MiY Product Line
Device User Guide

Version 2.2
### Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>10/11/2012</td>
<td>RS</td>
<td>Updated Factory Reset instructions. Updated the section on Relay and Line in. Added Wiegand Panel Wiring section</td>
</tr>
<tr>
<td>2.1</td>
<td>3/13/2013</td>
<td>MH</td>
<td>Updated information for the MiY-Touch product</td>
</tr>
<tr>
<td>2.2</td>
<td>6/22/2013</td>
<td>MH</td>
<td>Updated information for 1.8 release</td>
</tr>
</tbody>
</table>
Contents

1 Overview ............................................. 1
  1.1 MiY Product Line Introduction ................................................................. 1
  1.2 Safety Information ................................................................. 1
    1.2.1 Safety Messages ................................................................. 2
    1.2.2 EMC, USA, and Canada Compliance ................................................................. 2
      1.2.2.1 FCC Radio Frequency Rules and Regulations ................................................. 2
      1.2.2.2 FCC Intentional Radiator Certification ......................................................... 2
      1.2.2.3 Industry Canada Radio Frequency Rules and Regulations ........................................ 2
  1.3 Standard Features ................................................................. 2
    1.3.1 Optional Features ................................................................. 4
      1.3.1.1 MiY-ID Gov ................................................................. 5
  1.4 Types of Users ................................................................. 6
  1.5 Key Terms ................................................................. 6

2 MiY Devices ............................................. 7
  2.1 MiY Indoor Device Overview ................................................................. 7
    2.1.1 Physical Features ................................................................. 8
      2.1.1.1 Contactless Card Reader ................................................................. 8
      2.1.1.2 Display ................................................................. 8
      2.1.1.3 Keypad ................................................................. 10
      2.1.1.4 Fingerprint Sensor ................................................................. 10
      2.1.1.5 Contact Card Reader (MiY-ID) ......................................................... 10
      2.1.1.6 Admin Port and Reset Button ......................................................... 11
      2.1.1.7 Wall Mount ................................................................. 11
      2.1.1.8 Back Panel and Connections ......................................................... 13
      2.1.1.9 USB Ports ................................................................. 14
        2.1.1.9.1 USB Host Port ................................................................. 14
        2.1.1.9.2 OTG USB Port ................................................................. 15
    2.1.2 Certifications ................................................................. 15
  2.2 MiY Outdoor Device Overview ................................................................. 16
    2.2.1 Physical Features ................................................................. 16
      2.2.1.1 Display ................................................................. 16
      2.2.1.2 Fingerprint Sensor ................................................................. 17
      2.2.1.3 Admin Port and Reset Button ......................................................... 17
      2.2.1.4 Wall Mount ................................................................. 18
      2.2.1.5 Back Panel and Connections ......................................................... 19
      2.2.1.6 USB Ports ................................................................. 20
        2.2.1.6.1 USB Host Port (Rear of the device) ......................................................... 20
        2.2.1.6.2 USB Host Port (Front of the device) ......................................................... 21
        2.2.1.6.3 OTG USB Port ................................................................. 22
    2.2.2 Certifications ................................................................. 22

3 Installing a MiY Device ............................................. 23
3.1 Accessory List ........................................................................................................ 23
3.2 Mounting the Bracket ............................................................................................. 23
3.3 Wiring Installation .................................................................................................. 24
3.4 Connecting the Power Supply to the MiY Device .................................................. 26
  3.4.1 Connecting the Power Supply to the Terminal Blocks ........................................... 26
  3.4.2 Connecting the Power Supply by Ethernet Port (Power over Ethernet) .......... 27
3.5 Panel-in Wiring ....................................................................................................... 29
3.6 Relay & Line Trigger Wiring .................................................................................... 29
  3.6.1 Single Door Control ............................................................................................ 30
3.7 Securing the MiY Devices on the Wall ..................................................................... 31
3.8 Balancing the Termination ..................................................................................... 34
3.9 Wiegand Panel Wiring ............................................................................................. 36

4 Network Installation .................................................................................................. 38
  4.1 Manually Configuring the MiY-Device’s Connection ................................................ 38
    4.1.1 TCP/IP Configuration ....................................................................................... 38
      4.1.1.1 To configure TCP/IP on MiY Outdoor Devices: .............................................. 38
      4.1.1.2 To configure TCP/IP on MiY Indoor Devices: ............................................... 43
    4.1.2 Configuring RS485 Connection Settings .............................................................. 48
    This section will show you how to change the device communication from
    Ethernet to RS485........................................................................................................ 48
      4.1.2.1 To configure RS485 connection settings: ......................................................... 48
      4.1.2.2 To configure RS485 on MiY Indoor Devices: ................................................. 50

5 Registering the Reader with MiY-Security Manager .................................................. 54
  5.1 Basic Zone Creation ............................................................................................... 54

6 Upload Package via USB ............................................................................................ 57
  6.1 Deploying a Package ............................................................................................. 57

7 Cogent GateApp for Administrators ......................................................................... 63
  7.1 Logging in to Access Admin Functions ................................................................. 63
    7.1.1 To access the MiY Admin Menu on MiY Outdoor Devices: ............................... 63
    7.1.2 To access the MiY Admin Menu on MiY Indoor Devices: ................................ 64
  7.2 Managing the Device ............................................................................................. 67
    7.2.1 Viewing Device Info ........................................................................................ 67
      7.2.1.1 To view device settings on MiY Outdoor Devices: .......................................... 67
      7.2.1.2 To view device settings on MiY Indoor Devices: .......................................... 68
    7.2.2 Changing Device Network Settings ................................................................. 68
    7.2.3 Changing Device Security Settings .................................................................... 69
  7.3 Managing Users ..................................................................................................... 72
    7.3.1 Adding Users .................................................................................................... 73
      7.3.1.1 To add users on MiY Outdoor Devices: ......................................................... 73
      7.3.1.2 To add users on MiY Indoor Devices: ......................................................... 76
7.3.2 Modifying Users ........................................................................................................................................... 80
  7.3.2.1 To modify an existing user on MiY Outdoor Devices: ................................................................. 80
  7.3.2.2 To modify an existing user on MiY Indoor Devices: ........................................................................ 82
7.3.3 Deleting Users .................................................................................................................................................. 83
  7.3.3.1 To delete a user on MiY Outdoor Devices: ....................................................................................... 83
  7.3.3.2 To delete a user on MiY Indoor Devices: ....................................................................................... 84
7.3.4 Promoting Users ............................................................................................................................................... 85
  7.3.4.1 To promote an existing user on MiY Outdoor Devices: ................................................................. 85
  7.3.4.2 To promote an existing user on MiY Indoor Devices: .................................................................... 88
7.3.5 Demoting Users ............................................................................................................................................... 91
  7.3.5.1 To demote an existing user on MiY Outdoor Devices: ................................................................. 91
  7.3.5.2 To demote an existing user on MiY Indoor Devices: .................................................................... 92
7.4 Enabling the OTG USB Port ............................................................................................................................. 93
  7.4.1 To enable the OTG USB port on MiY Outdoor Devices: ................................................................. 93
  7.4.2 To enable the OTG USB port on MiY Indoor Devices: ........................................................................ 95
7.5 Enabling Panel-in Lock Icon ........................................................................................................................... 97
  7.5.1 To enable the Panel-in Lock Icon on MiY Outdoor Devices: ......................................................... 97
  7.5.2 To enable the Panel-in Lock Icon on MiY Indoor Devices: ............................................................. 98

8 Verifying Users for Access/Entry .......................................................................................................................... 100
  8.1 Verifying Users with the MiY-Search and MiY-Card ............................................................................... 100
  8.2 Verifying Users with the MiY-ID Device ............................................................................................... 102
  8.3 Verifying Users with the MiY-Touch ..................................................................................................... 103

A Optimizing Fingerprint Images .......................................................................................................................... 106
  A.1 Positioning the Finger on the Fingerprint Sensor ............................................................................... 106
  A.2 Things to Remember when Placing a Finger on the Sensor ............................................................. 107
  A.3 Capturing High-Quality Fingerprints ................................................................................................. 109

B Maintenance and Troubleshooting .................................................................................................................... 112
  B.1 Cleaning the Fingerprint Sensor ........................................................................................................... 112
  B.2 Caring for the Fingerprint Sensor ......................................................................................................... 112
  B.3 Resetting MiY Devices ............................................................................................................................ 113
    B.3.1 Factory Reset .................................................................................................................................... 113
  B.4 Contacting Your Distributor ..................................................................................................................... 116
1  Overview

1.1 MiY Product Line Introduction

The 3M Cogent MiY product line offers a complete range of highly sophisticated, accurate, and customizable biometric physical access control terminals which provide access security in a variety of environments.

All the devices of the MiY product line are designed to perform fast and efficient authentication and entry. Fingerprint data for users who no longer have access can be easily erased from the system in real-time.

The MiY product line provides multi-factor access control from single factors like fingerprint, pin, and card to three- or four-factor authentications. Enabling higher security access where it is required and convenience for high traffic areas.

The Cogent MiY product line offers the highest level of access security and flexibility available.

Refer to the MiY Security Manager User Guide for information on managing MiY devices with MiY Security Manager Software.

1.2 Safety Information

Read, understand, and follow all safety information contained in these instructions prior to installation of the 3M Cogent MiY device. Retain these instructions for future reference.

<table>
<thead>
<tr>
<th>Explanation of Signal Word Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANGER: Indicates a potentially hazardous situation, which, if not avoided, will result in death or serious injury and/or property damage.</td>
</tr>
<tr>
<td>WARNING: Indicates a potentially hazardous situation, which, if not avoided, could result in death or serious injury and/or property damage.</td>
</tr>
<tr>
<td>CAUTION: Indicates a potentially hazardous situation, which, if not avoided, may result in minor or moderate injury and/or property damage.</td>
</tr>
<tr>
<td>CAUTION: Indicates a potentially hazardous situation, which, if not avoided, may result in property damage.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Explanation of Product Safety Label Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Attention: Read accompanying documentation" /></td>
</tr>
<tr>
<td><img src="image" alt="Risk of Electric Shock" /></td>
</tr>
</tbody>
</table>
1.2.1 Safety Messages

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>To reduce the risk associated with fire and explosion:</td>
</tr>
<tr>
<td>- Do not use a power supply that is not 12V DC</td>
</tr>
<tr>
<td>- Do not improperly wire the relay output from the unit with disregard to the wiring instructions provided in this manual</td>
</tr>
<tr>
<td>- Do not improperly wire the line trigger output from the unit with disregard to the wiring instructions provided in this manual</td>
</tr>
</tbody>
</table>

To prevent overheating and the potential of fire, the power supply should:
- Be dedicated to the MiY reader(s)
- Regulated and filtered
- Be a UL-Listed Class II power supply at 12 VDC, 1A continuous

<table>
<thead>
<tr>
<th>CAUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>To reduce the risk associated with repetitive strain injuries from overuse of the MiY units:</td>
</tr>
<tr>
<td>- Operation of the 3M Cogent MiY device may involve repeated body movements. To minimize possibility of Repetitive Stress Injury, avoid prolonged repetitive movements, rest when becoming fatigued and, when possible, alternate job functions with other people. Avoid awkward reaching for items.</td>
</tr>
</tbody>
</table>

To reduce the risk associated with environmental contamination from the potentially hazardous chemicals within the lithium-ion battery:
- At the end of service life, dispose of the device in accordance with federal, state, and local requirements.

1.2.2 EMC, USA, and Canada Compliance

1.2.2.1 FCC Radio Frequency Rules and Regulations
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 a 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/her own expense.

1.2.2.2 FCC Intentional Radiator Certification

<table>
<thead>
<tr>
<th>MiY-ID with SCM Reader</th>
<th>MiY-ID with HID Reader</th>
<th>MiY-Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCC ID: DGFSSDIDSCM</td>
<td>FCC ID: DGFSSDIDHID</td>
<td>FCC ID: DGFSSDCARDSCM</td>
</tr>
</tbody>
</table>

This equipment contains an intentional radiator approved by the FCC under the FCC ID number shown above. 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.
NO MODIFICATIONS. Modifications to this device shall not be made without the written consent of 3M, Company. Unauthorized modifications may void the authority granted under Federal Communications Commission Rules permitting the operation of this device.

1.2.2.3 Industry Canada Radio Frequency Rules and Regulations
This Class A digital apparatus meets all requirements of the Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

MiY-ID with SCM Reader  MiY-ID with HID Reader  MiY-Card

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.
### 1.3 Standard Features

<table>
<thead>
<tr>
<th>MiY-Touch</th>
<th>MiY-Search</th>
<th>MiY-Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sandbox API framework support</td>
<td>• Sandbox API framework support</td>
<td>• Sandbox API framework support</td>
</tr>
<tr>
<td>• Touch-screen</td>
<td>• IP65 design</td>
<td></td>
</tr>
<tr>
<td>• Detachable contact/contactless smart card reader (optional)</td>
<td>• Non-mechanical 12-key keypad</td>
<td></td>
</tr>
<tr>
<td>• 3.5” color LCD display</td>
<td>• Rugged optical sensor</td>
<td></td>
</tr>
<tr>
<td>• Speaker audio with built-in microphone</td>
<td>• 2.2” color LCD display</td>
<td></td>
</tr>
<tr>
<td>• POE support</td>
<td>• Speaker audio with built-in microphone</td>
<td></td>
</tr>
<tr>
<td>• Protected admin port</td>
<td>• POE support</td>
<td></td>
</tr>
<tr>
<td>• External USB for add-on devices:</td>
<td>• Protected admin port</td>
<td></td>
</tr>
<tr>
<td>• 2D barcode readers</td>
<td>• External USB for add-on devices:</td>
<td></td>
</tr>
<tr>
<td>• Passport readers</td>
<td>• 2D barcode readers</td>
<td></td>
</tr>
<tr>
<td>• Other USB enabled readers</td>
<td>• Passport readers</td>
<td></td>
</tr>
<tr>
<td>• Various multi-color guidance LEDs</td>
<td>• Other USB enabled readers</td>
<td></td>
</tr>
<tr>
<td>• Easy installation</td>
<td>• Multi-color guidance LEDs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Easy installation</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>IP65 design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-mechanical 12-key keypad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full PC/SC ISO 14443 contactless card reader</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rugged optical sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2” color LCD display</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speaker audio with built-in microphone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POE support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected admin port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External USB for add-on devices:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2D barcode readers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passport readers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other USB enabled readers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-color guidance LEDs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy installation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### MiY-ID
- Sandbox API framework support
- IP64 design
- Non-mechanical 21-key keypad
- Full PC/SC ISO 14443 contactless card reader with optional ISO 15693 iClass reader
- Full PC/SC ISO 7816 Contact Smart Card Reader
- Rugged optical sensor
- 2.7” color LCD display
- Speaker audio with built-in microphone
- POE support
- Protected admin port
- External USB for add-on devices:
  - 2D barcode readers
  - Passport readers
  - Other USB enabled readers
- Various multi-color guidance LEDs
- Easy installation

### 1.3.1 Optional Features
Optional features are available within MiY’s range of devices, so that physical access control systems can be tailored to the specific needs of facilities and agencies.

**Optional features available MiY devices:**
- Centralized user administration and database software
- HID® iClass Contactless Smartcard reader supporting (MIFARE®, DESFire®, EV1)
- Additional Memory for storage of up to 1,000,000+ fingerprints on SD Card for 1:1
- Additional Memory for storage of up to 80,000 fingerprints in RAM for 1:N
- Server side matching
1.3.1.1 MiY-ID Gov

The MiY-ID Gov is an enhanced version of the standard MiY-ID reader, which includes full support for processing government credentials including PIV, TWIC and CAC. The MiY-ID Gov is configurable for use in all standard NIST approved PIV modes, TWIC MARSEC levels and standard CAC operating modes. In order to meet NIST cryptographic standards, the MiY-ID Gov utilizes RSA BSAFE Crypto-C Micro Edition, a FIPS 140-2 approved cryptographic module from RSA.

The MiY-ID Gov provides the following features to meet NIST standards as a Biometric Authentication System:

- FIPS 201 approved fingerprint capture device
- Fully integrated PIN input device within the device housing
- Provides the PIN (Personal Identification Number) to the government credential card (PIV/TWIC/CAC) to gain access to the biometric template
- Verifies the digital signature of the biometric template container and performs full path validation of the signing certificate using SCVP protocol to a GSA certification validation server. Supports all digital signature algorithms specified in NIST SP 800-78-2 Table 3-3, including RSA (2048 or 3072), ECDSA (Curve P-256/384) with SHA-1, SHA-256 and SHA-384 hash algorithms.
- Physically hardened to protect against direct electrical compromise
- Allows for all access controls decisions to be made by comparing the FASCN of the credential to an approved access control list
1.4 Types of Users

MiY devices provide access privileges for two types of users:

- Standard Users: Can access the Verify operation mode only. Enroll and Delete functions can also be performed, but only in the presence of and with the assistance of an Administrator.

- Administrators: Possess privileges for all operation modes available for the MiY devices, including setting the Verify, Enroll, and Delete modes using an Administrator Card where applicable.

1.5 Key Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIY</td>
<td>MiY (Make it Yours) is the generic designation of all biometric physical access control devices within the 3M Cogent MiY product line.</td>
</tr>
<tr>
<td>Enrollment</td>
<td>The initial process of capturing a fingerprint image, adjusting image quality, extracting the correct minutiae information, creating a minutiae template along with the user information, and storing the record to memory or another storage media. Overall system performance is increased by also evaluating the quality of enrollment before deciding to store the record.</td>
</tr>
<tr>
<td>Verification (Authentication)</td>
<td>The process of comparing a live fingerprint against the corresponding minutiae template stored during enrollment. This is used to confirm the identity of the person attempting to gain access. A pass/fail result is returned based on whether the score was above a pre-defined threshold value.</td>
</tr>
<tr>
<td>Identification</td>
<td>This is similar to verification, except that the user does not identify his or herself. The system must compare the live fingerprint against all stored minutiae templates in a database to determine a match. This is used to establish the identity of the person attempting to gain access.</td>
</tr>
<tr>
<td>Template</td>
<td>The data stored after the enrollment process, which is a collection of minutiae points from the captured fingerprint and does not contain the original fingerprint image.</td>
</tr>
<tr>
<td>Minutiae Record</td>
<td>The compilation of minutiae templates acquired during enrollment along with the other user information such as name, Wiegand ID, etc.</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet is made available using a PoE switch. This switch is able to deliver power to the devices over the same communication cable and allows installations to be simplified.</td>
</tr>
</tbody>
</table>
2 MiY Devices

2.1 MiY Outdoor Device Overview

The MiY Outdoor Devices come in three versions: MiY-Search, MiY-Card, and MiY-ID. These devices have similar appearances and functions.

**NOTE:** The MiY-Search and MiY-Card share the same physical specifications. However, the MiY-Card and MiY-ID come equipped with card readers.
2.1.1 Physical Features

MiY outdoor physical access devices are housed in a rugged plastic casing and can provide various modes for identification, verification and multi-factor authentication. The following subsections provide an introduction to the physical characteristics of MiY outdoor devices.

2.1.1.1 Contactless Card Reader

The MiY-Card and MiY-ID have guidance LEDs on the contactless reader that help direct the user’s attention to the top of the device during a contactless card read.

2.1.1.2 Display

All MiY Outdoor Devices have a color QVGA display and have workflow icons to show users the next step in the authentication process. The MiY-ID has a 2.7” display. The MiY-Search and MiY-Card have a 2.2” display.
The following are the available status Icon LEDs on the MiY-ID and MiY-Card/Search.

- Card Insertion Status Icon LED: ID Only
- Contactless Status Icon LED: ID/Card/Search
- Keypad Status Icon LED: ID/Card/Search
- Fingerprint Status Icon LED: ID/Card/Search
- Face Status Icon LED: ID Only
- Panel-In Lock Status Icon LED: ID/Card/Search

On the Cogent Gate application, the upper right screen of the display has a connectivity status icon. This icon shows the device’s registration and communication status:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Red Icon]</td>
<td>Device is unregistered to a server or running in standalone mode. It is considered “unmanaged” and no server on the network can be found</td>
</tr>
<tr>
<td>![Yellow Icon]</td>
<td>Device is unregistered to a server. The device has found a server on the network and is “pending registration”</td>
</tr>
<tr>
<td>![Green Icon]</td>
<td>Device is registered to a server and has exchanged security tokens for an encrypted TLS communication. The server is on-line and communicating with this device.</td>
</tr>
<tr>
<td>![Gold Icon]</td>
<td>Device is registered to a server and has security tokens. Currently the device cannot find the server BUT the server can communicate to the device.</td>
</tr>
<tr>
<td>![Key Icon]</td>
<td>Device is registered to a server and has security tokens. Currently the server cannot be found and is possibly offline. The Device is running independently until the server is available</td>
</tr>
<tr>
<td>![Communication Icon]</td>
<td>There is communication activity between the device and server.</td>
</tr>
</tbody>
</table>
2.1.1.3 Keypad
MiY Outdoor Devices have back-lit non-mechanical buttons that can be used for user PIN entry, functional selection, or device administration.

2.1.1.4 Fingerprint Sensor
MiY Outdoor Devices have a built-in fingerprint sensor that is rated for outdoor use.

2.1.1.5 Contact Card Reader (MiY-ID)
The MiY-ID device has a contact card reader on the bottom:
2.1.1.6 Admin Port and Reset Button
The bottom of the device has a weather protection rubber cover that protects the Admin port and reset button.

2.1.1.7 Wall Mount
The stainless steel mounting bracket can be attached to a single gang box or double gang box. MiY Outdoor Devices have a hinge at the bottom which allows installers to latch the device on the wall and open the back panel for easy wiring.
2.1.1.8 Back Panel and Connections
The back panel of MiY Outdoor Devices can be opened to expose the internal connections.

Back Panel

MiY Devices have the following rear connections:

- Power over Ethernet Port
- Terminal Block A
- Terminal Block B
- Terminal Block C
- External USB Port
- Soft Dip Switch
2.1.1.9 USB Ports

The MiY Outdoor Device has two (2) USB ports that are configurable. The device has a USB host port and OTG USB client port.

2.1.1.9.1 USB Host Port

The USB host port is only accessible from the back panel of the device. The USB host port is used to integrate additional USB components to the device, such as a camera, by adding a driver for the component to the firmware and updating GateApp's to use the new component.

The USB connectors can be created or purchased. Below are the USB Host Port Pin definitions.

The USB connector should be small and allows the wires to curl within the unit before exiting the compression door.
2.1.1.9.2 OTG USB Port

The OTG USB client port is located on the bottom of the device and is disabled by default. An administrator must login to the device menu to enable the OTG port for Normal or Development use.

![OTG USB Port](image)

Normal OTG mode allows for communication between the device and the Device Admin Utility running on a PC or laptop that has the MiY Device Driver installed. The Development mode is designed for use by developers that need the device to communicate with their PC or laptop via Microsoft ActiveSync or Windows Mobile Device Center. Make sure the USB cable on the device side is well connected; some USB cables are shorter and need to be snuggly inserted.

For instructions on enabling the OTG USB port, see the section *Enabling the OTG USB Port* in this document

2.1.2 Certifications

The MiY-ID, MiY-Card, and MiY-Search are FCC, CE, R&TTE (when optional radios are included), and RoHS certified.

Suggested Power Supplies:

12VDC Power supply

- Altronix AL175UL 12VDC UL 294 listed
- or another UL 294 approved 12VDC power supply

POE Power supply

- Infinias S-PCON-U Single port PoE power injector UL 294 Listed
- or another UL 294 approved PoE power injector
2.2  MiY Indoor Device Overview

2.2.1  Physical Features
MiY indoor physical access devices are housed in a rugged plastic casing and can provide various modes for identification, verification and multi-factor authentication. The following subsections provide an introduction to the physical characteristics of MiY indoor devices.

2.2.1.1  Display
All MiY-Touch devices have a 3.5” color QVGA screen.
On the Cogent Gate application, the upper right screen of the display has a connectivity status icon. This icon shows the device’s registration and communication status:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Device is unregistered to a server or running in standalone mode. It is considered “unmanaged” and no server on the network can be found.</td>
</tr>
<tr>
<td>🟠</td>
<td>Device is unregistered to a server. The device has found a server on the network and is “pending registration”</td>
</tr>
<tr>
<td>🕷️</td>
<td>Device is registered to a server and has exchanged security tokens for an encrypted TLS communication. The server is on-line and communicating with this device.</td>
</tr>
<tr>
<td>🕶️</td>
<td>Device is registered to a server and has security tokens. Currently the device cannot find the server BUT the server can communicate to the device.</td>
</tr>
<tr>
<td>🕶️</td>
<td>Device is registered to a server and has security tokens. Currently the server cannot be found and is possibly offline. The Device is running independently until the server is available.</td>
</tr>
<tr>
<td>�命周期</td>
<td>There is communication activity between the device and server.</td>
</tr>
</tbody>
</table>

### 2.2.1.2 Fingerprint Sensor

The MiY-Touch device has a built-in fingerprint sensor that is rated for indoor use ONLY.

![Fingerprint Sensor](image)

### 2.2.1.3 Admin Port and Reset Button

The bottom of the device has the Admin port and reset button.
2.2.1.4 Wall Mount
The stainless steel mounting bracket can be attached to a single gang box. The MiY-Touch has a hinge at the bottom which allows installers to latch the device on the wall and access the terminal blocks for ease of installation.
2.2.1.5 Back Panel and Connections
The back panel of MiY-Touch device is completely exposed.

MiY Devices have the following rear connections:

- Power over Ethernet Port
- Terminal Block A
- Terminal Block B
- Terminal Block C
- External USB Port
- Soft Dip Switch
2.2.1.6 USB Ports

The MiY-Touch device has three (3) USB ports that are configurable. The device has a USB host port on the rear of the device, a USB host port on the front of the device and OTG USB client port.

2.2.1.6.1 USB Host Port (Rear of the device)

The USB host port is only accessible from the back panel of the device. The USB host port is used to integrate additional USB components to the device, such as a camera, by adding a driver for the component to the firmware and updating GateApp’s to use the new component.

The USB connectors can be created or purchased. Below are the USB Host Port Pin definitions.

The USB connector should be small and allows the wires to curl within the unit before exiting the compression door.
2.2.1.6.2 USB Host Port (Front of the device)

The USB host port is only accessible by removing the metal lockout bracket from the device. The USB host port is used to integrate additional USB add on modules to the device, such as a card reader, thermal printer, etc.

With the lockout bracket removed, then the USB connector is now exposed on the front of the unit.

The add-on module should slide right into the USB connector.

After the new module has been inserted, then the lockout bracket needs to be secured to the rear of the device. This will help prevent the module from being removed when installed on the unit.
2.2.1.6.3 OTG USB Port

The OTG USB client port is located on the bottom of the device and is disabled by default. An administrator must login to the device menu to enable the OTG port for Normal or Development use.

Normal OTG mode allows for communication between the device and the Device Admin Utility running on a PC or laptop that has the MiY Device Driver installed. The Development mode is designed for use by developers that need the device to communicate with their PC or laptop via Microsoft ActiveSync or Windows Mobile Device Center. Make sure the USB cable on the device side is well connected; some USB cables are shorter and need to be snuggly inserted.

For instructions on enabling the OTG USB port, see the section Enabling the OTG USB Port in this document.

2.2.2 Certifications

The MiY-Touch is FCC and RoHS certified.

Suggested Power Supplies:

12VDC Power supply
- Altronix AL175UL 12VDC UL 294 listed
- or another UL 294 approved 12VDC power supply
POE Power supply

- Infinias S-PCON-U Single port PoE power injector UL 294 Listed
- or another UL 294 approved PoE power injector

3 Installing a MiY Device

3.1 Accessory List

The following items are included in the MiY package:

- Terminal blocks
- Security screws (2)
- Security screw tool
- Installation CD
- Installation Guide

3.2 Mounting the Bracket

To mount the wall bracket:

1. Screw the bracket into the gang box in the wall based on the below images. The MiY-Card, MiY-Search, and MiY-Touch bracket attaches to a single gang box, whereas the MiY-ID bracket will work on either a single gang or double gang box.
Mounting the Bracket

**NOTE:** Ensure that the wires are pulled through the bracket so they are easily accessible

2. Place the device’s bracket hinge pin on the hooked mounting bracket

![Attaching the Hinge Pin to the Mounting Bracket](image)

### 3.3 Wiring Installation

Lift the compression panel so that the terminal blocks and connectors are exposed. See below for a diagram which shows the connectors available under the compression panel.
The Ethernet port is a PoE port that can deliver both power and communication to MiY devices and allows the devices to function without requiring additional 12V cables. If both wires are connected to the device, the additional power source will work as a hot-swap redundant power source. Refer to the following tables for descriptions of the pins in Terminal Blocks A, B, and C.

### Pin descriptions for Terminal Blocks A, B, and C:

#### Low-Profile Terminal Block A

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Earth Ground</td>
</tr>
<tr>
<td>A2</td>
<td>Relay +</td>
</tr>
<tr>
<td>A3</td>
<td>Relay -</td>
</tr>
<tr>
<td>A4</td>
<td>Power GND</td>
</tr>
<tr>
<td>A5</td>
<td>Power (12 V DC)</td>
</tr>
</tbody>
</table>

#### Terminal Block C

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>RS-485 (−)</td>
</tr>
</tbody>
</table>
### 3.4 Connecting the Power Supply to the MiY Device

The following subsections detail the connection of a power supply to the MiY Device.

**NOTE**: All of the MiY electrostatic protection circuits are connected to the Earth Ground (also known as Safety Ground). It is recommended that it be connected to Earth if the Earth Ground is available on site.

#### 3.4.1 Connecting the Power Supply to the Terminal Blocks

To connect 12V power to the MiY-device:

1. Take the terminal block and connect the 12V wire to the last position and the ground wire to the next position.
2. Take a small flat-head driver and tighten the screws to hold the wires in-place.

3. Connect the terminal block to the terminal block connector A. When power is available, the MiY-Device will turn on.

3.4.2 Connecting the Power Supply by Ethernet Port (Power over Ethernet)

Category 5 (CAT-5) Ethernet cables that have Power over Ethernet (PoE) can be connected to the Ethernet port of the MiY device as a supply of power. If the MiY device cannot be powered by Power over Ethernet (PoE), troubleshoot using the procedure detailed in this subsection.

To troubleshoot the MiY's PoE:
1. Connect a CAT-5 Ethernet cable between the Ethernet port of the MiY device and an 802.3af PoE-enabled hub.
2. Connect a CAT-5 Ethernet cable between the Ethernet port of the MiY device and a midspan power injector unit.
3.5 Panel-in Wiring

The Panel in wiring can be done by placing the wire into terminal block slot (B4) LED – like Panel Input (0) as well as connecting a ground cable from the panel to either terminal block slot (A4) Power GND or (C4) Wiegand Input GND. If your device is connected via Wiegand to an access control panel, then you can connect a wire from (C3) Wiegand Output GND to (C4) Wiegand Input GND.

The administrator will also need to enable the Panel-in check under General settings in the Device Info admin menu.

![Panel-in Wiring Diagram](image)

This can also be done in the MiY-Security Manager under the system settings dialog. Refer to the MiY Security Manager User Guide for instructions.

For most physical access panels the Panel-in (LED line) can be directly connected without a resistor. It is recommended to use 18 gauge wire for the panel-in (LED line), using a thinner wire may cause the Lock Icon LED on the front of the device to toggle quickly between red/green during authentication. The amount of resistance depends on the gauge and length of the Panel-In (LED) wire. The resistor should be added in series. It is recommended to use a 2K ohm resistor to assist the signal; alternatively a 1K to 3K range can be used depending on the length and gauge of the wire.

3.6 Relay & Line Trigger Wiring

Relay and Line Trigger wiring can be done by placing the wire into the correct terminal block and turning the tightening screw to ensure the wire will stay in place.
Devices from the MiY product line have a built-in 12V relay with maximum amperage of 170mA and fingerprint support Integrated Door Access Control (Relay, REX, Contact Monitor).

When the MiY device is fully operational, the relay output signal is normally open. A successful authentication will close the circuit, sending a 5V 170mA signal to the relay.

Devices from the MiY product line also have a built-in 5V line trigger with maximum amperage of 170 mA that can be used to communicate with a door lock or an LED.

The device supports and is compatible with:

- A dead bolt or door strike
- A snubber diode to protect regulated DC power supply from inductive kickback (1N4007 diode or equivalent recommended)
- A separate power supply for the dead bolt or door strike based on supplier's recommendations
- An optional external relay for locks that are higher than 170 mA

3.6.1 Single Door Control

The Single-Door Control option does not require Wiegand Output signals

An example Single-Door Control option utilizes the following components or equivalent pieces:
- HES 5200 Striker
- HES Smart PAC II power controller
- 12V power supply
- NTE R40-11D2-12 relay coil
3.7 Securing the MiY Devices on the Wall

Once the wires are connected, run the wires downwards so that they pass the compression pad. The wires should be evenly distributed to create the best possible seal between the top and bottom compression pads.

**WARNING:** Grouping wires together can create a gap, allowing water and dust to enter the device. Also not screwing down the compression pad will reduce the Industrial Protection capabilities of the device.
Installing a MiY Device

Proprietary Wire Distribution

Top Compression Pad
Bottom Compression Pad
Ethernet
12V
Ground Wire

Good!

Bad!!!
1. Screw down and tighten the screws on the compression panel so the compression pads conform to the wires and create a seal.

2. Pivot the device on the bracket hinge and bring it up over the wall mount.
3 Secure the device by using the security-screw driver to insert and tighten the security screws on both sides of the MiY-Device.

4 Verify that the security screws are in place by attempting to rotate the device off the mounting bracket by its hinge at the bottom. The device should feel secured and not loose.

### 3.8 Balancing the Termination

For the last device on the line, you should add a termination resistor to the terminal block before plugging it into the device. The following information provides details to assist with the proper configuration of the RS-485 Standard and is reserved for expert users.

The RS-485 Standard permits a balanced transmission line to be shared in a multidrop mode. You are allowed up to 32 driver/receiver pairs that can share a multidrop network. The range of the common mode voltage $V_{cm}$ that the driver and receiver can tolerate is expanded to $+12$ to $-7$ volts. Since the driver can be disconnected from the line, it must withstand this common mode voltage range while in the tristate condition. Termination is required for high data rates and long wiring runs.

Termination is used to match impedance of a node to the impedance of the transmission line being used. When impedances are mismatched, the transmitted signal is not completely absorbed by the load and a portion is reflected back into the transmission line. If the source, transmission line, and load impedance are equal, these reflections are eliminated.

There are disadvantages to termination as well. Termination increases load on the drivers, increases installation complexity, changes biasing requirements, and makes system modification more difficult. The decision whether or not to use termination should be based on the cable length and data rate used by the system.
A good rule of thumb is that if the propagation delay of the data line is much less than one bit width, termination is not needed. This rule makes the assumption that reflections will damp out in several trips up and down the data line. Since the receiving UART will sample the data in the middle of the bit, it is important that the signal level be solid at that point. For example, in a system with 2000 feet of data line the propagation delay can be calculated by multiplying the cable length by the propagation velocity of the cable. This value, typically 66–75% of the speed of light (c), is specified by the cable manufacture.

For our example, a round trip covers 4000 feet of cable. Using a propagation velocity of 0.66 × c, one round trip is completed in approximately 6.16 μs. If we assume the reflections will damp out in three “round trips” up and down the cable length, the signal will stabilize 18.5 μs after the leading edge of a bit. At 9600 baud one bit is 104 μs wide. Since the reflections are damped out much before the center of the bit, termination is not required.

There are several methods of terminating data lines. The method recommended by B&B Electronics is parallel termination. A resistor is added in parallel with the receiver’s “A” and “B” lines in order to match the data line characteristic impedance specified by the cable manufacture (120 Ω is a common value)

This value describes the intrinsic impedance of the transmission line and is not a function of the line length. A terminating resistor of less than 90 Ω should not be used. Termination resistors should be placed only at the extreme ends of the data line, and no more than two terminations should be placed in any system that does not use repeaters. This type of termination clearly adds heavy DC loading to a system and may overload port powered RS-232 to RS-485 converters.

Another type of termination, AC coupled termination, adds a small capacitor in series with the termination resistor to eliminate the DC loading effect. Although this method eliminates DC loading, capacitor selection is highly dependent on the system properties.

System designers interested in AC termination are encouraged to read National Semiconductors Application Note 9032 for further information. Refer to the illustration of both parallel and AC termination on an RS-485 two-wire node. In four-wire systems, the termination is placed across the receiver of the node.
Parallel and AC Termination

### 3.9 Wiegand Panel Wiring

The Wiegand interface uses three wires, one of which is a common ground and two of which are data transmission wires usually called DATA0 and DATA1, alternately labeled 'D0' and 'D1' or 'Data Low' and 'Data High'. When no data is being sent both DATA0 and DATA1 are pulled up to the 'high' voltage level - usually +5 VDC. When a 0 is sent the DATA0 wire is pulled to a low voltage while the DATA1 wire stays at a high voltage. When a 1 is sent the DATA1 wire is pulled to a low voltage while DATA0 stays at a high voltage.

A high voltage level of +5VDC is used to accommodate for long cable runs (most reader manufacturers publish a maximum of 500 feet) from door readers to the associated access control panel typically located in a secure closet. An 18-22 AWG cable should be used for this connection. At 18 AWG, a distance of 500 feet between the reader and access control panel can be achieved.

**NOTE:** You **MUST** use 18 AWG wiring for distances greater than 100 feet

Most Wiegand panels have a built in pull-up circuit, but be aware that if your secure panel does not have this feature, it is required to add a 5V pull-up to the termination at the Wiegand panel.

![Pull up resistor for Wiegand output](image)
Installing a MiY Device

Sample UL294 compliant wiring diagram using Power Over Ethernet

Sample UL294 compliant wiring diagram using 12 VDC
4 Network Installation

MiY network installation is an automatic process. For details, see the MiY Security Manager User Guide.

However, should a manual installation be necessary, the following subsections contain details on manual network configuration for MiY devices.

4.1 Manually Configuring the MiY-Device's Connection

This procedure is performed from the Network screen in the Cogent GateApp. For more information on using the Cogent GateApp, refer to the section Cogent GateApp for Administrators.

4.1.1 TCP/IP Configuration

From the Network screen, you can set the device to either DHCP or Static mode, and enter the TCP listening port, TLS, and RS485 detection settings.

4.1.1.1 To configure TCP/IP on MiY Outdoor Devices:

1. From the Admin Menu screen select Device Info. The Device Info screen will be displayed
2 From the Device Info screen, select Network. The Network screen will be displayed.

![Network Screen]

3 From the Network screen, you can view the current network configuration. Select Change to modify the configuration. The Protocol screen will be displayed.

![Protocol Screen]
4 From the **Protocol** screen, select the **Ethernet** protocol and select **OK**. The **Mode** screen will be displayed.

![Mode Screen](image)

5 From the **Mode** screen, select the **DHCP** or **Static** mode and select **OK**.
   - If **Static**, the **IP Address** screen will be displayed
   - If **DHCP**, skip to step 9. The **TCP Port** screen will be displayed

![IP Address Screen](image)

6 From the **IP Address** screen, enter each Octet and select **Next** to move to the next Octet. Select **OK** when the **IP Address** is complete. The **Subnet** screen will be displayed.
7 From the **Subnet** screen, enter each Octet and select **Next** to move to the next Octet. Select **OK** when the Subnet is complete. The **Gateway** screen will be displayed.

8 From the **Gateway** screen, enter each Octet and select **Next** to move to the next Octet. Select **OK** when the Gateway is complete. The **TCP Port** screen will be displayed.
9 From the **TCP Port** screen, set the port and select **OK**. The **TLS Port** screen will be displayed.

10 From the **TLS Port** screen, set the port and select **OK**. The **Network Review** screen will be displayed.
11 From the **Network Review** screen, select **Save** to commit the changes or **Cancel** to abort the changes.

**4.1.1.2 To configure TCP/IP on MiY Indoor Devices:**

1. From the **Main MiY** screen select **Device Info**. The **Device Info** screen will be displayed.

2. From the **Device Info** screen, select **Network**. The **Network** screen will be displayed. The **Network** screen displays the current connection configuration.
3 Press the Checkmark to modify the configuration. The Protocol screen will be displayed.

4 From the Protocol screen, select the Ethernet protocol and select Checkmark. The Mode screen will be displayed.
5 From the Mode screen, select the DHCP or Static mode and select Checkmark.
   - If you select Static, the IP Address screen will be displayed.
   - If you select DHCP, skip to step 9. The TCP Port screen will be displayed. For an example of the TCP Port screen.

6 From the IP Address screen, click on the Keyboard and enter each Octet and select the #, Pound Button to move to the next Octet. Click on the Checkmark when the IP Address is complete. The Subnet screen will be displayed.
7 From the **Subnet** screen, click on the **Keyboard** and enter each Octet and select the #, **Pound Button** to move to the next Octet. Click on the **Checkmark** when Subnet is complete. The **Gateway** screen will be displayed.

8 From the **Gateway** screen, click on the **Keyboard** and enter each Octet and select the #, **Pound Button** to move to the next Octet. Click on the **Checkmark** when the Gateway is complete. The **TCP Port** screen will be displayed.
From the **TCP Port** screen, set the port and click on the **Checkmark**. The **TLS Port** screen will be displayed.

From the **TLS Port** screen, set the port and click on the **Checkmark**. The **Network Review** screen will be displayed.
11 From the Network Review screen, click on the Checkmark to commit the changes or the Arrow to abort the changes and return to the previous menu.

4.1.2 Configuring RS485 Connection Settings

This section will show you how to change the device communication from Ethernet to RS485.

4.1.2.1 To configure RS485 connection settings:

1. From the Admin Menu screen select Device Info. The Device Info screen will be displayed.

2. From the Device Info screen, select Network. The Network screen will be displayed
3 From the **Network** screen, you can view the current network configuration. Select **Change** to modify the configuration. The **Protocol** screen will be displayed.

![Network Screen]

4 From the **Protocol** screen, select the **RS485** protocol and select **OK**. The **Baud Rate** screen will be displayed.

![Protocol Screen]
5  From the **Baud Rate** screen, select the baud rate and select **OK**. The **Network Review** screen will be displayed.

6  From the **Network Review** screen, select **Save** to commit the changes or **Cancel** to abort the changes.

4.1.2.2 **To configure RS485 on MiY Indoor Devices:**

1  From the **Main MiY** screen, select **Device Info**. The **Device Info** screen will be displayed
2. From the **Device Info** screen, select **Network**. The **Network** screen will be displayed.
3 From the **Network** screen, you can view the current network configuration. Click on the **Checkmark** to modify the configuration. The **Protocol** screen will be displayed.

![Protocol Screen](image1)

4 From the **Protocol** screen, select the **RS485** protocol and click on the **Checkmark**. The **Baud Rate** screen will be displayed.

![Baud Rate Screen](image2)
5 From the Baud Rate screen, select the baud rate and click on the Checkmark. The Network Review screen will be displayed.

![Network Review Screen]

6 From the Network Review screen, click on the Checkmark to commit the changes or Arrow to abort the changes and return to the previous menu.
5 Registering the Reader with MiY-Security Manager

5.1 Basic Zone Creation

Once the MiY device has been installed, use MiY Security Manager software to register the device and set up zones. For details on managing devices, see the *MiY Security Manager User Guide*.
MiY Security Manager Zones & Devices Window
This page was intentionally left blank.
6 Upload Package via USB

NOTE: The Device Admin Utility can always export data from a device, but can only send data to a device when the device is in standalone mode.

MiY devices are shipped in Standalone mode (no MiY-Server or MiY-Security Manager required) and remain in standalone mode until registered to a server. Once registered to a server, the device is considered to be in managed mode because it is controlled by the server. To return the device back to standalone mode, the device must be unregistered from the server either from the device menu (Reset Sitekey) or from the MiY-Security Manager (Remove device).

All device data (users, operators, prints, logs, packages, etc.) can be imported and exported to and from the device via the OTG USB port with the MiY Device Admin Utility. The Device Admin Utility is used to deploy packages (Firmware, Nurse and GateApp) to the device while in standalone mode.

In order to use the OTG USB port, it must be enabled. To enable the OTG USB port, refer to the section Enabling the OTG USB Port.

6.1 Deploying a Package

To deploy a package using the Device Admin Utility:

1. Install and run the MiY Device Admin Utility application on your PC or laptop.
2. Connect the OTG USB port on the bottom of the device to your PC or laptop with a USB cable. We recommend that you use a USB cable with a ferrite bead embedded into the cable.
3. Set the OTG USB port on the MiY device to Normal mode. The device will be displayed in the PACS Device Manager as a “MiY Device”. Refer to the subsection Enabling the OTG USB Port for details.

NOTE: The MiY Device Driver should be installed by the Device Admin Utility installer. However, if the driver is not installed, the device will be displayed with an exclamation point. Perform a manual installation of the MiY Device Driver via the PC’s Device Manager, Add New Device wizard, or other preferred method. From here, you can point to the MiY Device Driver files to install the driver for the unknown device.
4 From the Device Admin Utility, select **Indicate** to verify you are connecting to the correct device. The device LEDs should flash and you should hear a sound.

5 Select **Connect** to connect to the device.

**NOTE:** If the connect button is disabled, communication between the device and the PC or laptop is not functioning correctly. This could be for several reasons: the device is not physically connected to the PC or laptop via USB cable, the device OTG USB mode is not set to Normal, the MiY Device Driver is not installed on the PC or laptop or the USB port on the device or PC/laptop is not functioning correctly.
6. After successfully connecting, select the top-left menu button.

7. Select **Open** from the menu. The **Open** window will be displayed.
8 From the **Open** window, browse for your file. Select the appropriate package and click **Open**. The **Open** window will close, and if the package is valid, its basic information will be displayed in the Device Admin Utility.
9 Click **Send** to upload the package to the device. The “Sending Package File…” message will be displayed in the output window, and the **Send/Send All** buttons are disabled until the operation is complete.

10 If successfully sent to the device, a success message will be displayed. Your package will be extracted and installed appropriately.

**NOTE:** Depending on the size of the package, the extraction and installation processing time will vary. If installing a GateApp package, the currently running GateApp on the device, exit, and the Nurse application will be displayed. This means that your package is being installed and should be complete in a few minutes.

**NOTE:** Firmware packages contain the entire Windows CE OS and take considerably longer than the Nurse and GateApp packages. Firmware and Nurse packages will automatically reboot the device before returning to normal operation. GateApp packages will automatically start the GateApp if no application errors exist. See the *MiY GateApp Development Guide* for details.
This page was intentionally left blank.
7  Cogent GateApp for Administrators

Each of the MiY devices has the Cogent GateApp installed. This section explains how to use the Cogent GateApp’s administrator functionality.

7.1  Logging in to Access Admin Functions

Once the MiY device has been installed and configured, the Operator Login screen will be displayed.

7.1.1  To access the MiY Admin Menu on MiY Outdoor Devices:

1  Select the “ * Star” button followed by the “ # Pound ” button to begin admin login. The Operator Login screen will be displayed.

   Operator Login Screen

2  Enter your **User Name** and select **OK**. The **Password Input** screen will be displayed.
3. From the **Password** screen, enter your password and select **OK**. The password will be displayed as asterisks as you enter it. Once the password has been entered, select **OK**. The **MiY Main** screen will be displayed.

4. From this screen you can obtain device information, manage users, view packages and logs, and use the **Nurse** functionality.

### 7.1.2 To access the MiY Admin Menu on MiY Indoor Devices:

1. Once the MiY device is powered on, press the top of the screen and swiping downward will take the user to the **Cogent Gate Log In** screen will be displayed.
5. Click on the **Keyboard** to enter your **User Name**. Once you have completed typing in the User Name, click on the **OK** button.

2. The **User Name** that you entered will now appear on the screen. Click on the **Checkmark** to continue to the **Password** screen.
6 From the **Password** screen, enter your password. The password will be displayed as asterisks. Once the password has been entered, click on the #, **OK key**.

**NOTE:** The default password for an unmanaged device (device is **NOT** registered to a server) is **7890**.

7 The **Main MiY** screen will be displayed
7.2 Managing the Device

The Device Info option allows you to set how the device will verify users, change network settings, security settings, and other device management.

7.2.1 Viewing Device Info

7.2.1.1 To view device settings on MiY Outdoor Devices:

1. From the Admin Menu screen, select Device Info. The Device Info screen will be displayed.

2. To view general information about the device, select General. The General screen will be displayed.
7.2.1.2 To view device settings on MiY Indoor Devices:

1. From the Admin Menu screen, select Device Info. The Device Info screen will be displayed.

2. To view general information about the device, select General. The General screen will be displayed.

7.2.2 Changing Device Network Settings

From the Network screen, you can set either DHCP or Static mode, and enter the TCP listening port, TLS, and RS485 detection settings.
MiY network installation is an automatic process in most cases. For details, refer to the *MiY Security Manager User Guide*.

For instructions regarding the manual configuration of MiY device network settings, refer to the section *Network Installation*.

**To view network information:**

From the **Device Info** screen, select **Network**. The **Network** screen will be displayed.

**7.2.3 Changing Device Security Settings**

From the **Security** screen, you can set the verification mode for the device, set capture timeout length, security level, server timeout length, and standalone mode.
To manage your device security settings:

1. From the **Device Info** screen, select **Security**. The **Security** screen will be displayed. Navigate up and down and select the item to edit.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthenticationMode</td>
<td>(6) Contactless +</td>
</tr>
<tr>
<td>SecurityLevel</td>
<td>Normal</td>
</tr>
<tr>
<td>CaptureTimeout</td>
<td>30</td>
</tr>
<tr>
<td>ServerMatchTimeout</td>
<td>60</td>
</tr>
<tr>
<td>Live Finger</td>
<td>Disabled</td>
</tr>
<tr>
<td>FailedMatchRetryAtt</td>
<td>1</td>
</tr>
<tr>
<td>PINRetryAttempts</td>
<td>1</td>
</tr>
<tr>
<td>CardFingerprintTemp</td>
<td>MMF</td>
</tr>
</tbody>
</table>

![Security Screen for MiY Outdoor Devices](image)

2. From the **Verify Mode** dropdown menu, select how you want the device to verify users. Depending on the MiY device you are using, the options are:

<table>
<thead>
<tr>
<th>Number</th>
<th>Authentication Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>On Device Finger Search</td>
</tr>
<tr>
<td>(2)</td>
<td>On-Server Finger Search</td>
</tr>
<tr>
<td>(3)</td>
<td>On-Device Finger Search, If no-hit On Server</td>
</tr>
<tr>
<td>(4)</td>
<td>Contactless</td>
</tr>
<tr>
<td>(5)</td>
<td>Contactless + PIN</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>(6)</td>
<td>Contactless + Finger</td>
</tr>
<tr>
<td>(7)</td>
<td>Contactless + PIN + Finger</td>
</tr>
<tr>
<td>(8)</td>
<td>Panel ID</td>
</tr>
<tr>
<td>(9)</td>
<td>Panel ID + PIN</td>
</tr>
<tr>
<td>(10)</td>
<td>Panel ID + Finger</td>
</tr>
<tr>
<td>(11)</td>
<td>Panel ID + PIN + Finger</td>
</tr>
<tr>
<td>(12)</td>
<td>Wiegand In + Finger</td>
</tr>
<tr>
<td>(13)</td>
<td>Multimode (On Device Finger Search, Contactless + Finger, Panel ID + Finger)</td>
</tr>
</tbody>
</table>

From the **Security Level** dropdown menu, select the level of security for the device. **The options are:**

Verify Mode for MiY Outdoor Devices

Verify Mode for MiY Indoor Devices
• **Convenient**: Finger matching thresholds and algorithms are tuned for convenience and security.

• **Normal**: Finger matching thresholds and algorithms are turned for security.

• **High**: Finger matching thresholds are set higher for added security.

4 From the **Capture Timeout** dropdown menu, select the number of seconds after a print is submitted before timeout.

5 From the **Server Match Timeout** dropdown menu, select the number of seconds until the server times out during a search.

6 From the **Live Finger** dropdown menu, select **Enabled** or **Disabled** depending on whether you want to enforce liveness detection. NOTE: This will increase the amount of time to capture a fingerprint.

7 From the **Failed Match Retry Attempts** menu, input the number of attempts you’ll allow a user to retry their biometric match before you deny them access.

8 From the **Pin Retry Attempts** menu, input the number of attempts you'll allow a user to retry entering their pin before you deny them access.

9 From the **Card Fingerprint Template Format** dropdown menu, select **MMF** or **MPK** depending if your facility is using a legacy population of MPK cards issued from SecurSetup.

10 From the **Card Site ID** menu, input the primary card Site ID that is written to the smart cards.

11 From the **Card Site ID Secondary** menu, input the secondary card Site ID that is accepted by the readers.

12 From the **Relay Out Duration** menu, input the amount of time (in milliseconds) that you want the 12V relay out to remain on after a successful authentication.

13 From the **Line Trigger Out Duration** menu, input the amount of time (in milliseconds) that you want the 5V line trigger to remain on after a successful authentication.

14 From the **Wiegand Output Enabled** dropdown menu, select **True** or **False** depending if the device is connected to a Physical Access Control Panel or another wiegand based device.

15 From the **Wiegand Passthrough** dropdown menu, select **Enabled** or **Disabled** depending if you have another device that outputs data over wiegand that you want funneled through the MiY device.

16 From the **Cardholder Assigned** dropdown menu, select **Enabled** or **Disabled** if you only want cardholders who have been added to the specific device to have access to the reader or not.

17 From the **Disable Tamper** dropdown menu, input the amount of time (in minutes) that you want the tamper switch notification to be disabled while the device is undergoing maintenance.

### 7.3 Managing Users

From the **Users** screen you can add, modify, delete, and promote users.
7.3.1 Adding Users

7.3.1.1 To add users on MiY Outdoor Devices:

1. From the Admin Menu screen, select Users. The Users screen will be displayed.

2. To add a new user, select Add User. The Add User Wizard will begin starting with the Panel ID screen.

3. From the Panel ID screen, enter the user’s Panel ID and select OK to proceed to the next step in the wizard. Similar screens for entering PIN, Last, and First name will follow. From the Special Flag dropdown menu, select None, No Fingers, or Poor Prints.

4. After you have finished the Add User Wizard, the User Information screen will be displayed.
5. From the **User Information** screen, select **Enroll** to begin capturing the new user's fingerprints. The **Finger Selection** screen will be displayed.

6. Select which finger you want to enroll and select **Capture**. The **Finger Enrollment** screen will be displayed.
7 Instruct the user to place and hold the finger indicated on screen on the fingerprint sensor. The **Enrolling** screen will be displayed. Note that a minimum of two impressions are required and if a poor quality image is captured the system will continue to ask for impressions up to six impressions. All impressions are used to improve the accuracy of the system.

8 Once enrollment is complete, the **Lift Finger** screen will be displayed. Instruct the user to briefly lift his or her finger during matching.
9 Instruct the user to place his or her finger on the sensor again. The **Enrollment Successful** screen will be displayed, indicating that enrollment is complete.

10 Repeat steps 5 thru 9 until all desired fingers are enrolled. Select **Return** from the **Finger Selection** screen when finished enrolling fingers.

11 Select **Save** from the **User Information** screen to commit all user information or **Cancel** to abort.

**7.3.1.2 To add users on MiY Indoor Devices:**

1 From the **Admin Menu** screen, select **Users**. The **Users** screen will be displayed.
2 To add a new user, select Add User. The Add User Wizard will begin starting with the Panel ID screen.

3 From the Panel ID screen, enter the user's Panel ID and select OK to proceed to the next step in the wizard. Similar screens for entering PIN, Last, and First name will follow. From the Special Flag dropdown menu, select None, No Fingers, or Poor Prints.

4 After you have finished the Add User Wizard, the User Information screen will be displayed.
From the User Information screen, click on the Fingerprint to begin capturing the new user’s fingerprints. The Finger Selection screen will be displayed.

Select which finger you want to enroll and select Capture. The Finger Enrollment screen will be displayed.
7 Instruct the user to place and hold the finger indicated on screen on the fingerprint sensor. The Enrolling screen will be displayed. Note that a minimum of two impressions are required and if a poor quality image is captured the system will continue to ask for impressions up to six impressions. All impressions are used to improve the accuracy of the system.

8 Once enrollment is complete, the Lift Finger screen will be displayed. Instruct the user to briefly lift his or her finger during matching.
9 Instruct the user to place his or her finger on the sensor again. The **Enrollment Successful** screen will be displayed, indicating that enrollment is complete.

10 Repeat steps 5 thru 9 until all desired fingers are enrolled. Click on the **Arrow** from the **Finger Selection** screen when finished enrolling fingers.

11 Click on the **Checkmark** from the **User Information** screen to commit all user information or click on the **Arrow** to abort and return to the previous screen.

### 7.3.2 Modifying Users

#### 7.3.2.1 To modify an existing user on MiY Outdoor Devices:

1 From the **Users** screen, select **Modify User**. The **Search User Wizard** will begin starting with the **Panel ID** screen.
2 Enter desired search criteria and select **OK** or simply select **OK** for each screen in the wizard to search all users. The **User List** will be displayed.

![User List](image)

3 From the list of users, select the user you want to modify. The **User Information** screen will be displayed.

![Modify User](image)

4 Enter your modifications and select **Save**. The **Success** screen will be displayed, and the device will return to the **Users** screen when the modifications have been accepted.
7.3.2.2 To modify an existing user on MiY Indoor Devices:

1. From the Users screen, select Modify User. The Search User Wizard will begin starting with the Panel ID screen.

2. Enter desired search criteria and click on the Checkmark or simply click on the Checkmark for each screen in the wizard to search all users. The User List will be displayed.

3. From the list of users, select the user you want to modify. The User Information screen will be displayed.
Enter your modifications and click on the **Checkmark** to save the changes. The **Success** screen will be displayed, indicating that the modifications have been accepted.

### 7.3.3 Deleting Users

**7.3.3.1 To delete a user on MiY Outdoor Devices:**

1. From the **Users** screen, select **Delete User**. The **Search User Wizard** will begin starting with the **Panel ID** screen.
2. Enter desired search criteria and select **OK** or simply select **OK** for each screen in the wizard to search all users. The **User List** will be displayed.
3 The **Success** screen will be displayed, indicating you have successfully deleted the user.

7.3.3.2 To delete a user on MiY Indoor Devices:

1. From the **Users** screen, select **Delete User**. The **Search User Wizard** will begin starting with the Panel ID screen.
2. Enter desired search criteria and click on the Checkmark or simply click on the Checkmark for each screen in the wizard to search all users. The User List will be displayed.

```
User List
```

3. The Success screen will be displayed, indicating you have successfully deleted the user.

```
Success Screen
```

### 7.3.4 Promoting Users

By Promoting Users, you can promote a user to an operator.

**7.3.4.1 To promote an existing user on MiY Outdoor Devices:**

1. From the Users screen, select Promote User. The Search User Wizard will begin starting with the Panel ID screen.
2 Enter desired search criteria and select OK, or select OK for each screen in the wizard to search all users. The User List will be displayed.

3 From the list of users, select the user you want to promote and select OK. The New Operator Wizard will be displayed starting with the User Name screen.

4 Enter the new operator’s User Name and select OK. The User Password screen will be displayed.
Enter the user password and select **OK**. The **User Password Confirmation** screen will be displayed.

Enter the confirm password and select **OK**. The **Success** screen will be displayed, indicating you have successfully added a new operator.
7.3.4.2 To promote an existing user on MiY Indoor Devices:

1. From the Users screen, select Promote User. The Search User Wizard will begin starting with the Panel ID screen.
2. Enter desired search criteria and click on the **Checkmark** or simply click on the **Checkmark** for each screen in the wizard to search all users. The **User List** will be displayed.

![User List](image1.png)

3. From the list of users, select the user you want to promote and click on the **Checkmark**. The **New Operator Wizard** will be displayed starting with the **User Name** screen.

![New Operator Screen](image2.png)
4 Enter the new operator’s User Name and click on the Checkmark. The User Password screen will be displayed.

5 Enter the user password and click on the Checkmark. The User Password Confirmation screen will be displayed.
6 Enter the confirm password and click on the Checkmark. The Success screen will be displayed, indicating you have successfully added a new operator.

7.3.5 Demoting Users

By Demoting Users, you can revoke an operator’s administrator status.

7.3.5.1 To demote an existing user on MiY Outdoor Devices:

1 From the Users screen, select Demote User. The Operator List will appear with all of the operators that are currently on the system.

2 Select the desired operator you want to demote and click OK. The Demote User Confirmation will be displayed.
3 Select OK to demote your desired user.

7.3.5.2 To demote an existing user on MiY Indoor Devices:

1 From the Users screen, select Demote User. The Operator List will appear with all of the operators that are currently on the system.

2 Select the desired operator you want to demote and click on the Checkmark. The Demote User Confirmation will be displayed.
3 Click on the Checkmark to demote your desired user.

7.4 Enabling the OTG USB Port
The OTG USB port allows administrators to transfer data between a MiY device in standalone mode and a PC. This subsection describes the process of enabling the OTG USB port.

7.4.1 To enable the OTG USB port on MiY Outdoor Devices:

1 From the Admin Menu screen, select the Device Info menu option. The Device Info screen will be displayed.
2. Select the **General** menu option. The **General Info** screen will be displayed. The **Otg Mode** is disabled by default.

![General Info Screen](image)

3. Navigate to the **Otg Mode** from the list of settings and select it. The **Otg Mode** drop-down menu will be displayed.

![Otg Mode Drop-Down Menu](image)

4. Choose the desired mode and select **OK**. The **General Info** screen will be displayed and you can confirm the mode change selected.
5. Select **Save** to commit the changes. A success screen will be displayed, followed by the **Device Info** menu.

### 7.4.2 To enable the OTG USB port on MiY Indoor Devices:

1. From the **Admin Menu** screen, select the **Device Info** menu option. The **Device Info** screen will be displayed.

![Device Info Screen](image)

2. Select the **General** menu option. The **General Info** screen will be displayed. The **Otg Mode** is disabled by default.
3 Navigate to the **Otg Mode** from the list of settings and select it. The **Otg Mode** drop-down menu will be displayed.

4 Choose the desired mode and click on the **Checkmark**. The **General Info** screen will be displayed and you can confirm the mode change selected.
5 Click on the **Checkmark** to commit the changes. A success screen will be displayed, followed by the **Device Info** menu.

### 7.5 Enabling Panel-in Lock Icon

The panel-in lock icon can tell the authenticating user the result of their credential information after it's been submitted to a physical access panel. When the Panel has decided to unlock the door the panel-in LED line can be given a high signal. This high signal can be received by the MiY Device.

**NOTE:** Please ensure that you refer to *Panel-In Wiring* in Section 3.5 of this manual prior to enabling the Panel-In logic.

#### 7.5.1 To enable the Panel-in Lock Icon on MiY Outdoor Devices:

1 From the **Admin Menu** screen, select the **Device Info** menu option. The **Device Info** screen will be displayed.
2. Select the **General** menu option. The **General Info** screen will be displayed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSUrl</td>
<td></td>
</tr>
<tr>
<td>RSSFile</td>
<td>/Storage</td>
</tr>
<tr>
<td>MaxEventLogRecords</td>
<td>600000</td>
</tr>
<tr>
<td>OtgMode</td>
<td>Development</td>
</tr>
<tr>
<td>HIDClassKey</td>
<td></td>
</tr>
<tr>
<td>AdminLockoutTime</td>
<td>5</td>
</tr>
<tr>
<td>UVLedDelay</td>
<td>5</td>
</tr>
<tr>
<td>UVLedDuration</td>
<td>2</td>
</tr>
<tr>
<td>LogsLastUploaded</td>
<td>2012-03-07T00:04:15</td>
</tr>
</tbody>
</table>

3. Browse through the **General Info** screen until you arrive at the following settings:

- **PanelInCheckEnabled**
- **PanelInCheckDuration**

4. Update “**PanelInCheckEnabled**” to be 1. Some Panel manufacturers will have a delayed panel-in response, for this the Check duration can be extended to work with varying panel settings.

### 7.5.2 To enable the Panel-in Lock icon on MiY Indoor Devices:
1 From the **Admin Menu** screen, select the **Device Info** menu option. The **Device Info** screen will be displayed.

![Device Info Screen](image)

2 Select the **General** menu option. The **General Info** screen will be displayed.

![General Info Screen](image)

3 Browse through the **General Info** screen until you arrive at the following settings:

- `PanelInCheckEnabled`
- `PanelInCheckDuration`

4 Update “**PanelInCheckEnabled**” to be “**True**”. Some Panel manufacturers will have a delayed panel-in response, for this the Check duration can be extended to work with varying panel settings.
8  Verifying Users for Access/Entry

MiY devices can support a number of configurations which can be found on the device admin menu under Security in the Device Info menu. The following subsections are examples of workflows readily available on the device which can be modified and configured through the Security menu for more information on the Security menu, refer to the subsection Changing Device Security Settings.

8.1  Verifying Users with the MiY-Search and MiY-Card

The MiY-Search and MiY-Card devices verify users through a combination of the following authentication factors: fingerprint, panel id, pin, and card. Since verification workflows are heavily customizable, the tables in the following subsection describe the step required for each screen displayed on the MiY-Search and MiY-Card devices.

<table>
<thead>
<tr>
<th>Verification Type</th>
<th>Screen Displayed</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fingerprint</strong></td>
<td><img src="image" alt="Fingerprint Screen" /></td>
<td>When prompted by the device, place the appropriate finger on the fingerprint sensor. Upon successful fingerprint verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td><strong>Panel ID</strong></td>
<td><img src="image" alt="Panel ID Screen" /></td>
<td>When prompted by the device with the top screen, press the “0” key on the number pad. The bottom screen will be displayed. Using the number pad, enter the appropriate Panel ID number. Upon successful Panel ID verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td>Verification Type</td>
<td>Screen Displayed</td>
<td>Instructions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PIN</td>
<td><img src="image1" alt="PIN Screen" /></td>
<td>When prompted by the device, use the number pad on the device to enter the appropriate PIN. Upon successful PIN verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td>(Personal Identification Number)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card*</td>
<td><img src="image2" alt="Card Screen" /></td>
<td>When prompted by the device with the top screen, place the appropriate card on the reader located on top of the device. This area will be indicated by blue flashing LEDs. Do not remove the card from the reader. While the bottom screen is displayed, keep the card on the reader. Upon successful card verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td>*Only available on MiY-Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-Mode Verification*</td>
<td><img src="image3" alt="Multi-Mode Screen" /></td>
<td>When this screen is displayed, it indicates that the device is in multi-mode. Presenting a card, finger, or Panel ID will initiate a multi-step workflow for verification.</td>
</tr>
<tr>
<td>*Only available on MiY-Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success</td>
<td><img src="image4" alt="Success Screen" /></td>
<td>Upon successful user verification, this screen will be displayed on the device. The device will then perform the action programmed for a verification event (e.g. unlock the door).</td>
</tr>
</tbody>
</table>

*Proprietary*
8.2 Verifying Users with the MiY-ID Device

Since verification workflows are heavily customizable, the tables in the following subsection describe the step required for each screen displayed on the MiY-ID device.

<table>
<thead>
<tr>
<th>Verification Type</th>
<th>Screen Displayed</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fingerprint</strong></td>
<td>![Fingerprint Screen]</td>
<td>When prompted by the device, place the appropriate finger on the fingerprint sensor. Upon successful fingerprint verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td><strong>Panel ID</strong></td>
<td>![Panel ID Screen]</td>
<td>When prompted by the device, use the number pad to enter the appropriate Panel ID number. Upon successful Panel ID verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td><strong>PIN</strong> (Personal Identification Number)</td>
<td>![PIN Screen]</td>
<td>When prompted by the device, use the number pad on the device to enter the appropriate PIN. Upon successful PIN verification, the device will display the next screen in the verification workflow.</td>
</tr>
</tbody>
</table>
## 8.3 Verifying Users with the MiY-Touch

The MiY-Touch devices verify users through a combination of the following authentication factors: fingerprint, panel id, pin, and card. Since verification workflows are heavily customizable, the tables in the following subsection describe the step required for each screen displayed on the MiY-Touch devices.

<table>
<thead>
<tr>
<th>Verification Type</th>
<th>Screen Displayed</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| **Card**          | ![Card Screen](image) | When prompted by the device with the top screen, place the appropriate card on the reader located on top of the device. This area will be indicated by blue flashing LEDs. Do not remove the card from the reader.  
Keep the card on the reader while the bottom screen is displayed.  
Upon successful card verification, the device will display the next screen in the verification workflow. |
| **Multi-Mode Verification** | ![Multi-mode Screen](image) | When this screen is displayed, it indicates that the device is in multi-mode.  
Presenting a card, finger, or Panel ID will initiate a multi-step workflow for verification. |
| **Success**       | ![Success Screen](image) | Upon successful verification, this screen will be displayed on the device.  
The device will then perform the action programmed for a verification event (e.g. unlock the door). |
<table>
<thead>
<tr>
<th>Verification Type</th>
<th>Screen Displayed</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fingerprint</strong></td>
<td><img src="image1" alt="Screen Displayed" /></td>
<td>When prompted by the device, place the appropriate finger on the fingerprint sensor. Upon successful fingerprint verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td><strong>Panel ID</strong></td>
<td><img src="image2" alt="Screen Displayed" /></td>
<td>When prompted by the device, use the number pad, and enter the appropriate Panel ID number. Upon successful Panel ID verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td><strong>PIN</strong></td>
<td><img src="image3" alt="Screen Displayed" /></td>
<td>When prompted by the device, use the number pad on the device to enter the appropriate PIN. Upon successful PIN verification, the device will display the next screen in the verification workflow.</td>
</tr>
<tr>
<td><strong>Card</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td><img src="image4" alt="Screen Displayed" /></td>
<td>When prompted by the device with the top screen, place the appropriate card on the reader in the add module area. Do not remove the card from the reader. While the bottom screen is displayed, keep the card on the reader. Upon successful card verification, the device will display the next screen in the verification workflow.</td>
</tr>
</tbody>
</table>

<sup>*</sup>Only available with add-on module
<table>
<thead>
<tr>
<th>Verification Type</th>
<th>Screen Displayed</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Mode Verification*</td>
<td><img src="image" alt="Multi-Mode Verification Screen" /></td>
<td>When this screen is displayed, it indicates that the device is in multi-mode.</td>
</tr>
<tr>
<td></td>
<td>* Only available with add-on module</td>
<td>Presenting a card, finger, or Panel ID will initiate a multi-step workflow for verification.</td>
</tr>
<tr>
<td>Success</td>
<td><img src="image" alt="Success Screen" /></td>
<td>Upon successful user verification, this screen will be displayed on the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The device will then perform the action programmed for a verification event (e.g. unlock the door).</td>
</tr>
</tbody>
</table>
A Optimizing Fingerprint Images

A.1 Positioning the Finger on the Fingerprint Sensor

During enrollment, be sure to properly position the finger on the sensor. Figure A-1 illustrates poorly placed fingers. The Cogent algorithm will reject images that do not contain enough minutiae points.

<table>
<thead>
<tr>
<th>Finger</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finger 1</td>
<td>The finger is positioned too high on the sensor and does not offer enough information to accurately enroll an image.</td>
</tr>
<tr>
<td>Finger 2</td>
<td>The finger is positioned too low on the sensor and may not be properly enrolled.</td>
</tr>
<tr>
<td>Finger 3</td>
<td>The fingers are off-center and somewhat rotated. Both of these fingerprint images can result in a failure to properly identify them later on, even if enough minutiae points have been detected.</td>
</tr>
</tbody>
</table>

To ensure successful fingerprint capture, the finger should be properly centered with the application of even pressure and minimal rotation. Figure A-2 is an example of proper finger placement.
## A.2 Things to Remember when Placing a Finger on the Sensor

<table>
<thead>
<tr>
<th>Place your finger quickly with confidently on the surface so that the finger is still when the image is taken.</th>
<th>Do not move or shift your finger while touching the surface. The optical fingerprint sensor is like a camera, so motion blur is or smudging may affect your image quality.</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Finger guide" /></td>
<td><img src="image2.png" alt="Smudging" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use the finger guide. By resting the base of the finger on the plastic and quickly placing the finger on to the optical glass, this will avoid any need for repositioning.</th>
<th>DO NOT poke the sensor and reposition the finger afterwards. This may result in an incomplete print.</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3.png" alt="Finger guide" /></td>
<td></td>
</tr>
</tbody>
</table>
A - Optimizing Fingerprint Images

1. Captured in Step #3 as a full print
2. Captured in Step #2 as an incomplete print
3. [Diagram of fingerprint capture steps]
## A.3 Capturing High-Quality Fingerprints

The condition of the finger itself may affect the image quality of the fingerprint. The following table provides descriptions of typical finger conditions and Cogent’s recommended solutions for ensuring the capture of the highest quality fingerprints.

<table>
<thead>
<tr>
<th>Image</th>
<th>Condition</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Dry Finger" /></td>
<td><strong>Dry Finger</strong>&lt;br&gt;The finger is very dry and difficult to capture.</td>
<td>Perform one of the following actions:&lt;br&gt;• Apply moisture to the finger using oil from your forehead.&lt;br&gt;• Breathe on the finger.&lt;br&gt;• Use a moisturizer that does not contain alcohol.&lt;br&gt;As a last resort, enroll a different finger.</td>
</tr>
<tr>
<td><img src="image2" alt="Wet Finger" /></td>
<td><strong>Wet Finger</strong>&lt;br&gt;Remove excessive moisture from either the finger or the fingerprint sensor.</td>
<td>Perform one of the following actions:&lt;br&gt;• To remove the excessive moisture from your finger, wipe your finger on a cloth or dry tissue to absorb the moisture.&lt;br&gt;• To remove excessive moisture from the fingerprint sensor, please refer to <em>Cleaning the Fingerprint Sensor</em>.</td>
</tr>
<tr>
<td><img src="image3" alt="Damage to Finger" /></td>
<td><strong>Damage to Finger</strong>&lt;br&gt;The fingerprint may have future issues with identification due to the damaged area of the finger.</td>
<td>Enroll a different finger.</td>
</tr>
<tr>
<td><img src="image4" alt="Not Enough Pressure" /></td>
<td><strong>Not Enough Pressure</strong>&lt;br&gt;The user did not apply enough pressure. As a result, the image looks very light and some of the surrounding areas are not captured.</td>
<td>The user should apply moderate but steady pressure; about the same pressure as pressing a button on a telephone.</td>
</tr>
<tr>
<td>Image</td>
<td>Condition</td>
<td>Solution</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="Fingerprint Image" /></td>
<td><strong>Too much Pressure</strong></td>
<td>The user should apply moderate but steady pressure; about the same pressure as pressing a button on a telephone.</td>
</tr>
<tr>
<td></td>
<td>The user is applying too much pressure on the sensor. This distorts the fingerprint image and will make it difficult to identify in the future.</td>
<td></td>
</tr>
</tbody>
</table>
This page was intentionally left blank.
B Maintenance and Troubleshooting

B.1 Cleaning the Fingerprint Sensor

The Fingerprint Sensor is a rugged optical device designed to provide years of trouble-free service. Although the sensor has few maintenance and handling requirements, basic precautions in caring for the sensor will help ensure the best performance over the life of the sensor.

Oily deposits from the user’s fingers can accumulate on the surface of the sensor after repeated uses of the device. These oily deposits may affect the functionality of the sensor. Cogent recommends that the sensor is cleaned once a week or whenever a noticeable accumulation occurs.

The manufacturer of the sensor recommends using rubbing alcohol to clean the sensor surface. The rubbing alcohol will not damage the sensor or reduce the life expectancy of the sensor. Rubbing alcohol is preferred for its ability to dissolve the oily residue, and it evaporates quickly without leaving a residue of its own on the sensor.

**WARNING:** Do not use nylon brushes, scouring pads, or abrasive cleansers even if they contain rubbing alcohol, powder cleaners, or steel wool. Using any of these types of cleaners on the sensor will damage the protective qualities of the sensor against electrostatic discharge. They may damage the sensor’s ability to capture a high quality image of the fingerprint and will void the warranty of the sensor.

Apply enough rubbing alcohol to saturate a clean, lint-free, soft cloth or tissue paper. Wipe the fingerprint sensor in a downward motion. This will remove the oily deposits and prevent any scratching on the surface of the sensor.

**WARNING:** Do not allow alcohol to pool along the edges of the sensor.

B.2 Caring for the Fingerprint Sensor

The fingerprint sensor is designed to perform well even under harsh operating conditions. As with all optical devices, some precautions should be taken to avoid damaging the sensor.

- Do not place the fingerprint sensor close to any heat source that would cause the unit to exceed its standard operating temperatures.
- Do not subject the sensor to shocks or vibrations.
- Do not allow any pointed objects to scratch the surface of the sensor.
- Do not allow any metal to contact the sensor surface.
B.3 Resetting MiY Devices

B.3.1 Factory Reset

To perform a factory reset on MiY Outdoor Devices:

1. Press the power reset button on the bottom of the device (Figure B-1).

2. The device will cycle power, and the keypad LED’s will begin to flash (Figure B-2).

3. While the keypad LED’s are flashing off and on, press the following key combination, depending on the model:

   - For the MiY-ID simultaneously press the first Function key and the 0 key (Figure B-3).
• For MiY-Card and MiY-Search simultaneously press the 1 key and the 0 key (*Figure B-4*).

![Figure B-4 MiY-Card and MiY Search 1 and 0 Keys](image)

4. Lift your fingers from the keypad and press the key combination again.

5. Once the factory reset is initiated, then the LEDs will turn solid; a four color palette will be displayed on the screen (*Figure B-5*). If the LEDs stop blinking and you do **NOT** see the color squares, then start from Step 1.

![Figure B-5 Factory Reset Successfully Initiated](image)

**NOTE:** When pressing the reset key combination, it is recommended to pulse the simultaneous key presses until factory reset is successfully initiated. Just make sure to move your fingers out of the capacitance field in between key presses.

**To perform a factory reset on MiY Indoor Devices:**

1. Flip the unit over, so that the rear of the device with the terminal blocks is facing towards you. Locate the dipswitches on the device (*Figure B-6*).
2. Move both of the dipswitches downward, so that they are both in the down position like in *(Figure B-7).*

![Figure B-7 Dipswitch Position](image)

3. Press the power reset button on the bottom of the device *(Figure B-8).*

![Figure B-8 Power Reset Button](image)

4. The device will power cycle. Once the factory reset is initiated, a four color palette will be displayed on the screen *(Figure B-9).*

![Figure B-9 Factory Reset Successfully Initiated](image)
5. Move the dipswitches upward so that they are in the following position (*Figure B-10*).

![Figure B-10 Dipswitches in Normal Position]

**NOTE:** After the unit is booted up, remember to move the dip switches back to their original position.

### B.4 Contacting Your Distributor

Contact 3M Cogent Support at:

639 North Rosemead Blvd.
Pasadena, CA 91107
(626) 325-9600
[www.cogentsystems.com](http://www.cogentsystems.com)

When you call, please provide:

- The customer name
- Customer phone number
- Contact person name
- A brief description of the problem