Installer reference guide

Security gateway

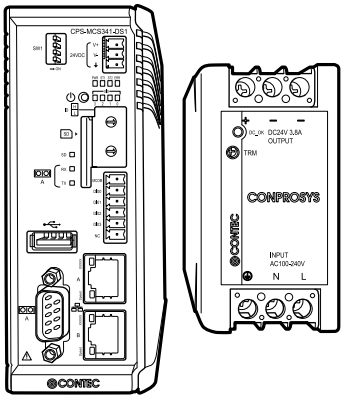


Table of contents

1 About this document

Target audience

Authorised installers

Documentation set

This document is part of a documentation set. The complete set consists of:

- **Installation manual:**
  - Installation instructions
  - Format: Paper (supplied in the kit)
- **Installer reference guide:**
  - Preparation of the installation, reference data,…
  - Format: Digital files on http://www.daikineurope.com/support-and-manuals/product-information/
- **Airnet handbook:**
  - Commissioning of the iTM or LC8 controller
  - Format: Digital files on http://www.daikineurope.com/support-and-manuals/product-information/
- **Intelligent Touch Manager installation manual (DCM601A51)**:
  - Installation instructions
  - Format: Digital files on http://www.daikineurope.com/support-and-manuals/product-information/
- **LC8 installation manual (DLC602B51):**
  - Installation instructions
  - Format: Digital files on http://www.daikineurope.com/support-and-manuals/product-information/

Latest revisions of the supplied documentation may be available on the regional Daikin website or via your dealer.

The original documentation is written in English. All other languages are translations.

Technical engineering data

- A **subset** of the latest technical data is available on the regional Daikin website (publicly accessible).
- The **full set** of latest technical data is available on the Daikin Business Portal (authentication required).

2 Installation

2.1 General safety precautions

Please read these general safety precautions carefully before installing air conditioning equipment, and be sure to install the equipment correctly.

Failure to follow these instructions properly may result in property damage or personal injury, which may be serious depending on the circumstances.

After completing the installation, make sure the power supply and controller modules operate properly during the startup operation.

Meaning of warnings and symbols

These safety messages are used to attract your attention. The meaning of each safety message is described below:

WARNING

Indicates a situation that could result in death or serious injury.

CAUTION

Indicates a situation that could result in minor or moderate injury.

DANGER

Indicates a situation that results in death or serious injury.

DANGER: RISK OF EXPLOSION

Indicates a situation that could result in explosion.

INFORMATION

Indicates useful tips or additional information.

NOTICE

Indicates a situation that could result in equipment or property damage.

2.1.1 General

If you are NOT sure how to install or operate the unit, contact your dealer.

WARNING

Improper installation or attachment of equipment or accessories could result in electrical shock, short-circuit, leaks, fire or other damage to the equipment. Only use accessories, optional equipment and spare parts made or approved by Daikin.

WARNING

Make sure installation, testing and applied materials comply with applicable legislation (on top of the instructions described in the Daikin documentation).

CAUTION

Wear adequate personal protective equipment (protective gloves, safety glasses,...) when installing, maintaining or servicing the system.

WARNING

Tear apart and throw away plastic packaging bags so that nobody, especially children, can play with them. Possible risk: suffocation.

2.1.2 Installation site

Do NOT install the equipment in a potentially explosive atmosphere.

2.1.3 Electrical

DANGER: RISK OF ELECTROCUTION

- Turn OFF all power supply before connecting electrical wiring or touching electrical parts.
- Disconnect the power supply for more than 10 minutes, and measure the voltage at the terminals of main circuit capacitors or electrical components before servicing. The voltage MUST be less than 50 V DC before you can touch electrical components. For the location of the terminals, see the wiring diagram.
- Do NOT touch electrical components with wet hands.
- Do NOT leave the unit unattended when the service cover is removed.

WARNING

A main switch or other means for disconnection, having a contact separation in all poles providing full disconnection under overvoltage category III condition, shall be installed in the fixed wiring.

WARNING

- ONLY use copper wires.
- Make sure the field wiring complies with the applicable legislation.
- All field wiring must be performed in accordance with the wiring diagram supplied with the product.
- Make sure to install earth wiring. Do NOT earth the unit to a utility pipe, surge absorber, or telephone earth. Incomplete earth may cause electrical shock.
- Make sure to use a dedicated power circuit. NEVER use a power supply shared by another appliance.
- Make sure to install the required fuses or circuit breakers.
- Make sure to install an earth leakage protector. Failure to do so may cause electric shock or fire.

WARNING

- After finishing the electrical work, confirm that each electrical component and terminal inside the electrical components box is connected securely.
- Make sure all covers are closed before starting up the unit.

2.2 Daikin system equipment

The installation requires:

- The gateway MCS341-DS1-111, spare part number EU.SB.5000072. The wiring to connect to the power convertor is included here.
- An AC/DC power convertor (PWD-90AW24), spare part number 999175A.

And one of the following:

- iTM controller, product number DCM601A51
- LC8 controller, product number DLC602B51

For more information on this equipment, see "4 To commission the iTM or LC8 controller" [▸ 21].

If there is a missing or defective part, contact the dealer where you purchased this product.

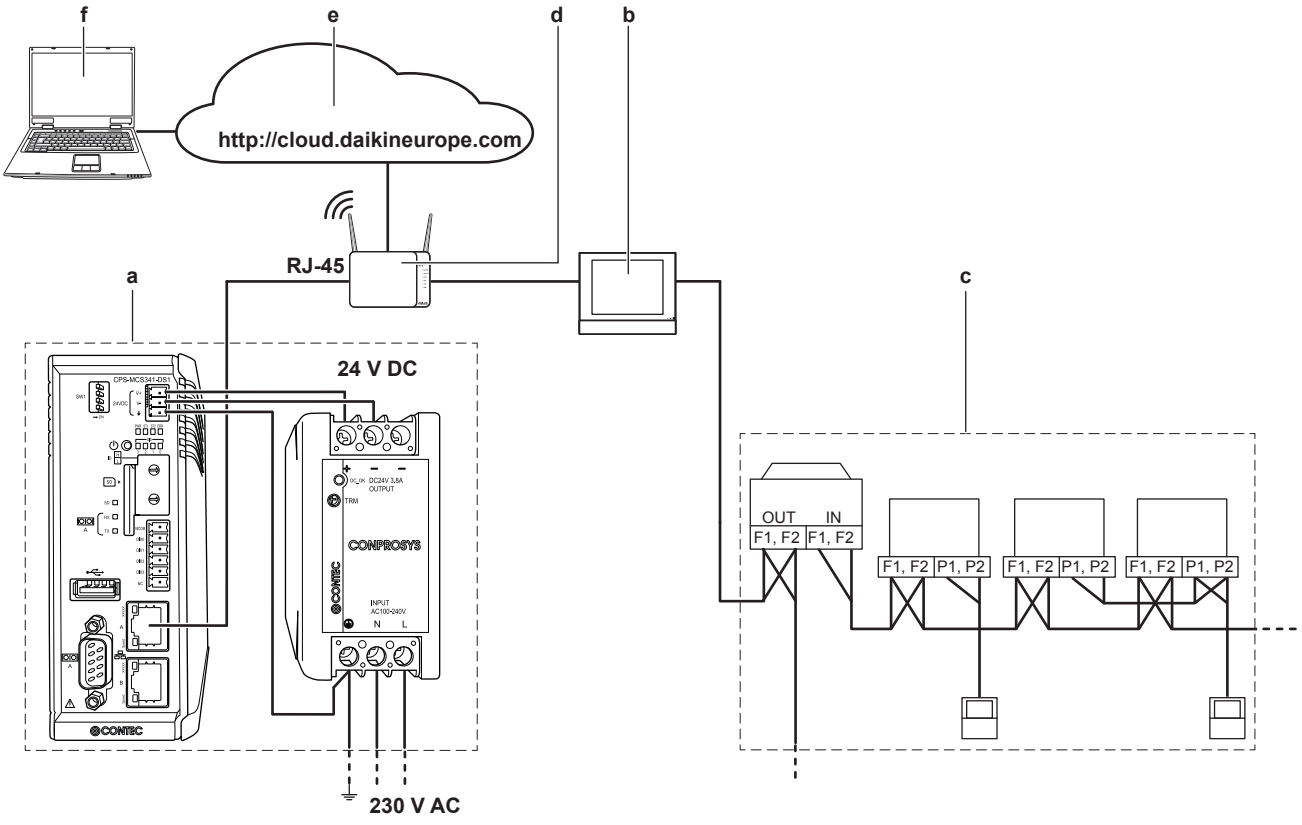
2.3 System description

The Security gateway allows the iTM and LC8 to connect through the Security gateway to the Daikin Cloud Service.

Now, instead of sending the report to the router directly, the iTM or LC8 controller sends the report to the Security gateway first. The Security gateway transforms the report format from http to https and then sends the transformed https report to the Daikin Cloud Service via the router.

2.3.1 Local network setup

Set up the local network as shown in the following diagram:



a Security gateway
b iTM or LC8
c Units
d LAN gateway
e Daikin Cloud Service
f Computer with connection to the Daikin Cloud Service

The table is only intended as an example and only applicable for the setup indicated in the image above.

	iTM or LC8	Security gateway	Router
IP Address	192.168.1.50	192.168.1.51	192.168.1.1
SubnetMask	255.255.255.0	255.255.255.0	255.255.255.0
Default gateway	192.168.1.51	192.168.1.1	
Preferred DNS	192.168.1.51	192.168.1.254	
Alternate DNS	192.168.1.51	192.168.1.254	

2.3.2 Specifications

Category	Class	Specifications	Remarks
Hardware	Manufacturer	CONTEC	—
	Model number	MCS341-DS1-111	—
	CPU	ARM Cortex-A8 600 MHz	—
	LAN port	10BASE-T/100BASE-TX	—
	RAM	512 MB	—
	ROM	32 MB	—
	OS	Ubuntu 14.04	—
	Temperature range	–20°C~+60°C	—
	SD card capacity	4 GB	—
	Boot disc	SD card	—

2.4 Before installation

Before you start installing the Security gateway, complete the following preparations:

- check that the Security gateway module and power supply come with all accessories,
- check that you have all equipment necessary to install the Security gateway modules, see "About necessary equipment" [▸ 7],
- familiarize yourself with the location of the terminals and switches of the Security gateway modules, see "About the location of the terminals" [▸ 8].

2.4.1 About necessary equipment

Use the following equipment to install Security gateway modules:

- a flat-blade screwdriver,

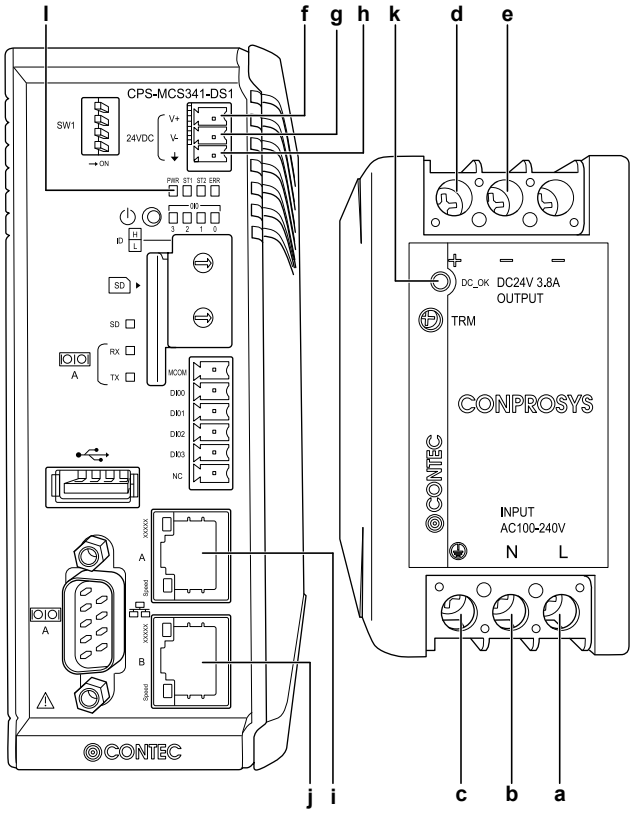
- a Phillips screwdriver,
- the necessary amount of electrical wires and appropriate wiring tools.

For more information on what wires to use, see "2.6 About electric wiring" [▸ 9].

2.4.2 About the location of the terminals

Understand the arrangement of terminals and the location of openings on the module and plan how to route the cable and in which order to connect its wires to facilitate the installation procedure.

For connection details see "2.6 About electric wiring" [▸ 9].



a Live terminal 230 V AC
b Neutral terminal 230 V AC
c Earth terminal
d Power supply output 24 V DC (+)
e Power supply output 24 V DC (–)
f Contact input 24 V DC (+)
g Contact input 24 V DC (–)
h Earth terminal
i Ethernet connection (A) Refer to Setup types in "8 Appendix A – About detecting the IP address of the Security gateway" [▸ 35] For correct wiring
J Ethernet connection (B) Refer to Setup types in "8 Appendix A – About detecting the IP address of the Security gateway" [▸ 35] For correct wiring
k "DC_OK" LED (DC_OK)
l "PWR" LED (PWR)

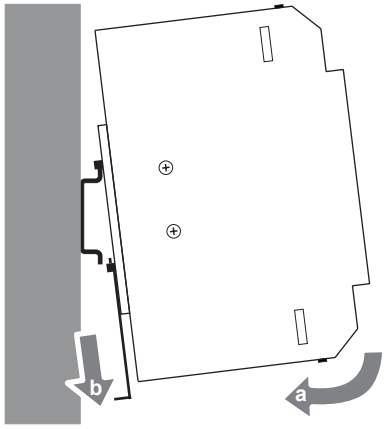
2.5 To install the 2 Security gateway hardware components

The Security gateway modules are to be mounted onto a 35 mm DIN rail.

1. Place the module over the top of the DIN-35 rail so that the upper hook on the rear face is hooked in.
2. Push the module in direction (a) until the lower hook snaps into the rail.

3 If necessary, pull the lever on the lower parts of the module in direction (b) to click the module onto the rail. Use a flat-blade screwdriver if necessary.

4 Repeat the previous steps for all other modules.



2.6 About electric wiring

This chapter will describe the procedure to connect the Security gateway components with Daikin devices and other equipment.

For all wiring requirements see "7.4 Wiring requirements Security gateway" [▸ 33].

WARNING

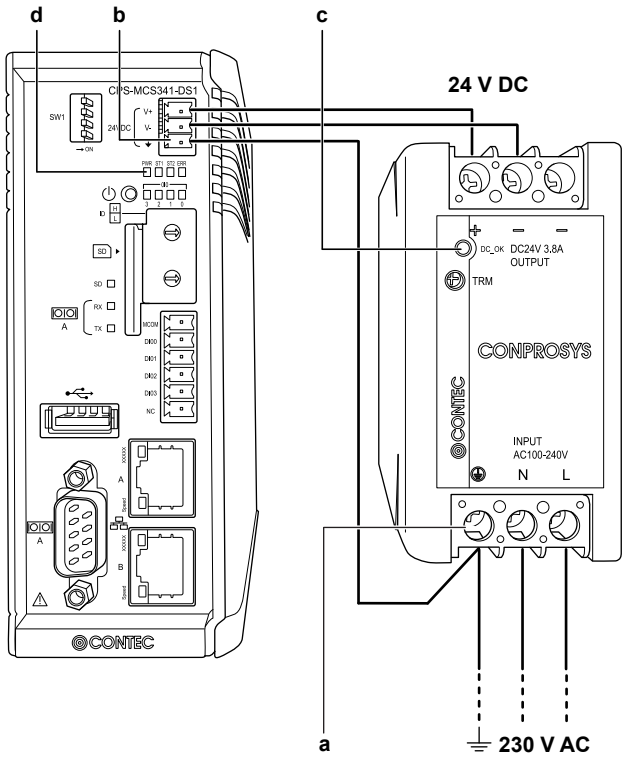
- Do NOT turn on the power supply before all wire connections are completed. Not doing so may cause an electric shock.
- After the wiring is completed, double-check that all wires are connected correctly before turning on the power supply.
- All field supplied parts, materials and electric works MUST comply with the applicable legislation.

INFORMATION

At the time of writing, some connectors are NOT active, but provided for future use.

2.6.1 To connect the power supply

Connect the power supply as shown in the following arrangement:



1 Connect the power supply to the 3 terminals, L (live), N (neutral) and ground in the input section of the power supply (PS).

Using the wiring delivered with the Security gateway:

2 Connect the DC power supply output terminals of the PS to the contact input terminals of the Security gateway module. Take the polarity of the wires into account.

3 Connect the earth terminal of the PS (a) to the earth terminal of the Security gateway (b).

Once all wiring has been completed:

4 Double-check and then turn on the power supply.

CAUTION

The power supply is **ONLY** guaranteed when the "DC_OK" LED (DC_OK)(c) on the PS **and** the "PWR" LED (PWR) (d) on the Security gateway module are green.

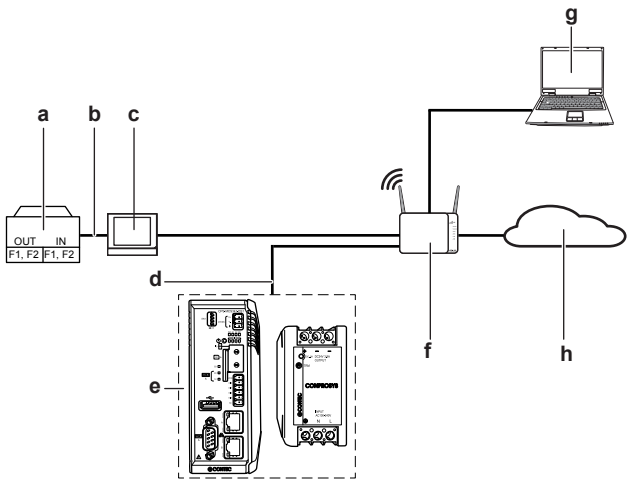
If one or more of the above LEDs are NOT lighting up, check for faulty wiring.

2.6.2 To connect the Security gateway to the local network

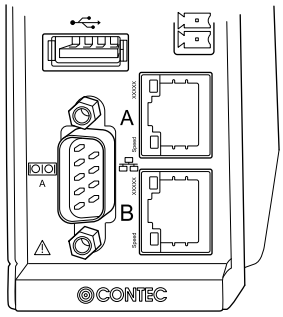
Basic setup (recommended)

1 Connect the power supply in the same way as shown in "To connect the power supply" [▸ 9].

2 Add the Security gateway to the local network as shown in the following figure:



Only LAN port A will be used in this case.



a Outdoor unit
b LAN connection (DIII)
c iTM or LC8 controller
d LAN connection to port A
e Security gateway
f LAN gateway (RJ-45)
g User PC
h Daikin Cloud Service

Plug in the power supply.

To connect to DIII-NET compatible equipment

Refer to:

- Ainet handbook:
  - For commissioning of the iTM or LC8 controller
  - Format: Digital files on http://www.daikineurope.com/support-and-manuals/product-information/
- iTM installation manual
- LC8 installation manual

To connect the LAN cable

For all wiring requirements see "2.3 System description" [▸ 6].

Do NOT connect the LAN cable until you start commissioning the LAN Gateway. Otherwise, a network address conflict may occur.

3 Commissioning

WARNING

Only qualified persons should conduct commissioning.

CAUTION

Preliminary electrical system checks such as earth continuity, polarity, resistance to earth and short circuit must be carried out by using a suitable test meter by a competent person.

3.1 About commissioning the Security gateway setup

After you have verified that the Security gateway components have been installed and all necessary wiring has been completed, you can start the commissioning of your Security gateway setup.

In this commissioning phase, you will do the following:

- Configure your computer to be able to connect to the Security gateway, see chapter "To connect to the intelligent Tablet Controller for the first time" in the intelligent Tablet Controller Installer reference guide.
- Configure the LAN settings, see "3.3 To connect to the Security gateway for the first time" [▸ 13] To configure the network settings (local commissioning tool).
- Configure the date and time, see "To set up the time zone of the Security gateway" [▸ 20].
- Add all attached (Daikin) equipment to the Security gateway web interface, see "4 To commission the iTM or LC8 controller" [▸ 21] to configure the connected devices quickly (local commissioning tool).

3.2 Minimum requirements for the commissioning

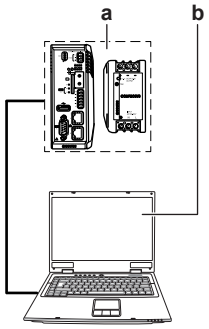
Before you start configuring the Security gateway, complete the following preparations.

- Make sure your computer specs comply with the minimal requirements mentioned in "7.5 System requirements" [▸ 34].
- Contact your network administrator for the following network information for the Security gateway:
  - the desired network name for the Security gateway,
  - the static IP address and corresponding subnet mask of the Security gateway,
  - the static IP address and corresponding subnet mask of the iTM or LC8 controller,
  - the IP address of the default gateway,
  - the IP address of the DNS server, and
  - the IP address of the alternate DNS (if applicable).
- Make sure the power of all connected equipment is turned on.

3.3 To connect to the Security gateway for the first time

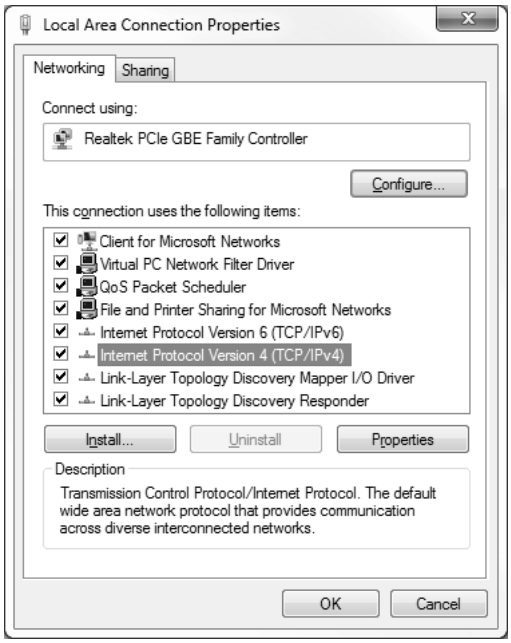
A new Security gateway module has a fixed IP address 192.168.0.126 and a subnet mask 255.255.255.0.

To connect to this device, you will have to change the IP address of your computer to the same range as this IP address.



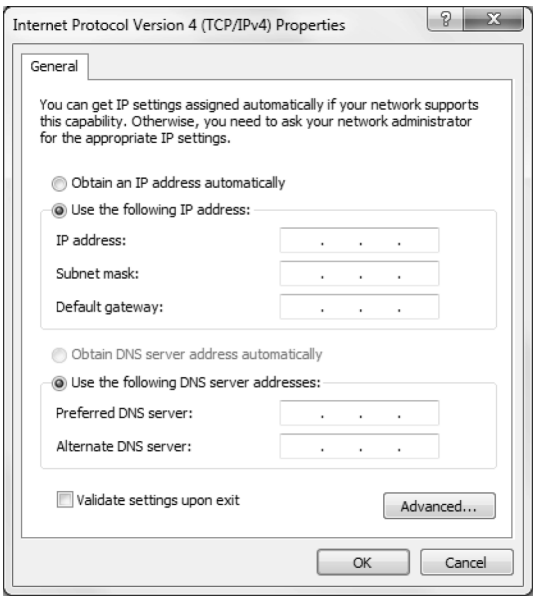
1. Plug a CAT 5e (or higher) Ethernet cable into the Security gateway module (a).
2. Connect the Ethernet cable with your computer (b) and change your IP address to match that of the Security gateway module.
3. On your computer, go to the Control Panel.
4. In the Control Panel, click the Network and Sharing Center option and then the Change Adapter Settings option.
5. In the Network Connections window, double-click the Local Area Connection option.

   Result: The following window appears.



6. Select the Internet Protocol Version 4 (TCP/IPv4) option and click the Properties button.

   Result: The following window appears.

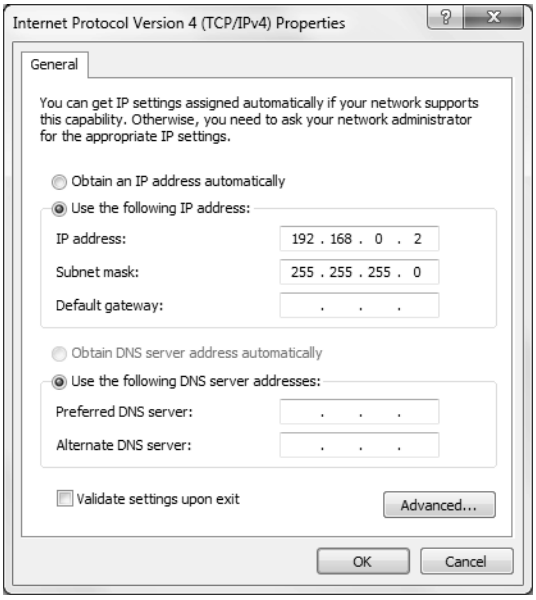


7 Click the Use the Following IP Address: radio button.

8 Set the following IP address (IP address): "192.168.0.2".

> **INFORMATION**
>
> This example uses 192.168.0.2, but you can choose any address in the range of 192.168.0.2~192.168.0.254 (except . 192.168.0.126).

9 Set the following Subnet mask (Subnet mask): "255.255.255.0".



10 Click the OK (OK) button.

To prevent interference from any wireless network, disable all wireless network cards on your computer as follows:

11 In the Network Connections window, right-click the Wireless Network Connection option.

12 Select the Disable option.

13 Check if you can make a connection from your computer to the Security gateway module. To do so, open the command prompt on your computer as follows:

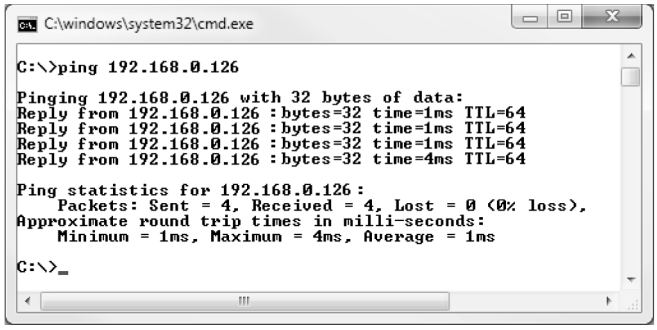
14 Click the Windows Start button.

15 In the Search box, type "Command Prompt", or alternatively "Cmd".

16 In the list of results, click the Command Prompt or Cmd option respectively.

17 Ping to the IP address of the Security gateway module. To do so, enter: "ping 192.168.0.126" and confirm by pressing the Enter key.

Result: You will receive an answer as the example below:



INFORMATION

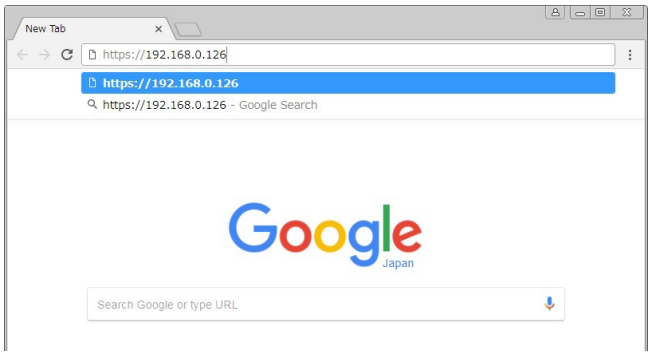
If you do NOT get replies, but time-outs instead, there might be something wrong with the connection. Refer to "6 Troubleshooting" [▸ 31] to fix the problem.

3.4 About configuring the Security gateway

3.4.1 To access the Security gateway

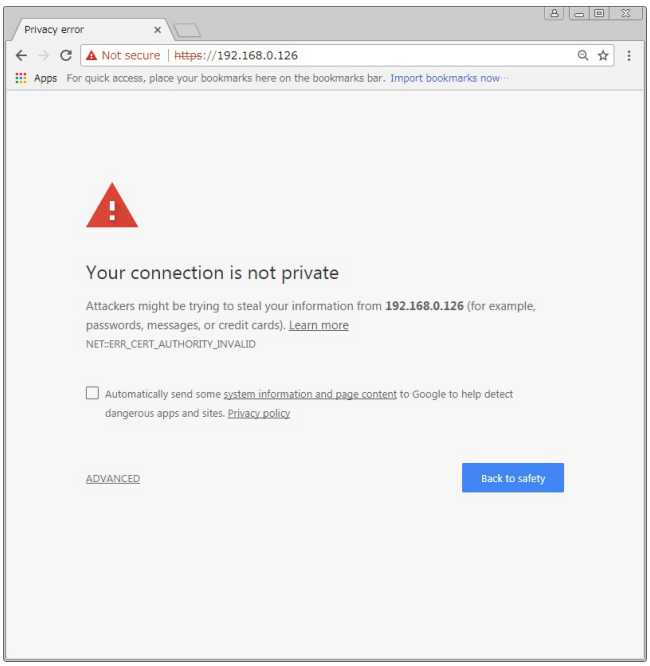
See "8 Appendix A – About detecting the IP address of the Security gateway" [▸ 35] for how to detect the IP address of the Security gateway in case you forgot it.

1 Type the default IP address of the Security gateway (https://192.168.0.126) in the URL bar of the web browser (Google Chrome or Microsoft Edge).

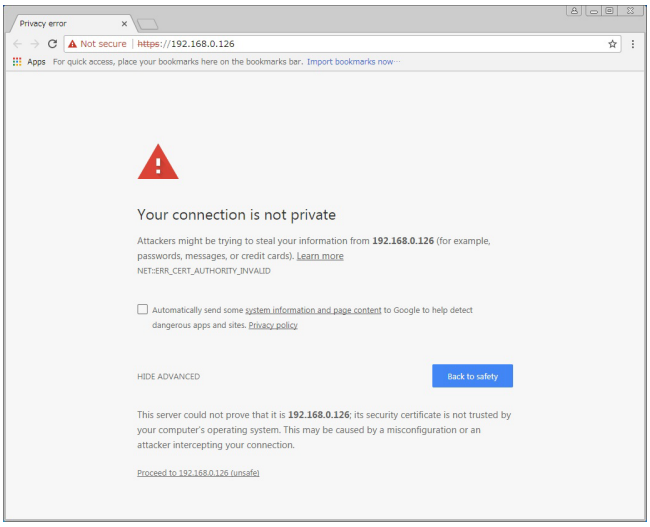


Result: A warning message about the connection appears.

2 Click ADVANCED (ADVANCED) to show the advanced setup window.

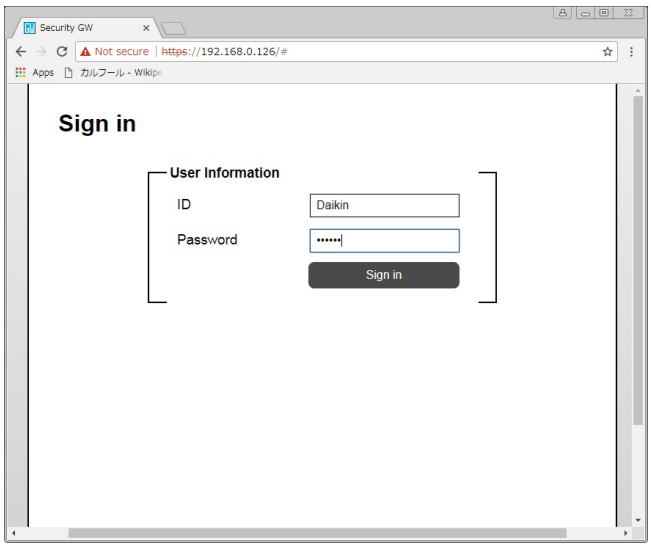


3 Click Proceed to 192.168.0.126 (unsafe) (Proceed to 192.168.0.126 (unsafe)).



Result: A login window appears

4 Fill out ID (ID) and Password (Password) (default ID: Daikin / default password: Daikin) of the Security gateway and click the Sign in (Sign in) button.

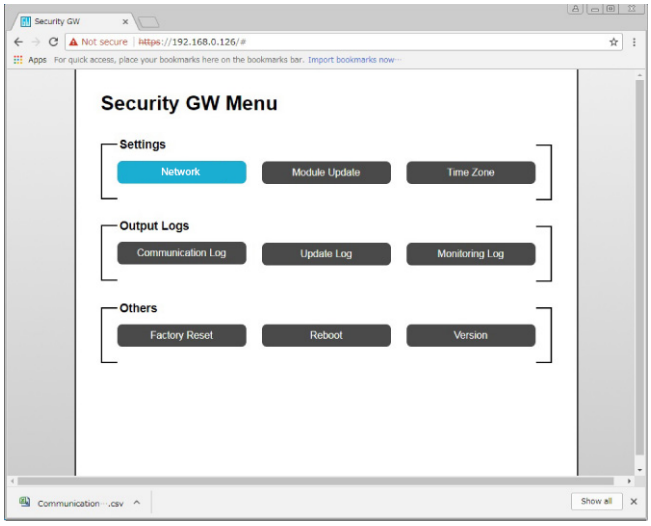


Result: The Security GW Menu (Security GW Menu) window appears.

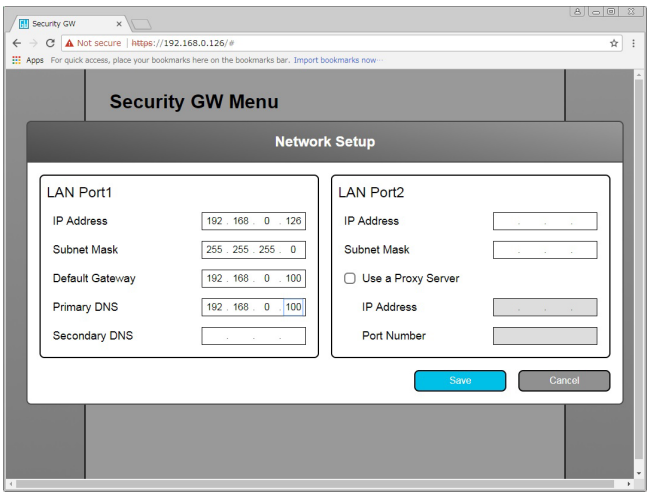
3.4.2 To set up the network of the Security gateway

To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▸ 15].

1 Click the Network (Network) button.



Result: The Network Setup (Network Setup) dialog appears.



2 Fill out the following network data:

LAN Port1 (LAN Port1) (=A)

- IP Address (IP address): Unique IP (default: 192.168.0.126) address in local network
- Subnet Mask (Subnet mask): 255.255.255.0
- Default Gateway (Default Gateway): IP address (default: 192.168.0.100) of local router
- Primary DNS (Primary DNS): IP address (default: 192.168.0.100) of local router
- Secondary DNS (Secondary DNS): leave blank

LAN Port2 (LAN Port2) (=B)

- Leave empty

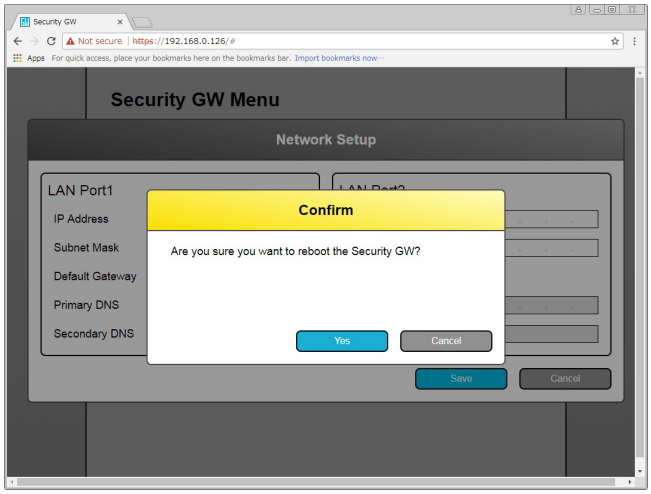
INFORMATION

If the IP address (IP address), default gateway (Default gateway) and primary DNS (Primary DNS) are according to the conditions of the local network, you do not need to change them.

3 Click the Save (Save) button.

Result: The Confirm (Confirm) dialog appears.

4 Click the Yes (Yes) button to reboot the Security gateway.



Result: This will reboot the Security gateway.

Result: The web browser window appears.

Result: The IP address will be changed.

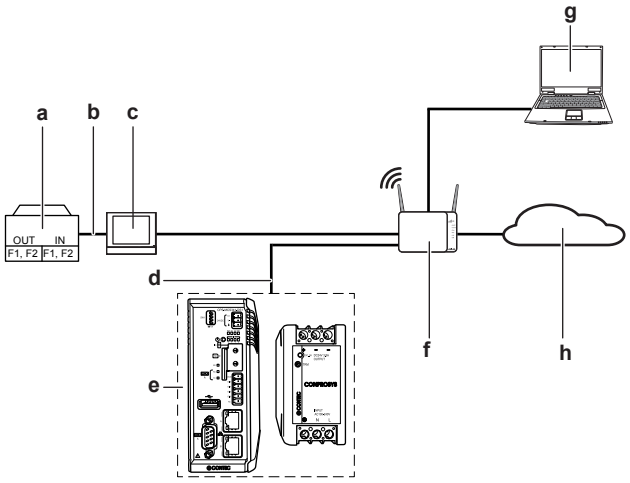
> **INFORMATION**
>
> The web browser communication will be lost once step 4 is executed. Follow the procedure as described in "To access the Security gateway" [▸ 15] to reconnect by using the new IP address.

5 Reset the LAN network settings of your computer to their original values.

6 If you disabled it before, enable the WiFi adapter of your computer.

7 Disconnect the Ethernet cable between your computer and the Security gateway module.

8 Connect an Ethernet cable between the Security gateway module and the local network.

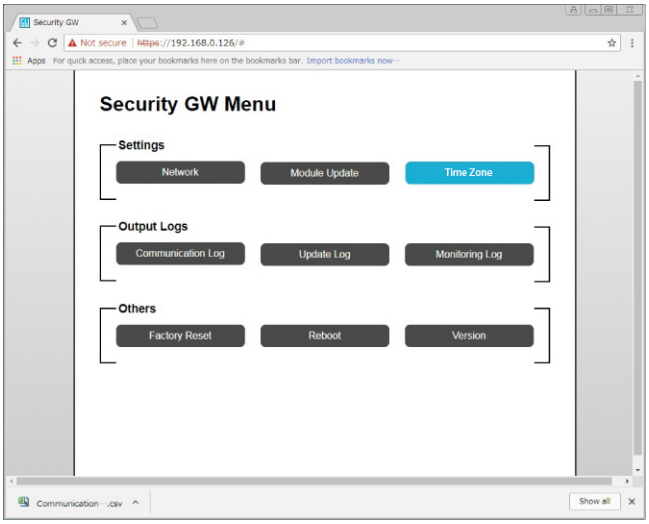


> **INFORMATION**
>
> For confirmation that the IP address is changed correctly, access the Security gateway as described in "To access the Security gateway" [▸ 15] by using the new IP address.

3.4.3 To set up the time zone of the Security gateway

To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▶ 15].

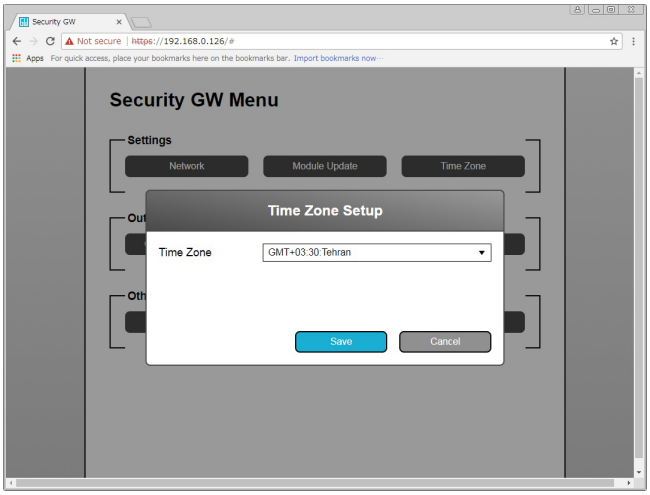
1 Click the Time Zone (Time Zone) button.



Result: The Time Zone Setup (Time Zone Setup) dialog appears.

2 Click the [▼] button to open Time Zone drop-down list >> select and click the time zone.

3 Click the Save (Save) button.



4 To commission the iTM or LC8 controller

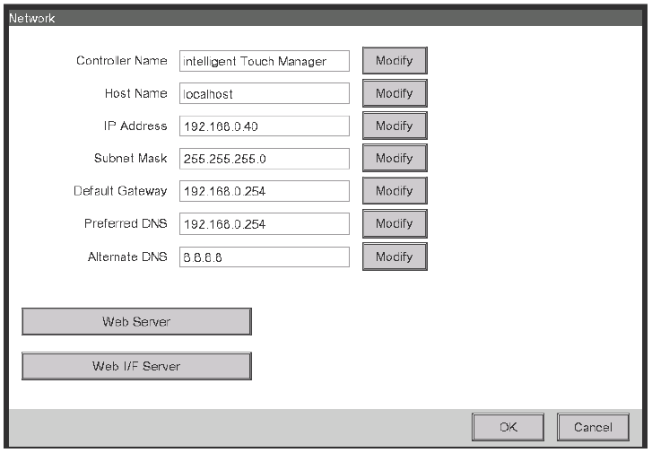
1 Refer to the Airnet Handbook for the Installation of the iTM or LC8 controller.

The next steps are a deviation of the Airnet Handbook, make sure the settings on the iTM or LC8 controller are as mentioned in step 3.

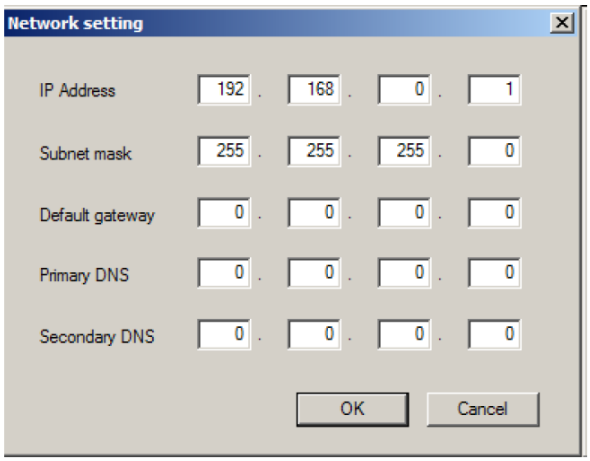
2 Refer to "2.3 System description" [▸ 6] fort he setup.

3 Setup the network of the local controller according to the table below.

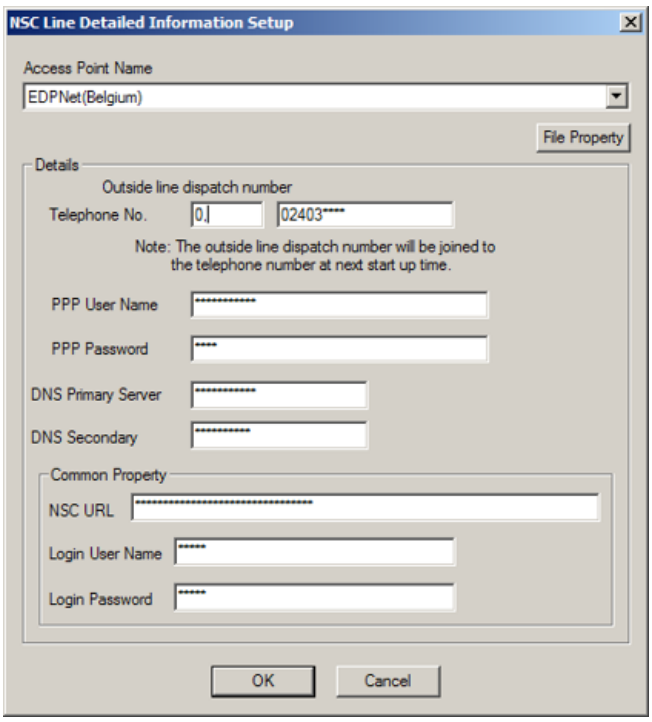
iTM



LC8

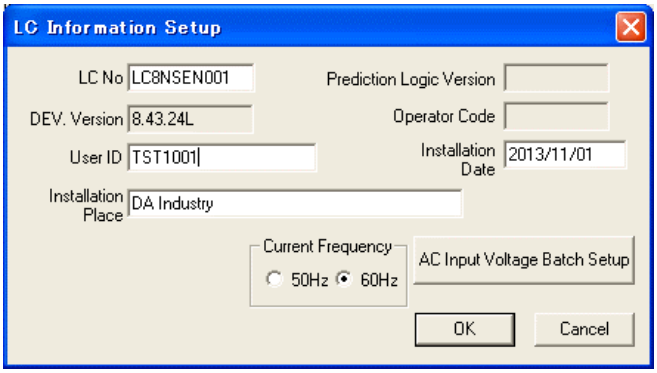


4 Set NSC URL http://Lcc.m2m.daikineurope.com/NSC and select the correct Access Point Name (Access Point Name) from the selection list. The details (Details) section can remain empty.



5 Connect with your Daikin Cloud Service credentials to https://cloud.daikineurope.com. and create a new site. As soon as the site is created, note down the iTM or LC8 number:

- iTM No: The registered id number of the intelligent Touch Manager. This number will be in the following format: LT2N###### (with # being an alphanumerical value).
- LC8 No: The registered id number of the LC8 Controller. This number will be in the following format: LC8N###### (with # being an alphanumerical value).



5 Operation

5.1 About logs download

You can record and download three logs via the web application of the Security gateway.

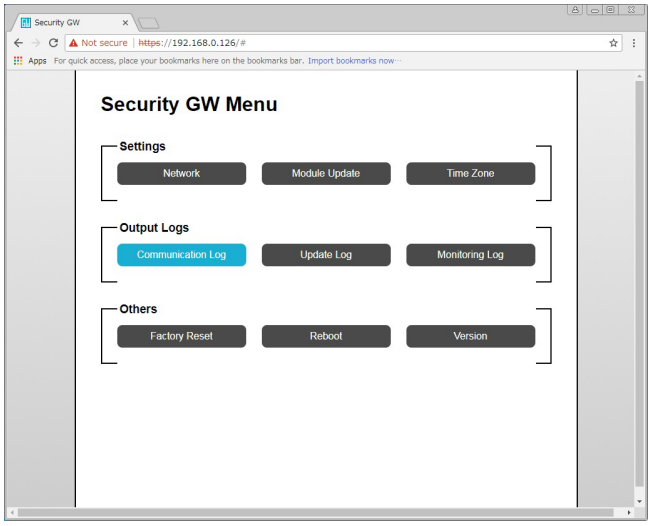
The following logs can be used to validate the correct functionality of the Security gateway in case of issues:

File type	Purpose
Communication Log	This will contain the information regarding the timing and the type of data the Security gateway sent to the cloud platform.
Update log	This will contain the information regarding the update check, timing of when the Security gateway checked for an available update, and the indication if a new software version was installed.
Monitoring log	This will contain the information regarding the actions executed on the Security gateway as example when it was turned off and when it was turned on.

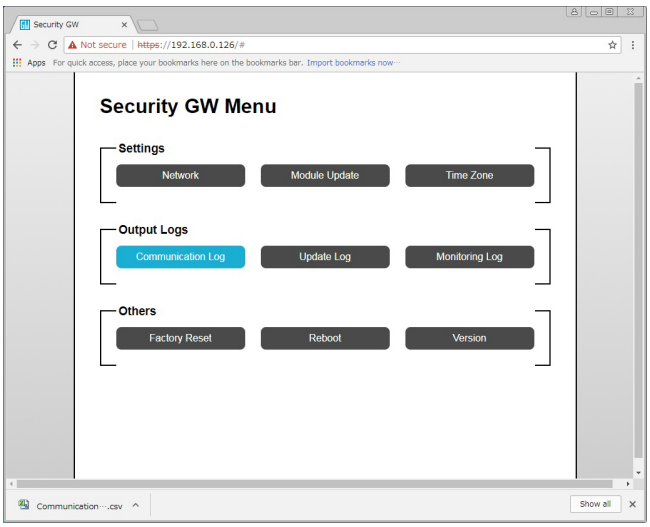
5.1.1 To download communication logs

To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▸ 15].

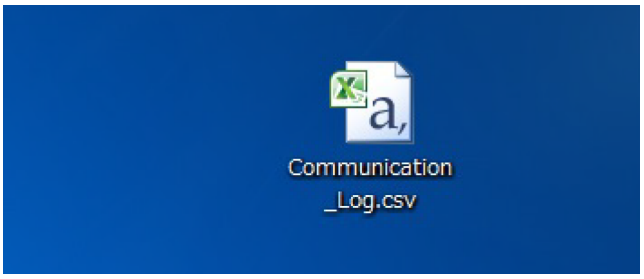
1 Click the Communication Log (Communication Log) button.



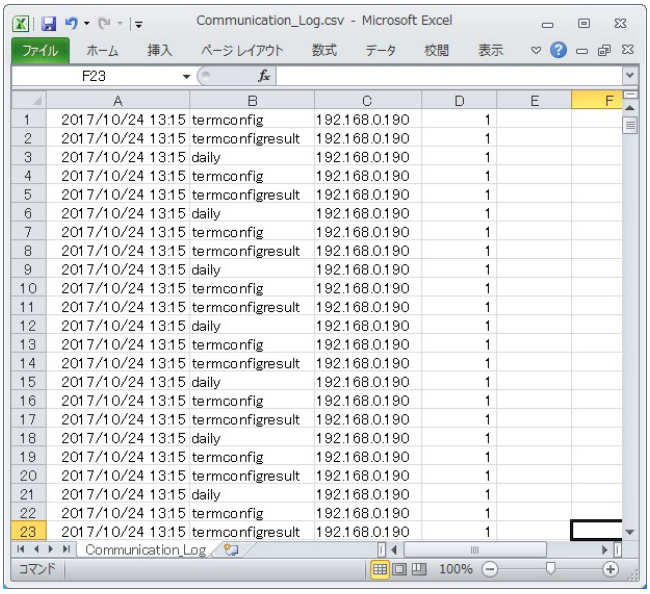
2 Check the download status in the download bar at the bottom of the window.



3 Find and double-click (to open) the downloaded communication log .csv (Communication_Log.csv) file on the desktop.



4 Check the details of the communication log .csv (Communication_Log.csv) file.



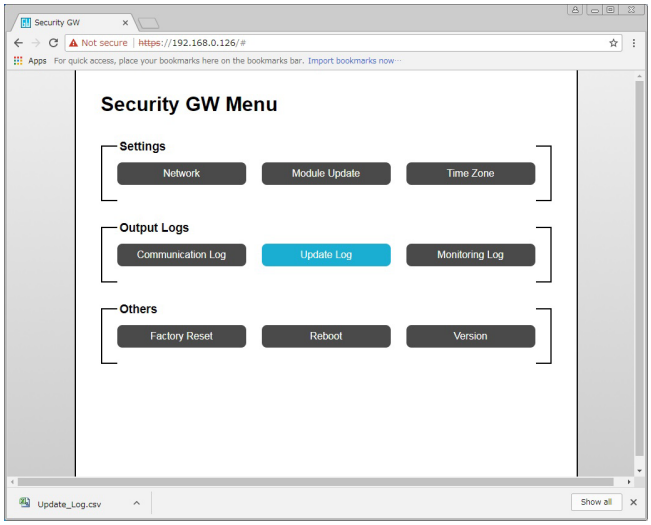
	A	B	C	D	E	F
1	2017/10/24 13:15	termconfig	192.168.0.190	1		
2	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
3	2017/10/24 13:15	daily	192.168.0.190	1		
4	2017/10/24 13:15	termconfig	192.168.0.190	1		
5	2017/10/24 13:15	termconfigresult	192.168.0.190	1		
6	2017/10/24 13:15	daily	192.168.0.190	1		
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 To download update logs

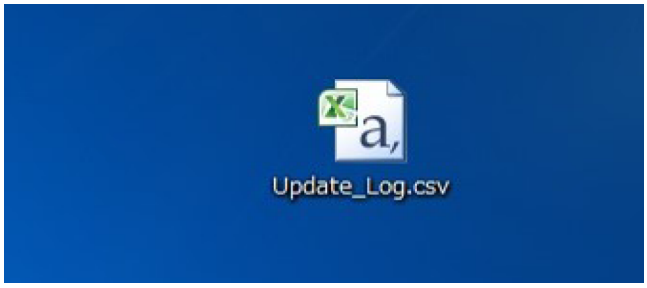
To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▶ 15].

1 Click the Update Log (Update Log) button.

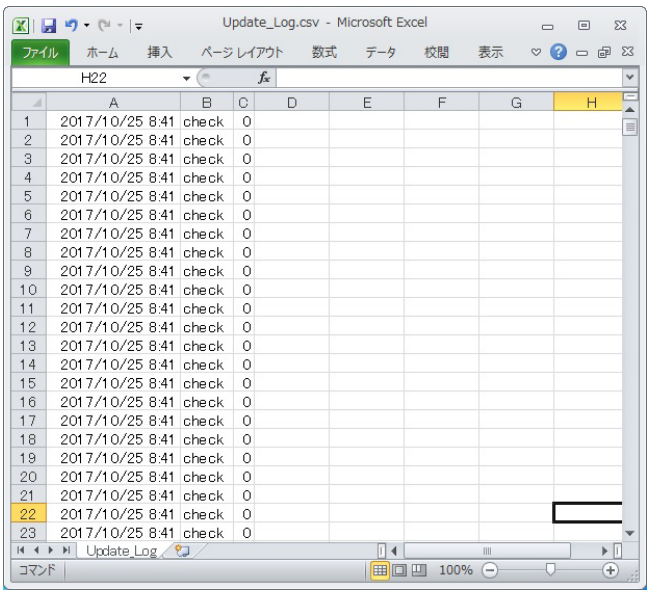
2 Check the download status in the download bar at the bottom of the window.



3 Find and double-click (to open) the downloaded update log .csv (Update_Log.csv) file.



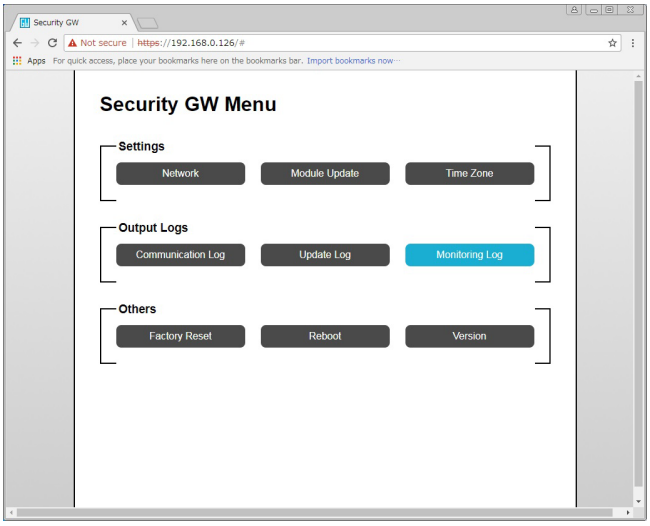
4 Check the details of the update log .csv (Update_Log.csv) file.



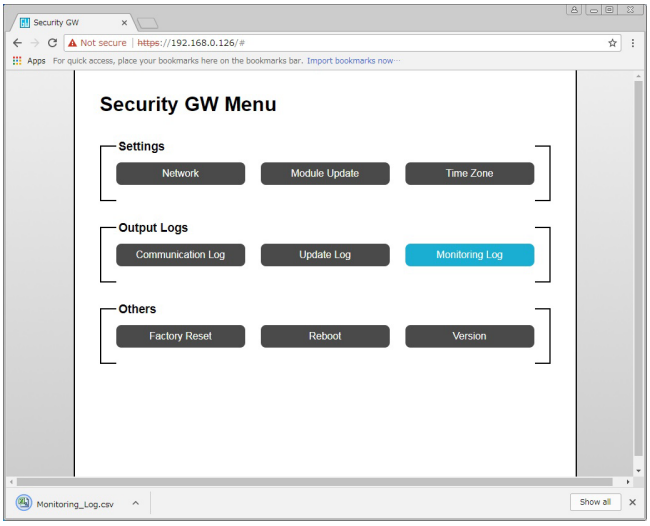
5.1.3 To download monitoring logs

To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▶ 15].

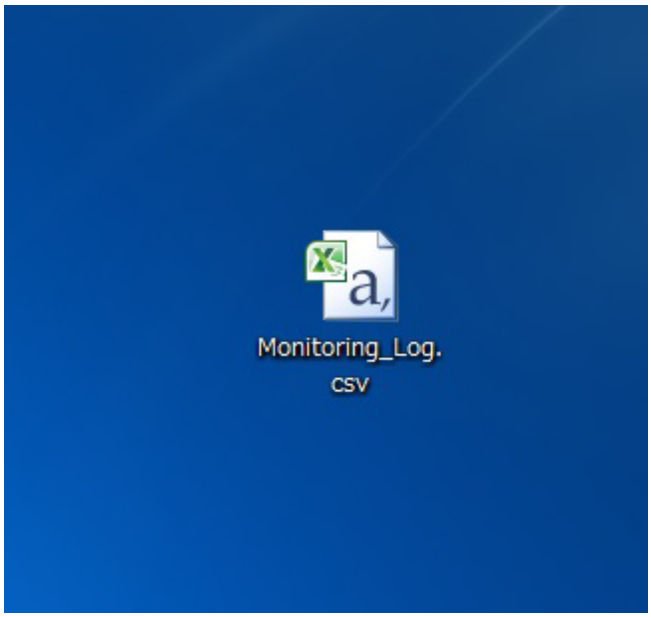
1 Click the Monitoring Log (Monitoring Log) button.



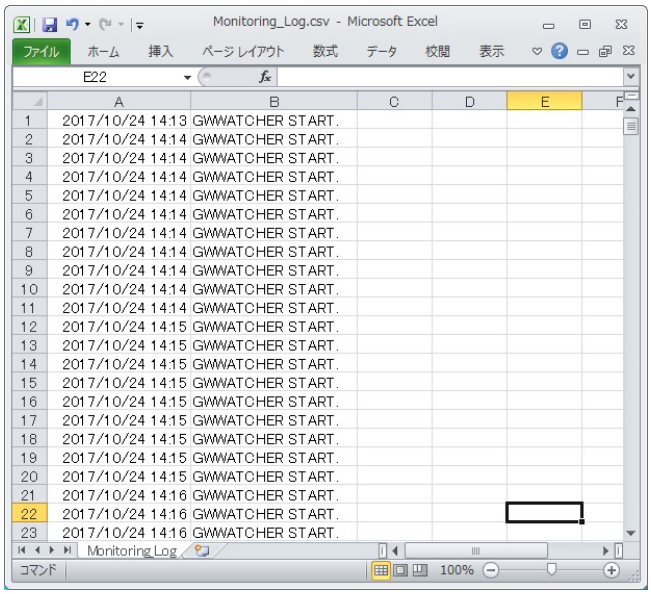
2 Check the download status in the download bar at the bottom of the window.



3 Find and double-click (to open) the downloaded monitoring log .csv (Monitoring_Log.csv) file on the desktop.



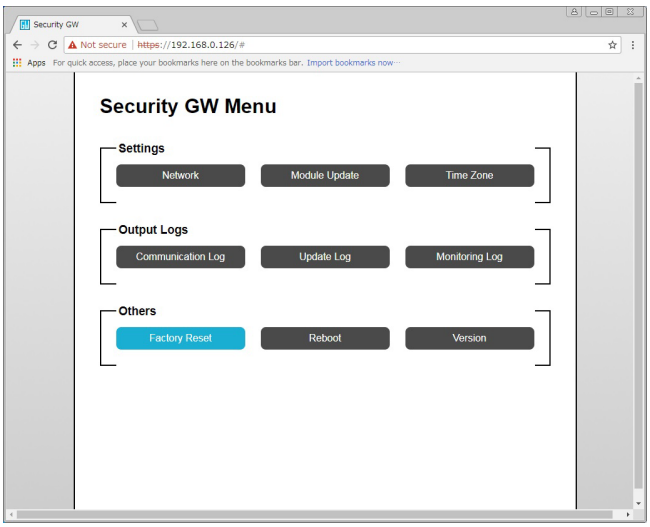
4 Check the details of the monitoring log .csv (Monitoring_Log.csv) file.



5.2 To reset the Security gateway to its factory settings

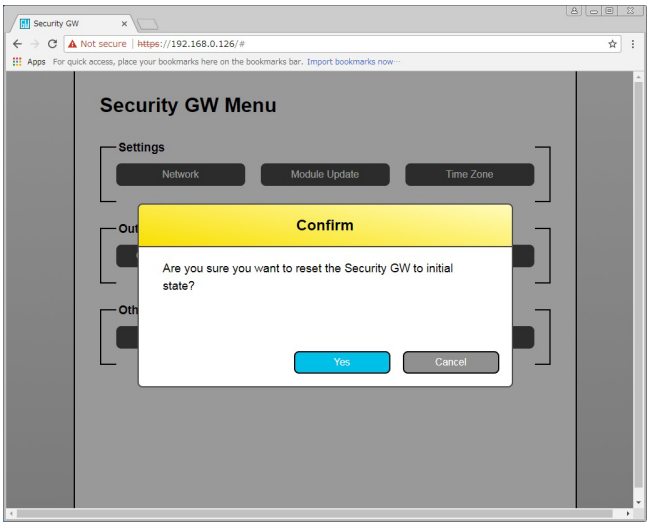
To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▸ 15].

1 Click the Factory Reset (Factory reset) button.



Result: The Confirm (Confirm) dialog appears.

2 Click the Yes (Yes) button of the confirmation dialog.

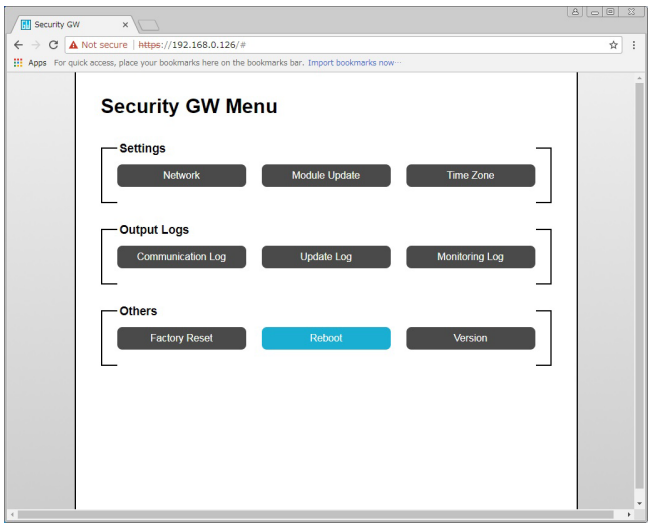


Result: The Security gateway is reset to the original manufacturer settings.

5.3 To reboot the Security gateway

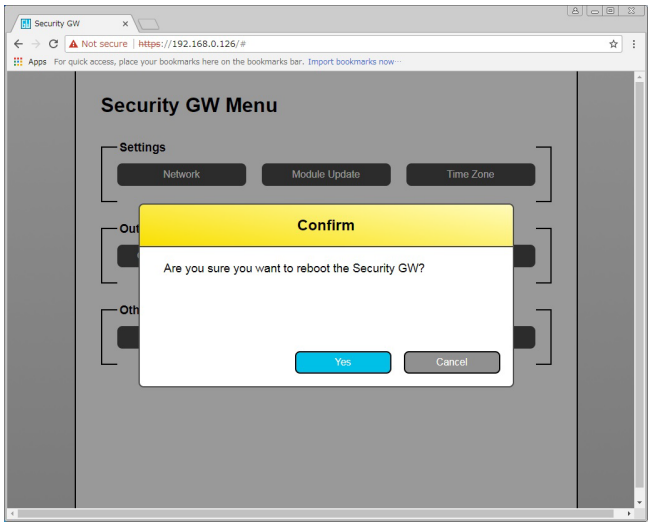
To access the Security GW Menu (Security GW Menu), refer to "To access the Security gateway" [▸ 15].

1 Click the Reboot (Reboot) button.

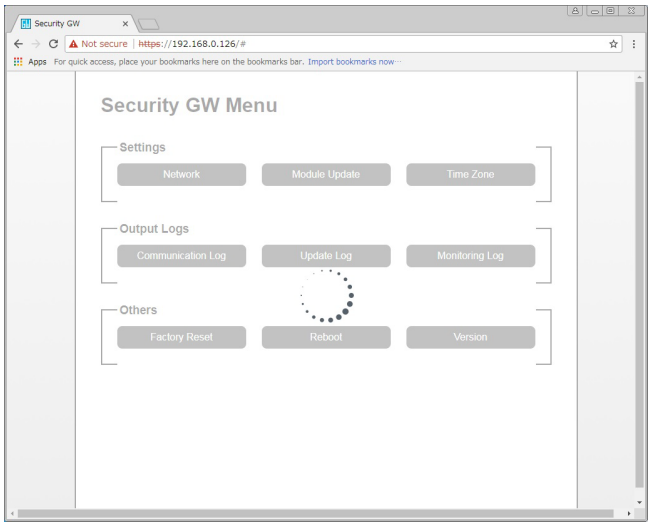


Result: The Confirm (Confirm) dialog appears.

2 Click the Yes (Yes) button.



Result: The confirmation dialog disappears and all of the buttons are grayed-out and disabled.



Result: The Security gateway is rebooted.

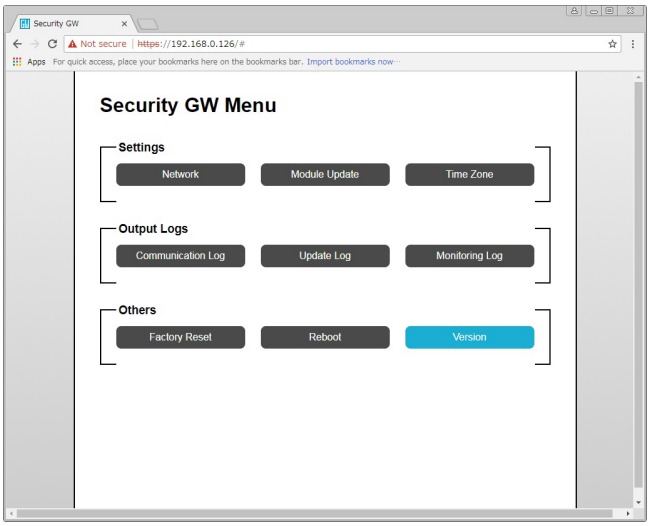
5.4 To check the version numbers

In some cases you might need to communicate the version numbers of your Security gateway. Via the web application's menu you can retrieve the version of:

- The web application (browser based and specific Security gateway setup tool) of the Security gateway. [Client Version]
- The Security gateway's hardware, firmware and OS. [Security GW Version]
- The unique serial number for the Security gateway management. [Security GW Number]

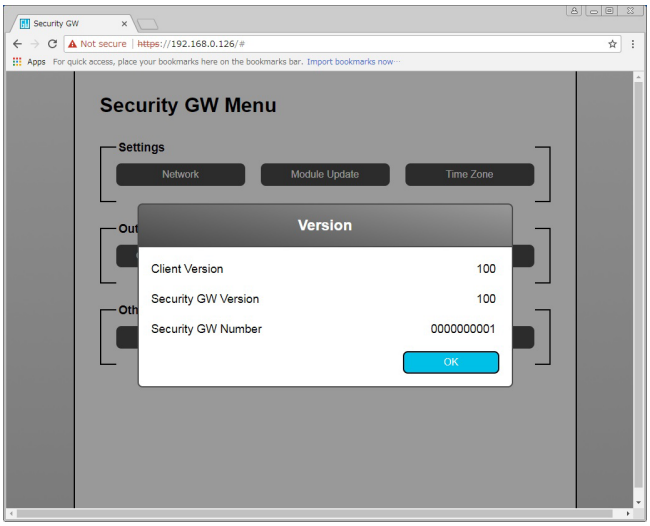
To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▸ 15].

1 Click the Version (Version) button.



Result: The Version (Version) dialog appears.

2 Check the versions.



3 Click the OK (OK) button to go back to the main screen.

Result: The main screen appears.

6 Troubleshooting

6.1 Conceivable failures

Failure	Cause	Solution
Connection failure	Cannot connect to the Security gateway. Check power.	Make sure that the RIGHT SD card is inserted in the SD card slot CORRECTLY. Make sure that the Security gateway is POWERED ON. Check the IP ADDRESS of the Security gateway and the setup PC. Make sure they are included in the same local network. Make sure that the RIGHT LAN ports are used and set: - Left side: Port A - Right side: Port B RESTART the Security gateway * Use the specific Security gateway setup tool when you forgot the IP address of the Security gateway as described in "8.2 To detect the IP address" [▸ 35].
Setup failure	Failure to: ▪ Perform setup, ▪ Download logfiles, ▪ Perform factory reset, ▪ Reboot, ▪ Check the version.	SIGN OUT of the web application of the Security gateway setup or the specific Security gateway setup tool. SIGN IN the web application of the Security gateway setup or the specific Security gateway setup tool again. TRY setup, download log file, factory reset, reboot and version check again.

6.2 Error messages

Category	Description	Remarks
1. Javascript invalid	1.1 Javascript unavailable. Enable Javascript and try again.	—
2. Cookie invalid	2.1 Cookie disabled. Enable cookies in your browser preferences and try again.	—
3. Security gateway connection	3.1 Failed to connect to Security gateway. Check if the Security gateway is connected to the same network.	—

Category	Description	Remarks
4. Sign in	4.1 User ID and/or password are not yet entered.	Input the user ID and password. Click the [Sign in] button.
	4.2 Authentication failed. Invalid User ID and/or password.	Confirm the user ID and password. Input the correct user ID and password. Click the [Sign in] button.
	4.3 Failed to communicate with the Security gateway.	Confirm that the SD card is inserted in the SD card slot. Confirm that the Security gateway is powered ON. Confirm that the LAN cable is inserted in both Security gateway and setup PC. Press the reset button of the Security gateway.
5. Security gateway menu	5.1 Failed to communicate with the Security gateway.	Same as 4.3
	5.2 Log acquisition failed.	—
6. Network setup	6.1 Failed to communicate with the Security gateway.	Same as 4.3
7. Module update setup	7.1 Failed to communicate with the Security gateway.	Same as 4.3
8. Time zone setup	8.1 Failed to communicate with the Security gateway.	Same as 4.3
9. Error dialog	9.1 Your session has expired. Try to sign in again.	—

7 Technical specifications

7.1 Commissioning computer requirements

Item	Specification
OS	Windows 7 Professional (32-bit) or higher
Memory	2 GB RAM or more
Hard drive	20 GB free HD space or more
Ports	1 RJ45 port
Browser	One of the following: ▪ Internet Explorer Version 9, 10 or 11 ▪ Google Chrome ▪ Mozilla Firefox ▪ Apple Safari

7.2 Power consumption specifications Security gateway

Item	Specification
Related input voltage	110~220 V AC
Input power frequency	50~60 Hz
Power consumption CPU module + I/O module	▪ Max.: 13 W (11 W+2 W) ▪ Typical: 5.5 W (4 W+1.5 W)

For more detailed specifications of the power supply, refer to the manual provided with the power supply.

7.3 Default tool passwords

Tool	Password
Authentication code Security gateway web interface	Not set (blank), see "To access the Security gateway" [▸ 15] ▪ default ID Daikin ▪ default password: Daikin

7.4 Wiring requirements Security gateway

WARNING

All field wiring and components MUST be installed by a licensed electrician and MUST comply with the applicable legislation.

All wiring must comply with the following requirements:

Connection	Cross section	Max. length	Remarks
LAN cable	—	100 m	▪ UTP CAT 5e or higher ▪ RJ45 connector
DIII-NET (F1/F2)	Ø0.75~1.25 mm² (terminal sized for maximum 1.5 mm²)	Total length[(a)]: 2000 m (<1500 m when using shielded wire) Max. length[(b)]: 1000 m	▪ Cable type: 2-core vinyl insulated vinyl-sheathed cable/vinyl cabtyre cable or 2-core shielded cable ▪ Do NOT use multicore cables with 3 or more cores ▪ Do NOT use mixed cable types ▪ NEVER bundle the cables ▪ When using a shielded cable, connect only one end of each shield wire to the ground ▪ Make sure the wiring is routed and fixed, so as NOT to touch unearthed accessible conductive parts ▪ Make sure a strain relief is available for each wire entering the electrical cabinet ▪ For more information on DIII-NET, refer to the DBACS design guide (ED72721)
230 V AC power supply to the PU	According to applicable legislation (terminal sized for maximum 4 mm²)	According to applicable legislation	▪ Solid or stranded wire allowed ▪ The internal protection of the WAGO PSU is fused at 2.5 A / 250 V
24 V DC power supply to the Security gateway module	According to applicable legislation	—	Solid or stranded wire allowed

(a) *Total length* is the sum of all wiring in the DIII-NET network.
(b) *Max. length* is the maximum distance between any 2 connection points in the DIII-NET network.

7.5 System requirements

The PC you use for setup of the Security gateway must comply with these minimum requirements:

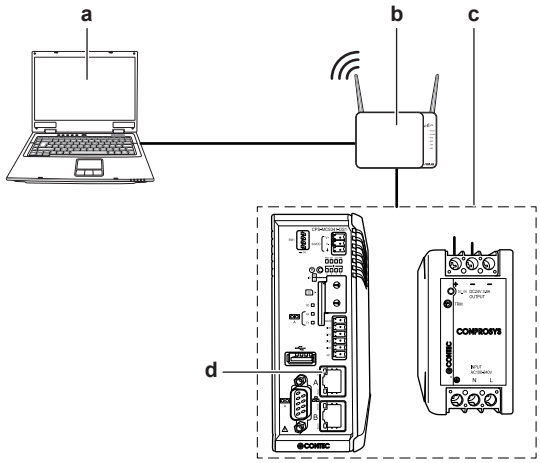
CPU	Intel i3 2.2 GHz or higher
Operating system	Microsoft Windows 7 or higher
Memory	512 MB RAM or more
Free space on hard drive	10 GB or more
Network	10 BASE-T or higher

8 Appendix A – About detecting the IP address of the Security gateway

This appendix explains how to detect the IP address of the Security gateway by using the specific setup tool for the Security gateway.

8.1 To wire the Security gateway

1. Connect the power supply in the same way as shown in "To connect the power supply" [▸ 9].
2. Add the Security gateway to the local network as shown in the following figure:



a PC
b Router
c Security gateway
d LAN port A

Only LAN port A will be used in this case.

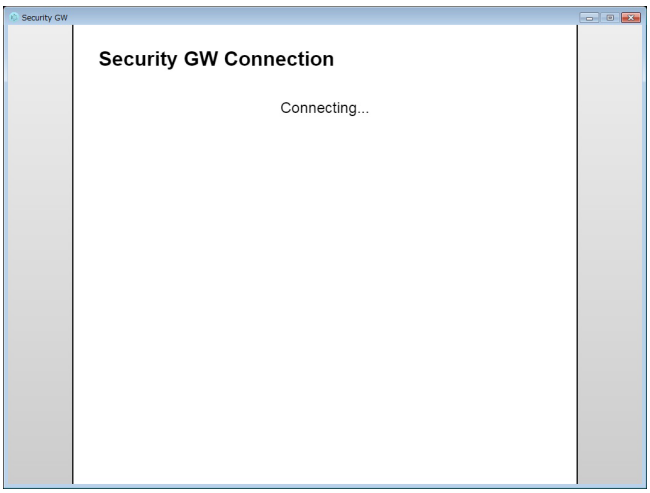
3. Plug in the power supply.

8.2 To detect the IP address

Make sure you have the latest version of the gateway setting tool. The latest version is available on https://my.daikin.eu/denv/en_US/home/applications/product-finder/Daikin-Cloud-Service.html.

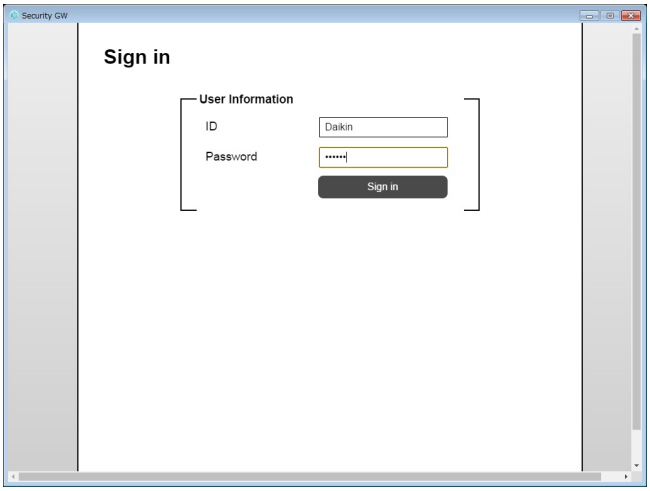
1. Download and extract the zip file containing the GwSettingTool.exe (GwSettingTool.exe) file to a folder on your local drive.
2. Double-click the GwSettingTool.exe file (GwSettingTool.exe) to start the Security gateway setup tool.

   Result: Connecting starts.



Result: After about 1 minute, a login window appears.

3 Fill out ID (ID) and password (Password) (default ID: Daikin / default password: Daikin) of the Security gateway and click the Sign in (Sign in) button.



Result: The Security GW Menu (Security GW Menu) window appears.

4 Click the Network (Network) button.

Result: The Network Setup (Network Setup) dialog appears.

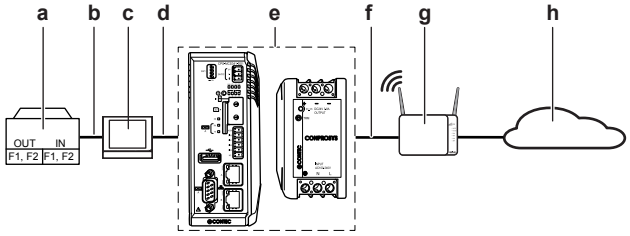
5 Check the IP address (IP address) of LAN Port1 (LAN Port1).

9 Appendix B – About commissioning in case of Proxy Server

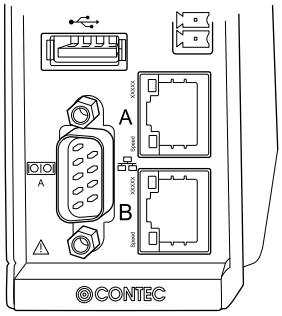
This appendix explains how to perform the initial setup of the Security gateway if the topological structure does not correspond to the standard one described "Local network setup" [▸ 6].

9.1 Alternative setup

1. Connect the power supply in the same way as shown in "To connect the power supply" [▸ 9].
2. Add the Security gateway to the local network as shown in the following figure:



Both LAN port A and LAN port B will be used in this case.



a Outdoor unit
b LAN connection (DIII)
c iTM or LC8 controller
d LAN connection to port A
e Security gateway
f iTM or LC8 controller to port B
g LAN gateway (RJ-45)
h Daikin Cloud Service

3. Plug in the power supply.

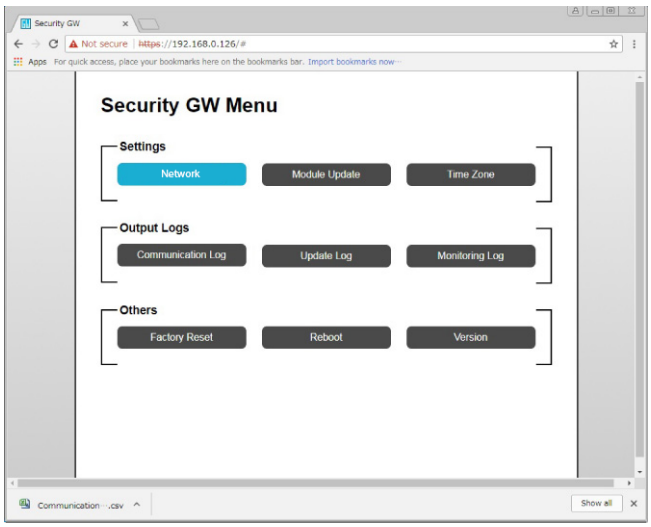
9.2 To access the Security gateway

See "To access the Security gateway" [▸ 15].

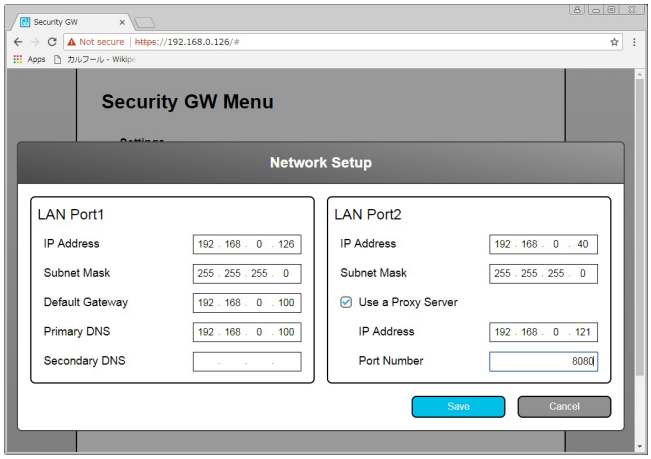
9.3 To set up the network of the Security gateway

To access the Security GW Menu (Security GW Menu), see "To access the Security gateway" [▸ 15].

1. Click the Network (Network) button.



Result: The Network Setup (Network Setup) dialog appears.



2 Fill out the following network data:

LAN Port1 (LAN Port1) (=A)

- IP Address (IP address): Unique IP (default: 192.168.0.126) address in local network
- Subnet Mask (Subnet mask): 255.255.255.0
- Default Gateway (Default Gateway): IP address (default: 192.168.0.100) of local router
- Primary DNS (Primary DNS): IP address (default: 192.168.0.100) of local router
- Secondary DNS (Secondary DNS): leave blank

LAN Port2 (LAN Port2) (=B)

- IP Address (IP address): select different IP range address than for port A (e.g. 192.168.10.5)
- Subnet Mask (Subnet mask): 255.255.255.0
- Use a Proxy Server (Use a Proxy Server): Check
- IP Address (IP address): IP Proxy Server
- Port Number (Port Number): Port Proxy Server

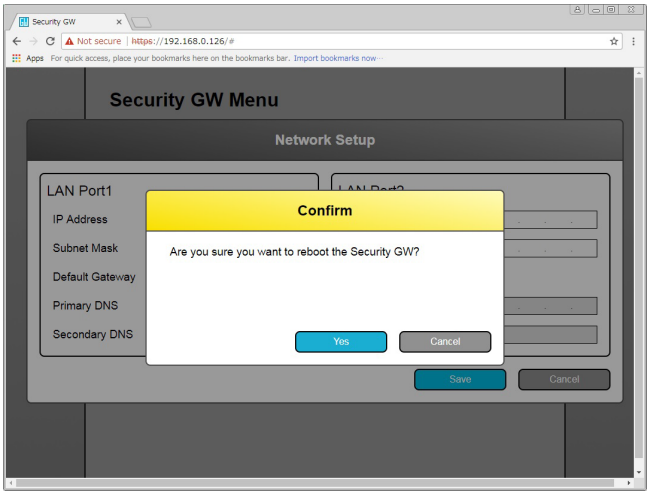
INFORMATION

If the IP address (IP address), default gateway (Default gateway) and primary DNS (Primary DNS) are according to the conditions of the local network, you do not need to change them.

3 Click the Save (Save) button.

Result: The confirm (Confirm) dialog appears.

4 Click the Yes (Yes) button to reboot the Security gateway.



Result: This will reboot the Security gateway.

Result: The web browser window appears.

Result: The IP address will be changed.

INFORMATION

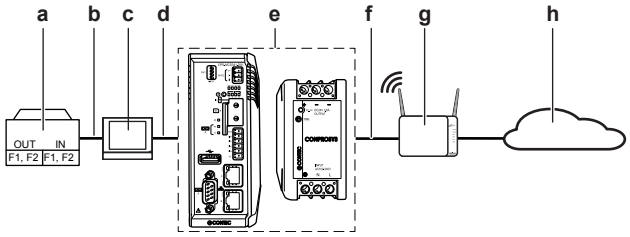
The web browser communication will be lost once step 4 is executed. Follow the procedure as described in "To access the Security gateway" [▸ 15] to reconnect by using the new IP address.

5 Reset the LAN network settings of your computer to their original values.

6 If you disabled it before, enable the WiFi adapter of your computer.

7 Disconnect the Ethernet cable between your computer and the Security gateway module.

8 Connect an Ethernet cable between the Security gateway module and the local network.



9.4 To set up the time zone of the Security gateway

See "To set up the time zone of the Security gateway" [▸ 20].

9.5 To commission the iTM or LC8 controller

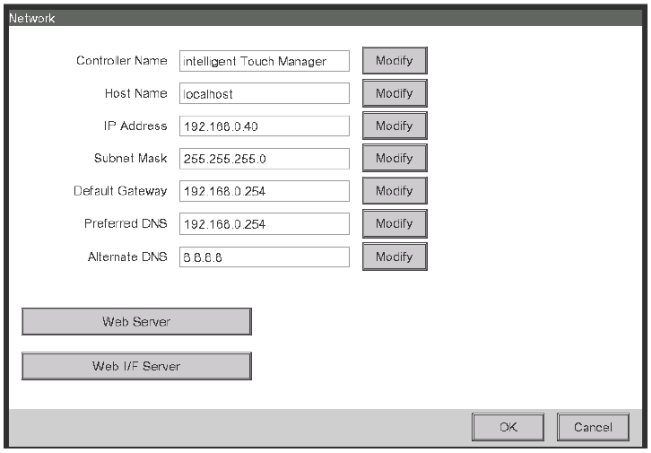
Refer to:

- Airnet handbook:
  - For commissioning of the iTM or LC8 controller
  - Format: Digital files on http://www.daikineurope.com/support-and-manuals/product-information/
- iTM installation manual
- LC8 installation manual

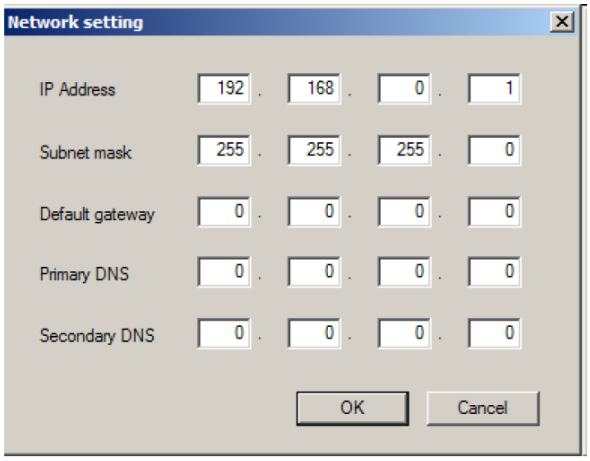
The next steps are a deviation of the Airnet Handbook, make sure the settings on the iTM or LC8 controller are as mentioned in step 1.

1 Setup the network of the local controller according to the table below.

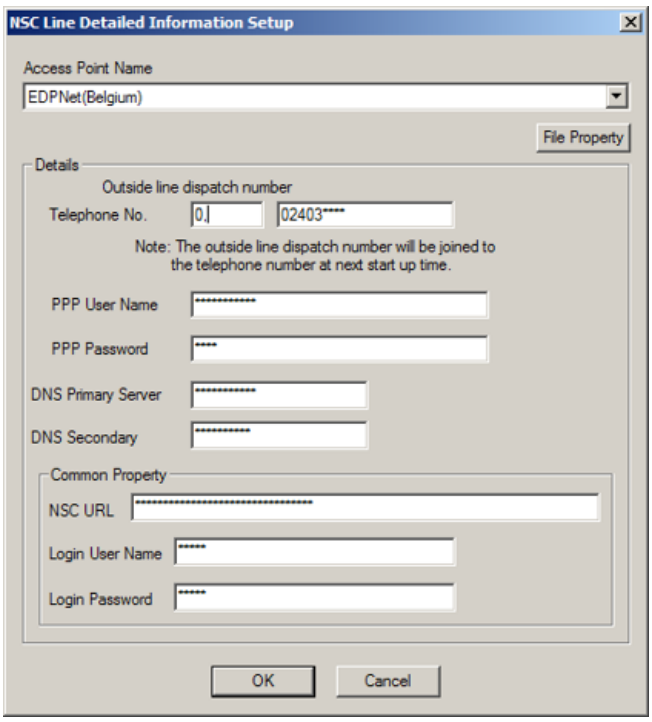
iTM



LC8

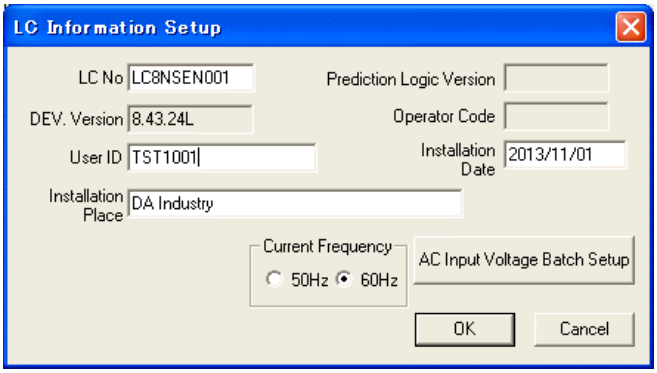


2 Set NSC URL http://Lcc.m2m.daikineurope.com/NSC and select the correct Access Point Name (Access Point Name) from the selection list. The details (Details) section can remain empty.



3 Connect with your Daikin Cloud Service credentials to https://cloud.daikineurope.com. and create a new site. As soon as the site is created, note down the iTM or LC8 number:

- iTM No: The registered id number of the intelligent Touch Manager. This number will be in the following format: LT2N###### (with # being an alphanumerical value).
- LC8 No: The registered id number of the LC8 Controller. This number will be in the following format: LC8N###### (with # being an alphanumerical value).



EAC

DAIKIN EUROPE N.V.

Zandvoordestraat 300, B-8400 Oostende, Belgium

4P529063-1A 2020.12