EXADIGM
DEDICATED SOLUTIONS
www.exadigm.com

NX2200 User Guide

Warranty

The information contained in this document is subject to change without notice.

ExaDigm makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties or merchantability and fitness for a particular purpose.

ExaDigm shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Table of Contents

1.0 NX2200 Handheld Mobile Terminal

The ExaDigm NX2200 terminal supports multiple applications and will communicate with the host via Ethernet, Cellular Modem CDMA or GSM/GPRS and WiFi.

- PCI information:
  - PCI PA-DSS approved payment applications
  - PCI PTS approved
- EMV Level 1 and 2 approved
- Modem versions:
  - TNW3T23.000 NX2200 CDMA Verizon
  - TNW4T21.000 NX2200 GSM

NX2200 features include:

- Integrated Bar Code Reader*
- Integrated Finger Print Reader*
- Smart Card Reader*
- SAM Card Reader
- SD Card Reader
- Resistive Touch Screen
- Integrated Contactless Card Reader*

*special order terminals

2.0 Accessories, Parts and Peripherals

Shipped items include:

- NX2200 unit
- Power adapter (8.5V)
- Lithium-ion Battery
- Retractable stylus
- Small paper roll (thermal 2 ¼ x 1.38”)

3.0 Installing the NX2200

When installing the ExaDigm NX2200 for countertop, use a location near a power outlet and Ethernet connectivity if using this option. Carefully plug the AC adapter into the terminal (the plug should insert into the power receptacle on the left side of the terminal) and secure it to a live electrical outlet.

The battery time will vary according to the terminal setup and merchants desired usage.

Certain conditions may damage the terminal or cause it to operate poorly. In general, avoid areas with:

- Excessive heat or dust
- Oil or moisture
- Excessive electrical noise (caused by air conditioners, motors, fans, neon signs, or power tools)
- Direct sunlight
- Artificial light that could reflect glare off the display panel

4.0 Terminal Components

4.1 Front View

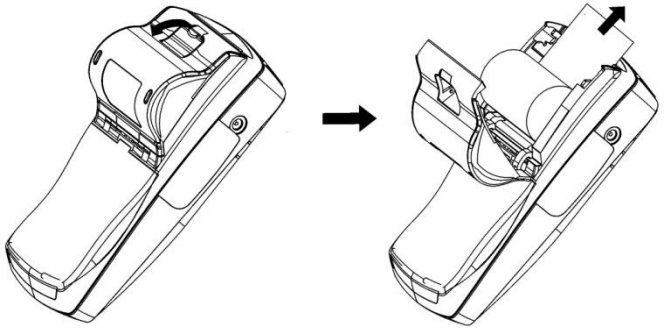
4.2 Terminal Ports

The figure below shows the ports used to connect the terminal to a power source, Ethernet port and various devices such as PIN pads using the multi-port connector.

5.0 Installing a Paper Roll

A paper roll is required to print receipts and reports. The NX2200 uses thermal 2 ¼ x 1.38" paper rolls.

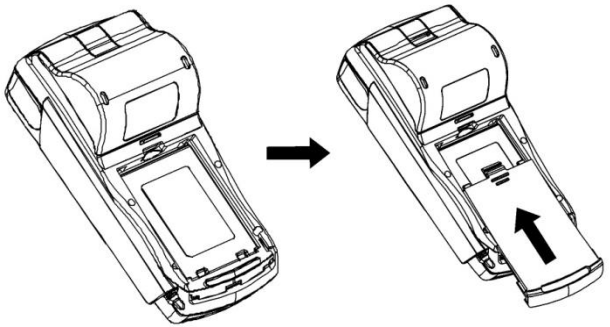
1. Place forefinger under flap at the bottom of the terminal and pull forward using force.
2. Using the tab lift compartment out.
3. Place the paper roll in the printer compartment.
4. Close the printer compartment door by pressing until it clicks into place.



6.0 Installing and Removing the Battery Pack

The power pack allows the terminal to operate when not connected to a power outlet. The NX2200 uses a Lithium-ion battery. Average battery life is 12 hours (utilizing power saving features).

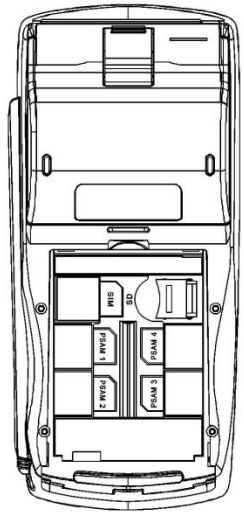
1. Remove the battery door by placing your finger on the door, push down on the ridges and slide down to remove.
2. Remove the battery by placing a finger on the opening and pulling up. The battery will loosen and fall out once the terminal is turned over.
3. To install slide the battery under the locking tabs and push down.
4. Replace the battery door by inserting the top hedge in first, slide up until it snaps into place.



7.0 SIM Chip Installation

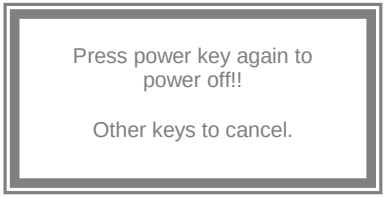
Note: SIM chips are only used in GSM/GPRS equipped terminals. The SIM chip slot is located with the terminal face down under the battery compartment. The battery door must be removed by placing your finger on the ridges of the door and sliding down to remove.

1. Remove the battery by placing a finger on the opening and pulling up. The battery will loosen and fall out once the terminal is turned over.
2. There is only one working compartment be sure to use the one located on the top left side. The SIM chip will be protected by a locking gate.
3. To open the gate, carefully use your fingernail or a small flathead screwdriver to slide the gate from the LOCKED to the UNLOCKED position (slide down to unlock). The distance required is about 1/8 inches or 3mm.
4. Once unlocked, use the square slot to open the gate. The gate is on a hinge and should NOT be removed from the modem.
5. Once the gate is open, the SIM chip can be easily placed into the slot by inserting the card into the grooves of the holder door. The metallic contact on the SIM card must be placed face down (toward the contacts on the unit).
6. Close the door by pushing down and slide the gate up to lock it.



8.0 Powering Terminal

To power on terminal press orange Power key until beep is heard. The boot up process will display.
To power down terminal press orange Power key until the message below appears. Press power again to complete process.



9.0 Card Entry

Swipe card through reader with the magnetic stripe facing down and toward the terminal.

Insert Smart Card into the reader slot below key pad.

10.0 Modem Configurations

Ensure that the terminal is properly connected to an active power source or with a fully charged battery in it.

10.1 CDMA

Before you use the terminal to do live transactions with TCP/IP connections, you need to make sure the modem is activated. Contact your network carrier, ISO or ExaDigm to confirm activation.

10.2 GSM/GPRS

Before you use the terminal to do live transactions with TCP/IP connections, you need to make sure the modem is activated by inserting the SIM card. Contact your network carrier, ISO or ExaDigm to confirm activation.

10.3 Ethernet

Connect the Ethernet cable to the Ethernet port (LAN) on the side of the terminal.

10.4 WiFi

Connect the mini USB stick to one of the available USB ports on the side of the NX2200.

11.0 Connecting External Readers

The multi-purpose USB port allows various devices to be attached and used. You can also attach the multi-purpose attachment to the RS-232 port located on the left side of the terminal.

12.0 Alpha/Numeric Keypad

To get a letter, press the corresponding number and then the alpha key until the letter is displayed.

Number	Alpha 1	Alpha 2	Alpha 3	Alpha 4	Alpha 5	Alpha 6
1	Q	Z	q	z	.	
2	A	B	C	a	b	c
3	D	E	F	d	e	f
4	G	H	I	g	h	i
5	J	K	L	j	k	l
6	M	N	O	m	n	o
7	P	R	S	p	r	s
8	T	U	V	t	u	v
9	W	X	Y	w	x	y
0	SPACE	@	-	,	_	$
	#	=	‘	“	+	!
	~	%	^	&	(	)
	<	>	?	/	*	|
	{	}	[	]	:	;

12.1 QWERTY Keyboard

To input capital letters press the up arrow **[⇧]** and press the key.

To input symbols press the **[?123]** key on the touch screen; the number and symbol screen will display. Press the **[ALT]** key for additional characters.

To backspace and clear characters use the **[DEL X]** key or **[CLEAR]** on the keypad.

13.0 Color-Coded Keys

The color-coded keys perform the following tasks:

- **Red CANCEL Key**: Press the red key to cancel the current operation or return to the previous menu.
- **Yellow CLEAR Key**: Press this key to clear an action and backspace clearing each character.
- **Green ENTER Key**: This key is used like the **ENTER** key on a computer keyboard. Press the green key to signify to the terminal that the task is complete, or press to enable a function or perform an action based on typed data.
- **Orange Power Key:** Press this key to turn on or off the terminal.

14.0 Terminal Indicators

Indicators are located on the display screen and will display when the mentioned peripheral or device is attached.

- Battery
  - Fully charged
  - Half full battery
  - Low battery
- Ethernet connection **<---->**
- Power Adapter
- Radio
  - WiFi signal strength
  - Cellular signal strength

15.0 Security Manager

Security manager is a service within the application that handles user authentication and the log-in process. At least one user (of any level) has to be logged in to use any of the various components. If any operation has access restriction, the service calls security manager to confirm the user has the necessary credentials.

To access the User Manager menu follow the instructions below:

1. Go to **Application Manager**
2. Go to **Admin**
3. Go to **System**
4. Go to **User Manager**
5. Enter **User Name** and **Password** to access

Note: Only Admin (Manager) level has access to this menu.

15.1 Managing User

Security manager provides the user interface to manage users. To access the user management area, the highest level (manager) credential is required to perform the following operations:

- Add User
- Edit User
  i. Unlock User
  ii. Change Name
  iii. Change Pwd
  iv. Change Role
  v. Enable/Disable
- Delete user
- Print users

Managers can add a new user, delete or edit current user or print users list in user management menu.

15.1.1 Roles:

Users are assigned to a specific role when they are created. Currently 3 predefined levels of roles are available:

- Clerk
- Supervisor
- Admin (Manager)

Users' role can be changed from user management area in the edit user section.

15.1.2 Default Users:

Security manager contains two default users, one with manager level credentials and the other with user level credentials.

- Manager level credential [id:manager1 pass:q123456 or q111111]
  - Immediately after setup of Managers the default admin account (manager1) password MUST be changed. The password must contain alpha, numeric and symbols to ensure the strength against non-authorized usage.
- User level credential [id:clerk1 pass:123456q]
  - The default user can be changed and deleted.

Default manager level user cannot be deleted and its credential level cannot be changed. The Default Manager is a root or administrator to the terminal and is required to access the user management area.

To reset the default manager the terminal must undergo a flash file system erase and the application downloaded via TMS.

15.2 User Passwords

- All user passwords must contain numeric and alpha characters. It must be a minimum of 7 and a maximum of 20 characters. If the requirement is not met the terminal will display an error message and the user will be forced to try again.
- User passwords expire every 90 days. Upon expiration the terminal will display a message to the User to change their password. If password has expired the User will be prompted to enter a new password.
- The previous four passwords cannot be used. If a previously used password is entered the terminal will display an error message requesting the correct password.
- Passwords are not stored in the system alone. Data with a combination of password and User ID is encrypted with SHA1 algorithm and kept in the system.
- A user can change their password by following the instructions below:
  1. Go to Application Manager
  2. Go to Admin
  3. Go to User Management
  4. Select Change Password
- The security manager forces users to change any default password after the first successful login.
- The security manager forces users to change any password changed in the user management menu after the first successful login.

15.3 User Rules

- Each user has a unique ID. No duplicate user IDs are allowed, the terminal will display message that the ID is already used.
- After 3 failed login attempts, the user's account is locked.
  - Lock duration is 15 minutes.
  - Managers can unlock the user from the user management menu in edit user section or the user needs to wait 15 minutes before trying to log in again.
- If terminal is in idle mode for more than 14 minutes, the terminal screen locks. In order to unlock it, the last logged in user's authentication is required.

16.0 Data Retention

The ExaDigm payment application is set to purge all cardholder information (all transactions) after reaching the customer defined retention period. The terminal will warn the user before purging, giving a chance to settle the transactions to the payment processor.

The parameter to set the retention period is TVO_CHRETENTIONTIME. The field is configurable to any number of accumulative hours – for example 720 equals 30 days. The maximum value is 9999.

To set the retention period, follow the instructions below:

1. Go to Admin
2. Go to App Setup

3. Go to Security Setup
4. Go to Retention Period
5. Enter the hours in XXXX
6. Press ENTER

16.1 Security Features

16.1.1 Variable Object Security Features

The application uses a module named Transaction Engine Variable Object to recognize if a variable is keeping any of the following account data:

- PAN
- Cardholder Data
- Full Track Data
- Sensitive Authentication Data
- Account Data

16.1.2 Transaction Object Security Features

In order to make sure storage of cardholder and full track data is in the database only when it is actually needed; transaction level controls are added as following:

- **Save Cardholder Data in Database:**
  Cardholder data is saved to database during regular credit transactions.
- **Save Full Track in Database:**
  Full track data is saved to database when store and forward transactions are accepted.

The application uses a module named Transaction Object Interface Processor that makes sure that all "*Transaction Variables*" are deleted from memory after it is processed.

Also the Transaction Object module checks for the following conditions before running a payment transaction and does not allow the transaction and forces the user to perform Settlement if **"any of"** the following initial conditions fails:

- The oldest transaction in database shouldn't be older than a configurable "Cardholder Retention Time" Variable Object.
- Number of transactions in database shouldn't exceed the configurable "Max Transaction Number" Variable Object.
- Total Amount of transactions in database shouldn't exceed the configurable "Max Transaction Total" Variable Object.
- Available free flash memory space in system should be more than "Min Free Memory Size" Variable Object.

16.1.3 Database Object Security Features

The application uses a module named the Database Interface Processor which gathers information from different sources to determine whether to write the account data in the database or not. These settings

are all hard coded and cannot be accessed by any user. The settings are based on PA-DSS requirements.

The following rules are applied in Database module:

- PIN Block Data is not stored in any case.
- CVV Data is not stored in any case.
- Full Magnetic Data is stored only if **"all"** of the following conditions are met:
  i. If offline transaction is supported (Defined in a Configuration Variable Object)
  ii. "Save Full Track Data in Database" flag is active in Transaction Object
  iii. If current transaction is performed offline (or Store and Forward).

17.0 Battery and Charger Safety

Proper battery and charger safety is necessary to ensure the terminal will perform to its potential and reduce the risk of overheating, igniting or explosion, resulting in serious bodily harm or property damage.

- Do not disassemble, open, crush, bend, deform, puncture, shred or attempt to modify the battery or charger.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery or charger, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazards.
- Only use the battery and charger for the terminal for which it was specified.
- Only use the battery with a charging system that has been qualified with the unit. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage or other hazard.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Replace the battery only with another battery that has been qualified with the unit. Use of an unqualified battery may present a risk of fire, explosion, leakage, or other hazard.
- Promptly dispose of used batteries in accordance with local regulations.
- Children should not touch battery and charger.
- Avoid dropping the battery and charger. If the battery or charger is dropped, especially on a hard surface, and the user suspects damage, contact ExaDigm for inspection.
- Improper battery or charger use may result in a fire, explosion, or other hazard.

18.0 Regulatory Notices and Certifications

18.1 Part 15 of FCC Rules

FCC Part 15 Class B Digital Device

The NX2200 has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can

be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Operation of the NX2200 in a residential installation, per Part 15 of the FCC rules, is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. The device must accept any interference received, including interference that may cause undesired operation.

18.2 Part 68 of FCC Rules

This equipment complies with the regulations in Part 68 of the FCC Rules. The FCC registration number and REN (ringer equivalence number) is located on the FCC label located in the back of the terminal.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs connected to the telephone line may result in the device not being able to communicate. Contact the telephone company to determine the maximum RENs for the calling area.

This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subjected to state/local fees.

The equipment uses RJ11C jacks.

The equipment is provided with a FCC compliant telephone cord and modular plug. It is designed to connect to a standard telephone network jack or compatible modular jack that is Part 68 compliant.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance of a disruption of service. If advance notice is not possible then the telephone company will notify you as soon as possible. You will be advised of your right to file a complaint with the FCC if you feel it necessary.

The telephone company may make changes to their facilities, equipment, operations, or procedures that could affect the connection of the equipment. If changes are occurring the telephone company will provide advance notice to allow for time to modify the equipment's connection access to maintain uninterrupted service.

If the equipment malfunctions notify ExaDigm Inc for repair and/or warranty information. If the equipment is causing trouble to the telephone network connection the telephone company may request the equipment to be discontinued until the problem is resolved. Customers are not to attempt to fix the equipment on their own.

ExaDigm Inc recommends connecting the equipment to an AC surge protector to avoid damage to the equipment in the event of electrical surges.

To reduce the risk of fire use only a No. 26 AWG or larger telecommunication line cord.

18.3 SAR Labeling

USA

CDMA SAR compliance for body-worn operating configurations is limited to the specific body-worn accessories, such as belt-clips and holsters, tested for FCC filing.
The highest reported SAR values are: Part 22 Body-worn: 0.228 W/kg, Part 24, Body-worn: 0.184 W/kg.

18.4 UL Standards

Follow the instructions below for Replaceable Batteries:
"CAUTION: Risk of Explosion if Battery is replaced by an Incorrect Type.
Dispose of Used Batteries According to the Instructions."
Follow the general "IMPORTANT SAFETY INSTRUCTIONS when using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.

SAVE THESE INSTRUCTIONS

Follow the instructions below for Telephone line cord safety:
"CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord"
For other TNV accessibility "Disconnect TNV circuit connector before accessing other port" or equivalent.