swoje dane, jeśli Twoje bezpieczne połączenie zostało utracone

Jeśli włączysz VPN, Twoje dane są chronione podczas surfowania w internecie. Jednakże, jeśli połączenie VPN spadnie, Twoje dane nie będą chronione i cyberprzestępcy będą mogli je wykraść. Aby Twoje dane były zawsze chronione, możesz użyć *Kill Switch*. Kill Switch przerwie przesyłanie danych przez internet, gdy następuje ponowne nawiązanie połączenia z VPN. Twoje połączenie z internetem zostanie przywrócone po włączeniu VPN.

Ważne: Aby chronić Twoje dane, Kill Switch całkowicie blokuje przesyłanie danych za pośrednictwem internetu, aż do przywrócenia połączenia VPN. To nie wpływa na przesyłanie danych w Twojej sieci lokalnej. Twój komputer Mac może wchodzić w interakcję z innymi urządzeniami w Twojej sieci lokalnej bez żadnych ograniczeń.

Domyślnie, Kill Switch zostanie wyłączony, a Kaspersky VPN nie blokuje dostępu do internetu, jeśli połączenie VPN zostanie przerwane.

Uwaga: Jeżeli Dzielone tunelowanie jest włączone i połączenie VPN zostanie przerwane, Kill Switch odetnie transfer danych przez Internet tylko dla aplikacji dodanych do listy Dzielone tunelowanie.

Włącz Kill Switch

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.
   Zostanie otwarte okno ustawień aplikacji.
2. W zakładce **Kill Switch** zaznacz pole **Włącz Kill Switch**.
   Zostanie otwarte okno z informacjami na temat Kill Switch.
3. Kliknij **Włącz mimo wszystko**.

Aplikacja zablokuje Twój dostęp do internetu, jeśli połączenie VPN zostanie przerwane.

Uwaga: Kill Switch jest dostępny tylko w wersji Unlimited programu Kaspersky VPN.

Konfigurowanie ustawień VPN dla znanych sieci Wi-Fi

Jeśli regularnie łączysz swój komputer Mac z określoną siecią Wi-Fi, możesz skonfigurować ustawienia VPN dla tej sieci.

Konfigurowanie ustawień VPN dla określonej sieci Wi-Fi

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W zakładce **Niezabezpieczona sieć Wi-Fi** wybierz działanie, które ma zostać wykonane po nawiązaniu połączenia z siecią Wi-Fi, dla której chcesz skonfigurować preferencje VPN:

   - **Nie określono**. Jeśli określona sieć Wi-Fi jest niezabezpieczona, aplikacja stosuje ustawienia określone dla niezabezpieczonych sieci Wi-Fi. Jeśli określona sieć jest zabezpieczona, aplikacja nic nie zrobi.
   - **Włącz VPN**. Aplikacja włącza VPN po podłączeniu komputera Mac do określonej sieci Wi-Fi.
   - **Nie wykonuj żadnych akcji**. Aplikacja nie włącza VPN po podłączeniu komputera Mac do określonej sieci Wi-Fi.

Włączanie i wyłączanie wysyłania danych w celach marketingowych

Możesz włączyć lub wyłączyć wysyłanie danych, które pomogą Kaspersky w udoskonaleniu jakości, wyglądu i działania aplikacji. Informacje na temat danych przesyłanych do Kaspersky znajdziesz w Oświadczeniu marketingowym.

Wyświetl Oświadczenie marketingowe

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W sekcji **Ulepszona użyteczność** kliknij **Pokaż Oświadczenie marketingowe**.

Zostanie otwarte okno zawierające Oświadczenie marketingowe.

Włączanie i wyłączanie wysyłania danych w celach marketingowych

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W sekcji **Ulepszona użyteczność** wykonaj jedną z następujących czynności:

   - Jeśli chcesz włączyć wysyłanie danych, zaznacz pole **Pomóż firmie Kaspersky ulepszać produkty wysyłając informacje dotyczące aplikacji i środowiska, w którym ona działa** i w otwartym oknie dialogowym kliknij **Potwierdzam**.
   - Jeśli chcesz wyłączyć wysyłanie danych, odznacz pole **Pomóż firmie Kaspersky ulepszać produkty wysyłając informacje dotyczące aplikacji i środowiska, w którym ona działa**.

Włączanie śledzenia

Śledzenie to sposób zapisywania szczegółowych informacji o aktywności aplikacji. Specjaliści z obsługi klienta Kaspersky wykorzystują pliki śledzenia do rozwiązywania problemów. Możesz włączyć rejestrowanie zdarzeń aplikacji, aby utworzyć pliki śledzenia i wysłać je do obsługi klienta, jeśli zostaniesz o to poproszony. Domyślnie, zapisywanie zdarzeń aplikacji jest wyłączone.
Włączanie zapisywania danych do plików śledzenia

1. Otwórz Kaspersky VPN.
2. Na pasku menu wybierz **Pomoc** > **Włącz śledzenie**.

Ważne: Śledzenie należy włączać tylko na wyraźną prośbę specjalistów z obsługi klienta.

Chroń swoje połączenie z niezabezpieczoną siecią Wi-Fi

Podczas nawiązywania połączenia z dowolną siecią Wi-Fi, Kaspersky VPN sprawdza stan sieci Wi-Fi zgodnie z danymi z Kaspersky Security Network i inne kryteria, takie jak, czy używany jest protokół szyfrowania podatny na ataki lub popularna nazwa sieci (SSID). Korzystając z tych informacji, Kaspersky VPN określa, czy sieć Wi-Fi jest bezpieczna.

Jeśli już nawiązałeś połączenie z niezabezpieczoną siecią Wi-Fi, możesz chronić swoje połączenie przy użyciu Kaspersky VPN.

Chroń swoje połączenie z niezabezpieczoną siecią Wi-Fi

1. W oknie głównym aplikacji włącz VPN.
2. W otwartym oknie powiadomienia kliknij **Tak, włącz**, jeśli chcesz, żeby Kaspersky VPN włączał VPN automatycznie podczas nawiązywania połączenia z niezabezpieczoną siecią Wi-Fi.

Włącz wykrywanie niezabezpieczonych sieci Wi-Fi przy użyciu Kaspersky Security Network

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W zakładce **Niezabezpieczona sieć Wi-Fi** zaznacz pole **Włącz wykrywanie w chmurze za pomocą Kaspersky Security Network**.

   If you don't have Location Services enabled for Kaspersky VPN, a window with instructions opens.

   > **Uwaga:** System macOS wymaga włączenia usług lokalizacji, aby Kaspersky VPN mógł uzyskać nazwę sieci Wi-Fi (BSSID). Kaspersky Security Network wykorzysta ją do wykrycia niezabezpieczonych sieci Wi-Fi. Nie będą one używane do określenia Twojej prawdziwej lokalizacji.

   Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

   A dialog with the Statement Regarding Data Processing For Purpose Of Providing Unsecured Wi-Fi Network Cloud Detection With Kaspersky Security Network Functionality (Unsecured Wi-Fi Network Cloud Detection Statement) opens.

3. Wykonaj jedną z następujących czynności:

   - If you don't accept the Unsecured Wi-Fi Network Cloud Detection Statement, click **Nie akceptuję**.
   - If you accept the Unsecured Wi-Fi Network Cloud Detection Statement, click **Akceptuję**.

     > **Note:** You can revoke your acceptance by unselecting the **Włącz wykrywanie w chmurze za pomocą Kaspersky Security Network** checkbox at any time.

Aplikacja użyje Kaspersky Security Network do wykrywania niezabezpieczonych sieci Wi-Fi.

Wybieranie działania, jakie Kaspersky VPN wykona po nawiązaniu połączenia z niezabezpieczoną siecią Wi-Fi

Możesz wybrać, czy chcesz, żeby po nawiązaniu połączenia z niezabezpieczoną siecią Wi-Fi program Kaspersky VPN wyświetlił pytanie o wybór działania lub automatycznie zabezpieczył połączenie.

Wybieranie działania, jakie Kaspersky VPN wykona po nawiązaniu połączenia z niezabezpieczoną siecią Wi-Fi

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W zakładce **Niezabezpieczona sieć Wi-Fi** wybierz akcję, jaką Kaspersky VPN ma wykonać.

W jaki sposób uzyskać obsługę klienta

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji lub w jednym ze źródeł informacji o aplikacji, skontaktuj się z działem obsługi klienta. Odwiedź stronę internetową obsługi klienta, aby skontaktować się ze specjalistą, którzy mogą odpowiedzieć na wszystkie Twoje pytania odnośnie instalowania i korzystania z aplikacji.

Uwaga: Przed skontaktowaniem się z obsługą klienta przeczytaj zasady korzystania z pomocy technicznej.

Znane problemy

Podczas korzystania z Kaspersky VPN możesz napotkać następujące znane problemy:

- Jeśli Power Nap jest włączony na Twoim komputerze Mac, Kaspersky VPN nie chroni wszystkich aktualizacji informacji, ponieważ program nie działa, gdy Twój komputer Mac jest w trybie uśpienia. Jeśli chcesz chronić wszystkie dane wysyłane i odbierane przez internet, zalecane jest wyłączenie funkcji Power Nap na komputerze Mac.

- Jeśli program Kaspersky Security Cloud / Kaspersky Internet Security for Mac został zainstalowany na komputerze Mac, a opcja Kill Switch jest włączona, wówczas Kaspersky VPN nie może nawiązać zaszyfrowanego, bezpiecznego połączenia. Aby nawiązać bezpieczne połączenie, wyłącz opcję Kill Switch lub zakończ działanie Kaspersky Security Cloud / Kaspersky Internet Security for Mac. Dzieje się tak w wyniku pewnych problemów z macOS. Skontaktowaliśmy się z firmą Apple w sprawie tego problemu i robimy co w naszej mocy, aby go rozwiązać jak najszybciej.

- Zaszyfrowanego bezpiecznego połączenia nie można nawiązać w ustawieniach systemu macOS.

- Ilość użytego bezpiecznego ruchu sieciowego wyświetlana w aplikacji może różnić się od rzeczywistej ilości zużytego bezpiecznego ruchu sieciowego. Taka sytuacja może mieć miejsce w przypadku połączeń o dużej przepustowości.

- Gdy aplikacja zmienia serwer wirtualny, bezpieczne połączenie może zostać na krótko przerwane. Przesyłane dane nie będą chronione, dopóki bezpieczne połączenie nie zostanie przywrócone.

- Po zakupie subskrypcji, może wystąpić kilkuminutowe opóźnienie w przełączeniu aplikacji do wersji Unlimited.

- Jeśli podczas nawiązywania połączenia z internetem komputer Mac zmienia sieć, bezpieczne połączenie może zostać na krótko przerwane. Przesyłane dane nie będą chronione, dopóki bezpieczne połączenie nie zostanie przywrócone.

- Zmiana serwera wirtualnego podczas odwiedzania stron internetowych banków, systemów płatniczych, stron internetowych systemów rezerwacji, serwisów społecznościowych, czatów i serwisów pocztowych może prowadzić do włączenia systemów antyoszustowych (systemy przeznaczone do analizowania transakcji finansowych online pod kątem oznak typowych dla oszukańczych działań).

- Jeśli Twój komputer Mac zmieni źródło zasilania (bateria/podłączenie do kontaktu), bezpieczne połączenie może zostać na krótko przerwane. Przesyłane dane nie są chronione do momentu ponownego nawiązania bezpiecznego połączenia. W tym przypadku Kill Switch nie przerywa przesyłania danych. Dzieje się tak w wyniku pewnych problemów z macOS. Skontaktowaliśmy się z firmą Apple w sprawie tego problemu i robimy co w naszej mocy, aby go rozwiązać jak najszybciej.

- Jeśli wylogujesz się z konta My Kaspersky, gdy jesteś połączony za pośrednictwem VPN i posiadasz aktywną subskrypcję, bezpieczne połączenie może zostać zerwane. Przesłane dane nie będą chronione, aż do ponownego nawiązania bezpiecznego połączenia.

- Przekazywanie prywatne iCloud i Ochrona prywatności w Mail są niekompatybilne z Kaspersky VPN na systemie macOS 12 lub nowszym.

Podczas nawiązywania połączenia z pewnymi stronami internetowymi poprzez VPN mogą wystąpić problemy.

Niektóre strony internetowe i usługi sieciowe odrzucają dostęp, jeśli próbujesz nawiązać z nimi połączenie poprzez VPN. Strony internetowe i usługi sieciowe mogą odrzucić dostęp poprzez VPN z następujących powodów:

- Właściciele stron internetowych chcą, aby licencjonowana zawartość, którą publikują, była dostępna tylko w określonym kraju, ponieważ dla różnych krajów istnieją różne oferty i ceny.

- Właściciele stron internetowych chcą, żeby strona internetowa była odwiedzana tylko w określonym regionie. Na przykład, loteria odbywa się tylko dla danego kraju, a więc dostęp z innych regionów jest zabroniony.

- Istnieją usługi sieciowe, które, z prawnych powodów, są dostępne w określonym regionie (na przykład, niektórzy dostawcy usług multimediów lub programy telewizyjne). Te usługi sieciowe stawiają opór anonimizerom i nie są dostępne, gdy używasz VPN (lub innego anonimizera), aby uzyskać do nich dostęp.

- Te usługi sieciowe nie tylko określają lokalizację klienta, ale także określają, czy klient używa anonimizera. Jeśli zostanie wykryta próba uzyskania dostępu do usługi sieciowej za pośrednictwem anonimizera, dostęp do usługi sieciowej zostanie zablokowany.

- Jeśli nie możesz uzyskać dostępu do określonej strony internetowej lub usługi sieciowej przy użyciu Kaspersky VPN, zalecamy skontaktowanie się z obsługą klienta. Zgłoś usługę sieciową, która jest niedostępna i z której lokalizacji. Firma Kaspersky zrobi wszystko, co w jej mocy, aby rozwiązać problem.

- Szybkość połączenia internetowego może zostać zmniejszona o ponad 50 procent przy uruchomionym Kaspersky VPN. Nie możemy zagwarantować minimalnej prędkości połączenia z internetem.

- Kaspersky VPN nie może ustanowić bezpiecznego szyfrowanego połączenia dla ruchu sieciowego wysyłanego i odbieranego przez protokół IPv6. Ruch internetowy IPv6 jest blokowany, gdy aktywny jest VPN. Na urządzeniach, które obsługują tylko protokół IPv6, Kaspersky VPN nie może ustanowić szyfrowanego połączenia i chronić ruchu sieciowego.

- Jeśli połączenie IPv6 zostało nawiązane przed włączeniem VPN, ruch sieciowy IPv6 nie zostanie zablokowany przez krótki czas.

Źródła informacji o aplikacji

Strona programu Kaspersky VPN na witrynie Kaspersky

Na stronie internetowej Kaspersky VPN na witrynie Kaspersky możesz przejrzeć ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona Kaspersky VPN w Bazie wiedzy

Baza wiedzy to sekcja na stronie działu obsługi klienta Kaspersky.

Na stronie internetowej Kaspersky VPN w Bazie wiedzy możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły w Bazie wiedzy mogą zawierać odpowiedzi na pytania dotyczące programu Kaspersky VPN i innych aplikacji Kaspersky. Artykuły w Bazie wiedzy mogą także zawierać nowości z działu obsługi klienta.

Otwieranie strony Bazy wiedzy z poziomu menu rozwijalnego Pomocy

Choose **Pomoc** > **Obsługa klienta**.

Porozmawiaj o aplikacjach Kaspersky na Forum pomocy technicznej Kaspersky

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je ze specjalistami z firmy Kaspersky Lab lub innymi użytkownikami jej oprogramowania na forum.

Na tym forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

Otwieranie strony Forum z poziomu menu rozwijalnego Pomocy

Wybierz **Pomoc** > **Forum**.

Uwaga: Do korzystania z zasobów strony internetowej konieczne jest połączenie internetowe.

Jeżeli nie znajdziesz rozwiązania problemu, skontaktuj się z działem obsługi klienta.

Informacje prawne

Przeglądanie warunków Umowy licencyjnej i Oświadczenia marketingowego

Warunki Umowy licencyjnej możesz sprawdzić:

- W sklepie App Store
- W pliku license.txt, dostępnym w folderze, w którym zainstalowano aplikację

Przeczytaj Oświadczenie marketingowe i wyłącz wysyłanie danych

1. Na pasku menu kliknij ikonę aplikacji i wybierz **Ustawienia**.

   Zostanie otwarte okno ustawień aplikacji.

2. W sekcji **Ulepszona użyteczność** kliknij **Pokaż Oświadczenie marketingowe**, jeśli chcesz przeczytać warunki Oświadczenia marketingowego.

   Zostanie otwarte okno zawierające Oświadczenie marketingowe.

3. Jeśli chcesz wyłączyć wysyłanie danych, odznacz pole **Pomóż firmie Kaspersky ulepszać produkty wysyłając informacje dotyczące aplikacji i środowiska, w którym ona działa**.

Informacje o kodzie firm trzecich

Informacje o kodzie firm trzecich znajduje się w pliku legal_notices.txt, w folderze, w którym zainstalowano aplikację.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

App Store, Apple, Finder, iCloud, iTunes, Launchpad, Mac, macOS, OS X i Touch ID są zastrzeżonymi znakami towarowymi firmy Apple Inc., zarejestrowanymi na terenie Stanów Zjednoczonych i innych krajów i regionów.

IOS jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Cisco Systems, Inc. i/lub jej oddziałów, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Android, Firebase, Google i Google Play są znakami towarowymi firmy Google LLC.

Microsoft i Windows są znakami towarowymi grupy firm Microsoft.

JavaScript jest zastrzeżonym znakiem towarowym firmy Oracle i/lub jej oddziałów.

Intel jest zastrzeżonym znakiem towarowym firmy Intel Corporation na terenie Stanów Zjednoczonych i/lub innych krajów.

Okno „Utwórz konto My Kaspersky”

Pole Wprowadź adres e-mail

Adres e-mail, który chcesz użyć ze swoim nowym kontem My Kaspersky.

Ten adres e-mail jest używany do odzyskiwania hasła i otrzymywania wiadomości od Kaspersky.

Pole Określ hasło

Hasło do nowego konta My Kaspersky. Hasło musi zawierać minimum osiem znaków, w tym przynajmniej jedną cyfrę, jedną małą literę oraz jedną dużą literę. Hasło nie może zawierać spacji.

Pole Potwierdź hasło

Potwierdzenie hasła do nowego konta My Kaspersky.

Domyślnie znaki hasła są ukryte ze względów bezpieczeństwa. Aby wyświetlić hasło, kliknij ikonę oka .

Menu wyskakujące wyboru kraju

Menu wyskakujące, z którego możesz wybrać kraj dla My Kaspersky. Ta opcja określa ustawienia regionalne dla Twojego konta My Kaspersky, na przykład, język wyświetlania i dostępne aplikacje firmy Kaspersky. Będziesz mógł zmienić region dla swojego konta My Kaspersky w późniejszym czasie tylko poprzez skontaktowanie się z działem obsługi klienta.

Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki Polityki prywatności opisującej zasady przetwarzania danych

Jeśli to pole jest zaznaczone, oznacza to, że wyrażasz zgodę na warunki Polityki prywatności, co opisuje sposób zarządzania danymi.

Uwaga: Przycisk **Utwórz** stanie się dostępny tylko wtedy, gdy potwierdzisz, że przeczytałeś, rozumiesz i akceptujesz Politykę prywatności.

Wyrażam zgodę na udostępnienie firmie Kaspersky mojego adresu e-mail w celu otrzymywania spersonalizowanych ofert marketingowych

To pole włącza/wyłącza otrzymywanie wiadomości e-mail z informacjami i promocjami od Kaspersky.

Utwórz

Kliknięcie tego przycisku spowoduje utworzenie nowego konta My Kaspersky.

Okno „Zaloguj się do My Kaspersky”

Zaloguj się przez konto Google

Kliknięcie tego przycisku spowoduje otwarcie okna przeglądarki, w którym możesz zalogować się do My Kaspersky za pośrednictwem konta Google.

Zaloguj się przez konto Facebook

Kliknięcie tego przycisku spowoduje otwarcie okna przeglądarki, w którym możesz zalogować się do My Kaspersky za pośrednictwem konta Facebook.

Uwaga: Dostępność opcji logowania za pośrednictwem Facebooka zależy od regionu.

Zaloguj się przez konto Apple

Kliknięcie tego przycisku spowoduje otwarcie okna systemowego, w którym możesz zalogować się do My Kaspersky za pośrednictwem konta Apple.

Pole Adres e-mail

Adres e-mail powiązany z kontem My Kaspersky.

Pole Hasło

Hasło do konta My Kaspersky.

Domyślnie znaki hasła są ukryte ze względów bezpieczeństwa. Aby wyświetlić hasło, kliknij ikonę oka .

Nie pamiętasz hasła?

Kliknięcie tego odnośnika otwiera okno przeglądarki, gdzie można zresetować hasło do konta My Kaspersky.

Zaloguj

Kliknięcie tego przycisku spowoduje połączenie Kaspersky VPN z My Kaspersky.

Utwórz konto

Kliknięcie tego przycisku otwiera okno, w którym można utworzyć konto My Kaspersky.

Zakładka „Ogólne”

W sekcji **Uruchom w tle** możesz skonfigurować, czy Kaspersky VPN będzie uruchamiany w tle, a także nawiązać bezpieczne połączenie od razu po uruchomieniu komputera Mac.

Pozwól Kaspersky VPN na działanie w tle (zalecane)

To pole włącza/wyłącza działanie Kaspersky VPN w tle.

Włącz VPN automatycznie po uruchomieniu komputera Mac

To pole włącza/wyłącza nawiązanie bezpiecznego połączenia od razu po uruchomieniu komputera Mac.

To pole jest dostępne, jeśli pole **Pozwól Kaspersky VPN na działanie w tle (zalecane)** jest zaznaczone.

W sekcji **Ulepszona użyteczność** możesz przeczytać warunki Oświadczenia marketingowego i wyrazić zgodę lub ją odrzucić na wysyłanie informacji wymienionych w Oświadczeniu marketingowym do Kaspersky.

Pomóż firmie Kaspersky ulepszać produkty wysyłając informacje dotyczące aplikacji i środowiska, w którym ona działa

To pole włącza/wyłącza wysyłanie informacji wymienionych w Oświadczeniu marketingowym do Kaspersky.

Pokaż Oświadczenie marketingowe

Kliknięcie tego odnośnika spowoduje otwarcie okna zawierającego treść Oświadczenia marketingowego.

Zakładka „Dzielone tunelowanie”

W zakładce **Dzielone tunelowanie** można skonfigurować włączenie połączenia VPN tylko dla wybranych aplikacji.

Uwaga: Dzielone tunelowanie jest dostępne tylko w wersji Unlimited programu Kaspersky VPN.

Uruchom VPN tylko dla wybranych aplikacji

To pole włącza/wyłącza Dzielone tunelowanie. Gdy włączone jest Dzielone tunelowanie, tylko wybrane aplikacje z poniższej listy będą się łączyć przez VPN, podczas gdy inne aplikacje będą się łączyć bezpośrednio z Internetem.

Domyślnie pole to jest odznaczone.

Zakładka „Kill Switch”

W zakładce **Kill Switch** możesz skonfigurować, czy Twoje dane będą chronione, gdy połączenie VPN zostanie zerwane.

Uwaga: Kill Switch jest dostępny tylko w wersji Unlimited programu Kaspersky VPN.

Włącz Kill Switch

To pole włącza/wyłącza Kill Switch. Kill Switch przerywa przesyłanie danych przez internet, gdy następuje ponowne nawiązanie połączenia z VPN. Twoje połączenie z internetem zostanie przywrócone po włączeniu VPN.

Domyślnie pole to jest odznaczone.

Zakładka „Niezabezpieczona sieć Wi-Fi”

W zakładce **Niezabezpieczona sieć Wi-Fi** można wybrać działanie, które Kaspersky VPN wykona podczas nawiązywania połączenia z niezabezpieczona siecią Wi-Fi.

Wykryj niezabezpieczone sieci Wi-Fi

To pole włącza/wyłącza wykrywanie niezabezpieczonych sieci Wi-Fi.

Włącz wykrywanie w chmurze za pomocą Kaspersky Security Network

To pole włącza/wyłącza wykrywanie niezabezpieczonych sieci Wi-Fi przy pomocy Kaspersky Security Network. Jeśli zaznaczasz to pole po raz pierwszy, będziesz musiał włączyć Usługi lokalizacji dla Kaspersky VPN.

Uwaga: System macOS wymaga włączenia usług lokalizacji, aby Kaspersky VPN mógł uzyskać nazwę sieci Wi-Fi (BSSID). Kaspersky Security Network wykorzysta ją do wykrycia niezabezpieczonych sieci Wi-Fi. Nie będą one używane do określenia Twojej prawdziwej lokalizacji

Unselecting this checkbox revokes your acceptance of the Unsecured Wi-Fi Network Cloud Detection Statement.

Pytaj o akcję

Kaspersky VPN wyświetli monit o wybranie akcji po nawiązaniu połączenia z niezabezpieczoną siecią Wi-Fi.

Akcja ta jest wybrana domyślnie.

Automatycznie włącz VPN

Po połączeniu z niezabezpieczoną siecią Wi-Fi program Kaspersky VPN automatycznie włącza VPN.

Nazwa sieci

Ta kolumna wyświetla nazwę sieci Wi-Fi.

Ostatnie połączenie

Ta kolumna wyświetla datę ostatniego połączenia z siecią Wi-Fi.

Po podłączeniu do sieci Wi-Fi

Ta kolumna wyświetla działanie, jakie Kaspersky VPN wykonuje po podłączeniu do sieci Wi-Fi:

Nie określono

Jeśli określona sieć Wi-Fi jest niezabezpieczona, aplikacja stosuje ustawienia określone dla niezabezpieczonych sieci Wi-Fi. Jeśli określona sieć jest zabezpieczona, aplikacja nic nie zrobi.

Włącz VPN

Aplikacja włącza VPN po podłączeniu komputera Mac do określonej sieci Wi-Fi.

Nie wykonuj żadnych akcji

Aplikacja nie włącza VPN po podłączeniu komputera Mac do określonej sieci Wi-Fi.

Okno „Twoje konto jest prawie gotowe”

Menu wyskakujące wyboru regionu

Menu wyskakujące, z którego możesz wybrać region dla My Kaspersky. Ta opcja określa ustawienia regionalne dla Twojego konta My Kaspersky, na przykład, język wyświetlania i dostępne aplikacje firmy Kaspersky. Będziesz mógł zmienić region dla swojego konta My Kaspersky w późniejszym czasie tylko poprzez skontaktowanie się z działem obsługi klienta.

Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki Polityki prywatności opisującej zasady przetwarzania danych

Jeśli to pole jest zaznaczone, oznacza to, że wyrażasz zgodę na warunki Polityki prywatności, co opisuje sposób zarządzania danymi.

Wyrażam zgodę na udostępnienie firmie Kaspersky mojego adresu e-mail w celu otrzymywania spersonalizowanych ofert marketingowych

To pole włącza/wyłącza otrzymywanie wiadomości e-mail z informacjami i promocjami od Kaspersky.

Utwórz

Kliknięcie tego przycisku spowoduje utworzenie nowego konta My Kaspersky.

Okno dialogowe „Serwer proxy wymaga uwierzytelniania”

Nazwa użytkownika

Pole służące do wprowadzenia nazwy użytkownika, który łączy się z serwerem proxy.

Hasło

Pole służące do wprowadzenia hasła.

Zapamiętaj hasło

To pole włącza/wyłącza użycie określonej nazwy użytkownika i hasła do autoryzacji na serwerze proxy.

Domyślnie pole to jest odznaczone.