DIGITAL AUTOMATION TECHNOLOGIES

ASEM UBIQUITY

PIERWSZE KROKI

Systemy automatyki

Autorzy : **Zespół SABUR Sp. z o.o.**

Wydanie : **6.2**

Data : **Czerwiec 2015**

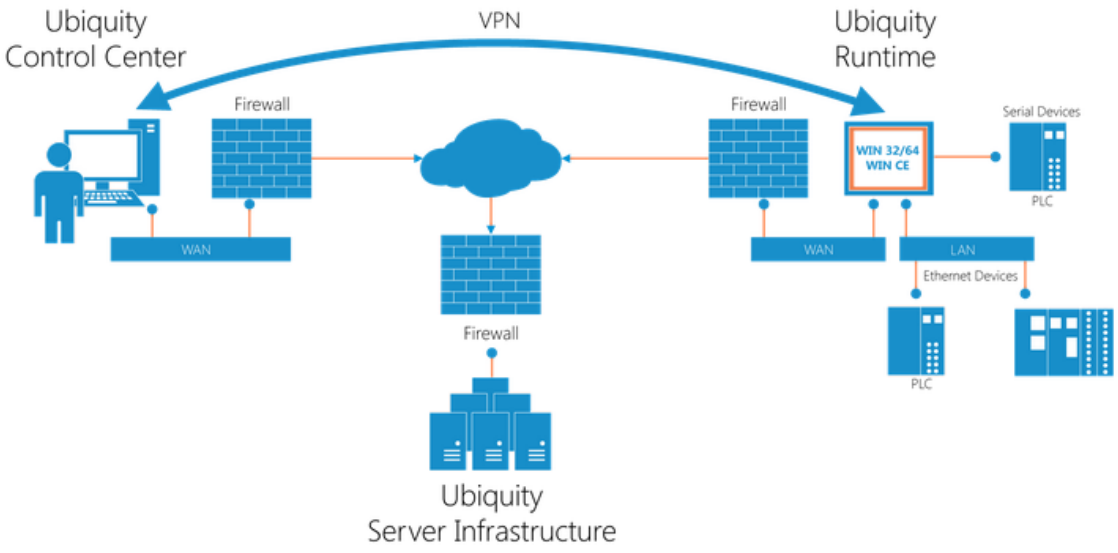
SPIS TREŚCI:

1. Wprowadzenie

1.1. O ASEM Ubiquity

ASEM Uqiuity to nowatorskie rozwiązanie na platformy Win 32/64 oraz Win CE wspierające zaawansowane funkcje zdalnego dostępu. Umożliwia ono nadzór, monitorowanie i konfigurację pracy systemu zdalnego przy jednoczesnym redukowaniu ograniczeń związanych z odległością połączenia.

Schemat połączenia ze zdalnym systemem za pośrednictwem ASEM Ubiquity:



Ubiquity do pakiet oprogramowania składający się z następujących elementów:

- **Ubiquity Control Center** – aplikacja instalowana na komputerze serwisowym, umożliwiająca konfigurację połączenia z urządzeniami zdalnymi. Aplikacja może pracować na komputerach z systemami operacyjnymi:
  - ✓ Windows XP;
  - ✓ Windows Vista 32-bit i 64-bit;
  - ✓ Windows 7 32-bit i 64-bit;
  - ✓ Windows 8 32 bit i 64 bit;
  - ✓ Windows Server 2008 i Server 2008 R2;

  Do poprawnego działania aplikacji niezbędne jest zainstalowanie pakietu .Net Framework 4.0. W przypadku jego braku, zostanie on automatycznie zainstalowany podczas instalacji aplikacji Control Center.

- **Ubiquity Runtime** – aplikacja instalowana na urządzeniu zdalnym, z którym będzie nawiązywana komunikacja. Aplikacja Ubiquity Runtime dostępna jest dla urządzeń HMI oraz dla urządzeń bazujących na PC, wyposażonych w system Windows 32-bit lub Windows CE. Dodatkowo dla urządzeń z systemem Windows CE wymagana jest instalacja pakietu .Net Compact Framework 3.5, a dla urządzeń z systemem Win 32-bit – pakietu .Net Framework 2.0.

1.2. Przegląd funkcjonalności

Przemysłowy VPN

Komunikacja VPN wykorzystywana przez Ubiquity jest inna niż standardowy VPN, ponieważ działa na poziomie łącza danych. Niesie to ze sobą wiele zalet:

- Stacja nadzorująca łączy się ze zdalną siecią i uzyskuje adres IP z zakresu adresów fizycznych;
- Stacja nadzorująca może wykorzystywać protokoły bazujące na trybie rozgłoszeniowym UDP;
- Nie ma potrzeby zmiany konfiguracji funkcji Gateway w urządzeniach zdalnych. Zdalny dostęp jest dla nich możliwy, ponieważ stacja nadzorująca wykorzystuje fizyczny adres IP.

Zdalna komunikacja szeregowa

Ubiquity może utworzyć wirtualny port szeregowy za pośrednictwem aplikacji Control Center PC. Utworzony port może być zmapowany do fizycznego portu dostępnego w urządzeniu zdalnym, korzystającego z aplikacji Ubiquity Runtime.

- Umożliwia to zdalne zarządzanie i diagnostykę urządzeń z wykorzystaniem oprogramowania zainstalowanego w stacji nadzorującej.

Zdalny pulpit

Aplikacja Control Center zapewnia funkcję zdalnego pulpitu:

- Brak potrzeby inicjalizacji RDP, VTC;
- Połączenie zabezpieczone w zaszyfrowanym tunelu.

Wymiana plików

Aplikacja Control Center zapewnia narzędzie do wymiany plików, za pomocą którego można szybko przesyłać i pobierać pliki, aktualizacje, dane logowania itp.:

- Brak potrzeby instalacji i konfiguracji serwerów FTP;
- Połączenie zabezpieczone w zaszyfrowanym tunelu.

Czat

Aplikacja Control Center oferuje prosty czat:

- Brak konieczności używania połączenia telefonicznego z operatorami zdalnych systemów – ograniczenie kosztów.

Tryb Multi-Klient

Ubiquity Runtime umożliwia obsługę wielu połączeń przychodzących z wielu stacji Control Center:

- Możliwość jednoczesnej pracy kilku operatorów na tym samym zdalnym urządzeniu.

Bezpieczeństwo i kontrola dostępu

Ubiquity umożliwia tworzenie grup użytkowników i urządzeń zdalnych ze zróżnicowanymi poziomami dostępu:

- Podniesienie poziomu bezpieczeństwa systemu, brak możliwości wprowadzania niepożądanych zmian przez użytkowników niepowołanych.

Statystyki i Audyt

Administratorzy mogą w dowolnym czasie sprawdzić odczyty parametrów, logowań użytkowników oraz drukować raporty dla poszczególnych urządzeń, operatorów, klientów itp.

Bezpieczeństwo systemowe

Struktura sieci Ubiquity zapewnia najwyższe standardy bezpieczeństwa poprzez zastosowanie protokołu SSL/TLS, zapewniającego poufność i integralność transmisji danych.

Kompatybilność z istniejącymi firewallami

Brak konieczności dodatkowej konfiguracji firewalli – Ubiquity automatycznie rozpoznaje i wykorzystuje dostępne protokoły TCP / UDP / HTTP / HTTPs.

Komunikacja oparta na połączeniu w chmurze

Domena Ubiquity jest hostowana w chmurze. Dzięki temu uzyskiwany jest wysoki poziom dostępności i bezpieczeństwa danych.

- Możliwość zdalnego dostępu z dowolnego miejsce za pośrednictwem aplikacji Ubiquity Control Center.

Dostępność na wszystkich platformach Windows

Ubiquity Runtime jest dostępny dla platform:

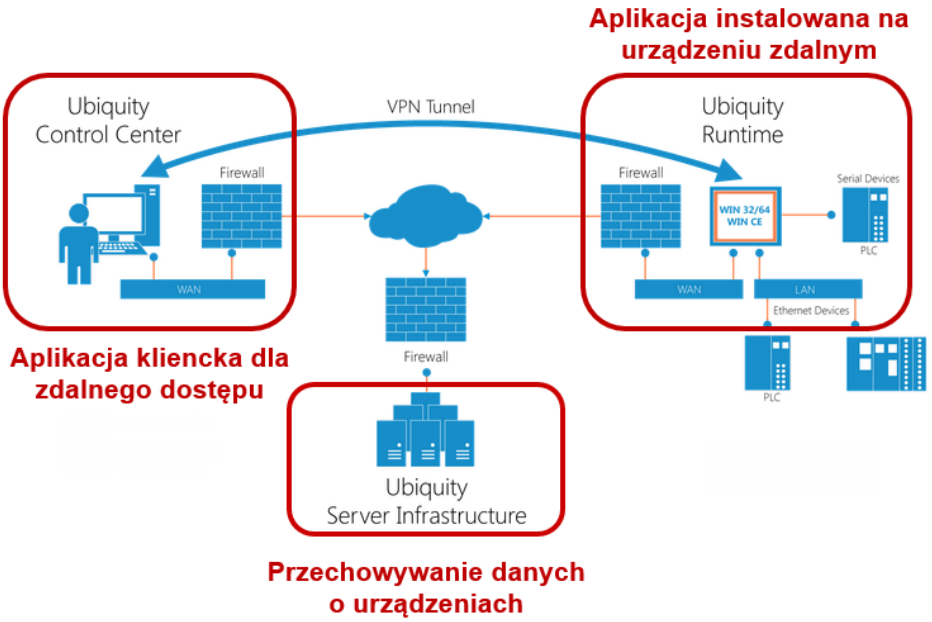
- Windows XP, Vista, 7 (32 i 64bit);
- Windows XP Embedded, Windows Embedded Standard;
- Windows CE 5.0, 6.0, Windows Embedded Compact 7.0.

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

2. Zasada działania systemu

Rozpoczęcie pracy z systemem Ubiquity możliwe jest po uprzednim zainstalowaniu aplikacji **Ubiquity Control Center**, dostępnej do pobrania ze strony www producenta. Na urządzeniu zdalnym, z którym chcemy nawiązać połączenie, powinna być zainstalowana aplikacja **Ubiquity Runtime**. Warto podkreślić, że wszystkie panele HMI firmy ASEM mają preinstalowaną aplikacją *Runtime*.

Autoryzacja połączenia pomiędzy urządzeniem lokalnym i zdalnym następuje poprzez Internet, z wykorzystaniem **serwera Ubiquity**. Aby uzyskać komunikację z serwerem, konieczne jest założenie na nim **domeny** (konta), do której przypisywane będą urządzenia z możliwością zdalnego dostępu oraz użytkownicy systemu.

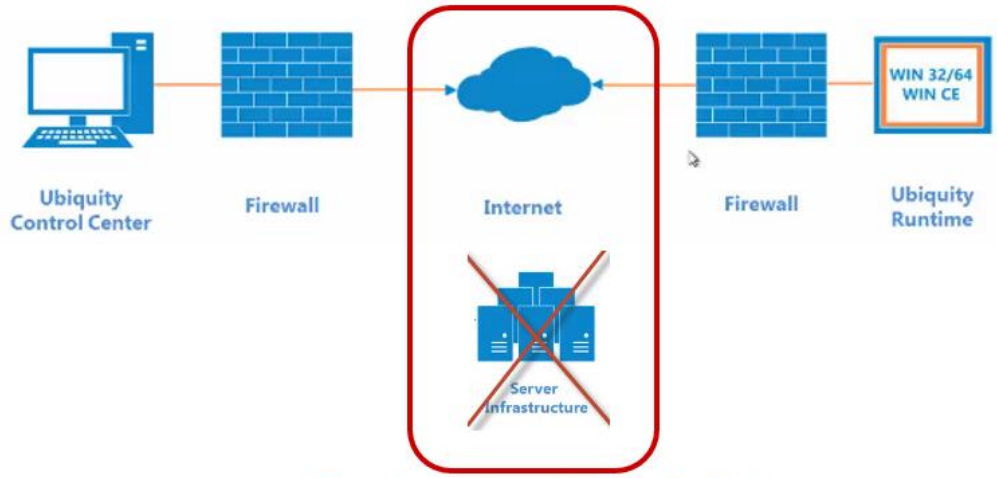


Inicjalizacja połączenia realizowana jest poprzez próbę nawiązania połączenia z serwerem Ubiquity, zarówno przez urządzenie lokalne, jak i zdalne (bezpieczne połączenie SSL/TLS). Warto zauważyć, że komunikacja z serwerem realizowana jest poprzez połączenia wychodzące, które interpretowane są przez zaporę systemową jako bezpieczne. Do realizacji połączenia wykorzystywane są porty: 80 (HTTP) lub 443 (HTTPS) lub dowolny port UDP:

Po nawiązaniu połączenia następuje proces autoryzacji:

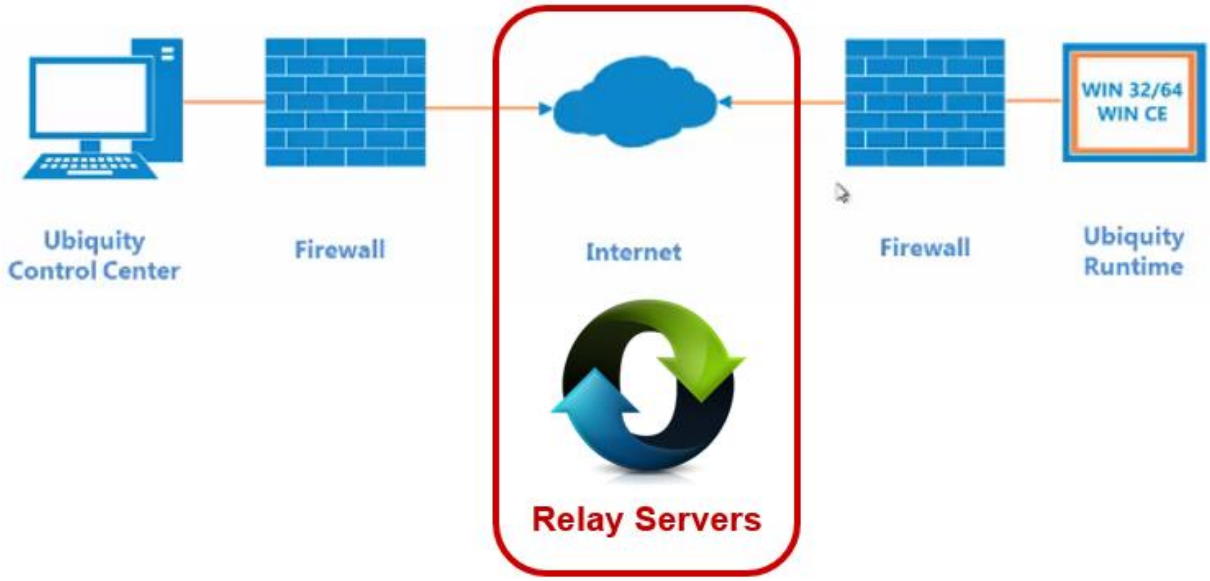
- **aplikacja Control Center** uzyskuje autoryzację serwera poprzez podanie: nazwy domeny, a także nazwy i hasła użytkownika przypisanego do domeny;
- **aplikacja Runtime** uzyskuje autoryzację serwera poprzez sprawdzenie cyfrowego certyfikatu powiązanego z konkretną domeną.

Po autoryzacji połączenia nawiązywana jest komunikacja z urządzeniem zdalnym. Warto zauważyć, że odbywa się ona bez udziału serwera, który w procesie komunikacji stanowi jedynie narzędzie do autoryzacji. Komunikacja pomiędzy urządzeniem lokalnym i zdalnym odbywa się na zasadzie bezpośredniego, wirtualnego połączenia End-To-End:



W niektórych przypadkach może się jednak zdarzyć, że zabezpieczenia sieci firmowych nie umożliwiają nawiązywania połączeń End-To-End. W tym wypadku komunikacja realizowana jest z wykorzystaniem tzw. serwerów przekazujących (*Relay Servers*), działających w chmurze, których zadaniem jest wyłącznie przekazywanie pakietów danych pomiędzy

urządzeniami. Serwery nie otrzymują natomiast żadnych informacji na temat zawartości przesyłanych danych i są one całkowicie transparentne pod względem funkcjonalności i wydajności systemu:



Po prawidłowym nawiązaniu połączenia można korzystać ze wszystkich funkcji systemu ASEM Ubiquity.

3. Rozpoczęcie pracy w środowisku ASEM Ubiquity

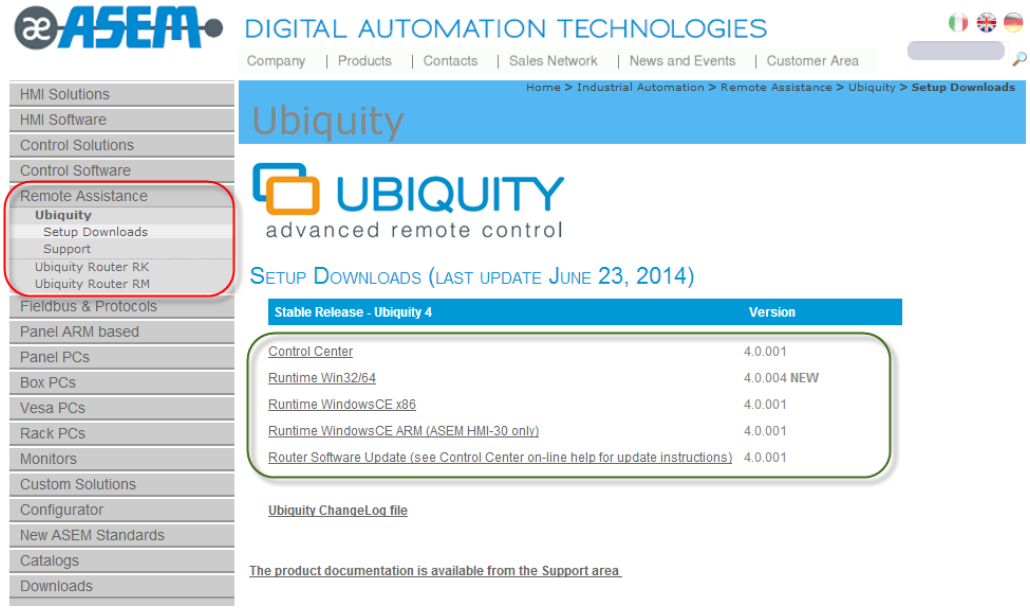
Pracę rozpoczynamy od zainstalowania na urządzeniu lokalnym i zdalnym aplikacji Ubiquity. Na komputerze serwisowym (lokalnym) należy zainstalować pakiet *Ubiquity Control Center*, natomiast na urządzeniu zdalnym aplikację *Ubiquity Runtime*. Jeżeli naszym urządzeniem zdalnym będzie panel firmy ASEM, to ma on już zainstalowany gotowy do użycia pakiet *Ubiquity Runtime*.

Aplikacja Ubiquity Runtime jest programem, który po jednorazowym skonfigurowaniu może rozpoczynać działanie wraz ze startem systemu operacyjnego (praca w tle) i automatycznie logować się do serwera Ubiquity.

3.1. Instalacja aplikacji Ubiquity

Aplikcje: *Ubiquity Control Center i Ubiquity Runtime* można pobrać ze strony producenta:

http://www.asem.it/en/products/industrial-automation/remote-assistance/ubiquity/downloads/

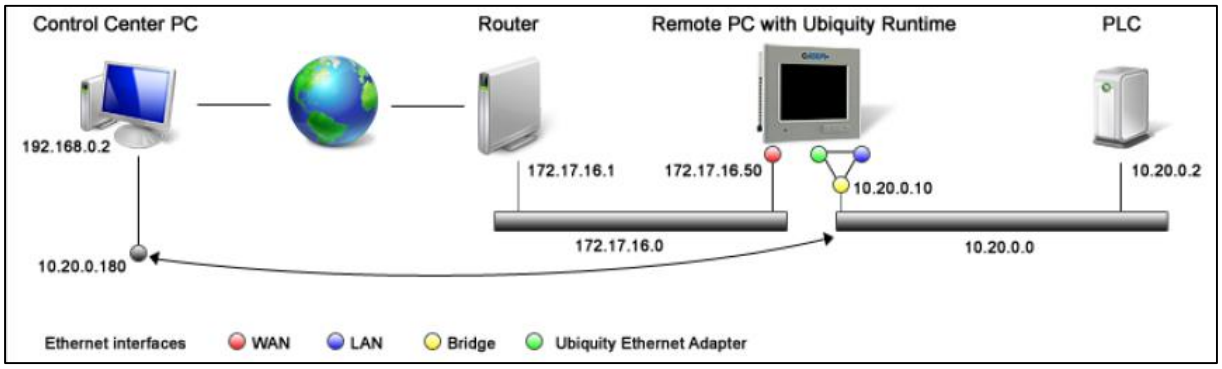


Po pobraniu aplikacji Ubiquity Control Center instalujemy ją na dysku twardym komputera lokalnego.

3.2. Konfiguracja połączeń sieciowych

3.2.1 Konfiguracja połączeń dla urządzenia wyposażonego w 2 porty Ethernet

Na poniższym rysunku przedstawiono strukturę połączeń sieciowych dla urządzenia wyposażonego w 2 porty Ethernet (np. ASEM HMI 30):

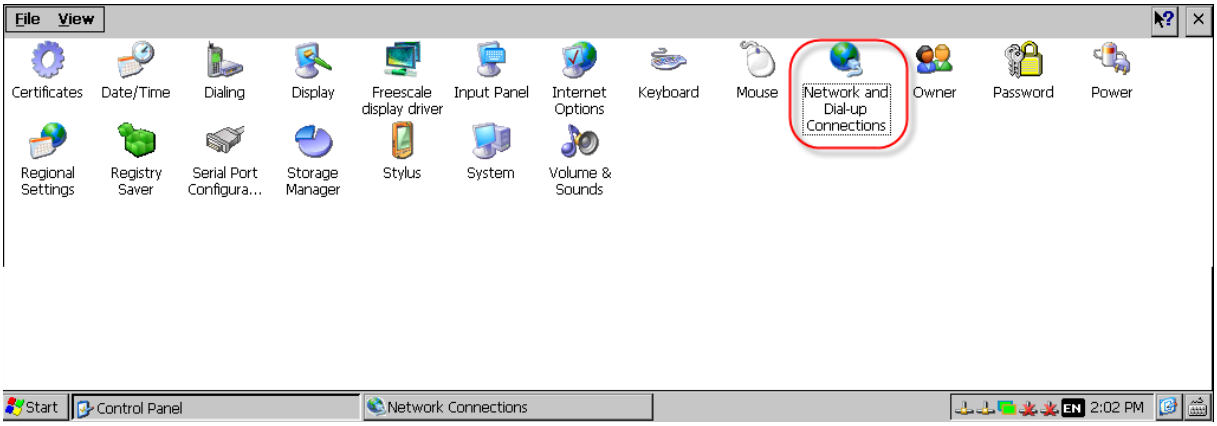


W tym przypadku konfiguracja połączeń powinna być realizowana w następujący sposób:

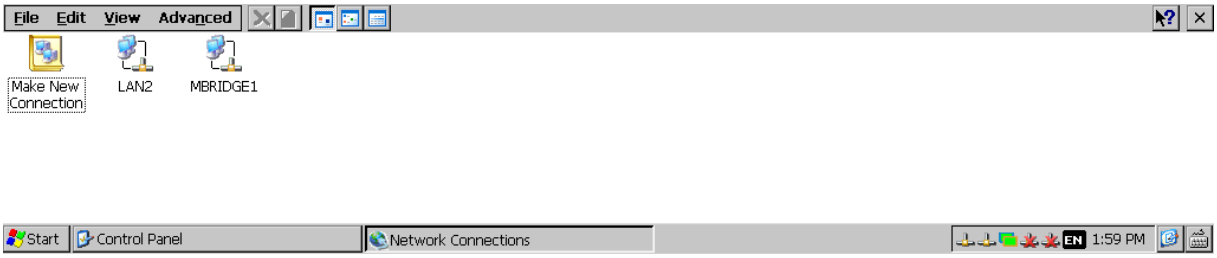
- port **WAN** powinien uzyskać adres IP zapewniający dostęp do sieci Internet (np. poprzez serwer DHCP);
- port **LAN** używany jest do komunikacji z urządzeniami w podsieci (np. 10.20.0.10);

W przypadku uruchomienia połączenia VPN dla panelu, aplikacja Control Center przypisze wirtualny adres IP komputerowi serwisowemu z zakresu adresów fizycznych urządzeń wchodzących w skład podsieci (np. 10.20.0.180).

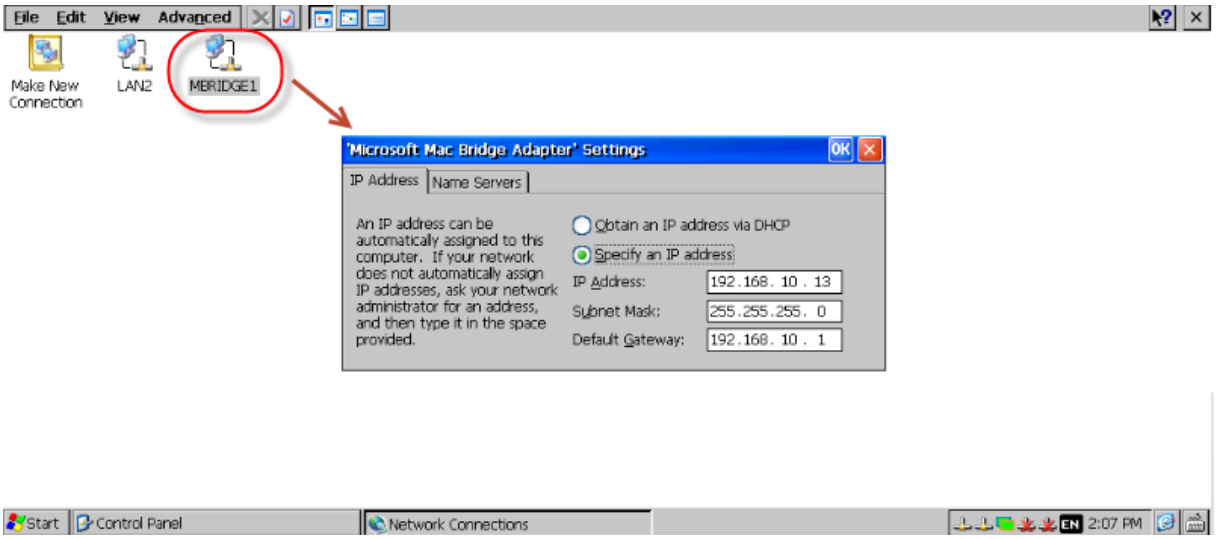
Ustawienia kart sieciowych definiowane są po naciśnięciu ikony *Network and Dial-Up Connections* na ekranie Panelu Sterowania:



Pojawia się okno dostępnych połączeń sieciowych:



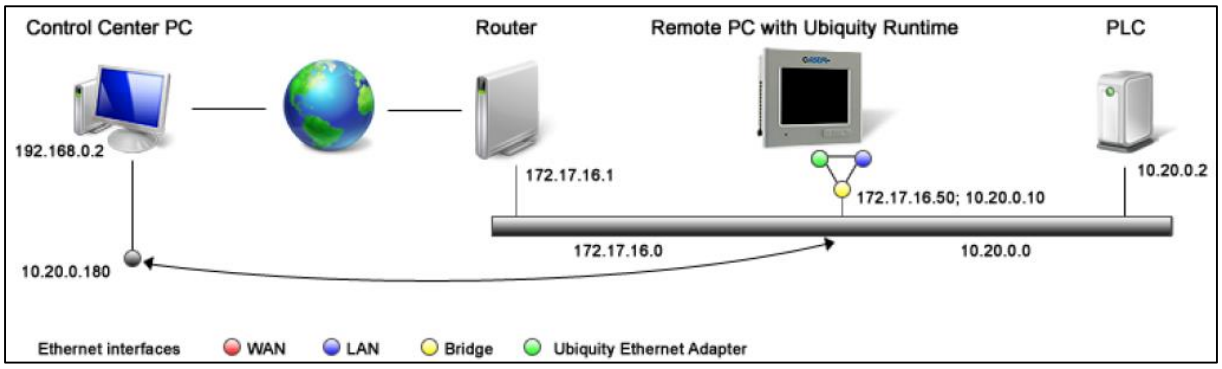
Po kliknięciu na ikonę *LAN2* przechodzimy do konfiguracji ustawień połączenia internetowego. Kliknięcie na ikonę *MBRIDGE1* pozwala na edycję parametrów połączenia z urządzeniami w podsieci.



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

3.2.2 Konfiguracja połączeń dla urządzenia wyposażonego w 1 port Ethernet

Na poniższym rysunku przedstawiono strukturę połączeń sieciowych dla panelu ASEM HMI wyposażonego w 1 port Ethernet (np. ASEM HMI 25):



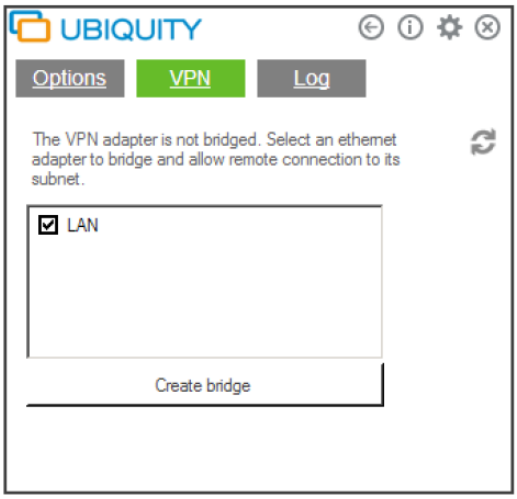
Jeden port Ethernet w urządzeniu musi być wykorzystany do uzyskania połączenia z Internetem. Podczas użytkowania systemu Ubiquity możemy jednak chcieć uzyskać dostęp poprzez VPN także do urządzeń znajdujących się w innych podsieciach. Na rysunku powyżej przedstawiono strukturę sieci z urządzeniem HMI wyposażonym w 1 port Ethernet, do którego przypisano 2 adresy IP:

- pierwszy adres IP (172.17.16.50) jest kompatybilny z siecią umożliwiającą dostęp do Internetu;
- drugi adres IP (10.20.0.10) należy do zakresu adresów urządzeń w podsieci;

Po uzyskaniu połączenia VPN pomiędzy urządzeniem HMI a komputerem serwisowym, aplikacja Control Center przypisze komputerowi zdalnemu adres IP z zakresu adresów fizycznych urządzeń wchodzących w skład podsieci (10.20.0.180). Umożliwia to połączenie nie tylko z panelem HMI (10.20.0.10), lecz także z innymi komponentami wchodzącymi w skład podsieci (np. sterownik PLC, 10.20.0.2).

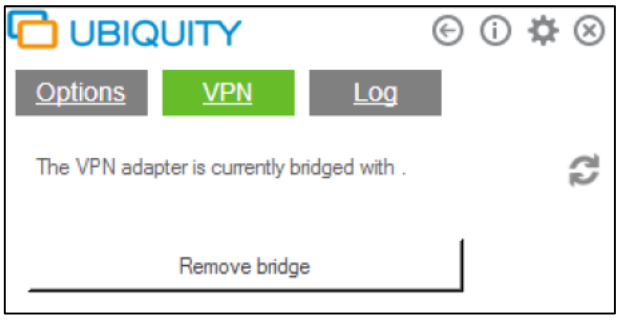
Konfiguracja tego rodzaju połączenia sieciowego umożliwia utworzenie mostka sieciowego (*Bridge*) w aplikacji Ubiquity Runtime urządzenia zdalnego (np. panelu HMI).

1. Otwieramy aplikację Ubiquity Runtime na urządzeniu zdalnym i klikamy na przycisk *VPN*:



W oknie dostępnych portów znajduje się tylko jedna pozycja (LAN). Zaznaczamy port i klikamy na przycisk *Create Bridge*. Po utworzeniu mostka sieciowego aplikacja wyświetli komunikat o konieczności zrestartowania urządzenia.

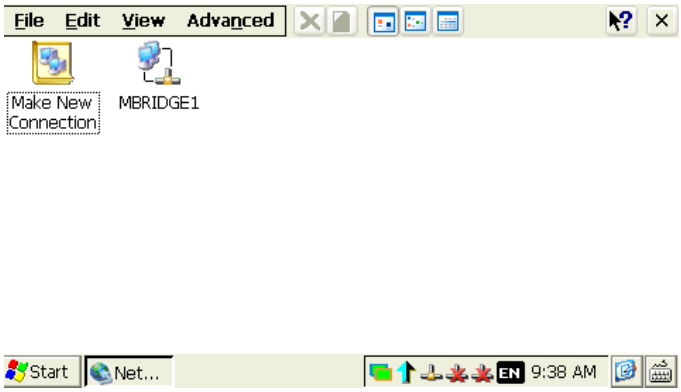
2. Po zrestartowaniu urządzenia w zakładce VPN okna Ubiquity Runtime pojawi się informacja o utworzeniu mostka sieciowego:



Kolejnym krokiem będzie konfiguracja połączenia mostkowego.

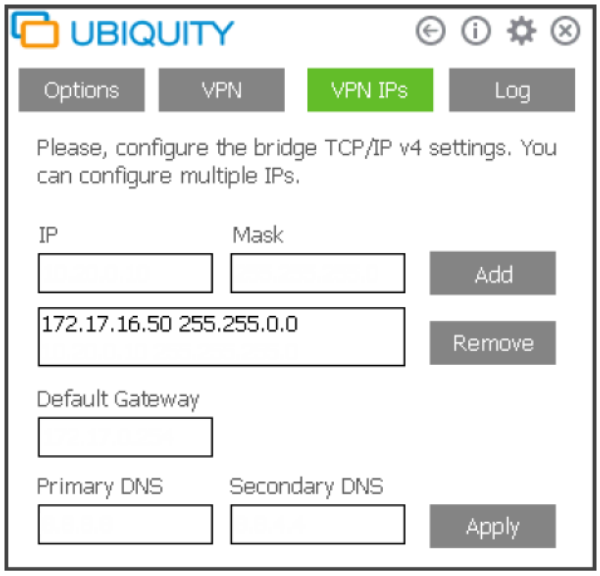
Konfiguracja połączenia dla systemu Windows CE:

System Windows CE nie obsługuje wielu konfiguracji adresów IP, dlatego w oknie połączeń sieciowych widoczne jest tylko jedno ustawienie:



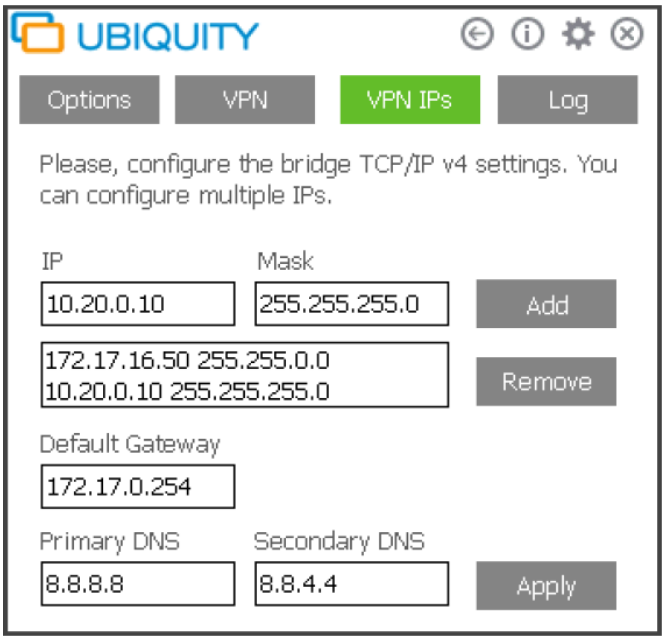
Ograniczenie to zostało usunięte w aplikacji Ubiquity Runtime, która pozwala na zdefiniowanie wielu obsługiwanych adresów IP.

1. Otwieramy aplikację Ubiquity Runtime i przechodzimy do zakładki *VPN IPs*:



2. Wypełniamy pole *IP* wpisując drugi adres IP, jaki ma uzyskać urządzenie do działania w podsieci. Wprowadzamy także maskę podsieci (*Mask*). Dodajemy wprowadzone ustawienia poprzez kliknięcie przycisku *Add*. W oknie możemy także zdefiniować adres bramy domyślnej oraz adresy DNS:

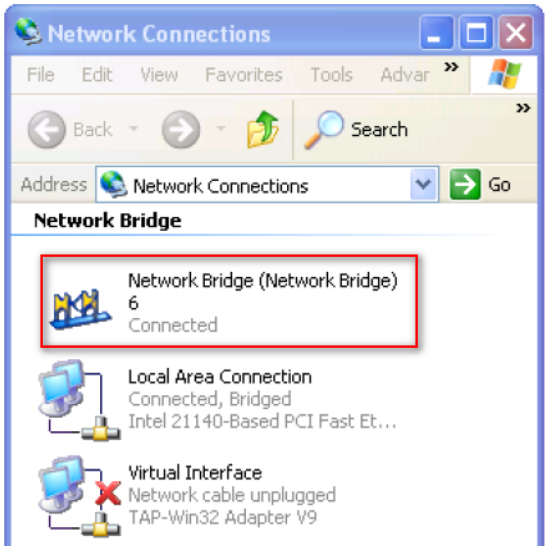
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl



3. Zatwierdzamy wprowadzone zmiany klikając na przycisk *Apply*. Aplikacja poprosi o zrestartowanie urządzenia. Mostek sieciowy został prawidłowo skonfigurowany.

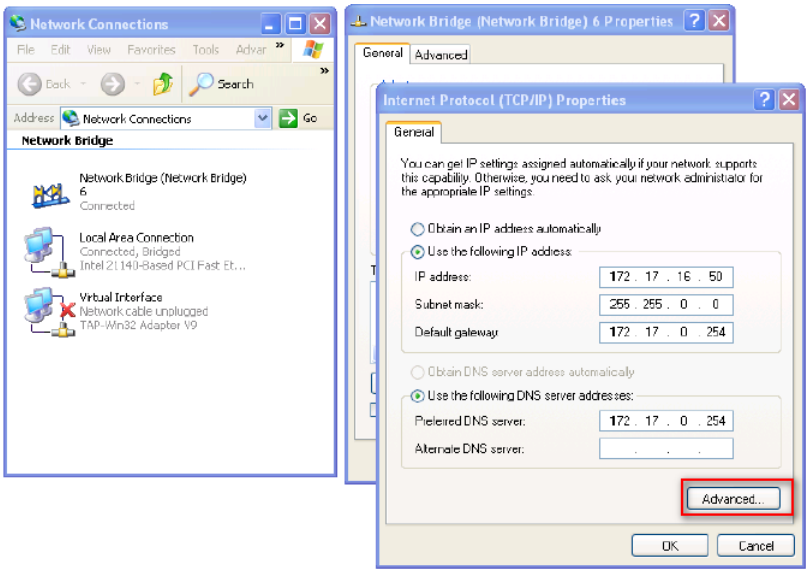
Konfiguracja połączenia dla systemów: Windows XP, Windows 7

1. Otwieramy okno połączeń sieciowych i przechodzimy do właściwości połączenia *Network Bridge*:

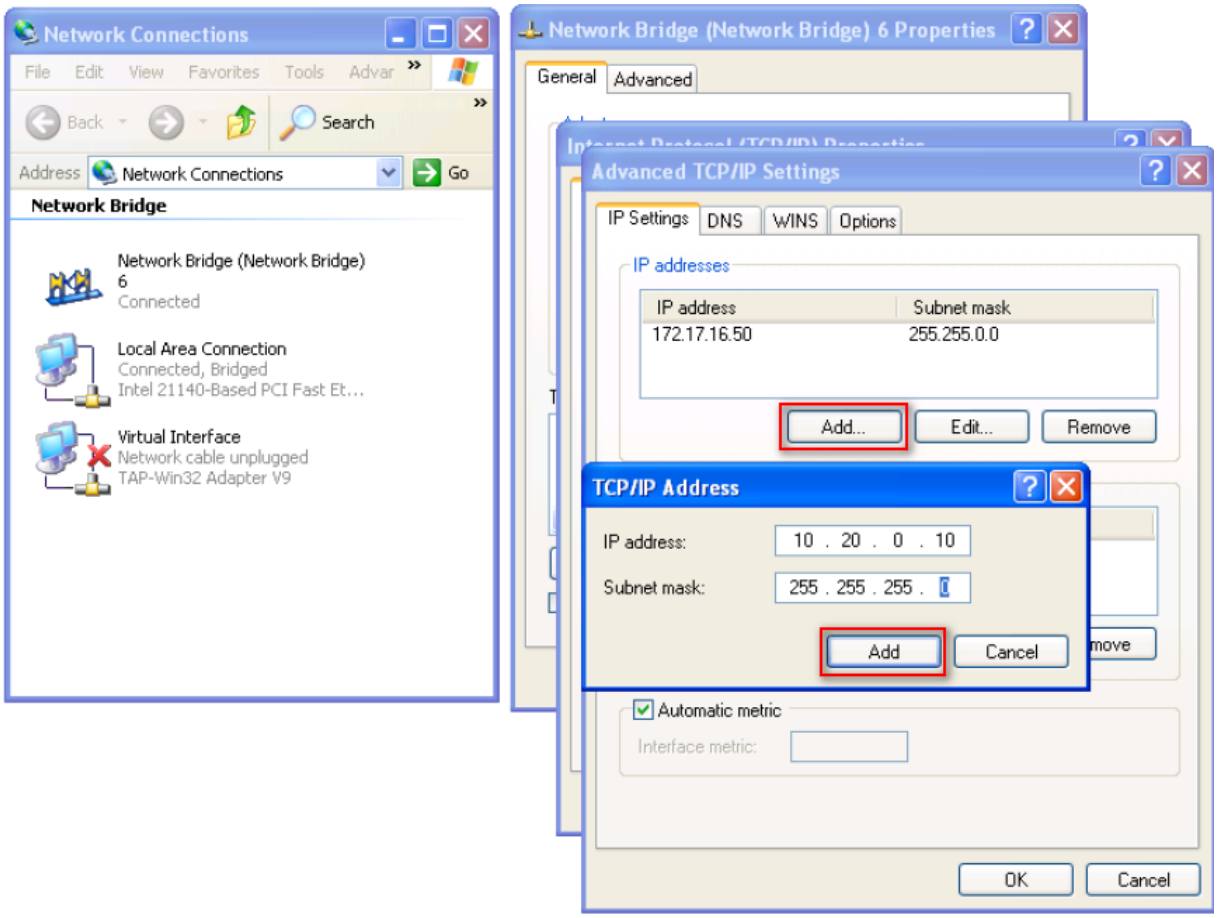


Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

2. W oknie właściwości klikamy na przycisk *Advanced*:



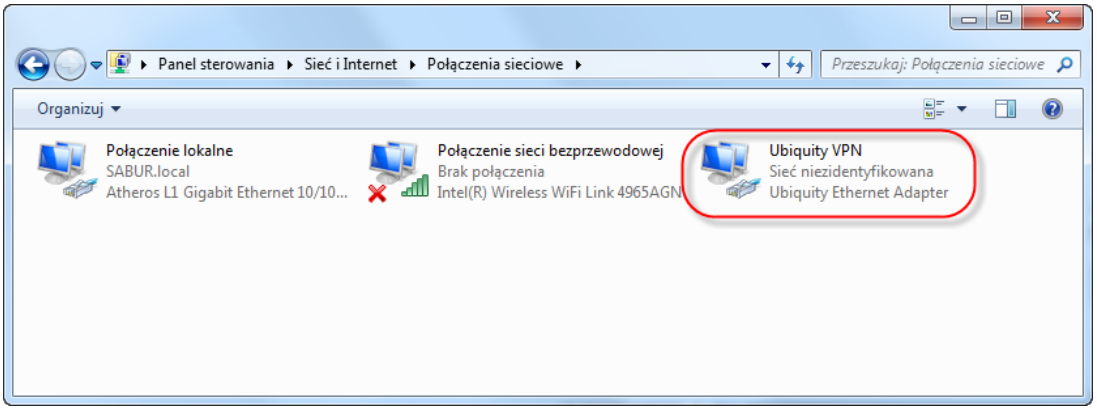
3. W nowym oknie klikamy na przycisk *Add*, a następnie podajemy adres IP z zakresu adresów zdalnej podsieci:



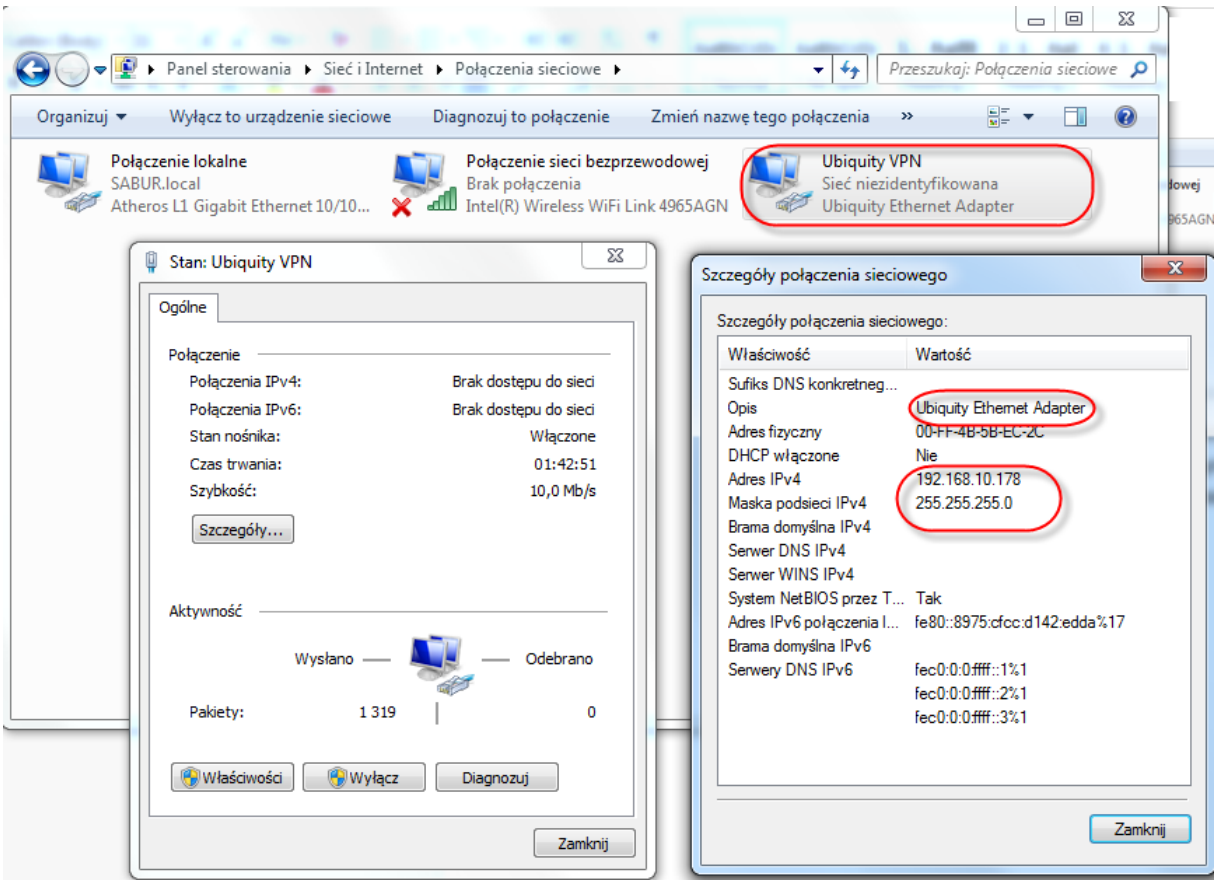
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl
SABUR Systemy automatyki

3.2.3 Konfiguracja połączeń sieciowych dla komputera zdalnego

Po zainstalowaniu aplikacji *Ubiquity Control Center* na komputerze zdalnym, w oknie ustawień kart sieciowych pojawia się nowy komponent o nazwie *Ubiquity VPN*:



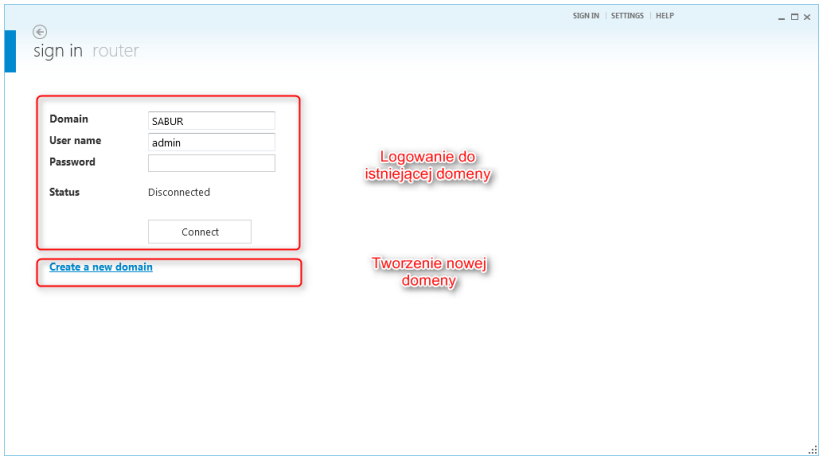
Połączenie *Ubiquity VPN* umożliwia komputerowi zdalnemu komunikację z urządzeniami znajdującymi się w zdalnej podsieci (np. ze sterownikami PLC podłączonymi do zdalnego panelu ASEM HMI). Po kliknięciu ikony połączenia możemy przeglądać jego konfigurację:



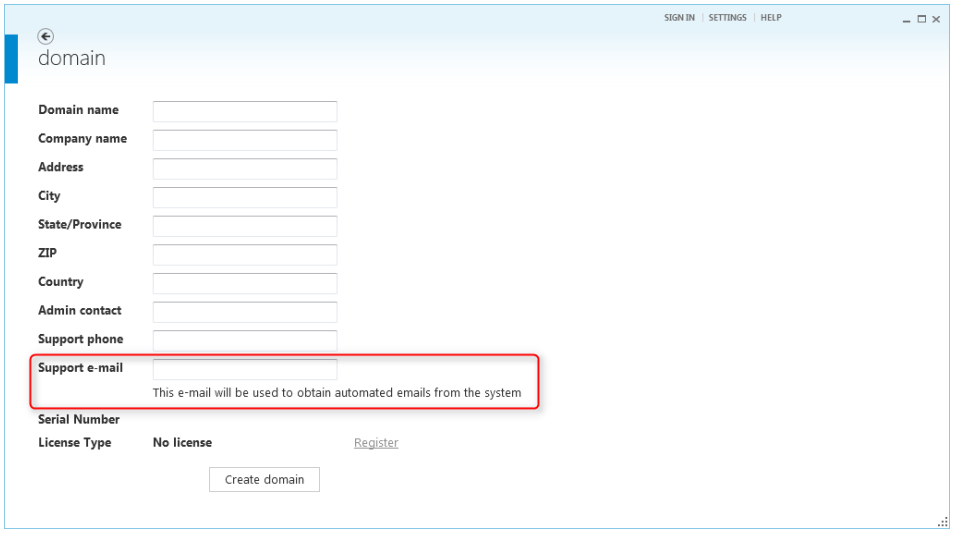
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

3.3. Zakładanie domeny

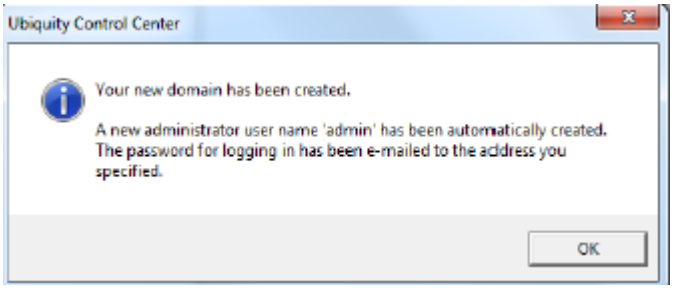
Po zainstalowaniu Ubiquity Control Center możemy założyć pierwszą domenę. Utworzona domena stanowi konto na serwerze Ubiquity, w którym przechowywane są informacje na temat urządzeń zdalnych, z którymi możemy nawiązać połączenie. Aby utworzyć nową domenę, na ekranie powitalnym aplikacji klikamy na *Create a New Domain*. Po utworzeniu domeny w odpowiednie pola wprowadzamy jej nazwę, a także nazwę i hasło użytkownika:



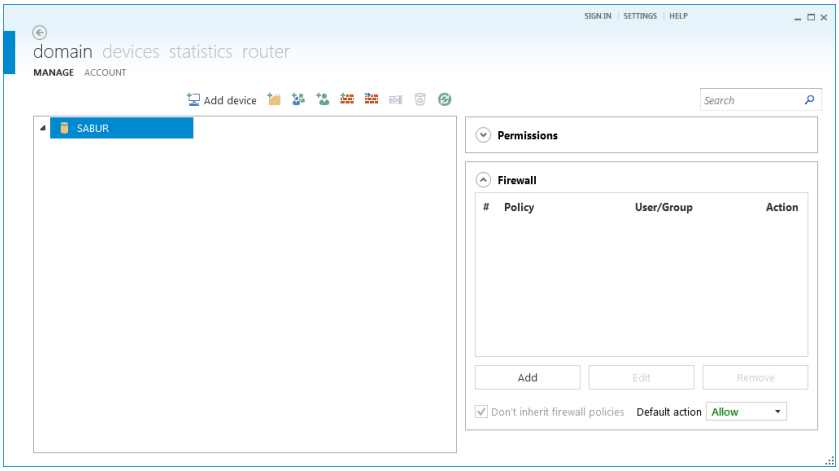
W nowym oknie wprowadzamy dane firmy, dla której tworzona jest domena. Należy zwrócić szczególną uwagę na prawidłowe wprowadzenie adresu e-mail, ponieważ po zakończeniu tworzenia domeny zostanie na niego wysłana wiadomość aktywująca konto:



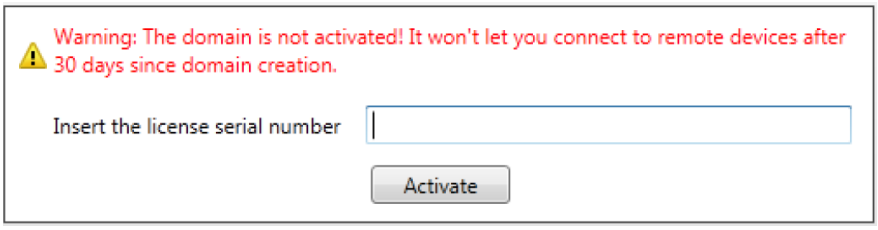
Po kliknięciu przycisku *Create Domain*, domena zostaje utworzona. Korzystanie z domeny jest możliwe dopiero po uzyskaniu hasła dostępu dla domyślnego użytkownika z prawami administratora (*admin*), które wysyłane jest na e-mail podany w formularzu rejestracji.



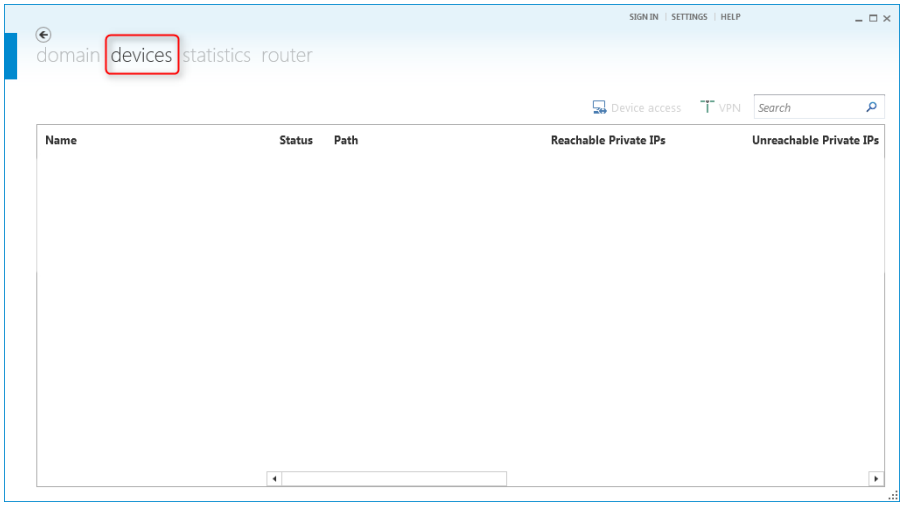
Po otrzymaniu hasła logujemy się do domeny, podając otrzymane hasło. Zostajemy przekierowani na stronę główną domeny:



Nowo zarejestrowana domena pracuje przez próbny okres 30 dni. Po tym czasie konieczne jest jej aktywowanie poprzez wprowadzenie kodu licencyjnego:

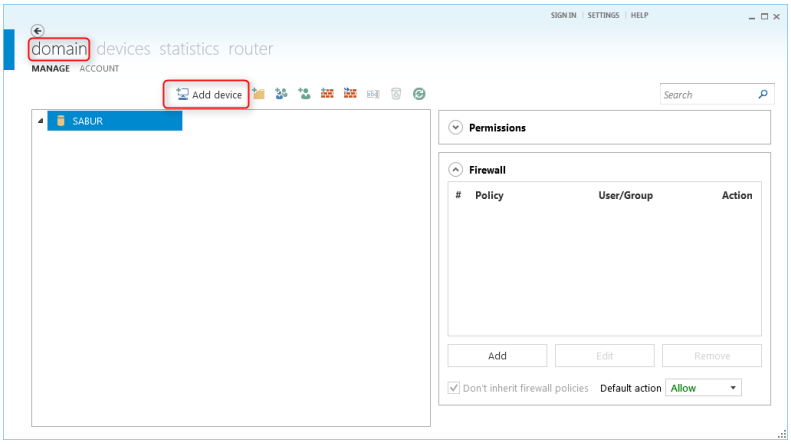


Po zalogowaniu do domeny przechodzimy do karty Devices, w której widoczne są wszystkie urządzenia zdalne, z którymi możemy nawiązać połączenie. Z uwagi na to, że nie zdefiniowaliśmy jeszcze żadnego urządzenia, lista będzie pusta:

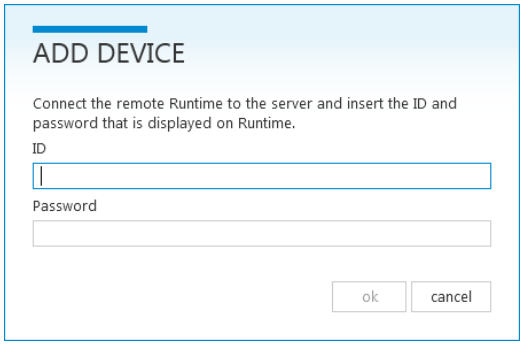


3.4. Dodawanie nowego urządzenia do domeny

W celu dodania nowego urządzenia do utworzonej domeny Ubiquity przechodzimy do karty Domain i klikamy na przycisk *Add Device*:

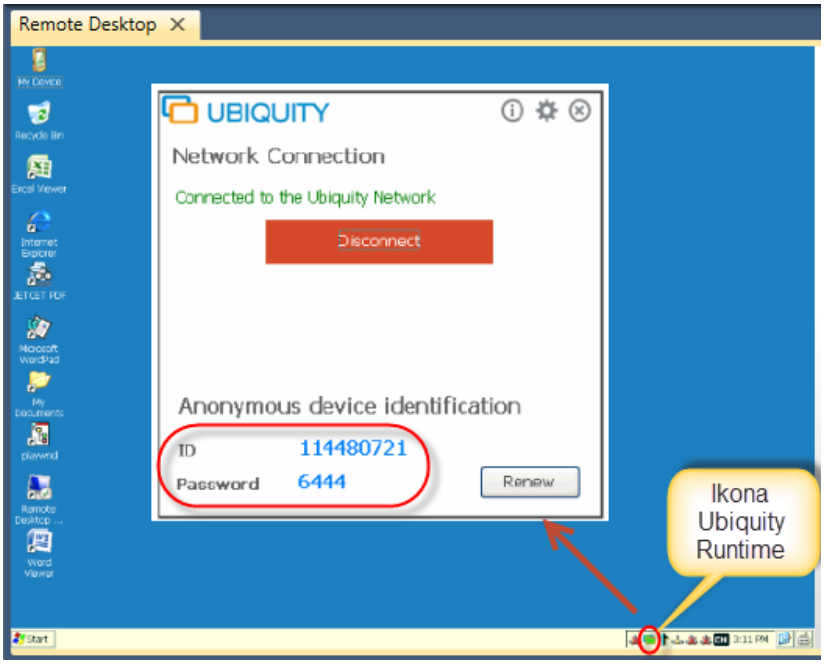


Pojawia się okno z polami, w które należy wpisać dane dostępu do urządzenia zdalnego: unikalny ID urządzenia oraz hasło dostępu:

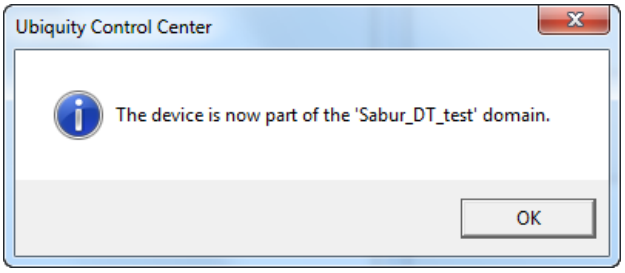


Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Parametry są możliwe do uzyskania z poziomu aplikacji Ubiquity Runtime na urządzeniu zdalnym:

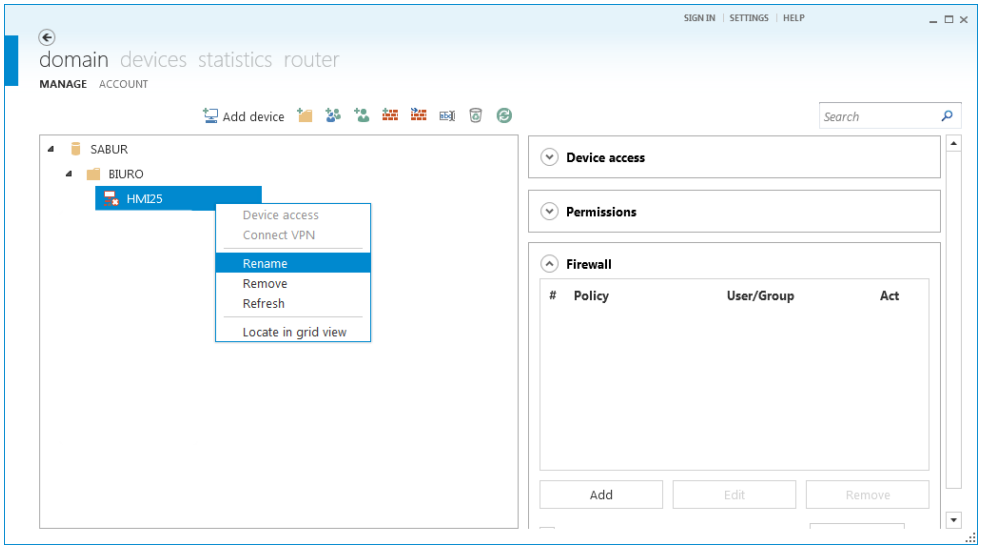


Wpisujemy parametry urządzenia zdalnego w odpowiednie pola i klikamy przycisk *OK*. Jeżeli wprowadzono poprawne dane, pojawia się komunikat o przypisaniu urządzenia do serwera Ubiquity:

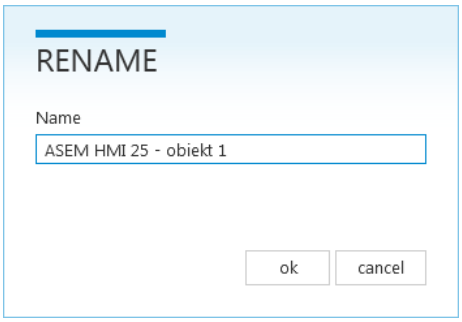


Urządzenie pojawia się na liście sprzętów przypisanych do domeny. Aby nadać nazwę dodanemu urządzeniu, klikamy prawym przyciskiem myszy na jego ikonę i wybieramy *Rename*:

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

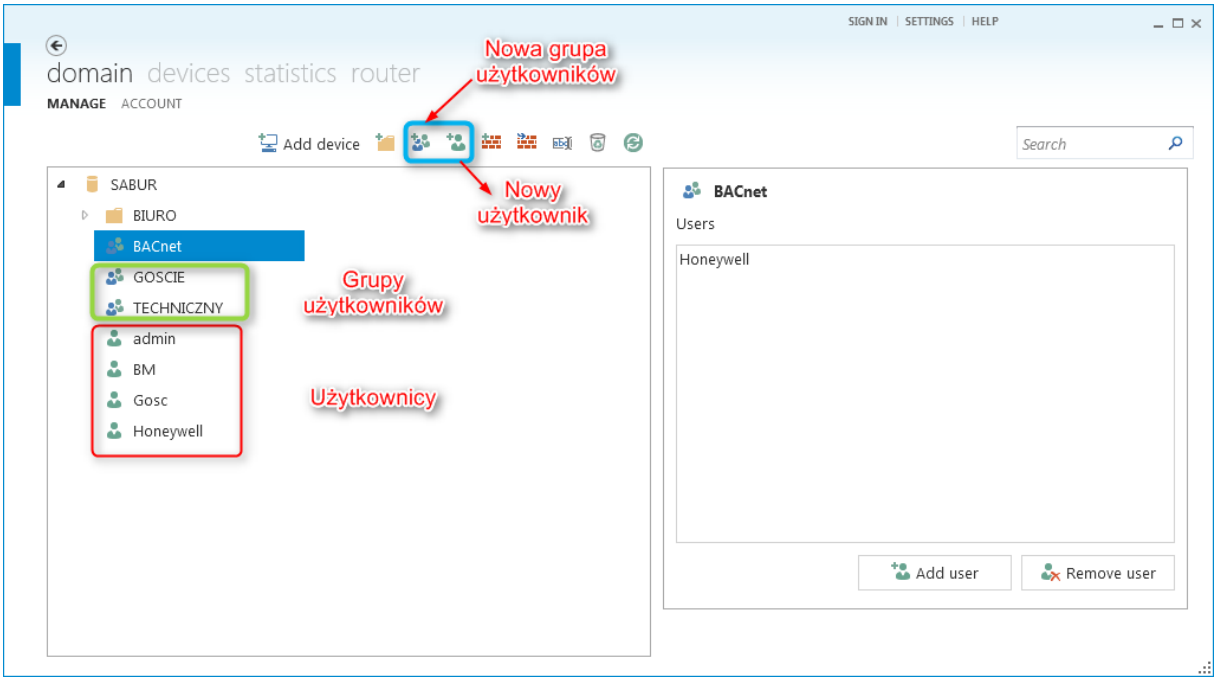


Wprowadzamy nazwę urządzenia. Zatwierdzamy zmiany, klikając przycisk OK. Urządzenie zostało poprawnie przypisane do domeny:

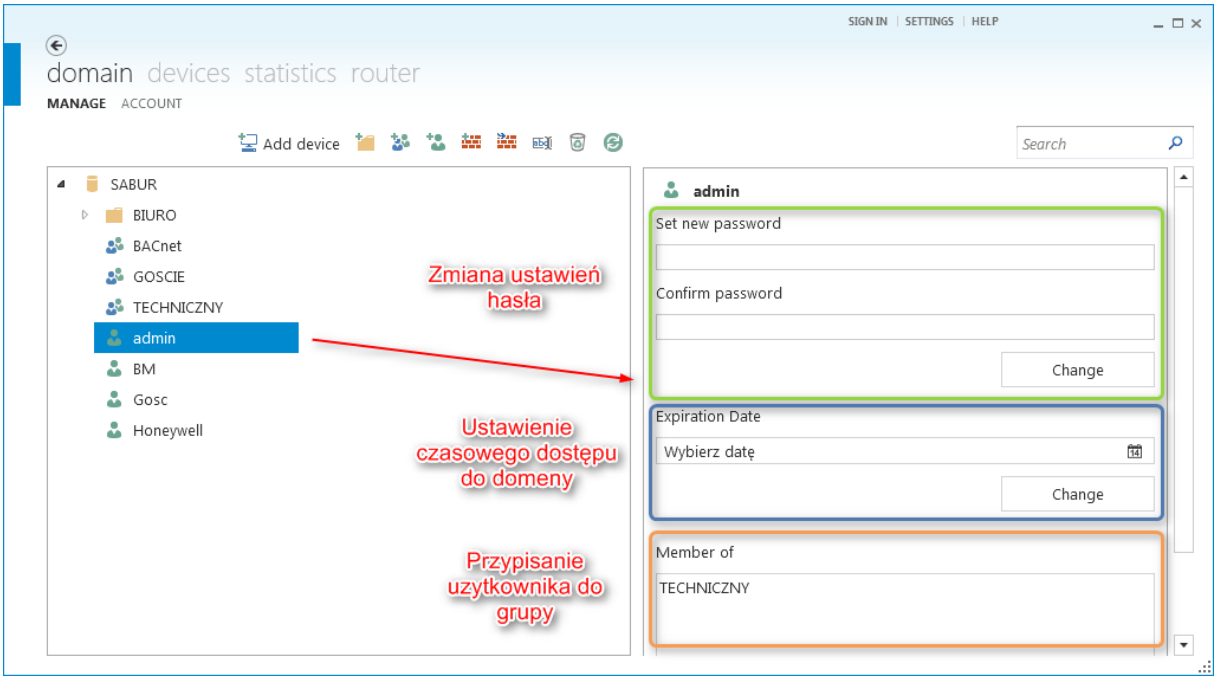


3.5. Zarządzanie użytkownikami

Aplikacja Ubiquity Control Center pozwala na zaawansowane zarządzanie dostępem do urządzeń zdalnych przypisanych do domeny. Kontrola dostępu odbywa się poprzez definiowanie użytkowników i przypisywanie im określonych praw. W celu zarządzania kontami użytkowników korzystamy z paska narzędzi w zakładce *Domain*:



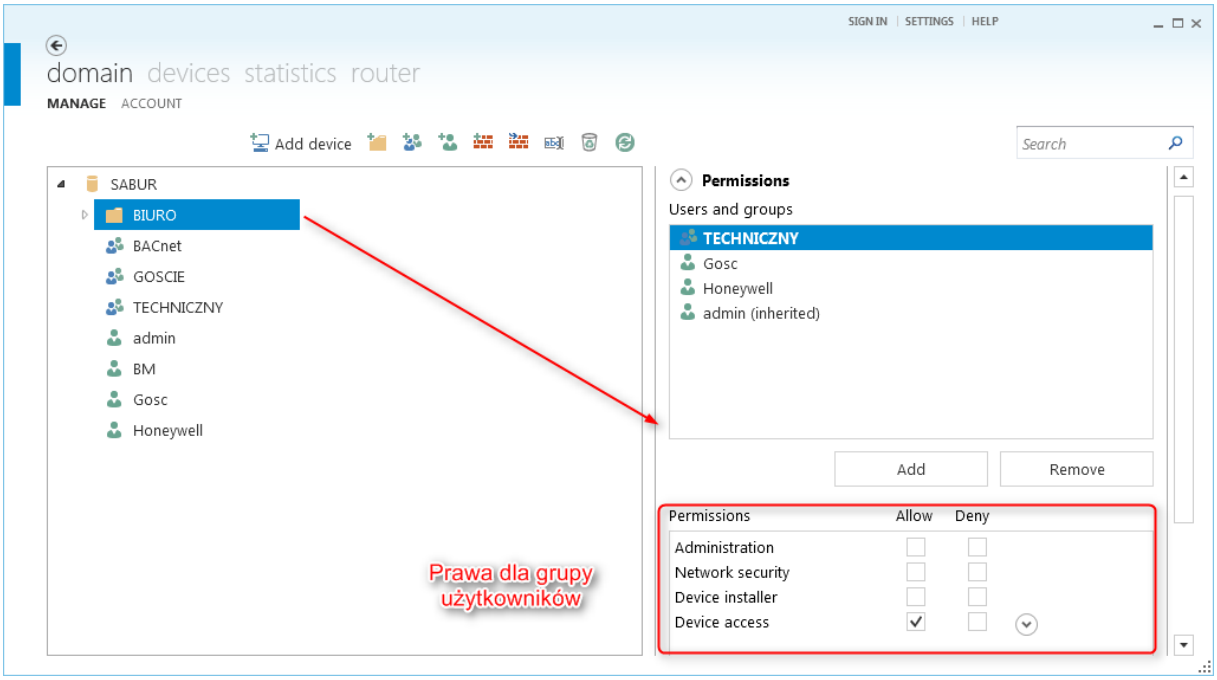
Program umożliwia dodawanie nowych użytkowników i modyfikowanie ich parametrów. Możemy m.in. zmienić hasło istniejącego użytkownika lub zdefiniować czasowy dostęp do zasobów domeny:



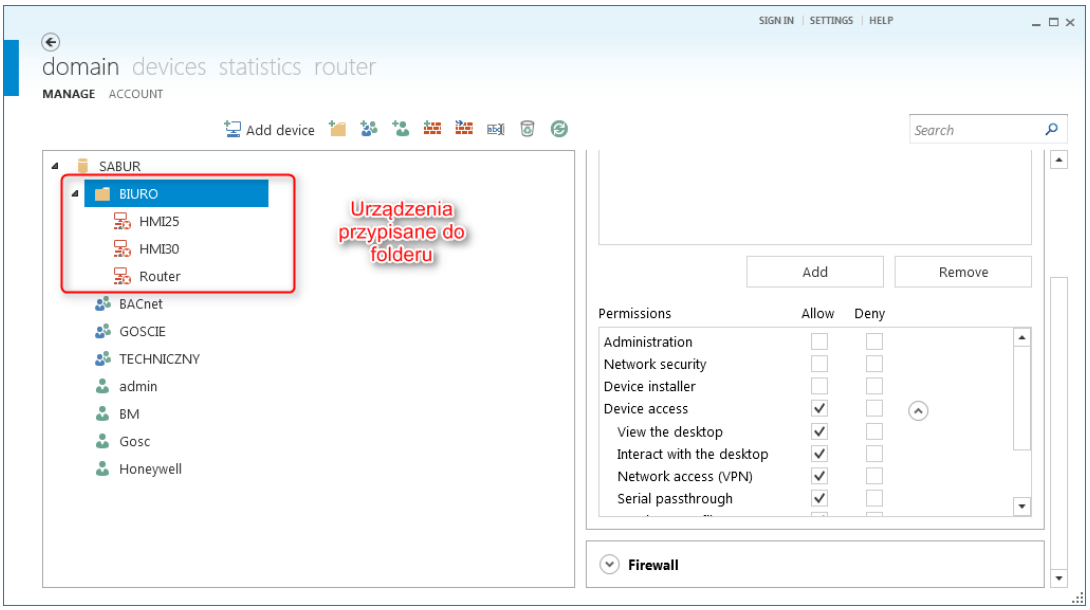
3.6. Grupowanie zasobów. Przypisywanie praw dostępu

Każdemu użytkownikowi lub grupie użytkowników możemy przypisać określone prawa dostępu do urządzeń zdalnych. W tym celu zaleca się grupowanie dodanych do domeny

urządzeń w folderach. Dla każdego folderu możemy bowiem określić, którzy użytkownicy lub grupy użytkowników mogą mieć do niego dostęp. W tym celu klikamy na nazwę domeny w karcie *Devices* i wybieramy opcję *Create folder*. Zostaje utworzony nowy folder, dla którego przypisujemy prawa dostępu:



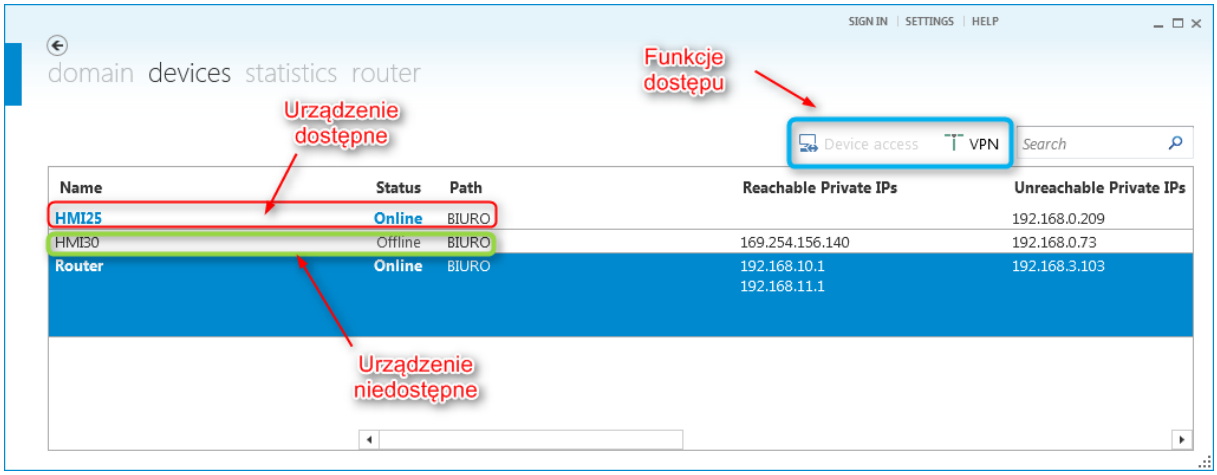
Po przypisaniu praw dostępu do folderu, możemy umieścić w nim zdefiniowane dla domeny urządzenia. W tym celu klikamy lewym przyciskiem myszy na wybrane urządzenie i przeciągamy je do folderu:



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

4. Funkcje systemu Ubiquity

Po dodaniu urządzenia do domeny Ubiquity mamy możliwość uzyskania do niego zdalnego dostępu. Jeżeli możliwe jest nawiązanie połączenia, urządzenie będzie podświetlone w kolorze niebieskim:

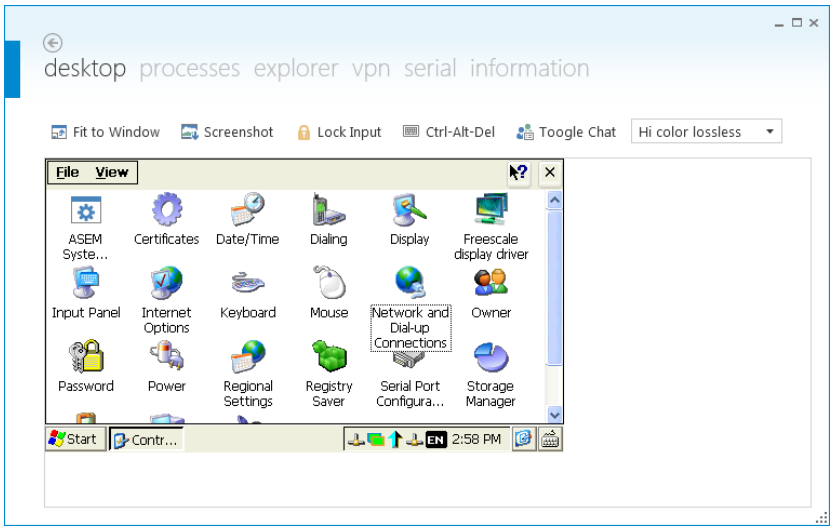


W liście urządzeń widoczne są szczegółowe informacje na temat zdalnego urządzenia np. adres IP, nazwa, status urządzenia. Dostępne są także 2 przyciski (oznaczone na rysunku powyżej), które umożliwiają bezpośrednie przejście do funkcji zdalnego pulpitu (*Device Access*) lub nawiązania połączenia poprzez VPN.

4.1. Funkcje zdalnego dostępu do urządzenia

Zdalny Pulpit:

Kliknięcie ikony *Device Access* powoduje uruchomienie funkcji zdalnego pulpitu:

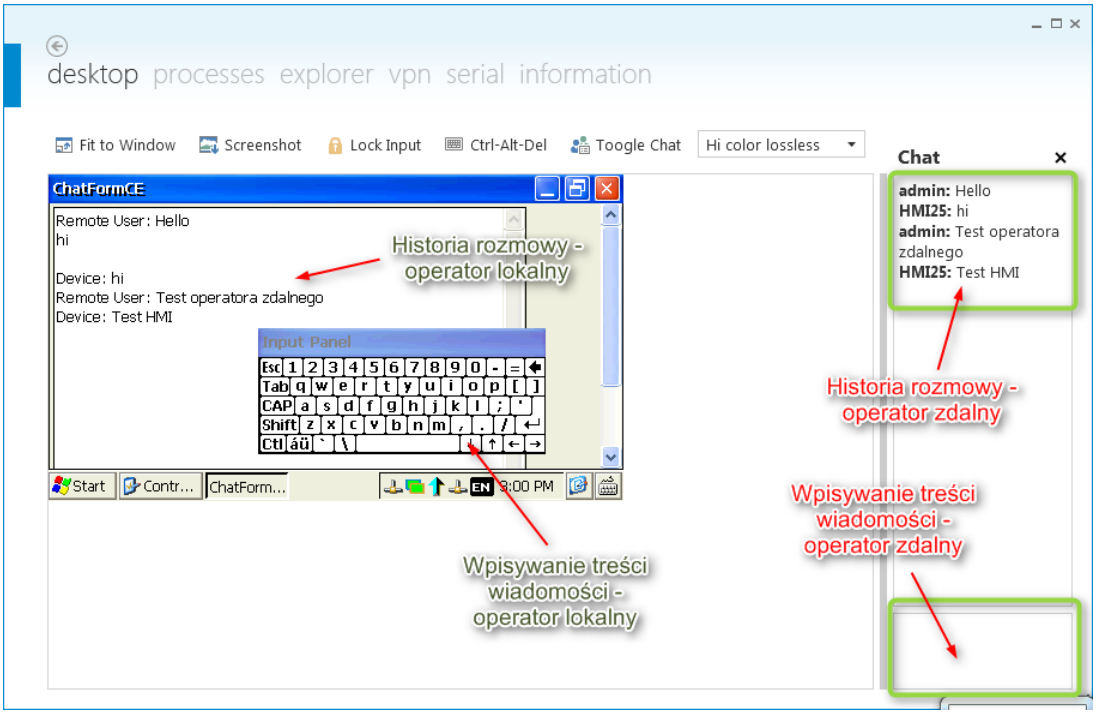


Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Warto zauważyć, że wszystkie działania operatora na komputerze z aplikacją Control Center są na bieżąco widoczne dla osoby pracującej na panelu HMI. Działa to także w drugą stronę – operator pracujący na komputerze serwisowym widzi na ekranie wszystkie działania wykonywane przez osobę pracującą na panelu HMI.

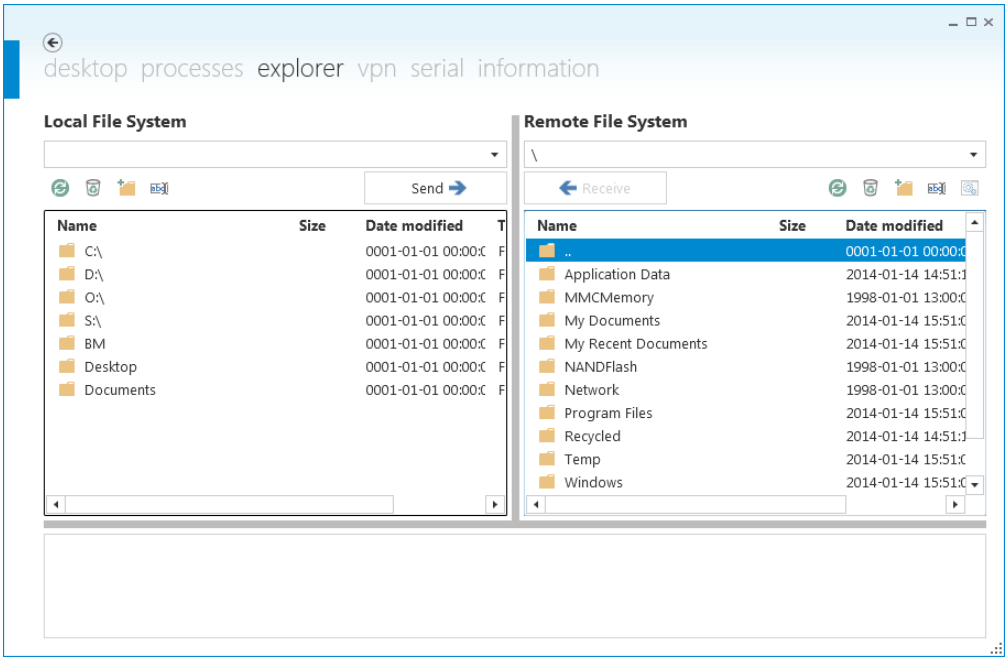
Czat:

Z funkcją zdalnego pulpitu bezpośrednio powiązana jest możliwość prowadzenia rozmów poprzez interfejs tekstowy. Aby rozpocząć rozmowę z górnego menu wybieramy ikonę *Czat*, która umożliwia nam wpisywanie tekstu po prawej stronie okna aplikacji:

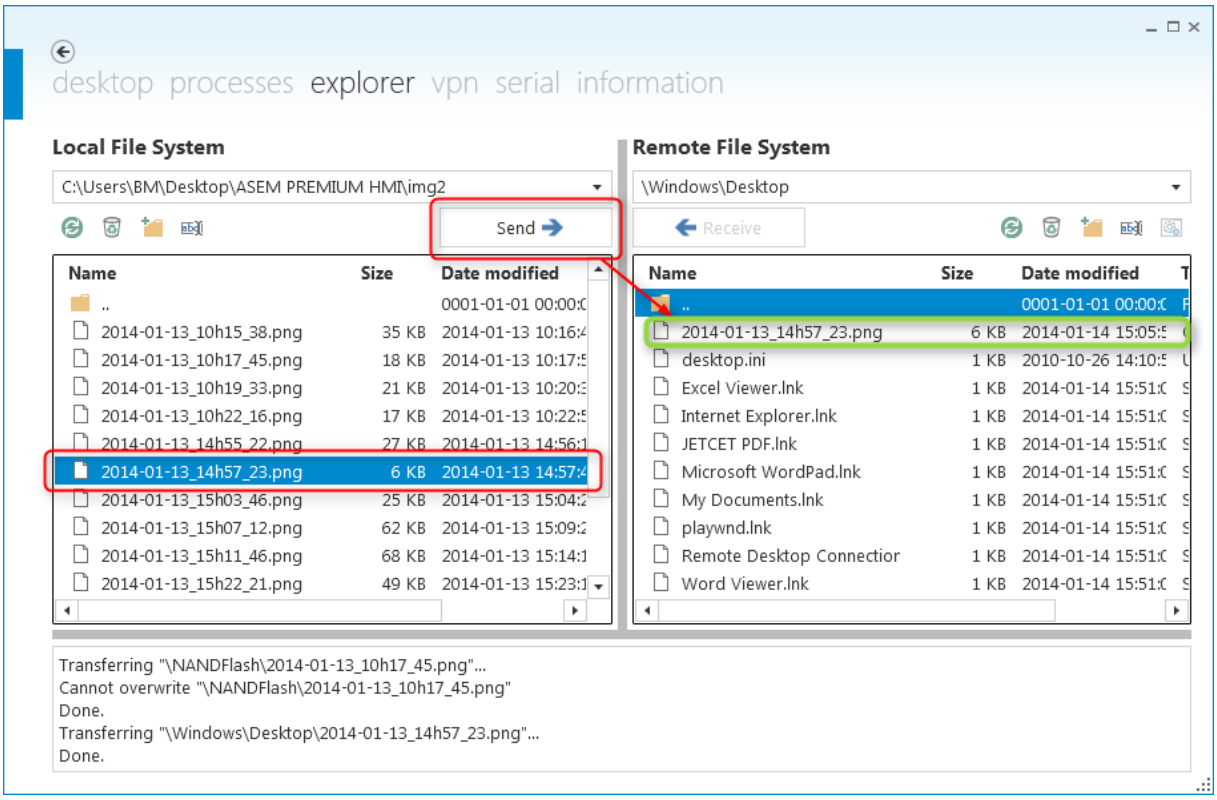


Transfer plików:

Za pomocą aplikacji Ubiquity Control Center możemy w prosty sposób dokonać transferu plików do i z urządzenia zdalnego. Warto zauważyć, że nie potrzebujemy do tego celu żadnego dodatkowego programu, ani połączenia FTP. Aby wejść w funkcję przesyłania plików klikamy na kartę *Explorer* znajdującą się w górnym pasku narzędzi:



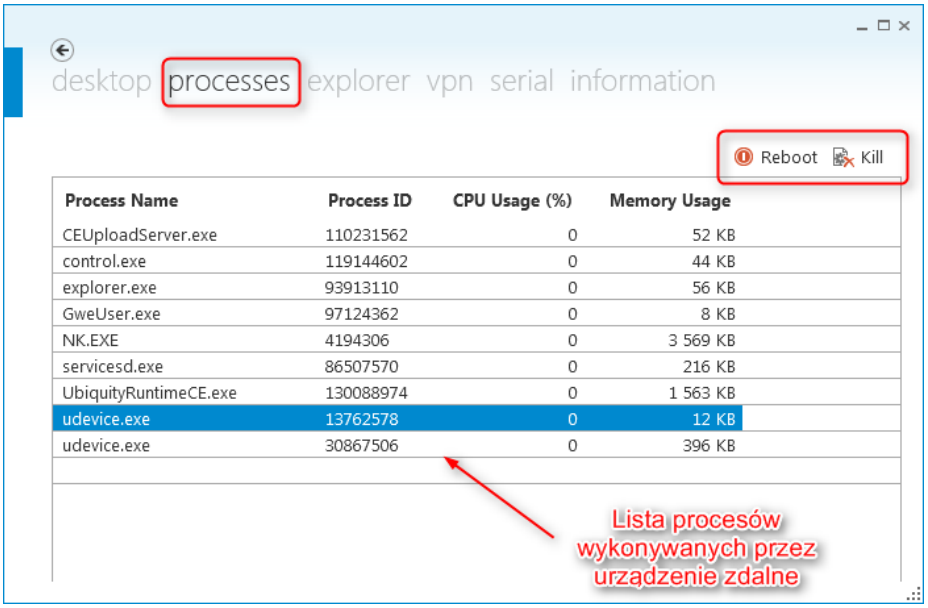
Wybieramy plik, który chcemy przesłać (np. z komputera zdalnego) i klikamy przycisk *Send*. Plik zostaje umieszczony we wskazanej lokalizacji na urządzeniu zdalnym:



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

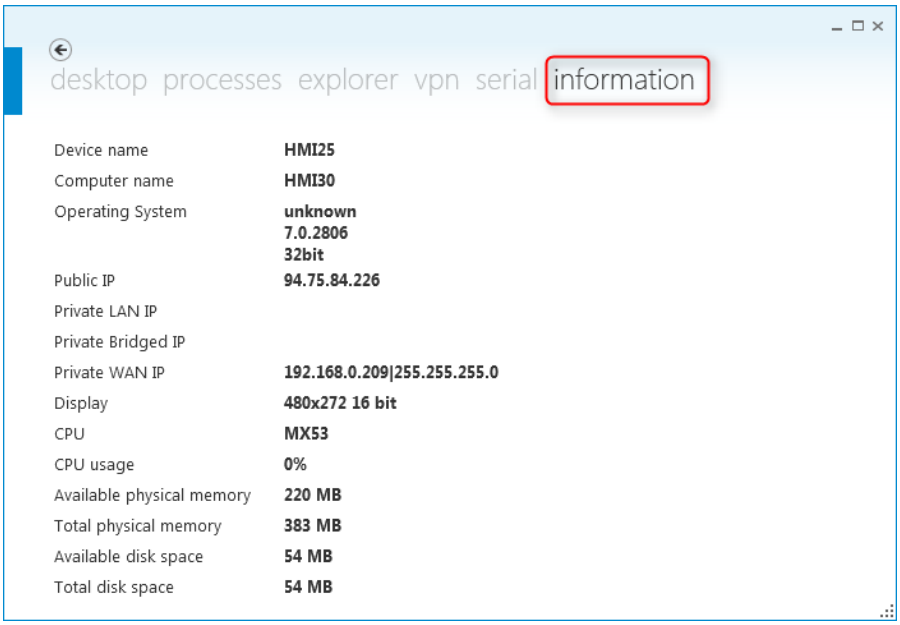
Menadżer zadań:

Wybór karty *Processes* pozwala na kontrolowanie zadań wykonywanych przez panel HMI. Operator zdalny może zakończyć wykonywanie danego zadania poprzez kliknięcie na przycisk *Kill.* Wybranie opcji *Reboot* powoduje ponowne uruchomienie urządzenia zdalnego:



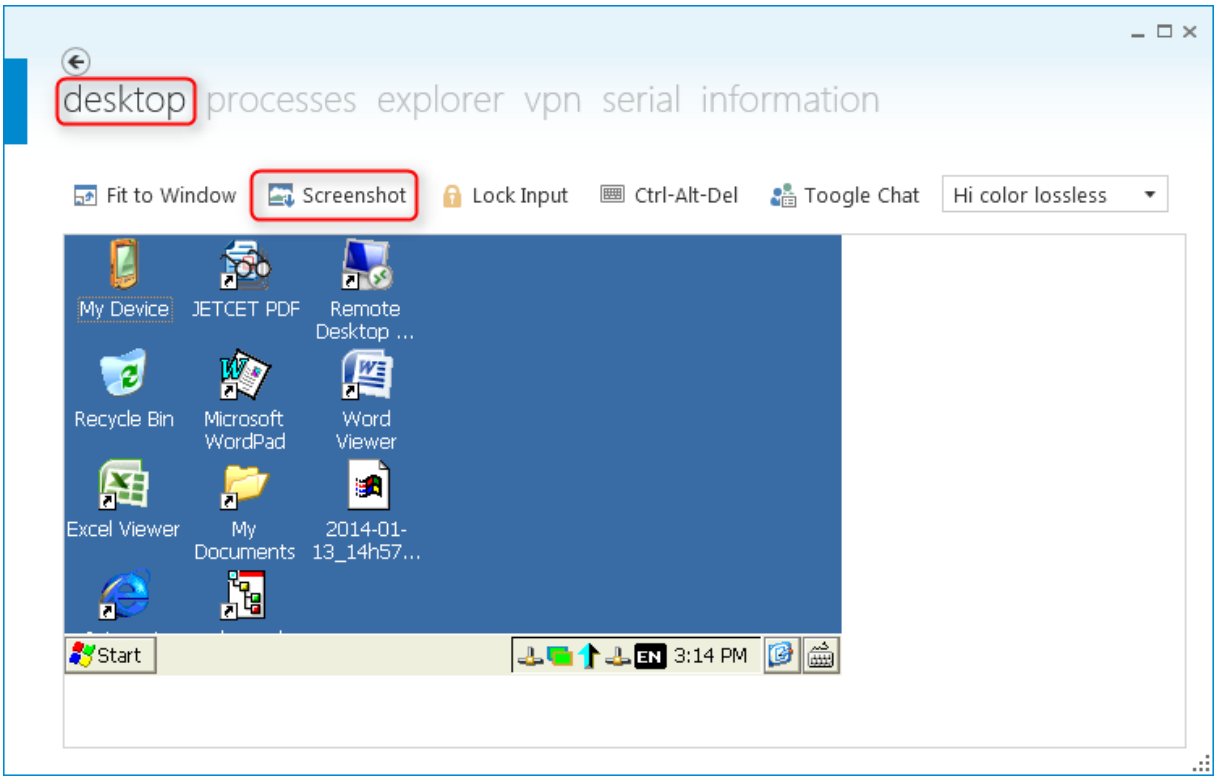
Pozostałe funkcje:

Oprócz funkcji wymienionych w rozdziałach 4.1-4.4 użytkownik Ubiquity Control Center uzyskuje możliwość dostępu do szczegółowych informacji na temat urządzenia. Jest to możliwe po kliknięciu na zakładkę *Information*:



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Ciekawą funkcją jest także możliwość szybkiego wykonywania zrzutów ekranowych z pulpitu urządzenia zdalnego. W tym celu, będąc w widoku pulpitu zdalnego należy wybrać opcję *Screenshot* z górnego paska narzędzi:

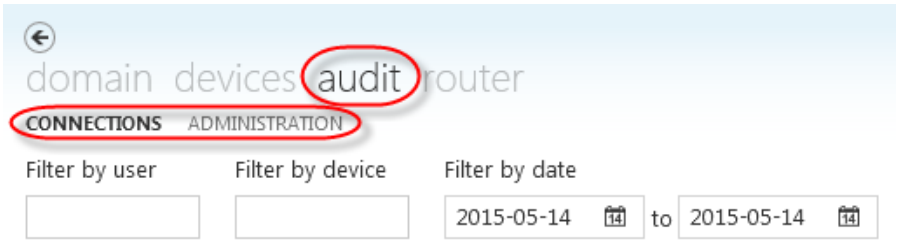


Z poziomu okna zdalnego pulpitu mamy także dostęp do funkcji:

- **Fit to Window** – dopasowanie rozmiaru widoku pulpitu zdalnego do okna aplikacji;
- **Lock / Unlock Input** – zablokowanie / odblokowanie klawiatury bądź myszy podłączonej do urządzenia zdalnego (jeżeli takie urządzenia zostały podłączone);
- **Ctr+Alt+Del** – wywoływanie komendy Ctrl+Alt+Del na urządzeniu zdalnym.

4.2. Statystyki i audyt

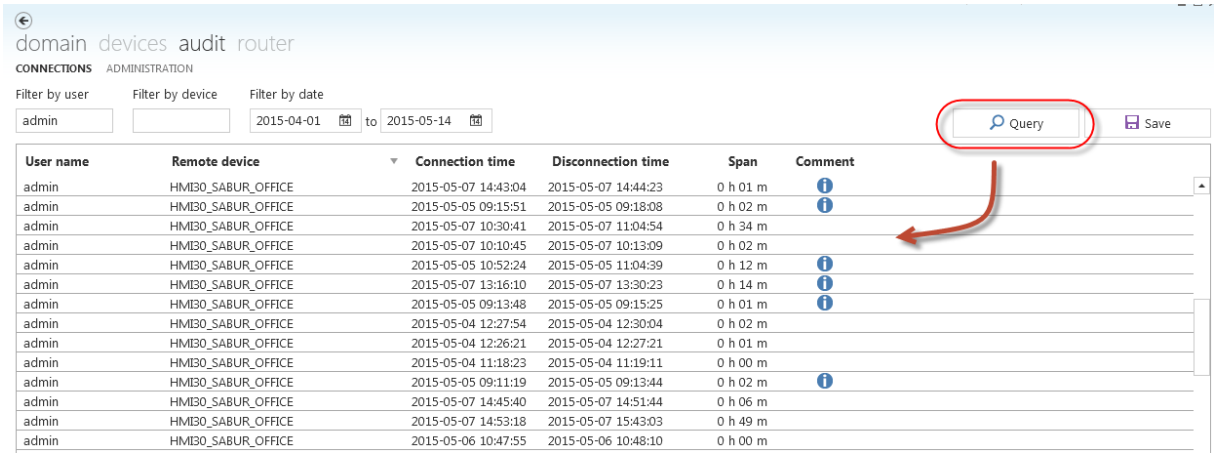
Funkcjonalność audytu Domeny Ubiquity pozwala na monitorowanie historii działań użytkowników obejmującej między innymi: połączenia z urządzeniami, logowanie, zmiany ustawień konta itp. Przejście do okna audytu jest możliwe z poziomu górnego menu, po zalogowaniu się do Domeny:



W ramach okna *Audit* możemy przełączać się pomiędzy dwiema zakładkami:

- **Connections** – okno wyświetlające informacje o połączeniach użytkowników z poszczególnymi urządzeniami przypisanymi do Domeny;
- **Administration** – okno wyświetlające informacje o zmianach (np. dodanie nowego użytkownika) i wydarzeniach (np. zalogowanie użytkownika do Domeny), które zostały zarejestrowane w Domenie;

Zakładka *Connections* zawiera dodatkowe menu pozwalające na filtrowanie wyników w zależności od: użytkownika, urządzenia oraz daty wydarzeń. Po wprowadzeniu interesującego nas filtru klikamy na przycisk *Query* – rezultaty pojawiają się na liście:



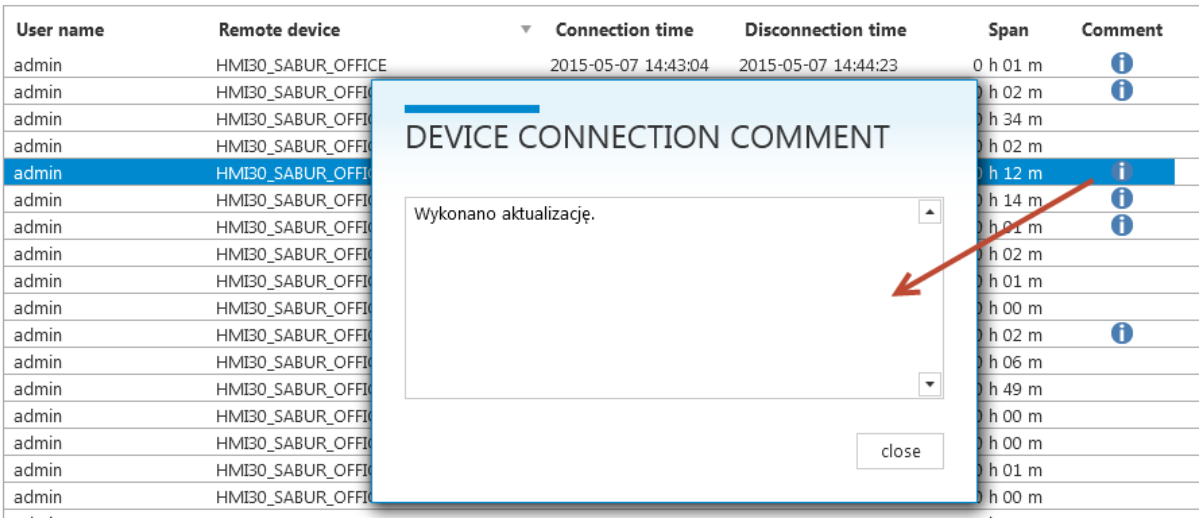
User name	Remote device	Connection time	Disconnection time	Span	Comment
admin	HMI30_SABUR_OFFICE	2015-05-07 14:43:04	2015-05-07 14:44:23	0 h 01 m	
admin	HMI30_SABUR_OFFICE	2015-05-05 09:15:51	2015-05-05 09:18:08	0 h 02 m	
admin	HMI30_SABUR_OFFICE	2015-05-07 10:30:41	2015-05-07 11:04:54	0 h 34 m	
admin	HMI30_SABUR_OFFICE	2015-05-07 10:10:45	2015-05-07 10:13:09	0 h 02 m	
admin	HMI30_SABUR_OFFICE	2015-05-05 10:52:24	2015-05-05 11:04:39	0 h 12 m	
admin	HMI30_SABUR_OFFICE	2015-05-07 13:16:10	2015-05-07 13:30:23	0 h 14 m	
admin	HMI30_SABUR_OFFICE	2015-05-05 09:13:48	2015-05-05 09:15:25	0 h 01 m	
admin	HMI30_SABUR_OFFICE	2015-05-04 12:27:54	2015-05-04 12:30:04	0 h 02 m	
admin	HMI30_SABUR_OFFICE	2015-05-04 12:26:21	2015-05-04 12:27:21	0 h 01 m	
admin	HMI30_SABUR_OFFICE	2015-05-04 11:18:23	2015-05-04 11:19:11	0 h 00 m	
admin	HMI30_SABUR_OFFICE	2015-05-05 09:11:19	2015-05-05 09:13:44	0 h 02 m	
admin	HMI30_SABUR_OFFICE	2015-05-07 14:45:40	2015-05-07 14:51:44	0 h 06 m	
admin	HMI30_SABUR_OFFICE	2015-05-07 14:53:18	2015-05-07 15:43:03	0 h 49 m	
admin	HMI30_SABUR_OFFICE	2015-05-06 10:47:55	2015-05-06 10:48:10	0 h 00 m	

W oknie widoczne są następujące informacje:

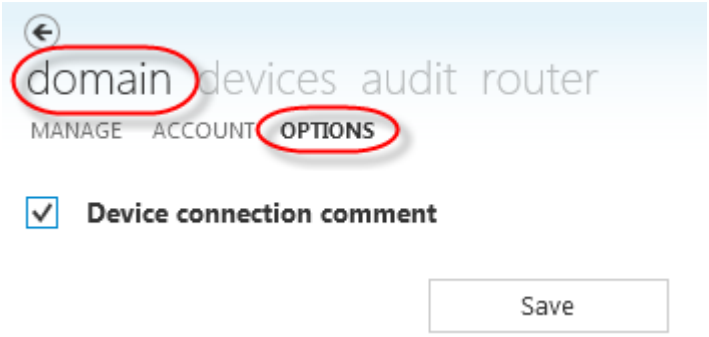
- **User name** – nazwa użytkownika, który nawiązał połączenie;
- **Remote device** – urządzenie zdalne, z którym nawiązano połączenie;
- **Connection time** – data i godzina rozpoczęcia połączenia;
- **Disconnection time** – data i godzina zakończenia połączenia;
- **Span** – czas trwania połączenia;
- **Comment** – komentarz użytkownika dotyczący zakończonej sesji.

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

W kolumnie *Comment* mogą być widoczne ikony , co oznacza, że użytkownik po zakończeniu połączenia uzupełnił informację dotyczącą działań prowadzonych podczas sesji:

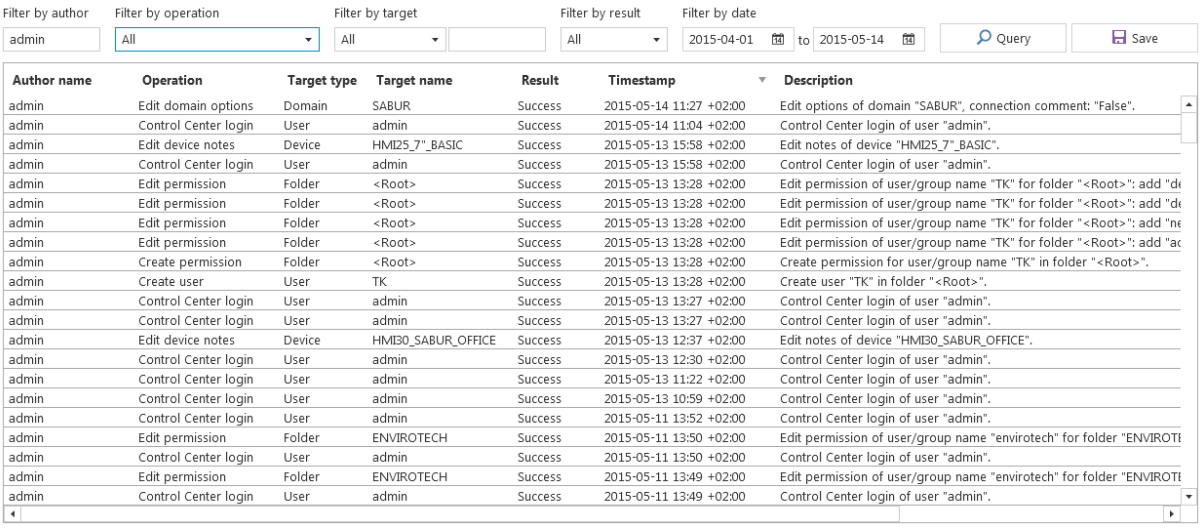


Opcja konieczności pozostawiania komentarzy po zakończeniu każdej sesji zdalnej może być aktywowana w zakładce *Options* menu *Domain* (opcja domyślnie nieaktywna):



W oknie zakładki *Administration* znajduje się menu, które pozwala na filtrowanie elementów wyświetlanych na liście, np. w zależności od użytkownika, typu zdarzenia lub daty jego wystąpienia. Po kliknięciu przycisku *Query* na liście pojawiają się rezultaty:

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

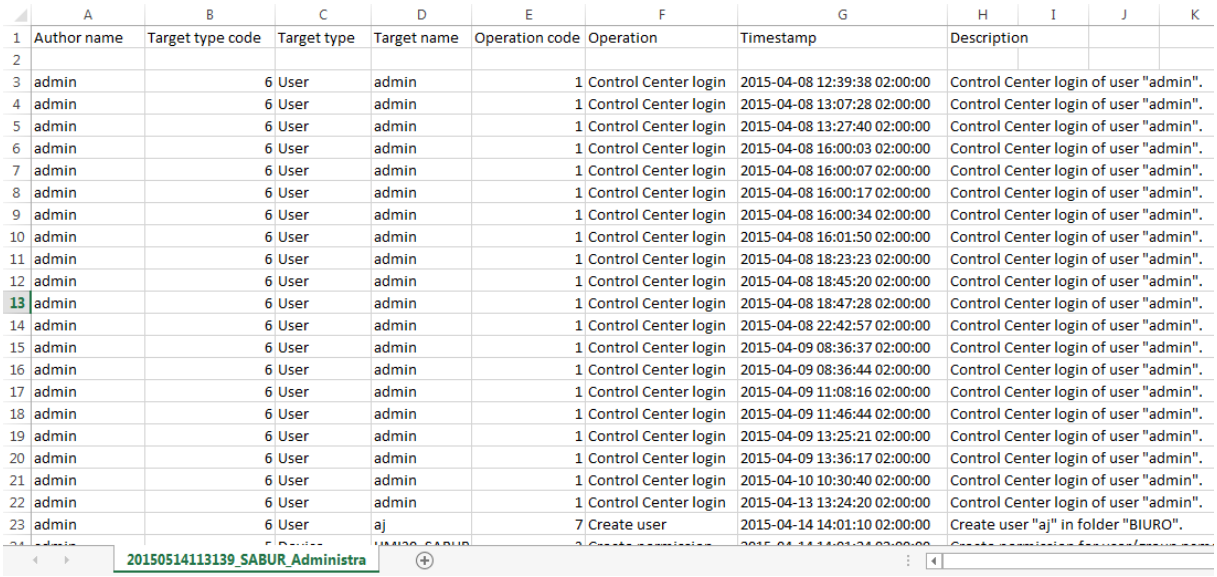


Author name	Operation	Target type	Target name	Result	Timestamp	Description
admin	Edit domain options	Domain	SABUR	Success	2015-05-14 11:27 +02:00	Edit options of domain "SABUR", connection comment: "False".
admin	Control Center login	User	admin	Success	2015-05-14 11:04 +02:00	Control Center login of user "admin".
admin	Edit device notes	Device	HMI25_7"_BASIC	Success	2015-05-13 15:58 +02:00	Edit notes of device "HMI25_7"_BASIC".
admin	Control Center login	User	admin	Success	2015-05-13 15:58 +02:00	Control Center login of user "admin".
admin	Edit permission	Folder	<Root>	Success	2015-05-13 13:28 +02:00	Edit permission of user/group name "TK" for folder "<Root>": add "d
admin	Edit permission	Folder	<Root>	Success	2015-05-13 13:28 +02:00	Edit permission of user/group name "TK" for folder "<Root>": add "d
admin	Edit permission	Folder	<Root>	Success	2015-05-13 13:28 +02:00	Edit permission of user/group name "TK" for folder "<Root>": add "n
admin	Edit permission	Folder	<Root>	Success	2015-05-13 13:28 +02:00	Edit permission of user/group name "TK" for folder "<Root>": add "a
admin	Create permission	Folder	<Root>	Success	2015-05-13 13:28 +02:00	Create permission for user/group name "TK" in folder "<Root>".
admin	Create user	User	TK	Success	2015-05-13 13:28 +02:00	Create user "TK" in folder "<Root>".
admin	Control Center login	User	admin	Success	2015-05-13 13:27 +02:00	Control Center login of user "admin".
admin	Control Center login	User	admin	Success	2015-05-13 13:27 +02:00	Control Center login of user "admin".
admin	Edit device notes	Device	HMI30_SABUR_OFFICE	Success	2015-05-13 12:37 +02:00	Edit notes of device "HMI30_SABUR_OFFICE".
admin	Control Center login	User	admin	Success	2015-05-13 12:30 +02:00	Control Center login of user "admin".
admin	Control Center login	User	admin	Success	2015-05-13 11:22 +02:00	Control Center login of user "admin".
admin	Control Center login	User	admin	Success	2015-05-13 10:59 +02:00	Control Center login of user "admin".
admin	Control Center login	User	admin	Success	2015-05-11 13:52 +02:00	Control Center login of user "admin".
admin	Edit permission	Folder	ENVIROTECH	Success	2015-05-11 13:50 +02:00	Edit permission of user/group name "envirotech" for folder "ENVIROTI
admin	Control Center login	User	admin	Success	2015-05-11 13:50 +02:00	Control Center login of user "admin".
admin	Edit permission	Folder	ENVIROTECH	Success	2015-05-11 13:49 +02:00	Edit permission of user/group name "envirotech" for folder "ENVIROTI
admin	Control Center login	User	admin	Success	2015-05-11 13:49 +02:00	Control Center login of user "admin".

- **Author name** – nazwa użytkownika wykonującego daną operację;
- **Operation** – nazwa operacji (np. zmiana poziomu dostępu, zalogowanie się itp.);
- **Target type** – obiekt, z którym związana jest operacja (urządzenie, folder, użytkownik, itp.);
- **Target name** – nazwa obiektu, z którym związana jest operacja (np. nazwa użytkownika);
- **Result** – rezultat operacji (sukces – porażka);
- **Timestamp** – czas wykonania operacji;
- **Description** – dodatkowy opis.

Obie listy (z zakładki *Connections* i *Administration*) mogą być wyeksportowane do pliku csv i zapisane na dysku twardym komputera po kliknięciu na przycisk *Save*:

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

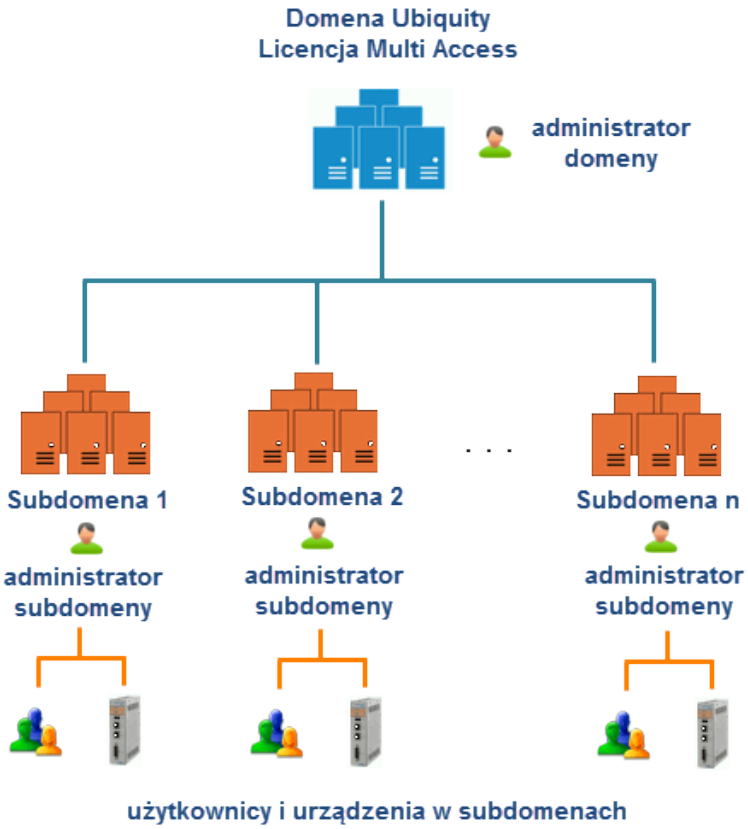


	A	B	C	D	E	F	G	H	I	J	K
1	Author name	Target type code	Target type	Target name	Operation code	Operation	Timestamp	Description			
2											
3	admin	6	User	admin	1	Control Center login	2015-04-08 12:39:38 02:00:00	Control Center login of user "admin".			
4	admin	6	User	admin	1	Control Center login	2015-04-08 13:07:28 02:00:00	Control Center login of user "admin".			
5	admin	6	User	admin	1	Control Center login	2015-04-08 13:27:40 02:00:00	Control Center login of user "admin".			
6	admin	6	User	admin	1	Control Center login	2015-04-08 16:00:03 02:00:00	Control Center login of user "admin".			
7	admin	6	User	admin	1	Control Center login	2015-04-08 16:00:07 02:00:00	Control Center login of user "admin".			
8	admin	6	User	admin	1	Control Center login	2015-04-08 16:00:17 02:00:00	Control Center login of user "admin".			
9	admin	6	User	admin	1	Control Center login	2015-04-08 16:00:34 02:00:00	Control Center login of user "admin".			
10	admin	6	User	admin	1	Control Center login	2015-04-08 16:01:50 02:00:00	Control Center login of user "admin".			
11	admin	6	User	admin	1	Control Center login	2015-04-08 18:23:23 02:00:00	Control Center login of user "admin".			
12	admin	6	User	admin	1	Control Center login	2015-04-08 18:45:20 02:00:00	Control Center login of user "admin".			
13	admin	6	User	admin	1	Control Center login	2015-04-08 18:47:28 02:00:00	Control Center login of user "admin".			
14	admin	6	User	admin	1	Control Center login	2015-04-08 22:42:57 02:00:00	Control Center login of user "admin".			
15	admin	6	User	admin	1	Control Center login	2015-04-09 08:36:37 02:00:00	Control Center login of user "admin".			
16	admin	6	User	admin	1	Control Center login	2015-04-09 08:36:44 02:00:00	Control Center login of user "admin".			
17	admin	6	User	admin	1	Control Center login	2015-04-09 11:08:16 02:00:00	Control Center login of user "admin".			
18	admin	6	User	admin	1	Control Center login	2015-04-09 11:46:44 02:00:00	Control Center login of user "admin".			
19	admin	6	User	admin	1	Control Center login	2015-04-09 13:25:21 02:00:00	Control Center login of user "admin".			
20	admin	6	User	admin	1	Control Center login	2015-04-09 13:36:17 02:00:00	Control Center login of user "admin".			
21	admin	6	User	admin	1	Control Center login	2015-04-10 10:30:40 02:00:00	Control Center login of user "admin".			
22	admin	6	User	admin	1	Control Center login	2015-04-13 13:24:20 02:00:00	Control Center login of user "admin".			
23	admin	6	User	aj	7	Create user	2015-04-14 14:01:10 02:00:00	Create user "aj" in folder "BIURO".			

20150514113139_SABUR_Administra

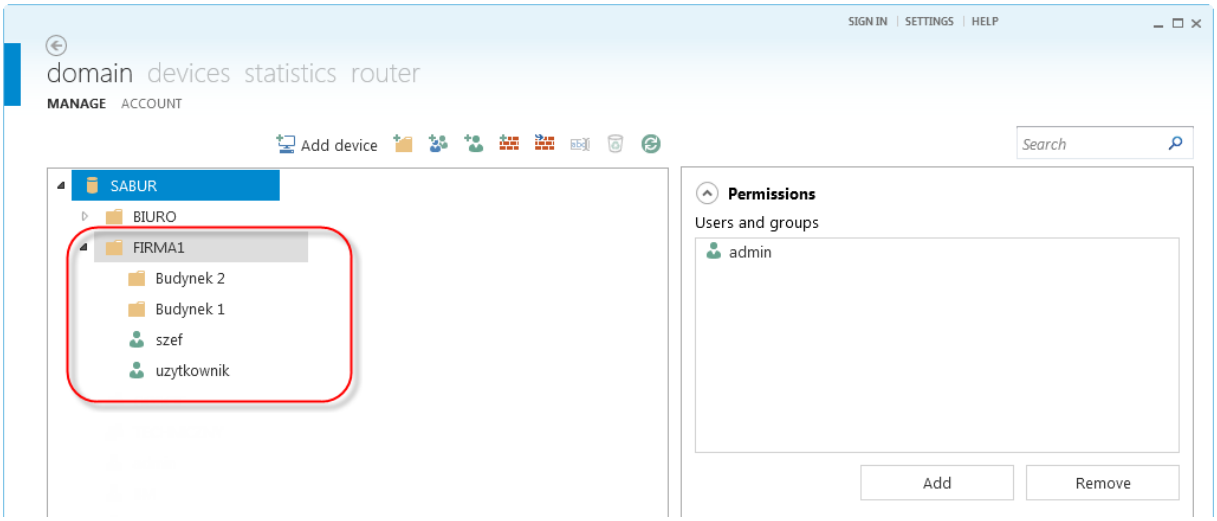
4.3. Subdomeny Ubiquity

Funkcja subdomeny pozwala na przejrzyste grupowanie uprawnień dostępu do poszczególnych urządzeń wybranym użytkownikom. Jest ona szczególnie przydatna w przypadku licencji Multi Access, w której to różne firmy mogą korzystać ze swoich urządzeń przypisanych do jednej Domeny głównej. Każda z subdomen może być zarządzana przez zdefiniowanego lokalnego administratora. Wszyscy użytkownicy przypisani jednej subdomeny nie mają dostępu do ustawień i urządzeń znajdujących się w innych subdomenach:



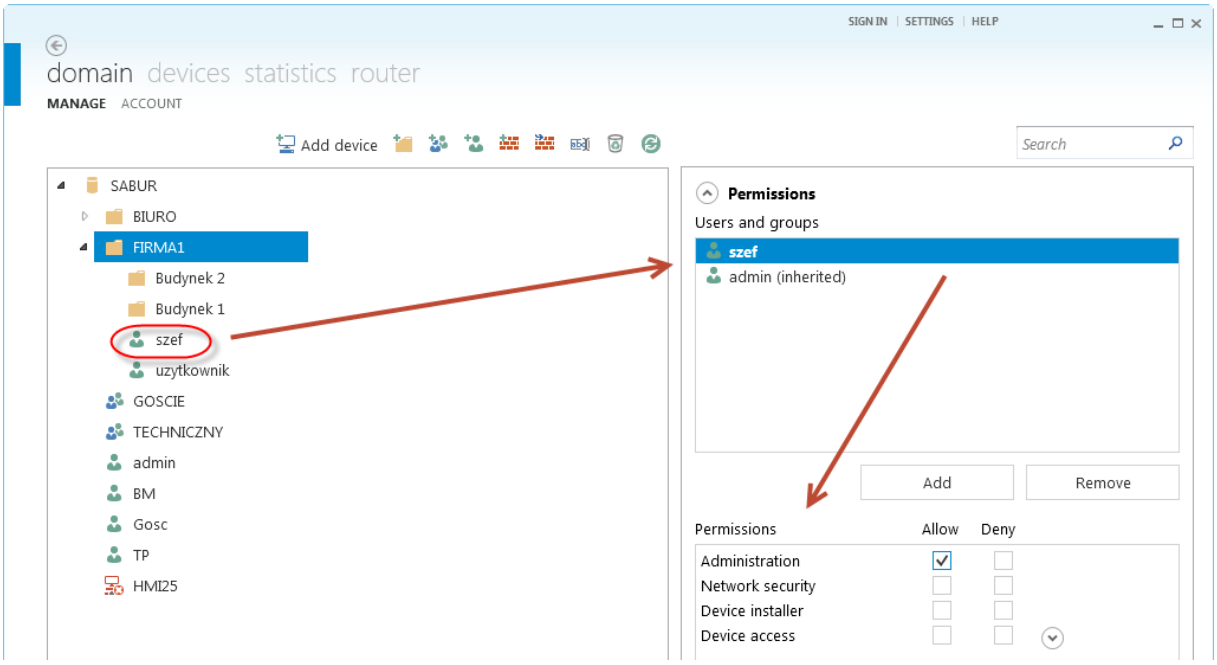
W podanym przykładzie utworzona zostanie subdomena o nazwie ”Firma1”, do której przypisane będą różne urządzenia. Zostanie utworzony także lokalny administrator subdomeny.

Zarządzanie strukturą domeny jest możliwe z poziomu użytkownika o prawach administratora. Tworzymy folder o nazwie *„Firma1”*, definiując w jego obszarze kolejne podfoldery i przyszłych użytkowników subdomeny:

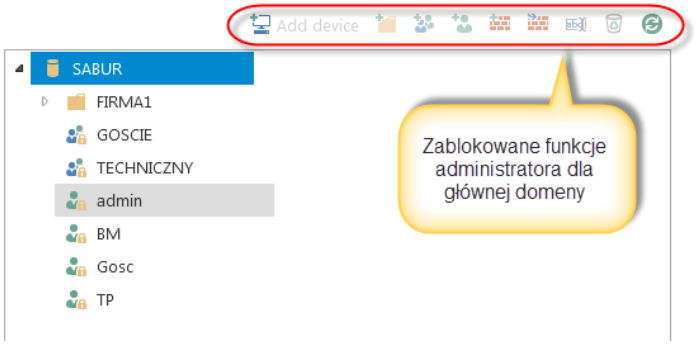


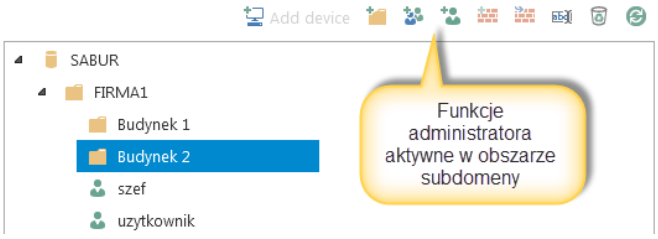
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

W tym momencie jedynym użytkownikiem mającym prawo do zarządzania folderem „Firma 1” jest administrator. W celu przypisania użytkownikowi *szef* prawa administratora lokalnego subdomeny, klikamy na jej główny folder (*Firma 1*), a następnie dodajemy go do okna *Permissions*:



Po zalogowaniu się do Domeny jako użytkownik *szef*, nie będziemy mieli prawa do konfiguracji ustawień w obszarze domeny głównej. W obszarze subdomeny *Firma 1* będziemy jednak mogli wykonywać wszystkie czynności administracyjne:

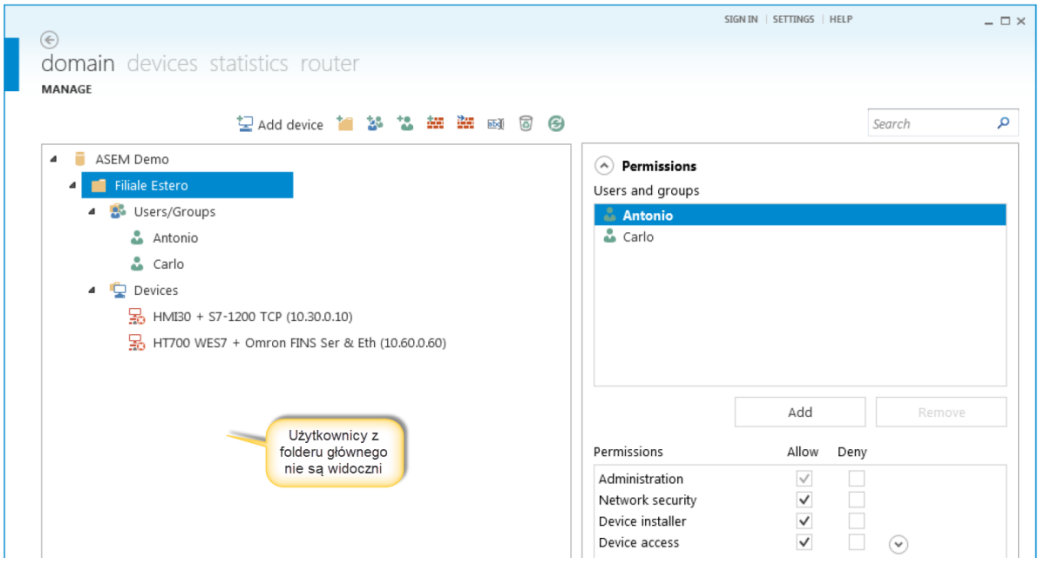




Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Funkcja subdomeny pozwala na przejrzyste grupowanie uprawnień dostępu do poszczególnych urządzeń wybranym użytkownikom. Jest ona szczególnie przydatna w przypadku licencji Multi Access, w której różne firmy mogą korzystać ze swoich urządzeń przypisanych do jednej Domeny głównej:

Przykładowa struktura Domeny Ubiquity – widok administratora subdomeny:



Wyróżnia się 4 podstawowe profile uprawnień:

- Administracja (Administration);
- Konfiguracja urządzenia (Device Installer);
- Dostęp do urządzenia (Device Access);
- Bezpieczeństwo sieci (Network Security);

Sekcja *Administration* listy uprawnień użytkownika zawiera dodatkowe opcje:

- **Access users** – pozwala na uzyskanie dostępu do danych użytkowników z wybranego folderu w celu przypisywania im praw np. do sub-domen;
- **Manage users** – pozwala na edycję użytkowników i grup;
- **Manage folders** – pozwala na zarządzanie folderami Domeny;
- **View statistics** – pozwala na wyświetlenie okna logowań użytkowników do Domeny – dzięki temu administrator sub-domeny może monitorować statystyki dla zarządzanej przez siebie części – w poprzedniej wersji opcja wyświetlania statystyk była dostępna tylko dla administratora Domeny.

Poniżej przedstawiono listę uprawnień, jakie przypisane są do konkretnego profilu:

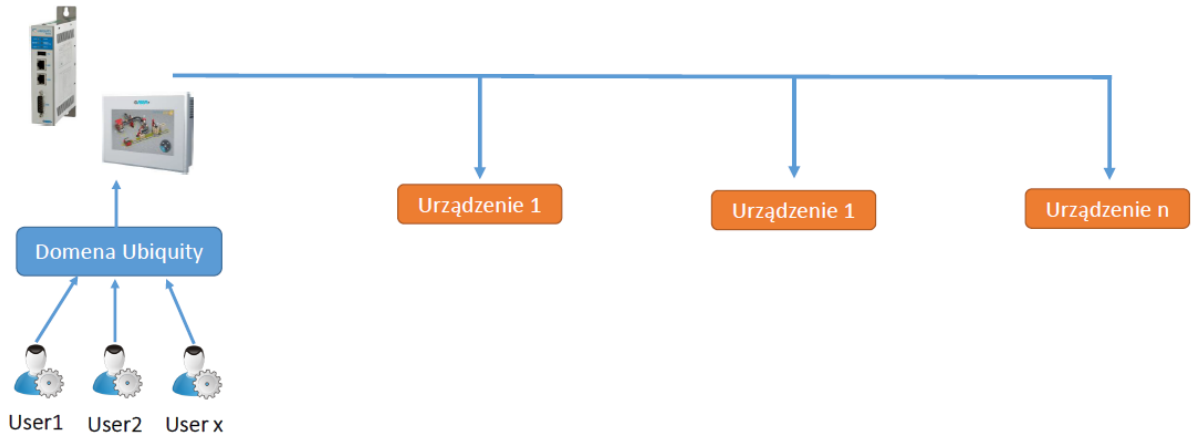
Parametr	Admin.	Konf.	Dostęp	Bezp.
Urządzenia:				
Dodawanie urządzenia do domeny		■		
Usuwanie urządzenia z domeny		■		
Przemieszczanie urządzeń pomiędzy folderami		■		
Zmiana nazwy domeny		■		
Rejestracja licencji Runtime		■		
Usunięcie licencji Runtime z urządzenia		■		
Zdalny dostęp			■	
VPN			■	
Konfiguracja funkcji dostępu dla użytkowników	■			
Wyświetlanie list dostępowych	■			
Zarządzenie ustawieniami VPN firewall				■
Foldery:				
Utworzenie folderu	■			
Usunięcie folderu	■			
Zmiana nazwy folderu	■			
Przypisywanie uprawnień użytkownikom	■			
Zarządzanie ustawieniami VPN firewall				■
Użytkownicy i grupy użytkowników:				
Dodawanie / usuwanie grup	■			
Zmiana nazwy grupy	■			
Wyświetlanie listy grup	■			
Przemieszczanie grup	■			
Dodawanie / usuwanie użytkownika	■			
Zmiana nazwy użytkownika	■			
Zmiana hasła użytkownika	■			
Dodawanie / usuwanie użytkownika do grupy	■			
Domena:				
Założenie nowej domeny	■	■	■	
Zmiana informacji o domenie	■			
Aktywacja domeny	■			
Zarządzenie Routerem		■		
Dostęp do statystyk	■			

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

4.4. Funkcja Firewall

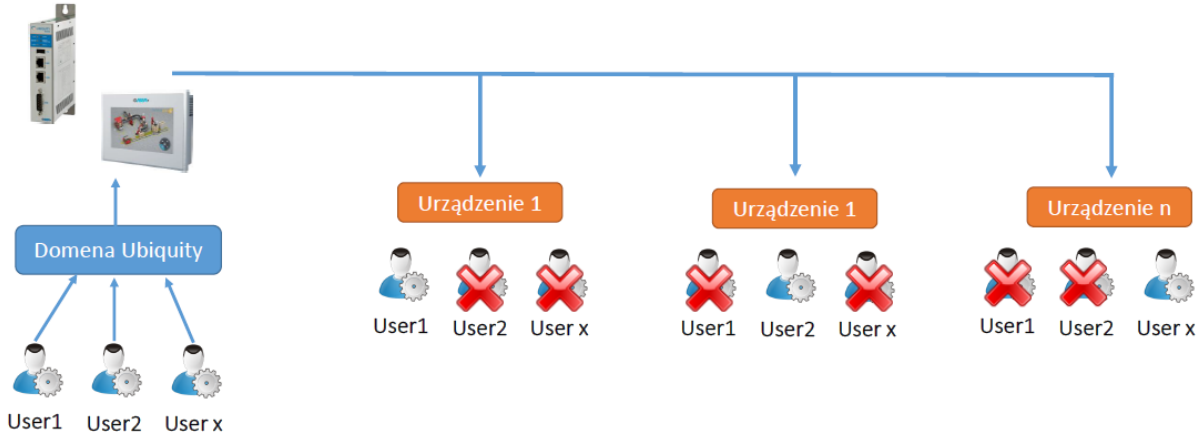
Funkcja Firewall może okazać się bardzo przydatnym narzędziem w momencie, gdy chcemy ograniczyć dostęp poszczególnym użytkownikom do wybranych urządzeń znajdujących się w zdalnych podsieciach komponentów przypisanych do Domeny (Routerów, paneli HMI). Zasada działania funkcji Firewall została przedstawiona na poniższych grafikach.

W podstawowej konfiguracji, jeżeli użytkownik ma prawa dostępu do wybranego urządzenia przypisanego do Domeny, może za jego pośrednictwem nawiązać połączenie z dowolnym urządzeniem znajdującym się w zdalnej podsieci LAN lub szeregowej:



Konfiguracja podstawowa – użytkownicy mają dostęp do wszystkich urządzeń w zdalnych podsieciach.

Zastosowanie funkcji Firewall pozwala na selekcjonowanie dostępu do poszczególnych urządzeń dla każdego z użytkowników:

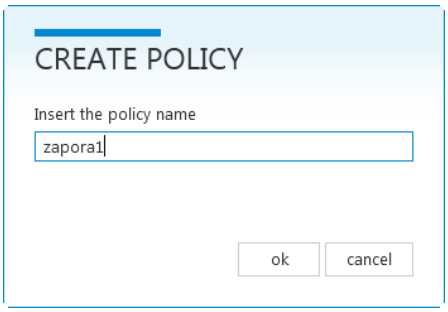


Funkcja Firewall – ograniczenie dostępu dla poszczególnych użytkowników do wybranych urządzeń w zdalnych podsieciach.

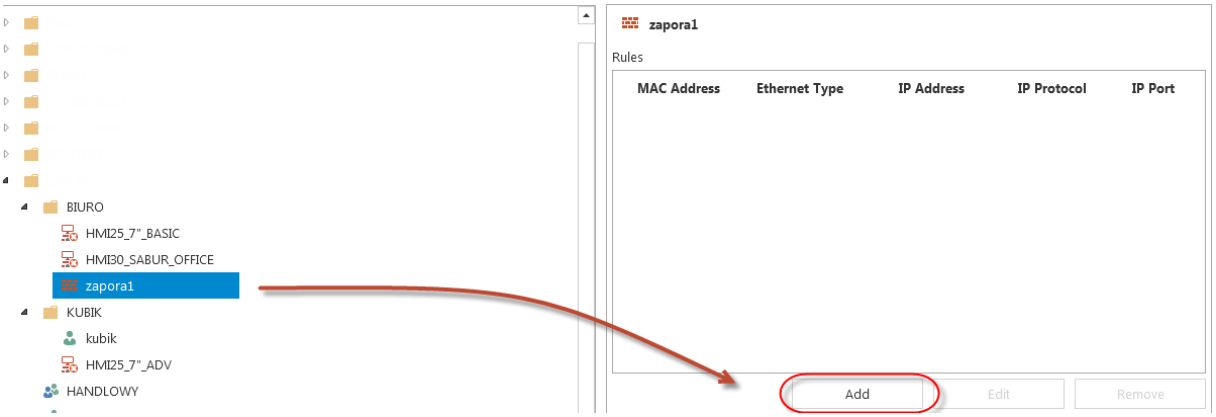
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Do obsługi funkcji Firewall służą dwie ikony znajdujące się w głównym widoku Domeny:

Pierwsza z ikon umożliwia dodanie nowej zapory, druga pozwala na import ustawień z pliku zewnętrznego. Po wybraniu opcji dodania nowej zapory pojawia się okno, w którym wpisujemy nazwę tworzonego elementu:



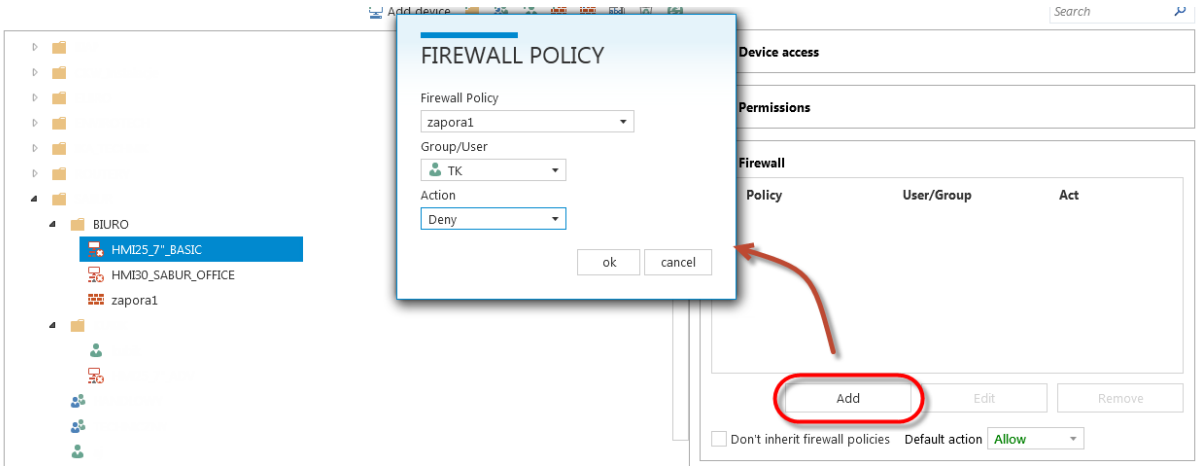
Po kliknięciu OK element pojawia się w strukturze Domeny. Klikamy na przycisk *Add* w celu zdefiniowania parametrów zapory:



Wybieramy rodzaj filtrowania (po adresie MAC lub po ustawieniach portu Ethernet) np.:

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Po zdefiniowaniu ustawień zapory możemy przypisać ją do wybranego urządzenia lub całego folderu i powiązać z konkretnym użytkownikiem. W tym celu zaznaczamy urządzenie lub folder, przechodzimy do zakładki *Permissions* i klikamy na przycisk *Add*:



W oknie *Firewall Policy* dokonujemy powiązania zapory z użytkownikiem:

- **Firewall Policy** – lista wyboru zapory do konfiguracji;
- **Group / User** – powiązanie zapory z wybranym użytkownikiem lub grupą użytkowników. Zapora może być także przypisana do wszystkich użytkowników Domeny (opcja *Any*).
- **Action** – definiuje działanie zapory:
  - **Allow** – wybrany użytkownik będzie mógł uzyskać dostęp do urządzenia / adresu, dla którego została zdefiniowana zapora;
  - **Deny** - wybrany użytkownik będzie miał zablokowany dostęp do urządzenia / adresu, dla którego została zdefiniowana zapora;

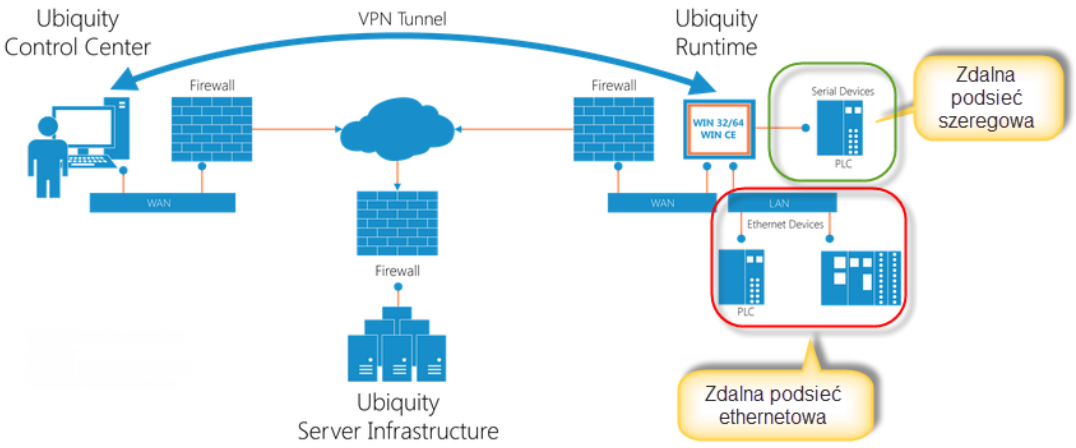
Klikamy przycisk OK w celu potwierdzenia zmian. Zapora została poprawnie skonfigurowana. Ustawiono więc następującą konfigurację:

Wprowadzone zmiany można interpretować w sposób następujący:

Użytkownik o nazwie *TK* został przypisany do zapory o nazwie zapora1, aktywnej dla urządzenia *HMI25_7"_BASIC*, która zabrania mu dostępu (opcja *Deny*) do adresu *192.168.12.45* znajdującego się w zdalnej podsieci panelu HMI.

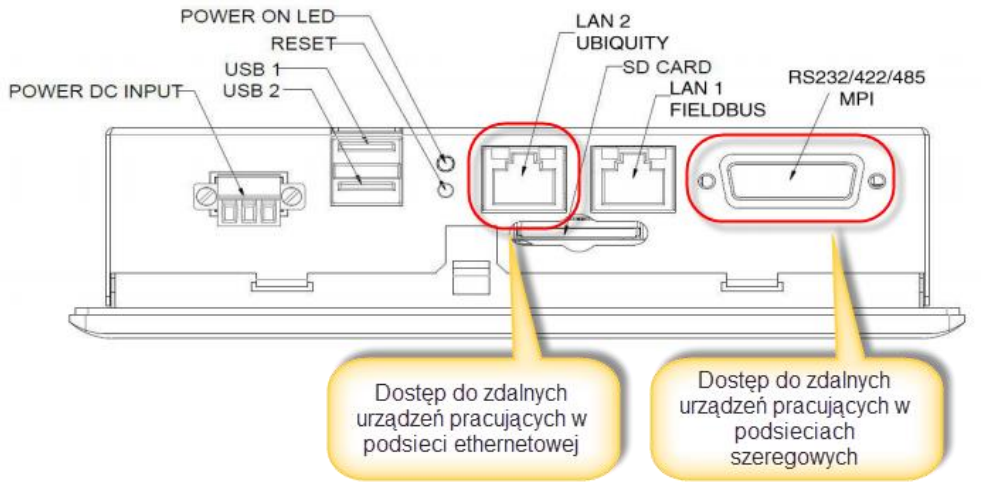
5. Połączenie VPN. Obsługa urządzeń w podsieciach.

ASEM Ubiquity, oprócz zdalnej komunikacji z panelem HMI umożliwia także połączenie z urządzeniami pracującymi w zdalnych podsieciach. Umożliwia to np. zdalne programowanie sterownika PLC.



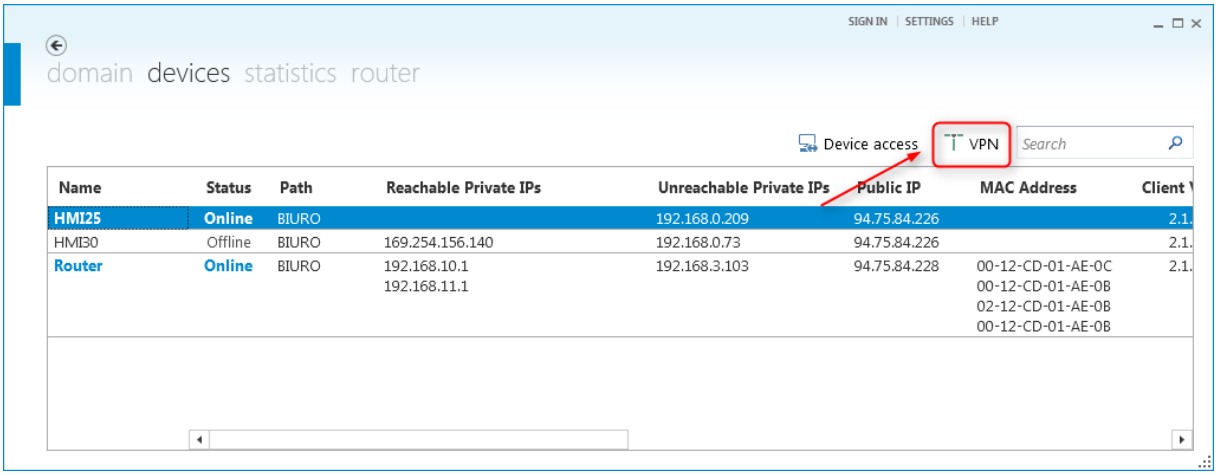
Panele ASEM HMI wyposażone są w różne porty komunikacyjne. System ASEM Ubiquity umożliwia zdalne połączenie z urządzeniami pracującymi w podsieciach szeregowych lub realizowanych poprzez port Ethernet. Poniżej przedstawiono widok obudowy panela ASEM HMI 30 wraz z oznaczonymi portami. Panel wyposażony jest w dwa gniazda Ethernet – jedno gniazdo (LAN 1) służy do połączenia urządzenia z Internetem. Gniazdo LAN2 może być użyte

jako port dostępowy dla systemu Ubiquity do urządzeń pracujących w zdalnej podsieci ethernetowej. Panel wyposażony jest także w port RS-232/422/485/MPI, który może stanowić kanał dostępu do urządzeń pracujących w zdalnych podsieciach szeregowych.



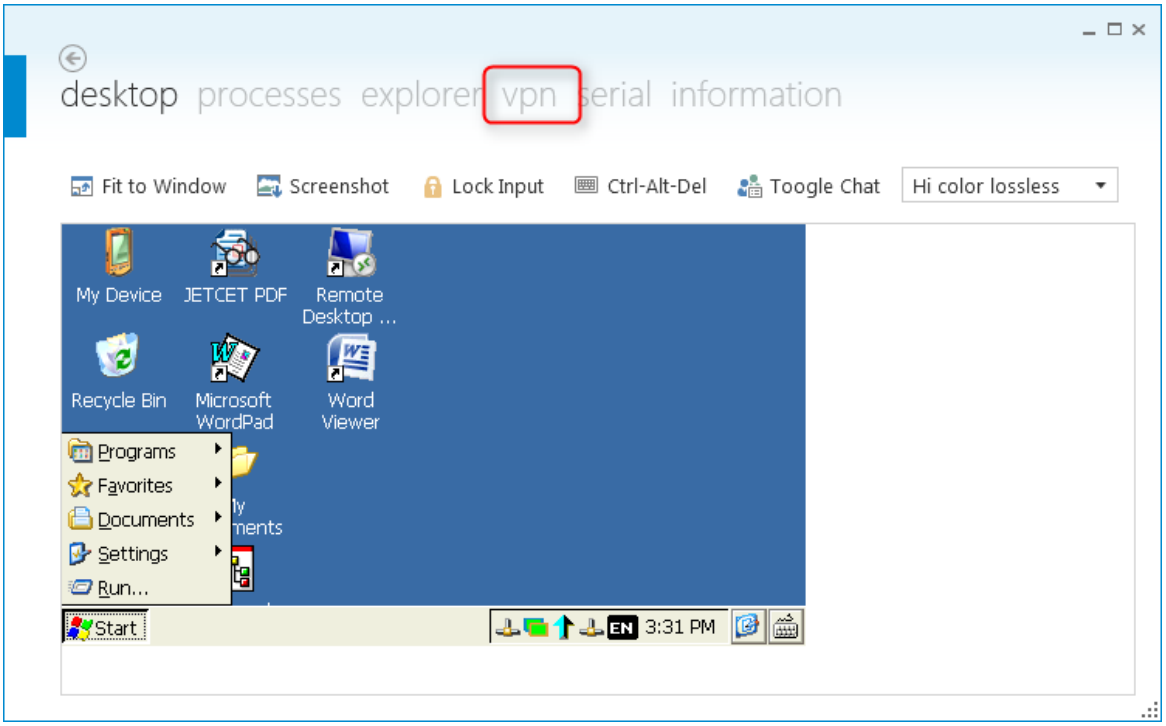
5.1. Praca z urządzeniami w zdalnej podsieci ethernetowej

W karcie *Devices* wybieramy urządzenie przypisane do domeny Ubiquity, z którym chcemy nawiązać połączenie, a następnie klikamy na przycisk VPN:

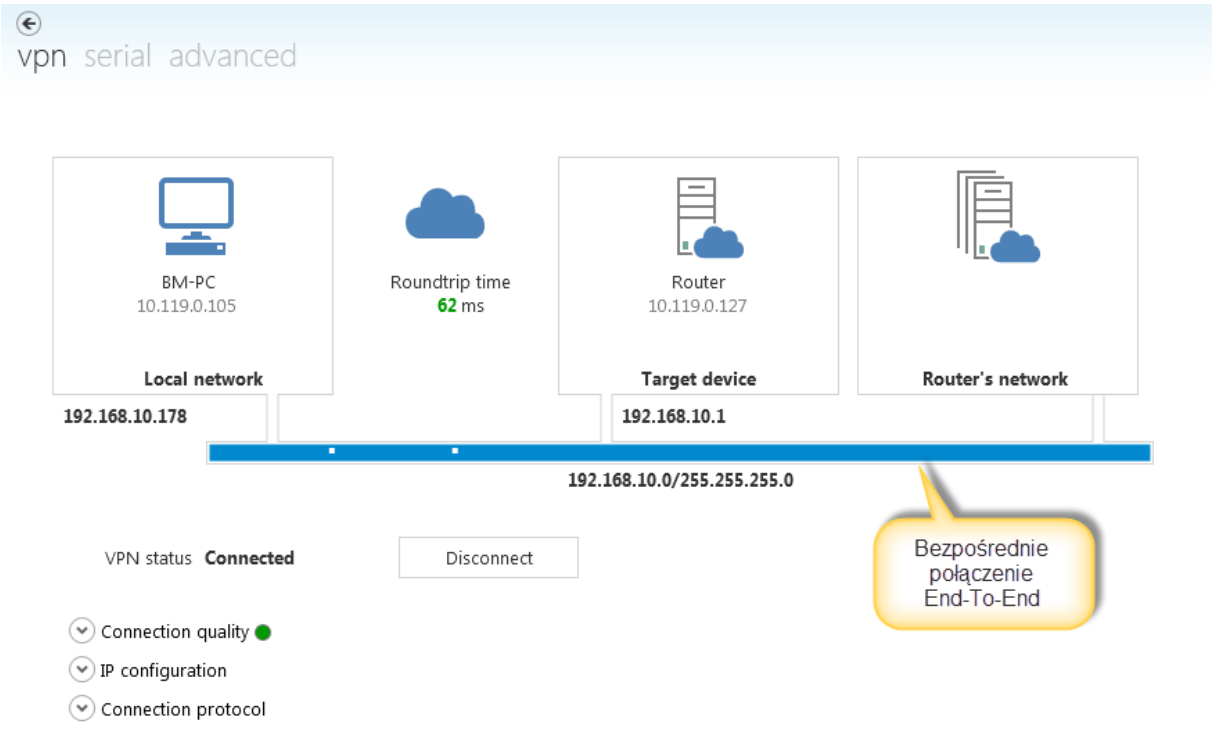


Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Połączenie poprzez VPN możemy także uzyskać z poziomu okna sterowania urządzeniem klikając na zakładkę VPN:

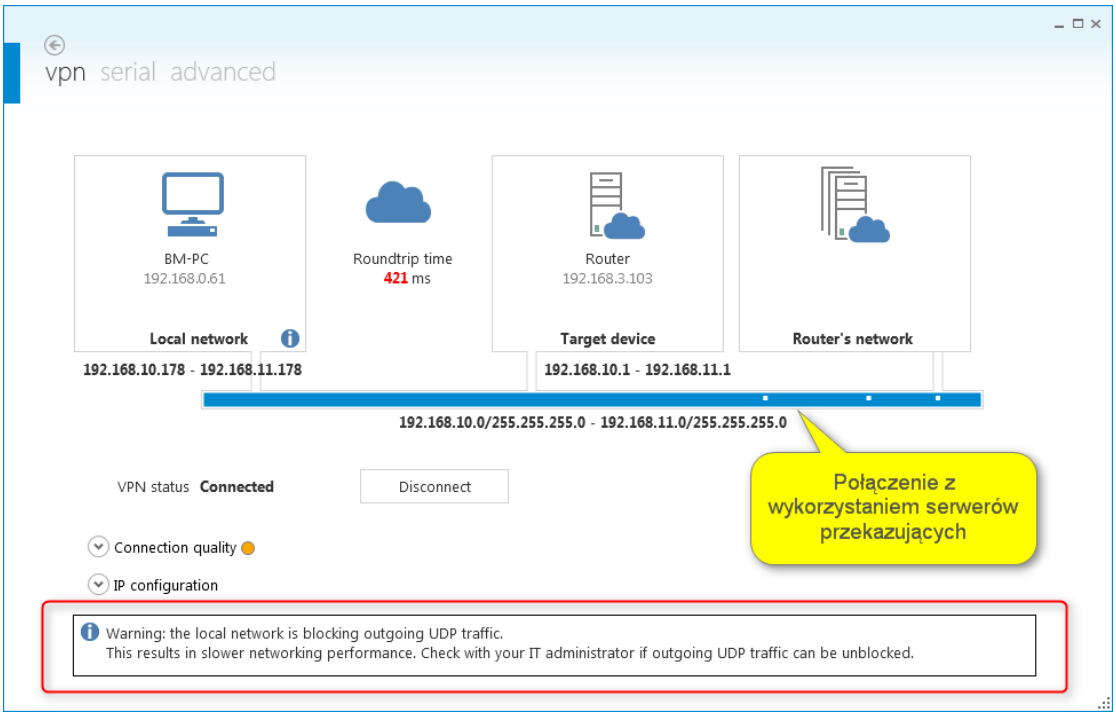


W nowym oknie widzimy szczegóły nawiązywanego połączenia. Jeżeli wszystko przebiegło pomyślnie, kanały połączenia powinny wyświetlać się w kolorze zielonym. Oznacza to utworzenie bezpośredniego połączenia typu End-To-End pomiędzy komputerem serwisowym, a urządzeniem zdalnym:

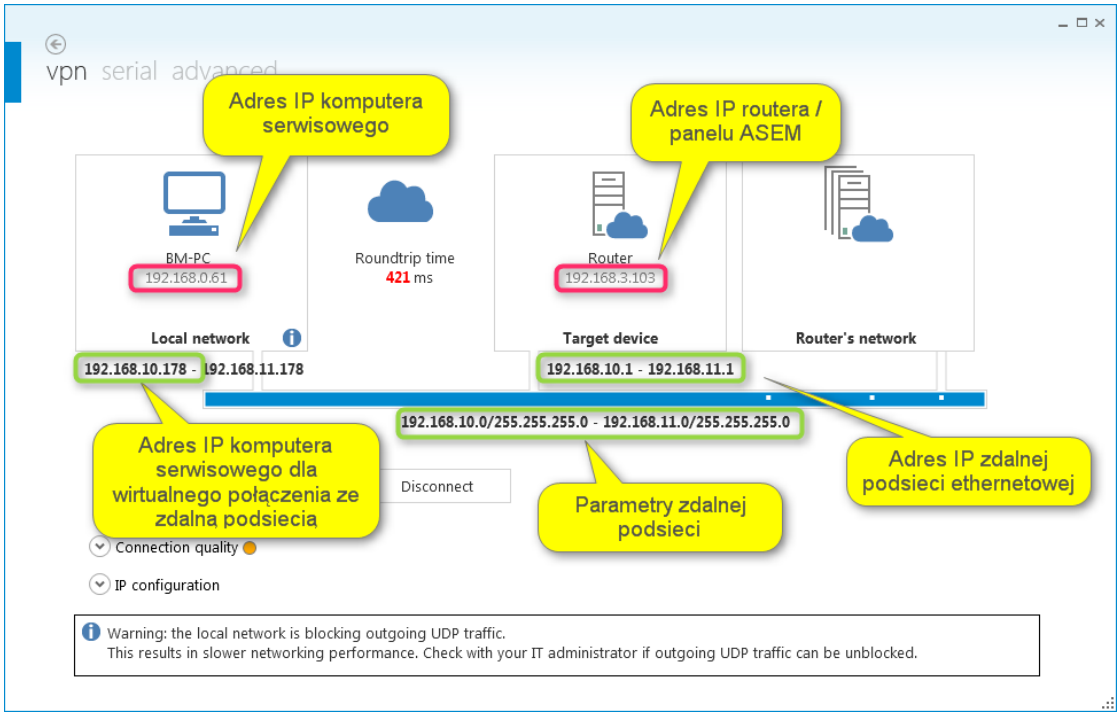


Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

W niektórych przypadkach może się zdarzyć, że zabezpieczenia sieci firmowych nie pozwalają na tworzenie połączeń typu End-To-End (rozdział 2, *Zasada działania systemu*). W takim przypadku, komunikacja z urządzeniem zdalnym odbywa się z wykorzystaniem tzw. serwerów przekazujących (*Relay Servers*). Jeżeli wystąpi taka sytuacja, kanały połączenia będą wyświetlały się w kolorze pomarańczowym:



W celu lepszego zrozumienia sposobu nawiązania połączenia, warto przeanalizować jego schemat ideowy:



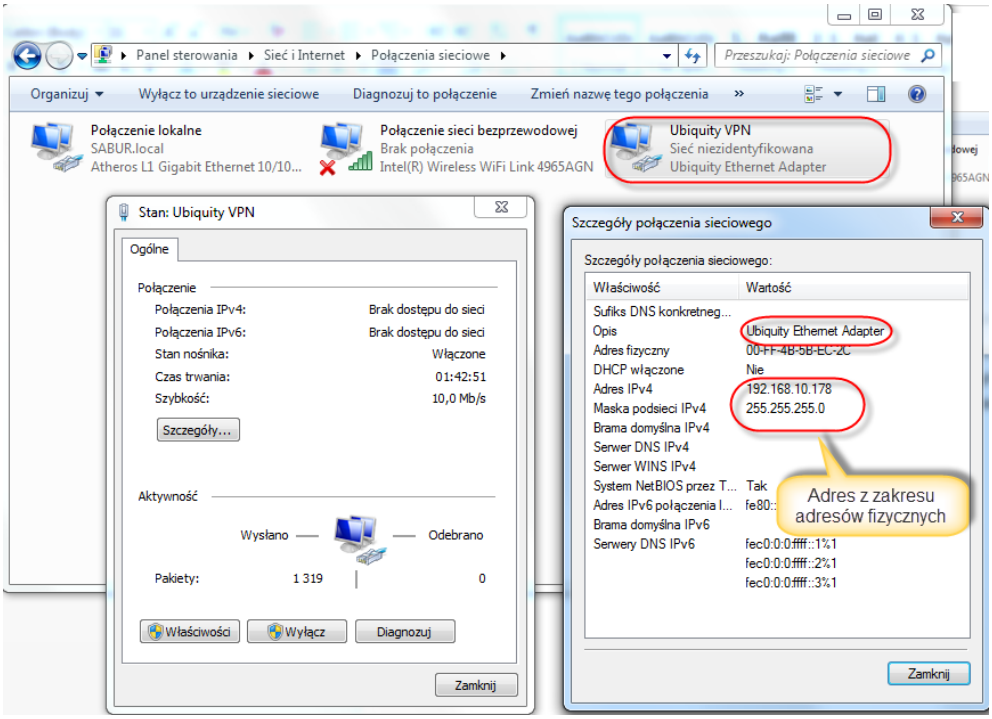
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

W polach przedstawiających urządzenia biorące udział w komunikacji, widzimy ich nazwy, a także adresy IP dla połączenia internetowego np.:

- 192.168.0.61 – adres IP komputera serwisowego;
- 192.168.3.103 – adres IP routera / panelu ASEM;

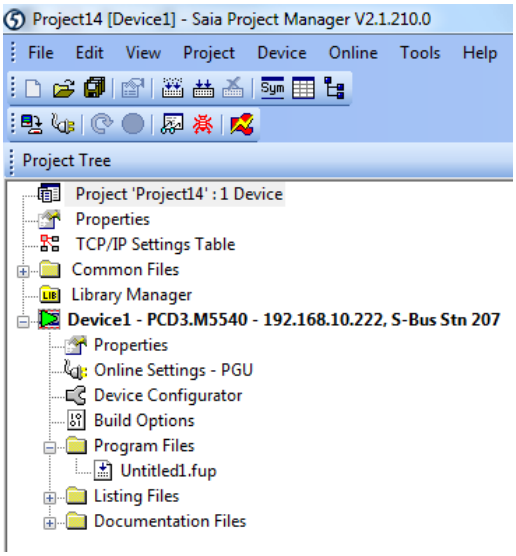
W momencie, gdy nawiązywane jest połączenie VPN, uzyskujemy informację o parametrach zdalnej podsieci (192.168.10.0 / 255.255.255.0). Widoczny jest także adres IP panelu HMI dla zdalnej podsieci (192.168.10.1).

Warto zauważyć, że po poprawnym nawiązaniu połączenia VPN ze zdalną podsiecią, komputer serwisowy (BM-PC) uzyskuje adres IP z zakresu adresów fizycznych podsieci (np. 192.168.10.178). Oznacza to, że wszystkie urządzenia pracujące w podsieci nr 10 interpretują komputer serwisowy jako element podsieci, a nie urządzenie zdalne. Dzięki temu nie musimy dokonywać żadnych modyfikacji ustawień komunikacyjnych urządzeń pracujących w zdalnej podsieci.

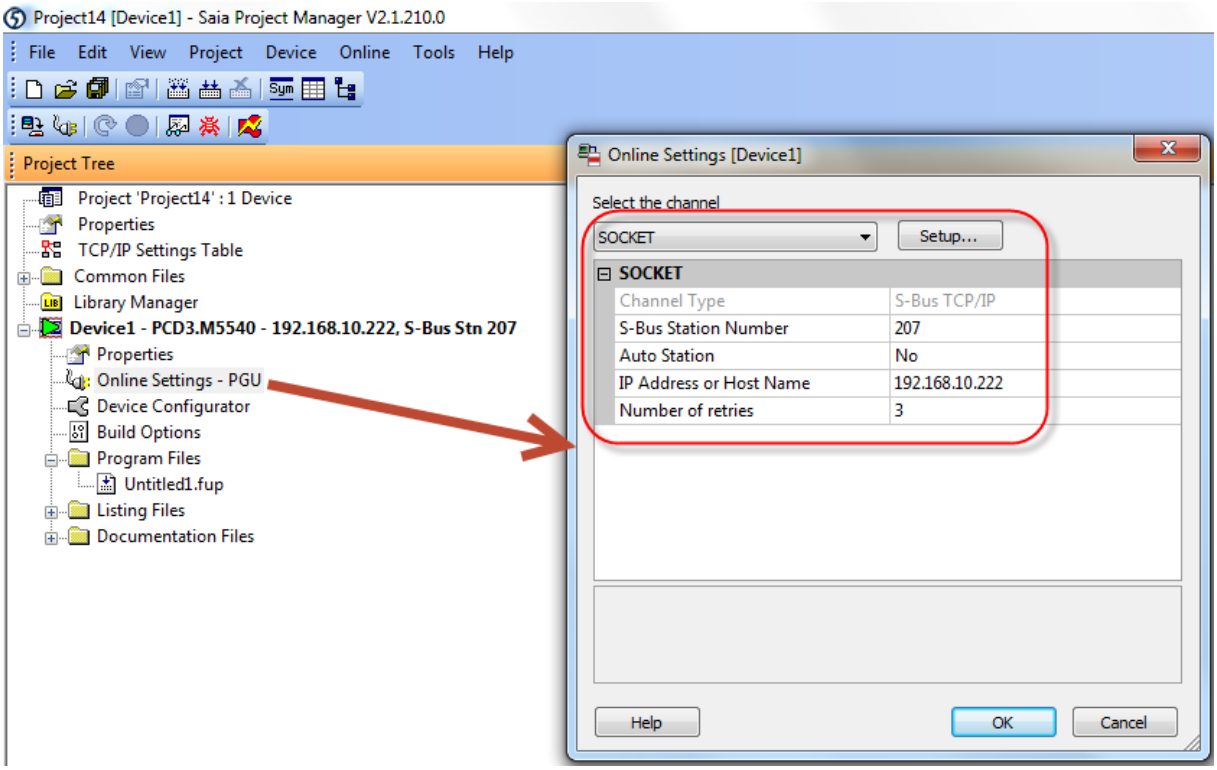


Nawiązanie połączenia ze zdalną po podsiecią umożliwia np. zdalną konfigurację urządzeń, aktualizacje oprogramowania lub dokonywanie prac serwisowych. W kolejnych krokach przedstawiono metodę zdalnego programowania sterownika PLC firmy Saia Burgess Controls.

1. Po nawiązaniu połączenia VPN uruchamiamy pakiet PG5 i tworzymy lub wybieramy istniejący projekt, który chcemy wgrać do sterownika:

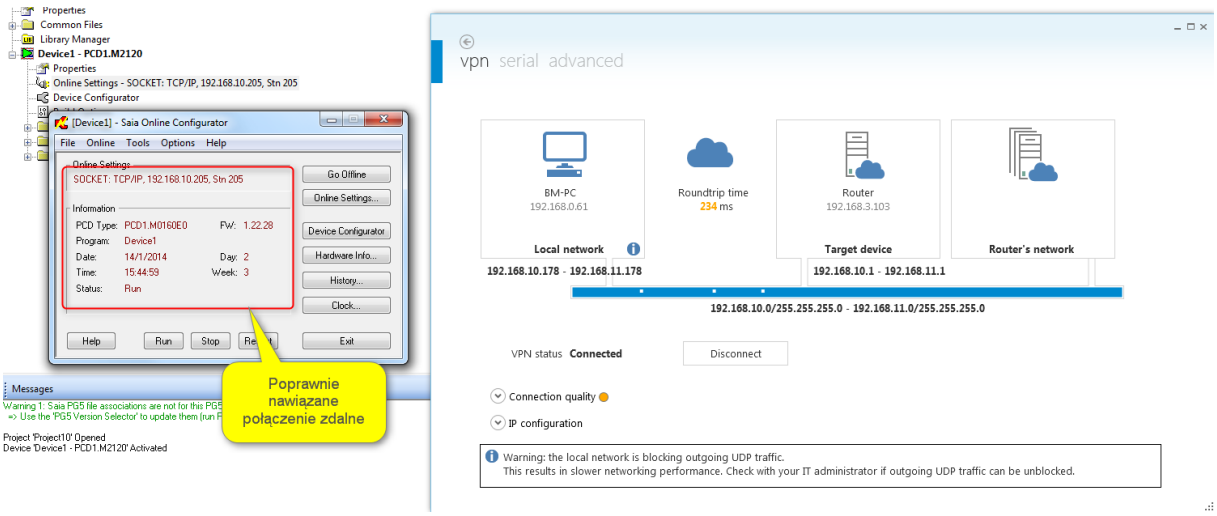


2. Otwieramy kartę Online Settings, w której definiujemy sposób komunikacji z urządzeniem. Z listy dostępnych połączeń wybieramy SOCKET, a następnie w pola: *Station Number* oraz *IP Address* wpisujemy parametry sterownika, z którym chcemy uzyskać połączenie:



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

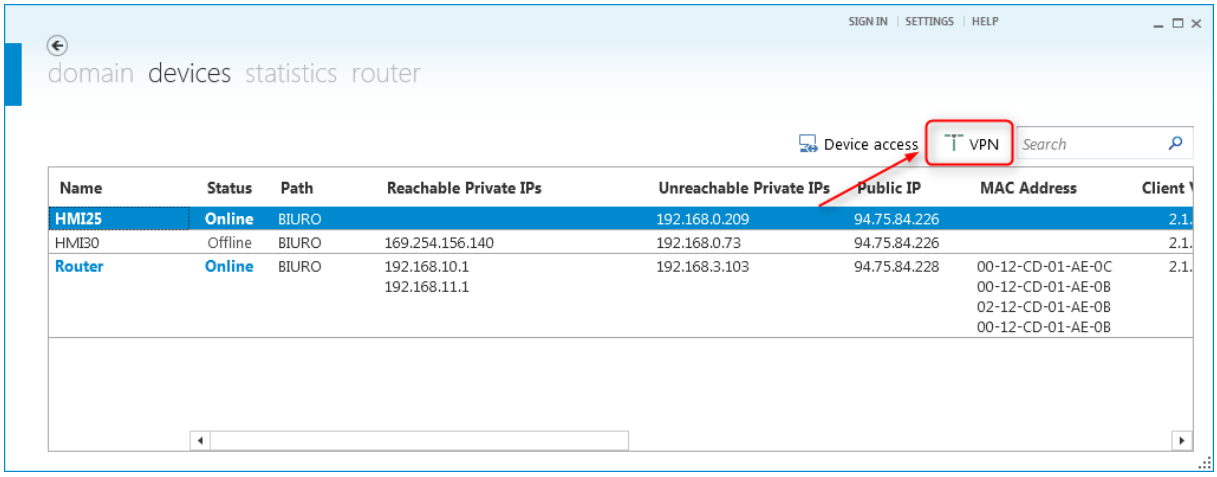
3. Zatwierdzamy zmiany, klikając przycisk OK. W celu sprawdzenia komunikacji klikamy na ikonę *Online Configurator* znajdującą się w górnym pasku ikon. Jeżeli połączenie zostało nawiązane w sposób poprawny, w nowym oknie pojawią się jego szczegóły:



4. Nawiązane połączenie umożliwia m.in.: wgranie programu do sterownika, a także monitorowanie jego pracy, wgrywanie konfiguracji itp.

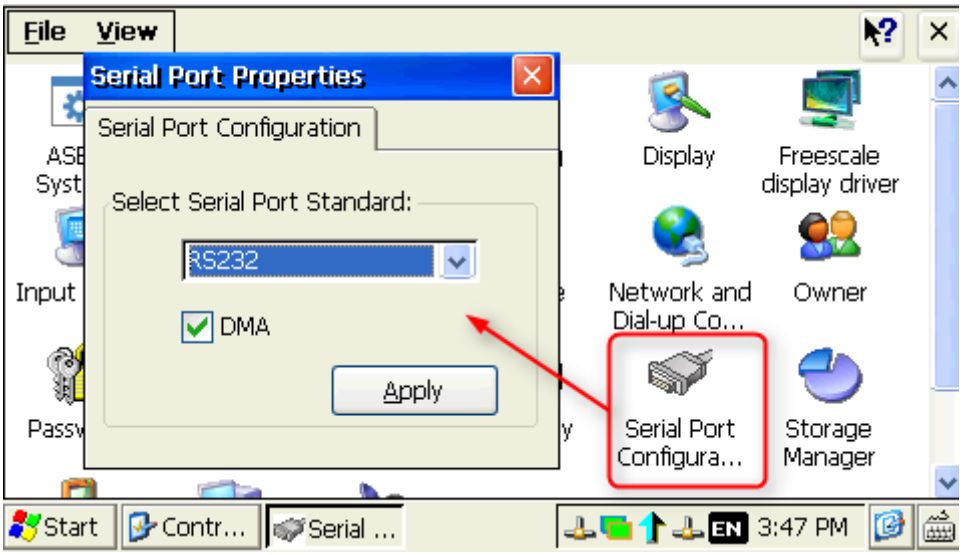
5.2. Praca z urządzeniami w zdalnej podsieci szeregowej

1. W karcie *Devices* wybieramy urządzenie przypisane do domeny Ubiquity, z którym chcemy nawiązać połączenie, a następnie klikamy na przycisk *VPN*:



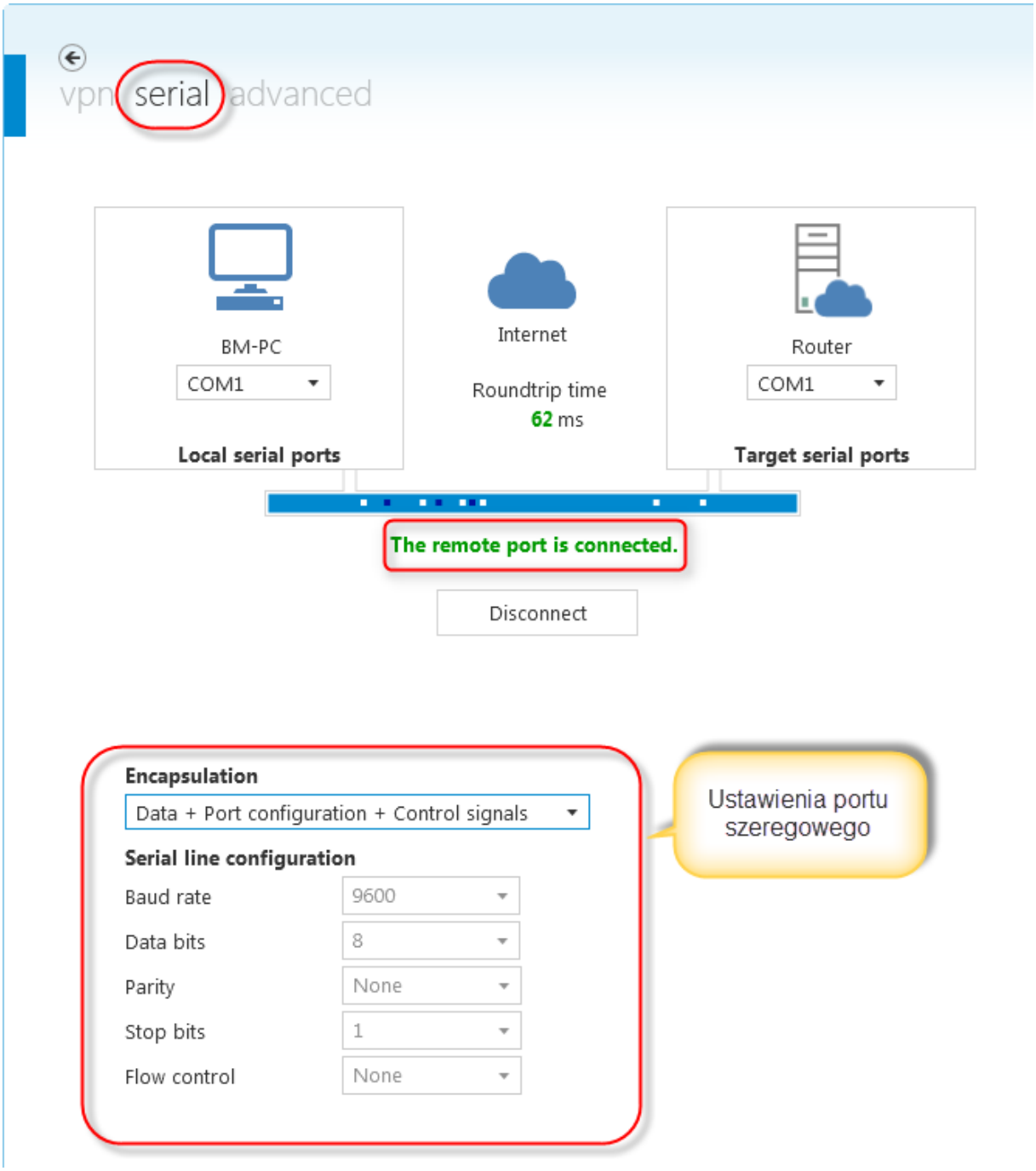
2. Przed nawiązaniem połączenia z podsiecią szeregową musimy określić, jaki standard komunikacji występuje pomiędzy zdalnym panelem a urządzeniem w podsieci. Wejście szeregowe panelu obsługuje połączenia poprzez RS-232/422/485 lub MPI.

Domyślnym ustawieniem jest komunikacja poprzez RS-232. Aby zmienić ustawienia domyślne, w panelu sterowania urządzenia HMI wybieramy ikonę *Serial Port Configuration*, a następnie określamy tryb komunikacji. Zmiany ustawień w panelu możemy dokonać za pomocą funkcji zdalnego pulpitu:



3. W aplikacji *Control Center* klikamy na zakładkę *Serial.* W nowym oknie otwieramy zakładę *Advanced* i definiujemy parametry połączenia. Po kliknięciu na przycisk *Connect*, komunikacja zostaje nawiązana (należy pamiętać, że aby mieć dostęp do uruchomienia połączenia poprzez port szeregowy, musimy mieć wcześniej nawiązane połączenie poprzez VPN):

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

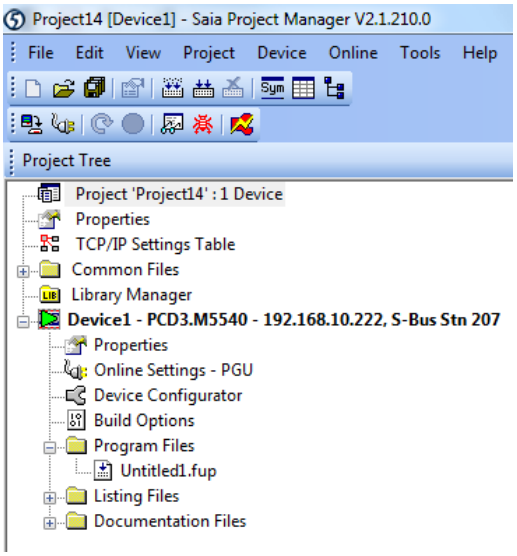


Nawiązanie połączenia ze zdalną podsiecią szeregową umożliwia np. zdalną konfigurację urządzeń, aktualizację oprogramowania lub dokonywanie prac serwisowych. Z listy rozwijalnej *Encapsulation* możemy wybrać jedną z dwóch opcji:

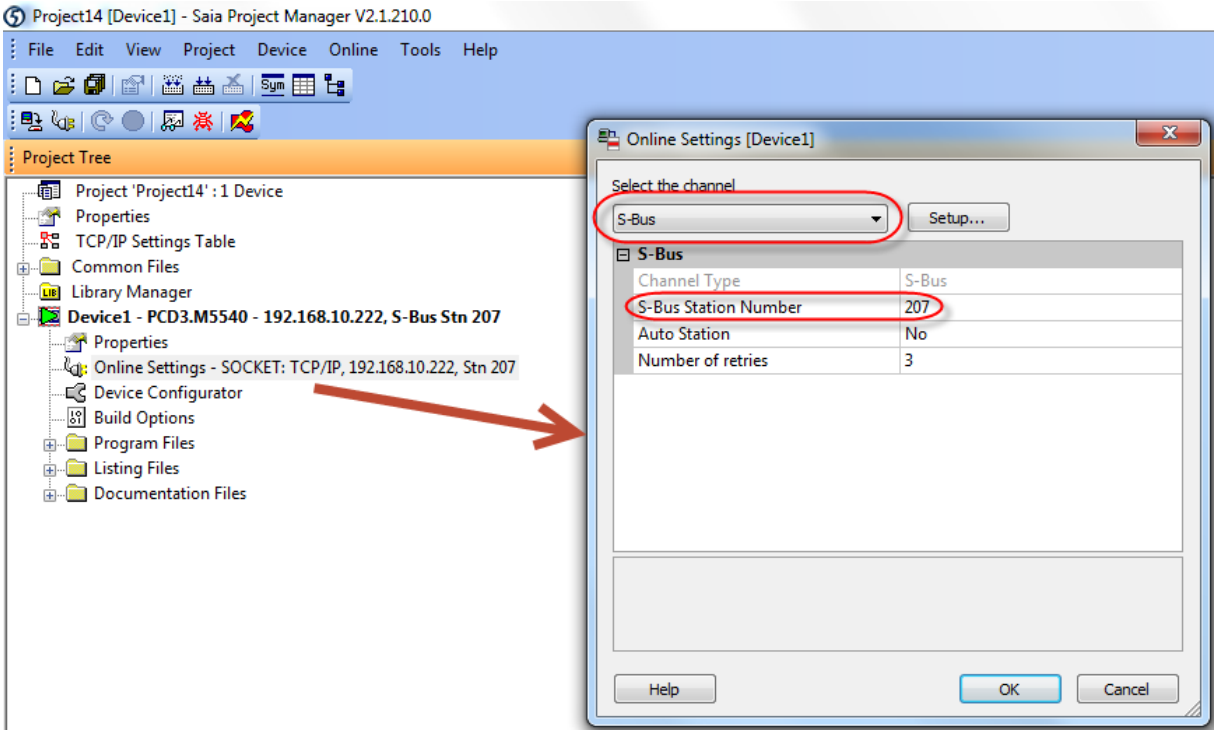
- **Data + Port Configuration + Control Signals** – automatyczne ustawienie parametrów komunikacji (np. prędkości transmisji, ilości bitów w ramce);
- **Data Only** – ręczne ustawienie parametrów komunikacji.

W kolejnych krokach przedstawiono metodę zdalnego programowania sterownika PLC firmy Saia Burgess Controls:

1. Po nawiązaniu połączenia poprzez port szeregowy, uruchamiamy pakiet PG5 i tworzymy lub wybieramy istniejący projekt, który chcemy wgrać do sterownika:

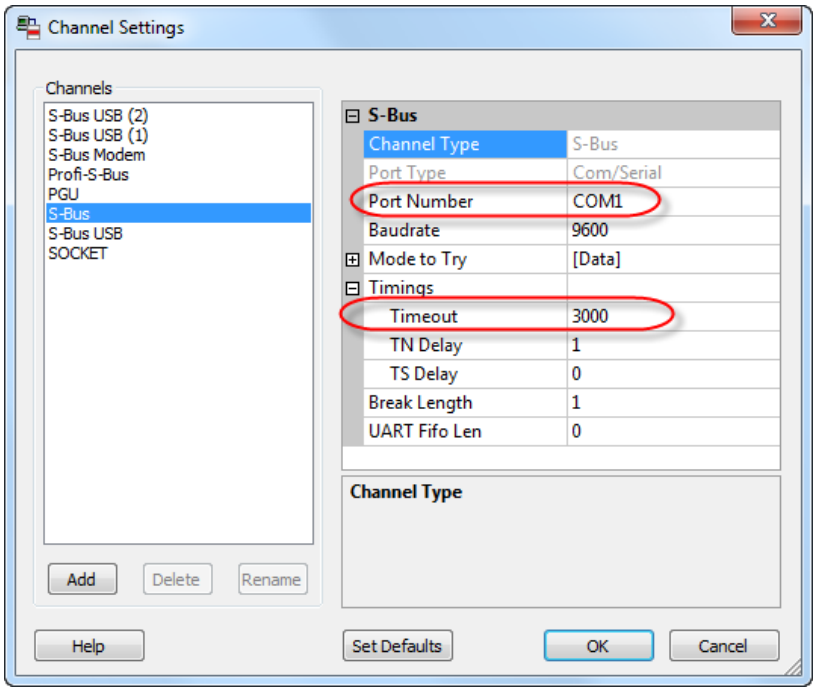


2. Otwieramy kartę Online Settings, w której definiujemy sposób komunikacji z urządzeniem. Z listy dostępnych połączeń wybieramy S-Bus i definiujemy numer stacji S-Bus sterownika, z którym chcemy uzyskać połączenie:

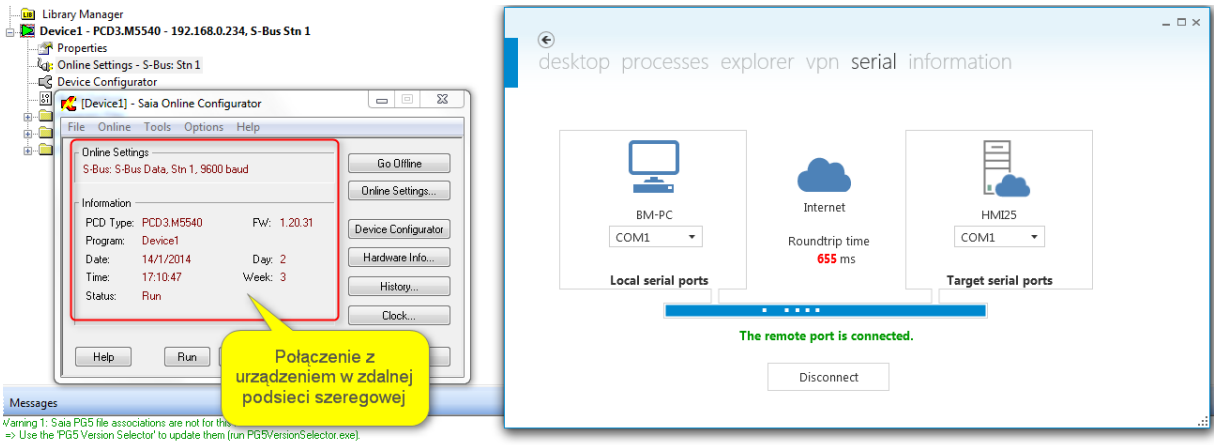


Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

3. Klikamy przycisk *Setup*. W nowym oknie określamy numer portu, poprzez który realizowane będzie połączenie. W tym przypadku warto sprawdzić numer portu, poprzez który realizowane jest wirtualne połączenie (punkt 3) – dla realizowanego zadania będzie to port COM1. Warto także zwiększyć domyślne ustawienie czasu oczekiwania na połączenie (parametr *Timeout*), np. z 250ms do 3000ms:



4. Zatwierdzamy zmiany klikając OK. W celu sprawdzenia komunikacji klikamy na ikonę *Online Configurator* znajdującą się w górnym pasku ikon. Jeżeli połączenie zostało nawiązane w sposób poprawny, w nowym oknie pojawią się jego szczegóły:



5. Nawiązane połączenie umożliwia m.in.: wgranie programu do sterownika, a także monitorowanie jego pracy, wgrywanie konfiguracji, itp.

6. Router Ubiquity

Router Ubiquity umożliwia nawiązywanie połączenia pomiędzy komputerem zdalnym (serwisowym) a urządzeniami wchodzącymi w skład systemu automatyki.

Router Ubiquity przeznaczony jest dla następujących systemów automatyki:

- z urządzeniami niewyposażonymi w port Ethernet;
- bez panelu operatorskiego;
- takich, w których chcemy uniknąć bezpośredniego połączenia panelu operatorskiego z Internetem;
- tych, w których nie chcemy instalować oprogramowania Ubiquity Runtime w panelu operatorskim;

Wyróżnia się następujące typy urządzeń:

Routery Ubiquity – rodzina RK

RK-10

RK-11

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

Routery Ubiquity serii RK wyposażone są w procesor ARM Cortex A8 1GHz. Urządzenia zasilane są napięciem stałym 9-24VDC. Możliwy jest montaż routera na szynie DIN. Routery RK11 posiadają wbudowany modem 2G/3G/3G+ EDGE/HSPA. Poniżej przedstawiono wybrane dane techniczne urządzeń:

	RK-10	**RK-11 ET**
System zdalnego dostępu	Preinstalowany ASEM UBIQUITY Router Runtime	
System operacyjny	Microsoft Windows Embedded Compact Pro 7	
Procesor	ARM Cortex A8 1GHz	
Pamięć RAM	512 MB	
Pamięć masowa	256MB (dla systemu operacyjnego i aplikacji Runtime)	
	2GB dla systemu plików, projektów i aplikacji	4GB dla systemu plików, projektów i aplikacji
Interfejsy	• 2 x Ethernet 10/100 (1xLAN – 1xWAN); • 1 x RS-232/422/485; • 1 x USB 2.0 Host; • 2 wejścia cyfrowe 24V; • 2 wyjścia cyfrowe 24VDC – 200mA;	
Obsługa sieci komórkowych	brak	• Zintegrowany modem 2G/3G/3G+ EDGE/HSPA; • 1 gniazdo antenowe SMA; • 1 slot na kartę SIM;
Zasilanie	24VDC (9-36VDC)	
Certyfikaty	CE, cULus	

Routery Ubiquity – rodzina RM

RM-10 **RM-11**

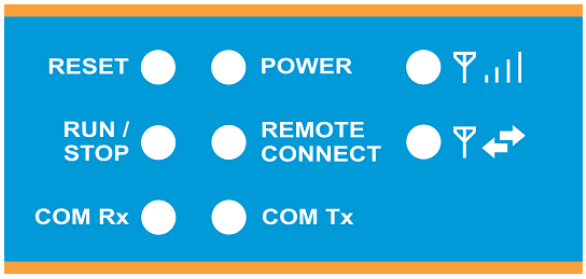
Routery serii RM stanowią w pełni zintegrowane rozwiązanie łączące w sobie zalety i funkcjonalności obecne w środowiskach: Premium HMI oraz Ubiquity. Routery serii RM, oprócz podstawowych funkcjonalności zapewnionych przez urządzenia serii RK, oferują dodatkową możliwość logowania danych historycznych. Dane są przechowywane w lokalnej pamięci routera i mogą być w prosty sposób pobrane na dysk twardy komputera z wykorzystaniem aplikacji Control Center. Dodatkowo istnieje możliwość ustawiania powiadomień alarmowych za pośrednictwem e-maili lub SMS-ów, a także ekranów graficznych, do których dostęp można uzyskać z poziomu: aplikacji Control Center, aplikacji mobilnej Premium HMI Mobile lub przeglądarki internetowej.

	RM-10	RM-11 ET
System zdalnego dostępu	Preinstalowany ASEM UBIQUITY Router Runtime	
System operacyjny	Microsoft Windows Embedded Compact Pro 7	
Procesor	ARM Cortex A8 1GHz	
Pamięć RAM	512 MB	
Pamięć masowa	256MB (dla systemu operacyjnego i aplikacji Runtime)	
	4GB dla systemu plików, projektów i aplikacji	

Interfejsy	• 2 x Ethernet 10/100 (1xLAN – 1xWAN); • 1 x RS-232/422/485; • 1 x USB 2.0 Host; • 2 wejścia cyfrowe 24V; • 2 wyjścia cyfrowe 24VDC – 200mA;	
Zdalny monitoring	Premium HMI RM Runtime: • Logowanie danych historycznych; • Obsługa ekranów graficznych; • Alarmowanie e-mail / SMS; • Dostęp z poziomu: aplikacji Control Center, aplikacji mobilnej Premium HMI Mobile oraz przeglądarki internetowej; • Obsługa skryptów VBA;	
Obsługa sieci komórkowych	brak	• Zintegrowany modem 2G/3G/3G+ EDGE/HSPA; • 1 gniazdo antenowe SMA; • 1 slot na kartę SIM;
Zasilanie	24VDC (9-36VDC)	
Certyfikaty	CE, cULus	

Diody LED:

Router Ubiquity wyposażony jest w 6 diod LED, których stan świadczy o trybie pracy urządzenia:



dioda RESET – kolor żółty;

dioda POWER – kolor zieloony;

dioda RUN/STOP – kolor zielony / czerwony;

dioda REMOTE CONNECTION – kolor zielony;

diody: COM Rx, COM Tx – kolor zielony;

Diody występujące tylko w Routerach wyposażonych w modem 2G/3G/3G+ EDGE / HSPA (seria RK/RM 11).

Wyróżnia się następujące tryby pracy diod:

- ciągłe swiecenie;
- mruganie;
- praca sekwencyjna;
- pojedyncza sekwencja;

Dioda LED	Status	Opis
RESET	Ciągłe świecenie	Dioda świeci, gdy wciśnięto przycisk RESET lub gdy wykryto błąd związany z hardwarem
POWER	Ciągłe świecenie	Dioda świeci się, gdy Router jest poprawnie podłączony do zasilania.

RUN / STOP	Ciągłe światło zielone	Nawiązano połączenie z serwerem Ubiquity
	Ciągłe światło czerwone	Brak połączenia z serwerem
	Migające światło zielone	Nawiązywanie połączenia z serwerem
	Migające światło czerwone	Połączenie z serwerem nie zostało nawiązane ze względu na nieprzypisanie Routera do żadnej domeny
	Dwa mignięcia diody czerwonej (praca sekwencyjna)	Próba nawiązania połączenia z inną domeną niż to zostało wprowadzone w początkowej rejestracji urządzenia
	2 mignięcia diody zielonej (pojedyncza sekwencja)	Konfiguracja Routera poprzez USB zakończona pomyślnie
	2 mignięcia diody czerwonej (pojedyncza sekwencja)	Podano nieprawidłowe dane użytkownika dot. dostępu do domeny
	3 mignięcia diody zielonej (pojedyncza sekwencja)	Uaktualnienie konfiguracji Routera poprzez USB zakończone pomyślnie
	3 mignięcia diody czerwonej (pojedyncza sekwencja)	Konfiguracja Routera poprzez USB zakończona błędem
	4 mignięcia diody czerwonej (pojedyncza sekwencja)	Rozpoczęcie procesu przywracania ustawień domyślnych
	5 mignięć diody czerwonej (pojedyncza sekwencja)	Błąd aplikacji Ubiquity Runtime, nastąpi restart systemu
	6 mignięć diody czerwonej (pojedyncza sekwencja)	Błąd formatu danych na nośniku USB lub nieznany błąd
REMOTE CONNECTION	Ciągłe świecenie	Dioda świeci, gdy nastąpiło połączenie z min. 1 klientem Control Center
COM Rx COM Tx	Obecność sygnału	Sygnalizacja połączenia – port szeregowy
	Ciągłe światło czerwone	Modem nie wykrył sygnału
	Migające światło zielone	Wykryto słaby sygnał
	Ciągłe światło zielone	Wykryto mocny sygnał
	Migające światło czerwone	Błąd karty SIM (np. zły PIN)
	Wyłączone	Modem nie wykrył karty SIM
	Migające światło zielone	Modem podłączony

6.1. Konfiguracja połączenia z Routerem Ubiquity

Konfiguracja połączenia z routerem Ubiquity została zaprojektowana w taki sposób, by do minimum ograniczyć ingerencję użytkownika i uprościć ustawienie podstawowych parametrów. Nie wymagane jest konfigurowanie ustawień związanych z połączeniem VPN, Ethernet.

Konfiguracja Routera ogranicza się do ustawienia adresów IP sieci, parametrów portu szeregowego oraz przypisania urządzenia do domenty Ubiquity.

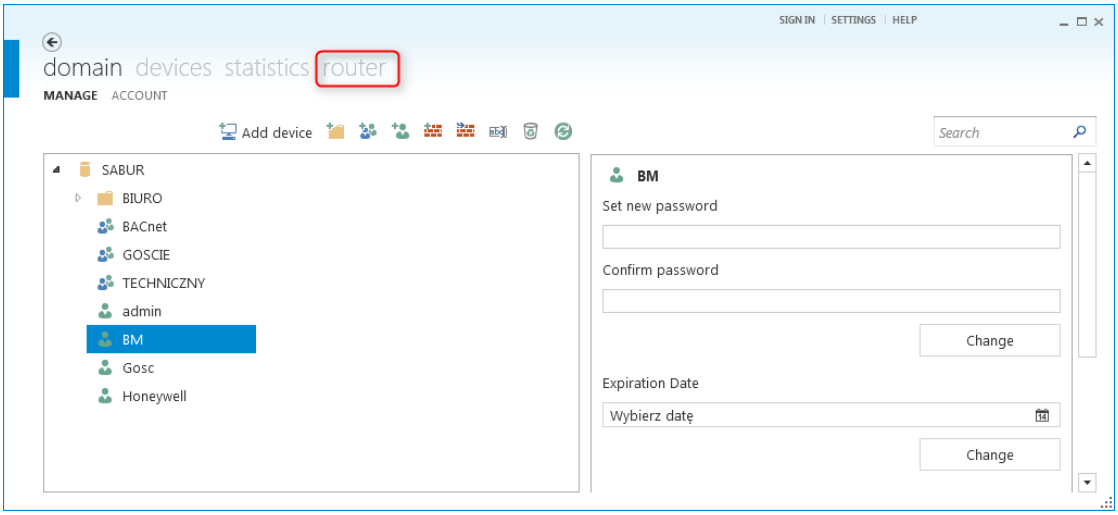
Konfiguracja Routera może odbywać się na 2 sposoby:

- Poprzez połączenie sieciowe;
- Poprzez nośnik USB, na którym znajduje się plik konfiguracyjny.

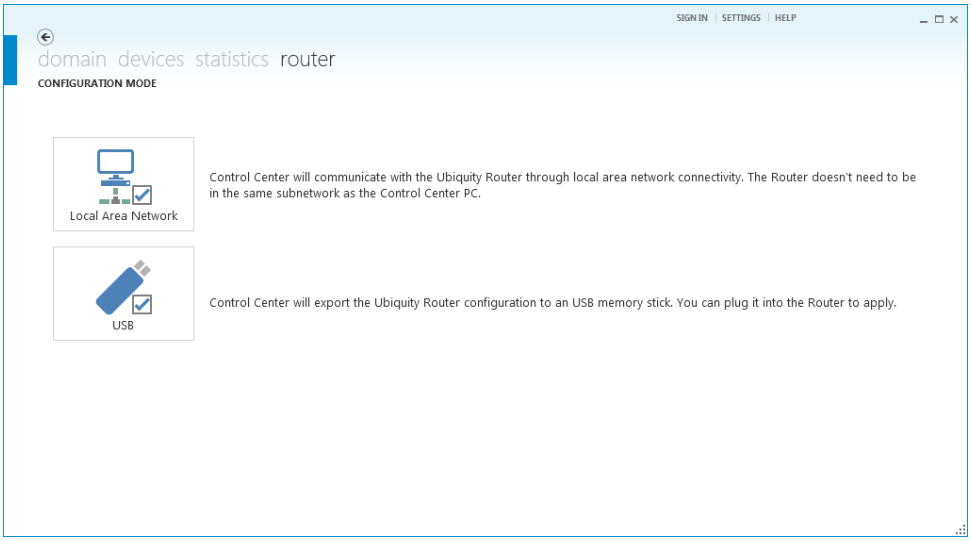
W obydwu przypadkach do konfiguracji używana jest aplikacja Control Center.

UWAGA: Warto zwrócić uwagę na to, że konfiguracja routera Ubiquity może być wykonana nawet w przypadku, gdy aplikacja Control Center nie jest połączona z Domeną. Nie będzie jednak możliwości przypisania Routera do domeny Ubiquity.

Dostęp do konfiguracji Routera Ubiquity uzyskujemy poprzez kliknięcie ikony *Router* w górnym menu aplikacji Control Center:



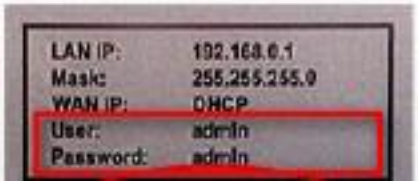
Otwiera się okno, w którym możemy wybrać tryb konfiguracji routera (poprzez USB lub poprzez połączenie sieciowe):



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

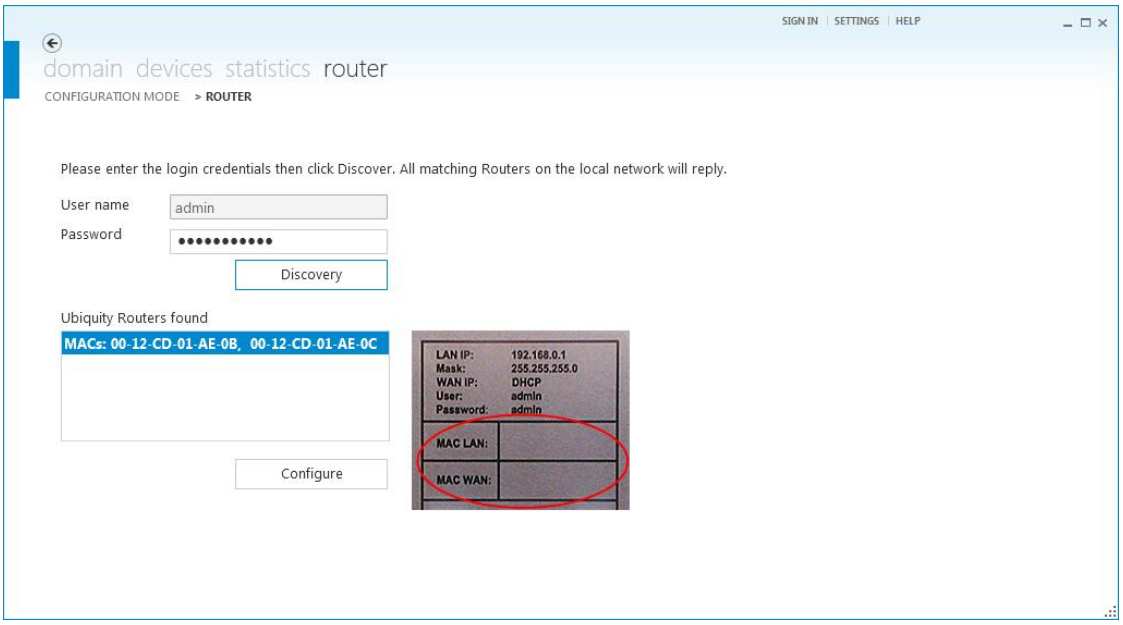
6.1.1. Konfiguracja poprzez połączenie sieciowe

1. Podłączamy router do zasilania i dołączamy go do sieci;
2. Uruchamiamy aplikację Control Center i klikamy na ikonę *Ubiquity Router* (rysunek powyżej);
3. W oknie wyboru konfiguracji wybieramy *Local Area Network;*
4. Otwiera się okno wyszukiwania urządzenia w sieci. Każdy Router Ubiquity posiada zabezpieczenie, które uniemożliwia dostęp do konfiguracji osobom niepowołanym. Kontrola dostępu odbywa się poprzez podanie nazwy użytkownika i hasła. Domyślne ustawienia podane są na obudowie Routera:



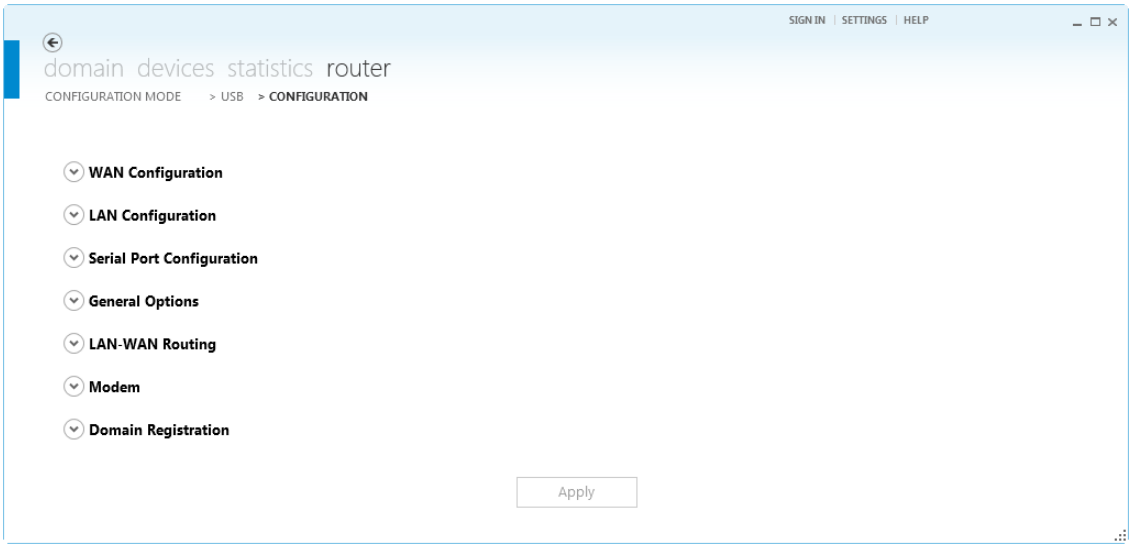
Domyślna nazwa użytkownika (niekonfigurowalna) dla dostępu do konfiguracji routera: **admin**. Domyślne hasło (konfigurowalne): **admin**.

5. Po wpisaniu nazwy i hasła użytkownika klikamy na przycisk *Discovery*. Ubiquity Control Center wyszukuje dostępne urządzenia w sieci i wyświetla je w polu *Ubiquity Routers Found*. Wyszukane routery reprezentowane są poprzez adresy: MAC LAN i MAC WAN, które znaleźć można na obudowie Routera:



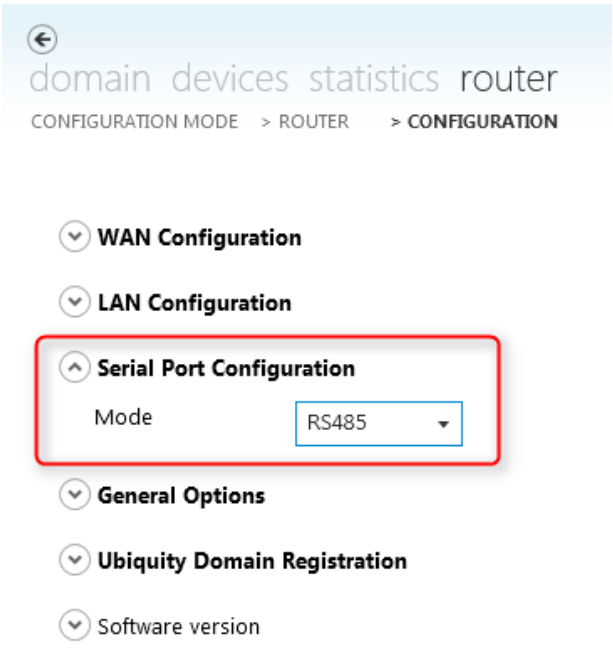
6. Wybieramy Router z listy i klikamy na przycisk *Open Configuration*. Pojawia się okno:

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl
SABUR Systemy automatyki

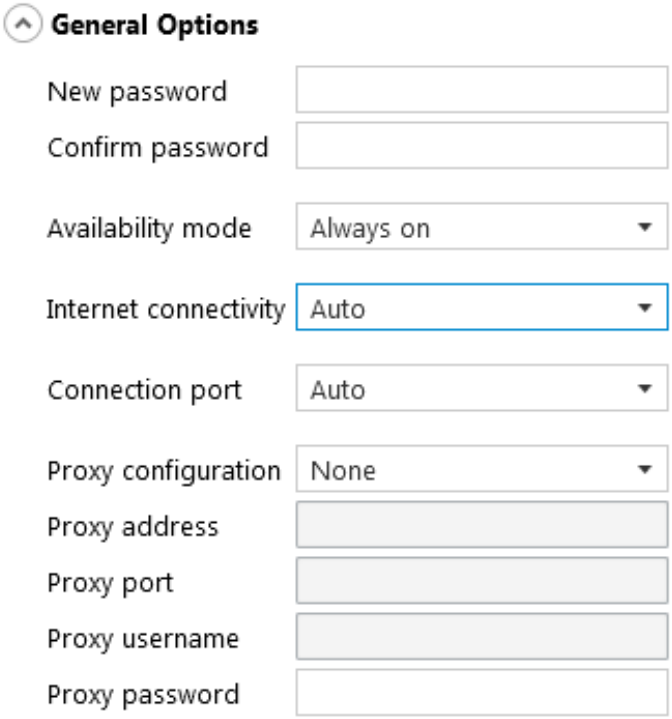


Otwierając kolejne zakładki, ustawiamy parametry konfiguracyjne routera:

- Zakładki **WAN/LAN Configuration** umożliwiają ustawienie parametrów połączeń sieciowych (adresy IP, maski podsieci, bramy domyślne);
- W zakładce **Serial Port Configuration** ustawiamy konfigurację portu szeregowego:



- W zakładce **General Options** możemy zmienić hasło dostępu do konfiguracji Routera, a także ustawić konfigurację Proxy (jeżeli jest taka potrzeba):



Z listy trybu połączenia (*Availability Mode*) możemy wybrać jedną z opcji:

- **Always-on** – połączenie Routera z domeną zostaje nawiązane natychmiast po włączeniu routera;

- **Digital input** – połączenie Routera z domeną zostaje nawiązane tylko w przypadku, gdy aktywne jest wejście cyfrowe IN0;

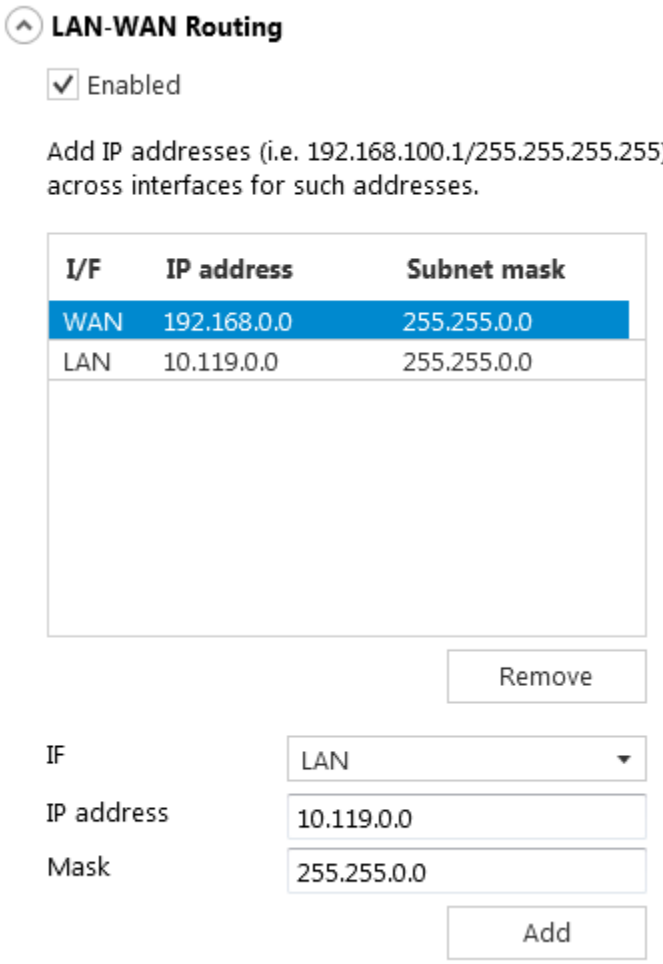
- **SMS** – nawiązanie połączenia w przypadku otrzymania przez urządzenie wiadomości SMS – składnia wiadomości:

<nazwa_użytkownika><hasło> CONNECT – podłączenie do domeny;

<nazwa_użytkownika><hasło> DISCONNECT – odłączenie do domeny;

UWAGA: Parametry: nazwa użytkownika oraz hasło utożsamiane są w tym przypadku z parametrami dostępu do konkretnego Routera, a nie z użytkownikiem Domeny;

- W zakładce **LAN-WAN Routing** istnieje możliwość konfiguracji opcji routingu pomiędzy portami WAN oraz LAN:



Funkcja pozwala na inicjalizację komunikacji pomiędzy urządzeniami znajdującymi się w dwóch różnych podsieciach (o różnych adresach). Może być ona zastosowana w przypadku konieczności wymiany danych pomiędzy np. sterownikami znajdującymi się w wewnętrznej podsieci LAN a systemami nadrzędnymi, które z reguły zainstalowane są na urządzeniach pracujących w sieci WAN. **UWAGA:** Funkcja routingu dostępna jest tylko dla routerów Ubiquity.

- W zakładce **Modem** istnieje możliwość definiowania parametrów konfiguracyjnych modemu (dla routerów serii Rx-11, wyposażonych w modem 2G/3G/3G+):

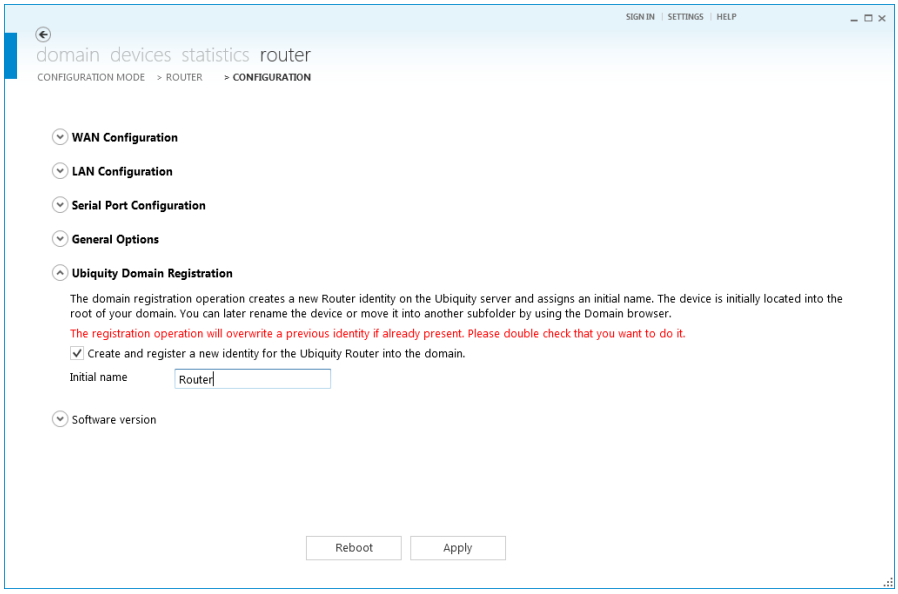
- **PIN code** – kod PIN używanej karty SIM;
- **APN (Access Point Name)** – nazwa APN zależna od operatora;
- **Username / Password** – parametry dostępu do sieci, zależne od operatora;
- **Dialed numer** – należy pozostawić wartość domyślną **99#;*

Parametry APN dla różnych operatorów przedstawiono w poniższej tabeli:

Operator	APN	Login	Hasło	Uwagi
Orange	internet	internet	internet	Konfiguracja podstawowa
	vpn.static.pl	internet	internet	Konfiguracja dla publicznego statycznego adresu IP (wymaga aktywacji u operatora).
	vpn	vpn	vpn	Konfiguracja dla publicznego dynamicznego adresu IP (wymaga aktywacji u operatora).
T-Mobile	internet	*brak*	*brak*	Konfiguracja podstawowa
	net	net	net	Ustawienia w przypadku wykupionej usługi zewnętrznego statycznego / dynamicznego adresu IP – opcja dostępna w taryfach postpaid
Plus	internet	internet	internet	Konfiguracja podstawowa
	m2m.plusgsm.pl	plusgsm	plusgsm	Konfiguracja dla zewnętrznego statycznego adresu IP (taryfy postpaid)
	pro.plusgsm.pl	plusgsm	Plusgsm	Konfiguracja dla zewnętrznego

				dynamicznego adresu IP (taryfy postpaid)
Play	internet	*brak*	*brak*	Konfiguracja podstawowa
Aero2	darmowy	*brak*	*brak*	Konfiguracja dla bezpłatnego dostępu do Internetu
Heyah	internet	internet	internet	Konfiguracja podstawowa
	heyah.pl	heyah	heyah	Konfiguracja alternatywna
Virgin Mobile	internet	*brak*	*brak*	Konfiguracja podstawowa
Nju Mobile	internet	internet	internet	Konfiguracja podstawowa

- W zakładce **Ubiquity Domain Registration** istnieje możliwość przypisania Routera do konkretnej domeny (jeżeli jesteśmy z nią połączeni) poprzez wpisanie jego nazwy, pod jaką ma się wyświetlać w liście urządzeń:



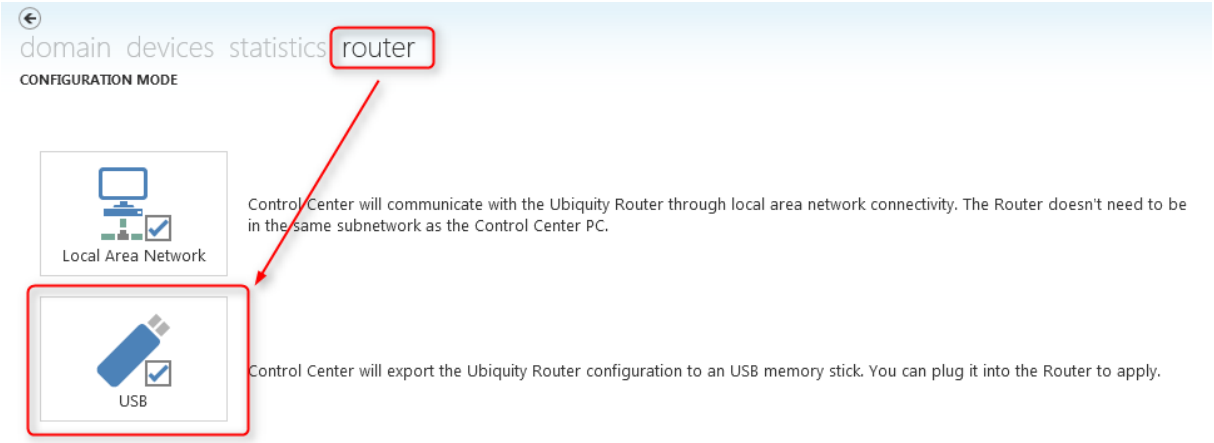
7. Klikamy przycisk *Apply*. W zależności od wprowadzonych zmian, może być wymagany restart Routera, który jest automatycznie wykonywany przez Control Center.

6.1.2. Konfiguracja z wykorzystaniem nośnika USB

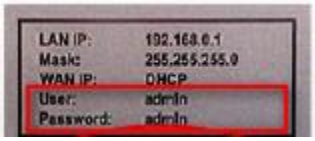
Konfigurację routera z wykorzystaniem nośnika USB wykonuje się w aplikacji Control Center, analogicznie jak dla połączenia sieciowego. Po zakończniu konfiguracji tworzony jest plik XML, który należy nagrać w folderze głównym nośnika USB, a następnie umieścić w porcie USB Routera.

Po umieszczeniu nośnika w porcie USB, Router automatycznie rozpoznaje obecność pliku konfiguracyjnego i aktualizuje ustawienia. Stan aktualizacji konfiguracji sygnalizowany jest poprzez diody LED (rozdział 6.1).

1. Po uruchomieniu aplikacji *Control Center* klikamy na ikonę *Router*, a następnie wybieramy opcję *USB*:



2. Każdy Router Ubiquity posiada zabezpieczenie, które uniemożliwia dostęp do konfiguracji osobom niepowołanym. Kontrola dostępu odbywa się poprzez podanie nazwy użytkownika i hasła. Domyślne ustawienia podane są na obudowie Routera:

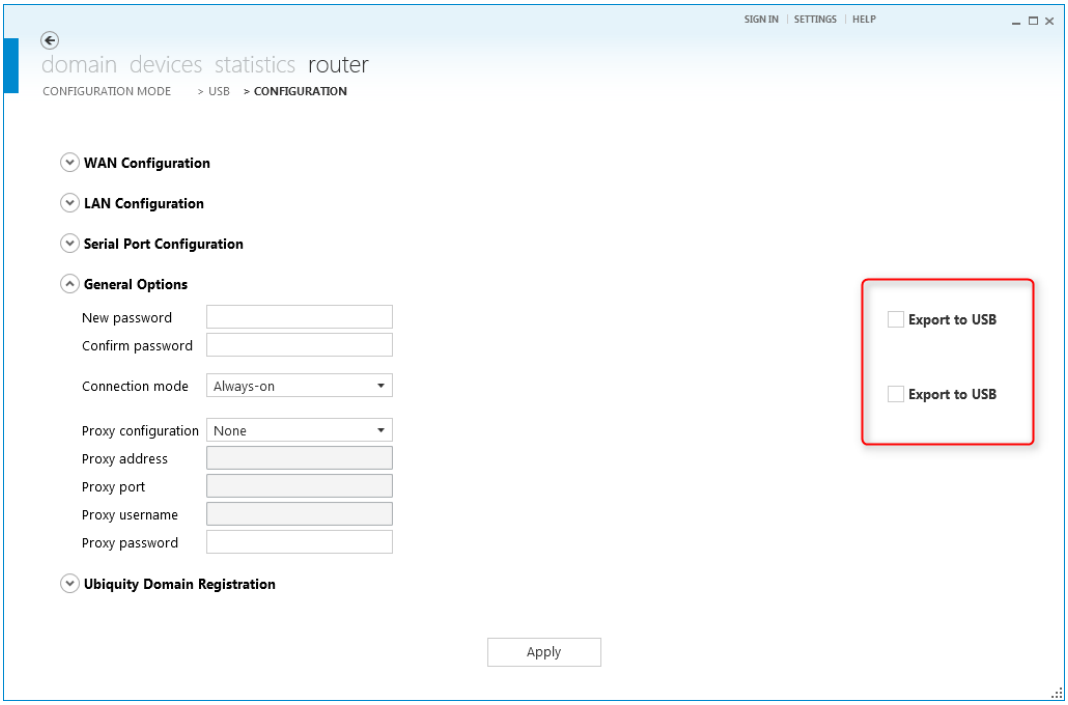


Domyślna nazwa użytkownika (niekonfigurowalna) dla dostępu do konfiguracji routera: **admin**. Domyślne hasło (konfigurowalne): **admin**.

3. Po wpisaniu nazwy i hasła użytkownika, klikamy przycisk *Next*. Pojawia się okno zmiany konfiguracji urządzenia. Zakładki konfiguracji opisane zostały w rozdziale 6.2.1.

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

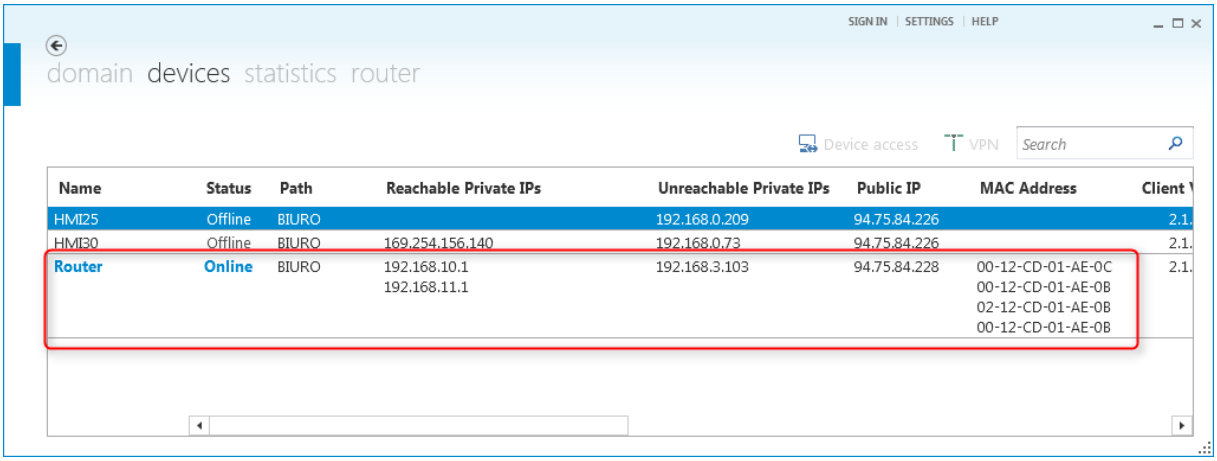
UWAGA: W przypadku konfiguracji ustawień routera poprzez USB, przy każdej z zakładek pojawia się pole wyboru *Export to USB*. Jeżeli pole jest zaznaczone, ustawienia z danej zakładki zostaną umieszczone w pliku konfiguracyjnym XML:



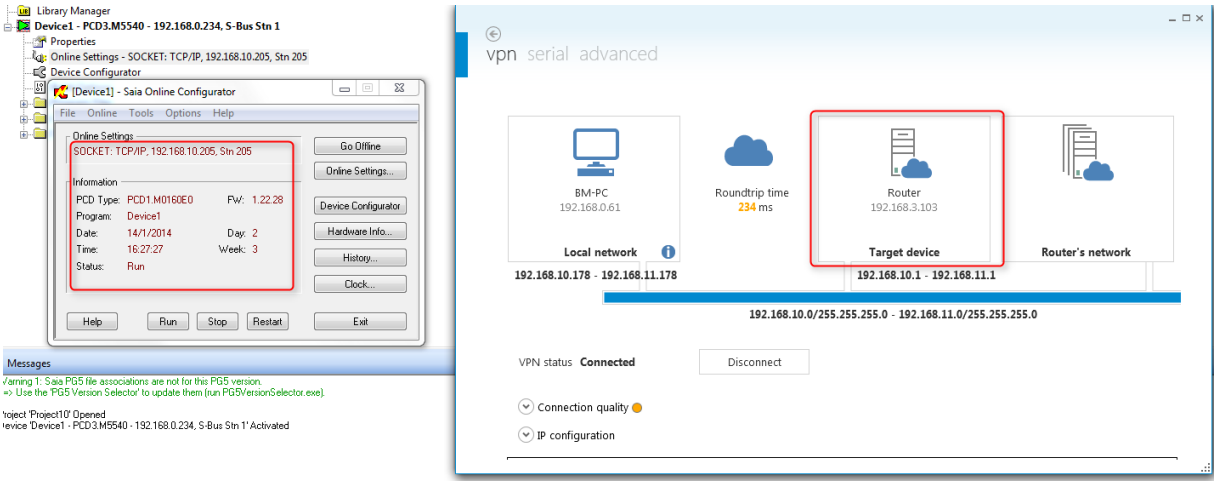
4. Po ukończeniu konfiguracji klikamy na przycisk *Apply*. Pojawia się okno, w którym możemy wybrać lokalizację zapisu pliku konfiguracyjnego. Zapisujemy plik konfiguracyjny XML w katalogu głównym nośnika USB i umieszczamy go w Routerze, który automatycznie rozpoznaje obecność pliku konfiguracyjnego i aktualizuje ustawienia. Stan aktualizacji konfiguracji sygnalizowany jest poprzez diody LED (rozdział 6.1).

6.1.3. Praca z Routerem zarejestrowanym na Domenie Ubiquity

Po przypisaniu Routera do domeny Ubiquity, pojawia się on w liście dostępnych urządzeń. Nazwa urządzenia odpowiada ciągowi znaków wpisanych w pole *Initial Name* w zakładce *Ubiquity Domain Registration* okna konfiguracji Routera:



Praca z Routerem przypisanym do Domeny Ubiquity odbywa się w sposób analogiczny jak dla panelu operatorskiego. Połączenie VPN z routerem uzyskujemy poprzez naciśnięcie przycisku VPN w oknie właściwości urządzenia. Dzięki temu możliwe jest np. zdalne programowanie sterowników PLC, zdalny serwis itp.



Opis funkcji i struktury połączeń systemu Ubiquity zamieszczono w rozdziałach: 4, 5.

6.2. Obsługa dodatkowych funkcji Routera Ubiquity (seria RM-11)

Dla routerów serii RM-11 istnieje możliwość konfiguracji i obsługi dodatkowych funkcji, dzięki czemu urządzenia łączą zalety obecne w środowiskach: Premium HMI oraz Ubiquity. Najważniejsze z nich to:

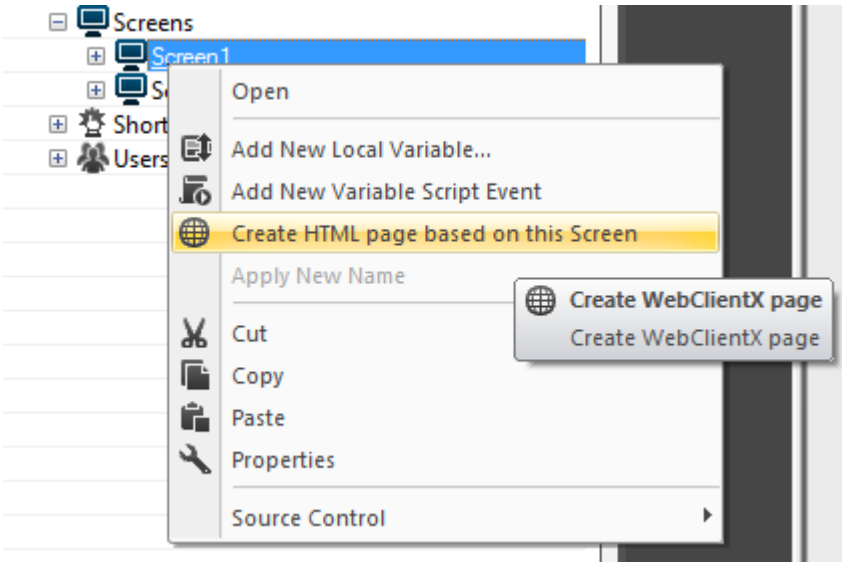
- Logowanie danych historycznych;
- Obsługa ekranów graficznych;
- Alarmowanie e-mail / SMS;

- Dostęp do wizualizacji z poziomu: aplikacji Control Center, aplikacji mobilnej Premium HMI Mobile oraz przeglądarki internetowej;
- Obsługa skryptów VBA;

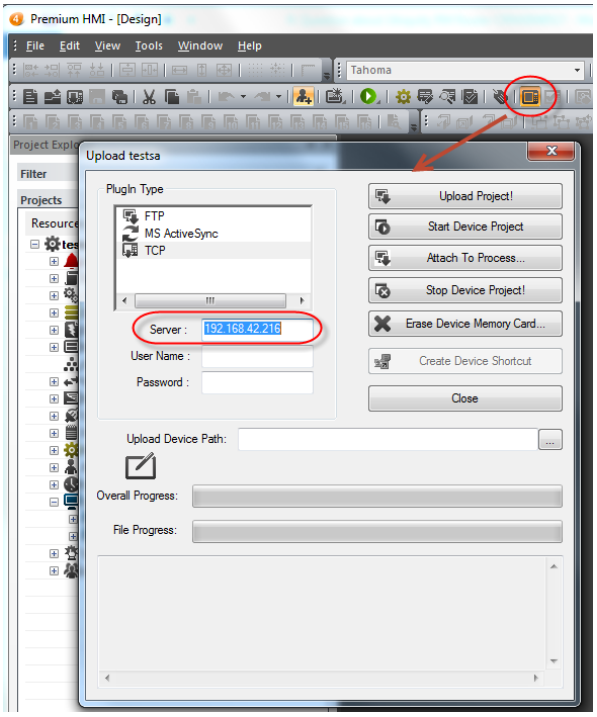
Wszystkie wyżej wymienione funkcjonalności programowane są z poziomu aplikacji Premium HMI, służącej do tworzenia wizualizacji na panele operatorskie firmy ASEM. Za jej pośrednictwem możemy m.in.: utworzyć ekrany graficzne czy zdefiniować moduły logowania danych ze sterownika oraz alarmowania e-mail / SMS. Szczegółowy opis obsługi aplikacji Premium HMI znajduje się w podręczniku *Premium HMI – Pierwsze Kroki*, który można pobrać pod adresem:

http://www.sabur.com.pl/wymiana/092feb4cfac9f7a8474d1f2f69495118/plik/PremiumHMI4_Podrecznik_PL.pdf

Po utworzeniu projektu wizualizacji w Premium HMI dla Routera Ubiquity należy odpowiednio przystosować jego ekrany tak, by mogły być one uruchomione z poziomu aplikacji mobilnej lub przeglądarki internetowej. W tym celu klikamy prawym przyciskiem myszy na nazwę ekranu, który ma pełnić rolę strony głównej wizualizacji, a następnie wybieramy opcję *Create HTML page based on this Screen*:



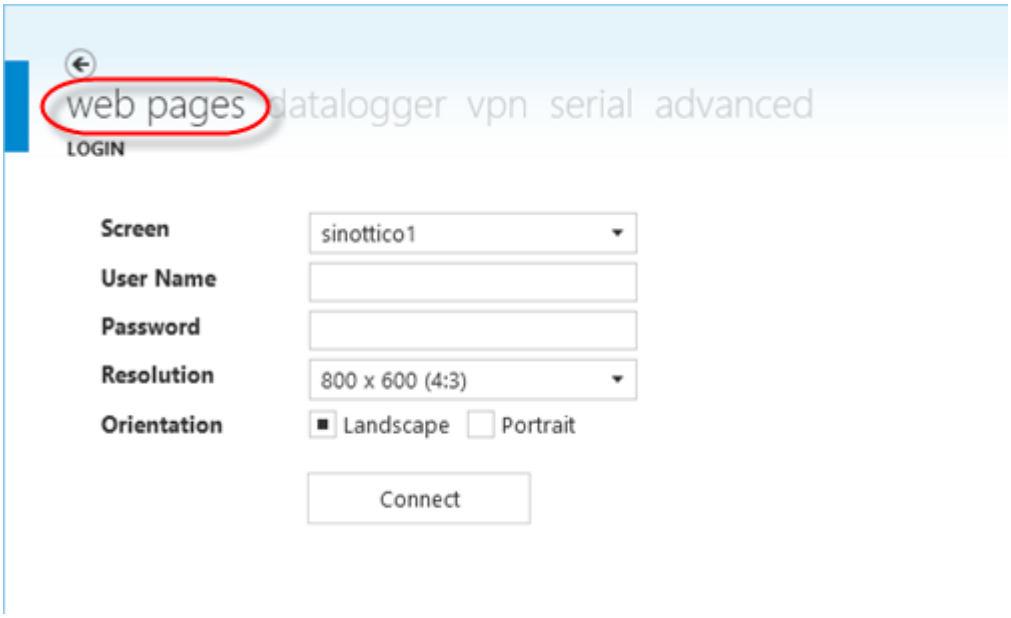
W nowym oknie definiujemy domyślną rozdzielczość tworzonego okna i zatwierdzamy wybór, klikając przycisk OK. Wgrywamy projekt do Routera w taki sam sposób, jak dla panelu HMI. W tym celu wybieramy ikonę *Upload Project to Device*, a następnie w pole *Server* wpisujemy adres IP urządzenia docelowego:



Po wgraniu projektu do Routera Ubiquity możemy uruchomić wizualizację za pośrednictwem aplikacji mobilnej Premium HMI Mobile lub przeglądarki internetowej, wpisując w pole adresu:

http://<adres_ip_urzadzenia>/weberver/<nazwa_ekranu>.html

Strony wizualizacji mogą być także uruchomione z poziomu aplikacji Ubiquity Control Center. W tym celu, po połączeniu się z urządzeniem z górnego menu wybieramy opcję *web pages*:



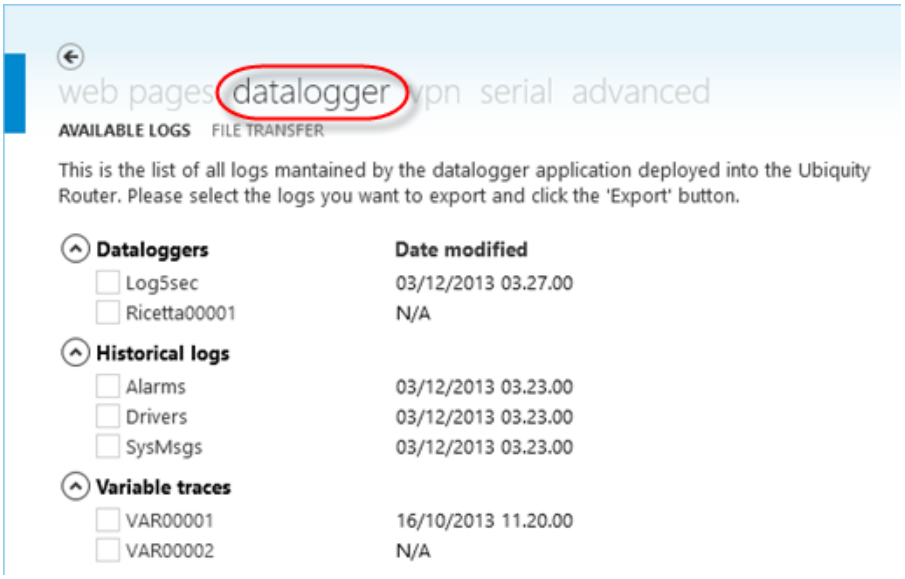
Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

W kolejnych polach definiujemy parametry aplikacji, z którą chcemy nawiązać połączenie:

- **Screen** – nazwa ekranu aplikacji (dla której zdefiniowaliśmy opcję *Create HTML page*);
- **User Name / Password** – nazwa użytkownika i hasło aplikacji wizualizacyjnej;
- **Resolution** – rozdzielczość okna wizualizacji;
- **Orientation** – orientacja pozioma (*landscape*) lub pionowa (*portrait*).

Po zdefiniowaniu wszystkich parametrów, klikamy na przycisk *Connect*, co powoduje uruchomienie ekranu wizualizacji.

Z poziomu aplikacji Ubiquity Control Center możemy bezpośrednio przeglądać i pobierać na dysk twardy komputera pliki z logowanymi danymi historycznymi. Aby móc korzystać z tej funkcjonalności należy w tworzonym projekcie wizualizacji dla Routera zdefiniować parametry, które mają być logowane do pamięci urządzenia (np. zmienne ze sterownika PLC, alarmy itp.). Dzięki temu po otwarciu zakładki *datalogger* w aplikacji Control Center mamy możliwość podglądu dostępnych modułów logowania oraz pobrania ich na dysk komputera:



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

7. Modyfikacja wyglądu i struktury systemu

System zdalnego dostępu serwisowego Ubiquity Control Center może być indywidualnie dostosowany przez każdego użytkownika do jego potrzeb. Istnieją dwie metody modyfikacji systemu:

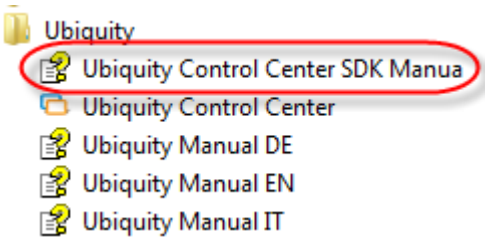
- Wykorzystanie narzędzia Ubiquity SDK (Software Development Kit) do implementacji funkcjonalności Ubiquity w tworzonych aplikacjach (funkcja dostępna od wersji 5 systemu Ubiquity);
- Modyfikacje elementów i motywów graficznych pojawiających się podczas korzystania z aplikacji Ubiquity Control Center (funkcja dostępna od wersji 6 systemu Ubiquity).

Ubiquity SDK:

Ubiquity SDK umożliwia implementację funkcjonalności, które można znaleźć w aplikacji Control Center we własnych programach. Narzędzie zapewnia zbiór bibliotek, z których możemy swobodnie korzystać, projektując nasze aplikacje. Z wykorzystaniem Ubiquity SDK istnieje możliwość np.:

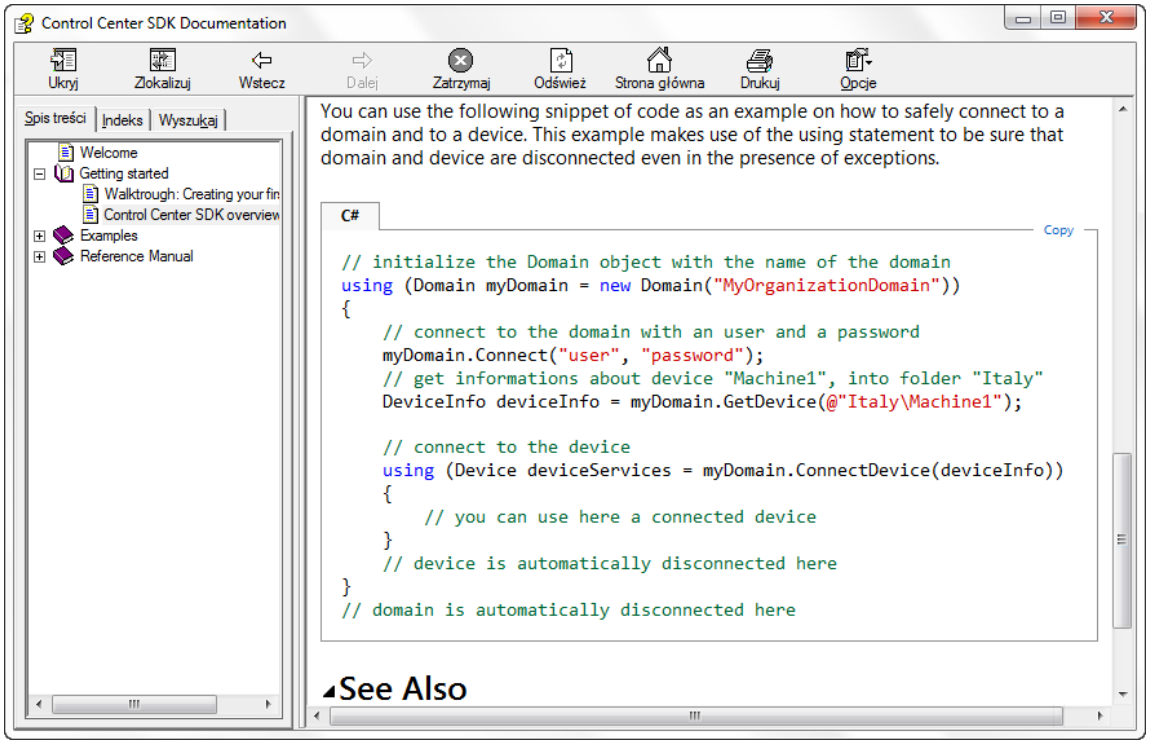
- Nawiązania połączenia z Domeną;
- Nawiązania połączenia VPN z wybranym urządzeniem;
- Uruchomienia zdalnej transmisji po porcie szeregowym.

Wraz z Ubiquity Control Center na komputerze użytkownika instalowany jest podręcznik opisujący funkcjonalności pakietu SDK:



W podręczniku znajdują się opisy dostępnych funkcji oraz przykładowe programy:

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl



Modyfikacje elementów graficznych:

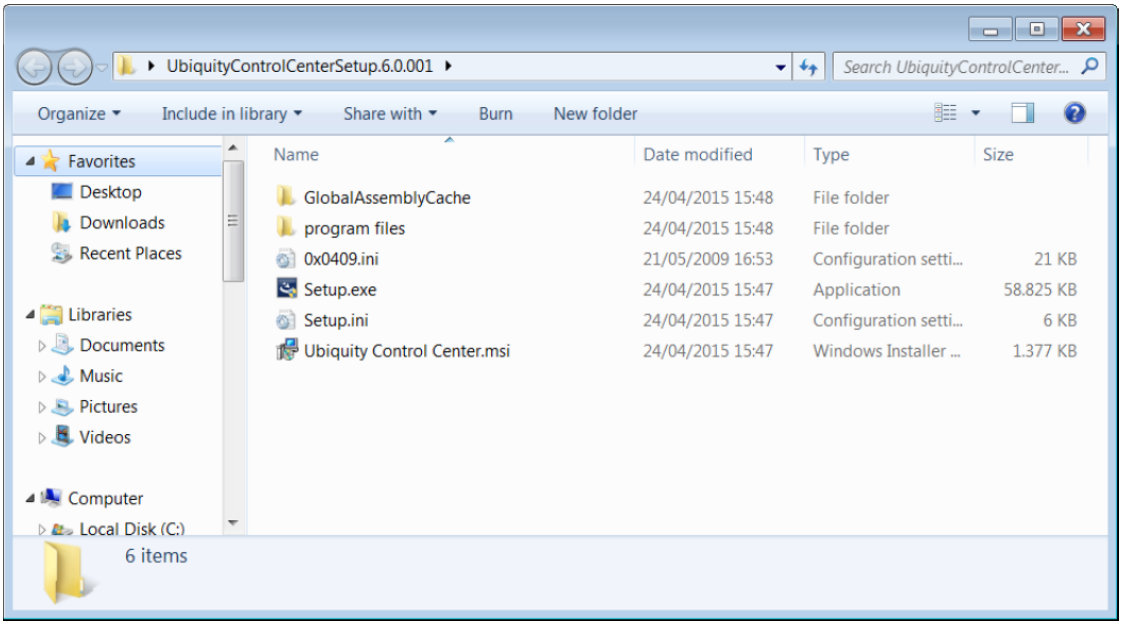
Wersja 6 systemu Ubiquity pozwala użytkownikowi na wprowadzanie zmian w wyglądzie aplikacji Ubiquity Control Center. Administrator aplikacji może dostosowywać jej wygląd na 2 sposoby:

- poprzez modyfikację plików dla aplikacji już zainstalowanej na komputerze;
- poprzez modyfikację plików instalatora aplikacji.

W przypadku modyfikacji plików instalatora wprowadzone zmiany będą widoczne w każdej nowo zainstalowanej kopii aplikacji, która została wgrana z wykorzystaniem zmodyfikowanego pliku.

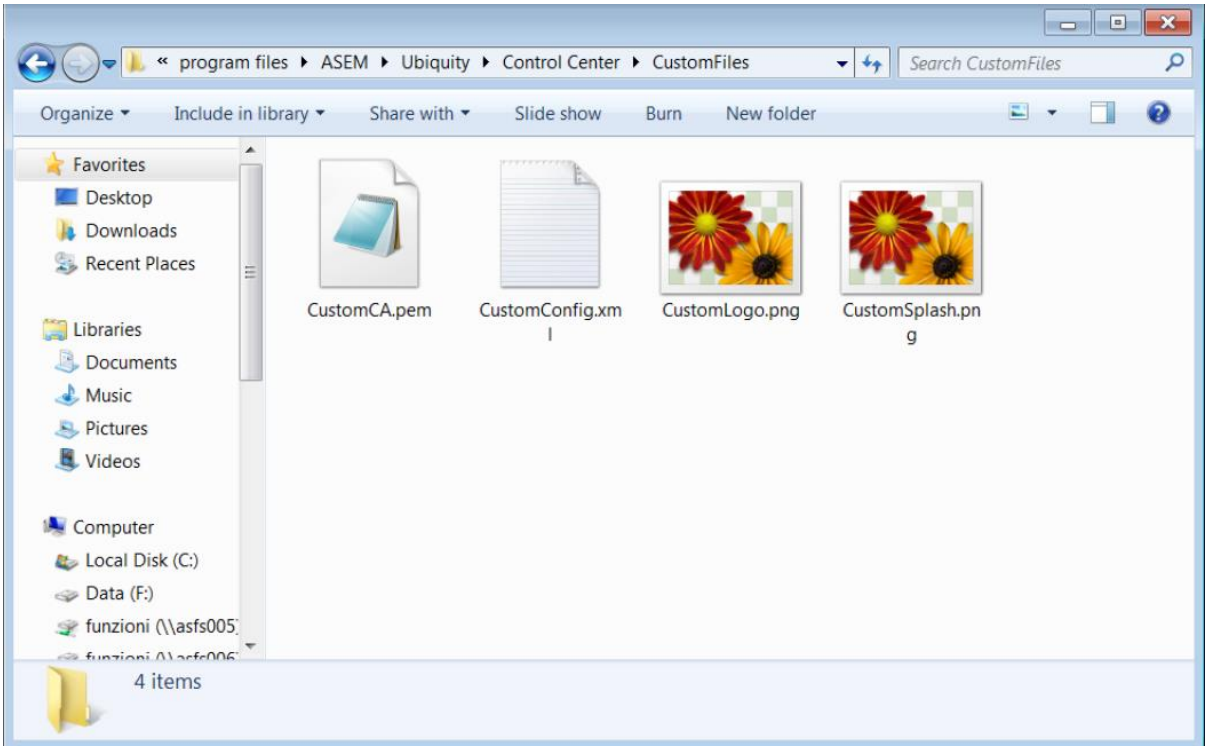
Struktura plików instalatora:

Instalator aplikacji Ubiquity Control Center v.6 reprezentowany jest jako archiwum, w skład którego wchodzą następujące elementy:



- **GlobalAssemblyCache** - zawiera biblioteki obiektów wykorzystywanych podczas działania aplikacji Control Center;
- **Program Files** – zawiera pliki instalacyjne i folder „Custom Files”, w którym przechowywane są pliki modyfikujące wygląd aplikacji;
- ***.ini** – pliki inicjalizacyjne;
- **Ubiquity Control Center.msi** – pakiet instalacyjny;
- **Setup.exe** – uruchomienie instalacji.

W lokalizacji *„\program files\ASEM\Ubiquity\Control Center\CustomFiles”* można umieszczać pliki, które wykorzystywane będą do modyfikcji wyglądu aplikacji:

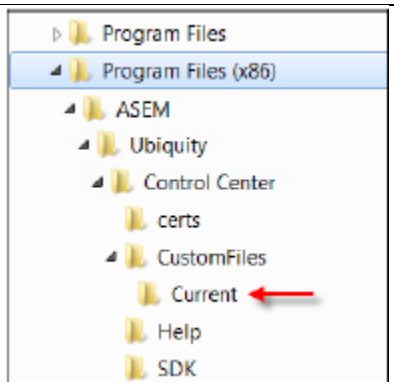


- **CustomCA.pem** – certyfikat pozwalający na połączenie z prywatnym serwerem;
- **CustomConfig.xml** – plik XML zawierający ustawienia aplikacji Control Center takich jak np. kolor przewodni okien, adresy serwerów, itp.;
- **CustomLogo.png** – ikona, która wyświetlana będzie w prawym górnym rogu aplikacji Ubiquity Control Center;
- **CustomSplash.png** – grafika, która jest wyświetlana podczas uruchamiania aplikacji Control Center.

Modyfikacja grafiki powitalnej:

Obszar działania	Opis
Zainstalowana aplikacja	Należy wykonać następujące kroki: 1. Przechodzimy do lokalizacji, w której zainstalowana jest aplikacja Ubiquity Control Center (domyślnie: *C:\Program Files(x86)\ASEM\Ubiquity\Control Center*) i otwieramy folder *Custom Files*. Tworzymy tam nowy folder o nazwie *Current* (jeżeli taki nie istnieje):

Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

	 2. Tworzymy własną grafikę powitalną w formie pliku z rozszerzeniem .PNG. Istnieje pełna dowolność co do rozmiaru obrazu (ale zalecany rozmiar to 640x800 px). Nadajemy plikowi nazwę: *CustomSplash.png*; 3. Umieszczamy utworzony plik w folderze *Current*. Podczas następnego startu Ubiquity Control Center wyświetli się utworzona grafika;
Plik instalatora	Należy wykonać następujące kroki: 1. Tworzymy własną grafikę powitalną w formie pliku z rozszerzeniem .PNG. Istnieje pełna dowolność co do rozmiaru obrazu (zalecany rozmiar to 640x800 px); 2. Nadajemy plikowi nazwę: *CustomSplash.png*; 3. Umieszczamy utworzony plik w folderze *Custom Files* znajdującym się w lokalizacji: *program files/ASEM/Ubiquity/Control Center* instalatora; Podczas uruchomienia instalacji na dowolnym komputerze domyślna grafika zostanie zastąpiona przez dodany obraz.

Modyfikacja logo aplikacji:

Obszar działania	Opis
Zainstalowana aplikacja	Należy wykonać następujące kroki: 1. Tworzymy własne logo w formie pliku z rozszerzeniem .PNG w rozmiarze 100x35 px. Nadajemy plikowi nazwę: *CustomLogo.png*; 2. Umieszczamy utworzony plik w folderze *Current* (patrz tabela powyżej). Podczas następnego startu Ubiquity Control Center w oknie aplikacji wyświetli się zdefiniowane logo;

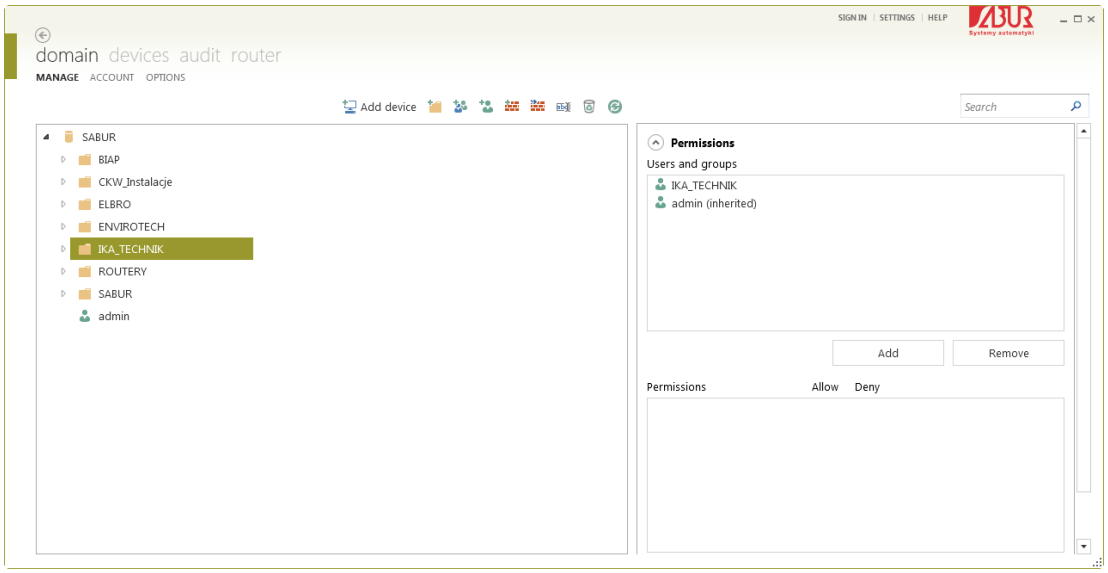
Plik instalatora	Należy wykonać następujące kroki: 1. Tworzymy własne logo w formie pliku z rozszerzeniem .PNG w rozmiarze 100x35px. Nadajemy plikowi nazwę: *CustomLogo.png*; 2. Umieszczamy utworzony plik w folderze *Custom Files* znajdującym się w lokalizacji: *program files/ASEM/Ubiquity/Control Center* instalatora; Podczas uruchomienia instalacji na dowolnym komputerze domyślne logo zostanie zastąpione przez dodany obraz.

Modyfikacja koloru przewodniego okien aplikacji:

W celu zmiany koloru przewodniego okien aplikacji należy dokonać zmian w pliku XML, który zawiera zbiór informacji o podstawowych ustawieniach programu.

Obszar działania	**Opis**
Zainstalowana aplikacja	Należy wykonać następujące kroki: 1. Otwieramy plik *config.xml* znajdujący się w lokalizacji: *„C:\Users\<nazwa użytkownika>\AppData\Local\ASEM\Ubiquity\Control Center*; **UWAGA:** Folder *AppData* może być folderem ukrytym – należy zaznaczyć opcję wyświetlania folderów ukrytych w ustawieniach widoku okien systemu; 2. Odszukujemy wpis *<Param Name="ThemeColor" Value="#98982D" />* lub jeśli nie istnieje – dodajemy go do listy pomiędzy wpisami *<Params>* oraz *</Params>*; 3. Wartość *"#98982D"* reprezentuje kolor okien aplikacji w formacie #RGB – zmiana tej wartości spowoduje zmianę koloru;
Plik instalatora	Należy wykonać następujące kroki: 1. Otwieramy plik *„CustomConfig.xml”* znajdujący się w folderze *”program files\ASEM\Ubiquity\Control Center\CustomFiles”* folderu instalacyjnego; 2. Modyfikujemy wpis *<Param Name="ThemeColor" Value="#98982D" />* znajdujący się pomiędzy liniami *<Params>* oraz *</Params>* wprowadzając nową wartość koloru w formacie #RGB (*Value=#xxxxxx*); Podczas uruchomienia instalacji na dowolnym komputerze ustawienia domyślnego koloru zostaną zaktualizowane zgodnie z wprowadzonymi zmianami.

Zmieniony kolor okien aplikacji:



Sabur Sp. z o.o. ul. Puławska 303, 02-785 Warszawa, tel. 22 549 43 53, fax 22 549 43 50
sabur@sabur.com.pl www.sabur.com.pl

NOTATKI: