

■ Version 1.0

MiY Product Line Device User Guide



©2011 3M Cogent, Inc. All rights reserved.

This document contains commercial information and trade secrets of Cogent, Inc. which are confidential and proprietary in nature and are subject to protection under law. Access to the information contained herein, howsoever acquired and of whatsoever nature, will not entitle the accessor thereof to acquire any right thereto. The data subject to this restriction are contained in all sheets of this document. Disclosure of any such information or trade secrets shall not be made without the prior written permission of Cogent, Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Cogent, Inc.

The information in this document is subject to change without notice. The software mentioned in this document is furnished under license and may only be used or copied in accordance with the terms of such license. Contact software manufacturers directly for terms of software licenses for any software mentioned in this document not originating from Cogent, Inc.

All brand or product names are the trademarks or registered trademarks of their respective holders.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide 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.

MiY-ID with SCM Reader
FCC ID: DGFSSDIDSCM

MiY-ID with HID Reader
FCC ID: DGFSSDIDHID

MiY-Card and MiY-Search
FCC ID: DGFSSDCARDSCM

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 and Industry Canada Rules permitting the operation of this device.

"This Class A digital apparatus complies with Canadian ICES-003."

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

MiY-ID with SCM Reader
IC ID: 458A-SSDIDSCM

MiY-ID with HID Reader
IC ID: 458A-SSDIDHID

MiY-Card and MiY-Search
IC ID: 458A-SSDCARDSCM

Cogent Document # HW-EXT-UG-1277-0.00 (1)

Document Revision History

Version	Date	Author	Comment
0.4	08/25/2010	RC	Initial version
0.5		JL	Updates
0.6	05/03/2011	CC	Updates
0.7	05/09/2011	MH	Updates
0.8	05/11/2011	JL	updates
0.9	05/12/2011	CC	Final review
1.0	07/20/2011	JL	Final release
1.1	09/06/2011	RS	Include unmanaged default password in section 7.1
1.2	10/26/2011	MH	Update OTG cable recommendation
1.3	12/08/2011	MH	Added FCC and IC information

Contents

1	Overview	1
1.1	MiY Product Line Introduction.....	1
1.2	Standard Features	2
1.2.1	Optional Features	3
1.3	Types of Users	4
1.4	Key Terms	4
2	MiY Devices	5
2.1	MiY-Search and MiY-Card Overview	5
2.2	Physical Features	6
2.2.1	Contactless Card Reader	6
2.2.2	Display	6
2.2.3	Keypad	6
2.2.4	Fingerprint Sensor	7
2.2.5	Contactless Card Reader (MiY-ID)	7
2.2.6	Admin Port and Reset Button	8
2.2.7	Wall Mount.....	8
	Back Panel and Connections	9
2.2.8	USB Ports	10
2.2.8.1	USB Host Port.....	10
2.2.8.2	OTG USB Port	10
3	Installing a MiY Device	11
3.1	Accessory List	11
3.2	Mounting the Bracket	11
3.3	Wiring Installation	12
3.4	Connecting the Power Supply to the MiY Device.....	13
3.4.1	Connecting the Power Supply to the Terminal Blocks.....	14
3.4.2	Connecting the Power Supply by Ethernet Port (Power over Ethernet).....	14
3.5	Panel-in Wiring	16
3.6	Relay & Line Trigger Wiring.....	16
3.7	Securing the MiY Devices on the Wall.....	17
3.8	Balancing the Termination	20
4	Network Installation	23
4.1	Manually Configuring the MiY-Device’s Connection.....	23
4.1.1	TCP/IP Configuration	23
4.1.2	Configuring RS485 Connection Settings	28
5	Registering the Reader with MiY-Security Manager	31

5.1	Basic Zone Creation.....	31
6	Upload Package via USB	33
6.1	Deploying a Package	33
7	Cogent GateApp for Administrators	39
7.1	Logging in to Access Admin Functions.....	39
7.2	Managing the Device	40
7.2.1	Viewing Device Info.....	40
7.2.2	Changing Device Network Settings.....	41
7.2.3	Changing Device Security Settings.....	42
7.3	Managing Users.....	44
7.3.1	Adding Users	44
7.3.2	Modifying Users	47
7.3.3	Deleting Users	49
7.3.4	Promoting Users	50
7.3.5	Demoting Users	52
7.4	Enabling the OTG USB Port	53
8	Verifying Users for Access/Entry	57
8.1	Verifying Users with the MiY-Search and MiY-Card.....	57
8.2	Verifying Users with the MiY-ID Device.....	59
A	Optimizing Fingerprint Images	61
A.1	Positioning the Finger on the Fingerprint Sensor.....	61
A.2	Capturing High-Quality Fingerprints	62
B	Maintenance and Troubleshooting	65
B.1	Cleaning the Fingerprint Sensor.....	65
B.2	Caring for the Fingerprint Sensor.....	65
B.3	Resetting MiY Devices	66
B.3.1	Factory Reset.....	66
B.4	Contacting Your Distributor.....	66

1 Overview

1.1 MiY Product Line Introduction

The 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 Standard Features

MiY-Search

- Sandbox API framework support
- IP65 design
- Non-mechanical 12-key keypad
- Rugged optical sensor
- 2.2" 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
- Multi-color guidance LEDs
- Easy installation



MiY-Card

- Sandbox API framework support
- IP65 design
- Non-mechanical 12-key keypad
- Full PC/SC ISO 14443 contactless card reader
- Rugged optical sensor
- 2.2" 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
- Multi-color guidance LEDs
- Easy installation



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



1.2.1 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 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.

1.4 Key Terms

Term	Description
MiY	MiY (Make it Yours) is the generic designation of all biometric physical access control devices within the Cogent MiY product line.
Enrollment	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.
Verification (Authentication)	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.
Identification	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.
Template	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.
Minutiae Record	The compilation of minutiae templates acquired during enrollment along with the other user information such as name, Wiegand ID, etc.
PoE	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.

2 MiY Devices

2.1 MiY-Search and MiY-Card Overview

The MiY-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.



MiY-Devices - Front View



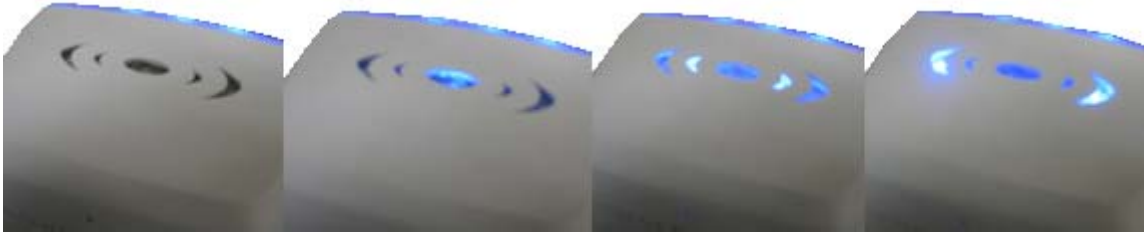
MiY-Devices - Rear View

2.2 Physical Features

MiY 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 devices.

2.2.1 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.



MiY-Card Front View

2.2.2 Display

All MiY-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 has a 2.4" display.



MiY-Card and Search



MiY-ID

2.2.3 Keypad

MiY-devices have back-lit non-mechanical buttons that can be used for user PIN entry, functional selection, or device administration.



MiY-Card and MiY-Search
12 Keys



MiY-Card
21 Keys

2.2.4 Fingerprint Sensor

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



Fingerprint Sensor

2.2.5 Contactless Card Reader (MiY-ID)

The MiY-ID device has a contact card reader on the bottom:



Contact Card Reader

2.2.6 Admin Port and Reset Button

The bottom of the device has a weather protection rubber cover that protects the Admin port and reset button.



Admin Port and Reset Button

2.2.7 Wall Mount

The stainless steel mounting bracket can be attached to a single gang box or double gang box. MiY-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.



MiY Wall Hinge

Back Panel and Connections

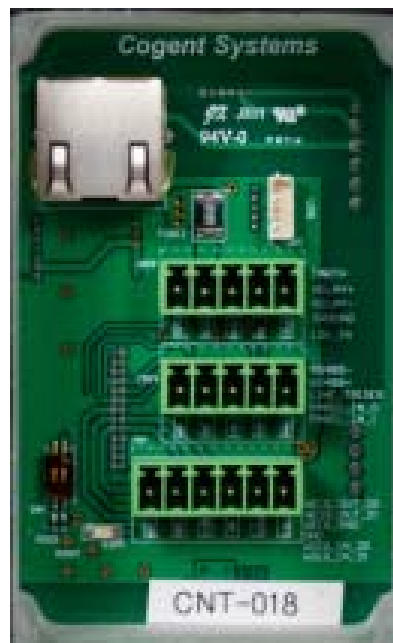
The back panel of MiY devices can be opened to expose the internal connections.



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

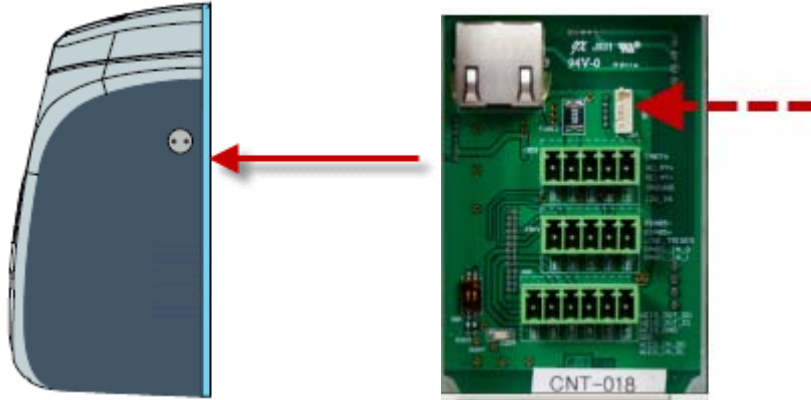


2.2.8 USB Ports

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

2.2.8.1 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.



2.2.8.2 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.



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.

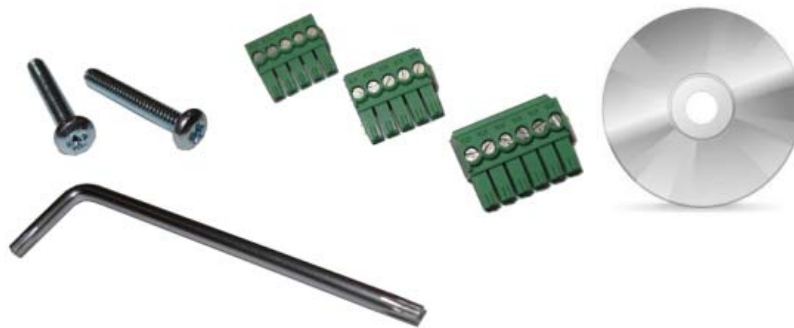
For instructions on enabling the OTG USB port, see the section *Enabling the OTG USB Port* in this document

3 Installing a MiY Device

3.1 Accessory List

The following items are included in the MiY package:

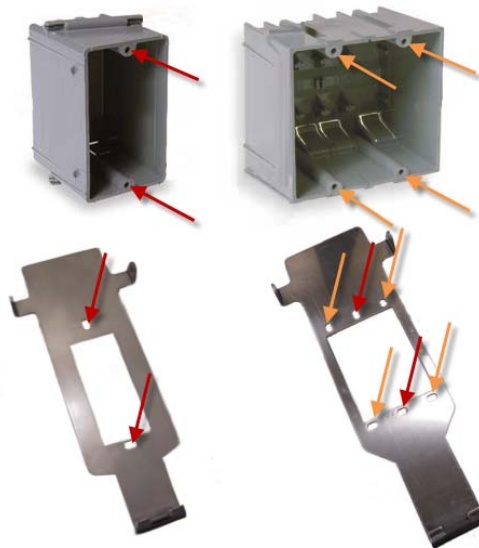
- Terminal blocks
- Security screws (2)
- Security screw tool
- Installation CD
- Installation Guide



3.2 Mounting the Bracket

To mount the wall bracket:

- 1 Screw the bracket into the gang box in the wall based the below images. The MiY-Card and MiY-Search bracket attaches to a single gang box, where as 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

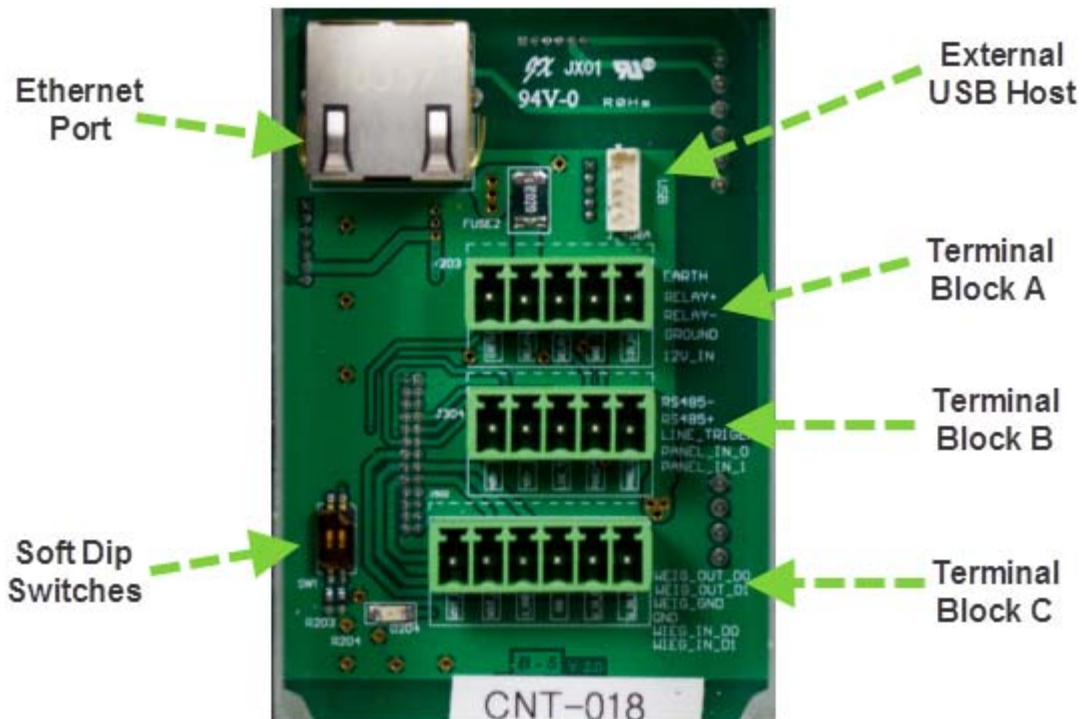
- 2 Place the device's bracket hinge pin on the hooked mounting bracket



Attaching the Hinge Pin to the Mounting Bracket

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:

Pin Number	Description
A1	Earth Ground
A2	Relay +
A3	Relay -
A4	Power GND
A5	Power (12 V DC)

Low-Profile Terminal Block A

Pin Number	Description
B1	RS-485 (-)
B2	RS-485 (+)
B3	Line Trigger (DRV_Out)
B4	LED-like Panel Input (0)
B5	LED-like Panel Input (1)

Low-Profile Terminal Block B

Pin Number	Description
C1	Wiegand Output Data 0
C2	Wiegand Output Data 1
C3	Wiegand Output GND
C4	Wiegand Input GND
C5	Wiegand Input Data 0
C6	Wiegand Input Data 1

Low-Profile Terminal Block C

3.4 Connecting the Power Supply to the MiY Device

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

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.



Terminal Positions (Red: 12V, Black: Ground)

- 2 Take a small flat-head driver and tighten the screws to hold the wires in-place



Tightening Screws

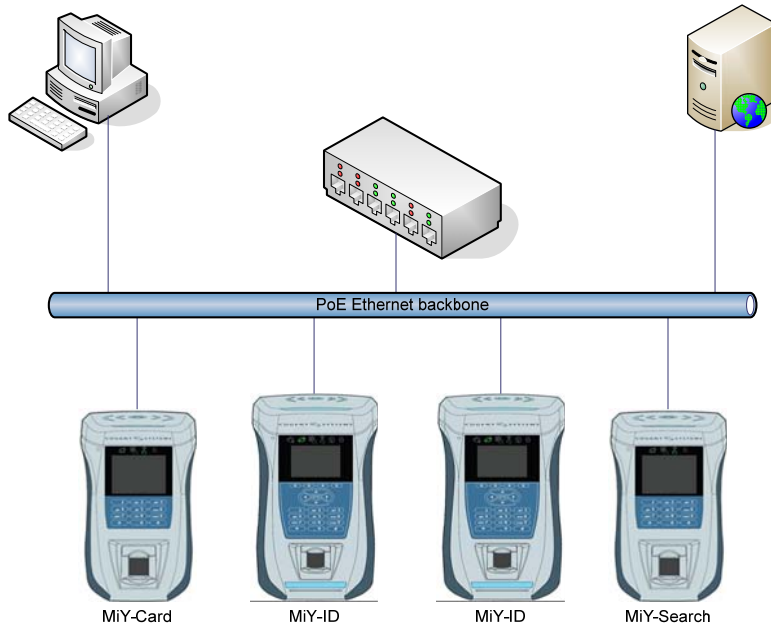
- 3 Connect the terminal block to the terminal block connector A. When power is available, the MiY-Device will turn on.

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 can not be powered by Power over Ethernet (PoE), troubleshoot using the procedure detailed in this subsection.

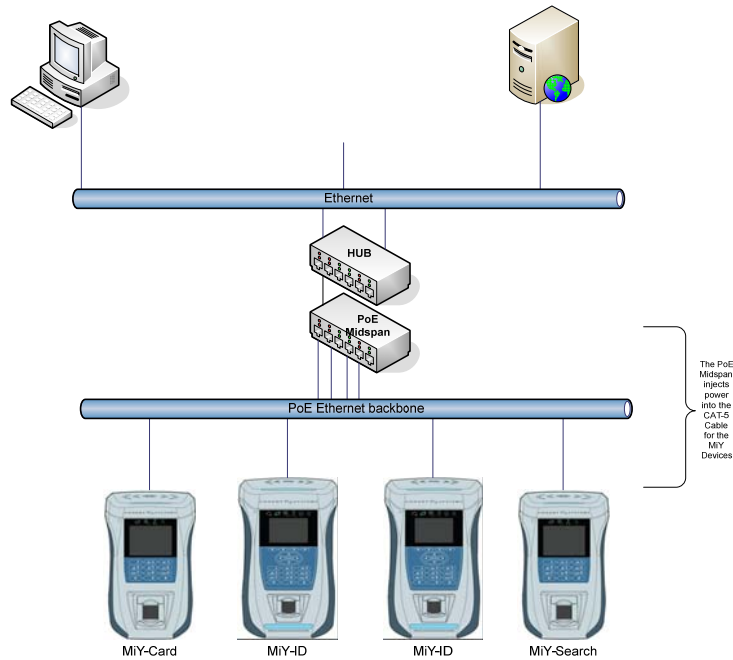
To troubleshoot the MiY's PoE:

- 1 Connect a CAT-5 Ethernet cable between the Ethernet port of the MiY device and an 802.3af PoE-enabled hub



PoE-Enabled Hub Connected Directly to MiY Device

- 2 Connect a CAT-5 Ethernet cable between the Ethernet port of the MiY device and a midspan power injector unit

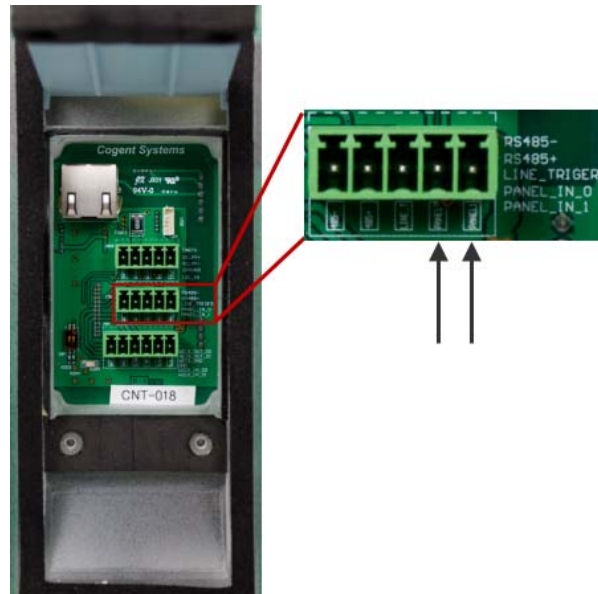


Hub Connected to MiY Devices via Midspan

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.

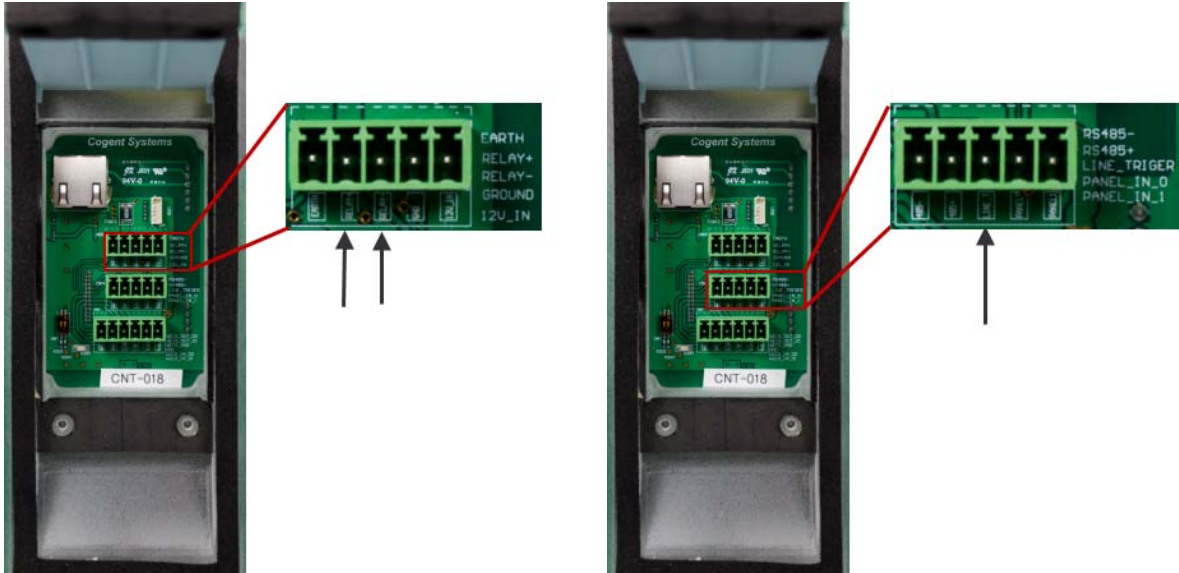
The administrator will also need to enable the Panel-in check under General settings in the Device Info admin menu.



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.

3.6 Relay & Line Trigger Wiring

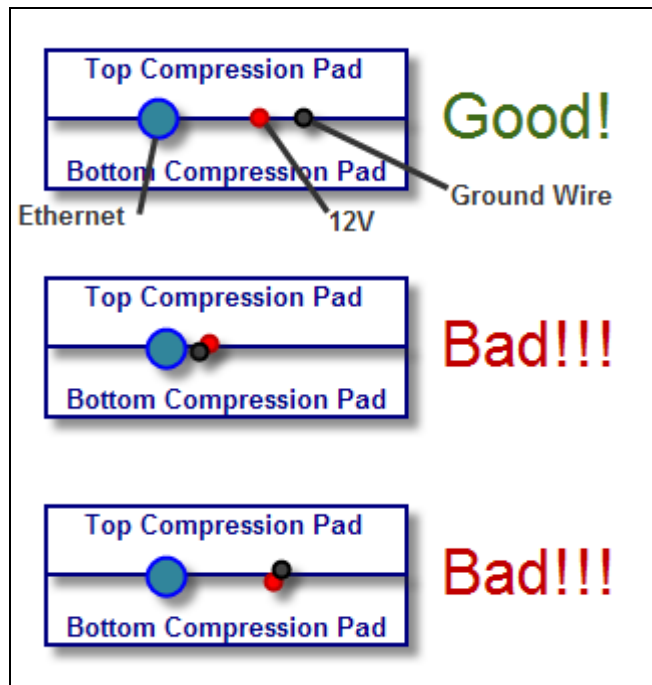
Relay and Line Trigger wiring can be done by placing the wire into the correct terminal block and turning the tightening screw to ensure the wire will stay in place.

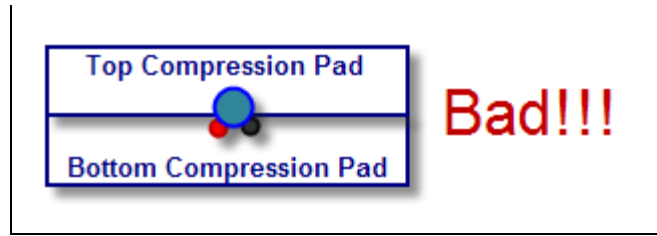


3.7 Securing the MiY Devices on the Wall

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.





Proper Wire Distribution

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



Compression Panel Screw Position

- 2 Pivot the device on the bracket hinge and bring it up over the wall mount.



Pivoting the Device Over the Wall Mount

- Secure the device by using the security-screw driver to insert and tighten the security screws on both sides of the MiY-Device.



Location of Security Screws

- 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.

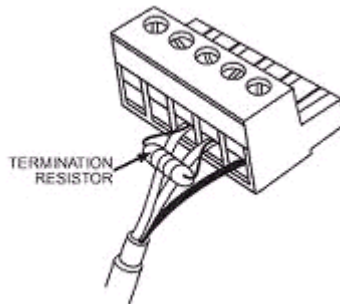
Termination is used to match impedance of a node to the impedance of the transmission line being used. When impedances are mismatched, the transmitted signal is not completely absorbed by the load and a portion is reflected back into the transmission line. If the source, transmission line, and load impedance 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 $0.66 \times c$, one round trip is completed in approximately $6.16 \mu\text{s}$. If we assume the reflections will damp out in three “round trips” up and down the cable length, the signal will stabilize $18.5 \mu\text{s}$ after the leading edge of a bit. At 9600 baud one bit is $104 \mu\text{s}$ 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 (120Ω is a common value)

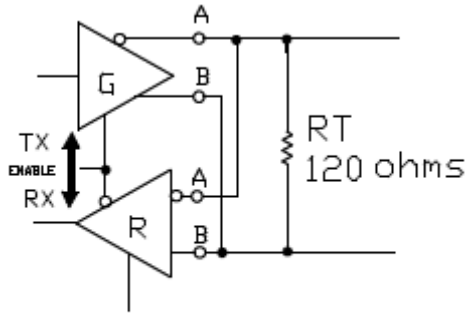


Termination Resistor

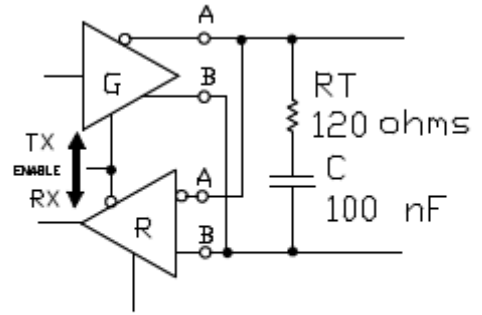
This value describes the intrinsic impedance of the transmission line and is not a function of the line length. A terminating resistor of less than 90Ω should not be used. Termination resistors should be placed only at the extreme ends of the data line, and no more than two terminations should be placed 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 Termination



AC-Coupled Termination

Parallel and AC Termination

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.

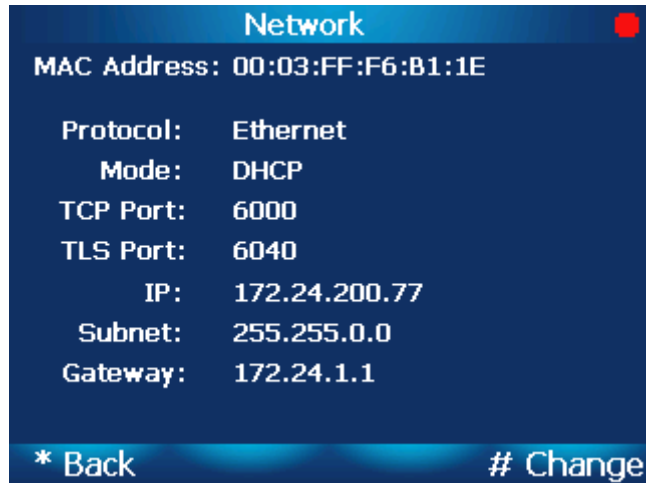
To configure TCP/IP:

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



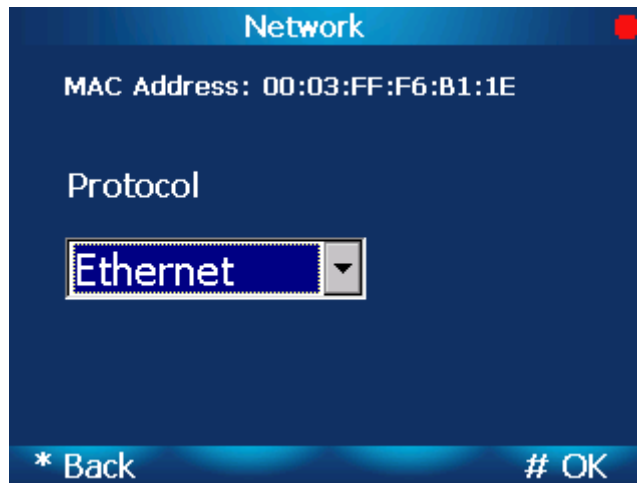
Device Info Screen

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



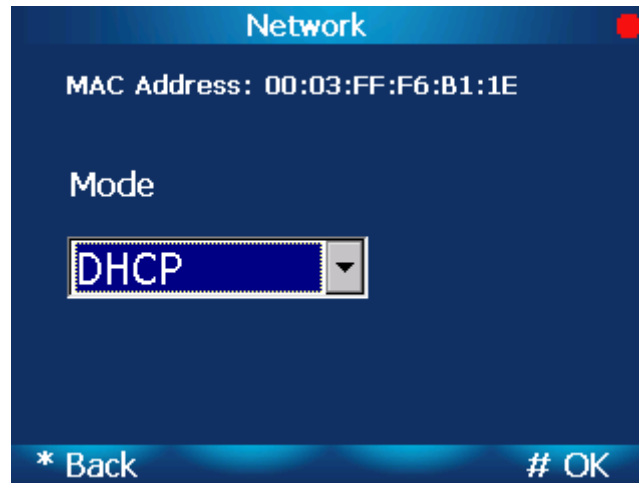
Network Screen

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



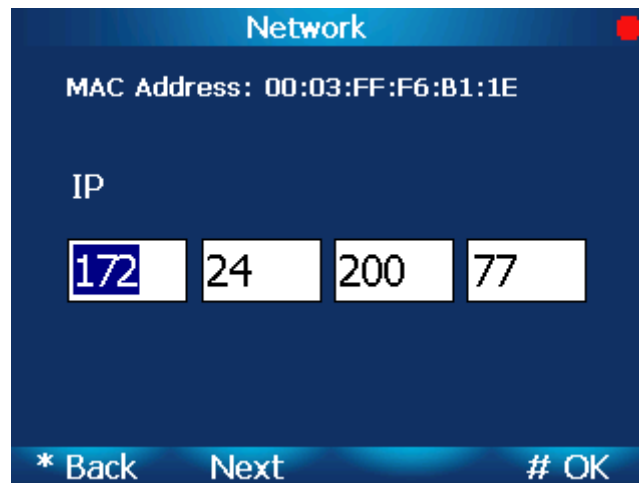
Protocol Screen

- 4 From the **Protocol** screen, select the **Ethernet** protocol and select **OK**. The **Mode** screen will be displayed



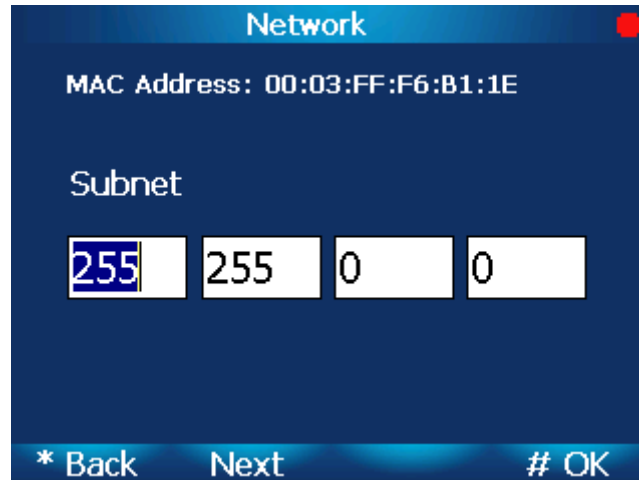
Mode Screen

- 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 8. The **TCP Port** screen will be displayed



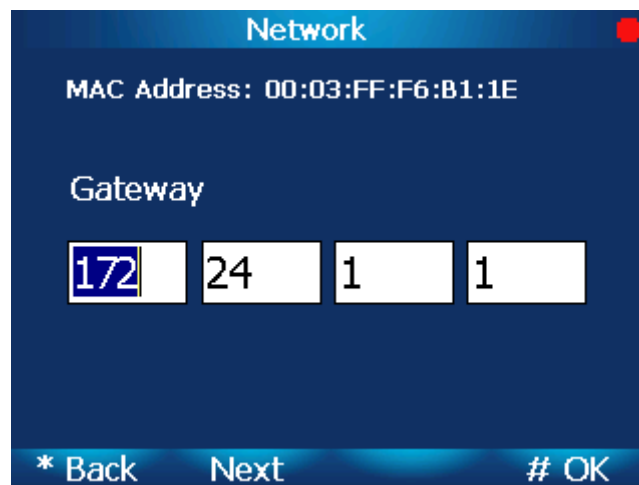
IP Address Screen

- 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.



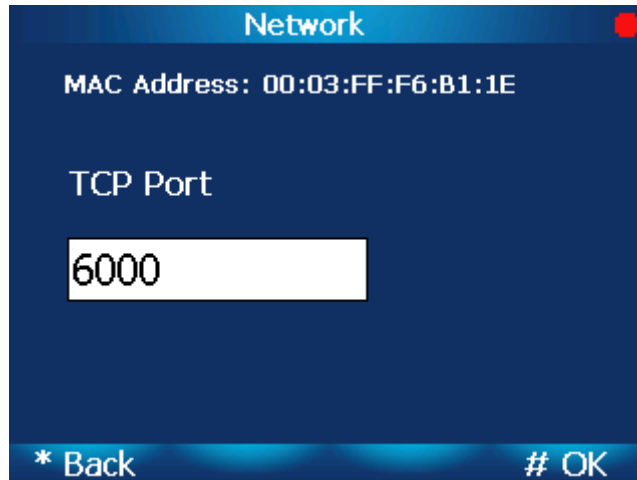
Subnet Screen

- 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.



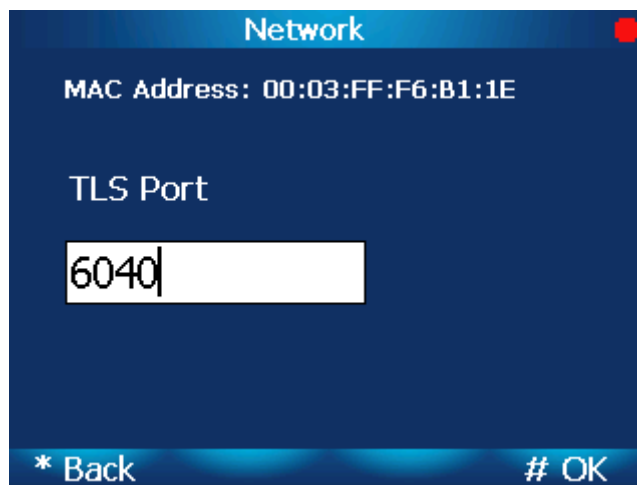
Gateway Screen

- 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.



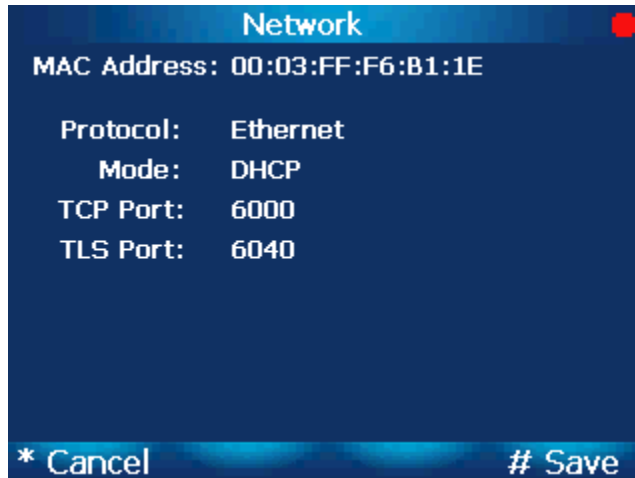
TCP Port Screen

- 9 From the **TCP Port** screen, set the port and select **OK**. The **TLS Port** screen will be displayed.



TLS Port Screen

- 10 From the **TLS Port** screen, set the port and select **OK**. The **Network Review** screen will be displayed.



Network Review Screen

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

4.1.2 Configuring RS485 Connection Settings

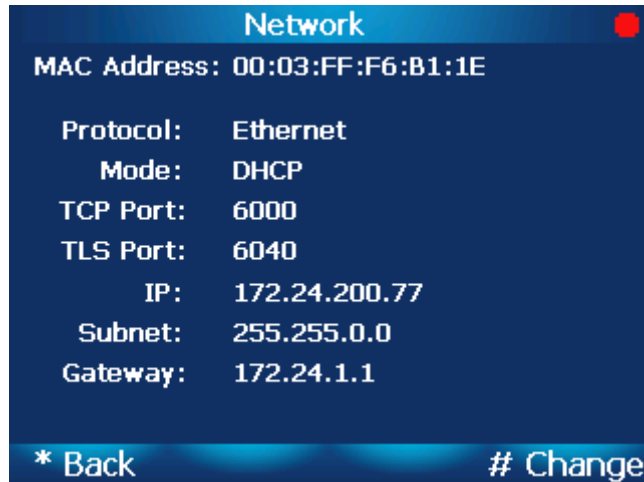
To configure RS485 connection settings:

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



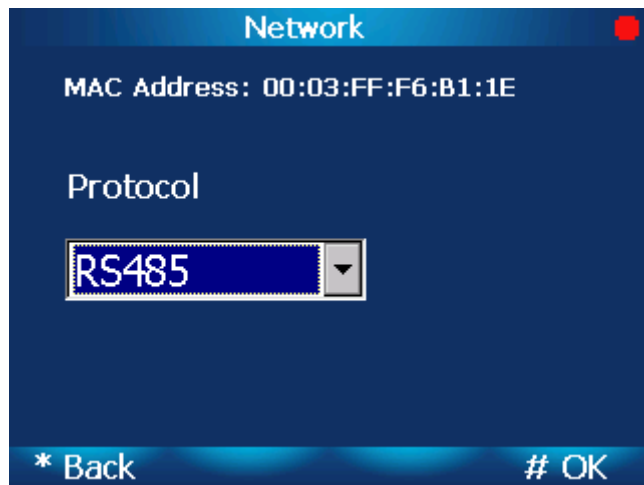
Device Info Screen

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



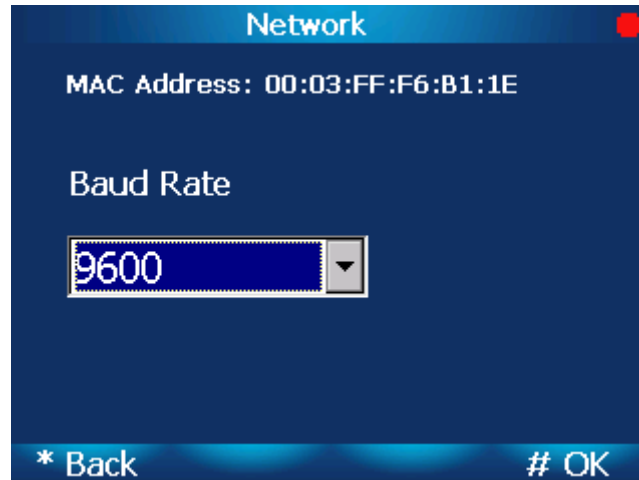
Network Screen

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



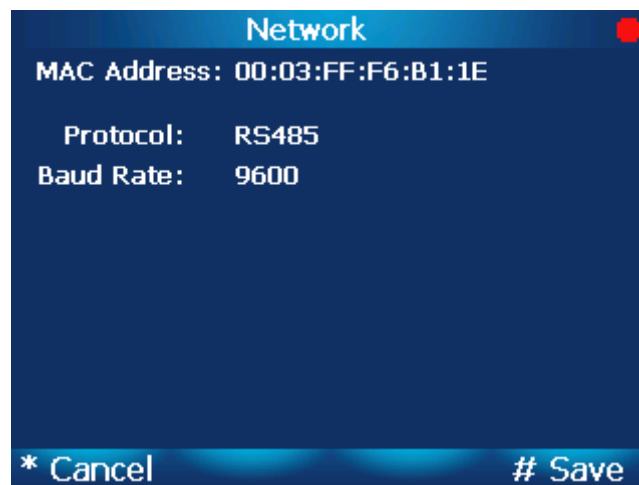
Protocol Screen

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



Baud Rate Screen

- 5 From the **Baud Rate** screen, select the baud rate and select **OK**. The **Network Review** screen will be displayed.



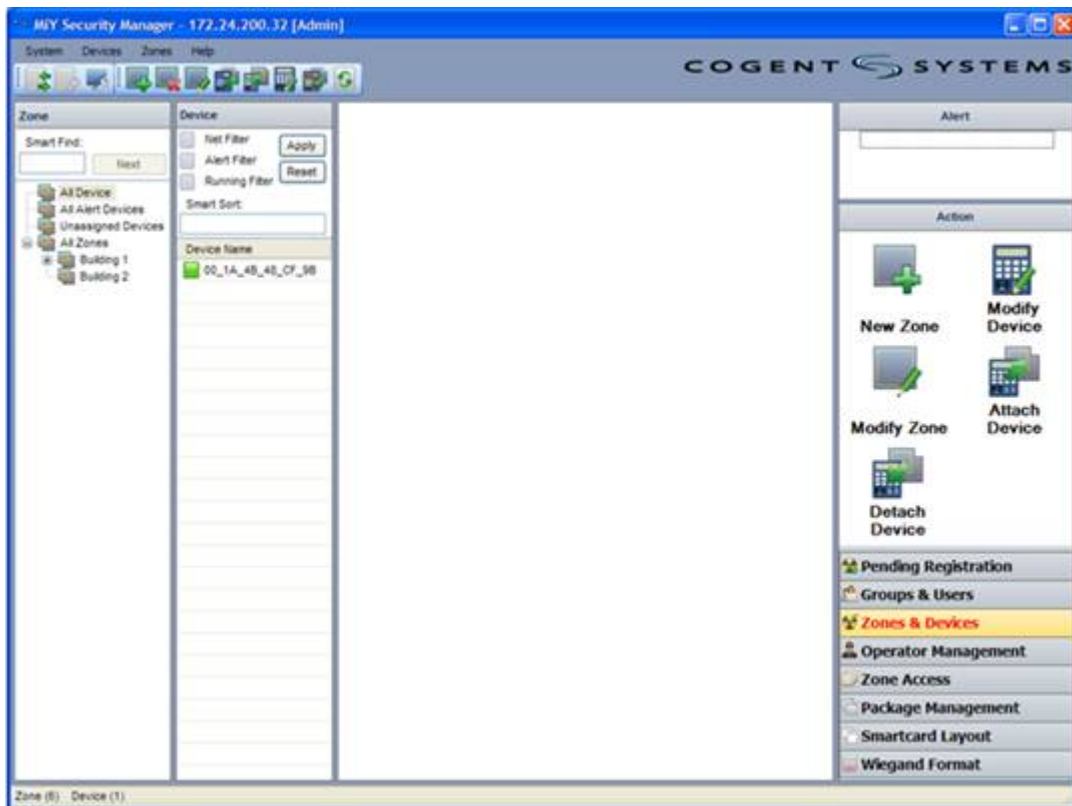
Network Review Screen

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

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 Manger (**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.

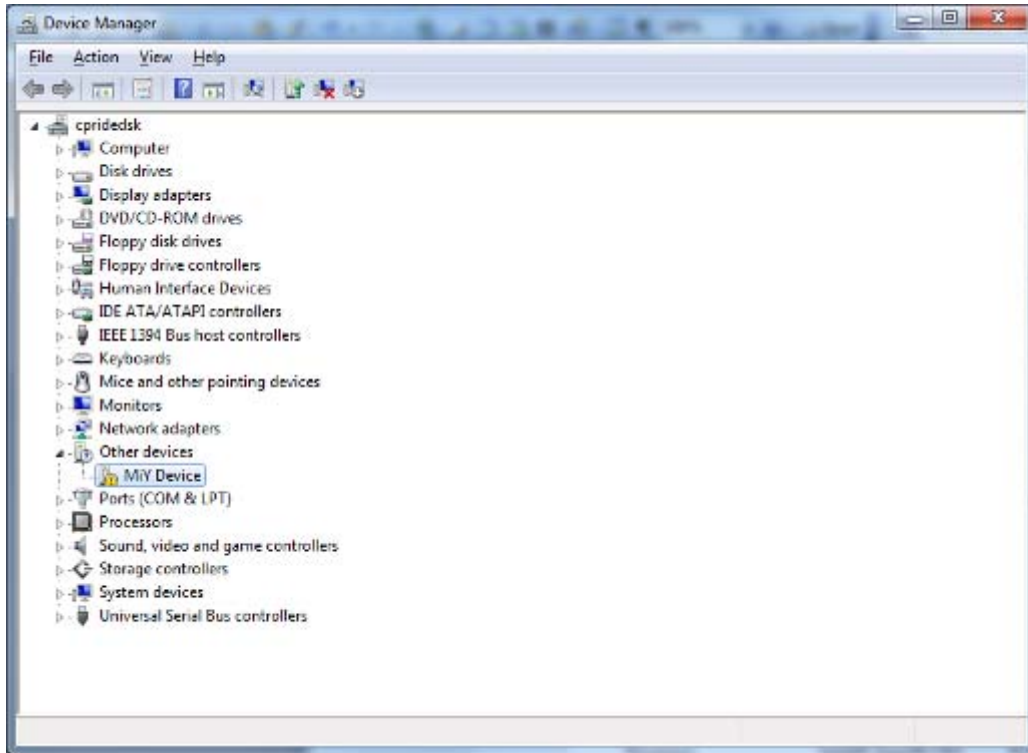
In order to use the OTG USB port, it must be enabled. To enable the OTG USB port, refer to the section *Enabling the OTG USB Port*.

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 Set the OTG USB port on the MiY device to **Normal** mode. Refer to the subsection *Enabling the OTG USB Port* for details.
- 3 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. The device will be displayed in the PACS Device Manager as a “MiY Device”.

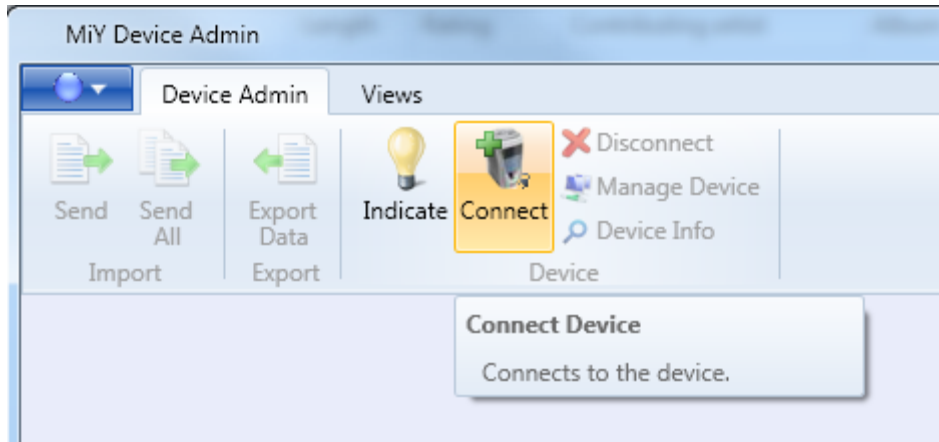
NOTE: The MiY Device Driver should be installed by the Device Admin Utility installer. However, if the driver is not installed, the device will be displayed with an exclamation point. Perform a manual installation of the MiY Device Driver via the PC’s Device Manager, Add New Device wizard, or other preferred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



PC Device Manager

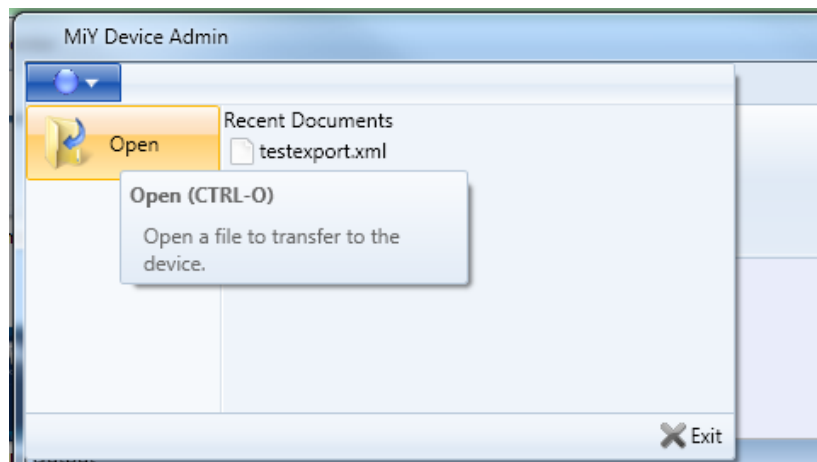
- 4 From the Device Admin Utility, select **Indicate** to verify you are connecting to the correct device. The device LEDs should flash and you should hear a sound.
- 5 Select **Connect** to connect to the device.

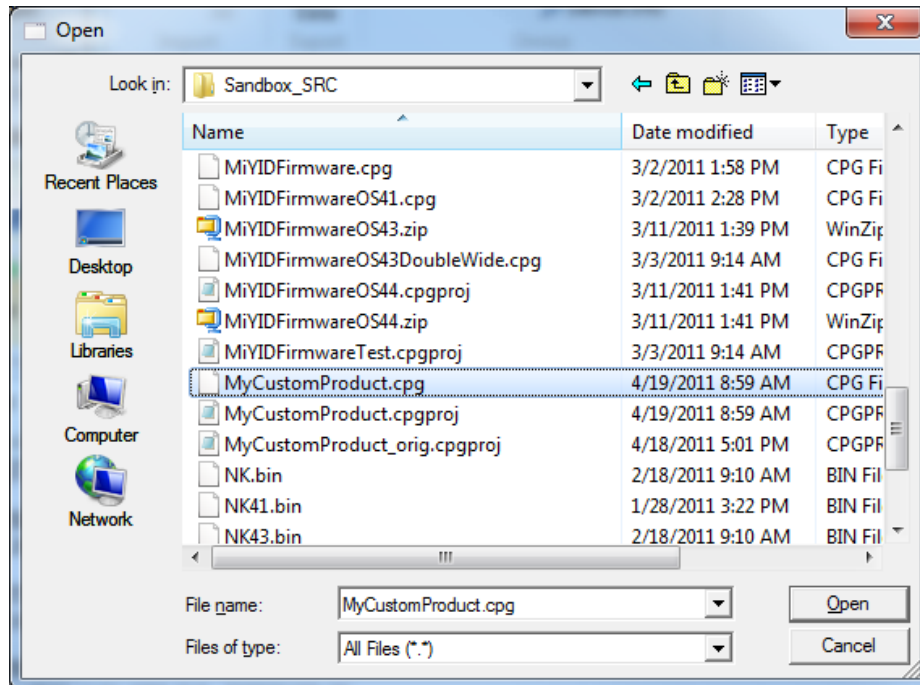
NOTE: If the connect button is disabled, communication between the device and the PC or laptop is not functioning correctly. This could be for several reasons: the device is not physically connected to the PC or laptop via USB cable, the device OTG USB mode is not set to Normal, the MiY Device Driver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



Connect Button

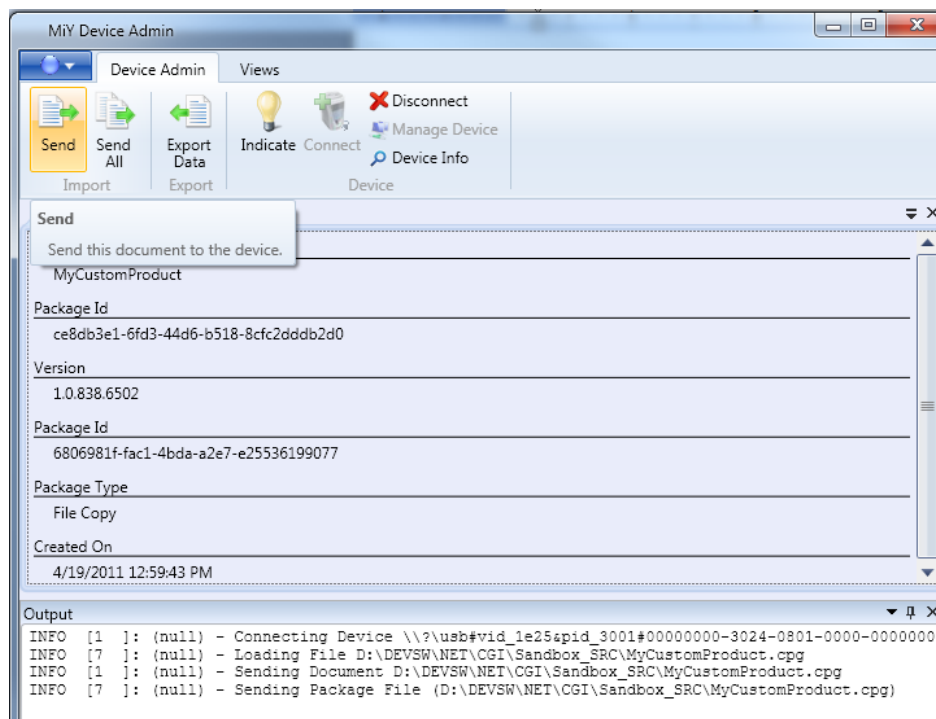
- 6 After successfully connecting, select the top-left menu button.
- 7 Select **Open** from the menu. The **Open** window will be displayed





Open Window

- 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.



Preparing to Send a Package File

- 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.

To access the MiY Admin Menu:

- 1 Select the top-left **Admin** button or bottom left ***Back** button to begin admin login. The **Operator Login** screen will be displayed.



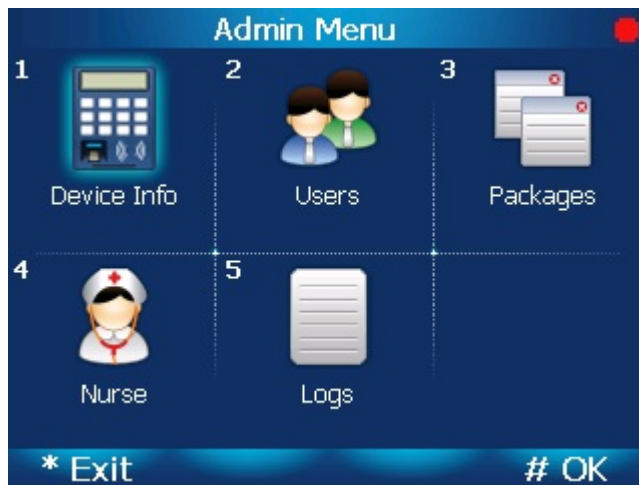
Operator Login Screen

- 1 Enter your **User Name** and select **OK**. The **Password Input** screen will be displayed



Password Input Screen (Password Hidden)

- From the **Password** screen, enter your password and select **OK**. The password is hidden as you enter it. The default value for an unmanaged device (not registered to a server) is **7890**.
- The **Admin Menu** screen will be displayed.



MiY Main Screen

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

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

To use Device Info to view device settings:

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



Device Info Screen

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

Name	Value
MAC Address	00:03:FF:F6:B1:1E
ServerAddress	
ServerTCPPort	6001
ServerTLSPort	6041
GateAppPath	CogentGate.exe
GateAppHealthCheck	30
GateAppMessageRes	60
Culture	
LogUploadInterval	3600

General Screen

Name	Value
UserActionTimeout	120
DisplayTimeout	900
FacilityCode	0
AgencyCode	0
WiegandFormatIn	
WiegandFormatOut	Standard 26
RSSUrl	
RSSFile	/Storage
MaxEventLogRecord	600000

General Screen (cont'd)

Name	Value
OtgMode	Disabled
HIDiClassKey	
AdminLockoutTime	5
UVLedDelay	5
UVLedDuration	2
LogsLastUploaded	
GateAppKillWaitTime	20
PanelInMonitorInterv	300
PanelInCheckEnable	False

General Screen (cont'd)

7.2.2 Changing Device Network Settings

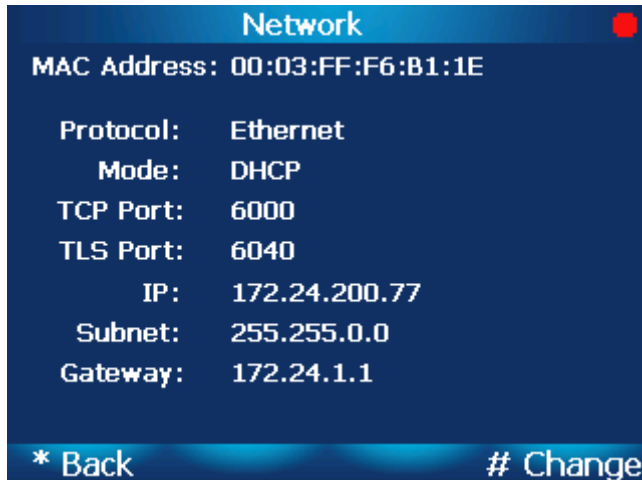
From the **Network** screen, you can set either **DHCP** or **Static** mode, and enter the **TCP listening port**, **TLS**, and **RS485 detection** settings.

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.



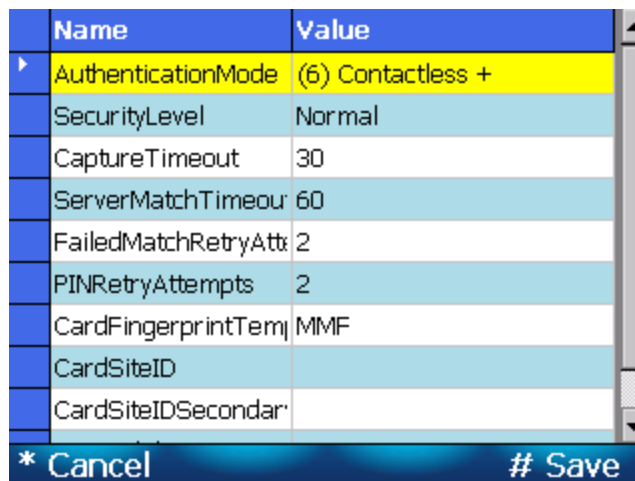
Network Screen

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:

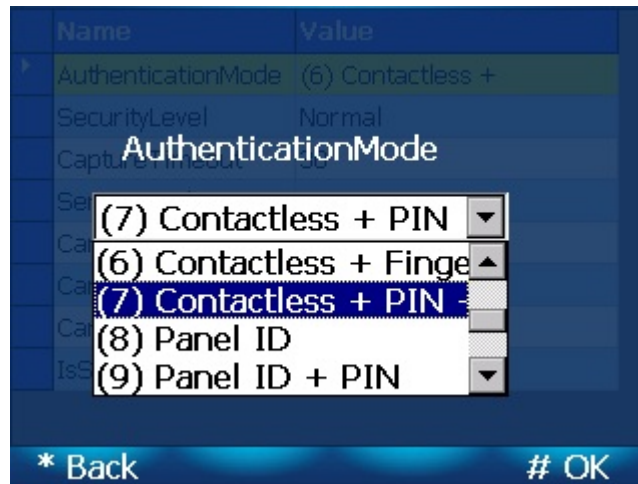
- 1 From the **Device Info** screen, select **Security**. The **Security** screen will be displayed. Navigate up and down and select the item to edit.



Security Screen

- 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:
 - On-Device Finger Search
 - On-Server Finger Search
 - On-Device Finger Search, If no-hit On-Server
 - Contactless
 - Contactless + PIN

- Contactless + Finger
- Contactless + PIN + finger
- Panel ID
- Panel ID + PIN
- Panel ID + Finger
- Panel ID + PIN + Finger
- Wiegand In + Finger
- Multimode (On-Device Finger Search, Contactless + Finger, Panel ID + Finger)



Verify Mode

- 3 From the **Print Capture Timeout** dropdown menu, select the number of seconds after a print is submitted before timeout.
- 4 From the **Security Level** dropdown menu, select the level of security for the device.
The options are:
 - 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.
- 5 From the **Server Match Timeout** dropdown menu, select the number of seconds until the server times out during a search.
- 6 From the **Standalone Mode** dropdown menu, select **True** or **False** depending on whether the device is part of a network or a single installation.

7.3 Managing Users

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

7.3.1 Adding Users

To add users:

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



Users Screen

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



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.

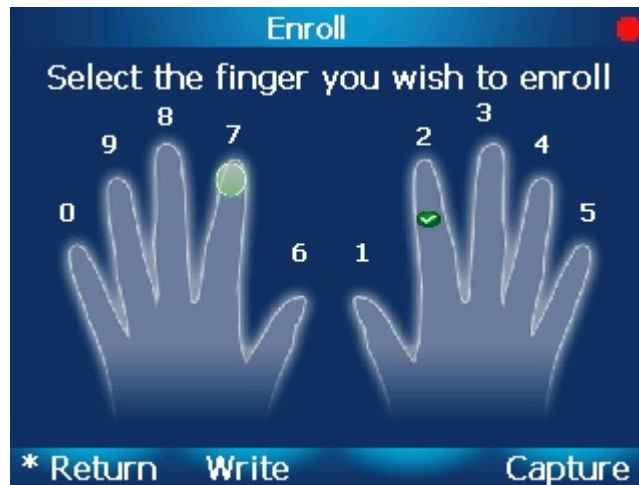


The screenshot shows a window titled "Add User" with a table of user information. The table has two columns: "Name" and "Value". The rows are: Panel ID: 1234, PIN: 123456, Special Flag: No Fingers, First Name: P, and Last Name: M. At the bottom, there are three buttons: "* Cancel", "Enroll", and "# Save".

Name	Value
Panel ID:	1234
PIN:	123456
Special Flag:	No Fingers
First Name:	P
Last Name:	M

User Information Screen

- 5 From the **User Information** screen, select **Enroll** to begin capturing the new user's fingerprints. The **Finger Selection** screen will be displayed.



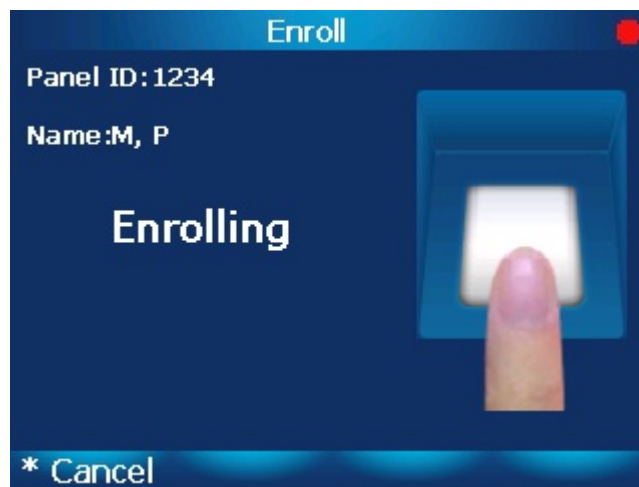
Finger Selection Screen

- 6 Select which finger you want to enroll and select **Capture**. The **Finger Enrollment** screen will be displayed.



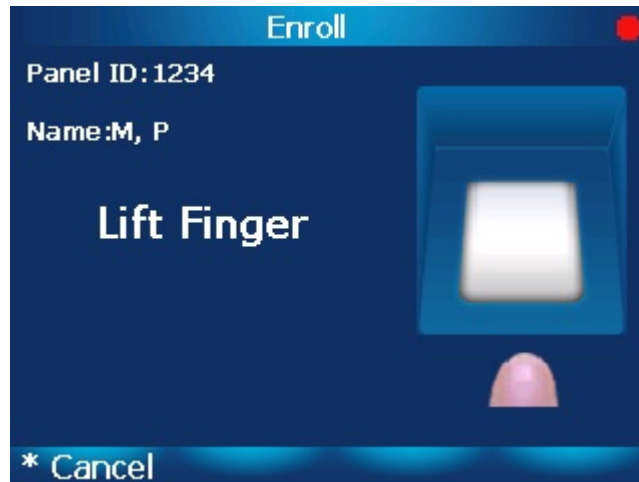
Finger Enrollment Screen

- 7 Instruct the user to place and hold the the finger indicated on screen on the fingerprint sensor. The **Enrolling** screen will be displayed



Enrolling Screen

- 8 Once enrollment is complete, the **Lift Finger** screen will be displayed. Instruct the user to briefly lift his or her finger during matching.



Lift Finger Screen

- 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.



Enrollment Successful Screen

- 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.

7.3.2 Modifying Users

To modify an existing user:

- 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.

Panel ID	Name
▶ 1234	M, P

* Back # OK

User List

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

Add User	
Name	Value
▶ Panel ID:	1234
PIN:	123456
Special Flag:	No Fingers
First Name:	P
Last Name:	M

* Cancel Enroll # Save

User Information Screen

- Enter your modifications and select **Save**. The **Success** screen will be displayed, indicating that the modifications have been accepted.



Success Screen

7.3.3 Deleting Users

To delete a user:

- 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

	Panel ID	Name
▶	1234	M, P

* Back # OK

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.

To promote an existing user:

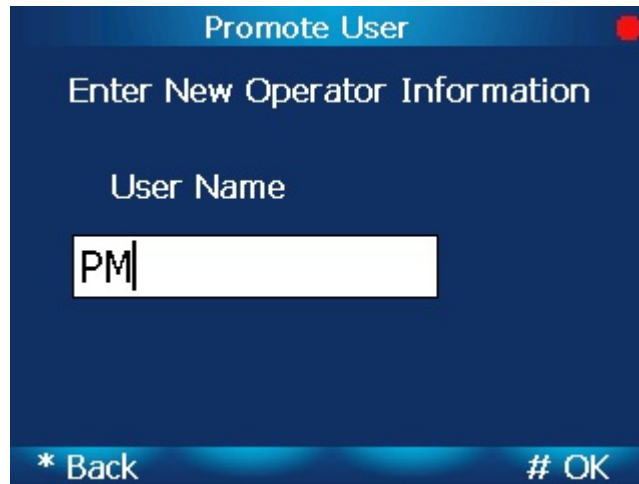
- 1 From the **Users** screen, select **Promote User**. The **Search User Wizard** will begin starting with the **Panel ID** screen.
- 2 Enter desired search criteria and select **OK**, or select **OK** for each screen in the wizard to search all users. The **User List** will be displayed.

	Panel ID	Name
▶	1234	M, P

* Back # OK

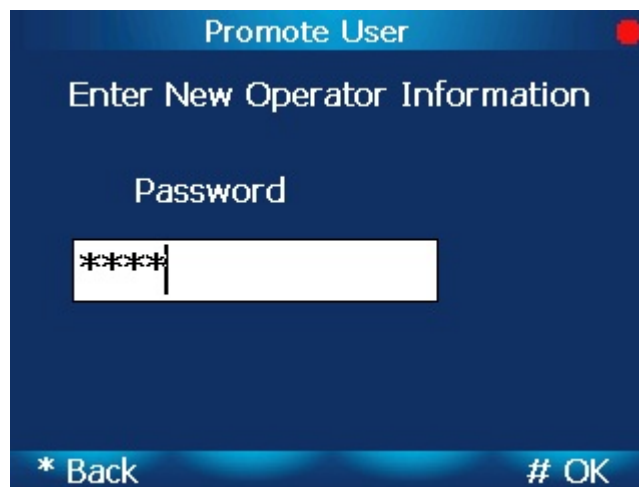
User List

- 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.



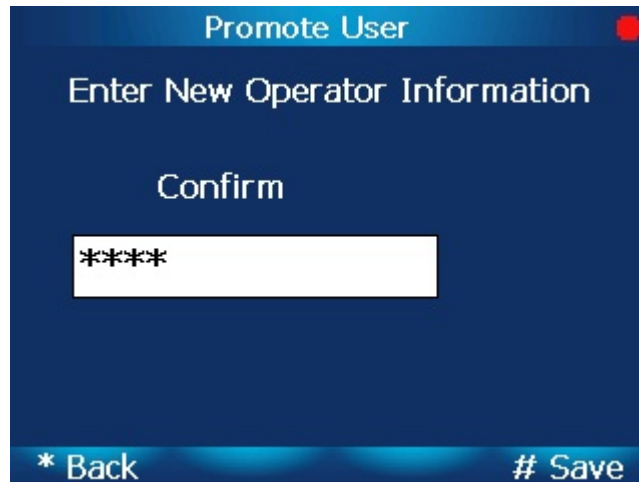
New Operator Screen

- 4 Enter the new operator's **User Name** and select **OK**. The **User Password** screen will be displayed



User Password Screen

- 5 Enter the user password and select **OK**. The **User Password Confirmation** screen will be displayed.



- 6 Enter the confirm password and select **OK**. The **Success** screen will be displayed, indicating you have successfully added a new operator



Success Screen

7.3.5 Demoting Users

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

To demote an existing user:

- 1 From the **Users** screen, select **Demote 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.

Panel ID	Name
1234	M, P

* Back # OK

User List

- From the list of users, select the user you want to demote and select **OK**.

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.

To enable the OTG USB port:

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



Device Info Screen

- Select the **General** menu option. The **General Info** screen will be displayed. The **Otg Mode** is disabled by default.

Name	Value
RSSFile	/Storage
MaxEventLogRecords	600000
OtgMode	Disabled
HIDiClassKey	
AdminLockoutTime	5
	5
UVLedDuration	2
LogsLastUploaded	4/18/2011 11:54:59 AM
GateAppKillWaitTime	10

* Cancel # Save

General Info Screen

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

Name	Value
RSSFile	/Storage
MaxEventLogRecords	600000
OtgMode	Disabled
HIDiClassKey	
Ad	
UV	
LogsLastUploaded	4/18/2011 11:54:59 AM
GateAppKillWaitTime	10

* Back # OK

Otg Mode Drop-Down Menu

- 4 Choose the desired mode and select **OK**. The **General Info** screen will be displayed and you can confirm the mode change selected.

Name	Value
RSSFile	/Storage
MaxEventLogRecords	600000
OtgMode	Development
HIDiClassKey	
AdminLockoutTime	5
UVLedDelay	5
UVLedDuration	2
LogsLastUploaded	4/18/2011 11:54:59 AM
GateAppKillWaitTime	10

* Cancel # Save

General Info Screen

- 5 Select **Save** to commit the changes. A success screen will be displayed, followed by the **Device Info** menu.


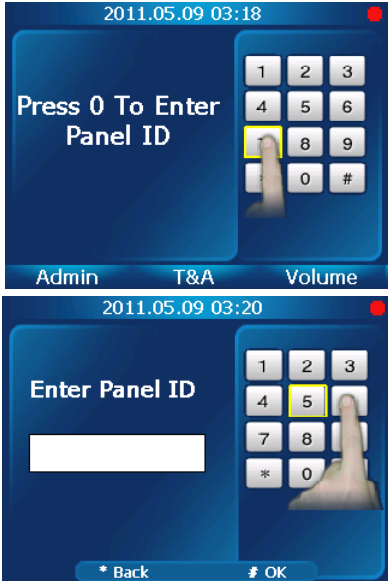
This page was intentionally left blank.


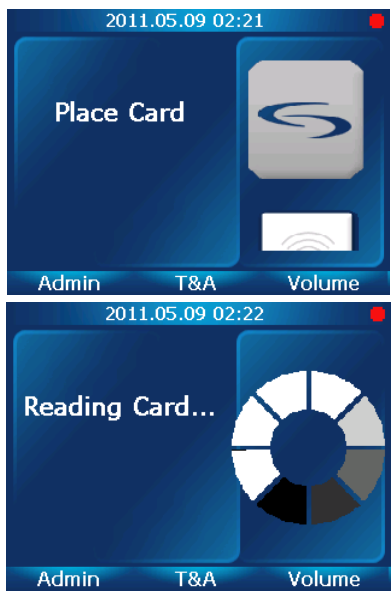

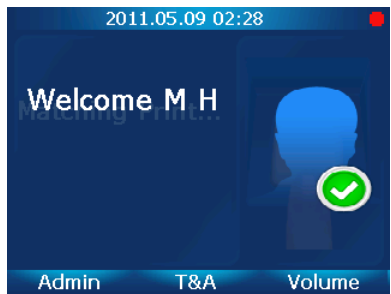
8 Verifying Users for Access/Entry

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



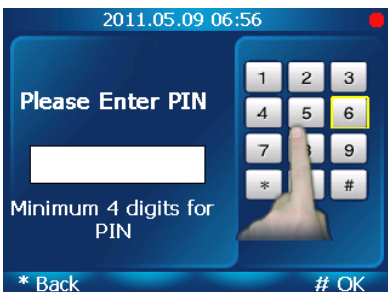
The MiY-Search and MiY-Card devices verify users through a combination of the following authentication factors: fingerprint, panel id, pin, and card. Since verification workflows are heavily customizable, the tables in the following subsection describe the step required for each screen displayed on the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

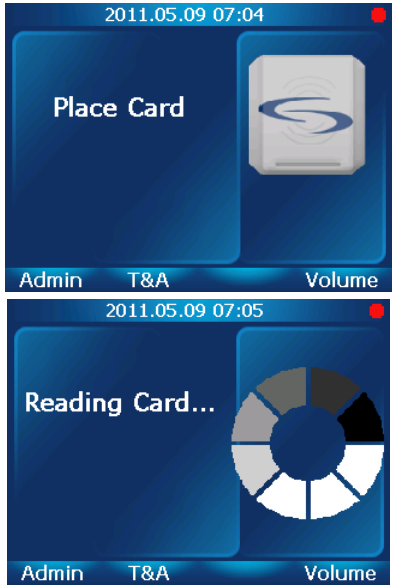

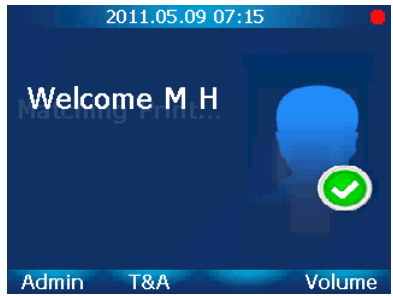
Verification Type	Screen Displayed	Instructions
Fingerprint		<p>When prompted by the device, place the appropriate finger on the fingerprint sensor.</p> <p>Upon successful fingerprint verification, the device will display the next screen in the verification workflow.</p>
Panel ID		<p>When prompted by the device with the top screen, press the “0” key on the number pad. The bottom screen will be displayed.</p> <p>Using the number pad, enter the appropriate Panel ID number.</p> <p>Upon successful Panel ID verification, the device will display the next screen in the verification workflow.</p>

Verification Type	Screen Displayed	Instructions
<p>PIN</p> <p>(Personal Identification Number)</p>	 <p>The screenshot shows a blue interface with the date and time '2011.05.09 03:39' at the top. The main text reads 'Please Enter PIN' above a white input field. Below the field, it says 'Minimum 4 digits for PIN'. On the right is a numeric keypad with a finger pressing the '1' key. At the bottom are buttons for '* Back' and '# OK'.</p>	<p>When prompted by the device, use the number pad on the device to enter the appropriate PIN.</p> <p>Upon successful PIN verification, the device will display the next screen in the verification workflow.</p>
<p>Card*</p> <p>*Only available on MiY-Card</p>	 <p>The first screenshot shows '2011.05.09 02:21' and 'Place Card' with an image of a card being placed on a reader. The second screenshot shows '2011.05.09 02:22' and 'Reading Card...' with a circular progress indicator. Both screens have 'Admin', 'T&A', and 'Volume' buttons at the bottom.</p>	<p>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.</p> <p>While the bottom screen is displayed, keep the card on the reader.</p> <p>Upon successful card verification, the device will display the next screen in the verification workflow.</p>
<p>Multi-Mode Verification*</p> <p>*Only available on MiY-Card</p>	 <p>The screenshot shows '2011.05.10 10:46' and 'Present Card, Finger or Press 0 for Panel ID' next to a card reader icon. It has 'Admin', 'T&A', and 'Volume' buttons at the bottom.</p>	<p>When this screen is displayed, it indicates that the device is in multi-mode.</p> <p>Presenting a card, finger, or Panel ID will initiate a multi-step workflow for verification.</p>
<p>Success</p>	 <p>The screenshot shows '2011.05.09 02:28' and 'Welcome M H' with a blue silhouette of a person and a green checkmark icon. It has 'Admin', 'T&A', and 'Volume' buttons at the bottom.</p>	<p>Upon successful user verification, this screen will be displayed on the device.</p> <p>The device will then perform the action programmed for a verification event (e.g. unlock the door).</p>

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.

Verification Type	Screen Displayed	Instructions
Fingerprint		<p>When prompted by the device, place the appropriate finger on the fingerprint sensor.</p> <p>Upon successful fingerprint verification, the device will display the next screen in the verification workflow.</p>
Panel ID		<p>When prompted by the device, use the number pad to enter the appropriate Panel ID number.</p> <p>Upon successful Panel ID verification, the device will display the next screen in the verification workflow.</p>
PIN (Personal Identification Number)		<p>When prompted by the device, use the number pad on the device to enter the appropriate PIN.</p> <p>Upon successful PIN verification, the device will display the next screen in the verification workflow.</p>

Verification Type	Screen Displayed	Instructions
Card		<p>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.</p> <p>Keep the card on the reader while the bottom screen is displayed.</p> <p>Upon successful card verification, the device will display the next screen in the verification workflow.</p>
Multi-Mode Verification		<p>When this screen is displayed, it indicates that the device is in multi-mode.</p> <p>Presenting a card, finger, or Panel ID will initiate a multi-step workflow for verification.</p>
Success		<p>Upon successful verification, this screen will be displayed on the device.</p> <p>The device will then perform the action programmed for a verification event (e.g. unlock the door).</p>

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.

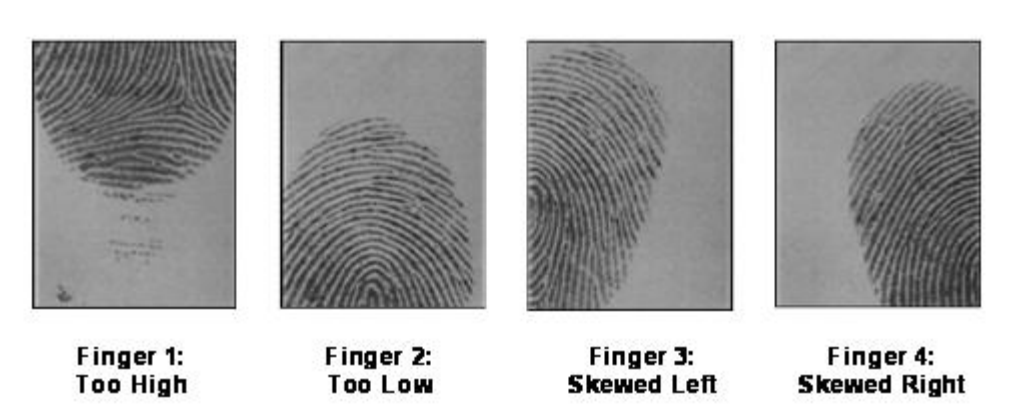


Figure A-1 Improper Finger Placement

Finger	Issue
Finger 1	The finger is positioned too high on the sensor and does not offer enough information to accurately enroll an image.
Finger 2	The finger is positioned too low on the sensor and may not be properly enrolled.
Finger 3 And Finger 4	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.

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.



Finger 5: Optimal Image

Figure A-2 Proper Finger Placement

A.2 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.






Image	Condition	Solution
	<p>Dry Finger</p> <p>The finger is very dry and difficult to capture.</p>	<p>Perform one of the following actions:</p> <ul style="list-style-type: none"> • Apply moisture to the finger using oil from your forehead. • Breathe on the finger. • Use a moisturizer that does not contain alcohol. <p>As a last resort, enroll a different finger.</p>
	<p>Wet Finger</p> <p>Remove excessive moisture from either the finger or the fingerprint sensor.</p>	<p>Perform one of the following actions:</p> <ul style="list-style-type: none"> • To remove the excessive moisture from your finger, wipe your finger on a cloth or dry tissue to absorb the moisture. • To remove excessive moisture from the fingerprint sensor, please refer to <i>Cleaning the Fingerprint Sensor</i>.
	<p>Damage to Finger</p> <p>The fingerprint may have future issues with identification due to the damaged area of the finger.</p>	<p>Enroll a different finger.</p>

Image	Condition	Solution
	<p>Not Enough Pressure</p> <p>The user did not apply enough pressure. As a result, the image looks very light and some of the surrounding areas are not captured.</p>	<p>The user should apply moderate but steady pressure; about the same pressure as pressing a button on a telephone.</p>
	<p>Too much Pressure</p> <p>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.</p>	<p>The user should apply moderate but steady pressure; about the same pressure as pressing a button on a telephone.</p>

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 set:

Hold down the following buttons, depending on the model:

- For the MiY-ID hold down the first Function key and the 0 key (*Figure B-1*).



Figure B-1 MiY-ID Function and 0 Key

- For MiY-Card and MiY-Search hold down the 1 key and the 0 key (*Figure B-2*).



Figure B-2 MiY-Card and MiY Search 1 and 0 Keys

Press the power reset button on the bottom of the device without letting go of the buttons (*Figure B-3*).



Figure B-3 Power Reset Button

Once the device boot up logo is loaded, release the buttons.

B.4 Contacting Your Distributor

Contact 3M Cogent Support at:

639 North Rosemead Blvd.
Pasadena, CA 91107
(626) 325-9600
www.cogentsystems.com

When you call, please provide:

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