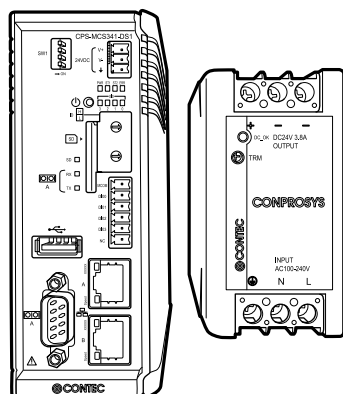


Справочно ръководство на монтажника

Security шлюз



Съдържание

1	За настоящия документ	3
2	Монтаж	4
2.1	Общи предпазни мерки за безопасност.....	4
2.1.1	Общи изисквания.....	4
2.1.2	Място за монтаж.....	5
2.1.3	Електрически.....	5
2.2	Оборудване на Daikin система.....	6
2.3	Описание на системата.....	6
2.3.1	Настройка на локална мрежа.....	7
2.3.2	Спецификации.....	8
2.4	Преди монтажа.....	8
2.4.1	Необходимо оборудване.....	8
2.4.2	За местоположението на клемите.....	8
2.5	За монтиране на 2-те компонента на хардуера на Security шлюз.....	9
2.6	За електрическите проводници.....	10
2.6.1	За свързване на захранването.....	10
2.6.2	За свързване на Security шлюз към локалната мрежа.....	11
3	Пускане в експлоатация	13
3.1	За пускане в експлоатация на настройка на Security шлюз.....	13
3.2	Минимални изисквания за пускане в употреба.....	13
3.3	За свързване към Security шлюз за първи път.....	14
3.4	За конфигуриране на Security шлюз.....	17
3.4.1	За получаване на достъп до Security шлюз.....	17
3.4.2	За настройка на мрежата на шлюза за сигурност.....	19
3.4.3	За настройка на часовата зона на шлюза за сигурност.....	21
4	За пускане в експлоатация на iTM или LC8 контролер	23
5	Работа	25
5.1	За изтегляне на логове.....	25
5.1.1	За изтегляне на комуникационни логове.....	25
5.1.2	За изтегляне на логове за актуализация.....	26
5.1.3	За изтегляне на логове за мониторинг.....	28
5.2	За връщане на Security шлюз към фабрични настройки.....	30
5.3	За рестартиране на Security шлюз.....	30
5.4	За проверка на номера на версии.....	32
6	Отстраняване на проблеми	33
6.1	Възможни неизправности.....	33
6.2	Съобщения за грешка.....	33
7	Технически спецификации	35
7.1	Изисквания към компютъра за пускане в употреба.....	35
7.2	Спецификации на консумацията на енергия Security шлюз.....	35
7.3	Подразбиращи се пароли на средствата.....	35
7.4	Изисквания към окабеляването Security шлюз.....	36
7.5	Изисквания към системата.....	36
8	Приложение А – За откриване на IP адреса на шлюза за сигурност	38
8.1	За окабеляване на Security шлюз.....	38
8.2	За откриване на IP адреса.....	38
9	Приложение В – За пускането в експлоатация в случай на прокси сървър	41
9.1	Алтернативна настройка.....	41
9.2	За получаване на достъп до Security шлюз.....	41
9.3	За настройка на мрежата на шлюза за сигурност.....	41
9.4	За настройка на часовата зона на шлюза за сигурност.....	43
9.5	За пускане в експлоатация на iTM или LC8 контролер.....	44

1 За настоящия документ

Целева публика

Упълномощени монтажници

Комплект документация

Този документ е част от комплекта документация. Пълният комплект се състои от:

▪ Ръководство за монтаж:

- Инструкции за монтаж
- Формат: Хартия (доставя се в комплекта)

▪ Справочно ръководство на монтажника:

- Подготовка за монтаж, референтни данни,...
- Формат: Дигитални файлове на <http://www.daikineurope.com/support-and-manuals/product-information/>

▪ Наръчник за Airnet:

- Пускане в експлоатация на iTM или LC8 контролер
- Формат: Дигитални файлове на <http://www.daikineurope.com/support-and-manuals/product-information/>

▪ Ръководство за монтаж на Intelligent Touch Manager (DCM601A51):

- Инструкции за монтаж
- Формат: Дигитални файлове на <http://www.daikineurope.com/support-and-manuals/product-information/>

▪ Ръководство за монтаж на LC8 (DLC602B51):

- Инструкции за монтаж
- Формат: Дигитални файлове на <http://www.daikineurope.com/support-and-manuals/product-information/>

Последните редакции на доставената документация може да са налични на регионалния уебсайт на Daikin или да ги получите чрез вашия дилър.

Оригиналната документация е написана на английски език. Всички други езици са преводи.

Технически данни

- **Извадка** от най-новите технически данни може да се намери на регионалния Daikin уеб сайт (публично достъпен).
- Пълният комплект с най-новите технически данни може да се намери в Daikin Business Portal (изисква се автентификация).

2 Монтаж

2.1 Общи предпазни мерки за безопасност

Моля, прочетете внимателно тези общи предпазни мерки за безопасност преди да монтирате климатичното оборудване и се уверете, че сте монтирали правилно оборудването.

Неспазването на тези инструкции може да доведе до материални щети или телесни повреди, които могат да бъдат сериозни в зависимост от обстоятелствата.

След приключване на монтажа се уверете, че модулите на захранването и контролера работят правилно по време на стартиране.

Значение на предупреждения и символи

Тези съобщения за безопасност се използват, за да привлекат вниманието ви. Значението на всяко съобщение за безопасност е описано по-долу:



ПРЕДУПРЕЖДЕНИЕ

Обозначава ситуация, което е възможно да причини смърт или тежко нараняване.



ВНИМАНИЕ

Обозначава ситуация, което е възможно да причини леко или средно нараняване.



ОПАСНОСТ

Обозначава ситуация, което причинява смърт или тежко нараняване.



ОПАСНОСТ: ОПАСНОСТ ОТ ЕКСПЛОЗИЯ

Обозначава ситуация, която е възможно да предизвика експлозия.



ИНФОРМАЦИЯ

Обозначава полезни съвети или допълнително информация.



ЗАБЕЛЕЖКА

Обозначава ситуация, което е възможно да причини увреждане на оборудването или на имуществото.

2.1.1 Общи изисквания

Ако НЕ сте сигурни как да монтирате или да работите с модула, свържете се с вашия дилър.



ПРЕДУПРЕЖДЕНИЕ

Неправилният монтаж или присъединяване на оборудване или аксесоари е възможно да причини токов удар, късо съединение, утечки, пожар или други повреди на оборудването. Използвайте само аксесоари, допълнително оборудване и резервни части, които са изработени или одобрени от Daikin.

**ПРЕДУПРЕЖДЕНИЕ**

Уверете се, че монтажът, изпитването и използваните материали отговарят на изискванията на приложимото законодателство (в началото на инструкциите, описани в документацията на Daikin).

**ВНИМАНИЕ**

При монтаж, поддръжка или сервизно обслужване на системата носете подходящи лични предпазни средства (предпазни ръкавици, защитни очила и т.н.).

**ПРЕДУПРЕЖДЕНИЕ**

Накъсайте на части и изхвърлете пластмасовите опаковъчни торби, за да не може с тях да си играе никой, и най-вече деца. Възможен риск: задушаване.

2.1.2 Място за монтаж

НЕ инсталирайте оборудването в потенциално експлозивна атмосфера.

2.1.3 Електрически

**ОПАСНОСТ: РИСК ОТ ТОКОВ УДАР**

- ИЗКЛЮЧЕТЕ цялото захранване, преди да свързвате електрическото окабеляване или да докосвате електрически части.
- Разкачете захранването за повече от 10 минути и измерете напрежението при клемите на кондензаторите на главната верига или електрическите компоненти, преди да извършвате сервизно обслужване. Напрежението ТРЯБВА да е по-малко от 50 V DC, преди да можете да докоснете електрическите компоненти. За местоположението на клемите, вижте схемата на окабеляването.
- НЕ докосвайте електрическото оборудване с мокри ръце.
- НЕ оставяйте модула без наблюдение, когато е свален сервизният капак.

**ПРЕДУПРЕЖДЕНИЕ**

В постоянното окабеляване трябва да се интегрира главен превключвател, който има отделяне на контакта във всички полюси, осигуряващ пълно разкачване при условие на свръхнапрежение от категория III.

**ПРЕДУПРЕЖДЕНИЕ**

- Използвайте САМО медни проводници.
- Уверете се, че монтажът на местното окабеляване отговаря на изискванията на приложимото законодателство.
- Цялото окабеляване на място трябва да се извърши съгласно доставената с продукта електромонтажна схема.
- Не забравяйте да монтирате заземяващо окабеляване. НЕ заземявайте модула към водопроводна или газопроводна тръба, преграден филтър за пренапрежения или заземяване на телефон. Неправилното заземяване може да причини токов удар.
- Уверете се, че използвате специално предназначена захранваща верига. НИКОГА не използвайте източник на захранване, който се използва съвместно с друг електрически уред.
- Уверете се, че сте монтирали необходимите предпазители или прекъсвачи.
- Уверете се, че сте монтирали прекъсвач, управляван от утечен ток. Неговата липса може да причини токов удар или пожар.

**ПРЕДУПРЕЖДЕНИЕ**

- След приключване на електротехническите работи потвърдете, че всеки електрически компонент и клема вътре в кутията за електрически компоненти са съединени надеждно.
- Преди да пуснете модула се уверете, че всички капацы са затворени.

2.2 Оборудване на Daikin система

Инсталацията изисква:

- Шлюзът MCS341-DS1-111, резервна част номер EU.SB.5000072. Проводниците за свързване към конвертора на захранването са включени тук.
- Конвертор на захранване AC/DC (PWD-90AW24), резервна част номер 999175A.

И едно от следните:

- iTM контролер, продуктов номер DCM601A51
- LC8 контролер, продуктов номер DLC602B51

За повече информация относно това оборудване, вижте "[4 За пускане в експлоатация на iTM или LC8 контролер](#)" [▶ 23].

Ако има липсващи или дефектни части, обърнете се към доставчика, от който сте закупили продукта.

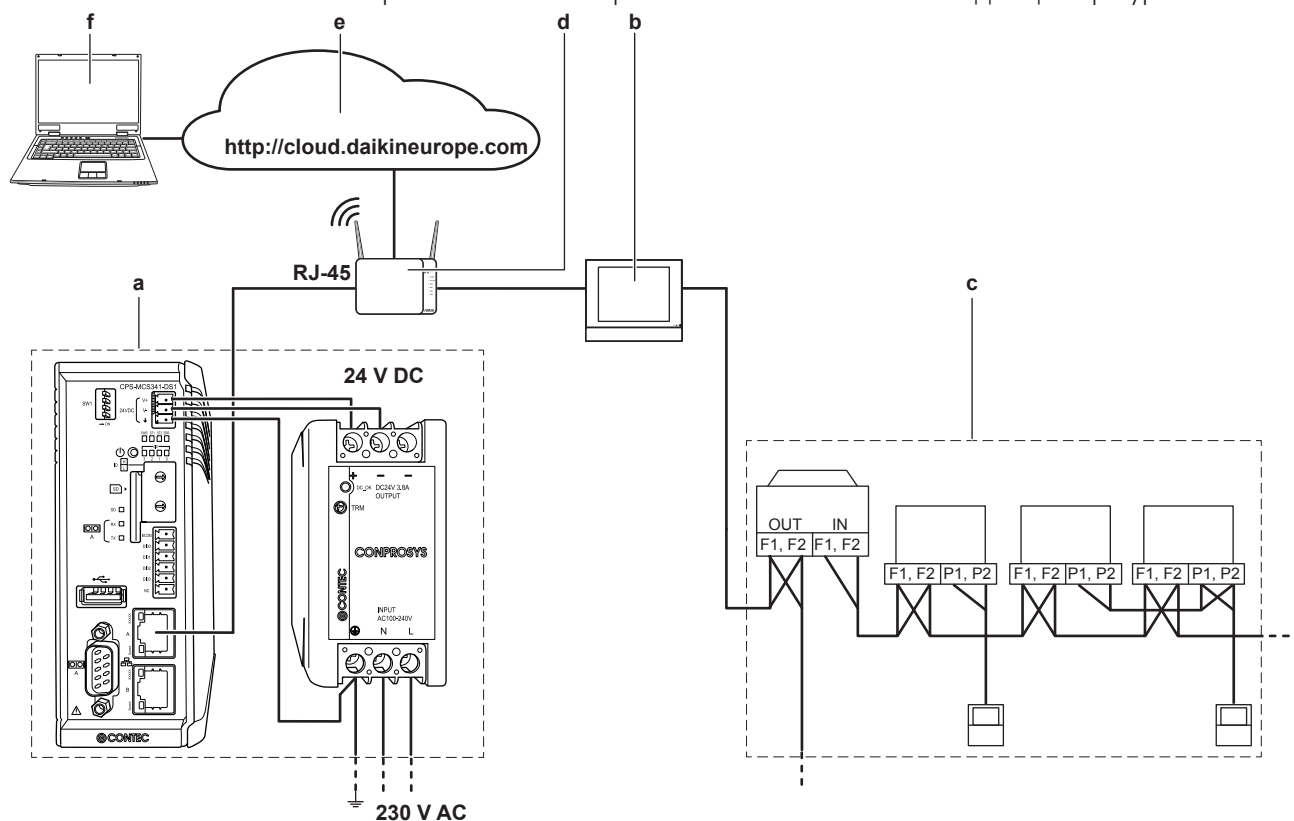
2.3 Описание на системата

Security шлюзът позволява свързване на iTM и LC8 чрез Security шлюз към Daikin Cloud Service.

Сега, вместо директно изпращане на отчета към рутера, iTM или LC8 контролерът изпраща отчета първо към Security шлюза. Security шлюзът трансформира формата на отчета от http на https и след това изпраща трансформирания https отчет към Daikin Cloud Service чрез рутера.

2.3.1 Настройка на локална мрежа

Настройте локалната мрежа както е показано на следващата фигура:



- a Security шлюз
- b iTM или LC8
- c Модули
- d LAN шлюз
- e Daikin Cloud Service
- f Компютър с връзка към Daikin Cloud Service

Таблицата е предназначена само за пример и е приложима само за настройката, показана на изображението по-горе.

	iTM или LC8	Security шлюз	Рутер
IP адрес	192.168.1.50	192.168.1.51	192.168.1.1
Маска на подмрежа	255.255.255.0	255.255.255.0	255.255.255.0
Шлюз по подразбиране	192.168.1.51	192.168.1.1	
Предпочитан DNS	192.168.1.51	192.168.1.254	
Алтернативен DNS	192.168.1.51	192.168.1.254	

2.3.2 Спецификации

Категория	Клас	Спецификации	Забележки
Хардуер	Производител	CONTEC	—
	Номер на модел	MCS341-DS1-111	—
	CPU	ARM Cortex-A8 600 MHz	—
	LAN порт	10BASE-T/100BASE-TX	—
	RAM	512 MB	—
	ROM	32 MB	—
	OS	Ubuntu 14.04	—
	Температурен диапазон	-20°C~+60°C	—
	Капацитет на SD карта	4 GB	—
	Диск за начално зареждане	SD карта	—

2.4 Преди монтажа

Преди да започнете инсталирането на Security шлюз, изпълнете следните подготовки:

- проверете дали модулът на Security шлюз и захранване съдържа всички аксесоари,
- проверете дали имате цялото необходимо оборудване за инсталиране на модулите на Security шлюз, вижте ["Необходимо оборудване"](#) [▶ 8],
- запознайте се добре с местоположението на клемите и превключвателите на модулите на Security шлюз, вижте ["За местоположението на клемите"](#) [▶ 8].

2.4.1 Необходимо оборудване

Използвайте следното оборудване за монтаж на модулите на Security шлюза:

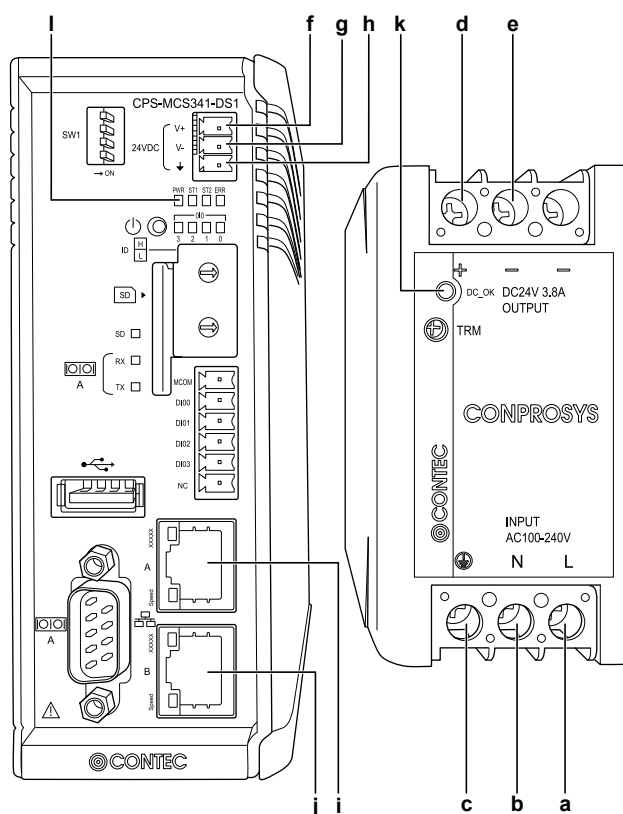
- отвертка с плоско острие,
- кръстовидна отвертка тип Phillips,
- необходимото количество електрически проводници и съответни инструменти за окабеляване.

За повече информация относно вида на използваните проводници, вижте ["2.6 За електрическите проводници"](#) [▶ 10].

2.4.2 За местоположението на клемите

Информирайте се за разположението на клемите и местата на отворите по модула, и планирайте как да прекарате кабела и в какъв ред да свържете проводниците му, за да се улесни монтажната процедура.

За повече информация, вижте ["2.6 За електрическите проводници"](#) [▶ 10].

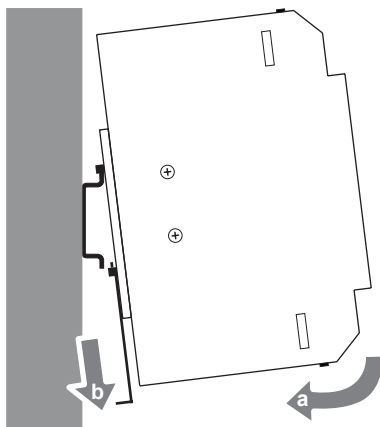


- a** Клема под напрежение 230 V AC
- b** Неутрална клема 230 V AC
- c** Заземяваща клема
- d** Изход електрозахранване 24 V DC (+)
- e** Изход електрозахранване 24 V DC (-)
- f** Входен контакт 24 V DC (+)
- g** Входен контакт 24 V DC (-)
- h** Заземяваща клема
- i** Ethernet връзка (A) Вижте типовете настройване в "8 Приложение А – За откриване на IP адреса на шлюза за сигурност" [► 38] относно правилното окабеляване
- j** Ethernet връзка (B) Вижте типовете настройване в "8 Приложение А – За откриване на IP адреса на шлюза за сигурност" [► 38] относно правилното окабеляване
- k** "DC_OK" LED (DC_OK)
- l** "PWR" LED (PWR)

2.5 За монтиране на 2-те компонента на хардуера на Security шлюз

Модулите на Security шлюза трябва да се монтират върху 35 mm DIN релса.

- 1** Поставете модула върху DIN-35 релсата така, че да се закачи горната кука на задната лицева повърхност.
- 2** Натиснете модула по посока (a), докато долната кука влезе в релсата.
- 3** Ако е необходимо, бутнете лостчето на долните части на модула по посока (b), за да щракнете модула върху релсата. Използвайте отвертка с плоско острие, ако е необходимо.
- 4** Повторете предходните стъпки за всички останали модули.



2.6 За електрическите проводници

Тази глава описва процедурата по свързване на компонентите на Security шлюза с Daikin устройства и друго оборудване.

За всички изисквания по електроокабеляването, вижте ["7.4 Изисквания към окабеляването Security шлюз" \[▶ 36\]](#).



ПРЕДУПРЕЖДЕНИЕ

- НЕ включвайте захранването, докато не завършите всички кабелни връзки. Ако не го направите, може да се получи удар от електрическия ток.
- След като бъде приключено свързването, проверете два пъти дали всички кабели са свързани правилно преди да включите захранването.
- Всички закупени отделно части и материали, и извършените електрически работи ТРЯБВА да отговарят на изискванията на приложимото законодателство.

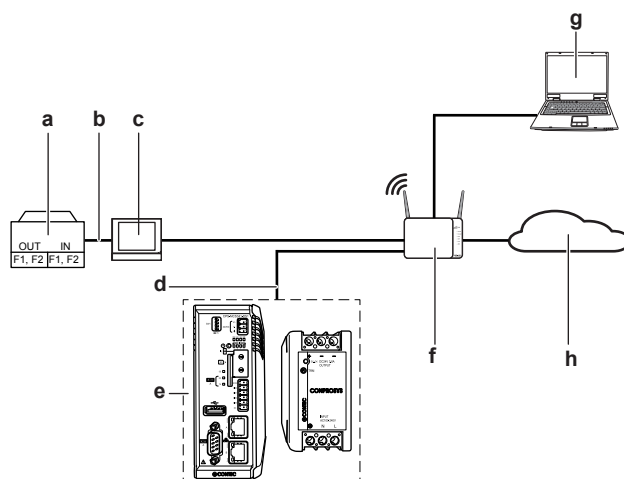


ИНФОРМАЦИЯ

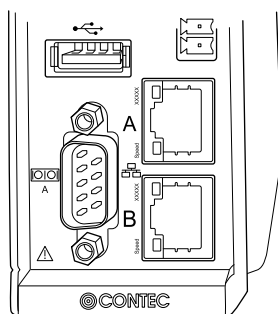
По време на написването някои конектори НЕ са активни, но са предоставени за бъдещо ползване.

2.6.1 За свързване на захранването

Свържете захранването както е показано на следната схема:



В този случай ще се използва само LAN port A.



- a** Външен модул
- b** LAN връзка (DIII)
- c** iTM или LC8 контролер
- d** LAN връзка към порт A
- e** Security шлюз
- f** LAN шлюз (RJ-45)
- g** Потребител PC
- h** Daikin Cloud Service

Включете захранването.

За свързване на съвместимо с DIII-NET оборудване

Вижте:

- Наръчник за Airnet:
 - За пускане в експлоатация на iTM или LC8 контролер
 - Формат: Дигитални файлове на <http://www.daikineurope.com/support-and-manuals/product-information/>
- Ръководство за монтаж на iTM
- Ръководство за монтаж на LC8

За свързване на LAN кабела

За всички изисквания по електроокабеляването, вижте "2.3 Описание на системата" [► 6].

НЕ свързвайте LAN кабела, докато не започнете пускането в експлоатация на LAN шлюза. В противен случай, може да се получи конфликт на мрежови адреси.

3 Пускане в експлоатация



ПРЕДУПРЕЖДЕНИЕ

Пускането в експлоатация трябва да се извършва от квалифициран персонал.



ВНИМАНИЕ

Предварителните проверки на електрическата система, като непрекъснатост на заземяването, поляритет, земно съпротивление и късо съединение, трябва да бъдат извършване посредством подходящ измервателен уред от компетентно лице.

3.1 За пускане в експлоатация на настройка на Security шлюз

След като сте проверили, че компонентите на шлюза за сигурност са инсталирани и цялото необходимо окабеляване е извършено, можете да започнете пускането в експлоатация на вашата настройка на Security шлюз.

В тази фаза на пускането в експлоатация ще направите следното:

- Конфигурирайте компютъра така, че да може да се свърже с шлюза за сигурност, вижте глава "За свързване към intelligent Tablet Controller за първи път" в справочното ръководство на монтажника на intelligent Tablet Controller.
- Конфигурирайте настройките на LAN, вижте "[3.3 За свързване към Security шлюз за първи път](#)" [► 14] за конфигуриране на мрежовите настройки (локално средство за пускане в употреба).
- Задайте дата и час, вижте "[За настройка на часовата зона на шлюза за сигурност](#)" [► 21].
- Добавете цялото свързано оборудване (Daikin) към уеб интерфейса на Security шлюз, вижте "[4 За пускане в експлоатация на iTM или LC8 контролер](#)" [► 23] за бързо конфигуриране на свързаните устройства (локално средство за пускане в употреба).

3.2 Минимални изисквания за пускане в употреба

Преди да започнете конфигурирането на Security шлюз, изпълнете следните подготовки.

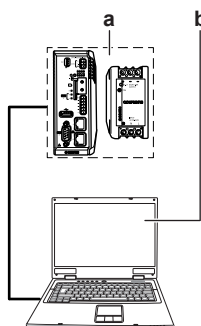
- Уверете се, че спецификациите на вашия компютър отговарят на минималните изисквания, посочени в "[7.5 Изисквания към системата](#)" [► 36].

- Свържете се с вашия мрежов администратор за следната мрежова информация за шлюза за сигурност:
 - желаното мрежово име за шлюза за сигурност,
 - статичен IP адрес и съответна маска на подмрежа на шлюза за сигурност,
 - статичен IP адрес и съответна маска на подмрежа на iTM или LC8 контролер,
 - IP адрес на подразбиращия се шлюз,
 - IP адрес на DNS сървър и
 - IP адрес на алтернативния DNS сървър (ако е приложимо).
- Уверете се, че захранването на цялото свързано оборудване е включено.

3.3 За свързване към Security шлюз за първи път

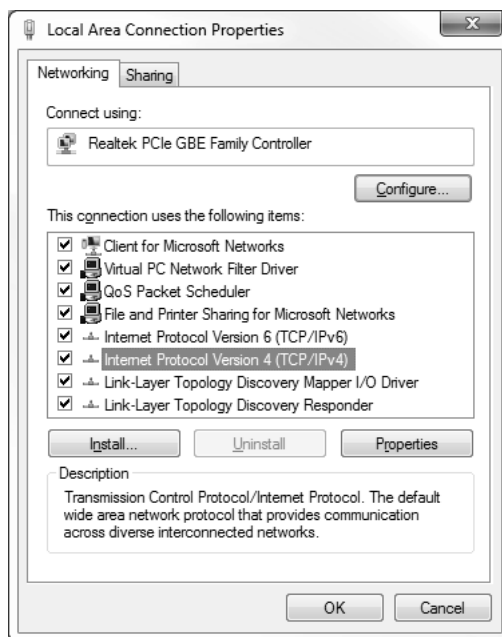
Новият модул на Security шлюз има фиксиран IP адрес 192.168.0.126 и маска на подмрежа 255.255.255.0.

За свързване към това устройство ще трябва да смените IP адреса на вашия компютър така, че да е в същия диапазон като този IP адрес.



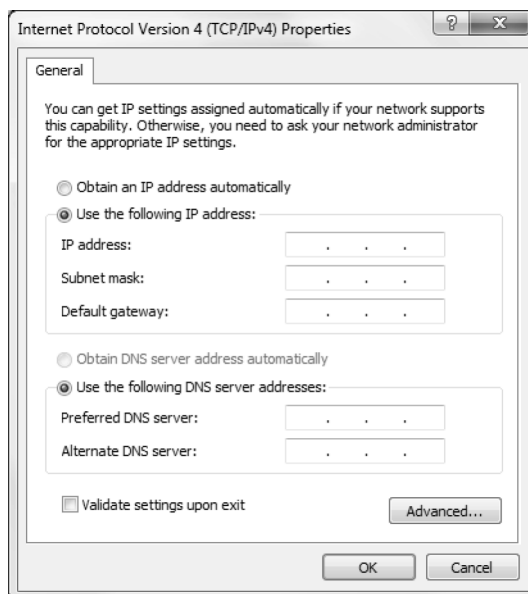
- 1 Включете CAT 5e (или следващ) Ethernet кабел в модула на шлюза за сигурност (a).
- 2 Свържете Ethernet кабела с вашия компютър (b) и сменете вашия IP адрес така, че да съвпада с този на модула на шлюза за сигурност.
- 3 От компютъра си изберете Control Panel.
- 4 В Control Panel изберете опцията Център за мрежи и споделяне и след това опцията Промяна на настройките на адаптера.
- 5 В прозореца Мрежови връзки кликнете два пъти на опцията Локална връзка.

Резултат: Извежда се следният прозорец.



- 6 Изберете опцията Интернет протокол версия 4 (TCP/IPv4) и кликнете върху бутона Свойства.

Резултат: Извежда се следният прозорец.



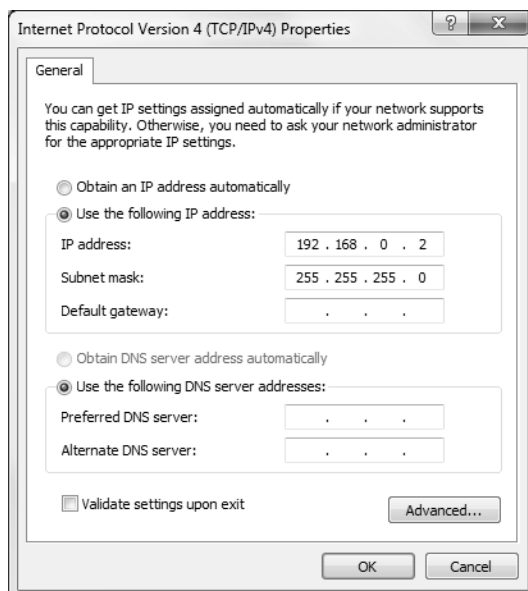
- 7 Кликнете върху радиобутона Използвай следния IP адрес:.
- 8 Задайте следния IP адрес (IP address): "192.168.0.2".



ИНФОРМАЦИЯ

Този пример използва адрес 192.168.0.2, но вие можете да изберете всеки адрес в диапазона 192.168.0.2~192.168.0.254 (освен 192.168.0.126).

- 9 Задайте следната маска на подмрежа (Subnet mask): "255.255.255.0".



10 Кликнете върху бутона ОК (OK).

За да предпазите от смущения, идващи от някоя безжична мрежа, деактивирайте всички безжични мрежови карти на вашия компютър както следва:

11 В прозореца Мрежови връзки кликнете с десния бутон на опцията Безжична мрежова връзка.

12 Изберете опцията забранявам.

13 Проверете дали можете да направите връзка от вашия компютър към модула на шлюза за сигурност. За целта отворете командния ред на вашия компютър по следния начин:

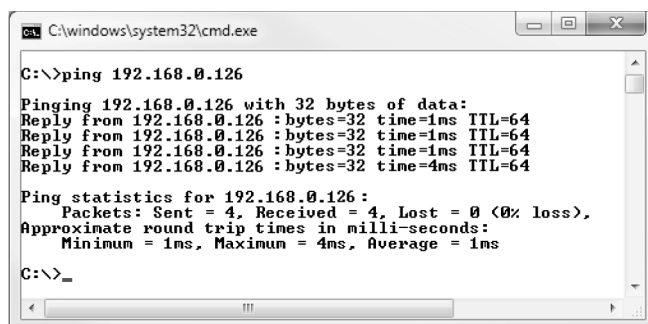
14 Кликнете върху бутона Windows Start.

15 В полето за търсене напишете "командна среда, подкана за (въвеждане на) команда" или алтернативно "Cmd".

16 В списъка с резултати от търсенето кликнете върху командна среда, подкана за (въвеждане на) команда или съответно опцията Cmd.

17 Направете Ping към IP адреса на модула на шлюза за сигурност. За целта напишете следното: "ping 192.168.0.126" и потвърдете с натискане на клавиша Enter.

Резултат: Ще получите отговор от типа на долния пример:



ИНФОРМАЦИЯ

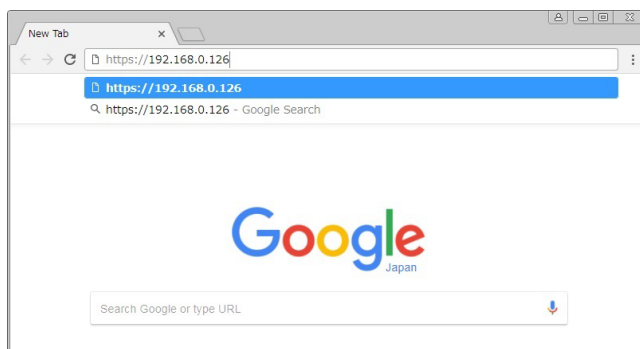
Ако НЕ получите отговори, а съобщение за изтекло време (time-out), вероятно нещо не е наред с връзката. Вижте "[6 Отстраняване на проблеми](#)" [▶ 33] за отстраняване на проблема.

3.4 За конфигуриране на Security шлюз

3.4.1 За получаване на достъп до Security шлюз

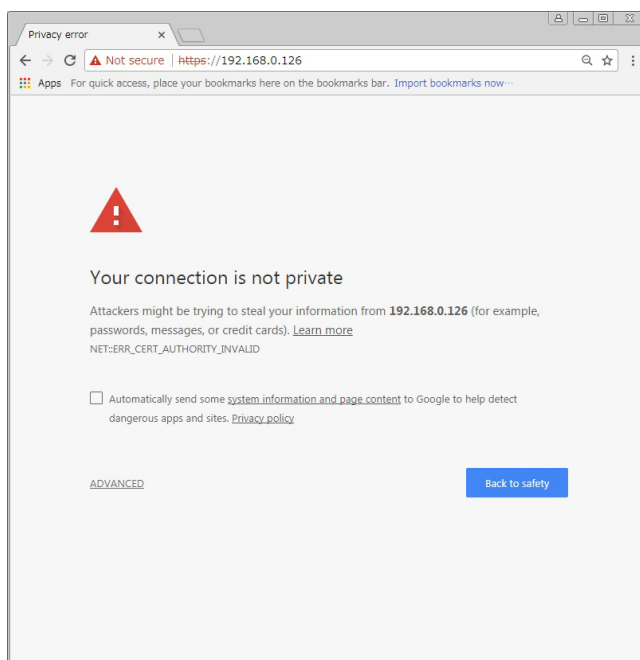
Вижте "8 Приложение А – За откриване на IP адреса на шлюза за сигурност" [▶ 38] относно начина за намиране на IP адреса на шлюза за сигурност, в случай, че сте го забравили.

- 1 Въведете подразбирация се IP адрес на шлюза за сигурност (<https://192.168.0.126>) в лентата за URL на уеб браузъра (Google Chrome или Microsoft Edge).

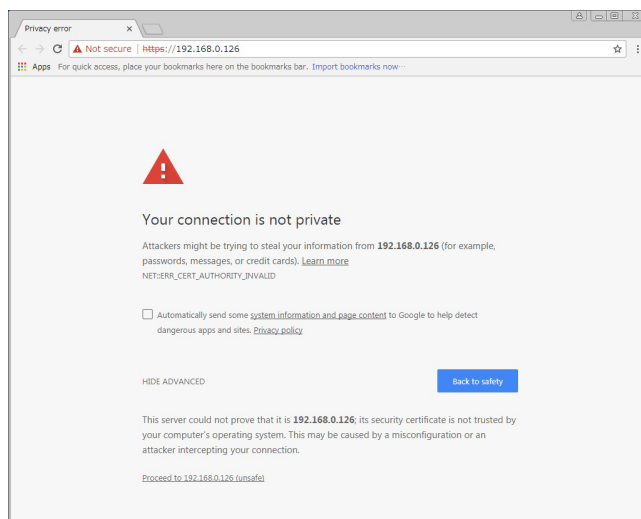


Резултат: Извежда се предупредително съобщение за връзката.

- 2 Кликнете върху ADVANCED (ADVANCED), за да се покаже прозорецът за разширена настройка.

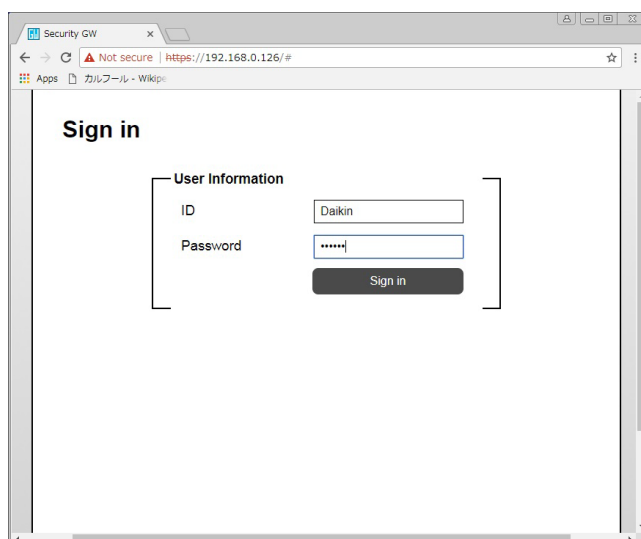


- 3 Кликнете върху Proceed to 192.168.0.126 (unsafe) (Proceed to 192.168.0.126 (unsafe)).

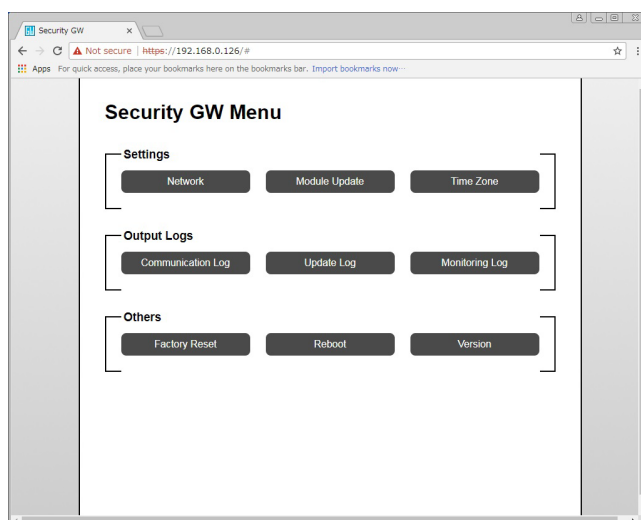


Резултат: Извежда се прозорец за вписване

- 4 Попълнете ID (ID) и парола (Password) (подразбиращ се ID: Daikin / подразбираща се парола: Daikin) на шлюза за сигурност и кликнете върху бутона за вписване (Sign in).



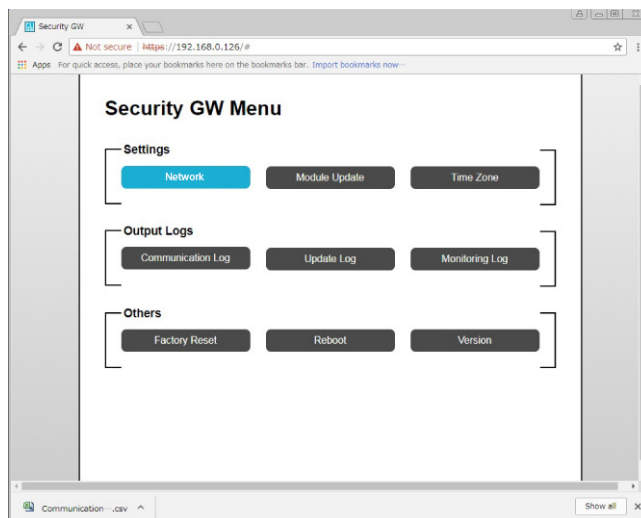
Резултат: Извежда се прозорецът на менюто на шлюза за сигурност (Security GW Menu).



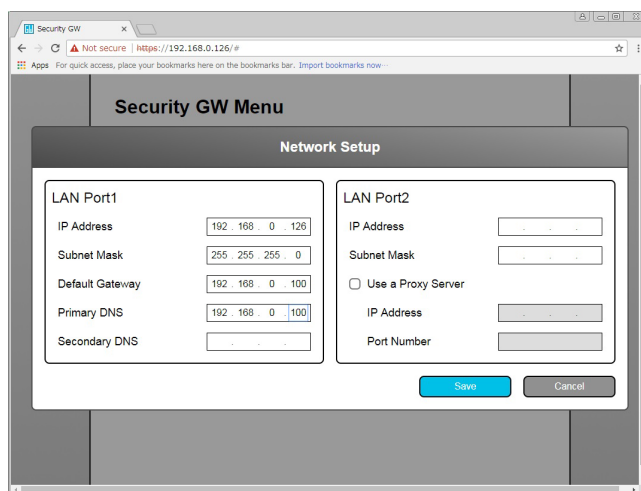
3.4.2 За настройка на мрежата на шлюза за сигурност

За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте ["За получаване на достъп до Security шлюз"](#) [► 17].

- 1 Кликнете върху бутона за мрежа (Network).



Резултат: Извежда се диалогов прозорец за настройка на мрежа (Network Setup).



- 2 Попълнете следните данни за мрежата:

LAN Port1 (LAN Port1) (=A)

- IP адрес (IP address): Уникален IP (по подразбиране: 192.168.0.126) адрес в локалната мрежа
- Маска на подмрежа (Subnet mask): 255.255.255.0
- Шлюз по подразбиране (Default Gateway): IP адрес (по подразбиране: 192.168.0.100) на локален рутер
- Първичен DNS (Primary DNS): IP адрес (по подразбиране: 192.168.0.100) на локален рутер
- Вторичен DNS (Secondary DNS): оставете празно

LAN Port2 (LAN Port2) (=B)

- Оставете празно

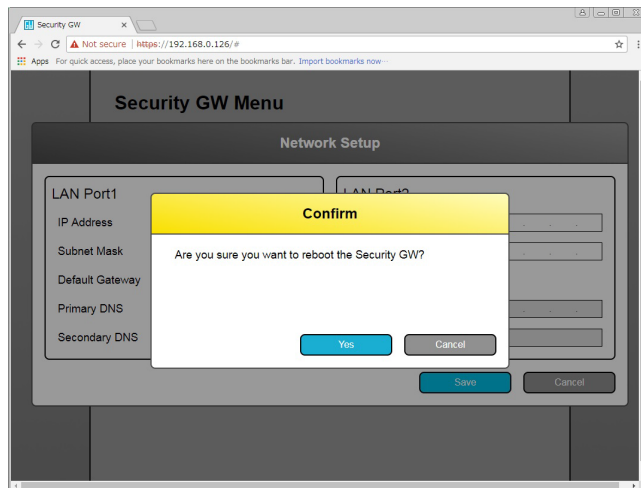
**ИНФОРМАЦИЯ**

Ако IP адрес (IP address), шлюз по подразбиране (Default gateway) и първичен DNS (Primary DNS) са съгласно локалната мрежа, не се налага да ги променят.

- 3 Кликнете върху бутона за запис (Save).

Резултат: Извежда се диалогов прозорец за потвърждение (Confirm).

- 4 Кликнете върху бутона Да (Yes) за рестартиране на шлюза за сигурност.



Резултат: Това ще рестартира шлюза за сигурност.

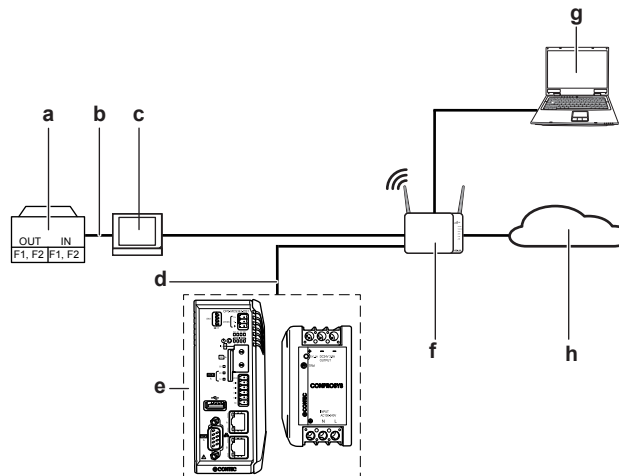
Резултат: Извежда се следният прозорец на уеб браузъра.

Резултат: IP адресът ще бъде променен.

**ИНФОРМАЦИЯ**

Комуникацията с уеб браузъра ще бъде загубена, след като се изпълни стъпка 4. Следвайте процедурата, описана в ["За получаване на достъп до Security шлюз"](#) [▶ 17] за повторно свързване с използване на новия IP адрес.

- 5 Върнете настройките на LAN на вашия компютър към първоначалните им стойности.
- 6 Ако сте го деактивирали по-рано, активирайте Wi-Fi адаптера на компютъра си.
- 7 Разкачете Ethernet кабела между вашия компютър и модула на шлюза за сигурност.
- 8 Свържете Ethernet кабел между модула на шлюза за сигурност и локалната мрежа.



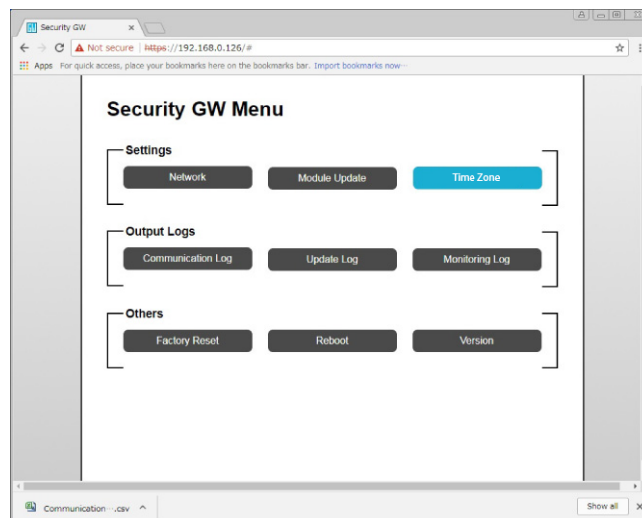
ИНФОРМАЦИЯ

За потвърждение, че IP адресът е променен правилно, достъпете шлюза за сигурност както е описано в "[За получаване на достъп до Security шлюз](#)" [▶ 17] като използвате новия IP адрес.

3.4.3 За настройка на часовата зона на шлюза за сигурност

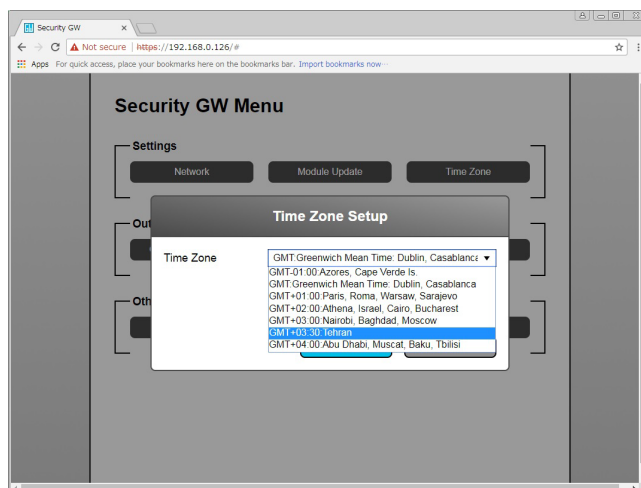
За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте "[За получаване на достъп до Security шлюз](#)" [▶ 17].

- 1 Кликнете върху бутона за часова зона (Time Zone).

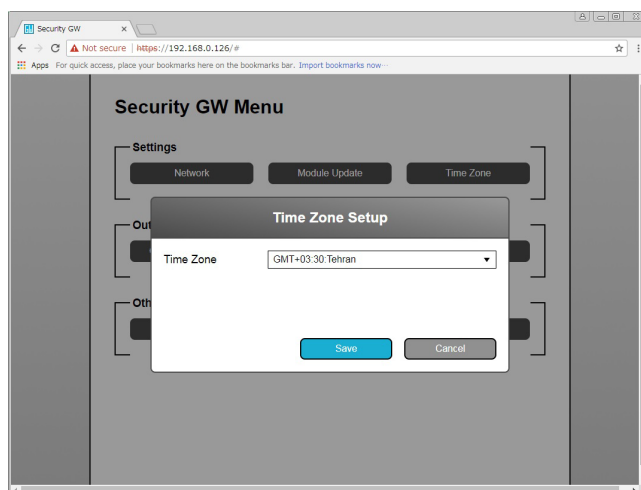


Резултат: Извежда се диалогов прозорец за настройка на часова зона (Time Zone Setup).

- 2 Кликнете върху бутона [▼] за отваряне на падащия списък с часови зони >> изберете и кликнете върху часовата зона.



3 Кликнете върху бутона за запис (Save).



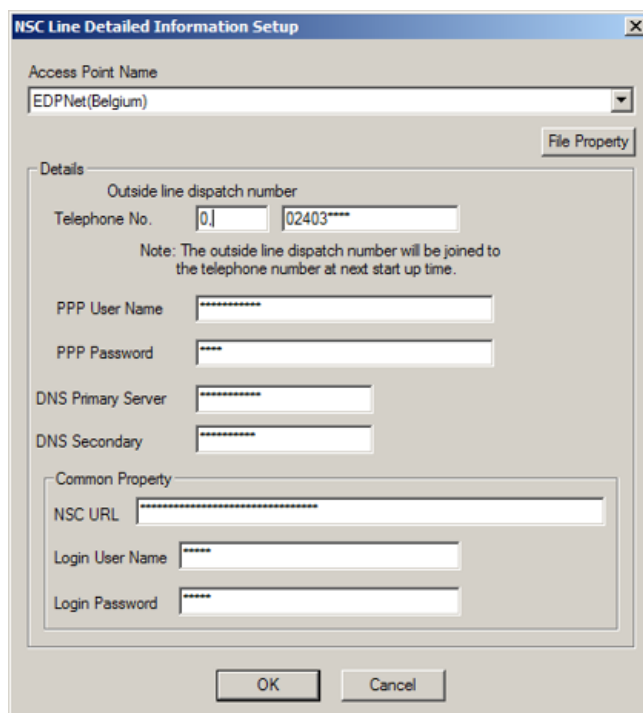
4 За пускане в експлоатация на iTM или LC8 контролер

- 1 Вижте Наръчник за Airnet относно монтажа на iTM или LC8 контролер.
Следващите стъпки са отклонение от наръчника за Airnet, уверете се, че настройките на iTM или LC8 контролера са както е посочено в стъпка 3.
- 2 Вижте "2.3 Описание на системата" [▶ 6] за настройката.
- 3 Настройте мрежата на локалния контролер съгласно следващата таблица.

iTM

LC8

- 4 Задайте NSC URL <http://Lcc.m2m.daikineurope.com/NSC> и изберете правилно име на точка за достъп (Access Point Name) от списъка за избор. Секцията с детайли (Details) може да остане празна.



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

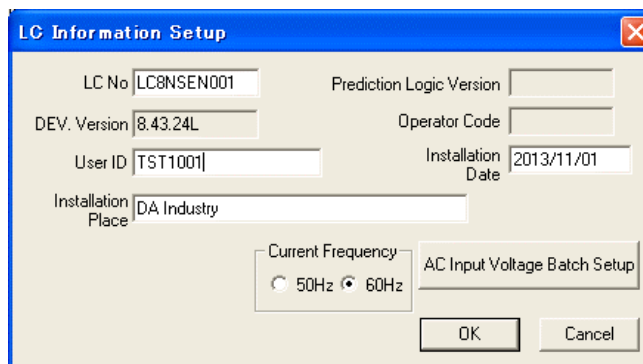
NSC URL *****

Login User Name *****

Login Password *****

OK Cancel

- 5 Свържете се чрез вашите данни за вписване в Daikin Cloud Service с <https://cloud.daikineurope.com> и създайте нов обект. Веднага след създаване на обекта, запишете номера на iTM или LC8:
 - iTM №: Регистрираният идентификационен номер на intelligent Touch Manager. Този номер трябва да е в следния формат: LT2N##### (където # е цифрова стойност).
 - LC8 №: Регистрираният идентификационен номер на LC8 контролер. Този номер трябва да е в следния формат: LC8N##### (където # е цифрова стойност).



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 Работа

5.1 За изтегляне на логове

Можете да записвате и изтегляте три лога чрез уеб приложението на шлюза за сигурност.

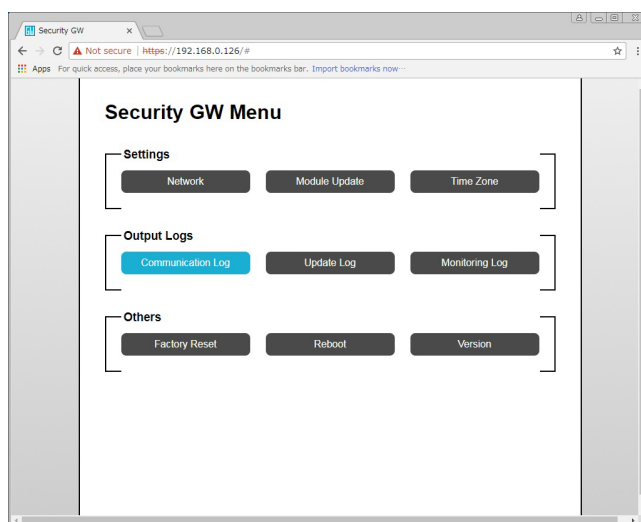
Следните логове могат да се използват за валидиране на правилната функционалност на шлюза за сигурност в случай на проблеми:

Тип на файл	Цел
Комуникационен лог	Той съдържа информация относно времето и типа на данните, изпратени от шлюза за сигурност към облачната платформа.
Лог за актуализация	Той съдържа информация относно проверките за актуализации, времето, когато шлюзът за сигурност е проверил за налична актуализация, както и индикация, ако е инсталирана нова версия на софтуера.
Лог за мониторинг	Той съдържа информация относно изпълнените от шлюза за сигурност действия, например, при включване и изключване.

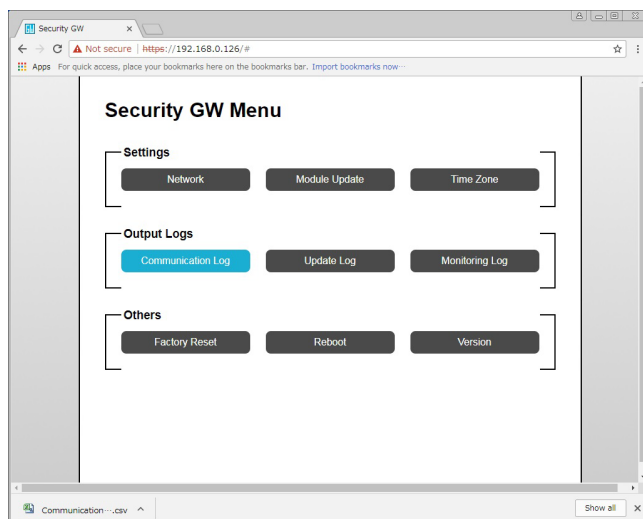
5.1.1 За изтегляне на комуникационни логове

За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте ["За получаване на достъп до Security шлюз"](#) [► 17].

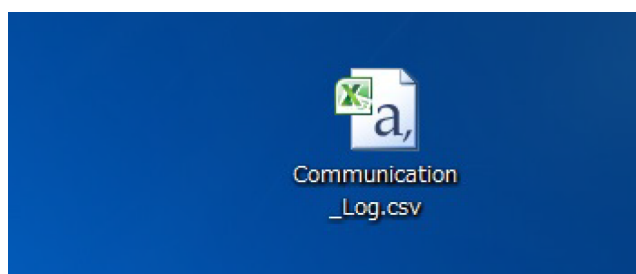
- 1 Кликнете върху бутона за комуникационен лог (Communication Log).



- 2 Проверете състоянието на изтегляне в лентата за изтегляне в долната част на прозореца.



- 3 Намерете и кликнете двукратно (за да отворите) изтегляния комуникационен лог .csv (Communication_Log.csv) файл на работния плот.



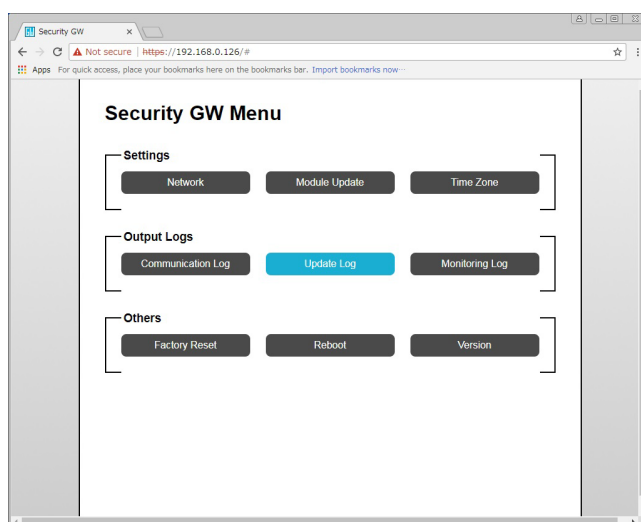
- 4 Проверете данните на .csv (Communication_Log.csv) файла с комуникационен лог.

	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		

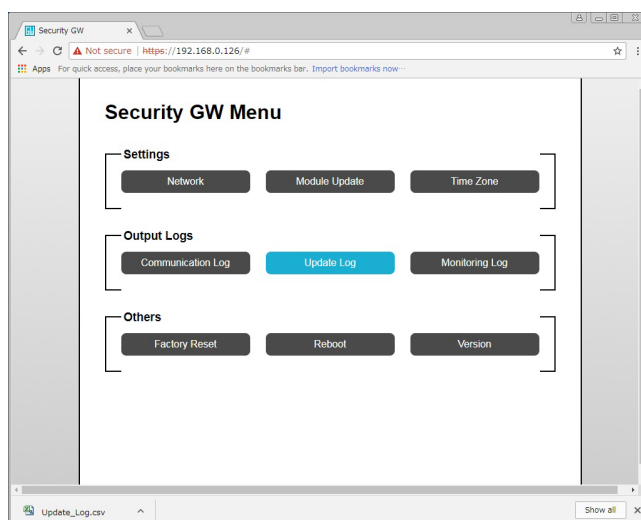
5.1.2 За изтегляне на логове за актуализация

За достъп до менюта на шлюза за сигурност (Security GW Menu) вижте "[За получаване на достъп до Security шлюз](#)" [► 17].

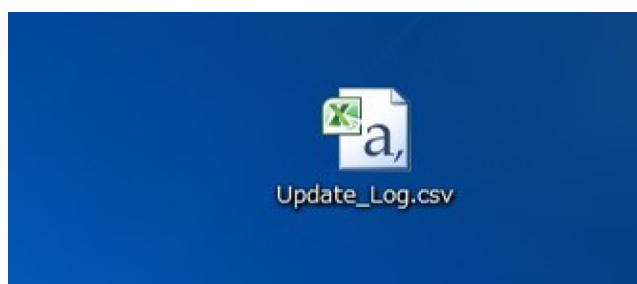
- 1 Кликнете върху бутона за лог за актуализация (Update Log).



- 2 Проверете състоянието на изтегляне в лентата за изтегляне в долната част на прозореца.



- 3 Намерете и кликнете двукратно (за да отворите) изтегления лог за актуализация .csv (Update_Log.csv) файл на работния плот.



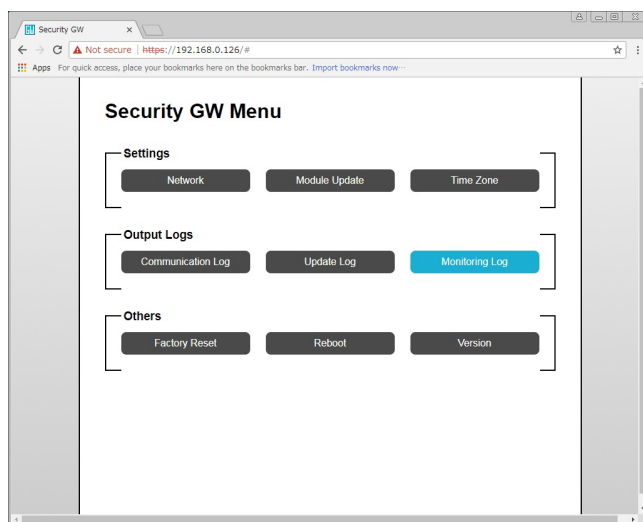
- 4 Проверете данните на .csv (Update_Log.csv) файла с лог за актуализация.

	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					

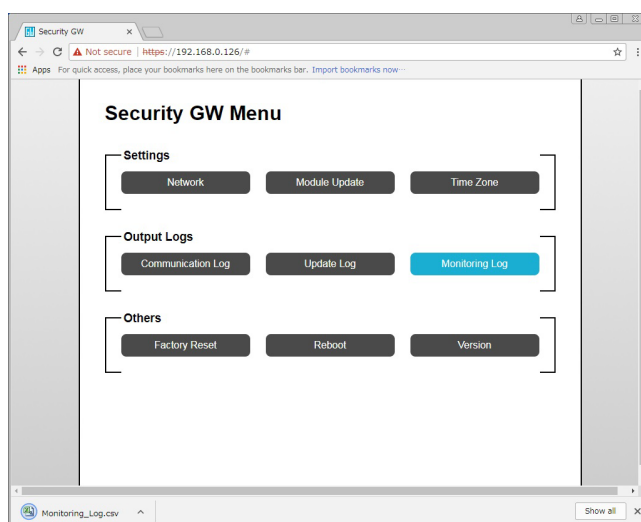
5.1.3 За изтегляне на логове за мониторинг

За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте "[За получаване на достъп до Security шлюз](#)" [▶ 17].

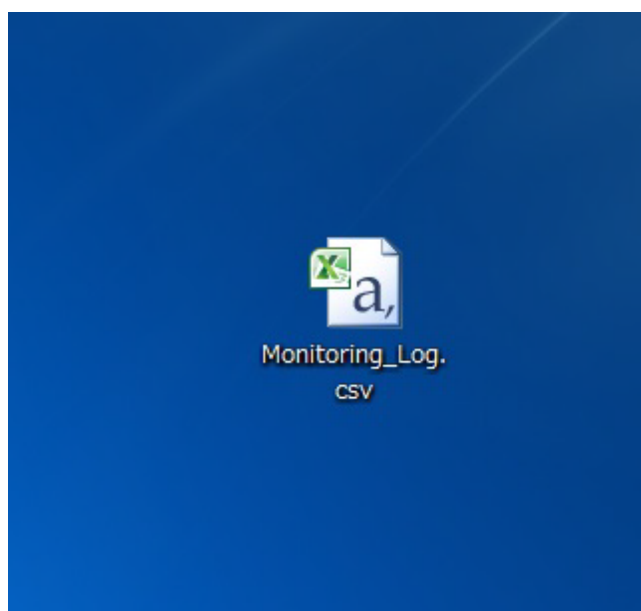
- 1 Кликнете върху бутона за лог за мониторинг (Monitoring Log).



- 2 Проверете състоянието на изтегляне в лентата за изтегляне в долната част на прозореца.



- 3 Намерете и кликнете двукратно (за да отворите) изтегления лог за мониторинг .csv (Monitoring_Log.csv) файл на работния плот.



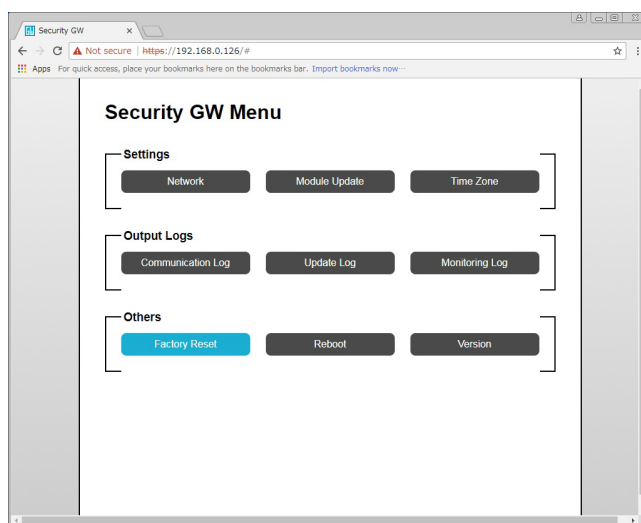
- 4 Проверете данните на .csv (Monitoring_Log.csv) файла с лог за мониторинг.

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

5.2 За връщане на Security шлюз към фабрични настройки

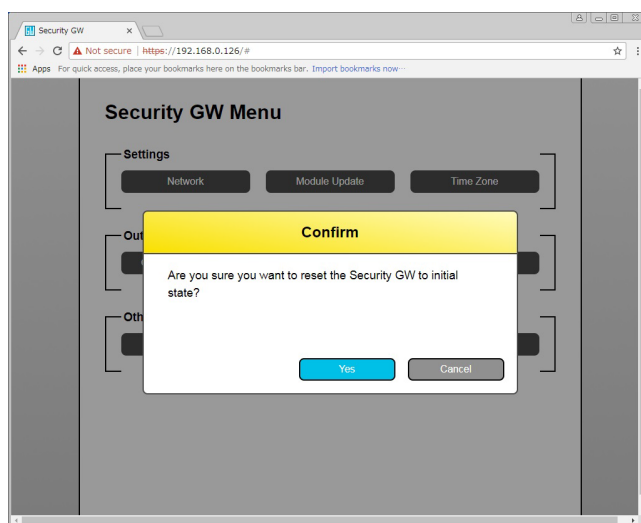
За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте "[За получаване на достъп до Security шлюз](#)" [► 17].

- 1 Кликнете върху бутона за фабрична настройка (Factory reset).



Резултат: Извежда се диалогов прозорец за потвърждение (Confirm).

- 2 Кликнете върху бутона Да (Yes) от диалога за потвърждение.

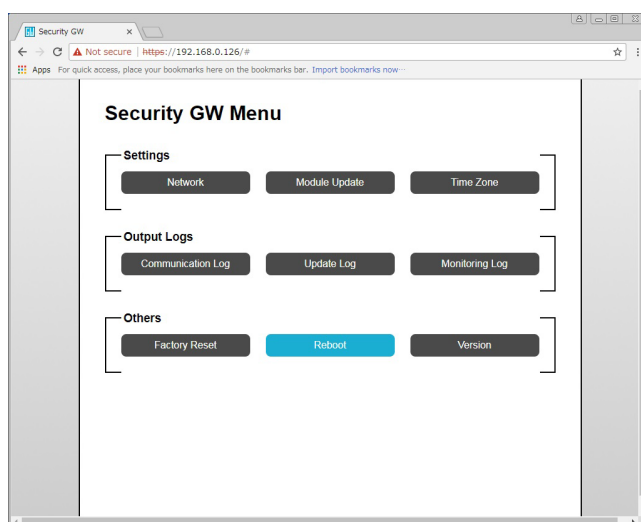


Резултат: Шлюзът за сигурност се връща към оригиналната фабричната настройка.

5.3 За рестартиране на Security шлюз

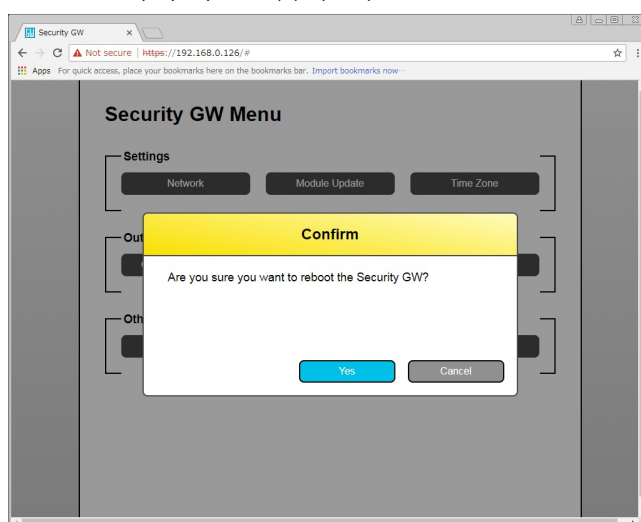
За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте "[За получаване на достъп до Security шлюз](#)" [► 17].

- 1 Кликнете върху бутона за рестарт (Reboot).

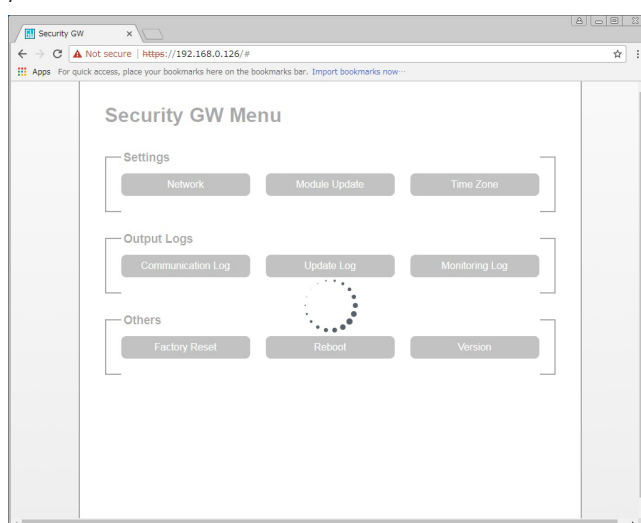


Резултат: Извежда се диалогов прозорец за потвърждение (Confirm).

- 2 Кликнете върху бутона Да (Yes).



Резултат: Диалоговият прозорец за потвърждение изчезва и всички бутони стават сиви и неактивни.



Резултат: Шлюзът за сигурност се рестартира.

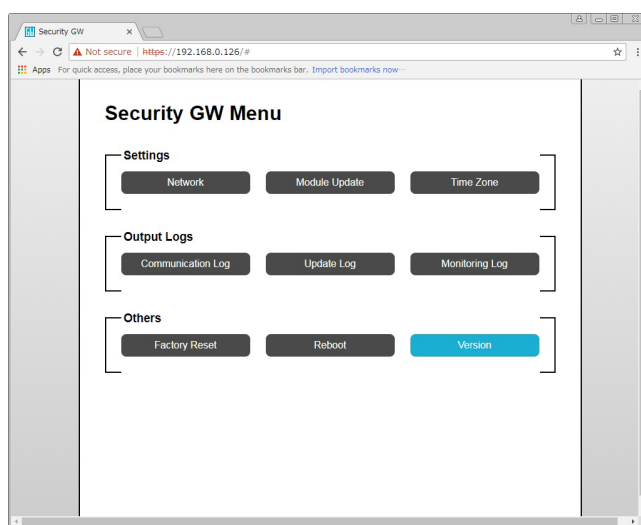
5.4 За проверка на номера на версии

В някои случаи може да се наложи да съобщите номерата на версиите на вашия Security шлюз. Чрез менюто на уеб приложението можете да изтеглите версията на:

- Уеб приложението (браузър и специфичен инструмент за настройка на Security шлюз) на шлюза за сигурност. [Клиентска версия]
- Хардуер, фърмуер и операционна система на Шлюза за сигурност. [Версия на Security шлюз]
- Уникалният сериен номер за управление на шлюза за сигурност. [Номер на Security шлюз]

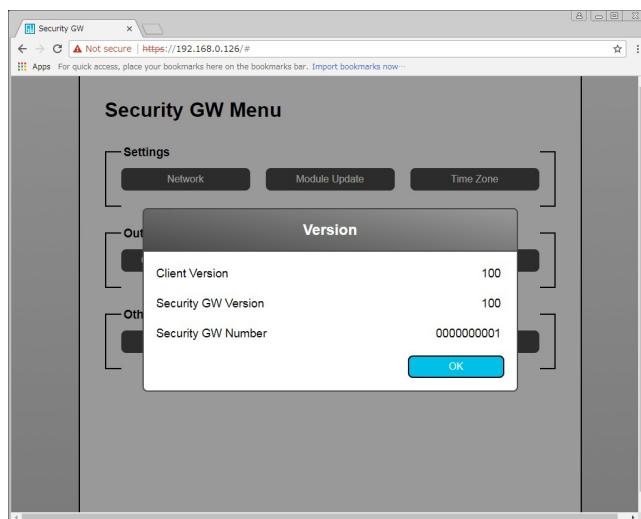
За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте ["За получаване на достъп до Security шлюз"](#) [▶ 17].

- 1 Кликнете върху бутона за версия (Version).



Резултат: Извежда се диалогов прозорец за версия (Version).

- 2 Проверете версиите.



- 3 Натиснете бутона ОК (OK), за да се върнете на екрана на главното меню.

Резултат: Извежда се основният екран.

6 Отстраняване на проблеми

6.1 Възможни неизправности

Неизправност	Причина	Решение
Неизправност на връзка	Невъзможно свързване към Security шлюз. Проверете захранването.	Уверете се, че ПРАВИЛНАТА SD карта е поставена ПРАВИЛНО в слота за SD карти. Уверете се, че модулът на шлюза за сигурност е ВКЛЮЧЕН. Проверете IP АДРЕСА на шлюза за сигурност и РС за настройка. Уверете се, че те са включен в същата локална мрежа. Уверете се, че се използват и са зададени ПРАВИЛНИТЕ LAN портове: - Лява страна: Порт А - Дясна страна: Порт В РЕСТАРТИРАЙТЕ шлюза за сигурност * Използвайте специфичния инструмент за настройка на шлюза за сигурност, ако сте забравили IP адреса на шлюза за сигурност, както е описано в "8.2 За откриване на IP адреса" [▶ 38].
Неизправност на настройка	Невъзможност за: ■ Извършване на настройка, ■ Изтегляне на лог файлове, ■ Възстановяване на фабрична настройка, ■ Рестартиране, ■ Проверете версията.	ОТПИШЕТЕ СЕ от уеб приложението за настройка на шлюза за сигурност или от специфичния инструмент за настройка на шлюза за сигурност. ВПИШЕТЕ СЕ в уеб приложението за настройка на шлюза за сигурност или в специфичния инструмент за настройка на шлюза за сигурност. ОПИТАЙТЕ отново настройка, изтегляне на лог файл, фабрична настройка, рестартиране и проверка на версия.

6.2 Съобщения за грешка

Категория	Описание	Забележки
1. Невалиден Javascript	1.1 Няма наличен Javascript. Разрешете Javascript и опитайте отново.	—
2. Невалидна "бисквитка"	2.1 Деактивирана "бисквитка". Разрешете "бисквитките" от настройките на браузъра си и опитайте отново.	—

Категория	Описание	Забележки
3. Връзка със Security шлюз	3.1 Неуспешно свързване към Security шлюз. Проверете дали шлюзът за сигурност е свързан със същата мрежа.	—
4. Вписване	4.1 Потребителски ID и/или парола още не са въведени.	Въведете потребителски ID и парола . Кликнете върху бутона [Sign in].
	4.2 Неуспешна автентификация. Невалиден потребителски ID и/или парола.	Потвърдете потребителския ID и парола. Въведете правилни потребителски ID и парола. Кликнете върху бутона [Sign in].
	4.3 Неуспешна комуникация с шлюза за сигурност.	Уверете се, че SD картата е поставена в слота за SD карти. Уверете се, че модулът на шлюза за сигурност е включен. Уверете се, че LAN кабелът е свързан към шлюза за сигурност и към PC за настройка. Натиснете бутона за нулиране на шлюза за сигурност.
5. Меню на Security шлюз	5.1 Неуспешна комуникация с шлюза за сигурност.	Същото като 4.3
	5.2 Неуспешно извличане на лог.	—
6. Настройка на мрежа	6.1 Неуспешна комуникация с шлюза за сигурност.	Същото като 4.3
7. Настройка за актуализация на модула	7.1 Неуспешна комуникация с шлюза за сигурност.	Същото като 4.3
8. Настройки на часова зона	8.1 Неуспешна комуникация с шлюза за сигурност.	Същото като 4.3
9. Диалог за грешка	9.1 Вашата сесия е изтекла. Опитайте да се впишете отново.	—

7 Технически спецификации

7.1 Изисквания към компютъра за пускане в употреба

Позиция	Спецификация
OS	Windows 7 Professional (32-bit) или следваща
Памет	2 GB RAM или повече
Твърд диск	20 GB свободно място на твърдия диск или повече
Портове	1 RJ45 порт
Браузър	Едно от следните: - Internet Explorer версия 9, 10 или 11 - Google Chrome - Mozilla Firefox - Apple Safari

7.2 Спецификации на консумацията на енергия Security шлюз

Позиция	Спецификация
Свързано входно напрежение	110~220 V AC
Входна честота	50~60 Hz
Разход на енергия CPU модул + I/O модул	- Макс.: 13 W (11 W+2 W) - Типична: 5,5 W (4 W+1,5 W)

За по-подробни спецификации на захранването, вижте ръководството, предоставено със захранването.

7.3 Подразбиращи се пароли на средствата

Средство	Парола
Код за автентификация Уеб интерфейс на Security шлюз	Не е зададен (празен), вижте "За получаване на достъп до Security шлюз" [► 17] - ID по подразбиране Daikin - подразбираща се парола: Daikin

7.4 Изисквания към окабеляването Security шлюз

**ПРЕДУПРЕЖДЕНИЕ**

Окабеляването и монтажът на компонентите ТРЯБВА да се извършват от лицензиран електротехник и СЛЕДВА да отговарят на съответните законови разпоредби.

Цялото окабеляване трябва да отговаря на следните изисквания:

Свързване	Напречно сечение	Макс. дължина	Забележки
LAN кабел	—	100 m	- UTP CAT 5e или по-висок - RJ45 конектор
DIII-NET (F1/F2)	$\varnothing 0,75 \sim 1,25 \text{ mm}^2$ (Клема, оразмерена за макс. $1,5 \text{ mm}^2$)	Обща дължина ^(a) : 2000 m (<1500 m при използване на екраниран проводник) Макс. дължина ^(b) : 1000 m	- Тип кабел: 2-жилен винилов изолиран с винилова екранировка/винилов шлангов кабел или 2-жилен екраниран кабел - НЕ използвайте многожилни кабели с 3 или повече жила - НЕ използвайте смесени типове кабели - НИКОГА не завързвайте кабелите на възел - При използване на екраниран кабел свържете само един край на всеки екраниран проводник към земята - Уверете се, че окабеляването е прекарано и закрепено така, че да НЕ допира незаземени и достъпни проводими части - Уверете се, че има съпротивление срещу деформация за всеки проводник при навлизането в електрическата кутия - За повече информация относно DIII-NET, вижте ръководството за проектиране на D-BACS (ED72721)
230 V AC захранване към PU	Съгласно приложимото законодателство (клема, оразмерена за макс. 4 mm^2)	Съгласно приложимото законодателство	- Допуска се едножилен или усукан проводник - Вътрешната защита на WAGO PSU е свързана с предпазител с 2,5 A / 250 V
24 V DC захранване към модул на Security шлюз	Съгласно приложимото законодателство	—	Допуска се едножилен или усукан проводник

(a) *Обща дължина* е сумата на цялото окабеляване в DIII-NET мрежата.

(b) *Макс. дължина* е максималното разстояние между кои да е 2 точки на свързване в DIII-NET мрежата.

7.5 Изисквания към системата

Компютърът, който използвате за настройка на шлюза за сигурност, трябва да отговаря на тези минимални изисквания:

СРУ Intel i3 2.2 GHz или следващ
Операцион Microsoft Windows 7 или следваща версия
на система

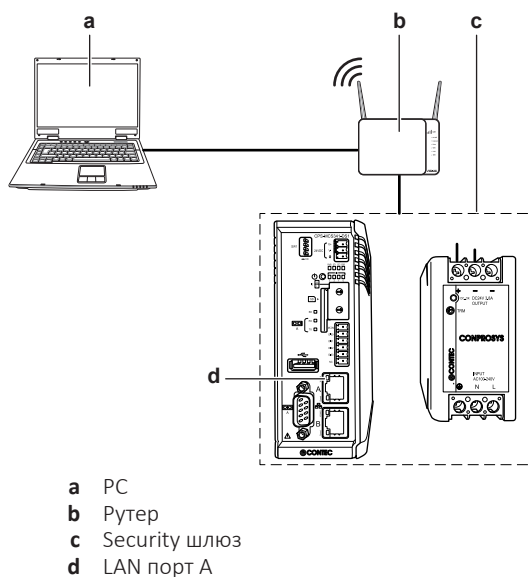
Памет	512 MB RAM или повече
Свободно пространство на твърдия диск	10 GB или повече
Мрежа	10 BASE-T или следваща

8 Приложение А – За откриване на IP адреса на шлюза за сигурност

Това приложение обяснява как да се открие IP адресът на шлюза за сигурност чрез използване на специфичния инструмент за настройка на шлюза за сигурност.

8.1 За окабеляване на Security шлюз

- 1 Свържете захранването по същия начин, както е показано в "За свързване на захранването" [► 10].
- 2 Добавете шлюза за сигурност към локалната мрежа както е показано на следващата фигура:



В този случай ще се използва само LAN порт A.

- 3 Включете захранването.

8.2 За откриване на IP адреса

Уверете се, че разполагате с най-новата версия на инструмента за настройка на шлюза. Най-новата версия е достъпна на https://my.daikin.eu/denv/en_US/home/applications/product-finder/Daikin-Cloud-Service.html.

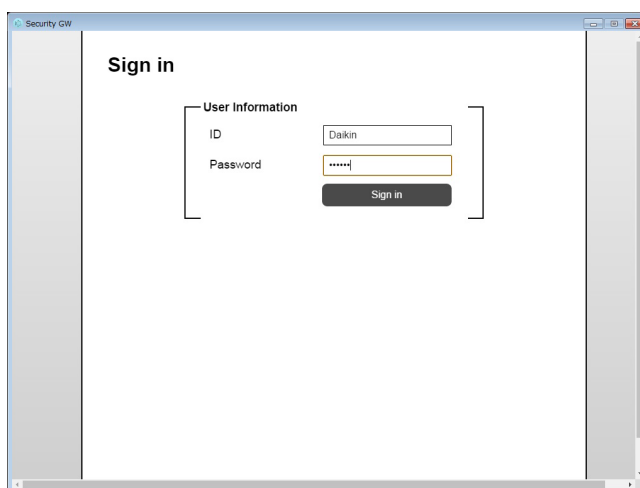
- 1 Изтеглете и разархивирайте zip файла, съдържащ GwSettingTool.exe (GwSettingTool.exe) в папка на локалното ви устройство.
- 2 Кликнете двукратно върху файла GwSettingTool.exe (GwSettingTool.exe) за да стартирате инструмента за настройка на шлюза за сигурност.

Резултат: Свързването започва.



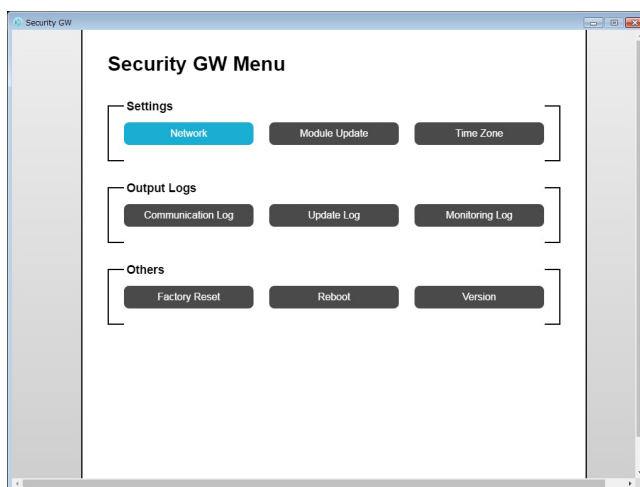
Резултат: След около 1 минута се извежда прозорец за вписване.

- 3 Попълнете ID (ID) и парола (Password) (подразбиращ се ID: Daikin / подразбираща се парола: Daikin) на шлюза за сигурност и кликнете върху бутона за вписване (Sign in).

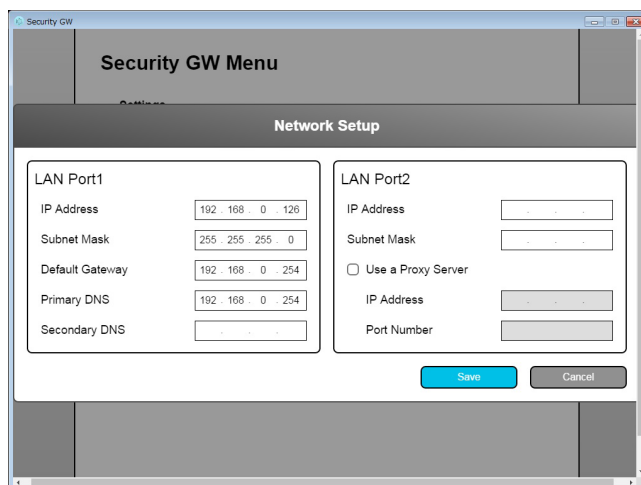


Резултат: Извежда се прозорецът на менюто на шлюза за сигурност (Security GW Menu).

- 4 Кликнете върху бутона за мрежа (Network).



Резултат: Извежда се диалогов прозорец за настройка на мрежа (Network Setup).



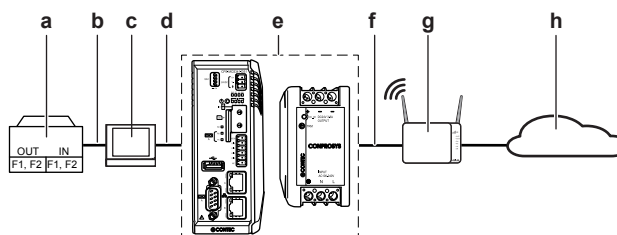
- 5 Проверете IP адреса (IP address) на LAN Port1 (LAN Port1).

9 Приложение В – За пускането в експлоатация в случай на прокси сървър

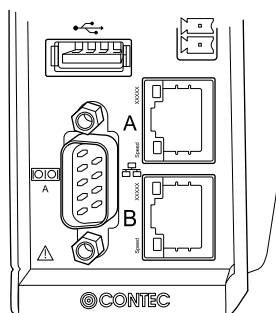
Това приложение обяснява как да се извърши първоначалната настройка на шлюза за сигурност, ако топологичната структура не съответства на стандартната, описана в "Настройка на локална мрежа" [► 7].

9.1 Алтернативна настройка

- 1 Свържете захранването по същия начин, както е показано в "За свързване на захранването" [► 10].
- 2 Добавете шлюза за сигурност към локалната мрежа както е показано на следващата фигура:



В този случай ще се използват едновременно LAN порт А и LAN порт В.



- a Външен модул
- b LAN връзка (DIII)
- c iTM или LC8 контролер
- d LAN връзка към порт А
- e Security шлюз
- f iTM или LC8 контролер към порт В
- g LAN шлюз (RJ-45)
- h Daikin Cloud Service

- 3 Включете захранването.

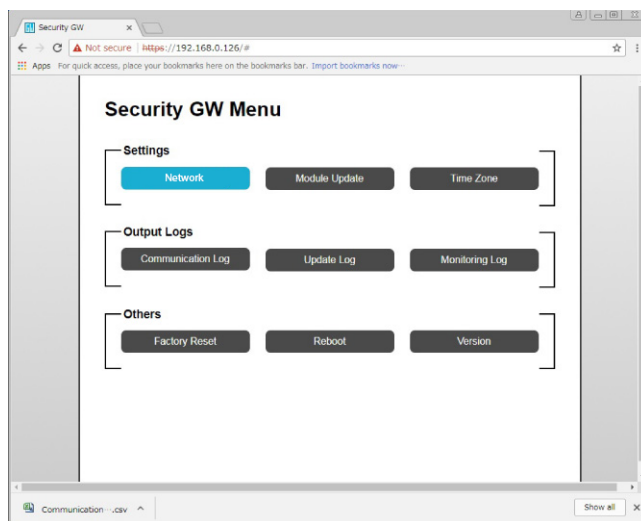
9.2 За получаване на достъп до Security шлюз

Вижте "За получаване на достъп до Security шлюз" [► 17].

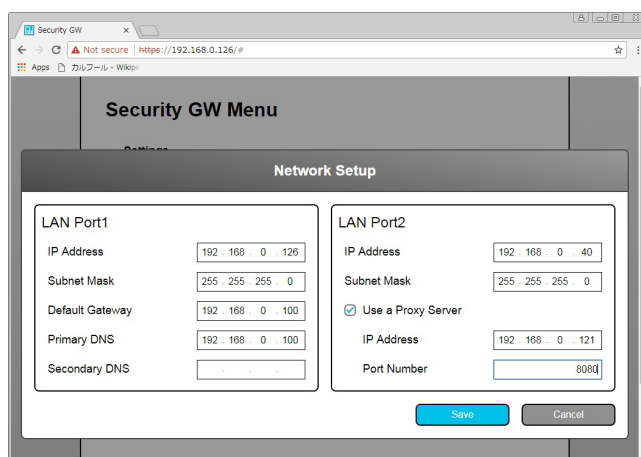
9.3 За настройка на мрежата на шлюза за сигурност

За достъп до менюто на шлюза за сигурност (Security GW Menu) вижте "За получаване на достъп до Security шлюз" [► 17].

- 1 Кликнете върху бутона за мрежа (Network).



Резултат: Извежда се диалогов прозорец за настройка на мрежа (Network Setup).



2 Попълнете следните данни за мрежата:

LAN Port1 (LAN Port1) (=A)

- IP адрес (IP address): Уникален IP (по подразбиране: 192.168.0.126) адрес в локалната мрежа
- Маска на подмрежа (Subnet mask): 255.255.255.0
- Шлюз по подразбиране (Default Gateway): IP адрес (по подразбиране: 192.168.0.100) на локален рутер
- Първичен DNS (Primary DNS): IP адрес (по подразбиране: 192.168.0.100) на локален рутер
- Вторичен DNS (Secondary DNS): оставете празно

LAN Port2 (LAN Port2) (=B)

- IP адрес (IP address): изберете диапазон от IP адреси, различен от този за порт A (напр. 192.168.10.5)
- Маска на подмрежа (Subnet mask): 255.255.255.0
- Използване на прокси сървър (Use a Proxy Server): Проверка
- IP адрес (IP address): IP прокси сървър
- Номер на порт (Port Number): Порт на прокси сървър



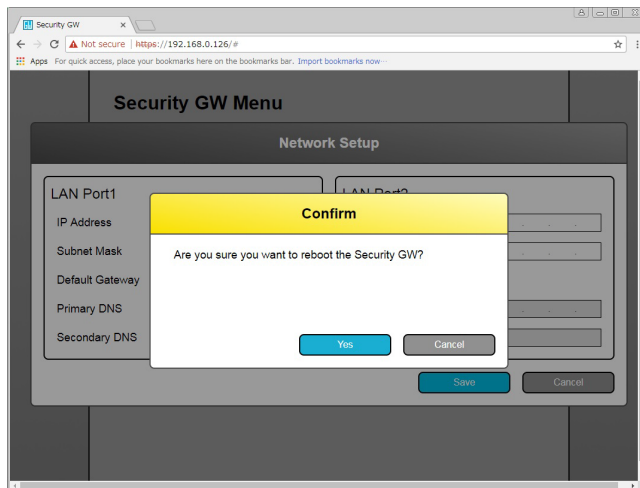
ИНФОРМАЦИЯ

Ако IP адрес (IP address), шлюз по подразбиране (Default gateway) и първичен DNS (Primary DNS) са съгласно локалната мрежа, не се налага да ги променят.

- 3 Кликнете върху бутона за запис (Save).

Резултат: Извежда се диалогов прозорец за потвърждение (Confirm).

- 4 Кликнете върху бутона Да (Yes) за рестартиране на шлюза за сигурност.



Резултат: Това ще рестартира шлюза за сигурност.

Резултат: Извежда се следният прозорец на уеб брауъра.

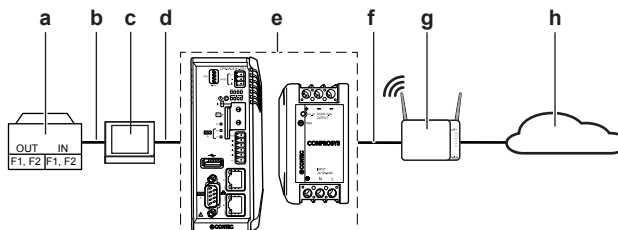
Резултат: IP адресът ще бъде променен.



ИНФОРМАЦИЯ

Комуникацията с уеб брауъра ще бъде загубена, след като се изпълни стъпка 4. Следвайте процедурата, описана в ["За получаване на достъп до Security шлюз"](#) [17] за повторно свързване с използване на новия IP адрес.

- 5 Върнете настройките на LAN на вашия компютър към първоначалните им стойности.
- 6 Ако сте го деактивирали по-рано, активирайте Wi-Fi адаптера на компютъра си.
- 7 Разкачете Ethernet кабела между вашия компютър и модула на шлюза за сигурност.
- 8 Свържете Ethernet кабел между модула на шлюза за сигурност и локалната мрежа.



9.4 За настройка на часовата зона на шлюза за сигурност

Вижте ["За настройка на часовата зона на шлюза за сигурност"](#) [21].

9.5 За пускане в експлоатация на iTM или LC8 контролер

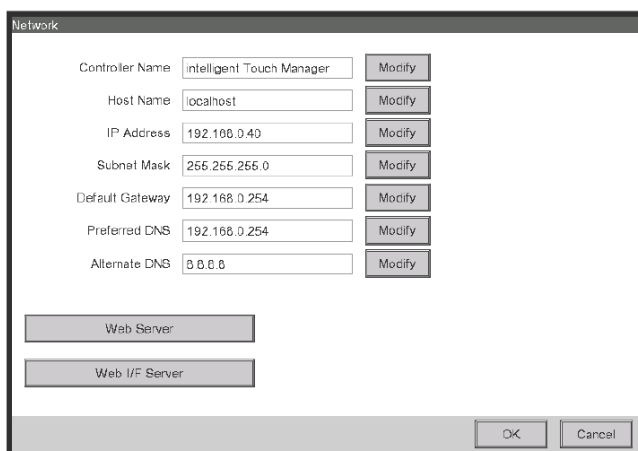
Вижте:

- Наръчник за Airnet:
 - За пускане в експлоатация на iTM или LC8 контролер
 - Формат: Дигитални файлове на <http://www.daikineurope.com/support-and-manuals/product-information/>
- Ръководство за монтаж на iTM
- Ръководство за монтаж на LC8

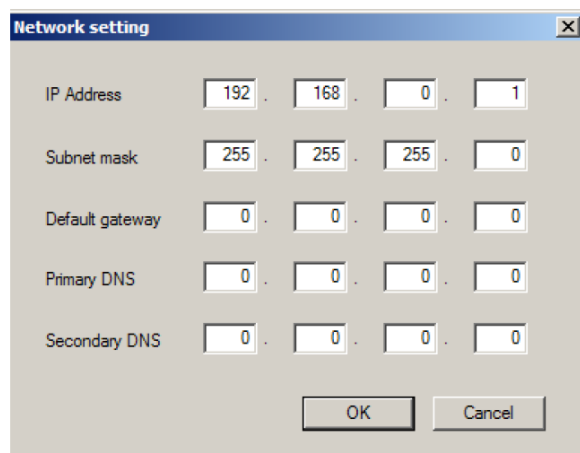
Следващите стъпки са отклонение от наръчника за Airnet, уверете се, че настройките на iTM или LC8 контролера са както е посочено в стъпка 1.

- 1 Настройте мрежата на локалния контролер съгласно следващата таблица.

iTM



LC8



- 2 Задайте NSC URL <http://Lcc.m2m.daikineurope.com/NSC> и изберете правилно име на точка за достъп (Access Point Name) от списъка за избор. Секцията с детайли (Details) може да остане празна.

- 3 Свържете се чрез вашите данни за вписване в Daikin Cloud Service с <https://cloud.daikineurope.com> и създайте нов обект. Веднага след създаване на обекта, запишете номера на iTM или LC8:
 - iTM №: Регистрираният идентификационен номер на intelligent Touch Manager. Този номер трябва да е в следния формат: LT2N##### (където # е цифрова стойност).
 - LC8 №: Регистрираният идентификационен номер на LC8 контролер. Този номер трябва да е в следния формат: LC8N##### (където # е цифрова стойност).





ERC

Copyright 2018 Daikin

DAIKIN EUROPE N.V.

Zandvoordestraat 300, B-8400 Oostende, Belgium

4P529063-1A 2020.12