Podstawowa konfiguracja modułu Scalance W788-1PRO

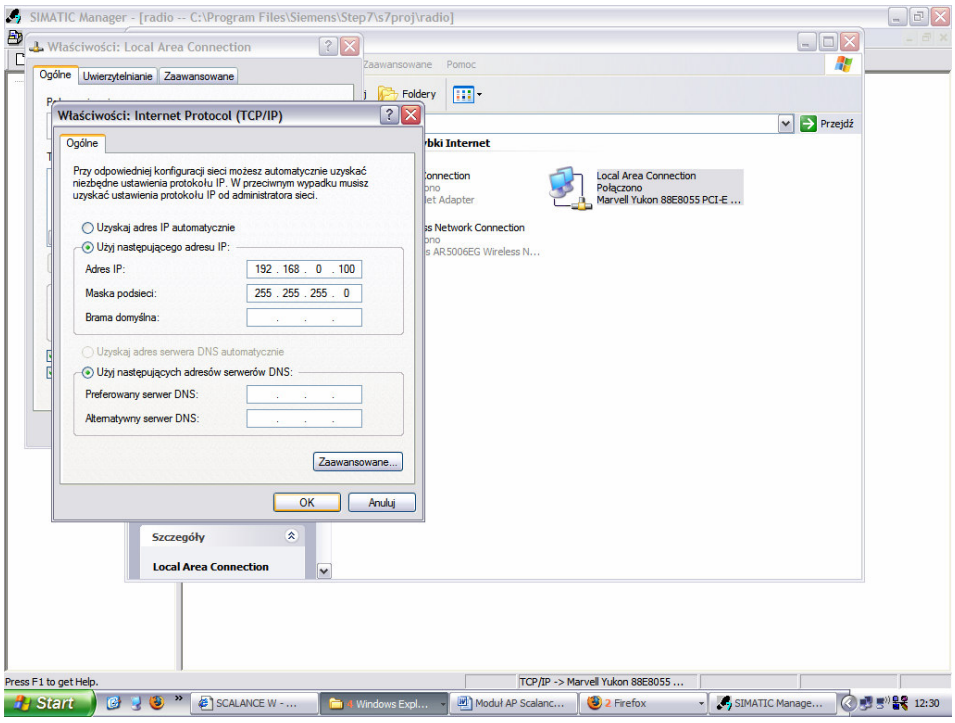
1. Połączenie z modułem oraz przypisanie adresu IP.

Pierwszym krokiem w konfiguracji modułu Scalance W788-1PRO jest przypisanie adresu IP, ponieważ fabrycznie jest on wyzerowany.

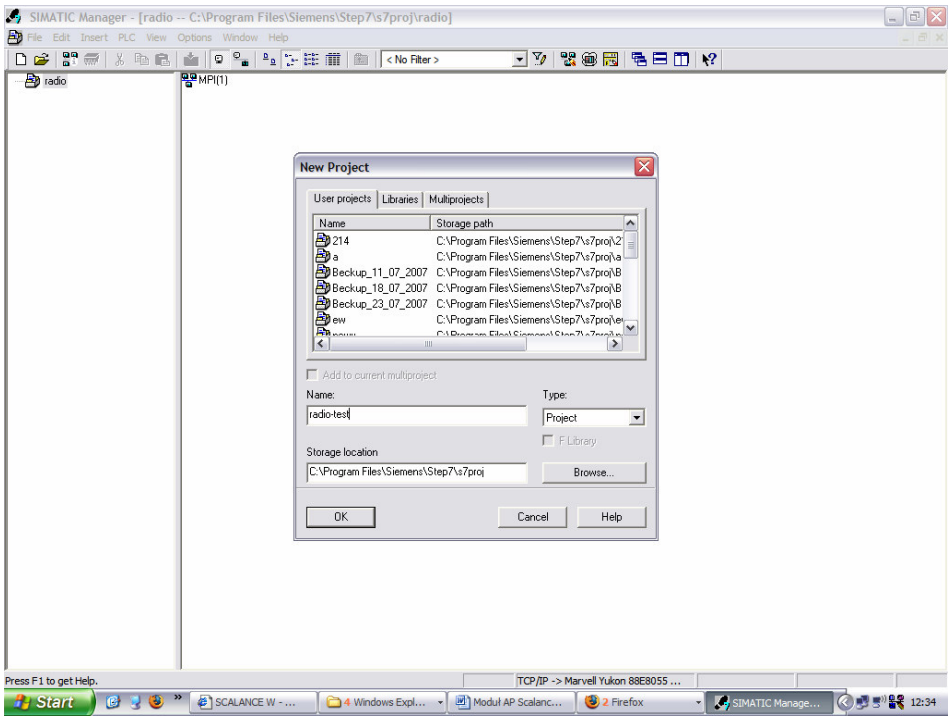
Konfigurację przeprowadzimy za pomocą narzędzia SIMATIC STEP 7.

Łączymy się z modułem przez łącze Ethernet'owe.

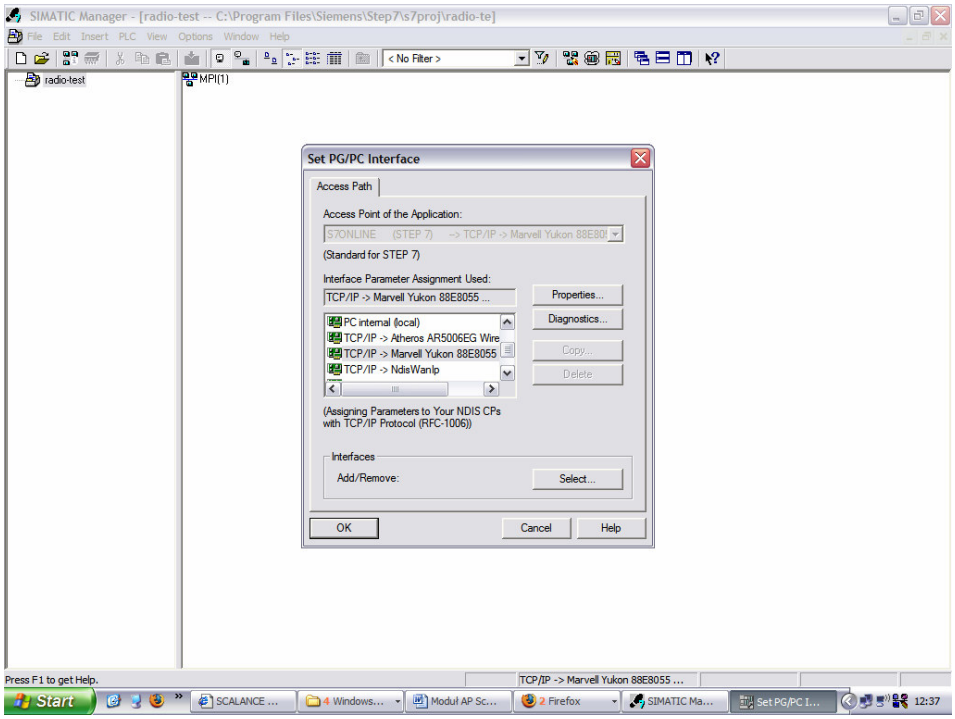
Należy pamiętać o ustawieniu adresu IP oraz maski podsieci karty sieciowej naszej stacji PC, np.: 192.168.0.100; 255.255.255.0



Uruchamiamy narzędzie STEP 7 i tworzymy nowy projekt.



Przechodzimy do menu „Options” i wybieramy „Set PG/PC Interface…”

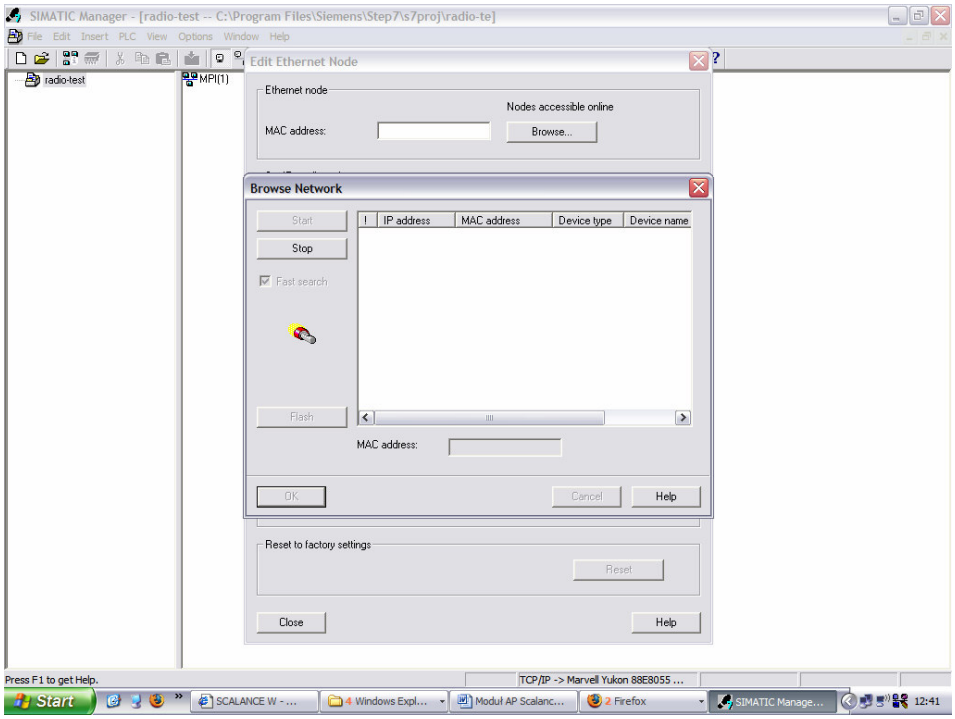


Wybieramy interfejs sieci Ethernet naszej stacji PC z protokołem TCP/IP.

Uwaga!
Konfigurację modułu możemy przeprowadzić również za pomocą połączenia bezprzewodowego; w takim przypadku konfigurujemy i wybieramy interfejs bezprzewodowy, a następnie łączymy się z modułem (SSID: „Siemens Wireless Network).

Przechodzimy do menu „PLC" i wybieramy „Edit Ethernet Node".

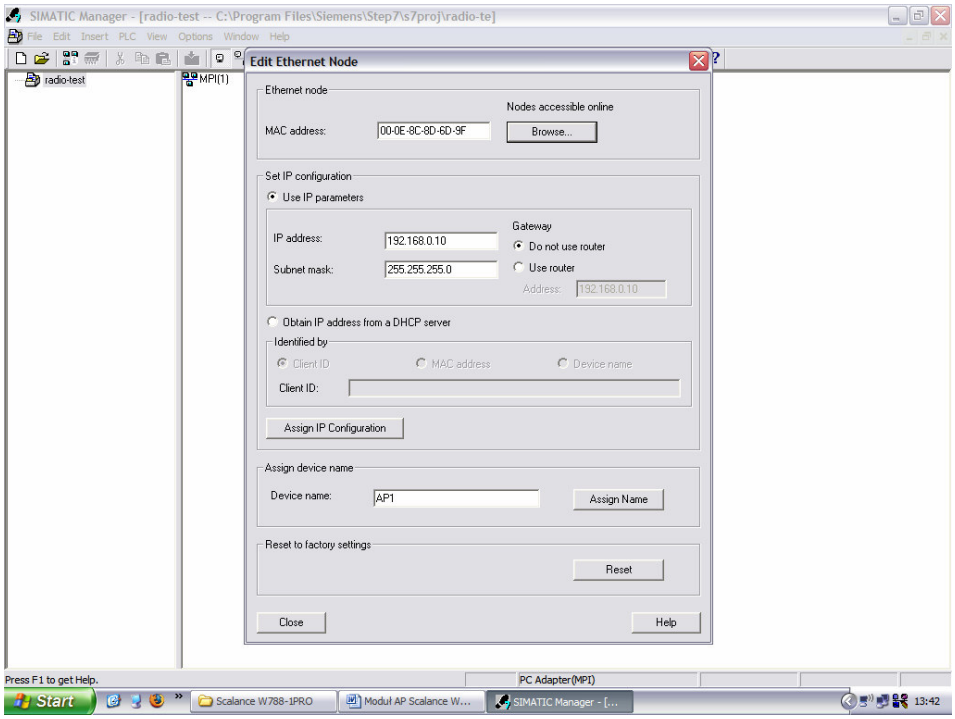
Następnie klikamy na przycisk „Browse…" w polu „Ethernet node".



Narzędzie wyszukuje dostępne w sieci urządzenia.

W przeglądarce powinien pojawić się nasz moduł, który rozpoznamy po adresie MAC oraz adresie IP 0.0.0.0 .

Zatwierdzamy wybór.



W polu „Set IP configuration” wybieramy „Use IP parameters” i wpisujemy adres oraz maskę z zakresu naszej podsieci,
np.: 192.168.0.10; 255.255.255.0

Zaznaczamy pole „Gateway -> Do not use router”.

Chcąc zatwierdzić konfigurację IP, klikamy na „Assign IP Configuration”.

W polu „Assign device name” wpisujemy dowolną nazwę naszego modułu,
np. „AP1”, i zatwierdzamy przyciskiem „Assign Name”.

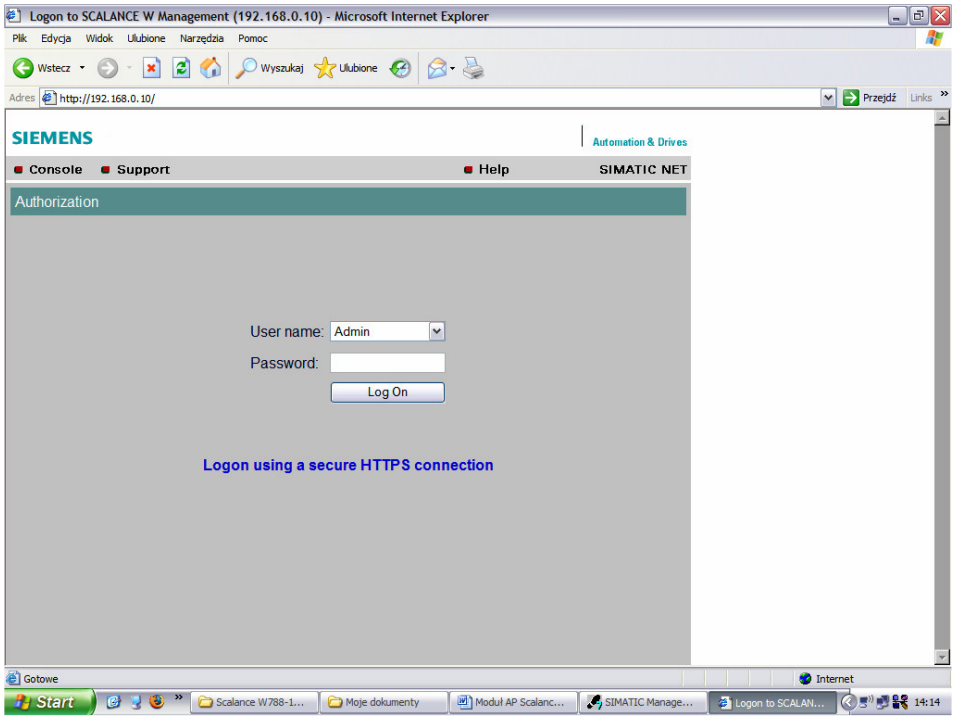
Opuszczamy okno konfiguracyjne klikając na „Close”, kończymy pracę z programem STEP 7.

W ten sposób skonfigurowaliśmy nasz moduł do komunikacji w sieci Ethernet, co pozwala nam na dalszą konfigurację z wykorzystaniem przeglądarki internetowej.

Uwaga.
Taką samą konfigurację możemy także przeprowadzić również za dostarczanego przez producenta narzędzia Primary Setup Tool (PST), które znajdziemy na dołączonej do urządzenia płycie CD.

2. Konfiguracja modułu z wykorzystaniem kreatora.

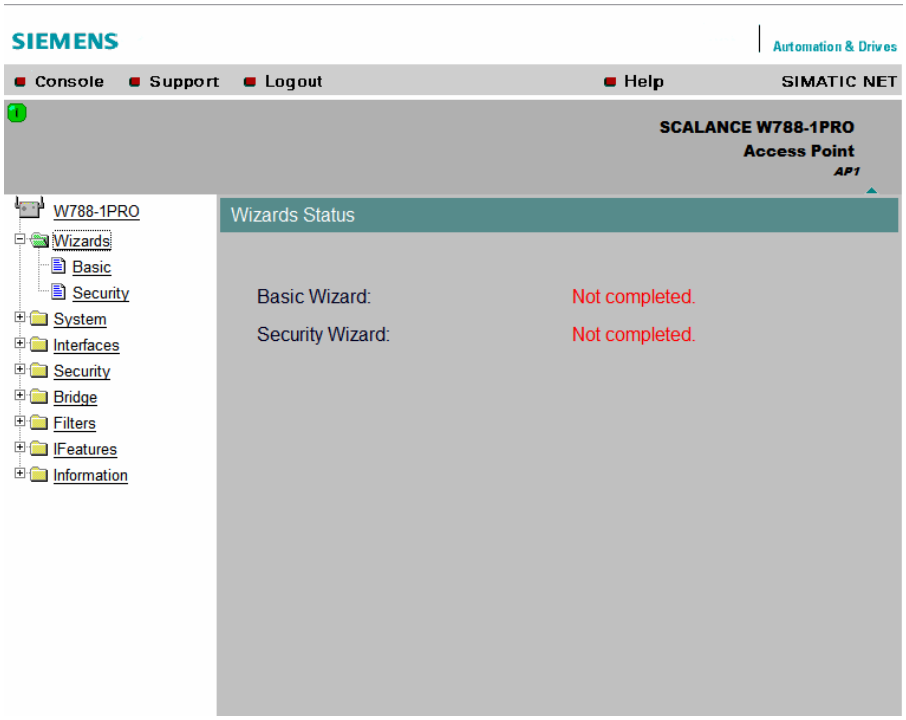
W przeglądarce internetowej wpisujemy adres IP, który przypisaliśmy naszemu modułowi.



Pojawia się okno logowania.
Domyślnie „User name” oraz „Password” ustawione są na wartości: Admin, admin lub User, user.

Ze względów bezpieczeństwa po pierwszym logowaniu wartości te należy zmienić!

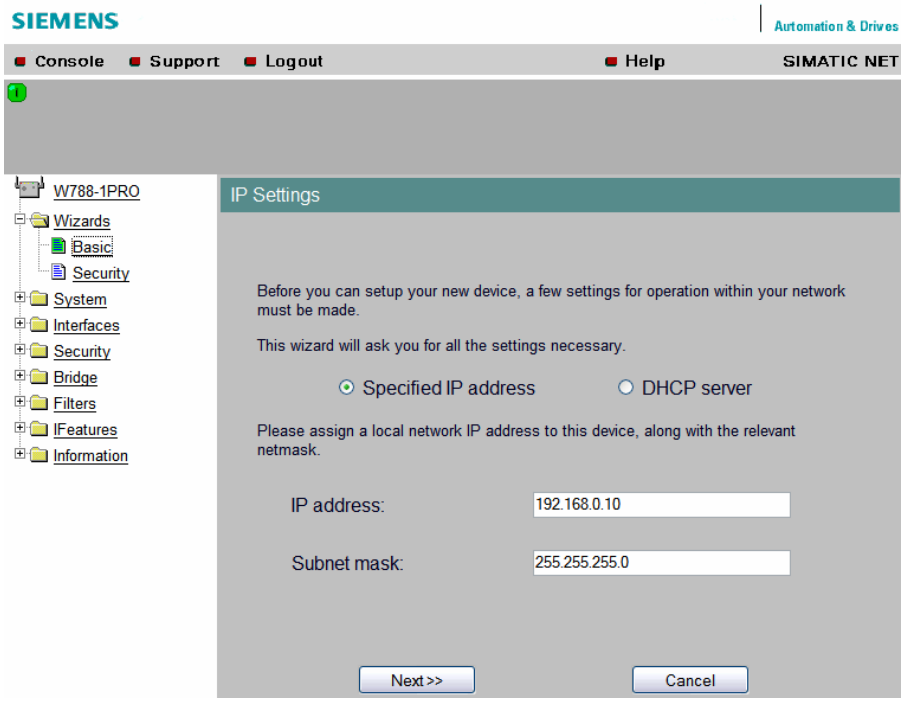
Po zalogowaniu przechodzimy do menu „Wizards”.
Producent zadbał o specjalne kreatory podstawowych ustawień, od których zaczynamy konfigurację modułu.



Wybieramy zakładkę „Basic” i pojawia się przed nami okno ustawień IP.

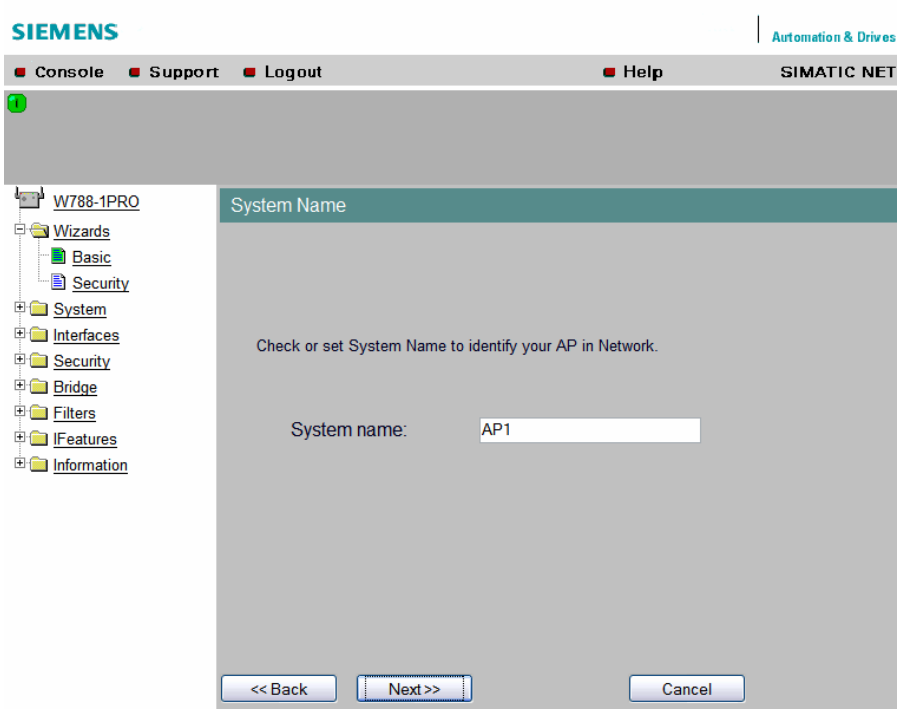
IP Settings

Widzimy, że moduł posiada przypisany przez nas adres i maskę, uprzednio wybierając opcję „Specified IP address”.
Jeżeli posiadamy w naszej sieci Server DHCP, który automatycznie przydziela adresy IP wszystkim stacjom w tej sieci, możemy wybrać opcję „DHCP server”.



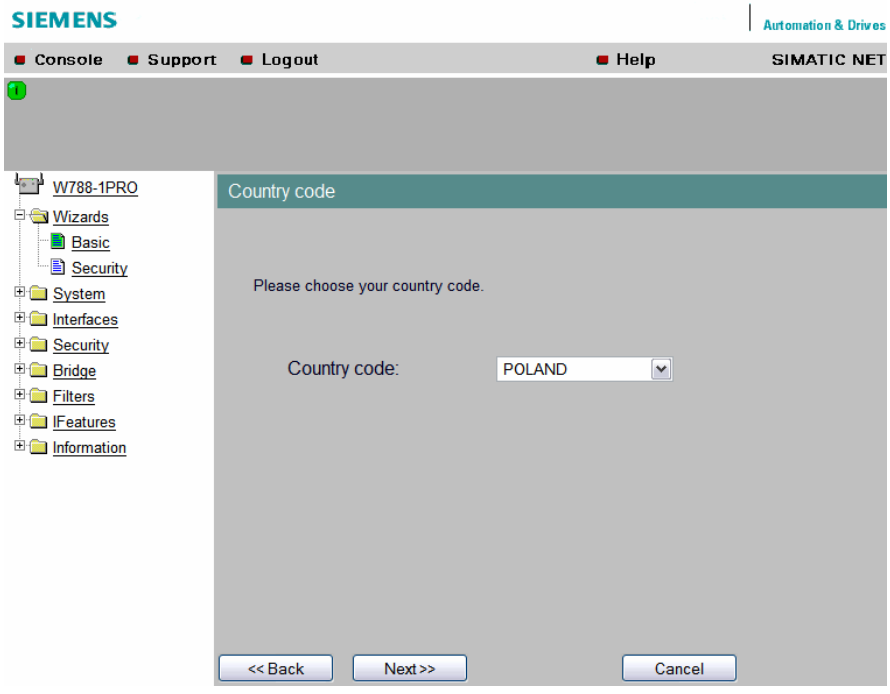
System Name

W następnym oknie widzimy nadaną wcześniej przez nas urządzeniu nazwę, którą możemy zmienić.



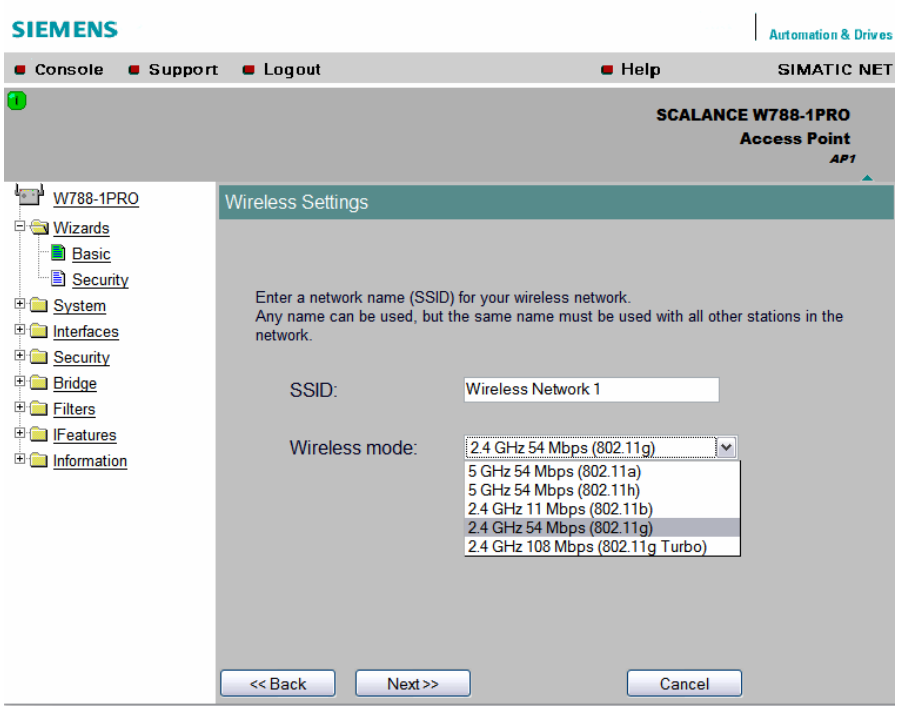
Country Code

Następne okno to wybór kodu kraju, w którym znajduje się nasz moduł. Dzięki temu automatycznie ustawiane są wartości m.in. mocy wyjściowej czy zakresów częstotliwości, obowiązujące w danym kraju.



Wireless Settings

Tutaj mamy możliwość nadania nazwy SSID, która będzie rozgłaszana na zewnątrz jako identyfikator naszej sieci bezprzewodowej.
Nazwa ta musi być unikalna, a ze względów bezpieczeństwa nie powinna zawierać informacji o charakterze sieci czy też jej zasobach.
Maksymalna długość 32 znaki, bez polskich znaków.



W tym samym oknie wybieramy tryb, w którym będzie pracowała nasza sieć bezprzewodowa, w zależności od pożądanego pasma, prędkości transmisji czy mocy sygnału.
Charakterystykę trybów pracy sieci bezprzewodowej przedstawia poniższa tabelka.

Standard	**802.11b**	**802.11g**	**802.11a/h**	**802.11a/h**	**802.11a/h**	**802.11a/h ***
Zakres	2,4 GHz	2,4 GHz	5,15-5,25 GHz	5,25-5,35 GHz	5,4-5,7 GHz	5,7-5,8 GHz
Maks. prędkość transmisji	11 Mbps	54 Mbps , 108 Mbps – tryb Turbo	54 Mbps	54 Mbps	54 Mbps	54 Mbps
Liczba nienakładających się kanałów	3	3	4	4	10/11	5/4
Transmitowana moc	100 mW EIRP (ETSI), 1 W (FCC)	100 mW EIRP (ETSI), 1 W (FCC)	200 mW EIRP (ETSI), 50 mW (FCC)	200 mW EIRP (ETSI), 250 mW (FCC)	1 W EIRP (ETSI)	1 W (FCC)
Modulacja	DSSS, HR-DSSS	DSSS, HR-DSSS, OFDM	OFDM	OFDM	OFDM	OFDM
Przenikanie przez ściany	Średnie	Średnie	Słabe	Słabe	Słabe	Słabe
Odbicia od przeszkód	Mocne	Brak informacji	Mocne	Mocne	Mocne	Mocne
Ryzyko interferencji z innymi urządzeniami	Średnie	Średnie	Małe	Małe	Bardzo małe	Bardzo małe

* - pasmo niedozwolone w Polsce.

Uwagi:

Standard 802.11h jest rozwinięciem 802.11a o mechanizmy kontroli mocy transmisji (TPC) oraz dynamicznego doboru częstotliwości (DFS), w celu uniknięcia zakłócania częstotliwości radarowych. Urządzenia posiadające te mechanizmy mogą pracować z wykorzystaniem większych mocy.

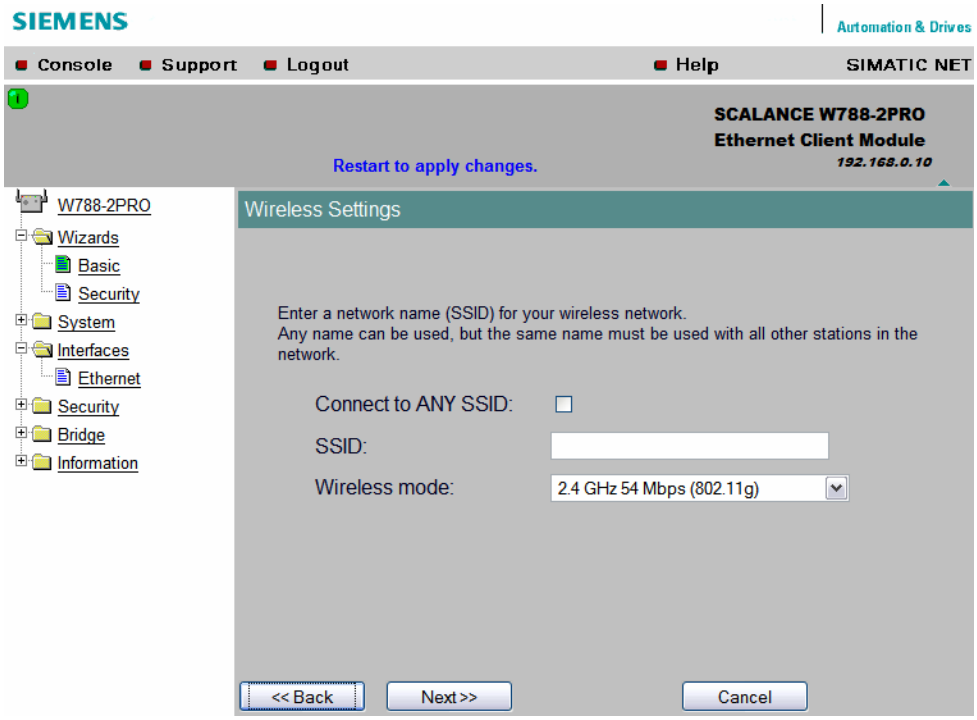
Podana maksymalna prędkość transmisji odnosi się do prędkości transmisji radiowej. Narzut protokołu powoduje, że efektywność transmisji wymiany danych pomiędzy użytkownikami wynosi ok. 50%.
Na prędkość transmisji ma wpływ wiele czynników zewnętrznych, tj.: odległość pomiędzy stacjami, moc zastosowanych anten, przeszkody pomiędzy stacjami czy interferencja kanałów z innymi urządzeniami.

W standardzie 802.11g niektóre urządzenia posiadają tryb Turbo (Super G). Pozwala on osiągnąć prędkość transmisji radiowej do 108 Mbps, dzięki wykorzystaniu kilku kanałów dostępnego pasma. Oczywiście chcąc wykorzystać ten mechanizm, musimy posiadać na naszym terenie dodatkowe wolne kanały, co staje się trudne do osiągnięcia, jeżeli mamy do czynienia z wieloma sieciami na jednym obszarze.

Standard 802.11g jest zgodny „w dół" ze standardem 802.11b, co oznacza, że urządzenia pracujące w tych trybach mogą się komunikować. Trzeba jednak zaznaczyć, że w takim przypadku maksymalna prędkość transmisji wynosi 11 Mbps.

Wszelkie ustawienia mocy transmisji oraz pasm częstotliwości konfigurowane są automatycznie, po wyborze odpowiedniego trybu.

Wireless Settings (w trybie klienta)

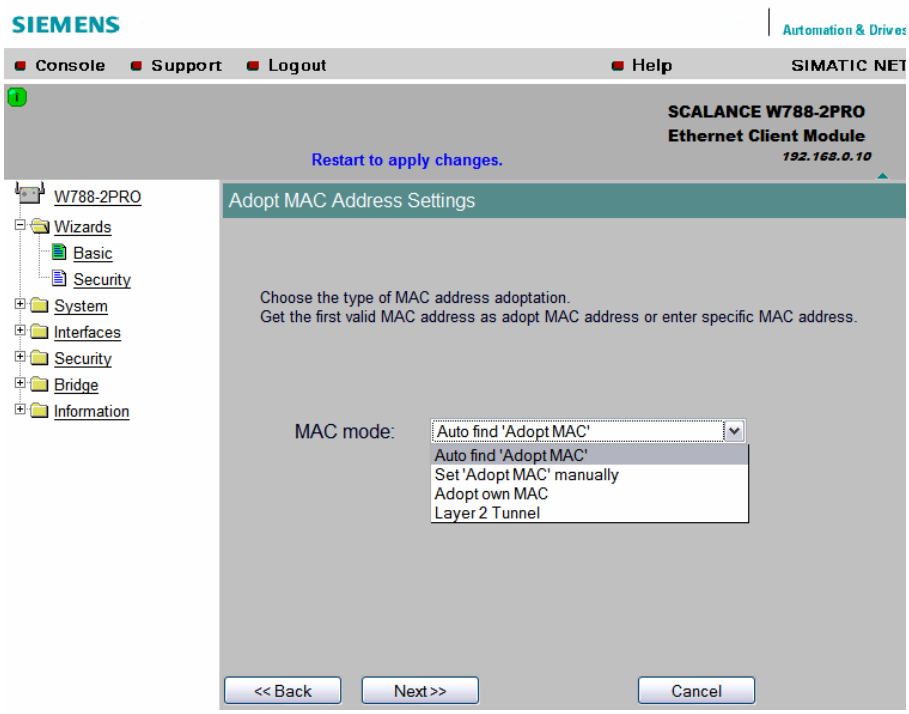


W trybie klienta, w polu „SSID” podajemy identyfikator istniejącej sieci WLAN oraz wybieramy tryb, w którym dana sieć pracuje.
Kanał transmisji dobierany jest automatycznie.

Opcja „Connect to ANY SSID” powoduje, że nasz klient połączy się z dowolną siecią, która odpowiada jego konfiguracji zabezpieczeń.
Jeżeli jest więcej takich sieci, czynnikiem decydującym jest jakość sygnału konkretnego AP.

Adopt MAC Address Settings (w trybie klienta)

Moduł klienta posiada opcję przypisania adresu MAC do jego interfejsu bezprzewodowego WLAN. Innymi słowy, mamy tutaj możliwość wyboru, urządzenia lub urządzeń, które będą widoczne dla nas od strony sieci bezprzewodowej.

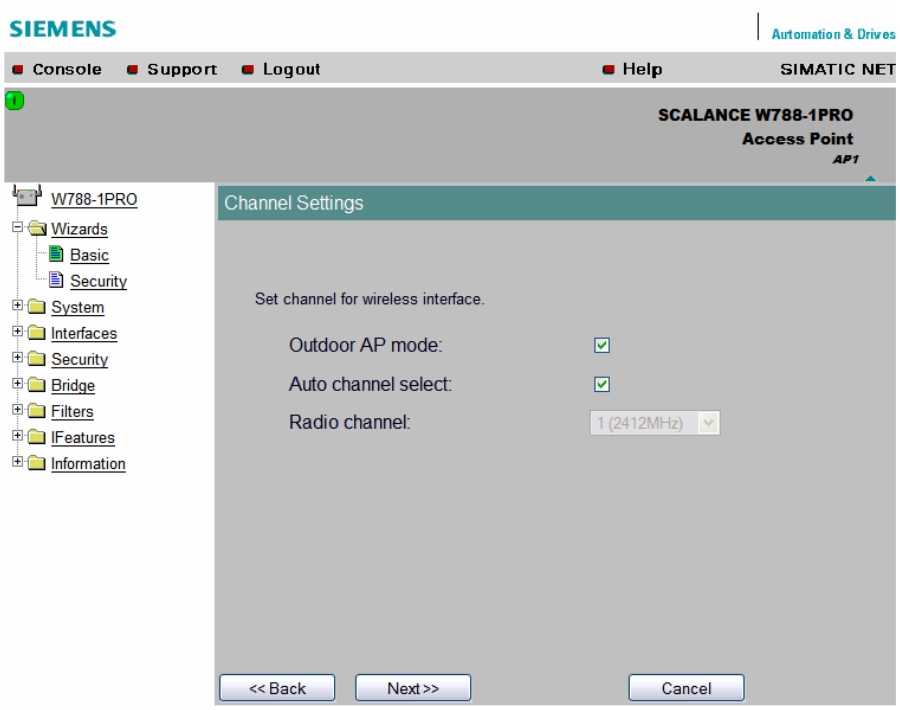


W polu wyboru *"MAC mode"* mamy opcje:

- *„Auto find 'Adopt MAC' „* – do interfejsu WLAN przypisany zostaje adres źródłowy pierwszej ramki, która pojawiła się w module od strony interfejsu Ethernet'owego, czyli adres stacji, za pomocą której jesteśmy połączeni z modułem klienta przez kabel. W ten sposób w sieci bezprzewodowej widoczny jest jeden adres MAC;
- *„ Set 'Adopt MAC' manually"* – podajemy adres MAC, który ma być widoczny z poziomy sieci bezprzewodowej;
- *„Adopt own MAC"* – do interfejsu WLAN modułu jest przypisywany adres MAC jego interfejsu Ethernet;
- *„Layer 2 Tunnel"* – do interfejsu WLAN przypisywany jest adres MAC interfejsu Ethernet'owego, natomiast w sieci bezprzewodowej widocznych jest do 8 adresów MAC urządzeń podłączonych do modułu klienta (np. za pomocą Switch'a).
  Opcja ta jest wykorzystywana w aplikacjach przemysłowych, które wymagają komunikacji na poziomie adresów MAC z kilkoma urządzeniami.
  Uwaga!
  Połączenia rezelizowane w ten sposób możliwe są tylko z urządzeniami *SCALANCE W* z firmwarem powyżej wersji 3.0 lub kompatybilnymi.

Channel Settings

W tym oknie konfigurujemy ustawienia dotyczące kanałów transmisji w wybranym paśmie.



Opcja „Outdoor AP mode” wybierana jest, jeżeli nasz moduł pracuje na zewnątrz i pozwala na automatyczny dobór mocy sygnału, ze względu na restrykcje obowiązujące w danym kraju.

Uwaga!
Jeżeli nasz SCALANCE W pracuje na zewnątrz, należy zabezpieczyć go przed deszczem oraz bezpośrednim działaniem słońca.

Zaznaczenie pola „Auto channel select” powoduje automatyczny i optymalny wybór kanału.
Jeżeli chcemy sami ustawić kanał transmisji, pole to musi być odznaczone.

Aktywne pole „Radio channel” pozwala na indywidualny wybór kanału.
Jest to opcja szczególnie przydatna, gdy mamy do czynienia z wieloma stacjami w naszej sieci, kiedy to ważny jest dobór kanałów w taki sposób, aby ich pasma „nie nachodziły” na siebie wzajemnie.

Warto w tym miejscu nadmienić, iż szerokość pasma jednego kanału wynosi 22 MHz, zatem w różnych trybach mamy do dyspozycji, różną liczbę „czystych” kanałów.

Wskazówki:
W trybie 802.11b/g, mamy do dyspozycji 3 nienakładające się kanały spośród 13 możliwych.
Jeżeli nasze stacje znajdują się na obszarze płaszczyzny, wybieramy kanały: 1, 6, 11.
Jeżeli stacje są rozmieszczone na różnych poziomach względem siebie, używamy 4 kanałów (rezygnujemy z szerokiego pasma na rzecz niepowtarzalności kanałów w sąsiedztwie): 1, 4, 8, 11 lub 1, 5, 9, 13.

W trybie 802.11a/h mamy do dyspozycji szersze pasma:

Zakres częstotliwości	Szerokość pasma	Nienakładające się kanały
5,15 – 5,25	100 MHz	4
5,25 – 5,35	100 MHz	4
5,47 – 5,725	200 MHz	10
5,725 – 5,825	100 MHz	4

W tych trybach kreator na podstawie wcześniejszych ustawień lokalizacji, selekcjonuje dla nas odpowiednie kanały automatycznie.

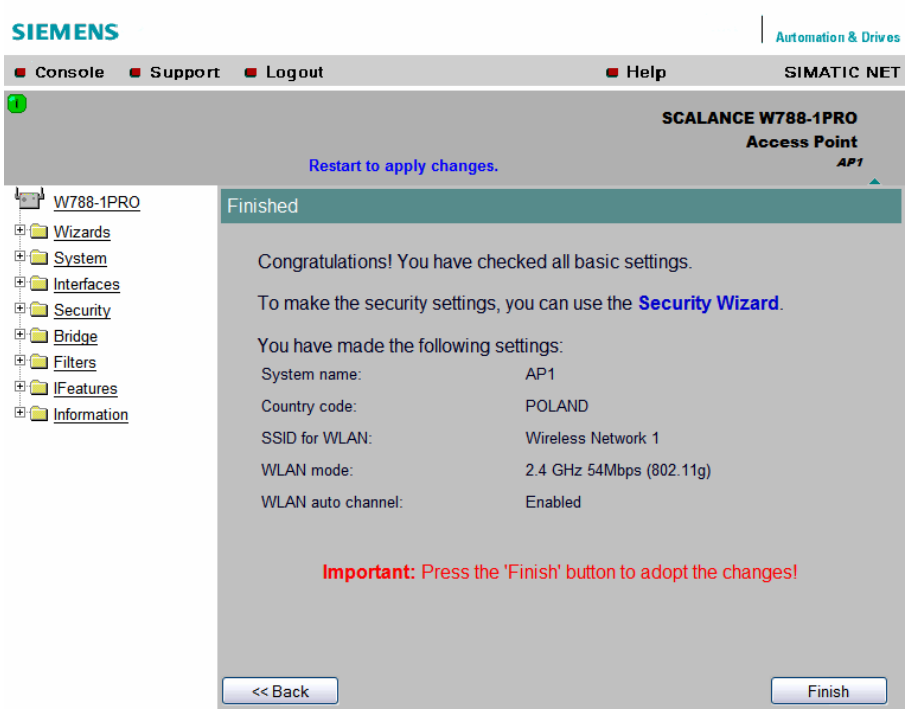
W trybie 802.11g Turbo nie mamy możliwości wyboru kanałów, ze względu na wbudowany mechanizm tego trybu.

W Polsce dozwolone są następujące moce transmisji w zależność od trybu pracy:

Tryb pracy	**Kanał**	**Częstotliwość**	**PWR(EIRP)**	**Miejsce pracy**
11b, 11g, g-Turbo				
	1-13	2412-2472 MHz	100 mW	w budynku/na zewnątrz
11a				
TPC	36	5180	60 mw	w budynku
TPC	40	5200	60 mw	w budynku
TPC	44	5220	60 mw	w budynku
TPC	48	5240	60 mw	w budynku
11h				
DFS+TPC	36	5180	200mW	w budynku
DFS+TPC	40	5200	200mW	w budynku
DFS+TPC	44	5220	200mW	w budynku
DFS+TPC	48	5240	200mW	w budynku
DFS+TPC	52	5260	200mW	w budynku
DFS+TPC	56	5280	200mW	w budynku
DFS+TPC	60	5300	200mW	w budynku
DFS+TPC	64	5320	200mW	w budynku
DFS+TPC	100	5500	1000mW	w budynku/na zewnątrz
DFS+TPC	104	5520	1000mW	w budynku/na zewnątrz
DFS+TPC	108	5540	1000mW	w budynku/na zewnątrz
DFS+TPC	112	5560	1000mW	w budynku/na zewnątrz
DFS+TPC	116	5580	1000mW	w budynku/na zewnątrz
DFS+TPC	120	5600	1000mW	w budynku/na zewnątrz
DFS+TPC	124	5620	1000mW	w budynku/na zewnątrz

DFS+TPC	128	5640	1000mW	w budynku/na zewnątrz
DFS+TPC	132	5660	1000mW	w budynku/na zewnątrz
DFS+TPC	136	5680	1000mW	w budynku/na zewnątrz

Zakończenie konfiguracji

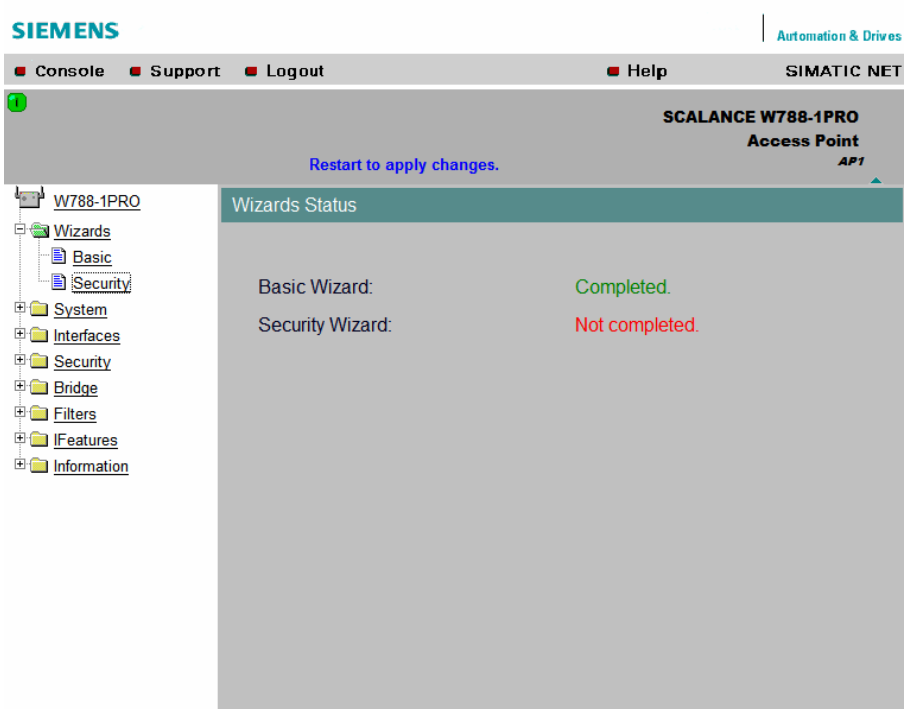


W ostatnim oknie kreatora konfiguracji widzimy podsumowanie wprowadzonych ustawień.
W celu zatwierdzenia zmian klikamy klawisz „Finish”.

Uwaga!
Zamiany najczęściej wymagają dodatkowo restartu sterownika.

3. Zabezpieczenie modułu z wykorzystaniem kreatora.

Po wprowadzeniu podstawowej konfiguracji do modułu, konieczne jest zabezpieczenie dostępu oraz transmisji.
Producent przypomina o tym przez komunikaty o stanie wykonania podstawowych ustawień konfiguracji oraz zabezpieczeń.



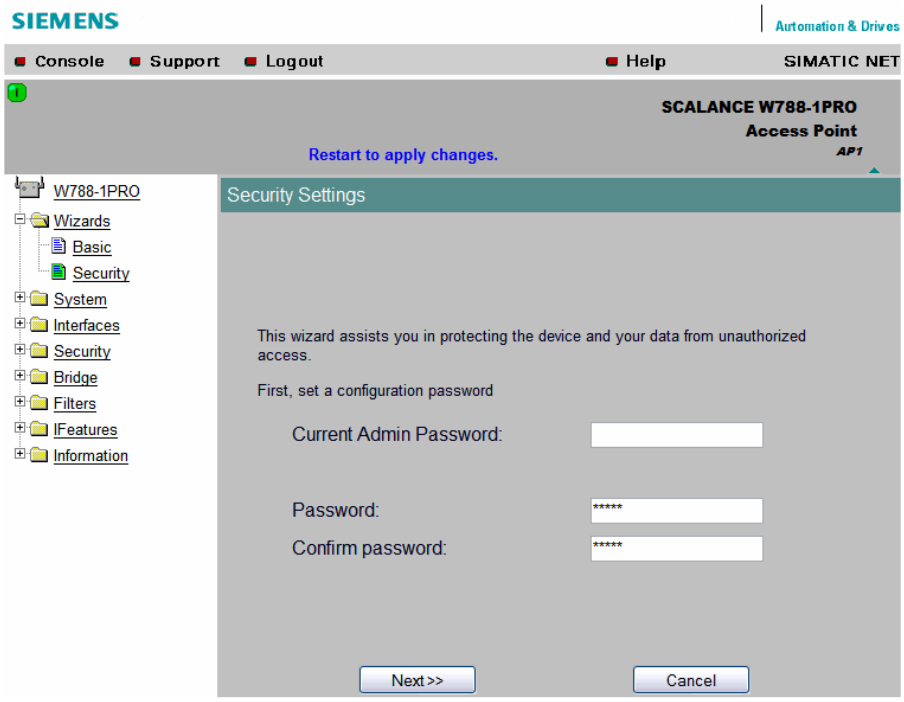
W celu przejścia do kreatora zabezpieczeń wybieramy opcję „Security” z zakładki „Wizards”.

Security Settings

W pierwszym oknie dokonujemy zmiany domyślnego (lub poprzednio wprowadzonego, w przypadku kolejnej konfiguracji) hasła dostępu do konfiguracji modułu.
Jest to bardzo ważne ze względów bezpieczeństwa i należy dokonać tej zmiany podczas pierwszej konfiguracji sterownika.

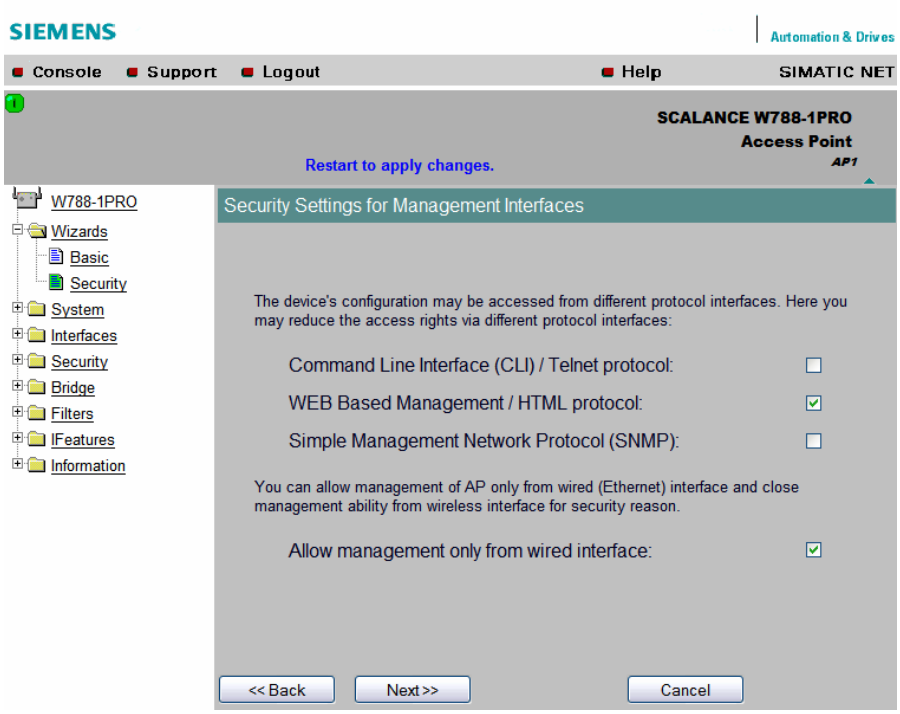
W polu „Current Admin Password" wpisujemy obowiązujące dotychczas hasło, a w polach „Password" i „Confirm password" wpisujemy nowe hasło.

Uwaga!
Należy pamiętać o „mocy" hasła, tzn. nie powinno ono być wyrazem, który możemy znaleźć w słowniku, najlepiej, aby był to losowy zlepek liter i cyfr.



Security Settings for Management Interfaces

Konfiguracji modułu możemy dokonywać wykorzystując trzy metody dostępu:
- CLI (interfejs linii komend), poprzez protokół Telnet;
- Przeglądarka WEB, poprzez protokół HTML;
- poprzez protokół SNMP,



Należy wybrać tylko te opcje, których mamy zamiar korzystać – im mniej dróg dostępu do naszego modułu, tym jest on bezpieczniejszy.

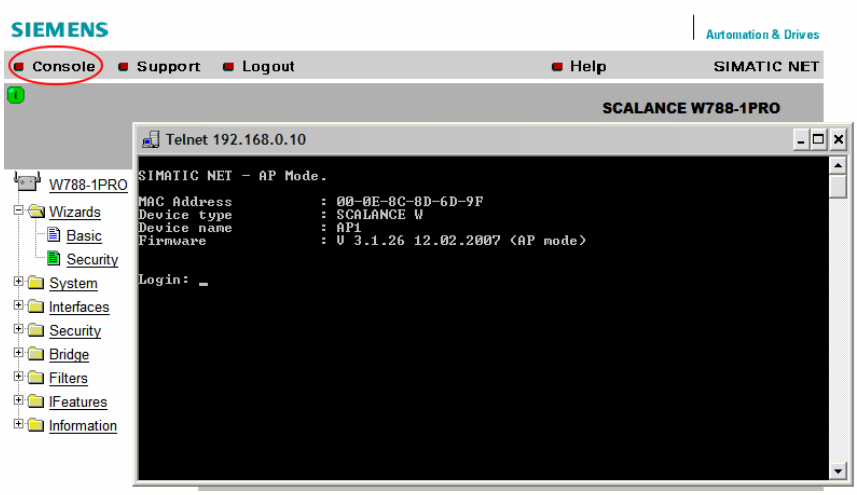
Ostatnia opcja pozwala na dostęp do modułu tylko przez interfejs Ethernet'owy, czyli innymi słowy, tylko „przez kabel".
Zaznaczając tą opcję uzyskujemy zabezpieczenie modułu na poziomie fizycznym.

Wskazówki.

CLI i Telnet.

CLI to zestaw komend tekstowych, dzięki którym możemy dokonywać konfiguracji i diagnostyki modułu poprzez protokół Telnet.
Aby połączyć się z modułem w tym protokole możemy wykorzystać konsolę systemową oraz polecenie „telnet".
W przypadku systemów Windows w menu Start->Uruchom wpisujemy:
„telnet adres", gdzie „adres" oznacza adres IP naszego modułu, np.:
telnet 192.168.0.10

Konsola CLI jest także dostępna w menadżerze Web.



Za pomocą komend CLI możemy dokonać wszystkich możliwych ustawień modułu. W wielu przypadkach jest to narzędzie, wbrew pozorom, wygodniejsze i szybsze.

Zestaw komend CLI można znaleźć w załączniku „CLI – komendy.pdf".

SNMP

SNMP (Simple Network Management Protocol) pozwala na odczyt i zapis ustawień urządzenia sieciowego w postaci strukturalnego obiektu MIB (Management Information Base).

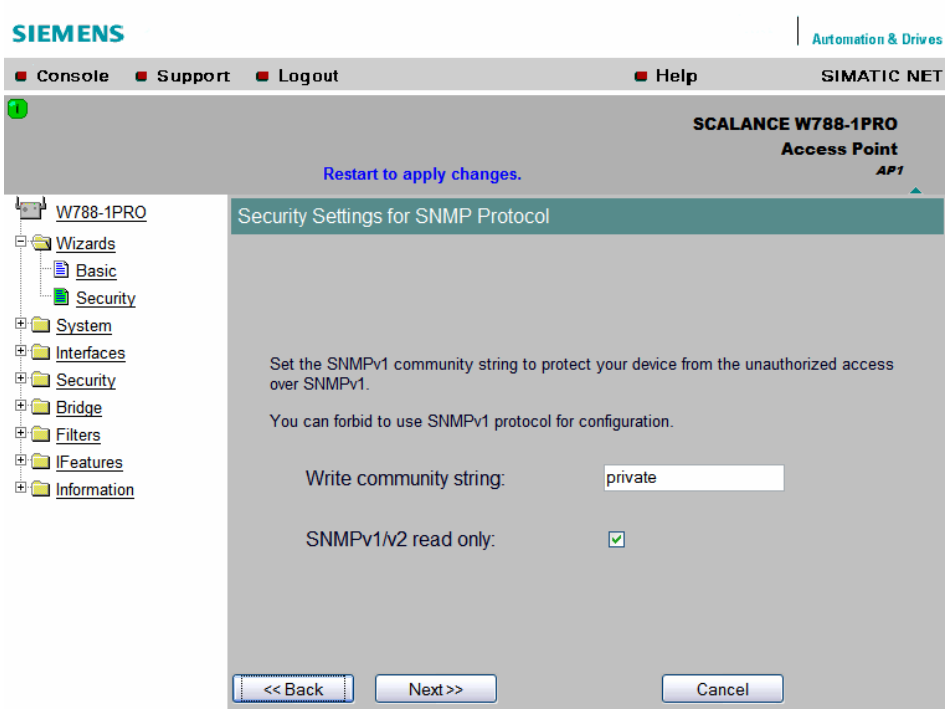
Protokół ten wykorzystywany jest do konfiguracji i diagnostyki urządzeń sieciowych w narzędziach takich, jak Simatic STEP 7, WinCC, PST (Primary Setup Tool) – dostępny wraz z modułem, MIB Browser, OPC Scout.

Jeżeli zamierzamy konfigurować lub diagnozować nasz moduł poprzez te narzędzia, należy włączyć opcję SNMP.

Więcej o SNMP oraz narzędziach wykorzystujących ten protokół w załączniku „IWLAN_Diag_SNMP.pdf".

Security Settings for SNMP Protocol

Jeżeli wybierzemy opcję obsługi SNMP, mamy w tym miejscu możliwość ustawienia zabezpieczeń dla tego protokołu.

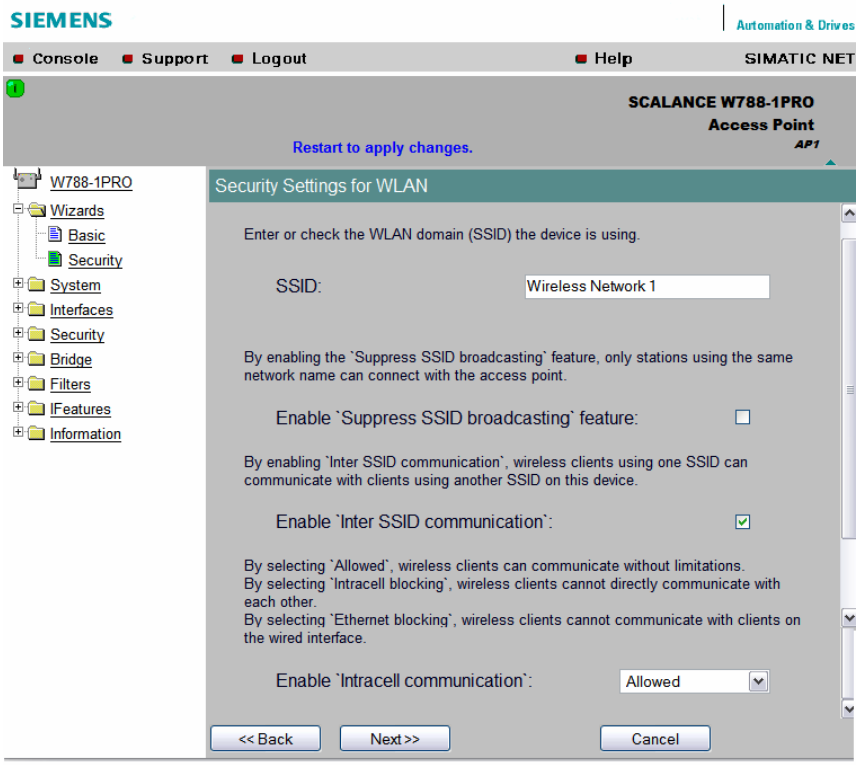


W polu „Write community string" wprowadzamy klucz, zabezpieczający dostęp przez protokół SNMP do naszego modułu (max. 63 znaki).
Klucz ten należy później wprowadzić w konfiguracji narzędzia, poprzez które będziemy się komunikować z modułem.

Opcja „SNMpv1/v2 read only" blokuje możliwość zapisu za pomocą tego protokołu.

Security Settings for WLAN (1)

Okno to pozwala nam na ustawienie zabezpieczeń dla sieci bezprzewodowej.



Pole „SSID" to identyfikator (nazwa) naszej sieci bezprzewodowej.
SSID jest domyślnie rozgłaszany na zewnątrz, tzn. nasza sieć (a właściwie jej identyfikator) jest „widoczna" dla wszystkich w jej zasięgu.

Zaznaczenie opcji „Enable 'Suppress SSID broadcasting' feature" powoduje wyłączenie rozgłaszania SSID, a więc użytkownik chcąc się połączyć z naszym modułem musi podać SSID naszej sieci bezprzewodowej.
Uzyskujemy w ten sposób dodatkowe zabezpieczenie.

W opisywanym module istnieje możliwość ustawienia kilku różnych SSID dla jednego interfejsu bezprzewodowego.
Opcja „Enable 'Inter SSID communication'" pozwala na komunikację pomiędzy użytkownikami, którzy połączyli się z modułem za pomocą różnych SSID.

Ustawienia w polu „Enable 'Intracell comunikation'", dotyczą połączeń pomiędzy użytkownikami naszej sieci.

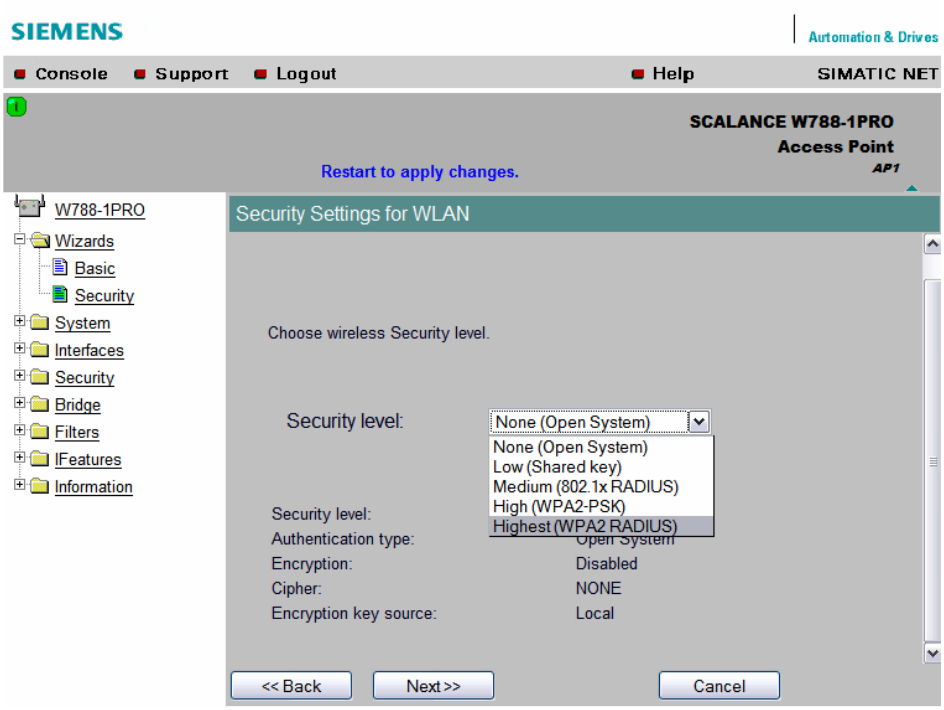
Opcja „Allowed" pozwala na każdy rodzaj połączenia pomiędzy użytkownikami zalogowanymi do naszej sieci poprzez interfejsy WLAN i Ethernet.

Opcja „Intracell blocking" wyłącza możliwość połączenia się użytkowników, którzy używają tego samego SSID.

Opcja „Ethernet blocking” blokuje połączenia klientów sieci WLAN z klientami sieci Ethernet.

Security Settings for WLAN (2)

W tym oknie wybieram poziom zabezpieczeń, który obejmuje sposób autentyfikacji użytkowników i metodę szyfrowania danych.



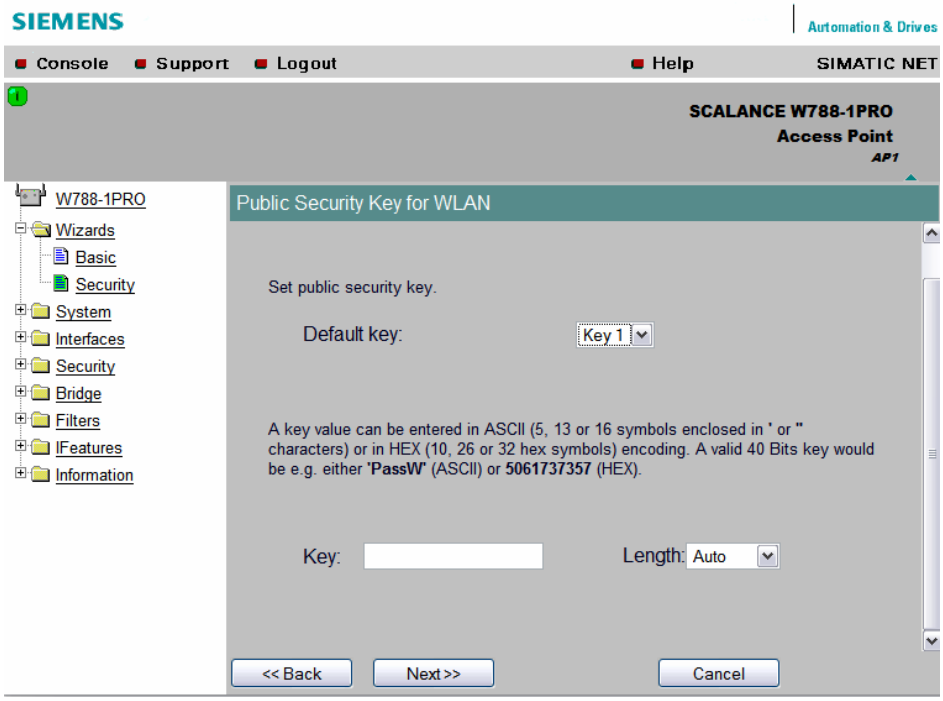
Do wyboru mamy 5 poziomów:

1) None (Open System)

   W tej opcji wyłączone są wszelkie zabezpieczenia, z naszym modułem może połączyć się każdy, kto jest w zasięgu sieci bezprzewodowej.
   Poziom ten jest ustawiony domyślnie i należy go jak najszybciej zmienić.
   W trybie tym możemy uzyskać pośrednio szyfrowanie danych, bez autentyfikacji, przez dodatkowe ustawienie klucza w karcie „Basic WLAN -> Encryption”.

2) Low (Shared key)

Zabezpieczenie na poziomie współdzielonego klucza. Po wybraniu tej opcji przechodzimy do okna, w którym podajemy klucz zabezpieczający dostęp i transmisję danych.



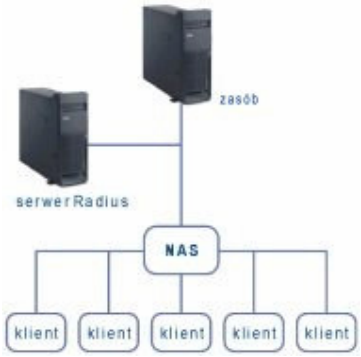
Wartość klucza może być podana w kodzie ASCII (znaki klawiatury) lub jako liczba szesnastkowa (cyfry 0-F).
Jego długość może wynosić 40, 104 lub 128 bitów (5, 13 i 16 znaków ASCII lub 10, 26 i 32 cyfry szesnastkowe).
Im dłuższy klucz tym lepsze zabezpieczenie, ale i większe obciążenie transmisji.

Możemy wprowadzić 5 różnych kluczy, natomiast w danym momencie używany będzie ten wybrany jako „Default key".

Używany klucz powinien być jak najczęściej zmieniany, ponieważ podsłuchanie ok. 2GB zaszyfrowanych danych pozwala na rozkodowanie klucza!

Skuteczność tych zabezpieczeń jest niska, aczkolwiek daje małe obciążenie transmisji.

3) Medium (802.1x RADIUS)

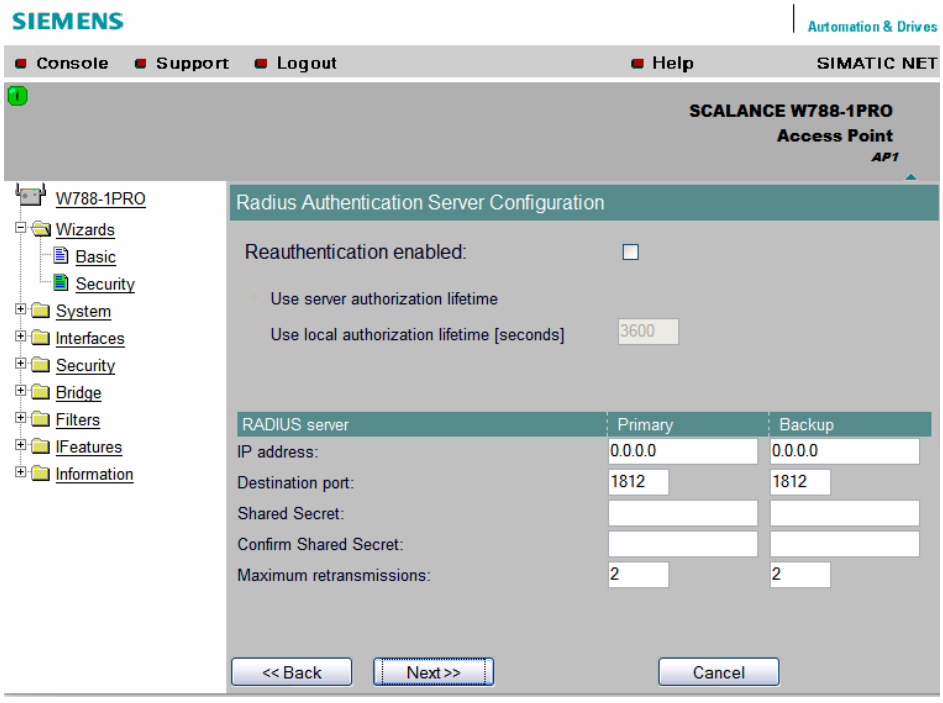


W przypadku dużej liczby klientów, proces uwierzytelniania, autoryzacji oraz rejestracji dostępu do zasobów przejmuje w sieci dodatkowy serwer RADIUS (Remote Authentication Dial In User Service), będący rozwiązaniem wchodzącym w skład standardu zabezpieczeń 802.1x.
Ideę przedstawia rysunek obok.
NAS (Network Access Server) to w naszym przypadku Access Point.
Jeżeli nasza sieć posiada taki serwer, mamy możliwość jego wykorzystania poprzez konfigurację naszego modułu, różniącą się w zależności od tego w jakim trybie pracuje.

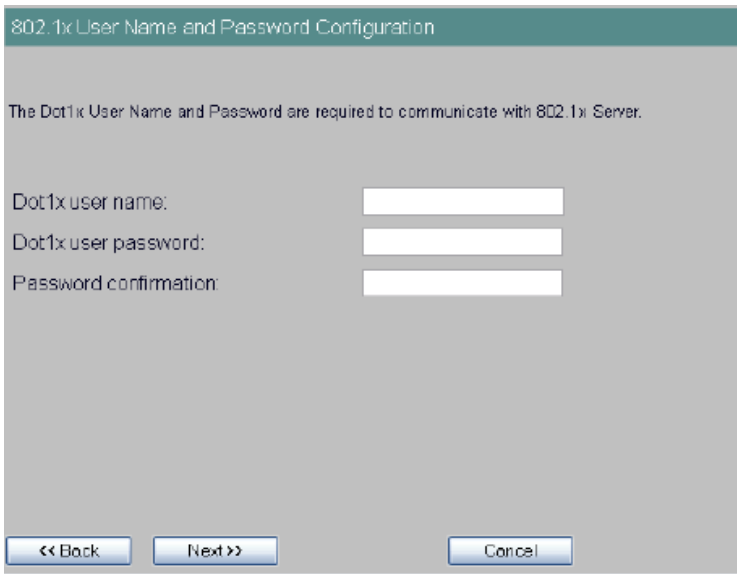
W trybie „Access Point”
podajemy adres IP oraz port serwera RADIUS. Dodatkowo musimy wpisać i potwierdzić hasło dostępu do serwera (Shared Secret – max. 128 znaków).

W polu „Maximum retransmission” podajemy liczbę prób połączenia (0-5). Oprócz podstawowej konfiguracji „Primary”, możemy wprowadzić ustawienia awaryjne „Backup”, które będą wykorzystanie w przypadku niepowodzenia w pierwszym przypadku.

Zaznaczenie opcji „Reauthentification enabled” powoduje wymuszenie ponownej autentyfikacji klienta po upływie określonego czasu.
Jeżeli wybierzemy „Use server authorization lifetime”, to czasem tym zarządza serwer RADIUS, natomiast wybór „Use local authorization lifetime” umożliwia wprowadzenie tego czasu w sekundach
(min. 60, domyślnie 3600, max. 43200 – 12 godzin).



W trybie „Client”
wprowadzamy nazwę użytkownika oraz hasło autentyfikacji w systemie 802.1x.



Na tym poziomie zabezpieczeń szyfrowanie danych realizowane jest za pomocą słabego klucza WEP generowanego przez serwer RADIUS, którego właściwości opisano wcześniej.

4) High (WPA2-PSK)

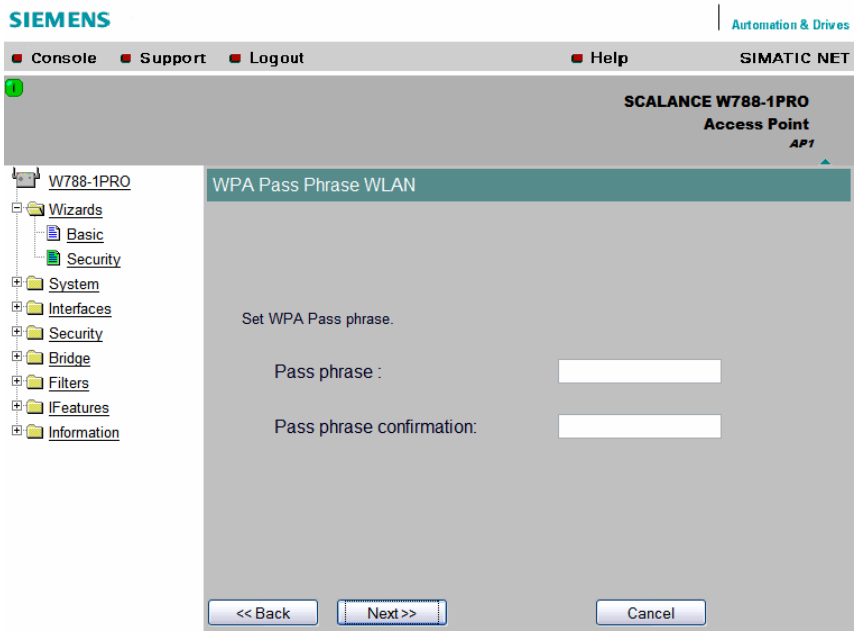
Rozwiązanie bazuje na standardzie WPA2 (Wi-Fi Protected Access 2) i implementuje funkcje 802.11i. WPA2 posiada dodatkowy protokół szyfrowania CCMP oraz umożliwia szybkie przełączanie się pomiędzy stacjami oraz logowanie na kilku punktach dostępowych bez standardowych procedur identyfikacji.

Do szyfrowania wykorzystywane są metody:
TKIP (Temporal Key Integrity Protocol) i AES (Advenced Encryption Standard).
TKIP wykorzystuje algorytm RC4, a jego główna siła to zmieniające się w czasie wartości kluczy, automatycznie wyprowadzane od klucza głównego. TKIP przeprowadza również korekcję uszkodzonych pakietów.
AES implementuje lepszy algorytm Rijndael'a i rozwija możliwości TKIP.

Wyboru metody szyfrowania dokonujemy w polu „Cipher".

WPA2-PSK, w odróżnieniu od WPA2, nie wykorzystuje serwera RADIUS, a jedynie klucz (pass phrase), który jest przechowywany na wszystkich stacjach należących do sieci.

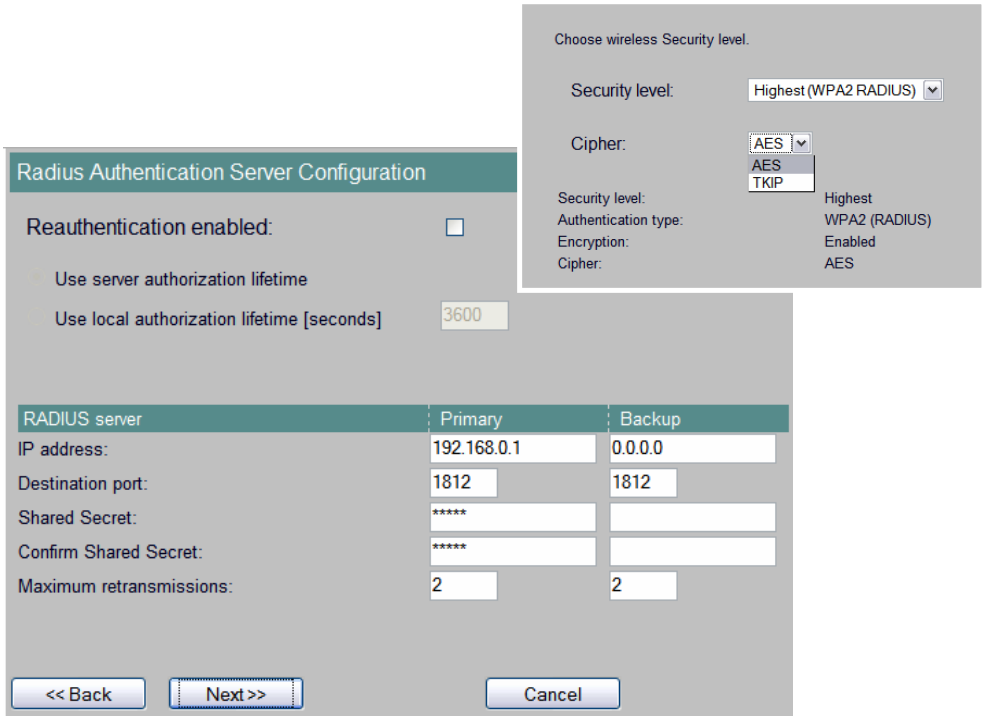
Ten właśnie klucz wprowadzamy do ustawień naszego modułu (min. 8 znaków).



5) Highest (WPA2-RADIUS)

Ten tryb zabezpieczeń posiada wszystkie wyżej wymienione właściwości, a ponadto zapewnia lepszy poziom autentyfikacji przez wykorzystanie serwera RADIUS.

Ustawiamy rodzaj metody szyfrowania (TKIP lub AES) w polu „Cipher" oraz wprowadzamy ustawienia połączenia z serwerem RADIUS w następnym oknie. (tak jak opisano to we wcześniejszych punktach.



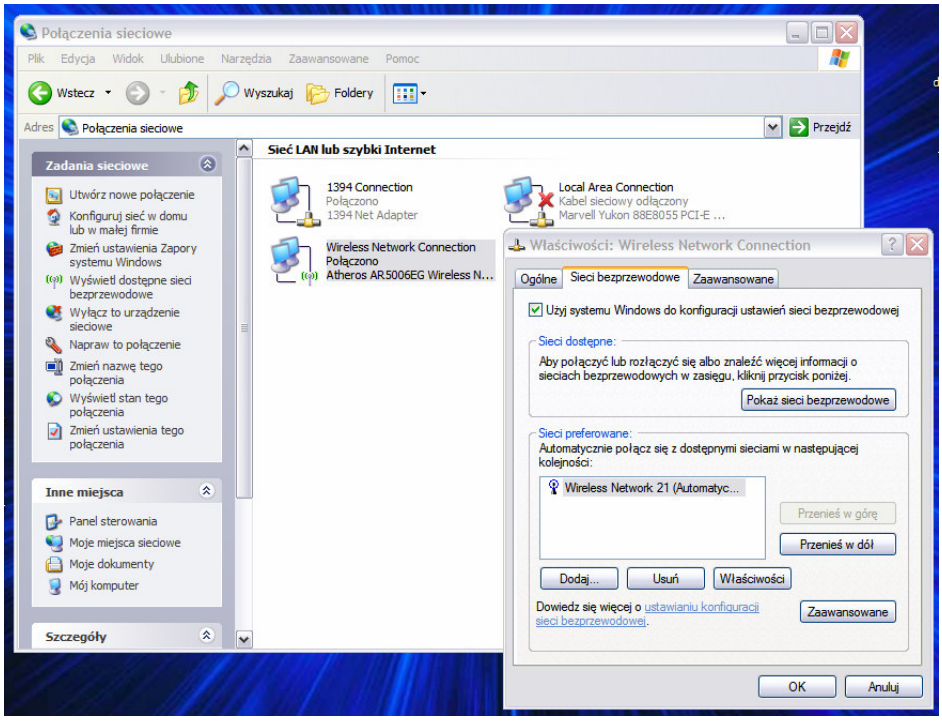
Uwaga!

Należy pamiętać, że stacja kliencka musi obsługiwać tryby zabezpieczeń, które ustawimy w naszym module.
O ile w przypadku współpracy modułów SCALANCE W nie ma tutaj żadnych problemów, o tyle sytuacja może ulec zmianie, jeżeli nasza stacja jest innego producenta lub zarządzana przez inny system operacyjny.

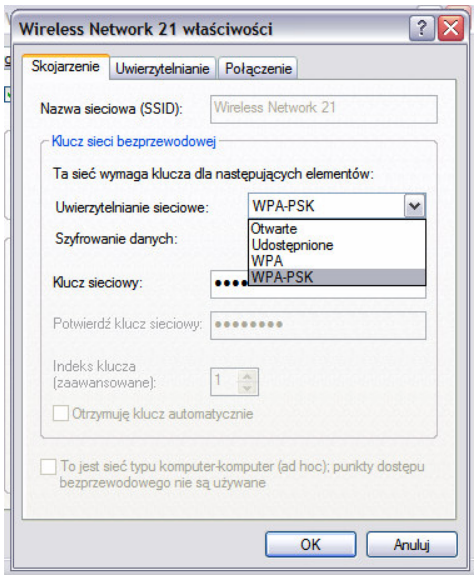
Warto przytoczyć przypadek stacji z systemem Windows.
Do systemu stacji klienckiej musimy wprowadzić odpowiedni dla danej sieci uwierzytelnienia.

System domyślnie przyjmuje zabezpieczenia na poziomie WEP i przy próbie połączenia z siecią zabezpieczoną prosi o podanie takowego klucza. Jeżeli mamy inne zabezpieczenia, musi skonfigurować je sami.

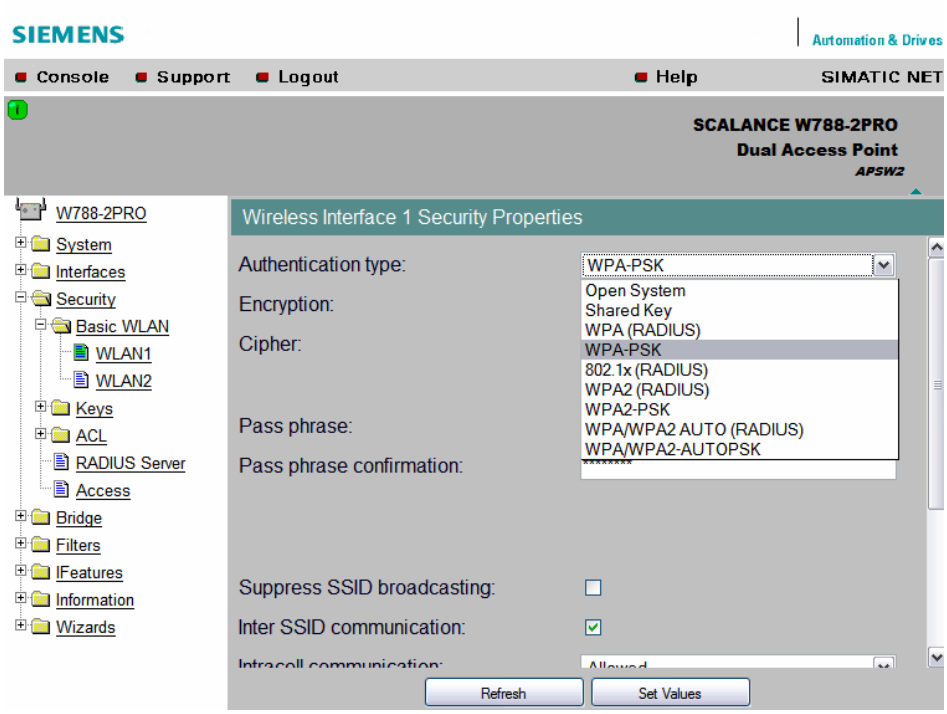
W tym celu przechodzimy do „Start -> Ustawienia -> Panel sterowania -> Połączenia sieciowe”, wybieram interfejs połączenia bezprzewodowego (zazwyczaj „Wireless Network Connection”), otwieramy „Właściwości” i przechodzimy do zakładki „Sieci bezprzewodowe”.



Jeżeli w oknie „Sieci preferowane” znajduje się nasz sieć to klikamy „Właściwości”, jeżeli nie to „Dodaj”.
Gdy dodajemy nową sieć, musimy podać jej SSID
W karcie „Uwierzytelnienia sieciowe” widzimy obsługiwania standardy zabezpieczeń, które musimy „zgrać” z naszym modułem AP.

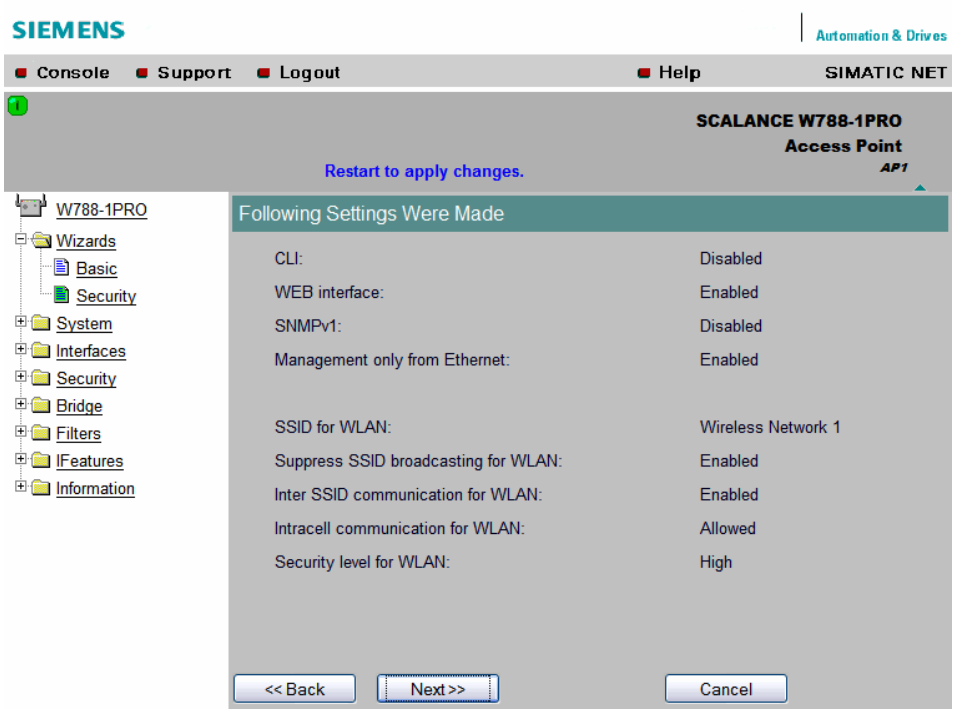


Kreatory dostępne w module SCALANCE W nie dają możliwości wyboru wszystkich możliwych trybów.
Aby uzyskać pełną listę trybów zabezpieczeń przechodzimy do „Security -> Basic WLAN”.
W polu „Autentification type” mamy pełną listę trybów.



Podsumowanie wprowadzonych ustawień

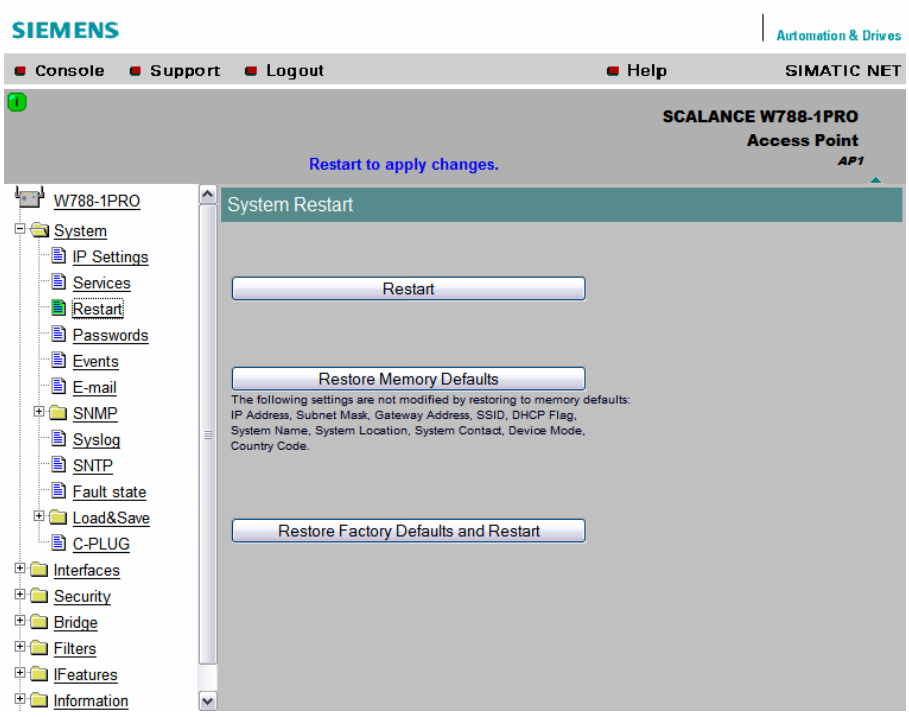
W tym oknie widzimy wykaz ustawień, które zostały wprowadzone.



Następne okno kreatora informuje o zakończeniu konfiguracji.
Naciśnięcie klawisza „Finish” powoduje zapisanie konfiguracji, ale nie wprowadza wszystkich ustawień do modułu.
Aby moduł zastosował nową konfigurację wymagany jest restart urządzenia.

4. Restartowanie modułu.

W celu zrestartowania modułu przechodzimy do menu „System”, zakładka „Restart”.



Do dyspozycji mamy 3 opcje restartu:

1) „Restart” – zwykły restart z zachowaniem zapisanych ustawień.
2) „Restore Memory Defaults” – restart z przywróceniem ustawień fabrycznych za wyjątkiem: adresu IP, maski podsieci, adresu bramy sieciowej, SSID, flagi DHCP, nazwy systemu, lokalizacji systemu, kontaktów systemowych, trybu pracy, kodu kraju.
3) „Restore Factory Defaults and Restart” – restart z przywróceniem wszystkich ustawień fabrycznych.

Oprócz restartu programowego możemy wykorzystać restart poprzez chwilowe odłączenie zasilania modułu (z zachowaniem konfiguracji) lub restart za pomocą przycisku „Factory Reset” z tyłu urządzenia.