



POLITECHNIKA WARSZAWSKA

VPN CI – Instrukcja użytkownika

Centrum Informatyzacji Politechniki Warszawskiej			
Autor: mgrinż. Robert Borysik		Zatwierdził: mgr Marcin Drozd	
Data publikacji: 2014.05.14	Sygnatura: USOS-SAP-VPN-A01	Wersja: 2.04-SAP	Dotyczy wersji USOS: 5.4.6
Dokument w wersji elektronicznej:		Docelowa grupa odbiorców: Pracownicy dziekanatów	

1. Wstęp

System USOS oraz SAP przetwarzają dane osobowe dlatego do korzystania z tych systemów niezbędne jest zestawienie szyfrowanego połączenia VPN pozwalającego na ochronę przesyłanych danych. Przed uzyskaniem dostępu do systemu USOS, SAP należy uzyskać formalną zgodę na przetwarzanie danych osobowych oraz wypełnić odpowiedni wniosek o uzyskanie dostępu potwierdzony przez kierownika danej jednostki organizacyjnej pracownika. Formularz wniosku przesyłany jest przez pracownika CI. Można także pobrać go ze strony z dokumentacją USOS na PW: <https://dokumentacja.usos.pw.edu.pl/>.

2. Inicjalizacja konta w systemie IDM

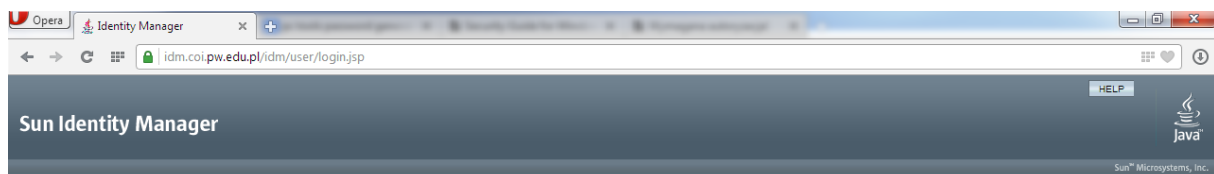
Pracownicy upoważnieni do przetwarzania danych osobowych i mający mieć dostęp do tych systemów otrzymują od Administratora VPN nazwę użytkownika oraz hasło pierwszego logowania.

Do poprawnego zadziałania połączenia VPN niezbędna jest zmiana otrzymanego hasła startowego usłudze SUN IDM. Procedura zmiany hasła wygląda następująco:

1. Przy pomocy dowolnej przeglądarki internetowej (należy udać się na stronę:

<https://idm.coi.pw.edu.pl/idm/user>

2. Następnie należy wprowadzić login i hasło otrzymane od Administratora:



Log In to Identity Manager

User ID

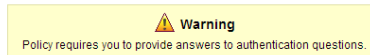
Password

[Forgot User ID?](#) [Forgot Password?](#)

Proszę zwrócić uwagę na małe i duże litery w hasle. W przypadku problemów z logowaniem trzeba zgłosić problem z kontem do działu Servicedesk CI – 5999@pw.edu.pl.



- W kolejnym kroku należy uzupełnić następujące informacje: numer PESEL, nazwisko panięskie matki oraz miejsce urodzenia. Dane te służą do weryfikacji tożsamości użytkownika. Opcja ta w przyszłości może pomóc w odzyskaniu zapomnianego lub utraconego hasła.



Change Answers to Authentication Questions

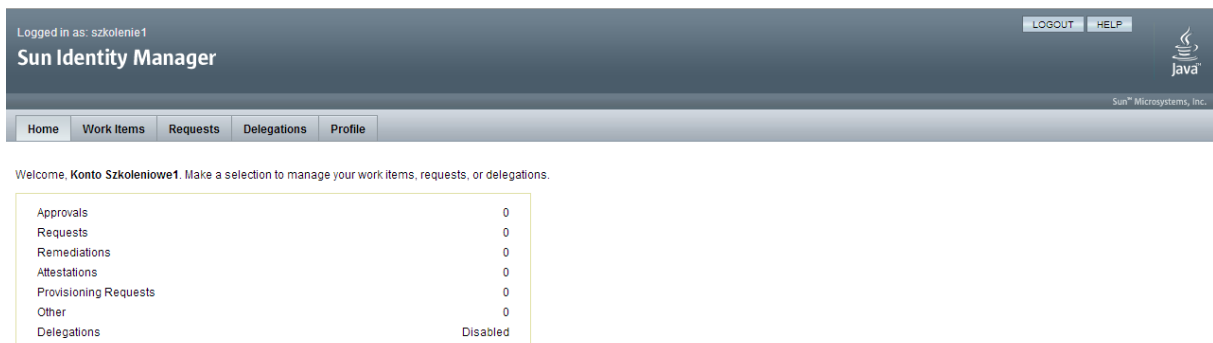
User Interface

Please answer the following questions. Answers will be automatically converted to upper-case.

Question	Answer
Podaj PESEL	<input type="text"/>
Podaj nazwisko panięskie matki	<input type="text"/>
Podaj miejsce urodzenia	<input type="text"/>

Policy	Constraints
Answer Policy Applies to all answers within a login interface.	None

- Po udzieleniu odpowiedzi należy nacisnąć przycisk „Save”. Po zapisaniu danych powinien zostać wyświetlony następujący ekran:



- Następnie należy kliknąć zakładkę „Profile”: W zakładce „ChangePassword” należy wpisać dwukrotnie nowe hasło do usług IDM i VPN i nacisnąć przycisk „Save”:



Change Password

To change your password, enter a new password below and click Save.

Password

Confirm Password

Passwords must conform to the following rules:

- Must be between 8 and 16 characters in length
- Must not contain values of attributes: email, lastname, firstname, fullname



Hasło musi spełniać założenia polityki bezpieczeństwa (długość od 8 do 16 znaków oraz składać się z trzech grup znaków np. DUŻE LITERY, małe litery, cyfry lub znaki specjalne, nie może natomiast zawierać w sobie adresu e-mail, imienia, nazwiska lub loginu).

6. Na kolejnym ekranie należy wprowadzić ponownie hasło startowe otrzymane od Administratora VPN (hasło, przy pomocy którego wykonywane było pierwsze logowanie do usługi IDM) i potwierdzić przyciskiem „OK”:

Logged in as: usos1st

Sun Identity Manager

LOGOUT HELP

Home Work Items Requests Delegations Profile

Sun Microsystems, Inc.

Enter Your Current Identity Manager Login Information

You are required to enter the information below before the requested action can be completed.

Password

OK Cancel

7. W przypadku, gdy nowe hasło nie spełni założeń polityki bezpieczeństwa pojawi się komunikat:

Logged in as: szkolenie1

Sun Identity Manager

LOGOUT HELP

Home Work Items Requests Delegations Profile

Change Password Account Attributes Authentication Questions Access Privileges

Error
Policy Violation (Password on Lighthouse User): Minimum length is 8.

Change Password

To change your password, enter a new password below and click Save.

Password

Confirm Password

Passwords must conform to the following rules:

- Must be between 8 and 16 characters in length
- Must not contain values of attributes: email, lastname, firstname, fullname

Save Cancel

Należy wówczas wprowadzić hasło zgodne z wymaganiami z pkt 5.

8. W przypadku błędnego wprowadzenia starego hasła w pkt 6 pojawi się komunikat:



Logged in as: usostst LOGOUT HELP

Sun Identity Manager

Home Work Items Requests Delegations Profile

✖ Error
Login attempt failed for user usostst.
- Identity Manager (Identity Manager):Invalid Password.

Enter Your Current Identity Manager Login Information

You are required to enter the information below before the requested action can be completed.

Password

OK Cancel

Należy wówczas wrócić do pkt 5.

9. Udaną operację zmiany hasła potwierdza komunikat:

Logged in as: usostst LOGOUT HELP

Sun Identity Manager

Home Work Items Requests Delegations Profile

✔ Operation Successful
The requested operation completed successfully.

OK

10. Należy zapamiętać lub zachować nowe hasło do usługi VPN. Proszę zauważyć, że login nie ulega zmianie. Nie jest dopuszczalne udostępnianie hasła innym osobom.

11. Ostatni krok w IDM polega na uzupełnieniu lub weryfikacji adresu email. W tym celu należy w zakładce „Profile” wybrać „AccountAttributes”, zweryfikować lub wprowadzić swój e-mail i zatwierdzić przyciskiem „Save”.

Logged in as: usostst LOGOUT HELP

Sun Identity Manager

Home Work Items Requests Delegations Profile

Change Password Account Attributes Authentication Questions Access Privileges

Change User Account Attributes

Use this page to change multiple user account attributes.
To save your changes, click **Save**.

Account ID usostst

Email Address

Authentication Questions

For Login Interface Default

Account Information

Assigned Resources usos-vpn

Current Resource Accounts usos-vpn: cn=usostst,ou=USOS,dc=ad,dc=pw,dc=edu,dc=pl

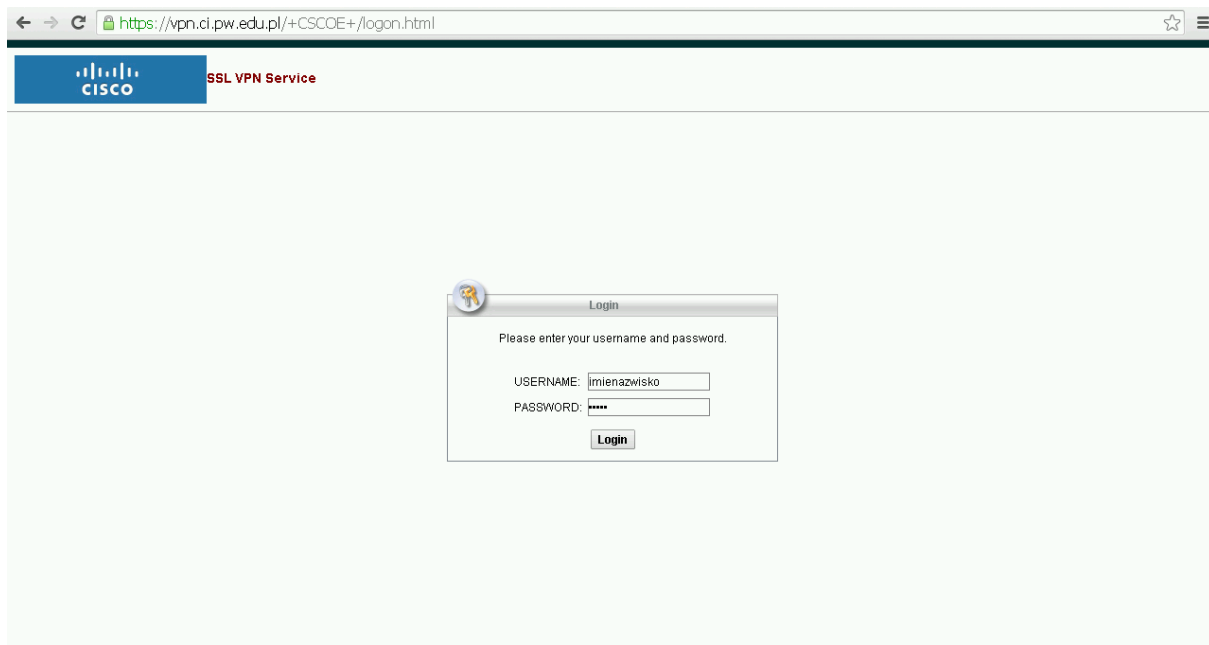
Save Cancel

3. Instalacja oprogramowania CISCO VPN

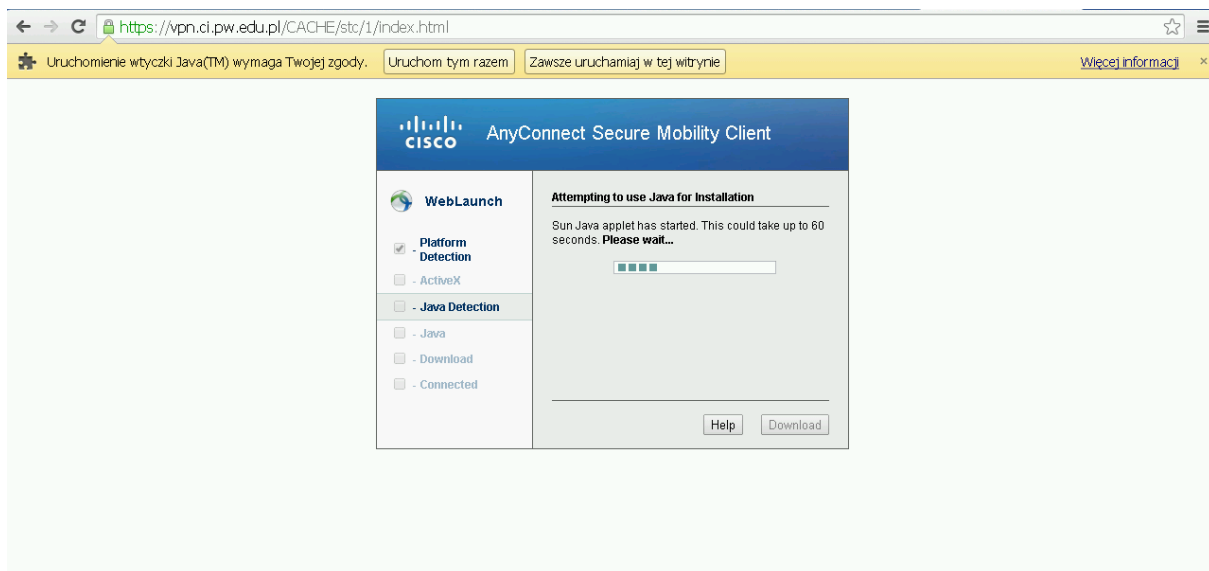
Warunkiem poprawnej instalacji jest posiadanie aktualnej wersji Javy (JRE w wersji nie niższej niż 7.55). Należy w przeglądarce wpisać adres:

<https://vpn.ci.pw.edu.pl>

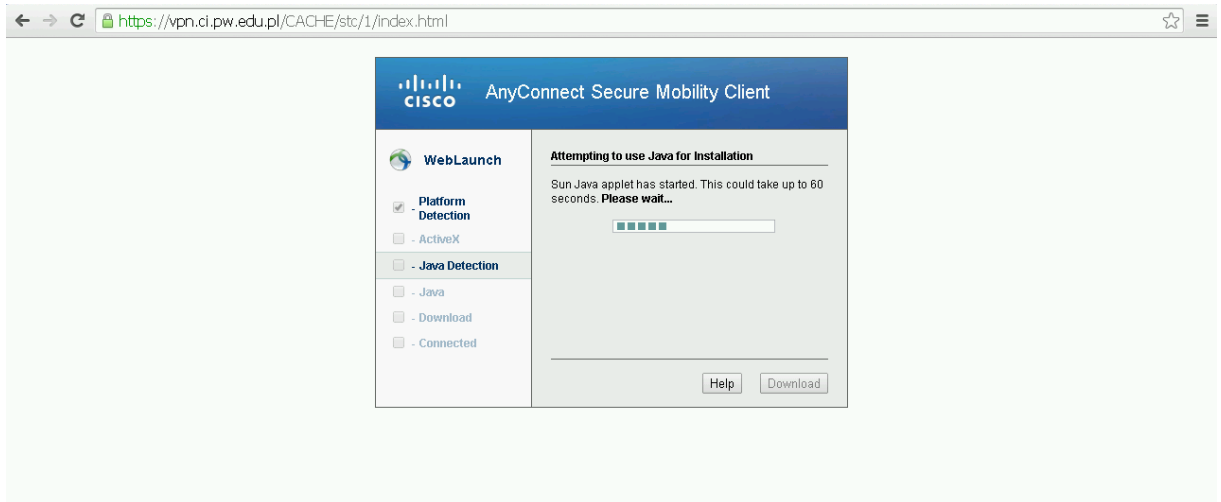
Należy podać login i hasło do usługi VPN, ustawione zgodnie z punktem 2.5:



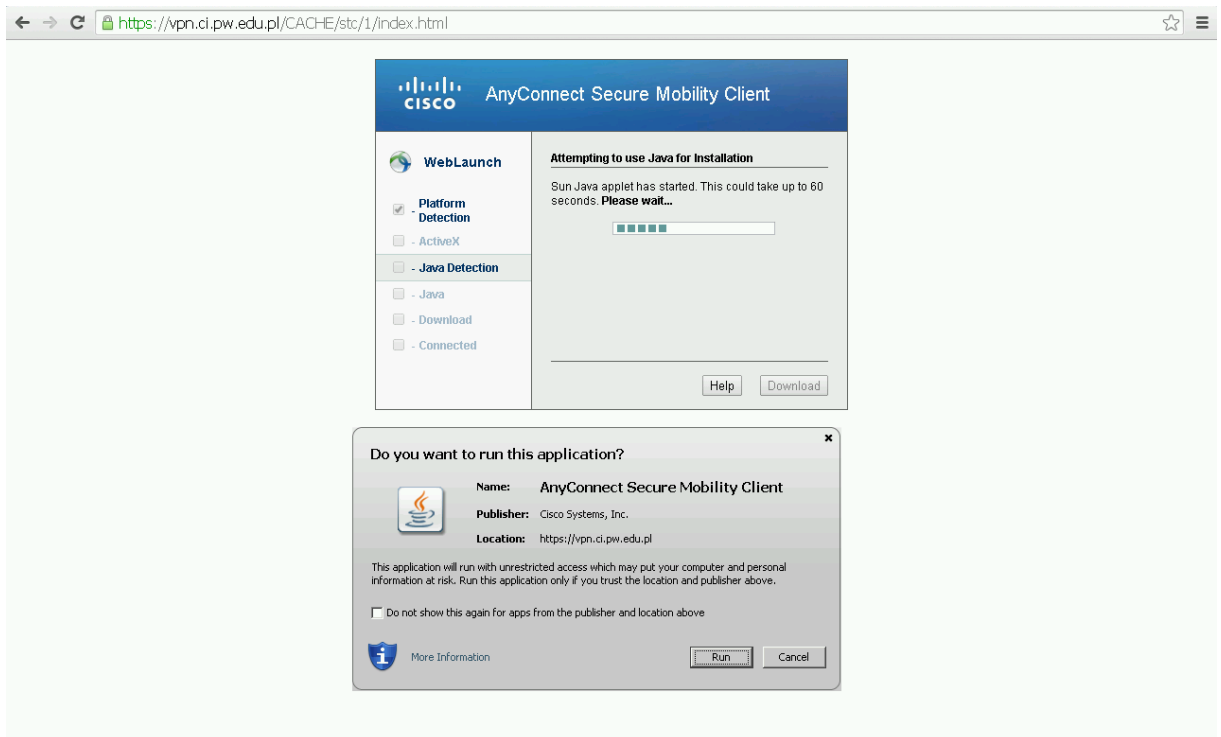
Należy zezwolić na uruchomienie wtyczki Java:



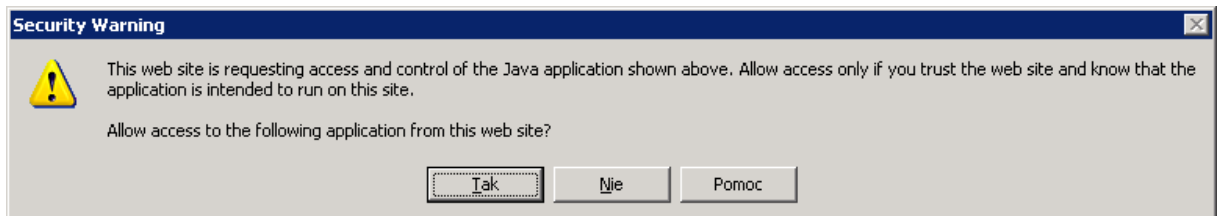
Rozpocznie się proces instalacji klienta Cisco Anyconnect:



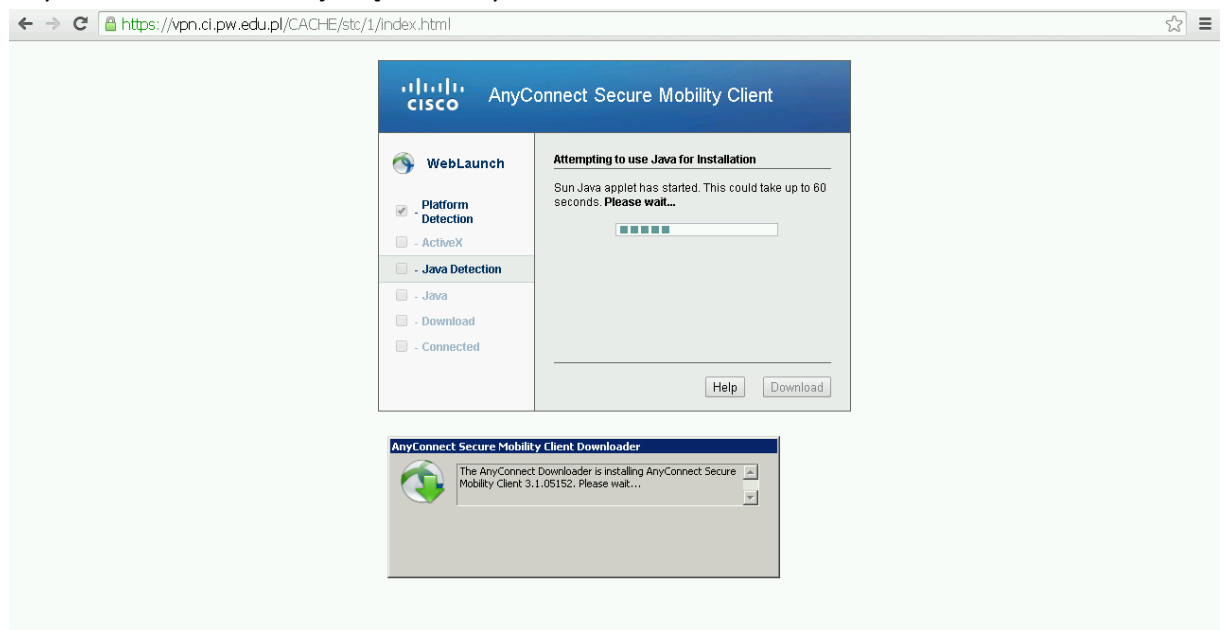
Należy zezwolić na uruchomienie aplikacji:



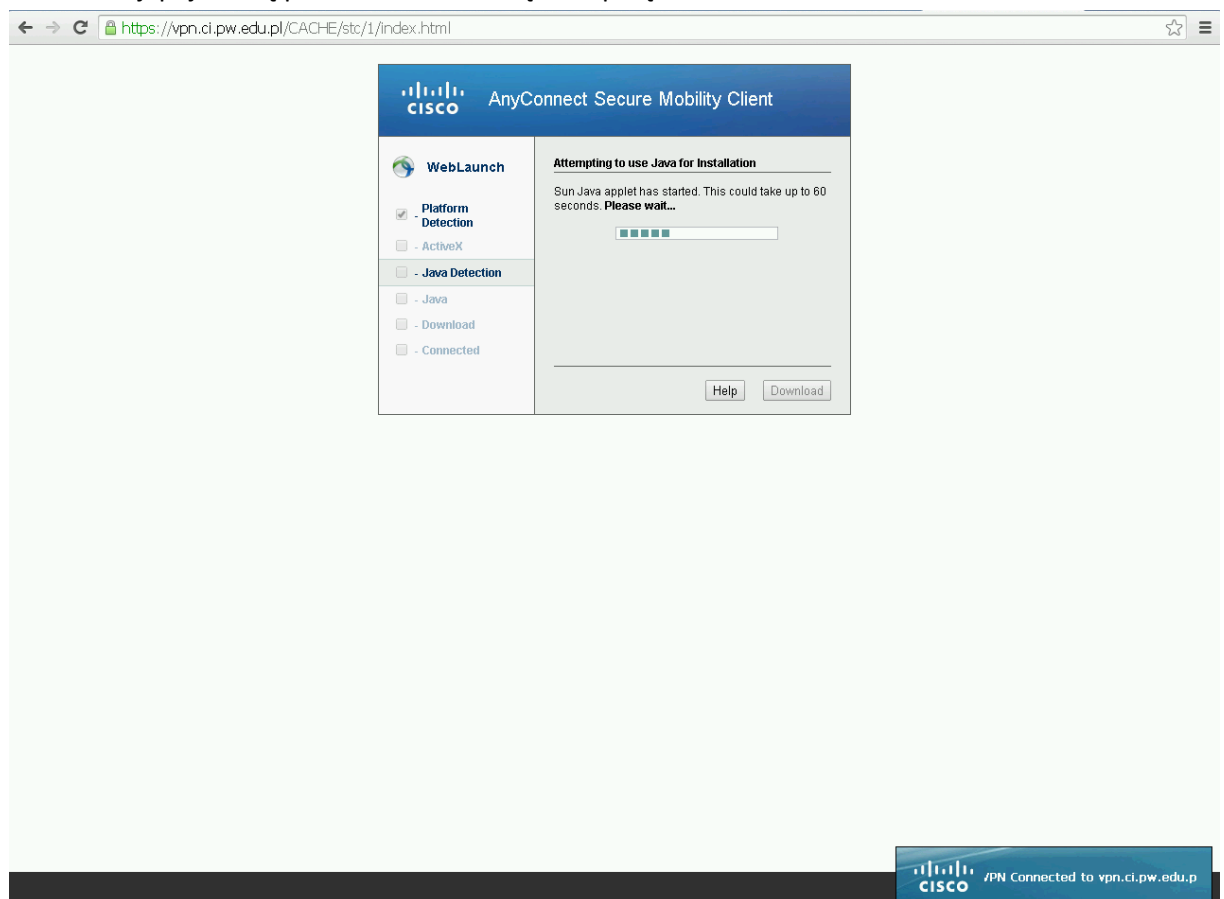
Należy odpowiedzieć TAK::



Anyconnect VPN zainstaluje się automatycznie:




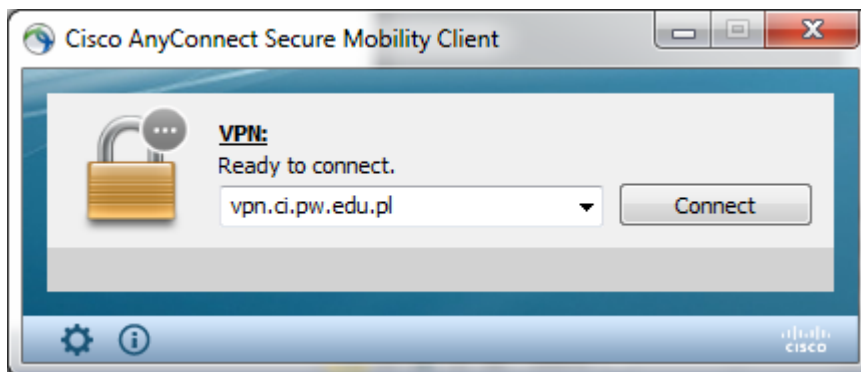
Po instalacji pojawi się potwierdzenie nawiązania połączenia z VPN.



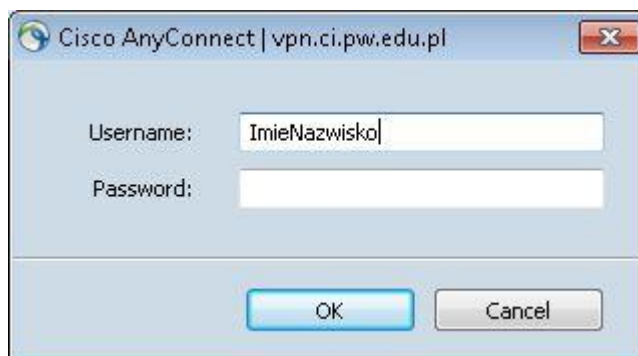



4. Uruchomienia oprogramowania CISCO VPN

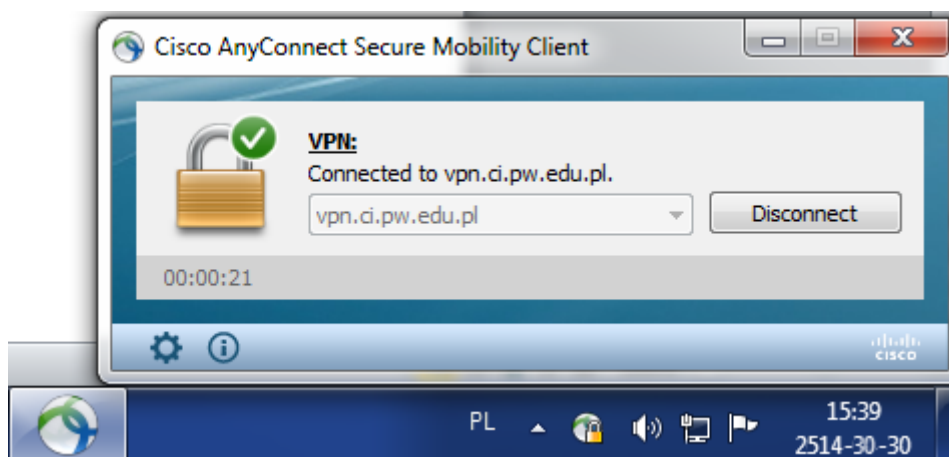
1. Należy uruchomić przy pomocy ikonki  z Pupitu lub Menu Start (Modern UI w systemach Windows 8.1 Update) CISCO AnyconnectSecureMobility Client.
2. W polu VPN powinien widnieć wpis vpn.ci.pw.edu.pl. Jeśli jest tam puste pole należy uzupełnić i kliknąć przycisk Connect:



3. Należy wprowadzić swój login (username) i hasło ustawione w pkt 2.5.



4. Zestawienie sesji VPN sygnalizuje ikonka z kłódką  na pasku zadań.
5. Po zakończeniu pracy można rozłączyć połączenie VPN przyciskiem Disconnect:



UWAGA:

Nie jest możliwe zestawienie więcej niż jednego połączenia przy pomocy tego samego loginu i hasła.