



VeriProx / VeriFlex / V-PASS / V-Smart

OPERATIONS MANUAL

Notices

The Veri-Series line of products has been tested for compliance with all applicable international standards. The resulting approvals are listed below, and are additionally printed on the labeling located on the rear panel of the product.

The power supply offered by Bioscrypt is CE and CSA approved and UL listed.

Veriflex	FCC, UL, ULC, CE
Veriprox	FCC, UL, ULC, CE
V-Pass	FCC, UL, ULC, CE
V-Smart	FCC, UL, ULC, CE

FCC Information to Users

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.

Warning to Users

Warning: Changes or modifications not expressly approved by Bioscrypt Inc. could void the user's authority to operate the equipment.

V-Smart, A Information for Users

The V-Smart, A includes a contact-less smart card reader (GemEasyLink680SL). This is a radio-transceiver with the following characteristics:

Operating Frequency Range:	13.553-13.567 MHz
RF Power Rating:	0.0 Watts
RF Output Impedance:	50 Ohms

V-Prox, A, H Information for Users

The V-Prox, A, H includes a HID contact-less proximity reader. This device has the following characteristics:

Transmit Frequency:	125 KHz
Excite Frequency:	125 KHz

Disclaimer

The instructions in this document have been carefully checked for accuracy and are presumed to be reliable. Bioscript, Inc. and its writers assume no responsibility for inaccuracies and reserve the right to modify and revise this document without notice. It is always our goal at Bioscript, Inc. to supply accurate and reliable documentation. If you discover a discrepancy in this document, please e-mail your comments to support@bioscript.com, or contact Bioscript Technical Support at the telephone number listed below.

No part of this publication may be placed in a retrieval system, transmitted, or reproduced in any way, including, but not limited to, photograph, photocopy, computer disk or other record, without prior agreement and written permission from:

Bioscript Inc.
5000 Van Nuys Blvd., Suite 300
Sherman Oaks, CA 91403
Phone (818).501.3908
Fax (818).461.0843
<http://www.bioscript.com>

Trademark Disclosures

Bioscrypt has made every effort to provide disclosures when using trademarks owned by other companies. Trademarked designations appear throughout this publication. The publisher states that it is using the designations only for editorial purposes, and to the benefit of the trademark owner with no intent to infringe upon that trademark. The following trademarks are found in this manual:

- Microsoft™, and Windows 95™, Windows 98™, Windows NT™, Windows 2000™, and Windows XP™ are trademarks of the Microsoft Corporation.
- VeriProx ®, VeriFlex ®, V-PASS ®, V-Smart ®, MV1100 ®, MV1200 ® are registered trademarks of Bioscrypt, Inc.
- HID™ is a trademark of the HID Corporation.
- Motorola™ Indala™ are trademarks of the Motorola Corporation.
- MIFARE™ is a trademark of Philips Electronics N.V.

Bioscript Warranty Policy

Bioscript, Inc. warrants its products to be free from defects caused by faulty materials or poor workmanship for a period of one year from date of shipment from Bioscript. Bioscript makes no warranty that its products are fit for the use or purpose to which they may be put by the buyer, whether or not such use or purpose has been disclosed to Bioscript in specifications or drawings previously or subsequently provided, or whether or not Bioscript's products are specifically designed and/or manufactured for buyer's use or purpose.

Bioscript's liability is limited to replacing, repairing or issuing credit, at its option, for any products that are returned by the original purchaser during the warranty period. Bioscript's liability on any claim for loss or damage arising out of the sale, resale or use of any of its products shall in no event exceed the selling price of the products. The buyer is responsible for making any claims for shipment damage (evident or concealed) with the carrier. Bioscript must be notified within 30 days of shipment of incorrect materials.

This warranty is voided if any component, subsystem, or element of the product(s) has been subject to electrical or physical abuse, tampering (such as opening a sealed housing or removal of a product serial number tag), or improper operation as determined by Bioscript. This warranty is also voided for failure to comply with Bioscript's return procedures as given in the Bioscript Technical Support Guide. Any service provided by unauthorized personnel voids the warranty.

Bioscript offers three (3) options to our customers that have a problem with one of our products.

- 1) Warranty Service if the unit is covered under either the factory one-year warranty period or any extended warranty the buyer may have purchased.
- 2) Fee-based Service if the unit is not covered under a warranty.
- 3) Return for credit if less than 30 days from the original date of shipment.

Service can be provided by Bioscript, the manufacturer.

Service can be provided by Authorized Service Representatives – contact Bioscript or visit our web site (<http://www.bioscript.com>) for a service representative near you. No service can be performed without first notifying Bioscript.

Service can be provided by Authorized Repair Center – contact Bioscript or visit our web site (<http://www.bioscript.com>) for a repair center near you. No service can be performed without first notifying Bioscript.

Any service provided by unauthorized personnel voids the warranty. No product may be returned, whether in warranty or out-of-warranty, without first obtaining approval from Bioscript. No credit will be given nor repairs made for products returned without such approval as described in the Returned Merchandise Authorization procedure as given in the Bioscript Technical Support Guide. Products must be returned, prepaid, to a Bioscript service center (no C.O.D. or Collect Freight shipments will be accepted). The

status of any product returned later than 30 days after the issuance of a return authorization will be subject to review. After Bioscrypt's examination, warranty or out-of-warranty status will be determined. If, upon Bioscrypt's examination, a warranted defect exists, the product(s) will be repaired at no charge and shipped, prepaid, back to the buyer. If the buyer desires an airfreight or other expedited return, the product(s) will be shipped collect, charged to the buyer's account with airfreight carrier, or charged to the buyer's account with Bioscrypt. Warranty repairs do not extend the warranty period. Repair work is warranted for 90 days from the date of shipment. Replacement components are warranted for one year from the date of shipment. Returned product(s), whether warranty or out-of-warranty, diagnosed as "No Problem Found" will be subject to a \$150 handling charge and will be returned as is, at the buyer's expense.

Privacy Statement

Bioscrypt's unique approach to fingerprint recognition provides the maximum in user privacy protection. Instead of storing a graphic representation of the user's finger (i.e., a picture), the VeriSeries products store a template, which is a highly processed mathematical model of the ridge pattern. This means that no direct personal data about the user is stored by the system.

Table of Contents

Notices	1
FCC Information to Users.....	1
Warning to Users.....	1
V-Smart, A Information for Users.....	1
V-Prox, A, H Information for Users.....	2
Disclaimer.....	2
Trademark Disclosures	3
Bioscrypt Warranty Policy.....	4
Privacy Statement.....	5
Introduction.....	10
Terminology.....	11
About Veri-Series Products.....	12
About the VeriProx.....	12
About the VeriFlex.....	12
About the V-PASS.....	12
About the V-Smart.....	13
Veri-Series – Physical Layout.....	14
Concepts of Operations.....	16
The VeriProx.....	16
The VeriFlex.....	18
The V-PASS.....	20
The Proximity Card.....	21
User Cards	21
Command Cards	21
Basic System Administration.....	22
Enrollment	22
Templates.....	22
Multiple Readers	23
Backing-Up Templates.....	23
Lights.....	24
VeriAdmin Management Software	25
Concepts of Operation.....	26
Transmit ID.....	26
Ports	26
Serial Port Settings and Baud Rates	26
Installing the Software	28
Setting up the ID File	29
ID File Format	29
Communication Settings file	30
Setting up a Network.....	31
Icons, Commands and Drop Downs	33
Template Manager.....	36
Edit Templates.....	37
QUICK Enrollment	38
Delete Templates.....	39
Verify Template.....	40
Transfer Templates	40
Download from Unit to PC.....	40

Download from Unit to Smart Card	41
Upload from PC to Unit	42
Upload from PC to Smart Card.....	43
Broadcast PC Template	44
Edit PC Template.....	46
Command Card Manager (VeriProx / VeriFlex).....	47
Administering Command Cards	47
Creating Command Cards.....	47
Reviewing Command Cards	47
Removing Command Cards	48
Using Command Cards	48
Enroll Command Card	48
Delete Command Card	49
Communication Settings.....	50
Unit Parameter Settings.....	51
Network Identification Number	53
Global Security Threshold	53
Setting the Security Threshold.....	53
MV1200 VeriSeries Port MODE.....	54
Host Port Protocol.....	54
Host Port and Aux Port Baud Rates	54
Quick COMM Test	55
Biometric Verification	55
Finger Detect (V-PASS only!).....	55
Wiegand Settings.....	55
Wiegand FORMAT.....	55
FailString Out.....	55
Alt Site Code.....	55
On Fail Send Inverse Parity	56
Enable INPUT.....	56
Enable OUTPUT.....	56
ALWAYS OUTPUT.....	56
Pulse Width	56
Pulse Interval	56
Wiegand PASS-THRU formats.....	56
Creating USER DEFINED PASS-THRU Format Options	58
AUX PORT SECURITY	60
Broadcast Parameters	61
Network Status.....	62
Advanced Enrollment.....	64
LED Table Settings	71
Sensor Configuration.....	72
Update Firmware	73
Restore Factory Defaults.....	74
Template Conversion	76
Verification Action Response	78
Wiegand Utilities.....	79
Getting Service and Support.....	80
Technical Support.....	80
Customer Service and Sales Support	80

World Wide Web Site	80
Appendix A – Quality and Content	81
Section A.1 - Basic Biometric Concepts	81
Biometric Definitions.....	81
Scanning an Image.....	82
Storing User Templates on the Unit.....	82
Section A.2 - Proper Finger Placement.....	83
Common mistakes.....	83
Image quality	83
Image consistency.....	84
Section A.3 - Using Content and Quality during Enrollments	85
False Acceptance and False Rejection	85
Quality.....	86
Content.....	87
Content and Quality Summary.....	88
Recommended Enrollment Process.....	88
Appendix B – Understanding the BROADCAST option in RS-485 Based Networks	89
Appendix C – V-PASS Template Differences.....	90
Appendix D – V-Smart Operations.....	92
Administrator's Note.....	92
V-Smart Terminology.....	93
V-Smart Smart Card Placement.....	94
Section D.1 – HOST Mode versus SLAVE Mode Operation	95
Section D.2 – Transferring a Template to a Smart Card	96
Section D.3 – Enrolling a Template Directly to a Smart Card.....	97
Section D.4 – Using the Smart Card Manager.....	98
Best Performance Practices / Finger placement	105
Appendix E – V-Smart Administrator SiteKey Management	106
What is a SiteKey?	106
Why do I Need a SiteKey?.....	106
What is the “Default” SiteKey?	107
Where is the SiteKey Stored?	107
What is the Difference Between PRIMARY and SECONDARY SiteKeys?	107
How do I Initially Set a SiteKey for V-Smarts at My Installation?	108
How do I Set the SiteKey on Individual Smart Cards?.....	110
How do I Change the SiteKey if I Already Have a User Base of Previously Created V-Smart Smart Cards?	111
What Happens if I FORGET My SiteKey?.....	112
What Happens if Someone Else Learns My Installation's SiteKey?.....	112
What is the 1-Way Hashing Function Option In VeriAdmin for SiteKeys?	113
Bioscrypt Contact Information	114

Notes

Introduction

Bioscrypt, the leader in fingerprint identification and verification systems, presents the VeriProx Fingerprint Verification System. Technology by Bioscrypt has been applied in various unique applications including Access Security, Time and Attendance, Political Polling, Computer Logon, and other applications where an individual must be clearly identified as being solely responsible for specific actions.

Bioscrypt (formerly BiometricID) was founded in 1996 with a mission to provide fingerprint recognition technology with the highest degree of accuracy at a reasonable cost while still being easy to use. Bioscrypt has successfully migrated technology once found only in government or military applications, toward private industry and small businesses around the globe.

It has been known for years that each person has unique fingerprints. Using fingerprints as a means of identification ensures a unique identifier for each tracked user, and protects users from the vulnerabilities associated with lost keys or identification cards. After installing Bioscrypt's product in your application, your company will be able to accurately identify, track, and automatically act according to each individual's identification and permissions.

Terminology

This document is intended for use with Bioscrypt's **Veri-Series** products. This includes the **VeriProx**, **VeriFlex**, **V-PASS**, and **V-Smart** hardware products. Although differing in exact function, these 4 products share many common aspects. When this manual refers to the 'VeriProx', unless specifically stated otherwise, you can assume that the entire Veri-Series is being described.

This document also refers to Bioscrypt's **MV1100** and **MV1200**. The MV1100/MV1200 is the internal hardware biometric engine that is the core of all Veri-Series products. This circuit board contains the DSP processor, support hardware, and interface to a variety of fingerprint sensors. The MV1100/MV1200 also contains **firmware**. The firmware is the low level software that controls the mathematical instructions that perform the actual fingerprint enrollment and verification processes.

About Veri-Series Products

About the VeriProx

Bioscrypt's VeriProx combines patented fingerprint verification technology with an industry-standard proximity card reader in a mullion-mountable case. This ensures greater security for the card issuer and the card user. Requiring that the fingerprint of the person seeking entry matches the identity of the cardholder eliminates access via lost or stolen proximity cards. Suitable for both standalone and network use, the system works with existing 26-bit proximity card infrastructures.

The unit operates in conjunction with administration software hosted on a PC. Once installed users simply present their identification cards when entering the secure area and then touch a fingertip to the recessed area on top of the unit. The system validates their fingerprint against a previously enrolled template stored in flash memory.

The VeriProx system provides security features that can minimize fraud and can tolerate changes to the user's finger like scarring or swelling. The VeriProx returns accurate pass and fail decisions in 99.99% of all cases.

Each VeriProx unit stores thousands of fingerprint templates, in a non-volatile memory. Response time is less than five seconds for fingerprint enrollment and less than 1.5 seconds for fingerprint verification. The system is compact, versatile, and configured to allow standalone, PC-connected, and multiple-unit operation.

About the VeriFlex

Bioscrypt's VeriFlex includes all features found in the VeriProx **except** it does not include the internal proximity card reader. External connections to Wiegand devices still exist and allow the VeriFlex to be added to installations that already have supported Wiegand devices installed. Whereas the VeriProx can operate as a standalone device, the VeriFlex requires an external device (such as an external Wiegand reader or PC) that initiates enrollment, verification, and template administration activities.

About the V-PASS

Bioscrypt's V-PASS is similar in construction to the VeriFlex but incorporates an entirely different biometric algorithm. Whereas the VeriProx and VeriFlex will perform a *1:1 matching verification* where an ID number is required, the V-PASS performs a searching algorithm that will compare the user's fingerprint with every stored template to find a potential match. This ability removes the requirement of telling the unit the ID number to verify. With the V-PASS, the user simply places their finger on the sensor, and a PASS / FAIL is determined. No external or internal Wiegand input device is required. Once the fingerprints are enrolled on the unit, the V-PASS can operate in a standalone mode. A V-PASS can still be connected to Wiegand Input devices similar to a VeriFlex. If a recognized Wiegand signal is received identifying an ID number, the V-PASS will perform a simple 1:1 verification and not a searching operation. PLEASE NOTE: the V-PASS

fingerprint templates are different the smaller VeriProx and VeriFlex fingerprint templates. Please see Appendix C for further details.

About the V-Smart

Bioscrypt's V-Smart provides all the capability of the Veriflex and includes an internal smart card reader. Fingerprint templates are securely stored on a smart card rather than the reader and carried by the employee or user. This allows for an unlimited population of users. The smart card is presented to the V-Smart and the template is read from the smart card and verified against the employee's live image. Storing the template on the smart card allows the V-Smart to have an unlimited user base and removes the need for a physically-wired network. Wiegand communication formats of up to 64 bits can also be stored on the smart card and optionally used with a Wiegand device.

Veri-Series – Physical Layout

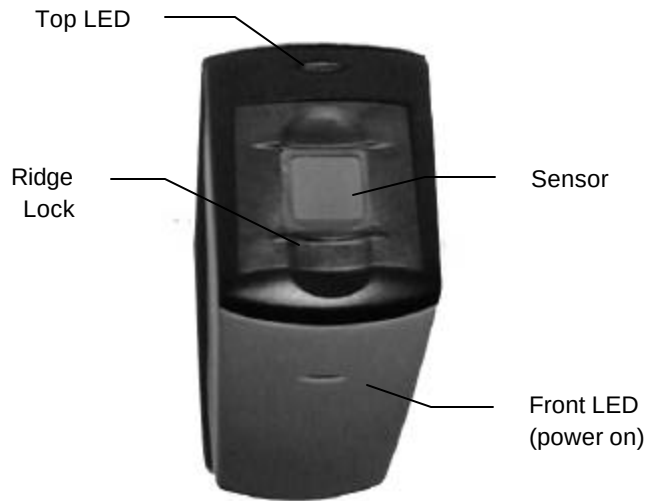


Figure 1: Top View

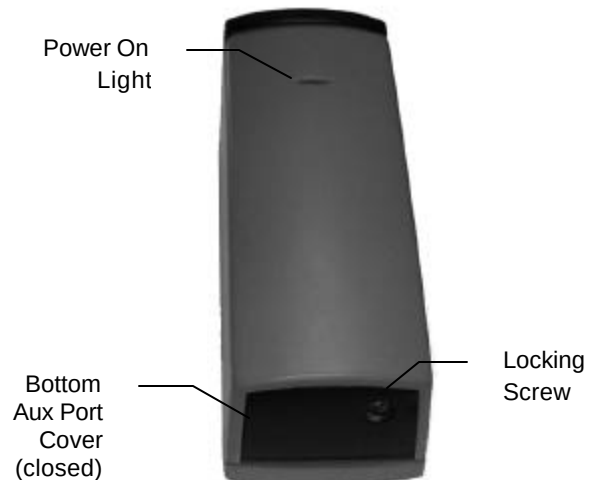


Figure 2: Bottom View

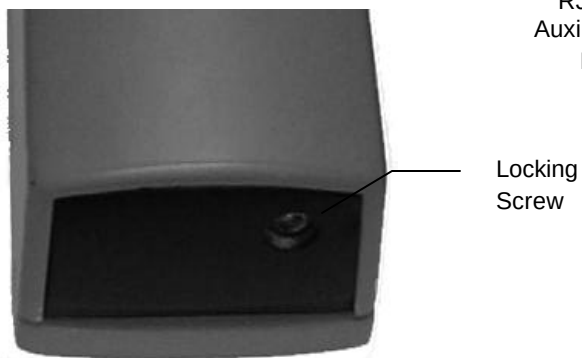


Figure 3: Bottom Panel – closed

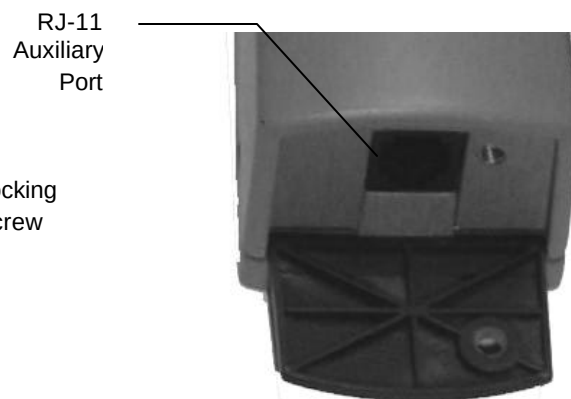


Figure 4: Bottom Panel – open

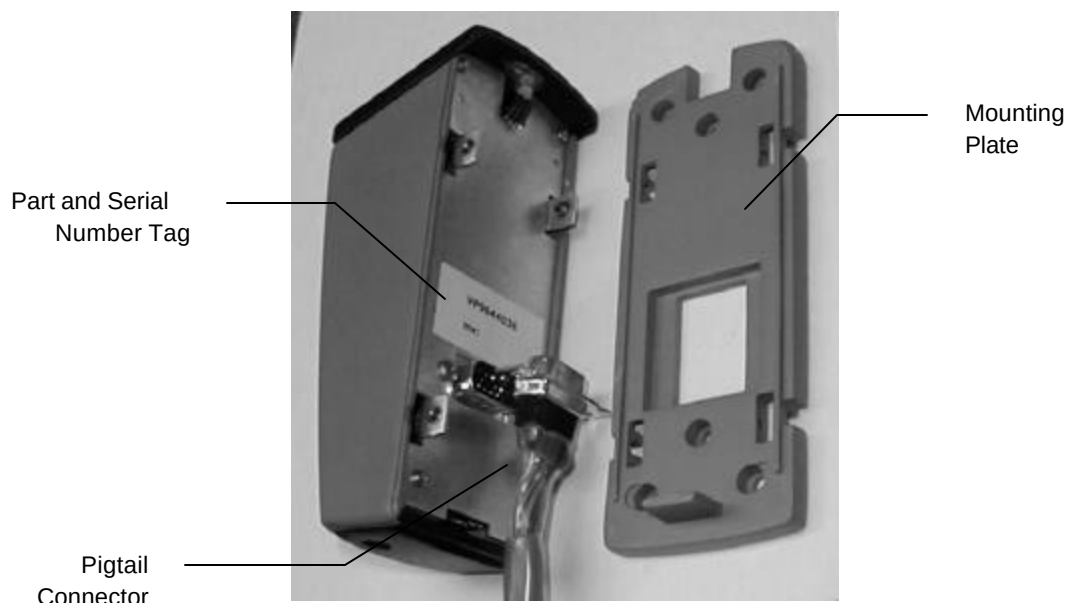


Figure 5: Veri-Series Unit and Mounting Plate

**For additional information on installing and connecting your Veri-Series unit,
please refer to the *VeriProx Installation Manual*.**

Concepts of Operations

The VeriProx

The VeriProx integrates an industry-standard proximity card reader with Bioscrypt's MV1100 fingerprint verification technology. A typical operation is described below.

- A user waves the proximity card near the front of the VeriProx.
- The ID number is read from the internal proximity card reader.
- The ID is transferred to the MV1100.
 - If the ID is invalid, the LED on the top of the VeriProx will glow red.
 - If the ID presents a valid previously enrolled template, the LED on the top of the reader will glow amber; indicating the user should place their finger on the sensor on the top of the reader.
- The User should place the correct finger on the scanner using the Bioscrypt Ridglock.
- The amber light will turn off, signaling the finger can be removed.
- The scanned image is compared with the data that is stored under the ID number in the memory of the VeriProx.
 - If the verification is positive, the top LED will glow green and the unit will emit an audible beep.
 - If the authentication fails, the LED will glow red and no beep will be generated.
- When authentication is successful a Wiegand string that contains the site code and ID number read from the proximity card is sent out for use by a standard door controller.
- Optionally, the VeriProx can be configured to send out a pre-determined "failure" ID whenever an unsuccessful verification occurs. An additional option allows the site code to be replaced with another number.

The VeriProx has several communication options. It is equipped with both a Host port and an auxiliary port. The Host port may be configured to operate in RS-232 mode or RS-485 mode. The auxiliary port is always set to RS-232. The Host port connections are made through the wiring pigtail on the back of the reader. The auxiliary port is accessed from an RJ-11 jack that is hidden under a door on the bottom of the VeriProx. This door is held shut with a security screw.

The VeriProx can be used as a stand-alone reader or multiple units can be configured on an RS-485 network. The manner in which you choose to install the VeriProx will determine which communications settings are most convenient for your configuration. Certain administrative functions are common to any installation. You must have a way to “enroll” users into the system, that is, you must be able to associate their fingerprint data with a specific proximity card ID number. You must have a way to distribute this user information to all other readers in your installation. The VeriAdmin Management Software is provided for this purpose.

The VeriFlex

The VeriFlex is similar to the VeriProx except that an external Wiegand device is used. A typical operation is described below.

- A user initiates the action with the external Wiegand device.
- The ID number is read from the external reader.
- The ID is transferred to the MV1100 inside the VeriFlex.
 - o If the ID is invalid, the LED on the top of the VeriFlex will glow red.
 - o If the ID presents a valid previously enrolled template, the LED on the top of the reader will glow amber; indicating the user should place their finger on the sensor on the top of the reader.
- The User should place the correct finger on the scanner using the Bioscrypt Ridglock.
- The amber light will turn off, signaling the finger can be removed.
- The scanned image is compared with the data that is stored under the ID number in the memory of the VeriFlex
 - o If the verification is positive, the top LED will glow green and the unit will emit an audible beep.
 - o If the authentication fails, the LED will glow red and no beep will be generated.
- When authentication is successful a Wiegand string that contains the site code and ID number read from the external Wiegand device is sent out for use by a standard door controller.
- Optionally, the VeriFlex can be configured to send out a pre-determined "failure" ID whenever an unsuccessful verification occurs. An additional option allows the site code to be replaced with another number.

The VeriFlex has several communication options. It is equipped with both a Host port and an auxiliary port. The Host port may be configured to operate in RS-232 mode or RS-485 mode. The auxiliary port is always set to RS-232. The Host port connections are made through the wiring pigtail on the back of the reader. The auxiliary port is accessed from an RJ-11 jack that is hidden under a door on the bottom of the VeriFlex. This door is held shut with a security screw.

The VeriFlex can be used as a stand-alone reader (with external Wiegand reader) or multiple units can be configured on an RS-485 network. The manner in which you choose to install the VeriFlex will determine which communications settings are most convenient for your configuration. Certain administrative functions are common to any installation. You must have a way to “enroll” users into the system, that is, you must be able to associate their fingerprint data with a specific Wiegand ID number. You must have a way to distribute this user information to all other readers in your installation. The VeriAdmin Management Software is provided for this purpose.

The V-PASS

The V-PASS is similar to the VeriProx and VeriFlex, but no Wiegand input device is required. The V-PASS will automatically detect when a finger is placed on the sensor, compare that fingerprint with all currently enrolled fingerprint templates and determine if there is a match. A typical operation is described below.

- The V-PASS top LED is yellow to indicate it is ready for a finger.
- A user initiates the action by placing their finger on the fingerprint sensor.
- The User should place the correct finger on the scanner using the Bioscrypt Ridglock.
- The V-PASS will recognize that a finger has been placed and will take an image of that finger's print.
- The amber light will turn off, signaling that the image has been scanned and the finger can be removed.
- The scanned image is compared with **ALL** enrolled templates in the memory of the V-PASS (maximum of 200).
 - o If the verification is positive, the top LED will glow green and the unit will emit an audible beep.
 - o If the authentication fails, the LED will glow red and no beep will be generated.
- When authentication is successful a Wiegand string can optionally be sent out for use by a standard door controller.

The V-PASS has several communication options. It is equipped with both a Host port and an auxiliary port. The Host port may be configured to operate in RS-232 mode or RS-485 mode. The auxiliary port is always set to RS-232. The Host port connections are made through the wiring pigtail on the back of the reader. The auxiliary port is accessed from an RJ-11 jack that is hidden under a door on the bottom of the V-PASS. This door is held shut with a security screw.

The V-PASS can be used as a stand-alone reader or multiple units can be configured on an RS-485 network. The manner in which you choose to install the V-PASS will determine which communications settings are most convenient for your configuration. Certain administrative functions are common to any installation. You must have a way to "enroll" users into the system, that is, you must be able to associate their fingerprint data with a specific Wiegand ID number. You must have a way to distribute this user information to all other readers in your installation. The VeriAdmin Management Software is provided for this purpose.

The Proximity Card

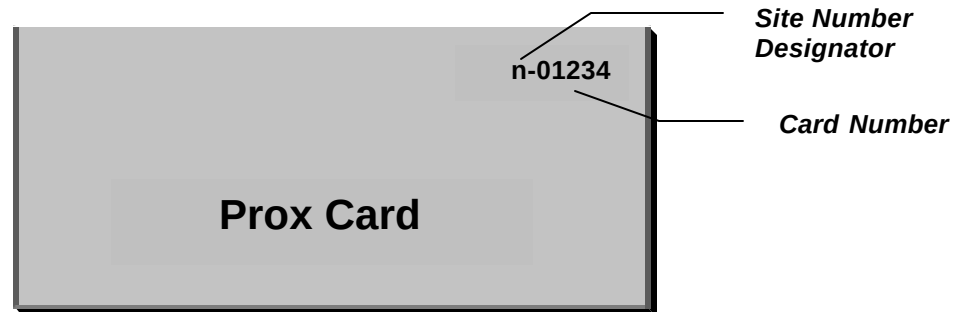


Figure 6: Veri-Series Card

There are three types of proximity cards split into two basic categories:

- User Cards
- Enroll Command Cards
- Delete Command Cards

User Cards

The VeriProx / VeriFlex can be programmed to use a given card ID number as a standard "user card". The majority of your cards will be of this type.

Command Cards

Command Cards can be created to add and remove users from a VeriProx / VeriFlex reader without using the PC based Administrative Software. These can be useful for creating and removing temporary visitor's badges or administering the system when your PC is down or unavailable. There are two types of Command Cards associated with the VeriProx / VeriFlex:

- Enroll Command Cards
- Delete Command Cards

Note: The command cards must be created using the Administration Software.

Once a card has been designated as one of the three types, it will remain that type unless it is deleted and re-enrolled (see Edit Templates on page 37).

Basic System Administration

Enrollment

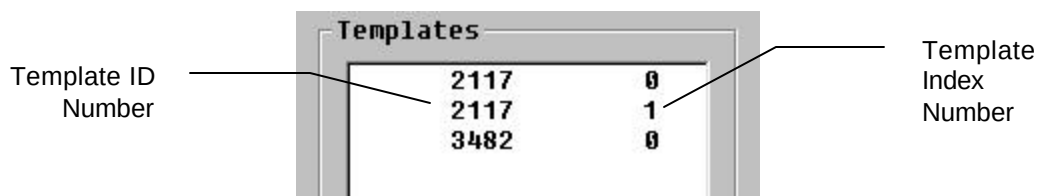
New users are entered into the system through the process of “enrollment”. This procedure scans the users fingerprint and produces a fingerprint template, a collection of data that is stored in memory on the Veri-Series product. This includes:

- User Name
- User Finger Identifier
- Template Security Threshold
- Template ID
- Template Index Number
- A mathematical model of the fingerprint ridge pattern

Templates

Every template on a Veri-Series unit has a unique identification tag consisting of a Template ID and a Template Index. Each time a fingerprint is enrolled a new template is generated using the number from the proximity card or PC as the Template ID number. Unless specifically defined, the Veri-Series product will automatically assign a unique index value to each template.

NOTE: The Template Index number will be the lowest value available for that ID number unless specially defined using an external PC application to define a specific Index.



Templates	
2117	0
2117	1
3482	0

Figure 7: Template ID Numbers

Please see Appendix A – Quality and Content for a technical description of what constitutes a good enrollment. A quality enrollment will ensure peak performance from the Bioscrypt fingerprint recognition algorithm.

Multiple Readers

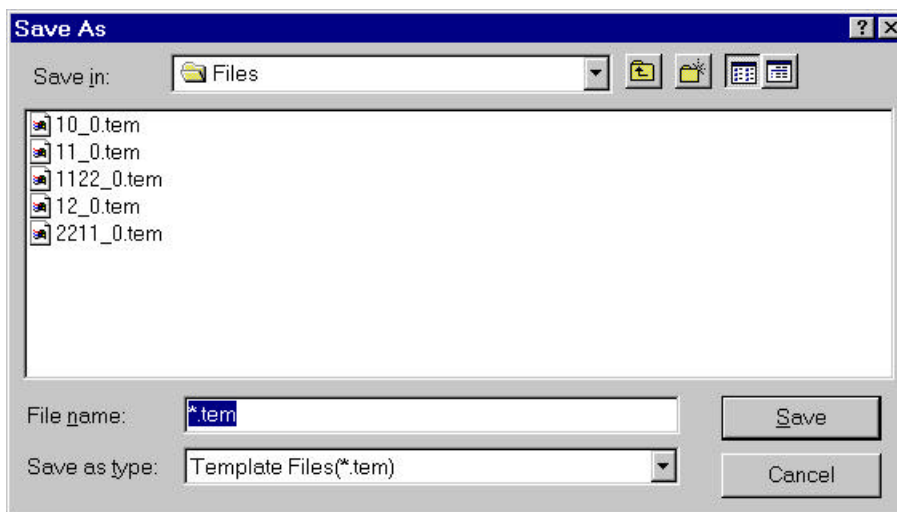
If your installation includes multiple Veri-Series readers that are used by a common population of users, you will need to distribute the fingerprint template of each user to all the readers.

Note: It is recommended that you designate one Bioscrypt Unit as the “administration reader” and enroll all new users on this unit.

After a new user is enrolled on the administration unit, the template can be copied to the other readers. If the units are networked, you can broadcast the new template to the other readers over the RS-485 lines using the VeriAdmin Management Software. If the readers are not interconnected, a laptop can be used to download the templates from the administration reader and then uploaded to each reader through its Aux Port.

Backing-Up Templates

Templates can be “backed-up” by downloading them to a PC. On the PC, template files are of the type “.tem” for 1:1 verification templates used with the VeriProx / VeriFlex / V-Smart and “.mtm.” for the larger searching templates used with a V-PASS (see Appendix C). The name of the file is derived from the Template ID Number and the Template Index Number. For example, the first file (1_4.tem) in Figure 8 below is of Template ID 1 and Template Index 4 (referred to as Template



1 4).

Figure 8: Template files on the PC

NOTE: when the template is uploaded from the PC to a Veri-Series reader, the Template ID Number and Index Number is taken from data within the file, not from the file name. Therefore, even if you change the name of the file on your PC, the

Template ID and index will remain the same. Please use the VeriAdmin Management Software to modify Template ID numbers.

Lights



The LED on top of the unit can illuminate in different colors and patterns.

Figure 9: Top LED

<i>Steady Amber</i>	the unit is requesting that a finger be placed on the sensor. This may be for verification or for enrollment. The user may remove the finger when the light goes out.
<i>Blinking Amber</i>	the unit is requesting a proximity card be waved for enrollment into the reader. The blinking amber light is seen when an Enroll Command Card is used to add a new user to the reader.
<i>Steady Green</i>	the unit is indicating the successful completion of one of the following operations: • Verification • Enrollment • Deletion A steady green light is accompanied by an audible beep.
<i>Steady Red</i>	the unit is indicating the current operation has failed.
<i>Blinking Red</i>	the unit is requesting a proximity card be waved. The card ID number will be deleted from the reader. The blinking red light is seen when a Delete Command Card is used to remove an existing ID from the reader.

VeriAdmin Management Software

The VeriAdmin Management Software is designed to run on Windows-based PC platforms and communicate with Bioscrypt's MV1100 and MV1200 based fingerprint recognition devices. Although oriented more towards the **Veri-Series** products, the application works well with any MV1100/MV1200-based device. In this documentation, the terms "unit" and "reader" are used as a generic term to refer to any MV1100/MV1200-based device. At this time, the VeriAdmin Management Software does NOT communicate with Bioscrypt's V2100 fingerprint recognition terminal.

Use the VeriAdmin Management software to perform the following functions:

- Enroll new user fingerprint templates.
- Edit user templates.
- Distribute the user templates from the administration reader or PC to other Bioscrypt readers in the installation.
- Create "command cards"; proximity cards with the privilege to enroll or delete other user cards when the unit is used in conjunction with a Proximity Reader as in VeriProx.
- Adjust the parameters (baud rate, security level, port configuration, Wiegand settings, etc) of individual units, or of all readers connected on an RS-485 network.
- Configure the layout and operation of Smart Cards (for V-Smart only)

NOTE: The recommended operating system for use with the VeriAdmin Management Software is Windows 2000™, Windows XP™, or Windows NT™ 4.0 (Service Pack 3 or greater). Operation is possible on Windows 98™ or ME™, however occasional communication packets can be dropped when multiple applications are running in the background. It is also possible to run the software on Windows 95™, however, this is not recommended due to communications irregularities in that version.

Concepts of Operation

Transmit ID

On the tool bar of the Administration Software, there is a drop-down list titled *Transmit ID* (see Figure 10 below). The ID number that appears in the field is the reader with which the software currently is communicating. For this reason, each reader must be assigned a Network ID, even if your installation consists of a single unit (the default setting is 0).



Figure 10: Transmit ID Drop-down

A special transmit ID number, “-1”, is assigned as a broadcast ID. All units on the current COMM Port will respond to this broadcast ID. For functions labeled “broadcast” the software uses the broadcast ID and all readers on the network will accept these commands. Using Broadcast commands is only recommended for advanced users. (See Appendix B for further understanding of the benefits and issues with Broadcasting commands.)

If the transmit ID is set to a number that is not assigned to any unit on the network, the software will report that there is no communication.

If two units on the network have the same ID assigned, there also will be communication problems, since both units would respond to commands sent to that ID. This causes the information packets to “collide” and become jumbled, resulting in communication errors.

Ports

Bioscrypt readers “talk” to the VeriAdmin Software using either the Host or Auxiliary (AUX) port. The Host port may be configured to use RS-232 or RS-485 protocol. The Host port is connected through the pigtail-wiring bundle at the back of the unit. Different wires are used for RS-485 versus RS-232. The Aux port is accessed using the RJ11 jack at the bottom of the VeriProx. Please refer to the *VeriSeries Installation Guide* (included on the Bioscrypt CD) for details.

Serial Port Settings and Baud Rates

Once the reader(s) have been connected to the PC, the next step is to identify which ports on the PC are talking with which readers.

As usual, the serial ports on the host PC are designated as COM1, COM2, etc. You may connect up to 31 Veri-Series readers to each COM line (using RS-485). You must provide the Administration Software with the information as to which Network ID has been assigned to which COM line.

This information is stored in an initialization file that is read by the software on application startup. The file is labeled "UNITIDS.DAT" and is located at the following path:

<Install Dir>\UNITIDS.DAT

Where <Install Dir> indicates the directory where the VeriAdmin Management Software was installed). The default installation path is:

C:\Program Files\BioID\VeriAdmin

Please refer to the Setting up the ID File section on page 29 for details.

In addition the baud rate may be set on each reader. It is essential that the baud rate used by the PC match the baud rate setting on the reader and that all readers on the network are set to the same baud rate.

The following settings are the factory defaults:

A **VeriProx/VeriFlex/V-PASS** should arrive with these settings in place:

Network ID:	0
Port Mode:	Mode 1 (Host RS-485 / Aux RS-232 (RJ11))
Host Port baud rate:	9600 baud
Aux Port baud rate:	57600 baud

A **V-Smart** should arrive with these settings in place:

Network ID:	0
Port Mode:	Mode 0 (Host RS-232 / Aux RS-232 (RJ11))
Host Port baud rate:	57600 baud
Aux Port baud rate:	57600 baud

Installing the Software

To install the software, run the **setup.exe** file on the VeriAdmin Management CD. You may accept the default path or choose an alternate directory in which to install the software. The default path is:

C:\Program Files\BioID\VeriAdmin

Like most Windows based installations, you will step through a number of windows (approximately 5) that will request basic installation information, such as, file name and directory location. It is recommended that the default settings are used, however, they can be changed.

Once the installation is complete, a short-cut icon for the Administration Software will appear on your desktop.



Setting up the ID File

Once you have installed the software on your PC, you will need to set up a communications port ID file. The software will use the information in this file to communicate with the VeriSeries reader(s) connected to the Host Port.

You can create and edit the file using the any standard Text Editor program provided with Microsoft Windows.

Access the file, UNITIDS.DAT located in the Install Directory. The default path is:

C:\Program Files\BioID\VeriProx\UNITIDS.DAT

ID File Format

The file format is as follows:

Line 1: Name the COMM port on the PC

Line 2: List the IDs for all units on this port. Identify V-PASS units by appending a “:M” to the corresponding ID. Separate each ID by a space.

Line 3: Type a % to end the COMM port.

Example:

```
COM#: 1
UNITIDS: 0 1 2:M 3 4:M 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
23 24 25 26 27 28 29 30
%
COM#: 2
UNITIDS: 31 32:M 33
%
```

Notice how the line for the Unit IDs for COMM 1 wraps; the software will continue to read the line until the %. A space should appear between each reader ID number and after the keywords “COM#:” and “UNITIDS:”. In the example above, IDs #2, #4 and #32 are designated as V-PASS units. ***It is important to designate V-PASS units appropriately to assist the VeriAdmin software in proper template management. Also, if this is not done, a “mismatch” message will appear when a network status is performed.***

Once you have completed editing the file, save it under the same name and to the same location.

Note: The VeriAdmin Software will first look for this file in the current directory. If not found, the software will then look in the Install Directory for this file.

The default UNITIDS.DAT file looks like this:

```
COM#: 1
UNITIDS: 0 1 2 3 4 5 6 7 8 9
%
```

Thus the software will initialize expecting to find 10 readers on the host port with assigned ID numbers of "0" through "9". There should be no communication problems if there are other readers on the network as long as each reader is configured correctly and with a unique ID number.

Communication Settings file

There is a second initialization file that is used by the Administrative Software. This is the **CommParameters.cfg** file. The program automatically writes this file when it is closed. The next time the program is opened, this file is read and the communication parameters are set to match their state when the program was last shut down.

The first time you run the VeriAdmin Management software this file does not exist. You will see the following dialog appear. Fill out the desired Transmit ID, Comm Port, and Baud Rate. Press the TEST button to verify these settings are correct, and then press ACCEPT and the initial CommParameters.cfg file will be created.

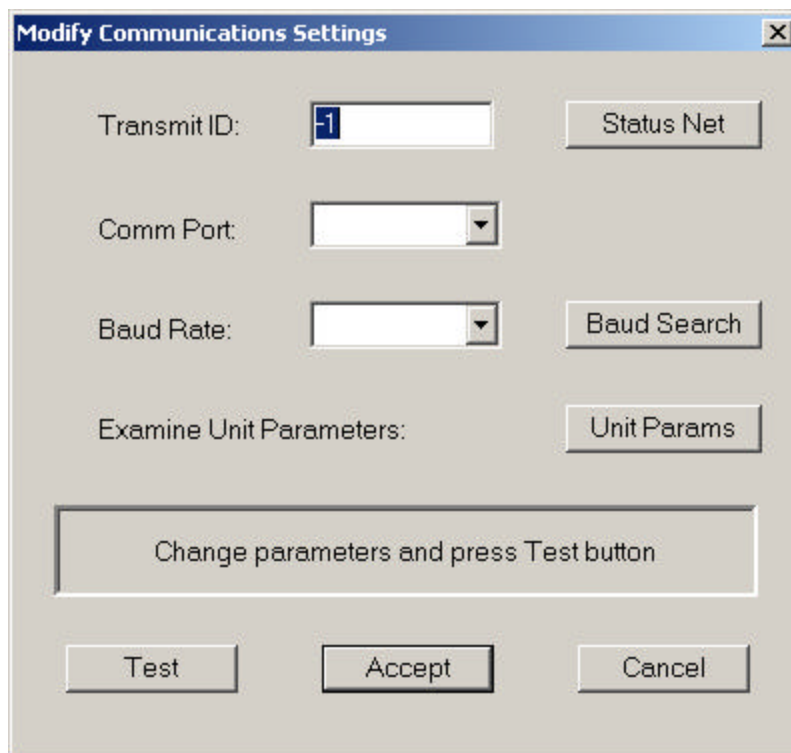


Figure 11: Modify Communications Settings

Setting up a Network

As described above, when setting up a network you will need to assign unique ID numbers to each Veri-Series reader and confirm the communication settings. The easiest way to do this is to cycle through each reader, setting the parameters by plugging into the Aux port. When using the Aux port you can set the transmit ID to -1 (broadcast). Since you are plugged into only one reader, you are assured that no other Veri-Series units will be responding to your commands. If the ID on the unit has been changed from its default you can still be confident it will respond to the Broadcast ID. After you set the parameters for each unit through the Aux Port you can connect them to your 485 network. To review, the recommended steps are:

- 1 Supply power to the proper wires in the pigtail on the back of the Veri-Series unit (Consult the Installation Manual for a wiring diagram).
When power is applied, the front LED will glow green, and the top LED will blink amber, then turn OFF for VeriProx/VeriFlex/V-Smart or remain ON for V-PASS units.
- 2 Plug into the Aux Port using the RJ-11 jack on the bottom of the unit and connect the cable to one of the serial ports on your PC
- 3 Access the **Communication Settings** window by clicking on the icon or using the menu.
- 5 Click the Modify button.
Set the Transmit ID to -1. Set the COMM Port setting to match the designation for the port you are using on the PC (e.g. COM1, COM2)
- 6 Set the baud rate setting to 9600 baud (the factory default).
- 7 Press the test button.
- 8 If necessary, use the Baud Search button to have the software test different baud rate settings and report which baud setting works. (For this function to succeed a valid transmit ID and valid COMM port must be set.
- 9 Click the Accept button to change the settings.
- 10 You can now set Network ID on the reader. Click the **UNIT PARAMS** button on the Modify Communications Settings dialog.
- 11 Type the desired ID number in the *Assign Unit Network ID* field. Press the "Set" button to make the change. Note this will change the ID in flash on the reader and will also modify the transmit ID that is being used by the PC so that you may continue to communicate without using the broadcast ID. The lower portion of this dialog box shows the current communication settings.

- 12 Select the appropriate baud rate from the *Host Port Baud Rate* drop down list (9600 is recommended). Keep in mind that you are currently talking over the AUX port, but you are changing the Host Port settings that will be used when you connect to the unit through the Host Port wires on the back of the unit.
- 13 Set the *Host Port Protocol* to RS-485 if you will be using a networked environment. Alternatively you may choose RS-232 if you will not be networking the VeriProx. Remember that the RS-232 and RS-485 connections are made through different wires on the pigtail. (Consult the installation guide).

Make sure that the Network IDs in the UNITIDS.DAT file match those assigned to the readers. If not, update accordingly.

Icons, Commands and Drop Downs



Figure 122: VeriAdmin Toolbar

Once you have the software installed and running, you will be able to access the features mentioned above either through the icons on the toolbar or through the command menus.

Template Manager (page 36)

Icon



Command Path

File > Template Manager

Command Card Manager (page 47)

Icon



Command Path

File > Command Card Manager

Smart Card Manager (page 98)

Icon



Command Path

File > Smart Card Manager

Communication Settings (page 50)

Icon



Command Path

Configure > Communication Settings

Unit Parameters (page 51)

Icon



Command Path

Configure > Unit Parameters

Broadcast Parameters (page 61)

Icon



Command Path

Configure > Broadcast Parameters

Network Status (page 62)

Icon



Command Path

File > Network Status

Advanced Enrollment (page 64)

Icon



Command Path

Configure > Advanced Enrollment

Quick Enrollment (page 38)

Icon



Command Path

Configure > Quick Enrollment

Transmit ID

Drop Down



The Transmit ID number refers to the IDs given to individual Veri-Series units. Whichever number appears in the box is the unit with which the software is communicating. If you have networked more than one unit, you can use the Transmit ID drop down box to access a specific unit by its ID number.

The ID numbers show in the drop down list come from the "UNITIDS.DAT" file described in the ID File Format section.

Current Communication Settings

Current ID: 5 – COMM Port: 4

The current Network ID and COMM Port are displayed here. These values will update as different communication and different settings are used throughout the VeriAdmin Management Software.

Template Manager

The Template Manager allows you to:

- Edit Templates
- Enroll Templates
- Delete Templates
- Verify Templates
- Transfer templates to and from a PC, from one unit to another, or to a Smart Card
- Edit Templates Stored on the PC
- Verify Templates Stored on the PC
- Broadcast a Template from the PC to ALL units identified in the UNITIDS.DAT file

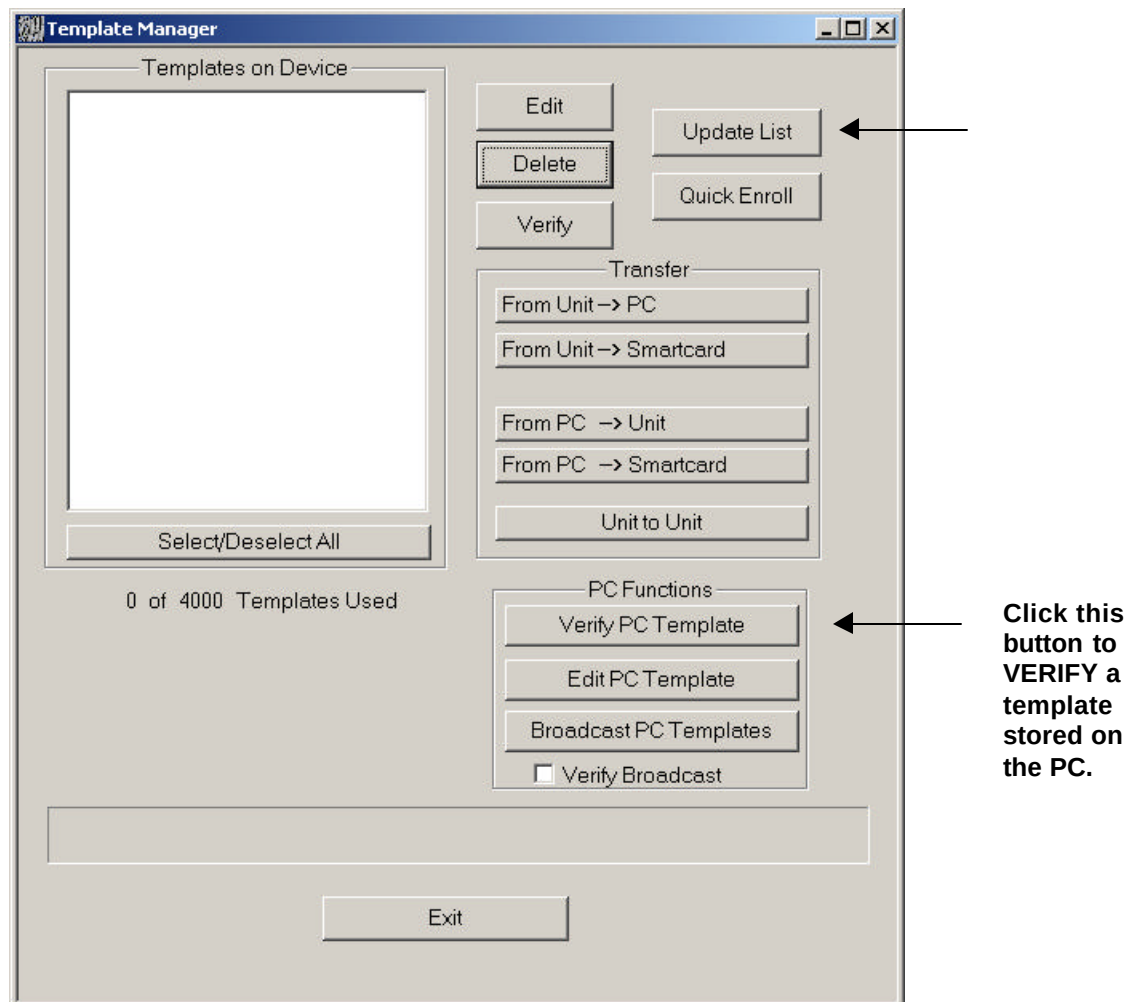


Figure 13: Template Manager

Edit Templates

To edit a template, select the appropriate ID number(s) in the *Templates* window and click the Edit button. Alternatively, you make double-click on the ID number in the window and an Edit box will open.

Note: While you can use the Shift and Ctrl keys to select multiple templates, realize that a separate window will open for each template you select.

A window like the one below will open.

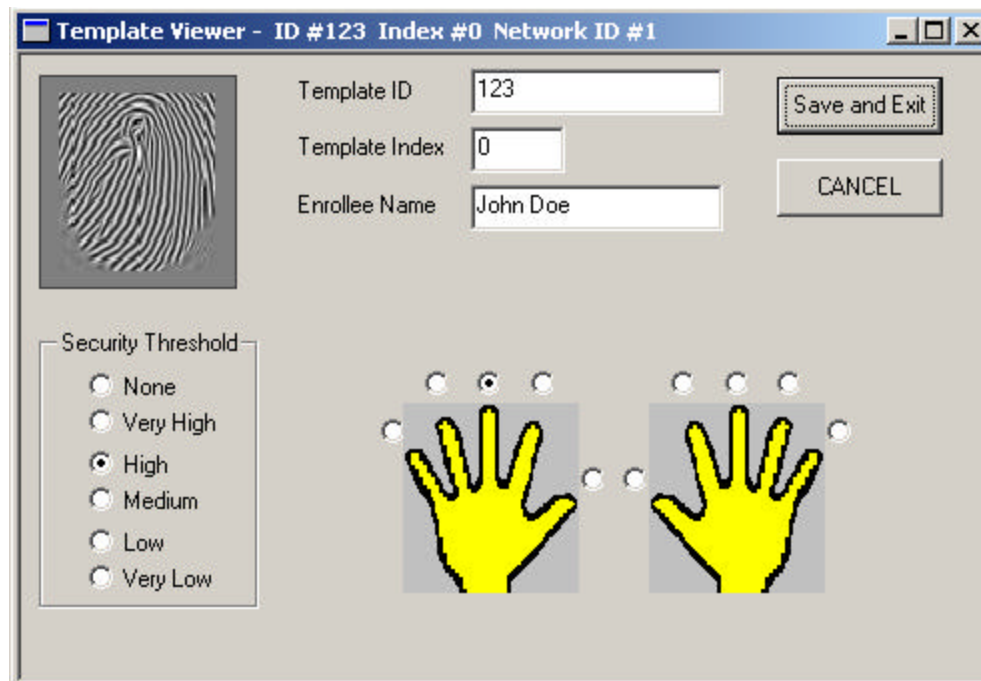


Figure 14: Template Viewer

From here you can view and edit the attributes of the template such as the Employee Name and Security Threshold. You can then save the template to the Current Unit specified by the current communication settings.

QUICK Enrollment

When you select the Quick Enroll button on the Template Manager window, the following window will appear:

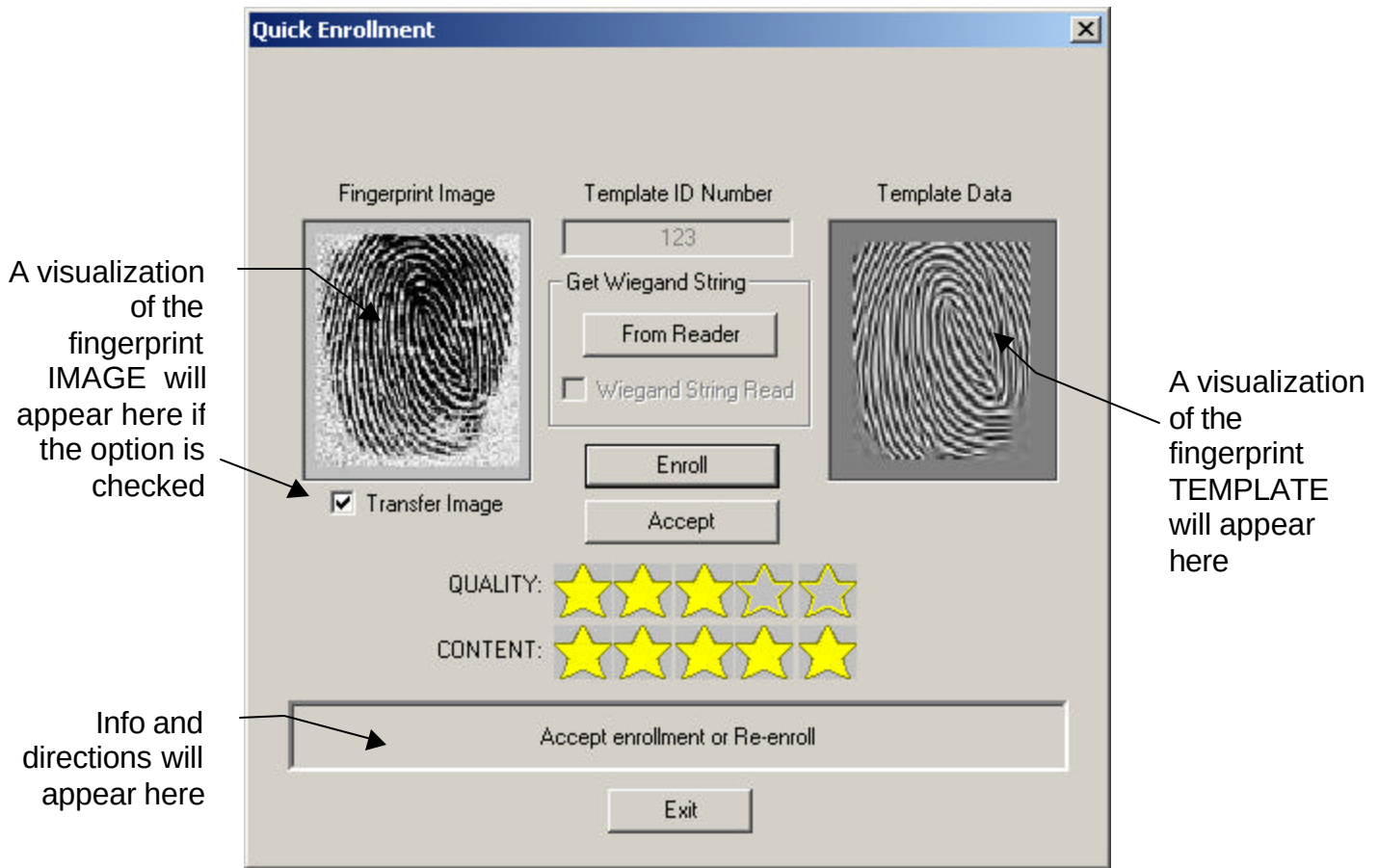


Figure 13: Quick Enrollment Screen

The process to enroll a new template is as follows:

- 1 In the *Template ID Number* field, type the desired ID number (for VeriProx, VeriFlex, and readers wired to a proximity reader or Wiegand input device, use the proximity card. Do **not** include a site code designation). **OR** Press the "From Reader" button (although the Wiegand ID can come from sources other than a prox reader) and wave the card in front of the Wiegand INPUT device to read the ID directly from the card

Note: If you are using a V-Smart and have selected Read/Write Wiegand String during Enroll/Verify from the Smart Card Manager, VeriAdmin will expect to receive the Wiegand String from the reader and will warn you if none was provided.

- 2 Click the Enroll button.
The light on the VeriProx will glow amber requesting the enrollee to place a finger on the sensor. Nestle the Ridglock into the first joint line on the finger. The finger may be removed when the amber light goes out and VeriAdmin instructs you to remove the finger.
- 3 The light will glow green and the unit will beep once to acknowledge that the fingerprint has been captured.
If a finger is not placed within ten seconds, the light will glow red and the unit will time out. Similarly the light will glow red if the unit was unable to image the fingerprint. (See the appendix for a discussion of proper enrollment).
- 4 On the Quick Enrollment screen, the *Quantity* and *Content* fields each will display from one to five stars indicating how well the print was read. In addition, a sample of the print will appear in the left center of the screen.
A rating of at least three stars in each field is recommended.
- 5 If you are unsatisfied with the read, repeat steps 3 and 4 above.
- 6 Press the Accept button to continue with the enrollment.
At this point, the Edit Template window will open (see page 37). Complete the *Username* field, identify the finger that was scanned, and select a *Security Threshold*. You may change the index if you are enrolling more than one finger under the same ID, but normally this should be zero.
- 7 Select the user type. This is either *User ID*, *Enroll ID*, or *Delete ID* depending on the type of card you are enrolling. The default is *User ID*.
Note: remember that if the card number already has been designated as one of the three types, then any subsequent templates assigned to the card must be of the same type.

Note: if you have more than one unit networked together, it is recommended that you broadcast the new enrollment to the other units at this time.

Delete Templates

Use this option to delete one or more templates from a single unit (if you are in a networked environment, see the *BROADCAST PARAMETERS* section).

Select the appropriate ID number(s) in the *Templates* window and click the Delete button (recall that you can use the Shift and Ctrl keys to select multiple templates).

Note: You WILL NOT receive a warning when you are deleting templates unless you are deleting all of them. Therefore, be

sure to confirm that you have selected the correct ones the first time.

Verify Template

Use this option to initiate a VERIFY function on the unit identified by the Current Unit specified by the current communication settings. Only one template can be selected for this operation

Transfer Templates

There are six primary ways you can transfer templates:

- Transfer selected Templates from unit to unit
- Download selected Templates from the unit to the PC
- Download selected Templates from the unit to a Smart Card
- Upload selected Templates from the PC to the unit
- Upload selected Templates from the PC to a Smart Card
- Upload from the PC to ALL units defined in Network

Download from Unit to PC

File names are derived from the Template ID # and the Template Index #: e.g., this is Template 1122 0

Default type is based on whether unit is V-PASS or VeriFlex / VeriProx / V-Smart

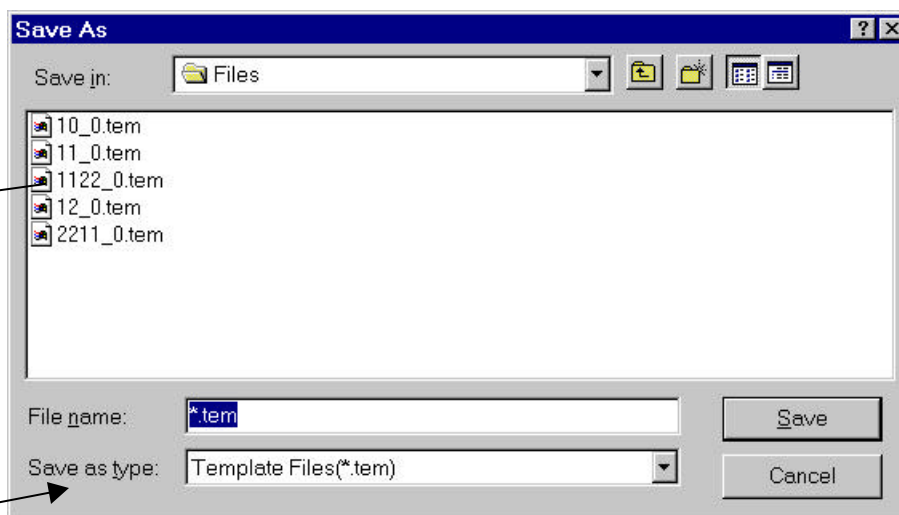


Figure 16: Download Template(s) to PC

- 1 In the **Template Manager** window, select the template(s) you wish to

transfer.

- 2 Click the *From Unit*→ *PC* button.
- 3 When the screen in Figure 16 appears, confirm the download path and directory; make any applicable changes.
- 4 Click the OK button.

When completed the files will be loaded in the designated directory on your PC.

Note: If you are in a networked environment, you only need to download from one unit since the template should be the same on all units.

Download from Unit to Smart Card

Downloading a template from the unit to a Smart Card requires that the current Site Key be entered which matches both the Site Key on the ESI and the Site Key on the Smart Card.

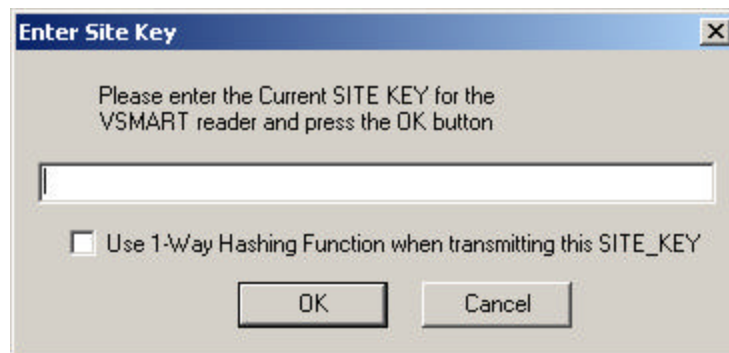


Figure 17a: Download Template(s) to Smart Card

Then present the Smart Card close to the reader and hold it until instructed to remove the card.

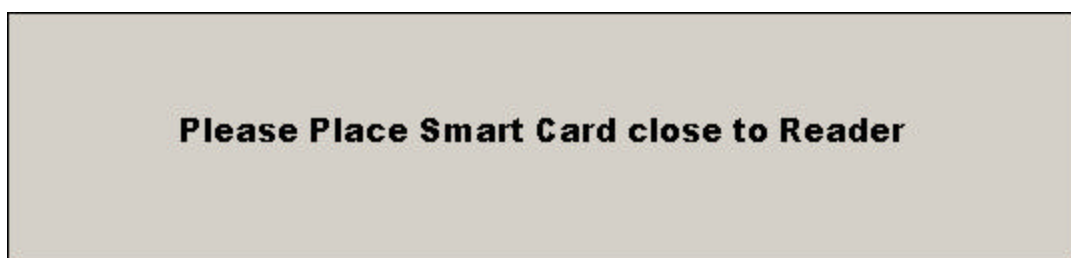


Figure 17b: Download Template(s) to Smart Card

If successful, the following message will be displayed:

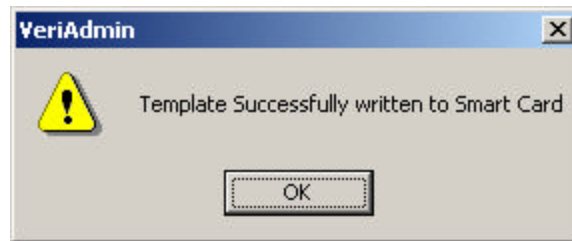


Figure 17c: Download Template(s) to Smart Card

Upload from PC to Unit

You can transfer templates from your PC to any unit. When you click the *From PC→Unit* button, a window like the one below will open:

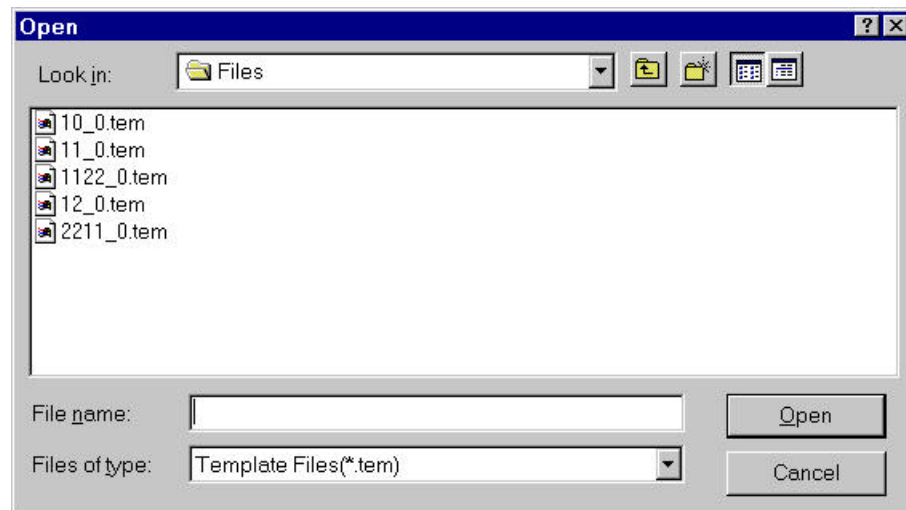


Figure 14: Upload Template(s) to Unit

- 1 Click the *From PC→Unit* button.
- 2 Use the window to browse for the correct directory.
- 3 Select the appropriate template(s).
- 4 Click the Open button.

Please note that when the template is uploaded, the Template ID Number and Index Number is taken from data within the file, not from the file name. Therefore, even if you change the name of the file on your PC, the Template number will remain the same. To change a Templates ID or index, always use the TEMPLATE EDIT feature within the application.

Upload from PC to Smart Card

The operation is similar to uploading from the unit and will require the current Site Key after selecting the desired template(s) from the PC.

Transfer from Unit to Unit

Use this option when you are in a networked environment.

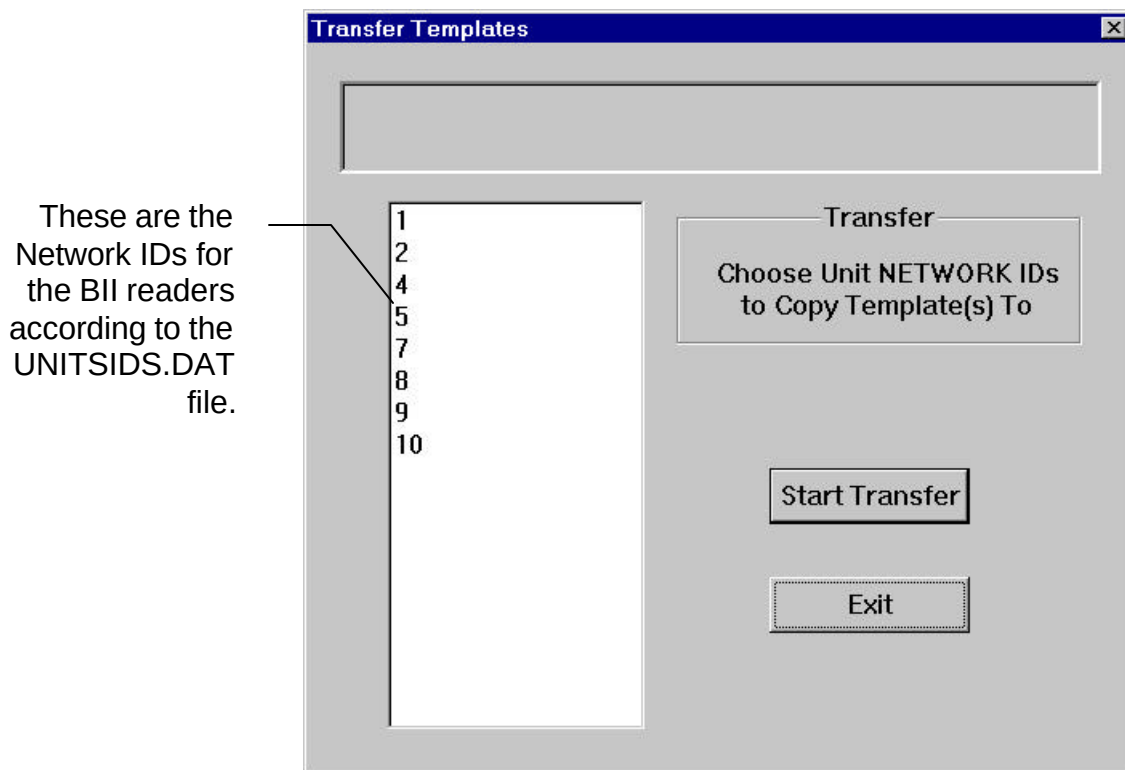


Figure 15: Transfer Templates from Unit to Unit

To transfer templates between units,

- 1 In the **Template Manager** window, select the template(s) you wish to transfer.
- 2 Click the Unit to Unit button.
- 3 When the screen in Figure 15 appears, highlight the IDs of the units to which you wish to transfer the templates.

Broadcast PC Template

This option will allow template(s) stored on the PC to be Broadcast to all units defined in the UNITIDS.DAT file. The process is as follows:

1. The templates will be read one-by-one from the PC.
2. Each specific template will be erased from all units on the network.

3. The template will be transferred using the ID of –1 on each defined Communication Port.

If the VERIFY BROADCAST is selected, the VeriAdmin software will attempt to verify that steps 2 and 3 were completed successfully. After step 2, each unit will be polled to determine if each template was removed correctly. If the template was NOT removed, another DELETE attempt will be made. After step 3, each unit will be polled to confirm that the template now exists on each unit. If the template does NOT exist on a particular unit, the TRANSFER function will be retried. Please see Appendix B for details of the benefits and potential issues with using Broadcast commands.

Edit PC Template

To edit a PC template, click the Edit PC Template button. A standard Windows File Selection window will open to allow the user to choose the template file to edit. Use the TYPE dropdown box to select between displaying VeriProx / VeriFlex / V-Smart templates (Verification Templates) and V-PASS templates (Searching Templates). Once chosen, the following window is opened:

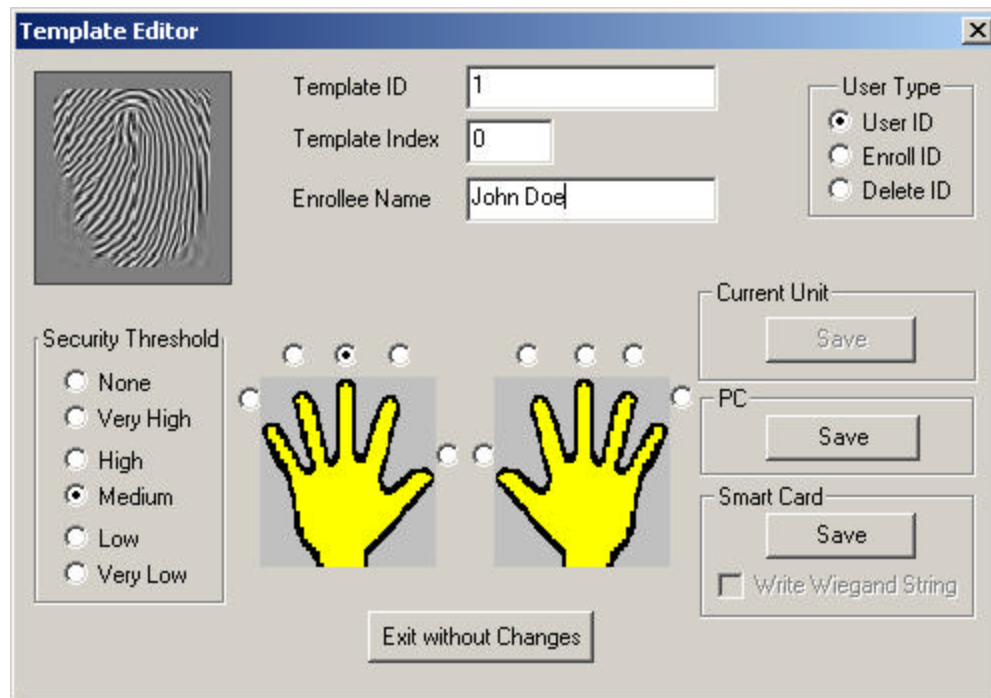


Figure 16: Edit PC Template

Within this window, all template data can be modified and saved back to the PC by pressing the SAVE button within the PC group box. You may optionally save to the unit or a Smart Card if desired.

NOTE: The filename is determined by the Template ID number and the Template Index number (See Figure 20). If these do not change, pressing SAVE (under the PC group box) will replace the previous file. If either value is changed, a NEW file is created.

Command Card Manager (VeriProx / VeriFlex)

Command Cards allow administrators to add and remove user IDs directly from the VeriProx or VeriFlex units without having to access the software. These can be useful for creating and removing temporary visitor's badges or administering the system when your PC is down or unavailable.

Administering Command Cards

Creating Command Cards

To create command cards, use the Template Manager (see QUICK Enrollment on page 38).

Reviewing Command Cards

By clicking the Command Card icon on the toolbar or selecting the option from the menu, the window below will appear. You will notice that the cards are listed by their Template ID numbers; all indices for each template are implied.

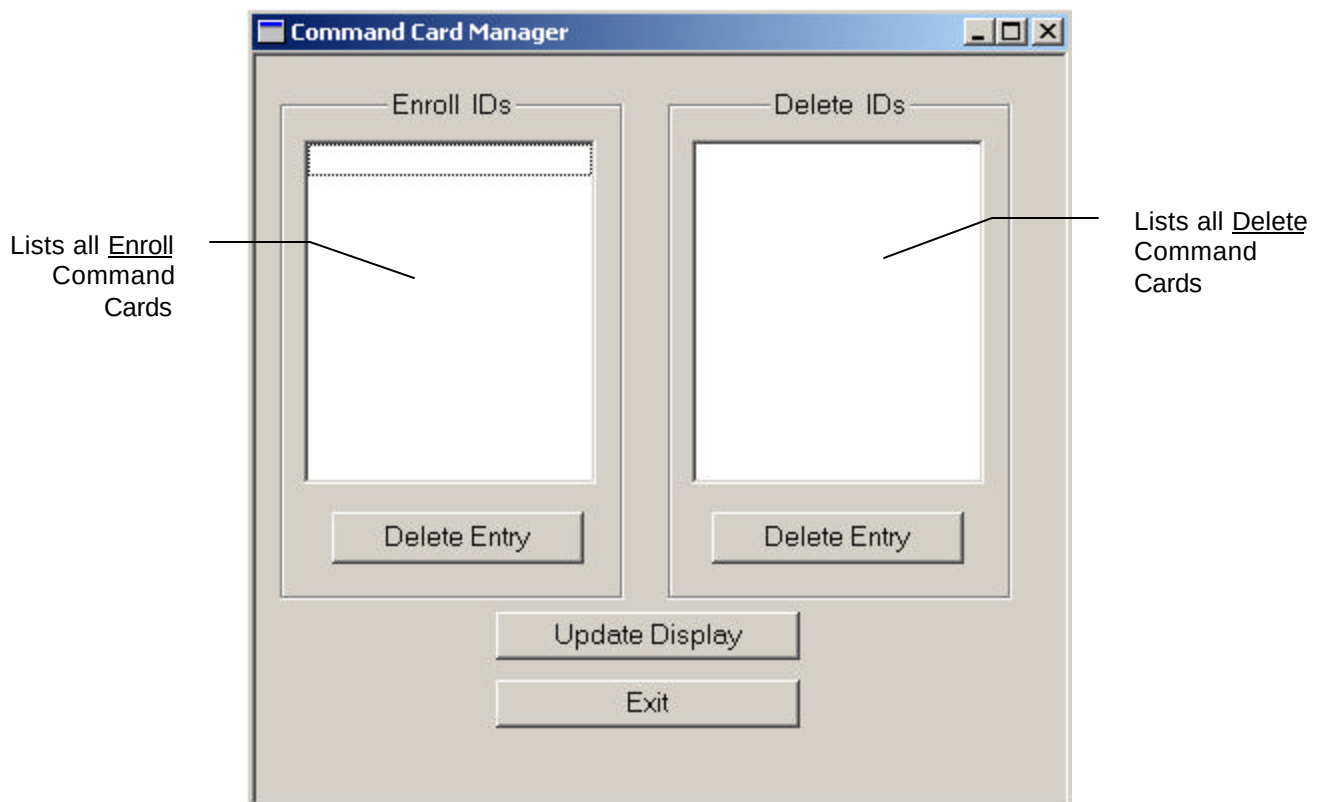


Figure 17: Command Card Manager

Removing Command Cards

To remove a command card, highlight the ID number in either the **Enroll IDs** or the **Delete IDs** window and click the *Delete Entry* button directly beneath the window. This will delete the template for all associated indices.

Note: You will not receive a warning when you click the button, therefore, make sure that you have selected the correct ID.

Using Command Cards

Once you have created Enroll and Delete Command Cards, they can be used as follows:

Enroll Command Card

To enroll a user:

- 1 Wave the Enroll Command Card near the front of the VeriProx / VeriFlex unit.
The light will glow amber directing the Administrator to place his/her finger on the unit.
- 2 If the Administrator is authorized to use the Command Card, the light will glow green and the unit will beep. Continue with the next step.
If not, the light will glow red. Return to Step 1 or stop.
- 3 The light will flash yellow, indicating the system is ready to enroll the new card. Wave the user card to be enrolled. The light will stop flashing.
The light will glow amber directing the User to place his/her finger on the unit.
- 4 If the print is accepted, the light will glow green and the unit will beep indicating that the card has been enrolled.

Delete Command Card

To delete a user:

- 1 Wave the Delete Command Card near the front of the VeriProx / VeriFlex unit.
The light will glow amber directing the Administrator to place his/her finger on the unit.
- 2 If the Administrator is authorized to use the Command Card, the light will glow green and the unit will beep. Continue with the next step.
If not, the light will glow red. Return to Step 1 or stop.
- 3 The light will flash red, indicating the system is ready to delete the card. Wave the user card to be deleted.
- 4 The light will glow green and the unit will beep indicating that the card has been deleted.

Communication Settings

From the Communication Settings dialog, you can modify the Transmit ID, the PC Comm Port, and the Communication Baud rate.

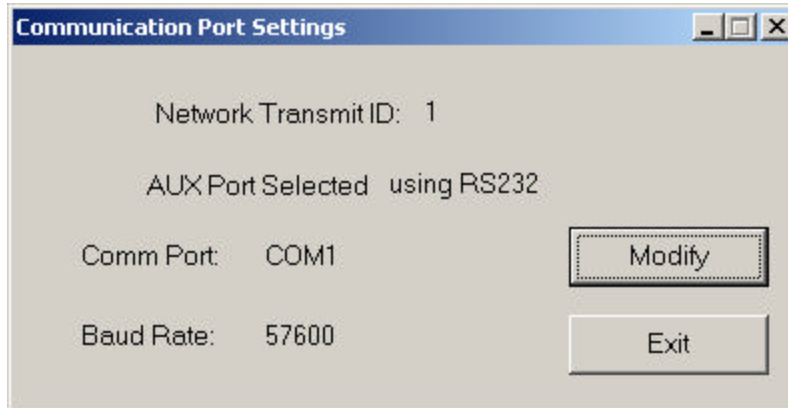


Figure 18: Communication Port Settings

Click the Modify button to change the displayed settings.

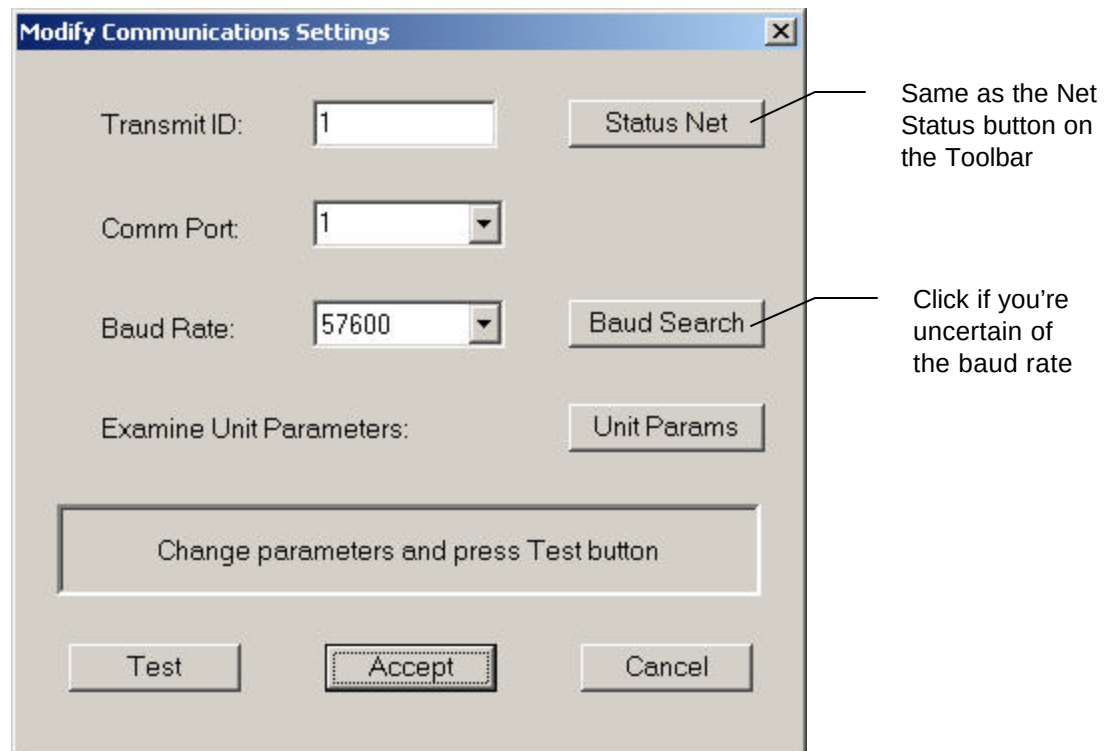


Figure 19: Modify Communications Settings

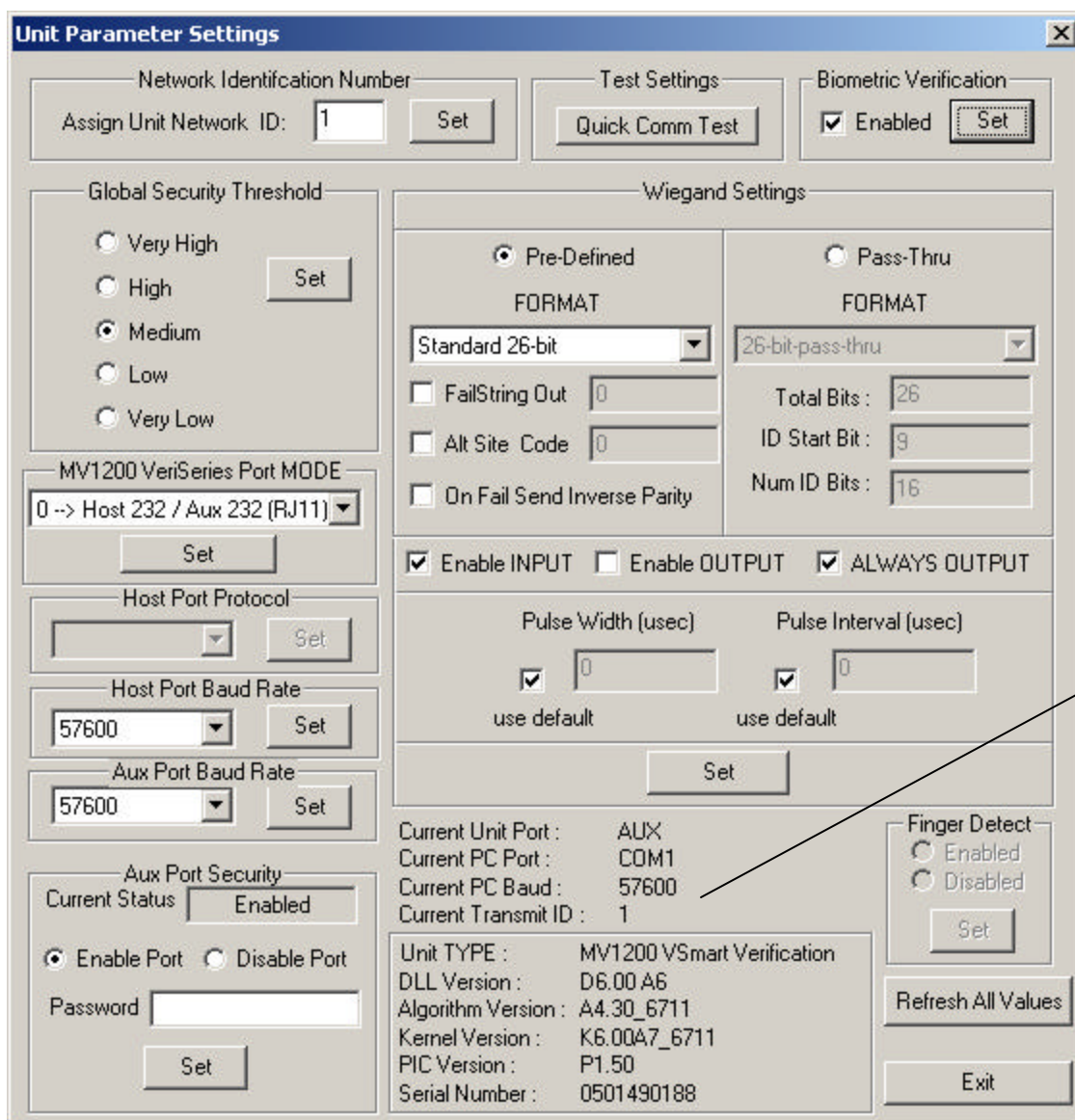
Note: Change only one setting at a time and be sure to test the change before clicking the Accept button.

Unit Parameter Settings

The Unit Parameter Settings window aids the Administrator in the following:

- Assigning a Network Identification Number to a unit
- Setting a Global Security Threshold for a unit
- Enabling/Disabling Wiegand Formats, Out Failure code, and Site codes
- Modify the Host and Aux Port baud rates
- Change the Host Protocol
- View the current statuses and settings of the various ports
- Performing a Quick COMM test that will flash the top LED and beep the current unit
- The ability to Password Protect the AUX port
- Setting of Wiegand PASS-THRU formats
- The ability to turn off biometrics (no recommended)

Select the change desired and press the corresponding Set button to transmit the change to the current unit.



The dialog box is titled "Unit Parameter Settings" and contains several sections for configuring the device. The "Network Identification Number" section has a text field for "Assign Unit Network ID" set to 1 and a "Set" button. The "Test Settings" section has a "Quick Comm Test" button. The "Biometric Verification" section has a checked "Enabled" checkbox and a "Set" button. The "Global Security Threshold" section has radio buttons for "Very High", "High", "Medium" (selected), "Low", and "Very Low", with a "Set" button. The "MV1200 VeriSeries Port MODE" section has a dropdown menu set to "0 --> Host 232 / Aux 232 (RJ11)" and a "Set" button. The "Host Port Protocol" section has a dropdown menu and a "Set" button. The "Host Port Baud Rate" section has a dropdown menu set to 57600 and a "Set" button. The "Aux Port Baud Rate" section has a dropdown menu set to 57600 and a "Set" button. The "Aux Port Security" section has a "Current Status" set to "Enabled", radio buttons for "Enable Port" (selected) and "Disable Port", a "Password" field, and a "Set" button. The "Wiegand Settings" section has two tabs: "Pre-Defined" (selected) and "Pass-Thru". The "Pre-Defined" tab has a "FORMAT" dropdown set to "Standard 26-bit", checkboxes for "FailString Out", "Alt Site Code", and "On Fail Send Inverse Parity", and input fields for "Total Bits" (26), "ID Start Bit" (9), and "Num ID Bits" (16). The "Pass-Thru" tab has a "FORMAT" dropdown set to "26-bit-pass-thru" and input fields for "Total Bits" (26), "ID Start Bit" (9), and "Num ID Bits" (16). Below the tabs are checkboxes for "Enable INPUT", "Enable OUTPUT", and "ALWAYS OUTPUT". The "Pulse Width (usec)" and "Pulse Interval (usec)" sections have checkboxes for "use default" and input fields set to 0. A "Set" button is at the bottom of the Wiegand section. The "Current Unit Port" section shows "AUX", "Current PC Port" shows "COM1", "Current PC Baud" shows "57600", and "Current Transmit ID" shows "1". The "Finger Detect" section has radio buttons for "Enabled" (selected) and "Disabled", and a "Set" button. The "Refresh All Values" and "Exit" buttons are at the bottom right. A line points from the text "Current statuses and settings" to the "Current Unit Port" section.

Current
statuses and
settings

Figure 20: VeriProx Parameter Settings

Note: Changes made to Unit ID and Host Baud Rate will also change the Current Transmit ID and Current PC Baud rate so that communications is still possible with the unit.

Network Identification Number

In a networked environment, a unique number must be assigned to each unit before adding that unit to the network (The default setting from the factory is "0"). If two or more units have the same Network ID on the same COMM Port, data collisions will cause poor communication on that COMM Line (See "Concepts of Operations" section).

Setting the Number

- 1 In the *Assign Unit Network ID* field, type the new Network ID number.
- 2 Click the Set button.

Global Security Threshold

There are two types of security settings: the local security level associated with the individual template; and, the global security level associated with the individual Veri-Series unit. You may recall that the system will authorize using the lower of the two. See the appendix for a discussion of security settings and algorithm performance.

Example: If the template is set for Very High, and the unit is set for Medium, the authorization will be performed at the Medium setting.

Because of the unit's high accuracy rate, which practically negates the possibility of a false read, the above affords the unit a high rate of true authorization.

Setting the Security Threshold

Select the threshold level:

- Very High
- High
- Medium
- Low
- Very Low

Click the Set button.

MV1200 VeriSeries Port MODE

In the MV1200 based versions of the VeriSeries products, certain combinations of ports and protocols are not allowed. To simplify this, each available mode is listed in a dropdown. This will only be enabled if the unit is a MV1200 based unit.

- 1 In the **MV1200 VeriSeries Port MODE** section, select the appropriate mode from the drop down list.
- 2 Click the Set button.

If the display in the lower right corner does not update, close and re-open the window.

Warning: Changing this may cause you to lose communication with the unit(s). If changing to mode 2 with a V-Smart, be sure you have an RS-485 converter!

Host Port Protocol

This dropdown is enabled only for older MV1100 based devices. The usual protocol settings are as follows:

RS-232 stand alone devices

RS-485 networked devices

- 1 In the **Host Port Protocol** section, select the appropriate protocol from the drop down list.
- 2 Click the Set button.

If the display in the lower right corner does not update, close and re-open the window.

Warning: Changing this may cause you to lose communication with the unit(s).

Host Port and Aux Port Baud Rates

You can change the baud rates of both the Host and Aux ports to match your PC and/or other networked devices.

In order to maintain communication, if you change the baud rate on the port you are using, the PC's baud rate automatically will update.

- 1 In the appropriate section (**Host Port** or **Aux Port**), select the appropriate baud rate from the drop down list.
- 2 Click the Set button.

If the display in the lower right corner does not update, close and re-open the window.

Quick COMM Test

The button will perform a quick COMM TEST with the device identified by the displayed Current COMM settings. The test will flash the LED each color then sound the buzzer.

Biometric Verification

This option allows the user to turn biometric verification on and off. Check or uncheck this option and press the SET button. Unchecking the box will cause the unit to bypass the core fingerprint authentication (i.e., no finger required) and allows for Wiegand pass-thru authentication alone. **Turning this off will result in a less secure system and is not recommended!** The user assumes all risk associated with disabling biometrics.

Finger Detect (V-PASS only!)

This section will show the current setting of the Auto Finger Detect function of the V-PASS product. The user can select the option desired and press the SET button to modify the setting on the current unit. This section is disabled when the current unit is not a V-PASS.

Wiegand Settings

This section allows you to send coded messages to your Wiegand device (where applicable). Pressing the SET button will transfer all WIEGAND SETTINGS values at once.

Wiegand FORMAT

This section allows you to select the desired Wiegand format for both INPUT and OUTPUT. 26-bit Standard is the default format. Other custom formats are available and can be selected using the dropdown box.

NOTE: the format for BOTH INPUT and OUTPUT will be the same

FailString Out

When you check the *FailString Out* box, whatever code you type into the *Failure Code* field will be sent to the Wiegand device when a failed authorization occurs.

The string is numeric and ranges from 0 to 65535.

If the box is unchecked then no string will be sent when a verification fails.

Alt Site Code

When you check the *Alt Site Code* box, whatever code you type in the *Site Code* field will override the site code on all cards used on the unit.

The string is numeric and ranges from 0 to 255.

If the box is unchecked the site code read from the proximity card will be passed through in the Wiegand out string.

On Fail Send Inverse Parity

When you check the *On Fail Send Inverse Parity* box, a failed verify will result in the Wiegand string being sent on the Wiegand out lines with inversed parity to indicate the failure.

Enable INPUT

This option in the Wiegand Settings section will enable Wiegand INPUT when checked and sent to the BII_UNIT. This allows all WIEGAND INPUT communications. If this option is unchecked and sent to the BII_UNIT, all WIEGAND INPUT data will be ignored.

Enable OUTPUT

This option in the Wiegand Settings section will enable Wiegand OUTPUT when checked and sent to the BII_UNIT. This causes the WIEGAND OUTPUT string to be sent whenever a WIEGAND INPUT is received (see PASS_THRU section Wiegand Output related to Pass-Thru formats). If this option is unchecked and sent to the BII_UNIT, all WIEGAND OUTPUT data will be ignored unless the ALWAYS OUTPUT is selected.

ALWAYS OUTPUT

This option in the Wiegand Settings section will enable Wiegand OUTPUT on ALL Verifications regardless of whether initiated by a Wiegand INPUT, a PC or any other device

Pulse Width

Unchecking the *USE DEFAULT* option will allow the user to enter a custom Pulse Width duration for Wiegand Output. This is NOT recommended unless the user is very familiar with the device connected to the BII_Unit.

Pulse Interval

Unchecking the *USE DEFAULT* option will allow the user to enter a custom Pulse Interval duration for Wiegand Output. This is NOT recommended unless the user is very familiar with the device connected to the BII_Unit.

Wiegand PASS-THRU formats

When used with MV1100/MV1200 firmware version 2.50 or higher, the VeriAdmin software allows expanded Wiegand compatibility by allowing definition

of a PASS-THRU format. In order to use this ability, the following information is required:

- Total number of Wiegand bits in Wiegand String (maximum = 64 bits)
- Start Bit of the ID FIELD (where first bit is bit 0)
- Number of bits in the ID FIELD (must be contiguous bits)

Using these 3 pieces of information, when a card is presented to the BII_Unit, it will attempt to decode the ID FIELD and use that information as the TEMPLATE ID number. All SITE codes, Parity, and any other data are ignored. Using this ID, the BII_Unit will attempt to VERIFY the template corresponding to the decoded ID.

If the ID is not found or if the VERIFICATION attempt FAILS, no Wiegand output is sent. To the controller, it will appear as if nothing was presented.

If the ID is valid and a SUCCESSFUL VERIFICATION is performed, the original Wiegand INPUT string (with SITE code, Parity, etc) will “PASS-THRU” to the WIEGAND OUTPUT unchanged.

Although this PASS-THRU option does not allow FAIL STRINGS, changing the SITE code or checking PARITY, it does provide a mechanism for using a wide variety of Wiegand formats.