Skorpio™ X4 - Android OS

Rugged Mobile Computer with 1D/2D Imager

User's Manual

Datalogic S.r.l.
Via San Vitalino 13
40012 Calderara di Reno (BO)
Italy
Tel. +39 051 3147011
Fax +39 051 3147205

©2017 Datalogic S.p.A. and/or its affiliates

◆ All rights reserved. ◆ Without limiting the rights under copyright, no part of this documentation may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means, or for any purpose, without the express written permission of Datalogic S.p.A. and/or its affiliates. Owners of Datalogic products are hereby granted a non-exclusive, revocable license to reproduce and transmit this documentation for the purchaser's own internal business purposes. Purchaser shall not remove or alter any proprietary notices, including copyright notices, contained in this documentation and shall ensure that all notices appear on any reproductions of the documentation. Should future revisions of this manual be published, you can acquire printed versions by contacting your Datalogic representative. Electronic versions may either be downloadable from the Datalogic website (www.datalogic.com) or provided on appropriate media. If you visit our website and would like to make comments or suggestions about this or other Datalogic publications, please let us know via the "Contact Datalogic" page.

Disclaimer

Datalogic has taken reasonable measures to provide information in this manual that is complete and accurate, however, Datalogic reserves the right to change any specification at any time without prior notice. Datalogic and the Datalogic logo are registered trademarks of Datalogic S.p.A. in many countries, including the U.S.A. and the E.U.
Skorpio is a trademark of Datalogic S.p.A. and/or its affiliates. All other brand and product names may be trademarks of their respective owners.

Patents

See www.patents.datalogic.com for patents list.

Table of Contents

Introduction 1
Conventions 1
Product Presentation 2
Available Models 3
Americas Models 3
Europe and Row Models 5
Out of the Box 8
General View 9
Front View 9
Back View 10
Top View 11
Bottom View 11
Accessories 12
Battery 17
Install the Battery 17
Charge the Battery 18
Charge with USB 18
Charge with the Single Slot Dock 19
Replace the Battery 21
SD Card 27
Install the MicroSD Card 27
Getting Started 29
Power Button 29
Power On 29
Suspend Mode 29

Long Press Power Menu 30
Home Screen 34
Home Screen Items 34
Customize the Home Screen 35
Virtual Keyboard 36
Applications 37
Using the Stylus Pen 40
Touchscreen Calibration 41
Keyboards 43
Full-alphanumeric Keyboard (50 Keys) 43
Alphanumeric Keyboard (38 Keys) 46
Numeric Keyboard (28 Keys) 48
Insert the Terminal Emulation Overlay 51
Resetting the Terminal 52
Configuration Reset 52
Device Reset 54
LED Indicators 56
Settings 57
Overview 57
Wi-Fi Settings 58
Connect to Wi-Fi Network 58
Add a Wi-Fi Network 60
Bluetooth Settings 61
Enable Bluetooth® 61
Connect to Other Bluetooth® Devices 62
Configure, Rename or Unpair Bluetooth® Devices 63
Ethernet Configuration 64
Sound 65
Scanner Settings 68
Notification 69
Good Read 72

Formatting 73
Scanner Options 76
Wedge 80
Symbology Settings 82
Global Settings 83
System Upgrade 84
Local Upgrade 84
Recovery Mode 87
Advanced Settings 89
Suspend Timeout 89
Wake-Up Configuration 91
Input Configuration 91
Accessibility 97
Device Info 102
Datalogic Applications 105
Desktop Configuration Utility (DXU) 105
How DXU Works 106
Installation 107
Controls 109
Simplified Deploy 120
Tasks 131
Configuring SureLock and SureFox 163
Command Line DXU Execution 166
SoftSpot™ 167
Tools 171
USB ADB Driver & USB CD-ROM 171
SDK Add-on 172
Install Android SDK 172
Install ADB Driver 174
SureLock 175
SureFox 176

MobiControl 177
Data Capture 179
Imager 1D Data Capture 179
Imager 2D Data Capture 181
Connections 183
USB Connection 183
USB Direct Connection 183
USB HandyLink™ Connection 184
USB Dock Connection 185
Connection to USB Peripherals 186
RS232 Connection 188
RS232 Dock Connection 188
WLAN Connection 189
WPAN Connection 190
Wireless and Radio Frequencies Warnings 192
Technical Features 195
Technical Data 195
Decode Distances 200
Skorpio X4 Imager 1D Linear CCD 200
Skorpio X4 Imager 2D 201
Test Codes 203
Maintenance 211
Cleaning the Device 211
Dock Contacts Cleaning Procedure 211
Ergonomic Recommendations 214
Safety and Regulatory Information 215
General Safety Rules 215
Power Supply 216
Laser Safety 217
LED Class 225
Marking and European Economic Area (EEA) 225

Simplified EU Declaration of Conformity 226
Statement of Compliance 226
Information for the User 228
FCC/IC Labeling 229
FCC Compliance 229
ISED Compliance 231
Radiofrequency Radiation Exposure Information 233
Radio Technologies and Frequency Bands 234
Europe 234
US and Canada 235
Waste Electrical and Electronic Equipment (WEEE) 236
Reference Documentation..... 239
Support Through the Website 239
Technical Support through email or phone. 239
Warranty Terms and Conditions 239
Glossary..... 241

NOTES

Introduction

Conventions

This manual uses the following conventions:

"Mobile computer" and "Skorpio X4" refer to Skorpio X4 mobile computer.

"Single Dock" refers to the Skorpio X4 Single Slot Dock.

The label artworks may be only a draft. Refer to the product labels for more precise information.

Product Presentation

Datalogic's Skorpio X4 mobile computer represents an important evolution for the extremely successful Skorpio product line of compact mobile computers that has set a new standard in the market! The strong commitment to the Retail market is confirmed, while Skorpio X4 represents a reliable and rugged companion for Manufacturing, Transportation & Logistics and Healthcare verticals in all their typical warehousing applications. Skorpio X4 features an all new architecture supporting tremendous speed improvements with Windows Embedded Compact (WEC7), while also supporting an easy migration path to Android.

Whether in department or specialty stores, in hyper stores and supermarkets, convenience stores, grocery or DIY, Datalogic's Skorpio X4 mobile computer fits most any retail in-store requirement for mobile data collection or validation. And with the optional pistol-grip, this unit is also ready for the demanding back-end receiving and warehousing environments as well!

The Skorpio X4 mobile computer is primarily used by the retail store associate for traditional shop floor applications, but can also be used for backend receiving activities.

Equipped with the largest high-visibility color graphics display (3.2 in.) in its class, the Skorpio X4 mobile computer helps users work more efficiently. With a choice of Windows Embedded or Android™ Operating Systems, the Skorpio X4 mobile computer delivers the ultimate in ergonomics, intuitive user interface, computing and data capture technologies, combined with best-in-class ruggedness.

Available Models

The Skorpio X4 is available in different models depending on the options it is equipped with. All options are listed below:

- communication options: 802.11 a/b/g/n radio, Bluetooth®
- data capture options: 1D, 2D imager
- keyboard options: full-alphanumeric, alphanumeric, numeric

For further details about the Skorpio X4 models refer to the web site:

http://www.datalogic.com.

For further information regarding Android refer to the website:

www.android.com.

Americas Models

Android 4.4 - Wi-Fi 1D Handheld

- 942550007 SKORPIO X4 00ANM4TN0HN0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, FCC.

- 942550008 SKORPIO X4 00ANM4TN0HS0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, Green Laser-like 1D Imager w Green Spot, Android 4.4, FCC.

- 942550009 SKORPIO X4 00ANM4TN0HF0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, FCC.

Android 4.4 - Wi-Fi 2D Handheld

- 942550010 SKORPIO X4 00ANM4HS0HN0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, FCC.

- 942550011 SKORPIO X4 00ANM4HS0HS0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, White Illumination 2D Imager w Green Spot, Android 4.4, FCC.

- 942550012 SKORPIO X4 00ANM4HS0HF0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, FCC.

Android 4.4 - Wi-Fi 1D Pistol Grip

- 942600007 SKORPIO X4 00ANM4TN0GN0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, FCC.

- 942600008 SKORPIO X4 00ANM4TN0GS0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, Green Laser-like 1D Imager w Green Spot, Android 4.4, FCC.

- 942600009 SKORPIO X4 00ANM4TN0GF0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, FCC.

Android 4.4 - Wi-Fi 2D Pistol Grip

- 942600010 SKORPIO X4 00ANM4HS0GN0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, FCC.

- 942600011 SKORPIO X4 00ANM4HS0GS0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, White Illumination 2D Imager w Green Spot, Android 4.4, FCC.

- 942600012 SKORPIO X4 00ANM4HS0GF0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, FCC.

Europe and Row Models

Android 4.4 - Wi-Fi 1D Handheld

- 942550019 SKORPIO X4 E00ANM4TN0HN0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, EU.

- 942550020 SKORPIO X4 E00ANM4TN0HS0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, Green Laser-like 1D Imager w Green Spot, Android 4.4, EU.

- 942550021 SKORPIO X4 E00ANM4TN0HF0A4

Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, EU.

Android 4.4 - Wi-Fi 2D Handheld

- 942550022 SKORPIO X4 E00ANM4HS0HN0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, EU.

- 942550023 SKORPIO X4 E00ANM4HS0HS0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, White Illumination 2D Imager w Green Spot, Android 4.4, EU.

- 942550024 SKORPIO X4 E00ANM4HS0HF0A4

  Skorpio X4 Handheld, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, EU.

Android 4.4 - Wi-Fi 1D Pistol Grip

- 942600019 SKORPIO X4 E00ANM4TN0GN0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, EU.

- 942600020 SKORPIO X4 E00ANM4TN0GS0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, Green Laser-like 1D Imager w Green Spot, Android 4.4, EU.

- 942600021 SKORPIO X4 E00ANM4TN0GF0A4

Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, Green Laser-like 1D Imager w Green Spot, Android 4.4, EU.

Android 4.4 - Wi-Fi 2D Pistol Grip

- 942600022 SKORPIO X4 E00ANM4HS0GN0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 28-Key Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, EU.

- 942600023 SKORPIO X4 E00ANM4HS0GS0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 38-Key Functional, White Illumination 2D Imager w Green Spot, Android 4.4, EU.

- 942600024 SKORPIO X4 E00ANM4HS0GF0A4

  Skorpio X4 Pistol-grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v4, 1GB RAM/8GB Flash, 50-Key Full Alpha Numeric, White Illumination 2D Imager w Green Spot, Android 4.4, EU.

Out of the Box

The Skorpio X4 package contains:

- Skorpio X4 mobile computer
- Rechargeable battery pack
- Terminal emulation overlay
- Belt clip (handheld models only)
- Belt clip pivot (handheld models only)
- Hand-strap
- Lanyard (for pistol grip models only)
- Quick Start Guide
- Safety & Regulatory Addendum
- End User License Agreement (EULA) Sheet

Remove all the components from their packaging; check their integrity and compare them with all the packing documents.

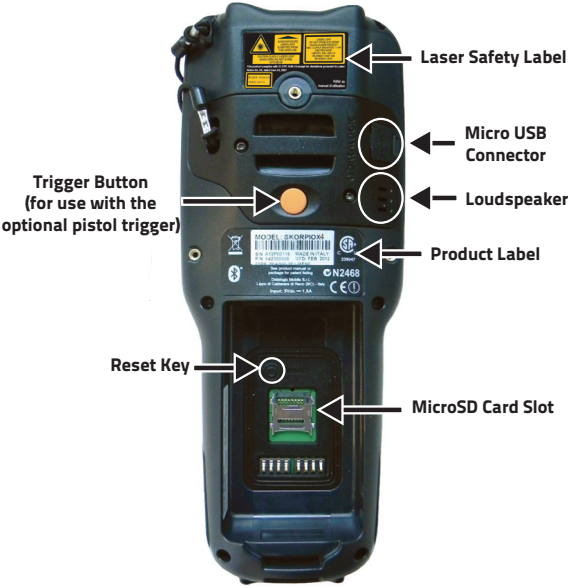
CAUTION

Keep the original packaging for use when sending products to the technical assistance center. Damage caused by improper packaging is not covered under the warranty.

General View

Front View

Back View


Laser Safety Label
Micro USB Connector
Loudspeaker
Trigger Button (for use with the optional pistol trigger)
Product Label
Reset Key
MicroSD Card Slot

Top View

Data Capture Window

Bottom View

HandyLink™ connector (host/device)

Accessories

Docks/Chargers

94A150062	Single Slot Desk Mount Dock with Spare Battery Charging Slot. High- Retention USB-R Type B (client only) and an RS-232 port. Includes Power Supply with Regional Plugs and USB Cable.
94A150067	Single Slot Desk Mount Dock with Spare Battery Charging Slot. High- Retention USB-R Type B (client only) and an RS-232 port (Requires Power Supply 94ACC1381 and Line Cord).
94A150032	Multi Charge Only Dock, recharges 4 terminals and 4 spare batteries (Requires Power Supply 94ACC1385).
94A150055	Multi Ethernet Dock, recharges 4 terminals and 4 spare batteries (Requires Power Supply 94ACC1385).
94A150034	Multi Battery Charger, recharges 4 spare batteries. (Requires Power Supply 94ACC1385).

Power Supplies/Cords

95ACC1113	Power Cord, 120V AC, IEC/US.
95ACC1213	Power Cord, 240V AC, UK.
95A051041	Power Cord, AC, IEC/EUR.
95ACC1215	Power Cord, IEC/Australian.
95ACC1212	Power Cord, IEC/Japan.
95ACC1284	Power Cord, IEC C13,Black Argentina, ROHS.
94ACC1385	Power supply for Multi Battery Charger, 4-Slot Dock. Power line cord has to be ordered separately.

94ACC1380	Power supply for Skorpio X3/X4, for direct charge.
94ACC1381	Power supply for single slot dock, regional plugs included.

Batteries

94ACC0046	Battery, 5200 mAh High Capacity, Skorpio X3/X4 (1 included with main device for pistol grip models).
94ACC0048	Battery, 3000 mAh Standard Capacity, Skorpio X3/X4 (1 included with main device for handheld models).

Cables

94A051020	Cable for dock-PC (RS232) communication.
94A051968	Cable from Micro USB (dock) to USB. Device works as client. 2m straight cable.
94A051969	Cable from Micro USB (dock) to female USB. Device works as host. 1m straight.
94A051970	Cable from device (Handylink) to USB. Device works as client. Connects to PC, 2m straight cable.
94A051971	Cable from device (Handylink) to female USB. Device works as host. Connects to printers or most other peripherals. 15cm straight cable.
94A051972	Cable from device (Handylink) to female DB9 RS232. Null Modem Cable. Connects to PC. 2m straight cable.
94A051973	Cable from device (Handylink) to male DB9 RS232. Straight through cable, Power on Pin 9 (5V @

	500mA). Connects to printers, scanners, or most other peripherals. 15cm straight cable.
94A051975	Car Adapter for PMD (to supply power to PMD from the cigarette lighter). 2m straight cable.
94A051976	Adapter, from PMD Car Adapter to device (to supply power from the cigarette lighter to device, both 94A051975 and 94A051976 are required). 15cm straight cable.

General Accessories

94ACC0079	Module, Ethernet Communication for Single Slot Dock.
94ACC1372	Module, Modem Communication for Single Slot Dock.
94ACC0043	Handle with Mounting Screws, Skorpio X3/X4.
94ACC0049	Hand-strap, Skorpio X3/X4
94ACC0044	Stylus and Tether Pack for Skorpio X3/X4, 5 Pack (one is included with all models of Skorpio X4).
94ACC0045	Quick Release Belt Clip for Skorpio X3/X4, 10 Pack (it includes the bolt and the screw to be fixed to the device, one is included with all the handheld models of Skorpio X4).
94ACC0081	Lanyard to tether the Skorpio X3/X4 to the wrist (it fits both Skorpio X3/X4 and Falcon X3+, one is included with all the pistol grip models of Skorpio X3/X4 and Falcon X3+).

Holsters/Cases

94ACC0050	Belt Holster for Skorpio X3/X4 (it fits both handheld and pistol grip configurations, belt clip included, belt not included).

94ACC0052	Rubber Boot, Skorpio X3/X4.
94ACC0051	Softcase for Skorpio X3/X4 (it fits both handheld and pistol grip configurations, belt clip and shoulder strap not included).
94ACC0151	Snap-on Adapter for Skorpio X3/X4.
94ACC0153	Softcase for Voice for Skorpio X3/X4 (it fits only handheld configurations, belt clip included).
94ACC0076	Heavy duty belt for use with Skorpio X3/X4 belt holster (2.7m in length, adjustable).
94ACC1240	Shoulder strap (5 pcs).
94A150041	Vehicle Holder for Skorpio X3/X4 (it includes two screws and relevant washers for RAM Mount, does not include the RAM Mount itself).
94ACC0075	RAM Mount for Vehicle Holder (it fits both the vehicle holders for Skorpio X3/X4 and Lynx).

CAUTION

Use only a Datalogic approved power supply and cables. Use of an alternative power supply will invalidate any approval given to this device and may be dangerous.

NOTES

Install the Battery

To install the battery pack, insert the battery's alignment lugs into the recesses, then press firmly until the battery latch clicks twice:

Charge the Battery

The rechargeable battery pack is less than half of full charge when delivered. Charge the battery with the USB cable or with the single dock, before using the Skorpio X4 terminal.

During the charging process the charging LED positioned at the top left side of the display glows red constantly. Once the charging process has been completed, the charging LED glows green constantly. The charging LED flashes red when a charging error is detected.

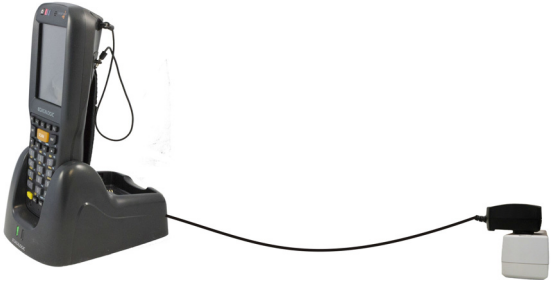
Charge with USB

You can use a standard micro USB to USB cable in conjunction with a power supply adapter to charge the Skorpio X4 from a power outlet.

The Micro-USB port can also be used to charge the Skorpio X4 battery pack from any self-powered USB hub or USB port on a computer.

Don't insert the wall charger into the micro USB port when the Skorpio X4 is inserted into the dock.

Charge with the Single Slot Dock



You can also charge an additional battery pack by inserting it into the rear slot of the dock.

NOTE

The Skorpio X4 may get warm during charging; this is normal and does not mean a malfunction.

CAUTION

By default, the battery pack is disconnected at the factory to avoid damage due to excessive draining.

CAUTION

Avoid storing batteries for long periods in a state of full charge or very low charge.

We recommend charging the battery pack every two to three months to keep its charge at a moderate level to maximize battery life.

Annual replacement of rechargeable battery pack avoids possible risks or abnormalities and ensures maximum performance.

CAUTION

The battery pack autonomy varies according to many factors, such as the frequency of barcode scanning, RF usage, battery life, storage, environmental conditions, etc.

Close to the limits of the working temperature, some battery performance degradation may occur.

CAUTION

The Skorpio X4 should be charged at an ambient temperature between 0 - 35° C (32 to 95 °F) to achieve the maximum charging rate.

Never charge the device battery in a closed space where excessive heat can build up.

As a safety precaution, the battery may stop charging to avoid overheating.

NOTE

To maximize battery life, turn off radios when they are not needed.

Replace the Battery

To replace the battery pack, follow the steps below:

1. Turn off the Skorpio X4 (press the power key and wait for device power off).
2. Press the latch release button and pull the battery latch down:

3. Remove the battery pack.

4. Insert the new battery pack into the slot (see Install the Battery on page 17).

Do not incinerate, disassemble, short terminals, or expose to high temperature. Risk of fire and explosion. Use specified charger only. Risk of explosion if the battery is replaced by an incorrect type. Dispose of batteries as required by local authorities.

Use only Datalogic approved batteries and accessories for battery charging.

Risk of explosion if battery is replaced by an incorrect type.

Dispose of used batteries according to the instructions.

Il y a risque d'explosion si la batterie est remplacée par une batterie de type incorrect.

Mettre au rebut les batteris usagées confor mément aux instructions.

Even if the storage temperature range is wider, it is recommended to store the terminal and the batteries at environmental temperature, in order to achieve the longest battery life.

WARNING

Installing, charging and/or any other action should be done by authorized personnel and following this manual.

The battery pack may get hot, explode, ignite, and/or cause serious injury if exposed to abusive conditions.

If the battery pack is replaced with an improper type, there is risk of explosion.

Do not place the battery pack in or near a fire or other heat source; do not place the battery pack in direct sunlight, or use or store the battery pack inside unventilated areas in hot weather; do not place the battery pack in microwave ovens, in clothes dryers, in high pressure containers, on induction cook surfaces or similar devices. Doing so may cause the battery pack to generate heat, explode or ignite. Using the battery pack in this manner may also result in a loss of performance and a shortened life expectancy.

To power the cradle, use only a Datalogic approved power supply. The use of an alternative power supply will void the product warranty, may cause product damage and may cause heat, an explosion, or fire.

The area in which the units are charged should be clear of debris and combustible materials or chemicals.

Do not use the battery pack of this terminal to power devices other than this device.

Immediately discontinue use of the battery pack if, while using, charging or storing the battery pack, the battery pack emits an unusual smell, feels hot, changes colour or shape, or appears abnormal in any other way.

WARNING

Do not short-circuit the battery pack contacts connecting the positive terminal and negative terminal. This might happen, for example, when you carry a spare battery pack in your pocket or purse; accidental short–circuiting can occur when a metallic object such as a coin, clip, or pen causes direct connection of the contacts of the battery pack (these look like metal strips on the battery pack). Short–circuiting the terminals may damage the battery pack or the connecting object.

Do not apply voltages to the battery pack contacts.

Do not pierce the battery pack with nails, strike it with a hammer, step on it or otherwise subject it to strong impacts, pressures, or shocks.

Do not disassemble or modify (i.e. bend, crush or deform) the battery pack. The battery pack contains safety and protection devices, which, if damaged, may cause the battery pack to generate heat, explode or ignite.

In case of leakage of liquid from the battery, avoid contact with liquid the skin or eyes. If the contact occurs, immediately wash the affected area with water and consult a doctor.

Do not solder directly onto the battery pack.

Do not expose the battery pack to liquids.

Avoid any knocks or excessive vibrations. If the device or the battery is dropped, especially on a hard surface, you should take it to the nearest Authorised Repair Centre for inspection before continuing to use it.

WARNING

If your device stops working for any reason, do not use its battery on other electronic devices without a prior check and approval by an Authorised Repair Centre.

Do not replace the battery pack when the device is turned on.

Do not remove or damage the battery pack's label.

Do not use the battery pack if it is damaged in any part.

Battery pack usage by children should be supervised.

Collect and recycle waste batteries separately from the device in compliance with European Directive 2006/66/EC, 2011/65, 2002/96/EC and subsequent modifications, with US and China regulatory laws and regulations about the environment.

NOTES

SD Card

Install the MicroSD Card

Skorpio X4 supports microSD memory cards. To access the microSD card slot and insert the card follow the steps below:

1. Turn off the Skorpio X4.
2. Remove the battery pack (see Replace the Battery on page 21, steps 1 to 3).
3. Shift the cardholder upwards and then pull it up:

4. Insert the microSD card with the written part upward:

5. Lock the card into place by pushing the cardholder down and then shifting it downwards:

6. Insert the battery pack into the slot (see Install the Battery on page 17).

Remove the MicroSD Card

To remove the microSD card, follow the steps above to access the microSD slot, and remove it from its slot.

Follow proper ESD precautions to avoid damaging the microprocessors in the Skorpio X4 or the microSD card itself. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

Do not force the card. If you feel resistance, remove the card, check the orientation, and reinsert it.

Do not use the microSD card slot for any other accessories.

It is highly recommended that users latch the card cage's bale even when the card is not present.

Power Button

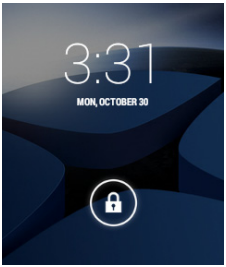
Power On

The Skorpio X4 turns on when the battery pack or the external supply is inserted and the **ON/OFF** Power button is pressed.

Suspend Mode

Suspend mode automatically turns the screen off and locks the terminal to save battery power when the terminal is inactive for a programmed period of time.

Press and release the power button to toggle the terminal in or out of suspend mode:

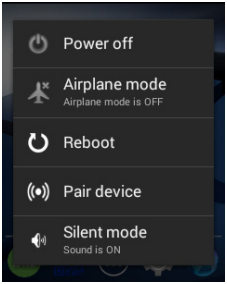


To unlock the home screen, tap and drag the **Lock** icon to the right side of the screen.

To set the timeout limit, see Suspend Timeout on page 89.

Long Press Power Menu

Press and hold the **Power** button until the **Long Press Menu** menu displays:



Power Off

Tap **Power Off** to turn off the terminal. When you turn off the terminal, the session you are working on expires and it won't be possible to restore it.

Airplane Mode

Tap **Airplane Mode** to toggle the mode **ON** or **OFF**.

Reboot

Tap Reboot to perform a Soft Reset (see Soft Reset on page 54).

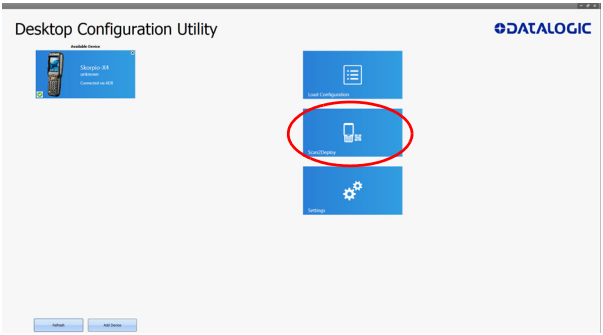
Pair Device

Tap **Pair Device** to start a pairing session with a PC via DXU software. DXU is the Datalogic system application for device configuration and firmware upgrade from a Windows PC. See Desktop Configuration Utility (DXU) on page 105 for further information.

Scan2Deploy

Starts a pairing with DXU by reading a barcode containing the configuration data of your PC.

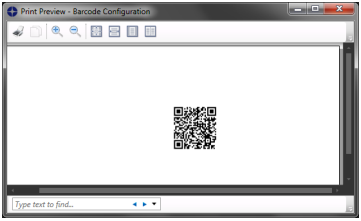
Open DXU on your PC and tap **Scan2Deploy**:



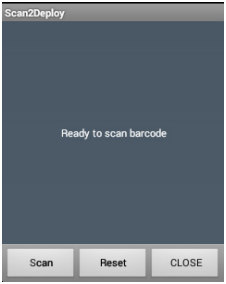
From the **Wi-Fi Configuration** window you can select the barcode type and set the Wi-Fi and pairing configuration data.

Tap **Print** to create the barcode; tap **Save** to save it on your hard disk:

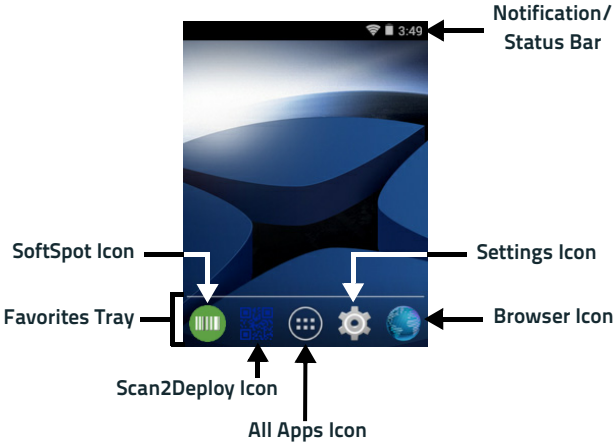
If you select **Print**, the barcode displays on the screen:



From Skorpio X4's **Long Press Power Menu**, tap **Pair Device.** Tap **Scan** to read the barcode:



Home Screen



Home Screen Items

Notification/ Status Bar	Displays the time, status icons (right side), and notification icons (left side).
Favorites Tray	It is like a dock for your home screen. By default, it includes commonly used apps, but you can customize it.
Scan2Deploy Icon	Launch the Scan2Deploy application.
SoftSpot Icon	Launch the SoftSpot application.
All Apps Icon	Opens the Apps window. Tap it to view the Apps and Widgets loaded on your device.
Settings Icon	Opens the Settings.
Browser Icon	Opens the Browser application.

Customize the Home Screen

Application shortcuts placed on the Home screen allow quick and easy access to applications. Widgets are self-contained applications placed on the Home screen to access frequently used features.

The user can add application icons, shortcuts, widgets and other items to any part of the Home screen where there is free space.

To add an application shortcut:

1. Tap the **All Apps** icon.
2. Tap and hold the app icon you want to add until the home screen appears.
3. Drag and drop the icon into position on the home screen panel or in an open spot in the Favorites tray.

To add a widget:

1. Tap the **All Apps** icon.
2. Tap the **Widget** tab.
3. Tap and hold the item you want to add until the home screen appears.
4. Drag and drop the widget into position on the home screen panel.

To create a folder:

Drag and drop an application icon on top of another icon.

Tap the folder.

Tap the title area and enter a folder name using the keyboard.

1. Tap anywhere on the home screen to close the folder. The folder name appears under the folder.

To delete items:

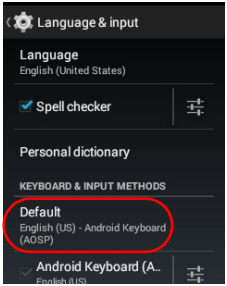
2. Tap and hold the shortcut, widget or folder until it floats on the screen.
3. Drag the item to "**X Remove**" at the top of the screen.

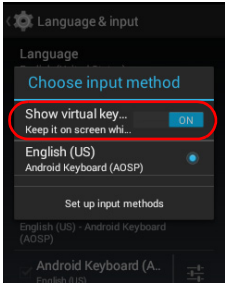
Virtual Keyboard

The virtual keyboard appears when you open an application or select a field that requires text or numerical input.

To configure the keyboard settings, tap **Settings** > **Language & input**.

Tap **Default** to enable/disable the virtual keyboard.





Applications

The **All Apps** screen displays icons for all installed applications. The table below lists the default applications installed on the Skorpio X4.

Icon	Description
	AnExplorer - Another Material File Manager you can use to easily find, browse, move, compress, and otherwise manage your apps.
	Browser - Use to access the Internet or intranet.
	Calculator - Provides the basic and scientific arithmetic functions.
	Calendar - Use to manage events and appointments.
	Clock - Use to schedule alarms for appointments or as a wake-up.
	Downloads - Lists all downloads files.
	DXU Agent - Launch to start a pairing with DXU by reading a barcode containing the configuration data of your PC (see Desktop Configuration Utility (DXU) on page 105).
	Email - Use to send and receive email.

Icon	Description
	Enterprise Agent- Enhances the lockdown functionalities of SureLock and SureFox to ensure advanced device security (see Connections on page 183 and SureFox on page 176).
	Gallery - Use to view photos stored on the internal storage memory and on the microSD card.
	MobiControl - An enterprise mobility management solution that secures and manages the Skorpio X4 and controls all aspects of business mobility (see MobiControl on page 177)
	Movie Studio - Create movie videos.
	Music - Play music stored on the internal storage memory and on the microSD card.
	People - Use to manage contact information.
	Phone - Use to make phone calls.
	Scan2Deploy – Enables data capture (see Data Capture on page 179).
	Scanner – Enables data capture (see Data Capture on page 179).

Icon	Description
	Search - Use the Google search engine to search the Internet and the Skorpio X4.
	Settings - Use to configure the Skorpio X4 (see Settings on page 57).
	SoftSpot - A configurable application meant to provide easy access to frequently used functionalities (see SoftSpot™ on page 167).
	Sound Recorder - Use to record audio.
	SureFox - Use to controls web access for the users (see SureFox on page 176).
	SureLock - Use to secure and lock your device (see Connections on page 183).
	Touchscreen Calibration - Use to calibrate the touchscreen (see Touchscreen Calibration on page 41).

Using the Stylus Pen

The stylus selects items and enters information. It functions as a mouse.

Tap	Tap the screen with the stylus to open items and select options.
Drag	Hold the stylus on the screen and drag across the screen to scroll or pan. Drag in a list to select multiple items.
Tap-and-hold	Tap and hold the stylus on an item to see a list of actions available for that item. On the pop-up menu that appears, tap the action you want to perform.

CAUTION

Use only original Datalogic styluses supplied with the product itself.

In harsh applications, use of screen protectors should be taken into consideration, in order to extend the touch screen operating life.

To prevent damage to the screen, do not use sharp devices or any device other than the Datalogic provided stylus.

Do not apply too much pressure when touching the screen.

For applications where an intensive use of the touch screen is foreseen, please consider that touch screen components are subject to progressive wear.

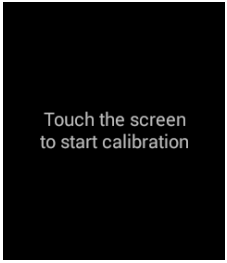
Touchscreen Calibration

After any reset of the Skorpio X4, the device will start and you will be asked to calibrate the screen (see Keyboards on page 43 for further information).

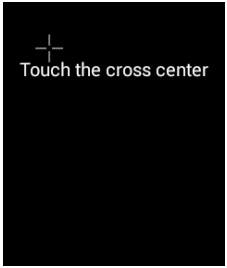
Also, you might need to recalibrate the touchscreen (i.e. when the screen does not respond properly to commands).

To recalibrate the touch screen, follow the steps below:

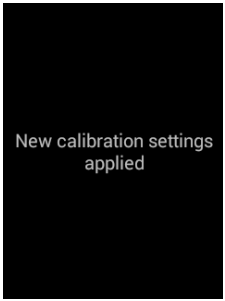
1. Tap **All Apps** ( ) > **Touchscreen Calibration**:



2. Tap/touch the screen to start calibration. Carefully press and briefly hold the stylus on the center of the target. Repeat as the target moves around the screen.



3. By completing the calibration procedure you implicitly accept the new calibration settings. Tap the screen to exit.



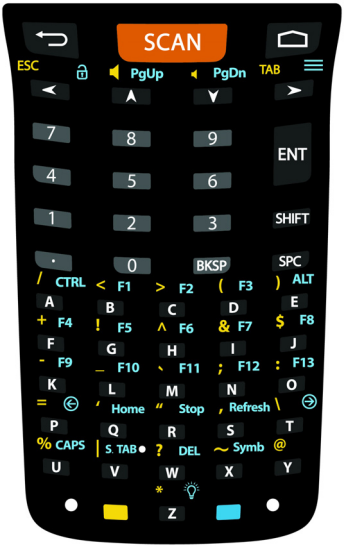
NOTE

The device becomes not usable if you fail touch screen calibration. If the calibration is not done correctly, the Touchscreen Calibration screen will appear, asking you to repeat the procedure.

Keyboards

The Skorpio X4 comes with three different keyboards: a full-alphanumeric keyboard, having 50 keys, an alphanumeric keyboard, having 38 keys and a numeric keyboard, having 28 keys. A 28 keys functional keypad is also available for special configurations.

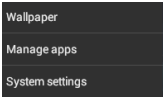
Full-alphanumeric Keyboard (50 Keys)



Main Keys Functions

Key	Function
SCAN	The SCAN key starts data capture. If enabled, it also wakes up the mobile computer from low-power (see Datalogic Applications on page 105). For pistol grip models only, the trigger performs the same function as the SCAN key.
	The Home button to returns you to the home page.
	The Back button returns you to the previous page.
	Arrow keys let you move forwards, backwards, upwards or downwards within text fields, scroll through a Menu list or browse among folder files.
	Yellow modifier (toggle key): when pressed before a standard key, it enables the character or function printed in yellow above the key.
	Blue modifier (one shot key): when pressed before a standard key, it enables the character or function printed in blue above the key.
	The ON/OFF Power button powers the Skorpio X4 ON or OFF. It is placed on the upper left side of the terminal.

Special Function Icons

Icon	Function
	After a Blue modifier key press, the Backlight key will pop up a dialog with backlight intensity selection.
	After a blue modifier key press (a yellow modifier in case of functional keypad), it turns off and on the screen.
	After a blue modifier key press, it simulates the Menu button and opens the following menu (e.g. while using the default Android launcher): 
	After a yellow modifier key press, it sets the volume up.
	After a yellow modifier key press, it sets the volume down.

Alphanumeric Keyboard (38 Keys)

Main Keys Functions

Key	Function
SCAN	The SCAN key starts data capture. If enabled, it also wakes up the mobile computer from low-power (see Datalogic Applications on page 105). For pistol grip models only, the trigger performs the same function as the SCAN key.
	The Back button returns you to the previous page.
	The Home button to returns you to the home page.
	The Menu button opens the following menu: Wallpaper / Manage apps / System settings
	Arrow keys let you move forwards, backwards, upwards or downwards within text fields, scroll through a Menu list or browse among folder files.
	Yellow modifier (toggle key): when pressed before a standard key, it enables the character or function printed in yellow above the key.
	Blue modifier (one shot key): when pressed before a standard key, it enables the character or function printed in blue above the key.
	The ON/OFF Power button powers the Skorpio X4 ON or OFF. It is placed on the upper left side of the terminal.

Special Function Icons

Icon	Function
	After a Blue modifier key press, the Backlight key will pop up a dialog with backlight intensity selection.

Numeric Keyboard (28 Keys)

Main Keys Functions

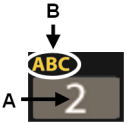
Key	Function
SCAN	The SCAN key starts data capture. If enabled, it also wakes up the mobile computer from low-power (see Datalogic Applications on page 105). For pistol grip models only, the trigger performs the same function as the SCAN key.
	The Back button returns you to the previous page.
	The Home button to returns you to the home page.
	The Menu button opens the following menu: Wallpaper / Manage apps / System settings
	Arrow keys let you move forwards, backwards, upwards or downwards within text fields, scroll through a Menu list or browse among folder files.
	Yellow modifier (toggle key): when pressed before a standard key, it enables the character or function printed in yellow above the key.
	Blue modifier (one shot key): when pressed before a standard key, it enables the character or function printed in blue above the key.
	The ON/OFF Power button powers the Skorpio X4 ON or OFF. It is placed on the upper left side of the terminal.
+	CTRL
+ 0	ALT

Special Function Icons

Icon	Function
	After a Blue modifier key press, the Backlight key will pop up a dialog with backlight intensity selection.

Multitap Function

In the numeric keypad the number keys (key 0 excluded) and the ESC key share the following behavior scheme:



A. Function of the key when directly pressed.
B. Modified by the Yellow key, repeated presses cycle through the letters shown on the keyboard overlay for each key. The letter is entered if you wait for a short timeout.

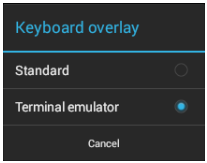
Insert the Terminal Emulation Overlay

To insert the terminal emulation overlay, proceed as follows:

1. Remove the overlay using a torx* screwdriver:

2. Insert the terminal emulation overlay (first the upper side). Fix the overlay with the screwdriver:

To enable the terminal emulator, go to the Settings screen (see Settings on page 57) and tap **Keypad** > **Keyboard overlay**. Select **Terminal emulator**:



* Always use a torx screwdriver to prevent screw damage.

Resetting the Terminal

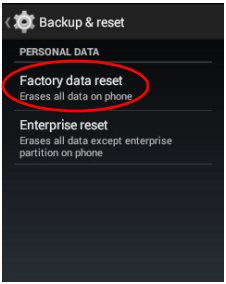
Configuration Reset

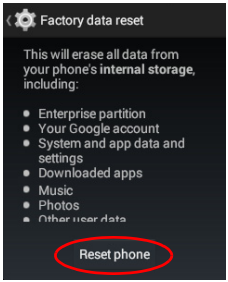
Configuration reset sets the configuration of the device (all its settings) to a known status: the factory status or an enterprise-user-defined status.

Factory Reset

Brings the device to the default configuration, clearing all the user-customized settings.

1. Tap **Settings** >**Backup&reset**.
2. Tap **Factory data reset**
3. Tap **Reset phone**.



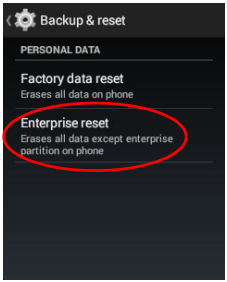


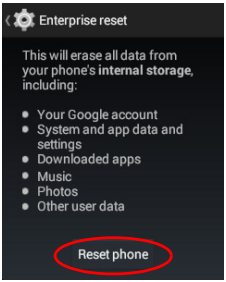
Enterprise Reset

Enterprise Reset brings the device to an enterprise-user-defined configuration, clearing all data and settings except the ones persisted by the enterprise system applications in the /enterprise flash partition and in the /splash flash partition.

The Enterprise folder is a file system storage that is used for deployment and device-unique data. It is persistent and maintains data after an Enterprise reset. Applications and custom settings (i.e. custom boot animation and wallpaper) can persist data after an Enterprise Reset by saving data to the enterprise folder.

1. Tap **Settings** >**Backup&reset**.
2. Tap **Enterprise reset**
3. Tap **Reset phone**.





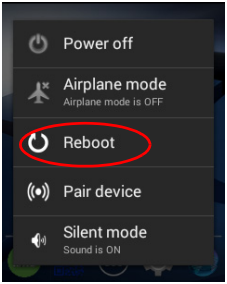
Device Reset

Device reset restarts the device.

Soft Reset

Restarts Android Operative System through an Android API function. It is generally used when some applications stop responding, or it is automatically issued by Android after a Configuration reset.

1. Press and hold the **Power** button.



2. Tap **Reboot**.
3. The device shuts down and then reboots.

Hard Reset

Restarts the device resetting all the hardware components. This procedure guarantees the safe reboot of the device in any condition, without causing damage to the device and without data loss. It is generally used when the device stops responding or after a critical failure that compromises its usability.

To perform a hard reset, do the following steps:

1. Turn off the Skorpio X4 by pressing the ON/OFF Power button.
2. Pull the battery latch down and remove the battery pack.

3. Simultaneously press the SCAN key and the Reset button in the battery compartment.
4. Insert the battery pack.

Turn on the Skorpio X4 by pressing the ON/OFF Power button.

LED Indicators

The LEDs illuminate to indicate various functions or errors on the reader. The following tables list these indications.

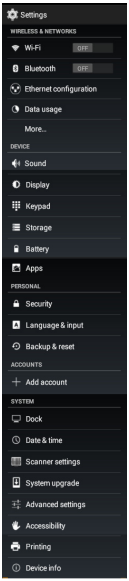
LED	Status	Description
Charging LED (left side)	Red Constant	Light is solid red while charging.
	Green Costant	Light is solid green once the charging process has completed (full charge).
	Red Blink	Blinking red indicates a charge fault.
Keyboard LED (center)	Off	Keyboard in primary.
	Yellow Constant	Yellow alternate key mode.
	Blue Constant	Blue alternate key mode.
Good Read LED* (right side)	Red	Light is red from the time the user presses the scan key (or trigger) until the barcode is decoded (1D models), until the scanner times out (2D imager models).
	Green	Light changes to green when a good decode is completed.

* The Good Read LED has also a "Suspend LED" feature. The decode LED will glow red when the device begins to suspend, and will turn off when the suspend completes successfully.

Settings

Overview

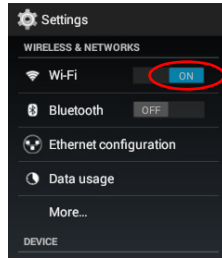
The **Settings** app allows you to check or set system parameters to customize your device. Tap the **Settings** icon on the **Favorites Tray** or on the **All Apps** screen to open the **Settings** screen:



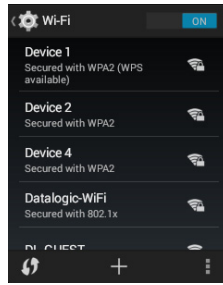
Wi-Fi Settings

Connect to Wi-Fi Network

1. To turn the Wi-Fi on, tap **Settings** and slide the **Wi-Fi** switch to the **ON** position:

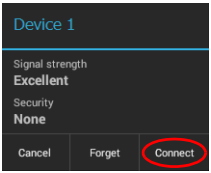


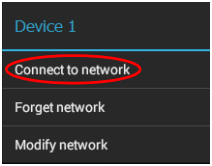
2. Tap **Wi-Fi**. The Skorpio X4 scans for available Wi-Fi networks within range and lists them. If the terminal previously connected to a Wi-Fi network, it automatically reconnects to the same network. Secured networks are indicated with a lock icon:



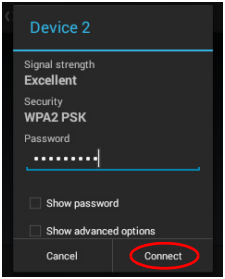
3. Select the network name you want to connect to from the available network list.

4. If the network is open, tap the profile and then tap **Connect**, or press and hold and then select **Connect to network**:



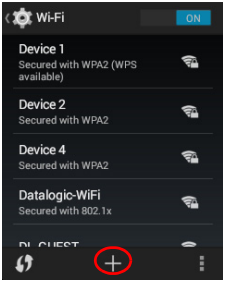


5. If the network is secured, a dialog box appears requesting information relevant to the network security protocol (e.g., password, key, or certificate). Enter the required information, then tap **Connect**:

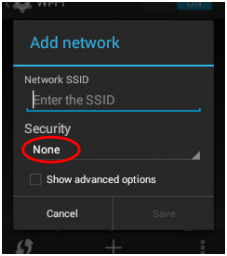


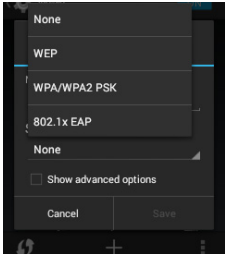
Add a Wi-Fi Network

1. Tap **Settings**, verify the Wi-Fi is turned on and then tap **Wi-Fi**.
2. Tap the Add Network icon '+' located at the bottom of the available Wi-Fi network list:



3. Enter the Network SSID (Wi-Fi network name). For secure Wi-Fi network connections, tap **None** under Security, and then select the type of security protocol required from the pop-up menu (e.g., WEP, WPA/WPA2 PSK or 802.1xEAP). Enter any additional security information required by the type of security protocol selected.





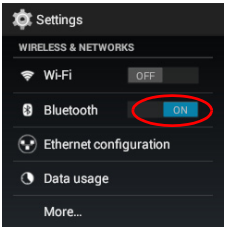
4. Tap **Save**.

Bluetooth Settings

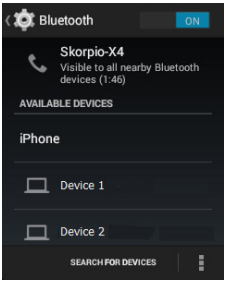
To create a Bluetooth® pairing between your device and another device that has Bluetooth® capabilities, ensure that the two devices are turned on, discoverable, and within close range.

Enable Bluetooth®

1. To turn the Bluetooth® on, tap **Settings** and slide the **Bluetooth** switch to the **ON** position. Once the Bluetooth® radio is enabled, the terminal automatically starts searching for discoverable devices.

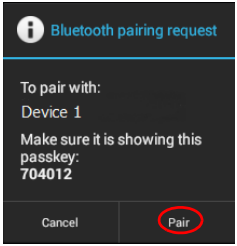


2. Tap **Skorpio X4** to make your device visible to other Bluetooth® devices. The device will be discoverable for 2 minutes.



Connect to Other Bluetooth® Devices

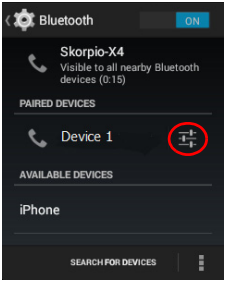
1. Tap **Settings** > **Bluetooth** to search for available Bluetooth® devices. Flick the list and select a device. The **Bluetooth pairing request** dialog box displays on the screen:



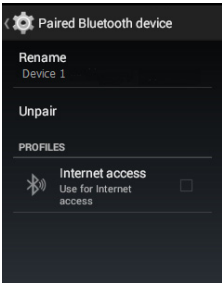
2. Make sure both devices show the same passkey and tap **Pair** on both devices.
3. The selected Bluetooth® device is added to the **Paired Devices** list and a paired connection is established.

Configure, Rename or Unpair Bluetooth® Devices

1. Tap **Settings** > **Bluetooth**.
2. Select a device from the **Paired Devices** list and tap the settings icon next to its name. The **Paired Bluetooth device** window displays on the screen:



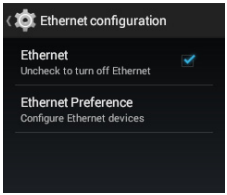
3. Tap **Rename**, **Unpair** or select a different profile from the **Profiles** list available for the paired device:



Ethernet Configuration

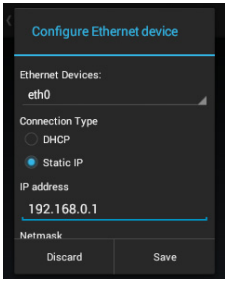
To enable ethernet communication:

1. Tap **Settings** > **Ethernet configuration**.
2. Select the **Ethernet** check box to turn on ethernet.



By default, the Skorpio X4 is configured to obtain IP addresses automatically via DHCP server. Alternatively, the device can be configured to use a statically assigned IP address.

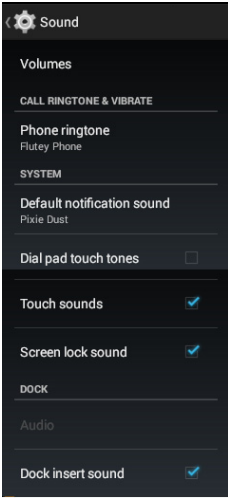
1. Tap **Ethernet Preference**.
2. Select **Static IP** under **Connection Type**, and then input the IP address and any additional information based on your network configuration.



Sound

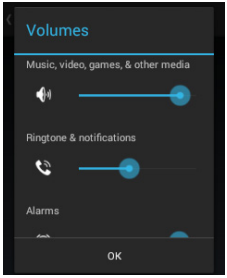
The **Sound** window allows to set the volume and to change the notification, touch and other sound settings.

Tap **Settings** > **Sound**.



Volumes

Sets the volume of music and other media, notifications and alarms.

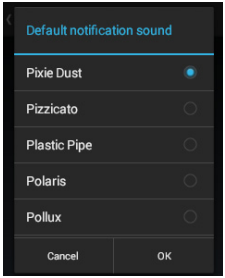


Phone Ringtone

Not used.

Default Notification Sound

Sets the default notification sound.



Dial Pad Touch Tones

Not used.

Touch Sounds

Select to enable touch sounds.

Screen Lock Sound

If selected, a notification sound will play when the screen is locked or unlocked.

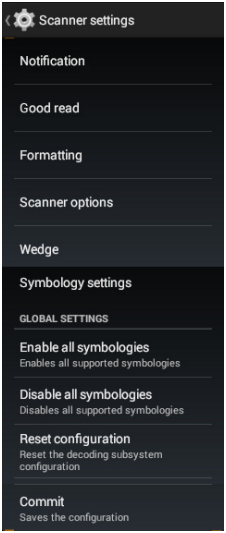
Dock Insert Sound

If selected, a notification sound will play when the Skorpio X4 is inserted into the dock.

Scanner Settings

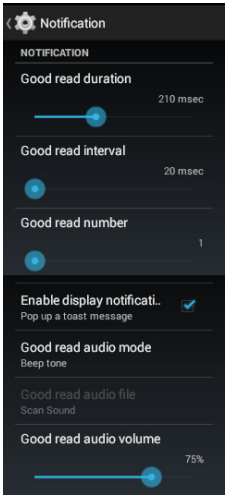
Before you start reading barcodes, use the **Settings** app to view and configure all settings for the scanner.

From the applications menu, tap **Settings** > **Scanner Settings**. Select the desired configuration from the following options:



Notification

Use it to configure the good read tone and display notification:



Good Read Duration

Sets the duration of the notification (LED, green spot or beep) the scanner emits on a good read.

Good Read Interval

Sets the interval between each notification (LED, green spot or beep) the scanner emits on a good read.

Good Read Number

Sets the number of notifications (LED, green spot or beep) the scanner emits on a good read.

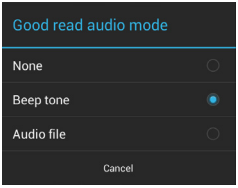
Enable Display Notification

If selected, it enables display notifications (toasts). If cleared, the scanner is disabled until you launch a scanner listener application developed using the Datalogic SDK or enable a keyboard/intent wedge.

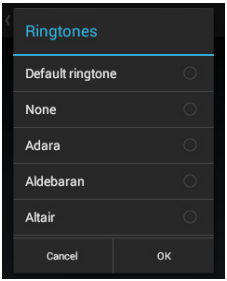
Good Read Audio Mode

Sets the audio tone to:

- None
- Beep tone
- Audio file



If **Audio file** is selected, the option **Good read audio file** displays. Tap it to select the file you want to use as good read ringtone.



NOTE

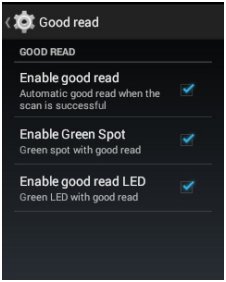
The Notification settings do not apply to an audio file.

Good Read Audio Volume

Sets the volume of beep tone or audio file (if enabled).

Good Read

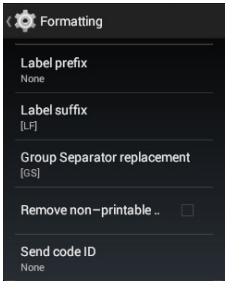
Use it to enable good read notifications (LED, Green Spot):



Tap **Enable good read** to enable/disable notifications (main enabler), then select the notification you want to use.

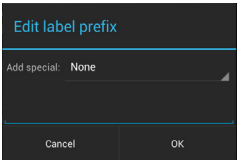
Formatting

Allows to format the barcode text by enabling and configuring the use of prefix, suffix, group separator and code identifier:



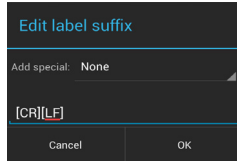
Label Prefix

Tap **Label prefix** to enter the characters you will be using as prefix. Tap **Add special** to select a special character to be added in the current cursor position:



Label Suffix

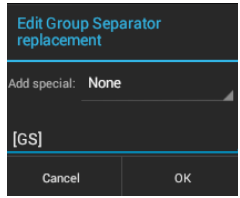
Tap **Label suffix** to enter the characters you will be using as suffix. Tap **Add special** to select a special character to be added in the current cursor position:



Group Separator Replacement

The Group Separator replacement is a non printable data separator character (ASCII code 1D hex). Tap **Group Separator replacement** to enter a string that will be used as GS data separator substituting the standard GS character found in GS1 compliant barcode labels.

Tap **Add special** to select a special character to be added in the current cursor position:

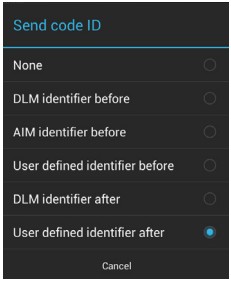


Remove Non-Printable Characters

Select it to remove non-printable characters from a unicode string.

Send Code ID

Tap **Send code ID** to add a code identifier prefix or suffix to the barcode string:



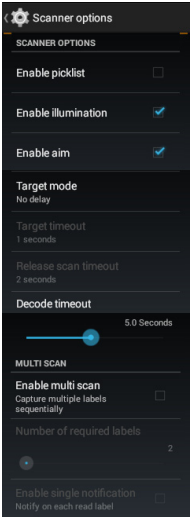
The AIM ID (Association for Automatic Identification and Mobility) is an international barcode identifier. When **AIM identifier before** is enabled, the AIM ID is inserted at the beginning of the decoded barcode.

DLM identifier is a Datalogic specific character identifier.

User defined identifier is a user specific character identifier you can set in the related symbology settings menu.

Scanner Options

Tap **Scanner Options** to customize the Skorpio X4 scanning behavior.



Enable Picklist

If selected, it allows you to pick and decode a barcode from multiple barcodes printed close together, when the scan illumination intersects more than one barcode. Only the targeted barcode will be returned.

Enable Illumination

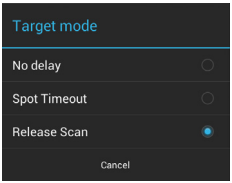
If selected, it causes the scanner to turn on the illumination to aid decoding.

Enable Aim

Enables the laser aim.

Target Mode

If enabled, when the scan button is pressed, the scanner will project an aiming pattern to assist in centering over the barcode before scanning. Tap **Target mode** to select the desired targeting behavior:

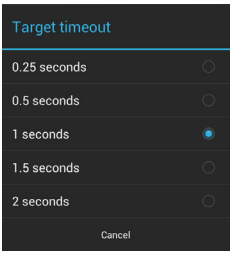


No Delay

Target mode is disabled.

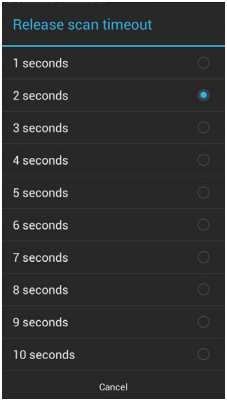
Spot Timeout

Scanning takes place after a programmable time upon pressing the scan button. Tap **Target timeout** to set the duration of the spot:



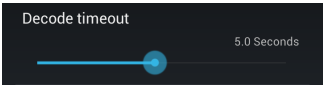
Release Scan

Scanning takes place after the scan button is released. Tap **Release scan timeout** to set the scanning timeout after releasing the scan button:



Decode Timeout

Drag the **Decode timeout** slider to set the maximum amount of time the scanner attempt to decode after target timeout (in case **Spot Timeout** is enabled) or after the scan button is pressed (in case **Target mode** is disabled):



Enable Multi Scan

If selected, it allows you to collect multiple barcodes you are pointing at.

Number of Required Labels

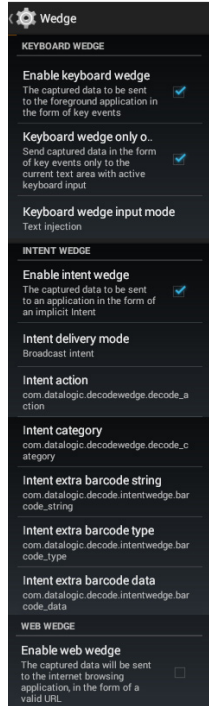
Drag the slider to indicate how many barcodes you want to collect.

Enable Single Notification

If selected, it enables indicators for each label, in order to get an intermediate notification for each label decoded.

Wedge

Use it to enable or disable the keyboard wedge and the intent wedge:



Enable Keyboard Wedge

Inputs the scanned data directly in the current text area in focus. The scanner is enabled whenever a text area is in focus and can receive text.

Keyboard Wedge Only on Focus

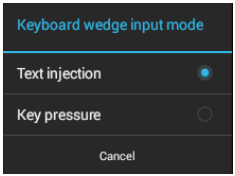
Provides a safer way to input keystrokes into the foreground app.

It allows to send captured data in the form of key events only to the current text area with active keyboard input.

If this setting is not enabled, keystrokes will be always dispatched to the foreground application.

Keyboard Wedge Input Mode

Allows to select the scanned data input mode.



Text Injection

The scanned barcode is injected into the text area.

Key Pressure

The scanned barcode is translated into keyboard strokes.

Enable Intent Wedge

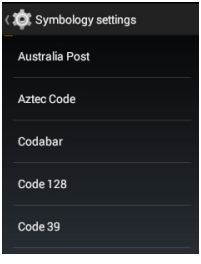
Enables the broadcast of specific intents to the listening applications. The broadcasted intent can have its custom Action, Category and extra content fields. The scanner is enabled whenever the intent option is flagged.

Enable Web Wedge

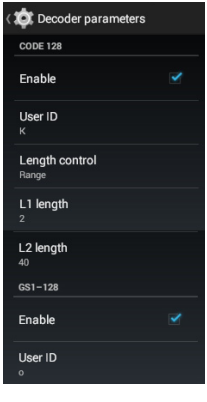
If selected, when a valid URL is found, the captured information is sent directly to the internet browsing application.

Symbology Settings

Each barcode symbology can be customized with additional settings that may affect that specific barcode decoding. Tap **Symbology settings** to configure symbology decoding options:

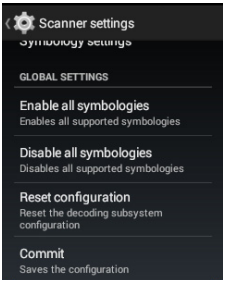


Refer to the sample symbology control panels for examples of the types of fields and options you can modify. The sample below shows the settings of a Code 128 barcode symbology:



Global Settings

Use this section to change symbologies settings globally and to persist them.



Enable All Symbologies

Enables all barcode symbologies.

Disable All Symbologies

Disables all barcode symbologies.

Reset Configuration

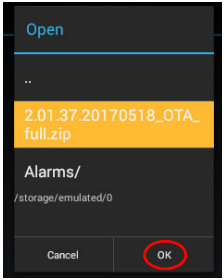
Resets back to default scanner configuration settings.

System Upgrade

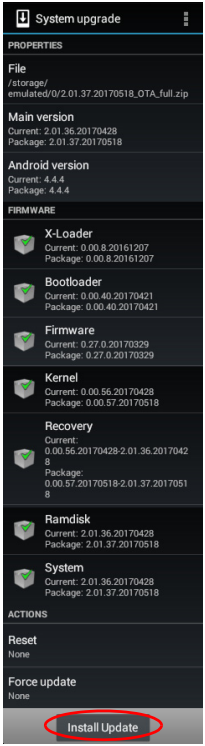
Allows you to upgrade your operative system to the latest version.

Local Upgrade

From the **Settings** menu, tap **System upgrade** > **Local upgrade**. Navigate the file system and select a pre-charged update package. Select the update package you want to install and then tap **OK**:



The following window displays on screen, showing information about the device and the update package components:



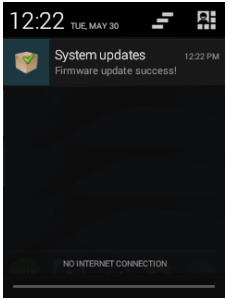
The **PROPERTIES** section shows information about the device model and OS version and the update package version.

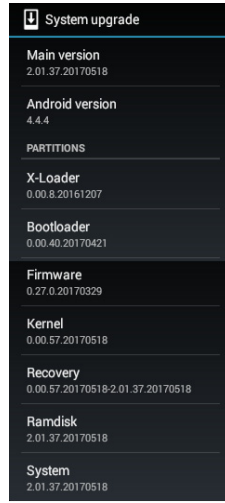
The **FIRMWARE** section shows information about each single update component.

The **ACTIONS** section allows to:

- reset the device after the update (see Resetting the Terminal on page 52)
- force the update of all components, including those already updated.

Tap **Install Update**. The device will reboot and a success notification will be displayed. Tap the notification to display a report showing the installed update components:





If the update fails, the screen will display a failure message and a report showing the reasons for failure.

NOTE

During the update, ensure that:

- **battery level is at least 40% in case of critical update (xloader, bootloader or recovery partition) and 20% in case of any other update;**

or

- **the Skorpio X4 is connected to a power source (USB or dock).**

NOTE

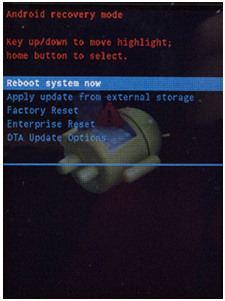
Update is always done in recovery mode (see Recovery Mode on page 87**).**

Recovery Mode

Recovery is an independent, runtime environment that's included on a separate bootable partition from the main Android OS. It contains tools to help repair your installations as well as install official OS updates by using a combination of key presses. Its main purpose is to reset the device, wipe data or perform system updates when the system crashes and the screen is unresponsive.

To enter **Recovery Menu**:

1. Turn off the Skorpio X4 (see Power Button on page 29).
2. Press and hold down the **BACK** + **0** keys simultaneously.
3. Press the **Power Button** while keeping pressed the **BACK** + **0** keys.
4. The **Recovery Menu** displays on the screen:



5. Use the **Up** and **Down** arrows to navigate the menu. You can apply/force updates and perform a configuration reset. Press the **Home Button** to select.
6. Select **Reboot system now**. The device reboot is complete.

NOTE

In Recovery mode, you can only apply updates from external storage (see Local Upgrade on page 84**).**

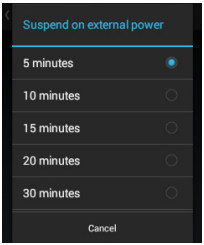
Advanced Settings

Suspend Timeout

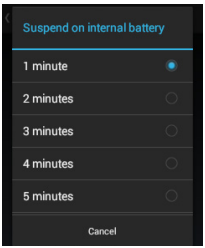
You have two options to set the suspend timeout (see Suspend Mode on page 29 for more information on Suspend Mode):

1. Tap **Settings** > **Advanced settings**:

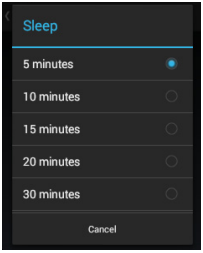
- **Suspend on external power** to set the number of seconds without user input activity before the system is suspended while running on external power:



- **Suspend on internal battery** to set the number of seconds without user input activity before the system is suspended while running on battery power:



2. Tap **Settings** > **Display** > **Sleep** to set the number of seconds without user input activity before the system is suspended while running on either battery power or external power:

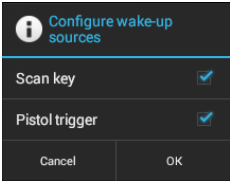


If you use the **Advanced settings** page to set the auto-suspend timeouts, then the **Display** page's **Sleep** control will display the **Suspend on external power** setting the next time you look in the **Display** page.

If you set the **Display** page's **Sleep** control to a new value, it will override both timeouts for external power and internal battery.

Wake-Up Configuration

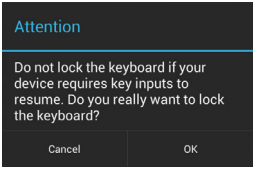
The default wake-up source is the Power button. Tap **Settings** > **Advanced settings** > **Configure wake-up sources** to configure other wake-up sources. Possible wake-up buttons are scan key and pistol trigger:



Input Configuration

Lock Keyboard Input

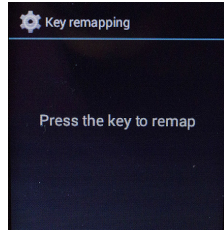
Select **Lock keyboard input** to lock user input from the keyboard. The following pop up windows displays on screen asking for confirmation:



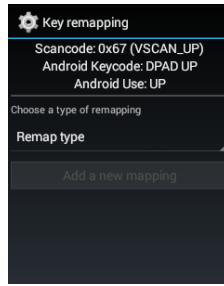
To unlock the keyboard, clear the **Lock keyboard input** check box**.**

Key Remapping

Tap **Key remapping** to remap an input key, then press the key you want to remap. You can remap all the hard keys, including the Power button.

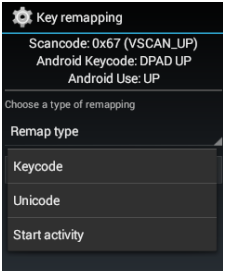


Press the key you want to remap. The following window displays on screen:



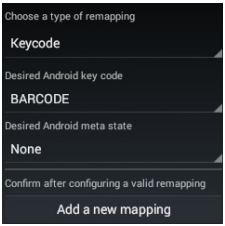
- **Scancode** represents the Linux scancode associated to a physical keyboard key.
- **Android Keycode** represents the Android Keycode associated to the scancode.
- **Android Use** represents a human readable description of the function associated to the Android Keycode.

Tap **Remap type** to select the remapping type:



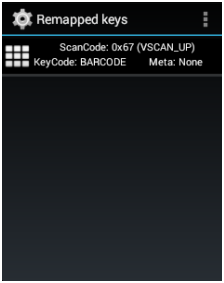
Keycode

Tap **Keycode** to map the selected key to a new function:



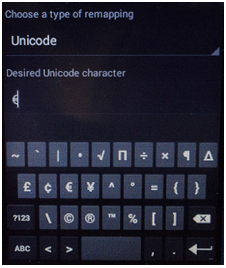
- Tap the second menu (default = **DISABLE KEY**) to select the new function you want to assign to the selected key.
- Tap the last menu (default = **None**) to add a modifier key (such as **Ctrl**, **Shift** or **Alt**).

Tap **Add a new mapping**. A window displays showing the new keymap.

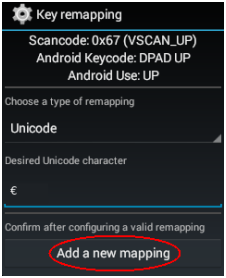


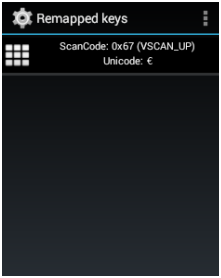
Unicode

Tap **Unicode** to remap a key to display Unicode characters (such as symbol '€'):



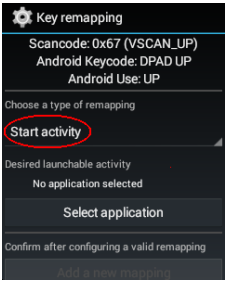
Press the Back Button on the physical keyboard and then tap **Add a new mapping**. A window displays showing the new keymap:

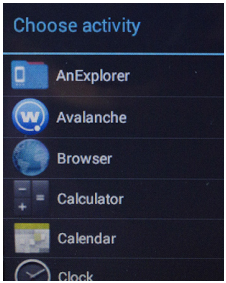




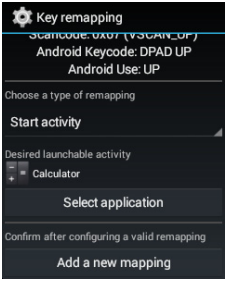
Start Activity

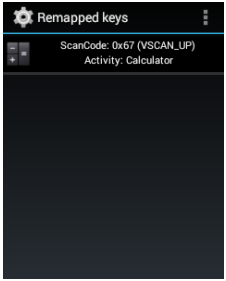
Tap **Start activity** to remap a key to launch an application loaded on your device:





Select the desired application and then tap **Add a new mapping**. A window displays showing the new keymap:





View All Remapped Keys

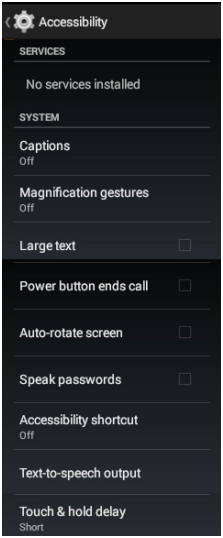
Tap **View all remapped keys** to display all remapped keys.

Swipe left or right to edit or remove an entry and reset the key mapping back to default.

Accessibility

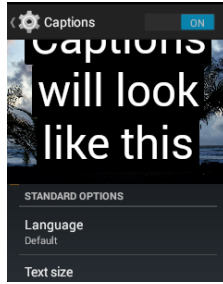
You can customize your Android device using accessibility settings.

Tap **Settings** > Accessibility:



Captions

Tap **Captions** and then tap the **ON/OFF** switch to turn on captions:



When captions are on, you can set the following options for closed captioning:

- **Language**: select the language in which you want captions to appear.
- **Text size**: select the size for your caption text.
- **Caption style**: select the style and color for your caption text and background.

Magnification Gestures

Tap **Magnification gestures** and then tap the **ON/OFF** switch to enable the magnification gestures. When this feature is turned on, you can zoom in and out by triple-tapping the screen.

While zoomed in, you can:

- Pan: drag two or more fingers across the screen.
- Adjust zoom levels: pinch two or more fingers together or spread them apart.

You can also temporarily magnify what's under your finger by triple-tapping and holding. In this magnified state, you can drag your

finger to explore different parts of the screen. Lift your finger to return to your previous state.

NOTE

Triple-tap for magnification works everywhere except the keyboard and the navigation bar.

Large Text

Select to increase the text size.

Power Button Ends Call

Not used.

Auto-Rotate Screen

When enabled, the screen automatically rotates when you move your phone between portrait mode and landscape mode.

Speak Passwords

This feature reads out passwords to you automatically to help fill them in correctly. If the check box is selected, password characters are announced audibly like any other typed characters. If is not selected, password characters are only audible via headset. (To protect your privacy, this setting is disabled by default.)

Accessibility Shortcut

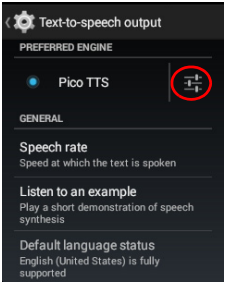
Tap **Accessibility shortcut** and then tap the **ON/OFF** switch to enable accessibility features in two steps:

1. Press and hold the power button until you hear a sound.
2. Touch and hold two fingers until you hear audio confirmation.

If the device has multiple users, using this shortcut on the lock screen temporarily enables accessibility until the device is unlocked.

Text-to-Speech Output

Text to speech output converts language text into spoken synthetic speech. This means you are able to type in content and have it read back to you aloud and automatically.



Tap the setting icon next to the name of your preferred engine (Pico TTS) to change the language and the settings for your engine.

Tap **Speech rate** to select the speed at which text is spoken.

Tap **Listen to an example** to hear a short demonstration of speech synthesis.

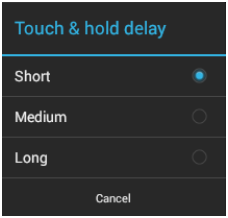
The **Default language status** field displays the current status of your default language. The default language is the language selected in your preferred Text-to-speech engine.

Touch & Hold Delay

This feature lets you set the recognition time for tapping and holding the screen.

A longer touch and hold delay means that you need to keep your finger in the same place for longer before your touch becomes a touch and hold. If you find that you accidentally touch and hold when you intend to tap, consider choosing a longer delay.

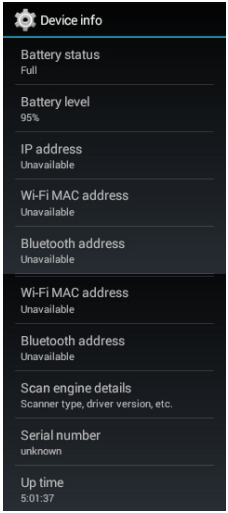
Tap Touch & hold delay to adjust the amount of time before your touch on the screen becomes a touch and hold:



Device Info

The **Device info** screen displays information about the terminal including: model number, Android OS version, open source licenses, baseband version, system versions, build number:

Tap **Status** to display terminal information including battery, network, roaming, IP address, serial number:



Tap **Factory** to display information on factory configuration.

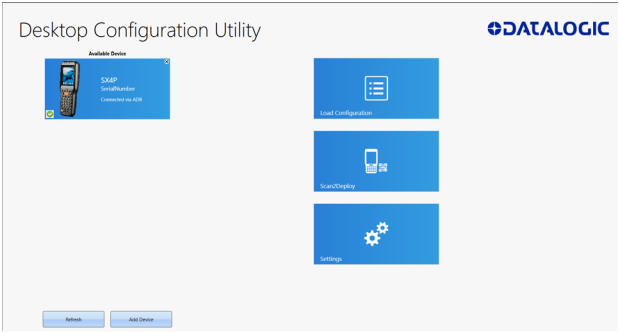
Tap **Legal information** > **Open source licenses** to display information on open source software licenses.

NOTES

Datalogic Applications

Desktop Configuration Utility (DXU)

Datalogic DXU is a unified device configuration utility and firmware update utility. DXU can connect directly to the Skorpio X4 that connects either directly to a PC via USB or remotely over a network, either via Ethernet or Wi-Fi. DXU reports information about currently connected devices.



DXU can configure a wide variety of device parameters, including the scanner and most decoding parameters, the touch screen and the keyboard, interfaces such as NFC, Wi-Fi, Bluetooth, USB, and Ethernet, device settings such as date, time, time zone, and power management, and security settings such as password access. DXU can also configure communication parameters between the

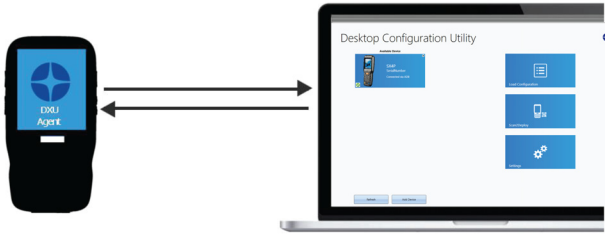
application that runs on a PC and the client applications that run on the device.

DXU offers a method to print out barcodes that Skorpio X4 users can scan to quickly connect to DXU, called Scan2Deploy. DXU also offers the capability to create barcodes that can completely configure the device by scanning specific configuration barcodes alone, without connecting to DXU via USB or via a network. This feature may prove helpful for configuring devices that operate in environments that forbid the use of networked computers.

DXU offers remote control capabilities for remote troubleshooting, allowing a DXU administrator an opportunity to remotely operate the device to check settings, configure the device using its own user interface, and to see what a user sees.

How DXU Works

DXU is really two applications working together. The DXU desktop application runs on a Windows PC, providing convenient UI to configure the Skorpio X4. An application runs continuously on the device to extract current configuration settings and send them to the DXU desktop application, and to receive updated settings from the DXU desktop application and apply those configuration settings to the device.



DXU configurations are stored as configuration files on the PC, and are transmitted to and from the Skorpio X4 as XML web pages. XML is a standard data format that is widely used for a variety of applications on the internet. Some data is encrypted in the XML file to protect your sensitive data from prying eyes, but most data which is not sensitive is transmitted in plain text that can be easily viewed and analyzed.

DXU can connect directly to devices that are plugged into your PC via USB, including those inserted into a powered dock which is connected to your PC via USB. Ask your network specialists for more information.

Installation

The DXU desktop application must be installed on a Windows PC. DXU Agent is already pre-installed on the Skorpio X4.

Supported Windows Versions

Windows Vista family

DXU is supported on both 32-bit and 64-bit versions of Windows Vista.

Windows 7 family

DXU is supported on both 32-bit and 64-bit versions of Windows 7.

Windows 8 family

DXU is supported on both 32-bit and 64-bit versions of Windows 8.

Windows 8.1 family

DXU is supported on both 32-bit and 64-bit versions of Windows 8.1.

Windows 10 family

DXU is supported on both 32-bit and 64-bit versions of Windows 10.

Unsupported Windows Versions

DXU may run on older, unsupported Windows versions, but Datalogic technical support will not support users who have problems if they install DXU on Windows versions no longer supported by Microsoft.

How to Install DXU

1. Copy the installer file to any convenient location on your PC.
2. Launch the installer.
3. If User Access Control (UAC) is enabled on your computer, authorize the installer to run. (UAC is enabled by default on all supported Windows operating systems, but it can be disabled by default. If you do not see this prompt, UAC may have been disabled.)
4. Follow on-screen prompts to finish installing DXU.
5. Follow on-screen prompts to finish installing Datalogic Device Support drivers.

Controls

DXU Agent Controls

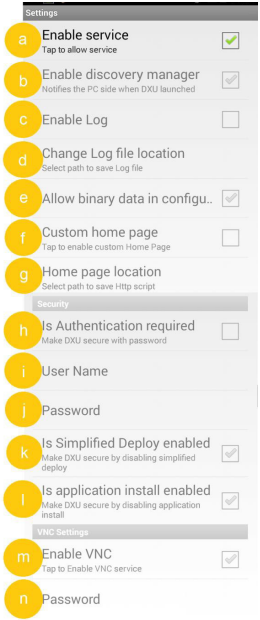
The most important thing to remember about changing DXU Agent settings is that the DXU Agent Service must be disabled before changing settings, and it must be enabled again after changing settings to put those settings into operation.

Find these settings in the DXU Agent application on the device.

1. Launch the DXU Agent application.
2. Tap the Menu button to display the menu.
3. Tap the Settings button.

DXU Agent Settings Window

Here is a brief overview of each of the settings:



a. Enable service

This check box is the key to changing any settings in DXU Agent. Clearing this check box allows you to edit almost all settings. Selecting this check box puts those settings into operation. This check box is selected by default.

Also, if for some reason you want to disable DXU on the Skorpio X4, you can clear this check box to prevent DXU from changing settings.

Doing this will not undo settings changes already made, but it will prevent DXU from getting the device's settings and will prevent DXU from changing any settings on the device.

b. Enable discovery manager

This check box controls the Skorpio X4's broadcast of its name and device type over USB or over a network to the DXU desktop application. When selected, DXU will automatically see when the device connects to USB or over a network. When cleared, DXU will not display when the device connects to USB or over the network. This check box is selected by default.

c. Enable Log

This check box enables DXU Agent's logging capability. When enabled, logs are written to the log file location. Logging can be helpful when diagnosing problems, but at a slight cost of slowing DXU and consuming slightly more power. This check box is not selected by default.

d. Change Log file location

This field allows you to specify where DXU Agent's log file is kept on your device. The default location on Android OS devices is /storage/sdcard0, which is located in the device's on-board flash memory. This location is a persistent location, so log files stored here are safe if the device reboots. If a MicroSD card is used, you may wish to specify that logs be kept on the card if the card has greater capacity than on-board flash. MicroSD cards are also persistent.

e. Allow binary data in configuration

This check box allows a few types of binary data to be transmitted from the Skorpio X4 to DXU, and from DXU to the Skorpio X4. The desktop wallpaper file is an example of binary data that can be controlled by DXU. Selecting this check box allows binary data to be

sent to or from the binary computer in the configuration file. Clearing this check box blocks transfer of binary data in the configuration file. Binary data can be quite large compared to other configuration data, so if performance is important and the desktop wallpaper file does not need to be changed remotely for example, the administrator can clear this check box to make configuration files smaller and quicker to apply. This check box is selected by default.

f. Custom home page

This check box enables a locally hosted web page that can be displayed on the device when network connectivity fails. Selecting this check box will set browsers' error pages to the home page located in the **Home page location** folder. Clearing this check box returns browsers to their default error behavior when they cannot load any particular web page.

g. Home page location

This field stores the path to a locally hosted web page that can be displayed on the device when network connectivity fails. This functionality is enabled by the **Custom home page** check box. This folder can be located in either internal flash (/storage/sdcard0) or in a MicroSD card (/storage/sdcard1). The default value is /storage/sdcard0.

h. Is Authentication required

This check box enables authentication to launch DXU Agent, and puts the User Name and Password into operation. When enabled, the user must correctly type both the user name and password to gain access to DXU Agent's settings. This check box is not selected by default.

Note that these settings are also enforced by the DXU desktop application when it loads the configuration from the device. The DXU administrator will be prompted to type this user name and password. Once authenticated, the DXU administrator can edit the user name and password in DXU and apply these to devices.

i. User Name

This field stores the user name used to log into DXU Agent. It is put into effect when the **Is Authentication required** check box is selected. The default value is "admin" and you can change it.

j. Password

This field stores the password used to log into DXU Agent. It is put into effect when the **Is Authentication required** check box is selected. The default value is "0000" and you can change it.

k. Is Simplified Deploy enabled

This checkbox enables Simplified Deploy. This is a security setting that could be used, for example, to allow use of Simplified Deploy only once as an out-of-box experience.

l. Is application install enabled

This checkbox enables installing applications with Simplified Deploy. This is a security setting that can be used to disable the feature of allowing Simplified Deploy to install customer applications onto the device.

m. Enable VNC

This check box enables VNC, a cross-platform standard for remotely controlling computers. DXU uses VNC to implement its Remote Control feature. Clearing this check box blocks DXU from remotely observing and controlling the device. Selecting this check box enables this feature. This check box is selected by default.

n. VNC Password

This field allows VNC communication to be authenticated, so prying eyes cannot remotely connect to and control your device. This field is blank by default.

Advanced Settings

These settings must match settings on DXU in order for the DXU desktop application to communicate with the your device. A mismatch will result in a communication failure, which will block all configuration functionality.

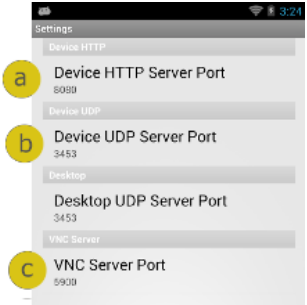
Change these settings only if you understand precisely any advantage you may gain by doing so. Most users will not realize any advantage from changing these port settings.

Find these settings in the DXU Agent application on the Skorpio X4.

To configure DXU Agent's **Advanced Settings**, do this:

1. Launch the DXU Agent application.
2. Tap the Recent Apps button to display the menu.
3. Tap **Advanced Settings**.

As with the DXU Agent settings listed above, these advanced settings can only be changed when the **Enable service** check box is cleared.



a. Device HTTP Server Port

This field configures the HTTP port for the DXU server running on the device. It is set to TCP port 80 by default, the same as most web servers.

b. Device UDP Server Port

This field configures the UDP port for the DXU server running on the device. It is set to UDP port 3453 by default.

Desktop UDP Server Port

This field configures the UDP port for communicating to the DXU desktop server. It is set to UDP port 3453 by default.

c. VNC Server Port

This field configures the HTTP port for VNC running on the device. It is set to TCP port 5900 by default, which is the customary port used by most VNC clients for connections.

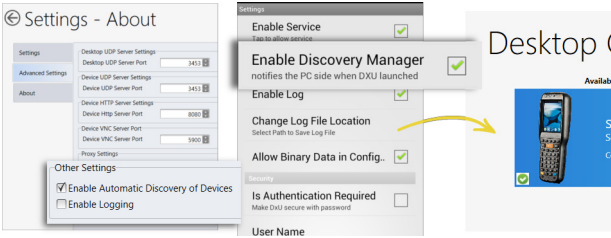
Version

This page displays the DXU Agent version number.

DXU Application Controls

Available Device List and Configuration

The Available Devices list displays devices which are either currently connected, have been connected since launching DXU, or were manually connected at some time in the past. You can refresh the view to automatically show devices or hide devices which connect while you work on another device. In general, they should appear automatically as they connect.

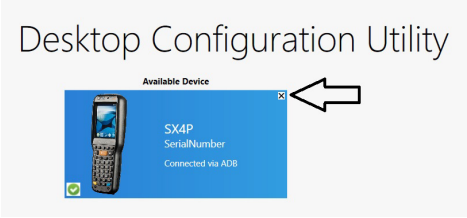


By default, **No Devices Available** will display when no devices announce themselves to DXU either when they connect via USB or when they connect over a network. Simply connecting the Skorpio X4 to a network, even on the same subnet as the PC running DXU, will not automatically display as being available. The device must try to connect to DXU, which sends an announcement packet to DXU. This can be done by scanning Scan2Deploy barcode labels. However, connecting a device to the PC running DXU via USB will automatically display it in DXU. You may also select the **Enable Automatic Discovery of Devices** check box in DXU's Settings view to automatically see any device that connects to the network, but

remember that automatic discovery is restricted to discovering devices only within your PC's subnet.

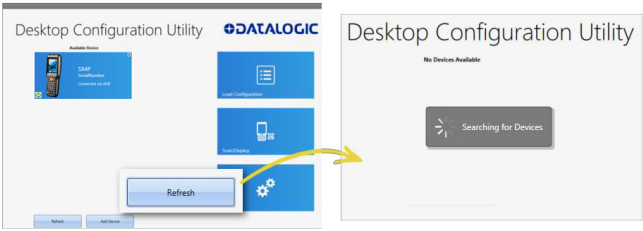
To configure a connected device, you simply click its button under Available Devices to load its configuration into DXU.

To return to the **DXU** main window, click the Back button (generally, a leftward pointing arrow in a circle).



Refresh

This button manually refreshes the display of currently connected devices. This can overcome problems with the automatic display of devices as they connect, and it can remove devices from the list that are not currently connected.



Add Device

This button opens the **Add Device** dialog box which allows you to type the IP address of a device. This dialog box does not support DNS naming of devices. You can also use a custom TCP port if you have configured your device to use one in DXU Agent. For convenience, this field pre-populates with your PC's IP subnet. You need only to type in the last number of your device's IP address if it is in the same subnet as your PC.

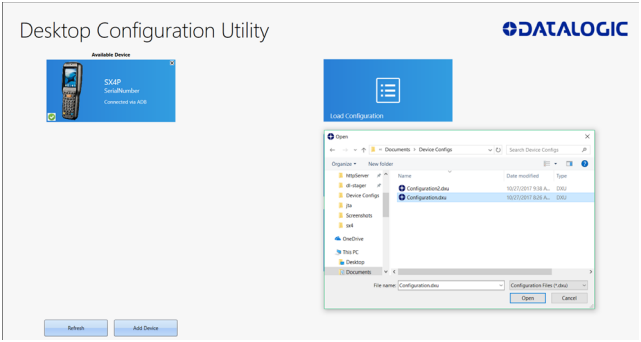
This dialog box allows you to manually connect to devices running DXU Agent that are either inside your PC's subnet or outside it. The limitation is that devices on other subnets must be on a subnet that is routable from your PC's subnet. Consult with your network expert for more information.

Once connected, devices that respond to DXU's query over the network will display in the Available Devices list.

Load Configuration

Clicking the **Load Configuration** button opens a standard file dialog box that allows you to explore for and select a DXU configuration file. Loading a configuration allows you to edit a device's configuration when the device is not connected to DXU. This also allows you to save copies of this configuration to new locations or file names, so

you can edit a copy of the configuration while leaving the original configuration unchanged.



To load a configuration:

1. Click the **Load Configuration** button.
2. Explore to any folder where DXU configuration files are located, then select any configuration file you wish. You can double-click it to streamline opening it.
3. Click the **Open** button.

Note that the default location is your user directory on your PC, but DXU remembers the last directory you opened a DXU configuration file, and always starts in that directory the next time you wish to open another DXU configuration file.

Simplified Deploy

DXU desktop can be configured to enable the Datalogic out-of-box experience Simplified Deploy, using Scan2Deploy. With Simplified Deploy you can automatically connect your device to the network and provision it. The **Scan2Deploy** button on DXU desktop can be used to print barcodes that allow factory reset (Android) or clean boot (WEC7) devices to automatically connect to Wi-Fi, update their firmware, configure the device, and install applications.

In order for Simplified Deploy to function:

- The PC where DXU desktop is installed must be accessible from the Wi-Fi network.
- There must be a Manifest File, a text file located in the folder C:\Datalogic\DXUManifests.
- A Simplified Deploy barcode must be generated and printed using the **Scan2Deploy** button on DXU desktop.

Manifest File

Manifest Files are text .ini files indicating which firmware versions to update devices to ([update] tag), which DXU configuration file to apply ([config] tag), and which .apk (Android) and .cab (WEC7) file applications to install ([install] tag). It is recommended that [update] tags be in separate manifest files. You can specify more than one DXU configuration file to apply and more than one application to install.

Additionally, you can have more than one active manifest files on the PC where DXU desktop is installed, each with its' own Simplified Deploy Barcode to be used by Scan2Deploy utility on the device. In this way you can easily have devices provisioned for different tasks.

By default, firmware, configuration files, and applications are assumed to reside in the C:\Datalogic\DXUManifests folder. If they don't, the Manifest File entry must specify the path.

Manifest File Format

```
[update]
<name of firmware file with full path on DXU Server PC>


[install]
<name of app1 to install file with full path on DXU
Server PC>
<name of app2 to install file with full path on DXU
Server PC>
...
<name of appN to install file with full path on DXU
Server PC>


[config]
<name of DXU configuration file file with full path on
DXU Server PC>
```

Android Example

```
[update] firmware.zip


[install] install.apk
C:\Users\DLUser\Documents\Android\my_terminal.apk


[config] defaultConfigAndroid.dxu
C:\Users\DLUser\Documents\Android\my_user.dxu
```

Scan2Deploy

Scan2Deploy allows the Skorpio X4 running DXU Agent to connect using DXU Agent's Scan2Deploy functionality by scanning a barcode. There are two different Scan2Deploy buttons in DXU, and they have different intentions and different scopes of functionality.

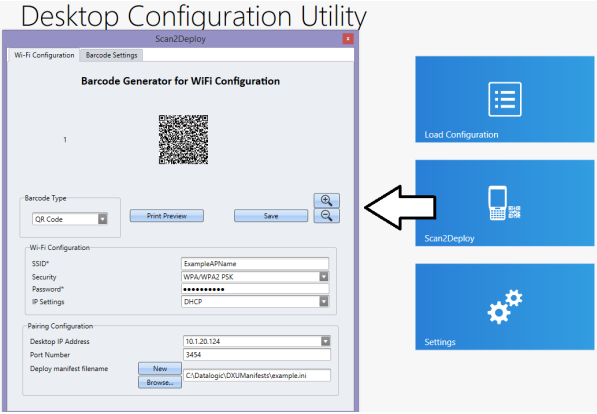
The **Scan2Deploy** button located on the main DXU page does not require an active connection to a device to create a Scan2Deploy barcode label. This button opens the Scan2Deploy dialog box streamlined to create Scan2Deploy labels that can automatically connect a device to a Wi-Fi access point on your PC's subnet and to automatically connect it to DXU, adding it to DXU's **Available Device** list.

Printing a Simplified Deploy Barcode

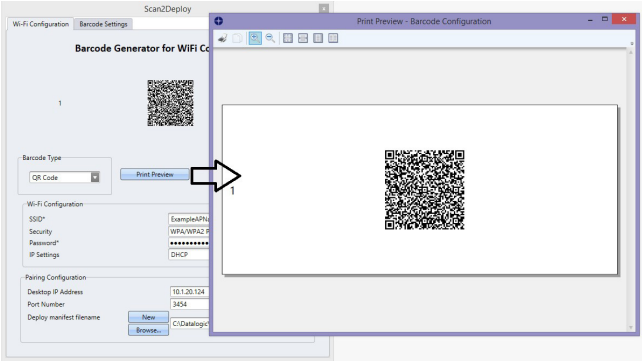
By embedding the IP address of the PC where DXU desktop is installed, the security information for accessing the Wi-Fi network and the name of the desired Manifest File, an encrypted barcode can be printed for use by Scan2Deploy on the device.

To print this barcode, from DXU desktop:

1. Launch **Scan2Deploy**.



2. Enter the Wi-Fi Configuration information so that the device can connect to the network, including SSID and password.
3. Enter the Pairing Configuration, including the IP Address of the PC which has DXU desktop installed, and the name of the manifest file to be used. You can also create a New manifest file as a template for either DXU configuration file or a firmware update file. You could then edit the Manifest File .ini file in a text editor, like Word Pad, to add applications to install.
4. Click the **Print Preview** button, enlarging the barcode view as needed. And then print by clicking the upper left hand printer button.

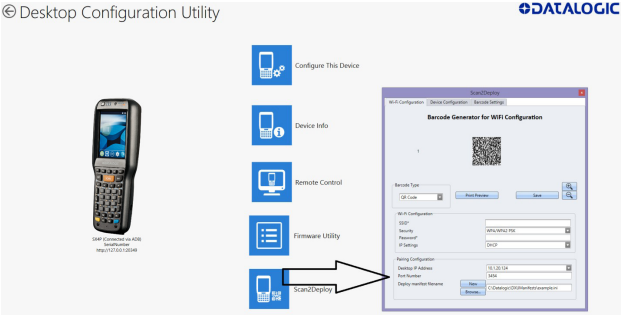


Printing Custom Configuration Barcodes

Outside of Simplified Deploy, the **Scan2Deploy** button located in the **Datalogic Configuration Utility** window can also automatically connect devices to Wi-Fi access points and to DXU. This window also has another tab which controls the ability to include configuration data in the printed barcodes. This version of Scan2Deploy can fully deploy a device configuration to devices which don't have network access to DXU on your PC. When the **Include Unmodified Changes** checkbox is selected, all configuration items will be included in the barcode set. This option results in several barcodes being generated as true Scan2Deploy labels. After scanning the first label in this set, DXU Agent's Scan2Deploy window on your device will display how many barcode labels must be scanned, and will display your progress in scanning them all. Once they are all scanned, DXU Agent will apply the configuration changes automatically, as if you had connected to DXU to transfer the changes.

While it is possible to generate a Simplified Deploy barcode using this window, it has the additional flexibility presented in the **Device**

Configuration tab, which allows printing barcodes to configure the device without the need of the PC with DXU desktop being accessible from the Wi-Fi network.



Wi-Fi Configuration Tab

Barcode Type Menu

The "Barcode Type" menu allows you to choose which barcode symbology that Scan2Deploy labels will be printed in. Each barcode symbology has advantages and disadvantages which may benefit your organization.

QR Code Aztec Data Matrix PDF417 Code 128

QR Code, Aztec Code, and Data Matrix are 2D barcodes that offer high data density and larger capacity, but require 2D scanners to scan them. PDF417 is a stacked linear barcode that offers moderate

data density and larger capacity than linear symbologies. Code 128 is a linear symbology that can be scanned by laser scanners, but its data capacity is low, which may result in a great many individual labels to be scanned in order to fully configure a device remotely.

Print Preview

The Wi-Fi Configuration tab offers a live preview of the barcode as you select the barcode type and enter data into the dialog box's fields.

Save Button

You may save Scan2Deploy labels as graphic files, should this prove convenient for including Scan2Deploy barcodes in an e-mail to a remote office, for example.

Wi-Fi Configuration Controls

As with the other version of the Scan2Deploy dialog box, this group of controls allows you to configure the automatic configuration of a device's Wi-Fi connection. Fields allow you to enter the SSID, password, security method, and IP settings. If you select **Static** in the **IP Settings** menu, additional field will appear allowing you to configure a static IP address for the device that will scan these Scan2Deploy barcodes.

WARNING

If you configure Scan2Deploy labels with a static IP address, do not have two different devices scan the same label set, or an IP conflict will result. Consult your network expert for more information.

Pairing Configuration Controls

These fields let you configure your connection to the PC you are running DXU on. These fields are filled in automatically, but you can

change them to deliberately connect to another IP address where another instance of DXU is running, for example.

Barcode Settings

As with the other version of the Scan2Deploy dialog box, this tab allows to set the maximum size of each label by symbology. For example, if you know that your devices can scan larger 2D labels than DXU's default setting, you can increase the size of your label so fewer labels are needed to fully deploy your configuration.

Settings Window

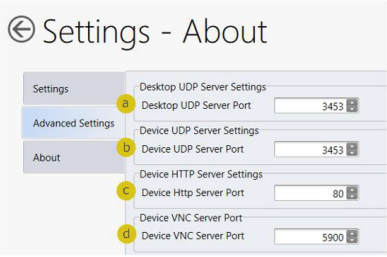
The **Settings** window is opened by clicking the Settings button on **DXU** main window. This view includes controls which should seldom need to be changed, such as the language that DXU displays in, TCP ports used to communicate with remote devices, and the About tab that displays DXU's version.

Language Tab

The **Language** tab allows to switch the language that strings in DXU are displayed in. The default language is US English, but you may choose Italian, Chinese Simplified, or Chinese Traditional. Additional languages may be added later without notice.

Advanced Settings Tab

The **Advanced Settings** tab allows to change TCP/IP ports that DXU uses to communicate several types of information with remote computers that are being configured.



The **Desktop UDP Server Port** (a) and the **Device UDP Server Port** (b) fields must be set to the same value as the matching ports on the remote device to ensure communication and remote configuration. The **Device HTTP Server Port** (c) field must be set to the same value as the matching ports on the remote device to ensure communication and remote configuration. The **Device VNC Server Port** field must be set to the same value as the matching ports on the remote device to enable Remote Control.

About Tab

The **About** tab displays DXU's version. This is likely the first question that Datalogic technical support may ask you if you call in with a question.

Desktop Configuration Utility View

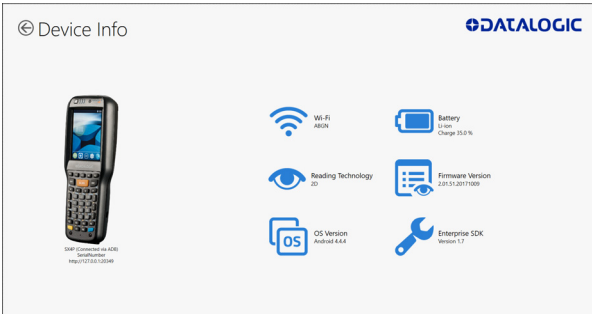
This is the view you see when you click on a device's button in the **Available Device** list. It displays a large picture of your device's model, along with the model name and serial number.

Configure this Device Button

This button allows to configure individual parameter values on your device from DXU. The types of settings include scanner settings, enterprise settings, system configuration settings, DXU Agent configuration settings, SoftSpot settings, Tap2Deploy device-side settings, and SureLock settings. Other settings may be added in the future. Additional settings may be available depending on hardware options installed on your device, and may depend on software installed on your device.

Device Info Button

Clicking this button displays the **Device Info** window, which displays your device's Wi-Fi radio capabilities, the type of barcode scanner on the device, the operating system version, battery information, the firmware version installed on your device, and the version of the enterprise SDK, which may be important for troubleshooting.

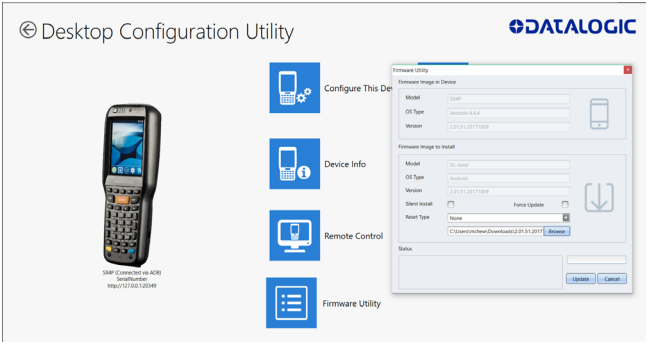


Remote Control Button

Clicking this button opens a **Remote Control** window that displays what is visible on the screen of the device you are currently connected to. This window also includes buttons to remotely activate the devices external buttons, and to capture a screen shot of what is visible on its screen.

Firmware Update Utility Button

Clicking this button opens the **Firmware Utility** dialog box, which you can use to update the firmware on your device.



Scan2Deploy Button

Clicking this button opens the **Scan2Deploy** dialog box (see see 'Printing Custom Configuration Barcodes" on page -124). Use it to create Scan2Deploy barcode sets that can fully configure a device without network access to DXU on your PC, containing all configuration settings in one set of barcodes and applying them by scanning the labels - all without the need to use Simplified Deploy.

Tasks

Connect to a Device via USB

You can connect to the Skorpio X4 by connecting it to your PC with a USB cable. DXU will connect to it directly without any further set-up.

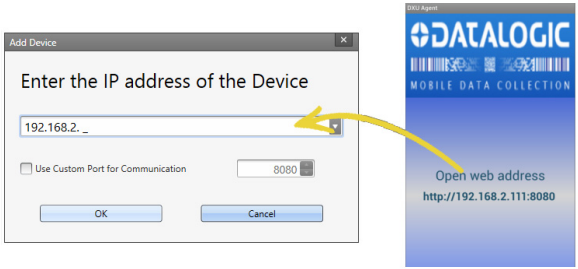
1. Launch **DXU**.
2. Connect your device to your PC with a **USB** cable.
3. Click the device's button in the **Available Device** list.

Connect to a Device via Network Manually

If DXU Agent on the device has its **Enable Discovery Manager** feature enabled and **DXU** has **Automatic Discovery of Devices** enabled under **Advanced Settings**, then clicking **Refresh** should display it in the **Available Device** list if it is in the same subnet.

However, if you want to manually add a device in **DXU,** make sure both device and system are in the same subnet and follow these steps:

1. From the **DXU** main window, click **Add Device**;



2. In the **Add Device** dialog box, enter the **IP address** of the device and optionally its port, if it is has been changed from the default;

NOTE

You will see the IP Address and port details displayed on the DXU main window along with the model name, serial number, and an illustration of the device.

3. Click **OK** to complete.

The added device will display on the left side of the console under **Available Device**.

NOTE

You can also directly connect the device to DXU using USB.

Connect to a Device via Network Using Scan2Pair

These steps assume you already have your network set up, and you already have your printer set up. To connect a device to a Wi-Fi access point and to DXU using the default settings, follow the steps below:

1. Launch **DXU**.
2. Click **Scan2Deploy** on the **DXU** main window.
3. Enter the **SSID** and **Password** for the Wi-Fi access point that your device will use to connect to your network.

NOTE

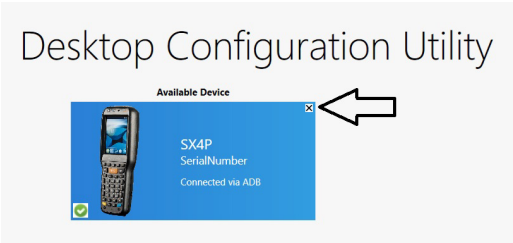
In most cases you should be able to leave other fields with their default values. You may, of course, change those values as needed to work with your network setup.

4. Click **Print Preview**.
5. Click **Print** in the button bar.
6. Since **Print** dialog boxes vary by the model of your printer, configure the print as you normally do. Close these dialog boxes to exit.
7. Resume the device and unlock its screen.
8. Launch the **DXU Agent** application.
9. Tap **Menu**, and then select the **Scan2Deploy** command.
10. Scan the barcode.

Your device should appear in the **Available Device** list of the **DXU** main window. Click **Available Device** to continue configuring your device.

Delete a Device from the Available Device List

Click the exit button (**X**) located at top right of the device.



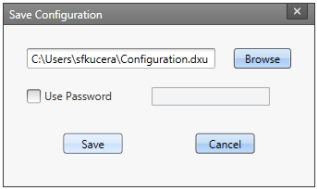
Configuration Files

DXU configuration files end with the *.dxu file extension. They are XML files that can contain binary data for some configuration items, such as wallpaper images.

Save a Configuration File

To save a configuration file, follow the steps below:

1. From the **Device Configuration** window, click the **Save As** button.

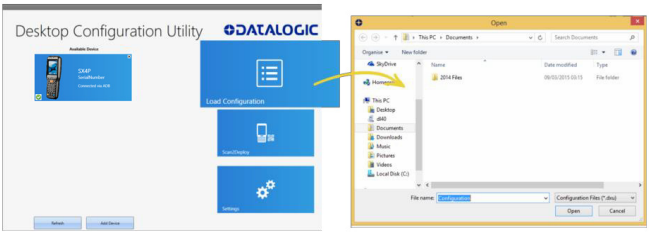


2. You may type the path and the file name in the field, or you can click the **Browse** button to use a standard file dialog box to explore to the folder of your choice and type the file name. Unusually, clicking the **Save** button in the **Save As** dialog box does not actually save the configuration file, but returns you to the **Save Configuration** dialog box.
3. Optionally, you may select the **Use Password** check box and type a password into the field. This will force anyone who opens this configuration file in the future to correctly type the password in order to open the file.
4. Click **Save**.
5. Click **OK** to dismiss the confirmation dialog box.

Open a Configuration File

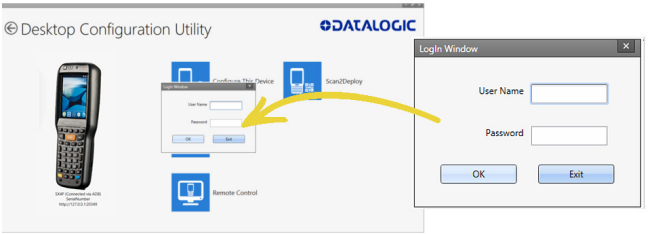
To load a configuration file previously saved, do this:

1. Launch **DXU**.
2. Click the **Load Configuration** file. This will open a standard file dialog box.
3. Explore to your configuration file, select it, and click **Open**.



Open a Configuration File Which is Authenticated

DXU displays a login prompt when you open a configuration file that requires authentication and when you connect to a device with a password set in the DXU Agent.



To open a configuration or to connect to a device which requires authentication:

1. Open a configuration file or load the configuration from a connected device.
2. Type the user name for this configuration/device into the **User Name** field.
3. Type the password for this configuration/device in the **Password** field.
4. Click **OK**.

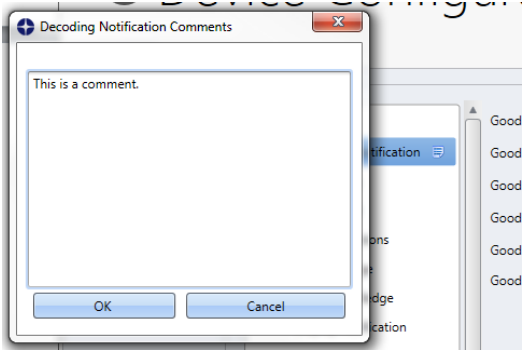
Edit a Configuration File Off-line

You can edit configuration files even when the device they were drawn from are not connected to DXU. Follow the steps below:

1. Open your configuration file.
2. Edit any settings you wish.
3. Either save the result to a new configuration file, or just save to the same configuration file.

Add Comments to Configuration Settings

Comments can be added to any tab, node, or parameter in the **Device Configuration** window. Comments are indicated with a small text balloon icon.



To add a comment:

1. Open a configuration file or load the configuration from a connected device.
2. Click **Configure This Device**.
3. Right-click any tab, node, or parameter, then select **Add comment** in the context-sensitive menu.
4. Type your comment.
5. Click **OK** save. A small text balloon will appear next to the item you commented on.

To edit a comment:

1. Right-click any item with a small comment icon.
2. Select **Edit comment** in the context-sensitive menu.
3. Edit your comment.
4. Click **OK** to save.

Show Comments

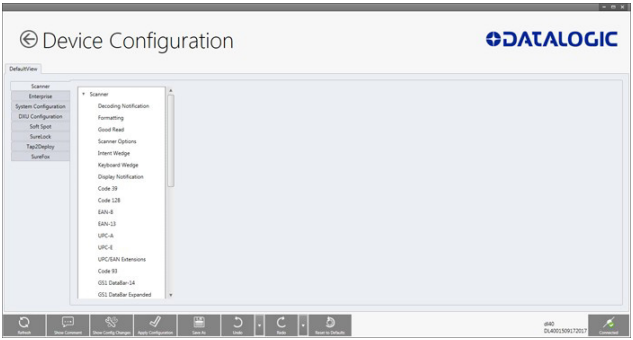
You can show all comments in a configuration file in one handy table by doing this:

1. Open a configuration file or load the configuration from a connected device.
2. Click **Configure This Device**.
3. If there are no comments, add them.
4. Click **Show Comments** in the button bar.

You can select and edit comments in this table by double-clicking the **Comment** field. Click the exit button (**X**) to close the dialog box.

Configure a Device On-line

Once you have added the device to **Desktop Configuration Utility**, you can click ist name under the **Available devices** list and use the **Configure This Device** option to start configuring the device. There is also an option to add comments on all the listed settings.



To configure a device that is directly connected via USB:

1. Launch **DXU**.
2. Connect your device to your PC via a USB cable.
3. Click the button for your connected device in the **Available Device** list.
4. Click **Configure This Device**.
5. Configure any settings you wish.
6. Save changes to a configuration file or apply the configuration changes to your device.

To configure a device that is connected over the network (either Ethernet or Wi-Fi):

1. Launch **DXU**.
2. Connect your device to DXU manually, using Scan2Pair labels or automatic discovery. (See instructions for these methods in this section.)
3. Click the button for your connected device in the **Available Device** list.
4. Click **Configure This Device**.
5. Configure any settings you wish.
6. Save changes to a configuration file or apply the configuration changes to your device.

Configure a Device Off-line via Scan2Deploy

DXU's **Desktop Configuration Utility** window allows to generate a **Scan2Deploy** barcode set for device configuration. The device settings modified using the console can be saved, printed and scanned by a remote user of a device to configure it.

The **Device Configuration** tab has the following additional options:

1. **Barcode Type**: selects the barcode symbology used to print the Scan2Deploy labels. Different symbologies have advantages and disadvantages, so DXU gives you a choice.

2. **Include Unmodified Changes:** when you configure a device using the console, you don't always wish to configure all the settings, so by default the generated codes for configuration do not include unmodified settings. However, once selected, the **Include Unmodified Changes** option allows you to also include unmodified changes in the barcode set, letting you fully configure a remote device even when it does not have network access to your DXU console computer.

3. **Include Binary Data**: DXU configuration files can contain some data in binary formats, like wallpaper images. The **Include Binary Data** option allows you to include all binary data in the barcode set. Note that excluding binary data can significantly reduce the size of your configuration file, and also the number of barcode labels in a set used to convey that configuration when printed as a **Scan2Deploy** label set.

To create a **Scan2Deploy** label set:

1. Open a configuration file or load the configuration from a connected device.
2. Click **Configure This Device**.
3. Configure any settings you wish.
4. (Optional) **Save** your configuration.
5. Click the **Back** button to return to the **Desktop Configuration Utility** window.
6. Click the **Scan2Deploy**
7. Click the **Device Configuration** tab.
8. (Optional) Select the **Include Unmodified Changes** check box to include all configuration settings in your Scan2Deploy barcodes.
9. (Optional) Select the **Include Binary Data** check box to include binary data like the desktop wallpaper image in the configuration barcodes.

NOTE

This option will increase the number of barcode labels in the Scan2Deploy label set.

10. (Optional) Select the barcode symbology in the **Barcode Type** menu.
11. Click **Save** to save your barcode label set as a graphic image file.
12. Click **Print Preview**, then click the **Print** button in the button bar and complete using your printer's **Print** dialog box.

To apply the configuration by scanning the **Scan2Deploy** barcodes:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu**, and then select the **Scan2Pair** command.
4. Scan any label in your Scan2Deploy label set.

NOTE

Some configurations are small enough to fit on only one barcode label, and others may have many barcodes to scan.

5. Continue to scan all the barcodes on the list. Once the last label is scanned, the configuration will be put into effect, and an on-screen notification will confirm that your configuration is complete.
6. Tap **Home** to exit.

Configure DXU

You can change DXU's language and the TCP/IP ports used to communicate with DXU Agent on remote devices, enable automatic discovery of devices, enable logging, and reset DXU's settings back to their default values.

Configure DXU's Language

DXU can display its controls in several languages. US English is the default, but you can also select Italian, Chinese Simplified or Chinese Traditional.

To change DXU's language:

1. From the **DXU** main window, click **Settings**.

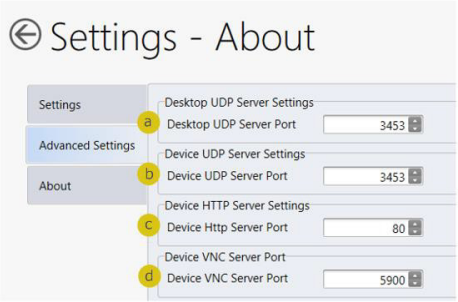
2. Select the language you prefer in the **Language** menu.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to **DXU** main window.

Configure DXU Communication Settings

You can configure the TCP/IP ports used by DXU to communicate with the DXU Agent on the Skorpio X4. Configure these settings only if you understand how these changes affect your network. Consult your network expert for more information.

To configure DXU's UDP and TCP ports:

1. From the **DXU** main window, click **Settings**.
2. Click the **Advanced Settings** tab.



3. Edit the port values to match the ports used by the DXU Agent on your devices:
   a. The **Desktop UDP Server Port** configures the UDP port for the DXU server running on the console PC. It is set to UDP port 3453 by default.
   b. The **Device UDP Server Port** configures the UDP port for the DXU Agent server running on the device. It is set to UDP port 3453 by default.
   c. The **Device HTTP Server Port** configures the TCP port for the DXU Agent server running on the device. It is set to TCP port 80 by default, like common web servers.
   d. The **Device VNC Server Port** configures the TCP port for VNC running on the device. It is set to TCP port 5900, like common VNC servers.

4. Click the **Back** button (a leftward pointing arrow in a circle to return to the **DXU** main window).

Enable Automatic Discovery of Devices

You can enable the automatic discovery of your device by the DXU. This is not enabled by default.

Do not enable automatic discovery if you have more than one user of DXU console in your subnet, or you risk having two DXU administrators changing the settings on any particular device in your subnet at once. DXU will warn you if it launches and detects another instance of DXU already running in your subnet.

To enable automatic discovery of devices:

1. From the **DXU** main window, click the **Settings** button.
2. Click the **Advanced Settings** tab.
3. Select the **Enable Automatic Discovery of Devices** check box.
4. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window.

Enable Logging on the DXU Console PC

DXU can log its activities, and this can be very helpful for technical support to help you diagnose those unexpected problems that always seem to pop up after software is released to actual users. Logging is not enabled by default. Once enabled, the DXU's default log file location is stored in your user directory at the following path: "C:\Users\<user>\AppData\Roaming\Datalogic DXU".

To enable logging:

1. From the **DXU** main window, click **Settings**.

2. Click the **Advanced Settings** tab.

3. Select the **Enable Logging** check box.
4. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window.

Reset Advanced Settings to Defaults

To reset the DXU's Advanced Settings to their default values follow the step below:

1. From the **DXU** main window, click the **Settings** button.
2. Click the **Advanced Settings** tab.
3. Click the **Reset Advanced Settings** button.
4. Click **Yes** to confirm.
5. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window.

Enable Logging on the Skorpio X4

DXU Agent can log its activities. When enabled, logs are written to the log file location. Logging can be helpful when diagnosing problems, but it slows down the DXU Agent and consumes slightly more power. This check box is not selected by default.

You can specify where the DXU Agent's log file is kept on your device. The default location on Android OS devices is /storage/sdcard0,

which is located in the device's on-board flash memory. This location is a persistent location, so log files stored here are safe if the device reboots. If a MicroSD card is used and it has greater capacity than on-board flash, you can specify to store the logs on the card. MicroSD cards are also persistent.

To enable DXU Agent logging on your device:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Clear the **Enable Service** check box.

NOTE

You must clear Enable Service before you can change any setting in DXU Agent.

6. Select the **Enable Log** check box.
7. Select the **Enable Service** check box.
8. Tap **Home** to exit.

To specify where the log files are stored on your device:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Clear the **Enable Service** check box.

NOTE

You must clear Enable Service before you can change any setting in DXU Agent.

6. Tap **Change Log File Location**.
7. Type a valid path on your device in the **Change Log File Location** field, and then tap **OK**.
8. (Optional, but desired if you wish to log to this new location) Select the **Enable Log** check box.
9. Select the **Enable Service** check box.
10. Tap **Home** to exit.

Set User Names, Passwords, and Prompt for Authentication on DXU Configuration Files

Configurations and configuration files can require authentication to open and apply. DXU implements an invisible sort of authentication by automatically applying a default user name and password to every DXU configuration and configuration file. You can display an authentication prompt whenever anyone attempts to connect to one of your devices with DXU, and change both the user name and the password to increase security of your devices.

Enable Authentication in DXU Agent

You can ensure that users are prompted to enter a user name and a password to open a configuration file in the DXU console or in the **DXU Agent's Settings** window on a device.

To enable authentication:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.

3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Clear the **Enable Service** check box.

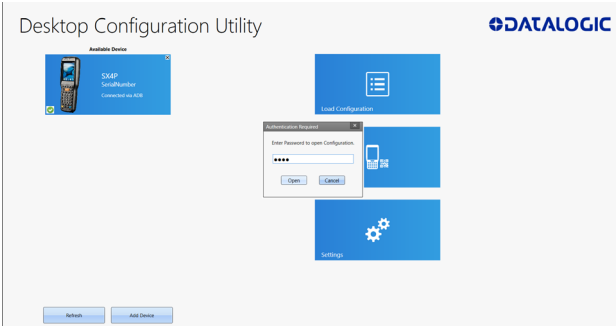
NOTE

You must clear Enable Service before you can change any setting in DXU Agent.

6. Select the **Is Authentication Required** check box.
7. Select the **Enable Service** check box.
8. Tap **Home** to exit.

To authenticate while opening DXU Agent's Settings window:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Type your password in the **Enter Password** field, and then tap **OK**.



Change the User Name in DXU Agent

Editing the user name adds an extra layer of complication to authentication. The default user name is 'admin'. You can change the user name to add another piece of information that a hacker must enter correctly to access the configuration in DXU.

To change the User Name:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Clear the **Enable Service** check box.

NOTE

You must clear Enable Service before you can change any setting in DXU Agent.

6. Tap the **User Name** button.

7. Delete the contents of the field, and then type a new user name.
8. Tap **OK**.
9. Select the **Is Authentication Required** check box.
10. Select the **Enable Service** check box.
11. Tap **Home** to exit.

Change the Password in the DXU Agent

You can edit the password to keep untrusted actors out of DXU Agent configuration settings. The default password is '0000'.

To change the Password:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Clear the **Enable Service** check box.

NOTE

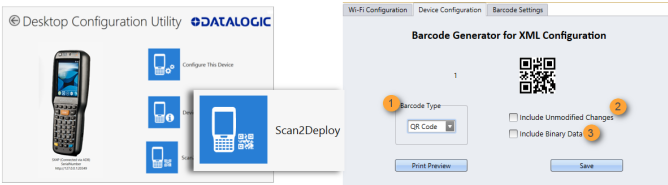
You must clear "Enable Service" before you can change any setting in DXU Agent.

6. Tap the **Password** button.
7. Delete the contents of the field, and then type a new password.
8. Tap **OK**.
9. Select the **Is Authentication Required** check box.
10. Select the **Enable Service** check box.
11. Tap **Home** to exit.

Create Scan2Deploy Labels to Fully Configure Remote Devices

The **Scan2Deploy** button in the **Datalogic Configuration Utility** window can automatically connect devices to Wi-Fi access points and to DXU. Also, the **Scan2Deploy** window has a further tab which allows you to include configuration data in the printed barcodes.

This version of Scan2Deploy can fully deploy a device configuration to devices which don't have network access to DXU on your PC. When the **Include Unmodified Changes** check box is selected, all the configuration items will be included in the barcode set. This option results in several barcodes being generated as true **Scan2Deploy** labels. After scanning the first label in this set, the **DXU Agent's Scan2Deploy** window on your device will display how many barcode labels must be scanned, and your progress in scanning them all. Once they are all scanned, the DXU Agent will apply the configuration changes automatically, as if you had connected to DXU to transfer the changes.



To create **Scan2Deploy** barcodes that can completely configure your device:

1. Open a configuration file or load the configuration from a connected device.
2. Click **Configure This Device**.
3. Configure any settings you wish.
4. (Optional) **Save** your configuration.

5. Click **Back** to return to the **Desktop Configuration Utility** window.
6. Click **Scan2Deploy**.
7. Click the **Device Configuration** tab.
8. (Optional) Select the **Include Unmodified Changes** check box to include all the configuration settings in your Scan2Deploy barcodes.

NOTE

This option will increase the number of barcode labels in the Scan2Deploy label set.

9. (Optional) Select the **Include Binary Data** check box to include binary data such as the desktop wallpaper image in the configuration barcodes.

NOTE

This option will increase the number of barcode labels in the Scan2Deploy label set.

10. (Optional) Select the barcode symbology in the **Barcode Type** menu.
11. Click **Save** to save your barcode label set as a graphic image file.
12. Click **Print Preview**, then click the **Print** button in the button bar and complete using your printer's **Print** dialog box.

To apply the configuration by scanning the **Scan2Deploy** barcodes:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu**, and then select the **Scan2Pair** command.

4. Scan any label in your Scan2Deploy label set.

NOTE

Some configurations are small enough to fit on only one barcode label, and others may have many barcodes to scan.

5. Continue to scan all barcodes on the list. Once the last label is scanned, the configuration will be put into effect, and an on-screen notification will confirm that your configuration is complete.
6. Tap **Home** to exit.

View Device Info for a Connected Device

You can view information about a device that is connected to DXU. This information includes the capabilities of the device's Wi-Fi radio, the type of barcode scanner it has, the OS version, the battery type and state of charge, the firmware version and the version of the Datalogic Enterprise SDK.

To view information about the device you are connected to:

1. Load the configuration from a connected device.
2. Click **Device Info**.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window.

View Device Info Recorded in a Configuration File

You can view information about the device from which a configuration file was extracted. This information includes the capabilities of the device's Wi-Fi radio, the type of barcode scanner it has, the OS version, the battery type and state of charge, the firmware version and the version of the Datalogic Enterprise SDK.

To view information about the device from which a configuration file was extracted:

1. Open a configuration file or load the configuration from a connected device.
2. Click **Device Info**.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window.

Remote Control

Remote Control allows to see what is displayed on the screen of a connected device. This window also includes buttons to remotely activate the device's external buttons, and to capture a screen shot of what is visible on its screen. Note that clicking a button on screen does not physically press a button, or even trigger it electrically, but sends an event message to the system as if you had pushed a physical key or tapped a physical button on the touch screen.

Unlock the Screen Using Remote Control

You can unlock the screen by dragging your mouse on the **Remote Control** screen.

To start **Remote Control** and unlock a device's screen:

1. Launch **DXU**.
2. Connect the device to DXU either directly using USB or through the network via Wi-Fi or Ethernet, or scan a Scan2Deploy label.
3. Click the device button in the **Available Device** list.
4. Click the **Remote Control**.
5. If the device is suspended, press the **Power** button at the bottom of the **Remote Control** window.
6. Click the **lock** icon and drag it rightward, releasing it over the **unlocked lock** icon at the right edge of the **Remote Control** window.

1. Home Button

At the bottom of the **Remote Control** window, the **Home** button activates the device's **Home** button, which switches the display to the **Home** screen.

2. Menu Button

At the bottom of the **Remote Control** window, the **Menu** button activates the device's menu. Not all the applications have a menu, so this feature depends on which application is active when you click the **Menu** button.

3. Power Button

At the bottom of the **Remote Control** window, the **Power** button toggles the device's power state as if you had pressed the device's **Power** button. If the device is awake, clicking the Power button will

turn off the screen, locking the screen if the device is configured to do that. If the device's screen is off, clicking the **Power** button will resume the device.

4. Back Button

At the bottom of the **Remote Control** window, the **Back** button takes the device to the previously viewed screen or application as if you had tapped the device's **Back** button.

5. Scan Button

At the bottom of the **Remote Control** window, the **Scan** button activates the device's barcode scanner as if you had pressed one of the **Scan** keys on the device. There are some limitations: the scanner will not scan if:

- there is no application running that can receive its data;
- the Camera application is showing its live preview or taking a photograph or recording a video;
- none of the device's scan buttons are configured to scan.

However, if your device is configured to scan barcodes and an application is receiving the data, then the **Scan** button will trigger a scan remotely.

6. Save a Screenshot of Remote Device

At the bottom of the **Remote Control** window, the **Save** button takes a screenshot of the remote computer and prompts to save it to your PC. The default path is your user folder.

Set a VNC Password

VNC is a standard protocol for remotely controlling PCs and other computers, and it allows the use of a password to prevent unwanted remote access to computers.

NOTE

The VNC password must match between the DXU console and the DXU Agent on the device.

Set a VNC Password in DXU Agent

You can set a password for VNC in DXU Agent. This field allows VNC communication to be authenticated, so prying eyes cannot remotely connect to and control your device. This field is blank by default.

To set or edit a VNC password in DXU Agent:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap **Menu** to display the menu.
4. Tap the **Settings** button.
5. Clear the **Enable Service** check box.

NOTE

You must clear "Enable Service" before you can change any setting in DXU Agent.

6. Tap the **Password** button in the **VNC Settings** section.
7. Type a password in the field. It can be numbers, letters, or some punctuation characters.
8. Tap **OK**.

9. Select the **Enable Service** check box.
10. Tap **Home** to exit.

To authenticate **Remote Control** when a password is set on the device:

1. Launch **DXU**.
2. Connect the device to DXU either directly using USB or through the network via Wi-Fi or Ethernet, or scan a Scan2Pair label.
3. Click the device button in the **Available Device** list.
4. Click the **Remote Control** button.
5. Type the device's **VNC password** in the field, and then click **OK**.

Set or Edit the VNC Authentication Password from DXU

You can change a device's VNC password from DXU. It is a configuration parameter in the **Device Configuration** window. Follow the steps below:

1. Open a configuration file or load the configuration from a connected device.
2. Click the **Configure This Device**.
3. Click the **DXU Configuration** tab.
4. Click the **General Settings** node in the middle pane.
5. Type a password in the **VNC Authentication Password** field, or edit the value in that field.

NOTE

The value in this field is encrypted for security. Once entered, it will be displayed as asterisks.

6. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window).

Update Firmware

You can update the Skorpio X4's firmware from DXU. DXU provides the following options:

- a **Silent Install** where no user interaction is required on the device;
- a **Force Update** where the firmware is reinstalled even if the device reports that it already has the same version installed;
- a factory data reset or an enterprise reset can be performed after updating the firmware;
- the update can simply reboot the device without performing an update.

NOTE

DXU firmware update is not the only way to update the firmware on the Skorpio X4. DXU's firmware update capability works only with connected devices. If you need a method that can update firmware on many devices remotely, especially if they are not connected to a network, then other methods may suit your needs better. Please consult your device's user reference guide for other firmware update methods.

NOTE

Customarily firmware update is referred to as "update" on devices that use Microsoft Windows operating systems, and it is referred to as "upgrade" on devices that use the Android operating system. These terms are used because the creators of these operating systems use these terms, but the terms essentially mean the same thing.

Silent Install

This option allows to perform an image update that does not require any user interaction on the device. If cleared, the user will be prompted to perform the update, but has the option to cancel the update. This check box is not selected by default.

Force Update

This option allows you perform a full upgrade of the firmware regardless of what is installed on the device. By default, the firmware upgrade utility will compare the version of the image file with what is already running on the device, and if they match it will skip updating. This is done to save time and prevent inconveniences for most users in the field. However, in rare circumstances a firmware image can become corrupted in the field, and this option allows a DXU administrator to perform a full firmware upgrade, disregarding the version reported by the device.

Factory Data Reset After Installing Firmware

A factory data reset is a full reset of the device intended to return it to factory defaults. This reset deletes all user data, settings and installed applications, and resets the device's real-time clock to its default date and time. Data on microSD cards is not affected.

Enterprise Reset After Installing Firmware

An enterprise reset is much like a factory data reset, except that it does not reset network connections (such as Wi-Fi settings), custom desktop wallpaper graphics and splash screen graphics. In every other way, it resets the device, including restoring flash memory to factory defaults, removing installed applications, deleting user data, and resetting the date and time to default levels.

Update Firmware on a Connected Device

You must first connect to a device to update its firmware with DXU. The connection can be either with USB, or over a network using Wi-Fi or Ethernet.

To perform a firmware update with DXU:

1. Launch **DXU**.
2. Connect the device to DXU either directly using USB or through the network via Wi-Fi or Ethernet, or scan a Scan2Pair label.
3. Click the device button in the **Available Device** list.
4. Click the **Firmware Utility** button.
5. Click the **Browse** button to open a standard file dialog box to browse for and select a suitable firmware image file.

NOTE

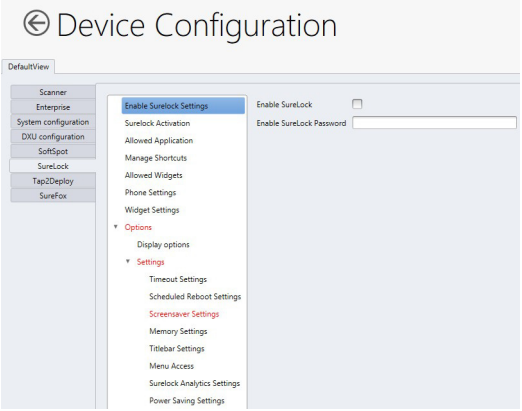
DXU will automatically filter your view of file types to those that are compatible with your device.

6. Navigate to your firmware image file, select it and click **Open**.
   - (Optional) Select the **Silent Install** check box if you wish to perform a firmware update that does not require user interaction on the device.
   - (Optional) Select the **Force Update** check box if you wish to force a complete reinstallation of this image on the device.
   - (Optional) Select an option from the **Reset Type** menu if you wish to perform a factory data reset or an enterprise reset after the image update is completed, or if you just want to have the device reboot without resetting at all.
7. Click **Update**.

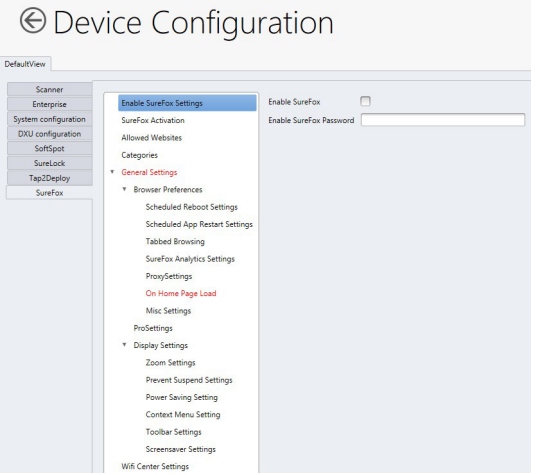
Configuring SureLock and SureFox

Device and browsing lockdown can occur using **SureLock** and **SureFox**. These lockdown settings can be set via the DXU desktop. There are two important prerequisites to configuring these settings when creating a DXU configuration file:

1. The EULA on the device must first be accepted. You can use DXU Desktop to remotely accept the SureFox and SureLock EULAs for all devices consuming a.dxu configuration file. Otherwise, you first need to launch **SureLock** or **SureFox** on each device and then accept the EULA.
2. The **Enable SureLock Password** and/or **Enable SureFox Password** fields must have the current password. The Default password is "0000".



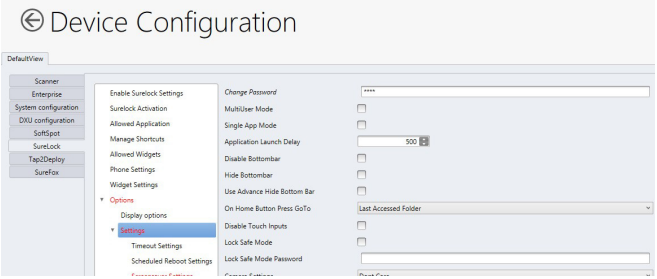
SureLock


Device Configuration
DefaultView
Scanner
Enterprise
System configuration
DXU configuration
SoftSpot
SureLock
Tap2Deploy
SureFox
Enable SureFox Settings
SureFox Activation
Allowed Websites
Categories
General Settings
Browser Preferences
Scheduled Reboot Settings
Scheduled App Restart Settings
Tabbed Browsing
SureFox Analytics Settings
ProxySettings
On Home Page Load
Misc Settings
ProSettings
Display Settings
Zoom Settings
Prevent Suspend Settings
Power Saving Setting
Context Menu Setting
Toolbar Settings
Screensaver Settings
Wifi Center Settings
Enable SureFox
Enable SureFox Password

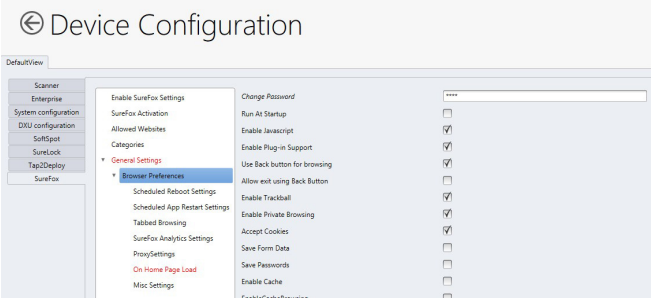
SureFox

Change the SureLock and/or SureFox Password

After completing the above steps, you can enter the new password in the **Change Password** field.



SureLock



SureFox

Command Line DXU Execution

DXU allows for command line execution, i.e. via a .bat batch file. This is a convenient method for configuring multiple devices without the need to launch the UI or the DXU desktop, or to configure Simplified Deploy. This configuration can happen via USB or through Wi-Fi (assuming the device has already been connected to the Wi-Fi network).

Optionally, you can perform Simplified Deploy with a manifest file, without using Scan2Deploy.

Usage

DXU command line options are:

- `DXU -put <filename.dxu>`
- Applies configuration file to any USB connected devices
- `DXU -put <filename.dxu> -ip <ipaddress>`

  Applies configuration file to device of specific IP address
- `DXU -man <filename.ini>`

  Applies Simplified Deploy to any USB connected devices
- `DXU -man <filename.ini> -ip <ipaddress>`

  Applies Simplified Deploy to device ofspecific IP address

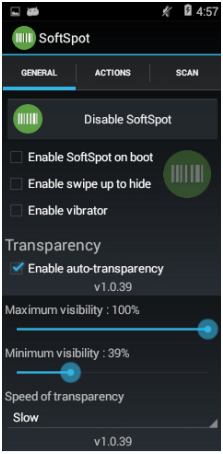
To output a log file, add the optional parameter:

`-log <logfilename>.`

SoftSpot™

Datalogic's SoftSpot technology is a user-definable 'floating soft trigger' meant to provide easy access to the barcode scanner application and other frequently used functionalities on mobile scanning devices.

Tap the SoftSpot icon on the favorites tray or on the All Apps screen to launch SoftSpot:



Tap the SoftSpot to scan barcodes.

Enable/Disable SoftSpot

Enables/disables the SoftSpot.

Enable SoftSpot on boot

Select it to enable SoftSpot on boot.

Enable swipe to hide

Allows to hide the SoftSpot from the screen by swiping it up in the Notification/Status bar.

Enable vibrator

This setting has no effect on Skorpio X4.

Enable auto-transparency

If selected, the SoftSpot turns transparent automatically when it is not used.

Maximum visibility

Sets the SoftSpot transparency level when it is used or when the auto-transparency feature is not enabled.

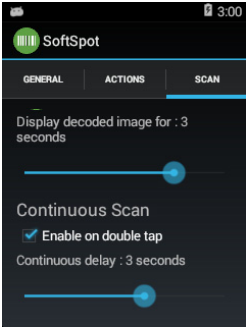
Minimum visibility

Sets the SoftSpot transparency level when it is not used and the auto-transparency feature is enabled.

Speed of transparency

Sets the lapse of time it takes for the SoftSpot to turn transparent.

To enable the Continuous Scan mode and scan barcodes consecutively, tap **SCAN** and select the **Enable on double tap** check box:



Then double-tap the SoftSpot. Tap one more time to stop laser emission.

You can also configure the SoftSpot from the DXU. For more details on DXU, Desktop Configuration Utility (DXU) on page 105.

NOTES

USB ADB Driver & USB CD-ROM

USB connection allows to read and write files on both the internal storage memory and the external storage memory, but doesn't allow to install applications.

Android Debug Bridge (ADB) is a command-line utility included with Google's Android SDK and you can use it to control your device over USB from a computer, copy files back and forth, install and uninstall apps and run shell commands.

Install either the Datalogic SDK Add-on or DXU Desktop to install the Windows drivers and then launch ADB to run a shell using the following tool command prompt: **Start/Datalogic Android/Device Tools Command Prompt**.

NOTE

USB debugging must be enabled on the device in order for ADB to function.

SDK Add-on

SDK add-on is a library which extends the Android SDK and development tools.

To install Datalogic SDK with Android Add-on, please consult https://datalogic.github.io/quick-start/android-studio.html for Android Studio or https://datalogic.github.io/quick-start/eclipse-adt.html for Eclipse ADT.

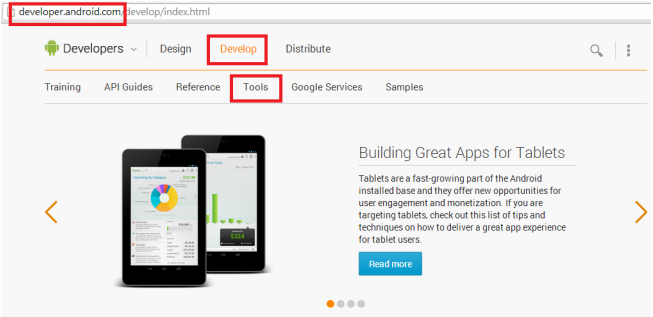
Xamarin developers should consult https://datalogic.github.io/xamarin.

More information can be found at https://datalogic.github.io/.

Install Android SDK

Visit the website https://developer.android.com for current instructions to install the Android SDK (the steps below may change).

1. Click on **Develop** > **Tools**:



2. Navigate to the **Downloads** section. Click on **VIEW ALL DOWNLOADS AND SIZES**.

3. You may need to drop down an extra menu for the actual download files.
4. Select the correct download for your operating system. For the Windows installer, follow the instructions on the screen. For other unzipped archives, you need to run the **Android** executable in the **tools** directory. This will bring up the Android SDK Manager and prompt you to download the tools you need.

developer.android.com/sdk/index.html

Develop > Tools > Android SDK

emulator

Download
Installing the SDK
Adding SDK Packages
Android Studio
Workflow
Support Library
Tools Help
Revisions
NDK
ADK

If you prefer to use an existing version of Eclipse or another IDE, you can instead download the stand-alone Android SDK Tools:

GET THE SDK FOR AN EXISTING IDE

SYSTEM REQUIREMENTS

VIEW ALL DOWNLOADS AND SIZES

ADT Bundle

Platform	Package	Size	MD5 Checksum
Windows 32-bit	adt-bundle-windows-x86-20140624.zip	377325518 bytes	5655cd8be53c4b27c5242d81943c5a25
Windows 64-bit	adt-bundle-windows-x86_64-20140624.zip	377477237 bytes	0f1fa29a0f229e36ba0fb87bb7ee68d4
Mac OS X 64-bit	adt-bundle-mac-x86_64-20140624.zip	327367424 bytes	7d16e832632598829 01f12055a8fe3f2
Linux 32-bit	adt-bundle-linux-x86-20140624.zip	378659422 bytes	692e6135ed459f1e8a10498363f19f67
Linux 64-bit	adt-bundle-linux-x86_64-20140624.zip	378966059 bytes	0f14b4aed1eb1feed778ad6ed76ba01c

SDK Tools Only

Platform	Package	Size	MD5 Checksum
Windows 32 & 64-bit	android-sdk_r23-windows.zip	138459944 bytes	9daba72b3a15a6154fe6ca1ada817553
	installer_r23-windows.exe (Recommended)	90065639 bytes	4564d1f1b30c001c78a22eec40444e5f
Mac OS X 32 & 64-bit	android-sdk_r23-macosx.zip	88015023 bytes	3869e5b9de8d69f90509568686fb7ce8
Linux 32 & 64-bit	android-sdk_r23-linux.tgz	137880976 bytes	fd768c56423e398b3e4aa8895c393bf5

Except as noted, this content is licensed under Creative Commons Attribution 2.5. For details and restrictions, see the Content License.

About Android | Legal | Support

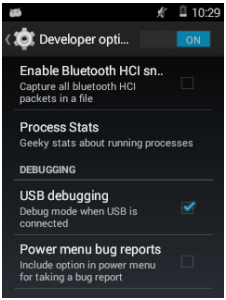
Install ADB Driver

1. Install Android SDK Manager (see 'Install Android SDK" on page -172 for further information).
2. Download and install the Google USB Driver (see https://developer.android.com for further information).

NOTE

Before installing the Google USB Driver, ensure you have installed the Datalogic plug-in.

3. In order to use ADB with your device connected over USB, you must enable USB debugging in the device system settings. To enable Android **Developer options**, go to **Settings** > **Device info** and tap on the **Build Number** section 7 times. After the 7th tap, the Developer options will be unlocked and available. Go back to **Settings** and tap **Developer options**. Select **USB debugging**:



SureLock

With **SureLock** you can secure and lock the Skorpio X4 to ensure its responsible usage, improve productivity and reduce maintenance cost.

It allows access to only required applications and prevents the users from making any intended or unintended changes in the device. Only administrators can access the password protected settings to either modify lockdown configurations or exit the lockdown.

You can use DXU Desktop to remotely accept the SureFox and SureLock EULAs for all devices consuming a.dxu configuration file (see 'Configuring SureLock and SureFox" on page -163).

A Datalogic Standard version of **SureLock** is preloaded on the Skorpio X4. You have the option to upgrade to the Advanced version by contacting 42Gears: http://www.42gears.com/contact.html.

Refer to the SureLock Documentation for Android on the 42Gears website for further details on **SureLock**.

SureFox

Businesses require use of browsers to run web applications on devices with Android and there may be situations when controlled web access for the users is required to ensure appropriate use of the devices.

SureFox creates locked browsing environment in your devices with Android making them apt for deployments as public web kiosks or as field devices for your mobile workforce. You can specify the websites that you wish to allow. **SureFox** will then block all other websites and allow the users to browse the allowed websites in locked down kiosk mode.

You can use DXU Desktop to remotely accept the SureFox and SureLock EULAs for all devices consuming a.dxu configuration file (see 'Configuring SureLock and SureFox" on page -163).

A Datalogic Standard version of **SureFox** is preloaded on the Skorpio X4. You have the option to upgrade to the Advanced version by contacting 42Gears: http://www.42gears.com/contact.html.

Refer to the SureFox Documentation for Android on the 42Gears website for further details on **SureFox**.

MobiControl

SOTI MobiControl is an enterprise mobility management solution that secures and manages the Skorpio X4 throughout its entire lifecycle, from deployment to retirement. It controls all aspects of business mobility — tracking physical assets, managing applications and content, as well as keeping the device and the data safe and secure.

For further details, refer to the SOTI website:

https://www.soti.net/products/mobicontrol.

NOTES

Data Capture

The Skorpio X4 has an integrated imager that collects data by scanning barcodes.

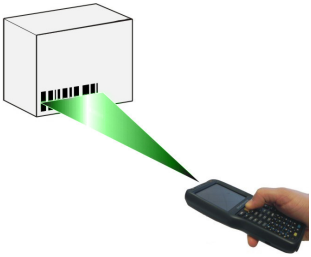
See Scanner Settings on page 68 for instructions on configuring the scanner settings.

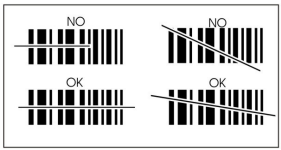
Imager 1D Data Capture

The imager uses digital camera technology to take a digital picture of a barcode, the image is stored in memory and software decoding algorithms are executed to extract the data from the image.

To scan a barcode symbol:

1. Point the scan window at the barcode from a distance within the reading range.
2. Press the scan key or the pistol trigger. The green lighted band emitted by the imager must completely cross the barcode as shown in the figure on the next page.





If the scan has been successful:

- If enabled, the good read LED glows steadily green for a configurable time.
- If enabled, the good read beep plays.
- If enabled, the Green Spot projects a green spot onto the barcode image.
- The barcode type and content data display on the screen.

The field of view changes its size as you move the reader closer or farther away from the barcode.

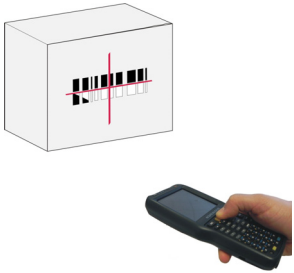
Scan symbols with smaller bars or elements (mil size) closer to the unit and those with larger bars or elements (mil size) farther from the unit. Hold the Skorpio X4 between two and nine inches (depending on symbol density) from the symbol.

Imager 2D Data Capture

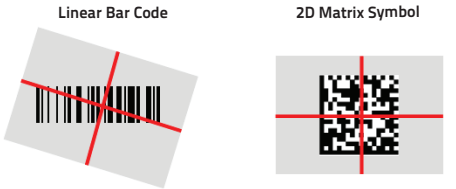
The imager uses digital camera technology to take a digital picture of a barcode, the image is stored in memory and software decoding algorithms are executed to extract the data from the image. The omni-directional scanning does not require that the operator orient the barcode to align with the scan pattern.

To scan a barcode symbol:

1. Point the scan window at the barcode from a distance within the reading range.
2. Press the scan key or the pistol trigger. The imager projects a laser aiming pattern similar to those used on cameras. The aiming pattern is used to position the barcode or object within the field of view.



3. Center the symbol in any orientation within the aiming pattern. Ensure the entire symbol is within the rectangular area formed by the brackets in the aiming pattern, then either wait for the timeout or release the scan key to capture the image. A red beam illuminates the symbol, which is captured and decoded.



If the scan has been successful:

- If enabled, the good read LED glows steadily green for a configurable time.
- If enabled, the good read beep plays.
- The barcode type and content data display on the screen.

The field of view changes its size as you move the reader closer or farther away from the barcode. The aiming pattern is smaller when the imager is closer to the barcode and larger when it is farther from the barcode.

Scan symbols with smaller bars or elements (mil size) closer to the unit and those with larger bars or elements (mil size) farther from the unit. Hold the Skorpio X4 between two and nine inches (depending on symbol density) from the symbol, centering the aiming pattern cross hairs on the symbol.

Connections

There is more than one way to connect the Skorpio X4 to a host PC running Windows. Each requires specific connections in order to function properly.

USB Connection

USB Direct Connection

You can use any standard USB charge/communication cable to directly connect the Skorpio X4 to a host computer and transfer data through the USB interface.

NOTE

Connection through the cable complies to USB 2.0 standard.

USB HandyLink™ Connection

You can use the Datalogic HandyLink cable 94A051970 to directly connect the Skorpio X4 to a host computer to transfer data through the USB interface.

NOTE

The HandyLink cable complies to USB 2.0 standard.

USB Dock Connection

The Single Dock can be connected to the host computer by means of the Micro-B USB cord 94A051968.

Once the host computer has been turned on, insert the Skorpio X4 mobile computer into the dock.

NOTE

Connection through the dock complies to USB 2.0 standard.

NOTE

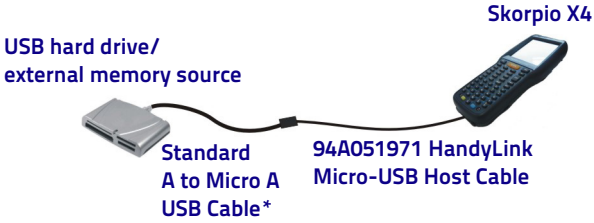
The actual data transfer speed can be appreciably lower than the maximum theoretical speed.

CAUTION

Don't insert the wall charger into the micro USB port when the Skorpio X4 is inserted into the dock.

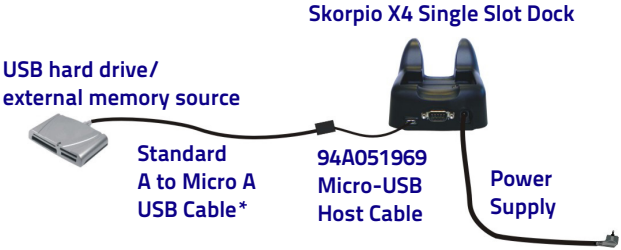
Connection to USB Peripherals

You can connect the Skorpio X4 to a standard 101-key USB keyboard or to a standard USB flash memory device. Connect the terminal to a standard USB cable or to the Datalogic 94A051971 HandyLink Micro-USB host cable (together with a standard USB cable* if needed). For all these devices maximum current draw must be less than 100mA.



* A standard USB cable is needed only if the USB hard driver or flash memory device does not include its own cable with a "A" plug on it.

Connect the Single Slot Dock to the peripheral by means of a Micro-A USB cord, or use a Micro-A to Std-A receptacle USB adapter such as Datalogic 94A051969 (together with a standard USB cable* if needed).



NOTE

Skorpio X4 works with most of the mentioned USB peripherals. Datalogic cannot guarantee the interoperability of Skorpio X4 with all devices on the market.

NOTE

Connection complies to USB 2.0 standard.

NOTE

The actual data transfer speed can be appreciably lower than the maximum theoretical speed.

* A standard USB cable is needed only if the USB hard driver or flash memory device does not include its own cable with a "A" plug on it.

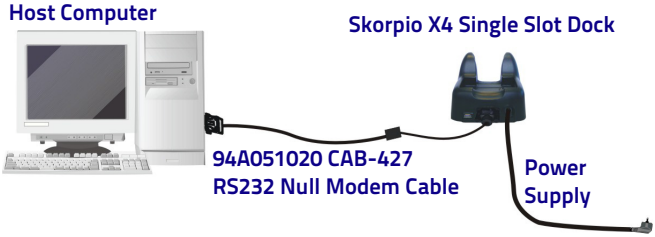
RS232 Connection

You can use the Datalogic 94A051972 cable to directly connect the Skorpio X4 to a host computer to transfer data through the RS232 interface.

RS232 Dock Connection

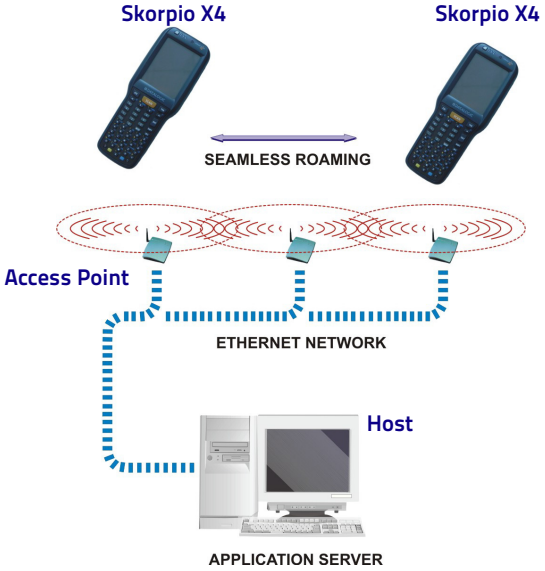
The Single Slot Dock can be connected to the Host by means of a standard null modem cable such as Datalogic 94A051020 CAB-427 for 9-pin connections.

Once the host computer has been turned on, insert the Skorpio X4 mobile computer into the cradle.



WLAN Connection

Skorpio X4 802.11 a/b/g/n radio models can communicate with the host using the on-board Wi-Fi radio and an Access Point connected to a network.



WPAN Connection

Skorpio X4 Bluetooth® models can communicate with a Bluetooth® device, such as a printer, within a range of 10 m, using the on-board Bluetooth® module.

NOTE

To extend battery life, the Bluetooth® module is off by default. To enable the Bluetooth®, open the Bluetooth Manager Window (see Bluetooth@ Manager Device Setup on page 83**).**

NOTE

Suspending the terminal powers off the Bluetooth® radio and drops the Bluetooth® connection. When the terminal resumes, it takes approximately 10 seconds for the Bluetooth® radio driver to re-initialize the radio.

NOTE

Area coverage and Bluetooth® radio performance may vary, due to environmental conditions or interference caused by other devices (microwave ovens, radio transmitters, etc.).

Wireless and Radio Frequencies Warnings

WARNING

Use only the supplied or an approved replacement antenna. Unauthorized antennas, modifications or attachments could damage the product and may violate laws and regulations.

Most modern electronic equipment is shielded from RF signals. However, certain electronic equipment may not be shielded against the RF signals generated by Skorpio X4.

Datalogic recommends persons with pacemakers or other medical devices to follow the same recommendations provided by Health Industry Manufacturers Associations for mobile phones.

Persons with pacemakers:

- **Should ALWAYS keep this device more than twenty five (25) cm from their pacemaker and/or any other medical device;**
- **Should not carry this device in a breast pocket;**
- **Should keep the device at the opposite side of the pacemaker and/or any other medical device;**
- **Should turn this device OFF or move it immediately AWAY if there is any reason to suspect that interference is taking place.**
- **Should ALWAYS read pacemaker or any other medical device guides or should consult the manufacturer of the medical device to determine if it is adequately shielded from external RF energy.**

WARNING

In case of doubt concerning the use of wireless devices with an implanted medical device, contact your doctor.

Turn this device OFF in health care facilities when any regulations posted in these areas instruct you to do so. Hospitals or health care facilities may use equipment that could be sensitive to external RF energy.

RF signals may affect improperly installed or inadequately shielded electronic systems in motor vehicles. Check with the manufacturer or its representative regarding your vehicle. You should also consult the manufacturer of any equipment that has been added to your vehicle.

An air bag inflates with great force. DO NOT place objects, including either installed or portable wireless equipment, in the area over the air bag or in the air bag deployment area. If a vehicle's wireless equipment is improperly installed and the air bag inflates, serious injury could result.

Turn off the device when in any area with a potentially explosive atmosphere. Observe restrictions and follow closely any laws, regulations, warnings and best practices on the use of radio equipment near fuel storage areas or fuel distribution areas, chemical plants or where any operation involves use of explosive materials.

WARNING

Do not store or carry flammable liquids, explosive gases or materials with the device or its parts or accessories.

Areas with a potentially explosive atmosphere are often, but not always, clearly marked or shown.

Sparks in such areas could cause an explosion or fire, resulting in injury or even death.

Technical Features

Technical Data

Physical Characteristics	
Dimensions	Handheld: 19.3 x 7.6 x 4.2 cm (6.1 x 3.5 cm at keyboard) / 7.6 x 3.0 x 1.3 in (2.4 x 1.4 in at keyboard). Pistol Grip: 19.3 x 7.6 x 15.6 cm / 7.6 x 3.0 x 6.2 in.
Weight	Handheld (with standard battery): 388 g / 13.7 oz. Handheld (with hi-cap battery): 422 g / 14.9 oz. Pistol Grip (with standard battery): 482 g / 17.0 oz. Pistol Grip (with hi-cap battery): 516 g / 18.2 oz.
Display	TFT / Transflective LCD with 240 x 320 pixel resolution. LED backlight and integrated touch screen, 3.2 inch diagonal.
Keyboard	50-key full alphanumeric, 38-key functional or 28-key numeric keyboard with backlight.

Environmental	
Drop Resistance	Withstands drops from 1.8 m / 6.0 ft onto concrete.
Particulate and Water Sealing Temperature	IP64 Operating: -10 to 50°C / 14 to 122°F Storage: -20 to 70°C / -4 to 158°F

Electrical	
Battery	Removable battery pack with rechargeable LiIon batteries; MicroUSB for fast battery charging. Standard: 3.7 V; 3,000 mAh (11.1 Watt-hours); standard on all handheld models. Extended: 3.7 V; 5,200 mAh (19.2 Watt-hours); standard on all Pistol Grip models.
Wireless Communications	
Local Area Network (WLAN)	TI Wi-Link 8, IEEE 802.11a/b/g/n. Frequency Range: Country dependent, typically 2.4 and 5 GHz; Cisco Compatible CCX v4 Security.
Personal Area Network (WPAN)	Bluetooth v4 with BLE (Android models). Bluetooth v2.1 + EDR (WEC7 models).
Interfaces	
Interfaces	Main connector with USB 2.0 High Speed Host (480 Mbps) and Client, RS-232 up to 115.2 Kbps. MicroUSB port for power and communications. Ethernet: via single dock (external module) or multi-slot dock.

System	
Operating System	Microsoft Windows Embedded Compact 7 (WEC7) or Android v4.4*.
Audio	Wideband Speech (HD Audio) supported on Android.
Expansion Slots	Micro Secure Digital slot (SDHC) up to 32 GB.
Microprocessor	TI OMAP4 @ 1 GHz.
Memory	RAM Memory: 1 GB. Flash Memory: 8 GB (partially used for firmware and reserved data).

* OS swap from WEC7 to Android 4.4 or from Android 4.4 to WEC7 is supported on all Skorpio X4 configurations. The OS swap must be performed at a Datalogic Service Center.

Software	
Applications	Pal Application Library pre-licensed (WEC7 only).
Configuration & Maintenance	Wavelink Avalanche® pre-licensed (WEC7 only), 42 Gears SureLock pre-licensed for device. lockdown (Android only); SOTI MobiControl, Datalogic xPlatform Utility (DXU) pre-licensed, Datalogic Desktop Utility (DDU) pre-licensed for device lockdown (WEC7 only).
Development	WEC7: Datalogic Windows SDK™, Wavelink® Studio™, MCL-Collection™. Android: Datalogic Android SDK, Xamarin SDK.
Browser	SureLock locked web browser pre-licensed for WEC7 and Android models.
Terminal Emulation	Wavelink® Terminal Emulation™ pre-licensed (for Pistol Grip/WEC7 models only). StayLinked SmartTE (for Android).

Decoding Capability	
1D / Linear Codes	Auto discriminates all standard 1D codes including GS1 DataBar™ linear codes.
2D Codes	Aztec Code, Data Matrix, MaxiCode, PDF417, MicroPDF417, Micro QR Code, QR Code.
Postal Codes	Australian Post, Japanese Post, KIX Code, Royal Mail, USPS Intelligent Mail, USPS PLANET, USPS POSTNET.
GS1 Composite Codes	UPC/EAN/JAN Composites, GS1 DataBar Composites and GS1-128 Composite (Composites supported on WEC7 only).
Reading Performance	
2D Imager (Standard Range)	Megapixel sensor for extended range. White LED Illumination. Optical Resolution: 1D codes: 3 mils; 2D codes: 6.6 mils. Depth of Field (typical): 4.5 to 74 cm / 1.7 to 29.1 in (13 mil/EAN), depending on bar code density and type.
1D Imager	2500 pixel sensor; Sharp green LED scan line. Optical Resolution: 2.5 mils (linear codes). Depth of Field: 4.0 to 74 cm / 1.5 to 29.1 in (13 mil/EAN), depending on bar code density and type.

Safety & Regulatory	
Agency Approvals	The product meets necessary safety and regulatory approvals for its intended use.
Enviromental Compliance	Complies to EU RoHS.
Laser Classifications	VLD - Class 2 IEC/EN60825-1; Compliant with 21 CFR 1040.10 except for deviations pursuant to laser notice No. 50 dated June 24, 2007.
LED Classification	Exempt Risk Group IEC/EN62471.
Warranty	
Warranty	1-Year Factory Warranty.

Decode Distances

Skorpio X4 Imager 1D Linear CCD

Resolution (mils)/ Barcode Type	Far Typical Working Ranges
3 mils Code 39	6.30 in 16 cm
5 mils Code 39	11.81 in 30 cm
10 mils Code 128	19.69 in 50 cm
13 mils EAN	25.20 in 64 cm
20 mils Code 39	47.24 in 120 cm

Skorpio X4 Imager 2D

Resolution (mils)/ Barcode Type	Far Typical Working Ranges
3 mils Code 39	7.48 in 19 cm
5 mils Code 39	12.99 in 33 cm
10 mils Datamatrix	9.84 in 25 cm
13 mils EAN13	25.59 in 65 cm
15 mils Datamatrix	13.78 in 35 cm
20 mils Code 39	39.37 in 100 cm

NOTES

Test Codes

High Density Codes - 0.25 mm (10 mils)
Code 39 17162
Interleaved 2/5 0123456784
Code 128 test

High Density Codes (continued) - 0.25 mm (10 mils)
80% EAN 13 8 012345 000012
80% EAN 8 6450 9723

Medium Density Codes - 0.38 mm (15 mils)
Code 39 17162
Interleaved 2/5 0123456784
Code 128 test

Medium Density Codes (continued) - 0.38 mm (15 mils)
100% EAN 13 8 012345 000012
100% EAN 8 6450 9723

Low Density Codes - 0.50 mm (20 mils)
Code 39 17162
Interleaved 2/5 0123456784
Code 128 test

Low Density Codes (continued) - 0.50 mm (20 mils)
120% EAN 13 8 012345 000012
120% EAN 8 6450 9723

2D Codes
Datamatrix ECC200   Example
Inverse Datamatrix ECC200   Example

NOTES

Maintenance

Cleaning the Device

Periodically clean the Skorpio X4 device using a soft cloth slightly dampened with only water or Isopropyl Alcohol (70%). Do not use any other cleaning agents (e.g. different alcohol, abrasive or corrosive products, solvents) or abrasive pads to clean the device.

Dock Contacts Cleaning Procedure

All exterior metal contacts/connectors exposed to spills, dirt or debris accumulation require periodic cleaning to ensure best performance during charging and data transmission.

Use a soft, lint-free dry cloth or lens tissue to clean the product (contacts and plastics). An antistatic cloth is preferable but you can also use a cotton cloth. Avoid wool, synthetic cloths or other materials that can cause electrostatic discharges.

If the contacts are very dirty, clean them with a soft cloth moistened with a diluted non-aggressive cleaning solution or a diluted isopropyl alcohol solution (20% maximum). A cotton swab may be used only on hard-to-reach contacts.

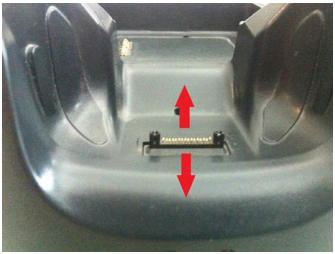
Clean the contacts when you see traces of dirt or when you experience solid connection issues between the terminal and its dock (device not charging or intermittent communications). It is however suggested to clean the contacts every 6 months (more often if the environment is dusty).

If the plastic areas are very dirty use only a cloth dampened with water.

Do not use abrasive or aggressive cleaning agents or abrasive pads to clean electric contacts, scan windows or plastics.

Cleaning the Dock Contacts

1. Remove the power cable before cleaning the contacts.
2. Use a soft dry cloth as suggested above. If the product is very dirty, moisten the cloth in a non-aggressive cleaning solution or diluted isopropyl alcohol solution (20% maximum).
3. Gently rub the cloth back and forth ONLY along the contacts, following the directions indicated by the red arrows. Use care not to leave any cloth residue.

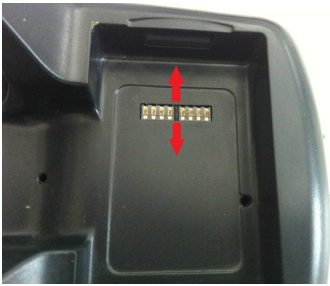


4. Use a dry cloth to remove any dirt near the contacts area and to clean the plastic parts. If the plastic parts of the equipment are very dirty, slightly dampen the cloth with only water.
5. Repeat steps 2, 3 and 4 using a clean dry cloth.

6. Allow the cleaning solution to fully evaporate before powering up the product.

Cleaning the Dock Auxiliary Battery Contacts

1. Remove the power cable and the Ethernet module before cleaning the contacts.
2. Use a soft dry cloth as suggested above. If the product is very dirty, moisten the cloth in a non-aggressive cleaning solution or diluted isopropyl alcohol solution (20% maximum).
3. Gently rub the cloth back and forth ONLY along the contacts, following the directions indicated by the red arrows. Use care not to leave any cloth residue.



4. Use a dry cloth to remove any dirt near the contacts area and to clean the plastic parts. If the plastic parts of the equipment are very dirty, slightly dampen the cloth with only water.
5. Repeat steps 2, 3 and 4 using a clean dry cloth.
6. Allow the cleaning solution to fully evaporate before powering up the product.

Ergonomic Recommendations

CAUTION

In order to avoid or minimize the potential risk of ergonomic injury follow the recommendations below. Consult with your local Health & Safety Manager to ensure that you are adhering to your company's safety programs to prevent employee injury.

- Reduce or eliminate repetitive motion
- Maintain a natural position
- Reduce or eliminate excessive force
- Keep objects that are used frequently within easy reach
- Perform tasks at correct heights
- Reduce or eliminate vibration
- Reduce or eliminate direct pressure
- Provide adjustable workstations
- Provide adequate clearance
- Provide a suitable working environment
- Improve work procedures.

Safety and Regulatory Information

NOTE

Read this manual carefully before performing any type of connection to the Skorpio X4.

The user is responsible for any damage caused by incorrect use of the equipment or by inobservance of the indication supplied in this manual.

General Safety Rules

- Before using the device and the battery pack, read carefully the chapter Battery on page 17.
- Use only the components and accessories supplied by the manufacturer for the specific Skorpio X4 being used.
- Do not attempt to disassemble the Skorpio X4, as it does not contain parts that can be repaired by the user. Any tampering will invalidate the warranty.
- When replacing the battery pack or at the end of the operative life of the Skorpio X4, disposal must be performed in compliance with the laws in force in your jurisdiction.
- Do not submerge the Skorpio X4 in liquid products.
- For further information or support, refer to this manual and to the Datalogic web site: www.datalogic.com.

Power Supply

The device is intended to be supplied by a self-contained rechargeable Lithium Ion battery pack (UL listed LPS/SELV power source) and/or by UL Listed/CSA Certified Power Unit LPS/SELV power source which supplies power directly to the unit via the micro USB connector of the cable.

The device could be also used with Certified Accessories (Dock/Cradle). The Dock/Cradle accessories are intended to be supplied by a UL Listed/CSA Certified Power Unit LPS/SELV which supplies power via the power connector of the cable.

Any changes or modifications to equipment, not expressly approved by Datalogic could void the user's authority to operate the equipment.

Laser Safety

The following information applies to Laser Aiming System, used on Skorpio X4 variants with 2D imager.

The laser light is visible to the human eye and is emitted from the window indicated in the figure below.

LASER LIGHT - DO NOT STARE INTO BEAM

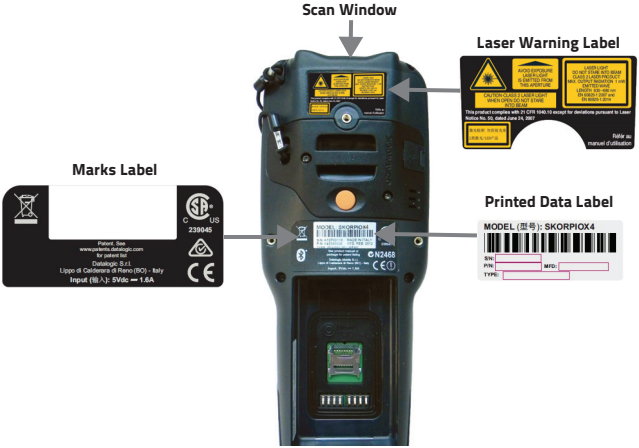
CLASS 2 LASER PRODUCT

MAX OUTPUT RADIATION 1 mW

COMPLIANT WITH EN 60825-1 (2007) and EN 60825-1 (2014)

NOTE

The artwork below may be only a draft. Please refer to the label attached to the product for information about certification marks.



ITALIANO	DEUTSCH	FRANÇAIS	ESPAÑOL
LA LUCE LASER È VISIBILE ALL'OCCHIO UMANO E VIENE EMESSA DALLA FINESTRA INDICATA NELLA FIGURA.	DIE LASER-STRAHLUNG IST FÜR DAS MENSCHLICHE AUGE SICHTBAR UND WIRD AM STRAHLAUS TRITTSFENSTER AUSGESENDET (SIEHE BILD)	LE RAYON LASER EST VISIBLE À L'OEIL NU ET IL EST ÉMIS PAR LA FENÊTRE DÉSIGNÉE SUR L'ILLUSTRATION DANS LA FIGURE	A LUZ LÁSER ES VISIBLE AL OJO HUMANO Y ES EMITIDA POR LA VENTANA INDICADA EN LA FIGURA.
LUCE LASER NON FISSARE IL FASCIO APPARECCHIO LASER DI CLASSE 2 MASSIMA POTENZA MEDIA DI USCITA: 1 mW LUNGHEZZA D'ONDA EMESSA: 630~680 nm CONFORME A EN 60825-1 (2007) E EN 60825-1 (2014)	LASERSTRAHLUNG NICHT IN DER STRAHL BLINKEN PRODUKT DER LASERKLASSE 2 MAXIMALE DURCHSCHNITTLICHE AUSGANGLEISTUNG: 1 mW WELLENLÄNGE: 630~680 nm ENTSPR. EN 60825-1 (2007) UND EN 60825-1 (2014)	RAYON LASER EVITER DE REGARDER LE RAYON APPAREIL LASER DE CLASSE 2 MAXIMUM PUISSANCE MOYENNE DE SORTIE: 1 mW LONGUER D'ONDE EMISE: 630~680 nm CONFORME A EN 60825-1 (2007) ET EN 60825-1 (2014)	RAYO LÁSER NO MIRAR FIJO EL RAYO APARATO LÁSER DE CLASE 2 MÁXIMA POTENCIA MEDIA DE SALIDA: 1 mW LONGITUD DE ONDA EMITIDA: 630~680 nm CONFORME A EN 60825-1 (2007) Y EN 60825-1 (2014)

ENGLISH

The following information is provided to comply with the rules imposed by international authorities and refers to the correct use of your device.

STANDARD LASER SAFETY REGULATIONS

This product conforms to the applicable requirements of both CDRH 21 CFR 1040 and EN 60825-1 at the date of manufacture.

For installation, use and maintenance, it is not necessary to open the device.

WARNING

Do not attempt to open or otherwise service any components in the optics cavity. Opening or servicing any part of the optics cavity by unauthorized personnel may violate laser safety regulations. The optics system is a factory only repair item.

WARNING

Use of controls or adjustments or performance of procedures other than those specified herein may result in exposure to hazardous visible laser light.

The product utilizes a low-power laser diode. Although staring directly at the laser beam momentarily causes no known biological damage, avoid staring at the beam as one would with any very strong light source, such as the sun. Avoid shining laser light into any person's eye, even through reflective surfaces such as mirrors, etc.

WARNING

Use of optical systems with the scanner will increase eye hazard. Optical instruments include binoculars, microscopes, eye glasses and magnifying glasses.

ITALIANO

Le seguenti informazioni vengono fornite dietro direttive delle autorità internazionali e si riferiscono all'uso corretto del terminale.

NORMATIVE STANDARD PER LA SICUREZZA LASER

Questo prodotto risulta conforme alle normative vigenti sulla sicurezza laser alla data di produzione: CDRH 21 CFR 1040 e EN 60825-1.

Non si rende mai necessario aprire l'apparecchio per motivi di installazione, utilizzo o manutenzione

ATTENZIONE

Non tentare di accedere allo scomparto contenete i componenti ottici o di farne la manutenzione.

L'apertura dello scomparto, o la manutenzione di qualsiasi parte ottica da parte di personale non autorizzato, potrebbe violare le norme della sicurezza. Il sistema ottico può essere riparato solamente alla fabbrica.

ATTENZIONE

L'utilizzo di procedure o regolazioni differenti da quelle descritte nella documentazione può provocare un'esposizione pericolosa a luce laser visibile.

Il prodotto utilizza un diodo laser a bassa potenza. Sebbene non siano noti danni riportati dall'occhio umano in seguito ad una esposizione di breve durata, evitare di fissare il raggio laser così come si eviterebbe qualsiasi altra sorgente di luminosità intensa, ad esempio il sole. Evitare inoltre di dirigere il raggio laser negli occhi di un osservatore, anche attraverso superfici riflettenti come gli specchi.

ATTENZIONE

L'uso di strumenti ottici assieme allo scanner può aumentare il pericolo di danno agli occhi. Tali strumenti ottici includono cannocchiali, microscopi, occhiali e lenti di ingrandimento.

DEUTSCH

Die folgenden Informationen stimmen mit den Sicherheitshinweisen überein, die von internationalen Behörden auferlegt wurden, und sie beziehen sich auf den korrekten Gebrauch vom Terminal.

NORM FÜR DIE LASERSICHERHEIT

Dies Produkt entspricht am Tag der Herstellung den gültigen EN 60825-1 und CDRH 21 CFR 1040 Normen für die Lasersicherheit.

Es ist nicht notwendig, das Gerät wegen Betrieb oder Installations-, und Wartungs-Arbeiten zu öffnen.

ACHTUNG

Unter keinen Umständen darf versucht werden, die Komponenten im Optikhohlraum zu öffnen oder auf irgendwelche andere Weise zu warten. Das Öffnen bzw. Warten der Komponenten im Optikhohlraum durch unbefugtes Personal verstößt gegen die Laser-Sicherheitsbestimmungen. Das Optiksystem darf nur werkseitig repariert werden.

ACHTUNG

Jegliche Änderungen am Gerät sowie Vorgehensweisen, die nicht in dieser Betriebsanleitung beschreiben werden, können ein gefährliches Laserlicht verursachen.

Der Produkt benutzt eine Laserdiode. Obwohl zur Zeit keine Augenschäden von kurzen Einstrahlungen bekannt sind, sollten Sie es vermeiden für längere Zeit in den Laserstrahl zu schauen, genauso wenig wie in starke Lichtquellen (z.B. die Sonne). Vermeiden Sie es, den Laserstrahl weder gegen die Augen eines Beobachters, noch gegen reflektierende Oberflächen zu richten.

ACHTUNG

Die Verwendung von Optiksystemen mit diesem Scanner erhöht die Gefahr einer Augenbeschädigung. Zu optischen Instrumenten gehören unter anderem Ferngläser, Mikroskope, Brillen und Vergrößerungsgläser.

FRANÇAIS

Les informations suivantes sont fournies selon les règles fixées par les autorités internationales et se réfèrent à une correcte utilisation du terminal.

NORMES DE SECURITE LASER

Ce produit est conforme aux normes de sécurité laser en vigueur à sa date de fabrication: CDRH 21 CFR 1040 s et EN 60825-1.

Il n'est pas nécessaire d'ouvrir l'appareil pour l'installation, l'utilisation ou l'entretien.

ATTENTION

Ne pas essayer d'ouvrir ou de réparer les composants de la cavité optique. L'ouverture de la cavité optique ou la réparation de ses composants par une personne non qualifiée peut entraîner le nonrespect des règles de sécurité relatives au laser. Le système optique ne peut être réparé qu'en usine.

ATTENTION

L'utilisation de procédures ou réglages différents de ceux donnés ici peut entraîner une dangereuse exposition à lumière laser visible.

Le produit utilise une diode laser. Aucun dommage aux yeux humains n'a été constaté à la suite d'une exposition au rayon laser. Eviter de regarder fixement le rayon, comme toute autre source lumineuse intense telle que le soleil. Eviter aussi de diriger le rayon vers les yeux d'un observateur, même à travers des surfaces réfléchissantes (miroirs, par exemple).

ATTENTION

L'utilisation d'instruments optiques avec le scanneur augmente le danger pour les yeux. Les instruments optiques comprennent les jumelles, les microscopes, les lunettes et les verres grossissants.

ESPAÑOL

Las informaciones siguientes son presentadas en conformidad con las disposiciones de las autoridades internacionales y se refieren al uso correcto del terminal.

NORMATIVAS ESTÁNDAR PARA LA SEGURIDAD LÁSER

Este aparato resulta conforme a las normativas vigentes de seguridad láser a la fecha de producción: CDRH 21 CFR 1040 y EN 60825-1.

No es necesario abrir el aparato para la instalación, la utilización o la manutención.

ATENCIÓN

No intente abrir o de ninguna manera dar servicio a ninguno de los componentes del receptáculo óptico. Abrir o dar servicio a las piezas del receptáculo óptico por parte del personal no autorizado podría ser una violación a los reglamentos de seguridad. El sistema óptico se puede reparar en la fábrica solamente.

ATENCIÓN

La utilización de procedimientos o regulaciones diferentes de aquellas describidas en la documentación puede causar una exposición peligrosa a la luz láser visible.

El aparato utiliza un diodo láser a baja potencia. No son notorios daños a los ojos humanos a consecuencia de una exposición de corta duración. Eviten de mirar fijo el rayo láser así como evitarían cualquiera otra fuente de luminosidad intensa, por ejemplo el sol. Además, eviten de dirigir el rayo láser hacia los ojos de un observador, también a través de superficies reflectantes como los espejos.

ATENCIÓN

El uso de sistemas ópticos con el escáner aumentará el riesgo de daños oculares. Los instrumentos ópticos incluyen binoculares, microscopios, lentes y lupas.

LED Class

LED illuminators integrated in the 1D and 2D imager are classified as "EXEMPT RISK GROUP" according to IEC62471.

Marking and European Economic Area (EEA) CE

In radio systems configured with mobile computers and access points, the frequencies to be used must be allowed by the spectrum authorities of the specific country in which the installation takes place. Be absolutely sure that the system frequencies are correctly set to be compliant with the spectrum requirements of the country.

The Radio modules used in this product automatically adapt to the frequencies set by the system and do not require any parameter settings.

Simplified EU Declaration of Conformity

Hereby, Datalogic S.r.l. declares that the radio equipment type Skorpio X4 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.datalogic.com.

Statement of Compliance

cs Česky [Czech]	Datalogic S.r.l. tímto prohlašuje, že tento Skorpio X4 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU - 2011/65/EU.
da Dansk [Danish]	Undertegnede Datalogic S.r.l. erklærer herved, at følgende udstyr Skorpio X4 overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU - 2011/65/EU.
de Deutsch [German]	Hiermit erklärt Datalogic S.r.l., dass sich das Gerät Skorpio X4 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU - 2011/65/EU befindet.
et Eesti [Estonian]	Käesolevaga kinnitab Datalogic S.r.l. seadme Skorpio X4 vastavust direktiivi 2014/53/EU - 2011/65/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
es Español [Spanish]	Por medio de la presente Datalogic S.r.l. declara que el Skorpio X4 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU - 2011/65/EU.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Datalogic S.r.l. ΔΗΛΩΝΕΙ ΟΤΙ Skorpio X4 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU - 2011/65/EU.

fr Français [French]	Par la présente Datalogic S.r.l. déclare que l'appareil Skorpio X4 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU - 2011/65/EU.
it Italiano [Italian]	Con la presente Datalogic S.r.l. dichiara che questo Skorpio X4 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU - 2011/65/EU.
Latviski [Latvian]	Ar šo Datalogic S.r.l. deklarē, ka Skorpio X4 atbilst Direktīvas 2014/53/EU - 2011/65/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Siuo Datalogic S.r.l. deklaruoja, kad šis Skorpio X4 atitinka esminius reikalavimus ir kitas 2014/53/EU - 2011/65/EU Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart Datalogic S.r.l. dat het toestel Skorpio X4 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU - 2011/65/EU.
mt Malti [Maltese]	Hawnhekk, Datalogic S.r.l., jiddikjara li dan Skorpio X4 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU - 2011/65/EU.
hu Magyar [Hungarian]	Alulírott, Datalogic S.r.l. nyilatkozom, hogy a Skorpio X4 megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU - 2011/65/EU irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym Datalogic S.r.l. oświadcza, że Skorpio X4 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU - 2011/65/EU.
pt Português [Portuguese]	Datalogic S.r.l. declara que este Skorpio X4 está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU - 2011/65/EU.
sl Slovensko [Slovenian]	Datalogic S.r.l. izjavlja, da je ta Skorpio X4 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU - 2011/65/EU.

Slovensky [Slovak]	Datalogic S.r.l. týmto vyhlasuje, že Skorpio X4 splňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU - 2011/65/EU.
fi Suomi [Finnish]	Datalogic S.r.l. vakuuttaa täten että Skorpio X4 tyyppinen laite on direktiivin 2014/53/EU - 2011/65/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar Datalogic S.r.l. att denna Skorpio X4 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU - 2011/65/EU.

Information for the User

Restrictions of use in all EU Countries. This device is restricted to indoor use when operated in the 5.15 to 5.25 GHz frequency range.

FCC/IC Labeling

HandHeld variants	Pistol Grip variants
FCC ID: U4GSX4WB IC: 3862E-SX4WB HVIN: SX4 WB HH	FCC ID: U4GSX4WB IC: 3862E-SX4WB HVIN: SX4 WB GUN

FCC Compliance

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.

NOTICE:

This device is restricted to indoor use when operated in the 5.15 to 5.25 GHz frequency range.

Changes or modifications made to this equipment not expressly approved by Datalogic S.r.l. may void the FCC authorization to operate this equipment.

NOTE:

This equipment 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.

ISED Compliance

NOTICE:

This device complies with Industry Canada licence-exempt RSS standard(s).

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.

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.

CAUTION:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

AVERTISSEMENT:

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiofrequency Radiation Exposure Information

This device was tested for handheld and body-worn conditions, according to international Standards covering human exposure to electromagnetic fields from radio devices.

More information about the relevant Standards for SAR measurement methods and procedures may be found in the CE DoC included in the product user manual available at www.datalogic.com website and at the FCC public listing www.fcc.gov under the FCC IDs specified in the FCC/IC labeling section.

Europe

This device is compliant with SAR limits for general population/uncontrolled exposure specified in Council Recommendation 1999/519/EC Annex II.

US and Canada

For body worn operation, this device has been tested and meets the

FCC/ISED RF exposure guidelines for use with an accessory that contains no metal and the positions the handset a minimum of 0 cm from the body. Use of other enhancements may not ensure compliance with FCC/ISED RF exposure guidelines.

Cet équipement peut être installé et utilisé à une distance minimale de 0 cm entre le radiateur et votre corps.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter, expect those approved under the filing.

Radio Technologies and Frequency Bands

Skorpio X4 incorporates the following radio technologies and supports the corresponding Frequencies and Radio-Frequency transmitted power, as specified below:

Europe

Radio Technology	Frequency Bands	Radio-Frequency Transmitted Power
WLAN IEEE 802.11b/g/n ▪ SISO 20MHz channels bandwidth (HT-20) ▪ MIMO support 20MHz channels bandwidth (HT-20)	2.4GHz Frequency Bands: 2.412 – 2.472 MHz	19.45 dBm
WLAN IEEE 802.11a/n ▪ SISO 20MHz and 40Mhz channels band-width (HT-20 and HT-40)	5GHz Frequency Bands: 5.180 – 5.240 MHz 5.260 – 5.320 MHz 5.500 – 5.700 MHz	19.27 dBm
Bluetooth® V4.0 – EDR/LE	2402-2480Mhz	9.95 dBm

US and Canada

Radio Technology	Frequency Bands
WLAN IEEE 802.11b/g/n ▪ SISO 20MHz channels bandwidth (HT-20) ▪ MIMO support 20MHz channels bandwidth (HT-20)	2.4GHz Frequency Bands: 2.412 – 2.462 MHz
WLAN IEEE 802.11a/n ▪ SISO 20MHz and 40Mhz channels bandwidth (HT-20 and HT-40)	5GHz Frequency Bands: 5.180 – 5.240 MHz 5.260 – 5.320 MHz 5.500 – 5.700 MHz 5.735 – 5.825 MHz
Bluetooth® V4.0 – EDR/LE	2402-2480Mhz

Waste Electrical and Electronic Equipment (WEEE)

Information for the user

At the end of its useful life, the product marked with the crossed out wheeled wastebin must be disposed of separately from urban waste.

For more detailed information about disposal, contact the supplier that provided you with the product in question or consult the dedicated section at the website http://www.datalogic.com.

Informazione per gli utenti

L'apparecchiatura che riporta il simbolo del bidone barrato deve essere smaltita, alla fine della sua vita utile, separatamente dai rifiuti urbani.

Per maggiori dettagli sulle modalità di smaltimento, contattare il Fornitore dal quale è stata acquistata l'apparecchiatura o consultare la sezione dedicata sul sito http://www.datalogic.com.

Information aux utilisateurs

Au terme de sa vie utile, le produit qui porte le symbole d'un caisson à ordures barré ne doit pas être éliminé avec les déchets urbains.

Pour obtenir des informations complémentaires concernant l'élimination, veuillez contacter le fournisseur auprès duquel vous

avez acheté le produit ou consulter la section consacrée au site Web http://www.datalogic.com.

Información para el usuario

Al final de su vida útil, el producto marcado con un simbolo de contenedor de bassura móvil tachado no debe eliminarse junto a los desechos urbanos.

Para obtener una información más detallada sobre la eliminación, por favor, póngase en contacto con el proveedor donde lo compró o consultar la sección dedicada en el Web site http://www.datalogic.com.

Benutzerinformation bezüglich

Am Ende des Gerätelebenszyklus darf das Produkt nicht über den städtischen Hausmüll entsorgt werden. Eine entsprechende Mülltrennung ist erforderlich.

Weitere Informationen zu dieser Richtlinie erhalten sie von ihrem Lieferanten über den sie das Produkt erworben haben, oder besuchen sie unsere Hompage unter http://www.datalogic.com.

NOTES

Reference Documentation

For further information regarding Skorpio X4 refer to the SDK Help on-line.

Support Through the Website

Datalogic provides several services as well as technical support through its website.
Log on to www.datalogic.com and click on the **SUPPORT** link which gives you access to:
Downloads by selecting your product model from the dropdown list in the Search by Product field for specific Data Sheets, Manuals, Software & Utilities, and Drawings;
Repair Program for On-Line Return Material Authorizations (RMAs) plus Repair Center contact information;
Customer Service containing details about Maintenance Agreements;

Technical Support through email or phone.

Warranty Terms and Conditions

The warranty period is 1 year for the device and 90 days for consumables (e.g. battery, power supply, cable etc.) from date of purchase at our company.

NOTES

Glossary

Access Point

A device that provides transparent access between Ethernet wired networks and IEEE 802.11 interoperable radio-equipped mobile units. Hand-held mobile computers, PDAs or other devices equipped with radio cards, communicate with wired networks using Access Points (AP). The mobile unit (mobile computer) may roam among the APs in the same subnet while maintaining a continuous, seamless connection to the wired network.

Applet

Diminutive form of app (application), it refers to simple, single-function programs that often ship with a larger product. Programs such as Windows' Calculator, File Manager, Control Panel and Notepad are examples of applets.

ASCII

American Standard Code for Information Interchange. A 7 bit-plus-parity code representing 128 letters, numerals, punctuation marks and control characters. It is a standard data transmission code in the U.S.

Barcode

A pattern of variable-width bars and spaces which represents numeric or alphanumeric data in binary form. The general format of a barcode symbol consists of a leading margin, start character, data or message character, check character (if any), stop character, and

trailing margin. Within this framework, each recognizable symbology uses its own unique format.

Bit

Binary digit. One bit is the basic unit of binary information. Generally, eight consecutive bits compose one byte of data. The pattern of 0 and 1 values within the byte determines its meaning.

Bluetooth®

A standard radio technology using a proprietary protocol. The onboard Bluetooth® module in the device is compatible with the 2.1 protocol with Enhanced Data Rate (EDR).

Boot

The process a computer goes through when it starts. During boot, the computer can run self-diagnostic tests and configure hardware and software.

Byte

On an addressable boundary, eight adjacent binary digits (0 and 1) combined in a pattern to represent a specific character or numeric value. Bits are numbered from the right, 0 through 7, with bit 0 the low-order bit. One byte in memory can be used to store one ASCII character.

CDRH

Center for Devices and Radiological Health. A federal agency responsible for regulating laser product safety. This agency specifies various laser operation classes based on power output during operation.

Character

A pattern of bars and spaces which either directly represents data or indicates a control function, such as a number, letter, punctuation mark, or communications control contained in a message.

Decode

To recognize a barcode symbology (e.g., Codabar, Code 128, Code 3 of 9, UPC/EAN, etc.) and convert the content of the barcode scanned from a visual pattern into electronic data.

Density (Barcode Density)

The number of characters represented per unit of measurement (e.g., characters per inch).

Depth of Field (DOF)

The portion of a scene that appears acceptably sharp in the image. Although a lens can precisely focus at only one distance, the decrease in sharpness is gradual on each side of the focused distance, so that within the DOF, the unsharpness is imperceptible under normal viewing conditions.

Dock

A dock is used for charging the terminal battery and for communicating with a host computer, and provides a storage place for the terminal when not in use.

ESD

Electro-Static Discharge

Ethernet

The standard local area network (LAN) access method. A reference to "LAN", "LAN connection" or "network card" automatically implies Ethernet. Defined by the IEEE as the 802.3 standard, Ethernet is

used to connect computers in a company or home network as well as to connect a single computer to a cable modem or DSL modem for Internet access.

Firmware

A software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. Firmware is typically stored in the flash ROM of a hardware device. While ROM is "read-only memory," flash ROM can be erased and rewritten because it is actually a type of flash memory.

Flash Memory

Non-volatile memory for storing application and configuration files.

Host

A computer that serves other mobile computers in a network, providing services such as network control, database access, special programs, supervisory programs, or programming languages.

IEC

International Electrotechnical Commission. This international agency regulates laser safety by specifying various laser operation classes based on power output during operation.

IEEE 802.11

A set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee.

IP

Internet Protocol. The IP part of the TCP/IP communications protocol. IP implements the network layer (layer 3) of the protocol, which contains a network address and is used to route a message to a different network or subnetwork. IP accepts "packets" from the layer 4 transport protocol (TCP or UDP), adds its own header to it and delivers a "datagram" to the layer 2 data link protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

IP Address

(Internet Protocol address) The address of a computer attached to an IP network. Every client and server station must have a unique IP address. A 32-bit address used by a computer on a IP network. Client workstations have either a permanent address or one that is dynamically assigned to them each session. IP addresses are written as four sets of numbers separated by periods; for example, 204.171.64.2.

LAN

Local area network. A radio network that supports data communication within a local area, such as within a warehouse of building.

Laser

Light Amplification by Stimulated Emission of Radiation.The laser is an intense light source. Light from a laser is all the same frequency, unlike the output of an incandescent bulb. Laser light is typically coherent and has a high energy density.

Light Emitting Diode (LED)

A low power electronic light source commonly used as an indicator light. It uses less power than an incandescent light bulb but more than a Liquid Crystal Display (LCD).

Liquid Crystal Display (LCD)

A display that uses liquid crystal sealed between two glass plates. The crystals are excited by precise electrical charges, causing them to reflect light outside according to their bias. They use little electricity and react relatively quickly. They require external light to reflect their information to the user.

MIL

1 mil = 1 thousandth of an inch.

Null Modem Cable

RS-232 serial cable where the transmit and receive lines are crosslinked. In some cables there are also handshake lines crosslinked. In many situations a straight through serial cable is used, together with a null modem adapter. The adapter contains the necessary crosslinks between the signals.

One shot key

Pressing a one shot key actives the state. The state remains active until any other key is pressed. If you hold down a one shot state key and you press another key the state will remain active until you release the one-shot key.

Pairing

A Bluetooth® pairing occurs when two Bluetooth® devices agree to communicate with each other and establish a connection.

Parameter

A variable that can have different values assigned to it.

RAM

Random Access memory. Data in RAM can be accessed in random order, and quickly written and read.

Resolution

The narrowest element dimension which is distinguished by a particular reading device or printed with a particular device or method.

RF

Radio Frequency.

Scanner

An electronic device used to scan barcode symbols and produce a digitized pattern that corresponds to the bars and spaces of the symbol. Its three main components are:

- Light source (laser or photoelectric cell) - illuminates a barcode.
- Photodetector - registers the difference in reflected light (more light reflected from spaces).
- Signal conditioning circuit - transforms optical detector output into a digitized bar pattern.

SDK

Software Development Kit.

Subnet

A subset of nodes on a network that are serviced by the same router.

Symbol

A scannable unit that encodes data within the conventions of a certain symbology, usually including start/stop characters, quiet zones, data characters and check characters.

Symbology

The structural rules and conventions for representing data within a particular barcode type (e.g. UPC/EAN, Code 39, PDF417, etc.).

Toggle key

Pressing a toggle key activates the state. The state remains active until the toggle key is pressed again.

USB

Universal Serial Bus. Type of serial bus that allows peripheral devices (disks, modems, printers, digitizers, data gloves, etc.) to be easily connected to a computer. A "plug-and-play" interface, it allows a device to be added without an adapter card and without rebooting the computer (the latter is known as hot-plugging). The USB standard, developed by several major computer and telecommunications companies, supports data-transfer speeds up to 12 megabits per second, multiple data streams, and up to 127 peripherals.

Visible Laser Diode (VLD)

A solid state device which produces visible laser light.

WLAN

A Wireless Local Area Network links devices via a wireless distribution method (typically spread-spectrum or OFDM radio), and usually provides a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.

WPAN

A Wireless Personal Area Network is a personal area network - a network for interconnecting devices centered around an individual person's workspace - in which the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about 10 meters - in other words, a very short range.

www.datalogic.com

©2017 Datalogic S.p.A. and/or its affiliates. All rights reserved.
Datalogic and the Datalogic logo are registered trademarks of Datalogic S.p.A. in many countries, including the U.S. and the E.U.

Datalogic S.r.l.
Via S. Vitalino, 13 | Calderara di Reno
40012 BO | Italy | Tel. +39 051 3147011
Fax +39 051 3147205

822002300 (Rev A) December 2017