# NOKIA 9300i

9243058
Wydanie 1 PL

# Klient VPN
# Instrukcja obsługi

9243058

Wydanie 1

# Spis treści


**Wirtualne sieci prywatne ..... 5**

Porządkowanie wirtualnych sieci prywatnych ..... 5
Instalowanie programu Klient VPN ..... 6
Wymagania systemowe ..... 6
Porządkowanie zasad VPN ..... 6
Instalowanie zasad VPN z serwera zasad VPN ..... 7
Instalowanie zasad VPN z plików SIS ..... 7
Wyświetlanie zasad VPN ..... 8
Sprawdzanie stanu zasad ..... 8
Sprawdzanie stanu certyfikatów ..... 9
Aktualizowanie zasad VPN ..... 9
Usuwanie zasad VPN ..... 9
Porządkowanie serwerów zasad VPN ..... 10
Nawiązywanie połączenia z serwerami zasad VPN ..... 10
Instalowanie ustawień z plików SIS ..... 10
Dodawanie serwerów zasad VPN ..... 11
Edytowanie serwerów zasad VPN ..... 12
Synchronizowanie serwerów zasad VPN ..... 13
Rejestrowanie certyfikatów VPN ..... 13
Usuwanie serwerów zasad VPN ..... 13
Porządkowanie punktów dostępu VPN ..... 14
Wyświetlanie rejestru VPN ..... 15
Hasła magazynu kluczy ..... 15
Tworzenie lub zmiana hasła magazynu kluczy ..... 15
Wprowadzanie haseł magazynu kluczy ..... 16
Korzystanie z sieci VPN przy użyciu aplikacji ..... 16
Uwierzytelnianie w bramach VPN ..... 16
Rozwiązywanie problemów ..... 17

**Skorowidz ..... 19**

# Wirtualne sieci prywatne

**Wirtualne sieci prywatne** (Virtual Private Network, VPN) umożliwiają tworzenie zaszyfrowanych połączeń ze źródłami informacji, które dzięki temu stają się dostępne dla pracowników przebywających poza swoim miejscem pracy. Dzięki zaszyfrowanym połączeniom z siecią firmową użytkownik pozostaje dostępny, mogąc korzystać z poczty elektronicznej, aplikacji baz danych oraz intranetu.

Zdalne połączenia z sieciami komputerowymi muszą być chronione. W tym celu firma może używać technologii VPN do tunelowania ruchu oraz do wymuszania odpowiedniej polityki zabezpieczeń. Technologia VPN pomaga zapewnić bezpieczeństwo i spójność transakcji sieciowych, umożliwiając uwierzytelnianie i autoryzację użytkowników przy dostępie do sieci i usług sieciowych.

Aby utworzyć sieć VPN, brama oraz urzšdzenie dokonują wzajemnego uwierzytelnienia oraz negocjują algorytmy szyfrowania i uwierzytelniania w celu zapewnienia prywatności i spójności udostępnianych danych.

## Porządkowanie wirtualnych sieci prywatnych

Aby móc korzystać z połączeń VPN, należy najpierw utworzyć punkty dostępu VPN, a następnie wybrać te punkty dostępu podczas prób łączenia się z firmą przy użyciu aplikacji. Połączenie VPN z siecią firmową jest tworzone na bazie innego połączenia z punktem dostępu do internetu. Połączenie jest tworzone i szyfrowane zgodnie z zasadami polityki VPN, które są pobierane podczas łączenia się z punktem dostępu VPN.

**Aby skorzystać z wirtualnej sieci prywatnej**

1 Zainstaluj program Klient VPN.
Aby uzyskać więcej informacji, patrz "Instalowanie programu Klient VPN" na stronie 6.

2 Określ połączenie z serwerem zasad VPN.
Ustawienia serwera zasad VPN można określić w oknie dialogowym *Zarządzanie VPN* lub też zainstalować je z pliku SIS (Symbian Installation System).
Aby uzyskać więcej informacji, patrz "Nawi±zywanie po³±czenia z serwerami zasad VPN" na stronie 10.

**Uwaga:** Jeśli zasady VPN są instalowane z plików SIS, nie jest konieczne tworzenie połączeń z serwerami zasad VPN.

3 Zainstaluj zasady VPN z serwera zasad VPN.
Aby uzyskać więcej informacji, patrz "Instalowanie zasad VPN z serwera zasad VPN" na stronie 6.

4 Utwórz punkty dostępu VPN.
Punkty dostępu VPN określają punkt dostępu do internetu oraz zasady VPN.

**Uwaga:** Punkty dostępu VPN stanowią połączenie zasad VPN oraz punktów dostępu do internetu. Podczas odbywającej się po raz pierwszy synchronizacji serwera zasad VPN dla każdej zasady zainstalowanej na urzšdzeniu są tworzone odpowiadające im punkty dostępu VPN.

Aby uzyskać więcej informacji o tworzeniu i wybieraniu punktów dostępu VPN, patrz "Porz±dkowanie punktów dostêpu VPN" na stronie 14.

5 Wybierz punkt dostępu VPN, jeśli zamierzasz łączyć się z siecią firmową za pośrednictwem aplikacji. Aby uzyskać więcej informacji, patrz "Korzystanie z sieci VPN przy u¿yciu aplikacji" na stronie 16. Połączenie VPN jest tworzone jako nakładka na połączenie z punktem dostępu do internetu.

# Instalowanie programu Klient VPN

Program Klient VPN jest dostarczany klientom w postaci standardowego pliku SIS. Program Klient VPN jest instalowany w urzšdzeniu w identyczny sposób jak pozostałe oprogramowanie. Więcej informacji o instalowaniu oprogramowania na urzšdzeniu można znaleźć w dokumentacji urzšdzenia.

Po zakończeniu instalacji plik SIS z programem Klient VPN nie będzie już potrzebny. Można usunąć plik SIS, aby zwolnić pamięć.

## Wymagania systemowe

Oprogramowanie klienta VPN można zainstalować na karcie pamięci lub w pamięci urządzenia. Aby program klienta VPN mógł działać, w urządzeniu musi znajdować się karta pamięci.

Podczas instalacji programu Klient VPN w urzšdzeniu musi być dostępne co najmniej 1,5 MB pamięci.

Po zainstalowaniu program Klient VPN rezerwuje 900 KB pamięci urzšdzenia lub karty pamięci. Każda zasada VPN wymaga przeciętnie od 1 KB to 16 KB pamięci urzšdzenia.

# Porządkowanie zasad VPN

Zasady VPN definiują metodę używaną przez program Klient VPN i bramę VPN do wzajemnego uwierzytelniania oraz algorytm szyfrowania, który jest używany do zapewnienia poufności danych. Administratorzy tworzą zasady VPN oraz przechowują je na serwerze zasad VPN lub też przekazują użytkownikom w postaci plików SIS. Użytkownik instaluje zasady VPN z serwera zasad VPN, używając okna dialogowego *Zarządzanie VPN*.

## Instalowanie zasad VPN z serwera zasad VPN

W oknie dialogowym *Zarządzanie VPN* użytkownik może zainstalować zasady VPN z serwera zasad VPN.

**Porada!** Serwery zasad VPN są serwerami znajdującymi się w sieci firmowej, na których przechowywane są zasady VPN.

**Aby zainstalować zasady VPN**

1. Przejdź do okna dialogowego *Narzędzia* > *Panel sterowania* > *Połączenia* > *Zarządzanie VPN*.
2. Naciśnij przycisk *Tak*, gdy w oknie dialogowym *Zarządzanie VPN* wyświetlone zostanie pytanie o zainstalowanie zasad VPN.
3. Naciśnij ponownie przycisk *Tak*, aby dodać serwery zasad VPN.
4. Podaj ustawienia połączenia z serwerem zasad VPN i naciśnij przycisk *Gotowe*.
   Aby uzyskać więcej informacji, patrz "Nawi±zywanie po³±czenia z serwerami zasad VPN" na stronie 10.
5. Naciśnij przycisk *Tak*, aby zsynchronizować serwer zasad VPN.
6. Utwórz hasło magazynu kluczy i naciśnij przycisk *OK*.

   **Porada!** Hasło magazynu kluczy chroni przed nieautoryzowanym dostępem klucze prywatne stosowane przez zasady VPN oraz używane podczas połączeń z serwerami zasad VPN.

   Aby uzyskać więcej informacji, patrz "Tworzenie lub zmiana has³a magazynu kluczy" na stronie 15.
   Komunikator łączy się z serwerem zasad VPN.
7. Sprawdź kod tożsamości serwera zasad VPN i wprowadź brakujące znaki w celu ustanowienia zaufania pomiędzy urzšdzeniem i serwerem zasad VPN, a następnie naciśnij przycisk *OK*.
   Można pominąć tę czynność, jeśli ustawienia serwera zasad VPN są instalowane z pliku SIS.

   **Porada!** Kod tożsamości serwera zasad VPN jest "odciskiem palca" certyfikatu serwera zasad VPN, który służy do identyfikacji tego certyfikatu.

   Aby uzyskać więcej informacji, patrz "Dodawanie serwerów zasad VPN" na stronie 11.
8. Wprowadź dane uwierzytelniające umożliwiające dostęp do serwera zasad VPN i naciśnij przycisk *OK*.
   Informacje, które należy wprowadzić, można uzyskać od administratora.

Zasady VPN zostają zainstalowane na urzšdzeniu.

**Uwaga:** Naciśnięcie przycisku Anuluj spowoduje rezygnację z instalowania zasad VPN. Wybierz przycisk Instaluj, aby zainstalować zasady VPN z serwera zasad VPN.

## Instalowanie zasad VPN z plików SIS

Administrator może dostarczyć zasady VPN w postaci plików SIS. Jeśli zasady VPN są instalowane z plików SIS, nie jest konieczne definiowanie połączeń z serwerami zasad VPN. Po zainstalowaniu zasad VPN użytkownik może utworzyć punkty dostępu VPN i powiązać je z aplikacjami.

Jeśli zasady VPN zawierają klucze prywatne oraz odpowiadające im certyfikaty, administratorzy definiują **hasła importu kluczy** w celu ochrony kluczy prywatnych. Administratorzy powinni dostarczać użytkownikom hasła importu kluczy z wykorzystaniem bezpiecznych metod.

**Porada!** Hasło importu kluczy służy do ochrony kluczy prywatnych znajdujących się w pliku zasad VPN.

**Aby zainstalować zasady VPN z pliku SIS,** wpisz hasło importu klucza w polu *Hasło* i naciśnij przycisk *OK*. Następnie w polu *Hasło* wpisz hasło magazynu kluczy i naciśnij przycisk *OK*.

## Wyświetlanie zasad VPN

W oknie dialogowym *Zarządzanie VPN* można wyświetlać, aktualizować i usuwać zasady VPN zainstalowane w urządzeniu.

**Aby wyświetlić szczegółowe informacje o zasadach VPN,** wybierz zasadę VPN i naciśnij przycisk *Otwórz* w celu wyświetlenia informacji.

Przewiń okno, aby wyświetlić następujące informacje o każdej z zasad VPN:

- W polu *Opis* wyświetlane są dodatkowe informacje o danej zasadzie VPN. Opis ten jest odczytywany z zasady VPN. Administratorzy definiują opis podczas tworzenia zasady VPN.
- *Stan zasad* wskazuje, czy zasada VPN jest gotowa do użycia, czy też nie, lub też czy jest aktualnie używana.
- *Stan certyfikatów* wskazuje, czy w urzsdzeniu dostępne są prawidłowe certyfikaty użytkownika.
- *Nazwa zasad* wskazuje nazwę zasady VPN. Administratorzy definiują tę nazwę podczas tworzenia zasady VPN.
- *Nazwa serwera zasad* wskazuje nazwę serwera zasad VPN, z którego zainstalowana została zasada VPN. Użytkownik nadaje nazwy serwerom zasad VPN podczas definiowania połączeń z serwerami zasad VPN. Pole to pozostaje ukryte, jeśli zasada VPN została zainstalowana z pliku SIS.
- *Zaktualizowano* zawiera datę ostatniej aktualizacji zasady VPN na żądanie serwera zasad VPN. Pole to pozostaje ukryte, jeśli zasada VPN została zainstalowana z pliku SIS.

### Sprawdzanie stanu zasad

*Stan zasad* może przybierać następujące wartości:

*Aktywny* - użytkownik utworzył połączenie z punktem dostępu VPN, który jest powiązany z zasadą VPN. Po utworzeniu połączenia zasada VPN staje się aktywna.

*Skojarzono z punktem dostępu VPN* - użytkownik skojarzył zasadę VPN z jednym lub kilkoma punktami dostępu VPN. W celu aktywowania zasady VPN użytkownik może wybrać dowolny z punktów dostępu VPN.

*Nie skojarzono z punktem dostępu VPN* - aby aktywować zasadę VPN, użytkownik musi skojarzyć zasadę VPN z punktem dostępu VPN.

**Uwaga:** Jeśli widok szczegółów zasad VPN pozostawał otwarty podczas zmiany stanu zasad, nie zostanie on odświeżony.

### Sprawdzanie stanu certyfikatów

*Stan certyfikatów* może przybierać następujące wartości:

*OK* - w urzšdzeniu dostępny jest co najmniej jeden prawidłowy certyfikat lub też użytkownik nie używa certyfikatów do uwierzytelniania w bramach VPN.

*Nieważny* - skończył się okres ważności jednego lub kilku certyfikatów. Jeśli nie można utworzyć połączenia VPN, należy zaktualizować zasadę VPN w celu dołączenia nowych certyfikatów.

*Brak* - w urzšdzeniu nie można odszukać jednego lub kilku wymaganych certyfikatów. Jeśli nie można utworzyć połączenia VPN, spróbuj zaktualizować zasadę VPN, aby dołączyć nowe certyfikaty.

*Jeszcze nieważny* - jeden lub kilka certyfikatów jest przeznaczonych do wykorzystania w przyszłości. Wartość ta może również oznaczać, że data i godzina ustawiona w urzšdzeniu wskazuje przeszłość, strefa czasowa jest ustawiona nieprawidłowo lub też włączono czas letni.

**Aby usunąć zasadę VPN,** naciśnij przycisk *Delete*.

**Aby zamknąć widok szczegółów zasad VPN,** naciśnij przycisk *Zamknij*.

## Aktualizowanie zasad VPN

Podczas tworzenia połączenia z punktem dostępu VPN program Klient VPN sprawdza na serwerze zasad VPN stan zasady VPN, która jest powiązana z tym punktem dostępu VPN. Jeśli administrator utworzył nową wersję zasady VPN, zostaje ona zainstalowana na urzšdzeniu. Jeśli administrator usunął zasadę VPN z serwera zasad VPN, zostaje ona usunięta z urzšdzenia.

Zmiany stają się obowiązujące podczas następnego tworzenia połączenia z punktem dostępu VPN, a zatem nie wpływają na bieżące połączenie VPN.

Aktualizacji zasady VPN można również dokonać w oknie dialogowym *Zarządzanie VPN*.

**Aby zaktualizować zasadę VPN,** wybierz tę zasadę i naciśnij przycisk *Aktualizuj*. Program Klient VPN sprawdzi stan zasady VPN zapisany na serwerze zasad VPN.

## Usuwanie zasad VPN

Zasady VPN są usuwane automatycznie po usunięciu ich z przez administratora z serwera zasad VPN lub też po dokonanej przez użytkownika aktualizacji zasady VPN lub synchronizacji serwera zasad VPN.

Jeśli w oknie dialogowym *Zarządzanie VPN* usunięto zasadę VPN, która nadal znajduje się na serwerze zasad VPN, zasada ta zostanie zainstalowana ponownie podczas synchronizacji zasad z serwerem zasad VPN.

**Aby usunąć zasadę VPN,** zaznacz tę zasadę i naciśnij kombinację klawiszy Ctrl + *D*.

Nie można używać punktu dostępu VPN, jeśli usunięto skojarzoną z nim zasadę VPN.

# Porządkowanie serwerów zasad VPN

Za pomocą funkcji *Serwery zasad* użytkownik może zainstalować zasady z serwerów zasad VPN. Podczas tworzenia połączenia z punktem dostępu VPN komunikator łączy się z serwerem zasad VPN w celu automatycznej aktualizacji zasady VPN powiązanej z tym punktem dostępu VPN. Aby zaktualizować wszystkie zasady VPN, należy zsynchronizować serwery zasad VPN z urzšdzeniem.

## Nawiązywanie połączenia z serwerami zasad VPN

Przez zainstalowanie zasad VPN z serwera zasad VPN użytkownik tworzy relację zaufania między urzšdzeniem a serwerem zasad VPN. Aby utworzyć relację zaufania, użytkownik musi dokonać uwierzytelnienia serwera zasad VPN, zaś serwer zasad VPN musi dokonać uwierzytelnienia użytkownika.

Po dokonaniu uwierzytelnienia użytkownika przez serwer zasad VPN program Klient VPN generuje klucz prywatny i pobiera przeznaczony dla użytkownika certyfikat. Klucz prywatny i certyfikat są przechowywane w magazynie kluczy w urzšdzeniu. Certyfikat uwierzytelnia użytkownika wobec serwera zasad VPN.

**Porada!** Administrator może dostarczyć użytkownikowi plik SIS zawierający ustawienia określające połączenie z serwerem zasad VPN lub też użytkownik może dodać serwer zasad VPN w oknie dialogowym *Zarządzanie VPN*.

## Instalowanie ustawień z plików SIS

Użytkownik może zainstalować ustawienia serwera zasad VPN na serwerze zasad VPN, posługując się plikiem SIS. Ustawienia są instalowane na urzšdzeniu w taki sam sposób jak inne oprogramowanie.

Na ustawienia składają się: adres oraz certyfikat serwera zasad VPN. Dzięki certyfikatowi serwera komunikator może zaufać serwerowi zasad VPN, dzięki czemu użytkownikowi pozostaje tylko podanie swojej nazwy i hasła w celu potwierdzenia tożsamości.

Plik SIS nie zawiera ustawień dla punktu dostępu do internetu, który służy do łączenia się z serwerem zasad VPN. Aby określić punkt dostępu do internetu, użytkownik musi dokonać edycji ustawień serwera zasad VPN. Użytkownik może również wybrać punkt dostępu do internetu podczas łączenia się z serwerem zasad VPN.

Jeśli administrator nie podpisał pliku SIS, podczas instalacji pliku wyświetlane jest ostrzeżenie dotyczące bezpieczeństwa. Można zignorować to ostrzeżenie, jeśli plik SIS został na pewno otrzymany od administratora.

Przed instalacją ustawień z pliku SIS należy zamknąć okno dialogowe *Zarządzanie VPN*, gdyż w przeciwnym przypadku instalacja nie powiedzie się.

## Dodawanie serwerów zasad VPN

Jeśli nie zainstalowano ustawień serwera zasad VPN z pliku SIS, można je podać w oknie dialogowym *Serwery zasad*.

Podczas łączenia się po raz pierwszy z adresem serwera zasad VPN komunikator nie ufa jeszcze serwerowi zasad VPN i użytkownik musi uwierzytelnić serwer zasad VPN. Użytkownik otrzymuje kod tożsamości serwera zasad VPN od administratora. Użytkownik sprawdza i uzupełnia kod tożsamości serwera zasad VPN, a program Klient VPN weryfikuje go.

Po pomyślnym uwierzytelnieniu program Klient VPN pobiera certyfikat z serwera zasad VPN w celu późniejszego uwierzytelnienia się wobec serwera zasad VPN.

**Aby dodać serwer zasad VPN,** naciśnij przycisk *Nowy*. Wprowadź następujące ustawienia:

- *Nazwa serwera zasad* – możesz wybrać dowolną nazwę, unikalną w obrębie pola *Serwery zasad VPN*. Jeśli pole to pozostanie puste, zostanie w nie wstawiony *Adres serwera zasad*. Nazwa serwera zasad jest wyświetlana na liście serwerów zasad VPN oraz na pasku tytułu okna dialogowego służącego do zmiany ustawień serwera zasad VPN.
- *Adres serwera zasad* – nazwa hosta lub adres IP serwera zasad VPN, z którego instalowane są zasady VPN. Można również podać numer portu oddzielony dwukropkiem (:). Adres serwera zasad można otrzymać od administratora.
- *Punkt dostępu do internetu* – punkt dostępu do internetu używany do łączenia się z danym serwerem zasad VPN. Od administratora można uzyskać informację o punkcie dostępu, który należy wybrać.

**Aby zainstalować zasady VPN z serwera zasad VPN,** naciśnij przycisk *Tak*, gdy okno dialogowe *Zarządzanie VPN* wyświetli zachętę do synchronizacji serwera zasad VPN.

**Porada!** Synchronizowanie oznacza, że program Klient VPN nawiązuje połączenie z serwerem zasad VPN w celu sprawdzenia, czy znajdują się na nim nowe lub zaktualizowane zasady, albo czy usunięto z niego jakieś zasady, a następnie instaluje zasady VPN na urzśdzeniu.

Podczas łączenia się po raz pierwszy z serwerem zasad VPN o podanym adresie serwer ten nie jest zaufany i użytkownik musi go uwierzytelnić. Użytkownik otrzymuje kod tożsamości serwera zasad VPN od administratora.

**Aby zweryfikować tożsamość serwera zasad VPN,** porównaj dokładnie kod tożsamości serwera zasad VPN wyświetlony w oknie dialogowym *Kod tożsamości serwera zasad VPN* z kodem otrzymanym od administratora, wpisz

brakujące znaki w polu *Brakujące znaki* i naciśnij przycisk *OK*.

**Uwaga:** Jeśli ustawienia serwera zasad VPN są instalowane z pliku SIS, weryfikacja tożsamości serwera VPN nie jest konieczna i widok ten nie jest nigdy wyświetlany.

**Aby dokonać uwierzytelnienia serwera zasad VPN,** wpisz nazwę użytkownika w polu *Nazwa użytkownika serwera zasad* oraz hasło w polu *Hasło serwera zasad*, a następnie naciśnij przyisk *OK* w oknie dialogowym *Uwierzytelnianie serwera zasad VPN*.

Nazwę i hasło użytkownika, które należy wpisać, można uzyskać od administratora.

**Porada!** Nazwa i hasło użytkownika serwera zasad chronią serwer zasad VPN przed nieautoryzowanym dostępem.

Program Klient VPN rejestruje certyfikat w celu przyszłego uwierzytelnienia na serwerze zasad VPN i instaluje zasady VPN w urzšdzeniu.

**Porada!** Rejestracja certyfikatu polega na wysłaniu żądania certyfikacji do urzędu certyfikacji i otrzymaniu certyfikatu.

Od tego momentu można tworzyć punkty dostępu VPN i wiązać je z aplikacjami.

## Edytowanie serwerów zasad VPN

W oknie dialogowym *Serwery zasad* użytkownik może wyświetlać, edytować, synchronizować i usuwać serwery zasad VPN.

**Aby wyświetlić lub zmienić ustawienia serwera zasad VPN,** zaznacz serwer zasad VPN i naciśnij przycisk *Edytuj* w celu dokonania zmian następujących ustawień:

- *Nazwa serwera zasad* - nazwa nadana serwerowi zasad. Nowa nazwa wyświetlona zostaje w polu *Serwery zasad*.
- *Punkt dostępu do internetu* - punkt dostępu do internetu używany do łączenia się z danym serwerem zasad VPN. Jeśli usunięto punkt dostępu powiązany z serwerem zasad VPN, w polu *Punkt dostępu do internetu* wyświetlany jest tekst *(nie wybrano)*. Jeśli usunięto wszystkie punkty dostępu, w oknie dialogowym *Zarządzanie VPN* nie można zapisać ustawień.

Po zainstalowaniu zasad VPN z serwera zasad VPN nie można zmienić wartości w polu *Adres serwera zasad*, ponieważ podczas pierwszego połączenia serwer zasad VPN wysyła ten adres do okna dialogowego *Zarządzanie VPN*.

**Aby usunąć serwer zasad VPN,** naciśnij przycisk *Usuń*.

**Aby zapisać ustawienia,** naciśnij przycisk *Gotowe*.

**Porada!** Aby zamknąć widok bez zapisywania zmian, naciśnij klawisz Esc.

## Synchronizowanie serwerów zasad VPN

**Aby zainstalować zasady z serwera zasad VPN i dokonać ich aktualizacji,** zaznacz serwer aktualizacji i naciśnij przycisk *Synchronizuj*. Program Klient VPN nawiązuje połączenie z serwerem zasad VPN w celu sprawdzenia, czy administrator dodał, zaktualizował lub usunął zasady VPN.

Jeśli serwer zasad VPN zawiera nowe zasady VPN lub nową wersję zasad VPN, są one instalowane w urzšdzeniu. Jeśli administrator usunął zasady VPN z serwera zasad VPN, zasady te są usuwane z urzšdzenia.

**Uwaga:** Podczas pierwszej synchronizacji serwera zasad VPN dla każdej zasady zainstalowanej w urzšdzeniu jest tworzony odpowiadający jej punkt dostępu VPN. Punkty dostępu VPN stanowią połączenie zasad VPN oraz punktów dostępu do internetu.

Podczas łączenia się z serwerem zasad VPN w celu zainstalowania lub zaktualizowania zasad VPN może zajść potrzeba zarejestrowania certyfikatów VPN z serwera zasad VPN.

## Rejestrowanie certyfikatów VPN

Program Klient VPN tworzy żądanie certyfikatu dla każdego wymaganego certyfikatu i wysyła je do serwera zasad VPN. Serwer zasad VPN rejestruje każdy wymagany certyfikat w **urzędzie certyfikacji** i zwraca go do programu Klient VPN.

Żądanie certyfikacji oraz odpowiadający mu certyfikat zawierają informacje określające tożsamość użytkownika. W zależności od konfiguracji serwera zasad VPN jako tożsamości użytkownika w certyfikacie VPN można użyć tożsamości użytkownika tego serwera. Jeśli nie jest to możliwe, w oknie dialogowym *Zarządzanie VPN* pojawia się pytanie o tożsamość użytkownika w danej domenie. Informacje, które należy wprowadzić, można uzyskać od administratora.

**Aby utworzyć żądania certyfikatów,** w oknie dialogowym *Tożsamość użytkownika VPN* należy w polu *Tożsamość użytkownika* wprowadzić informacje dotyczące tożsamości użytkownika w konkretnej domenie, a następnie nacisnąć przycisk *OK*.

## Usuwanie serwerów zasad VPN

**Aby usunąć serwer zasad VPN,** zaznacz serwer zasad VPN i naciśnij kombinację klawiszy Ctrl + *D*.

W oknie dialogowym *Zarządzanie VPN* wyświetlane jest zapytanie o potwierdzenie usunięcia zasad VPN zainstalowanych z serwera zasad VPN.

# Porządkowanie punktów dostępu VPN

Punkt dostępu VPN jest wirtualnym punktem dostępu będącym połączeniem zasady VPN oraz punktu dostępu do sieci internet. Aby utworzyć połączenie VPN, z listy punktów dostępu do internetu wybierz punkt dostępu VPN.

W oknie dialogowym *Punkty dostępu VPN* użytkownik może wyświetlać, tworzyć i usuwać punkty dostępu VPN używane przez komunikator. Przejdź do okna dialogowego *Narzędzia* > *Panel sterowania* > *Połączenia* > *Punkty dostępu VPN*. Wyświetlana ikona wskazuje typ połączenia z internetem, które jest używane do utworzenia połączenia VPN.

Aby utworzyć punkty dostępu VPN, naciśnij przycisk *Nowy*. W oknie dialogowym *Ustawienia ogólne* wprowadź następujące ustawienia:

- *Nazwa punktu dostępu VPN* - identyfikuje punkt dostępu VPN na liście punktów dostępu do internetu.
- *Punkt dostępu do internetu* - nazwa połączenia z internetem używanego do utworzenia połączenia VPN.
- *Zasady VPN* - nazwa zasady VPN, która jest skojarzona z danym punktem dostępu VPN.
- *Sieć* - identyfikuje sieć VPN. Należy wybrać inną sieć niż używana przez punkt dostępu do internetu.

**Uwaga**: Jeśli tworzone są połączenia VPN z kilkoma bramami VPN, dla każdej bramy VPN należy utworzyć osobną sieć.

**Aby wybrać sieć,** przejdź do okna dialogowego *Sieć* i naciśnij przycisk *Zmień*:

- Zaznacz sieć i naciśnij przycisk *OK*.
- **Aby dodać sieć,** naciśnij przycisk *Dodaj sieć*, wprowadź nazwę sieci w polu *Nazwa sieci* i naciśnij przycisk *OK*.
- **Aby zmienić nazwę sieci,** naciśnij przycisk *Zmień nazwę sieci*, zmień nazwę sieci w polu *Nazwa sieci* i naciśnij przycisk *OK*.

**Aby określić ustawienia serwera proxy w sieci firmowej,** przejdź do widoku *Ustawienia serwera proxy* i wprowadź następujące ustawienia:

**Uwaga:** Serwer proxy jest serwerem pośredniczącym, który pełni rolę bariery zabezpieczającej umieszczonej między intranetem a internetem. Odpowiednie ustawienia można uzyskać od administratorów.

- *Protokół proxy* - protokół używany przez serwer proxy.
- *Używaj serwera proxy* - wybierz opcję *Tak*, aby określić ustawienia serwera proxy znajdującego się w sieci firmowej.
- *Serwer proxy* - adres serwera proxy znajdującego się w sieci firmowej.
- *Numer portu* - numer portu używanego do łączenia się z serwerem proxy.
- *Nie używaj proxy z* - adresy internetowe określonych witryn wymagające ominięcia serwera proxy.

**Aby wyświetlić i dokonać edycji ustawień punktu dostępu VPN,** wybierz punkt dostępu VPN i naciśnij przycisk *Edytuj*.

**Aby usunąć punkt dostępu VPN,** zaznacz punkt dostępu VPN i naciśnij kombinację klawiszy Ctrl + *D*.

**Aby zapisać ustawienia,** naciśnij przycisk *Gotowe*.

**Porada!** Aby zamknąć widok bez zapisywania zmian, naciśnij klawisz Esc.

# Wyświetlanie rejestru VPN

Rejestr VPN zawiera wiadomości zapisane podczas aktualizacji i synchronizowania zasad sieci VPN oraz podczas korzystania z punktów dostępu VPN w celu utworzenia połączeń VPN do bram VPN.

*Rejestr* umożliwia przeglądanie i czyszczenie wiadomości rejestru. Można wyświetlić typ wiadomości, godzinę, o której została zapisana, oraz początek każdej z wiadomości rejestru.a

oznacza błąd, - ostrzeżenie, a - informację.

**Aby wyświetlić całą wiadomość rejestru,** naciśnij *Otwórz*.

W oknie *Rejestr* wiadomości są sortowane według godziny i daty zapisania, przy czym na początku znajdują się wiadomości najnowsze. Można przeglądać wiadomości zapisane do momentu otwarcia okna *Rejestr*.

**Aby przejrzeć najnowsze wiadomości rejestru,** naciśnij *Odśwież*.

Wiadomości rejestru mogą zawierać kody błędu, stanu oraz przyczyny. Podczas zgłaszania błędów należy podawać ich kody administratorom.

**Aby usunąć wszystkie wiadomości rejestru,** naciśnij *Wyczyść rejestr*.

Wiadomości rejestru są zapisywane w buforze cyklicznym. Gdy rejestr osiągnie rozmiar 20 kilobajtów, stare wiadomości rejestru są zastępowane nowymi.

# Hasła magazynu kluczy

*Hasło* umożliwia tworzenie lub zmianę hasła magazynu kluczy. Hasło magazynu kluczy chroni przed nieautoryzowanym dostępem klucze prywatne stosowane podczas połączeń urzsdzenia z serwerem zasad VPN.

## Tworzenie lub zmiana hasła magazynu kluczy

Hasło magazynu kluczy jest tworzone przy instalacji pierwszej zasady sieci VPN. Tworzone hasła magazynu kluczy powinny być długie i na tyle trudne, aby zabezpieczały informacje w urzsdzeniu. W przypadku złamania hasła magazynu kluczy nieupoważniona osoba może uzyskać dostęp do całej sieci przedsiębiorstwa.

**Porada!** Hasło magazynu kluczy musi się składać z co najmniej sześciu znaków i zawierać litery, liczby i znaki specjalne.

**Aby zmienić hasło magazynu kluczy,** naciśnij *Zmiana hasła*.

Jako *Hasło* wpisz takie hasło, które będzie dla Ciebie łatwe do zapamiętania, ale trudne do odgadnięcia dla innych osób. Aby zapobiec skutkom błędów podczas wpisywania, wpisz to hasło ponownie w polu *Potwierdzenie* i naciśnij przycisk *OK*.

## Wprowadzanie haseł magazynu kluczy

Hasło magazynu kluczy należy wprowadzić, gdy:

- instalujesz nowe lub aktualizowane zasady sieci VPN z serwerów zasad VPN
- korzystasz z aplikacji do łączenia się z punktami dostępu VPN, które wymagają uwierzytelnienia certyfikatu

# Korzystanie z sieci VPN przy użyciu aplikacji

Jeśli do utworzenia połączenia z punktem dostępu do sieci VPN używana jest aplikacja, komunikator:

- nawiązuje połączenie z punktem dostępu do internetu skojarzonym z punktem dostępu do sieci VPN
- ładuje zasadę VPN skojarzoną z punktem dostępu do sieci VPN
- łączy się z bramą VPN, aby utworzyć połączenie z siecią VPN

## Uwierzytelnianie w bramach VPN

Podczas logowania się do firmowej sieci VPN należy udowodnić swoją tożsamość. Zasady sieci VPN określają stosowaną metodę uwierzytelniania:

- Uwierzytelnianie oparte na certyfikacie - wymagany jest certyfikat podpisany przez zaufany urząd certyfikacji. W celu otrzymania certyfikatu należy zarejestrować certyfikat online lub zainstalować certyfikaty podczas instalacji zasad sieci VPN z pliku SIS.
- Uwierzytelnianie klasyczne - do uwierzytelniania stosowane są nazwy użytkowników, hasła lub kody. Zadaniem administratorów jest tworzenie nazw użytkowników i haseł lub przekazywanie tokenów SecurID służących do generowania kodów.

**Jeśli do uwierzytelniania stosowane są certyfikaty,** należy wprowadzić hasło magazynu kluczy.

**Jeśli stosowane jest uwierzytelnianie klasyczne,** podczas korzystania z aplikacji służących do łączenia z punktami dostępu VPN należy wprowadzić informacje o uwierzytelnianiu w sieci VPN, aby komunikator przeprowadził negocjacje zaszyfrowanych połączeń z bramą VPN.

**Aby korzystać z nazw użytkowników i haseł przy uwierzytelnianiu w bramie VPN,** wpisz nazwę użytkownika sieci VPN w polu *Nazwa użytkownika VPN* oraz hasło VPN w polu *Hasło VPN*. Naciśnij *OK*.

**Aby korzystać z nazw użytkowników i kodów przy uwierzytelnianiu w bramie VPN,** wpisz nazwę użytkownika sieci VPN w polu *Nazwa użytkownika VPN*. Wygeneruj kod SecurID i wpisz go w polu *Kod VPN*. Naciśnij *OK*.

Jeśli token SecurID utraci synchronizację z zegarem serwera ACE / Server, zostanie wyświetlony monit o następny kod, którego serwer ACE / Server użyje jako nowej referencji dla podstawy czasu tokena. Wpisz nazwę użytkownika sieci VPN w polu *Nazwa użytkownika VPN*. Wygeneruj i wpisz nowy kod w polu *Następny kod* i naciśnij *OK*. W razie niepowodzenia należy skontaktować się z administratorami.

## Rozwiązywanie problemów

W tej sekcji wymieniono w porządku alfabetycznym komunikaty o błędach oraz opisano możliwe przyczyny błędów i sugerowane czynności mające na celu usunięcie ich skutków.

*Błąd uwierzytelniania.*

- Podczas uwierzytelniania na serwerze zasad VPN lub logowania do sieci VPN wprowadzono nieprawidłową nazwę użytkownika lub hasło.
- Wprowadzono zły kod w monicie o następny kod.

Wypróbuj następujące rozwiązania:

- Sprawdź nazwę użytkownika i hasło, po czym ponów próbę.
- Wygeneruj i wpisz kod.

*Błąd automatycznego logowania do serwera zasad. Aby kontynuować, wprowadź nazwę użytkownika i hasło serwera zasad.*

Certyfikat uwierzytelniający użytkownika na serwerze zasad VPN stracił ważność lub administratorzy odwołali certyfikat.

Zgłoś ten problem administratorom, którzy udostępnią jednorazowe hasło umożliwiające zalogowanie. Wpisz nazwę użytkownika i jednorazowe hasło w celu uwierzytelnienia na serwerze zasad VPN. Klient VPN dołączy nowy certyfikat dla użytkownika.

*Błąd automatycznego logowania do serwera zasad. Aby uzyskać szczegółowe informacje, zobacz rejestr VPN.*

Nie rozpoczął się jeszcze okres ważności certyfikatu uwierzytelniającego użytkownika na serwerze zasad VPN.

Sprawdź ustawienia daty i godziny lub poczekaj, aż rozpocznie się okres ważności certyfikatu.

*Biblioteka kryptograficzna jest niewystarczająca.*

Jeśli biblioteka kryptograficzna zainstalowana na urzšdzeniu jest niewystarczająca, nie można korzystać z połączeń VPN.

Skontaktuj się z administratorami.

*Nieprawidłowe hasło.*

Wpisano nieprawidłowe hasło magazynu kluczy lub hasło importu kluczy.

Sprawdź hasło i ponów próbę.

Hasło importu kluczy otrzymuje się od administratorów. Hasło magazynu kluczy tworzy się samodzielnie.

*Serwer zasad jest aktualnie zajęty. Nie można usunąć.*

Nie można usunąć serwera zasad VPN podczas aktualizacji zasad VPN z tego serwera. W przypadku korzystania z aplikacji tworzącej połączenie z punktem dostępu do sieci VPN zasady VPN są aktualizowane automatycznie.

Poczekaj, aż aktualizacja zasad VPN zostanie ukończona, a następnie ponów próbę.

*Błąd logowania do serwera zasad. Usuń i utwórz ponownie definicję serwera.*

Certyfikat serwera należący do serwera zasad VPN stracił ważność.

**Aby usunąć serwer zasad VPN,** zaznacz odpowiedni serwer zasad VPN w oknie *Serwery zasad* i naciśnij klawisze Ctrl + *D*.

**Aby dodać ponownie serwer zasad VPN,** naciśnij *Nowy* lub poproś administratorów o plik SIS zawierający nowe ustawienia serwera zasad VPN.

*Błąd uaktualnienia zasad. Aby uzyskać szczegółowe informacje, zobacz rejestr VPN.*

*Błąd synchronizacji serwera zasad. Aby uzyskać szczegółowe informacje, zobacz rejestr VPN.*

Podczas pobierania zasad VPN z serwera zasad VPN lub podczas instalowania zasad VPN na urzšdzeniu wystąpił błąd.

**Aby zaktualizować zasadę VPN,** wybierz odpowiednią zasadę VPN w oknie *Zasady* i naciśnij *Aktualizuj*.

**Aby zainstalować zasady z serwera zasad VPN,** zaznacz odpowiedni serwer zasad VPN w oknie *Serwery zasad* i naciśnij przycisk *Synchronizuj*.

*Nieprawidłowy kod tożsamości serwera.*

Jako kod tożsamości serwera zasad VPN wpisano nieprawidłowy ciąg.

Porównaj dokładnie kod tożsamości serwera zasad VPN z kodem otrzymanym od administratorów i wpisz ponownie brakujące znaki.

*Błąd uaktywniania połączenia VPN. Aby uzyskać szczegółowe informacje, zobacz rejestr VPN.*

Błąd uwierzytelniania klasycznego lub brak certyfikatu używanego do uwierzytelniania w bramie VPN, certyfikat stracił ważność lub jego okres ważności jeszcze się nie rozpoczął.

Sprawdź ustawienia daty i godziny na urzšdzeniu.

**Aby zaktualizować zasadę VPN,** wybierz odpowiednią zasadę VPN w oknie *Zasady* i naciśnij *Aktualizuj*.

*Używana zasada VPN została usunięta. Skonfiguruj ponownie punkt dostępu do internetu.*

Zasada VPN skojarzona z punktem dostępu do sieci VPN była przestarzała i została usunięta automatycznie.

Aby skojarzyć z punktem dostępu do sieci VPN inną zasadę sieci VPN, w oknie *Punkty dostępu VPN* zaznacz odpowiedni punkt dostępu VPN, a następnie naciśnij przycisk *Edytuj*.

# Skorowidz


**B**

Błąd automatycznego logowania do serwera zasad 17
Błąd automatycznego logowania do serwera zasad. 17
Błąd logowania do serwera zasad 18
Błąd uaktualnienia zasad 18
Błąd uaktywniania połączenia VPN 18
Błąd uwierzytelniania 17
brakujące certyfikaty 9

**C**

certyfikaty
- rejestrowanie 13
- stan 9
- tożsamość użytkownika 13
- uwierzytelnianie wobec serwerów zasad VPN 10

certyfikaty jeszcze nieważne 9

**D**

Dodaj sieć, przycisk 14
dodawanie sieci 14

**E**

edytowanie punktów dostępu VPN 14
Edytuj, przycisk 14

**H**

hasła magazynu kluczy
- informacje 15
- tworzenie 15
- wprowadzanie 16

hasła magazynu kluczy, przeglądanie 15
Hasło serwera zasad, pole 12
Hasło VPN, pole 16
Hasło, pole 16

**I**

instalowanie
- programu Klient VPN 6
- ustawienia serwera zasad VPN z plików SIS 10
- zasady VPN 7, 13

**K**

Klient VPN
- instalowanie 6
- wprowadzenie 5
- wymagania systemowe 6

kod SecurID 17
Kod VPN, pole 17
komunikaty o błędach 17

**N**

Następny kod, pole 17
Nazwa punktu dostępu VPN, pole 14
Nazwa serwera zasad, pole 8, 11
Nazwa użytkownika serwera zasad, pole 12
Nazwa użytkownika VPN, pole 16, 17
Nazwa zasady, pole 8
Nie używaj proxy z, pole 14
Nieprawidłowe hasło 17
Nieprawidłowy kod tożsamości serwera 18
nieważne certyfikaty 9
Numer portu, pole 14

**O**

Odśwież, przycisk 15
Opis, pole 8

**P**

pola
- Adres serwera zasad 11
- Hasło 16
- Hasło serwera zasad 12
- Hasło VPN 16
- Kod VPN 17
- Następny kod 17
- Nazwa punktu dostępu VPN 14
- Nazwa serwera zasad 8, 11
- Nazwa użytkownika serwera zasad 12

Nazwa użytkownika VPN 16, 17
Nazwa zasady 8
Nie używaj proxy z 14
Numer portu 14
Opis 8
Potwierdzenie 16
Protokół proxy 14
Punkt dostępu do internetu 11, 14
Serwer proxy 14
Sieć 14
Stan certyfikatów 8
Stan zasad 8
Tożsamość użytkownika 13
Używaj serwera proxy 14
Zaktualizowano 8
Zasady VPN 14
pole Adres serwera zasad 11
Potwierdzenie, pole 16
Protokół proxy, pole 14
Punkt dostępu do internetu, pole 11, 14
punkty dostępu VPN
edytowanie 14
porządkowanie 14
usuwanie 15
widok 14

R

rejestr VPN
czyszczenie 15
wyświetlanie 15
rejestrowanie certyfikatów 13

S

Serwer proxy, pole 14
Serwer zasad jest aktualnie zajęty 18
serwery zasad VPN
dodawanie 11
instalowanie ustawień z plików SIS 10
nawiązywanie połączenia 10
porządkowanie 10
usuwanie 12, 13
Sieć, pole 14
sieci
dodawanie 14
wybieranie 14
zmiana nazwy 14
Stan certyfikatów, pole 8
Stan zasad, pole 8

T

Tożsamość użytkownika, pole 13
tworzenie punktów dostępu VPN 14

U

Używaj serwera proxy, pole 14
Używana zasada VPN została usunięta 18
Ustawienia serwera proxy, widok 14
Usuń, przycisk 9, 12
usuwanie 9
punkty dostępu VPN 15
serwery zasad VPN 12, 13
zasady VPN 9
uwierzytelnianie klasyczne 16
uwierzytelnianie oparte na certyfikacie 16

V

VPN
informacje 5
korzystanie przy użyciu aplikacji 16
uwierzytelnianie 16

W

wybieranie sieci 14
Wybierz sieć, widok 14
Wyczyść rejestr, przycisk 15
wymagania dotyczące pamięci 6
wymagania systemowe 6

Z

Zaktualizowano, pole 8
zasady VPN 9
aktualizowanie 9
informacje 7
instalowanie 7
porządkowanie 6
stan 8
szczegóły 8
usuwanie 9
Zasady VPN, pole 14
Zmiana hasła, przycisk 16
Zmień nazwę sieci, przycisk 14