

WELCOME,

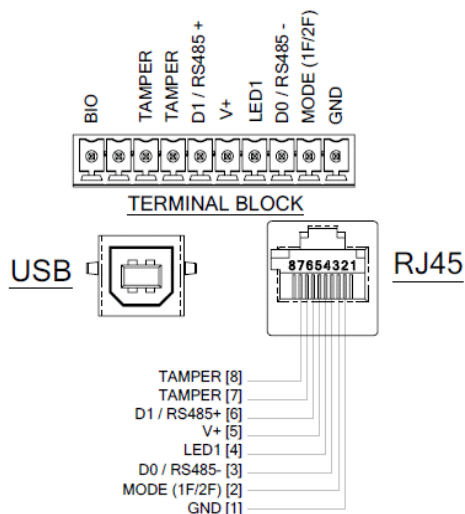
At IDFACTORS, we work hard to make your installation task easy because we know you may have an impatient customer or a challenging installation. **We make it our business to ship Readers configured for plug-and-play installation**, but there are times when we just do not get the needed information. No matter, we are here to help.

This short GUIDE will help you install an IDFACTORS Reader. If you have installed access systems that use PIV or CAC cards, you probably know the information provided herein. If not, it will be of value for a successful installation.



1.0 How to install an IDFACTORS Reader

Reader connections are provided on both a screw terminal block and an RJ-45 socket suitable for a pre-terminated cable (shown in the diagram below). The terminal block is detachable for easy wiring.



V+	9 -18VDC (12V nominal)	D0/D1	Wiegand/RS485 data
LED1	Panel grant/deny signal	MODE	1 or 2 factor mode select

Wire Gauge	22AWG	20AWG	18AWG	CAT5
Cable Distance	200 feet (60m)	300 feet (90m)	500 feet (150m)	150 feet (45m)

2.0 A Brief Introduction to CAC and PIV Cards

This Matters: The CAC and PIV work differently than old HID prox or iClass-type cards. First, they have a 4 to 8 digit PIN that was set by the User when the Card was issued. Government standards require this PIN to be sent to the card to “unlock” it when using 2-Factor Mode. The PIN is not stored the panel.

Many sites prefer to use the more traditional Pin to Panel setup. To do this, the IDFACTORS Reader must be “re-configured” using the IDFACTORS ReaderConfig Application.

The unique identifier for physical access is called the FASC-N (the Federal Agency Smart Credential Number), which is a 16-digit number (64 bits). Be sure that any access system using the CAC or PIV can process a minimum of 64-bits of the FASC-N. Any fewer bits will not be secure. Most modern access systems are capable of 200 bits, which is the Government standard for the full FASCN.

Note there is no Site Code or Facility Code on the CAC or PIV Cards.

3.0 How CAC and PIV Cards Work Differently from Legacy Cards

CAC and PIV cards are used differently between 1-Factor Card Only and 2-Factor Card+PIN Modes:

- 1-Factor Mode: the card can be presented by Contact (inserting the card with the chip up and facing you) or Contactless (holding the card about 1" from the reader for about 1 second).
- 2-Factor Mode: The card must be inserted into the Contact slot and then the PIN is entered (followed by the ETR button) before the card is removed.

The NOTES below will be helpful:

NOTE 1: Every CAC or PIV cardholder has already selected a PIN to "unlock" their card for computer and physical access. This was done when the card was being issued.

NOTE 2: IDFACTORS readers are configured to send the PIN to the card per the FIPS-201 Standard. However, the Readers also support Pin to Panel* Mode.

NOTE 3: At the request of the Government, our 2-Factor Readers are shipped from the factory set to the more secure 2-Factor PIN to Card mode.

NOTE 4: Per Government Standards, the CAC card "locks" after 3 incorrect PIN attempts. PIV cards lock after 4 to 6 incorrect PIN attempts.

NOTE 5: 2-Factor Readers can also be configured to operate in 1-Factor mode.

5.0 Setting the Reader Security Mode

If the Security Mode needs to be switched to 1-Factor Mode, it can be done in firmware or hardware:

- In firmware, using the ReaderConfig application, type **CMD>SM 1F** from the Command Line. You can get the App by emailing customerservice@idfactors.com or by calling 510-346-1510.
- In hardware, add a jumper (strap wire) between positions 1 and 2 on the Terminal Block on the back of the Reader (see Figure above).
- The Security Mode can also be dynamically controlled via a setting in the PACS panel that controls a relay that is wired to the Reader. Similar to the hardware jumper described above, closing a relay on the Panel will switch the Reader into 1-Factor Mode.

6.0 Setting the Wiegand Format

If the Reader's Wiegand Format can be changed using the ReaderConfig Application*. The App will display multiple formats and the desired one is selected by typing **WF xx**.

7.0 Testing the Reader – Access System Interface

You will need a CAC, PIV or PIV Compatible card and you will need to know the card PIN if using PIN to Card mode. Proprietary proximity and contactless smart cards will not work! Also note that the test card must be enrolled into the PACS system and authorized for access for the door to open.

For testing, first be sure the Readers and panel are in the correct Mode and try the following:

- For 1-Factor contactless access, hold the card about 1 inch from the Reader and you should see the Yellow LED turn on and then the Green LED will flash briefly and the door will open.
- For 1-Factor contact access, insert the card into the contact slot (chip up and facing you) and you should see the Green LED flash briefly and the door open (if the card is enrolled).

- For 2-Factor Readers, insert the card into the contact slot (chip up and facing you) and you will see the Yellow LED turn on. Enter the card's PIN, then press ETR and the Green LED should flash briefly and the door open.
- If you do not have success, do not blame the Reader just yet. Experience has shown that it could be the Card being used, the 1-Factor or 2-Factor settings in the access system, or wiring somewhere in the panel. First check for the following:

If the Green LED on the Reader flashed Green (and beeped) then the Card was read successfully and the FASCN was sent to the access system panel.

If the door did not open, then check the panel wiring, check the Wiegand format in the system against the format setting in the Reader and confirm the card is enrolled.

- The table below will help you troubleshoot the possible cause behind any abnormal function:

Red	Yellow	Green	Meaning	Behavior	Troubleshoot Possible Cause
⊗ S	⊗ S	⊗ S	Power On/Reset	Reader beeps and LEDs occasionally flash in sequence during testing	Reader may be re-setting: Check Power to the Reader
⊗ F	⊗ F	○	Card Reset Error	Red and yellow flash rapidly in sequence on Card insertion	Possible fault in Card or Reader – try another Card or Reader Combination to verify faulty item
○	○	○	Card Inserted	All LEDs off	
○	○	⊗ 1	Card Read Good	Green flash briefly	
⊗ A	⊗ A	○	Card Error	Red and yellow toggle rapidly	Try another known good Card and try Card in another Reader to verify
⊗	○	○	Card Expired	Red on solid	
⊗ A	⊗ A	○	PIN Locked	Red and yellow alternately toggle rapidly	Reset Card at PC with good PIN entry or go to PIN reset station
○	⊗	○	PIN Request	Yellow on solid	
⊗ 1	○	○	Pin Key Press	One red flash per key-press	
○	○	⊗ 1	PIN Good	Green flash briefly	
⊗ A	⊗ A	○	PIN Bad	Red and yellow toggle rapidly	Re-enter PIN. If problem repeats reset Card at PC or go to PIN reset station
○	⊗ 1	○	Pin Restart	One yellow flash per key-press	
○	○	⊗	Access Granted	Green on solid after Card scan + Green flash	Check panel and wiring to door and door locking device
⊗	○	○	Access Denied	Red on solid after Card scan + Green flash	Verify access credential and privileges in access system

○ LED off

⊗ 1 LED flash once

⊗ A LEDs alternating

⊗ LED on (solid)

⊗ F LED flashing

⊗ S LEDs flashing in sync

If you are not able to resolve your problem, Contact Customer Service at www.customerservice@idfactors.com