



WL-AP

Protege Wireless Access Point

Installation Manual



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2025. All rights reserved.

Last Published: 06-May-25 12:00 PM

Contents

Introduction	4
Product Diagram	4
Installation Requirements	4
Wiring Options	6
Planning the Installation	8
Installation Examples	9
Connections and Power Supply	11
Ethernet Connection	11
RS-485 Connection	12
Mounting	14
Tamper Sensor	17
Technical Specifications	18
FCC Compliance Statements	20
Industry Canada Statement	21
Disclaimer and Warranty	22

Introduction

The Protege Wireless Access Point connects Protege wireless locks to the Protege GX system, combining live online access control with the convenience of wireless door installation. Each access point saves you time and money that would otherwise be spent running cables for traditional wired card readers and locks.

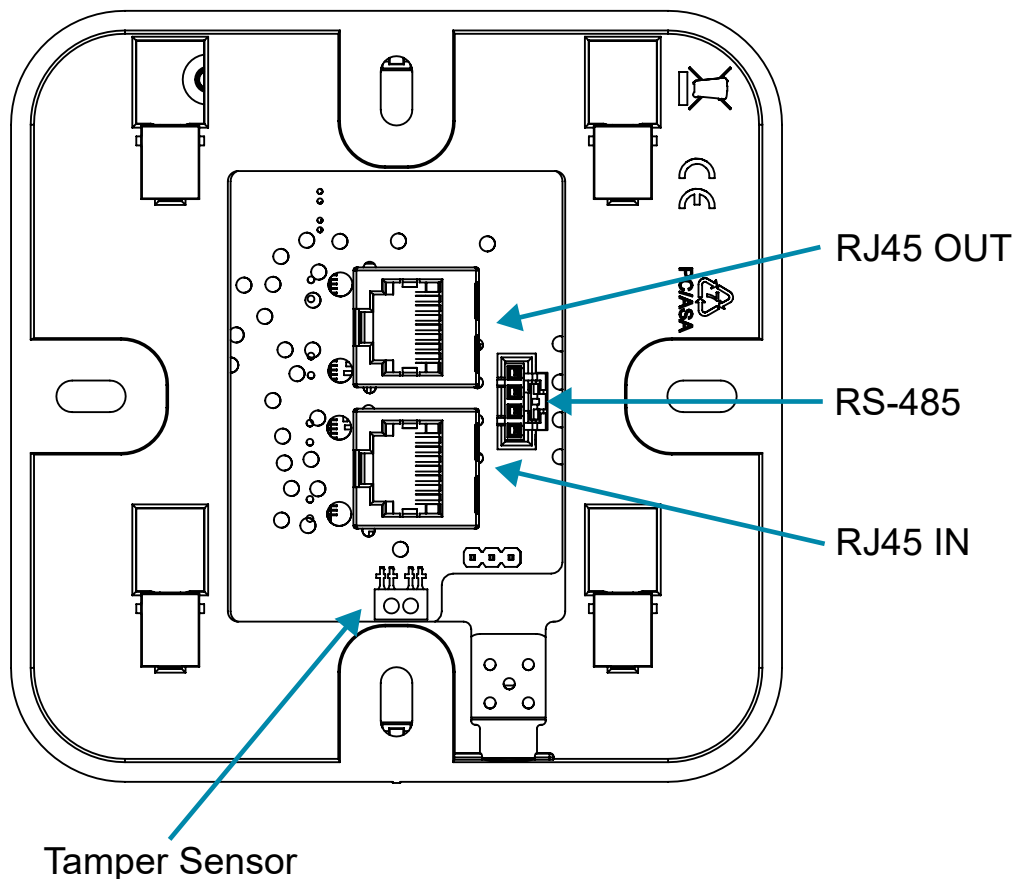
The access point's features include:

- Option of ethernet (with Power over Ethernet) or 12V RS-485 wiring
- Each access point connects to up to eight locks via Bluetooth® Wireless Technology, allowing one controller to support 128 online wireless locks
- Daisy chain up to six access points on one ethernet cable run
- Configure access points and locks using the convenient Protege Config App

This document provides instructions for physical installation of the Protege Wireless Access Point.

Product Diagram

This diagram shows the access point's connectors and sensors to assist you with installation.



Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- The National Electrical Code, ANSI/NFPA 70

- The Canadian Electrical Code, Part I, CSA C22.1
- The Local Authority Having Jurisdiction (AHJ)

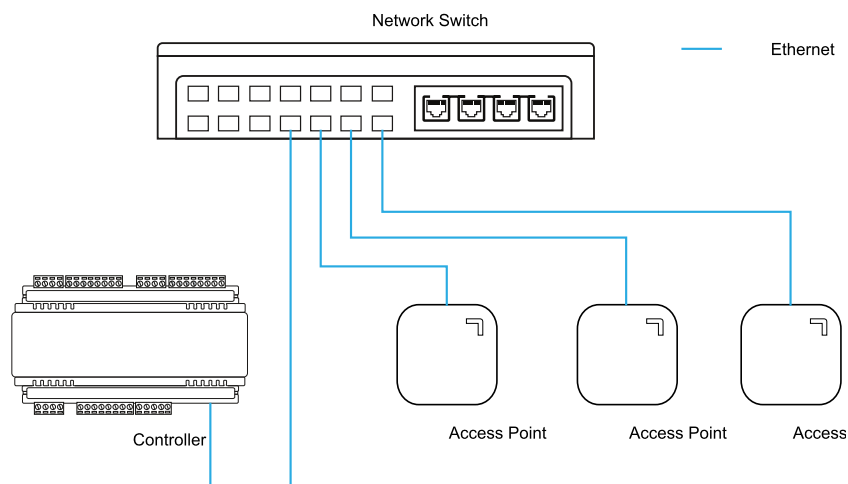
Wiring Options

There are three methods for wiring access points.

Ethernet (Point-to-Point)

Each access point is connected directly to a network switch by ethernet (Cat6 or better). The switch routes communications to the controller so the access points can come online as part of the module network. Power over ethernet (PoE) is provided by the switch or a PoE injector.

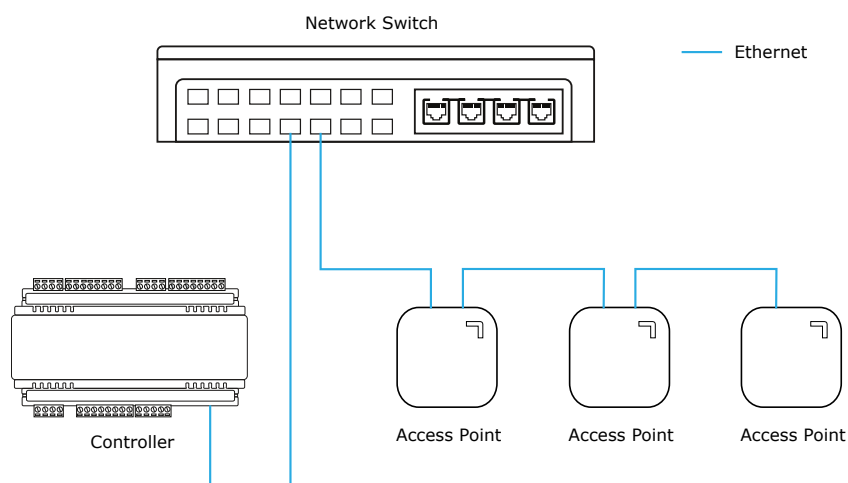
This method provides the greatest reliability. Each access point is independent, so one lost connection does not affect any other access points.



Ethernet (Daisy Chain):

Up to six access points are connected together in a daisy chain. The first access point in the chain receives PoE from the network switch or injector, then injects power to the next access point in the chain, and so on. Each access point communicates as if it were connected directly to the switch, with no additional networking required.

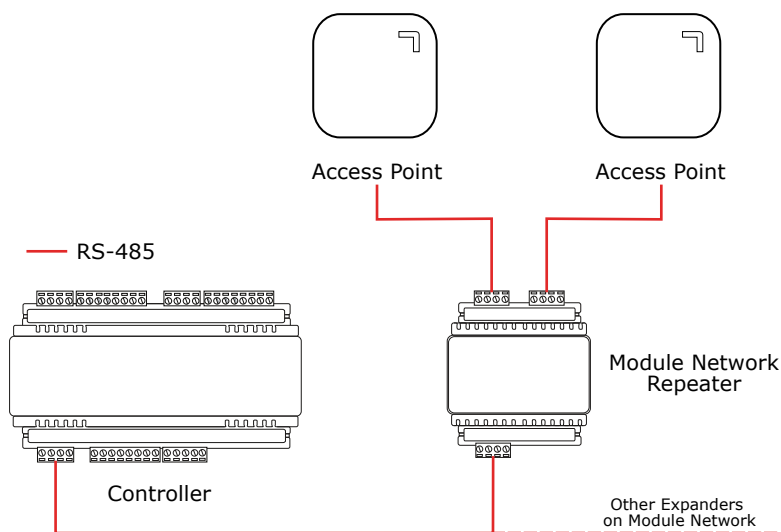
This method provides the greatest flexibility for deploying several access points along corridors. However, if one access point shuts down or the connection is broken, all modules further down the daisy chain will be lost.



RS-485 (Point-to-Point)

Access points can be connected to the controller via the RS-485 module network, with 12V power provided by the Protege power supply.

Access points cannot be daisy chained on the module network, so in most cases it will be necessary to use a Protege Module Network Repeater (PRT-MNR2-DIN) to provide additional spurs.



Planning the Installation

Access points must be positioned on the ceiling of rooms or corridors where online wireless locks have been installed. They are not rated for outdoor installation, so must be installed inside the building.

Before you begin running cabling and mounting access points, we recommend that you plan their positioning carefully to ensure that there is a strong Bluetooth® connection to every lock.

Controller	
Access Points per Controller	16
Locks per Controller	128
Access Points (Ethernet)	
Maximum Cable Run	200m (660ft)
Maximum Cable Run between Adjacent Modules	100m (330ft)
Access Points per Daisy Chain	6
Access Points (RS-485)	
Maximum Cable Run (RS-485)	900m (3000ft)
Access Points per PRT-MNR2-DIN	2
Wireless Locks	
Locks per Access Point	8
Maximum Bluetooth® Connection Range	25m

The Bluetooth® connection range is influenced by a variety of environmental and installation factors, so it might not be possible to achieve the maximum range in all circumstances. For example, consider the following factors:

- Locks with line-of-sight to the access point will have the most reliable Bluetooth® connection.
- If there are multiple access points with overlapping Bluetooth® ranges, ensure that you pair each lock to the access point with the strongest connection.
- A metal door or wall between the access point and the lock can have a large impact on the Bluetooth® signal. Wooden doors have a smaller effect.
- Other sources of 2.4GHz signals, such as WiFi or Bluetooth® transmitters, can interfere with the access point's signal.
- Equipment rooms, server rooms or other spaces with large amounts of electronic activity may generate interference that could affect the reliability of the Bluetooth® connection.

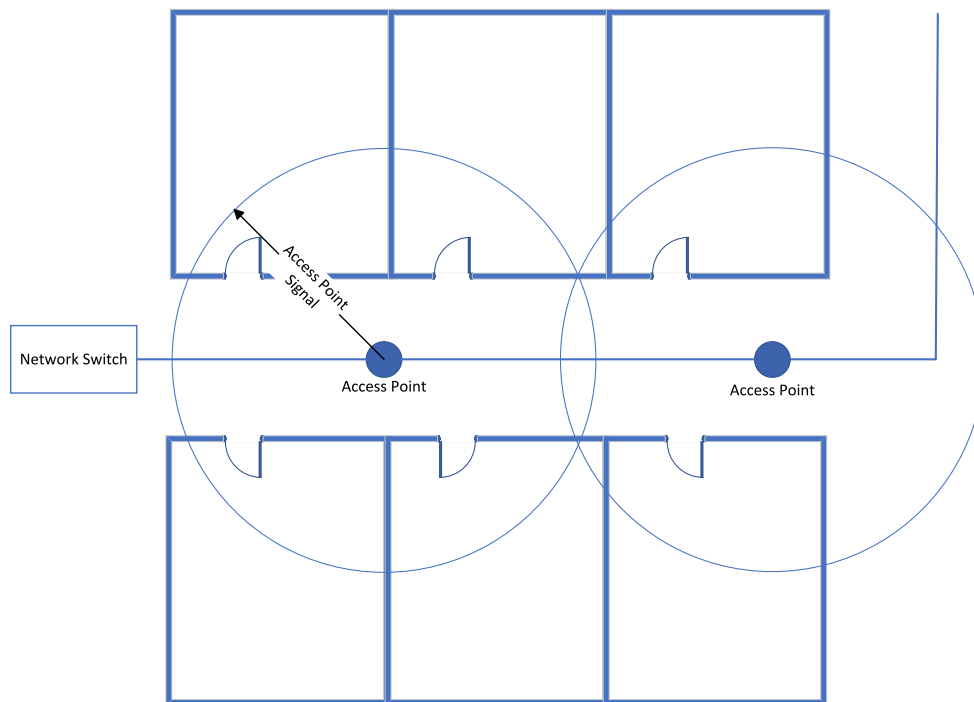
To comply with FCC and ISED Canada radiation exposure limits, the access point must be installed at a minimum distance of 20cm from all people during normal operation.

Installation Examples

Corridor

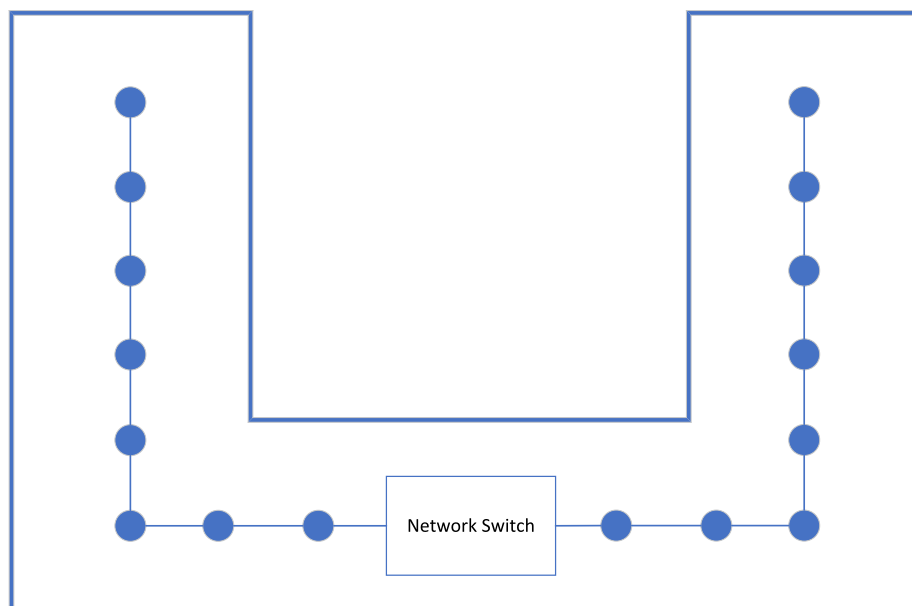
In an apartment building with long corridors, install access points down the center of the corridor, ensuring that every lock has an access point within Bluetooth® range. For point-to-point connections, run one cable per access point. Alternatively, you can connect up to six access points in a daisy chain.

It is recommended that you initially plan to connect up to five access points in each daisy chain. If you later discover that some locks do not have a good Bluetooth® connection, you can easily add another access point to the chain without running another cable all the way from the switch.



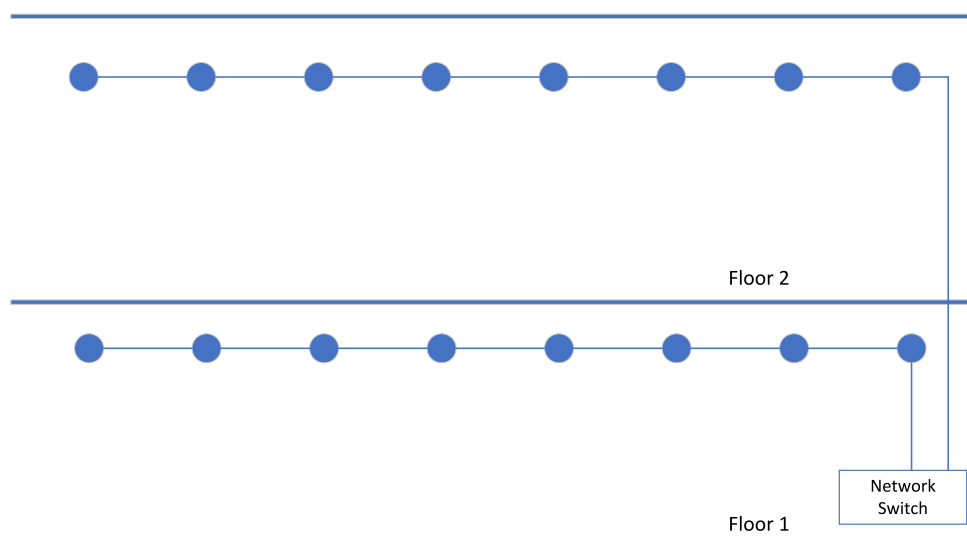
U-Shaped Building

In a U-shaped apartment building, you can install one daisy chain in each arm of the U. For point-to-point connections, run one ethernet cable per access point.



Multistory Installation

The network switch may be installed on one floor of a multistory building, with daisy chains or point-to-point connections running to adjacent floors.



Connections and Power Supply

Ethernet Connection

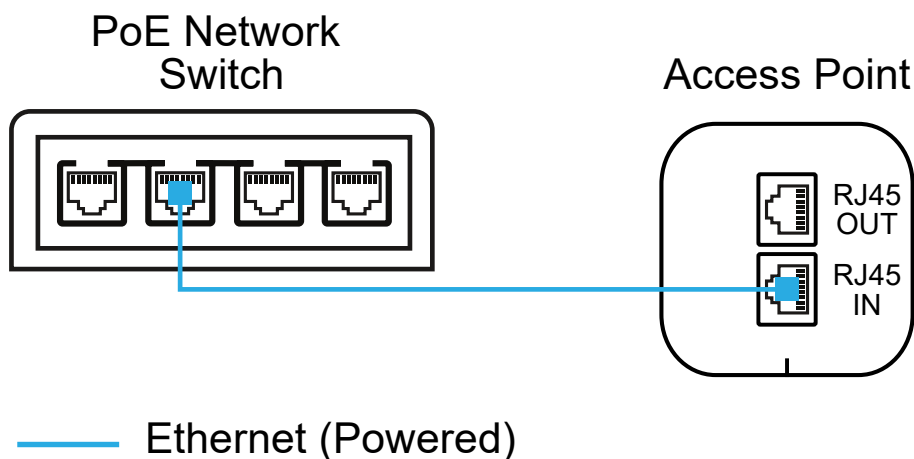
With the ethernet wiring method, the access point is connected to the building's local area network via a network switch. Power is provided by the switch or a PoE injector (see the [Technical Specifications](#) for supported protocols).

When access points are connected in a daisy chain, each module injects power to the next module in the chain. The output voltage is equal to the input voltage. Ensure that there is sufficient current to supply the operating power of each access point: 1.44W (Typical).

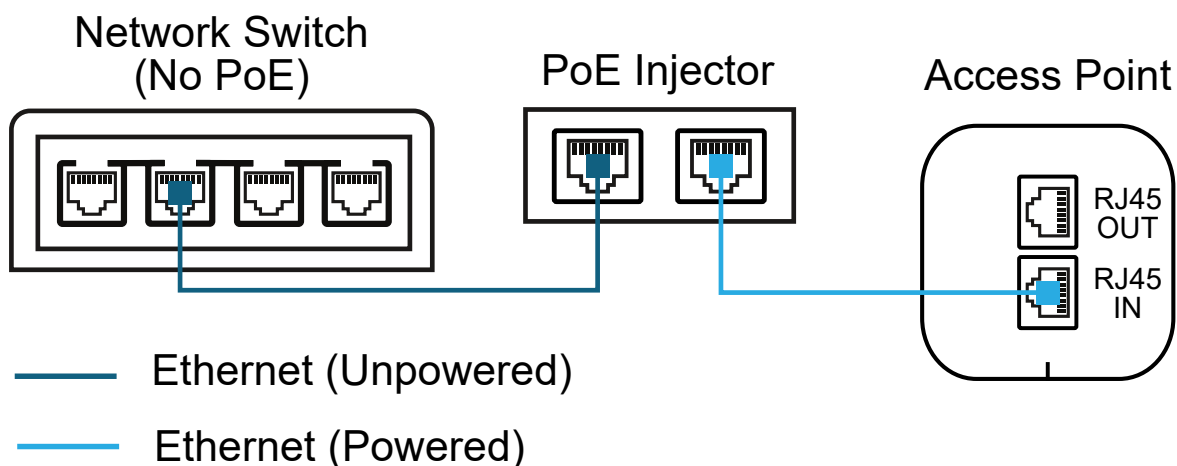
The recommended ethernet wiring specifications are:

- Cat6 or better ethernet cables
- The maximum length of cable between adjacent modules is 100m (330ft)
- The maximum total length of cable is 200m (660ft)

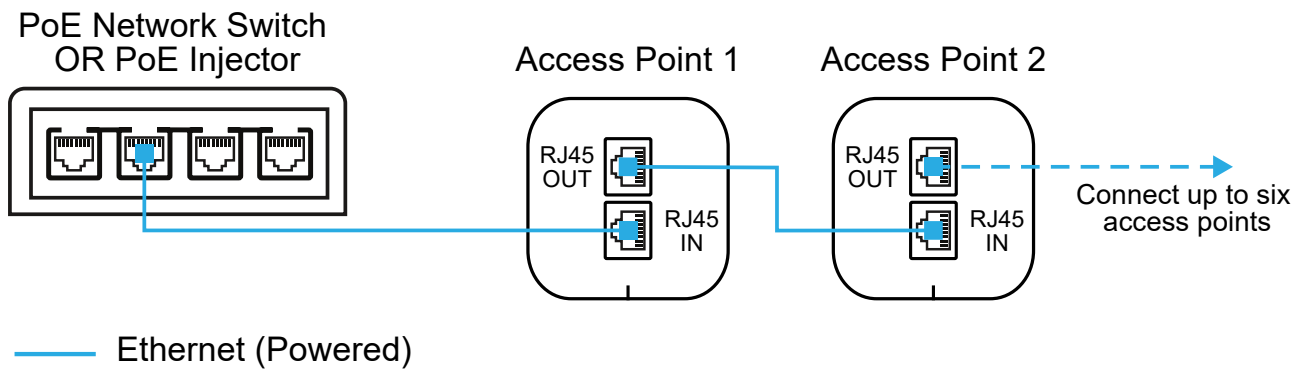
To connect the access point to a PoE network switch, run an ethernet cable from the switch to RJ45 IN:



To connect the access point to a network switch that does not provide power, use a PoE injector:



To daisy chain the access points, run a new segment from RJ45 OUT of the first access point to RJ45 IN of the next access point:



Do not connect more than six access points in a single daisy chain.

RS-485 Connection

With the RS-485 wiring method, the access point is connected to the controller via the RS-485 module network. Daisy chain is not supported for access points using RS-485.

The number of access points can be expanded with the use of a Protege Module Network Repeater (PRT-MNR2-DIN). Each module network repeater provides two spurs, each of which supports one access point.

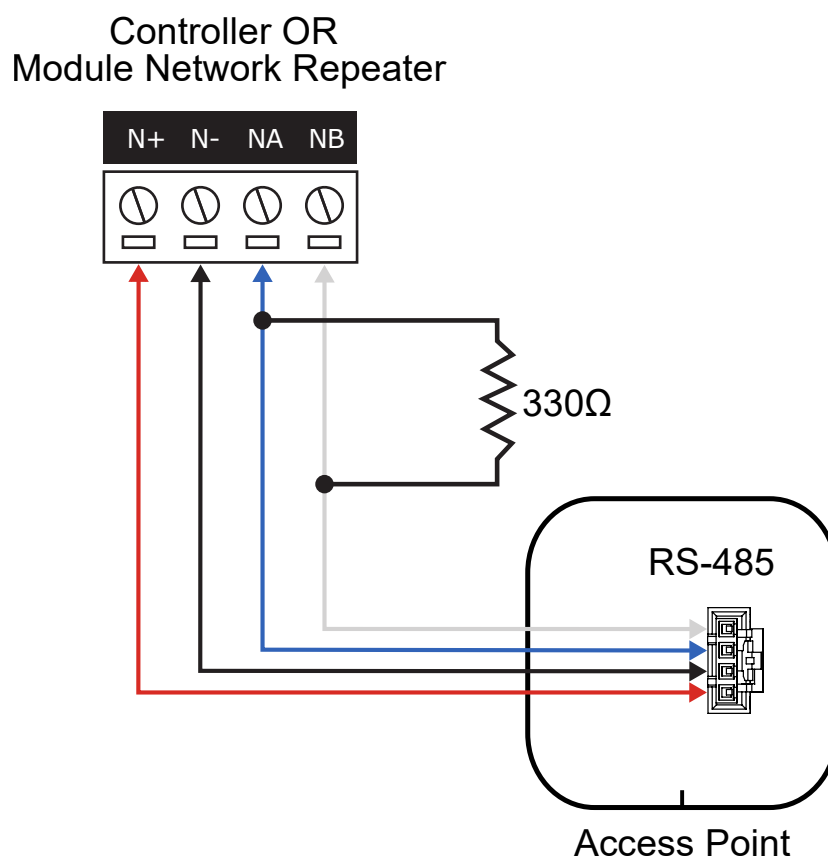
Power is supplied at 12V by a Protege power supply. Ensure that the operating power requirements are met: 1.44W (Typical).

The recommended module network wiring specifications are:

- Minimum 24AWG (0.51mm) shielded twisted pair with characteristic impedance of 120 ohm
- Maximum total length of cable is 900m (3000ft)
- CAT5e / CAT6 are also supported for data transmission when using ground in the same cable (to a maximum length of 100m (328ft))

Warning: Unused wires in the cable must not be used to carry power to other devices.

To connect the access point to a controller or module network repeater, use the RS-485 wiring shown below:

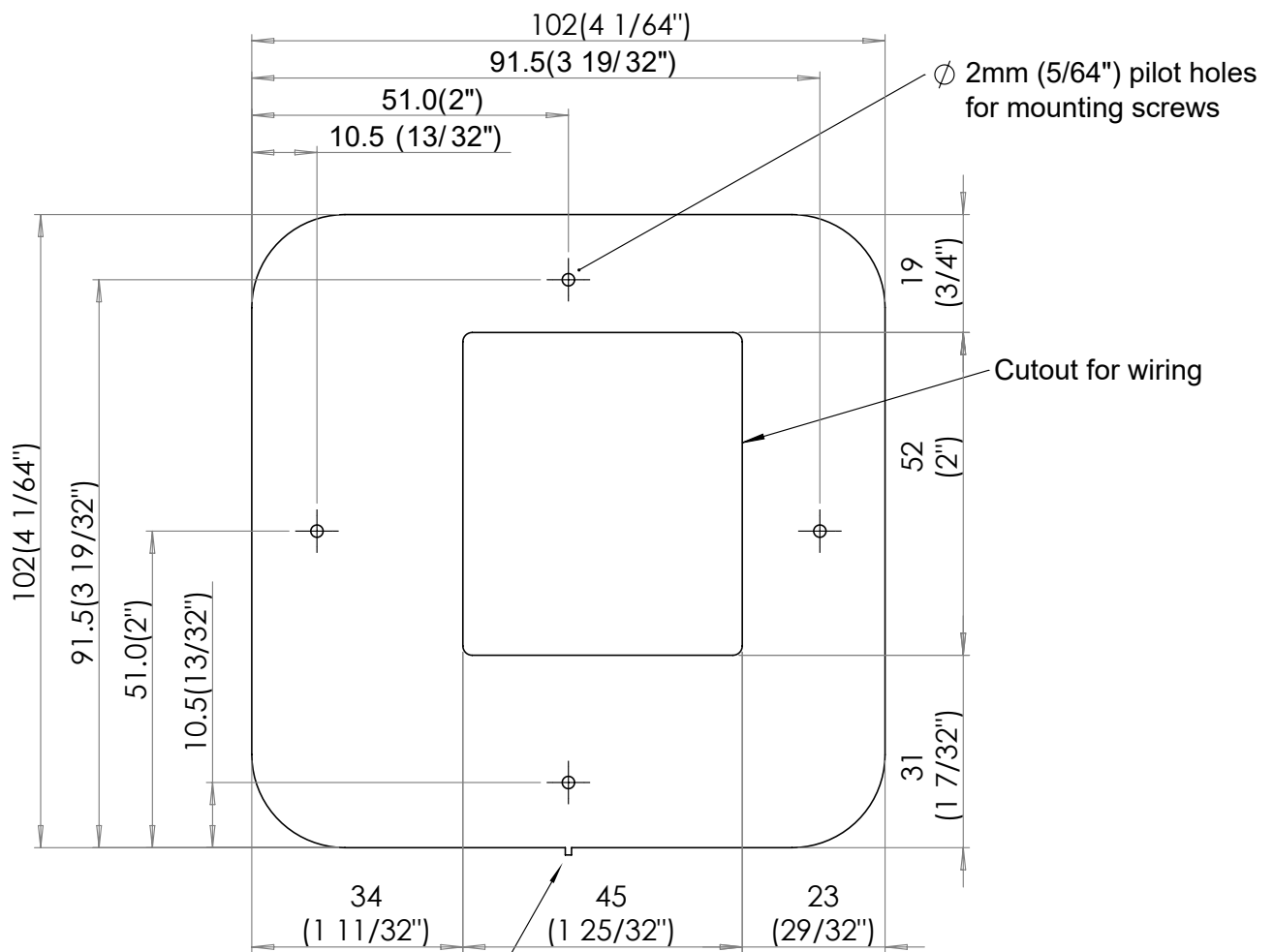


A 330Ω end-of-line resistor must be inserted between the NA and NB terminals.

Mounting

1. Run the ethernet or RS-485 cabling to the desired location.
2. If using RS-485, connect the wires to the plastic connector provided.
3. Use the access point's base or the mounting template below as a guide for positioning the unit on the ceiling.

View of Unit from Below



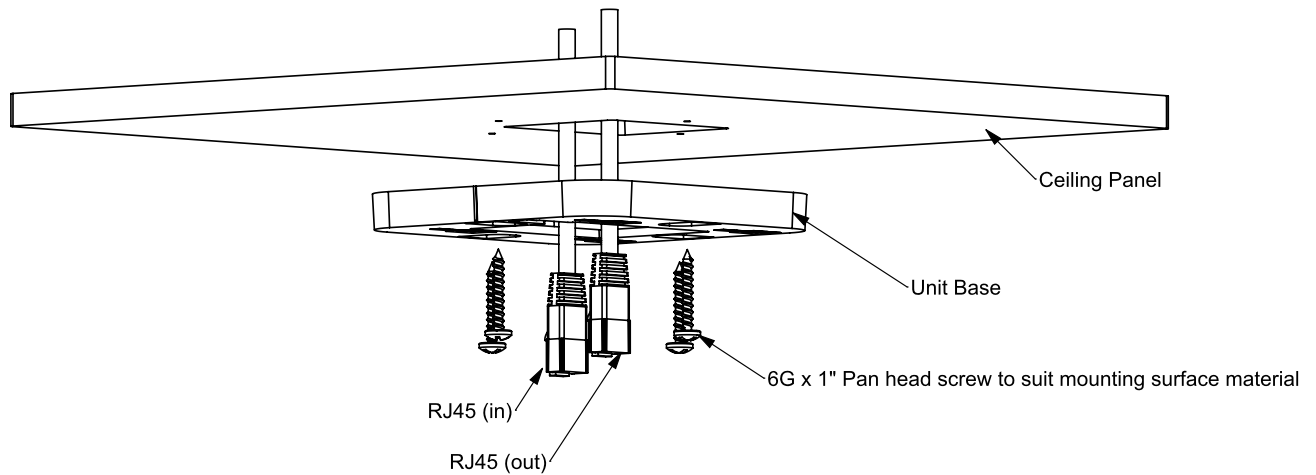
Raised line on outside of case

4. Mark and cut the wiring cutout. Pull the ethernet or RS-485 cables through the cutout.

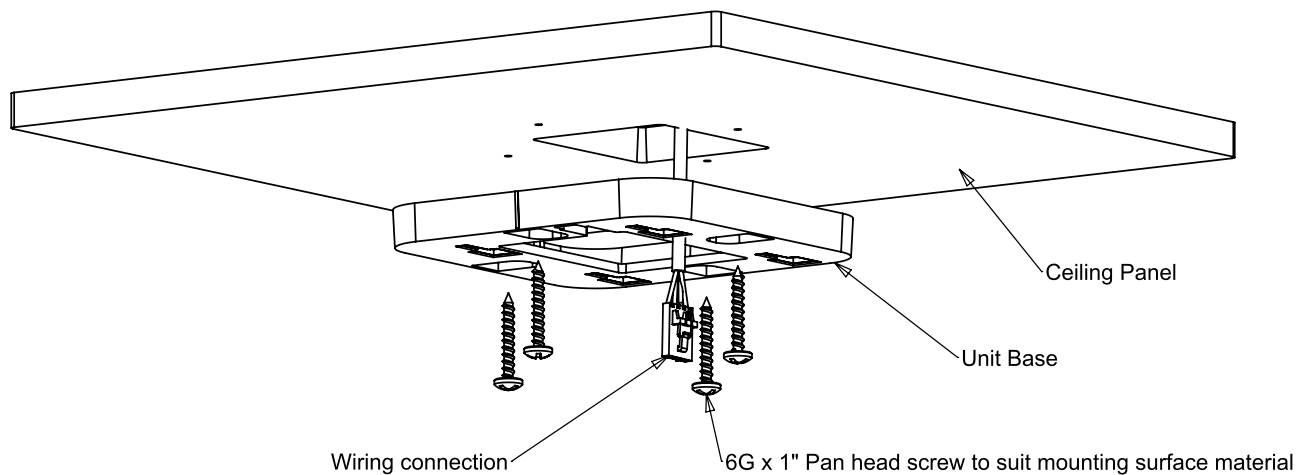
Do not make the cutout larger than necessary, as this can prevent the tamper switch from functioning correctly.

5. Mark and drill 2mm (5/64") diameter pilot holes for the mounting screws.
6. Place the unit's base against the ceiling. Pull the wiring through the hole.

For **ethernet** wiring:

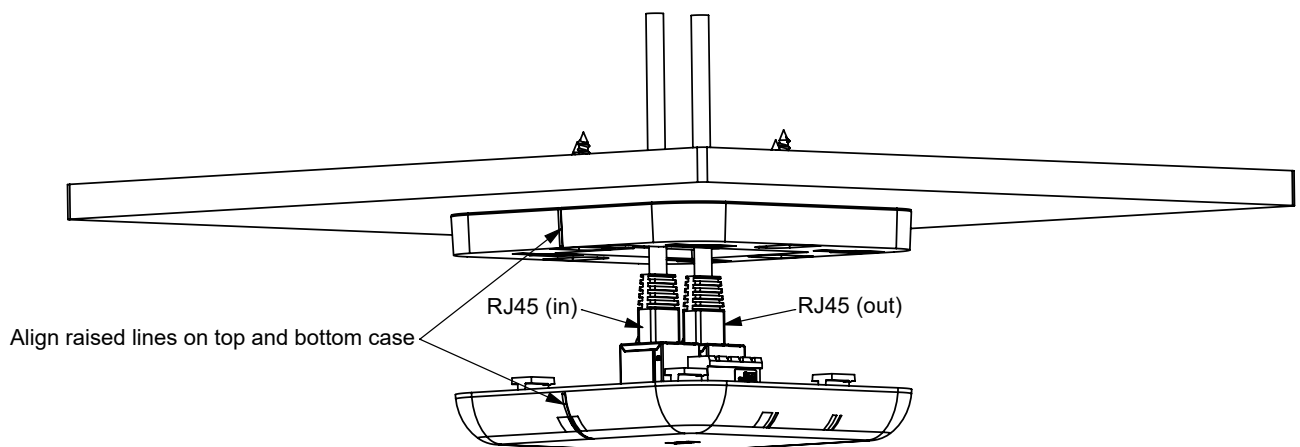


For **RS-485** wiring:

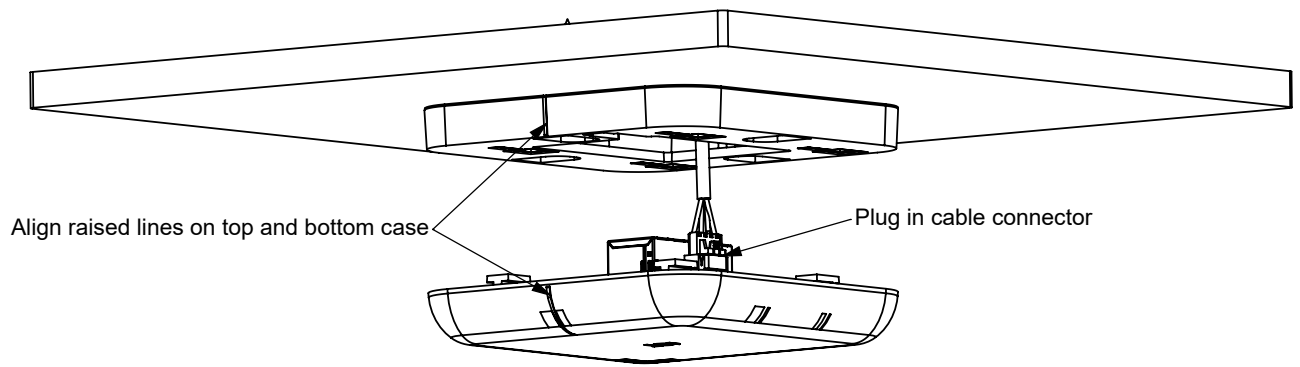


7. Use four 6G x 1" pan head screws (suitable for the ceiling material) to affix the base to the ceiling.
8. Hold the front of the unit up to the base, aligning the raised lines at the bottom of each half of the case.
9. Plug in the ethernet or RS-485 cables as shown.

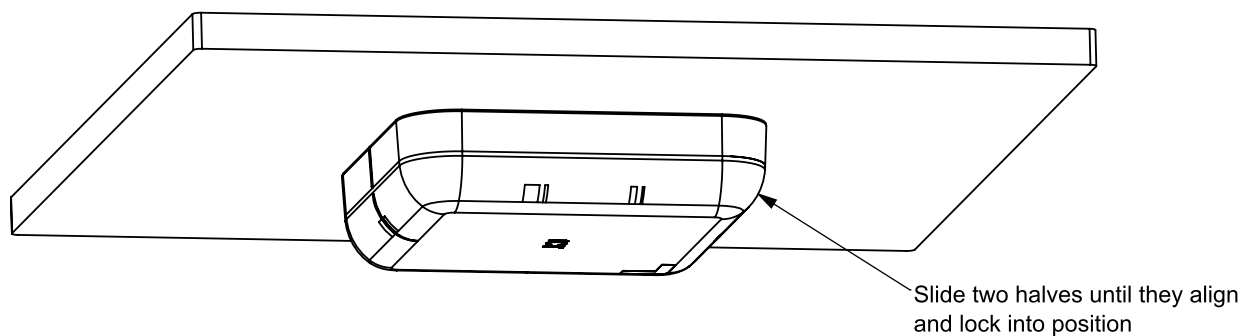
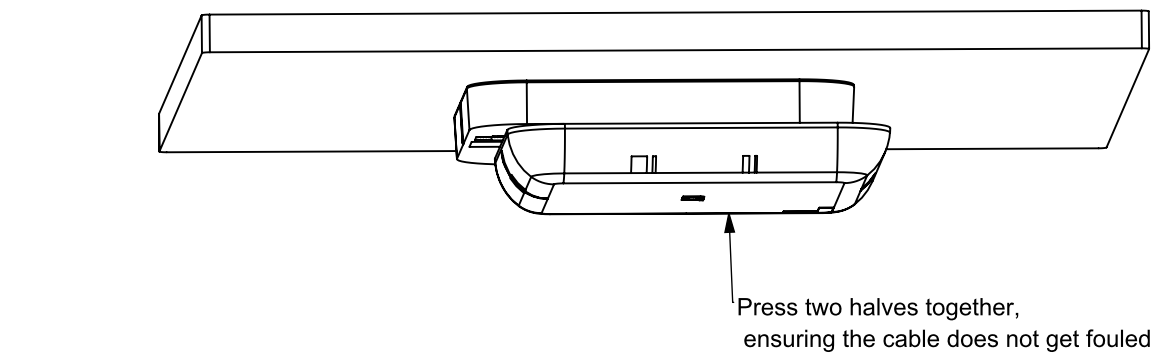
For an **ethernet connection**, connect the cable that brings power in to the ethernet port closest to the raised line. If you are daisy chaining access points, connect the cable that sends power out to the other ethernet port.



For an **RS-485 connection**, plug in the plastic connector.



10. Align the mounting posts on each corner with the cavities and press the two halves together, ensuring that the cable does not get fouled. Slide the two halves together until they align and lock into position.



Tamper Sensor

The access point includes an infrared tamper sensor that detects when the module is removed from the ceiling. The infrared sensor monitors the distance to the ceiling surface and opens the Module Tamper trouble input when the distance increases.

If the tamper switch is always open even when the unit is in place, check that it is facing towards the ceiling surface and not into the wiring cutout. You may need to reposition the module so that the tamper switch is not aligned with the cutout.

Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information	
Protege Wireless Access Point (Black)	WL-AP-B
Protege Wireless Access Point (White)	WL-AP-W
Power Supply	
Power Supply Options	PoE RS-485
Operating Power	1.44W (Typical)
PoE Protocols (Input Voltage)	IEEE 802.3AF (44-57VDC) IEEE 802.3AT (50-57VDC)
PoE Output Voltage	44-57VDC (equivalent to input voltage)
RS-485 Input Voltage	12VDC (9.5-14VDC)
Communications	
Wired Communication Interfaces	2 × 10/100Mbps Ethernet RS-485 (Protege Module Network)
Wireless Communication Interfaces	Bluetooth® Wireless Technology
Bluetooth® Interface	
Bluetooth® Protocol	Bluetooth® Low Energy (BLE), version 5.2 compliant
Bluetooth® Frequencies	2402 - 2480MHz
Bluetooth® Connection Range	Up to 25m (82ft) The Bluetooth® range is affected by location, construction material, interference and other factors. It may not be possible to achieve the maximum range in all installations.
Security	
Security Module	Contains integrated Hardware Security Module (HSM)
Encryption Level	AES256
Dimensions	
Dimensions (H × W × D)	102mm × 102mm × 25.7mm (4" × 4" × 1")
Net Weight	135g (4¾oz)
Gross Weight	TBC
Operating Conditions	
Operating Temperature	UL/cUL 0° to 49°C (32° to 120°F)

Storage Temperature	-10 ° to 85 °C (14 ° to 185 °F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)

The **Bluetooth**® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Integrated Control Technology is under license. Other trademarks and trade names are those of their respective owners.

FCC Compliance Statements

Product Name: Protege Wireless Access Point

FCC ID: UAU-WLAP

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment complies with the limits for a Class A 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, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into 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.

Changes or modifications not authorized by the party responsible for compliance could void the user's authority to operate this product.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Radiation Exposure Limits

This equipment complies with the FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and all persons during normal operation.

Industry Canada Statement

ISED ID: 10012A-WLAP

Model Numbers (HIVN): WL-APB, WL-APW

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference;
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radiation Exposure Limits

This equipment complies with the ISED Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and all persons during normal operation.

Cet équipement est conforme aux limites d'exposition aux rayonnements de la ISED Canada établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20cm entre le radiateur et toutes les personnes pendant le fonctionnement normal.

Disclaimer and Warranty

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our [Standard Product Warranty](#).

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2025. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.