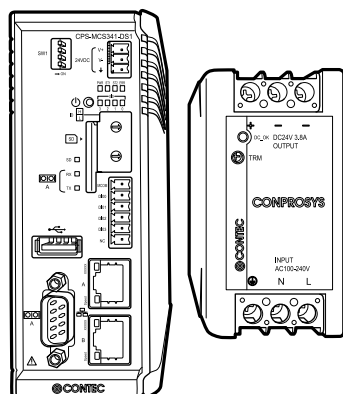


Podręcznik referencyjny dla instalatora
Security gateway



Spis treści

1	Informacje o tym dokumencie	3
2	Montaż	4
2.1	Ogólne środki ostrożności	4
2.1.1	Informacje ogólne	4
2.1.2	Miejsce montażu	5
2.1.3	Elektryczne	5
2.2	Wypożyczenie systemowe firmy Daikin	6
2.3	Opis systemu	6
2.3.1	Konfiguracja sieci lokalnej	7
2.3.2	Specyfikacja	8
2.4	Przed rozpoczęciem montażu	8
2.4.1	Niezbędne elementy wyposażenia	8
2.4.2	Informacje o lokalizacji zacisków	8
2.5	Instalacja 2 komponentów sprzętowych bramy Security gateway	9
2.6	Informacje o przewodach elektrycznych	10
2.6.1	Podłączanie przewodów zasilających	10
2.6.2	Podłączanie bramy Security gateway do sieci lokalnej	11
3	Rozruch	13
3.1	Informacje o rozruchu konfiguracji z bramą Security gateway	13
3.2	Minimalne wymagania dotyczące rozruchu	13
3.3	Nawiązywanie po raz pierwszy połączenia z bramą Security gateway	14
3.4	Informacje o konfigurowaniu bramy Security gateway	16
3.4.1	Dostęp do bramy Security gateway	16
3.4.2	Konfigurowanie sieci bramy Security gateway	18
3.4.3	Konfigurowanie strefy czasowej bramy Security gateway	21
4	Pierwszy rozruch sterownika iTM lub LC8	22
5	Obsługa	24
5.1	Informacje o pobieraniu dzienników	24
5.1.1	Pobieranie dzienników komunikacji	24
5.1.2	Pobieranie dzienników aktualizacji	25
5.1.3	Pobieranie dzienników monitorowania	27
5.2	Przywracanie ustawień fabrycznych bramy Security gateway	28
5.3	Restartowanie bramy Security gateway	29
5.4	Odczytywanie numerów wersji	31
6	Rozwiązywanie problemów	32
6.1	Potencjalne niepowodzenia	32
6.2	Komunikaty o błędach	32
7	Dane techniczne	34
7.1	Wymagania dotyczące komputera służącego do rozruchu	34
7.2	Pobór mocy przez bramę Security gateway	34
7.3	Domyślne hasła narzędzi	34
7.4	Wymagania dotyczące przewodów elektrycznych bramy Security gateway	35
7.5	Wymagania systemowe	35
8	Dodatek A — Informacje o wykrywaniu adresu IP bramy Security gateway	37
8.1	Podłączanie bramy Security gateway	37
8.2	Wykrywanie adresu IP	37
9	Dodatek B — Rozruch w konfiguracji z serwerem proxy	40
9.1	Konfiguracja alternatywna	40
9.2	Dostęp do bramy Security gateway	40
9.3	Konfigurowanie sieci bramy Security gateway	40
9.4	Konfigurowanie strefy czasowej bramy Security gateway	42
9.5	Pierwszy rozruch sterownika iTM lub LC8	43

1 Informacje o tym dokumencie

Czytelnik docelowy

Autoryzowani instalatorzy

Zestaw dokumentacji

Niniejszy dokument jest częścią zestawu dokumentacji. Pełen zestaw składa się z następujących elementów:

- **Instrukcja montażu:**

- Instrukcje dotyczące instalacji
- Format: Papierowa (dołączana do zestawu)

- **Podręcznik referencyjny dla instalatora:**

- Przygotowanie do instalacji, dane referencyjne,...
- Format: Pliki w formacie cyfrowym dostępne pod adresem <http://www.daikineurope.com/support-and-manuals/product-information/>

- **Podręcznik Airnet:**

- Pierwszy rozruch sterownika iTM lub LC8
- Format: Pliki w formacie cyfrowym dostępne pod adresem <http://www.daikineurope.com/support-and-manuals/product-information/>

- **Instrukcja instalacji urządzenia Intelligent Touch Manager (DCM601A51):**

- Instrukcje dotyczące instalacji
- Format: Pliki w formacie cyfrowym dostępne pod adresem <http://www.daikineurope.com/support-and-manuals/product-information/>

- **Instrukcja instalacji sterownika LC8 (DLC602B51):**

- Instrukcje dotyczące instalacji
- Format: Pliki w formacie cyfrowym dostępne pod adresem <http://www.daikineurope.com/support-and-manuals/product-information/>

Najnowsze wersje dostarczonej dokumentacji mogą być dostępne na regionalnej stronie internetowej firmy Daikin lub u przedstawiciela handlowego.

Oryginalna dokumentacja została napisana w języku angielskim. Dokumentacja we wszystkich pozostałych językach jest tłumaczeniem.

Dane techniczne

- **Podzbiór** najbardziej aktualnych danych technicznych jest dostępny w regionalnej witrynie WWW Daikin (ogólnodostępnej).
- **Kompletny zestaw** aktualnych danych technicznych jest dostępny w serwisie internetowym Daikin Business Portal (wymagane jest uwierzytelnienie).

2 Montaż

2.1 Ogólne środki ostrożności

Przed przystąpieniem do montażu klimatyzatora należy dokładnie zapoznać się z częścią dotyczącą środków ostrożności. Urządzenie musi być zamontowane prawidłowo.

Nieprzestrzeganie tych instrukcji może spowodować uszkodzenie mienia lub obrażenia ciała, które mogą, w zależności od okoliczności, okazać się bardzo poważne w skutkach.

Po zakończeniu montażu należy podczas rozruchu upewnić się, że zasilanie urządzenia jest prawidłowe oraz że moduły sterownika działają właściwie.

Znaczenie ostrzeżeń i symboli

Te komunikaty dotyczące bezpieczeństwa mają zwracać uwagę użytkownika. Poniżej przedstawiono znaczenia poszczególnych komunikatów dotyczących bezpieczeństwa:



OSTRZEŻENIE

Wskazuje na sytuację, która może doprowadzić do zgonu lub poważnych obrażeń ciała.



OSTROŻNIE

Wskazuje na sytuację, która może doprowadzić do niewielkich lub umiarkowanych obrażeń ciała.



NIEBEZPIECZEŃSTWO

Wskazuje na sytuację, która powoduje zgon lub poważne obrażenia ciała.



NIEBEZPIECZEŃSTWO: NIEBEZPIECZEŃSTWO WYBUCHU

Wskazuje sytuację, która może doprowadzić do wybuchu.



INFORMACJE

Wskazuje na przydatne wskazówki lub informacje dodatkowe.



UWAGA

Wskazuje na sytuację, która może doprowadzić do uszkodzenia sprzętu lub innego mienia.

2.1.1 Informacje ogólne

W przypadku braku pewności co do sposobu obsługi urządzenia należy skontaktować się z dealerem.

**OSTRZEŻENIE**

Nieprawidłowy montaż lub podłączenie urządzenia i akcesoriów może spowodować porażenie prądem elektrycznym, zwarcie, wycieki, pożar lub inne uszkodzenia sprzętu. Należy stosować wyłącznie akcesoria, sprzęt opcjonalny i części zamienne wyprodukowane lub zatwierdzone przez Daikin.

**OSTRZEŻENIE**

Należy upewnić się, że montaż, testowanie i zastosowane materiały są zgodne z właściwymi przepisami (obowiązującymi przed instrukcjami opisanymi w dokumentacji Daikin).

**OSTROŻNIE**

Podczas montażu, konserwacji lub serwisowania układu należy nosić odpowiedni sprzęt ochrony osobistej (rękawice ochronne, okulary...).

**OSTRZEŻENIE**

Rozedrzeć i wyrzucić torby plastikowe, tak aby nikt, a w szczególności dzieci, się nimi nie bawił. Możliwe ryzyko: uduszenie.

2.1.2 Miejsce montażu

NIE NALEŻY instalować urządzenia w atmosferze potencjalnie wybuchowej.

2.1.3 Elektryczne

**NIEBEZPIECZEŃSTWO: RYZYKO PORAŻENIA PRĄDEM ELEKTRYCZNYM**

- WYŁĄCZYĆ całe zasilanie przed podłączeniem okablowania elektrycznego lub dotknięciem części elektrycznych.
- Przed przystąpieniem do czynności serwisowych odłączyć zasilanie na więcej niż 10 minut i zmierzyć napięcie pomiędzy bolcami kondensatorów obwodu głównego bądź komponentów elektrycznych. Zanim będzie można dotknąć komponentów elektrycznych, napięcie MUSI być mniejsze niż 50 V prądu stałego. Informacje na temat lokalizacji styków zawiera schemat okablowania.
- NIE NALEŻY dotykać komponentów elektrycznych mokrymi rękami.
- NIE NALEŻY pozostawiać urządzenia bez nadzoru, o ile zdjęto panel serwisowy.

**OSTRZEŻENIE**

W stałych elementach okablowania należy (o ile nie został zainstalowany fabrycznie) umieścić wyłącznik główny lub inny element odcinający z separacją styków wszystkich bolców, zapewniający pełne odłączenie w sytuacji przeciążenia kategorii III.

**OSTRZEŻENIE**

- Stosować TYLKO przewody miedziane.
- Należy upewnić się, że instalacja elektryczna w miejscu instalacji jest zgodna z mającymi zastosowanie przepisami.
- Okablowanie musi być instalowane zgodnie ze schematem dostarczonym z produktem.
- Należy pamiętać o instalacji przewodów uziemiających. NIE NALEŻY uziemiać urządzenia do rur, ochronnika przepięciowego lub uziemienia telefonicznego. Nieprawidłowe uziemienie może być przyczyną porażenia elektrycznego.
- Należy koniecznie stosować oddzielne źródło zasilania. NIGDY nie używać zasilania wykorzystywanego równolegle przez inne urządzenie.
- Należy upewnić się, że zainstalowano wymagane bezpieczniki lub wyłączniki automatyczne.
- Należy zainstalować detektor prądu upływowego. W przeciwnym razie dojść do porażenia prądem elektrycznym lub pożaru.

**OSTRZEŻENIE**

- Po zakończeniu prac elektrycznych należy sprawdzić, czy wszystkie komponenty elektryczne oraz zaciski wewnątrz skrzynki elektrycznej są solidnie podłączone.
- Przed uruchomieniem urządzenia należy upewnić się, że wszystkie pokrywy są zamknięte.

2.2 Wyposażenie systemowe firmy Daikin

Do instalacji potrzebne są następujące elementy:

- Brama MCS341-DS1-111, numer części zamiennej EU.SB.5000072. Dołączone są przewody służące do podłączania przetwornicy zasilania.
- Przetwornica zasilania AC/DC (PWD-90AW24), numer części zamiennej 999175A.

Oraz jeden z następujących elementów:

- Sterownik iTM, numer produktu DCM601A51
- Sterownik LC8, numer produktu DLC602B51

Więcej informacji na temat tych urządzeń zawiera sekcja ["4 Pierwszy rozruch sterownika iTM lub LC8"](#) [► 22].

W przypadku stwierdzenia braku lub uszkodzenia którejkolwiek części należy skontaktować się z dealerem, u którego zakupiono urządzenie.

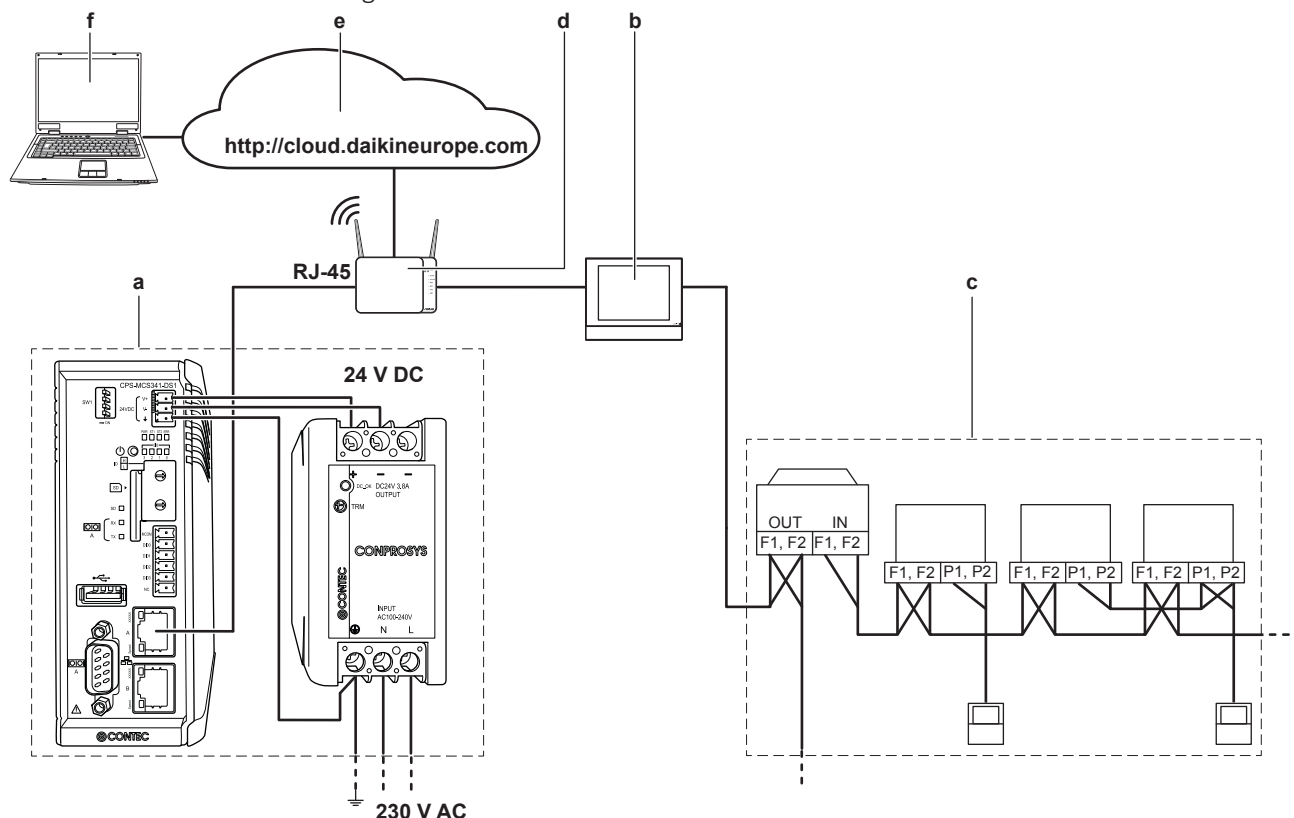
2.3 Opis systemu

Brama Security gateway umożliwia połączenie sterowników iTM i LC8 z chmurą Daikin Cloud Service za pośrednictwem bramy.

Zamiast wysyłać raport bezpośrednio do routera, sterownik iTM lub LC8 wysyła raport najpierw do bramy Security gateway. Brama Security gateway przekształca raport z protokołu http na https i wysyła przekształcony raport https do chmury Daikin Cloud Service za pośrednictwem routera.

2.3.1 Konfiguracja sieci lokalnej

Należy skonfigurować sieć lokalną w sposób przedstawiony na poniższym diagramie:



- a Security gateway
- b iTM lub LC8
- c Urządzenia
- d Brama sieci LAN
- e Chmura Daikin Cloud Service
- f Komputer z połączeniem z chmurą Daikin Cloud Service

Ta tabela ma charakter wyłącznie przykładowy i ma zastosowanie tylko do konfiguracji przedstawionej na powyższej ilustracji.

	iTM lub LC8	Security gateway	Router
Adres IP	192.168.1.50	192.168.1.51	192.168.1.1
Maska podsieci	255.255.255.0	255.255.255.0	255.255.255.0
Brama domyślna	192.168.1.51	192.168.1.1	
Preferowany serwer DNS	192.168.1.51	192.168.1.254	
Alternatywny serwer DNS	192.168.1.51	192.168.1.254	

2.3.2 Specyfikacja

Kategoria	Klasa	Specyfikacja	Uwagi
Sprzęt	Producent	CONTEC	—
	Numer modelu	MCS341-DS1-111	—
	Procesor	ARM Cortex-A8 600 MHz	—
	Port LAN	10BASE-T/100BASE-TX	—
	RAM	512 MB	—
	ROM	32 MB	—
	System operacyjny	Ubuntu 14.04	—
	Zakres temperatur	-20°C~+60°C	—
	Pojemność karty SD	4 GB	—
	Dysk startowy	Karta SD	—

2.4 Przed rozpoczęciem montażu

Przed przystąpieniem do instalacji bramy Security gateway należy wykonać opisane poniżej czynności przygotowawcze:

- Sprawdzić, czy zestaw modułu Security gateway i zasilacza zawiera wszystkie akcesoria.
- Sprawdzić, czy masz wszystko, co potrzebne do instalacji modułów Security gateway. Informacje można znaleźć w sekcji "[Niezbędne elementy wyposażenia](#)" [► 8].
- Zapoznać się z lokalizacją zacisków i przełączników na modułach Security gateway. Informacje można znaleźć w sekcji "[Informacje o lokalizacji zacisków](#)" [► 8].

2.4.1 Niezbędne elementy wyposażenia

Do instalacji modułów bramy Security gateway potrzebne są następujące elementy wyposażenia:

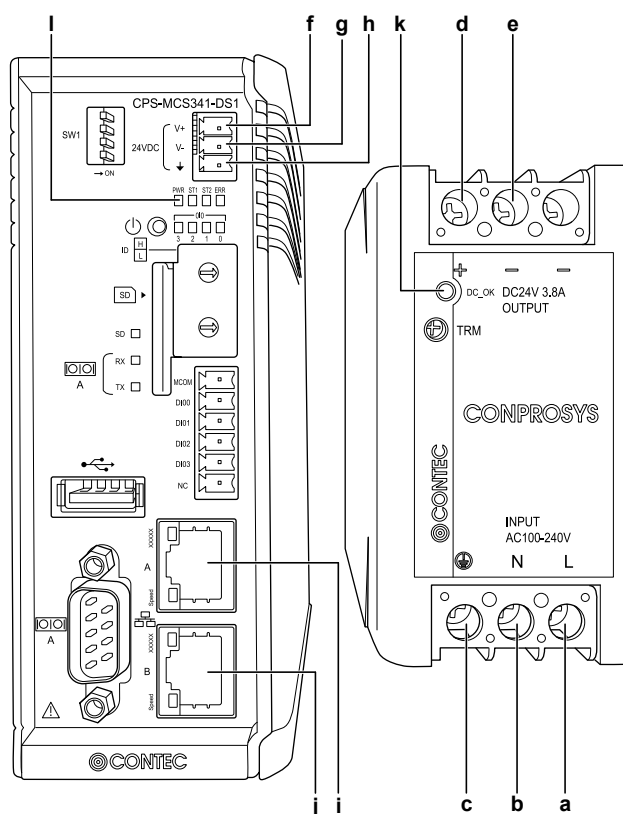
- wkrętak z płaską końcówką,
- wkrętak krzyżakowy,
- niezbędna ilość przewodów elektrycznych i odpowiednie narzędzia do ich podłączania.

Więcej informacji na temat przewodów elektrycznych, które należy stosować, można znaleźć w sekcji "[2.6 Informacje o przewodach elektrycznych](#)" [► 10].

2.4.2 Informacje o lokalizacji zacisków

Należy zapoznać się z rozmieszczeniem zacisków oraz lokalizacją otworów na module, a następnie rozplanować sposób prowadzenia kabli oraz kolejność ich podłączania celem uproszczenia procedury instalacji.

Więcej informacji o połączeniu zawiera sekcja "[2.6 Informacje o przewodach elektrycznych](#)" [► 10].

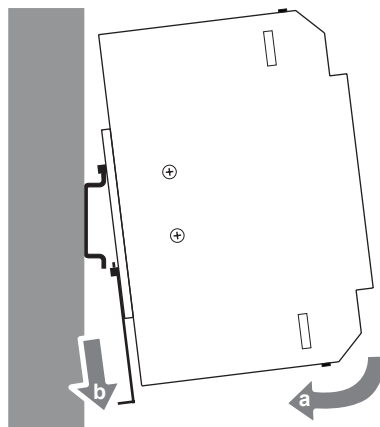


- a Zacisk pod napięciem 230 V AC
- b Zacisk neutralny (N) 230 V AC
- c Zacisk uziemienia
- d Wyjście zasilania 24 V DC (+)
- e Wyjście zasilania 24 V DC (-)
- f Wejście ze styku 24 V DC (+)
- g Wejście ze styku 24 V DC (-)
- h Zacisk uziemienia
- i Połączenie Ethernet (A) Informacje o prawidłowym sposobie wykonywania połączenia zawiera sekcja Typy konfiguracji, "8 Dodatek A — Informacje o wykrywaniu adresu IP bramy Security gateway" [► 37].
- j Połączenie Ethernet (B) Informacje o prawidłowym sposobie wykonywania połączenia zawiera sekcja Typy konfiguracji, "8 Dodatek A — Informacje o wykrywaniu adresu IP bramy Security gateway" [► 37].
- k Dioda LED "DC_OK" (DC_OK)
- l Dioda LED "PWR" (PWR)

2.5 Instalacja 2 komponentów sprzętowych bramy Security gateway

Komponenty bramy Security gateway są przystosowane do montażu na szynie DIN 35 mm.

- 1 Umieścić moduł na szynie DIN-35, tak aby górny zaczepek w tylnej części został zaczepiony.
- 2 Wpychać moduł w kierunku (a) aż do wczepienia dolnego zaczepek w szynę.
- 3 W razie potrzeby pociągnąć dźwignię w dolnej części modułu w kierunku (b), tak aby spowodować wczepienie modułu w szynę. W razie potrzeby użyć wkrętaka z płaską końcówką.
- 4 Powtórzyć poprzednie kroki dla wszystkich pozostałych modułów.



2.6 Informacje o przewodach elektrycznych

W tym rozdziale opisano procedurę podłączania komponentów bramy Security gateway do urządzeń Daikin oraz pozostałego sprzętu.

Wszystkie wymagania dotyczące instalacji elektrycznej opisano w sekcji "7.4 Wymagania dotyczące przewodów elektrycznych bramy Security gateway" [▶ 35].



OSTRZEŻENIE

- Nie należy WŁĄCZAĆ zasilania, dopóki nie zostaną wykonane wszystkie połączenia. Nieprzestrzeganie tego zalecenia może doprowadzić do porażenia prądem elektrycznym.
- Po wykonaniu okablowania, przed włączeniem zasilania należy ponownie sprawdzić, czy wszystkie przewody zostały prawidłowo podłączone.
- Wszystkie nie należące do wyposażenia części i materiały oraz prace elektryczne MUSZĄ być zgodne z odpowiednimi przepisami.

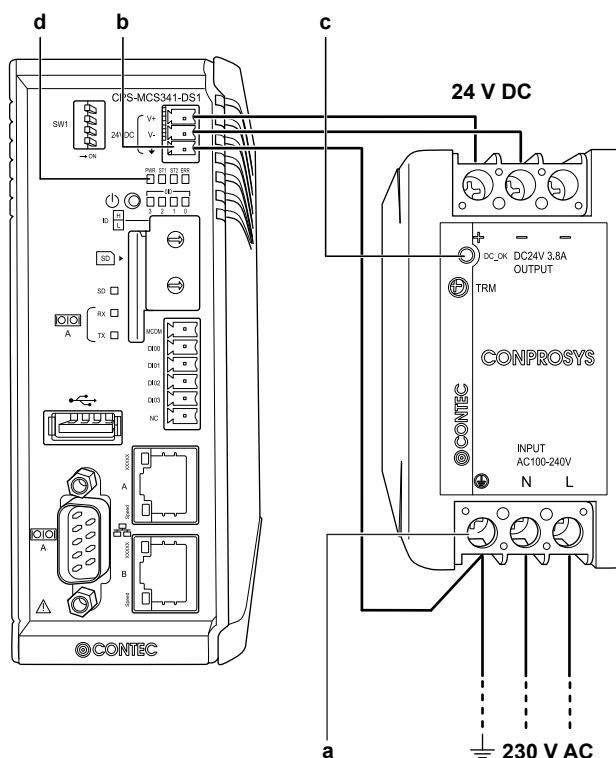


INFORMACJE

W chwili opracowywania niniejszej instrukcji niektóre złącza były NIEAKTYWNE, lecz są dostępne do wykorzystania w przyszłości.

2.6.1 Podłączanie przewodów zasilających

Podłączyć zasilanie w następujący sposób:



- 1 Zasilanie należy podłączyć do 3 złączy: L (napięcie), N (neutralny) i uziemienie w sekcji wejściowej jednostki zasilacza (PS).

Korzystając z przewodów dostarczonych razem z bramą Security gateway:

- 2 Podłączyć zaciski wyjściowe zasilania DC z zasilacza (PS) do zacisków wejść ze styków na module bramy Security gateway. Należy uwzględnić biegunowość przewodów.
- 3 Podłączyć zacisk uziemienia zasilacza (PS) (a) do zacisku uziemienia bramy Security gateway (b).

Po podłączeniu wszystkich przewodów:

- 4 Sprawdzić połączenia i włączyć zasilanie.



OSTROŻNIE

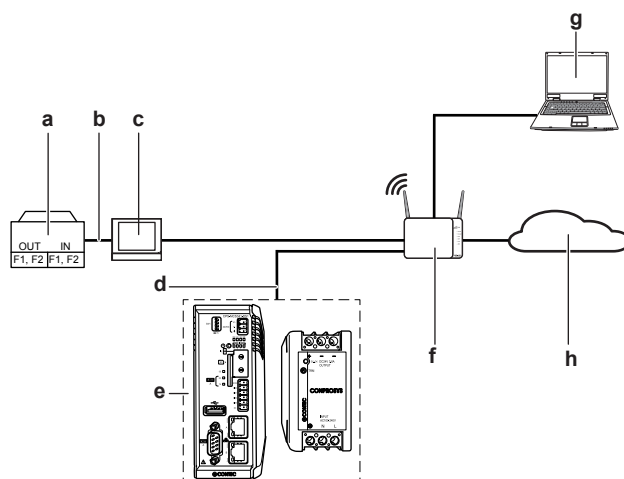
Zasilanie jest zapewnione **TYLKO** wtedy, gdy dioda LED "DC_OK" (DC_OK) (c) na zasilaczu (PS) i dioda LED "PWR" (PWR) (d) na module Security gateway świecą na zielono.

Jeśli którakolwiek lub obie z powyższych diod LED NIE świecą, należy sprawdzić, czy okablowanie nie jest uszkodzone.

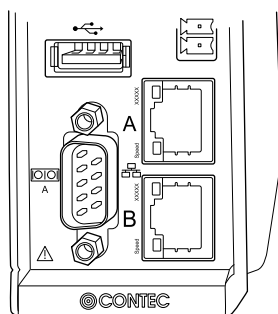
2.6.2 Podłączanie bramy Security gateway do sieci lokalnej

Konfiguracja podstawowa (zalecana)

- 1 Podłączyć zasilanie tak, jak opisano to w sekcji "[Podłączanie przewodów zasilających](#)" [► 10].
- 2 Dodać bramę Security gateway do sieci lokalnej tak, jak przedstawiono to na poniższym rysunku:



W tym przypadku będzie używany tylko port LAN A.



- a Urządzenie zewnętrzne
- b Połączenie LAN (DIII)
- c Sterownik iTM lub LC8
- d Połączenie LAN do portu A
- e Security gateway
- f Brama sieci LAN (RJ-45)
- g Komputer PC użytkownika
- h Chmura Daikin Cloud Service

Podłączyć zasilanie.

Podłączanie do sprzętu kompatybilnego z siecią DIII-NET

Patrz:

- Podręcznik Airnet:
 - Pierwszy rozruch sterownika iTM lub LC8
 - Format: Pliki w formacie cyfrowym dostępne pod adresem <http://www.daikineurope.com/support-and-manuals/product-information/>
- Instrukcja instalacji sterownika iTM
- Instrukcja instalacji sterownika LC8

Podłączanie przewodu sieci LAN

Wszystkie wymagania dotyczące instalacji elektrycznej opisano w sekcji "2.3 Opis systemu" [▶ 6].

NIE należy podłączać przewodu sieci LAN aż do chwili rozruchu bramy sieci LAN. W przeciwnym wypadku może wystąpić konflikt adresów sieciowych.

3 Rozruch



OSTRZEŻENIE

Tylko wykwalifikowane osoby powinny dokonywać rozruchu.



OSTROŻNIE

Wstępne kontrole układu elektrycznego, takie jak ciągłość ziemi, polaryzacja, opór do ziemi i zwarcie powinna wykonać wykwalifikowana osoba za pomocą odpowiedniego miernika.

3.1 Informacje o rozruchu konfiguracji z bramą Security gateway

Po upewnieniu się, że komponenty bramy Security gateway zostały zainstalowane, a wszystkie niezbędne połączenia elektryczne wykonane, można przystąpić do rozruchu konfiguracji z bramą Security gateway.

W tej fazie rozruchu można wykonać następujące czynności:

- Skonfigurować komputer w taki sposób, aby mógł łączyć się z bramą Security gateway, patrz rozdział "Nawiązywanie po raz pierwszy połączenia ze sterownikiem intelligent Tablet Controller" w podręczniku referencyjnym dla instalatora sterownika intelligent Tablet Controller.
- Skonfigurować ustawienia sieci LAN; informacje na temat ustawień sieci (narzędzia do rozruchu lokalnego) zawiera sekcja ["3.3 Nawiązywanie po raz pierwszy połączenia z bramą Security gateway"](#) [► 14].
- Ustawić datę i godzinę, patrz ["Konfigurowanie strefy czasowej bramy Security gateway"](#) [► 21].
- Dodać wszystkie dołączone urządzenia (Daikin) do interfejsu WWW bramy Security gateway; informacje na temat szybkiego konfigurowania podłączonych urządzeń (narzędzia do rozruchu lokalnego) zawiera sekcja ["4 Pierwszy rozruch sterownika iTM lub LC8"](#) [► 22].

3.2 Minimalne wymagania dotyczące rozruchu

Przed przystąpieniem do konfigurowania bramy Security gateway należy wykonać opisane poniżej czynności przygotowawcze.

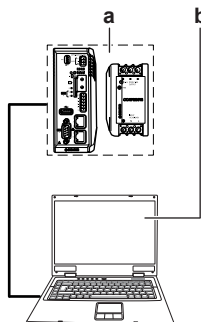
- Należy upewnić się, że parametry komputera spełniają wymagania minimalne określone w sekcji ["7.5 Wymagania systemowe"](#) [► 35].
- Należy skontaktować się z administratorem sieci w celu uzyskania na potrzeby konfigurowania bramy Security gateway następujących danych:
 - oczekiwanej nazwy sieciowej dla bramy Security gateway,
 - statycznego adresu IP i odpowiadającej mu maski podsieci bramy Security gateway,
 - statycznego adresu IP i odpowiadającej mu maski podsieci sterownika iTM lub LC8,
 - adresu IP bramy domyślnej,
 - adresu IP serwera DNS, oraz
 - adresu IP alternatywnego serwera DNS (jeśli ma zastosowanie).

- Należy upewnić się, że zasilanie wszystkich podłączonych urządzeń jest włączone.

3.3 Nawiązywanie po raz pierwszy połączenia z bramą Security gateway

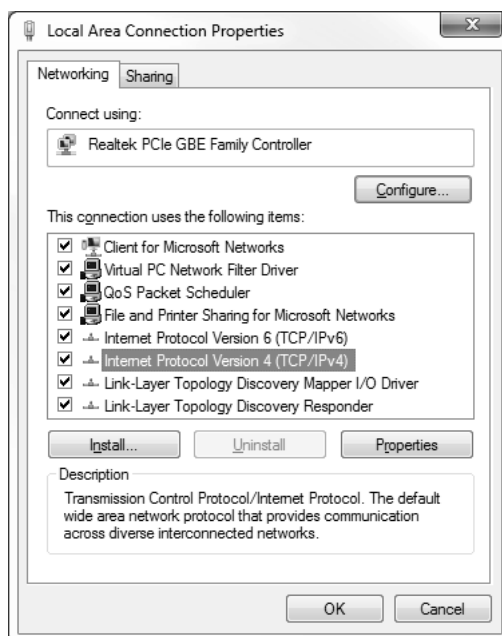
Nowy moduł Security gateway ma stały adres IP 192.168.0.126 oraz maskę podsieci 255.255.255.0.

Aby nawiązać połączenie z tym urządzeniem, trzeba zmienić adres IP komputera tak, by mieścił się w tym samym zakresie, co podany adres IP modułu.



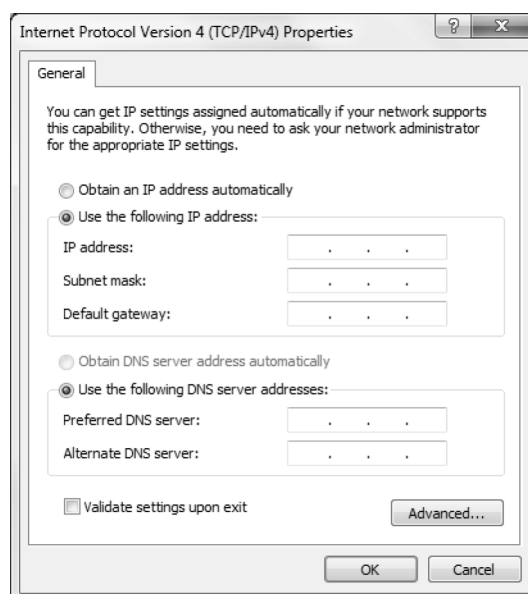
- 1 Podłączyć kabel ethernetowy KAT 5e (lub wyższej) do modułu Security gateway (a).
- 2 Podłączyć kabel ethernetowy do komputera (b) i zmienić adres IP komputera tak, by odpowiadał adresowi bramy Security gateway.
- 3 Na komputerze należy przejść do Panelu sterowania.
- 4 W Panelu sterowania kliknąć opcję Centrum sieci i udostępniania, a następnie opcję Zmień ustawienia karty sieciowej.
- 5 W oknie Połączenia sieciowe kliknąć dwukrotnie opcję Połączenie lokalne.

Wynik: Zostanie wyświetlone następujące okno.



- 6 Wybrać opcję Protokół internetowy w wersji 4 (TCP/IPv4), a następnie kliknąć przycisk Właściwości.

Wynik: Zostanie wyświetlone następujące okno.



7 Kliknąć przycisk opcji Użyj następującego adresu IP:.

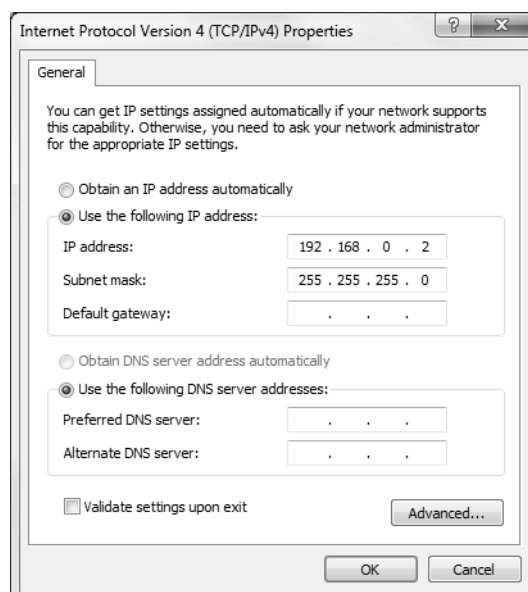
8 Ustawić następujący adres IP (IP address): 192.168.0.2.



INFORMACJE

W tym przykładzie użyto adresu 192.168.0.2, jednak można wybrać dowolny adres z zakresu 192.168.0.2~192.168.0.254 (z wyjątkiem 192.168.0.126).

9 Ustawić następującą maskę podsieci (Subnet mask): 255.255.255.0.



10 Kliknąć przycisk OK (OK).

Aby uniknąć zakłóceń pochodzących od innych sieci bezprzewodowych, należy wyłączyć wszystkie bezprzewodowe karty sieciowe, wykonując następujące czynności:

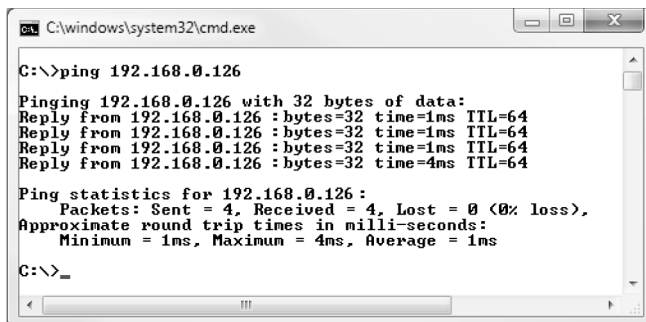
11 W oknie Połączenia sieciowe kliknąć prawym przyciskiem myszy opcję Połączenie sieci bezprzewodowej.

12 Wybrać opcję wyłączyć.

13 Sprawdzić, czy można nawiązać z komputera połączenie z modułem Security gateway. W tym celu utworzyć wiersz poleceń na komputerze, wykonując następujące czynności:

- 14 Kliknąć przycisk Start systemu Windows.
- 15 W polu Wyszukaj należy wpisać "wiersz polecenia" albo "Cmd".
- 16 Na liście wyników kliknąć odpowiednio opcję wiersz polecenia albo Cmd.
- 17 Wysłać pakiet ping na adres IP modułu Security gateway. W tym celu wpisać: "ping 192.168.0.126", potwierdzając naciśnięciem klawisza Enter.

Wynik: Zostanie wyświetlona odpowiedź jak w przykładzie poniżej:



```

C:\windows\system32\cmd.exe

C:\>ping 192.168.0.126

Pinging 192.168.0.126 with 32 bytes of data:
Reply from 192.168.0.126 : bytes=32 time=1ms TTL=64
Reply from 192.168.0.126 : bytes=32 time=1ms TTL=64
Reply from 192.168.0.126 : bytes=32 time=1ms TTL=64
Reply from 192.168.0.126 : bytes=32 time=4ms TTL=64

Ping statistics for 192.168.0.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\>_

```



INFORMACJE

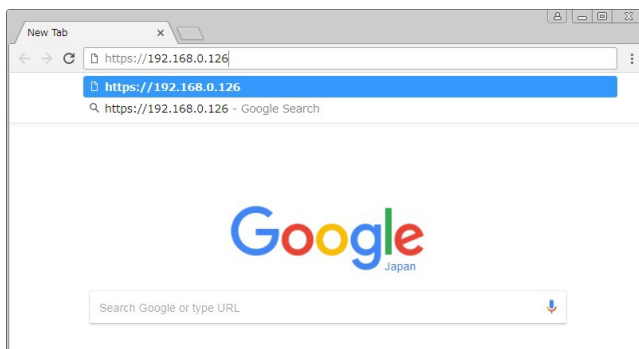
BRAK odpowiedzi i otrzymanie zamiast niej informacji o przekroczeniu czasu może wskazywać na problem z połączeniem. W celu wyeliminowania problemu należy zapoznać się z treścią punktu "[6 Rozwiązywanie problemów](#)" [▶ 32].

3.4 Informacje o konfigurowaniu bramy Security gateway

3.4.1 Dostęp do bramy Security gateway

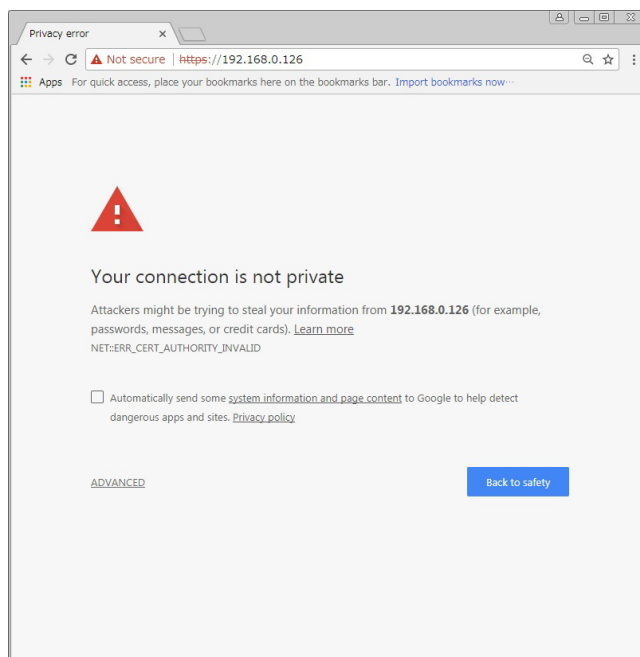
Aby uzyskać instrukcję wykrywania adresu bramy Security gateway, jeśli został zapomniany, patrz "[8 Dodatek A — Informacje o wykrywaniu adresu IP bramy Security gateway](#)" [▶ 37].

- 1 Wpisać domyślny adres IP bramy Security gateway (<https://192.168.0.126>) w pasku adresu URL przeglądarki WWW (Google Chrome lub Microsoft Edge).

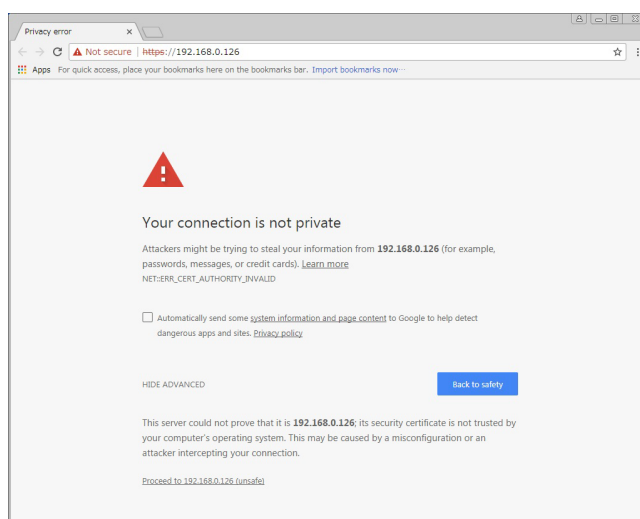


Wynik: Zostanie wyświetlony komunikat ostrzegawczy dotyczący połączenia.

- 2 Kliknąć opcję ADVANCED (ADVANCED), aby wyświetlić okno ustawień zaawansowanych.

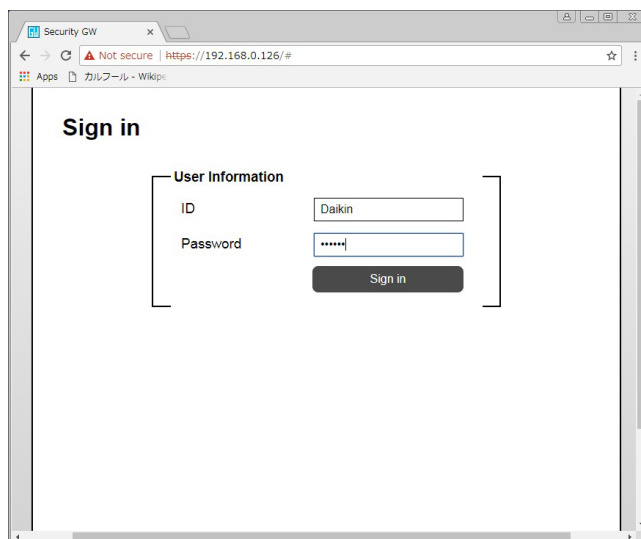


- 3 Kliknąć opcję Proceed to 192.168.0.126 (unsafe) (Proceed to 192.168.0.126 (unsafe)).

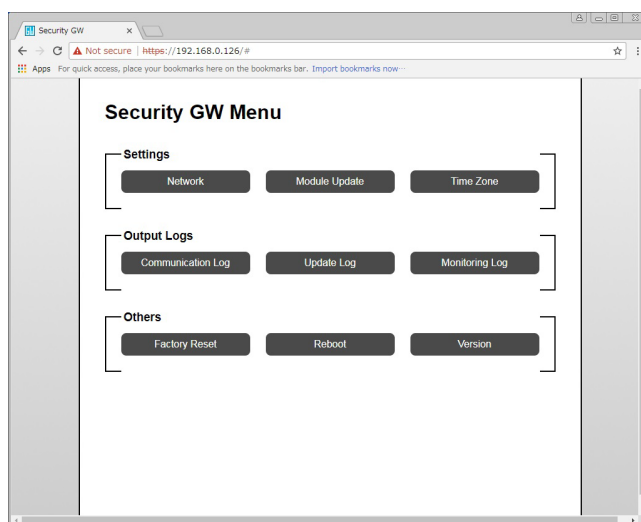


Wynik: Zostanie wyświetlone okno logowania.

- 4 Wprowadzić identyfikator (ID) i hasło (Password) (domyślny identyfikator to: Daikin / domyślne hasło to: Daikin) bramy Security gateway i kliknąć przycisk logowania (Sign in).



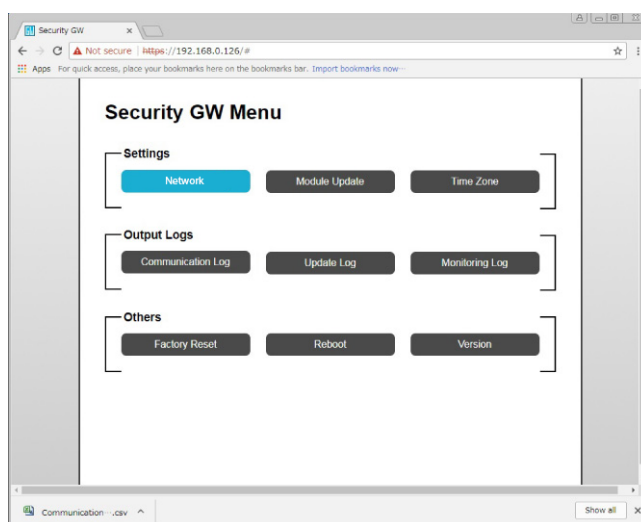
Wynik: Zostanie wyświetlone okno menu bramy Security gateway (Security GW Menu).



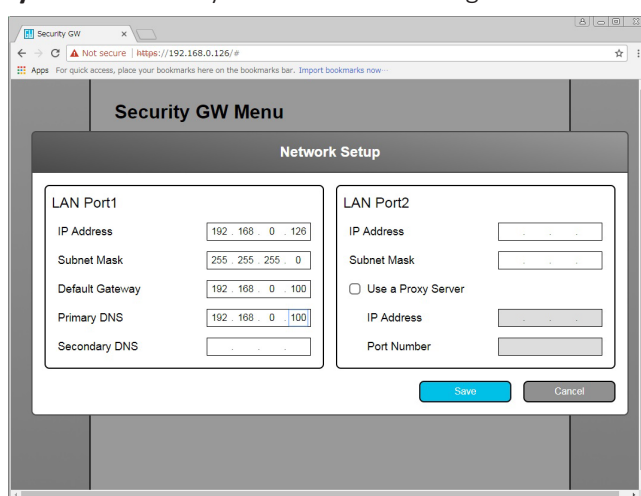
3.4.2 Konfigurowanie sieci bramy Security gateway

Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

- 1 Kliknąć przycisk sieci (Network).



Wynik: Zostanie wyświetlone okno dialogowe ustawień sieci (Network Setup).



2 Wprowadzić następujące dane sieci:

Port 1 sieci LAN (LAN Port1) (=A)

- Adres IP (IP address): Unikalny adres IP (domyślnie: 192.168.0.126) w sieci lokalnej
- Maska podsieci (Subnet mask): 255.255.255.0
- Brama domyślna (Default Gateway): Adres IP (domyślnie: 192.168.0.100) routera lokalnego
- Podstawowy serwer DNS (Primary DNS): Adres IP (domyślnie: 192.168.0.100) routera lokalnego
- Dodatkowy serwer DNS (Secondary DNS): pozostawić puste pole

Port 2 sieci LAN (LAN Port2) (=B)

- Pozostawić puste pole



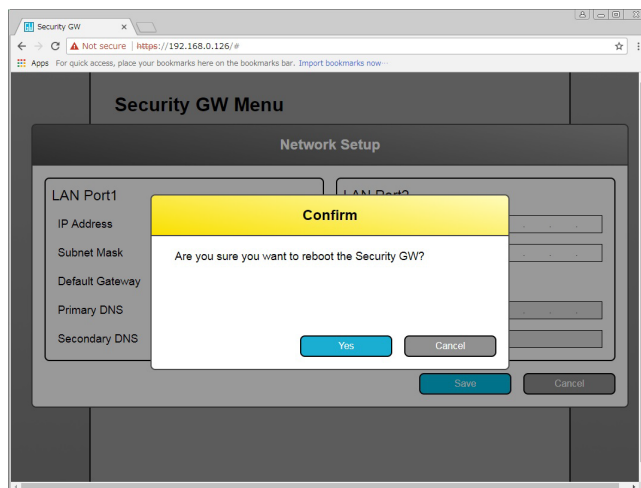
INFORMACJE

Jeśli adres IP (IP address), brama domyślna (Default gateway) i podstawowy serwer DNS (Primary DNS) są skonfigurowane zgodnie z ustawieniami sieci lokalnej, nie trzeba ich zmieniać.

3 Kliknąć przycisk zapisu (Save).

Wynik: Zostanie wyświetlone okno dialogowe potwierdzenia (Confirm).

- 4 Kliknąć przycisk Tak (Yes), aby zrestartować bramę Security gateway.



Wynik: Spowoduje to restart bramy Security gateway.

Wynik: Zostanie wyświetlone okno przeglądarki.

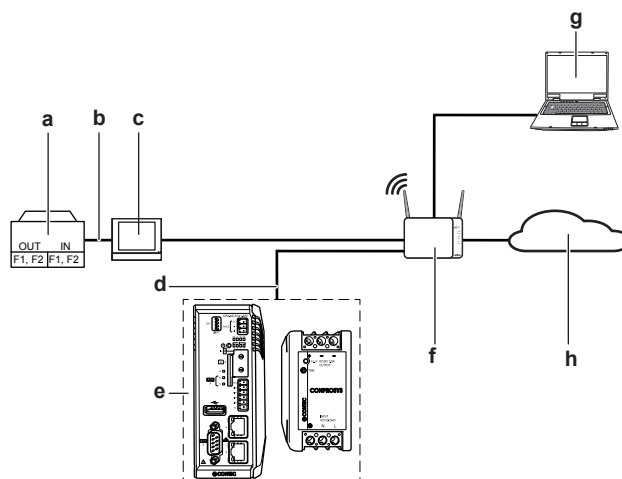
Wynik: Adres IP będzie zmieniony.



INFORMACJE

Po wykonaniu kroku 4 komunikacja z przeglądarką WWW zostanie utracona. Wykonać procedurę opisaną w sekcji "[Dostęp do bramy Security gateway](#)" [▶ 16], aby ponownie nawiązać połączenie, używając nowego adresu IP.

- 5 Zresetować ustawienia sieci LAN komputera, przywracając wartości domyślne.
- 6 Włączyć kartę WiFi komputera, jeśli wcześniej została wyłączona.
- 7 Rozłączyć przewód sieci Ethernet między komputerem a modulem Security gateway.
- 8 Podłączyć przewód sieci Ethernet między modulem Security gateway a siecią lokalną.



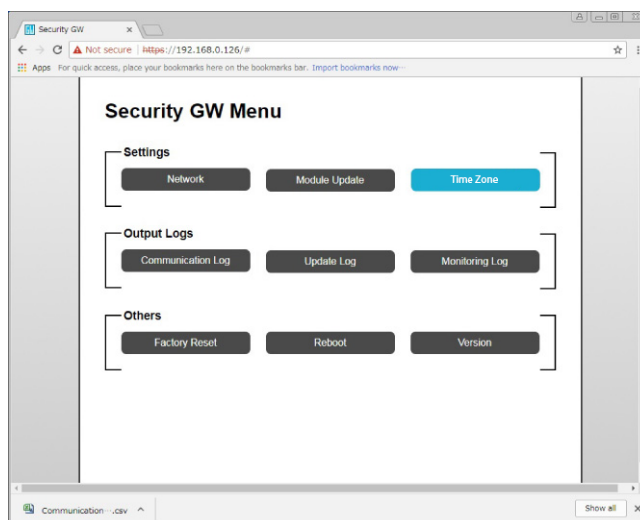
INFORMACJE

Aby upewnić się, że adres IP został poprawnie zmieniony, uzyskać dostęp do bramy Security gateway w sposób opisany w sekcji "[Dostęp do bramy Security gateway](#)" [▶ 16], używając nowego adresu IP.

3.4.3 Konfigurowanie strefy czasowej bramy Security gateway

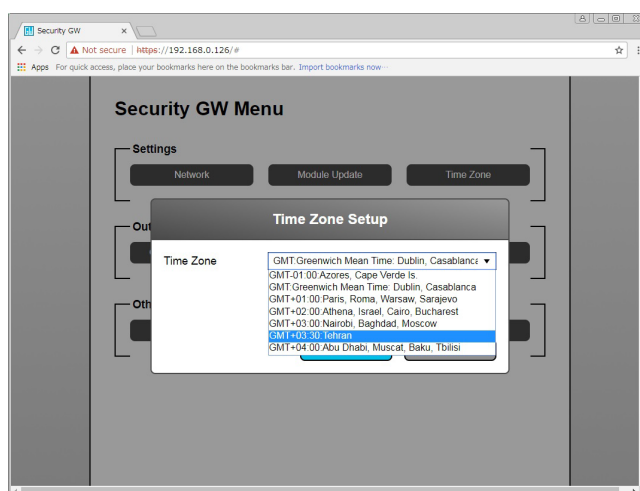
Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

- 1 Kliknąć przycisk strefy czasowej (Time Zone).

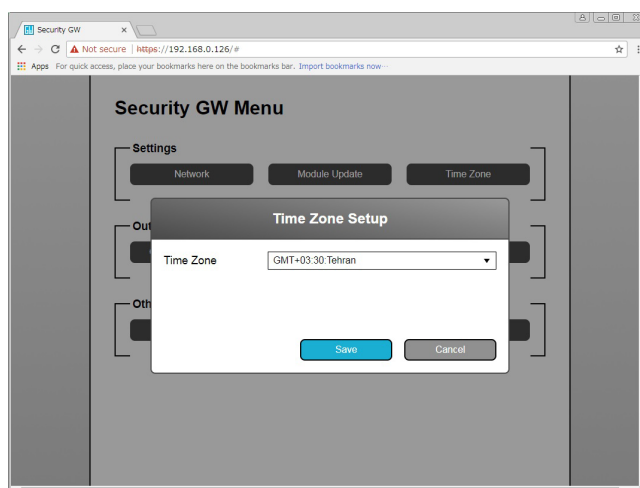


Wynik: Zostanie wyświetlone okno dialogowe ustawień strefy czasowej (Time Zone Setup).

- 2 Kliknąć przycisk [▼], aby otworzyć listę rozwijaną stref czasowych >> wybrać i kliknąć strefę czasową.



- 3 Kliknąć przycisk zapisu (Save).



4 Pierwszy rozruch sterownika iTM lub LC8

1 Instrukcję instalacji sterownika iTM lub LC8 zawiera podręcznik Airnet.

Następne kroki różnią się od opisanych w Podręczniku Airnet. Należy dopilnować, aby ustawienia w sterowniku iTM lub LC8 były takie, jak opisano to w kroku 3.

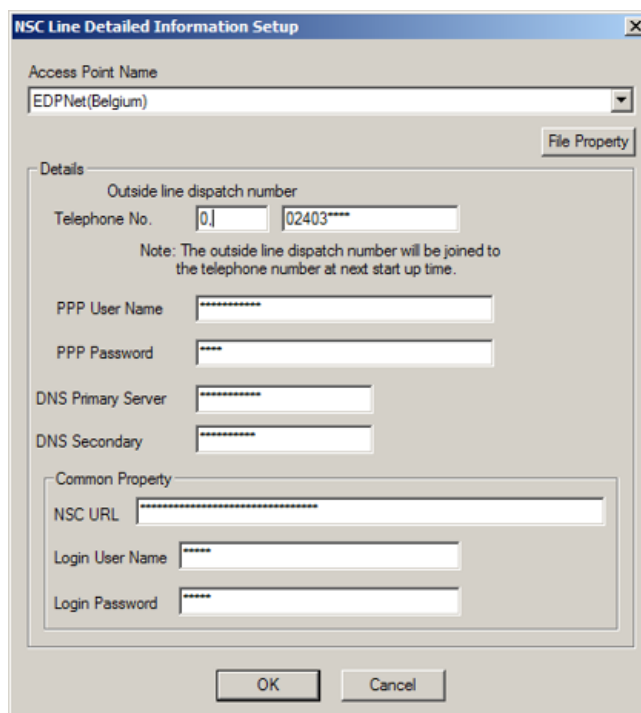
2 Informacje o konfiguracji zawiera sekcja "2.3 Opis systemu" [▶ 6].

3 Skonfigurować sieć sterownika lokalnego zgodnie z poniższą tabelą.

iTM

LC8

4 Wybrać adres URL NSC <http://Lcc.m2m.daikineurope.com/NSC> i wybrać poprawną nazwę punktu dostępu (Access Point Name) z listy wyboru. Sekcja szczegółów (Details) może pozostać pusta.



NSC Line Detailed Information Setup

Access Point Name
EDPNet(Belgium)

File Property

Details

Outside line dispatch number
Telephone No. 01 02403****

Note: The outside line dispatch number will be joined to the telephone number at next start up time.

PPP User Name

PPP Password

DNS Primary Server

DNS Secondary

Common Property

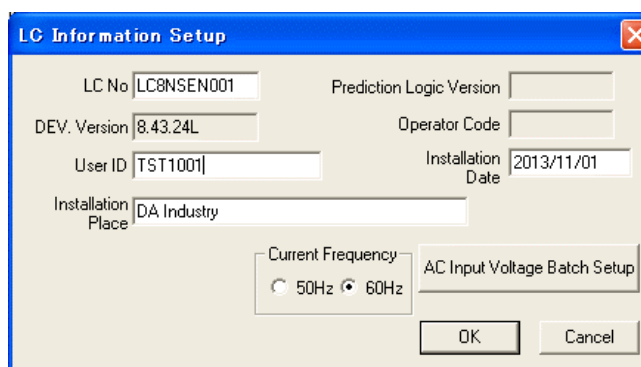
NSC URL

Login User Name

Login Password

OK Cancel

- 5 Wprowadzając dane uwierzytelniające chmury Daikin Cloud Service, nawiązać połączenie z witryną <https://cloud.daikineurope.com> i utworzyć nową lokalizację. Po utworzeniu lokalizacji zanotować numer iTM lub LC8:
 - Numer iTM: Zarejestrowany numer identyfikacyjny urządzenia intelligent Touch Manager. Numer ten będzie mieć następujący format: LT2N##### (gdzie # jest znakiem alfanumerycznym).
 - Numer LC8: Zarejestrowany numer identyfikacyjny sterownika LC8. Numer ten będzie mieć następujący format: LC8N##### (gdzie # jest znakiem alfanumerycznym).



LC Information Setup

LC No LC8NSEN001 Prediction Logic Version

DEV. Version 8.43.24L Operator Code

User ID TST1001 Installation Date 2013/11/01

Installation Place DA Industry

Current Frequency 50Hz 60Hz

AC Input Voltage Batch Setup

OK Cancel

5 Obsługa

5.1 Informacje o pobieraniu dzienników

Korzystając z aplikacji WWW bramy Security gateway, można rejestrować i pobierać trzy dzienniki.

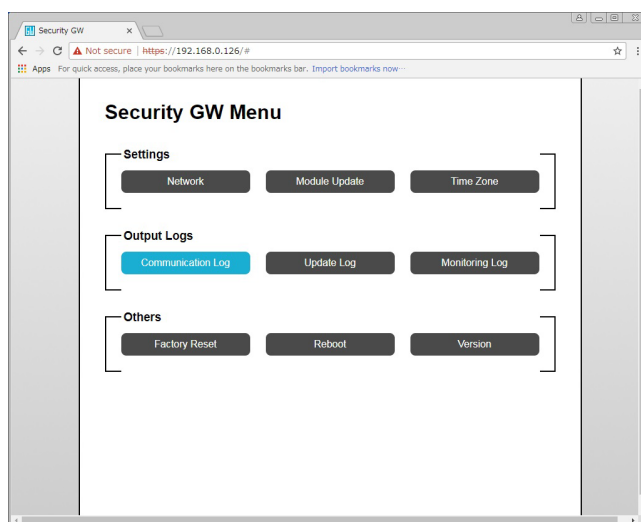
Następujące dzienniki można wykorzystać do weryfikacji działania bramy Security gateway w przypadku wystąpienia problemów:

Typ pliku	Przeznaczenie
Dziennik komunikacji	Będzie zawierał informacje o rodzajach danych wysłanych przez bramę Security gateway do platformy chmurowej i o tym, kiedy te dane były wysyłane.
Dziennik aktualizacji	Będzie zawierał informacje o sprawdzeniach aktualizacji, o tym, kiedy brama Security gateway sprawdzała dostępność aktualizacji, oraz o tym, czy nowa wersja oprogramowania została zainstalowana.
Dziennik monitorowania	Będzie zawierał informacje o czynnościach wykonywanych w bramie Security gateway, np. o tym, kiedy została wyłączona, a kiedy włączona.

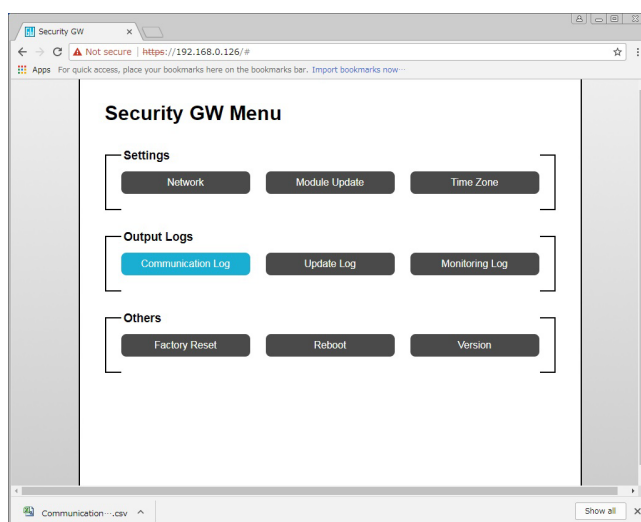
5.1.1 Pobieranie dzienników komunikacji

Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

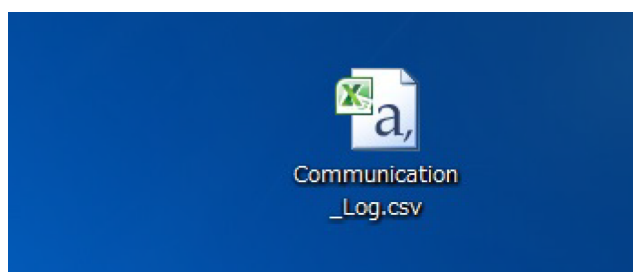
- 1 Kliknąć przycisk dziennika komunikacji (Communication Log).



- 2 Sprawdzić status pobierania na pasku pobierania u dołu okna.



- 3 Odszukać i kliknąć dwukrotnie (w celu otwarcia) pobrany plik .csv (Communication_Log.csv) dziennika komunikacji na pulpicie.



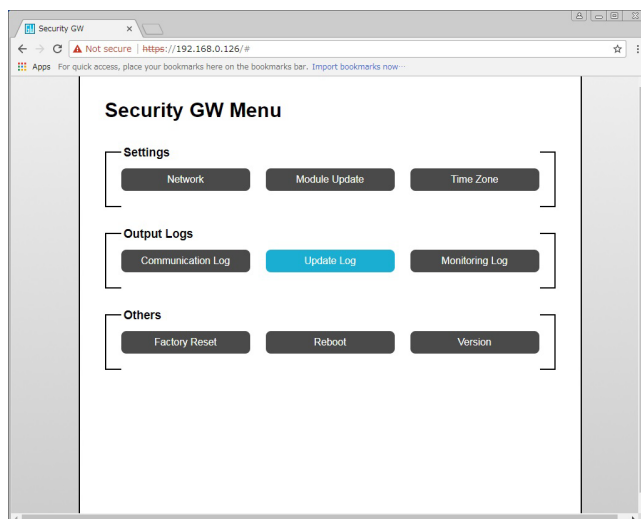
- 4 Zapoznać się z zawartością pliku .csv (Communication_Log.csv) dziennika komunikacji.

	A	B	C	D	E	F
1	2017/10/24 13:15	termconfig	192.168.0.190	1		
2	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
3	2017/10/24 13:15	daily	192.168.0.190	1		
4	2017/10/24 13:15	termconfig	192.168.0.190	1		
5	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
6	2017/10/24 13:15	daily	192.168.0.190	1		
7	2017/10/24 13:15	termconfig	192.168.0.190	1		
8	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
9	2017/10/24 13:15	daily	192.168.0.190	1		
10	2017/10/24 13:15	termconfig	192.168.0.190	1		
11	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
12	2017/10/24 13:15	daily	192.168.0.190	1		
13	2017/10/24 13:15	termconfig	192.168.0.190	1		
14	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
15	2017/10/24 13:15	daily	192.168.0.190	1		
16	2017/10/24 13:15	termconfig	192.168.0.190	1		
17	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
18	2017/10/24 13:15	daily	192.168.0.190	1		
19	2017/10/24 13:15	termconfig	192.168.0.190	1		
20	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
21	2017/10/24 13:15	daily	192.168.0.190	1		
22	2017/10/24 13:15	termconfig	192.168.0.190	1		
23	2017/10/24 13:15	termconfigresult	192.168.0.190	1		

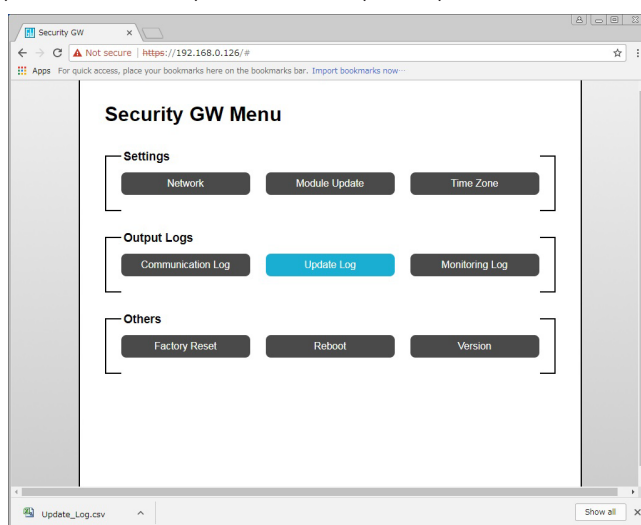
5.1.2 Pobieranie dzienników aktualizacji

Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

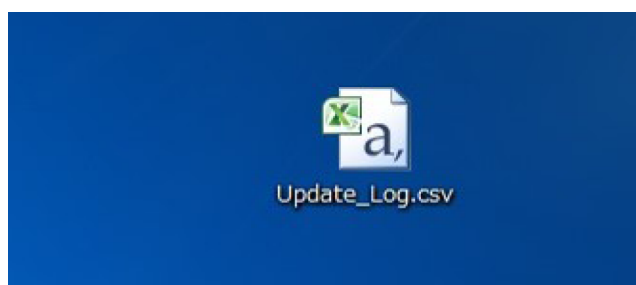
- 1 Kliknąć przycisk dziennika aktualizacji (Update Log).



- 2 Sprawdzić status pobierania na pasku pobierania u dołu okna.



- 3 Odszukać i kliknąć dwukrotnie (w celu otwarcia) pobrany plik .csv (Update_Log.csv) dziennika aktualizacji.



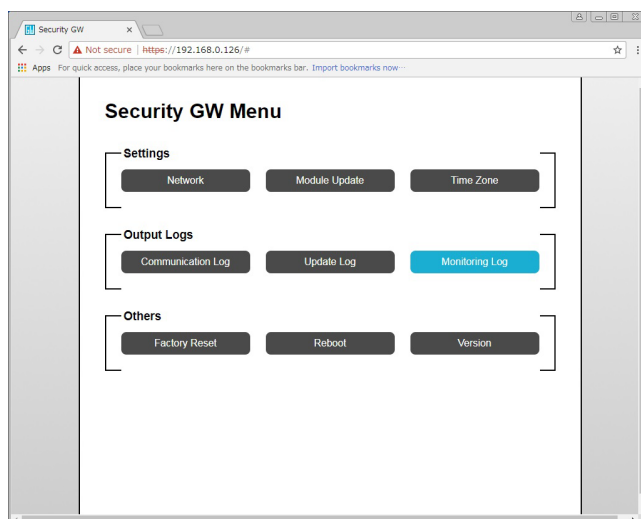
- 4 Zapoznać się z zawartością pliku .csv (Update_Log.csv) dziennika aktualizacji.

	A	B	C	D	E	F	G	H
1	2017/10/25 8:41	check	0					
2	2017/10/25 8:41	check	0					
3	2017/10/25 8:41	check	0					
4	2017/10/25 8:41	check	0					
5	2017/10/25 8:41	check	0					
6	2017/10/25 8:41	check	0					
7	2017/10/25 8:41	check	0					
8	2017/10/25 8:41	check	0					
9	2017/10/25 8:41	check	0					
10	2017/10/25 8:41	check	0					
11	2017/10/25 8:41	check	0					
12	2017/10/25 8:41	check	0					
13	2017/10/25 8:41	check	0					
14	2017/10/25 8:41	check	0					
15	2017/10/25 8:41	check	0					
16	2017/10/25 8:41	check	0					
17	2017/10/25 8:41	check	0					
18	2017/10/25 8:41	check	0					
19	2017/10/25 8:41	check	0					
20	2017/10/25 8:41	check	0					
21	2017/10/25 8:41	check	0					
22	2017/10/25 8:41	check	0					
23	2017/10/25 8:41	check	0					

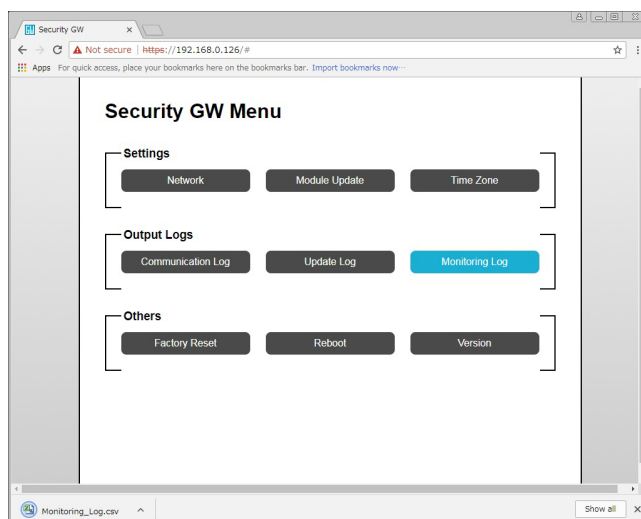
5.1.3 Pobieranie dzienników monitorowania

Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

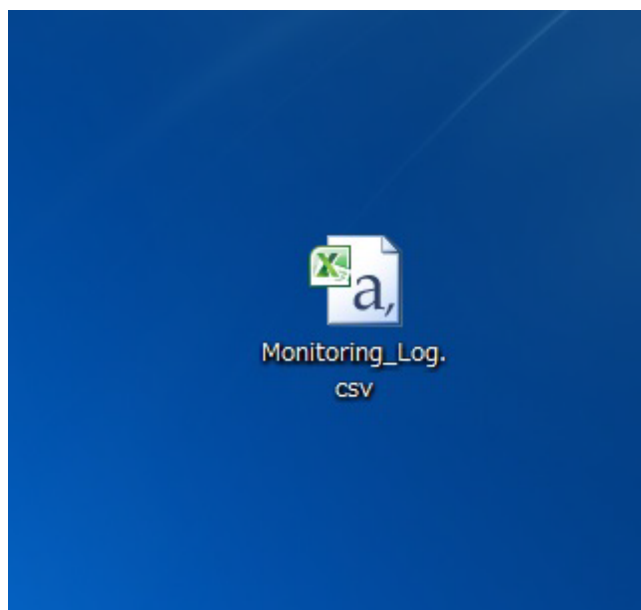
- 1 Kliknąć przycisk dziennika monitorowania (Monitoring Log).



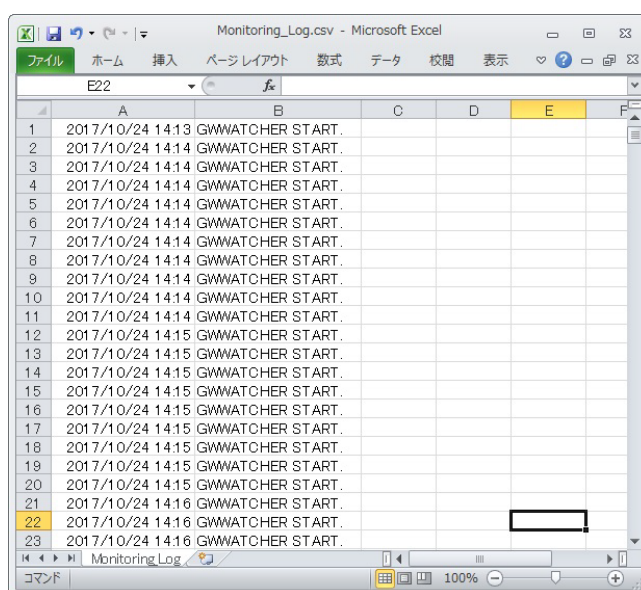
- 2 Sprawdzić status pobierania na pasku pobierania u dołu okna.



- 3 Odszukać i kliknąć dwukrotnie (w celu otwarcia) pobrany plik .csv (Monitoring_Log.csv) dziennika monitorowania na pulpicie.



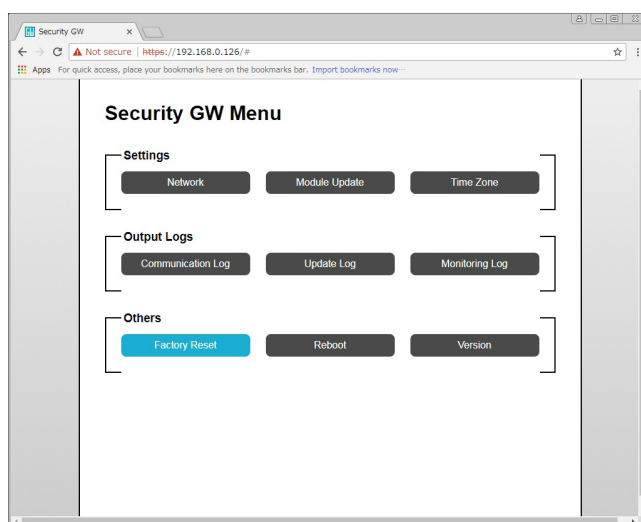
- 4 Zapoznać się z zawartością pliku .csv (Monitoring_Log.csv) dziennika monitorowania.



5.2 Przywracanie ustawień fabrycznych bramy Security gateway

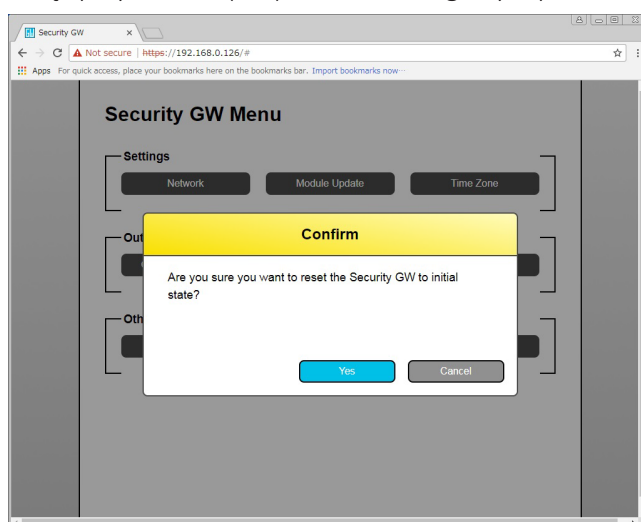
Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

- 1 Kliknąć przycisk przywracania ustawień fabrycznych (Factory reset).



Wynik: Zostanie wyświetlone okno dialogowe potwierdzenia (Confirm).

- 2 Kliknąć przycisk Tak (Yes) w oknie dialogowym potwierdzenia.

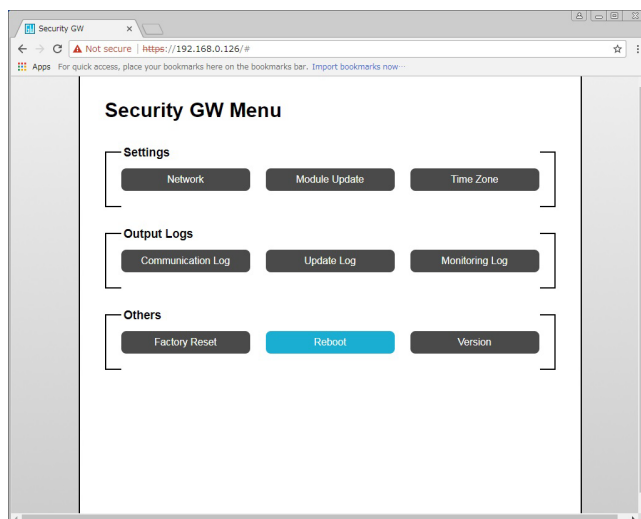


Wynik: Zostaną przywrócone pierwotne ustawienia bramy Security gateway określone przez producenta.

5.3 Restartowanie bramy Security gateway

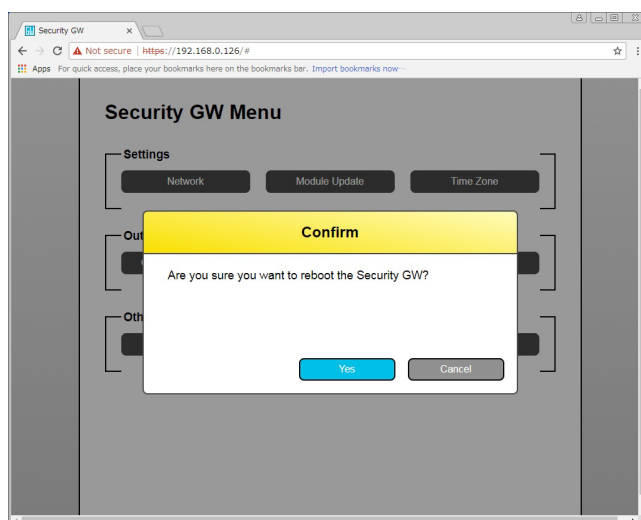
Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

- 1 Kliknąć przycisk restartu (Reboot).

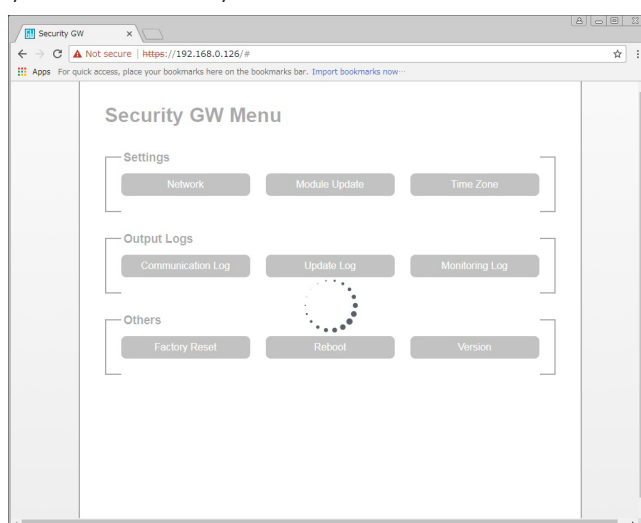


Wynik: Zostanie wyświetlone okno dialogowe potwierdzenia (Confirm).

2 Kliknąć przycisk Tak (Yes).



Wynik: Okno dialogowe potwierdzenia zniknie, a wszystkie przyciski będą wyszarzone i nieaktywne.



Wynik: Nastąpi restart bramy Security gateway.

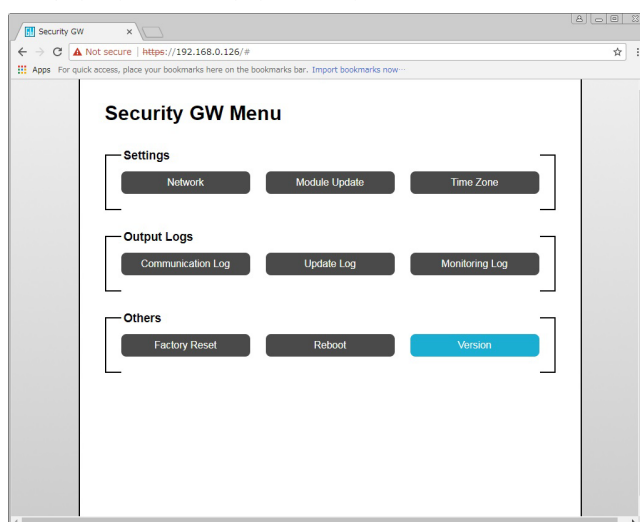
5.4 Odczytywanie numerów wersji

W niektórych przypadkach może być konieczne podanie numerów wersji bramy Security gateway. Za pośrednictwem menu aplikacji WWW można odczytać wersje następujących komponentów:

- Aplikacja WWW (działająca w przeglądarce oraz narzędzie konfiguracyjne bramy Security gateway) bramy Security gateway; [Client Version]
- Wersja sprzętu, oprogramowania sprzętowego i systemu operacyjnego. [Security GW Version]
- Unikalny numer seryjny bramy Security gateway. [Security GW Number]

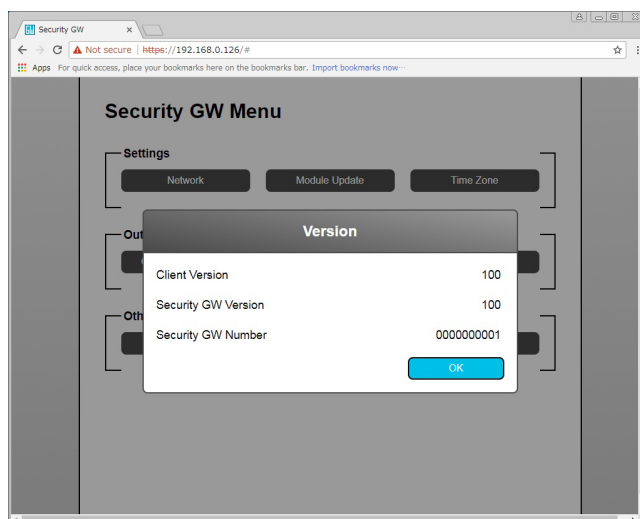
Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

- 1 Kliknąć przycisk wersji (Version).



Wynik: Zostanie wyświetlone okno dialogowe wersji (Version).

- 2 Odczytać wersje.



- 3 Kliknąć przycisk OK (OK), aby wrócić do ekranu głównego.

Wynik: Zostanie wyświetlony ekran główny.

6 Rozwiązywanie problemów

6.1 Potencjalne niepowodzenia

Niepowodzenie	Przyczyna	Rozwiązanie
Niepowodzenie połączenia	Nie można połączyć się z bramą Security gateway. Sprawdzić zasilanie.	Upewnić się, że WŁAŚCIWA KARTA SD jest PRAWIDŁOWO włożona do gniazda na kartę SD. Upewnić się, że zasilanie bramy Security gateway jest WŁĄCZONE. Sprawdzić ADRES IP bramy Security gateway i komputera PC używanego do konfiguracji. Upewnić się, że należą do tej samej sieci lokalnej. Upewnić się, że używane i wybrane są WŁAŚCIWE porty LAN: - Lewa strona: Port A - Prawa strona: Port B ZRESTARTOWAĆ bramę Security gateway * W przypadku zapomnienia adresu IP bramy Security gateway należy użyć specjalnego narzędzia konfiguracyjnego, tak jak opisano to w sekcji "8.2 Wykrywanie adresu IP" [▶ 37].
Niepowodzenie konfiguracji	Nie udaje się: ▪ Wykonać konfiguracji. ▪ Pobrać plików dzienników. ▪ Przywrócić ustawień fabrycznych. ▪ Zrestartować. ▪ Odczytać wersji.	WYLOGOWAĆ SIĘ z aplikacji WWW do konfiguracji bramy Security gateway lub z narzędzia do konfiguracji bramy Security gateway. Z powrotem ZALOGOWAĆ SIĘ do aplikacji WWW do konfiguracji bramy Security gateway lub do narzędzia do konfiguracji bramy Security gateway. Ponownie SPRÓBOWAĆ wykonać konfigurację, pobrać plik dziennika, przywrócić ustawienia fabryczne, zrestartować lub odczytać wersję.

6.2 Komunikaty o błędach

Kategoria	Opis	Uwagi
1. Niepoprawne środowisko Javascript	1.1 Obsługa Javascript niedostępna. Włączyć obsługę Javascript i spróbować ponownie.	—
2. Niepoprawny plik cookie	2.1 Wyłączona obsługa plików cookie. Włączyć obsługę plików cookie w preferencjach w przeglądarce i spróbować ponownie.	—

Kategoria	Opis	Uwagi
3. Połączenie z bramą Security gateway	3.1 Nie udało się nawiązać połączenia z bramą Security gateway. Sprawdzić, czy brama Security gateway jest podłączona do tej samej sieci.	—
4. Logowanie	4.1 Nie wprowadzono jeszcze identyfikatora użytkownika i/lub hasła.	Wprowadzić identyfikator użytkownika i hasło. Kliknąć przycisk [Sign in].
	4.2 Uwierzytelnianie nie powiodło się. Niepoprawny identyfikator użytkownika i/lub hasło.	Zweryfikować identyfikator użytkownika i hasło. Wprowadzić poprawny identyfikator użytkownika i hasło. Kliknąć przycisk [Sign in].
	4.3 Niepowodzenie komunikacji z bramą Security gateway.	Upewnić się, że karta SD jest włożona do gniazda na kartę SD. Upewnić się, że zasilanie bramy Security gateway jest włączone. Upewnić się, że przewód sieci LAN jest podłączony zarówno do bramy Security gateway, jak i do komputera PC używanego do konfiguracji. Nacisnąć przycisk resetowania na bramie Security gateway.
5. Menu bramy Security gateway	5.1 Niepowodzenie komunikacji z bramą Security gateway.	Patrz 4.3
	5.2 Tworzenie dziennika nie powiodło się.	—
6. Konfiguracja sieci	6.1 Niepowodzenie komunikacji z bramą Security gateway.	Patrz 4.3
7. Konfiguracja aktualizacji modułów	7.1 Niepowodzenie komunikacji z bramą Security gateway.	Patrz 4.3
8. Ustawienia strefy czasowej	8.1 Niepowodzenie komunikacji z bramą Security gateway.	Patrz 4.3
9. Okno dialogowe o błędzie	9.1 Sesja wygasła. Zalogować się ponownie.	—

7 Dane techniczne

7.1 Wymagania dotyczące komputera służącego do rozruchu

Element	Parametry techniczne
System operacyjny	Windows 7 Professional (32-bitowy) lub nowsza wersja
Pamięć	Minimum 2 GB RAM
Dysk twardy	Minimum 20 GB wolnego miejsca na dysku twardym
Porty	1 port RJ-45
Przeglądarka	Jedna z następujących: ▪ Internet Explorer w wersji 9, 10 lub 11 ▪ Google Chrome ▪ Mozilla Firefox ▪ Apple Safari

7.2 Pobór mocy przez bramę Security gateway

Element	Parametry techniczne
Znamionowe napięcie wejściowe	110~220 V AC
Częstotliwość zasilania	50~60 Hz
Pobór energii modułów CPU + we/wy	▪ Maks.: 13 W (11 W+2 W) ▪ Typowa wartość: 5,5 W (4 W+1,5 W)

Szczegółowe dane dotyczące zasilania można znaleźć w podręczniku dołączonym do zasilacza.

7.3 Domyślne hasła narzędzi

Narzędzie	Hasło
Kod uwierzytelniania do interfejsu WWW bramy Security gateway	Nie ustawione (puste), patrz "Dostęp do bramy Security gateway" [▶ 16] ▪ Domyślny identyfikator Daikin ▪ Domyślne hasło: Daikin

7.4 Wymagania dotyczące przewodów elektrycznych bramy Security gateway



OSTRZEŻENIE

Okablowanie i elementy elektryczne MUSZĄ być montowane przez uprawnionego elektryka i zgodne z odpowiednimi przepisami.

Wszystkie przewody muszą spełniać następujące wymagania:

Połączenie	Przekrój poprzeczny	Maks. długość	Uwagi
Przewód sieci LAN	—	100 m	- UTP KAT 5e lub wyższa - Złącze RJ45
DIII-NET (F1/F2)	$\varnothing 0,75 \sim 1,25 \text{ mm}^2$ (złącze przystosowane do przekroju maks. $1,5 \text{ mm}^2$)	Długość całkowita ^(a) : 2000 m (<1500 m w przypadku przewodu ekranowanego) Maks. długość ^(b) : 1000 m	- Typ kabla: kabel 2-żyłowy w izolacji z winylu z osłoną z winylu/winyłowy kabel wielożyłowy lub 2-żyłowy kabel w osłonie - NIE należy używać kabli wielożyłowych o co najmniej trzech żyłach - NIE stosować kabli różnych typów - NIGDY nie zbierać kabli w wiązki - W przypadku korzystania z kabli ekranowanych należy podłączać do masy tylko jeden koniec każdego przewodu ekranu. - Należy upewnić się, że przewody zostały poprowadzone i unieruchomione, tak aby NIE doszło do zetknięcia z nieziemionymi łatwodostępnymi podzespołami przewodzącymi prąd elektryczny - Należy upewnić się, że dla każdego przewodu wprowadzonego do skrzynki elektrycznej pozostawiono pewien luz - Więcej informacji dotyczących sieci DIII-NET można znaleźć w podręczniku projektowania D-BACS (ED72-721)
Zasilanie 230 V AC modułu PU	Zgodnie z odpowiednimi przepisami (złącze przystosowane do przekroju maks. 4 mm^2)	Zgodnie z obowiązującymi przepisami	- Dozwolone żyły lite lub skrętka - Ochronę wewnętrzną modułu PSU WAGO stanowi bezpiecznik 2,5 A / 250 V
Zasilanie 24 V DC modułu Security gateway	Zgodnie z obowiązującymi przepisami	—	Dozwolone żyły lite lub skrętka

(a) Całkowita długość jest sumą wszystkich przewodów w sieci DIII-NET.

(b) Maks. długość to maksymalna odległość między dowolnymi 2 punktami w sieci DIII-NET.

7.5 Wymagania systemowe

Komputer PC używany do konfigurowania bramy Security gateway musi spełniać następujące minimalne wymagania:

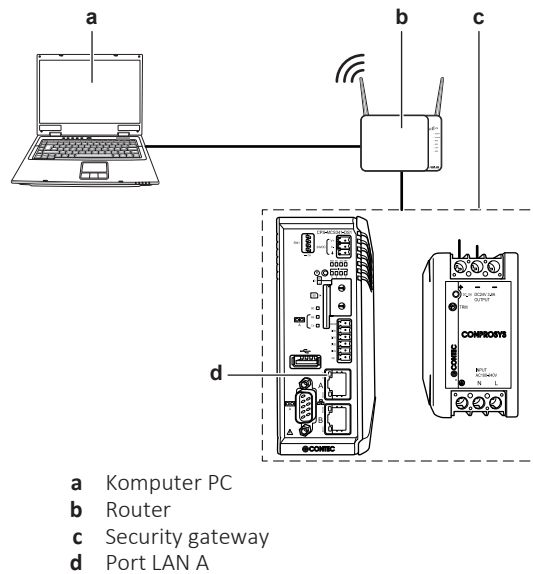
Procesor	Intel i3 2,2 GHz lub szybszy
System operacyjny	Microsoft Windows 7 lub wyższa wersja
Pamięć	Minimum 512 MB RAM
Wolne miejsce na dysku twardym	Co najmniej 10 GB
Sieć	10 BASE-T lub szybsza

8 Dodatek A — Informacje o wykrywaniu adresu IP bramy Security gateway

W tym dodatku wyjaśniono, w jaki sposób wykryć adres IP bramy Security gateway, korzystając ze specjalnego narzędzia konfiguracyjnego.

8.1 Podłączanie bramy Security gateway

- 1 Podłączyć zasilanie tak, jak opisano to w sekcji "[Podłączanie przewodów zasilających](#)" [► 10].
- 2 Dodać bramę Security gateway do sieci lokalnej tak, jak przedstawiono to na poniższym rysunku:



W tym przypadku będzie używany tylko port LAN A.

- 3 Podłączyć zasilanie.

8.2 Wykrywanie adresu IP

Upewnić się, że posiadana wersja narzędzia do konfiguracji bramy jest jego najnowszą wersją. Najnowsza wersja jest dostępna pod adresem https://my.daikin.eu/denv/en_US/home/applications/product-finder/Daikin-Cloud-Service.html.

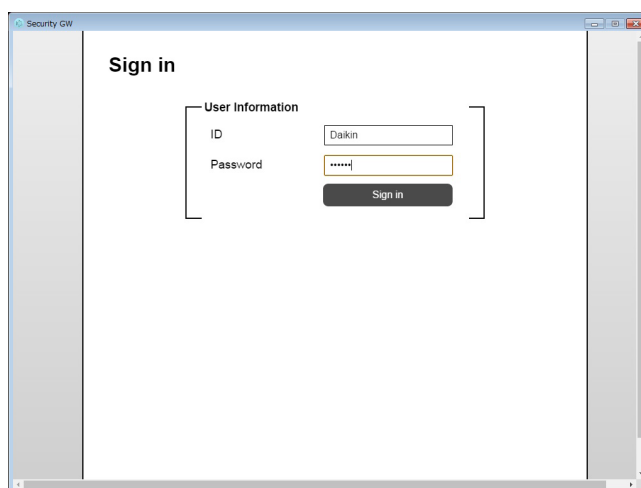
- 1 Pobrać plik ZIP zawierający narzędzie GwSettingTool.exe (GwSettingTool.exe) i rozpakować go do folderu na dysku lokalnym.
- 2 Kliknąć dwukrotnie plik GwSettingTool.exe (GwSettingTool.exe), aby uruchomić narzędzie konfiguracyjne bramy Security gateway.

Wynik: Rozpocznie się nawiązywanie połączenia.



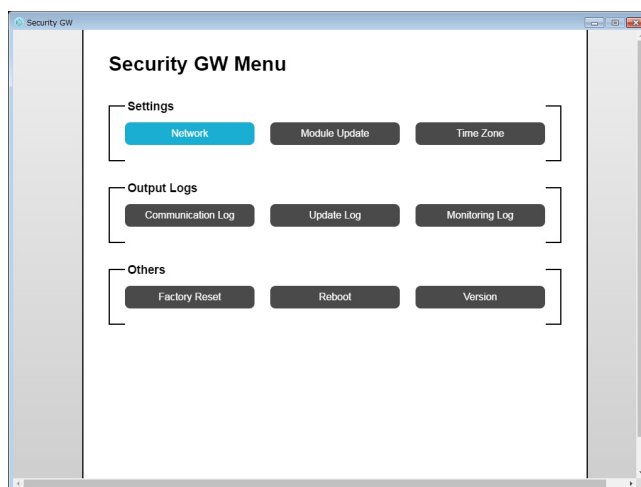
Wynik: Po około 1 minucie zostanie wyświetlone okno logowania.

- 3 Wprowadzić identyfikator (ID) i hasło (Password) (domyślny identyfikator to: Daikin / domyślne hasło to: Daikin) bramy Security gateway i kliknąć przycisk logowania (Sign in).

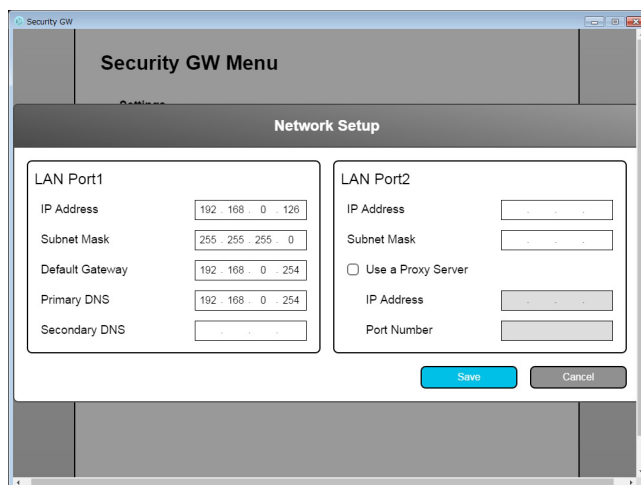


Wynik: Zostanie wyświetlone okno menu bramy Security gateway (Security GW Menu).

- 4 Kliknąć przycisk sieci (Network).



Wynik: Zostanie wyświetlone okno dialogowe ustawień sieci (Network Setup).



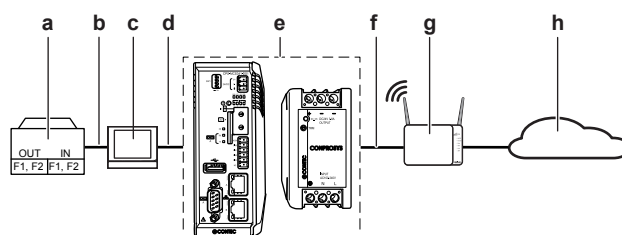
- 5 Odczytać adres IP (IP address) Portu 1 sieci LAN (LAN Port1).

9 Dodatek B — Rozruch w konfiguracji z serwerem proxy

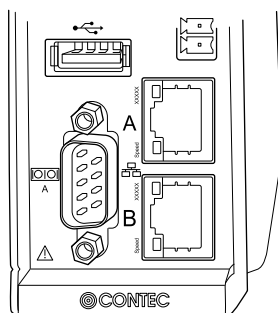
W tym dodatku wyjaśniono, jak wstępnie skonfigurować bramę Security gateway, jeśli topologia sieci różni się od standardowej, opisanej w sekcji "[Konfiguracja sieci lokalnej](#)" [▶ 7].

9.1 Konfiguracja alternatywna

- 1 Podłączyć zasilanie tak, jak opisano to w sekcji "[Podłączanie przewodów zasilających](#)" [▶ 10].
- 2 Dodać bramę Security gateway do sieci lokalnej tak, jak przedstawiono to na poniższym rysunku:



W tym przypadku będzie używany zarówno port LAN A, jak i LAN B.



- a Urządzenie zewnętrzne
- b Połączenie LAN (DIII)
- c Sterownik ITM lub LC8
- d Połączenie LAN do portu A
- e Security gateway
- f Sterownik ITM lub LC8 do portu B
- g Brama sieci LAN (RJ-45)
- h Chmura Daikin Cloud Service

- 3 Podłączyć zasilanie.

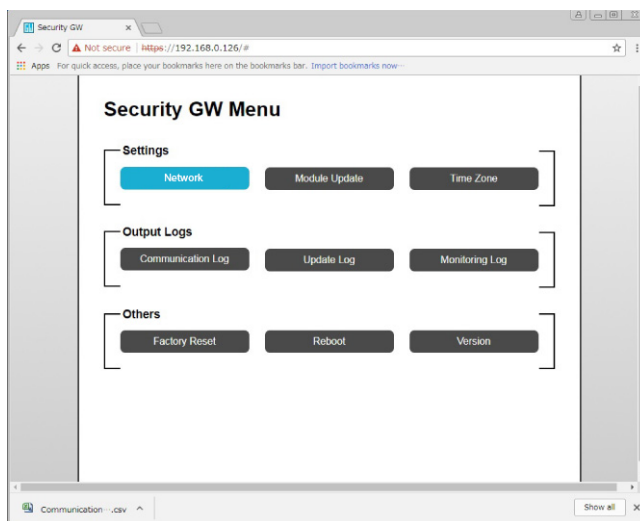
9.2 Dostęp do bramy Security gateway

Patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

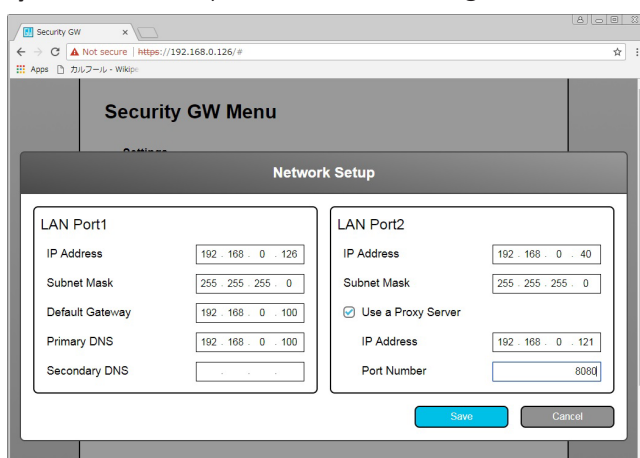
9.3 Konfigurowanie sieci bramy Security gateway

Aby uzyskać dostęp do okna menu bramy Security gateway (Security GW Menu), patrz "[Dostęp do bramy Security gateway](#)" [▶ 16].

- 1 Kliknąć przycisk sieci (Network).



Wynik: Zostanie wyświetlone okno dialogowe ustawień sieci (Network Setup).



2 Wprowadzić następujące dane sieci:

Port 1 sieci LAN (LAN Port1) (=A)

- Adres IP (IP address): Unikalny adres IP (domyślnie: 192.168.0.126) w sieci lokalnej
- Maska podsieci (Subnet mask): 255.255.255.0
- Brama domyślna (Default Gateway): Adres IP (domyślnie: 192.168.0.100) routera lokalnego
- Podstawowy serwer DNS (Primary DNS): Adres IP (domyślnie: 192.168.0.100) routera lokalnego
- Dodatkowy serwer DNS (Secondary DNS): pozostawić puste pole

Port 2 sieci LAN (LAN Port2) (=B)

- Adres IP (IP address): wybrać adres z innego zakresu niż dla portu A (np. 192.168.10.5)
- Maska podsieci (Subnet mask): 255.255.255.0
- Użyj serwera proxy (Use a Proxy Server): Zaznaczone
- Adres IP (IP address): Adres IP serwera proxy
- Numer portu (Port Number): Numer portu serwera proxy

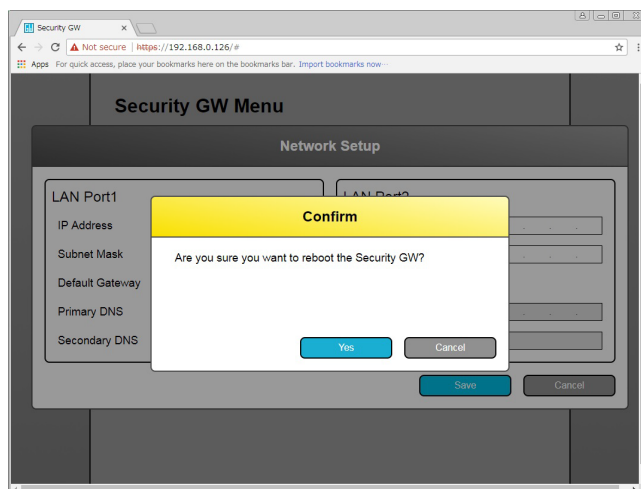
**INFORMACJE**

Jeśli adres IP (IP address), brama domyślna (Default gateway) i podstawowy serwer DNS (Primary DNS) są skonfigurowane zgodnie z ustawieniami sieci lokalnej, nie trzeba ich zmieniać.

- 3 Kliknąć przycisk zapisu (Save).

Wynik: Zostanie wyświetlone okno dialogowe potwierdzenia (Confirm).

- 4 Kliknąć przycisk Tak (Yes), aby zrestartować bramę Security gateway.



Wynik: Spowoduje to restart bramy Security gateway.

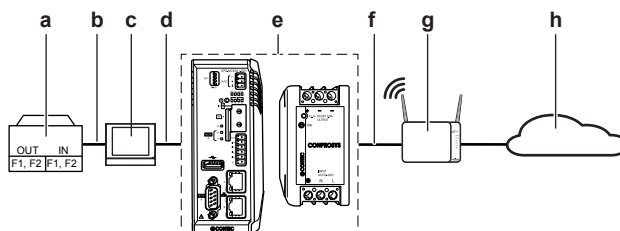
Wynik: Zostanie wyświetlone okno przeglądarki.

Wynik: Adres IP będzie zmieniony.

**INFORMACJE**

Po wykonaniu kroku 4 komunikacja z przeglądarką WWW zostanie utracona. Wykonać procedurę opisaną w sekcji "[Dostęp do bramy Security gateway](#)" [▶ 16], aby ponownie nawiązać połączenie, używając nowego adresu IP.

- 5 Zresetować ustawienia sieci LAN komputera, przywracając wartości domyślne.
- 6 Włączyć kartę WiFi komputera, jeśli wcześniej została wyłączona.
- 7 Rozłączyć przewód sieci Ethernet między komputerem a modułem Security gateway.
- 8 Podłączyć przewód sieci Ethernet między modułem Security gateway a siecią lokalną.



9.4 Konfigurowanie strefy czasowej bramy Security gateway

Patrz "[Konfigurowanie strefy czasowej bramy Security gateway](#)" [▶ 21].

9.5 Pierwszy rozruch sterownika iTM lub LC8

Patrz:

- Podręcznik Airnet:
 - Pierwszy rozruch sterownika iTM lub LC8
 - Format: Pliki w formacie cyfrowym dostępne pod adresem <http://www.daikineurope.com/support-and-manuals/product-information/>
- Instrukcja instalacji sterownika iTM
- Instrukcja instalacji sterownika LC8

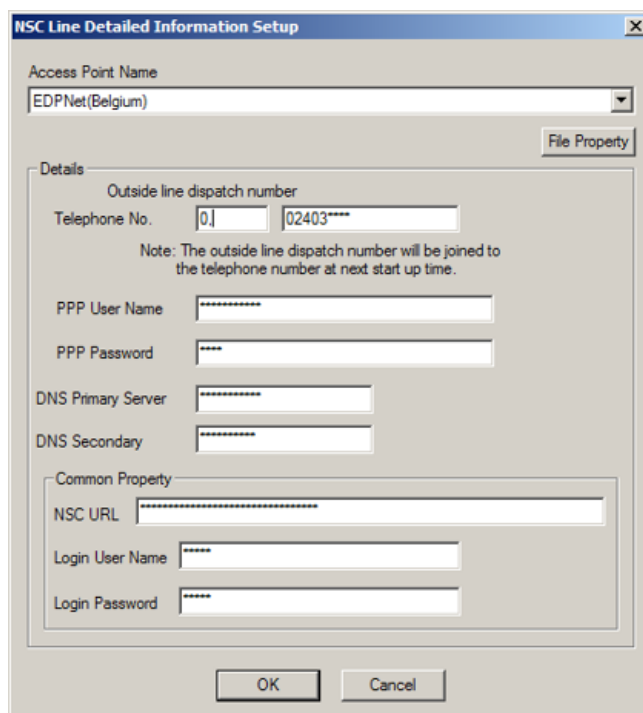
Następne kroki różnią się od opisanych w Podręczniku Airnet. Należy dopilnować, aby ustawienia w sterowniku iTM lub LC8 były takie, jak opisano to w kroku 1.

- 1 Skonfigurować sieć sterownika lokalnego zgodnie z poniższą tabelą.

iTM

LC8

- 2 Wybrać adres URL NSC <http://Lcc.m2m.daikineurope.com/NSC> i wybrać poprawną nazwę punktu dostępu (Access Point Name) z listy wyboru. Sekcja szczegółów (Details) może pozostać pusta.



NSC Line Detailed Information Setup

Access Point Name
EDPNet(Belgium)

File Property

Details

Outside line dispatch number
Telephone No. 0 02403****

Note: The outside line dispatch number will be joined to the telephone number at next start up time.

PPP User Name

PPP Password

DNS Primary Server

DNS Secondary

Common Property

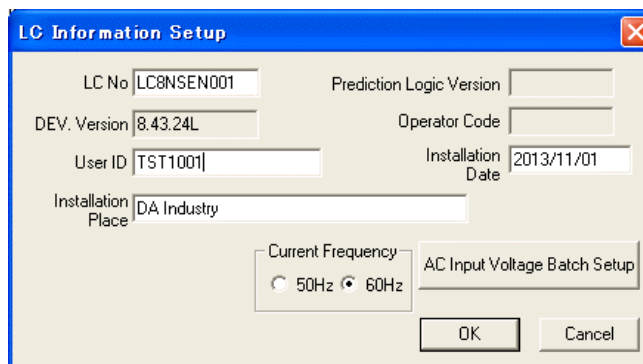
NSC URL

Login User Name

Login Password

OK Cancel

- 3 Wprowadzając dane uwierzytelniające chmury Daikin Cloud Service, nawiązać połączenie z witryną <https://cloud.daikineurope.com> i utworzyć nową lokalizację. Po utworzeniu lokalizacji zanotować numer iTM lub LC8:
 - Numer iTM: Zarejestrowany numer identyfikacyjny urządzenia intelligent Touch Manager. Numer ten będzie mieć następujący format: LT2N##### (gdzie # jest znakiem alfanumerycznym).
 - Numer LC8: Zarejestrowany numer identyfikacyjny sterownika LC8. Numer ten będzie mieć następujący format: LC8N##### (gdzie # jest znakiem alfanumerycznym).



LC Information Setup

LC No LC8NSEN001 Prediction Logic Version

DEV. Version 8.43.24L Operator Code

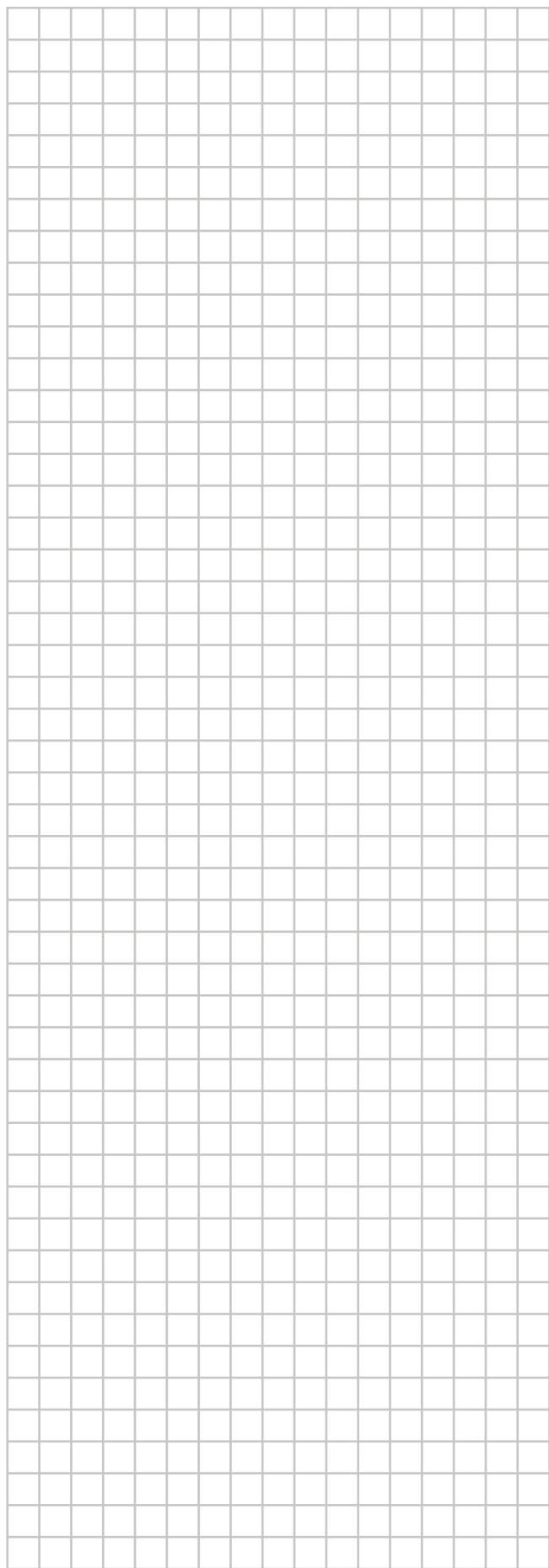
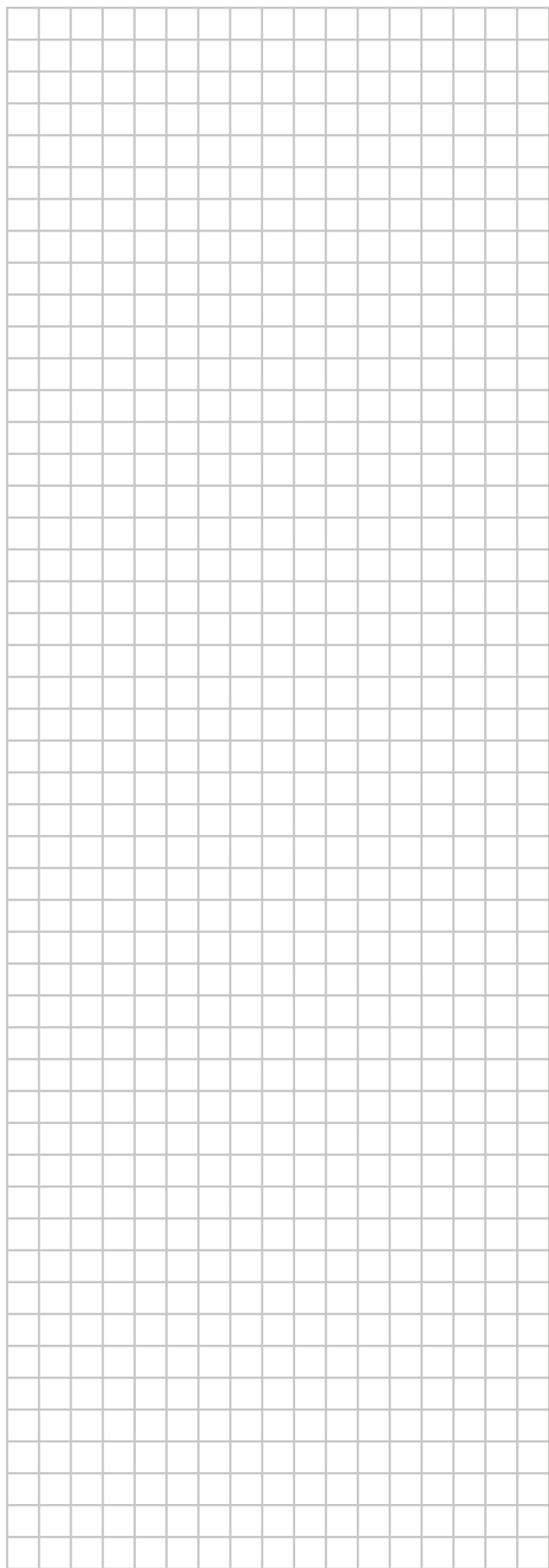
User ID TST1001 Installation Date 2013/11/01

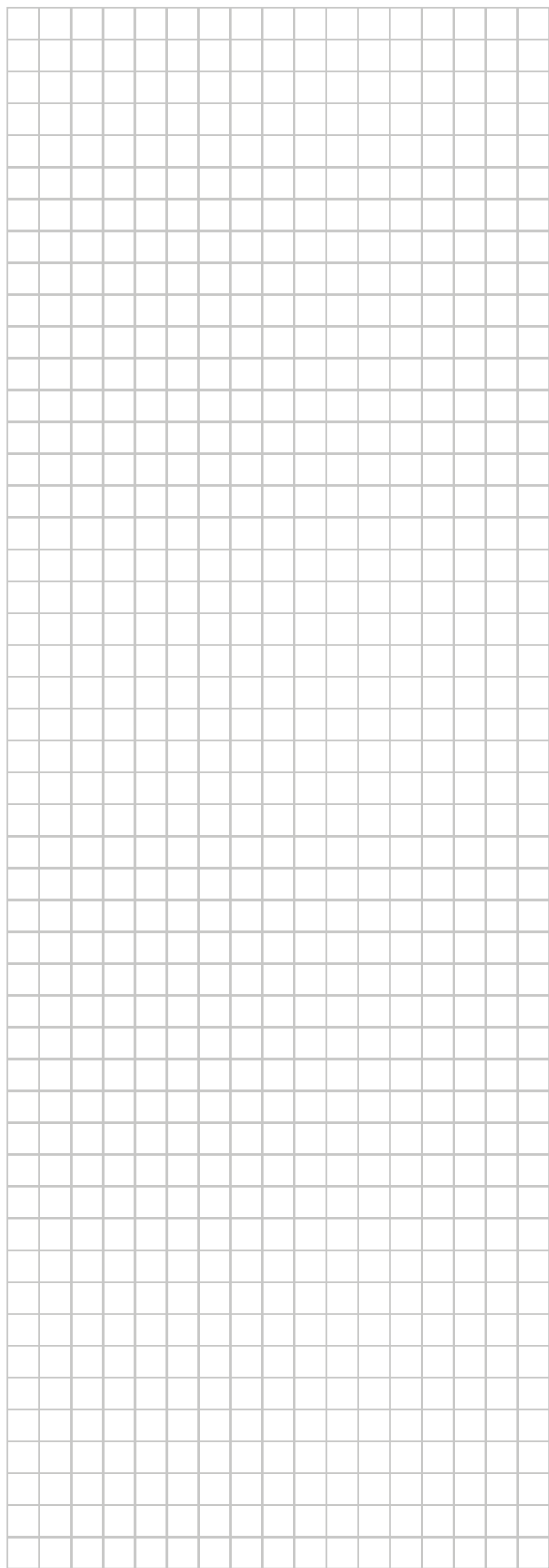
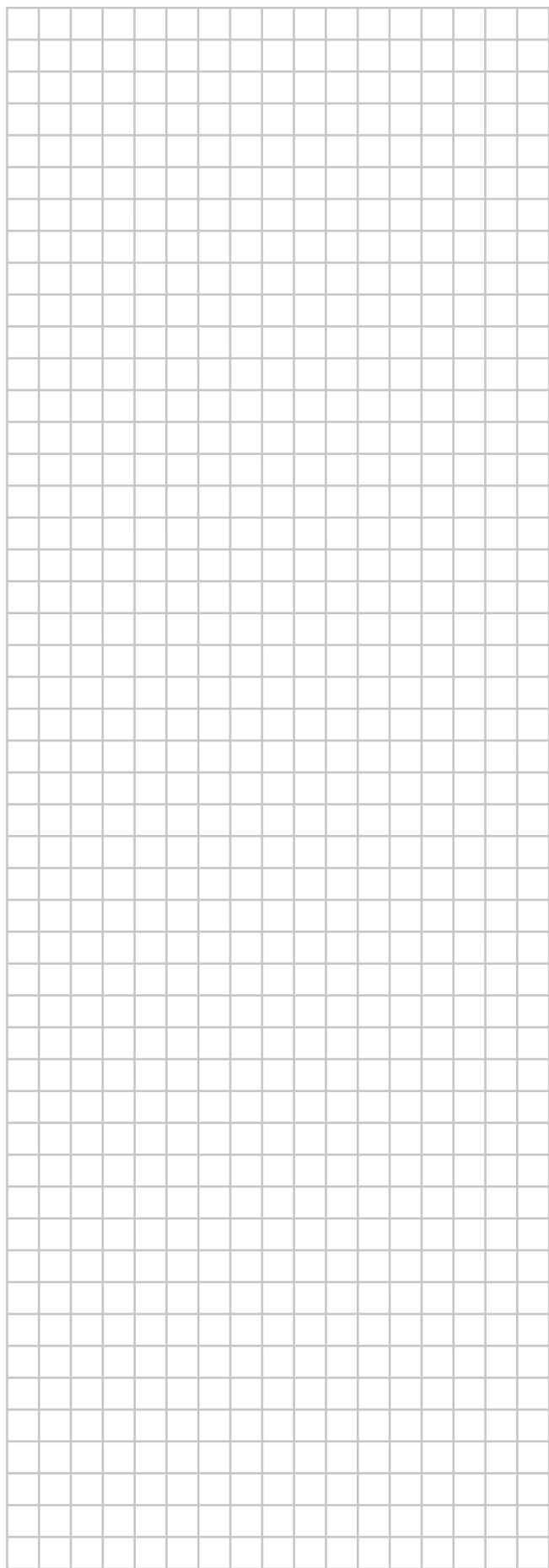
Installation Place DA Industry

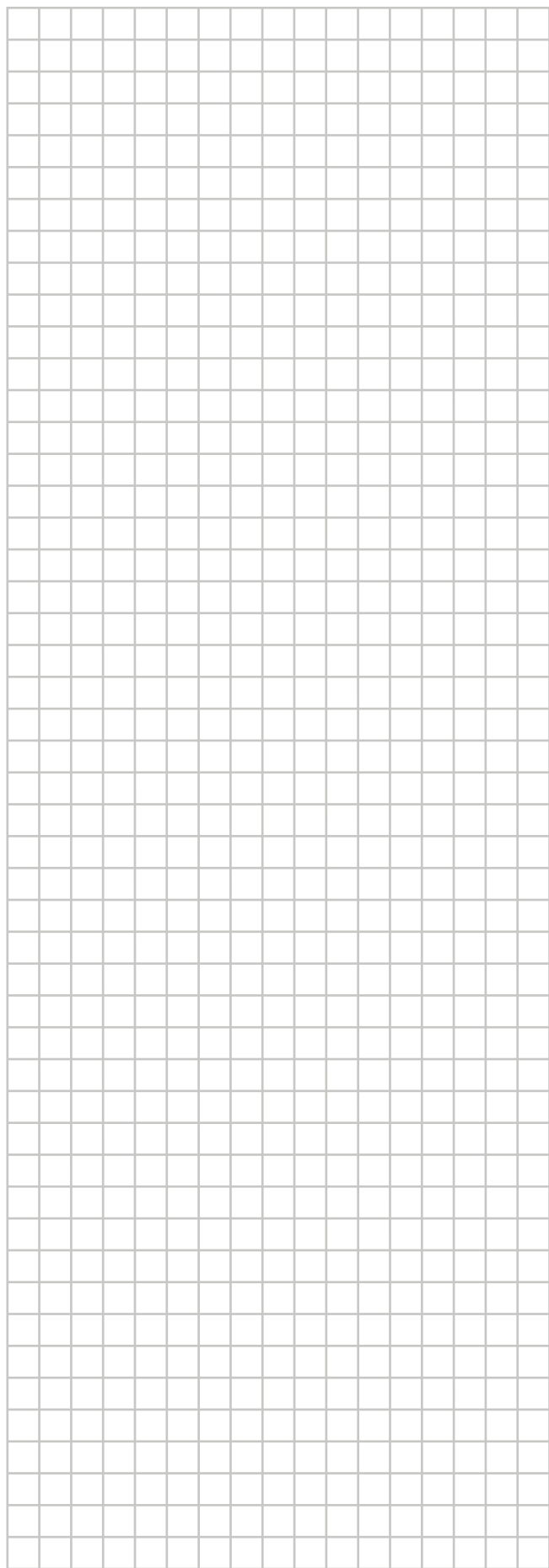
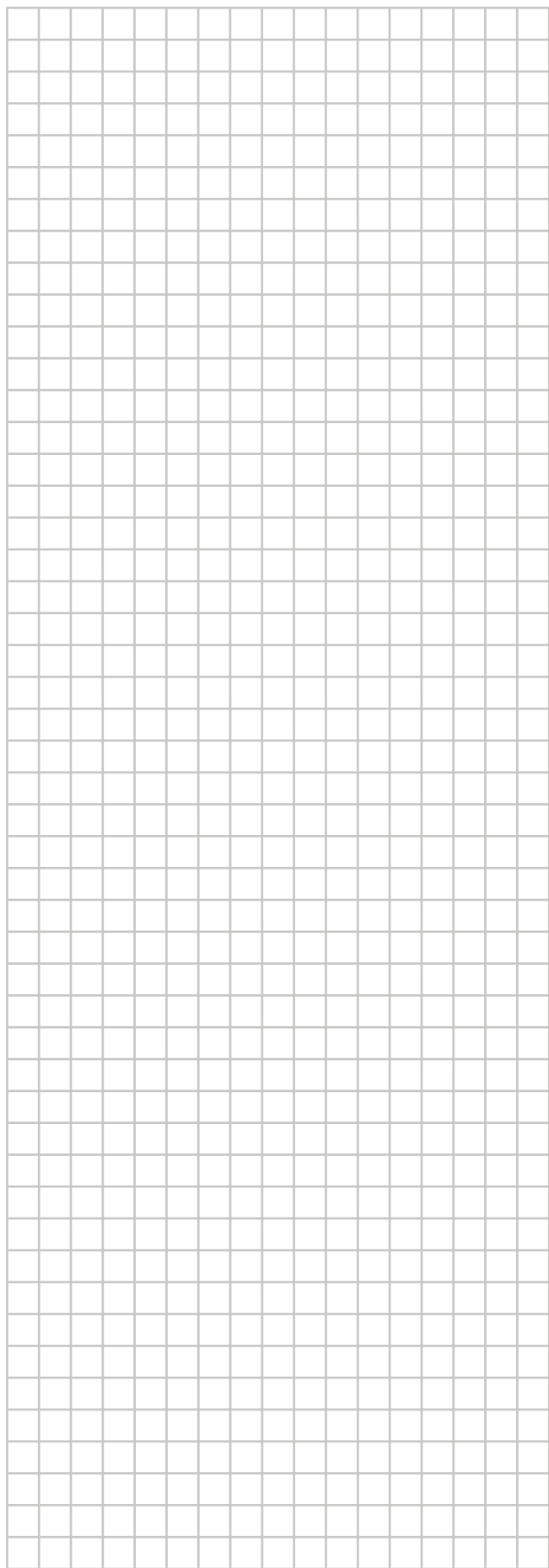
Current Frequency
☐ 50Hz ☒ 60Hz

AC Input Voltage Batch Setup

OK Cancel







ERC

Copyright 2018 Daikin

DAIKIN EUROPE N.V.

Zandvoordestraat 300, B-8400 Oostende, Belgium

4P529063-1A 2020.12