

**Instrukcja instalacji, konfiguracji oraz użytkowania
oprogramowania Cisco VPN Client, wykorzystywanego
w ramach systemu ESDK.**

1. Wstęp	3
2. Instrukcja instalacji oprogramowania Cisco VPN Client.	4
3. Instrukcja importu certyfikatów.....	9
4. Instrukcja konfiguracji oprogramowania Cisco VPN Client	13
5. Instrukcja użytkowania oprogramowania Cisco VPN Client.	17

1. Wstęp

Niniejsza instrukcja przedstawia sposób instalacji, konfiguracji oraz użytkowania programu Cisco VPN Client, dla potrzeb komunikacji z Krajowym Depozytem Papierów Wartościowych S.A. w ramach systemu ESDK.

Oprogramowanie Cisco VPN Client dostarczane jest użytkownikom ESDK przez KDPW na podstawie warunków licencyjnych Cisco, dopuszczających możliwość przekazywania oprogramowania VPN Client podmiotom trzecim, pod warunkiem wykorzystywania go tylko i wyłącznie do zestawiania połączeń pomiędzy systemem klienta a koncentratorem VPN Cisco, użytkowanym w KDPW.

2. Instrukcja instalacji oprogramowania Cisco VPN Client.

Oprogramowanie Cisco VPN Client dostarczane jest użytkownikowi na płycie CD. Dopuszczalne jest zainstalowanie tego oprogramowania na dowolnej ilości stacji klienckich ESDK, z których zestawiane jest połączenie VPN z węzłem VPN w sieci KDPW S.A.

Przed rozpoczęciem instalacji oprogramowania VPN Client, należy zalogować się do stacji roboczej profilem z uprawnieniami administratora lokalnego stacji. Zalecane jest także zakończenie działania wszystkich innych aplikacji.

Dla prawidłowego działania oprogramowania Cisco VPN Client, niezbędne jest zapewnienie komunikacji pomiędzy stacją kliencką a węzłem VPN pracującym w KDPW S.A. . W tym celu należy zmodyfikować konfigurację urządzeń sieciowych klienta (routery, firewall'e itp.) w taki sposób, aby zezwolić na ruch sieciowy pomiędzy stacją kliencką a węzłem VPN w KDPW S.A. dostępnym w sieci internet (Informacje na temat adresu IP oraz portu węzła VPN, dostępne są w załączniku nr 1 do instrukcji instalacji i konfiguracji oprogramowania Cisco VPN Client).

W przypadku gdy stacja kliencka wyposażona jest w oprogramowanie typu personal firewall, niezbędna może okazać się jego rekonfiguracja lub wyłączenie. Reguły tego oprogramowania powinny zezwalać na komunikację stacji klienckiej z węzłem VPN pracującym w KDPW S.A..

UWAGA:

W przypadku instalacji oprogramowania Cisco VPN Client na stacji z systemem Windows XP SP2 z uaktywnioną zaporą sieciową, należy w konfiguracji zapory wprowadzić następujące wyjątki dla ruchu przychodzącego:

udp 500

tcp 55005

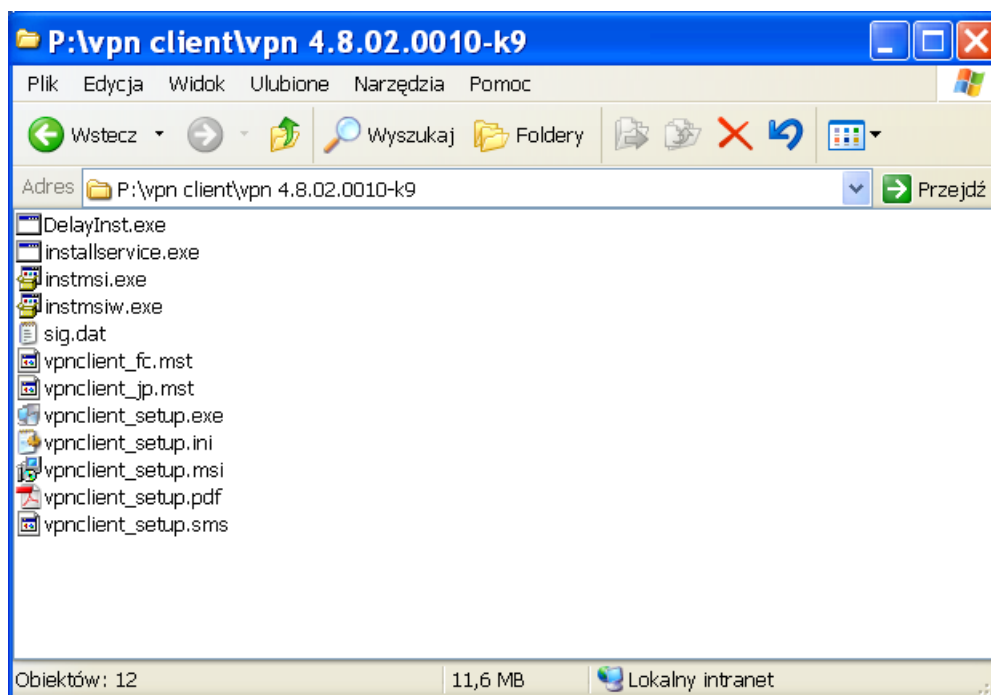
tcp 62514

udp 62514

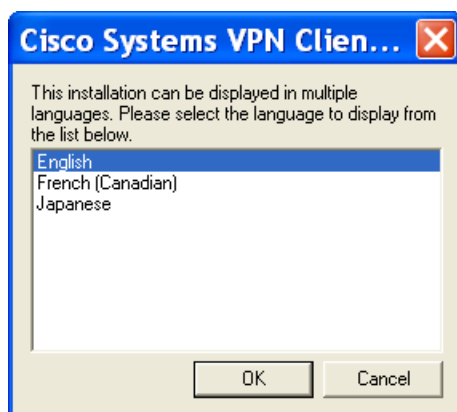
tcp 62515

udp 62515

2.1. W celu rozpoczęcia procesu instalacji należy uruchomić program „vpnclient_setup.exe” z katalogu instalacyjnego na CD-ROM:

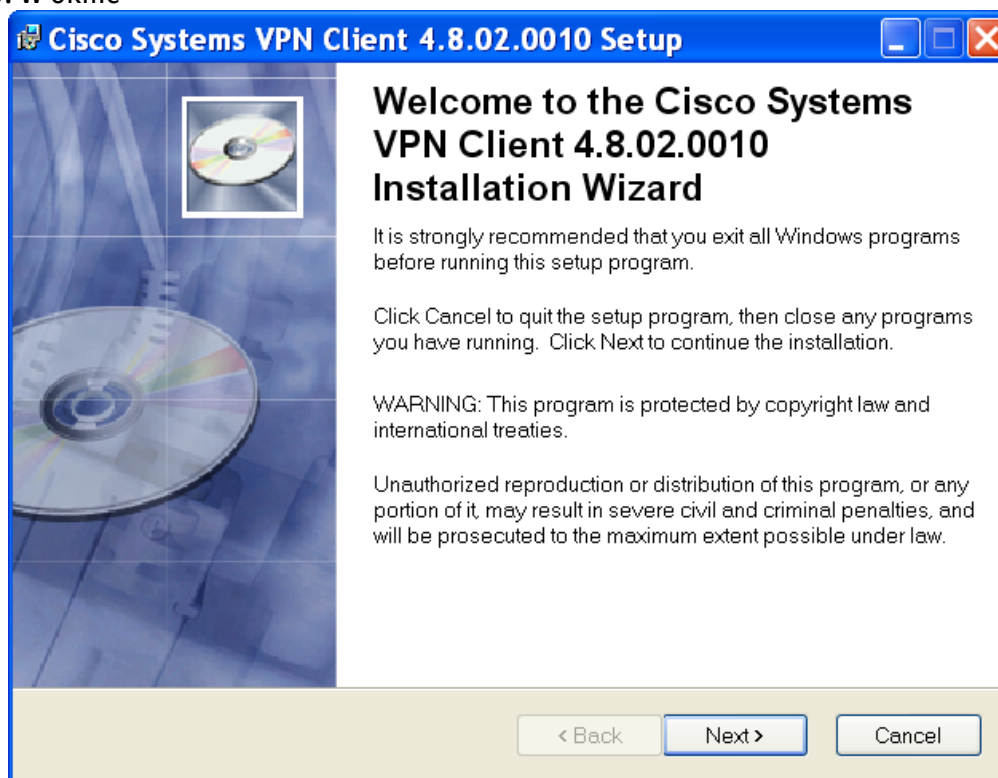


2.2. W oknie



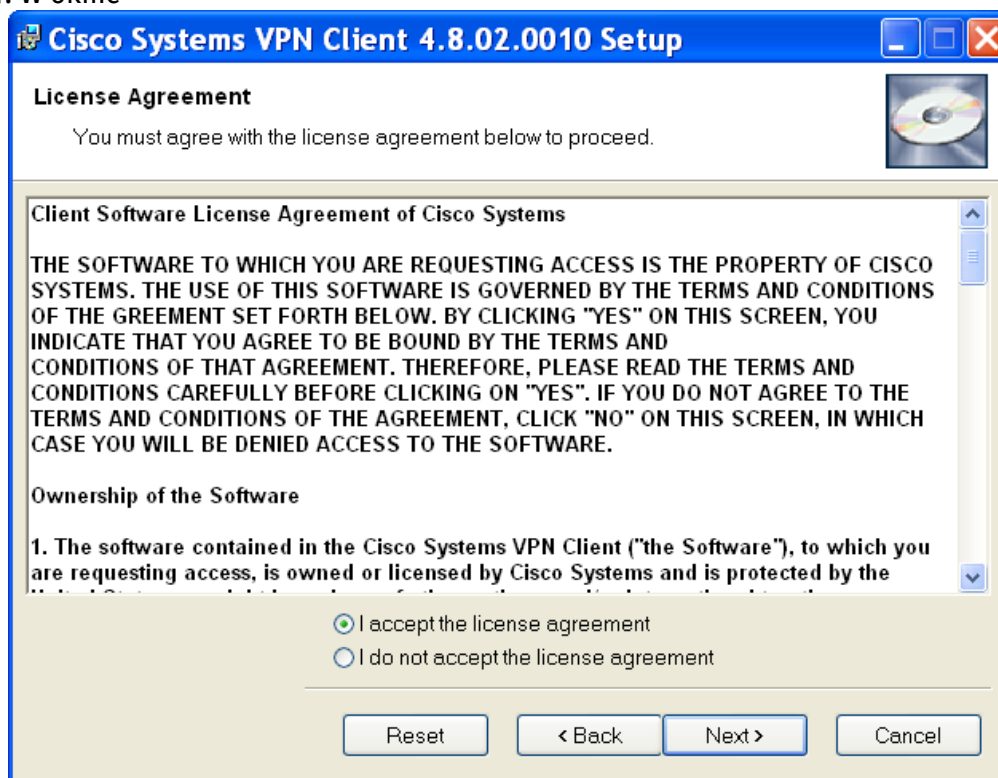
należy wybrać język, w którym będzie przeprowadzony proces instalacji oprogramowania, a następnie nacisnąć przycisk „OK.”

2.3. W oknie



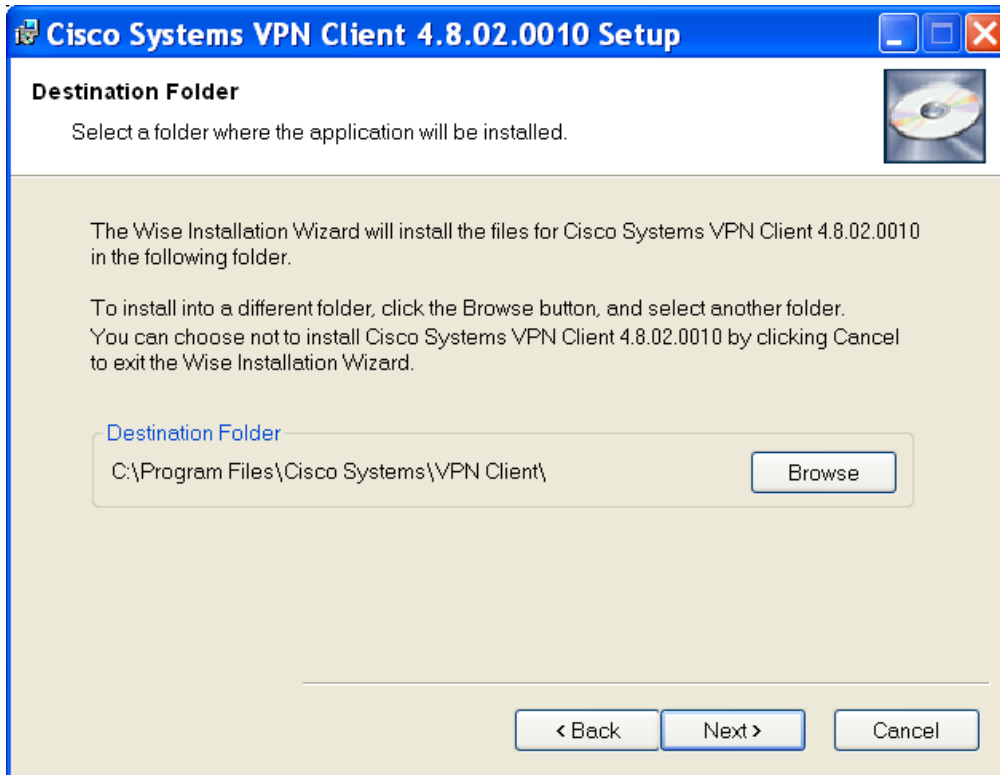
należy nacisnąć przycisk „Next >”

2.4. W oknie



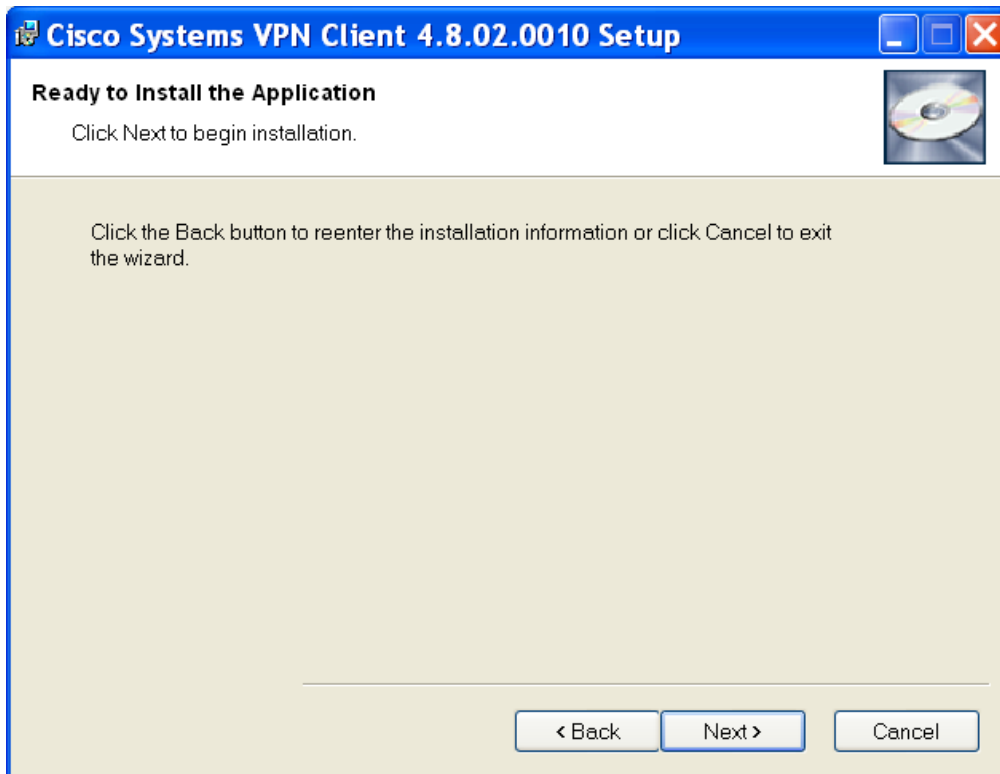
należy zaakceptować warunki licencji zaznaczając opcję „I accept the license agreement”, a następnie nacisnąć przycisk „Next >”

2.5. W oknie



należy wskazać folder, w którym zostanie zainstalowane oprogramowanie, a następnie nacisnąć przycisk „Next >”

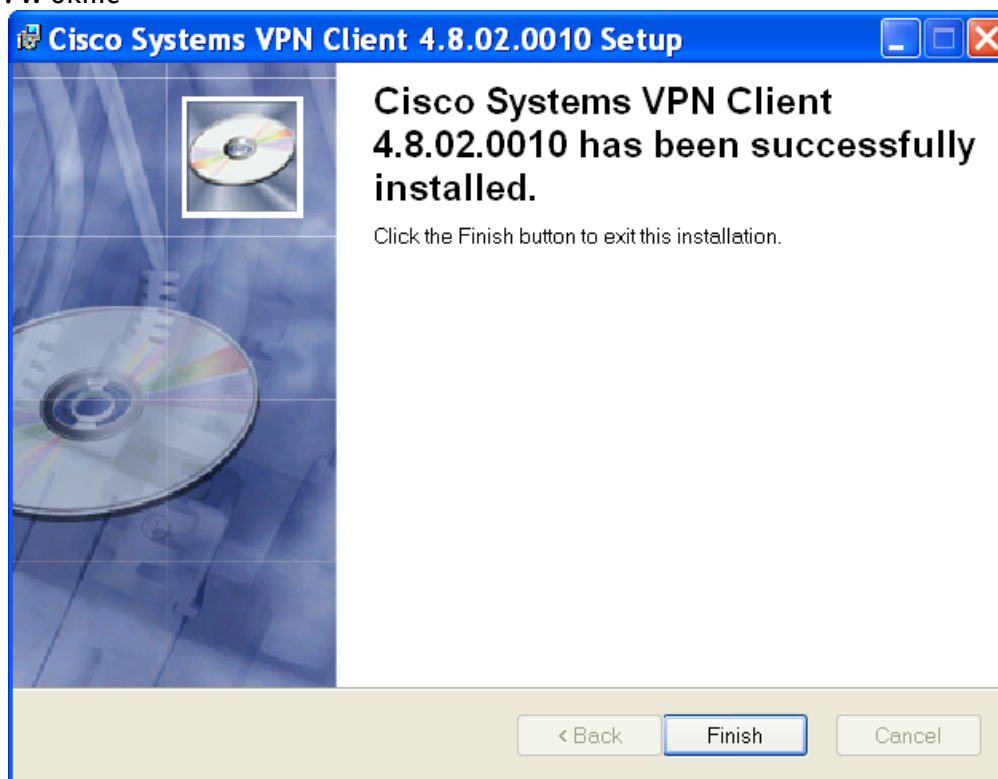
2.6. W oknie



należy nacisnąć przycisk „Next >”

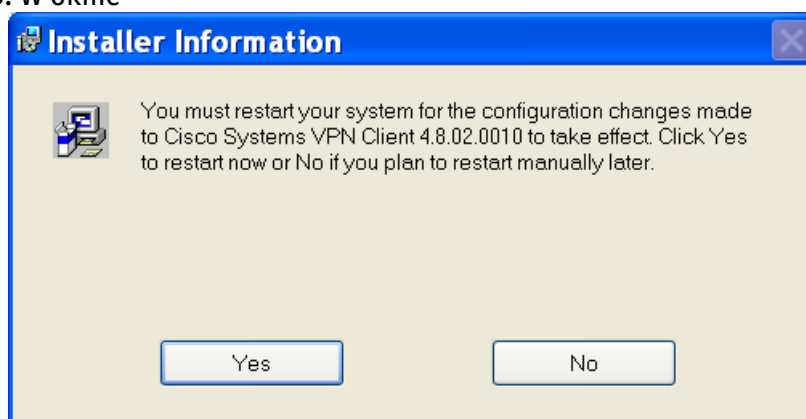
Rozpoczęty właśnie proces kopiowania plików, może potrwać kilka minut.

2.7. W oknie



należy nacisnąć przycisk „Finish”, kończący proces instalacji.

2.8. W oknie



należy nacisnąć przycisk „YES”, akceptując tym samym ponowne uruchomienie systemu operacyjnego.

2.9. Po wykonaniu powyższych czynności proces instalacji oprogramowania Cisco VPN Client został zakończony.

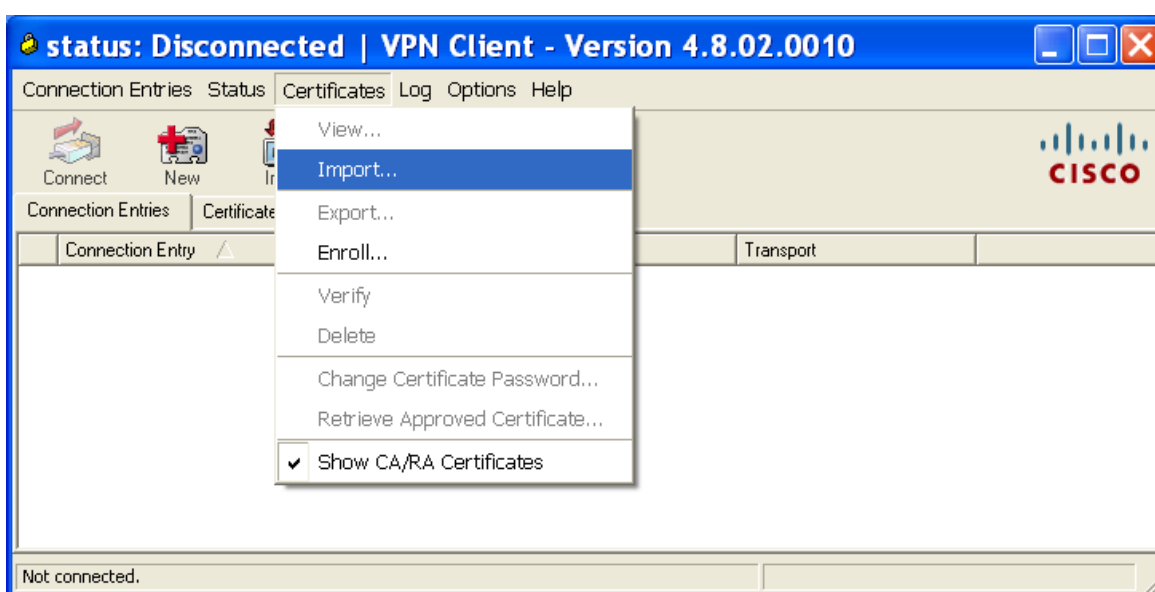
3. Instrukcja importu certyfikatów.

3.1. W celu dokonania importu certyfikatów, należy uruchomić program Cisco VPN Client.

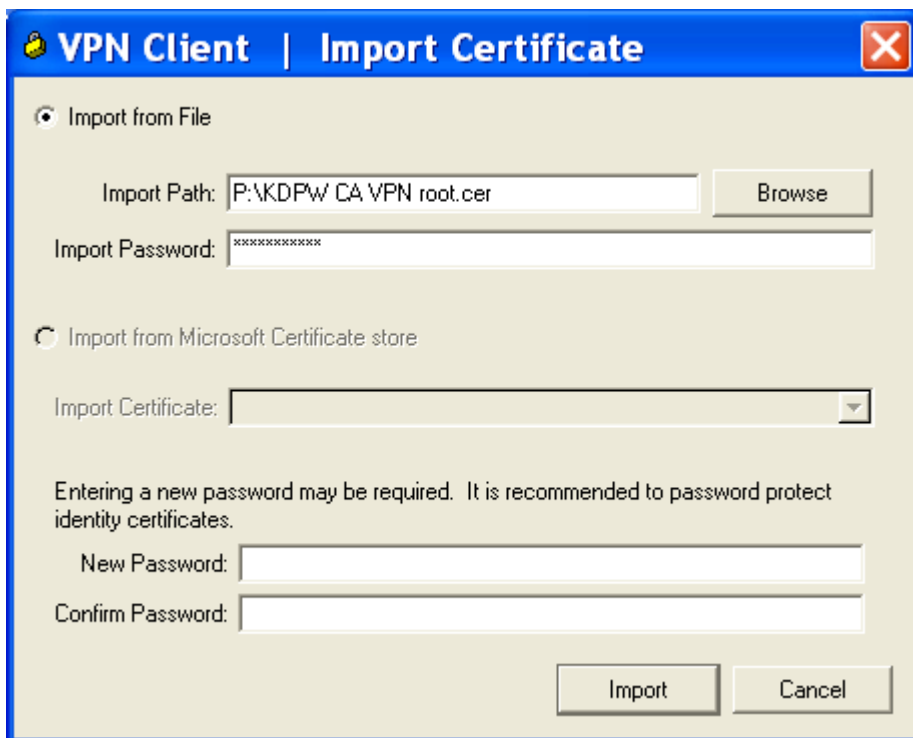
Start > Programy > Cisco System VPN Client > VPN Client

3.2. Import certyfikatu Centrum Autoryzacji KDPW.

Korzystając z uruchomionego graficznego interfejsu użytkownika, należy zaimportować certyfikat centrum autoryzacji, poprzez wybranie opcji „Import...” z menu „Certificates”.



W oknie importu certyfikatu należy zaznaczyć opcję „*Import from File*”, a następnie korzystając z przycisku „*Browse*” odszukać plik zawierający certyfikat. W polu „*Import Password:*” należy wprowadzić hasło certyfikatu, a na zakończenie nacisnąć przycisk „*Import*”.

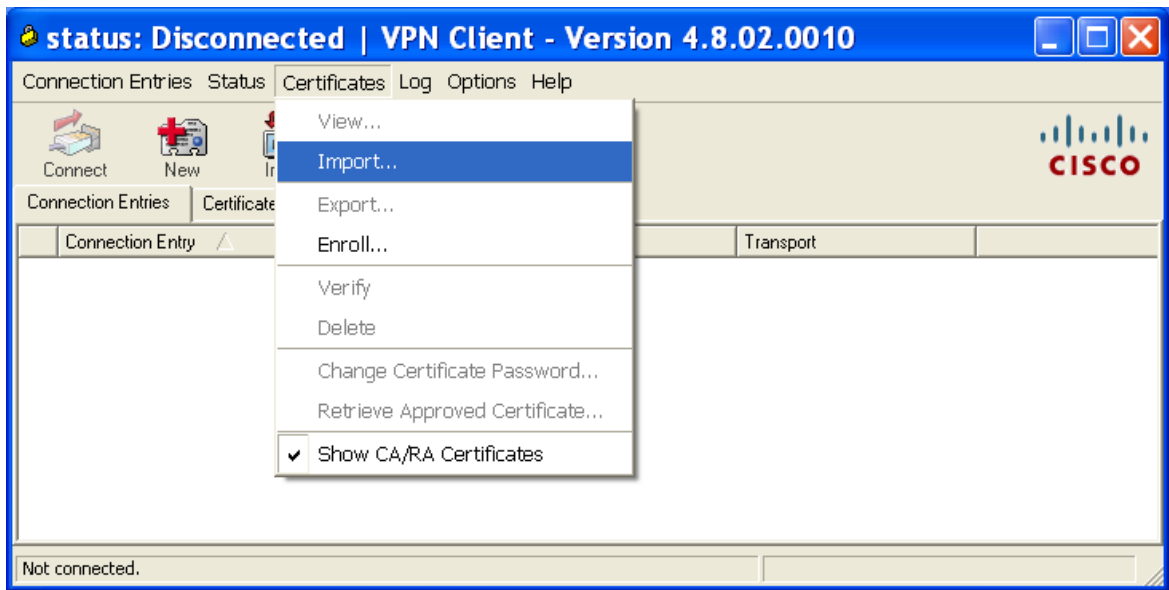


Poprawny import certyfikatu zakończony jest pojawieniem się następującego okna informacyjnego:

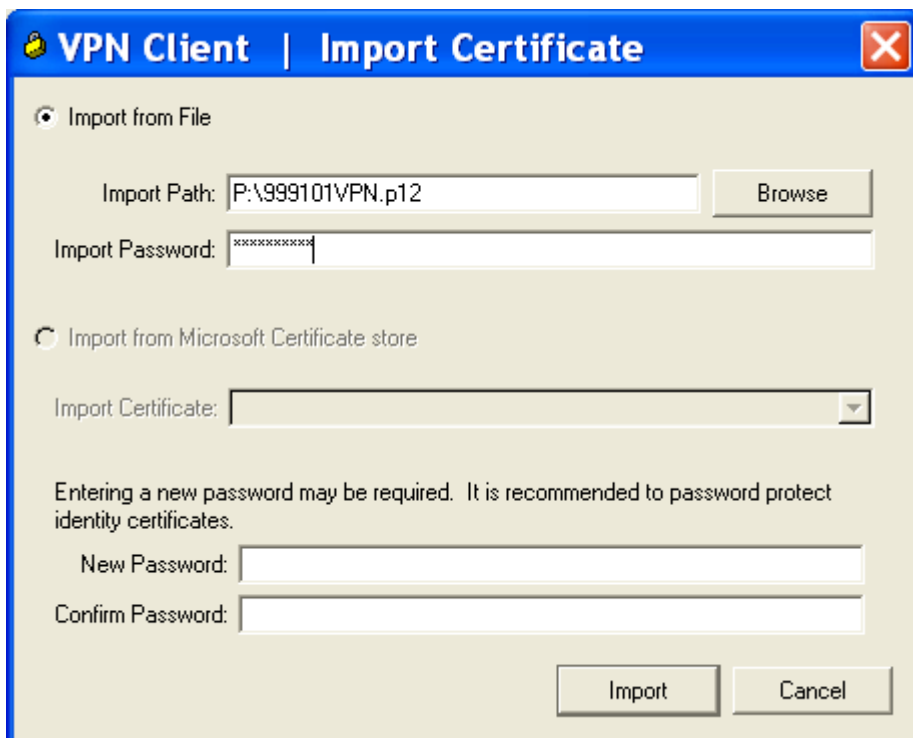


3.3. Import certyfikatu użytkownika.

Korzystając z uruchomionego graficznego interfejsu użytkownika, należy zaimportować certyfikat użytkownika, poprzez wybranie opcji „*Import...*” z menu „*Certificates*”.



W oknie importu certyfikatu należy zaznaczyć opcję „Import from File”, a następnie korzystając z przycisku „Browse” odszukać plik zawierający certyfikat. W polu „Import Password:” należy wprowadzić hasło certyfikatu, a na zakończenie nacisnąć przycisk „Import”.



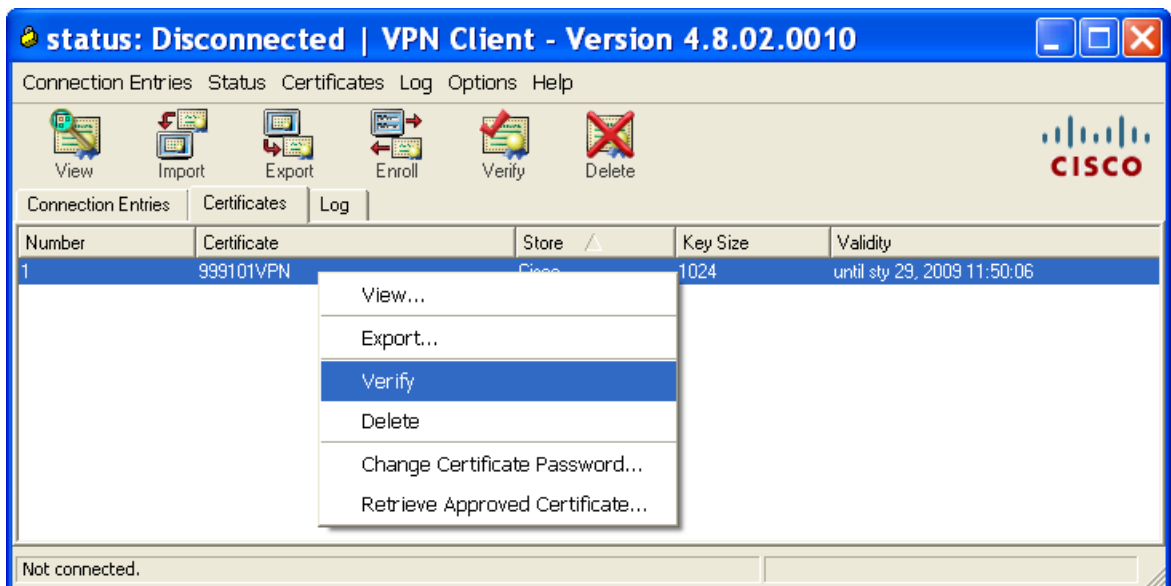
Poprawny import certyfikatu zakończony jest pojawieniem się następującego okna informacyjnego:



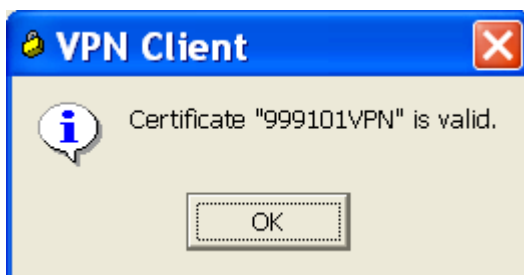
3.4. Weryfikacja poprawności importu certyfikatów.

Po zaimportowaniu certyfikatu Centrum Autoryzacji KDPW oraz certyfikatu użytkownika, należy zweryfikować poprawność wykonania w/w czynności (ważność certyfikatu).

Korzystając z graficznego interfejsu użytkownika, należy uaktywnić zakładkę „Certificates”, następnie wybrać uprzednio zaimportowany certyfikat użytkownika poprzez kliknięcie na nim prawym przyciskiem myszy. Z menu kontekstowego należy wybrać opcję „Verify”.



Ważność certyfikatu użytkownika, potwierdzona jest pojawieniem się następującego okna informacyjnego:

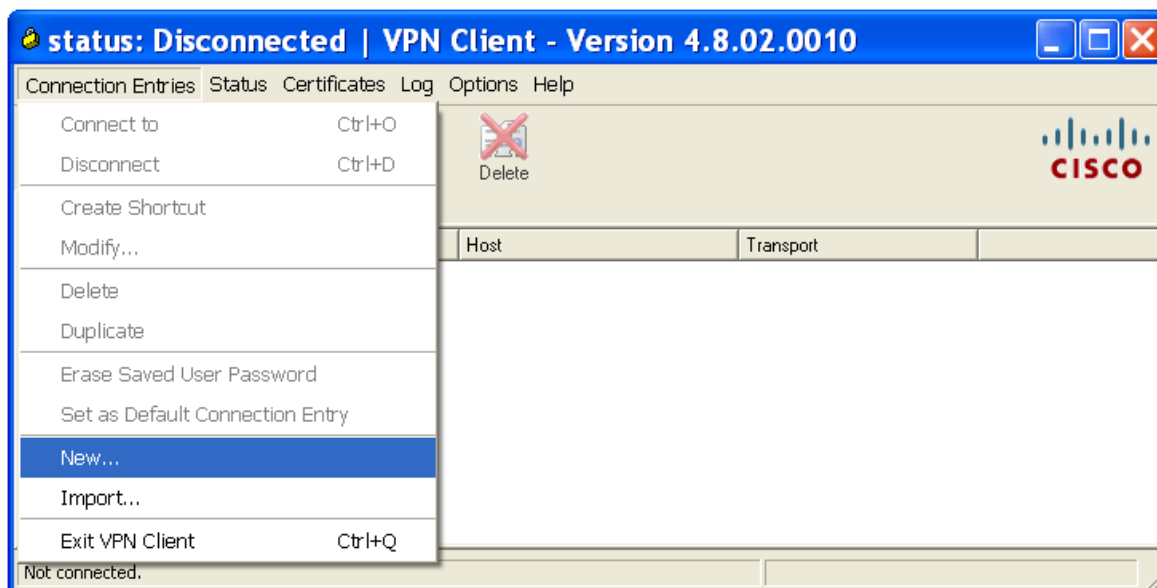


4. Instrukcja konfiguracji oprogramowania Cisco VPN Client

4.1. W celu dokonania konfiguracji należy uruchomić program Cisco VPN Client.

Start > Programy > Cisco System VPN Client > VPN Client

4.2. Korzystając z uruchomionego graficznego interfejsu użytkownika, należy stworzyć nowe połączenie – wybrać opcję „New...” z menu „Connection Entries”



4.3. W oknie nowego połączenia należy wprowadzić kolejno:

- W polu: „*Connection Entry:*” ESDK
(Dowolna nazwa identyfikująca połączenie).
- W polu: „*Description:*” Połączenie z systemem ESDK w KDPW S.A.
(Dowolny opis określający połączenie).
- W polu: „*Host:*” Adres IP węzła VPN w KDPW S.A.
(Informacje na temat adresu IP węzła VPN, dostępne są w załączniku nr.1 do instrukcji instalacji i konfiguracji oprogramowania Cisco VPN Client).



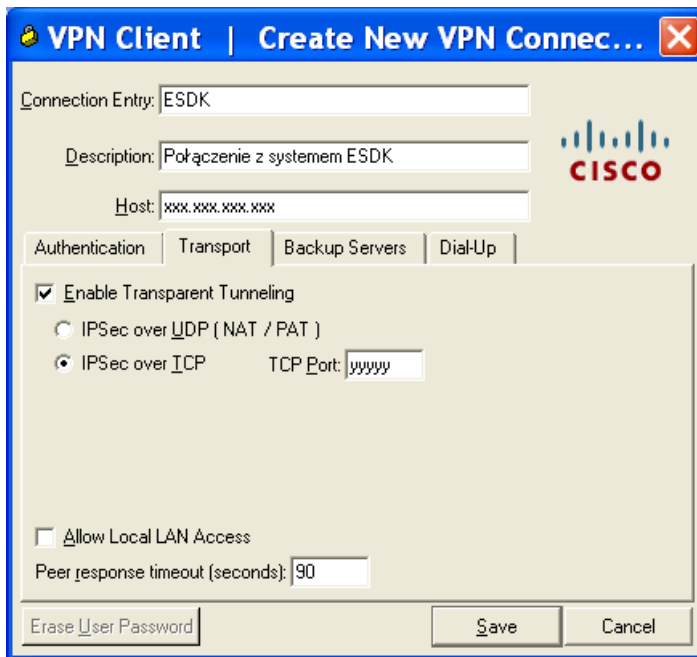
4.4. W oknie nowego połączenia, w zakładce „Authentication” należy:

- Zaznaczyć opcję „Certificate Authentication”.
- W polu „Name:” wybrać uprzednio zaimportowany certyfikat.

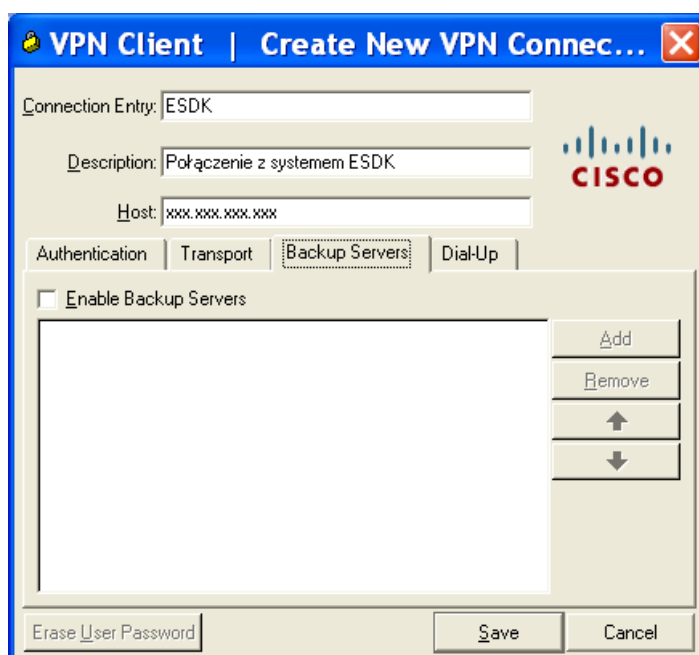


4.5. W oknie nowego połączenia, w zakładce „*Transport*” należy:

- Zaznaczyć opcję „*Enable Transparent Tunneling*”
- Wybrać opcję „*IPSec over TCP*”
- W polu „*TCP Port:*” wprowadzić numer portu TCP. Informacje na temat portu TCP węzła VPN, dostępne są w załączniku nr.1 do instrukcji instalacji i konfiguracji oprogramowania Cisco VPN Client.



4.6. Zakładkę „*Backup Servers*” w oknie nowego połączenia należy pozostawić bez zmian.



4.7. Zakładkę „Dial-Up” w oknie nowego połączenia należy pozostawić bez zmian.



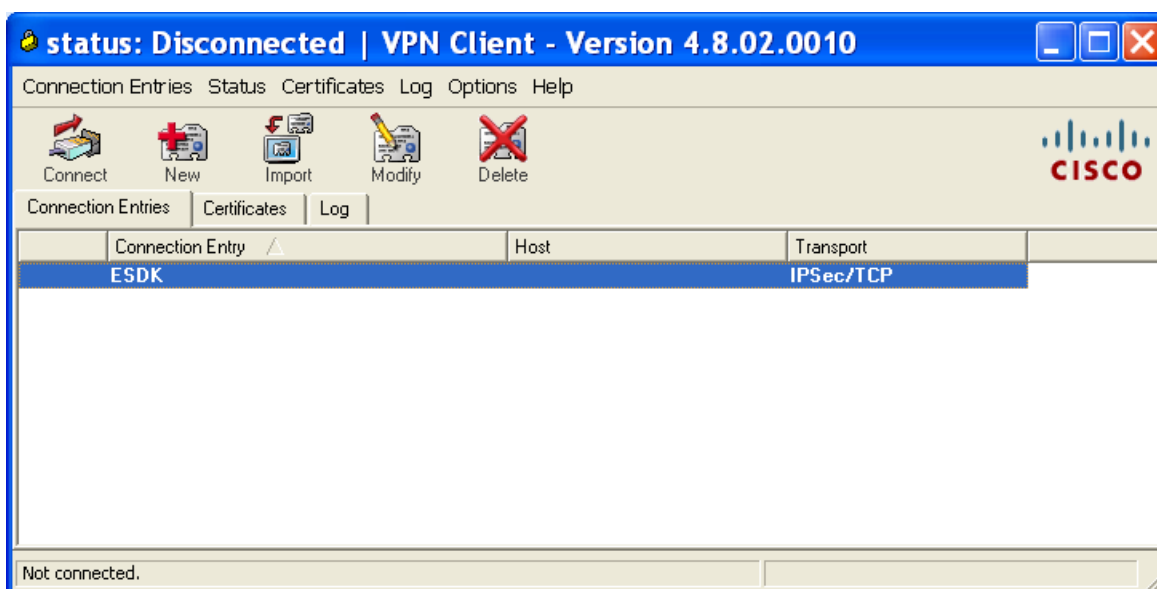
4.8. Po wykonaniu powyższych czynności należy zapisać konfigurację naciskając przycisk „Save”.

5. Instrukcja użytkowania oprogramowania Cisco VPN Client.

5.1. Nawiązywanie połączenia VPN z KDPW S.A.

W celu rozpoczęcia działania połączenia VPN z KDPW S.A. należy:


- uruchomić oprogramowanie Cisco VPN Client.
Start > Programy > Cisco System VPN Client > VPN Client
- W oknie graficznego interfejsu użytkownika oprogramowania „Cisco VPN Client” uruchomić uprzednio skonfigurowane połączenie z KDPW S.A. poprzez dwukrotne przyciśnięcie lewego przycisku myszy.



- W oknie dialogowym



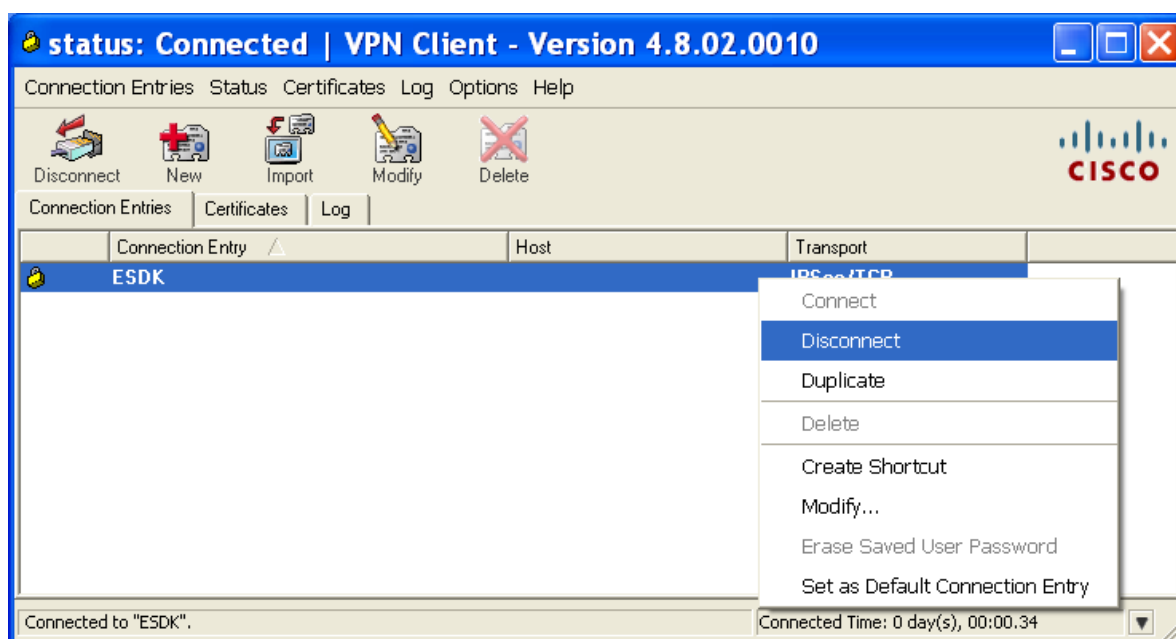
należy wprowadzić nazwę użytkownika oraz hasło użytkownika a następnie nacisnąć przycisk „OK”.

- Poprawne zestawienie tunelu VPN, zasygnalizowane jest pojawieniem się odpowiedniej ikony w obszarze powiadomień (obok zegara systemowego). 

5.2. Zakończenie połączenia VPN z KDPW S.A.

W celu zakończenia działania połączenia VPN z KDPW S.A. należy:

- uruchomić interfejs graficzny oprogramowania Cisco VPN Client.
Start > Programy > Cisco System VPN Client > VPN Client
- następnie kliknąć prawym przyciskiem myszy na aktywnym połączeniu i z menu kontekstowego wybrać opcję „Disconnect”.



- Zakończenie działania tunelu VPN, zasygnalizowane jest pojawieniem się odpowiedniej ikony w obszarze powiadomień (obok zegara systemowego). 