INSTRUKCJA 12/016

Dotyczy: dostępu zdalnego do zasobów sieci MAN Wrocław

– instrukcja działania Użytkownika

OPRACOWAŁ:	ZWERYFIKOWAŁ:	ZATWIERDZIŁ:
Grzegorz Zegler Sławomir Gordziejewski	Dariusz Dauksz	Dariusz Jędryczek

Spis treści

1. Cel dokumentu

Celem dokumentu jest przedstawienie sposobu postępowania podczas instalacji, konfiguracji i zbierania logów do dostępu zdalny do zasobów sieci MAN Wrocław.

2. Słownik pojęć i skrótów

Certyfikat – generowany przez Użytkownika na podstawie Klucza przy użyciu Klienta VPN plik o rozszerzeniu .p12 wraz z hasłem umożliwiający uzyskanie zdalnego połączenia do sieci MAN Wrocław. Posiadanie Certyfikatu jest niezbędne do uzyskania zdalnego dostępu do zasobów sieci MAN Wrocław. Certyfikat jest ważny przez okres 2 lat od dnia jego utworzenia, chyba że administrator unieważni taki Certyfikat wcześniej (ważność Certyfikatu zostaje automatycznie przedłużona w przypadku gdy użytkownik przynajmniej jeden raz połączy się z zasobami sieci MAN Wrocław w ostatnim miesiącu okresu ważności). Wygaśnięcie Certyfikatu jest jednoznaczne z utratą dostępu zdalnego do zasobów sieci MAN Wrocław i koniecznością złożenia nowego wniosku o udzielenie dostępu. Zabezpieczenie Certyfikatu przed dostępem osób nieuprawnionych jest obowiązkiem Użytkownika.

CUI – Centrum Usług Informatycznych we Wrocławiu będące jednostką organizacyjną Gminy Wrocław w formie jednostki budżetowej.

HelpDesk – elektroniczny system obiegu zleceń serwisowych z zakresu informatyki i telekomunikacji zarządzany przez CUI (HelpDesk.um.wroc.pl).

Klient VPN – oprogramowanie niezbędne do zainstalowania i skonfigurowania na komputerze, z którego będzie uzyskiwany zdalny dostęp do zasobów sieci MAN Wrocław.

Klucz rejestracyjny VPN – ciąg znaków wymagany do samodzielnego wygenerowania Certyfikatu. Klucz jest ważny 21 dni od daty jego

wygenerowania – jeżeli w tym okresie Certyfikat nie zostanie utworzony należy wystąpić o ponowne wygenerowanie Klucza dla Użytkownika.

Kontener – skompresowany plik z rozszerzeniem „.zip" zawierający zaszyfrowany klucz do certyfikatu VPN.

Konto Dostępowe – dedykowany profil Użytkownika do którego przypisywane są reguły dostępu umożliwiające zdalny dostęp do konkretnych zasobów sieci MAN Wrocław. Konto Dostępowe jest ściśle powiązane z Certyfikatem. Utworzenie Konta Dostępowego dla Użytkownika nie jest jednoznacznie z uzyskaniem dostępu do zasobu sieciowego (np. do zalogowania się do serwera wymagane jest posiadanie loginu oraz hasła dostępowego).

MAN Wrocław – publiczna sieć telekomunikacyjna Gminy Wrocław, której operatorem jest Centrum Usług Informatycznych we Wrocławiu.

Osoba Wnioskująca – osoba uprawniona do złożenia wniosku o założenie konta dla Użytkownika usługi VPN. Dopuszcza się założenie wniosku w imieniu osoby nie posiadającej konta w systemie HelpDesk (np. dla pracownika firmy zewnętrznej). Osoba Wnioskująca jest odpowiedzialna za wszelkie działania podejmowane przez Użytkownika w sieci MAN Wrocław, za zgłoszenie konieczności odebrania uprawnień oraz zobowiązana jest do zgłaszania w jego imieniu incydentów związanych z nieprawidłowym działaniem usługi.

Użytkownik – osoba, która uzyskuje zdalny dostęp do zasobów sieci MAN Wrocław.

VPN (ang. Virtual Private Network, pol. Wirtualna Sieć Prywatna) – technologia umożliwiająca zdalny, szyfrowany dostęp do zasobów i usług sieci teleinformatycznej poprzez sieć publiczną operatora telekomunikacyjnego.

3. Zasady ogólne

1. Klucz rejestracyjny VPN oraz instrukcja instalacji są przekazywane Użytkownikowi:

a) instrukcja instalacji na adres mailowy Użytkownika podany w zgłoszeniu,

b) hasło niezbędne do utworzenia certyfikatu zgodnie z dyspozycją (SMS/odbiór osobisty/przesyłka pocztowa), zgodnie z dyspozycjami zawartymi we wniosku o utworzenie konta VPN.

2. Jeżeli Użytkownik nie posiada konta w systemie HelpDesk wszystkie zlecenia i incydenty musi składać za pośrednictwem Osoby Wnioskującej.

3. Proces generowania certyfikatu VPN, instalacji i konfiguracji Klienta VPN jest realizowany samodzielnie przez Użytkownika zgodnie z przekazaną instrukcją (patrz punkty 3-4).

4. W przypadku braku/ograniczenia dostępu VPN Użytkownik zobowiązany jest do zebrania logów Klienta VPN (patrz punkt 5).

5. CUI nie gwarantuje ciągłego działania usługi VPN jednak dołoży wszelkich starań, aby przerwy w dostępie działania usługi były jak najkrótsze.

6. CUI nie bierze odpowiedzialności za nieprawidłowe działanie Klienta VPN w przypadku gdy ruch jest blokowany na stacji Użytkownika (oprogramowanie typu: firewall, antywirus, inne oprogramowanie do uzyskiwania połączeń typu VPN) lub przez urządzenia bezpieczeństwa w sieci z której łączy się Użytkownik.

7. Dopuszcza się czasowe lub bezterminowe odebranie udzielonego dostępu:

   a) w przypadku wystąpienia okoliczności uzasadniających odebranie dostępu (np. ustanie stosunku pracy, brak obowiązków służbowych niezbędnych do posiadania zdalnego dostępu),

   b) w przypadku wykorzystywania przez Klienta VPN dostępu w sposób niezgodny z przeznaczeniem,

c) w przypadku udostępnienia danych umożliwiających uzyskanie zdalnego dostępu osobie nieuprawnionej,

d) w przypadku wystąpienia incydentu bezpieczeństwa w sieci MAN Wrocław,

e) na wniosek Osoby Wnioskującej o nadanie dostępu zdalnego.

8. Konto VPN jest ważne przez okres jednego roku od utworzenia i wymaga złożenia wniosku o przedłużenie jego ważności.

9. Certyfikat VPN niezbędny do autoryzacji połączenia zdalnego jest ważny przez okres 2 lat od jego utworzenia (certyfikat jest samodzielnie tworzony przez Użytkownika na podstawie instrukcji instalacji Klienta VPN). Wygaśnięcie Certyfikatu uniemożliwia połączenie zdalne z siecią VPN.

10. Ważność Certyfikatu VPN jest automatycznie przedłużana na okres 2 lat jeżeli Użytkownik w ostatnim miesiącu ważności certyfikatu wykona co najmniej jedno udane połączenie zdalne do sieci MAN Wrocław.

11. Przedłużenie obowiązywania ważnego Certyfikatu wymaga zgłoszenia w systemie HelpDesk (zaleca się samodzielne przedłużanie Certyfikatu zgodnie z punktem 3.10).

12. W przypadku wygaśnięcia Certyfikatu wymagane jest złożenie wniosku o utworzenie nowego Klucza rejestracyjnego VPN.

13. W przypadku utraty hasła lub Certyfikatu wymagane jest złożenie wniosku o utworzenie nowego Klucza rejestracyjnego VPN, przy czym stary Certyfikat zostaje unieważniony w systemie.

14. Umieszczenie Certyfikatu na dysku usb, sieciowym lub ścieżce użytkownika systemu, może wiązać się z niepoprawnym odczytaniem certyfikatu przez aplikację Klienta VPN. Certyfikat należy umieścić na dysku lokalnym np. C:\.

15. Połączenie VPN może nie działać poprawnie w przypadku, gdy Użytkownik znajduje się w sieci lokalnej o adresacji:

    a) 192.168.1.0/24,

    b) 192.168.10.0/24,

    c) 192.168.5.11/24,

    d) 192.168.33.199/24,

    e) 192.168.46.0/24,

    f) 192.168.200.0/24,

    g) 192.168.67.0/24,

    h) 192.168.231-243.0/24,

    i) 192.168.141-143.0/24,

    j) 192.168.150-151/24, w celu rozwiązania problemu należy zmienić adresację sieci lokalnej.

16. Producent oprogramowania Klient VPN w celu zapewnienia pełnej komunikacji wskazuje konieczność otwarcia ruchu na portach (TCP): 80, 81, 443, 1080, 1081, 6666, 8005, 8009, 8080.

17. W celu poprawnego działania zalecane jest posiadanie łącza internetowego o minimalnej przepustowości 2Mbps.

18. Administratorzy CUI dołożą wszelkich starań aby poinformować Użytkowników, którzy w procesie rejestracji podali adres poczty elektronicznej o:

    a) konieczności aktualizacji oprogramowania VPN,

b) awariach oraz planowych pracach prowadzących do braku możliwości zdalnego dostępu do zasobów sieciowych MAN Wrocław,

c) wygaśnięciu konta VPN (na miesiąc przed wygaśnięciem konta).

19. Użytkownik jest zobowiązany do zabezpieczenia stacji roboczej, z której wykonuje połączenie do sieci MAN Wrocław oprogramowaniem typu antywirus oraz fizyczną ochronę stacji roboczej w celu uniemożliwienia nieuprawnionego dostępu do udostępnianych zasobów osobom trzecim (np. poprzez zakończenie połączenia w momencie przerwania pracy w zdalnym systemie).

4. Instalacja Klienta VPN

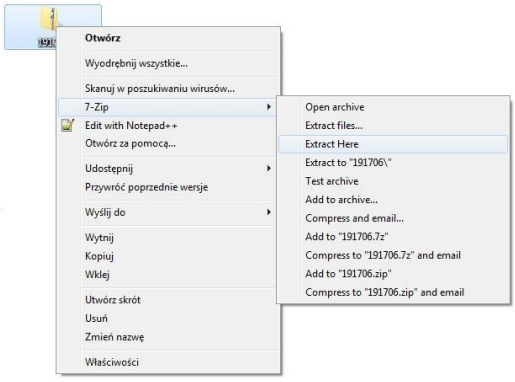
1. W celu odbioru klucza rejestracyjnego należy zapisać zaszyfrowany plik Kontenera (przykładowa nazwa: „HD_191706.zip”) będący załącznikiem wiadomości e-mail przesłanej przez administratora sieci MAN Wrocław na adres poczty elektronicznej wskazanej w zgłoszeniu o utworzenie nowego konta dla Użytkownika.

2. Hasło do Kontenera, Użytkownik otrzyma w wiadomości SMS wysłanej na numer telefonu komórkowego wskazanego w zgłoszeniu zaraz po zakończeniu jego realizacji. Jeżeli osoba ubiegająca się o Klucz rejestracyjny VPN nie podała numeru komórkowego, to w takim przypadku hasło zostanie wysłane drogą alternatywną tj. listem poleconym za potwierdzeniem odbioru. W przypadku niedostarczenia wiadomości SMS z hasłem, w ciągu 24 godzin od otrzymania emaila z plikiem Kontenera, należy zgłosić ten fakt w aplikacji HelpDesk lub Osobie Wnioskującej.

3. W celu odczytania Klucza rejestracyjnego VPN należy zapisać plik z rozszerzeniem „.zip” przesłany pocztą elektroniczną. Następnie wykonać

dekompresję pliku wskazując docelowe miejsce klucza oraz wprowadzić hasło otrzymane wiadomością SMS lub listem poleconym.

4. Uwaga: aplikację do dekompresji pliku „.zip" można pobrać bezpośrednio z witryny http://cui.wroclaw.pl/index.php/vpn, dla systemów Windows o architekturze 64 bitowej 7z920-x64.msi lub 32 bitowej 7z920.exe.

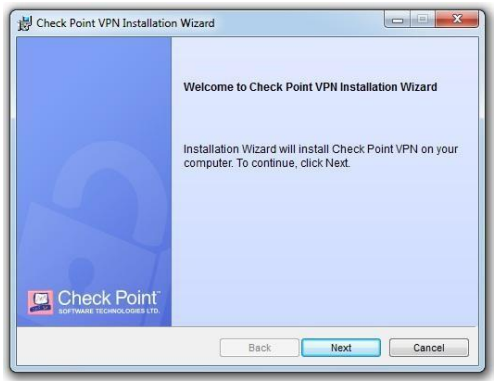


5. Aktualną wersje instalacyjne Klienta VPN należy pobrać z witryny http://cui.wroclaw.pl/index.php/vpn (dla systemu operacyjnego Windows: przykładowa nazwa CP_EPS_E80.51_RAC_Windows.msi oraz dla systemu operacyjnego MacOS: CP_EPS_E80.50.03_Client_Mac.zip).

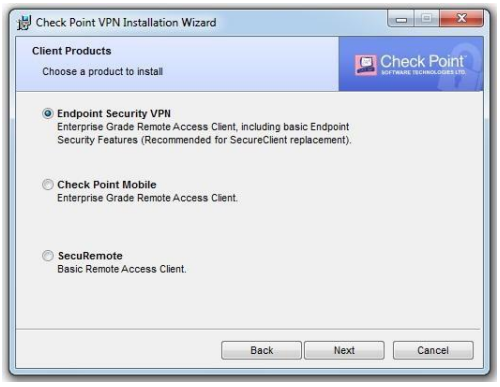
6. Przed rozpoczęciem konfiguracji wymagane jest podłączenie komputera do sieci Internet. Instalacja musi być wykonywana przez użytkownika z uprawnieniami administracyjnymi systemu.

7. Uwaga: na czas instalacji zalecane jest wyłączenie zapory sieciowej oraz ochrony antywirusowej.

8. Po uruchomieniu programu instalacyjnego w kreatorze instalacji należy wybrać Next:

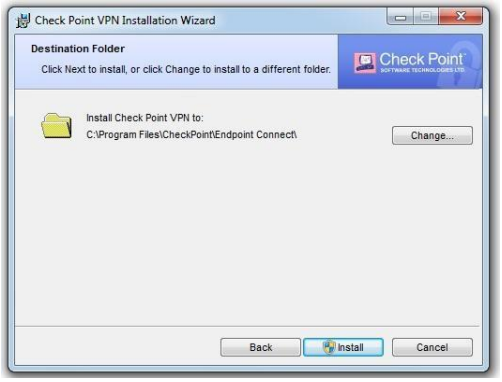


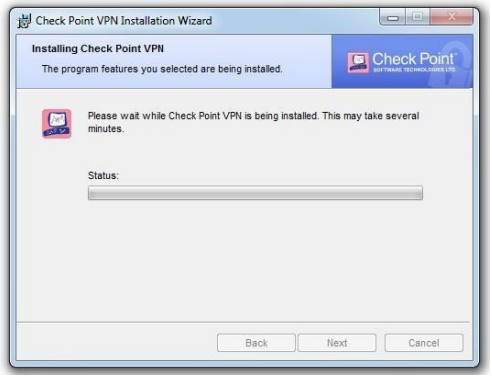
9. Typ klienta Endpoint Security VPN:



10. Zaakceptować licencję.

11. Zaakceptować domyślną ścieżkę katalogu do instalacji lub wskazać inną (przycisk „Change...” , domyślna ścieżka to C:\Program Files\CheckPoint\Endpoint Connect\), po czym wybrać „Install”:





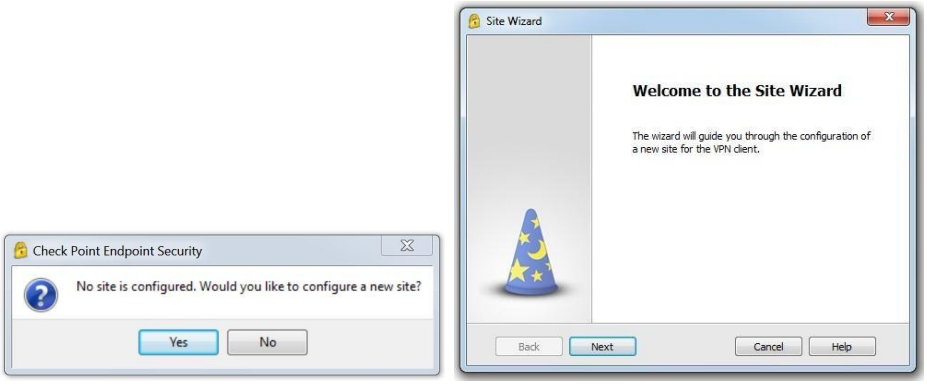
12. Po otrzymaniu monitu o instalacji zakończonej sukcesem, należy wykonać restart systemu operacyjnego poprzez wybór opcji Yes, bądź w sposób manualny:

13. Po wykonaniu restartu klient VPN jest gotowy do pierwszej konfiguracji.

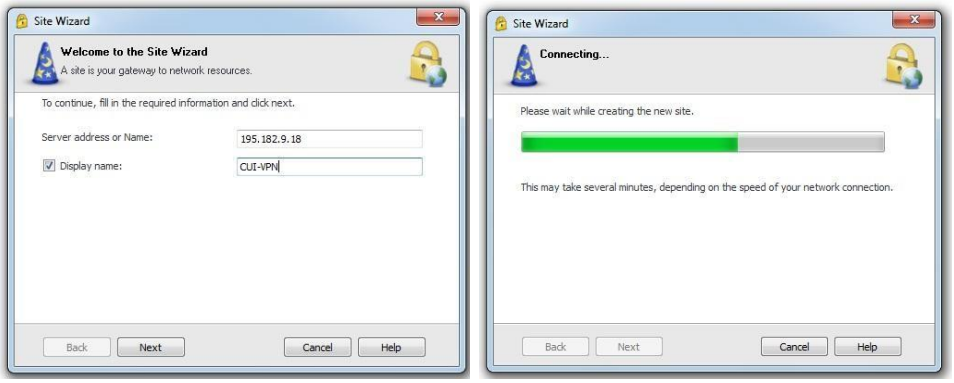
5. Konfiguracja Klienta VPN

1. Generowanie przez Użytkownika Certyfikatu VPN następuje po instalacji klienta VPN tj. Endpoint Security VPN, bądź poprzez zainstalowaną wcześniej aktualną wersje klienta.

2. Po wykonaniu instalacji i uruchomieniu aplikacji klienta VPN, oprogramowanie zasugeruje wykonanie pierwszej konfiguracji. Należy wybrać Yes a następnie Next:



3. Należy wprowadzić adres IP strony serwera, tj. 195.182.9.18 oraz opcjonalnie wybrać dla niego nazwę:



4. Po weryfikacji i nawiązaniu połączenia należy potwierdzić certyfikat strony serwera poprzez wybranie opcji Trust and Continue:

5. Wybrać metodę autentykacji Certificate, następnie wybrać Next:

6. Następnie wybieramy typ autentykacji klucza publicznego tj. Use certificate from Public-Key Cryptographic Standard (PKS #12) file oraz Check this if you don't have a certificate yet (Works Only with ICA certificates), po czym przechodzimy do kolejnego kroku wybierając Next:

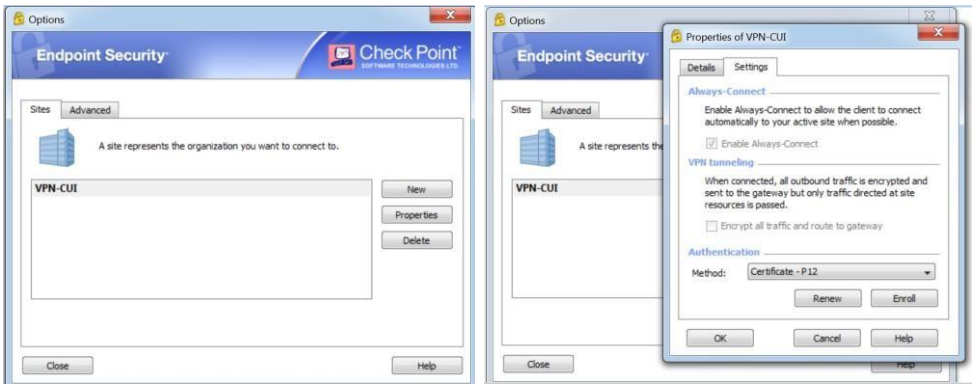
7. Po zakończeniu konfiguracji bramy dostępu VPN, należy utworzyć certyfikat wybierając opcję Yes:

8. Proces tworzenia Certyfikatu VPN wymaga utworzenia nowego hasła składającego się z minimum 8 znaków alfanumerycznych (zaleca się używania co najmniej trzech grup znaków w haśle tj. A..Z, a..z, 0..9) oraz powtórzenia go w celu potwierdzenia zgodności. Utworzone hasło posłuży do uwierzytelnienia użytkownika podczas połączenie poprzez sieć VPN. Ostatnim krokiem jest wprowadzenie otrzymanego wcześniej klucza rejestracyjnego VPN. Po wypełnieniu odpowiednich pól należy wybrać Enroll:

9. Po otrzymaniu informacji o poprawnym wygenerowaniu certyfikatu należy zapisać go na dysku lokalnym (nie należy zapisywać na dysku usb, sieciowym, ścieżce użytkownika systemu lub w katalogu instalacyjnym). Usunięcie Certyfikatu uniemożliwi wykonanie zdalnego połączenia do sieci.

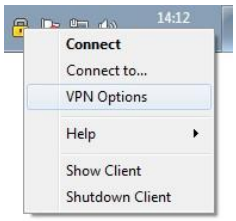
10. Przy wykorzystaniu nowo utworzonego hasła można połączyć się poprzez sieć VPN:

11. W przypadku generowania certyfikatu VPN na zainstalowanej wcześniej wersji klienta VPN lub próbie późniejszego generowania certyfikatu VPN należy wejść do panelu opcji VPN Options , następnie opcje Properties, zakładka Settings i wybór metody autentykacji Certificate – P12. Po potwierdzeniu poprzez Enroll należy postępować zgodnie procedurą opisaną w punkcie 5.8.

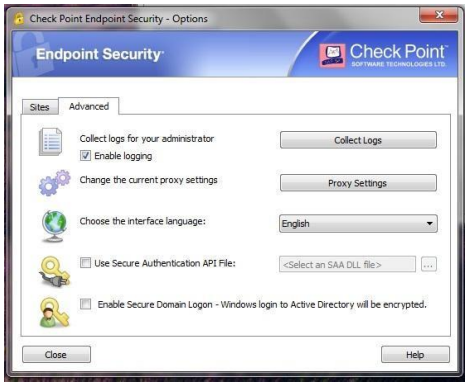


6. Zebranie logów Klienta VPN

1. Wybieramy opcję VPN Options.



2. Następnie zakładka Advanced i zazaczamy Enable logging. Następnie używamy klienta VPN jak dotychczas – do etapu wystąpienia błędów.



3. W celu zebrania logów należy wybrać „Collect Logs” po czym otworzy się docelowa paczka w katalogu Temp Windowsa, np. „trlogs_15-04-2015_13.05.21.cab”. Uwaga: będąc w paczce wychodzimy z niej, po czym kopiujemy w bezpieczne miejsce.