



## HARDWARE INSTALLATION GUIDE

# RA621EX OUTDOOR SERVICE POINT



Doc No.: PRDT-0046 | Version 2.0 | Date 2023-12-13

## TRADEMARKS



The Relay2 logo is a trademark of Relay2, Inc. of the US.

## COMPANY HEADQUARTERS

1525 McCarthy Boulevard, Suite 209  
Milpitas, CA 95035, USA

[www.relay2.com](http://www.relay2.com)

+1 (408) 380-0031

## PRODUCT OVERVIEW

The RA621EX is a cloud-managed Outdoor Service Point, offering Edge Computing and storage capabilities integrated with a high-performance wireless access point. It enables businesses to deliver superior venue experiences, enhance business operations, and create competitive advantages.

For more information about the RA621EX, please refer to [www.relay2.com](http://www.relay2.com).



## Opening the Package

- Please ensure that all ordered optional accessories are included in the separate accessory box.
- Please peel off the protective film before using the AP.
- Please do not use a different power adapter than the one included with the package.
- Please check the packaging list first. If there are any missing or broken parts, please contact the authorized distributor of Relay2, Inc.

## Safety

- Read the hardware installation guide carefully before installation and power-up.
- Power supply is IEEE 802.3at-compatible PoE+.
- Make sure the power input matches the voltage range of the power adapter.
- To avoid overheating, make sure the AP allows for proper heat dissipation, and leave enough room for air circulation.
- Do not directly touch the bottom of the AP to avoid scalding. When the AP is in operation, the surface temperature of the back plate will be very hot.
- Any unauthorized modification of the product structure and safety design is not allowed.
- Do not put anything on top of the AP. If the AP gets liquid in it, please disconnect the power supply, disconnect all network connections, and contact authorized distributor of Relay2, Inc.

## Before You Start

- Before installation, a signal detecting test can be used to determine the best installation position.
- Keep your body at least 20 cm away from the AP during installation and operation.
- Install the AP at least 1 m distance from any metal obstructions to avoid the radio signal being affected by metal shielding.
- To avoid radio interference, keep the device away from magnets or magnetic fields (e.g., do not place near a microwave, refrigerator, etc.).
- If there is a statement prohibiting the use of wireless devices in restricted places and explosive areas, please do not install this wireless AP.

## Warranty

- Please provide the device model, MAC address, and serial number shown on the tag of the side panel.
- The warranty does not cover any product that has been opened without authorization from Relay2 Inc.
- Reasonable repair and shipping costs will be charged for product faults or damage caused by using non-Relay2 accessories or improper operation.



# PACKAGE CONTENT - RA621EX

---

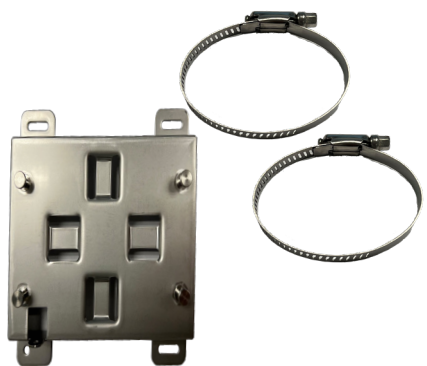


Access Point



2.4 GHz Detachable Antenna

5 GHz Detachable Antenna



Pole/Wall Mount Kit



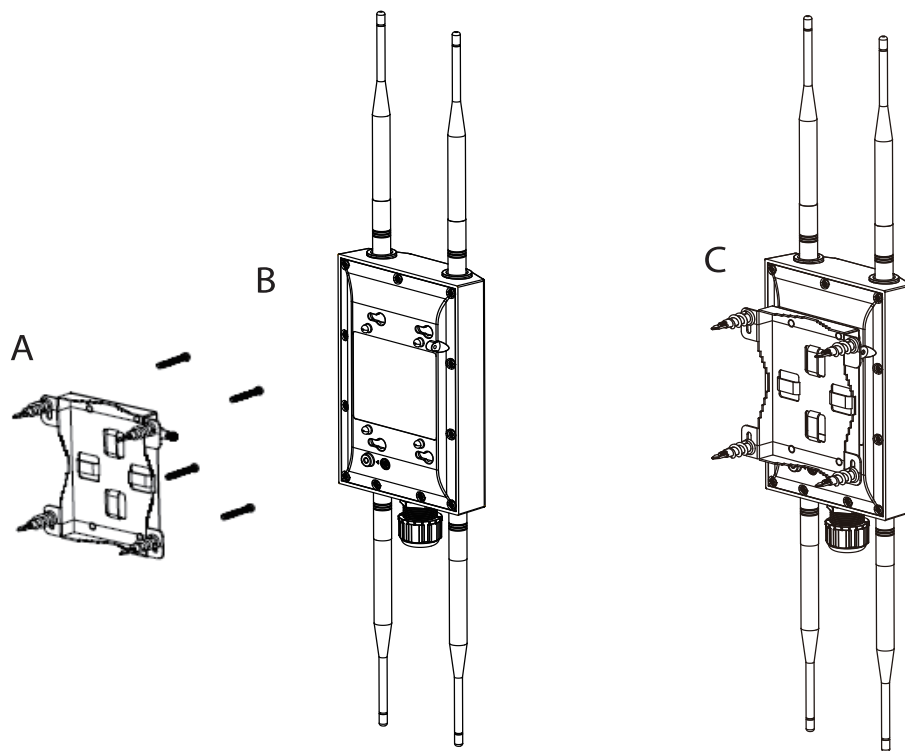
Ground Cable  
and screw



Screws

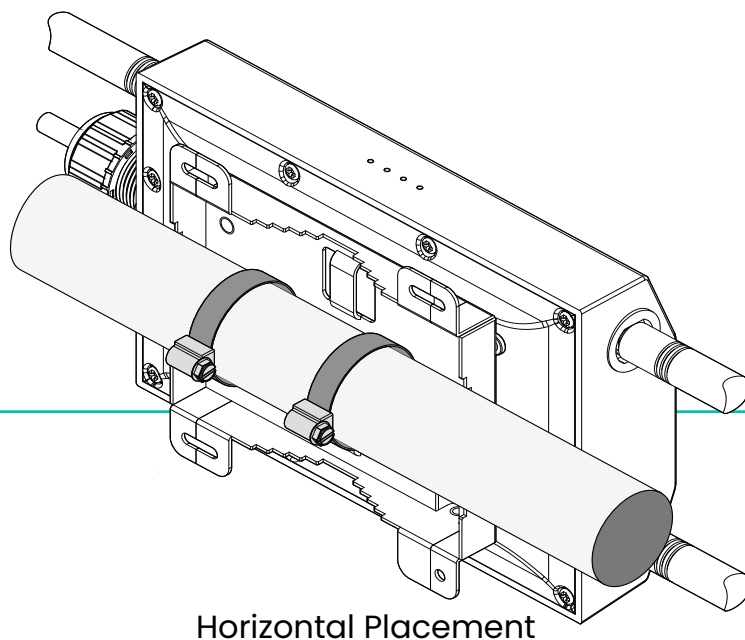
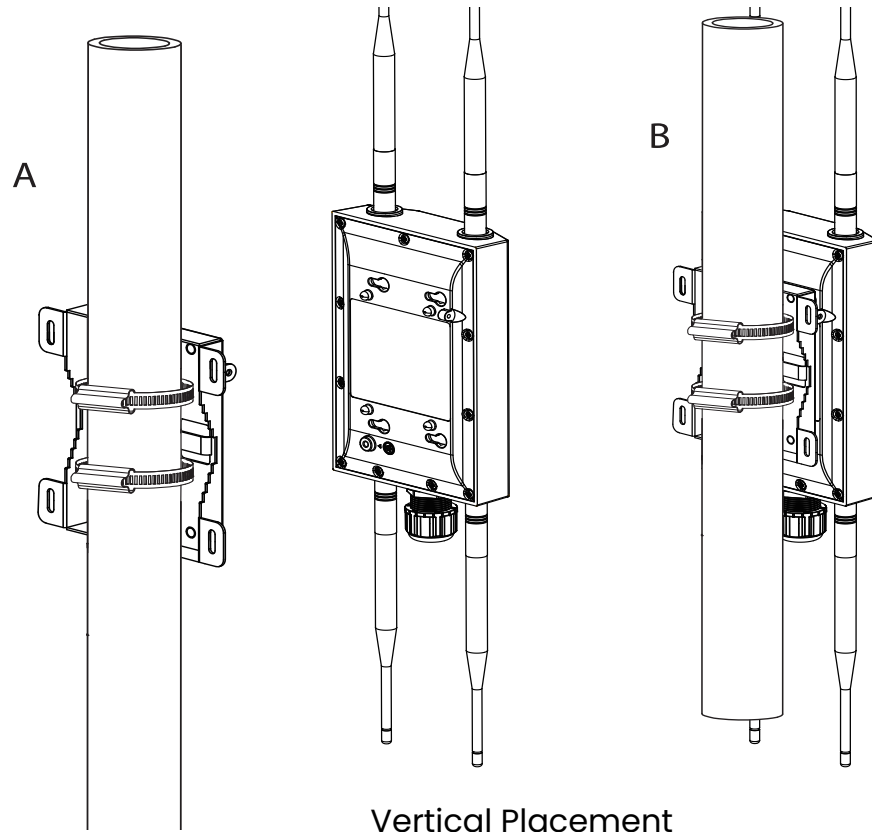
## Wall Mount the AP

- A. There are two types of anchors and screws set. One is for drywall and the other is for concrete.  
Determine where the AP is to be placed and mark the location on the surface for the four mounting holes. You may adjust the position with a level.  
Use the appropriate drill bit to drill four 8 mm diameters and 25 mm depth holes in the markings and hammer the bolts into the openings. (concrete wall case)
- B. Fasten mounting base with the screws.
- C. Slide the AP into the wall mounting plate.



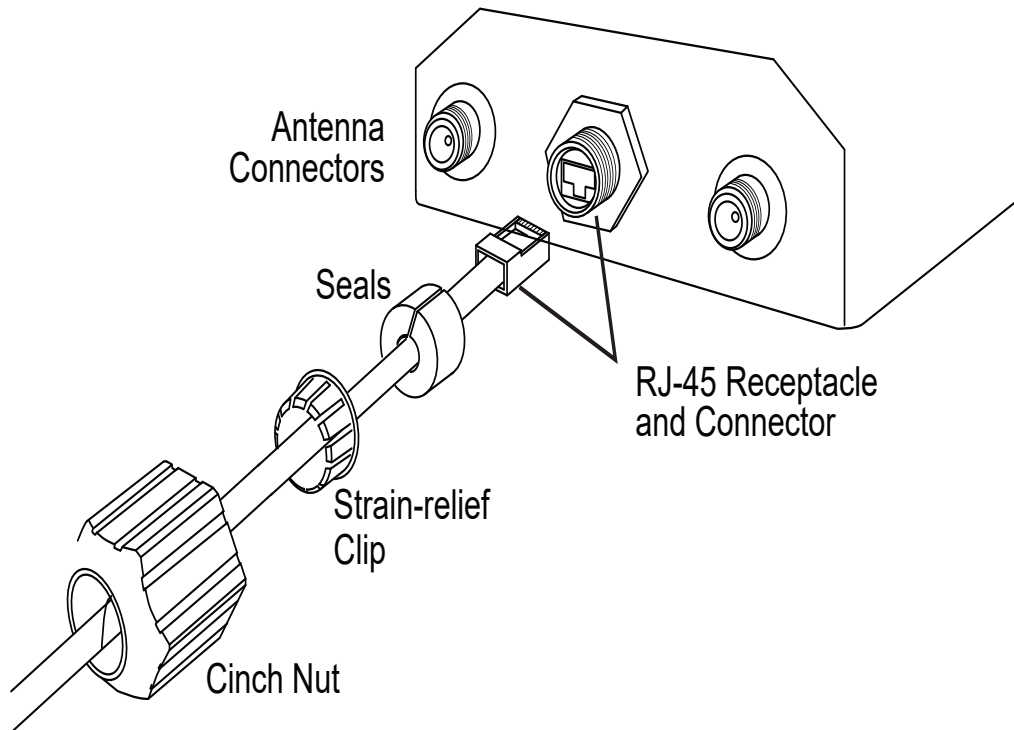
## Pole Mount the AP

- A. Determine where the AP is Placed. Then, set the mounting plate with provided band. Note that the provided band is able to apply from 40 mm to 63 mm diameters of the pole.
- B. Slide the AP to the mounting kit.



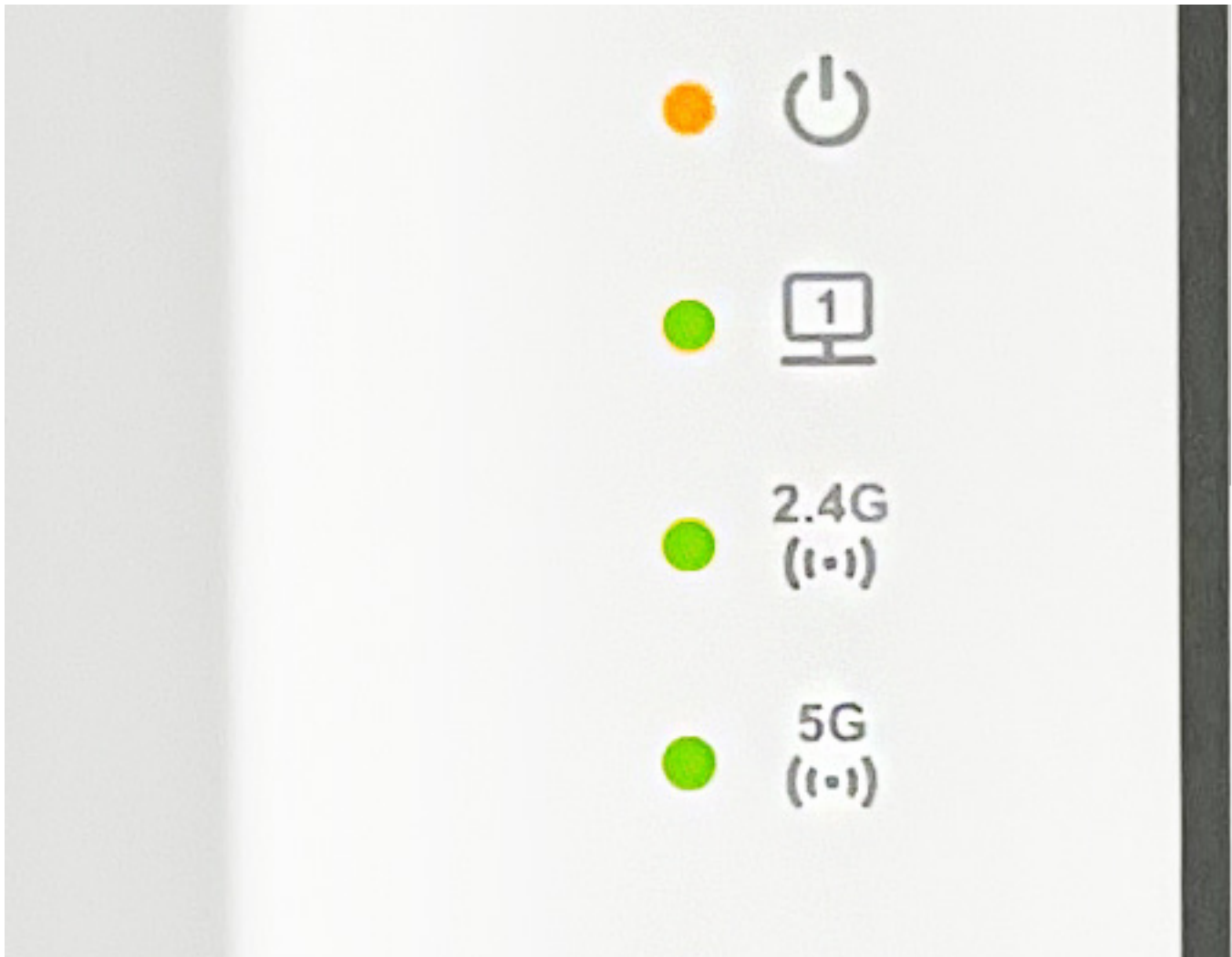
## LAN Cable Connection

- A. Use LAN cable for outdoor deployment.  
Thread cinch nut and strain-relief clip to the cable, and put the rubber seals to the cable.  
Then, connect the LAN cable to the AP. Make sure the cinch nut is set to the connector properly, and is tightened correctly.



## LED

- There are 4 status LEDs at a side face of the AP.
  - Power Status
  - Ethernet Link Status
  - 2.4GHz Radio Status
  - 5GHz Radio Status



LEDs







# VERIFY RA621EX FUNCTIONALITY

First, check if the power LED is solid orange. During the first boot, it is highly likely that the AP is automatically updating its firmware, indicated by green fast blinking the Ethernet LED. The Eth LED should turn solid green after the upgrade process has finished (normally within a few minutes). See LED indicator table below for more details.

Verify access point connectivity—use any 802.11 client device to connect to the RA621 AP and verify network connectivity using the client device web browser by going to a well-known web page.

Check network coverage and confirm good signal strength in the desired coverage area.

States	AP Status LED Display			
		2.4G 	5G 	
State 1: Power on (until kernel up)	Orange solid	Off	Off	Off then green solid
State 2: R2OS starting	Orange solid	Green solid	Green solid	Green solid
State 3: R2OS initializing	Orange solid	Green slow blinking	Green slow blinking	Green slow blinking
State 4: Radio up and ready	Orange solid	Green solid	Green solid	Green slow blinking
State 5: SCM connecting	Orange solid	Green solid	Green solid	Green fast blinking
State 6: CWCL connecting	Orange solid	Green solid	Green solid	Green fast blinking
State 7: AP up and running	Orange solid	n/a	n/a	Green solid
State 8: Image upgrade	Orange solid	n/a	n/a	Green fast blinking
State 9: AP connected	Orange solid	n/a	n/a	Green solid

*Table 1 RA621EX LED booting states*

## FCC Disclaimer

### § 15.19 Labeling Requirements

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### § 15.21 Information to User

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### § 15.105 Information to the User

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, resolve the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Operations in the 5.15–5.35 GHz band are restricted to indoor usage only.

## CE Disclaimer



- **Manufacturer:** Emplus Technologies, Inc.
- **Address:** 10F., Building B, No. 209, Sec. 1, Nangang Rd., Nangang Dist., Taipei City 11568, Taiwan
- **Product Name:** Smart Access Point
- **Trademark:** Relay2
- **Model Number:** RA621EX
- This device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. All essential radio test suites have been carried out.

Function	Operation Frequency	Max RF Output Power	Limit
Wi-Fi 2.4 G	2412–2472 MHz	19.93 dBm	≤20 dBm
Wi-Fi 5.8 G	5745–5825 MHz	13.98 dBm	≤23 dBm



BE	BG	CZ	DK	DE	EE	IE	EL
ES	FR	HR	IT	CY	LV	LT	LU
HU	MT	NL	AT	PL	PT	RO	SI
SK	FI	SE	NO	IS	LI	CH	TR

## EU Declaration of Conformity

- We, Relay2, Inc. (1525 McCarthy Blvd., Suite 209, Milpitas, CA 95035, USA) hereby declares that this Smart Access Point is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
- According to Article 10(2) of Directive 2014/53/EU, RA621 can be used in Europe without restriction.

# (APPENDIX A) DEVICE MANAGER USER INTERFACE

---

## Introduction

The Relay2 Access Point (AP) starts functioning without preconfiguration under typical network condition. The AP is able to connect to the Relay2 NMS when the following prerequisites are met:

- The DHCP server is reachable, and the AP can get an IP address.
- The AP is able to reach the DNS server.
- The AP is able to send https packets to the internet directly.\*
- Uplink packet, MTU = 1500, from the AP is accepted by the network.
- The L2 packet is accepted by the network without VLAN tagging.

In case any item in the list above is not supported—which is a special environment for Relay2 AP and requires manual preconfiguration—this document shows the procedure of such manual configuration through the Relay2 Device Manager UI.

The procedure in this document shows the example of the minimal environment in which the AP is only connected to a PC.

\*No proxy between AP and NMS

## Preparation

This section shows the preparation for the manual configuration.

### Hardware

The required hardware for the configuration is listed below:

- Relay2 AP to configure
- AC adapter or POE+ connection
- PC (web browser used for the configuration)
- LAN cable (with RJ45 connectors)
- Ethernet hub (in case it is necessary to connect the AP and PC via the hub)

## Additional Information Needed

The information listed below is used during the preconfiguration process:

- MAC address and serial number of the target AP (You can find them on the label at the bottom of the AP.)
- IP address for the target AP in case configuring AP is executed under a network with a DHCP server

## IP Address of the AP

The IP address of the target AP is used to access DM GUI even at stand-alone.

## Link-Local IP Address of RA621EX

The link-local IP address of the Relay2 AP, 169.254.0.0 network, is calculated from the right four digits of the AP MAC address. For example, if the MAC address is B4:82:C5:00:6B:E6, then the link-local IP address of that AP is 169.254.107.230. (i.e., hex: 6B => dec: 107 and hex: E6 => dec: 230).

## IP Address for the PC

The Ethernet port of the AP shall be in the same VLAN for the AP.

In case the PC is connected with the AP directly, the AP assigns the link-local IP address to itself. Thus, the IP address of the PC shall be the same network.

A normal PC assigns its own IP address in the 169.254 network and in the same manner as the AP.

## Connecting the AP with the PC

**DM GUI Step 1:** Connect between the AP LAN port and the PC with a LAN cable. Then power up by connecting the DC power unit to the power connectors.

Confirm that the Ethernet link is active with the LED at the LAN port or the LED on the AP.

- In the case that the AP and PC are connected directly for RA621EX, both nodes utilize the link-local IP address with the 169.254.0.0 network.



## Accessing the DM GUI

**DM GUI Step 2:** Access to <https://<AP IP address>:9999> with any browser application on the PC.

E.g., in the case that the AP IP address is 169.254.107.230, then <https://169.254.107.230:9999>.

**Note:** Relay2 AP is not registered for CA certification, so a warning message for a privacy error could be seen upon the first DM GUI access, like below. Please continue the access.

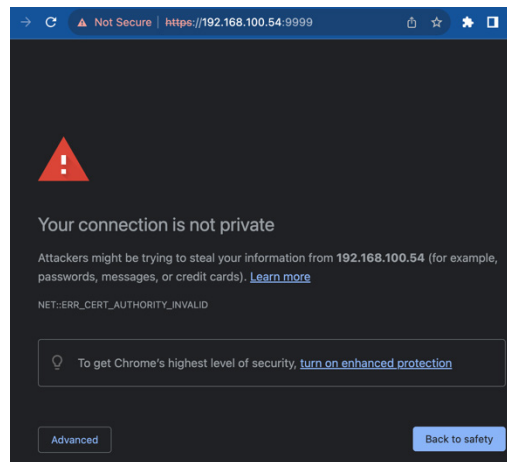


Figure 1: Example of privacy error (Microsoft edge)

**DM GUI Step 3:** In the case of MS Edge, continue by clicking “advanced.”

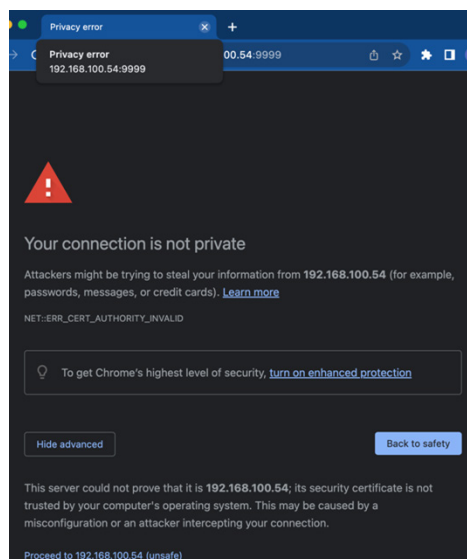


Figure 2: Advanced window at privacy error (edge)  
(Proceed to 192.168.100.54 (unsafe)  
at the bottom line)

**DM GUI Step 4:** Click “Proceed to <IP address> unsafe” for the DM GUI page to be shown.

(Refer to Figure 3 below)



The image shows the DM GUI login window. At the top is the Relay2 logo. Below it is the title "AP Device Management (b482c5006be6)". There are two input fields: "Username" and "Password". Below these fields is a "Login" button. At the bottom, there is a copyright notice: "© 2011-2021 Relay2, Inc."

Figure 3: DM GUI login window

## DM GUI Login

Fill in the username and password, then click “Login.” At default,

**Username:** AP mac address without colons (“:”)

**Password:** AP S/N with capital letters

E.g., MAC address = B4:82:C5:00:7D:DB, S/N = EMP6610100C00617

Username:      b482c5007ddb

Password:      EMP6610100C00617

If login is successful, the initial page, as below, is shown.



The image shows the DM GUI initial page. At the top is the Relay2 logo. Below it is the title "AP Device Management (b482c5006be6)". There are two tabs: "Device" and "User". Below the tabs is a table with three rows: "Commands", "Configurations", and "Diagnostics". Each row has a "+" button on the right.

Figure 4: DM GUI initial page

## Error Case

In case the PC and AP are in different segments, the browser will display a time-out error.

- Please double-check the AP IP address and that there is no typo in the browser input.
- Please check that the PC IP address and AP IP address are in the same VLAN.
- Please check that there is no IP address conflict in the network.

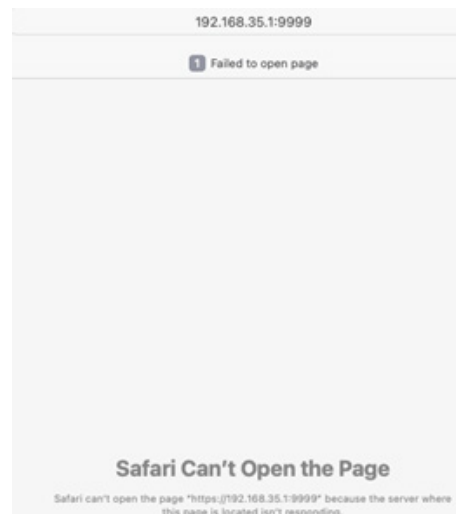


Figure 5: Sample of error case (Safari)

## DM GUI Device Operation

DM GUI provides commands, configurations, and diagnosis.

### Commands

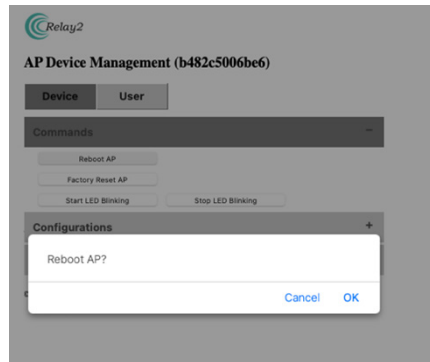
By clicking the “+” mark to right of the Commands tab, the list of available commands opens.



Figure 6: Commands

## Reboot AP

By clicking “Reboot AP” and “OK” on the confirmation pop-up window, the AP is rebooted.



**Note:** A confirmation pop-up window will appear for all “command” actions. Designated action is triggered by clicking “OK.”

Figure 7: Confirmation pop-up window for reboot action

## Factory Reset AP

Factory reset is initiated by clicking “Factory Reset AP” followed by “OK” on the confirmation window.

Note that the AP configuration, including AP logs, will be cleared by a factory reset.

## Start LED Blinking

By clicking “Start LED Blinking” followed by “OK” on the confirmation window, the three LEDs below will start blinking. This feature can be used to identify deployed APs easily at the site.

Note that LEDs do not show the AP status when this command is active.



## LEDs

### Stop LED Blinking

This is to stop the “blinking” triggered in the previous section and set the LEDs back to normal.

### Configurations

All configurable parameters via DM GUI are shown by clicking the “+” mark to the right of Configuration.

Input designated values in “New Config” while “Current Config” shows the setting in the AP.

After the input is completed, click “Apply and Reboot AP.” Then click “OK” in the confirmation pop-up. A new configuration will be valid once the reboot is completed.

You can leave the parameters empty in case you want to keep the current values.

	Current Config	New Config
<b>LAN Network</b>		
Protocol	dhcp	dhcp
Address	-	
Netmask	-	
Gateway	-	
DNS Server	-	
VLAN	-	
MTU	0	0
<b>HTTP Proxy</b>		
Server Address	-	
Port	-	
Username	-	
Password	-	
<b>Cellular</b>		
PIN		
APN	lte-d.ocn.ne.jp	lte-d.ocn.ne.jp
Auth	chap	chap
Username	mobileid@ocn	mobileid@ocn
Password	mobile	mobile
Modes		
<b>Local NTP Server</b>		
Server Address	-	
Port	-	
<b>Version</b>		
R2OS	3.1.1-20220114_ra6xx	
Device Mgmt GUI	0-1.6	

Apply and Reboot AP Cancel

Figure 8: AP configuration



## LAN Network

These are the AP LAN-related configuration parameters for the target network:

Protocol	IP address allocation for that AP (DHCP or Static)
IP Address	(Valid for "Static" only) AP IP address
Netmask	(Valid for "Static" only) netmask of the network
Gateway	(Valid for "Static" only) Gateway address of the network
DNS Server	(Valid for "Static" only) DNS server address of the network
VLAN	VLAN ID for tag on AP management packet (if unnecessary, set "0")
MTU	Packet length of the network

## HTTP Proxy

These are the parameters of proxy in case the network requires it for communication with NMS:

Server	
Address	IP address of HTTP proxy server
Port	Port number of http packets toward the proxy server
Username	Username for authentication for the proxy server access if it is required
Password	Password for authentication for the proxy server access if it is required
Cellular	(not applicable for RA641)

## USIM Parameters for LTE Module in RA620M and LTE Dongle (NCXX-UX302NCR) for RA621 and RA620

PIN	PIN for USIM access if PIN is enabled (PIN is recommended for disabling the operation. There is a risk of locking the USIM by using the wrong PIN if the AP retries many times in the case of a failed authentication.)
APN	APN for USIM
Auth	Authentication mode of network access via USIM (both, chap or pap) (small letters only)
Username	Username for authentication of network access

Password	Password for authentication of network access
Modes	Target cellular mode LTE or "" (blank: WCDMA + LTE)
Local Subnets	Local subnet via LAN1 (With RA620M only, the Wi-Fi user is able to access the local network subnet connected with LAN1 port. This parameter defines that subnet.)

### Local NTP Server

In the case that access to the NTP server in the internet is blocked by a firewall, and in the case that the NTP server is located in an intranet, these parameters are configured to make the AP access to the server for calendar clock sync:

Server Address	NTP server address
Port	Port for NTP access

### Versions

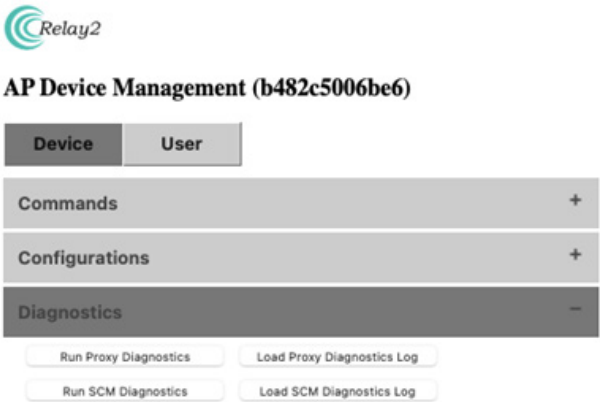
This is the information of the AP software image and DM GUI:

R2OS	AP software image version
Device Mtmt GUI	DM GUI version

### Diagnostics

Diagnostics help to identify the issue when the AP fails to reach NMS.

Available diagnostics options are shown by clicking the “+” mark to the right of Diagnostics.



**Note:** The results of diagnostics appear in a pop-up window. Please allow pop-ups on this site (IP address) before the execution.

Figure 9: Diagnostics

## Proxy Diagnostics

This is the test script to check proxy server access.

By clicking “Run Proxy Diagnostics,” the script is executed, and the messages are seen on a pop-up window.

## SCM Diagnostics

This is the test script to check SCM server access. The SCM server is one server in NMS and the first server when the AP starts communication with NMS.

By clicking “Run SCM Diagnostics,” the script is executed, and the messages are seen on a pop-up window.



Figure 10: Example of SCM diagnostics results

## Load Proxy Diagnostics Log, Load SCM Diagnostics Log

The log shows the latest test result.

By clicking “Load Proxy Diagnostics Log” or “Load SCM Diagnostics Log,” the latest results of “Proxy Diagnostics” or “SCM Diagnostics,” respectively, are shown on the pop-up window.

The pop-up window page supports “Re-run Diagnostics” and “Re-load Diagnostics” for re-execution.

# User

DM GUI supports adding user access and changing user passwords.

## Changing Default User Password

By clicking the “User” tab on the DM GUI initial page (refer to Figure 8: DM GUI Initial Page), the page for password change will open. Input the new password twice (Password and Confirm Password) and click “Apply,” followed by “OK” at the confirmation window, and the password is changed.



Figure 11: User Management

## Adding Administrators

By clicking “Add New Users,” a window for new-user registration pops up.

Input the username and password (twice), then click “Apply.”

By clicking “-” on the right, the defined user is deleted.

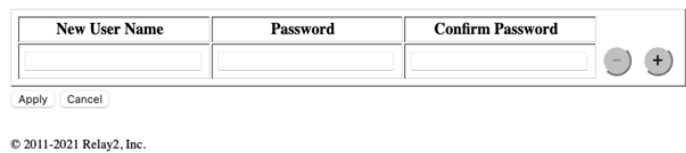


Figure 12: User Management (Add New User)