7463 Network Thinline™ Keypad

INSTALLATION AND PROGRAMMING GUIDE
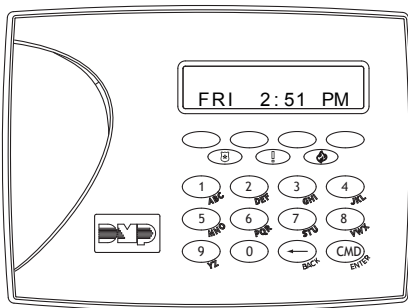

FRI   2:51 PM

TABLE OF CONTENTS

ABOUT THE 7463

The 7463 Network Thinline™ Keypads allow you to add IP keypads to XT Series and XTL Series panels with Version 202 or higher and XR150/XR550 Series panels with Version 201 or higher. For XR150 panels connected over Ethernet, seven network keypads may be used with device numbers 2-8. For XR550 panels connected over Ethernet, fifteen network keypads may be used with device numbers 2-16. For XT Series and XTL Series panels connected over Wi-Fi, one network keypad is permitted with any address other than 1.

The network keypads provide all the same functionality and performance of keypad bus hardwired keypads in situations where running new wire is impossible or cost prohibitive, but network connections are readily available. The keypad provides a built-in prox reader for arming and disarming.

Note: The 7463 Network Thinline™ Keypads must use a hardwired connection with the panel, and are not compatible with DMP 763 Wi-Fi Modules.

KEYPAD FEATURES

Select Keys

1   *2*   *3*   *4*

Armed/Power LEDs

FRI   2:51 PM

Keypad Display/Status List

Panic Keys

Proximity Credential Reader and Backlit Logo

Command (CMD) Key

Back Arrow Key
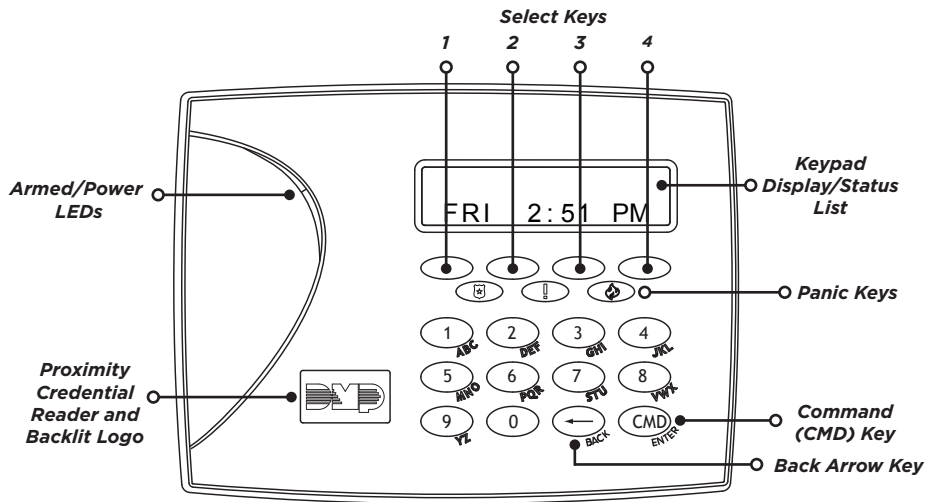
Figure 1: 7463 Keypad Features

ENTER CHARACTERS

Number Pad

1. Choose a character from Table 1.
2. Identify the **Number** the character correlates with and press that number on the number pad.
3. Identify the **Select Key** for the character and press that select key on the keypad. Press that select key again for the lowercase letter (Latin characters only).
4. When the desired character displays on the keypad, return to step 1 to enter another character or press **CMD** if finished.

NUMBER	SELECT KEY			
	1	**2**	**3**	**4**
1	A	B	C	([{
2	D	E	F	)] }
3	G	H	I	! ^ -
4	J	K	L	? " |
5	M	N	O	/ \ `
6	P	Q	R	& $
7	S	T	U	@ %
8	V	W	X	, =
9	Y	Z	Space :	_ ;
0	- +	. '	* <	# >

Table 1: Latin Characters

Panic Key Options

2-Button Panic Keys

All keypads offer a panic key function that allows users to send panic, emergency, or fire reports to the central station in an emergency. Enable the panic key function in the keypad user menu. Place the supplied icon stickers below the top row select keys. The user must press and hold the two select keys for two seconds until a beep is heard.

- **Panic** (left two select keys)—Zone 19 + Device Address
- **Emergency Non-Medical** (center two select keys)—Zone 29 + Device Address
- **Fire** (right two select keys)—Zone 39 + Device Address

User Options Menu

To access the Options menu, press and hold the back arrow and **CMD** keys for 2 seconds.

Backlighting Brightness

Adjust the LCD display brightness level, power and armed LEDs, the green keyboard, and the logo backlighting. At **SET BRIGHTNESS**, use the left select key to decrease the brightness and the right select key to increase the brightness. If the brightness level is lowered, it reverts to maximum intensity whenever a key is pressed. If no keys are pressed, and the speaker has not sounded for 30 seconds, the user-selected brightness level restores.

Internal Speaker Tone

Adjust the keypad internal speaker tone. At **SET TONE**, use the left select key to decrease the tone and the right select key to increase the tone.

Internal Volume Level

Adjust the keypad internal speaker volume for key presses and entry delay tone conditions. During alarm and trouble conditions, the volume is always at maximum level. At **SET VOLUME LEVEL**, use the left select key to decrease the volume and the right select key to increase the volume.

Model Number

Display the keypad model number, firmware version, and date.

Keypad Address

Display the current keypad address.

Connect Status

Display the status of the connection with the panel.

INSTALL THE KEYPAD

1 *Remove the Cover*

1. Insert a flat screwdriver into one of the slots on the bottom of the keypad and gently lift the screwdriver handle toward you while pulling the halves apart. See Figure 2. Repeat with the other slot.

2. Using your hands, gently separate the front from the base and set the front and components aside.

Cover

Base
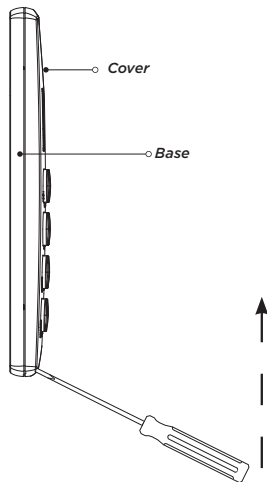
Figure 2: Separate the Keypad Housing

2 *Wire the Keypad*

Use the model 300-7400-6 6-wire network harness to connect the keypad to a LAN and power. One end of the harness connects to the 6-pin header on the back of the keypad. The other end connects to RJ-45 network connector and 12 VDC power. See Figure 3.

Surface and Backbox Mounting Holes

Keypad Back

6-wire Harness

Network

Power

Red Black

Combined 4-square and 3-gang Switch Box Mounting Holes
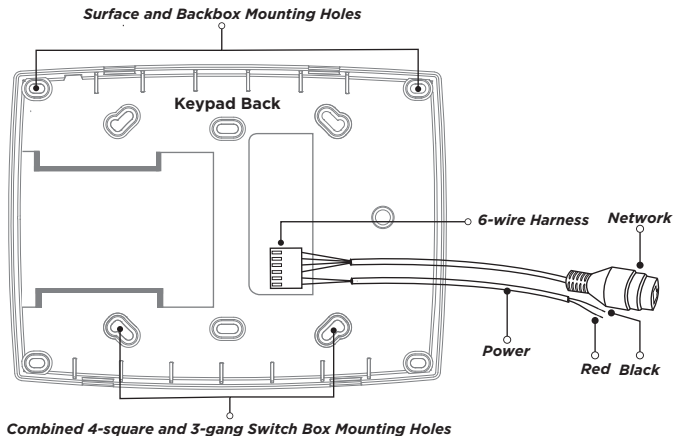
Figure 3: 7463 Keypad

3 Network Connection

Connect an IP network cable from the LAN/WAN connection to the female RJ-45 connector on the 300-7400-6 network harness.

The 7463 keypads communicate AES encrypted TCP with XR Series panels with v201 or higher and with XT Series and XTL Series panels with v202 and higher that have hardwired network installed.

4 Power Connection

Observing polarity, connect the positive (red) and negative (black) wires of the 300-7400-6 network harness to the corresponding positive and negative wires of a 12 VDC power supply, the 371-500L. See Figure 4.

Figure 4: Power Supply to Harness

5 *Optional POE Connection*

The 7463 network keypad cannot be powered directly over the ethernet connection (POE). If it is desired to use a POE connection, a third party POE splitter can be used to separate 12 VDC from the POE connection to connect to the red and black power wires on the 300-7400-6 harness. See Figure 5.
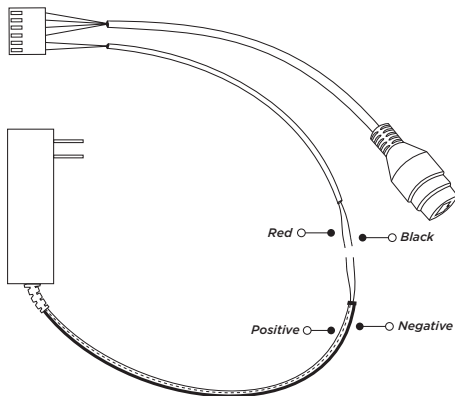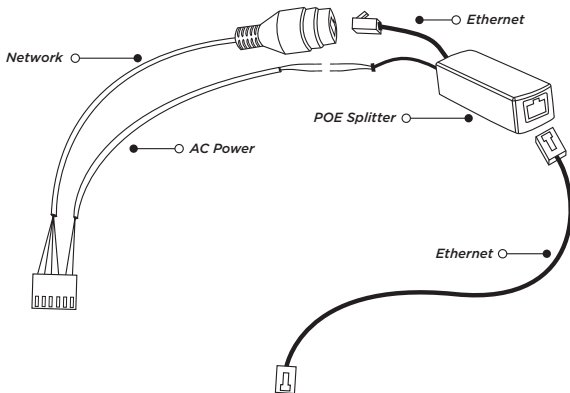

Figure 5: Power Supply to POE Splitter to Harness

PROGRAM THE KEYPAD

Device Setup

After completing each of the following steps, press **CMD** to advance to the next option.
Refer to the panel programming guide as needed.

PROGRAMMER	**Programming** Enter **6653** (PROG) at the keypad.
DEVICE SETUP	**Device Setup** Press **CMD** to advance to **DEVICE SETUP** and select it.
DEVICE SETUP DEVICE NO: -	**Device Number** Press **CMD** to advance to **DEVICE NO** and enter a device number.
DEVICE SETUP * UNUSED *	**Device Name** At ***UNUSED***, enter the device name.
DEVICE SETUP TYPE: KPD	**Device Type** At **TYPE**, select **KPD** (Keypad).

```
DEVICE SETUP
COMM TYPE      NET
```

Communication Type
At **COMM TYPE**, select **NET** (Network).

Note: For XT Series and XTL Series panels, this is only available with panel firmware Version 202 and higher.

```
STOP
```

Save
Press **CMD** until **STOP** displays. Press a top row select key or area to save programming.

Keypad Options

Keypad Options and Keypad Diagnostic menus allow install and service technicians to configure and test keypad operation. To access the installer options:

1. Hold down the back arrow and **CMD** keys for two seconds.
2. At **SET BRIGHTNESS**, enter **3577** (INST) and press **CMD**.

The display changes to **KPD OPT KPD DIAG** and **STOP**. The Keypad Options menu allows you to set the keypad address, select Supervised or Unsupervised mode, change the default keypad message, selectively enable the 2-button Panic keys, Bypass, REX, and set entry card options.

Note: All programming options display on all keypads. However, actual operation for some programming options is restricted to the appropriate model.

KPD KPD		
OPT DIAG		STOP

Keypad Options
To program keypad options, press **KPD OPT**.

INITIALIZE ALL?	
NO	YES

Initialize Option
These options can set the keypad programming memory back to factory defaults. Press any select key or area to enter the initialization menu.

```
INITIALIZE ALL?
SURE?       YES  NO
```

Initialize Confirm Option
The module displays **SURE? YES NO** for confirmation to clear the memory. This is a safeguard against accidentally erasing the programming. No memory is cleared from the programming until you answer **YES** to the **SURE?** option. Selecting **NO** leaves communication options unchanged.

```
CURRENT KEYPAD
ADDRESS: 1
```

Current Keypad Address
Set the current keypad address from 01 to 08 for XT Series, XTL Series, and XR150 Series panels or 01 to 16 for XR550 Series panels. The default address is **01**. To change the current address, press any select key and enter the new address. Do not enter a leading zero for addresses 01 to 09.

```
7400
DHCP?      NO  YES
```

7400 DHCP
Select **YES** to use dynamic IP address information for the module's IP Address, Subnet Mask, and Gateway Address. Select **NO** to enter static IP information.

```
7400 IP ADDRESS
192.168.0.201
```

7400 IP Address
Enter the static IP address of the keypad if the DHCP is set to **NO**. Default is **192.168.0.201**.

```
 SUBNET MASK
 255.255.255.0
```

Subnet Mask
Enter the local subnet mask assigned to the keypad. Default is **255.255.255.0**.

```
 GATEWAY ADDRESS
 192.168.0.1
```

Gateway Address
Enter the local gateway address of the keypad. Default is **192.168.0.1**.

```
 PANEL IP ADDR
 192.168.0.1
```

Panel IP Address
Enter the panel's IP address. Default is **192.168.0.1**.

📝 **Note:** This IP address must match the address programmed in the panel at the Local IP Address option in Network Options. The DHCP programming in the panel must be set to **NO**.

```
 PANEL IP PORT
 2002
```

Panel IP Port
Enter the port number that the keypad uses to send communication to the panel. This must be the same port that is programmed in the 734N Listen Port in Network Options programming of the panel. The panel IP port cannot be the same as the panel network programming port. Default is **2002**.

📝 **Note:** For XT panels, leave the panel's IP port at the default of **2002**.

734N PASSPHRASE

734N Passphrase (XR and XT75 Only)
You must enter an 8-16 character alphanumeric passphrase to encrypt communication with the panel. The 7400 passphrase must match the 734N passphrase entered in Network Options programming of the panel. The passphrase is blank by default.

DEFAULT KPD MSG:

Default Keypad Message
Enter a custom message of up to 16 characters to appear at the top of the keypad display. Press any select key, enter a new message, and press **CMD**.

ARM PANIC KEYS: *PN   EM   *FI

Arm Panic Keys
Use this option to configure the select keys as two-button panic keys. To enable or disable a panic option, press the select key under the desired name: **PN** (panic), **EM** (emergency), and **FI** (fire). Press the select key again to disable the panic option. Once the panic option is enabled, an asterisk displays next to the selected option(s).

ACTIVATE ZONE 2 BYPASS

Activate Zone 2 Bypass
This is a read-only menu item.

RELOCK ON ZONE 2 CHANGE

Relock on Zone 2
This is a read-only menu item.

```
ACTIVATE ZONE 3
REX
```

Activate Zone 3 Bypass
This is a read-only menu item.

```
ALL?: NO      YES
DELAY:          2
```

All? NO YES Delay
Select the number of seconds (1-9) the keypad should wait when an area system displays **ALL? NO YES** during arming/disarming or a Home/Sleep/Away system waits during arming only. The delay also occurs when any credential is presented for arming the Home/Sleep/Away system. If the user doesn't make a selection before the timer expires, the keypad automatically selects **YES** or **AWAY**. Select zero (**0**) to disable this feature. Default is **2**.

```
CARD FORMATS
DMP   CUSTOM   ANY
```

Card Formats
Select **DMP** to allow credentials that use a 26-45 bit data string. The menu advances to **REQUIRE SITE**.

Select **CUSTOM** to disable DMP format and program slots 1-8 as needed. The menu advances to **FORMAT NO**.

Select **ANY** to allow all Wiegand card reads to activate the door strike relay. The door strike relay is activated for the length of time programmed in **ZN 3 REX TIME**. No user code information is sent to the panel. The menu advances to **NO COMM WITH PNL**.

The default card format is **DMP**.

```
CARD FORMATS
FORMAT NO:        -
```

Card Format Number

Select the slot number (1-8) that you want to program for a custom non-DMP card format. The format that is programmed into slot 1 is the default format. In the event that a card with an unrecognized format is used, that card will be read in the format that is programmed in slot 1. To restrict card reads to specific formats, only program slots 2-8.

See Table 2 *Public Card Formats* for some publicly available card formats that can be used with the keypad. Other private or custom formats may also be compatible. Please contact the credential supplier or manufacturer for the bit structure.

Note: If you select slot 1 and you are upgrading from XR panel version 182 or earlier, **FORMAT NAME** will automatically be named **SINGLE CARD FORMAT** and **WIEGAND CODE LENGTH** will default to **45**.

```
FORMAT NAME
*UNUSED*
```

Format Name

Press any select area to rename the card format. Press **CMD** to save and advance.
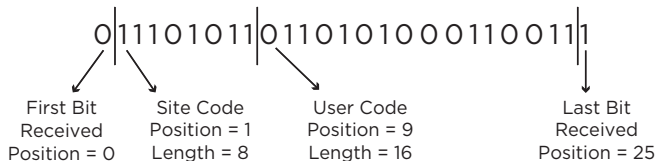
```
WIEGAND CODE
LENGTH:          26
```

Wiegand Code Length

When using a custom credential, enter the total number of bits to be received in Wiegand code including parity bits.

Press any select key or area to enter a number between 1-255 to equal the number of bits. Default is **26** bits.

An access card contains data bits for a site code, user code, and start/stop/parity bits. The starting position, location, and code length must be determined and programmed into the keypad. See Figure 6.

$$0|11101011|0110101000110011|1$$

First Bit
Received
Position = 0

Site Code
Position = 1
Length = 8

User Code
Position = 9
Length = 16

Last Bit
Received
Position = 25

Example: Wiegand Code Length = 26 bits

Figure 6: Wiegand Data Stream Bit Location

```
SITE CODE
POS:  1        LEN:  8
```

Site Code Position and Length

Enter the site code start position in the data string. Press select area 2 to clear the site code start position and enter a number between 0-255. Press **CMD** to save. Default is **1**.

Enter the site code start length in the data string. Press select area 4 to clear the site code length and enter a number between 1-24. Press **CMD** to save. Default is **8**.

```
USER CODE
POS: 9         LEN: 16
```

User Code Position and Length

Define the user code start bit position and length. Press select area 2 to clear the user code position and enter a number between 0-255. Press **CMD** to save. Default is **9**.

Define the user code start bit position and length. Press select area 4 to clear the user code length and enter a number between 16-64. Press **CMD** to save. The default is the DMP value of **16**.

```
REQUIRE SITE
CODE:      NO  YES
```

Require Site Code

Press the top row select key or area under **YES** to use a site code and press **CMD** to view the site code entry display. Press **NO** to advance to **NO OF USER CODE DIGITS**. Default is **NO**.

In addition to user code verification, door access is only granted when any one site code programmed at the **SITE CODE ENTRY** option matches the site code received in the Wiegand string.

```
NO OF USER CODE
DIGITS:           5
```

Number of User Code Digits

The keypad recognizes user codes from 4-12 digits long. Press any top row select key or area to enter a user code digit length. This number must match the user code number length being programmed in the panel. The device will recommend a number of user code digits based on the user code length. Default is **5**.

All bits are read and converted into a decimal number string. The number string is left padded with 0 (zero) if needed for long user code lengths.

Example:

# decoded	1234567
10 digits	0001234567
4 digits	4567

```
NO COMM WITH PNL
OFF  SITE  ANY  ON
```

No Communication with Panel

Define the relay action when communication with the panel has not occurred for 5 seconds. Default is **OFF**. Press any select key or area to change the default relay action:

Press the first select key or area to choose **OFF** (Relay Always Off). The relay does not turn on when any Wiegand string is received. **OFF** does not affect any REX operation. If communication is lost during a door strike, the relay remains on for the door strike duration but turns off at the end of the door strike timer.

Press the second select key or area to choose **SITE** (Accept Site Code). Door access is granted when the Wiegand site code string received matches any site code programmed at **SITE CODE DISPLAY.** Refer to **REQUIRE SITE CODE** for more information.

Press the third select key or area to choose **ANY** (Any Wiegand Read). Access is granted when any Wiegand string is received.

Press the fourth select key or area to choose **ON** (Relay Always On). The relay is always on. Press **CMD** to display the next action.

```
NO COMM WITH PNL
LAST
```

Press the first select key or area to choose **LAST** (Keep Last State). The relay remains in the same state and does not change when communication is lost.

KPD	KPD	
OPT	DIAG	**STOP**

Save Programming
Select **STOP** to save and exit programming.

TEST THE KEYPAD

Test the keypad to ensure alarm backlighting abd individual shortcut keys. To begin testing, access the Installer Options menu. Hold down the **back arrow** and **CMD** keys at the same time until **SET BRIGHTNESS** displays. Enter **3577** and press **CMD**.

```
KPD  KPD
OPT  DIAG    STOP
```

Keypad Diagnostics
Press the select key under **KPD DIAG**. The keypad lights all display segments and illuminates the keyboard in red. The display backlighting then changes to green. The keypad alternates between these two states for approximately two minutes. Press **CMD** at any time to begin testing individual keys.

```
PRESS KEY TO
TEST
```

Test Individual Keys
The keypad lights in red, and the display changes to **PRESS KEY TO TEST**. This option tests each key on the keyboard to ensure it is operating properly. Press and hold each key for two seconds. The key number being held appears in the display. Verify the correct number displays before testing the next key.

```
ZONE 1: OK  ZONE 2: OK
ZONE 3: OK  ZONE 4: OK
```

Zones Okay
This is a read-only menu item.

```
KPD  KPD
OPT  DIAG    STOP
```

Save Programming
Select **STOP** to save and exit programming.

END USER TRAINING

Keypad Arming and Disarming

Area System Arming and Disarming

1. Press **CMD** until the keypad displays **ARM DISARM**.

2. Press the select key under the preferred option.

3. The keypad displays **ENTER CODE: -**. The user presents their card to the reader.

Once validated by the system, all areas assigned to that code arm or disarm automatically. See Figure 7.
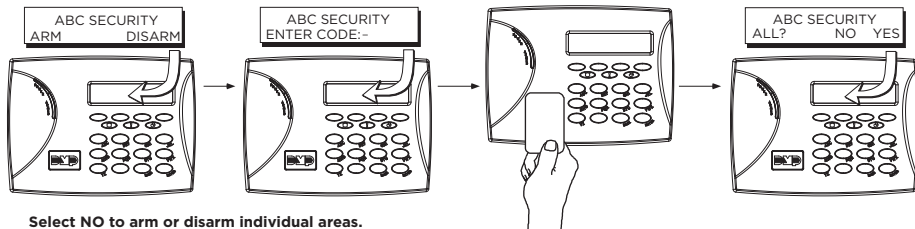
Select NO to arm or disarm individual areas.
Select YES, or simply wait, to automatically arm or disarm all areas for which you are authorized.
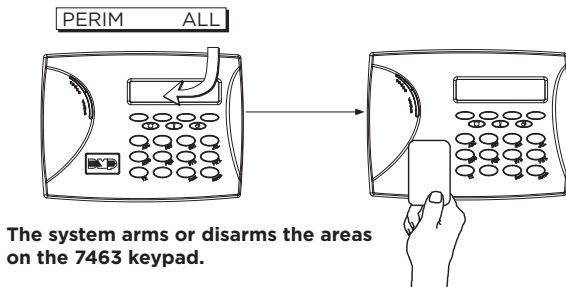
Figure 7: Area Arming and Disarming

All/Perimeter System Arming and Disarming

Present the card to the reader or press **CMD**, the keypad displays **DISARM?** or **PERIM ALL** (when arming). Press the select key under the desired option. The keypad displays **ENTER CODE: -**. Present the card to the reader. Once validated by the system, the selected areas arm or disarm automatically.

Home/Away System Arming and Disarming

Present your card to the reader. If the system is armed, once the card is validated, all areas are disarmed and the keypad displays **ALL SYSTEM OFF**. If the system is disarmed when you present your card, once the card is validated, **HOME SLEEP AWAY** displays. Manually select **HOME**, **SLEEP**, **AWAY** or after a short time-out, all areas automatically arm in the **AWAY** mode.

The system arms or disarms the areas on the 7463 keypad.

Figure 8: All Perimeter Arming and Disarming

Clean the Keypad

Failure to follow cleaning recommendations may result in equipment damage.

- Do not use harsh cleaners to clean keypad surfaces.

- Do not spray cleaner directly onto the keypad.

- Do not oversaturate cleaning cloths or allow cleaner to make contact with internal electronic components, cables, or power sources.

- Do not apply excessive force to keypad displays, touchscreens, keys, or housings when cleaning.

- Use alcohol sprays or wipes that contain 70% isopropyl alcohol.

Method 1

1. Spray a small amount of rubbing alcohol onto a clean, dry microfiber cloth and gently wipe down all keypad touch surfaces, removing any excess cleaner.

2. Wait 10 seconds, then completely dry all keypad surfaces.

3. If necessary, use a clean, dry microfiber cloth to gently remove streaking.

Method 2

1. Use an alcohol wipe to gently wipe down all keypad touch surfaces, removing any excess cleaner.

2. Wait 10 seconds, then use a clean, dry microfiber cloth to completely dry keypad all surfaces.

3. If necessary, use a clean, dry microfiber cloth to gently remove streaking.

REPLACE THE BATTERY

DMP recommends replacing the battery every 3 years under normal use.

Remove the Keypad PCB

1. Disconnect the power supply connector from the back of the keypad.
2. Loosen the top PCB snaps. See Figure 9.
3. Lean the keypad backwards and lift out from the bottom PCB snaps.

Replace Battery

1. Disconnect the battery lead connector from the keypad battery header.
2. Remove the standby battery from the PCB.
3. Observe polarity and connect the battery lead connector to the keypad battery header.
4. Using double-sided tape, place the new battery on the keypad PCB.
5. Properly dispose of the used battery.

⚡ **Caution:** Risk of fire, explosion, and burns. Do not disassemble, heat above 212 ° F (100 ° C), or incinerate.

Install the Keypad PCB

1. Set the PCB into the bottom snaps with the elastomer keyboard already in place. See Figure 9.

2. Line up the PCB alignment post with the hole in the PCB.

3. Press the PCB into the top PCB snaps to secure in place.
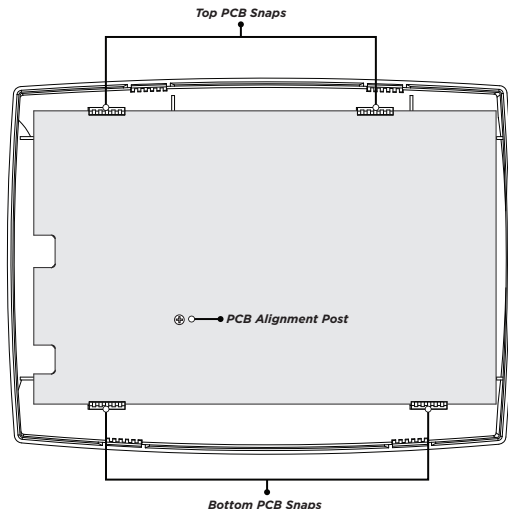
4. Replace the base.

Top PCB Snaps

PCB Alignment Post

Bottom PCB Snaps

Figure 9: PCB Snaps

PRODUCT SPECIFICATIONS

Operating Voltage   12 VDC

Current Draw:
    Standby   100 mA
    Alarm   100 mA
    Max Battery Charging   285 mA

Dimensions   7" W x 5.25" H x 0.5" D
                             17.78 W x 13.34 H x 1.27 D cm

Backup Battery   800 mAh (4 hours standby power)

ACCESSORIES

300-7400-6 6-Wire Network Harness
371-500L Power Supply
695 or 696 Keypad Backbox
777 Protective Keypad Cover
9000BAT/8 Replacement Battery

CERTIFICATIONS

FCC Part 15 RFID Reader FCC ID: CCKPC0216

Industry Canada ID: 5251A-PC0216

COMPATIBILITY

XR Series panels with v201 firmware or higher
XT Series and XTL Series panels with v202 firmware or higher

BUILT-IN PROXIMITY CARD READER

The network keypad provides a built-in proximity card reader that is compatible with most standard 125 kHz proximity credentials. For a list of publicly supported card formats, see Table 2.

CARD FORMAT	WIEGAND CODE LENGTH	SITE CODE POSITION	SITE CODE LENGTH	USER CODE POSITION	USER CODE LENGTH	USER CODE DIGITS
H10301 26 bit	26	1	8	9	16	5
H10302 37 bit W/O FAC	37	0	1	1	35	11
H10304 37 bit W/FAC	37	1	16	17	19	6
Farpointe 39 bit	39	1	17	18	20	7
Corporate 1000 35 bit	35	2	12	14	20	6
Corporate 1000 48 bit	48	2	22	24	23	7

Table 2: Public Card Formats

Some proximity credentials are not compatible with DMP proximity keypads. Test the intended proximity credentials with the application before installation. DMP does not guarantee compatibility with credentials not purchased from DMP.

See Table 3 for a list of some compatible credentials.

125 kHZ PROXIMITY CREDENTIALS	
PSC-1	STANDARD LIGHT PROXIMITY CARD
PSK-3	PROXIMITY KEY RING TAG
PSM-2P	ISO IMAGEABLE PROXIMITY CARD
1306	PROX PATCH™
1326	PROXCARD II® CARD
1346	PROXKEY III® ACCESS DEVICE
1351	PROXPASS®
1386	ISOPROX II® CARD

Table 3: Credentials

FCC INFORMATION

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.

Changes or modifications made by the user and not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

INDUSTRY CANADA INFORMATION

This device complies with Industry Canada License-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. *l'appareil ne doit pas produire de brouillage, et*
2. *l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

Information furnished is believed to be accurate and reliable.
This information is subject to change without notice.