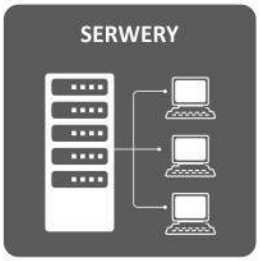
EVER POWER SYSTEMS

INSTRUKCJA OBSŁUGI



Karta Zarządzająca EVER SNMP/HTTP do zasilaczy UPS

POWERLINE 33
POWERLINE GREEN 33
POWERLINE GREEN 33 LITE
POWERLINE GREEN 33 PRO

POLSKI PRODUCENT

EVER Sp. z o.o.
ul. Wołczyńska 19, 60-003 Poznań
www.ever.eu, ups@ever.eu
tel. +48 61 6500 400, faks +48 61 6510 927

SPIS TREŚCI

CHARAKTERYSTYKA KARTY ZARZĄDZAJĄCEJ

Sieciowy system wizualizacji i zarządzania układami zasilania umożliwia integrację zasilaczy awaryjnych EVER z siecią komputerową typu ETHERNET. Pozwala to na zdalne zarządzanie całym systemem zasilania z dowolnego komputera znajdującego się w sieci. Usługi dostępne w ramach systemu wizualizacji i zarządzania przedstawiono w tabeli 1.

Tabela 1. Usługi dostępne w ramach systemu wizualizacji i zarządzania

Nazwa usługi	Protokół	Wartości domyślne	
		Stan	Port
WEB	HTTP	nieaktywny	80
	HTTPS	aktywny	443
SNMP	SNMPv1	nieaktywny	161
	SNMPv2c	nieaktywny	
	SNMPv3	aktywny	

Usługi WWW oraz SNMP są w pełni konfigurowalne – użytkownik ma możliwość wyboru jakie protokoły będą obsługiwane przez kartę oraz na jakim porcie będą dostępne.

Dostęp do interfejsu WEB wymaga autoryzacji. Karta posiada dwa konta: dla użytkownika bez uprawnień (tylko odczyt) oraz konto administratora (odczyt i zapis). Standardowe (domyślne) parametry autoryzacji dla interfejsu WEB przedstawiono w tabeli 2.

Tabela 2. Domyślne konta użytkowników interfejsu WEB

Użytkownik	Hasło	Uwagi
ever	ever	Standardowy użytkownik (tylko odczyt)
admin	ever	Administrator (odczyt i zapis)

Administrator ma możliwość zmiany nazw użytkowników oraz haseł.

Uwaga!
Ze względów bezpieczeństwa nie zaleca się korzystania z domyślnych haseł.

Uwaga!
Dane przesyłane za pomocą protokołu HTTP nie są szyfrowane. Zaleca się korzystanie wyłącznie z protokołu HTTPS. Administrator może wyłączyć obsługę HTTP w konfiguracji karty.

Informacja
Protokół HTTP jest domyślnie wyłączony.

Parametry autoryzacji dla Agenta SNMP zamieszczono w tabeli 3. Parametry domyślne dostępne są wyłącznie dla SNMPv1 oraz SNMPv2c. W przypadku SNMPv3 autoryzacja bazuje na kontach użytkowników i domyślnie wszystkie konta są nieaktywne (brak więc domyślnego użytkownika).

Tabela 3. Domyślne parametry autoryzacji SNMP

Wersja protokołu	Community (odczyt)	Community (zapis/odczyt)
SNMPv1	public	private
SNMPv2c	public	private

Uwaga!
Dane przesyłane za pomocą protokołów SNMPv1 oraz SNMPv2c nie są szyfrowane. Zaleca się korzystanie wyłącznie z protokołu SNMPv3. Administrator może zablokować protokoły SNMPv1 oraz SNMPv2c w konfiguracji karty.

Informacja
Protokoły SNMPv1 oraz SNMPv2c są domyślnie wyłączone.

INSTALACJA I URUCHOMIENIE

WYMAGANIA

Podstawowym wymaganiem sprzętowym jest posiadanie przez użytkownika instalacji sieci komputerowej typu ETHERNET (RJ-45) oraz zasilacza awaryjnego EVER umożliwiającego instalację karty zarządzającej.

Wymagania dla przeglądarki WWW:

- Zgodność z HTML 5.0,
- Obsługa JavaScript v.1.1.

MONTAŻ

Montaż karty zarządzającej należy przeprowadzić zgodnie z wytycznymi zawartymi w instrukcji obsługi urządzenia, w którym ma być zamontowana karta.
Po prawidłowym wykonaniu instalacji karty w urządzeniu, należy za pomocą kabla sieciowego (skrętka Ethernet UTP/STP ze złączem RJ-45) połączyć kartę zarządzającą z lokalną siecią komputerową.

KONFIGURACJA PARAMETRÓW SIECI (LAN)

Fabrycznie nowa karta ma domyślnie ustawioną opcję pobierania adresu IP z serwera DHCP, można więc skonfigurować ją przez przeglądarkę internetową.

W celu przeprowadzenia konfiguracji należy:

1) Zainstalować kartę zarządzającą w zasilaczu zgodnie z opisem w instrukcji obsługi UPS-a.
2) Sprawdzić przydzielony adres IP dla karty SNMP przez serwer DHCP.
3) Zapamiętać lub zanotować stan połączenia (adres IP).
4) W przeglądarce internetowej wpisać adres IP karty SNMP.
5) Przeprowadzić konfigurację karty SNMP.

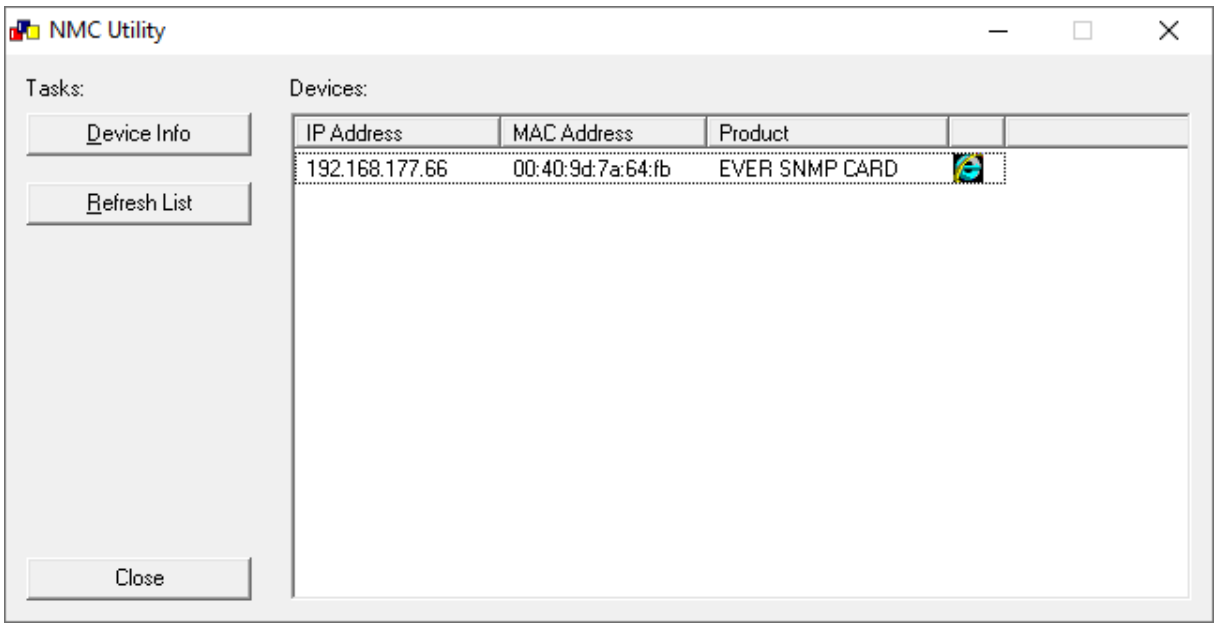
WYKRYWANIE KARTY SNMP

Adres karty może być wykryty przez oprogramowanie NMC Utility.exe (system operacyjny MS Windows).

W tym celu należy uruchomić program NMC Utility.exe. Program wykorzystuje transmisję UDP Broadcast na adres 224.0.5.128.

Informacja
Do prawidłowego wykrywania karty SNMP wymagane jest, aby urządzenia warstwy sieciowej zezwalały na komunikację UDP Broadcast. Sposób konfiguracji urządzeń warstwy sieciowej opisany jest w dokumentacji danego produktu.

Przykładowy zrzut ekranu z poprawnie wykrytą kartą SNMP został zaprezentowany na rys. 1.



Rys. 1. Widok wykrytej karty w NMC Utility

ZARZĄDZANIE Z POZIOMU WWW

ŁĄCZENIE Z INTERFEJSEM WWW KARTY

Karta Zarządzająca EVER SNMP/HTTP posiada wbudowany serwer protokołu HTTP/HTTPS, pozwalający na podgląd i modyfikację parametrów karty oraz zasilacza z poziomu przeglądarki WWW.

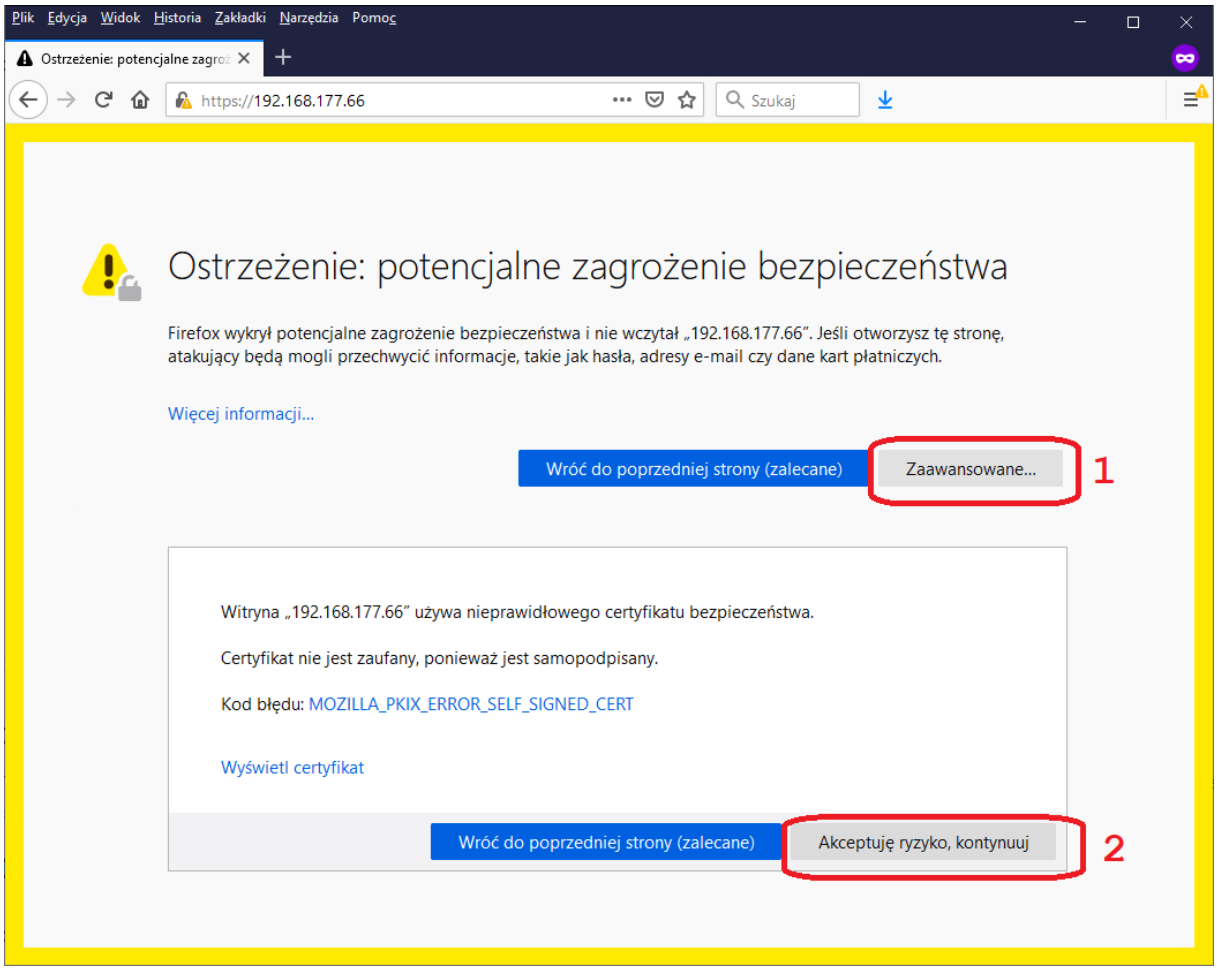
Domyślnie karta pracuje z obsługą protokołu HTTPS na standardowym porcie 443. Aby połączyć się z interfejsem WEB należy jako adres strony w przeglądarce internetowej wprowadzić adres IP karty (np.: https://192.168.0.1).

Informacja
Jeżeli serwer WEB karty pracuje na niestandardowym porcie to nr portu należy określić po dwukropku:
http://192.168.0.1:8080 (dla HTTP na porcie 8080)
https://192.168.0.1:4433 (dla HTTPS na porcie 4433)

Informacja
Aby połączyć się z serwerem WEB poprzez IPv6 należy w pasku adresu przeglądarki wprowadzić adres IPv6 w nawiasach kwadratowych:
http://[FE80::123:45FF:FE67:89AB] (dla HTTP)
https://[FE80::123:45FF:FE67:89AB] (dla HTTPS)

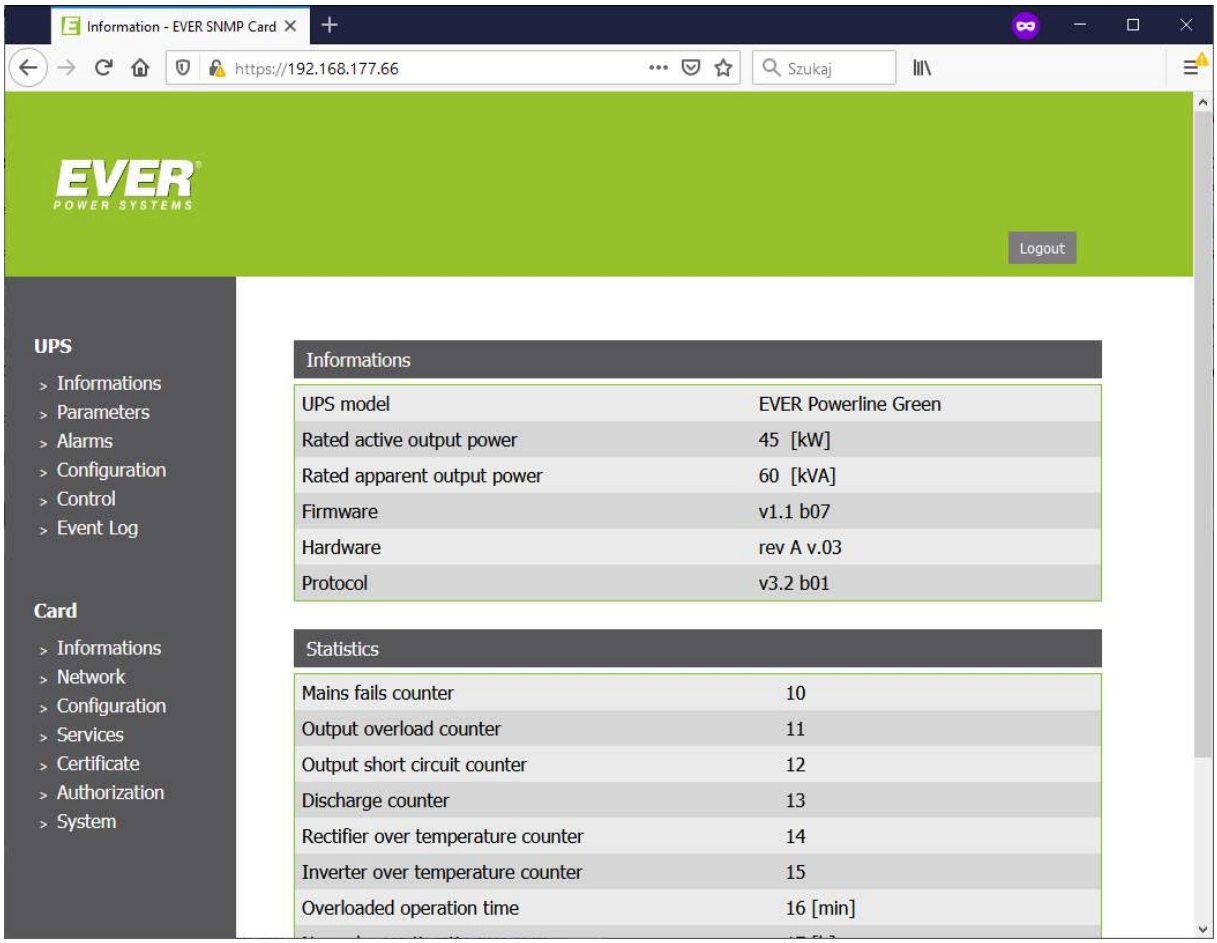
Jeżeli serwer pracuje z niestandardowym portem to port określamy po dwukropku:
http://[FE80::123:45FF:FE67:89AB]:8080 (dla HTTP na porcie 8080)
https://[FE80::123:45FF:FE67:89AB]:4433 (dla HTTPS na porcie 4433)

Jeżeli karta posiada prawidłową konfigurację sieciową, w oknie przeglądarki powinien pojawić się monit o podanie nazwy użytkownika i hasła (domyślne parametry autoryzacji przedstawiono w rozdziale CHARAKTERYSTYKA KARTY ZARZĄDZAJĄCEJ). Ponieważ domyślnie karta korzysta z własnego certyfikatu SSL (certyfikat self-signed) przeglądarka wyświetli komunikat o niezaufanym połączeniu (rys. 2). Aby móc wyświetlić zawartość strony należy kliknąć przycisk ***Zaawansowane*** a następnie ***Akceptuję ryzyko, kontynuuj***.



Rys. 2. Komunikat o niezaufanym połączeniu

Po pozytywnej weryfikacji danych uwierzytelniających załadowana zostanie strona główna Karty Zarządzającej (rys. 3).



Rys. 3. Strona główna Karty Zarządzającej EVER

ZARZĄDZANIE I MONITOROWANIE UPS

Parametry informacyjne i konfiguracyjne zasilacza znajdują się w kategorii **UPS**. Dostępność poszczególnych nastaw/informacji zależy od typu konta, na które nastąpiło logowanie w systemie karty.

Tabela 4. Parametry konfiguracyjno-informacyjne UPS

Karta	Opis	Widoczność dla konta	
		Użytkownik	Administrator
Informacje (Informations)	Podstawowe informacje oraz statystyka pracy UPS.	Tak	Tak
Parametry (Parameters)	Parametry pracy UPS.	Tak	Tak
Alarmy (Alarms)	Sygnalizacja newralgicznych zdarzeń w systemie zasilania.	Tak	Tak
Konfiguracja (Configuration)	Konfiguracja parametrów zasilacza UPS.	Nie	Tak
Kontrola (Control)	Kontrola pracy zasilacza UPS.	Nie	Tak
Zdarzenia (Event Log)	Lista zdarzeń zarejestrowanych przez UPS	Tak	Tak

Informacje (Informations)

Zawiera podstawowe informacje dotyczące UPS (model, moc znamionowa, wersje oprogramowania, protokołu) oraz liczniki wystąpień danych zdarzeń i czasów pracy w tych trybach (statystyki). Wykaz dostępnych parametrów wraz z opisem zestawiono w tabeli 5 i 6.

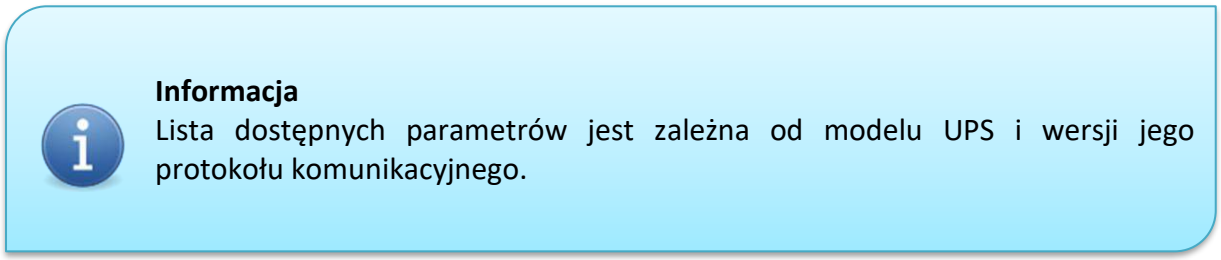


Tabela 5. Informacje - wykaz parametrów

Parametr	Opis
Model zasilacza (UPS model)	Model zasilacza
Znamionowa moc czynna (Rated active output power)	Moc czynna przenoszona przez zasilacz wyrażona w kW
Znamionowa moc pozorna (Rated apparent output power)	Moc pozorna przenoszona przez zasilacz wyrażona w kVA
Firmware (Firmware)	Wersja oprogramowania UPS
Hardware (Hardware)	Wersja platformy sprzętowej UPS
Protokół (Protocol)	Wersja protokołu komunikacyjnego UPS

Tabela 6. Statystyki - wykaz parametrów

Parametr	Opis
Liczba wystąpień nieprawidłowych parametrów sieci zasilającej (Mains fails counter)	Licznik wystąpień zdarzeń związanych z przekroczeniem dopuszczalnych parametrów sieci zasilającej
Liczba przeciążeń zasilacza (Output overload counter)	Licznik zdarzeń związanych z przeciążeniem zasilacza
Liczba zwarć na wyjściu zasilacza (Output short circuit counter)	Licznik zdarzeń związanych ze zwarciem wyjścia zasilacza w falownikowych trybach pracy
Liczba całkowitych rozładowań akumulatorów (Discharge counter)	Liczba całkowitych rozładowań akumulatorów zasilacza
Liczba przegrzań prostownika (Rectifier over temperature counter)	Liczba zdarzeń związanych z przegrzaniem prostownika
Liczba przegrzań falownika (Inverter over temperature counter)	Liczba zdarzeń związanych z przegrzaniem falownika
Czas pracy przeciążonego zasilacza (Overloaded operation time)	Czas pracy urządzenia UPS w przeciążeniu wyrażony w minutach
Czas pracy w trybie normalnym (sieciowym) (Normal operation time)	Czas pracy w trybie NORMALNYM urządzenia UPS wyrażony w godzinach
Czas pracy w trybie rezerwowym (bateryjnym) (Battery backup operation time)	Czas pracy w trybie REZERWOWYM urządzenia UPS wyrażony w minutach
Czas pracy w trybie obejściowym (bypass) (Bypass operation time)	Czas pracy zasilacza w trybie BYPASS wyrażony w godzinach

Parametry (Parameters)

Lista parametrów mierzonych przez UPS. Informacje zostały podzielone na grupy **Parametry pracy zasilacza (UPS Operating Parameters)**, **Parametry środowiskowe (Environmental Parameters)**, **Parametry wejściowe (Input Parameters)**, **Parametry wyjściowe (Output Parameters)** oraz **Parametry wejściowe układu obejściowego (Bypass Parameters)**. Podział ten wynika z budowy wewnętrznej urządzenia. Każdy blok funkcjonalny posiada własną grupę parametrów informujących o jego pracy.

Parametry pracy zasilacza (UPS Operating Parameters)

Lista parametrów mierzonych przez UPS. Dostępne parametry wraz z opisem zestawiono w tabeli 7.

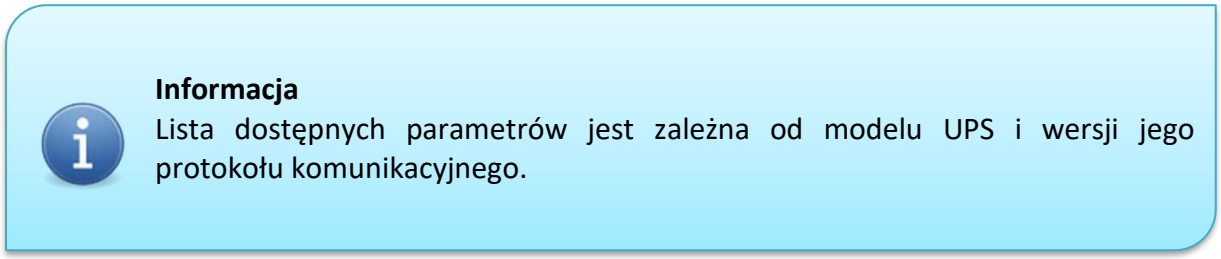


Tabela 7. Parametry pracy zasilacza

Parametr	Opis
Tryb pracy (Operating Mode)	Aktualny tryb pracy, w którym znajduje się zasilacz UPS (tabela 8)
Tryb pracy równoległej (Parallel Mode)	Aktualny tryb pracy równoległej zasilacza UPS (tabela 9)
Przewidywany czas pracy autonomicznej zasilacza (Autonomy Time)	Przewidywany czas pracy zasilacza na pracy bateryjnej dla aktualnego obciążenia
Stopień naładowania akumulatorów (Available Battery Capacity)	Wartość dostępnej pojemności dołączonych akumulatorów, podana z rozdzielczością jednego procenta
Napięcie dodatniej / ujemnej sekcji akumulatorów (Battery Voltage)	Wartość napięcia dodatniego (+) i ujemnego (–) stringu akumulatorów podana z rozdzielczością jednego wolta
Prąd dodatniej / ujemnej sekcji akumulatorów (Battery Current)	Prąd pobierany z dodatniego (+) i ujemnego (–) stringu akumulatorów podawany z rozdzielczością jednej dziesiętnej ampera
Stopień dostępnej pojemności akumulatorów (Battery Condition)	Wartość aktualnej dostępnej pojemności akumulatora określana po wykonaniu testu baterii, odniesiona do wartości nominalnej, podana z rozdzielczością jednego procenta
Temperatury bloków wewnętrznych UPS (Internal Temperatures)	Temperatury wewnętrznych bloków zasilacza UPS podawana z rozdzielczością 1 stopnia Celsjusza

Tabela 8. Tryby pracy zasilacza

Tryb pracy (Operating Mode)	Opis
Nieznany (Unknown)	Stan pośredni załączany w czasie startu zasilacza oraz w trakcie zmiany trybów pracy.
Sieciowy (Normal)	Zasilacz dostarcza energię z sieci zasilającej do wyjścia za pomocą układu falownikowego.
ECO (ECO)	Zasilacz dostarcza energię z sieci zasilającej do wyjścia za pomocą układu obejściowego (bypass-u).
BYPASS (BYPASS)	Zasilacz dostarcza energię do wyjścia, po spełnieniu kryterium poprawności zasilania, za pomocą układu obejściowego (bypass-u). Tryb wymuszany przez użytkownika lub występujący w trakcie przekroczenia dopuszczalnej mocy wyjściowej.
Rezerwowy (bateryjny) (Battery backup)	Do wyjścia zasilacza energia dostarczana jest z baterii.
Oczekiwanie (STANDBY) (Standby)	Zasilacz czeka na powrót sieci zasilającej o poprawnych parametrach. Po powrocie sieci zasilacz podejmuje pracę zgodnie z konfiguracją.
Czuwanie (Watch)	Do zasilacza jest dostarczana energia z sieci o poprawnych parametrach. Dostarczanie energii do wyjścia, po spełnieniu kryterium poprawności zasilania, następuje przez układ obejściowy. Działają mechanizmy konserwacji baterii.
Awaryjny (Emergency)	Wystąpił stan awaryjny w urządzeniu. Zasilanie dostarczane jest z linii obejściowej. Przy niespełnieniu kryterium poprawności zasilania lub wywołaniu EPO wyjście zasilacza jest odłączane.
Inicjalizacja (Initialization)	Stan pośredni występujący po zainicjowaniu platformy sprzętowej urządzenia wartościami startowymi.
STOP (STOP)	Brak zasilania o prawidłowych parametrach.
Hybrydowy (Hybrid)	Zasilacz dostarcza energii do wyjścia z sieci, uzupełniając brakującą część z akumulatorów.

Tabela 9. Tryby pracy równoległej

Tryb pracy równoległej (Parallel Mode)	Opis
Praca autonomiczna (Single Unit)	UPS pracuje jako samodzielny zasilacz
Master (Master)	Sygnalizacja jednostki master w systemie równoległym
Slave (Slave)	Sygnalizacja jednostki slave w systemie równoległym
Jednostka zatrzymana (Unit stopped)	Sygnalizacja logicznego odłączenia jednostki od systemu pracującego równolegle
Brak redundancji (Redundancy lost)	Sygnalizacja braku jednostki redundantnej.
Jednostka nieaktywna (Unit inactive)	Sygnalizacja braku dołączenia (logicznego) nowo załączonej jednostki do systemu pracy równoległej
Brak minimalnej liczby jednostek (Not enough units)	Sygnalizacja braku dostępnej minimalnej ilości jednostek aktywnych w systemie

Parametry środowiskowe (Environmental Parameters)

Lista parametrów środowiskowych mierzonych przez UPS. Dostępne parametry wraz z opisem zestawiono w tabeli 10.

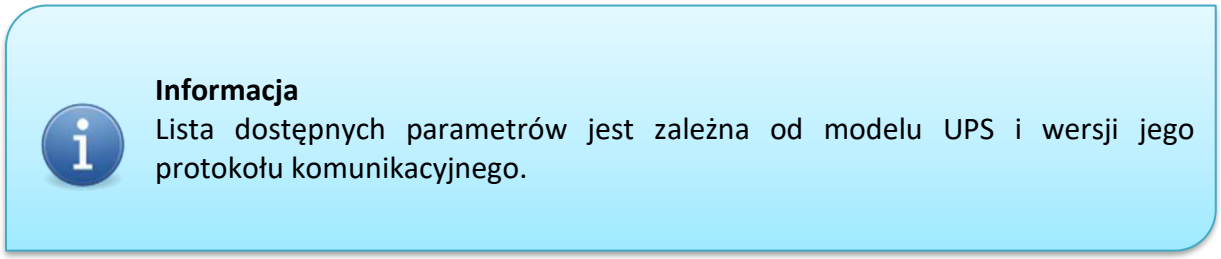


Tabela 10. Parametry środowiskowe

Parametr	Opis
Temperatura otoczenia (Ambient Temperature)	Temperatura otoczenia podawana z rozdzielczością jednego stopnia Celsjusza
Wilgotność względna (Relative Humidity)	Wilgotność względna podawana z rozdzielczością jednego procenta

Parametry wejściowe (Input Parameters)

Lista parametrów wejściowych mierzonych przez UPS. Dostępne parametry wraz z opisem zestawiono w tabeli 11.

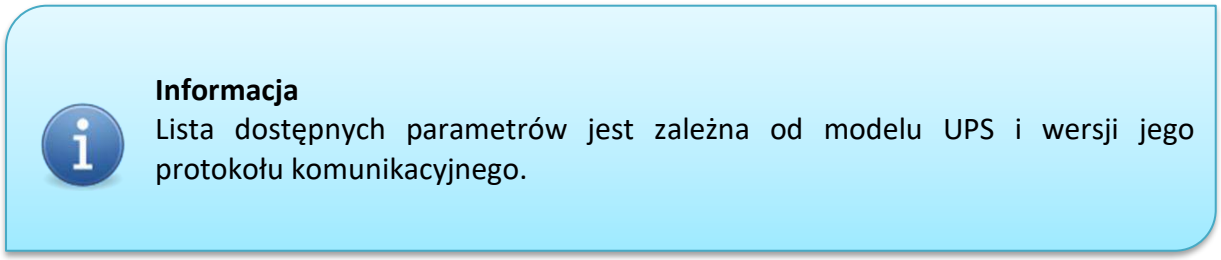
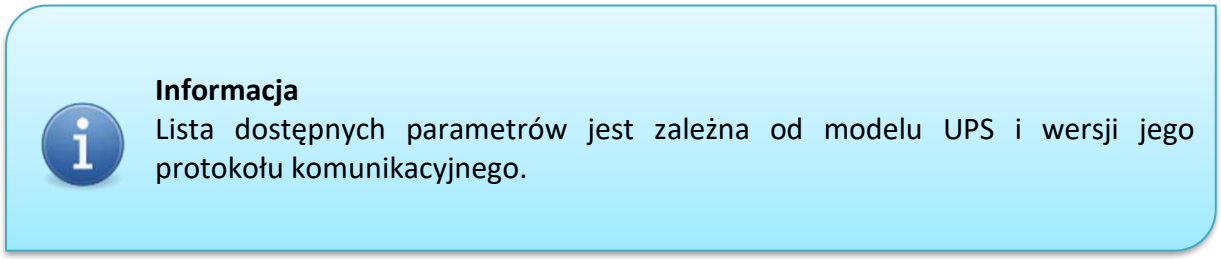


Tabela 11. Parametry wejściowe

Parametr	Opis
Napięcie wejściowe Ln (Input Voltage Ln)	Napięcie wejściowe prostownika dla linii n podawane z rozdzielczością 1 V
Prąd wejściowy Ln (Input Current Ln)	Prąd wejściowy prostownika dla linii n podawany z rozdzielczością 0.1 A
Częstotliwość wejściowa (Input Frequency)	Częstotliwość wejściowa prostownika (pomiar dla linii L1) podawana z rozdzielczością 0.1 Hz
Moc czynna wejściowa Ln (Input Active Power Ln)	Wejściowa moc czynna prostownika dla linii n podawana z rozdzielczością 0.1 kW
Moc pozorna wejściowa Ln (Input Apparent Power Ln)	Wejściowa moc pozorna prostownika dla linii n podawana z rozdzielczością 0.1 kVA
Współczynnik mocy wejściowej PF Ln (Input Power Factor Ln)	Wejściowy współczynnik mocy prostownika dla linii n

Parametry wyjściowe (Output Parameters)

Lista parametrów wyjściowych mierzonych przez UPS. Dostępne parametry wraz z opisem zestawiono w tabeli 12.



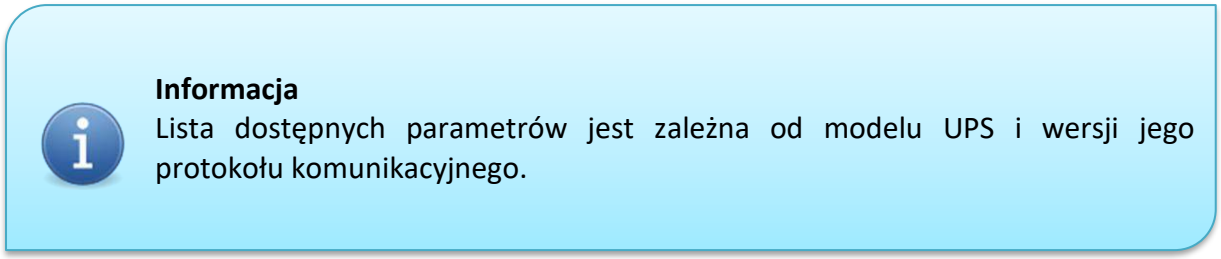
Informacja
Lista dostępnych parametrów jest zależna od modelu UPS i wersji jego protokołu komunikacyjnego.

Tabela 12. Parametry wyjściowe

Parametr	Opis
Napięcie wyjściowe Ln (Output Voltage Ln)	Napięcie wyjściowe zasilacza dla poszczególnych linii podawane z rozdzielczością 1 V
Prąd wyjściowy Ln (Output Current Ln)	Prąd wyjściowy zasilacza dla poszczególnych linii podawany z rozdzielczością 0.1 A
Częstotliwość wyjściowa (Output Frequency)	Częstotliwość wyjściowa zasilacza podawana z rozdzielczością 0.1 Hz
Moc czynna wyjściowa Ln (Output Active Power Ln)	Wyjściowa moc czynna zasilacza dla poszczególnych linii podawana z rozdzielczością 0.1 kW
Moc pozorna wyjściowa Ln (Output Apparent Power Ln)	Wyjściowa moc pozorna zasilacza dla poszczególnych linii podawana z rozdzielczością 0.1 kVA
Współczynnik mocy wyjściowej PF Ln (Output Power Factor Ln)	Wyjściowy współczynnik mocy dla linii n
Poziom obciążenia wyjścia Ln (Output Load Ln)	Poziom obciążenia zasilacza dla linii n

Parametry wejściowe układu obejściowego BYPASS (Bypass Parameters)

Lista parametrów układu obejściowego mierzonych przez UPS. Dostępne parametry wraz z opisem zestawiono w tabeli 13.



Informacja
Lista dostępnych parametrów jest zależna od modelu UPS i wersji jego protokołu komunikacyjnego.

Tabela 13. Parametry wejściowe układu obejściowego BYPASS

Parametr	Opis
Napięcie wejściowe Ln (Input Voltage Ln)	Napięcie wejściowe układu BYPASS dla poszczególnych linii podawane z rozdzielczością 1 V
Prąd wejściowy Ln (Input Current Ln)	Prąd wejściowy układu BYPASS dla poszczególnych linii podawany z rozdzielczością 0.1 A
Częstotliwość wejściowa (Input Frequency)	Częstotliwość wejściowa układu BYPASS (pomiar dla linii L1) podawana z rozdzielczością 0.1 Hz
Moc czynna wejściowa Ln (Input Active Power Ln)	Wejściowa moc czynna układu BYPASS dla poszczególnych linii podawana z rozdzielczością 0.1 kW
Moc pozorna wejściowa Ln (Input Apparent Power Ln)	Wejściowa moc pozorna układu BYPASS dla poszczególnych linii n podawana z rozdzielczością 0.1 kVA
Współczynnik mocy wejściowej PF Ln (Input Power Factor Ln)	Wejściowy współczynnik mocy układu BYPASS dla linii n

Alarmy (Alarms)

Lista komunikatów i alarmów sygnalizowanych przez UPS.

Komunikaty to ostrzeżenia o zbliżaniu się do wartości krytycznych dla danych parametrów pracy (np. przegrzewanie) oraz informacje o stanie pracy bloków funkcjonalnych urządzenia.

Alarmy to stany awaryjne których wystąpienie uniemożliwia dalszą pracę urządzenia (przekroczenie wartości krytycznych dla danych parametrów pracy, błędy w działaniu bloków funkcjonalnych zasilacza UPS.

Alarmy (Alarms)

Lista sygnalizowanych (aktywnych) stanów alarmowych przez urządzenie. Listę wszystkich możliwych alarmów zestawiono w tabeli 14.

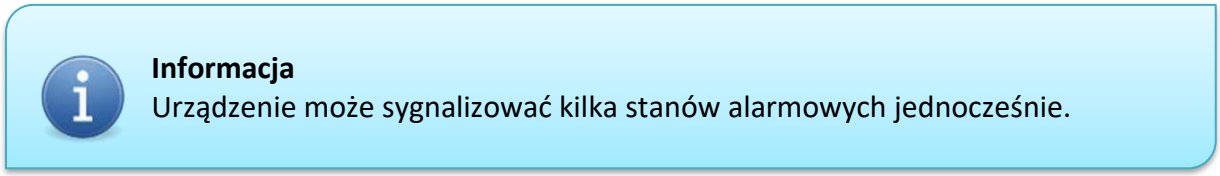


Tabela 14. Lista dostępnych alarmów

Alarm	Opis
Zwarcie na wyjściu zasilacza (Output short circuit)	Zwarcie wyjścia na pracy falownikowej
Przeciążenie wyjścia (Output overload)	Sygnalizacja przeciążenia zasilacza
Nadmierny wzrost temperatury prostownika (Rectifier over temperature)	Sygnalizacja nadmiernego wzrostu temperatury prostownika
Nadmierny wzrost temperatury falownika (Inverter over temperature)	Sygnalizacja nadmiernego wzrostu temperatury falownika
Błąd akumulatora (Battery fault)	Sygnalizacja problemu występującego w obwodzie baterii
Aktywne EPO (EPO active)	Sygnalizacja wywołania stanu awaryjnego wyłączenia zasilania wyjścia (EPO)
Błąd wewnętrzny prostownika (Rectifier internal error)	Błąd wewnętrzny bloku prostownika
Błąd wewnętrzny falownika (Inverter internal error)	Błąd wewnętrzny bloku falownika
Błąd pracy równoległej (Parallel operation fault)	Błąd w systemie jednostek pracujących równolegle powodujący zatrzymanie systemu

Komunikaty (Warnings & Informations)

Lista sygnalizowanych (aktywnych) komunikatów przez urządzenie. Listę wszystkich możliwych komunikatów zestawiono w tabeli 15.

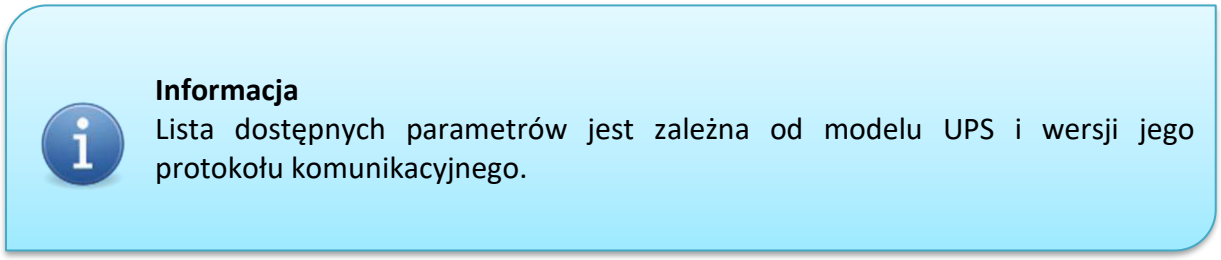
Informacja
Urządzenie może sygnalizować kilka komunikatów jednocześnie.

Tabela 15. Lista dostępnych komunikatów

Komunikat	Opis
Ładowanie baterii (Battery charging)	Sygnalizacja ładowania baterii
Przeciążenie zasilacza (UPS output overload)	Sygnalizacja przeciążenia falownika
Nadmierny wzrost temperatury prostownika (Rectifier over temperature)	Sygnalizacja nadmiernego wzrostu temperatury prostownika
Nadmierny wzrost temperatury falownika (Inverter over temperature)	Sygnalizacja nadmiernego wzrostu temperatury falownika
Oczekiwanie na ładunek minimalny (Waiting for the minimum state of battery charge)	Sygnalizacja oczekiwania na zgromadzenie minimalnego ładunku akumulatora (powyżej wartości ***Minimalny stopień naładowania akumulatorów dla powrotu z trybu STANDBY*** dostępnego w ***UPS: Konfiguracja***)
Stan niskiej baterii (Low battery)	Sygnalizacja stanu niskiej baterii
Serwis (Service)	Sygnalizacja zalecanego przeglądu zasilacza
Bypass (Bypass)	Sygnalizacja fizycznego załączenia elektronicznego układu obejściowego
Brak komunikacji z prostownikiem (Rectifier communication fail)	Sygnalizacja utraty komunikacji z modułem prostownika
Brak komunikacji z falownikiem (Inverter communication fail)	Sygnalizacja utraty komunikacji z modułem falownika
Niepoprawna kolejność faz linii BYPASS (Bypass input phase sequence fail)	Sygnalizacja niepoprawnej kolejności faz linii Bypass
Zasilanie linii BYPASS poza zakresem (Bypass input out of range)	Sygnalizacja braku poprawnego zasilania linii Bypass
Otwarty obwód baterii (Battery open circuit)	Sygnalizacja przerwy w obwodzie baterii
Zasilanie linii podstawowej poza zakresem (Mains input out of range)	Sygnalizacja nieprawidłowych parametrów (napięcie, częstotliwość) dla linii podstawowej
Niepoprawna kolejność faz linii podstawowej (Mains input phase sequence fail)	Sygnalizacja nieprawidłowej kolejności faz dla linii podstawowej
Terminarz aktywny (Scheduler active)	Sygnalizacja aktywności terminarza
Dynamiczna kompensacja mocy biernej (Dynamic reactive power compensation active)	Sygnalizacja aktywności dynamicznej kompensacji mocy biernej

Konfiguracja (Configuration)

Lista nastaw konfiguracyjnych UPS. Dostępne parametry wraz z opisem zestawiono w tabeli 16.



Informacja
Lista dostępnych parametrów jest zależna od modelu UPS i wersji jego protokołu komunikacyjnego.

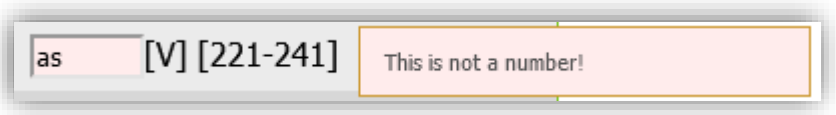
Tabela 16. Parametry konfiguracyjne zasilacza

Parametr	Opis
Napięcie wyjściowe Ln (Output voltage Ln)	Ustawienie wartości napięcia wyjściowego zasilacza dla linii n (zmiana napięcia wyjściowego, po wprowadzeniu zmian wartości parametru podczas falownikowych trybów pracy, nastąpi dopiero po zmianie trybu pracy falownika, np. w wyniku wyłączenia i ponownego załączenia UPS)
Górny próg napięciowy dla linii BYPASS (Bypass voltage upper threshold)	Ustawienie górnego progu kryterium poprawności napięcia dla linii BYPASS
Dolny próg napięciowy dla linii BYPASS (Bypass voltage lower threshold)	Ustawienie dolnego progu kryterium poprawności napięcia dla linii BYPASS
Górny próg częstotliwościowy dla linii BYPASS (Bypass frequency upper threshold)	Ustawienie górnego progu kryterium poprawności częstotliwości dla linii BYPASS
Dolny próg częstotliwościowy dla linii BYPASS (Bypass frequency lower threshold)	Ustawienie dolnego progu kryterium poprawności częstotliwości dla linii BYPASS
Ustawienie czasu opóźnienia przy przechodzeniu do trybu STANDBY (Delay before Standby)	Ustawienie czasu opóźnienia przy przechodzeniu zasilacza do trybu STANDBY przy wymuszonym przez użytkownika przełączeniu; w przypadku stosowania oprogramowania zarządzającego, czas ten powinien być większy od czasu wyłączenia systemu zarządzającego
Minimalny stopień naładowania akumulatorów dla powrotu z trybu STANDBY (Level of minimum state of battery charge)	Ustawienie minimalnego stopnia naładowania, który akumulatory muszą osiągnąć, aby zasilacz uruchomił się po rozładowaniu akumulatorów i powrocie napięcia sieciowego (ładowania akumulatorów)
Poziom obciążenia dla wyjścia z przeciążenia (Output overload clear threshold)	Stopień obciążenia, przy którym zasilacz przestaje sygnalizować przeciążenie
Pojemność zastosowanych akumulatorów (Battery capacity)	Wprowadzenie pojemności zastosowanych akumulatorów
Liczba sekcji akumulatorów (wewnętrznych i zewnętrznych) (Number of battery strings - paralleled)	Wprowadzenie liczby sekcji akumulatorów (suma sekcji akumulatorów wewnętrznych i zewnętrznych)
Całkowity prąd ładowania akumulatorów (Total charging current)	Określenie sumarycznej wielkości prądu ładowania akumulatorów
Adres zasilacza w przypadku pracy równoległej lub redundantnej (Unit address – parallel operation)	Ustawienie adresu zasilacza w przypadku pracy równoległej lub redundantnej. W pracy pojedynczej jednostki należy ustawić 0.
Adres urządzenia w sieci MODBUS (Modbus address)	Ustawienie adresu urządzenia w sieci MODBUS – dostępne w wersji z MODBUS
Pozostały czas autonomii zgłaszania niskiego poziomu baterii (Remaining autonomy time for low battery signaling)	Ustawienie czasu autonomii, przy którym zostanie zgłoszony niski poziom naładowania baterii

Weryfikacja poprawności wprowadzonych danych

Weryfikacja danych następuje po stronie strony www. Podczas kontroli stosowane są następujące kryteria:

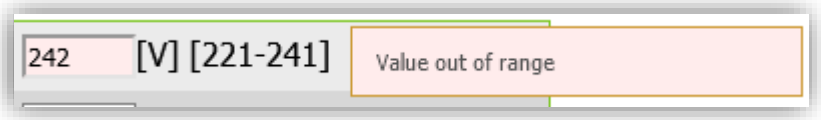
- ✓ Czy parametr jest liczbą?



- ✓ Czy parametr jest liczbą dodatnią?

- ✓ Czy parametr jest liczbą całkowitą?

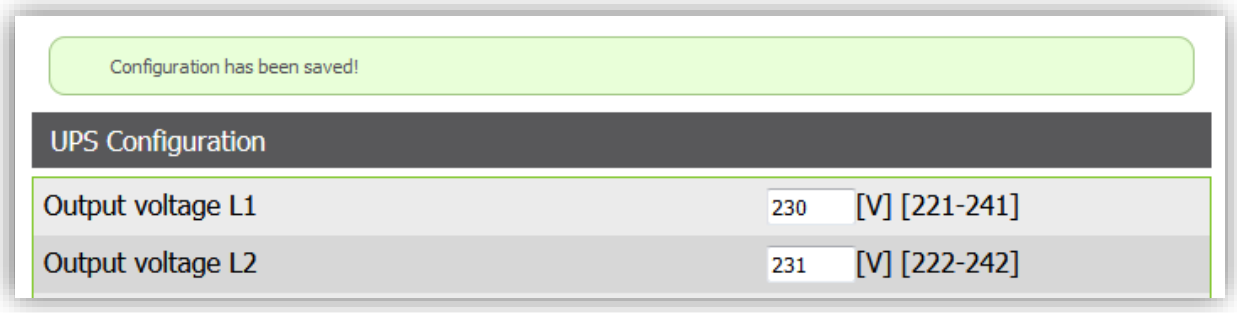
- ✓ Czy parametr znajduje się w dopuszczalnym zakresie?



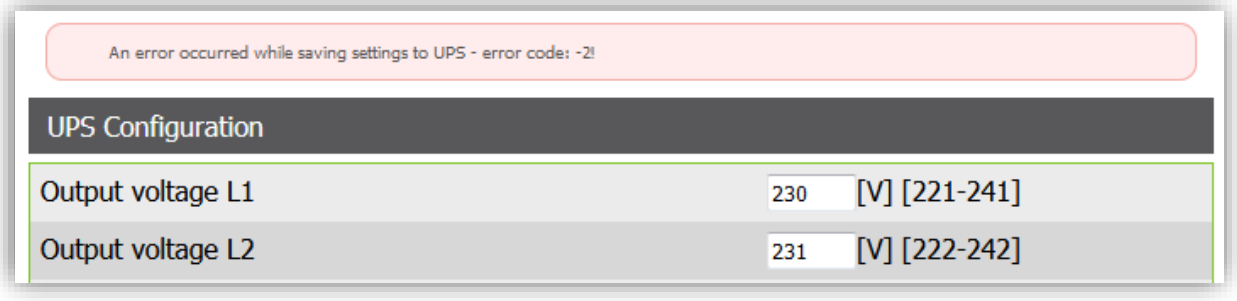
Nieprawidłowa wartość parametru blokuje zapis nastawy do UPS.

Informacja
Zakresy wartości parametrów konfiguracyjnych dostępne są tylko w przypadku, gdy zasilacz udostępnia takie dane. Ich niedostępność spowoduje, że karta pominie etap kontroli zakresu podczas walidacji danych z formularza. Poprawność zakresów nastaw weryfikowana jest wówczas tylko po stronie UPS.

Jeżeli wprowadzone dane są poprawne to po zatwierdzeniu przyciskiem ***Zastosuj*** (***Apply***) nastąpi zapis konfiguracji do UPS. Wynik operacji zapisu zostanie potwierdzony komunikatem o powodzeniu operacji (rys. 4) lub niepowodzeniu, zgłaszając kod błędu (rys. 5).



Rys. 4. Potwierdzenie zapisu konfiguracji UPS



Rys. 5. Komunikat o błędzie podczas zapisu konfiguracji UPS

W tabeli 17 przedstawiono możliwe kody błędów wraz z ich opisem.

Tabela 17. Parametry konfiguracyjne zasilacza

Kod błędu	Opis
-1	Błąd połączenia lub tworzenia zapytania do UPS
-2	Przekroczono czas oczekiwania na synchronizację z UPS
-3	Błąd wysyłania danych do UPS
-4	
-5	Przekroczono czas wysyłania danych do UPS
-8	Zbyt krótka odpowiedź z UPS
-9	Błąd zapisu danych – niepoprawne parametry

Uwaga!
Zmiana parametrów bez zatwierdzenia przyciskiem „Zastosuj” nie wywołuje reakcji w urządzeniu UPS. Przejście na inną stronę karty i powrót do konfiguracji powoduje wyświetlanie aktualnych parametrów pobranych z urządzenia UPS, pomijając zmiany wprowadzone przez użytkownika.

Informacja
Nastawy konfiguracyjne zasilacza przechowywane są w urządzeniu UPS.

Kontrola (Control)

Zarządzanie pracą UPS. Dostępne funkcje wraz z opisem zestawiono w tabeli 18.

Informacja
Lista dostępnych funkcji jest zależna od modelu UPS i wersji jego protokołu komunikacyjnego.

Tabela 18. Zarządzanie pracą UPS

Funkcja	Opis
Sygnalizacja dźwiękowa (Sound signaling)	Włączanie/wyłączanie sygnalizacji akustycznej (stany alarmowe są sygnalizowane zawsze)
Wymuszenie pracy zasilacza w trybie obejściowym (BYPASS) (Bypass mode forcing)	Ręczne wymuszenie trybu pracy BYPASS
Włączenie urządzenia (UPS ON)	Włączanie/wyłączanie zasilacza
Wymuszenie przejścia zasilacza do trybu oczekiwania (STANDBY) (Standby mode forcing)	Ręczne wymuszenie trybu oczekiwania (STANDBY)
Blokada klawiatury (Keyboard lock)	Wymuszenie blokady klawiatury panelu urządzenia
Test akumulatorów (Battery test enable)	Zezwolenie na aktualizację wskaźnika stanu akumulatorów po całkowitym rozładowaniu akumulatorów
Uaktywnienie funkcji EPO (EPO ON)	Aktywacja wejścia i funkcji EPO
Kasowanie stanów awaryjnych prostownika (Rectifier fault clear)	Kasowanie trybu AWARYJNEGO (awaria prostownika)
Kasowanie stanów awaryjnych falownika (Inverter fault clear)	Kasowanie trybu AWARYJNEGO (awaria falownika)
Przełączenie zasilacza w tryb ECO (ECO mode ON)	Przełączenie zasilacza do trybu pracy ECO
Czasowa blokad funkcji EPO (Temporary EPO function deactivation)	Czasowa dezaktywacja (1 min) wejścia EPO
Kontrola parametrów dla linii BYPASS (Bypass check)	Włączenie/wyłączenie kontroli linii BYPASS; parametr automatycznie włączany przy konfiguracji zasilacza do pracy w trybie ECO; kontrola linii BYPASS funkcjonuje jedynie przy włączonym zasilaczu

Zmiana parametrów kontroli pracy następuje poprzez zaznaczenie lub odznaczenie wybranej funkcji i zatwierdzenie zmian przyciskiem ***Zastosuj*** (***Apply***). Potwierdzenie, odrzucenie i kody błędów są identyczne jak w menu ***Konfiguracja*** (***Configuration***) – patrz rys. 4, rys. 5 i tabela 17.

Uwaga!
Zmiana parametrów bez zatwierdzenia przyciskiem „Zastosuj” nie wywołuje reakcji w urządzeniu UPS. Przejście na inną stronę karty i powrót do konfiguracji powoduje wyświetlanie aktualnych parametrów pobranych z urządzenia UPS, pomijając zmiany wprowadzone przez użytkownika.

Informacja
Nastawy konfiguracyjne zasilacza przechowywane są w urządzeniu UPS.

Zdarzenia (Event Log)

Zawiera listę zdarzeń zarejestrowanych przez UPS. Format prezentacji zdarzenia: **Miesiąc / Dzień Godzina:Minuty:Sekundy Zarejestrowane zdarzenie**

Informacja
Data i czas wystąpienia zdarzenia pobierane są z UPS – zależą więc od konfiguracji zegara w urządzeniu.

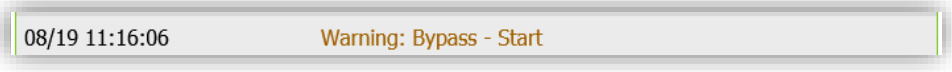
Zdarzenia to zarejestrowane komunikaty, alarmy oraz tryby pracy – z informacją o czasie wystąpienia.

Kolorystyka zdarzeń

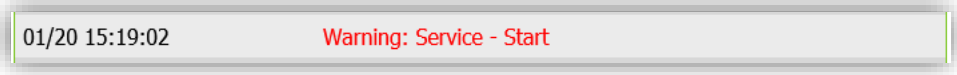
Wszystkie zdarzenia zostały podzielone na 3 grupy:

- Niewymagające interwencji użytkownika – kolor zielony

- Wymagające uwagi – kolor brązowy:



- Wymagające interwencji – kolor czerwony:



KONFIGURACJA KARTY

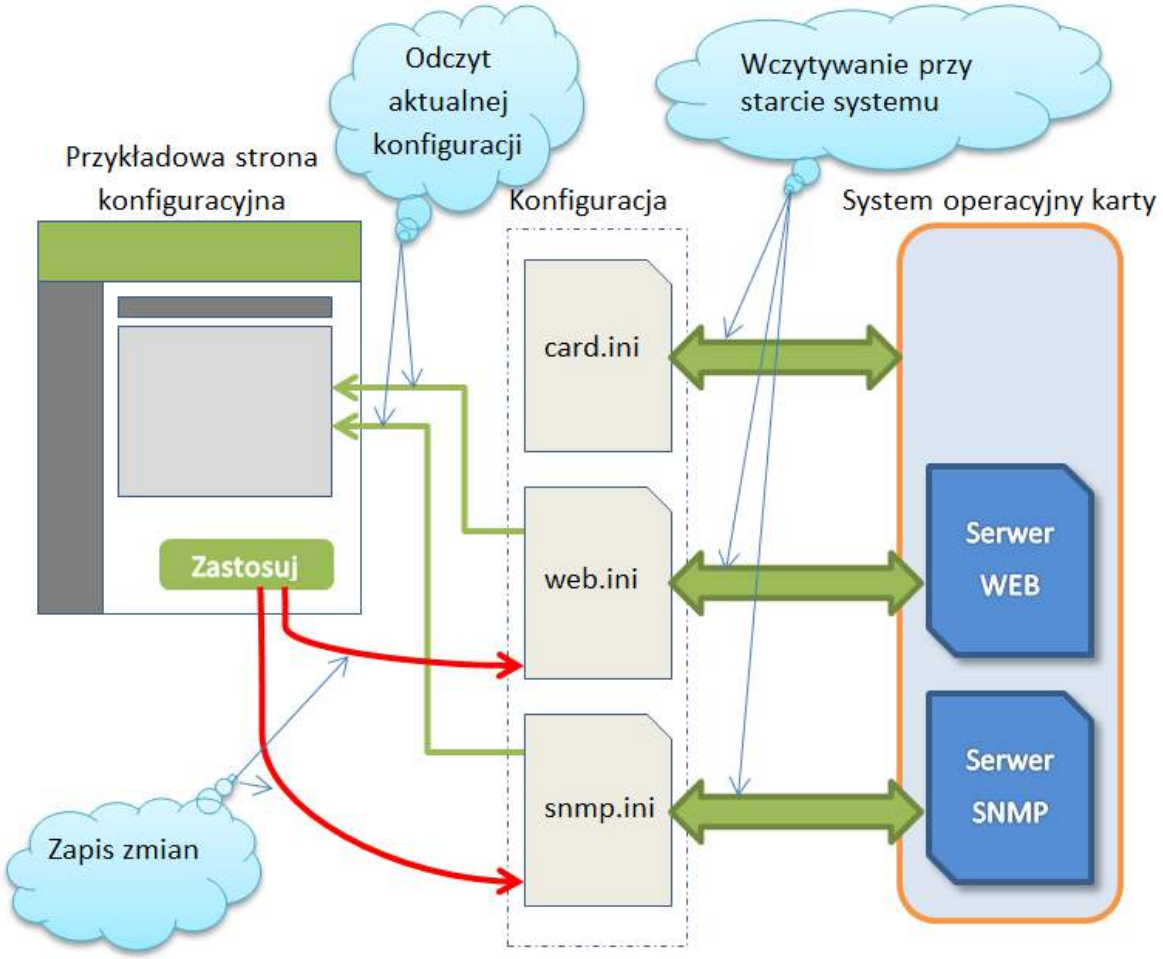
Parametry konfiguracyjne Karty Zarządzającej znajdują się w grupie **Karta (Card)**. Dostęp do konfiguracji możliwy jest tylko z poziomu konta administratora w systemie karty.

Uwaga!
Zmiana parametrów konfiguracyjnych karty może wiązać się z koniecznością jej ponownego uruchomienia. Odbywa się to w sposób automatyczny ale powoduje, że karta przez pewien czas będzie niedostępna w sieci LAN. Niektóre urządzenia monitorujące UPS poprzez SNMP mogą po utracie komunikacji rozpocząć procedurę wyłączania.

Uwaga!
Zmiana niektórych parametrów (takich jak konfiguracja sieciowa, dostępne usługi, porty, loginy i hasła) może doprowadzić do sytuacji, w której karta przestanie być dostępna. Jeżeli zmiany te zostały wprowadzone błędnie możliwe jest przywrócenie konfiguracji domyślnej - więcej informacji w rozdziale PRZYWRACANIE USTAWIEŃ DOMYŚLNYCH.

Wprowadzenie

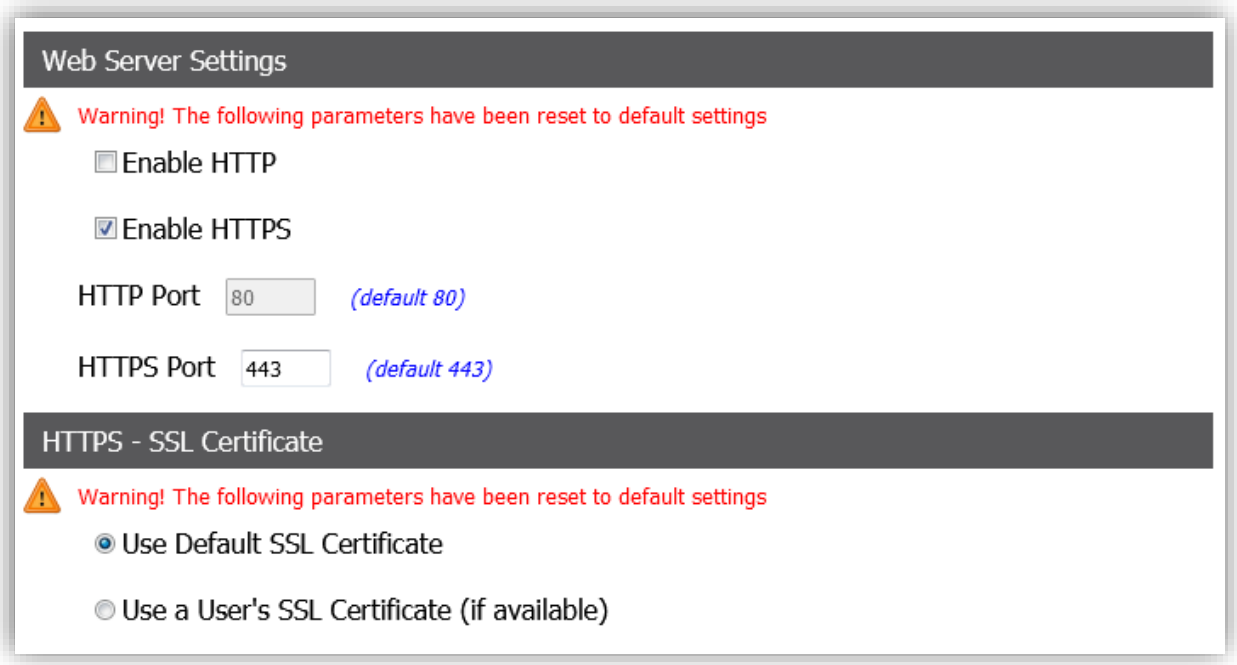
Konfiguracja Karty Zarządzającej przechowywana jest w plikach konfiguracyjnych. Każdy plik zawiera ustawienia dla odrębnego modułu. Nastawy ogólne karty znajdują się w pliku *card.ini*, konfiguracja dla usługi SNMP przechowywana jest w pliku *snmp.ini* a konfiguracja serwera www w pliku *web.ini*. Takie rozwiązanie zapewnia większą elastyczność w zarządzaniu konfiguracją (kopie zapasowe, przenoszenie konfiguracji). Aby lepiej wyjaśnić mechanizm działania systemu konfiguracji posłużono się przykładem obrazującym etap wczytywania nastaw oraz ich modyfikacji za pomocą interfejsu WEB – rysunek 6.



Rys. 6. Działanie systemu konfiguracji Karty Zarządzającej

Cały proces rozpoczyna się w chwili startu systemu operacyjnego karty (jej uruchomienie lub restart). W pierwszym etapie następuje próba załadowania ustawień z plików konfiguracyjnych. Jeżeli załadowanie konfiguracji z danego pliku zakończy się powodzeniem to taka konfiguracja trafia do weryfikacji poprawności nastaw – sprawdzane są m.in. zakresy parametrów, długości nazw, weryfikacja pod kątem występowania niedozwolonych znaków. Po pomyślnym przejściu walidacji konfiguracja aktualnego pliku uznawana jest za poprawną. Następuje przetwarzanie kolejnych plików konfiguracyjnych. Jeżeli na którymkolwiek etapie (wczytywania pliku lub weryfikacji nastaw) wystąpi błąd, to taka konfiguracja uznawana jest za uszkodzoną – wówczas system zastąpi uszkodzony plik konfiguracją domyślną – plik konfiguracyjny zostanie zastąpiony nastawami domyślnymi dla tego pliku i taka konfiguracja będzie używana przez kartę. Etap wczytywania konfiguracji karty kończy się po przetworzeniu wszystkich wymaganych plików konfiguracyjnych – następuje uruchomienie systemu.

Drugi z rozpatrywanych przypadków (rys. 6) ma miejsce wówczas, gdy użytkownik korzystając z interfejsu WEB chce dokonać odczytu aktualnej konfiguracji karty (np. w celu jej modyfikacji lub weryfikacji). Wymagane parametry pozyskiwane są bezpośrednio z odpowiednich plików konfiguracyjnych i prezentowane na stronie konfiguracyjnej. Wspomniano wcześniej, że w przypadku uszkodzenia pliku(ów) konfiguracyjnych ich zawartość (lub po wykonaniu resetu do ustawień fabrycznych - zawartość wszystkich plików konfiguracyjnych) zostanie zapisana wartościami domyślnymi. Użytkownik zostanie poinformowany o tym, które z prezentowanych na stronie konfiguracyjnej nastaw mają wartości domyślne (rys. 7). Należy mieć na uwadze, że informacja o domyślnej nastawie nie jest ustawiana dla każdego parametru ale ustawiana jest dla całego pliku konfiguracyjnego podczas jego resetowania. Użytkownik dokonując zapisu konfiguracji z poziomu interfejsu WEB modyfikuje wszystkie te pliki, z których dana strona konfiguracyjna korzysta. Na rysunku 6 przedstawiono uproszczony schemat konfiguracyjny podobny do tego, jaki występuje w przypadku konfiguracji **Autoryzacja** – tutaj konfiguracja odbywa się dla serwera WEB oraz SNMP jednocześnie – korzystamy więc z dwóch plików i zatwierdzając konfigurację nastąpi zapis w tych plikach. Zapis konfiguracji oznacza akceptację aktualnych nastaw – skasowany zostanie więc znacznik konfiguracji domyślnej dla modyfikowanych plików konfiguracyjnych – ostrzeżenia dla tych plików (nastaw z tych plików) nie będą już wyświetlane.



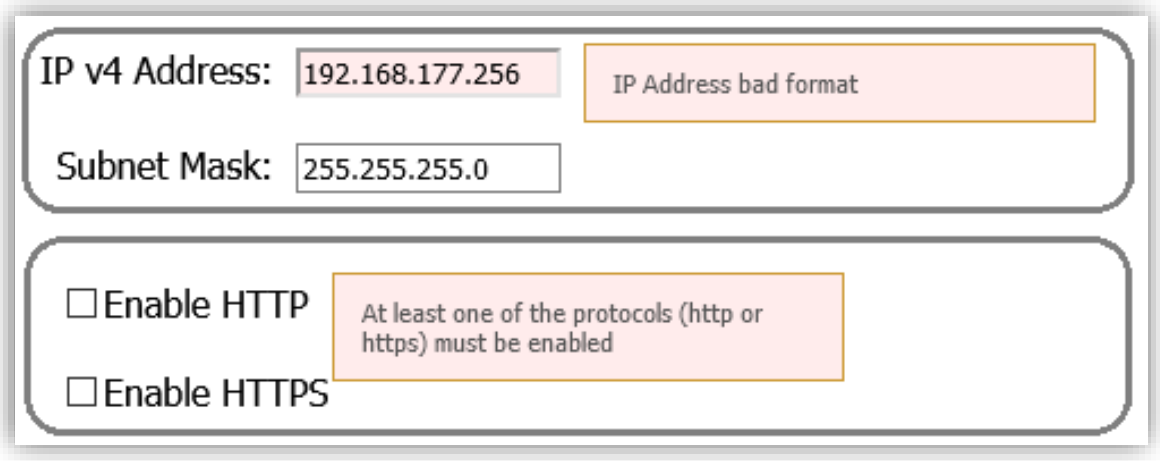
Rys. 7. Ostrzeżenie o przywróceniu wartości domyślnych dla danej grupy parametrów

W ten sposób odbywa się kasowanie ostrzeżeń o domyślnej konfiguracji – poprzez zatwierdzenie nastaw (nie jest wymagana ich zmiana – wystarczy zatwierdzenie). Komunikatów o konfiguracji domyślnej nie można wyłączyć. Będą widoczne zawsze po przywróceniu domyślnej konfiguracji do czasu ich zatwierdzenia.

Uwaga!
Po wystąpieniu ostrzeżeń o przywróceniu nastaw domyślnych zaleca się w pierwszej kolejności przejrzenie stron konfiguracyjnych i zanotowanie, które grupy parametrów zostały objęte konfiguracją domyślną. Dopiero po upewnieniu się, jakie parametry zostały zmienione na domyślne można rozpocząć proces przywracania wymaganych nastaw.

Zatwierdzenie zmian na jednej stronie konfiguracyjnej (np. Autoryzacja) może modyfikować kilka plików konfiguracyjnych jednocześnie (web.ini oraz snmp.ini) – modyfikacja zawartości pliku konfiguracyjnego przez użytkownika powoduje zatwierdzenie całej jego zawartości. Od tej chwili wszystkie ostrzeżenia dla parametrów pochodzących z tego pliku nie będą sygnalizowane.

Zatwierdzenie zmian na stronie konfiguracyjnej rozpoczyna weryfikację poprawności wprowadzonych danych. Składa się ona z dwóch etapów – pierwszy z nich odbywa się po stronie przeglądarki internetowej. Każda napotkana nieprawidłowość będzie sygnalizowana stosownym komunikatem obok parametru, którego komunikat ten dotyczy (rys. 8). Zapisanie danych do karty nastąpi dopiero po pomyślnej weryfikacji pól formularza na stronie konfiguracyjnej.

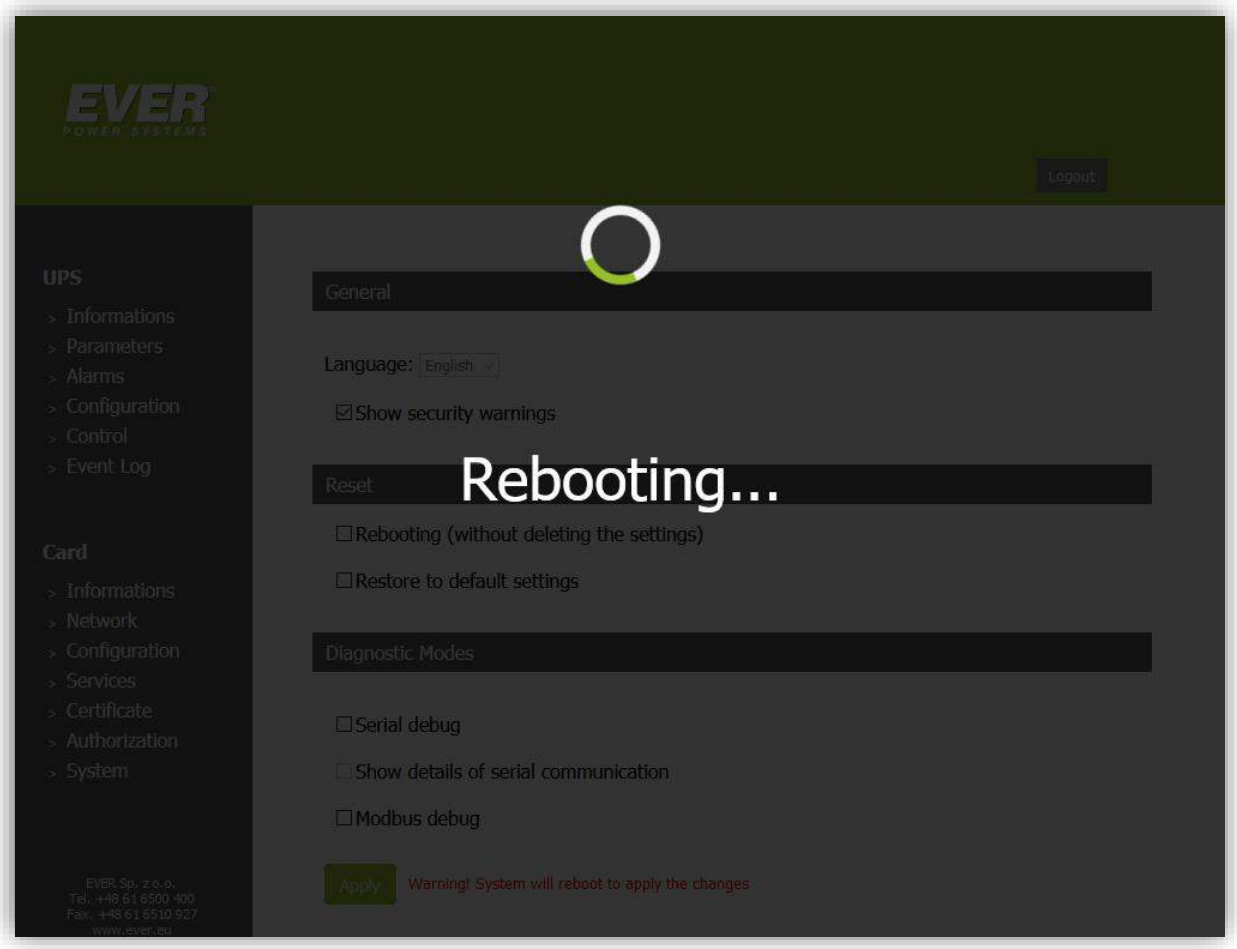


Rys. 8. Walidacja poprawności parametrów – sygnalizacja nieprawidłowej konfiguracji

Drugi etap weryfikacji realizowany jest przez system karty. Jeżeli oba etapy weryfikacji zakończyły się pomyślnie to nastąpi potwierdzenie przyjęcia konfiguracji (rys. 9). W analogiczny sposób sygnalizowane będą błędy wewnętrzne – czerwony kolor tła komunikatu.

Rys. 9. Przykładowy komunikat potwierdzający zapisanie nowej konfiguracji

Większość zmian w konfiguracji karty wymaga jej ponownego uruchomienia. Restart następuje po kilku sekundach od zapisania danych. Karta informuje użytkownika o przebiegu procesu ponownego uruchomienia a po jego zakończeniu automatycznie przeładuje stronę (rys. 10).



Rys. 10. Ponowne uruchamianie systemu karty

Uwaga!
Strona konfiguracyjna karty po restarcie powinna wczytać się automatycznie. Po zmianie adresu IP (używanego do połączenia z serwerem WEB) lub nr-u portu nie będzie to jednak możliwe. W tym przypadku należy odczekać kilkanaście sekund na zakończenie procedury ponownego uruchamiania systemu karty i w pasku adresu przeglądarki prowadzić nowy adres IP karty.

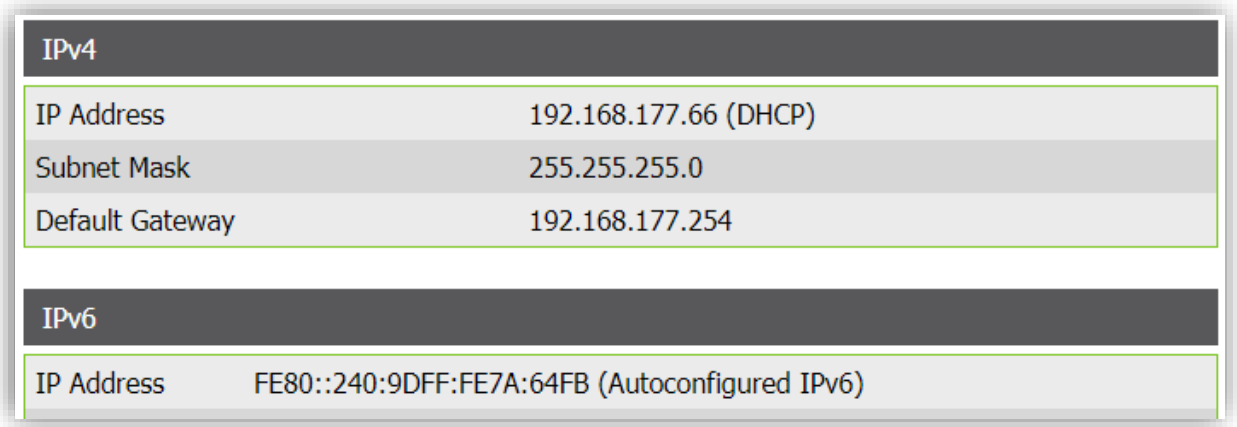
Informacje (Informations)

Zawiera zbiór informacji o Karcie Zarządzającej i jej konfiguracji. Dane zostały podzielone na sekcje. Dostępne parametry opisano w tabeli 19.

Tabela 19. Karta Zarządzająca - informacje

Parametr	Opis
Sekcja Informacje (Informations)	
Wersja firmware SNMP (SNMP Firmware)	Wersja oprogramowania wewnętrznego karty
Adres MAC (MAC Address)	Adres fizyczny interfejsu sieciowego Karty Zarządzającej
Czas pracy (Uptime)	Czas pracy karty (liczony od chwili uruchomienia systemu karty lub jego resetu)
Sekcja IPv4	
Adres IP (IP Address)	Adres(y) IP karty
Maska podsieci (Subnet Mask)	Maska sieci wyznaczająca domenę rozgłoszeniową
Brama domyślna (Default Gateway)	Brama domyślna
Sekcja IPv6	
Adres IP (IP Address)	Adres(y) IP karty
Brama domyślna (Default Gateway)	Brama domyślna
Sekcja Serwery DNS (DNS Servers)	
<DNS IP>	Adresy serwerów DNS dla IPv4 oraz IPv6 – zapisane w formacie IPv6 (adresy IPv4 są mapowane do IPv6 i zapisywane w formacie ::FFFF:adres_ip_v4 – adres 192.168.1.1 będzie zapisany jako ::FFFF:192.168.1.1)

Dla adresów IP prezentowana jest metoda, za pomocą której adres został pozyskany (rys. 11).



Rys. 11. Informacja o aktualnej konfiguracji sieciowej

Listę metod pozyskania adresu przedstawiono w tabeli 20.

Tabela 20. Metody pozyskiwania adresów IP

Metoda	Opis
static	Konfiguracja statyczna (ręczna)
DHCP	Konfiguracja automatyczna (z serwera DHCP)
AUTOIP	APIPA - Automatic Private IP Addressing – mechanizm przydzielający automatycznie adres IP w przypadku niepowodzenia pozyskania adresu z serwera DHCP
Autoconfigured IPv6	Konfiguracja bezstanowa IPv6
DHCPv6	Konfiguracja automatyczna (z serwera DHCPv6)
Static IPv6	Konfiguracja statyczna (ręczna) IPv6

Sieć (Network)

Konfiguracja ustawień sieciowych karty. Składa się z dwóch sekcji: IPv4 oraz IPv6.

Uwaga!
Konfiguracja sieciowa nie jest przechowywana w plikach konfiguracyjnych – nie można jej więc wyeksportować ani przywrócić.

Uwaga!
Po zatwierdzeniu zmian w konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

Konfiguracja IPv4 (IPv4 Settings)

Parametry odpowiedzialne za adresację IPv4 zostały przedstawione w tabeli 21.

Tabela 21. Parametry konfiguracyjne IPv4

Parametr	Opis
Uzyskaj automatycznie adres IP (Obtain an IP address automatically)	Adres IP jest automatycznie pobierany z serwera DHCP
Użyj następującego adresu IP (Use the following IP address)	Konfiguracja ręczna wg zadanych parametrów. Po wybraniu tej opcji uaktywniają się pola do edycji parametrów IPv4
Adres IPv4 (IPv4 Address)	Adres IP
Maska podsieci (Subnet Mask)	Maska sieci wyznaczająca domenę rozgłoszeniową
Brama domyślna (Default Gateway)	Brama domyślna
Główny DNS (Primary DNS)	Adres głównego serwera DNS
Pomocniczy DNS (Secondary DNS)	Adres pomocniczego serwera DNS

Konfiguracja IPv6 (IPv6 Settings)

Parametry odpowiedzialne za adresację IPv6 zostały przedstawione w tabeli 22. W adresacji IPv6 adresy przypisywane są kilkoma metodami. IPv6 w odróżnieniu od IPv4 może posiadać równocześnie kilka adresów dla jednego interfejsu sieciowego. Wyróżniamy tutaj konfigurację bezstanową, ręczną oraz z udziałem serwera DHCPv6.

Informacja
Karta nie zezwala na całkowite wyłączenie IPv6 (ograniczenie systemu operacyjnego karty) – z tego względu opcja ***Włącz IPv6 (konfiguracja bezstanowa)*** jest zawsze aktywna.

Tabela 22. Parametry konfiguracyjne IPv6

Parametr	Opis
Włącz IPv6 (konfiguracja bezstanowa) (Enable IPv6 (Stateless Auto Configuration))	Włączenie obsługi adresu IPv6 – metoda konfiguracji bezstanowej. Parametr jest zawsze włączony
Włącz klienta DHCPv6 (Enable DHCPv6 Client)	Włączenie klienta DHCPv6 – karta pobierze dodatkową konfigurację za pośrednictwem serwera DHCPv6
Użyj następującego konfiguracji statycznej IPv6 (Use the following static IPv6 address)	Umożliwia dodanie dodatkowej konfiguracji statycznej adresu IPv6 – konfiguracja manualna. Po wybraniu tej opcji uaktywniają się pola do edycji parametrów IPv6
Adres IPv6 (IPv6 Address)	Adres IP konfiguracji statycznej jaki zostanie dodany do interfejsu sieciowego
Długość prefiksu (Prefix Length)	Długość prefiksu podsieci
Brama domyślna (IPv6 Gateway)	Brama domyślna dla IPv6

Uwaga!
Zmiana parametrów bez zatwierdzenia przyciskiem „Zastosuj” nie wywołuje zmian w konfiguracji karty SNMP. Przejście na inną stronę karty i powrót do konfiguracji powoduje wyświetlanie aktualnych, pomijając zmiany wprowadzone przez użytkownika.

Uwaga!
Strona www karty po restarcie powinna wczytać się automatycznie. W przypadku zmiany adresu IP (używanego do połączenia z serwerem WEB) nie będzie to jednak możliwe. W tym przypadku należy odczekać kilkanaście sekund na zakończenie procedury ponownego uruchamiania systemu karty i w pasku adresu przeglądarki prowadzić nowy adres IP karty.

Uwaga!
Zmiana niektórych parametrów (takich jak konfiguracja sieciowa, dostępne usługi, porty, loginy i hasła) może doprowadzić do sytuacji, w której karta przestanie być dostępna. Jeżeli zmiany te zostały wprowadzone błędnie możliwe jest przywrócenie konfiguracji domyślnej - więcej informacji w rozdziale PRZYWRACANIE USTAWIEŃ DOMYŚLNYCH.

Konfiguracja (Configuration)

Parametry konfiguracyjne Karty Zarządzającej podzielono na kilka grup funkcjonalnych opisanych poniżej.

Uwaga!
Po zatwierdzeniu zmian w konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

Ogólne (General)

Parametry ogólne dotyczące działania karty. Lista parametrów konfiguracyjnych została przedstawiona w tabeli 23.

Tabela 23. Ogólne parametry konfiguracyjne karty

Parametr	Opis
Język (Language)	Wersja językowa interfejsu WEB karty.
Pokazuj ostrzeżenia bezpieczeństwa (Show security warnings)	Zaznaczenie tej opcji powoduje wyświetlanie komunikatów ostrzegających o konfiguracji uznawanej za niebezpieczną (np. praca na domyślnych hasłach użytkowników).

Informacja
W obecnej wersji oprogramowania karty opcja zmiany języka jest zablokowana. Karta pracuje tylko w angielskiej wersji językowej.

Reset (Reset)

Opcje resetowania i przywracania konfiguracji fabrycznej. Lista parametrów konfiguracyjnych została przedstawiona w tabeli 24.

Tabela 24. Parametry restartu karty

Parametr	Opis
Uruchom ponownie (bez usuwania konfiguracji) (Rebooting (without deleting the settings))	Zaznaczenie tej opcji spowoduje, że po zatwierdzeniu zmian karta uruchomi się ponownie. Nie nastąpi usunięcie aktualnej konfiguracji karty.
Przywróć ustawienia domyślne (Restore to default settings)	Zaznaczenie tej opcji spowoduje, że po zatwierdzeniu zmian karta przywróci konfigurację domyślną. Funkcja jest odpowiednikiem resetu za pomocą przycisku fizycznego RESET.

Tryby diagnostyczne (Diagnostic Modes)

Funkcje użyteczne podczas diagnostyki działania karty. Lista parametrów konfiguracyjnych została przedstawiona w tabeli 25.

Tabela 25. Parametry diagnostyczne karty

Parametr	Opis
Komunikaty diagnostyczne (Serial debug)	Po zaznaczeniu tej opcji karta będzie wysyłała specjalne komunikaty przydatne do diagnozowania problemów z jej działaniem.
Pokaż szczegóły komunikacji szeregowej (Show details of serial communication)	Prezentowane są dodatkowe informacje o przebiegu komunikacji wewnętrznej UPS-Karta. Funkcja dostępna tylko po zaznaczeniu opcji **Komunikaty diagnostyczne**
Komunikaty diagnostyczne Modbus (Modbus debug)	Po zaznaczeniu tej opcji karta będzie wysyłała specjalne komunikaty przydatne do diagnozowania problemów z komunikacją Modbus

Komunikaty diagnostyczne przesyłane są za pomocą pakietów sieciowych – do ich odczytu niezbędne jest oprogramowanie serwisowe.

Informacja
Opcje ***Tryby diagnostyczne*** są trybami serwisowymi i standardowo nie są dostępne dla użytkownika.

Usługi (Services)

Konfiguracja usług uruchomionych na karcie. Parametry konfiguracyjne zostały pogrupowane w sekcje przypisane konkretnej usłudze.

Uwaga!
Po zatwierdzeniu zmian w konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

Ustawienia SNMP (SNMP Settings)

Lista parametrów konfiguracyjnych została przedstawiona w tabeli 26.

Tabela 26. Parametry konfiguracyjne SNMP

Parametr	Opis
Obsługiwane wersje protokołu SNMP (Supported SNMP protocol versions)	Wybór wersji protokołów SNMP obsługiwanych przez kartę. Użytkownik ma możliwość wyboru dowolnej kombinacji protokołów, które będą dopuszczone przez kartę. Odznaczone protokoły będą odrzucane.
Port SNMP (SNMP Port)	Nr portu używanego do komunikacji SNMP. Domyślna wartość: 161 Nr portu musi być z zakresu 1-65534. Port 2362 jest zastrzeżony przez system operacyjny karty.

Usługa SNMP korzysta z kont użytkowników. Konfiguracja użytkowników dla SNMP znajduje się w sekcji **Autoryzacja**. Domyślnie wszystkie konta użytkowników SNMPv3 w systemie są wyłączone. Nie istnieje żaden domyślny użytkownik dla SNMPv3.

Uwaga!
Protokół SNMPv3 wymaga, aby było dostępne przynajmniej jedno konto dla użytkownika SNMPv3 – w przeciwnym razie karta zablokuje SNMPv3 do czasu, aż takie konto nie zostanie utworzone. Więcej o kontach użytkowników opisano w dziale **Autoryzacja**

Uwaga!
Dane przesyłane za pomocą protokołów SNMPv1 oraz SNMPv2c nie są szyfrowane. Zaleca się korzystanie wyłącznie z protokołu SNMPv3. Administrator może zablokować protokoły SNMPv1 oraz SNMPv2c w konfiguracji karty.

Informacja
Protokoły SNMPv1 oraz SNMPv2c są domyślnie wyłączone.

Ustawienia serwera WEB (Web Server Settings)

Lista parametrów konfiguracyjnych została przedstawiona w tabeli 27.

Tabela 27. Parametry konfiguracyjne serwera WEB

Parametr	Opis
Włącz protokół HTTP (Enable HTTP)	Zezwolenie na obsługę protokołu HTTP. Po zaznaczeniu opcji uaktywnia się pole umożliwiające określenie portu, na którym dostępna będzie usługa HTTP
Włącz protokół HTTPS (Enable HTTPS)	Zezwolenie na obsługę protokołu HTTPS. Po zaznaczeniu opcji uaktywnia się pole umożliwiające określenie portu, na którym dostępna będzie usługa HTTPS
Port HTTP (HTTP Port)	Nr portu używanego do komunikacji HTTP. Domyślna wartość:80 Nr portu musi być z zakresu 1-65534 i nie może być taki sam jak port używany do HTTPS
Port HTTPS (HTTPS Port)	Nr porty używanego do komunikacji HTTPS. Domyślna wartość: 443 Nr portu musi być z zakresu 1-65534 i nie może być taki sam jak port używany do HTTP

Usługa WEB korzysta z kont użytkowników. Konfiguracja użytkowników dla WEB znajduje się w sekcji **Autoryzacja**. Domyślne loginy i hasła dla serwisu WEB podano w dziale CHARAKTERYSTYKA KARTY ZARZĄDZAJĄCEJ.

Usługa WEB nie może zostać wyłączona. Przynajmniej jeden z protokołów HTTP lub HTTPS musi być aktywny.

Uwaga!
Dane przesyłane za pomocą protokołu HTTP nie są szyfrowane. Zaleca się korzystanie wyłącznie z protokołu HTTPS. Administrator może wyłączyć obsługę HTTP w konfiguracji karty.

Informacja
Protokół HTTP jest domyślnie wyłączony.

Informacja
Aby za pomocą przeglądarki internetowej połączyć się z serwerem WEB pracującym na niestandardowym porcie należy nr portu określić po dwukropku:
http://192.168.0.1:8080 (dla HTTP na porcie 8080)
https://192.168.0.1:4433 (dla HTTPS na porcie 4433)

Informacja
Aby połączyć się z serwerem WEB poprzez IPv6 należy w pasku adresu przeglądarki wprowadzić adres IPv6 w nawiasach kwadratowych:
http://[FE80::123:45FF:FE67:89AB] (dla HTTP)
https://[FE80::123:45FF:FE67:89AB] (dla HTTPS)

Jeżeli serwer pracuje z niestandardowym portem to port określamy po dwukropku:
http://[FE80::123:45FF:FE67:89AB]:8080 (dla HTTP na porcie 8080)
https://[FE80::123:45FF:FE67:89AB]:4433 (dla HTTPS na porcie 4433)

HTTPS – Certyfikat SSL (HTTPS – SSL Certificate)

Protokół HTTPS wymaga certyfikatu SSL. Karta posiada wbudowany, domyślny, certyfikat SSL. Użytkownik ma możliwość wgrania własnego certyfikatu. Więcej informacji odnośnie certyfikatów opisano w dziale **Certyfikat**. Użytkownik może określić, z jakiego certyfikatu będzie korzystała karta. Dostępne opcje przedstawiono w tabeli 28.

Tabela 28. Konfiguracja HTTPS – wybór certyfikatu

Parametr	Opis
Użyj domyślnego certyfikatu SSL (Use Default SSL Certificate)	Serwer WEB karty będzie wykorzystywał domyślny (wbudowany) certyfikat SSL do komunikacji
Użyj certyfikatu SSL użytkownika (gdy dostępny) (Use a User's SSL Certificate (if available))	Serwer WEB karty będzie wykorzystywał certyfikat użytkownika. W przypadku, gdy certyfikat ten będzie niedostępny (lub uszkodzony) serwer będzie korzystał z certyfikatu domyślnego.

Informacja
Jeżeli wybrano certyfikat użytkownika i jest on niedostępny w systemie, to do czasu jego wgrania karta automatycznie wczyta certyfikat domyślny.

Uwaga!
W przypadku, gdy wczytywanie certyfikatów użytkownika oraz domyślnego zakończy się niepowodzeniem serwer WEB uruchomi się w trybie HTTP (nawet, jeśli HTTP był wyłączony w konfiguracji serwera WEB).

Certyfikat (Certificate)

Certyfikat SSL (*Secure Sockets Layer*) służy do zwiększenia bezpieczeństwa przesyłania informacji pomiędzy serwerem a klientem (przeglądarką internetową). W tym celu wykorzystywane są zaawansowane algorytmy kryptograficzne sprawiające, że transmisja danych odbywa się w sposób bezpieczny i integralny. Wszystkie dane i hasła przesyłane przez sieć są poufne i trafią do odbiorcy w stanie, w jakim zostały nadane (bez możliwości ingerencji w dane). Karta posiada domyślny certyfikat SSL. Oprócz certyfikatu domyślnego użytkownik może wgrać własny certyfikat SSL (wykupiony lub wygenerowany i podpisany samodzielnie – self-signed). Opis generowania i podpisywania własnego certyfikatu opisano w rozdziale **Generowanie certyfikatu SSL**. Certyfikat domyślny nie może zostać usunięty ani podmieniony przez użytkownika. Dostarczany jest wraz z oprogramowaniem wbudowanym karty i tylko w ten sposób może być aktualizowany. Certyfikat SSL używany jest tylko w przypadku, gdy aktywowano obsługę protokołu HTTPS (rozdział **Usługi**).

Uwaga!
Po zatwierdzeniu zmian w konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

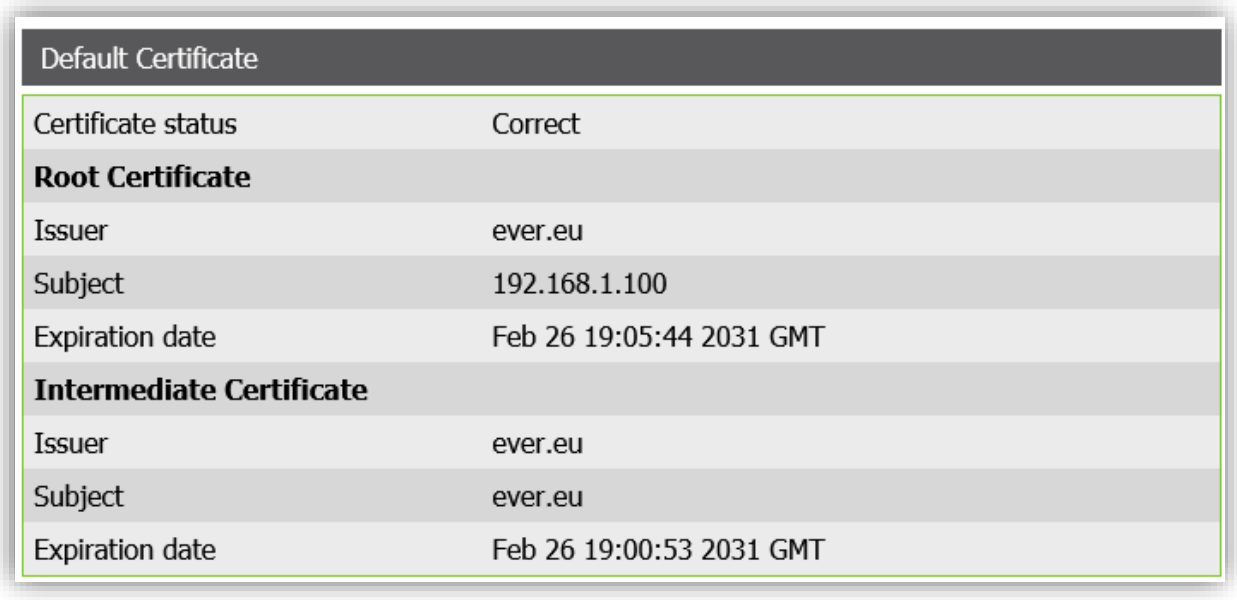
Informacja
Jeżeli wybrano certyfikat użytkownika i jest on niedostępny w systemie, to do czasu jego wgrania karta automatycznie wczyta certyfikat domyślny.

Informacja
Karta akceptuje certyfikaty w formacie PEM z kluczem RSA o długości do 2048 bitów.

Certyfikat domyślny (Default Certificate)

W tej sekcji prezentowane są informacje o certyfikacie domyślnym (wbudowanym w system karty). Certyfikat może zawierać tylko certyfikat główny (Root Certificate) oraz opcjonalnie dodatkowy certyfikat pośredniczący (Intermediate Certificate). Informacje dla tych certyfikatów są jednakowe dlatego w przypadku wystąpienia obu certyfikatów pojawią się

dodatkowe wiersze pozwalające na identyfikację jakiego typu certyfikatu dotyczą (rys. 12).



Rys. 12. Informacje o certyfikacie SSL

Opis parametrów informacyjnych certyfikatu SSL przedstawiono w tabeli 29.

Tabela 29. Certyfikat SSL – parametry informacyjne

Parametr	Opis
Stan certyfikatu (Certificate status)	Informacja o stanie certyfikatu. Listę możliwych wartości wraz z opisem przedstawiono w tabeli 30.
Nazwa wystawcy (Issuer)	Nazwa podmiotu wystawiającego certyfikat
Nazwa podmiotu (Subject)	Nazwa podmiotu dla którego wystawiono certyfikat
Ważność (Expiration date)	Termin ważności certyfikatu

Tabela 30. Certyfikat SSL – stan certyfikatu

Wartość	Opis
Prawidłowy (Correct)	Certyfikat obecny w systemie, prawidłowy. Certyfikat może być używany w systemie.
Nieprawidłowy (Incorrect)	Certyfikat obecny w systemie, nieprawidłowy (uszkodzony). Nie nadaje się do użytku.
Brak (Not found)	Brak certyfikatu.

Certyfikat użytkownika (User Certificate)

W tej sekcji prezentowane są informacje o certyfikacie użytkownika. Certyfikat może zawierać tylko certyfikat główny (Root Certificate) oraz opcjonalnie dodatkowy certyfikat pośredniczący (Intermediate Certificate). Informacje dla tych certyfikatów są jednakowe dlatego w przypadku wystąpienia obu certyfikatów pojawią się dodatkowe wiersze pozwalające na identyfikację jakiego typu certyfikatu dotyczą. Więcej informacji o prezentowanych danych przedstawiono w sekcji **Certyfikat Domyślny** (rys. 12, tabela 29 i 30).

Użytkownik może wgrać własny certyfikat (sekcja **Importuj certyfikat użytkownika**). Przycisk **Usuń certyfikat użytkownika** (**Delete User Certificate**) usuwa certyfikat użytkownika z systemu. Jeżeli wybrano opcję **Użyj certyfikatu SSL użytkownika (gdy dostępny)** w karcie **Usługi** to usunięcie certyfikatu spowoduje, że przy kolejnym uruchomieniu systemu serwer WEB będzie korzystał z certyfikatu domyślnego. Nie ma potrzeby usuwania certyfikatu przed jego podmianą – procedura podmiany certyfikatu użytkownika automatycznie usunie poprzedni certyfikat i zastąpi go nowym.

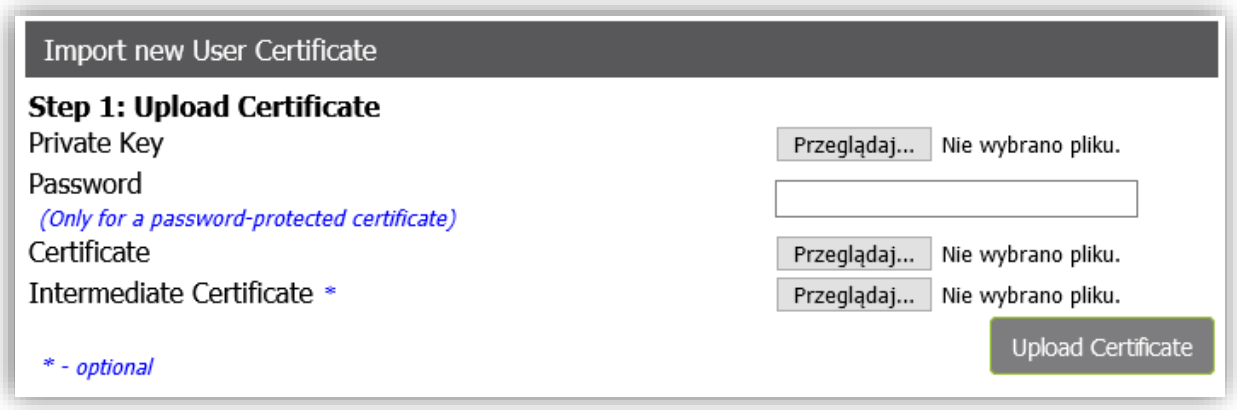
Uwaga!
Certyfikat użytkownika nie jest przechowywany w plikach konfiguracyjnych – nie można go więc wyeksportować a jedyna metoda przywrócenia to wgranie certyfikatu (sekcja **Importuj certyfikat użytkownika**).

Importuj certyfikat użytkownika (Import new User Certificate)

Sekcja służy do wgrywania nowego certyfikatu użytkownika. Procedura importu certyfikatu składa się z trzech kroków:

- **Krok 1: Prześlij certyfikat** (**Step 1: Upload Certificate**)

  Użytkownik wskazuje pliki składowe nowego certyfikatu: klucz prywatny (Private Key), certyfikat główny (Certificate) oraz opcjonalnie certyfikat pośredniczący (Intermediate Certificate). Jeżeli klucz prywatny chroniony jest hasłem, to hasło to należy wprowadzić w pole Hasło (Password). Formularz importu certyfikatu przedstawiono na rys. 13.

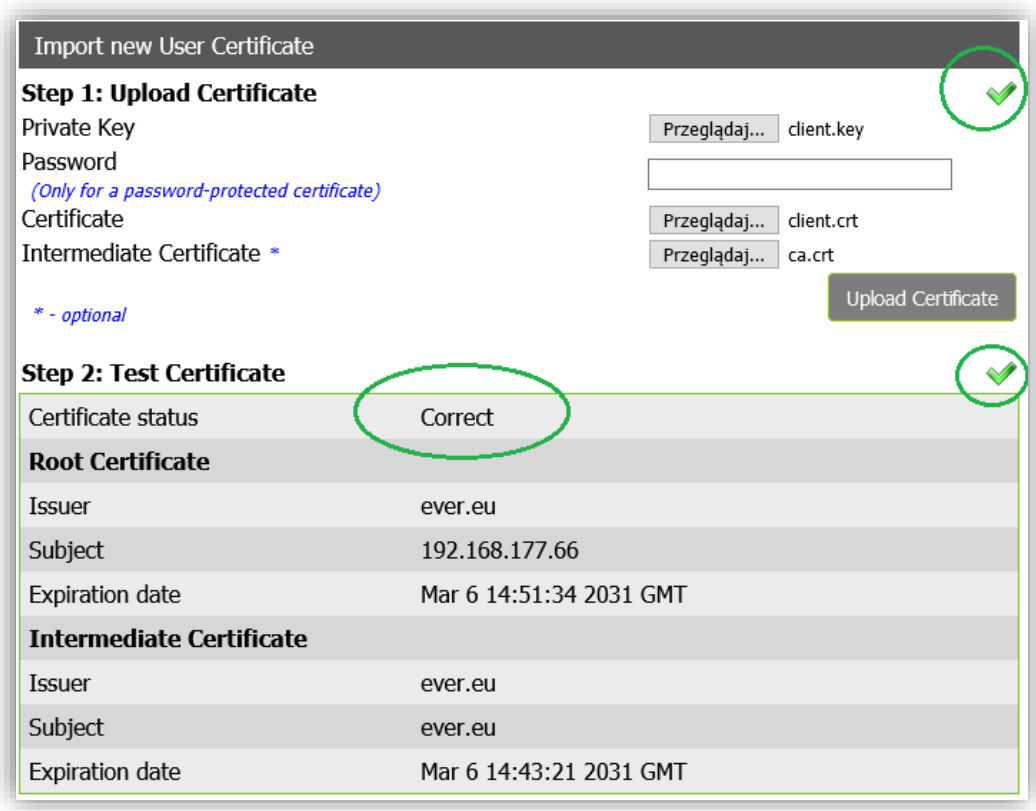


Rys. 13. Formularz importowania certyfikatu użytkownika

Po wskazaniu plików składowych importowanego formularza należy przesłać pliki do karty – przycisk **Wyślij certyfikat** (**Upload Certificate**). Karta po otrzymaniu plików rozpoczyna procedurę weryfikacji certyfikatu.

- **Krok 2: Weryfikacja certyfikatu** (**Step 2: Test Certificate**)

  Karta wykonuje testy przesłanego certyfikatu. Ich wynik prezentowany jest w tabeli. Informacje prezentowane w tabeli opisano dokładniej w sekcji **Certyfikat Domyślny** (rys. 12, tabela 29 i 30) – mają taką samą formę. Jeżeli import certyfikatu zakończy się powodzeniem to krok 1 i 2 będą zaznaczone jako ukończone pomyślnie a pole **Stan certyfikatu** w wyniku będzie miało status **Prawidłowy** (rys. 14).



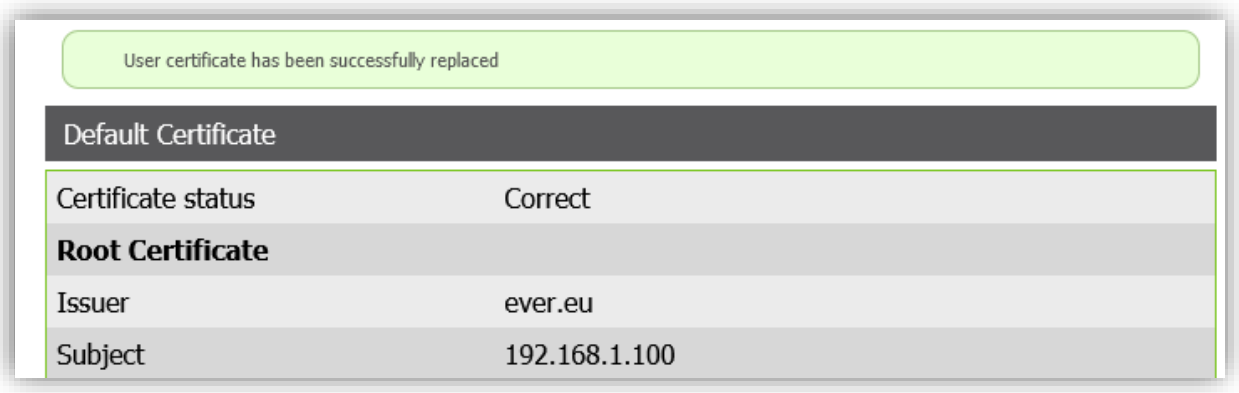
Rys. 14. Import certyfikatu zakończony powodzeniem

Tylko w przypadku udanego importu certyfikatu możliwa jest jego podmiana.

Informacja
Importowany certyfikat użytkownika trafia do lokalizacji tymczasowej w systemie karty. Aby mógł być używany należy wykonać operację podmiany certyfikatu – krok 3.

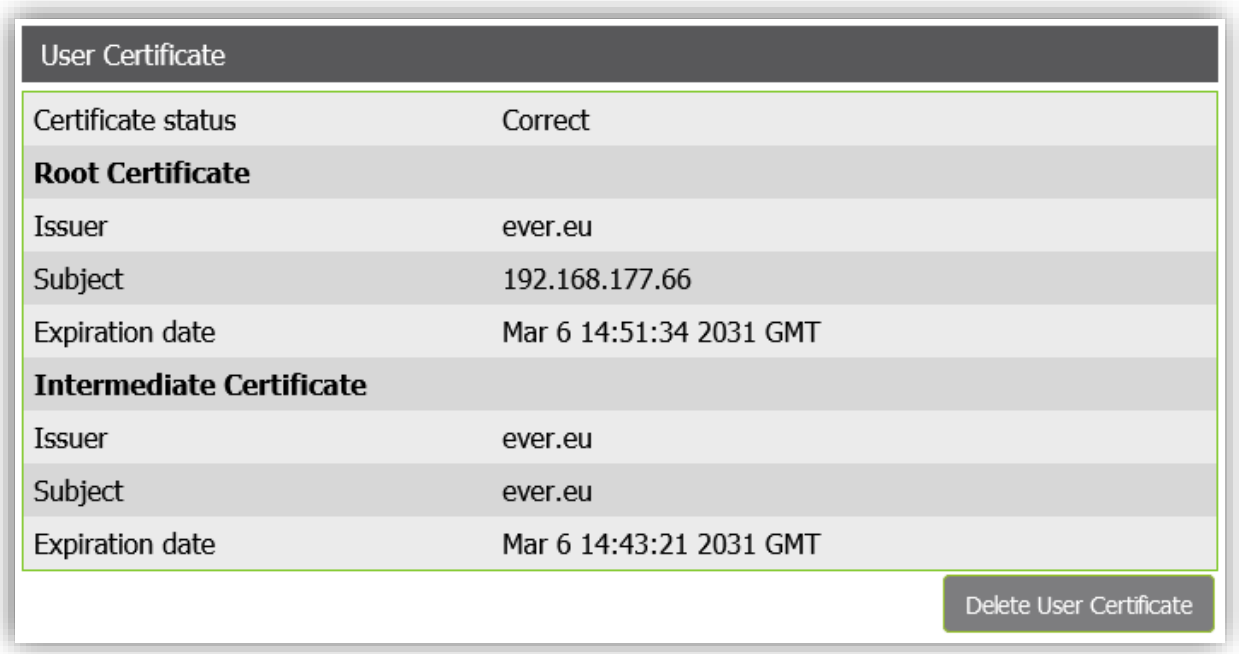
- **Krok 3: Podmiana certyfikatu użytkownika** (**Step 3: Replacing User Certificate**)

  W przypadku, gdy import certyfikatu użytkownika zakończył się powodzeniem (rys. 14) możliwe jest zastąpienie certyfikatu użytkownika w systemie nowym (zaimportowanym) certyfikatem. Zatwierdzenie nowego certyfikatu następuje za pomocą przycisku **Zastąp certyfikat użytkownika** (**Replace User Certificate**). Podmiana certyfikatu zostanie potwierdzona odpowiednim komunikatem (rys. 15) – jeżeli karta została skonfigurowana wcześniej do pracy z certyfikatem użytkownika to nastąpi jej restart.



Rys. 15. Potwierdzenie zastąpienia certyfikatu użytkownika

Nowy certyfikat użytkownika powinien być widoczny w sekcji **Certyfikat użytkownika (User Certificate)** (rys. 16).



Rys. 16. Widok nowego certyfikatu użytkownika po jego pomyślnym zaimportowaniu

Autoryzacja (Authorization)

Dostęp do usług uruchomionych na Karcie Zarządzającej wymaga autoryzacji. Karta posiada dwa konta dla serwisu WEB (jedno tylko do odczytu, drugie z uprawnieniami administracyjnymi), konto dla SNMPv1/v2c oraz 10 kont dla SNMPv3.

Uwaga!
Ze względów bezpieczeństwa nie zaleca się korzystania z domyślnych haseł.

Uwaga!
Zmiana niektórych parametrów (takich jak konfiguracja sieciowa, dostępne usługi, porty, loginy i hasła) może doprowadzić do sytuacji, w której karta przestanie być dostępna. Jeżeli zmiany te zostały wprowadzone błędnie możliwe jest przywrócenie konfiguracji domyślnej - więcej informacji w rozdziale PRZYWRACANIE USTAWIEŃ DOMYŚLNYCH.

Uwaga!
Po zatwierdzeniu zmian w konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

WWW dostęp administracyjny (WWW admin access)

Konto użytkownika o uprawnieniach administracyjnych – zezwala na odczyt i zapis parametrów i konfiguracji do UPS oraz administrowanie Kartą Zarządzającą. Możliwe jest określenie własnej nazwy użytkownika oraz hasła. Parametry autoryzacyjne przedstawiono w tabeli 31.

Tabela 31. Konto użytkownika serwisu WEB

Parametr	Opis
Użytkownik (User)	Nazwa użytkownika dla konta. Wymagania dla nazwy użytkownika: • Długość od 1 do 32 znaków • Niedozwolone jest użycie nazwy „root” • Nazwy użytkowników konta administracyjnego i standardowego muszą być różne • Nazwa użytkownika może zawierać następujące znaki: ○ Litery z zakresu a-z oraz A-Z ○ Cyfry 0-9 ○ Znak _ Pozostałe znaki są niedozwolone
Hasło (Password)	Hasło dla konta. Wymagania dla hasła: • Długość od 1 do 40 znaków • Hasło może zawierać następujące znaki: ○ Litery z zakresu a-z oraz A-Z ○ Cyfry 0-9 ○ Znaki: **~ @ # $ % ^ & * - _ = + { } [ ] ? , . ; |** ○ Znak spacji Pozostałe znaki są niedozwolone
Powtórzone hasło (Repeated password)	Pole zabezpieczające przed wpisaniem błędnego hasła – musi mieć taką samą zawartość co pole **Hasło**

Informacja
Domyślny użytkownik i hasło dla konta administracyjnego:
Użytkownik: ***admin***
Hasło: ***ever***

Uwaga!
Ze względów bezpieczeństwa nie zaleca się korzystania z domyślnych haseł.

WWW dostęp normalny (WWW normal access)

Konto użytkownika o standardowych uprawnieniach – zezwala tylko na odczyt parametrów UPS. Możliwe jest określenie własnej nazwy użytkownika oraz hasła. Parametry autoryzacyjne przedstawiono w tabeli 31.

Informacja
Domyślny użytkownik i hasło dla konta standardowego:
Użytkownik: ***ever***
Hasło: ***ever***

Uwaga!
Ze względów bezpieczeństwa nie zaleca się korzystania z domyślnych haseł.

Autoryzacja SNMP v1/2 (SNMP v1/2 authorization)

Dane autoryzujące dla SNMP w wersji v1 oraz v2c. Znaczenie poszczególnych parametrów opisano w tabeli 32.

Tabela 32. Parametry autoryzujące SNMPv1 oraz SNMPv2c

Parametr	Opis
Public community	Hasło dla notyfikacji tylko do odczytu. Wymagania: • Długość od 1 do 32 znaków • Niedozwolone jest użycie nazwy „root” • Nazwy community ***public*** i ***private*** muszą być różne • Community może zawierać następujące znaki: ○ Litery z zakresu a-z oraz A-Z ○ Cyfry 0-9 ○ Znak _ Pozostałe znaki są niedozwolone
Private community	Hasło dla notyfikacji do odczytu i zapisu. Wymagania takie same jak dla ***Public community***

Informacja
Domyślne wartości dla pól community:
Public (tylko odczyt): ***public***
Private (zapis/odczyt): ***private***

Uwaga!
Ze względów bezpieczeństwa nie zaleca się korzystania z domyślnych haseł.

Uwaga!
Dane przesyłane za pomocą protokołów SNMPv1 oraz SNMPv2c nie są szyfrowane. Zaleca się korzystanie wyłącznie z protokołu SNMPv3. Administrator może zablokować protokoły SNMPv1 oraz SNMPv2c w konfiguracji karty.

Informacja
Protokoły SNMPv1 oraz SNMPv2c są domyślnie wyłączone.

Autoryzacja SNMPv3 (SNMPv3 authorization)

Ustawienia dla kont użytkowników protokołu SNMPv3. Karta nie posiada domyślnych kont – wszystkie konta są domyślnie nieaktywne. SNMPv3 do prawidłowego działania wymaga minimum jednego aktywnego konta użytkownika. W systemie dostępnych jest 10 kont użytkowników. Konta mogą być aktywowane i używane w dowolnej kolejności.

Uwaga!
Po zatwierdzeniu zmian w konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

W tabeli 33 opisano znaczenie poszczególnych parametrów używanych do autoryzacji.

Tabela 33. Parametry autoryzacji SNMPv3

Parametr	Opis
Aktywny (Enable)	Zaznaczenie pola przy danym numerze konta użytkownika powoduje aktywację tego konta. Konta nieaktywne są wyłączone z systemu – nie podlegają też walidacji.
Nazwa użytkownika (User Name)	Nazwa użytkownika dla wybranego konta. Wymagania dla nazwy użytkownika: • Długość od 1 do 32 znaków • Niedozwolone jest użycie nazwy „root” • Nazwy użytkowników dla wszystkich kont SNMPv3 muszą być różne • Nazwa użytkownika może zawierać następujące znaki: ○ Litery z zakresu a-z oraz A-Z ○ Cyfry 0-9 ○ Znak _ Pozostałe znaki są niedozwolone
Uwierzytelnienie (Authentication)	Hasło dla autoryzacji. Wymagania dla hasła: • Długość od 8 do 40 znaków • Hasło może zawierać następujące znaki: ○ Litery z zakresu a-z oraz A-Z ○ Cyfry 0-9 ○ Znaki: **~ @ # $ % ^ & * - _ = + { } [ ] ? , . ; |** ○ Znak spacji Pozostałe znaki są niedozwolone Hasło wymagane tylko w przypadku, gdy wybrano protokół dla uwierzytelnienia.
Uwierzytelnienie: protokół (Authentication: protocol)	Typ protokołu uwierzytelniającego. Możliwe są następujące ustawienia: • ***None*** – uwierzytelnienie wyłączone • ***MD5*** – uwierzytelnienie za pomocą algorytmu HMAC-MD5-96
Prywatność (Privacy)	Hasło do szyfrowania transmisji SNMP. Wymagania dla hasła: • Długość od 8 do 40 znaków • Hasło może zawierać następujące znaki: ○ Litery z zakresu a-z oraz A-Z ○ Cyfry 0-9 ○ Znaki: **~ @ # $ % ^ & * - _ = + { } [ ] ? , . ; |** ○ Znak spacji Pozostałe znaki są niedozwolone Hasło wymagane tylko w przypadku, gdy wybrano protokół dla prywatności.
Prywatność: protokół (Privacy: protocol)	Typ protokołu szyfrującego. Możliwe są następujące ustawienia: • ***None*** – szyfrowanie wyłączone • ***DES*** – szyfrowanie algorytmem CBC-DES
Uprawnienia (Permission)	Określa poziom uprawnień dla wybranego konta użytkownika. Możliwe są następujące ustawienia: • ***No Access*** – całkowity brak uprawnień dla użytkownika • ***Read Only*** – możliwy tylko odczyt parametrów • ***Read/Write*** – pełen dostęp (zapis i odczyt dozwolone)

Uwaga!
SNMPv3 zapewnia wysoki poziom bezpieczeństwa tylko w przypadku, gdy konto korzysta jednocześnie z uwierzytelnienia i szyfrowania.

SNMPv3 może pracować w trzech trybach autoryzacji:

- *noAuthNoPriv* – całkowity brak szyfrowania i autoryzacji. Użytkownik identyfikowany jest wyłącznie po nazwie użytkownika. Aby wybrać ten tryb należy ustawić **Uwierzytelnienie: protokół** na wartość **None** oraz **Prywatność: protokół** na wartość **None**.

  Ze względu na całkowity brak zabezpieczeń tryb ten nie zapewnia żadnego bezpieczeństwa.
- *authNoPriv* – w tym trybie użytkownik podlega autoryzacji za pomocą hasła. Brak szyfrowania powoduje jednak, że dane przesyłane są w sposób jawny. Aby wybrać ten tryb należy ustawić **Uwierzytelnienie: protokół** na wartość **MD5** oraz **Prywatność: protokół** na wartość **None**.

  Tryb ten nie jest zalecany ze względów bezpieczeństwa.
- *authPriv* – tryb zapewniający autoryzację użytkownika za pomocą hasła oraz pełne szyfrowanie transmisji. Aby wybrać ten tryb należy ustawić **Uwierzytelnienie: protokół** na wartość **MD5** oraz **Prywatność: protokół** na wartość **DES**.

  Ten tryb pracy zapewnia najwyższy poziom bezpieczeństwa i z tego powodu jest zalecany.

System (System)

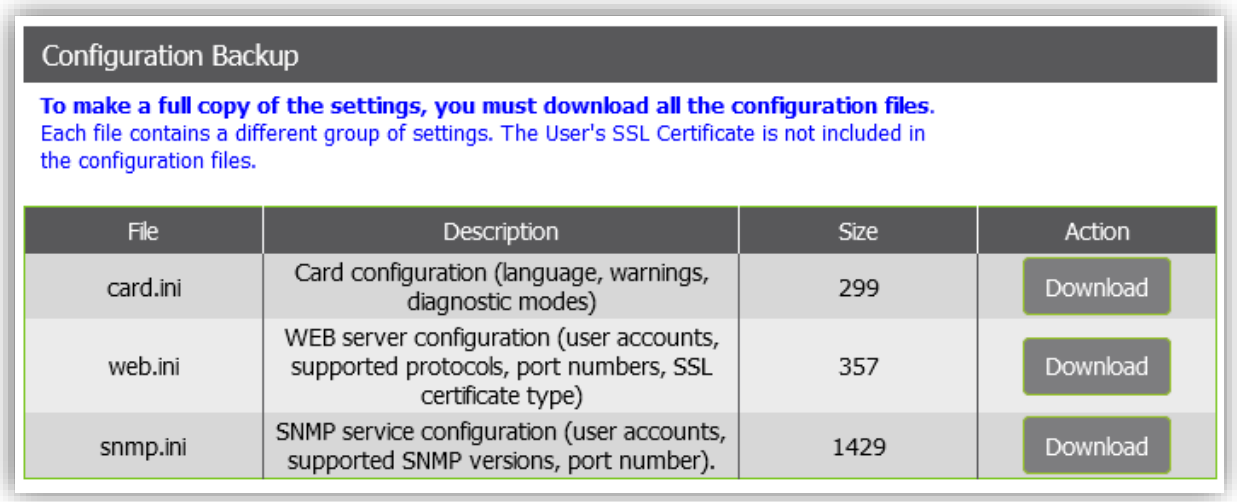
Karta Zarządzająca umożliwia tworzenie kopii zapasowej dla konfiguracji karty. Pliki konfiguracyjne mogą być w łatwy sposób przenoszone między innymi kartami.

Uwaga!
Kopia zapasowa konfiguracji dotyczy tylko nastaw Karty Zarządzającej.
Konfiguracja UPS przechowywana jest w zasilaczu i nie podlega kopii zapasowej.

Użytkownik ma możliwość samodzielnej aktualizacji oprogramowania wbudowanego Karty Zarządzającej – czynność tę wykonuje się z poziomu przeglądarki internetowej.

Kopia zapasowa konfiguracji (Configuration Backup)

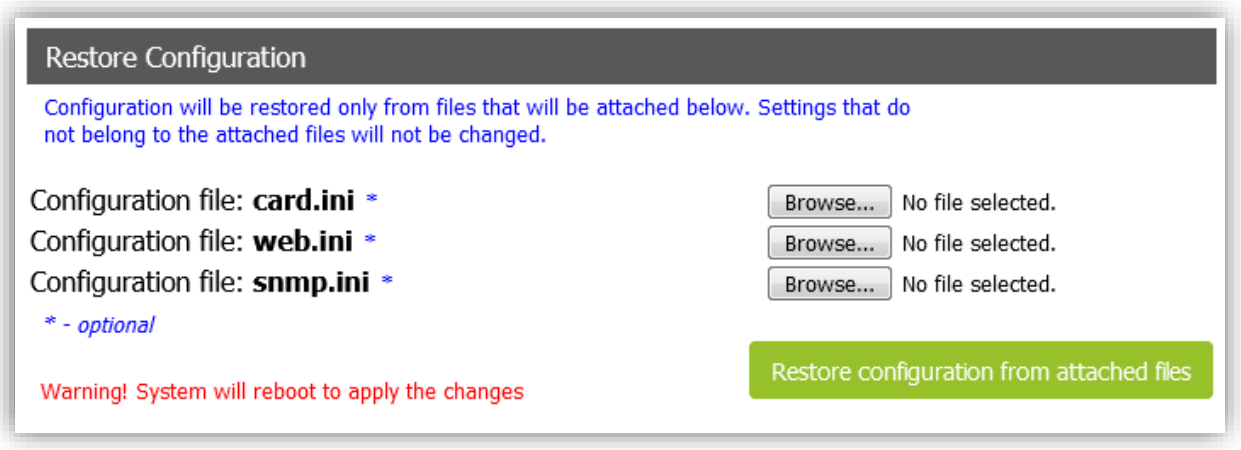
W tabeli znajduje się lista dostępnych plików konfiguracyjnych wraz z opisem za jakie funkcje odpowiadają (rys. 17). Aby wykonać pełną kopię zapasową należy pobrać wszystkie dostępne pliki konfiguracyjne.



Rys. 17. Wykonywanie kopii zapasowej konfiguracji

Przywracanie konfiguracji (Restore Configuration)

Możliwe jest przywrócenie dowolnego pliku lub kilku plików jednocześnie. W formularzu należy załączyć odpowiednie pliki konfiguracyjne i zatwierdzić przyciskiem **Przywróć konfigurację z wybranych plików** (**Restore configuration from attached files**). System weryfikuje poprawność nazw plików dlatego niedozwolona jest zmiana nazw plików konfiguracyjnych. Po przesłaniu plików do karty następuje weryfikacja ich poprawności. Wykrycie błędu w konfiguracji danego pliku (np. parametr poza zakresem, niedozwolone nazwy, znaki) powoduje odrzucenie całego pliku konfiguracyjnego. Wyjątkiem jest plik *snmp.ini* w którym lista użytkowników SNMPv3 traktowana jest odrębnie – wystąpienie błędu w konfiguracji danego użytkownika spowoduje, że ten konkretny użytkownik zostanie wyzerowany i wyłączony. Formularz importu konfiguracji przedstawiono na rys. 18.



Rys. 18. Przywracanie kopii zapasowej konfiguracji

Należy mieć na uwadze, że modyfikowana będzie tylko ta konfiguracja, której pliki załączono do formularza. Pozostałe (brakujące) pliki pozostaną nienaruszone.

Uwaga!
Po przywróceniu konfiguracji karty konieczne będzie jej ponowne uruchomienie. Restart karty następuje w sposób automatyczny.

Wszystkie pliki które zostały przesłane do karty muszą być prawidłowe. Wystąpienie błędu w dowolnym pliku spowoduje odrzucenie całej wysłanej konfiguracji.

Aktualizacja oprogramowania (Firmware Update)

Użytkownik ma możliwość samodzielnej aktualizacji oprogramowania karty.

Uwaga!
Przed aktualizacją oprogramowania wbudowanego Karty Zarządzającej zaleca się wykonanie pełnej kopii zapasowej konfiguracji.

Uwaga!
Podczas aktualizacji oprogramowania karta będzie niedostępna przez cały czas trwania procedury aktualizującej. Niektóre urządzenia monitorujące UPS poprzez SNMP mogą po utracie komunikacji rozpocząć procedurę wyłączania.

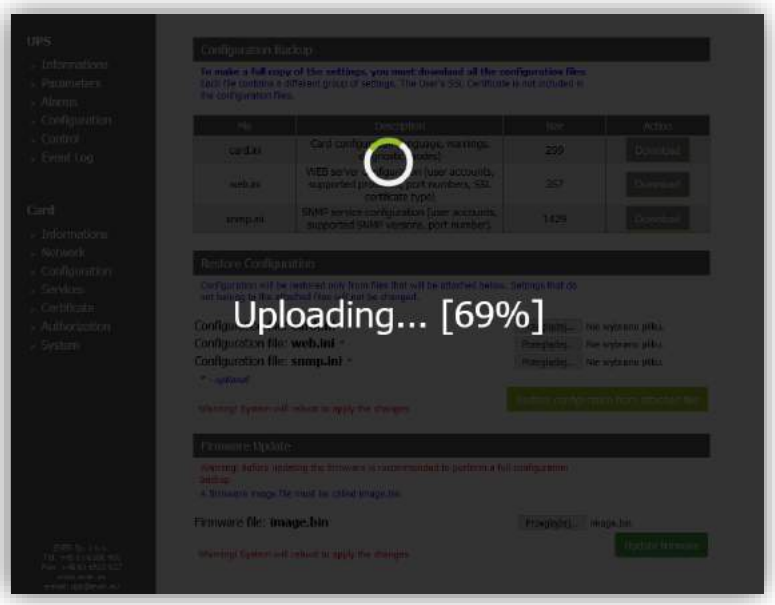
Uwaga!
Przed rozpoczęciem procedury aktualizacji (przed wybraniem pliku z obrazem firmware) należy zatwierdzić aktualizację przyciskiem **Aktualizuj firmware** (**Update firmware**) – w przeciwnym razie system operacyjny karty zerwie połączenie podczas przesyłania pliku z obrazem firmware. Ważne, aby zatwierdzenie nastąpiło bez załącznika w polu **Plik z firmware** (**Firmware file**).

Po tej czynności karta będzie przez chwilę sygnalizowała przesyłanie pliku i jego sprawdzanie po czym procedura zostanie przerwana – jest to normalne zachowanie karty.

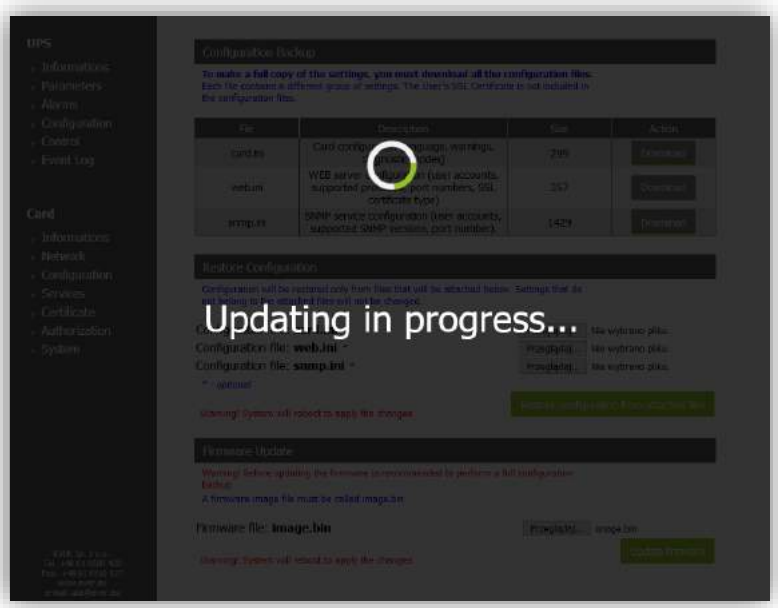
Uwaga!
Opisana procedura dotyczy karty z oprogramowaniem w wersji 2.0 i nowszym. Starsza wersja firmware posiada odmienny interfejs i procedura aktualizacji została opisana w rozdziale **Aktualizacja karty z firmware < 2.0**

Plik z obrazem oprogramowania wewnętrznego karty musi mieć nazwę ***image.bin*** – wielkość znaków ma znaczenie w nazwie pliku. Po wskazaniu pliku z firmware należy zatwierdzić aktualizację przyciskiem **Aktualizuj firmware** (**Update firmware**) – rozpocznie się etap aktualizacji oprogramowania wewnętrznego. Składa się on z kilku etapów:

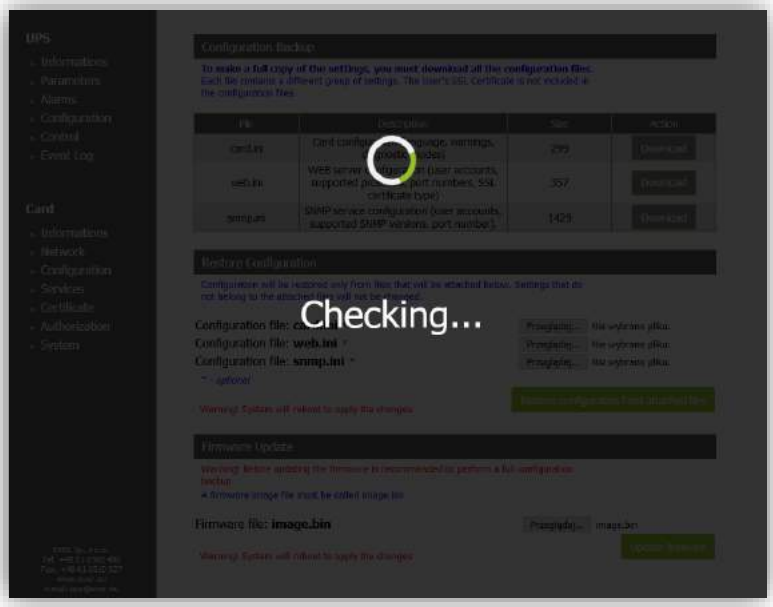
- Przesyłanie pliku obrazu do karty:



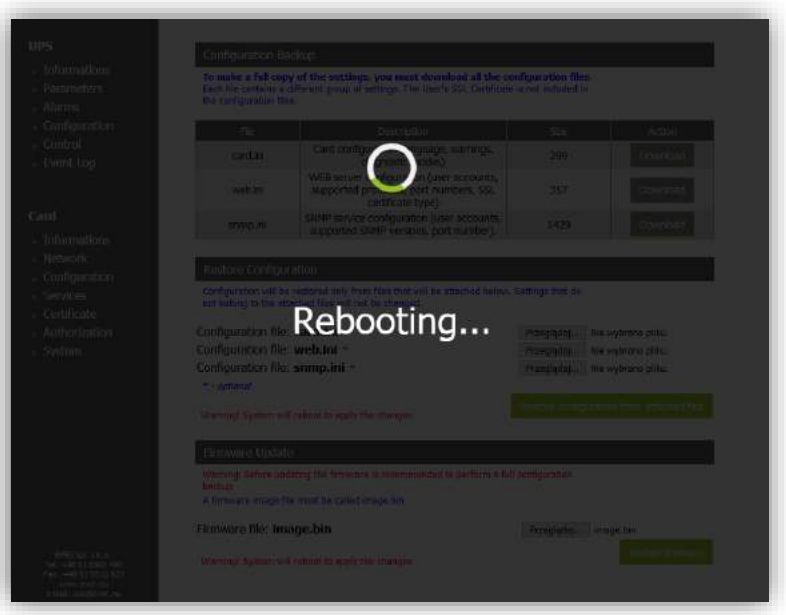
- Aktualizacji karty:



- Weryfikacji poprawności obrazu firmware:



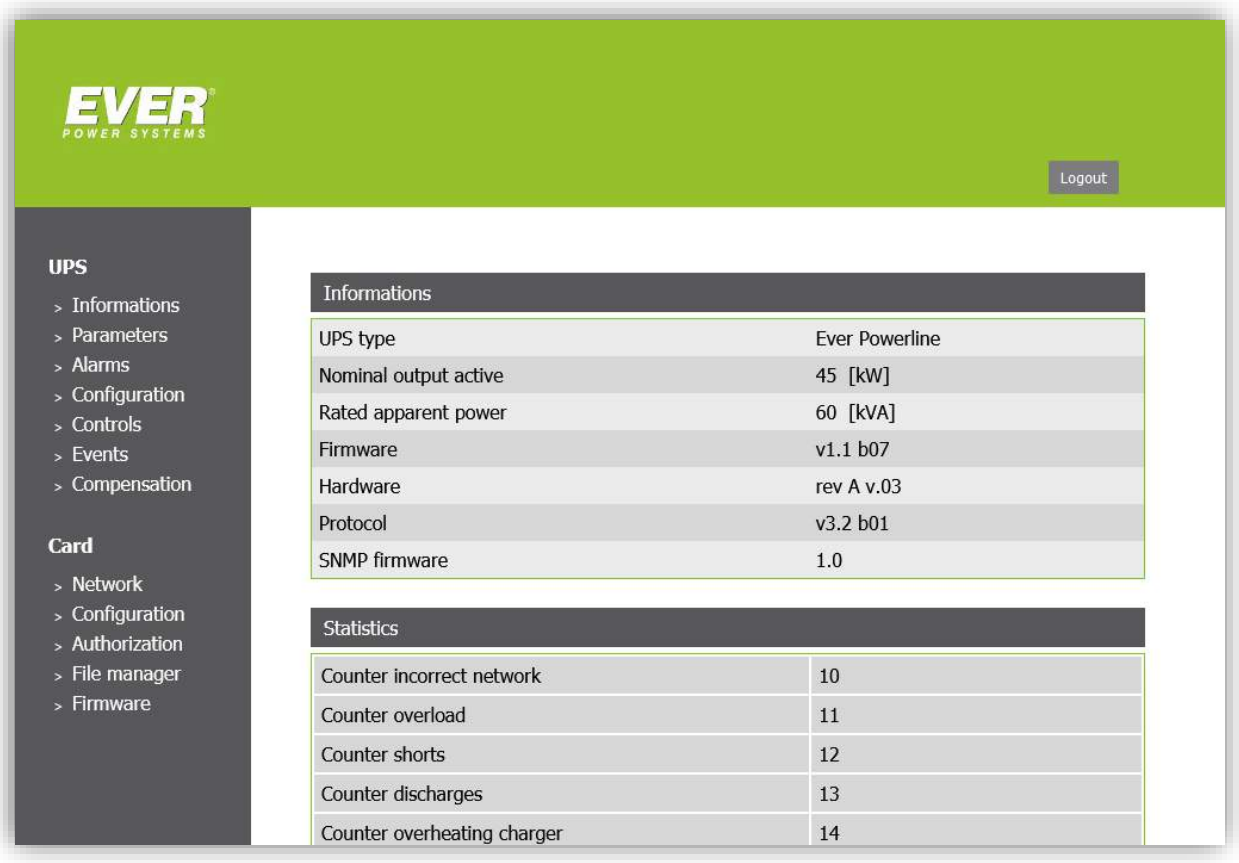
- Ponownego uruchomienia systemu karty:



Po pomyślnym zakończeniu aktualizacji karta uruchomi się ponownie i nastąpi automatyczne przeładowanie strony www karty.

Aktualizacja karty z firmware < 2.0

Aktualizacja karty z firmware w wersji poniżej 2.0 przebiega w podobny sposób jednak ze względu na odmienny interfejs wymaga odrębnego omówienia.



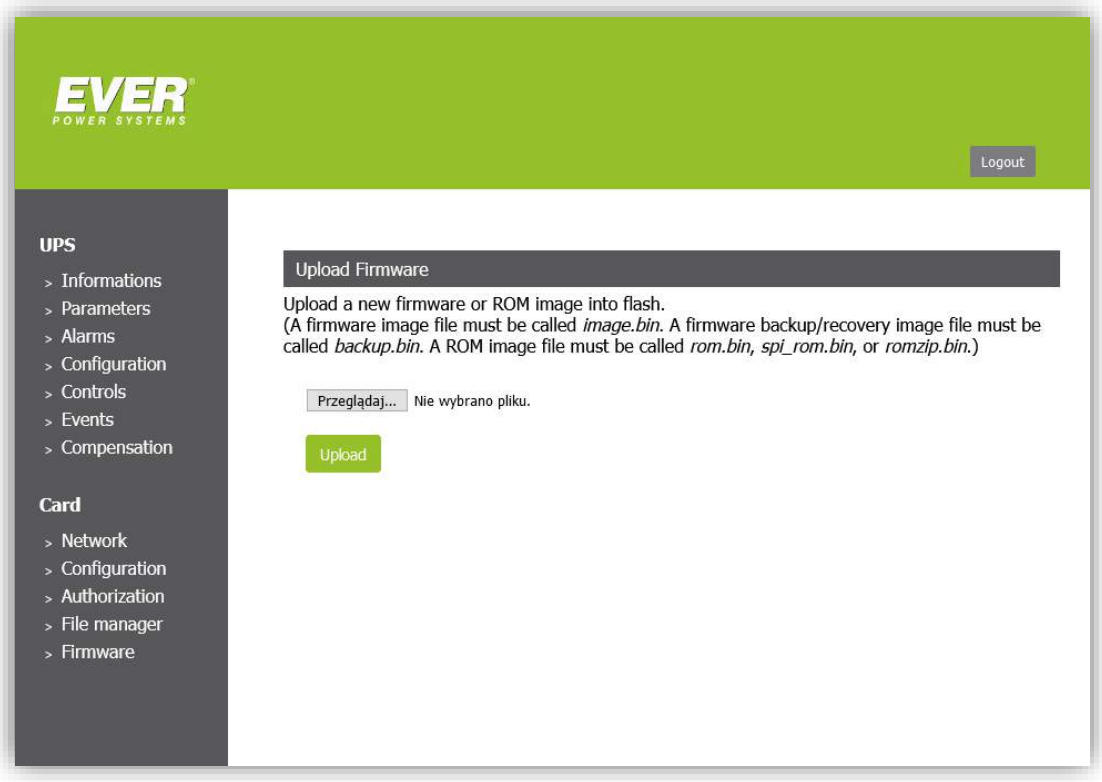
Aktualizacja oprogramowania dostępna jest z poziomu menu **Karta** (**Card**) -> **Firmware**.

Uwaga!
Podczas aktualizacji oprogramowania karta będzie niedostępna przez cały czas trwania procedury aktualizującej. Niektóre urządzenia monitorujące UPS poprzez SNMP mogą po utracie komunikacji rozpocząć procedurę wyłączania.

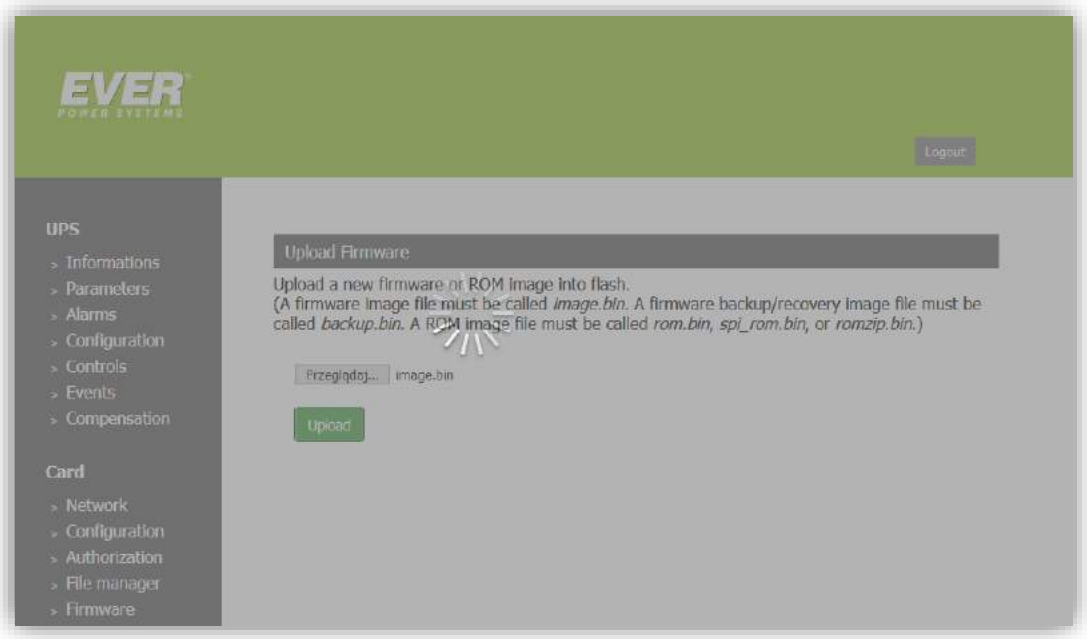
Uwaga!
Przed rozpoczęciem procedury aktualizującej (przed wybraniem pliku z obrazem firmware) należy zatwierdzić aktualizację przyciskiem **Wyślij** (**Upload**) – w przeciwnym razie system operacyjny karty zerwie połączenie podczas przesyłania pliku z obrazem firmware. Ważne, aby zatwierdzenie nastąpiło bez załączonego pliku firmware.

Po tej czynności karta będzie przez chwilę sygnalizowała przesyłanie po czym procedura zostanie przerwana – jest to normalne zachowanie karty.

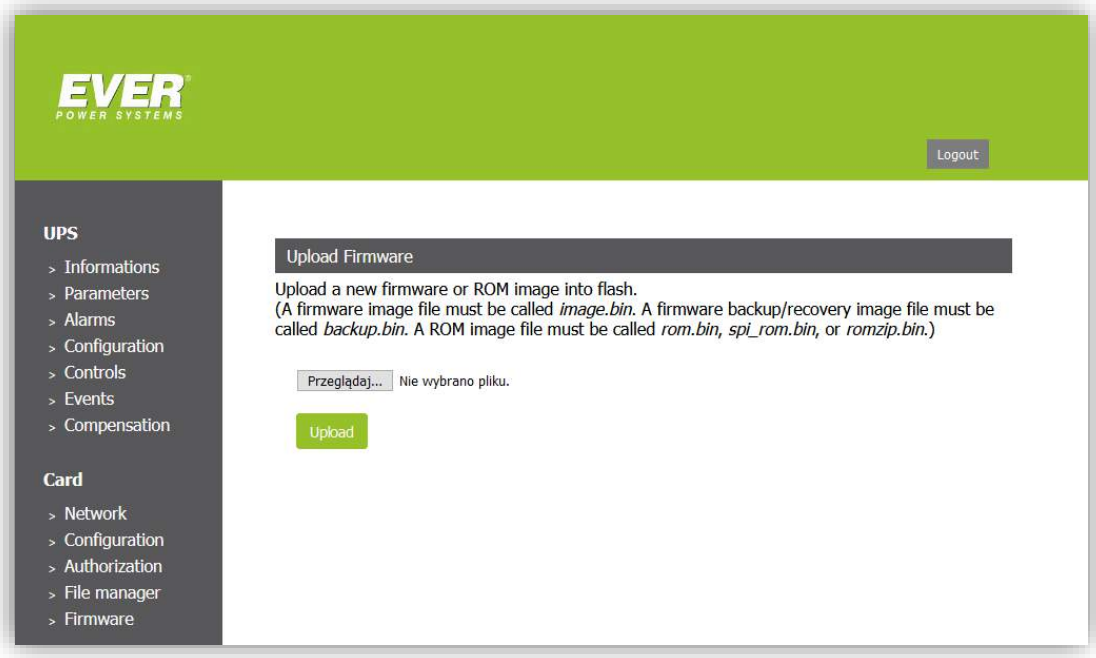
Strona aktualizacji firmware wygląda jak poniżej:



Plik z obrazem oprogramowania wewnętrznego karty musi mieć nazwę ***image.bin*** – wielkość znaków ma znaczenie w nazwie pliku. Po wskazaniu pliku z firmware należy zatwierdzić aktualizację przyciskiem **Wyślij** (**Upload**) – rozpocznie się etap aktualizacji oprogramowania wewnętrznego. Użytkownik będzie informowany tylko o procesie wysyłania pliku do karty:



Po zakończeniu wysyłania pliku animacja zostanie wyłączona i ukaże się podstrona aktualizująca:



Należy odczekać kilka sekund i dokonać odświeżenia strony www – po kilkunastu sekundach strona powinna się załadować a karta będzie pracowała z firmware w wersji, jaka została użyta do aktualizacji.

GENEROWANIE CERTYFIKATU SSL

Użytkownik może samodzielnie wygenerować i podpisać certyfikat SSL na potrzeby serwera HTTPS w Karcie Zarządzającej.

Niniejszy opis dotyczy generowania i podpisywania certyfikatu SSL z wykorzystaniem oprogramowania OpenSSL (www.openssl.org). Aby możliwie uprościć przygotowanie środowiska do pracy z OpenSSL zdecydowano wykorzystać system operacyjny Linux. W tym konkretnym przykładzie jest to dystrybucja Debian 10.8 (www.debian.org). Pakiet OpenSSL jest już domyślnie zainstalowany w tym systemie.

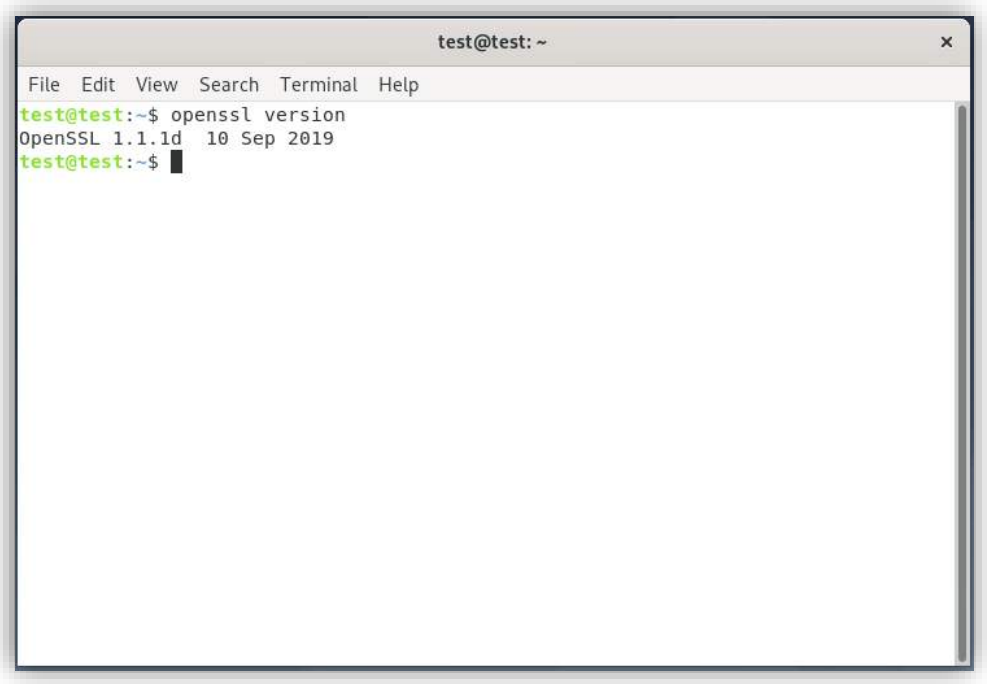
Informacja
Karta akceptuje certyfikaty w formacie PEM z kluczem RSA o długości do 2048 bitów.

Generowanie certyfikatu składa się z dwóch etapów. Pierwszy z nich to wygenerowanie własnego CA (jednostki certyfikującej). Drugi etap to wygenerowanie certyfikatu i podpisanie wygenerowanym wcześniej CA.

Wszystkie poniższe czynności przeprowadza się z wiersza poleceń. Należy upewnić się, że pakiet OpenSSL jest dostępny – wydajemy polecenie

```
openssl version
```

Jeżeli pakiet jest dostępny to w odpowiedzi ukaże się zainstalowana wersja:



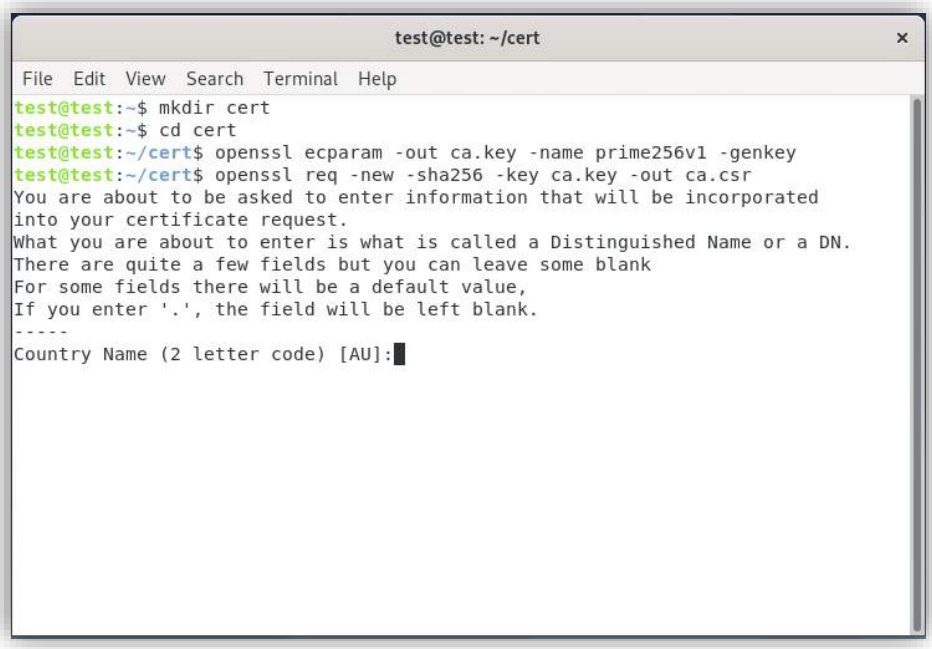
Certyfikat będzie generowany w katalogu „cert” – tworzymy katalog i przechodzimy do niego:

```
mkdir cert
cd cert
```

Wszystkie polecenia wykonujemy wewnątrz tego katalogu.

W pierwszej kolejności należy utworzyć certyfikat CA (jednostki certyfikującej).

1. Generujemy klucz prywatny dla CA (ce.key):
   ```
   openssl ecparam -out ca.key -name prime256v1 -genkey
   ```
2. Generujemy żądanie utworzenia CA (ca.csr)
   ```
   openssl req -new -sha256 -key ca.key -out ca.csr
   ```



Po wydaniu tego polecenia należy wprowadzić dodatkowe dane:

- Country Name (2 letter code) [AU]

  PL *(kod kraju)*
- State or Province Name (full name) [Some-State]

  Greater Poland *(województwo)*
- Locality Name (eg, city) []

  Poznan *(miasto)*
- Organization Name (eg, company) [Internet Widgits Pty Ltd]

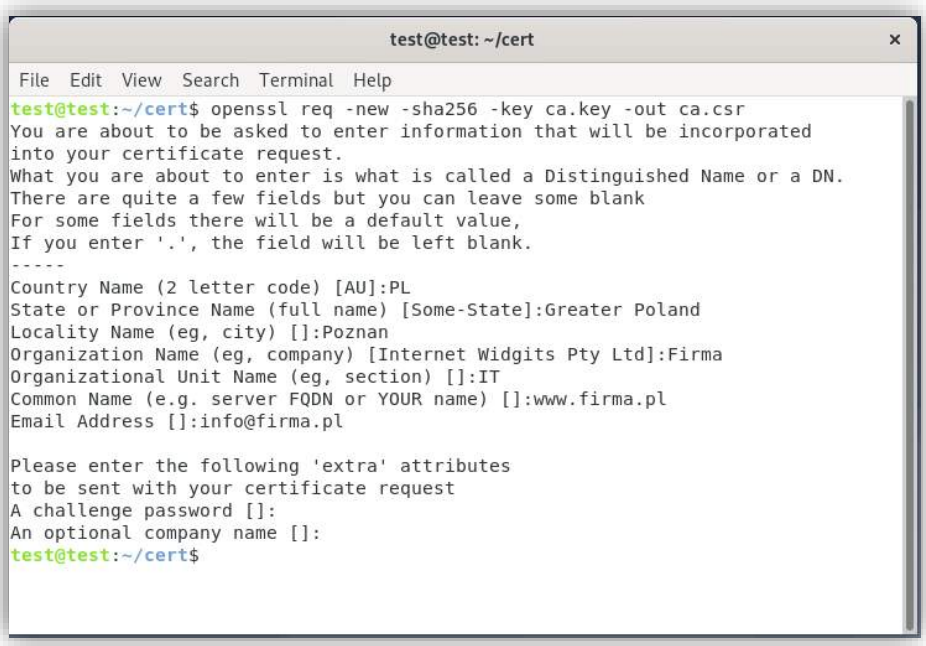
  Firma *(nazwa organizacji/firmy)*
- Organizational Unit Name (eg, section) []

  IT *(dział)*
- Common Name (eg, YOUR name) []

  www.firma.pl *(nazwa zwykła)*
- Email Address []

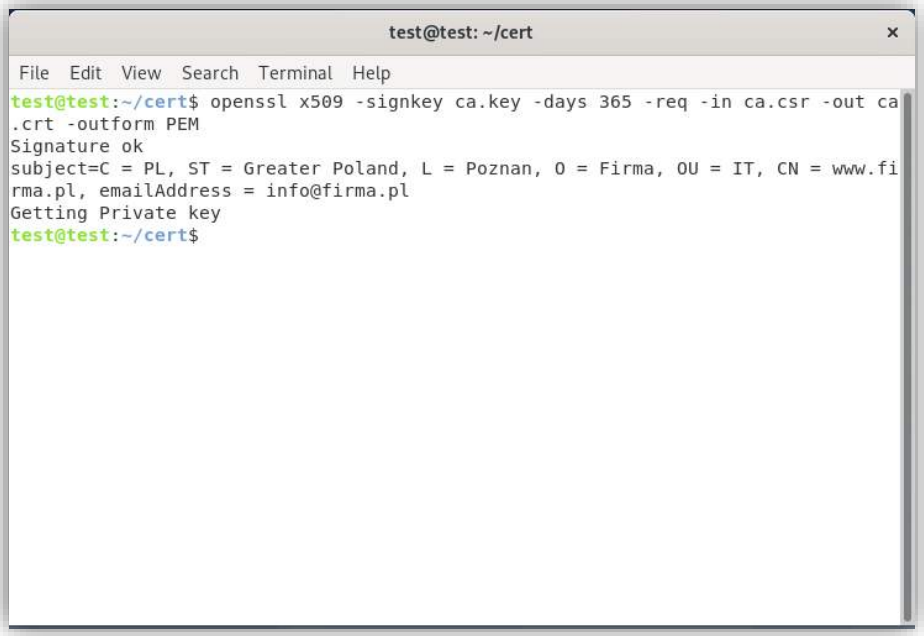
  info@firma.pl *(adres email)*

Pozostałe (opcjonalne) parametry pozostawiamy domyślne.



3. Podpisujemy nasz CA (ca.crt)

   `openssl x509 -signkey ca.key -days 365 -req -in ca.csr -out ca.crt -outform PEM`

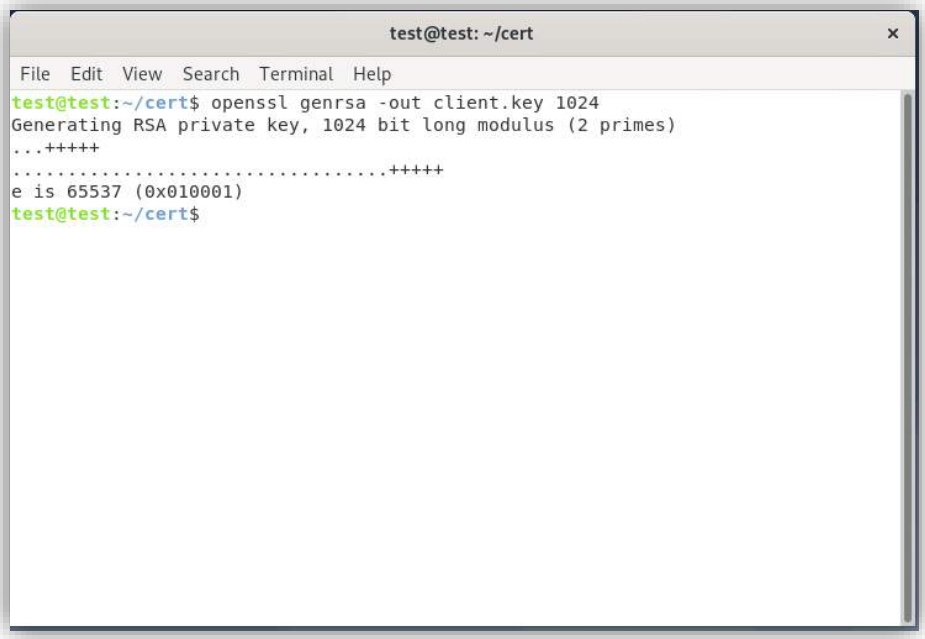


W drugim etapie wygenerowany zostanie certyfikat główny który zostanie podpisany utworzonym właśnie certyfikatem CA.

1. Generujemy klucz prywatny dla certyfikatu głównego – jest to klucz RSA o długości 1024 bitów (możemy wygenerować klucz o długości 2048 bitów – zamieniając

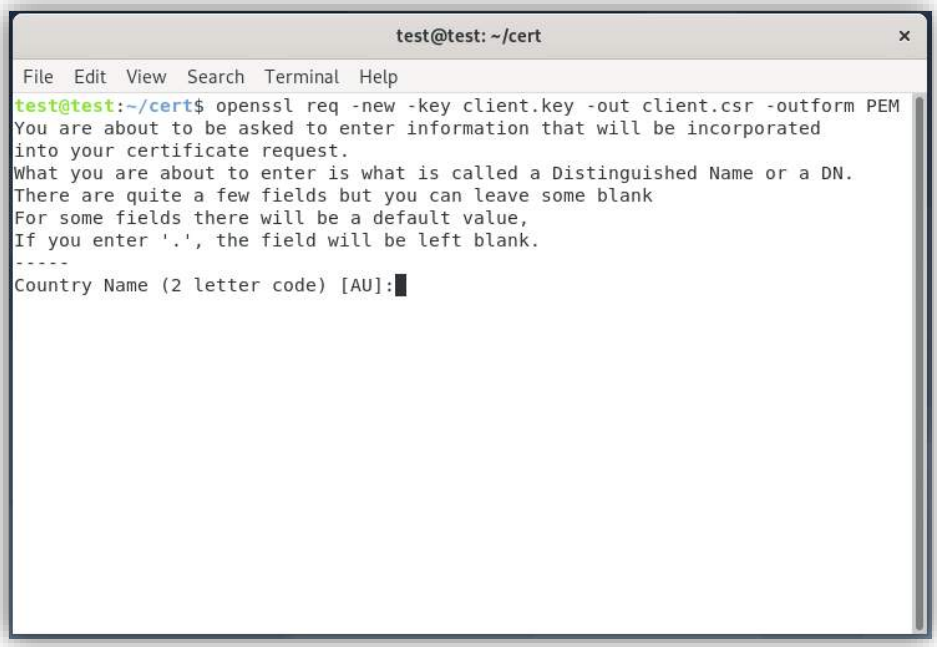
parametr 1024 w poleceniu na 2048). Plik z generowanym kluczem prywatnym to client.key:

```
openssl genrsa -out client.key 1024
```



2. Generujemy żądanie utworzenia certyfikatu głównego (client.csr)

```
openssl req -new -key client.key -out client.csr -outform PEM
```



Po wydaniu tego polecenia należy wprowadzić dodatkowe dane:

- Country Name (2 letter code) [AU]

PL *(kod kraju)*

- State or Province Name (full name) [Some-State]

  Greater Poland *(województwo)*

- Locality Name (eg, city) []

  Poznan *(miasto)*

- Organization Name (eg, company) [Internet Widgits Pty Ltd]

  Firma *(nazwa organizacji/firmy)*

- Organizational Unit Name (eg, section) []

  IT *(dział)*

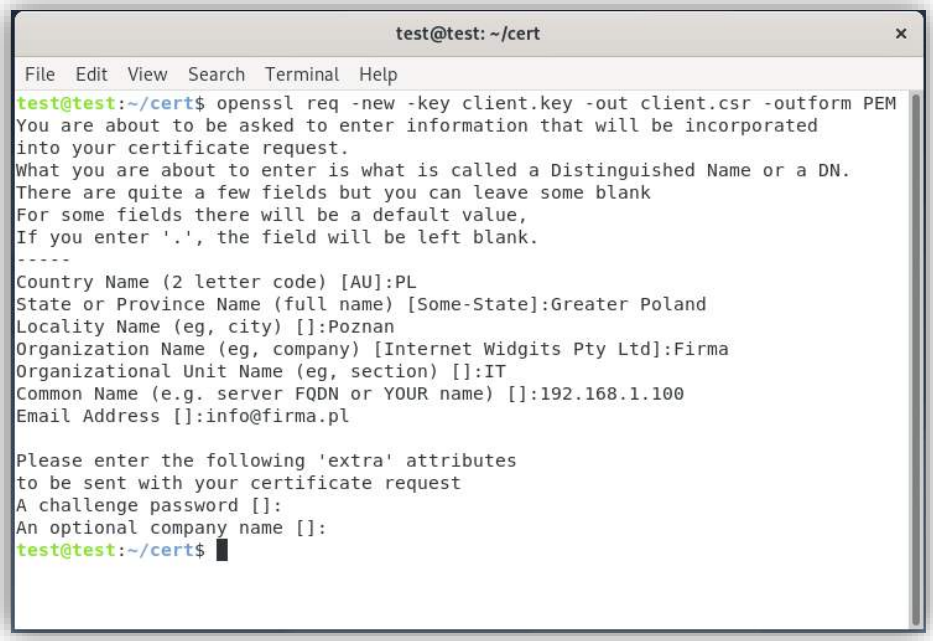
- Common Name (eg, YOUR name) []

  192.168.1.100 *(nazwa zwykła) – tutaj podajemy nazwę domeny (w naszym przypadku IP urządzenia dla którego generujemy certyfikat)*

- Email Address []

  info@firma.pl *(adres email)*

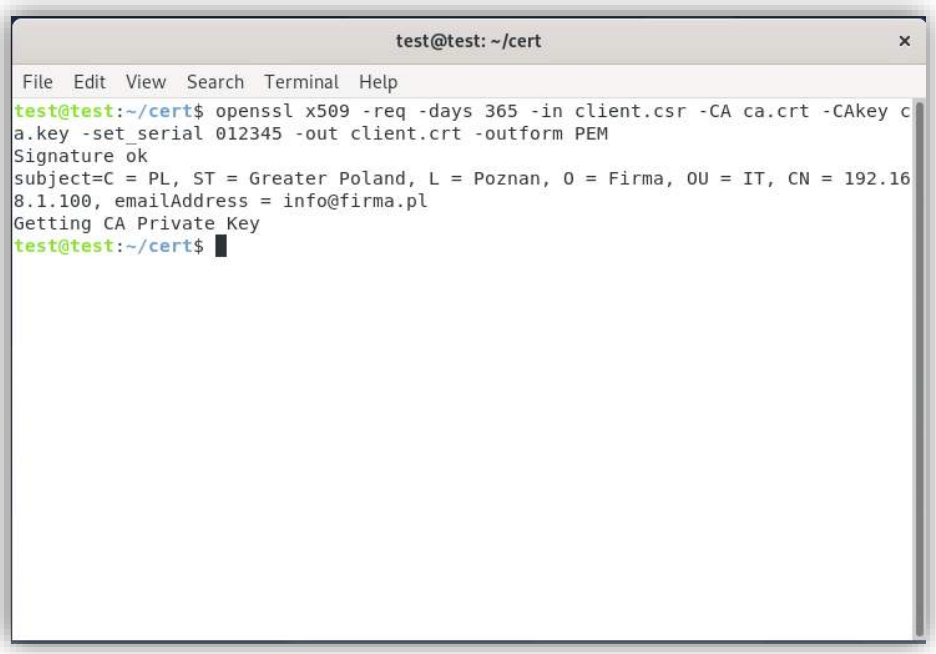
Pozostałe (opcjonalne) parametry pozostawiamy domyślne.



3. Podpisujemy certyfikat główny naszym certyfikatem CA

   ```
   openssl x509 -req -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 012345 -out client.crt -outform PEM
   ```

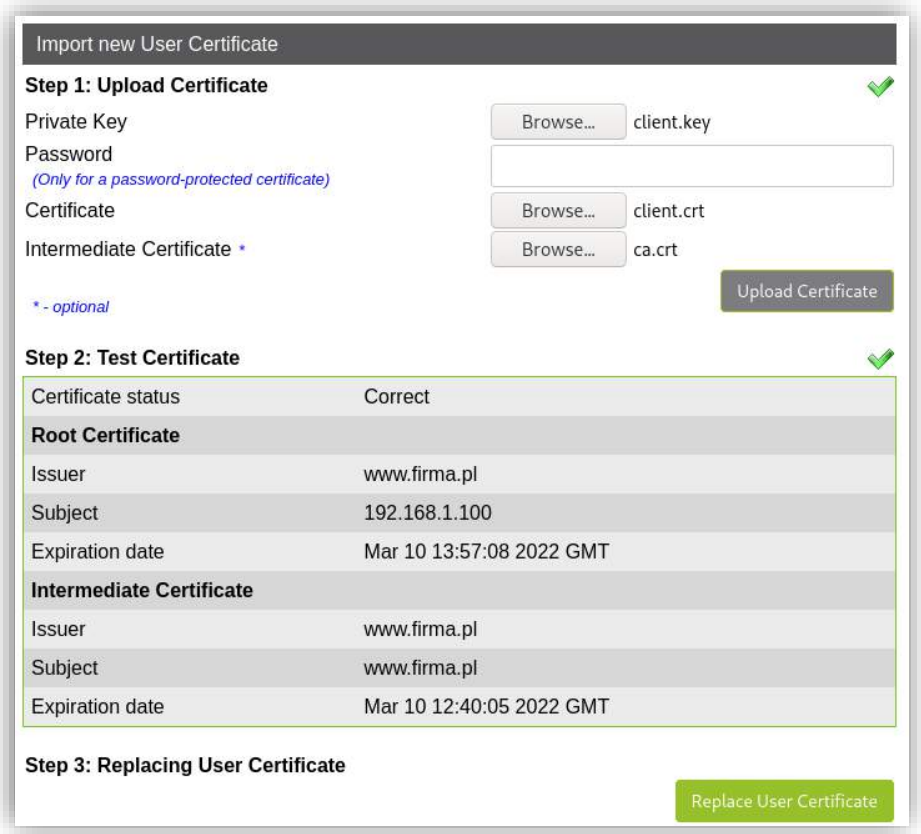
   Certyfikat będzie ważny rok czasu (*-days 365*)



Procedura generowania i podpisywania certyfikatu jest zakończona. Otrzymane pliki *client.key* (klucz prywatny) oraz *client.crt* (certyfikat) można wysłać do Karty Zarządzającej jako certyfikat użytkownika. Opcjonalnie można załączyć plik *ca.crt* jako certyfikat pośredniczący.

Wygenerowany certyfikat importujemy do karty:

Po wysłaniu i weryfikacji:



Certyfikat jest gotowy do zapisania jako certyfikat użytkownika – po zatwierdzeniu przyciskiem **Replace User Certificate** zostanie zapisany w systemie karty, gotowy do użycia.

RESTART SYSTEMU KARTY

Aby dokonać sprzętowego resetu karty (bez utraty konfiguracji) należy na krótko (poniżej 1 sekundy) wcisnąć przycisk RESET na panelu Karty Zarządzającej.

PRZYWRACANIE USTAWIEŃ DOMYŚLNYCH

W przypadku utraty dostępu do Karty Zarządzającej (np. z powodu niepoprawnej konfiguracji sieciowej, zapomnienia hasła) lub konieczności dokonania przywrócenia konfiguracji fabrycznej Karty Zarządzającej należy nacisnąć i przytrzymać przycisk RESET na panelu Karty Zarządzającej przez minimum 10 sekund. Po tej operacji karta przywróci swoją pierwotną konfigurację. Interfejs sieciowy zostanie skonfigurowany do pobierania adresu IPv4 z serwera DHCP (konfiguracja automatyczna) a wszystkie hasła dostępu przyjmą wartość domyślną.

ZARZĄDZANIE Z POZIOMU AGENTA SNMP

FILOZOFIA ZARZĄDZANIA

Protokół SNMP (Simple Network Management Protocol) jest ogólnie przyjętym standardem w zarządzaniu różnego rodzaju urządzeniami poprzez sieci komputerowe. Zasilacze awaryjne, jako nieodłączna część systemów komputerowych, także mają możliwość kontroli z poziomu SNMP.

Standardowy model systemu zarządzania składa się z Agenta i Menedżera SNMP. Karta Zarządzająca EVER jest kartą rozszerzeń do zasilaczy EVER i wraz z oprogramowaniem PowerSoft oferuje możliwość zarządzania systemem zasilania z poziomu SNMP.

Menadżer SNMP zawarty w oprogramowaniu PowerSoft jest specjalizowanym systemem uruchamianym na stacji zarządzającej zwanej NMS (Network Management Station), służącym do komunikacji z Agentem i wymiany informacji. Menedżer posiada bazę obiektów zarządzania „MIB” (Management Information Base), która określa, jakiego rodzaju parametry mogą być zmienione lub odczytane z Agenta.

BAZA OBIEKTÓW MIB (MANAGEMENT INFORMATION BASE)

Każdemu parametrowi urządzenia zarządzanego z poziomu SNMP jest przyporządkowany odpowiedni obiekt bazy MIB. Definicja obiektu w bazie jednoznacznie określa typ obiektu, jego położenie w bazie, sposób dostępu itp., do definicji bazy używa się notacji ASN.1. Wszystkie obiekty są zorganizowane w formie drzewa. Podstawowe obiekty bazy zostały zdefiniowane przez organizację standaryzacji protokołów sieciowych i opublikowane w odpowiednich dokumentach STD i RFC. W drzewie obiektów zostały przewidziane miejsca na własne definicje baz zawierających obiekty wykorzystywane przy zarządzaniu produktami specjalnymi. Jednym z takich miejsc jest grupa „ENTERPRISE", w której to została zarejestrowana baza obiektów do administracji produktami firmy EVER.

CHARAKTERYSTYKA AGENTA

Zaimplementowanie w karcie zarządzającej EVER Agent SNMP pozwala na uzyskanie informacji i kontrolę najważniejszych parametrów zasilacza awaryjnego. Agent obsługuje protokoły SNMP w wersji 1, 2 oraz 3, firmową bazę obiektów zarejestrowaną w grupie „enterprise" pod numerem 9797, czyli „ever" oraz bazę UPS-MIB (standard RFC1628).

Odczyt i zapis obiektów bazy Agenta SNMP może zostać dokonany z dowolnej stacji roboczej w sieci, pod warunkiem podania prawidłowego hasła do odczytu lub zapisu.

MENEDŻER SNMP

OPIS

EVER SNMP Menedżer zawarty w oprogramowaniu PowerSoft jest przeznaczony do zarządzania komputerami podłączonymi do sieci komputerowej i zasilanych UPS'ami posiadającymi kartę zarządzającą („z protokołem SNMP"). Umożliwia proste i bezpieczne zamknięcie systemu lub wykonanie innych zadań w przypadku wystąpienia zdarzeń na serwerze lub dowolnych stacjach roboczych, na których zainstalowany jest Klient sieciowy.

INSTALACJA PROGRAMU

Aby poprawnie zainstalować oprogramowanie, należy postępować zgodnie z wytycznymi zawartymi w instrukcji programu PowerSoft.

KONFIGURACJA MENADŻERA SNMP

Konfiguracja menadżera SNMP została przedstawiona w instrukcji programu PowerSoft.

Aktualizacje oprogramowania, opisy techniczne oraz aktualne informacje można znaleźć na naszej stronie internetowej **https://www.ever.eu**.

Nazwy rzeczywistych firm i produktów wymienione w niniejszym dokumencie mogą być znakami towarowymi zarejestrowanymi przez ich właścicieli.