

For Veridt Readers with Base Part Number:

3-Factor Readers:

900W2031

900W2030

2-Factor Readers:

900W2036

900W2026

1-Factor Readers:

900W2037

900W2027

General Information

Veridt Stealth series readers are designed to be operated as a Class 1 access control system component for use without requirements to withstand a destructive attack. A Tamper Indicator switch is available to provide a supervisory indication to the PACS in the event the reader is removed from its installed location.

Veridt Stealth series readers are designed to meet the requirements of the National Electrical Code for Class 2 systems and are intended to be used with UL294 listed control equipment

Veridt Stealth series readers are tested to meet the following UL294 Levels

Destructive Attack:	Level I
Line Security:	Level I
Endurance:	Level I
Standby Power:	Level I

The installation of these readers, and the materials used for installation, should be in accordance with the location requirements and the wiring methods defined by the National Electrical Code for Class 2 systems. Connect only to a Listed Access Control / Burglary power-limited power supply.

The connections of the reader pigtail to the wiring system must insure a thoroughly good physical connection without damaging the conductors and should be made by means of pressure connectors or pressure splices suitable for 22-to-26-gauge stranded copper wire.

Installation should be performed by qualified individuals who have the skills and knowledge related to the installation and operation of the equipment and have received the proper safety training to recognize and avoid any hazards that may be involved.

Stealth series readers are designed for an input power range of 11VDC to 13VDC. Operation above the maximum voltage of 13VDC may damage the reader, and operation below the minimum voltage of 11VDC may cause intermittent or complete loss of reader operation.

Stealth readers are designed for use in a wide range of environmental conditions. Biometric readers should be mounted to protect the surface of the fingerprint sensor from accumulating water on its surface. A rain shroud may be required.

Stealth series readers have no user replaceable components. Any unit that does not operate properly must be returned to the factory for any service requirements

Stealth series readers come preconfigured and require no user programming.

Stealth series readers require no periodic maintenance or calibration. If it becomes necessary to clean the outer surfaces, use a moist, non-abrasive cloth with a mild detergent and gently wipe the external surfaces. Do not immerse the reader.

Successful operation of the reader is indicated by the access control system granting access to a valid, registered card and denying access to an invalid or non-registered card.

• TECHNICAL NOTE •

Stealth Series User Guide

Stealth Reader Series

Veridt
Verify • Identify

#120

Stealth Series and Part Numbers - Summary

Stealth Bio-Q PN 900W2031	Stealth Bio PN 900W2030	Stealth Dual PN 900W2036	Stealth Dual Lite PN 900W2037	Stealth PN 900W2026	Stealth Lite PN 900W2027
 Patent Pending					

Reader Name	Stealth Bio-Q	Stealth Bio	Stealth Dual	Stealth	Stealth Dual Lite	Stealth Lite
Part Number	900W2031	900W2030	900W2036	900W2026	900W2037	900W2027
Multifactor	3-Factor	3-Factor	2-Factor	2-Factor	1-Factor	1-Factor
Biometrics	Facial Imaging	Fingerprint				
Keypad	✓	✓	✓	✓		
Contact	✓	✓	✓	✓		
Contactless	✓	✓	✓	✓	✓	✓

Dimensions	900W2031	900W2030	900W2036, 900W2026 900W2037, 900W2027
	7.0 x 4.0" x 1.5" 17.78cm x 10.16cm x 3.81cm	7" x 3" x 1.5" 17.78cm x 7.62cm x 4.0cm	5.5" x 3.0" x 1.5" 13.97cm x 7.62 cm x 4.0 cm

Stealth Series Hardware Platform Components

Stealth Bio-Q PN 900W2031

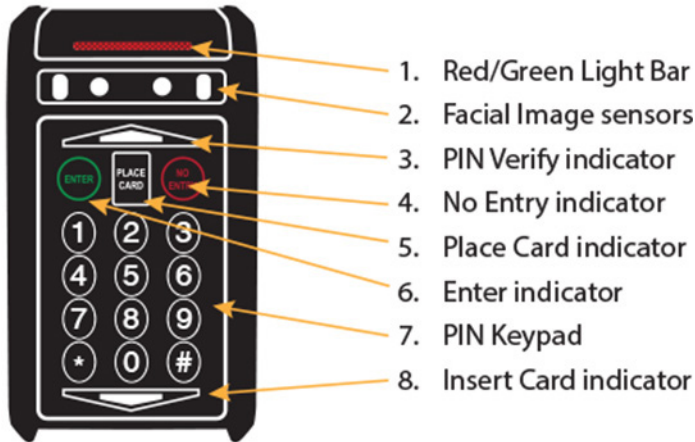


Figure 1

Stealth Bio PN 900W2030

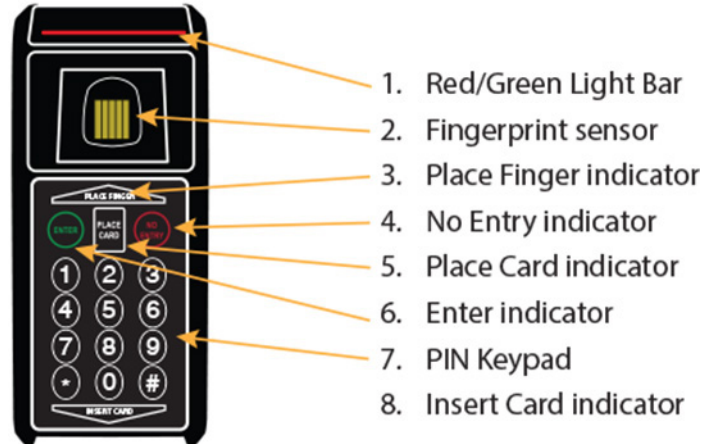


Figure 2

Stealth Dual PN 900W2036
Stealth Dual Lite PN 900W2026

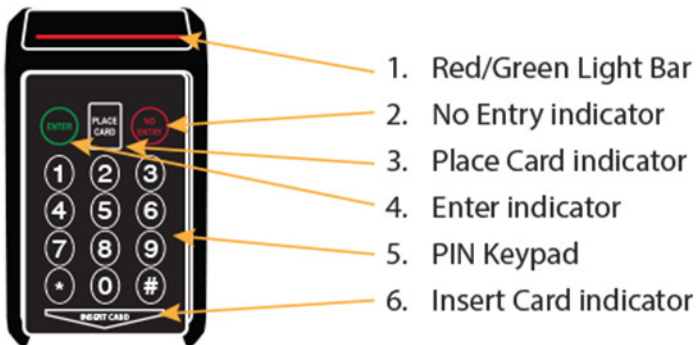


Figure 3

Stealth PN 900W2037
Stealth Lite PN 900W2027

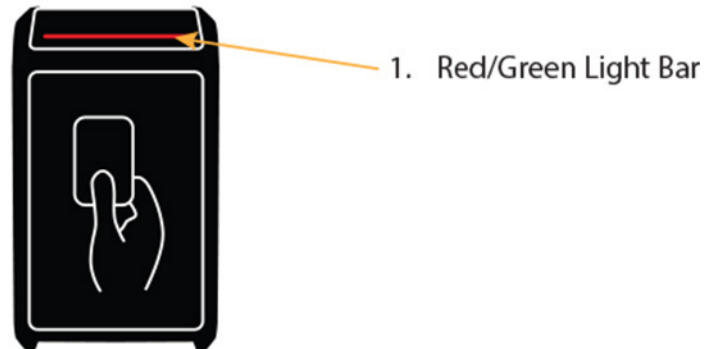


Figure 4

Stealth Series Operation Instruction

Idle State

Upon power-up, the reader will boot to the idle state. The idle state is indicated by a red light bar #1 in figures 1-4

The Stealth family of card readers are designed to read government issued ID cards (TWIC, CAC, PIV or PIV-I) In reader models with a keypad, the No Entry indicator, #4 in figures 1 & 2, and #2 in figure 3, is on. The active interfaces for the dual interface readers (900W2030 and 2036) with keypad are indicated by a slowly blinking Place Card #4 or Insert Card #8. For reader 900W2026 the contactless interface is indicated by a slowly blinking Place Card #4. In the reader models without a keypad 900W2037 both Contact and Contactless interfaces are active and for the 900W2027 the Contactless interface is active

Basic Operating Modes:

1) Card + PIN + Facial Image - Only reader model 900W2031 supports the Card + PIN + Facial Image mode. The only interface active for this mode is the contact interface. Insert the card with the chip oriented as shown in figures 9. The card read is indicated by the light bar turning amber and the no entry indicator blinking. The keypad will light up when the reader is ready for the pin entry. Enter your pin by pressing the correct keys and end with the # key. If the pin is invalid an access denied will be indicated. If the pin is valid the light bar will blink amber as it reads the template from the card and then blink faster when ready to perform the match. Look directly into the camera. If the facial image matches the template stored on the card, an access granted is indicated. If the match fails, access denied is indicated.

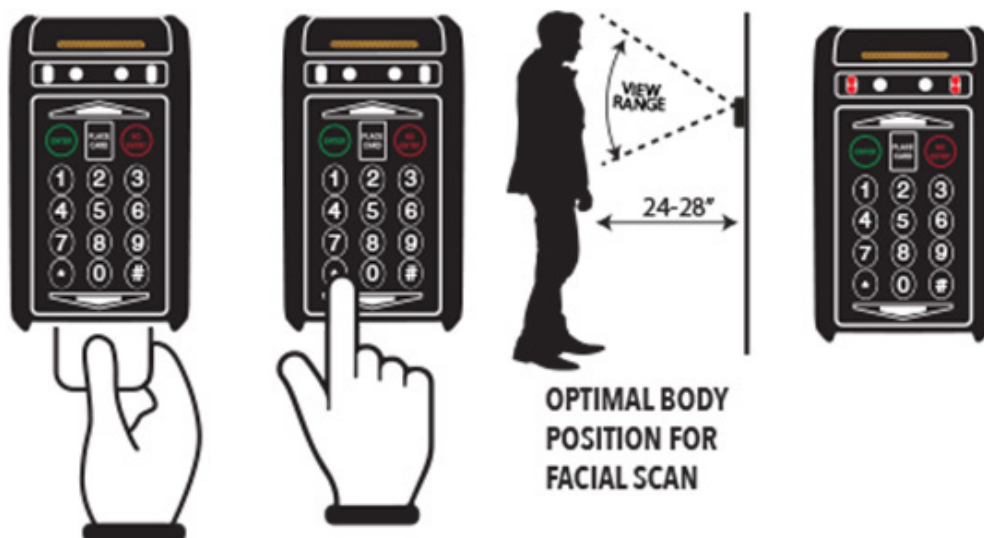


Figure 5

2) Card + PIN + Fingerprint - Only reader model 900W2030 supports the Card + PIN + Fingerprint mode. The only interface active for this mode is the contact interface. Insert the card as shown in figure 6 with the chip oriented up. The card read is indicated by the light bar turning amber and the no entry indicator blinking. The keypad will light up when the reader is ready for the pin entry. Entry your pin by pressing the correct keys and end with the # key. If the pin is invalid an access denied will be indicated. If the pin is valid the Place Finger prompt will turn on. Place your finger flat on the sensor. If the fingerprint matches the template stored on the card, an access granted is indicated. If the fingerprint match fails, the reader will try two more fingerprint reads indicated by a beep. Remove your finger and try again. If the two attempts fail, an access denied is indicated.



Figure 6

3) Card + PIN - Only readers with keypads support Card + PIN. The only interface active for this mode is the contact interface. Insert the card with the chip oriented as shown in figures 6 & 7. The card read is indicated by the light bar turning amber and the no entry indicator blinking. The keypad will light up when the reader is ready for the pin entry. Entry your pin by pressing the correct keys and end with the # key. An access granted or access denied will be indicated as described in the Card only mode.

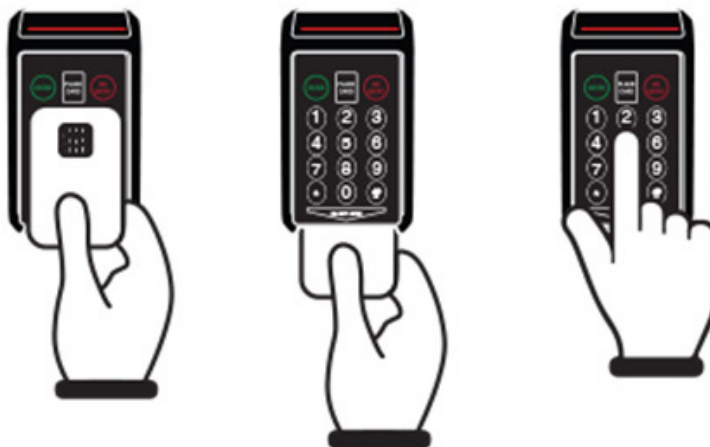


Figure 7

4) Card Only Mode - On the dual interface readers both the contact and contactless interfaces are active. On the single interface readers the contactless interface is active. To use the contactless interface, place the card on the front of the reader as indicated in figures 6, 7 and 8. If the card is read the light bar turns amber, For access granted, the light bar will flash green and reader beeps fast 4 times (on all readers) and the entry indicator turns on green for readers with keypads. For access denied the light bar flashes red and the reader sounds 3 long beeps (all readers). To use the contact interface insert the card with the chip oriented as shown in figures 4 and 6. The access granted and access denied indicators are the same as the contactless interface.



Figure 8

Stealth Series Troubleshooting

Veridt Stealth family readers have no user replaceable parts. All of the Stealth family readers are preconfigured and require no user programming.

The only supervisory function associated with the reader is the tamper switch which is monitored by the access control system.

The only maintenance required is the periodic cleaning of the fingerprint sensor and imager windows with alcohol and an optical tissue when necessary

Stealth Series Maintenance

- Reader does not turn on - Check on Power connection, make sure the 12V power supply has sufficient capacity to power the system
- Reader only indicates access denied
 - A) Is the card valid and entered into the access control system (see manufacturers user manual)?
 - B) Is the reader communicating with the reader service? Check the reader service log file (see manufacturer user manual)
- Reader not communicating with the reader service - Check that RS485 connections are correctly connected to 900M2000 Communications module.
- The contactless interface is not reading a card. - The card antennae may be damaged try the contactless interface if available

For other issues or questions contact Veridt customer service at 608-833-1840 or email: support@veridt.com.

Compliance Statements

FCC 15.105 FCC (US)

(a) For a Class A digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

Note: 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 ICES-003 Compliance CAN ICES-3 (A)/NMB-3(A)

FCC 15.19 FCC (US):

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.

IC (Canada):

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.

Cet appareil est conforme aux normes Industry Canada exemptes de licence RSS standard(s). Son fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas provoquer d'interférences et (2) cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable.

FCC 15.21

IMPORTANT! Changes or modifications not expressly approved by Veridt Inc could void the user's authority to operate the equipment.

IC (Canada):

IMPORTANT! Changes or modifications not expressly approved by Veridt Inc could void the user's authority to operate the equipment.

IMPORTANT ! Les changements ou modifications non approuvés expressément par Veridt, Inc pourrait annuler l'autorité de l'utilisateur à faire fonctionner l'équipement.

UL-294

The products listed in this Guide meet Standard UL 294 ED 8.

3.1.1 ACCESS CONTROL - The monitoring or control of traffic through portals of a protected area by identifying the requestor and approving entrance or exit.

Veridt's Stealth series readers are designed to be operated as a Class 1 Access control system component with no requirement to withstand a destructive attack. A Tamper Indicator switch is available to provide a supervisory indication to the PACS in the event the reader is removed from its installed location.

Veridt's Stealth series readers are designed to meet the requirements of the National Electrical Code for Class 2 systems and are intended to be used with UL294 listed control equipment.

The installation of these readers, and the materials used for installation, should be in accordance with the location requirements and the wiring methods defined by National Electrical Code (NFPA70) for Class 2 environments. Connect only to a Listed Access Control / Burglary power-limited power supply.

The connections of the reader pigtail to the wiring system must insure a thoroughly good physical connection without damaging the conductors and should be made by means of pressure connectors or pressure splices suitable for 18 to 26 gauge stranded copper wire.

Installation should be performed by qualified individuals who have the skills and knowledge related to the installation and operation of the equipment and have received the proper safety training to recognize and avoid any hazards that may be involved.

Stealth series readers are designed for an input power range of 11VDC to 13VDC. Operation above the maximum voltage of 13VDC may damage the reader, and operation below the minimum voltage of 11VDC may cause intermittent or complete loss of reader operation.

Stealth series readers are designed for use in a wide range of environmental conditions. Fingerprint Biometric readers should be mounted to protect the surface of the finger print sensor from accumulating water on its surface. A rain shroud may be required.

Stealth series readers have no user replaceable components. Any unit that does not operate properly must be returned to the factory for any service requirements

Stealth series readers require no periodic maintenance or calibration. If it becomes necessary to clean the outer surfaces, use a moist, non-abrasive cloth with a mild detergent and gently wipe the external surfaces. Do not immerse the reader.

RS-485 capability not verified to UL 294 by Intertek

CE STANDARDS

Stealth readers are designed to comply with EU regulatory requirements necessary to support the CE marking.

See the Stealth Users Guide for complete operation of all modes. Successful operation of the reader is indicated by the access control system granting access to a valid, registered card and denying access to an invalid or non-registered card.

Document Control - 269-2011

Date	Revisions	Description
March 11, 2025	Rev 05	Addition of Compliance Statements
December 24, 2024	Rev 04	Minor updates
December 2, 2024	Rev 03	Addition of Bio-Q other updates
November 14, 2024	Rev 02	Addition of Bio-Q other updates
June 14, 2021	Rev 01	Release
May 16, 2014	Rev 00	Original

Contact Information

Veridt, Inc.
7182 US Highway 14,
Ste 401
Middleton, WI 53562
Tel: 608-833-1840
FAX 608 833-1806
www.veridt.com