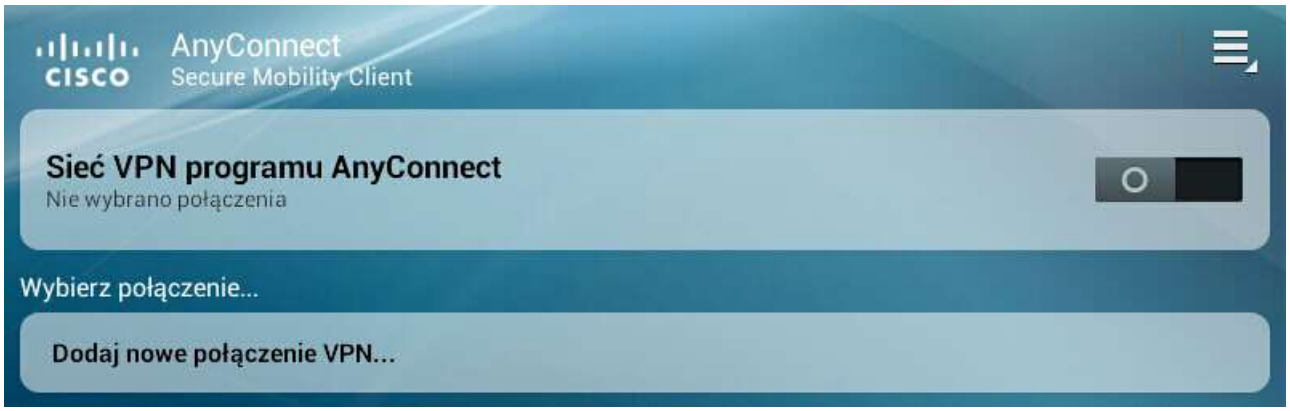
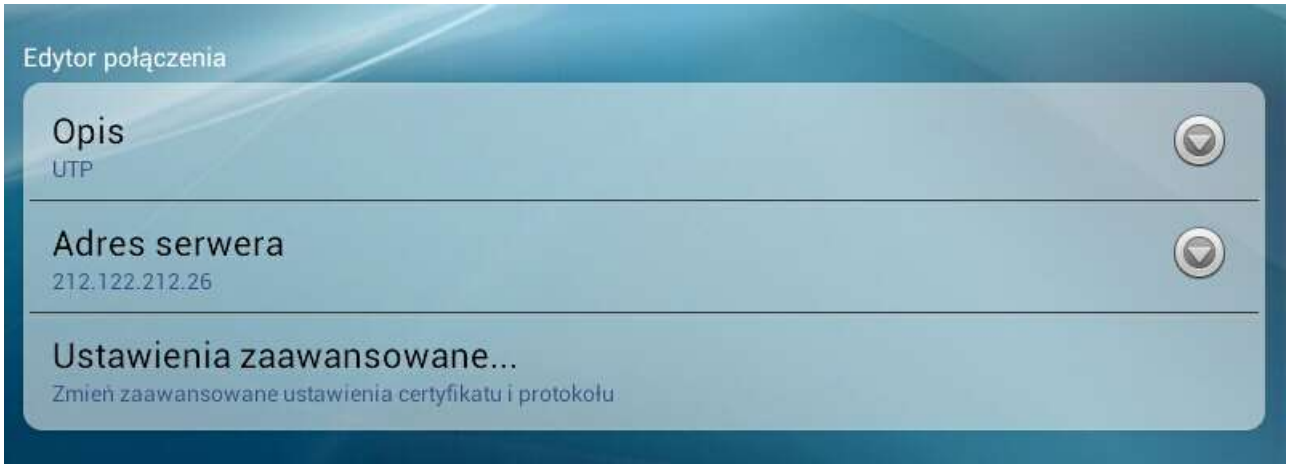
1. Uzyskanie dostępu do usługi VPN dla pracowników Uniwersytetu Technologiczno-Przyrodniczego

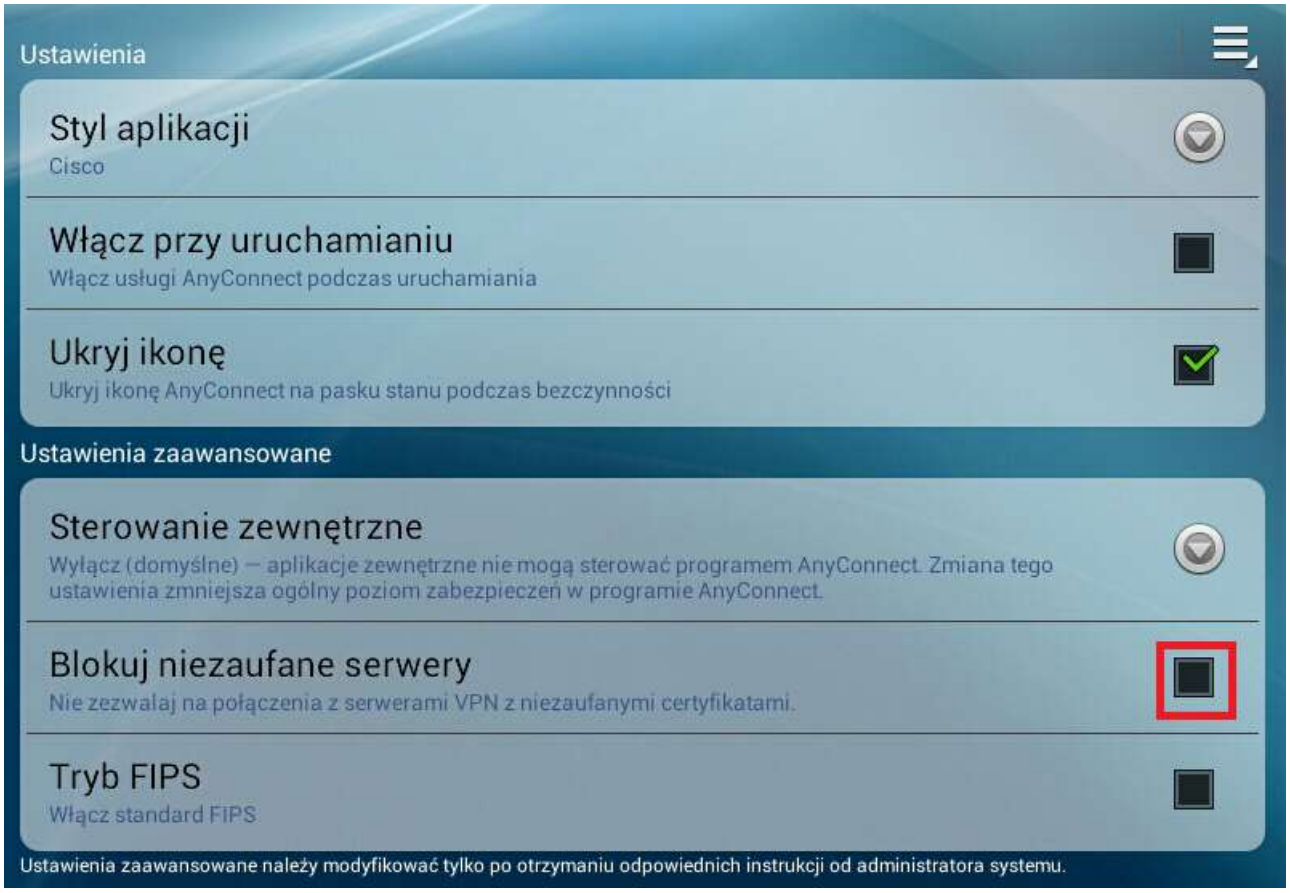
   Aby aktywować dostęp zdalny dostęp do zasobów ogólnych UTP (np. intra) i/lub zasobów dostępnych w sieciach wydziałowych należy:
   a) posiadać aktywne konto pocztowe zabezpieczone zgodnie z aktualnymi wytycznymi bezpieczeństwa. W przypadku braku konta można je założyć osobiście wypełniając formularz:
   http://uorsk.utp.edu.pl/download.php?file=wniosek-mail-PRACOWNIK.doc
   Zmianę hasła na spełniające wymogi można dokonać na stronie:
   https://mail.utp.edu.pl/haslo/
   W celu odzyskania zapomnianego hasła należy skontaktować się z Działem Teleinformatyki(DT).
   b) zgłosić chęć korzystania z VPN do pracownika DT dodając informację do jakich zasobów pracownik chciałby mieć dostęp

2. Urządzenia z systemem operacyjnym Android
   a. Krokiem pierwszym jest ściągnięcie ze sklepu Google play odpowiedniej wersji aplikacji „AnyConnect". Ogólne porady przy wybieraniu swojej wersji:
      i. Firma Cisco pracuje z niektórymi producentami urządzeń mobilnych i dostarcza oprogramowanie w wersji „VENDOR AnyConnect", gdzie VENDOR to producent sprzętu. W chwili pisania tej instrukcji były dostępne wersje dla Samsunga, HTC oraz Kindle. Producent oprogramowania zaleca skorzystania z takiej wersji w pierwszej kolejności
      ii. Jeżeli poprzedni klient nie może zadziałać na konkretnym urządzeniu należy skorzystać z wersji „AnyConnect ICS+". Aplikacja ta będzie pracowała tylko na systemach Android w wersji przynajmniej 4.0 oraz może nie wspierać wszystkich funkcjonalności
      iii. Dla systemów z wersją oprogramowania starszą niż 4.0 można skorzystać z wersji „Rooted AnyConnect" albo inną już nieaktualizowaną, dostępną dla niektórych dostawców
   b. Po zainstalowaniu należy uruchomić aplikację, przeczytać i zaakceptować regulamin
   c. Klikamy „Dodaj nowe połączenie VPN…", uzupełniamy parametry zgodnie z rysunkiem i naciskamy gotowe

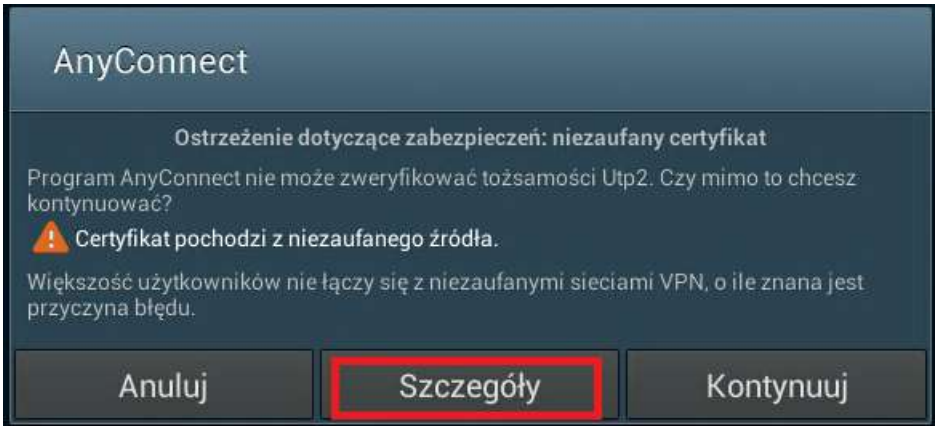


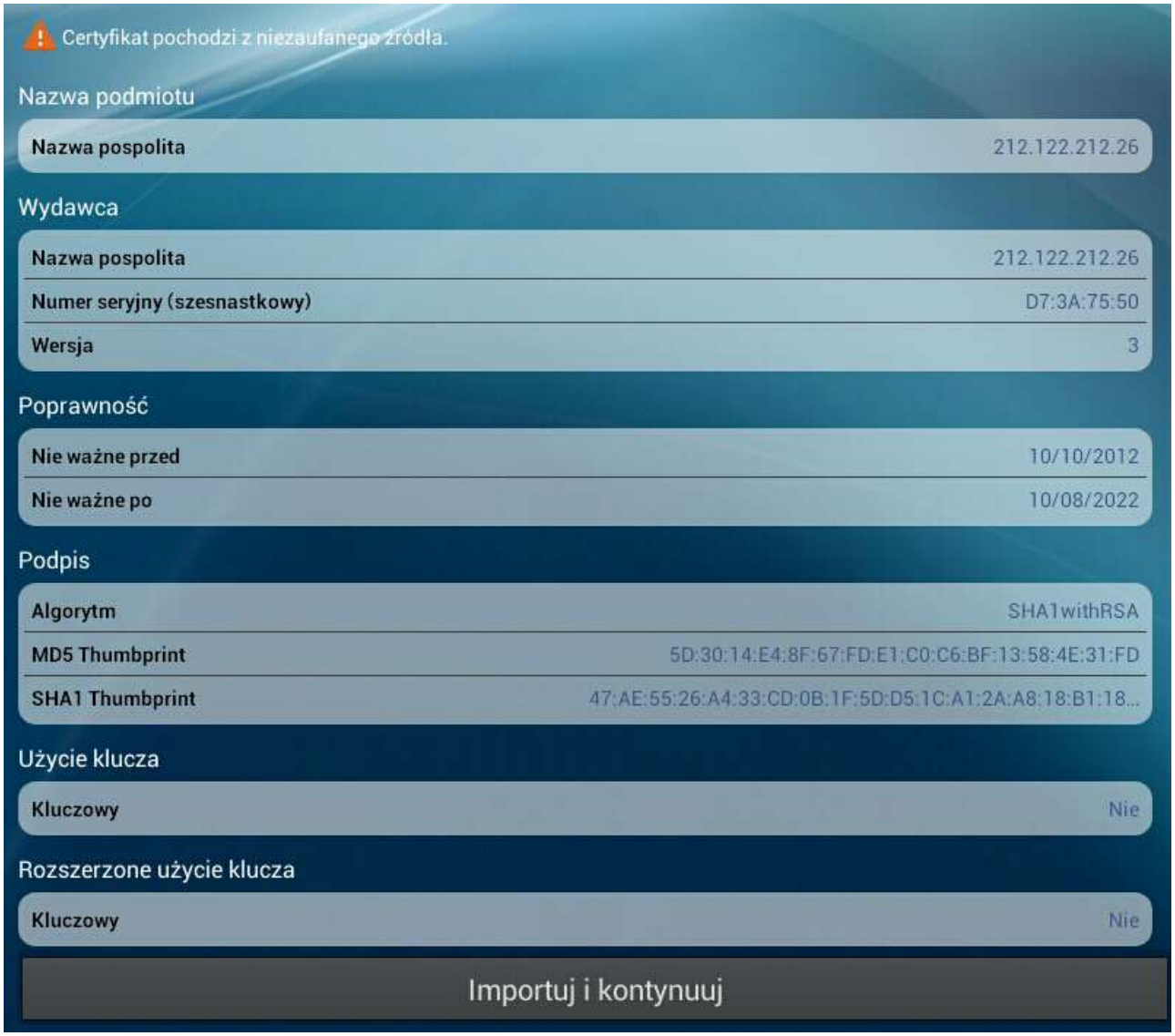


d. Przed pierwszym połączeniem należy przejść do ustawień aplikacji i wyłączyć opcję „Blokuj niezaufane serwery”

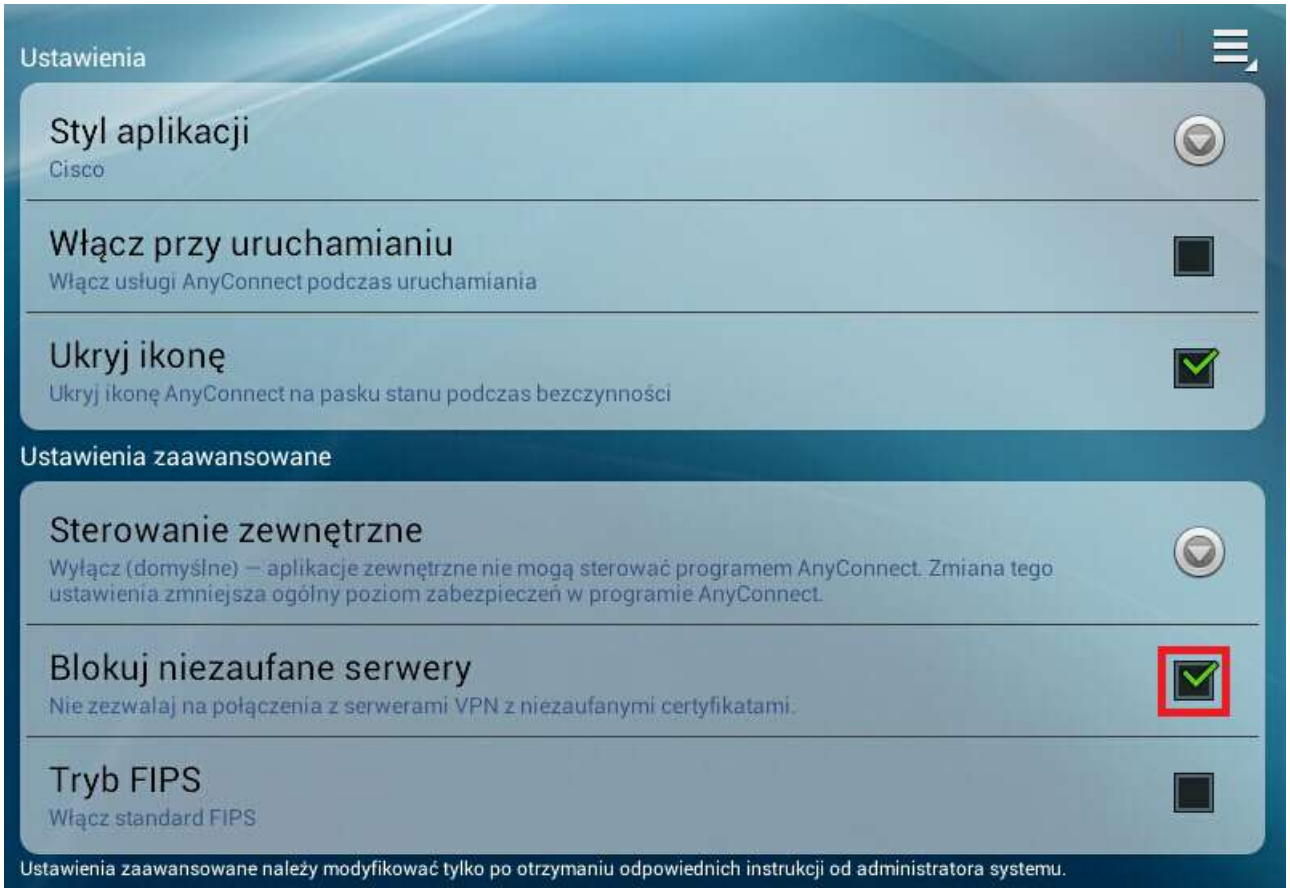


e. Podczas łączenia musimy dodać certyfikat serwera VPN do zaufanych. Najpierw klikamy szczegóły, a potem





f. Po połączeniu i dodaniu certyfikatu należy z powrotem aktywować opcję „Blokuj niezaufane serwery”



Pełna instrukcja wraz z listą wspieranych urządzeń znajduje się na stronie producenta:

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/user/xmart/b_Android_User_Guide.pdf