Access200w

Installation Guide

Princeton IDENTITY

Package Contents

Included in the box

- 1x Access200w outdoor biometric reader
- 1x QR code card
- 1x Ferrite bead
- 1x IP67-rated four pin male connector for site installation
- 1x Single page and expanded booklet instructions

Installation Requirements

Installation to be performed only by certified installer

Additional tools may be required for environmental modifications such as creating wall openings, mounting the gang box, locating/cutting/crimping wires, etc.

Recommended Mounting Height:

It is recommended to mount the device at 36” (91.44 cm) from the ground to the bottom on the mounting cover. Use discretion when mounting the device based off of the average user base height. If the user population is on the shorter side consider mounting the device lower by a few inches/centimeters, if the user population is on the taller side consider mounting the device higher by a few inches/ centimeters.

Required materials and tools:

- Phillips Head Screwdriver
- CAT5e (or better) cable connected to a POE+ (802.3at) Switch or Injector capable of supporting 30 Watts
- Single Gang Box or other compatible electrical box
- Identity Server - required for system operation

47in (120cm)

Access Control Connection Diagram

Cat5e+

PoE+ Ethernet

Identity Server

Wiegand / OSDP

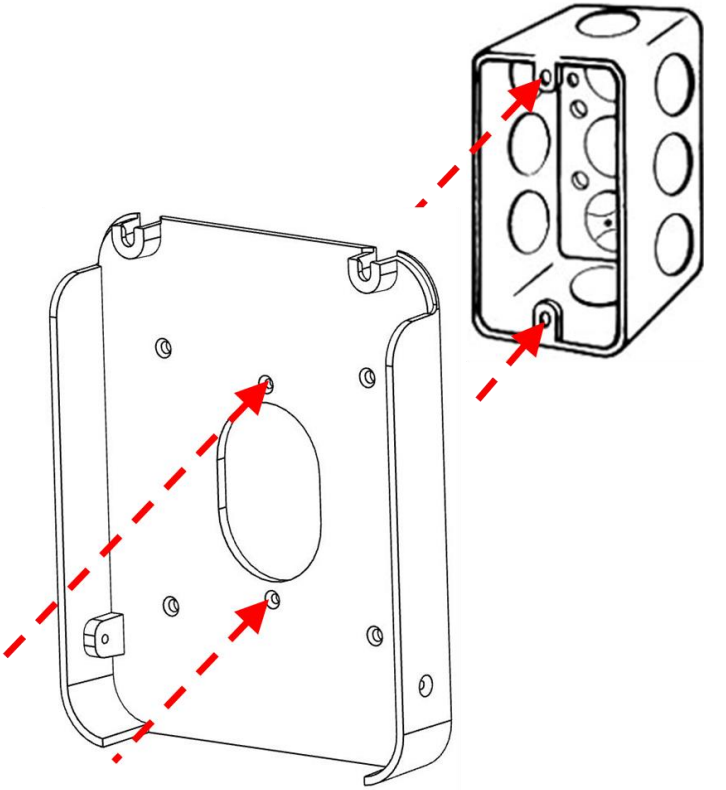
Panel

Access Control

Step 1 – Install Access200w back cover

NOTE: The Access200w outdoor biometric reader is sealed during the production process before it is shipped from the factory. This is done in order to maintain the device's IEC IP65 ingress protection rating. Opening the device will break the seal and void the warranty.

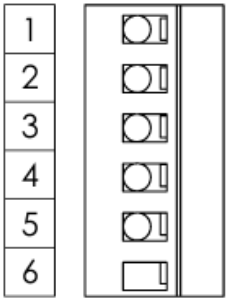
Install the back cover using the M5 screws to the Single Gang Adaptor Plate. Ensure that the mounting cover is level to the ground.



Step 2 – Prep Gang Box Wiring

Wiegand wires to wall cabling

Pull your CAT5e and access control wires through the opening on the gang box and wire the I/O interface Cable to the access control wires for the desired configuration using the table below.



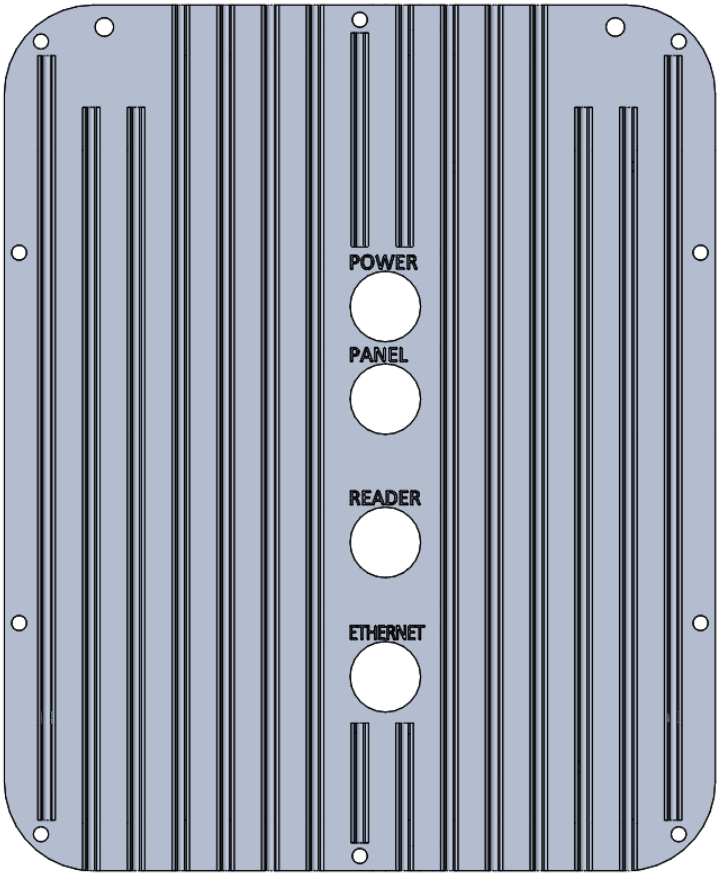
SCALE: 2:1

WIRE NO.	COLOR	FUNCTION
1	RED	12V POWER
2	BLACK	GND
3	GREEN	D0
4	WHITE	D1
5	BROWN/ORANGE	STATUS
6	BLUE	UNUSED
7	ORANGE	RELAY | COMMON
8	YELLOW	RELAY | NORMALLY OPEN

Wiring Layout

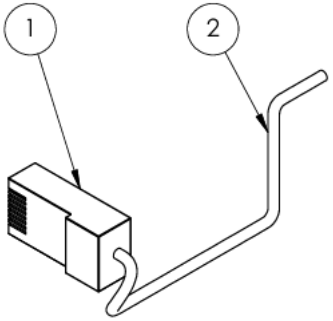
The Access200w is shipped from the factory with four cables exiting the rear of the device

- Power
- Panel (Wiegand wires to the access control panel)
- Reader (Wiegand wires for an external card reader)
- Ethernet



Ethernet Cable Layout

The Ethernet cable is terminated at the factory with a standard RJ45 Cat6 connector. However, included in the Access200w box is a male/female four-pin IP67-compliant connector assembly should the customer site wish to remove the installed RJ45 connector and replace it.

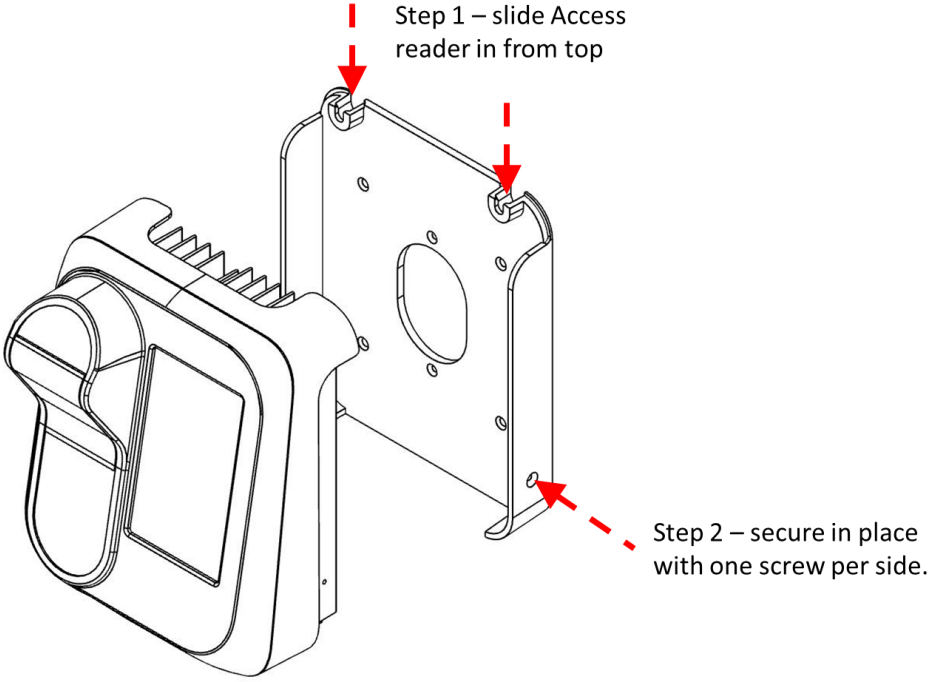


WIRE LAYOUT				
M12	RJ45	FUNCTION	PAIR	COLOR
1	1	TD+	1	WHITE/ORANGE
3	2	TD-	1	ORANGE
2	3	RD+	2	WHITE/GREEN
4	6	RD-	2	GREEN

Step 3 – Secure the Access200w onto mount

Include connecting Wiegand / OSDP wires to wall cabling

Once the cables of the device are terminated and connected to the facility wires, the Access200w unit can be mounted to the wall. Then secure the Access200w to the mounting panel as shown below.



Step 4 – Physical Installation Complete

Next…

Now that your Access200w edge device is physically mounted and electrically connected, you'll next need to complete the initiation activities detailed on the following pages:

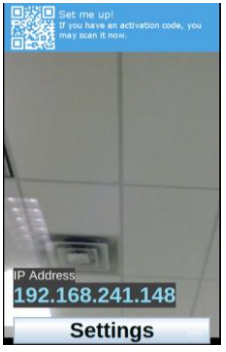
- Calibrate the proximity sensor on the Access200w edge device
- Digitally connect the Access200w edge device to your Identity Server
- Verify system operation

Calibrating Access200w's Proximity Sensor

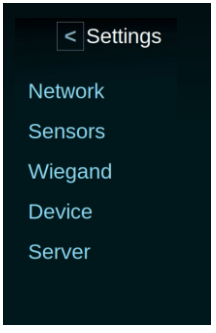
It is recommended that you calibrate the Access200w whenever it is installed / moved

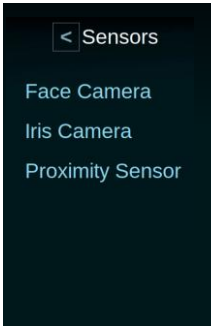
Access200w devices may require periodic calibration of the Proximity Sensor. Follow the steps detailed below to complete the calibration procedure. If already connected to an IDS, take it offline, then press and hold your finger in the top right corner of the device's screen until the settings button appears. If it is not connected to an IDS, you may proceed:

1) On the device's screen, tap the "Settings" button.

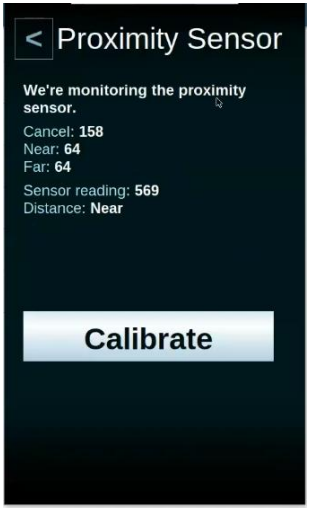


2) Next, tap "Sensors" and then "Proximity Sensor".





3) On the resulting screen, you should be able to see a metric called “Sensor reading". This is an indication of how close someone/something is to the device. If you stand in front of it, the number increases, and if you step to the side of it, the number decreases. The "Distance" label changes between "Near" & "Far" depending on where you’re standing. The Near/Far will change roughly 2 feet away from the front of the unit.

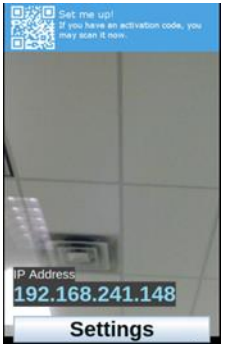


4) Tap on the "Calibrate" button. You’ll see the "Cancel" value change depending on the calibration. A normal cancel value is less than 1000. During the calibration, ensure that there is no movement in front of the device, as this will greatly affect the reading.

Connecting your Access200w to IDS

Installation to be performed only by certified installer

Once physical Installation is complete, using a computer and web browser connected to the same network as the device, navigate to the IP address on the screen to complete setup of the device.



You should now be able to proceed with accessing the webpage

For additional setup instructions for the device, go to https://support.princetonidentity.com

Installation to be performed only by certified installer

Once on the device's webpage click "Connect to Identity Server". You will then see this screen. Populate the fields with the server's address and credentials, then click "Test Connection".

If the connection was successful, you'll see a green checkmark and text stating, "Connection Successful". Click "Save" to finalize the connection. If it was unsuccessful, you will receive a red banner stating, "Failed to authenticate with remote server". In this case, click "Save Diagnostic" and submit the logs to support@princetonidentity.com.

Successful

Unsuccessful

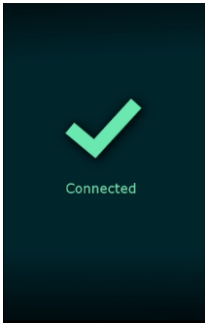
Installation to be performed only by certified installer

Once the connection is finalized, you should see the host name and a green checkmark, indicating the connection status each time you log in to the device, provided that the Identity Server is running.

If the device was connected to an Identity Server previously but loses connection to/is powered down without disconnecting first/the server goes down, the device will display a red checkmark, indicating that the connection is lost.

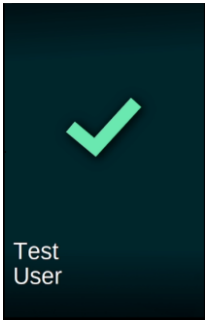
Verifying operation

Connecting to IDS:
The device should be able to connect to an IDS by using the webpage or by scanning a QR code from an IDS. You should see “Connected” with a green checkmark, indicating that the connection was successful.



Running:
The device’s idle screen should be stable, with no flashing or dim output.

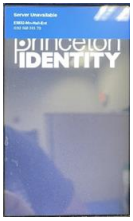
Functionality Tests:
Upon authenticating with biometrics, the device should not reboot, otherwise there is a power issue. When equipped with a card reader, the device should beep and display a green check or your name and/or portrait (if you have the setting “Report Credentials to the Identity Server” enabled), when it is scanned, indicating access granted/a successful read.



Troubleshooting

Installation to be performed only by certified installer

Server Unavailable: This occurs when an IDS is offline, or the device is unable to make the connection to the IDS. Try disconnecting and reconnecting the device to the IDS.



Wiegand unavailable/Wiegand to ACS panel failed: This most often occurs when a device's wiring is adjusted while powered on or has a wiring issue. Try restarting the device from the homepage ("Restart Device"). If that doesn't work, reboot the device by disconnecting/reconnecting the ethernet cable.

Optional Mounting Accessories

Installation to be performed only by certified installer

Please contact us for additional mounting materials.

Optional Mounting Accessories

Installation to be performed only by certified installer

Please contact us for additional mounting materials.

Warranty Coverage for Access200w

Princeton Identity is pleased to offer a limited 10-year warranty on your Acces200w (and/or EyeAllow) hardware purchase. Note coverage excludes product damage resulting from installation or service that is out of compliance with our published instructions.

Go to support.princetonidentity.com for all current documentation.

Limited Warranty and Limitation of Liability

Princeton Identity warrants that our hardware products shall be free from material defects for a period of ten (10) years from the date of purchase (the "Warranty Period"). This warranty shall apply only to the original purchaser unless the buyer is authorized by Princeton Identity to resell the products, in which event this warranty shall apply only to the first repurchase.

It is necessary to obtain a Return Material Authorization (RMA) number before returning suspected defective products to Princeton Identity. An RMA number may be requested by contacting Princeton Identity support through our ticketing system at support.princetonidentity.com or by emailing support@princetonidentity.com. The RMA number must be written on the documentation accompanying the return. If the product is delivered by mail or by an equivalent shipping carrier, the purchaser agrees to insure the product or assume the risk of loss or damage in transit, to prepay shipping charges to the warranty service location and to use the original shipping container or equivalent.

Princeton Identity will in its sole discretion decide either to repair or replace the returned product. Repair parts and replacement products will be furnished on an exchange basis and will be either reconditioned or new. All replaced parts and products become the property of Princeton Identity. In the event of a verified warranty claim and RMA, Princeton Identity will generally expedite shipment of replacement products before suspected defective products are returned. In this way the suspected defective products can be uninstalled, and products installed in their place, during one field service call, avoiding two separate service calls and minimizing service interruption to the customer. Suspected defective products must be received at the warranty service location within thirty (30) days of shipment of replacement products. If the suspected defective products are not received within thirty (30 days, Princeton Identity will invoice the purchaser for the then current list price of the replacement unit(s).

This limited warranty does not include service to repair damage to the product resulting from accident, disaster, unreasonable use, misuse, abuse, customer's negligence, reseller's negligence, or from installation or service that is out of compliance with our published instructions, or from non-Princeton Identity modification of the product. Princeton Identity reserves the right to examine the alleged defective goods to determine whether the warranty is applicable. Without limiting the generality of the foregoing, Princeton Identity disclaims any liability or warranty for goods resold in other than Princeton Identity's original packages, and for goods modified, altered, or treated by customers.

PRINCETON IDENTITY MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND PRINCETON IDENTITY DISCLAIMS ANY WARRANTY OF ANY OTHER KIND, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. PRINCETON IDENTITY SPECIFICALLY DISCLAIMS ANY WARRANTY COVERING LABOR TO UNINSTALL AND REINSTALL PRODUCTS. EACH PURCHASER UNDERSTANDS THAT THE PRINCETON IDENTITY PRODUCT IS OFFERED AS IS. IF THIS PRODUCT DOES NOT CONFORM TO PRINCETON IDENTITY'S SPECIFICATIONS, THE SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT AS PROVIDED ABOVE. PRINCETON IDENTITY'S LIABILITY, IF ANY, TO AN END USER OR RESELLER, SHALL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID TO PRINCETON IDENTITY FOR THE APPLICABLE PRINCETON IDENTITY PRODUCT. IN NO EVENT WILL PRINCETON IDENTITY BE LIABLE TO AN END USER OR RESELLER FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF PRINCETON IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

Active contract required

When hardware products are purchased, they typically require a contracted software license to operate. Note the Warranty Period equals the length of the contiguous software (or service) contracts, up to a maximum term of ten (10) years provided contract payments are current. Any practical lapse in license / service contract will void remaining years of the hardware warranty. IF THE SOFTWARE LICENSE CONTRACT EXPIRES BEFORE BEING EXTENDED, OR IF CONTRACT PAYMENTS LAPSE, THE WARRANTY PERIOD IS IRREVOCABLY TERMINATED.

Compliance Statements

UL294 Statement:
Compliance with IEEE 802.3 Specifications was not verified for UL294 This device is intended to operate, and comply with the National Electrical Code as a Class 2 and Class 3 Circuit

FCC Statement:
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. This equipment has been tested and found to comply 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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Industry Canada Statement:
This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. This Class A digital apparatus complies with Canadian ICES-003. Model 2000-0202 Contains: FCC ID: WP5TWN4F21 IC: 7948A-TWN4F21 CAN ICES-3 (A)/NMB-3(A) 7 6 Once physical Installation is complete, using a computer and web browser connected to the same network as the device, navigate the to the IP address on the screen to complete setup of the device.

	Access200w
Modes	
Identify Mode	YES
Verify Mode	YES
Enrollment / Seamless Enrollment Modes	NO
Modalities	
Iris Biometrics	YES
Face Biometrics	YES
PIN (randomized on-screen keypad)	YES
Card	With Optional Internal Card Reader or External Reader
Digital Mobile Credential	With Optional Internal Card Reader or External Reader
QR	YES
Biometrics on Card	With Optional Internal Card Reader only
Connectivity	
Wiegand	YES
OSDP	With Optional Add-On
External Reader In	YES
Relay	Dry Contact 24V, 100mA
Networking	Ethernet
Specifications	
Local Caching	YES – 6,000 users
Encryption at Rest	YES
Data Transit Security	TLS 1.2, 1.3
Certifications/Compliance	FCC, CE, IEC 62471, ROHS
Power	
Input	POE+ or 24V DC, 1 A
MAX Power Consumption	30W peak for POE+, 24W for 24V DC
Physical Specifications	
Recommended Mounting Height	36" (91.5 cm) to the bottom of the mounting plate
Dimensions (in)	6.5" x 7.9" x 4.0" (W x H x D)
Dimensions (cm)	16.5 cm x 20 cm x 10.3 cm (W x H x D)
Weight	5.8 lbs (2.6 kg)
Environmental	
Intended Use	Outdor
Operating Temperature	-10 to122 Degrees F (-23 to 50 Degrees C)
Weather Rating	IP65

Princeton Identity is a leading innovator of iris-biometric and multi-factor authentication technologies, transforming how businesses and governments around the globe achieve secure and reliable identity assurance. Backed by over two decades of research and product design, our solutions are trusted by some of the most recognized names in banking, industry, higher education, healthcare, transit, and border control. Princeton Identity systems are proudly manufactured in the USA, and deliver unparalleled flexibility, accuracy, convenience, and scalability.

princeton IDENTITY

300 Horizon Dr. Suite 308
Hamilton, NJ 08691
609-270-3220