# DATALOGIC

## Falcon X4 with Windows Embedded Compact 7

# Rugged Mobile Computer with 1D/2D Imager



**User's Manual**

# Table of Contents

# NOTES

# Introduction

## Conventions

This manual uses the following conventions:

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

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

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

# Product Presentation

Datalogic is pleased to announce its new Falcon X4 Mobile Computer: this legendary Mobile Computer strikes a new hit along a long track of worldwide successes!

A plurality of markets, including verticals like Retail, Manufacturing, Transport & Logistics and Healthcare, will benefit of upgraded Falcon performance for their back office and warehousing applications, together with the well-known ergonomics and reliability of this high end Mobile Computer.

Falcon X4 represents the best choice for any kind of player in such markets requiring reliable data collection in mobility, from store floor to back office inventory, from warehouse management to distribution center, from 3PL to traceability in intralogistics:

Users will appreciate along the full shift the difference of ergonomic handheld and pistol grip form factors, together with a 3.5 inch crystal clear display, an exceptional tactile feeling of the different backlit keyboards, and a hot swappable one-piece 5,200 mAh battery.

With a choice of Windows Embedded and Android™ Operating Systems, and an easy upgradability to Android, the Falcon 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 Falcon X4 is available in different models depending on the options it is equipped with. All options are listed below:

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

All options are listed below:

### WI-FI 1D HAND HELD

- 945500002  Falcon X4 Hand held, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Numeric, Green Laser-like 1D Imager w Green Spot, Windows Embedded Compact 7, EU.
- 945500004  Falcon X4 Hand held, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 52-Key Alpha Numeric, Green Laser-like 1D Imager w Green Spot, Windows Embedded Compact 7, EU.
- 945500010  Falcon X4 Hand held, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Functional Numeric F1-F12, Green Laser-like 1D Imager w Green Spot, Windows Embedded Compact 7, EU.

### WI-FI 2D HAND HELD

- 945500006  Falcon X4 Hand held, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Numeric, White Illumination 2D Imager w Green Spot, Windows Embedded Compact 7, EU.
- 945500005  Falcon X4 Hand held, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 52-Key Alpha

Numeric, White Illumination 2D Imager w Green Spot, Windows Embedded Compact 7, EU.

- 945500011 Falcon X4 Hand held, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Functional Numeric F1-F12, White Illumination 2D Imager w Green Spot, Windows Embedded Compact 7, EU.

## WI-FI 1D PISTOL GRIP

- 945550005 Falcon X4 Pistol Grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Numeric, Green Laser-like 1D Imager w Green Spot, Windows Embedded Compact 7, EU.

- 945550004 Falcon X4 Pistol Grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 52-Key Alpha Numeric, Green Laser-like 1D Imager w Green Spot, Windows Embedded Compact 7, EU.

- 945550010 Falcon X4 Pistol Grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Functional Numeric F1-F12, Green Laser-like 1D Imager w Green Spot, Windows Embedded Compact 7.

## WI-FI 2D PISTOL GRIP

- 945550006 Falcon X4 Pistol Grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Numeric, White Illumination 2D Imager w Green Spot, Windows Embedded Compact 7, EU.

- 945550002 Falcon X4 Pistol Grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 52-Key Alpha Numeric, White Illumination 2D Imager w Green Spot, Windows Embedded Compact 7, EU.

- 945550011  Falcon X4 Pistol Grip, 802.11 a/b/g/n MIMO CCX v4, Bluetooth v2.1, 1GB RAM/8GB Flash, 29-Key Functional Numeric F1-F12, White Illumination 2D Imager w Green Spot, Windows Embedded Compact 7, EU.

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

http://www.datalogic.com.

For further information regarding WEC7 refer to the website:

http://www.microsoft.com/windowsembedded.

# Out of the Box

The Falcon X4 package contains:

- Falcon X4 mobile computer
- Rechargeable battery pack
- Blank keypad overlay
- 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



**LEDs**

**ON/OFF Power Key**

**QVGA Color Display**

**Front Scan Key**

**Keyboard**

**Microphone**

## Back View

**Product Label**

**Laser Safety Label**

**Loudspeaker**

**Reset Key Under Battery**

**MicroSD Card Slot (Under Battery)**

## Top View

## Bottom View



**Data Capture Window**
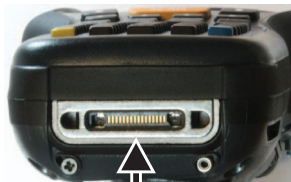


**HandyLink™ connector
(host/client)**

# Accessories

### Docks/Chargers

- 94A150057   Single Slot Desk Mount Dock with Spare Battery Charging Slot. High-Retention USB Type B (client only) and RS-232 ports. Includes Power Supply with Regional Plugs and USB Cable.

- 94A150056   Multi Ethernet Dock, recharges 4 terminals and 4 spare batteries. Power supply included in the box. Power cord ordered separately.

- 94A151131   Vehicle Dock, Falcon X3/X4. With RS-232 and USB I/O. Includes power cable and fuse. Requires input power source 9-30V DC.

- 94A151135   Multi Charge Only Dock, recharges 4 terminals and 4 spare batteries. Power supply included in the box. Power cord ordered separately.

- 94A151137   Multi Battery Charger recharges 4 spare batteries. Power supply included in the box. Power cord ordered separately.

### Power Supplies/Cords

- 95ACC1113   POWER LINE CORD, 3-PIN IEC C13, USA.
- 95ACC1213   POWER LINE CORD, 3-PIN IEC C13, UK.
- 94ACC1150   POWER LINE CORD, 3-PIN IEC C13, EU (5 PCS).
- 95A051041   POWER LINE CORD, 3-PIN IEC C13, EU.
- 95ACC1215   POWER LINE CORD, 3-PIN IEC C13, AUSTRALIA.
- 95ACC1212   POWER LINE CORD,3-PIN IEC C13, JAPAN.
- 95ACC1284   POWER LINE CORD, 3-PIN IEC C13, ARGENTINA.

- 94ACC1381   Power supply for single slot dock, regional plugs included.

- 94ACC1385   Power supply for Multi Battery Charger, 4-Slot Dock. Power line cord has to be ordered separately.

- 95ACC1049   DC/DC Converter for 24 V to 48 VDC Trucks (18-55 VDC/10 Amp) for PVD.

### Batteries

- 94ACC1386   Battery, 5200 mAh High Capacity, Falcon X3/X4.

### Cables

- 94A051020   Cable for dock-PC (RS-232) communication.

- 94A051970   Cable from device (Handylink) to USB. Device works as client. Connects to PC, 2 m straight cable.

- 94A051971   Cable from device (Handylink) to female USB. Device works as host. Connects to printers or most other peripherals. 15 cm straight cable.

- 94A051972   Cable from device (Handylink) to female DB9 RS-232. Null Modem Cable. Connects to PC. 2m straight cable.

- 94A051973   Cable from device (Handylink) to male DB9 RS-232. Straight through cable, Power on Pin 9 (5V @ 500mA). Connects to printers, scanners, or most other peripherals. 15 cm straight cable.

- 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.

- 94A051975   Car Adapter for PMD (to supply power to PMD from the cigarette lighter).  2 m 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). 15 cm straight cable.
- 95ACC0003 Clip for Micro USB and Power Supply cables. To be fastened to the RS-232 port of the Single Slot Dock.
- 94A050037 Handylink quick-disconnect audio cable for VR12 headsets.

## Holster/Cases

- 95ACC1161 Belt for Falcon Holster and Softcase.
- 94ACC1387 Holster, Falcon X3/X4 (Belt Sold Separately).
- 94ACC0104 RUBBER SHELL FALCONX3/X4.
- 94ACC0063 SOFTCASE HEAVY DUTY W/SHOULDER STRAP for Falcon X3/Falcon X4.
- 94ACC0047 Standard Softcase with Quick Release Belt Clip for Falcon X3/X4 (Belt Sold Separately).

## General Accessories

- 94ACC0121 Cover plate, Falcon X3/X4.
- 94ACC1390 Handle with Mounting Screws, Falcon X3/X4.
- 94ACC0073 Limited Power Source protection for Falcon X3/X4 Vehicle Dock. 12-24V, 1.5A. For vehicle power supplies not compliant IEC/UL 60950.
- 94ACC1372 Module, Modem Communication for Single Slot Dock.
- 94ACC0079 Module, Ethernet Communication for Single Slot Dock.
- 95ACC1033 Screen Protector Kit, 3.5", 5 Pack.
- 94ACC1240 Shoulder Strap (5 pcs).

- 94ACC0145 Stylus and Tether Pack for Falcon X3/X4, 5 Pack.

- 95ACC0002 VR12 Headsets. Requires Handylink audio cable 94A050037.

- 95ACC3420 RAM Mount, 1.5in Arm, with 2.75in and 2.5in bases. Recommended RAM mount for Falcon X3/X4 Powered Mobile Dock.

- 94ACC0049 Hand-strap, Skorpio X3/X4 and Falcon X3/X4.

- 94ACC0081 Lanyard to tether the Skorpio X3/X4 or Falcon X3/X4 to the wrist. Included with all pistol grip models of Skorpio X3/X4 and Falcon X3/X4).

**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.**

**CAUTION**

# NOTES

# Battery

## Install the Battery

Insert the battery with the contacts down, 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 single slot dock*, before using the Falcon X4 terminal.
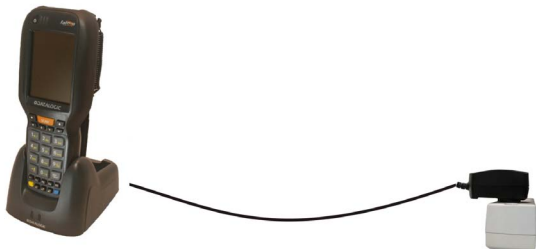


You can also charge an additional battery pack by inserting it into the rear slot of the dock.

**Do not use the Falcon X4 until batteries are charged for minimum 4 hours.**

**CAUTION**

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

**NOTE**

---

\* The power supply for the single slot dock is included in the single slot dock box (P/N 94A150057).

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

**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.**

**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.**

**The Falcon 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.**

# Replace the Battery

To replace the battery pack, follow the steps below:

1. Turn off the Falcon X4 (press the power key and wait for device power off).

2. Press the latch release button, pull the battery latch down and remove the battery pack.



3. Insert the new battery pack into the slot (Install the Battery on page 15).

**WARNING**

**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.**

**CAUTION**

**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.**

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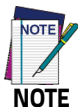
**Even if the storage temperature range is wider, it is recommended to store the terminal and the batteries at environmental temperature, in order to achieve the longest battery life.**

**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.**

**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.**

WARNING

# SD Card

## Install the MicroSD Card

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

1. Turn off the Falcon X4.
2. Remove the battery pack (see 'Replace the Battery" on page -18, steps 1 to 3).
3. Slide the cardholder to the right and then pull it up:

4. Insert the microSD card with the written part upward. Lock the card into place by pushing the cardholder down and then sliding it to the left:



5. Replace the battery pack (Install the Battery on page 15).

## Remove the MicroSD Card

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

**CAUTION**

**Follow proper ESD precautions to avoid damaging the microprocessors in the Falcon 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.**

# Getting Started

## Power On

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

As soon as the mobile computer is on, the Windows Embedded Compact 7 desktop will appear on the screen. Wait a few seconds before starting any activity so that the mobile computer completes its startup procedure.

The mobile computer goes into power-off (low power with display and keyboard backlight off), when it is not used for more than a programmable timeout, which can be defined in the **Power** applet of the Control Panel. In this mode it can be awakened by the **ON/OFF** key.

> **NOTE**
>
> **The mobile computer can also be awakened or suspended programmatically.**

# Desktop Window

As soon as the mobile computer is on, the Windows Embedded Compact 7 desktop appears on the screen. Wait a few seconds before starting any activity so that the mobile computer completes its startup procedure.
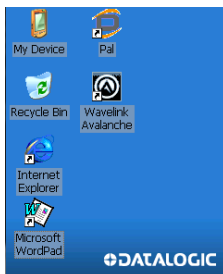


**Windows Embedded Compact 7 Desktop**

# Taskbar



| Icons | Descriptions |
|---|---|
|  | The Start button opens the Start Menu. |
|  | ActiveSync connection icon is displayed when connected to ActiveSync or Windows Mobile Device Center either by USB, RS232, or Bluetooth®. Double-tap it to open a status dialog box that will let you disconnect the ActiveSync session without physically disconnecting the device from the PC. It is the only way to disconnect a Bluetooth® ActiveSync connection. |
|  | Battery icons display the system battery status. |
|  | Bluetooth® Manager icon displays whether Bluetooth® is enabled, paired, or turned off. Double-tap this icon to open the Bluetooth® Manager control panel applet. |
|  | Network connectoid icon displays whether you are connected or not to Ethernet, Wi-Fi, or Bluetooth® Personal Area Network. |

# Using the Stylus Pen

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

| | |
|---|---|
| **Double Tap** | Double 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 select text and images. 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.**

# WEC7 Touch Screen Calibration

At the very first Falcon X4 startup, after any cold boot (if the user skipped stylus calibration earlier) or following a clean boot, a Welcome Wizard with Stylus Calibration comes up.

Also, you might need to recalibrate the touch screen (i.e. when you attempt to select an item with the stylus, another item is erroneously selected).

To recalibrate the touch screen, following the steps below:

1. Tap **Start** > **Settings** > **Control Panel**. Double tap the **Stylus** icon to open the **Stylus Properties** window:
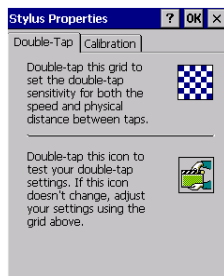
Tap **Calibration** to open the **Calibration** tab. Tap **Recalibrate**:
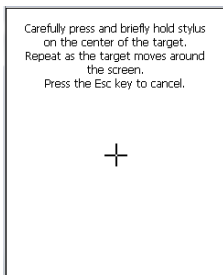
2. Carefully press and briefly hold the stylus on the center of the target. Repeat as the target moves around the screen.

3. By completing the calibration procedure you implicitly accept the new calibration settings.

4. The new calibration settings are persistently saved in the Registry.

# Keyboards

The Falcon X4 comes with three different keyboards: a 52-key alphanumeric keyboard, a 29-key numeric keyboard and a 29-key functional numeric keyboard.

## Alphanumeric Keyboard (52 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 DL Buttons on page 81). For pistol grip models only, the trigger performs the same function as the SCAN key. |
| F1◄ F2▲ F3▼ ►F4 | Direct access to F1-F4. If pressed after the Yellow toggle, these keys enable you to 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 Falcon 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 Start menu key opens the Start menu.

After a Blue modifier key press, the Lock key locks the keyboard.

# Numeric Keyboard (29 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 DL Buttons on page 81). For pistol grip models only, the trigger performs the same function as the SCAN key. |
| ◄ ▲ ▼ ► | Arrow keys let you move forwards, backwards, upwards or downwards within text fields, scroll through a Menu list or browse among folder files. |
| (yellow) | Yellow modifier (toggle key): when pressed before a standard key, it enables the character or function printed in yellow above the key. |
| (blue) | Blue modifier (one shot key): when pressed before a standard key, it enables the character or function printed in blue above the key. |
| (power) | The ON/OFF Power button powers the Falcon 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 Start menu key opens the Start menu. |
| | After a Blue modifier key press, the Lock key locks the keyboard. |

## Multitap Function

In the numeric keypad the number keys (key 0 excluded) and the ESC key share the following behavior scheme:
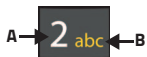
A. Function of the key when directly pressed.

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.

# Functional Keyboard (29 Keys; F1-F12)

## 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 DL Buttons on page 81). For pistol grip models only, the trigger performs the same function as the SCAN key. |
| F1◄ F2▲ F3▼ ►F4 | Direct access to F1-F4. If pressed after the Yellow toggle, these keys enable you to move forwards, backwards, upwards or downwards within text fields, scroll through a Menu list or browse among folder files. |
| (yellow key) | Yellow modifier (toggle key): when pressed before a standard key, it enables the character or function printed in yellow above the key. |
| (blue key) | Blue modifier (one shot key): when pressed before a standard key, it enables the character or function printed in blue above the key. |
| (power button) | The ON/OFF Power button powers the Falcon X4 ON or OFF. It is placed on the upper left side of the terminal. |

## Special Function Icons

| Icon | Function |
|------|----------|
| (windows icon) | After a Blue modifier key press, the Start menu key opens the Start menu. |
| (folder icon) | After a Yellow modifier key press, the File Manager key opens the file manager. |
| (lock icon) | After a Blue modifier key press, the Lock key locks the keyboard. |

## Multitap Function

In the functional keypad the number keys (key 0 excluded) and the Period 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.

# Resetting the Terminal

There are several reset methods for the Falcon X4.

A warm boot terminates an unresponsive application and clears the working RAM, but preserves the file system. The Registry is restored from persistent memory if available or returned to factory default.

A cold boot forces all applications to close, completely reinitializing the system. It clears the working RAM, but the file system is preserved. The Registry is restored from persistent memory.

A clean boot restores the Falcon X4 to a clean configuration: both the Registry and the file system returns to a clean status that conforms to factory default.

## Warm Boot

To perform a warm boot, press and hold the following keys simultaneously:

 +  + ESC

## Cold Boot

To perform a cold boot, do the following steps:

1. Turn off the Falcon 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.
5. Turn on the Falcon X4 by pressing the ON/OFF Power button.

# Clean Boot

To perform a clean boot, do the following steps:

1. Perform a Cold Boot (see Cold Boot).

2. Press and hold down the 'Esc' + '0' keys simultaneously, promptly after resetting:



A dialog box will appear asking for confirmation. Press the Enter Key.

|  | Warm Boot | Cold Boot | Clean Boot |
|---|---|---|---|
| **Registry** | Restored from flash | Restored from flash | Clean configuration (no user config) |
| **File System** | Preserved | Preserved | Clean Installation (no user files) |

# 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. |
| | Amber Blink | Light is blinking amber when the device raises a notification to the user. |
| Keyboard LED (center) | Off | Keyboard in primary. |
| | Yellow Constant | Yellow alternate key mode. |
| | Blue Constant | Blue alternate key mode. |
| | Pink | CapsLock enabled. |
| 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), or 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.

# NOTES

# Settings

## Control Panel

From the Start menu, tap **Settings** > **Control Panel.** Below is an expanded view of the Control Panel showing all of the applets.
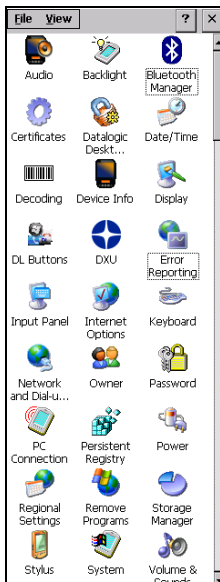
# Data Capture Configuration

Before you start reading barcodes, use the **Decoding Properties** window to view and configure all settings for the scanner.

From the control panel main window, double tap the **Decoding** icon:
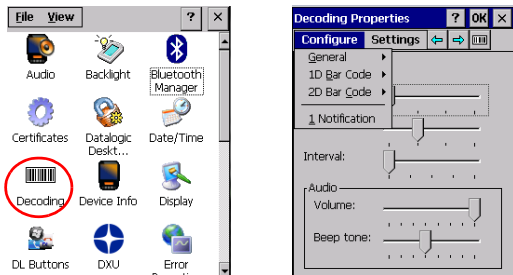


Tap **Configure** and select **General**, **1D barcode** or **2D barcode**, then use the menu or tap the left and right arrow keys to navigate the different pages of the **Decoding Properties** window. The menu options will change to reflect the items most recently selected.

# General Decoding Properties

Tap **Configure** > **General** and select the desired configuration from the options shown in the figure below:
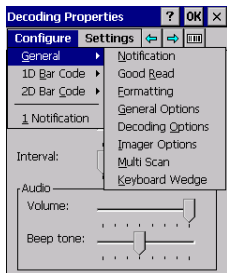
## Notification

Use it to set the number, the duration and the interval of notifications (LED, green spot, beep or vibration) the scanner emits on a good read.

You can also set the volume and tone of the beeps.
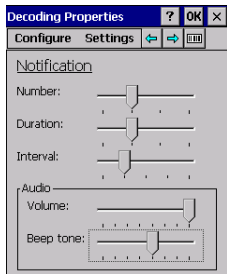
## Good Read

Use it to enable/disable good read notifications (LED, Green Spot, LED). Drag the **Timeout** slider to set the maximum amount of time the scanner attempt to decode after the scan key (or the trigger) is pressed:
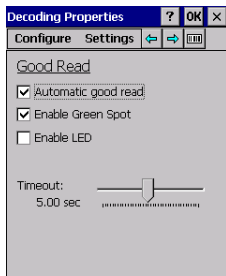
## Formatting

Allows to format the barcode text by enabling and configuring the use of prefix, suffix and data separator.

Scroll the **Add special** drop-down list to select a special character to be added in the current cursor position.
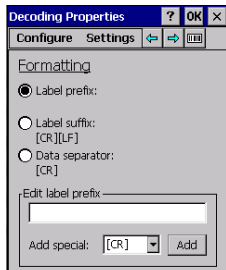
## General Options

Select the **Label programming enable** check box to enable the scanner to read specific barcodes.

Scroll the **Symbology ID** drop-down list to select and add a code identifier prefix or suffix to the barcode string.

AIM ID (Association for Automatic Identification and Mobility) is

an international barcode identifier. When **AIM IDs Before** is enabled, the AIM ID is inserted at the beginning of the decoded barcode.

DL ID is a Datalogic specific character identifier.

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

Group Separator replacement is a non printable data separator

character (ASCII code 1D hex). Scroll the **Group Separator replacement** drop-down list to select a string that will be used as GS data separator substituting the standard GS character.

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

Use the **1D Inverse** drop-down list to enable the scanner to read inverse 1D barcodes.
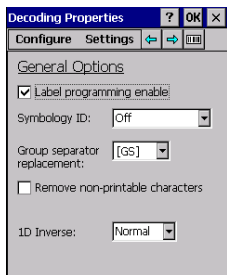
## Decoding Options

Use it to configure the User ID for symbologies, Redundancy and Aggressive Decoding (if supported by the decoding module). Select a symbology to view or change the available properties settings.
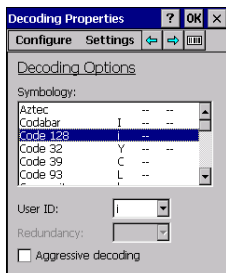
## Imager Options

It allows to customize the 2D imager behavior. It is only available on devices equipped with 2D decoding engines.
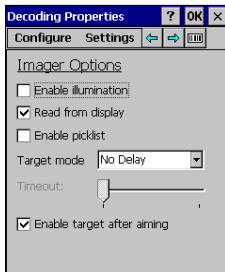


### Enable illumination

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

### Read from display

It improves capability to read barcodes from LCD screen (e.g. displayed on smartphone display).

### 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.

### 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. Use the drop-down list to select the desired targeting behavior:
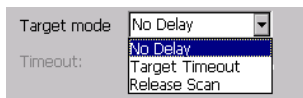


### No Delay

Target mode is disabled.

### Target Timeout

Scanning takes place after a programmable time upon pressing the scan button. Drag the **Timeout** slider to set the maximum amount of time the scanner attempt to decode after target timeout.

### Release Scan

Scanning takes place after the scan button is released. Drag the **Timeout** slider to set the scanning timeout after releasing the scan button.

**Enable target after aiming**

It enables aiming before scanning.

## Multi Scan

If enabled, the device goes on scanning until the number of **Labels for good read** is reached.

Select **Enable indicators for each label** to get an intermediate notification for each label decoded.
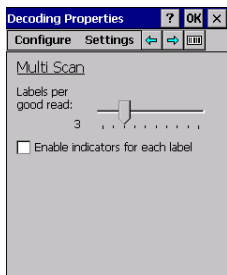
## Keyboard Wedge

Use it to enable or disable the keyboard wedge for barcode scanner:
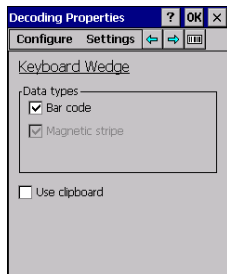
# Symbology Settings

Each barcode symbology can be customized with additional settings that may affect that specific barcode decoding.

Tap **Configure** and use the **1D barcode**/ **2D barcode** drop-down menus to configure symbology decoding options:
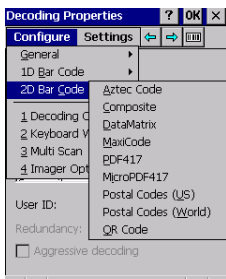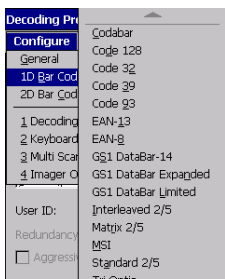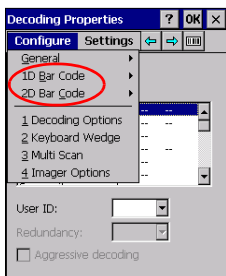
Refer to the sample symbology control panels for examples of the types of fields and options you can modify. The sample below shows the settings of a Code 128 barcode symbology:
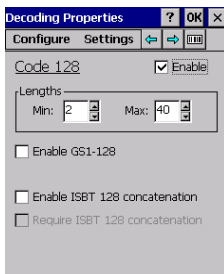


Tap the left and right arrow keys to navigate the different pages of the barcode symbology pages.

# Decoding Settings

Tap **Settings** to change symbologies settings or to restore previous configurations and/or other available default settings.
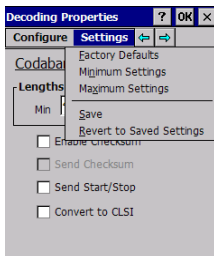


The settings are saved when you tap **Yes**. Any change you make is temporary and will be lost when the system restarts. To save these settings to a persistent storage, you need to save the **Registry** using the **Persistent Registry** applet in the **Control Panel**.

# Wi-FI

Wi-Fi is an application that provides an interface for configuring and operating an installed wireless network interface card (wireless adapter).

To open the Wi-Fi screen, you choose one of the following options:

- From the control panel main window, double tap **Wi-Fi**:
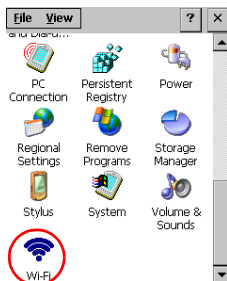


- Double tap the WiFi connectivity status icon in the taskbar:
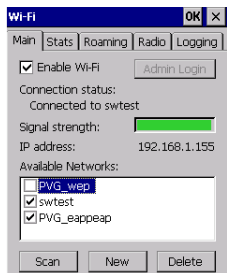
**Enable Wi-Fi**

Select to enable the radio.

**Admin Login**

The **Admin Login** button is displayed only if the Administrator Login feature is enabled. Tap this button to open the following dialog and login as Administrator:
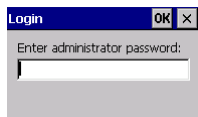
You can enter the password, which is protected with asterisks as it is entered. Tap **OK** to verify the password. If it is not correct, an error message will appear below the edit box and the dialog will allow you to change the password. Tap the **X** to cancel the login attempt.

**Connection status**

Displays the current radio connection status, using the Network Name assigned to a network profile (not the SSID).

**Signal strength**

Fills a bar which reflects the RSSI of the radio signal. The bar is full when near 100% (0 dBm) and empty when near 0% (-100 dBm). The color also changes to match the size of the bar: Red = Low, Yellow = Medium, Green = High.

**IP Address**

Displays the IPv4 address currently assigned to the device on the Wi-Fi network. When not connected, it displays "0.0.0.0".

The bottom of the **Main** tab shows a list of existing network profiles. The device will automatically connect to any of the checked

networks. More than one network can be checked at once. There is no priority implied in the order of the networks in the list; a network will be selected based on other factors (such as signal strength and security).

Up to 24 networks can be added to the list. If this limit is reached, then the **Scan** and **New** buttons will be disabled until a network is deleted. The buttons below the network list allow to add or remove networks from the list.

### Scan

Displays a list of available networks detected by the device. See Scan for Networks on page 58 for details.

### New

Allows to define a network without scanning for networks. This is useful when the network's definition is known, but it is currently out of range. See Create a New Network on page 60 for details.

### Delete

Deletes a network from the list. It is disabled until a network is selected from the list (by tapping on its name).

# Scan for Networks

From the Main tab, tap **Scan**. A screen appears showing all the detected networks.
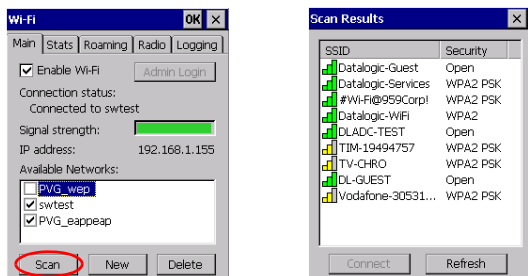
Only allowed networks will be displayed (WPA networks using TKIP will not be displayed unless enabled). Each entry displays the following information:

**Signal strength**: the icon on the far left indicates the relative signal strength of the network. The number of bars and color coding is the same as the RSSI on the Main tab: 1/Red = Low, 2/Yellow = Medium, 3/Green = High.

**SSID**: the SSID assigned to the access point on the network.

**Security**: the type of security detected on the network.

## Connect to/Disconnect from a Network

1. Select a network from the list. Depending on whether or not the adapter network is connected to that network, the **Connect** or **Disconnect** button will be enabled.

2. Tap **Connect** or **Disconnect**.

3. The **Configure Network** screen is displayed:

4. Enter a network name or leave the default name.

5. Tap **OK** to save the profile and connect the device to the network, or **Cancel** to return to the current view without saving the profile.

## Refresh

Tap **Refresh** to manually refresh the scan list. Each click on this button triggers a scan request to driver.

# Create a New Network

Tap **New** from the **Main** tab.

Enter information for the **SSID**, **Network name** and **Security**.
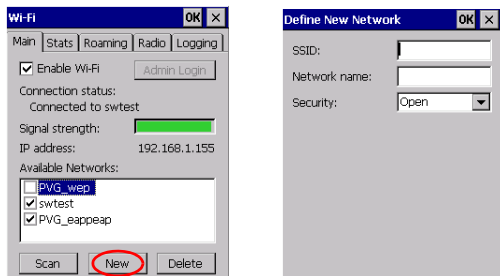
## Security: Open

No additional controls will be shown for a network with open security.

## Security: WEP

For a network with WEP security, the following additional controls are shown:

### WEP key

This is the security key string used to connect to the network. It must be 5 or 13 characters in length. Optionally, all characters may be entered using their hexadecimal values. In this case, the characters must be 0-9, a-f, A-F, and must be 10 or 26 characters in

length. When you type a value in this field, the text is replaced by asterisks for additional security.

### Confirm WEP key

It must match the previous field exactly. This provides a greater chance of entering the correct value for the security key.

### Key index

This is the WEP key index used by the network. It can be set to a value from 1 to 4.

## Security: WPA / WPA2

For a network with WPA or WPA2 security, the following additional controls are shown:
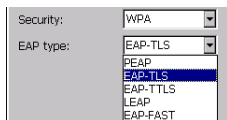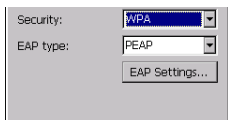


### EAP type
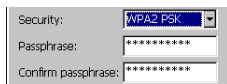
Specifies the EAP method to use when connecting to the network. The available options are listed in the diagram above.

### EAP Settings

Opens a dialog which allows to supply authentication and user credential information specific to the selected EAP method.

## Security Type: WPA (or WPA2) PSK

For a network using PSK security, the following additional controls are shown:

| | |
|---|---|
| Security: | WPA2 PSK |
| Passphrase: | ********* |
| Confirm passphrase: | ********* |
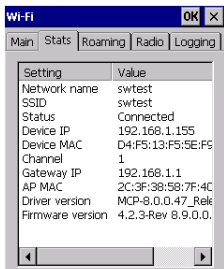
### Passphrase

This is the security passphrase string used to connect to the network. It must be 8 - 63 characters in length. When you type a value in this field, the text is replaced by asterisks for additional security.

### Confirm passphrase

It must match the previous field exactly. This provides a greater chance of entering the correct value for the security key.

# Stats Tab

This tab displays advanced radio information. These are regularly updated as long as the radio is connected to a network. When the radio is disabled, most of the values listed are zero or blank.



### Network name, SSID, Status

Display the names and connection status of the current network.

### Device IP, Device MAC

Display the IPv4 address and MAC address of the radio module in the device.

### Channel

Displays the radio channel currently used for communicating on the network.

### Gateway IP, AP MAC

Display the IPv4 address and MAC address of the access point the device is currently associated with.

### Driver version

Displays the version of the radio driver. It is blank when the radio is disabled.

**Firmware version**

Displays the version of the firmware in the radio module. It is blank when the radio is disabled.

# Roaming Tab

This tab contains advanced settings that impact the roaming behavior of the radio. Tap **Apply** to save the changes in the slider controls. Tap **Reset** to reset the controls to factory defaults.
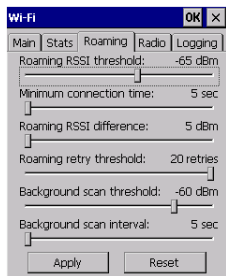


**Roaming RSSI threshold**

This is the RSSI threshold below which the radio starts roaming. Its default value is -65 dBm.

**Minimum connection time**

This is the minimum time the radio is connected to an access point before it starts roaming. Its default value is 5 seconds.

**Roaming RSSI difference**

This is the minimum difference in signal strength between one access point and another before roaming to the second access point. Its default value is 5 dBm.

### Roaming retry threshold

This is the maximum number of retries connecting to an access point before scanning for a new one. Its default value is 20 retries.

### Background scan threshold

This is the RSSI threshold below which the radio will start a background scan for another access point. Its default value is -60 dBm.

### Background scan interval

This is the time between background scans. Its default value is 5 seconds.

The roaming RSSI threshold cannot be greater than the background scan threshold. If you attempt to move the slider of one of these controls beyond this constraint, the slider will snap back to the value where these control are equal, and a message box will appear explaining why the change was made.

# Radio Tab

This tab contains advanced settings that affect general radio behavior. Tap **Apply** to save the changes in the slider controls. Tap **Reset** to reset the controls to factory defaults.
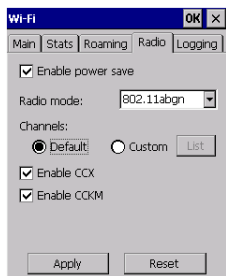


### Enable power save

If enabled, the radio operates with reduced power. Its default value is enabled.

### Radio mode

Specifies which frequencies the radio can use. The options are: 802.11na (5 GHz), 802.11ng (2.4 GHz), 802.11abgn (both). Its default value is 802.11abgn.

### Enable CCX

Enables CCX features. Its default value is enabled.

### Enable CCKM

Enables the CCKM feature. It is disabled when CCX is disabled. Its default value is enabled.

## Selecting Radio Channels

The **Channels** buttons select the channels that the radio is allowed to use.  Select **Default** to limit use to the factory default channels: 1-11, 36, 40, 44, 48, 149, 153, 157, 161, 165.  Channels 12 and 13 are also included if the device is configured (in production) for ETSI regulatory domain.

Select **Custom** to define a custom list of channels that the radio can use. Tap the **List** button to open the **Channel Selection** dialog:
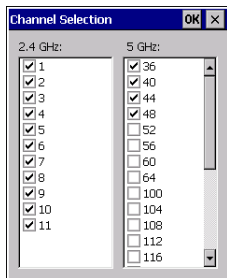


This dialog lists the available radio channels, grouped by frequency range. The custom list is initially set to the factory defaults. On a device configured for ETSI, channels 12 and 13 are also listed under 2.4 GHz. The channels currently enabled in the custom list are checked, and you can turn on/off any combination of channels. When finished, tap **OK** to return to the **Radio** tab, then tap **Apply** to send the custom channel list to the radio. Tap **X** to cancel any changes to the custom list.

# Logging Tab

This tab manages the logging of debug information for the radio device driver and module firmware. Logging is disabled after a reboot, and the debug configuration is not persisted across reboots. The log files are written to the FlashDisk with a file name drv_hh.mm.ss or fw_hh.mm.ss (the time logging is started is used to generate the filename). The files are not automatically deleted if logging is stopped and restarted.
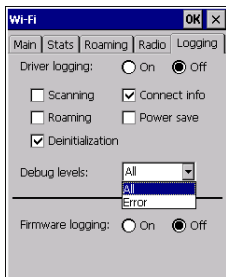


The top section manages logging of device driver debug. This logging can be turned on or off by using the top radio buttons. The check boxes specify the areas of activity which are logged and the **Debug levels** drop-down list box specifies the amount of detail included in the debug log. By default, only full details of **Connect info** and **Deinitialization** activity are logged. While logging is turned on, the controls that specify the type of logging are disabled.

The bottom radio buttons turn on/off logging of debug messages from the radio firmware.

# Audio Settings

There are two applets that control volume: **Audio** and **Volume & Sounds**.

## Audio

The **Audio Properties** window allows to set the volume for the speaker, the microphone, the receiver and the headset.

From the control panel main window, double-tap the **Audio** icon:
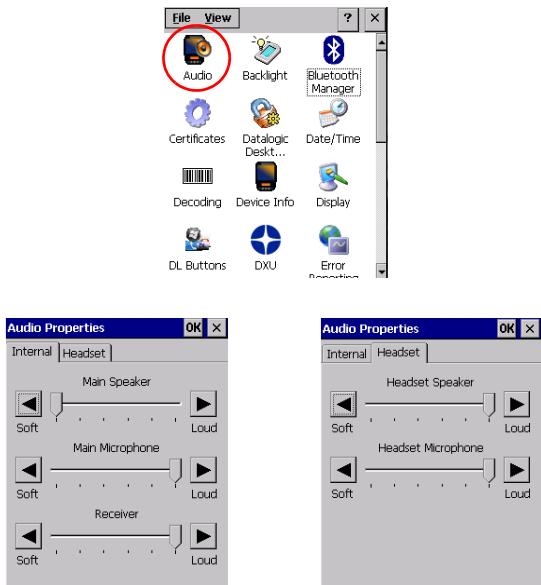
# Volume & Sounds

From the control panel main window, double-tap the **Volume & Sounds** icon:



The **Volume & Sounds** applet configures audio features of all speakers and headphones.
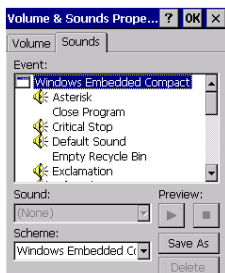
# Bluetooth® Manager Device Setup

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.

> **NOTE**
>
> **By default, Bluetooth® is turned off. If you turn it on, and then turn off your device, Bluetooth® also turns off. When you turn on your device again, Bluetooth® turns on automatically.**

## Enable Bluetooth®

To turn the Bluetooth® on:

1. Double-tap the **Bluetooth Manager** icon from the **Control Panel** window:



2. Tap **Settings**. The Settings tab allows you to enable or disable the Bluetooth® radio and specify settings for Incoming Connections. Select **Enable Bluetooth Radio**.
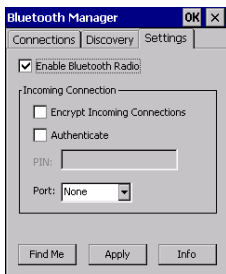
3. If you're going to connect a serial device (i.e. a scanner) to the Falcon X4, use the **Port** control to select a virtual COM port to use for the connection.

4. Tap **Find Me** if you want to make the Falcon X4 discoverable to other Bluetooth® devices for 60 seconds, allowing them to set up a connection. Tap **OK** on the **Find Me** pop-up window.
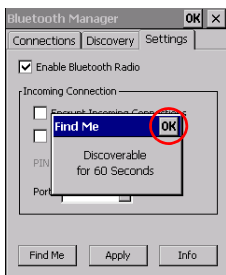


5. Tap **Apply**.

6. Once the Bluetooth® radio is enabled, the terminal automatically starts searching for discoverable devices.

# Connect to Other Bluetooth® Devices

1. From the **Bluetooth Manager** control panel, tap **Connections**:
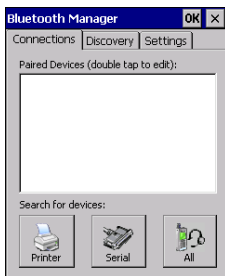


2. Search for available Bluetooth® devices by tapping the button for the type of device you want (**Printer**, **Serial** or **All**) or tap **Discovery** > **Discover** to skip this step. The Falcon X4 will search for Bluetooth® devices within range.
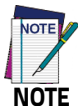
> **NOTE**
>
> **If you attempt to set up a connection when the Bluetooth® radio is disabled, you will receive a message reminding you that the radio is turned off, and asking if you want to turn it on. Tap Yes if you need to enable the Bluetooth® radio.**

| Icon | Service |
|:---:|:---|
| | Dialup Networking |
| | Printer |
| | Object Push (OPP) Object Exchange (OBEX) |
| | ActiveSync |
| | Human Interface Device (HID) - Keyboard |
| | Serial |
| | Personal Area Network (PAN) |
| | Modem |
| | Headset |
| | Handsfree |

3. Once searching is complete, Bluetooth® device profiles will be displayed in the **Discovery** tab. Flick the list and select a device to set up a connection and then tap **Connect**.
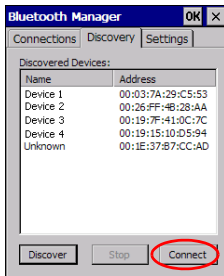
4.  Select a service and configure any encryption, authentication, or virtual port options required by the service selected. Virtual Port allows you to specify the incoming port, which is used to communicate serially with an incoming device just as if it were a physical COM port. This option is available only if you have selected a Printer or Serial service.
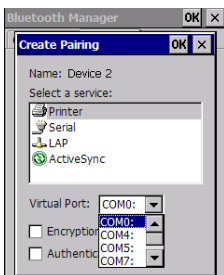


5.  To require Authentication, select the **Authenticate** check box, then tap **OK**.
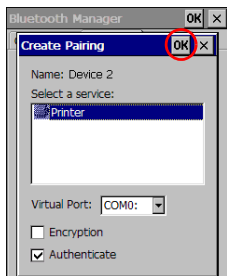
6.  The **Authentication Request** dialog box will request that you enter a PIN. Use the Input Panel or the keyboard to type the PIN. Tap **OK** to complete. The dialog box will also appear when an authentication request is received from another device.
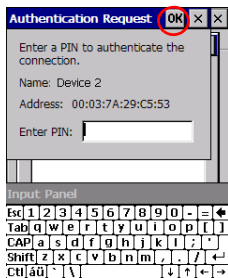


**NOTE**

**You can also select Encrypt or Authenticate from the Settings tab of the Bluetooth Manager control panel.**

# Configure or Unpair Bluetooth® Devices

Once you have set up a pairing, you can view and edit the pairing settings by double-tapping the paired device from the **Connections** tab.
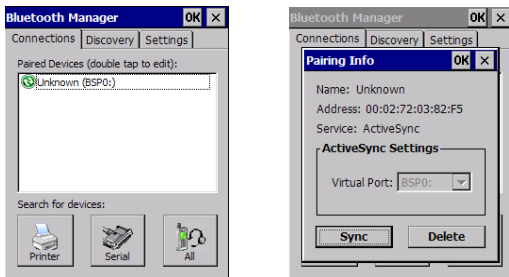


Use the **Virtual Port** drop-down menu to change the Virtual Port. Tap **Sync** to initiate a Sync (available only if the service is an ActiveSync connection). Tap **Delete** to remove the device pairing.

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:

# Persistent Registry

The Registry stores information that are necessary to configure the system for applications and hardware devices. The Registry also contains information that the operating system continually references to during operation.

To persist the Registry settings between boots, follow the steps below:

1. From the **Control Panel** main window, double-tap the **Persistent Registry** icon.

2. Tap **Persist**.

3. Tap **OK** to exit.
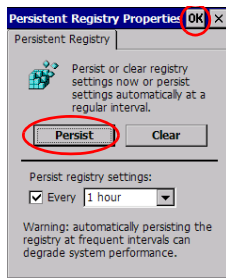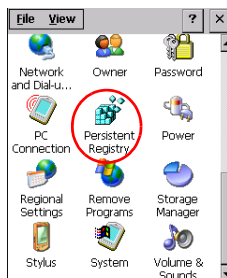
To change the Persistent Registry timing:

1.  From the **Persistent Registry** window, select a time interval from the menu.

2.  Tap **OK** to save and exit.
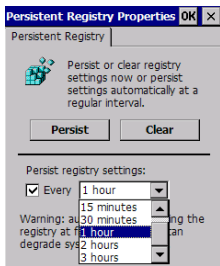


To cancel the Persistent Registry timing:

1.  From the **Persistent Registry** window, deselect the **Persist Registry settings** check box

2.  Tap **OK** to save and exit.

# NOTES

# Datalogic Applications

## DL Buttons

You can use the **DL Buttons** tab to associate specific keys, such as **<F1>-<F10>**, with specific applications.

From the control panel main window, double tap the **DL Buttons** icon to open the **DL Buttons** tab.

Customize the program hardware buttons to launch your most used applications. Use the **Select a button** drop-down menu to select the button you want to assign a function to, and then select an application from the **Assign a function** drop-down menu.
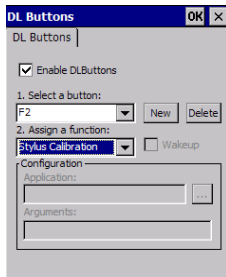


| Command | Description |
|---------|-------------|
| **Select a Button** | This drop-down list shows the available function keys to define. Select the desired one from the list. |
| **New** | Tap to define a new button. |

| Command | Description |
|---|---|
| **Delete** | Tap to delete the selected Button. You can only delete the Buttons you have added. You cannot delete the following buttons: **Alt + 6**, **Left Button**, **Pistol Trigger**, **Right Button**, **Scan**. |
| **Assign a function** | This drop-down list shows the available functions. |
| **Application** | Displays the path to the selected application. |
| **Browse** | Tap ⬚ to browse for application files. You can associate an executable program with the specified button. |
| **Arguments** | Type the command-line arguments that are needed for the specified application. This option is only available when **Launch Application** is selected from the **Assign a function** drop-down list. |

# Add a New Button

To define a new button, follow the steps below:

1. Tap New on the **DL Buttons** tab to open the **Add Key** text box.

2. Enter the desired key combination.
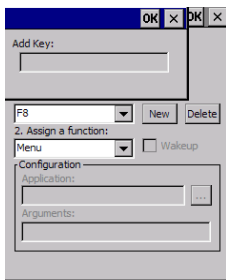


3. Tap **OK** to save the new button. Tap **X** to cancel.

> **NOTE**
>
> **Make sure you do not attempt to add a button that is already defined.**

> **CAUTION**
>
> **The keyboard wedge can activate assigned buttons using alphanumeric characters. Barcodes containing characters associated with assigned buttons will trigger the action or application assigned to that button.**

# Triggers

Triggers are special customizable buttons that are mapped by default by DL Buttons. Also, they can be set as wakeup buttons:
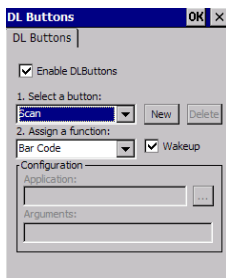


| Triggers | Available Functions |
|---|---|
| Scan | Barcode: activates the scanner. |
| Pistol Trigger | |

# Application Switcher

The application switcher provides the same functionality as the standard Windows® "Alt + Tab" function. This allows the user to switch between the various open applications.

The application switcher is activated via an assigned shortcut key specified in the **DL Buttons** tab (see Persistent Registry on page 78). When the assigned button is pressed, the dialog box below is displayed:
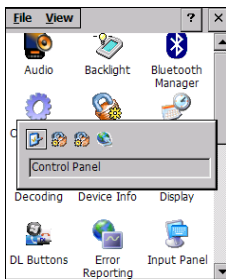


Press the assigned button to cycle through the running applications when the dialog box is open. Press **Enter** to switch to the selected application or **Esc** to close the application switcher.

# Desktop Configuration Utility (DXU)

Datalogic DXU is a unified device configuration utility and firmware update utility. DXU can connect directly to the Falcon 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.
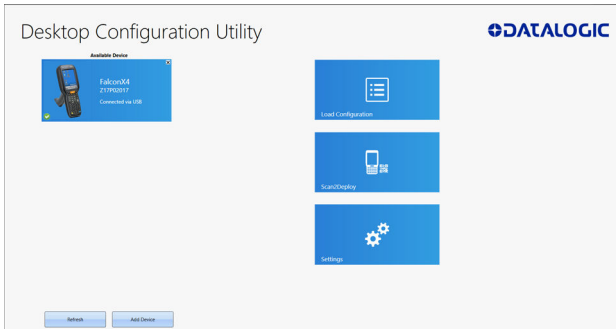


DXU can configure a wide variety of device parameters, including the scanner and most decoding parameters, the touch screen and the keyboard, interfaces such as NFC, Wi-Fi, Bluetooth, USB, and Ethernet, device settings such as date, time, time zone, and power management, and security settings such as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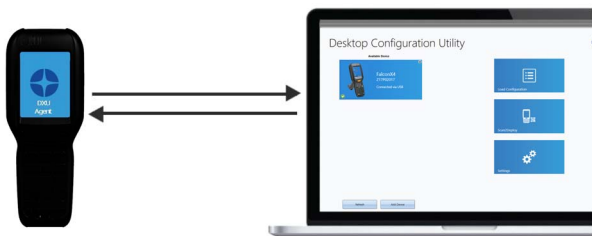


DXU configurations are stored as configuration files on the PC, and are transmitted to and from the Falcon X4 as XML web pages. XML is a standard data format that is widely used for a variety of applications on the internet. Some data is encrypted in the XML file to protect your sensitive data from prying 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. DXU can also connect to devices on your network.

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 Falcon 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

DXU settings on the device can be configured with the DXU control panel.



The following options are available in the DXU control panel:

1. **Desktop Port** number – needs to match setting on DXU Desktop. Requires warm boot for change to take effect.

2. **Pair** – Button to broad case UDP packets to automatic discovery of device by DXU Desktop.

3. **Enable service** – when enabled DXU Agent on the device will function. Requires a warm boot for change to take effect.



### 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.
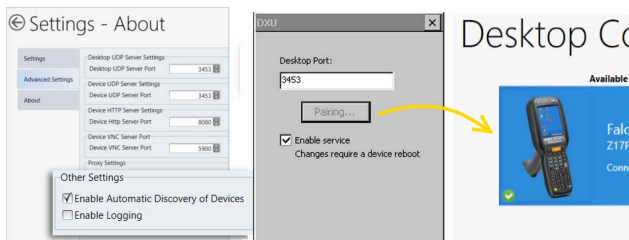


By default, **No Devices Available** will display when no devices announce themselves to DXU either when they connect via USB or when they connect over a network. Simply connecting the Falcon X4 to a network, even on the same subnet as the PC running DXU, will not automatically display as being available. 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 will need to enter the DXU control panel on the device and press the Pair button in order to Automatic Discovery of Devices to properly function.

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.
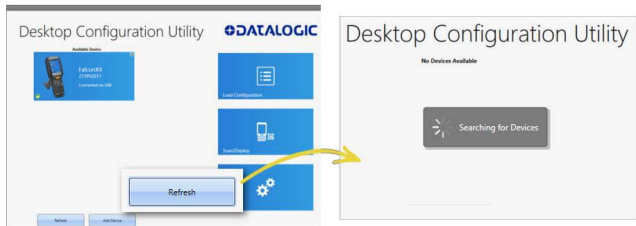


### Add Device

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.
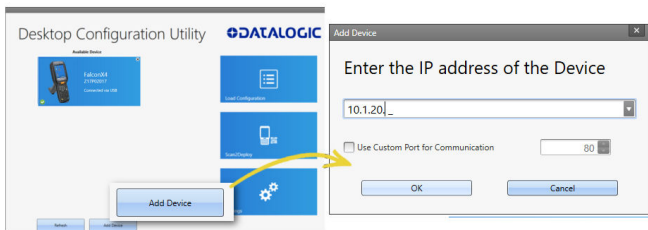


This dialog box allows you to manually connect to devices running DXU Agent that are either inside your PC's subnet or outside it. The limitation is that devices on other subnets must be on a subnet that is routable from your PC's subnet. Consult with your network expert for more information.

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.
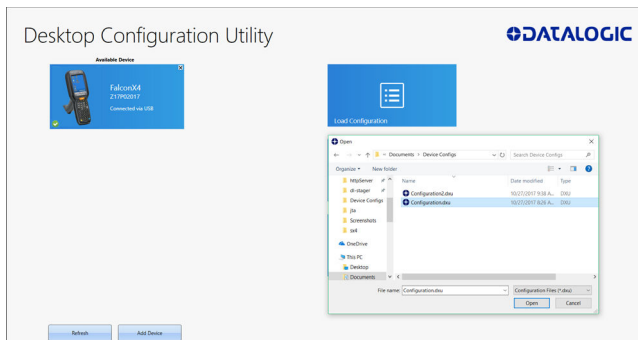
To load a configuration:

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>
```

**WEC7 Example**

```
[update] firmware.img

[install] install.cab
C:\Users\DLUser\Documents\Wec7\auto_sync.cab

[config] defaultConfigWec7.dxu
C:\Users\DLUser\Documents\Wec7\my_user.dxu
```

## Scan2Deploy

Scan2Deploy allows the Falcon 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**.
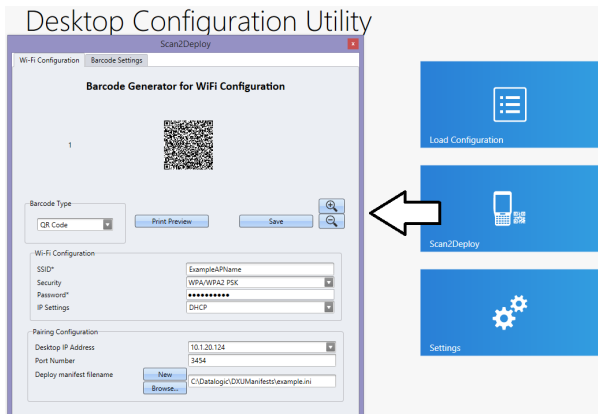
2. Enter the Wi-Fi Configuration information so that the device can connect to the network, including SSID and password.

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.
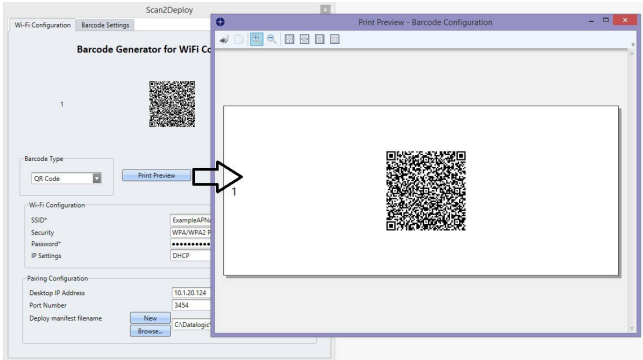
## Printing Custom Configuration Barcodes

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.
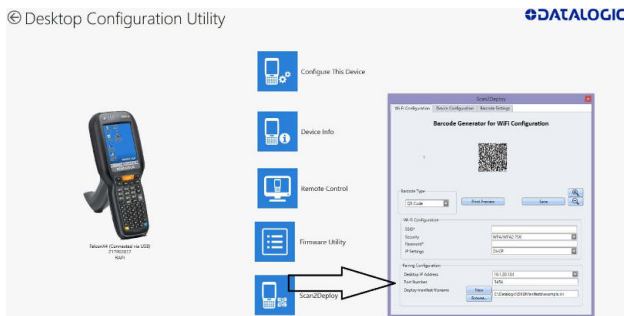


## Wi-Fi Configuration Tab

### 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.

**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.**

**WARNING**

## 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.
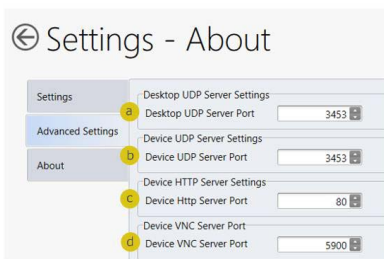


The **Desktop UDP Server Port** (a) and the **Device UDP Server Port** (b) fields must be set to the same value as the matching ports on the remote device to ensure communication and remote configuration. The **Device HTTP Server Port** (c) field must be set to the same value as the matching ports on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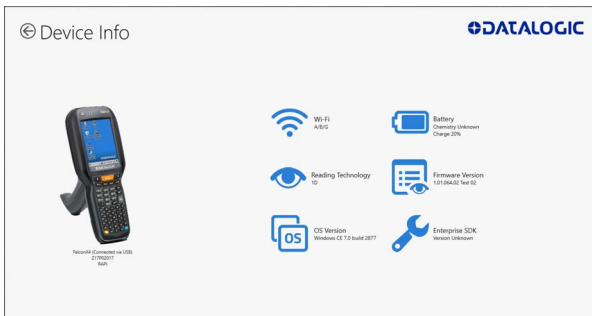
## Remote Control Button

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.
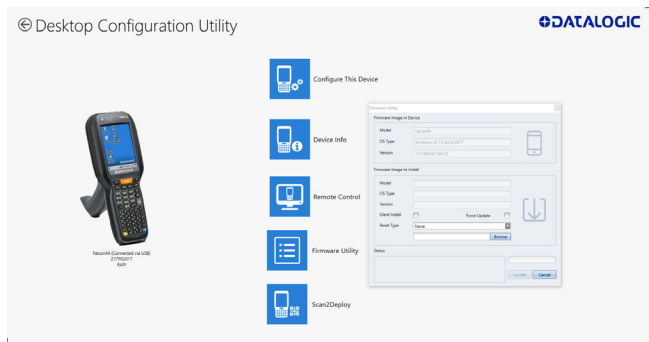
## Scan2Deploy Button

Clicking this button opens the **Scan2Deploy** dialog box (see see 'Printing Custom Configuration Barcodes" on page -99). 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 Falcon 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**;
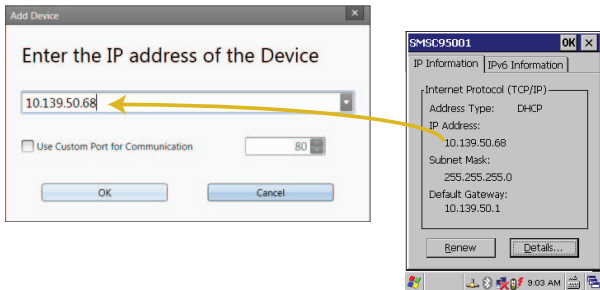


2. In the **Add Device** dialog box, enter the **IP address** of the device and optionally its port, if it is has been changed from the default;

**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. Click **Start menu** > **Programs** > **Device Tools** > **Scan2Deploy**.

> **NOTE**
>
> **Scan to Configure, also under Device Tools, allows you to configure a Wavelink Avalanche barcode to configure.**

8. 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.
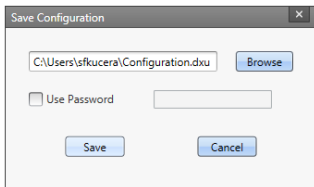


2. You may type the path and the file name in the field, or you can click the **Browse** button to use a standard file dialog box to explore to the folder of your choice and type the file name. Unusually, clicking the **Save** button in the **Save As** dialog box does not actually save the configuration 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**.
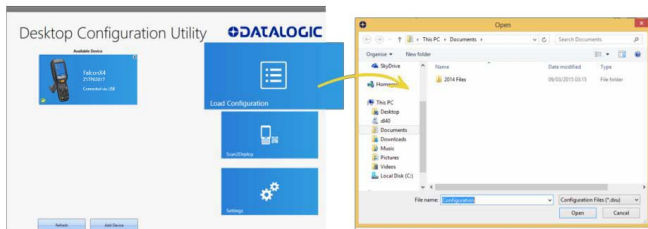


## Open a Configuration File Which is Authenticated

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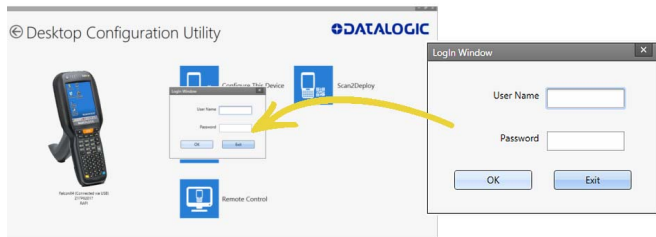
To open a configuration or to connect to a device which requires authentication:

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.
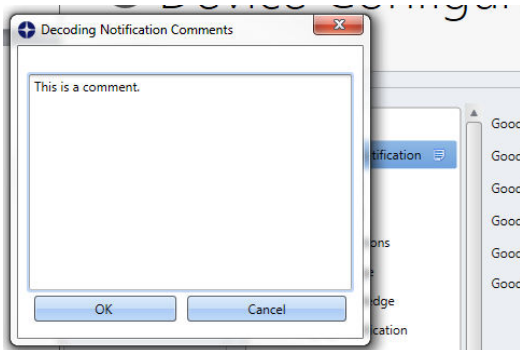
To add a comment:

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.
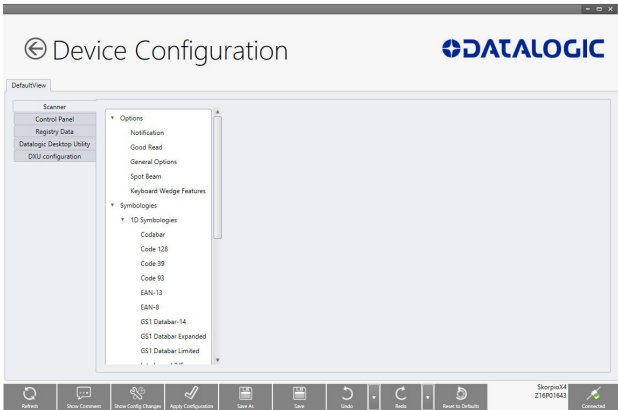
## Configure a Device Off-line via Scan2Deploy

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.
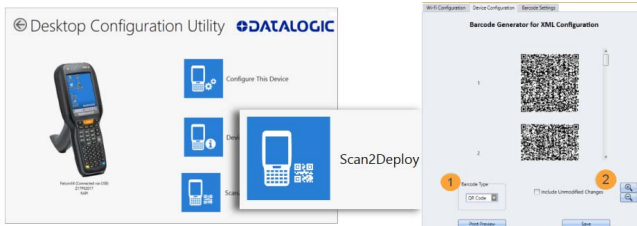


The **Device Configuration** tab has the following additional options:

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.



| QR Code | Aztec | Data Matrix | PDF417 | Code 128 |

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.



**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 Falcon 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.
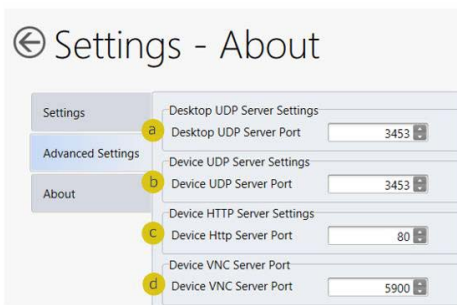


3. Edit the port values to match the ports used by the DXU Agent on your devices:

   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.

> ⚠️ **WARNING**
>
> **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.

### 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.
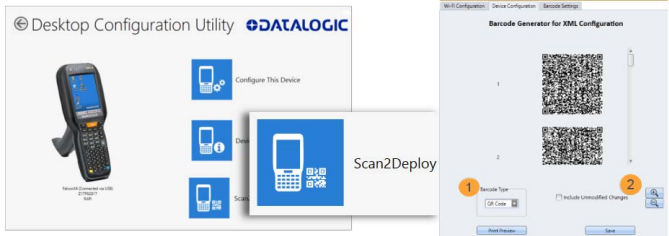


To create **Scan2Deploy** barcodes that can completely configure your device:

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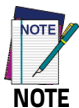
> **NOTE**
>
> **The value in this field is encrypted for security. Once entered, it will be displayed as asterisks.**

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 Falcon 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.
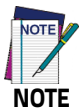
> **NOTE**
>
> **DXU firmware update is not the only way to update the firmware on the Falcon X4. DXU's firmware update capability works only with connected devices. If you need a method that can update firmware on many devices remotely, especially if they are not connected to a network, then other methods may suit your needs better. Please consult your device's user reference guide for other firmware update methods.**
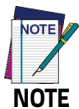
> **NOTE**
>
> **Customarily firmware update is referred to as "update" on devices that use Microsoft Windows operating systems, and it is referred to as "upgrade" on devices that use the Android operating system. These terms are used because the creators of these operating systems use these terms, but 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.
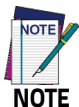
> **NOTE**
>
> **DXU will automatically filter your view of file types to those that are compatible with your device.**

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**.

# 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>.`

# Datalogic Desktop Utility

Datalogic Desktop Utility (DDU) allows administrators to configure Windows® devices to control individual user access. This includes the ability to:

- Prevent users from changing your device OS settings.
- Use the Application Selector to replace the desktop with a selection of authorized applications.
- Restrict user access in Internet Explorer.
- Set up configuration and customized error recovery mechanisms.
- Create quick access hot keys and configure trigger actions.

To open the DDU, double-tap the **DDU** icon on the Control Panel:
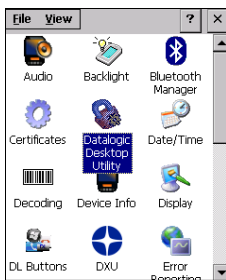


You can also open the DDU by pressing the appropriate key shortcut. The default is "Alt + 6".

| NOTE | **You can change the key combination and specific keys (such as <F1>-<F10>) by using DL Buttons. See DL Buttons on page 81 for more information.** |

# Administrative Options (Admin tab)
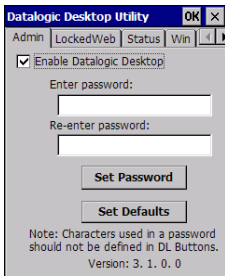


| Command | Description |
|---------|-------------|
| **Enable Datalogic Desktop** | Select to activate the DDU functions such as Windows Access Restrictions and Application Selector. |
| **Enter password** | Allows to specify a password when this utility is launched. |
| **Re-enter password** | Re-enter the password for confirmation. |
| **Set Password** | Tap to enable the password. |
| **Set Defaults** | Tap to reset the default values of all the functions on all the tabs. After you select this option, you will receive a prompt to verify this selection. |

## Set a Password

To set a password, follow the steps below:

1. Enter a password in the Enter password text box. By default the password is "1234". A password can consist of all standard keyboard characters.

2. Re-enter the password in the second text box.

3. Tap **Set Password** to enable the password.

4. Tap **OK** to close the **Password Set** dialog box.
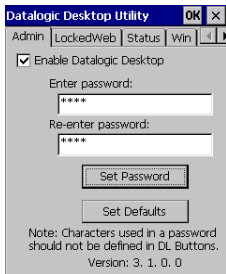
**Be sure to record the Password for future reference.**

**Tap "Set Password" before exiting DDU in order to store and activate your new password. It is not necessary to select Enable Datalogic Desktop.**

> ⚠️ **CAUTION**
>
> **Set Defaults removes all custom settings and restore all the factory default settings, except a previously set password.**

## Change a Password

To change to a new password:

1. Enter a new value in the **Enter password** text box.
2. Re-enter the new value in the **Re-enter password** text box
3. Tap **Set Password**.

## Remove a Password

To remove a password:

1. Enter blank in both password fields.
2. Tap **Set Password**.

## Password Request Dialog Box

Once the password is set, the next time you launch the **Datalogic Desktop Utility**, the DDU password dialog box opens:
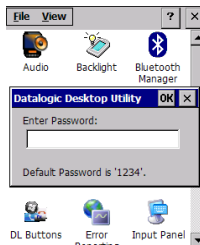
1. Type in your password using either the keypad on the unit, or using the stylus on the soft input panel (SIP). If you enter an incorrect password, the system will prompt you to input the correct one.

2. Tap OK to verify the password, or tap X to cancel.

# Locked Web Browser Options (LockedWeb Tab)

Tap the **LockedWeb** tab to access the Locked Web Browser configuration.

> **NOTE**
>
> **Locked Web Browser is disabled by default. To enable, use the Advanced Settings tab.**

For further information about Locked Web Browser commands and metatags, see Locked Web Browser Options (LockedWeb Tab) on page 139.

## Error Page Redirection

Use the **Error redirection** option to provide customized recovery from common errors. When an error occurs, the browser can redirect access to a specified error page with instructions on how to recover from the problem.

| Error Redirection Options | |
|---|---|
| **Error Type** | The **Error Type** drop-down list displays available Error Types: (400) Invalid Syntax, (403) Request Forbidden, (404) Object Not Found, (406) No Response Format, (410) Page Doesn't Exist, (500) Internal Server Error, (501) Server Can't Do That, Generic Error, Network Disconnected. |
| **Error Page** | Edit this textbox to associate a website or html file with the specified error. |
| Other Options | |
| **Full Screen** | Sets the web browser in full screen mode. |
| **Status Icon** | Enables or disables the status icons view (see Status Icons Options (Status Tab) on page 144). The status icons can be configured on the **Status** tab of DDU. |
| **Trap Keys** | When selected:<br><br>• all key presses will be trapped by the Locked Web Browser to prevent the user from accessing unsafe parts of the system. For example, pressing "Ctrl + O" to open a file will not work;<br><br>• safe key presses (e.g. Alpha numeric) will still get processed by the Locked Web Browser as normal. For example entering a number in a text field on a web page;<br><br>• DL Buttons keys will not work in the LockedWeb Browser;<br><br>• all Locked Web Browser command keys will work (e.g. "Ctrl + O" to exit).<br><br>When not selected:<br><br>• all keys will be processed normally by the system and the browser;<br><br>• DL Buttons keys will work normally;<br><br>• all Locked Web Browser command keys will work (e.g. "Ctrl + O" to exit). |

| Other Options | |
|---|---|
| **Exit password** | When selected, you are prompted for a password to exit the Locked Web Browser. This password is different than the DDU password, with a default value of "0000", and can be changed in the **Advanced** settings. |
| **Browser Home Page** | Sets the Internet Explorer home page, regardless of the enable state of the Locked Web Browser. |
| **Advanced** | Allows to enable the Locked Web Browser and to configure advanced settings. |
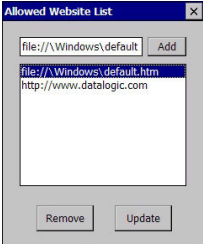
## Advanced Settings
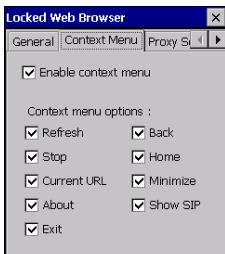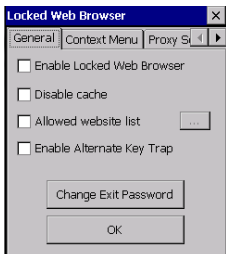


| Advanced Locked Web Browser Options | |
|---|---|
| **General** | |
| **Enable Locked Web Browser** | Enables the Locked Web Browser when Internet Explorer is launched. |
| **Disable Cache** | Prevents the browser from loading the local intranet page from cache instead of navigating to the **Network Disconnected** error redirection page. |

## Advanced Locked Web Browser Options

| | |
|---|---|
| **Allowed Website List** | Restricts browsing only to files and URLs in the **Allowed Website List** (accessed by the ▣ button). The following dialog box appears:<br><br>**Allowed Website List** ☒<br><br>`file://\Windows\default`  Add<br><br>`file://\Windows\default.htm`<br>`http://www.datalogic.com`<br><br>Remove     Update<br><br>Tap **Add** to add allowed URLs to the white list. Other sites will be restricted when the option is enabled. Domain names must be exactly specified. |
| **Enable Alternate Key Trap** | Enables different key trapping mechanism to allow the keyboard usage in network resource access credentials window (recommended setting in case of error when accessing a network shared folder). |
| **OK** | Tap to save changes. |
| **Change Exit Password** | Allows to change the password required to exit the Locked Web Browser (when the **Exit password** option is selected on the **LockedWeb** tab in DDU). |
| **Context Menu** | |
| **Enable Context Menu** | Enables the context menu accessed by a touch screen tap in the Locked Web Browser. |
| **Refresh** | Adds a **Refresh** item to the Locked Web Browser context menu. |
| **Stop** | Adds a **Stop** item to the Locked Web Browser context menu. Selecting during navigation stops the downloading of a page. |

| Advanced Locked Web Browser Options | |
|---|---|
| **Current URL** | Adds a **Current URL** item to the Locked Web Browser context menu. Selecting the item pops up a dialog displaying the URL for the current web page. |
| **About** | Adds an **About** item to the Locked Web Browser context menu. Selecting the item pops up the **About** dialog. |
| **Exit** | Adds an **Exit** item to the Locked Web Browser context menu. Selecting the item exits the Locked Web Browser with an optional password (set in the Locked Web Browser Advanced options). |
| **Back** | Adds a **Back** item to the Locked Web Browser context menu. Selecting the item allows to navigate to the previous page. |
| **Home** | Adds a **Home** item to the Locked Web Browser context menu. Selecting the item allows to navigate to the IE home page. |
| **Minimize** | Adds a **Minimize** item to the Locked Web Browser context menu. Selecting the item minimizes the Locked Web Browser and allows access to other programs. |
| **Show SIP** | Adds a **Show SIP** item to the Locked Web Browser context menu. Selecting the item toggles the show state of the SIP. |

# Status Icons Options (Status Tab)

Tap the **Status** tab to access the Status Icons option. You can configure the view of some status icons that are used in **LockedWeb** and in **Application Selector** to display the status of Wi-Fi radio and battery.
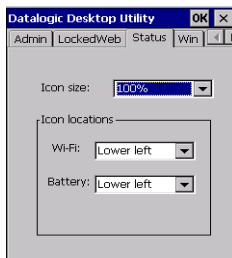


| Status Icons Options | |
|---|---|
| **Icon size** | Sets the status icons' size. |
| **Icon locations** | Selects the preferred location for each status icon. |

# Windows Controls (Win Tab)

Tap the **Win** tab to allow or restrict access to Windows system functions.



You can disable normal Windows functions such as the taskbar, leaving nothing but a blank workspace. This allows to run applications in full screen mode and prevents users from accidental or unauthorized use of the taskbar, Internet Explorer, and any other resident applications.

| Windows Controls | |
|---|---|
| **Show taskbar** | Select to display/hide the Taskbar. |
| **Taskbar enabled** | Select to display the taskbar. This option is only available when **Show taskbar** is selected. |
| **Start menu enabled** | Select to display the **Start Menu**. This option is only available when **Taskbar enabled** is selected. |
| **AutoSIP enabled** | Enables the AutoSIP Windows feature. |
| **Scroll bars enabled** | Select to display horizontal and vertical scroll bars to help view large web pages which do not fit the screen. This control only takes effect in Locked Web Browser. |
| **WEC7 desktop enabled** | Select to display the desktop icons. |

**Changes require a device reboot.**

# AppSelector Options (AppSelect Tab)

The Application Selector replaces the desktop and allows only authorized use of applications.

Tap the Application Selector tab (**AppSelect**) to edit, add, or delete applications for the application selector.
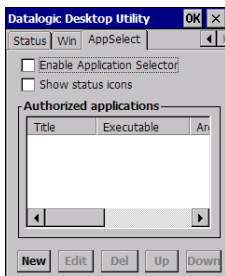


| Application Selector Options | |
|---|---|
| **Enable Application Selector** | Select to enable the application selector. |
| **Show status icons** | Select to enable the status icons view (see Status Icons Options (Status Tab) on page 144). The status icons can be configured on the **Status** tab of DDU. |
| **Authorized applications** | List of applications that the user can access. |
| **Application Selector Commands** | |
| **New** | Tap to create a new application entry. |
| **Edit** | Tap to edit the selected entry. |
| **Del** | Tap to delete the selected entry. |
| **Up/Down** | Tap to move an entry up or down in the ListView. |

## Add Application

The **Add Application** dialog opens when you tap either **New** or **Edit**. Use it to configure and/or add/change a new application entry in the list.

Applications with the **Run Application at Startup** option enabled will start automatically when the Application Selector starts up.
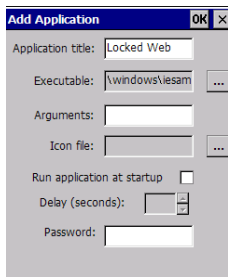


| Command | Description |
|---|---|
| **Application Title** | Type the name of the application in the way it should appear on screen for the end-user. |
| **Executable** | Displays the path for the executable file you want to run. |
| **Browse** | Tap ⌐⌐ to browse for the desired executable file. You can associate an executable program with the specified button. The results of this search are displayed in the **Executable** textbox. |
| **Arguments** | Type any command line arguments to be used when an application is executed. |
| **Icon File** | Displays the path to the desired icon file. |
| **Browse** | Tap ⌐⌐ to browse for the desired icon file. The results of this search are displayed in the **Icon file** textbox. |

| Command | Description |
|---|---|
| **Run Application at Startup** | Select to force the application to auto start when the Application Selector starts up. Applications will be started in the order listed in the authorized application list. |
| **Delay** | Enter a delay duration in seconds in the combo box. This option delays auto start of application(s) to allow drivers to load before starting applications. |
| **OK** | Tap to add/save changes. |
| **X** | Tap to cancel. |

# App Selector (Application Selector)

The Application Selector is an application allowing a device to run in kiosk mode. The administrator can choose for the user to have access to the desktop or not.

The Application Selector can replace the desktop and limit the user to the specified list of applications.

By default, the Application Selector comes with no applications preset.
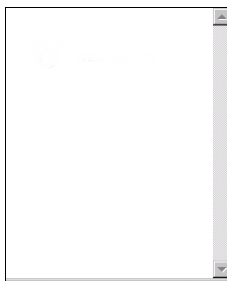


The administrator can customize this list as shown in AppSelector Options (AppSelect Tab) on page 147. Additionally, the page template can be modified to display a different background. Contact your Datalogic representative for more information on this feature.

To run an application, tap its name.

To exit the Application Selector, press "ALT + 6", deselect the **Enable Application Selector** check box on the **AppSelect Tab** and press **OK** to exit DDU.

# Locked Web Browser

The Locked Web Browser is a browser helper object for Internet Explorer. It allows an administrator to define a restricted internet usage environment. Once in the restricted environment, a password is required to exit. This means users can only access web applications and websites set by the administrator.

> **NOTE**
>
> **Configuration is set up through the DDU control panel. See Locked Web Browser Options (LockedWeb Tab) on page 139 for more information.**
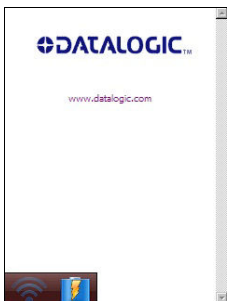


**Full Screen Mode**



**CE Mode**

In full screen mode, status icons may be used to display signal strength and battery status. In CE mode, the status bar is displayed but the user interaction is disabled.

In the restricted environment, the user can navigate by using the following keyboard shortcuts:

| Home | Ctrl + 7 |
| --- | --- |
| Refresh | Ctrl + 8 |
| Cancel | Ctrl + 9 |
| Exit | Ctrl + 0 |

For firmware versions 1.60 and greater, the following command line arguments are supported:

- /E optional parameter which allows for Exit without entering a password

- @URL optional parameter which specifies a URL to use as a home page.

- /C optional parameter which disables the ctrl keys (including the one to exit).

# Locked Web Browser Special Metatags

## General Metatag Comments

A metatag is a special HTML tag that stores information about a Web page but does not display in a Web browser. For example, metatags provide information such as the program used to create the page, a description of the page, and keywords relevant to the page.

As per the HTML specification, all metatags must be contained within a <head> ...

</head> tag set.

Also, the head tag set must be complete within the first 15K of the web page.

The Datalogic Locked Web Browser defines some special metatags that allow the web application to interact with the device:

In particular, the special metatags allow it to:

- enable/disable scan engine triggers
- enable/disable specific symbologies in the scan engine
- easily assign a key press to a javascript function.

Metatag settings of trigger enable, symbology enable, or DL_Key assignments persist past the page in which they are loaded. The settings stay in effect until they are changed by another metatag.

### Trigger Metatag

DL_Triggers – "Enable" or "Disable" all triggers

If the page contains this tag, the triggers are enable or disable depending on the "content=" value.

Example:

<meta http-equiv="DL_Triggers" content="Disable">

## GetSerialNumber Meta-tag

DL_GetSerialNumber – Obtains the device serial number and sends it as an argument to a customer's javascript function.

Content – name of function to pass serial number to.

Example:

<meta http-equiv="DL_GetSerialNumber" content=

"Javascript:CustomerFunction">

When a page with this metatag is loaded, the content should be a javascript function that receives one parameter, the serial number. An example would be function CustomerFunction(SerialNumber).

## Reboot – Warm Boot Device Metatag

DL_Reboot – Warm boot device.

Content – "OnPageLoad" – Warm boot immediately upon page load.

Example:

<meta http-equiv="DL_Reboot" content=" OnPageLoad ">

## Exit Metatag

DL_Exit – Exit the Locked Web Browser.

Content – "OnPageLoad" – Exit immediately upon page load. If "Exit password" has been enabled in the Locked Web Browser options, the Exit password will be required before exit.

Example:

<meta http-equiv="DL_ Exit " content=" OnPageLoad ">

## Decoding Metatags

Each decoding metatag has a possible content of "Enable" or "Disable". The settings are valid for the entire page (enables/disables each symbology).

DL_Code_39    DL_Code_128    DL_Code_I25    DL_Code_S25
DL_Code_M25  DL_Code_CODABAR  DL_Code_93  DL_Code_UPCA
DL_Code_UPCE  DL_Code_EAN13  DL_Code_EAN8  DL_Code_MSI
DL_Code_MSR          DL_Code_GS1_14          DL_Code_GS1_LIMIT
DL_Code_GS1_EXP  DL_Code_PDF417  DL_Code_DATAMATIX
DL_Code_MAXICODE
DL_Code_TRIOPTIC
DL_Code_PHARMA39
DL_Code_RFID
DL_Code_MICROPDF417
DL_Code_COMPOSITE
DL_Code_QRCODE  DL_Code_AZTEC
DL_Code_POSTAL

Examples:
<meta http-equiv="DL_Code_39" content="Disable">
<meta http-equiv="DL_Code_I25" content="Enable">

## Key Press Metatags

The key press metatags can be used to call JavaScript functions. They have the name structure: "DL_Key_xxx" where xxx is the VKey code.

Example:

<meta http-equiv="DL_Key_13" content="Javascript:CheckEnter();">

Assigning a key press via a DL_Key metatag overrides its use on the page. For instance, when entering data in a text box a character assigned as a DL_Key would not be entered in the text box. Instead, the javascript action would occur.

Refer to the Microsoft website to find the list of all the possible Vkey codes:

http://msdn.microsoft.com/en-us/library/bb431750.aspx

http://msdn.microsoft.com/en-us/library/aa243025(VS.60).aspx

**NOTE**

**Because DL_Keys persist past the page in which they were loaded, the DL_Clear metatag is provided to clear the settings on subsequent page loads.**

## Scanning Metatags

DL_Scan – Captures scan results and sends barcode/tag value to a javascript function on the web page.

If the "content=" value is a javascript function the device will be taken out of keyboard wedge mode and start listening for scan events. A scanned barcode/tag result will be used as an argument to that javascript function which is then invoked.

If the "content=" value is "Wedge" then the device will stop listening for scanned event and enter keyboard wedge mode.

If the "content=" value is "Disable" then the device will stop listening for scanned events but not enter keyboard wedge mode.

Example:

<meta http-equiv="DL_Scan" content="Javascript:ValidateInput()">.

# PAL and PAL Communicator

Pal is an easily customizable program that is ready-to-use for data entry needs.

Pal Communicator is a PC application that allows you to manage the data transfer between a host computer and mobile devices.

For further information refer to the Pal & Pal Communicator User's Guide, downloadable from our website (see Support Through the Website on page 235).

# Autostart

The AutoStart program provides three functions:

- allows to create a list of applications (with optional command line arguments) to run automatically before loading CAB files;
- automatically reinstalls specified CAB files when the Falcon X4 is cold booted;
- allows to create a list of applications (with optional command line arguments) to run automatically after loading CAB files.

AutoStart launches each time the Falcon X4 is rebooted executing each line with the specified command line arguments. It will take into account any AutoStart options at the beginning of the line.

Upon a Cold Boot, AutoStart installs all the CAB files located in the \FlashDisk\CAB folder. If the CAB folder does not exist, no CAB files will be installed.

AutoStart will then run the **Autostart.ini** from the \flashDisk directory, executing each line with the specified command line arguments. It will take into account any AutoStart options at the beginning of the line.

## Installing CAB Files

Copy any CAB files you want to install into the \FlashDisk\CAB folder. These CAB files will then be automatically in-stalled in alphabetical order the next time you start the device.

# How AutoStart Uses Wceload

**NOTE**

**If you intend to create highly interactive installers, you should either install the CABs manually or review the section Interactive CAB Install on page 161.**

**CAUTION**

**In certain environments, CAB files will be deleted after execution. To prevent the CAB file from being deleted, write protect the file before copying the file onto the device.**

CAB files are installed by AutoStart using the **Wceload.exe** application. The following table shows available command line option:

| Option | Description |
|--------|-------------|
| **/noui** | Specifies that you will not be prompted for any input during the installation. If the CAB file is signed, any responses will automatically be answered **Yes**. If the CAB is unsigned, then any responses will be answered **No**. |
| **/silent** | Suppresses dialog boxes during the installation. |

Please refer to the Microsoft documentation on your device for further details on **Wceload.exe**.

Sample:

```
\Windows\Wceload.exe /delete 1 /noui /silent
"\FlashDisk\CAB\<cab file>"
```

# Interactive CAB Install

If the CAB installer requires user interaction that must be performed during the AutoStart CAB installation process, you can specify a special file name to disable the silent mode installation. If this mode is specified, the CAB file will be installed with Wceload without any command line arguments specified.

An example of what AutoStart would execute is:

`\Windows\Wceload.exe <cab file>`

To force this mode of installation via AutoStart, rename the CAB file to include a **_** character before the **.cab** extension of the file.

Example:

`File.cab` should be renamed `File_.cab` to force AutoStart to not install the CAB in silent mode. This specially-named CAB file should be placed in the AutoStart folder with other CAB files intended for installation on the next reboot.

# Autostart.ini

> **NOTE**
>
> **A file named PreAuto.ini can also be created in addition to or instead of Autostart.ini. PreAuto.ini is executed before CAB files in the \FlashDisk\CAB folder are installed. Autostart.ini is executed after CAB files in the \FlashDisk\CAB folder are installed. The format for the PreAuto.ini is identical to that of Autostart.ini.**

Autostart.ini is a text file that AutoStart will run upon startup of the Falcon X4, and after any CAB files are installed. This file should be placed in the \flashDisk folder. AutoStart will run the Autostart.ini file on each reboot of the device.

## Line Formatting

Each line of the Autostart.ini can consist of Autostart options, an executable, and any command line arguments.

**`< Autostart option(s)> <full path to executable> <command line arguments>`**

Sample:

**`- \windows\pword.exe \file.doc`**

The following table breaks down the sample Autostart.ini line:

| Autostart Option(s) | Full Path to Executable | Command Line Arguments |
|---|---|---|
| - | \windows\pword.exe | \file.doc |

Spaces must be placed between each component of the line in the Autostart.ini.

If the executable path is in a folder that contains spaces in the name, quotes are required to distinguish what the actual executable name is. The following is an example of this:

```
"\Program Files\ScannerApp.exe" /run
     (valid)
\Program Files\ScannerApp.exe /run
     (invalid)
```

The second line is an invalid line because there is no way to distinguish the executable from the argument.

## AutoStart Options

The table below shows the options you can use when writing a line in the Autostart.ini file.

| Description | Character | Comments |
|---|---|---|
| Comment: This line will not be executed. | '#' OR ' ' (space) | This may only be used as the first character of the line. If the comment option is specified in the options elsewhere, it is ignored. |
| Do not wait on line completion: This will cause the line to execute and immediately move onto the next line. | '-' | |
| Query: Request user confirmation when running the executable. | '?' | This will halt parsing the Autostart.ini until the confirmation is answered. This is intended for debugging the Autostart.ini file. |
| Execute only on Cold Reset | '!' | |
| Execute only after a warm boot | '%' | |

**Cold Reset Only**: This will cause the line to execute only after a Cold Reset.

**An empty line will be treated as a comment line.**

## Combining Options

Autostart options can be combined together as shown in the following sample:

**`?- \Windows\Pword.exe`**

This line would:

- request confirmation before executing the line. The next line would not be processed before the confirmation is answered;
- run the next line without waiting on the current line to complete execution.

## Query Option

The query option is intended for use when debugging the autostart.ini. When a line with this option is executed, the fol-lowing dialog box will appear with the specified executable and command line arguments. The populated fields shown in the AutoStart Execute Query are described the next table:
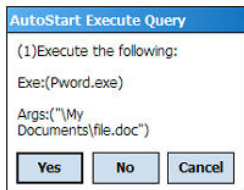


| Field | Description |
|-------|-------------|
| Line Number | The line number in the script being executed. |
| Exe | The executable as parsed by AutoStart. |
| Args | The argument as parsed by AutoStart. |

**NOTE**

**The fields may be broken up into multiple lines (as shown in the example) due to limited space in the dialog box.**

## AutoStart Query Options

Parentheses are used to surround the given field and make clear what the value of the field is.

The following table describes the results of each choice:

| Button | Action |
|--------|--------|
| Yes | The current line will execute. |
| No | The current line will not execute. AutoStart will continue parsing the Autostart.ini. |
| Cancel | The current line will not execute and AutoStart will discontinue parsing the Autostart.ini. |

## Autostart.ini Samples

The next table is a collection of sample Autostart.ini lines:

| Line | Description |
|------|-------------|
| ? \windows\wceload.exe "\My Documents\Sample.cab" | This will confirm the execution of \Windows\wceload.exe with specified argument "\My Documents\Sample.cab" |
| \Program Files\App.exe | (invalid) This will execute \Program with the argument Files\App.exe. |
| \Program Files\App.exe /run | (invalid) This will execute \Program with the argument Files\App.exe /run. |
| "\Program Files\App.exe" /run | This will execute the program \Program Files\App.exe with the argument /run. |
| ?- \Windows\Pword.exe | This will confirm the execution of \Windows\Pword.exe. If the execution is confirmed, AutoStart will immediately process the next line. |
| !"\Program Files\App.exe" /run | This will execute the program \Program Files\App.exe with the argument /run ONLY after a Cold Reset. |

# NOTES

# Tools

# Windows Embedded Compact 7 SDK

The latest version of the Windows CE SDK can be downloaded from http://www.datalogic.com on the Falcon X4 product page. This installer includes a detailed help file and sample applications.

## Prerequisites

- ActiveSync 4.5 for Windows XP computers:
  *http://www.microsoft.com/download/en/details.aspx?id=15*

- Windows Mobile Device Center 6.1 or newer for Windows 7 32-bit computers:
  http://www.microsoft.com/download/en/details.aspx?id=14

- Windows Mobile Device Center 6.1 or newer for Windows 7 64-bit computers:
  http://www.microsoft.com/download/en/details.aspx?id=3182

- For C, C++, C# development, Microsoft Visual Studio 2008:

  - Microsoft Visual Studio 2008 Service Pack 1:
    http://go.microsoft.com/fwlink/?LinkId=122094 or
    https://www.microsoft.com/en-us/download/details.aspx?id=13276 (iso file)

  - https://www.microsoft.com/en-us/download/details.aspx?id=11935: when debugging Windows Embedded Compact 7 application using the Visual Studio 2008 for Smart

Devices debugger, a user might not be able to use the single step function. This update addresses this issue

- http://www.microsoft.com/en-us/download/details.aspx?id=27729: an update is available for Microsoft Visual Studio 2008 Service Pack 1 (SP1) that extends support for Windows Embedded Compact 7 (https://support.microsoft.com/en-us/kb/2468183)

- Windows Mobile 6 Professional Development Kits Refresh is required for all Windows Mobile or Windows Embedded Handheld 6.5 devices using C, C++, C# languages. Go to this link to download the file:
  http://www.microsoft.com/en-us/download/details.aspx?id=6135

- Windows Mobile 6 Professional Development Kits Refresh is also required for Windows CE devices using C, C++, C# languages when developing on a Windows 7 64-bit computer.

# Data Capture

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

See "Data Capture Configuration" on page -44 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.  From the **Decoding Properties** window, tap the barcode icon to open the **Decoded Data** window.

or
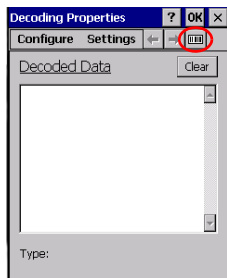
From the WEC7 desktop, double-tap the **Microsoft WordPad** icon:
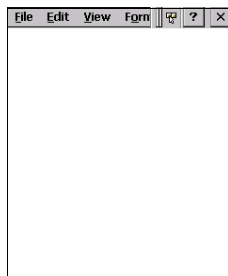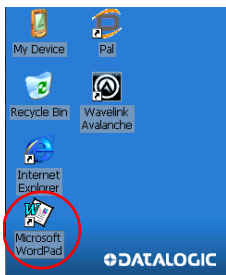


2. Point the scan window at the barcode from a distance within the reading range.

3. 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.
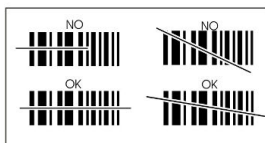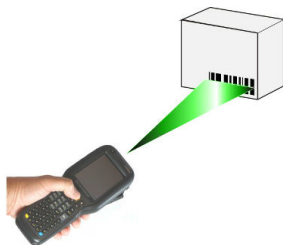
If the scan has been successful:

- 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 Falcon 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. From the **Decoding Properties** window, tap the barcode icon to open the **Decoded Data** window.



    or
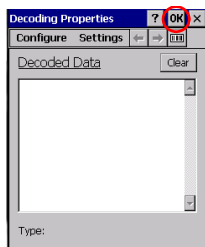
    From the WEC7 desktop, double-tap the Microsoft WordPad icon:
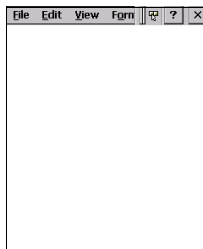
2. Point the scan window at the barcode from a distance within the reading range.

3. 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.



4. 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.



Linear Bar Code     2D Matrix Symbol

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 Falcon 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 Falcon X4 to a host PC running Windows. Each requires specific connections in order to function properly.

## Windows Mobile® Device Center

The desktop application Windows Mobile® Device Center allows you to synchronize information between a desktop computer and your Falcon X4. Synchronization compares the data on the Falcon X4 with that on the desktop computer and updates both with the most recent information.

Windows Mobile® Device Center can be downloaded from Microsoft website www.microsoft.com. It is only compatible with Windows Vista and Windows 7; if you run Windows XP or earlier, you have to download Microsoft ActiveSync.

You can establish a connection to your Falcon X4 through the following interfaces:

- USB either directly or through the Single Dock.
- RS232 either directly or through the Single Dock.
- Bluetooth® (see Bluetooth® Manager Device Setup on page 71)

To establish a partnership between the Falcon X4 and a host PC, start Windows Mobile® Device Center and follow the steps below:

1. Connect the Falcon X4 to the host PC. Windows Mobile® Device Center configures itself and then opens.

2. On the license agreement screen, click Accept.

3. On the Windows Mobile® Device Center's Home screen, click Set up your device.

4. Select the information types that you want to synchronize, then click Next.

5. Enter a device name and click Set Up.

When you finish the setup wizard, Windows Mobile® Device Center synchronizes the mobile computer automatically. Microsoft® Office Outlook® emails and other information will appear on your device after synchronization.

> **The Falcon X4 running WEC7 does not come equipped with Microsoft Office Outlook or any other application that allows users to view contact, calendar, e-mail, or task data. Users can view files copied to the Falcon X4 by WMDC's file synchronization feature.**

# USB Connection

## USB HandyLink™ Connection

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

**Host Computer**



**Falcon X4**

**94A051970 HandyLink
USB Client Cable**

**NOTE**
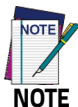
**The HandyLink cable complies to USB 2.0 standard.**

# USB Dock Connection

The single dock can be connected to the host computer using the A to B USB cord included in the box.

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



**Host Computer**

**94A150057**
**Single Slot Dock**

**A to B USB**
**straight cable**

**94ACC1381**
**Power Adapter**

**NOTE**
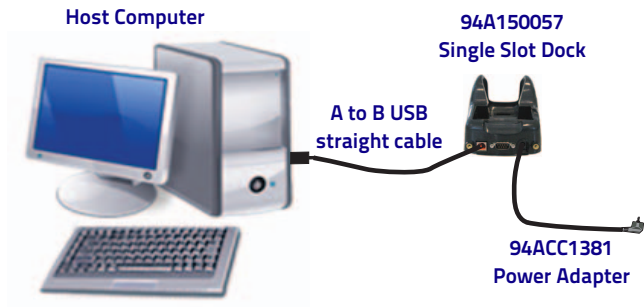
**Connection through the dock complies to USB 2.0 standard.**

**NOTE**

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

# Connection to USB Peripherals

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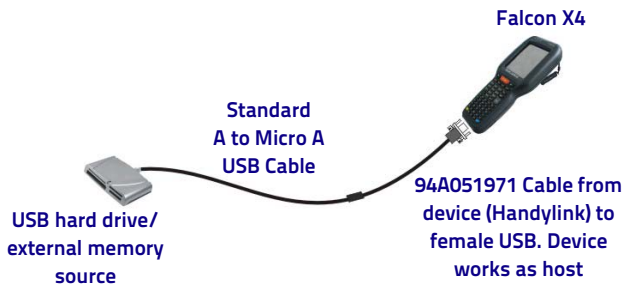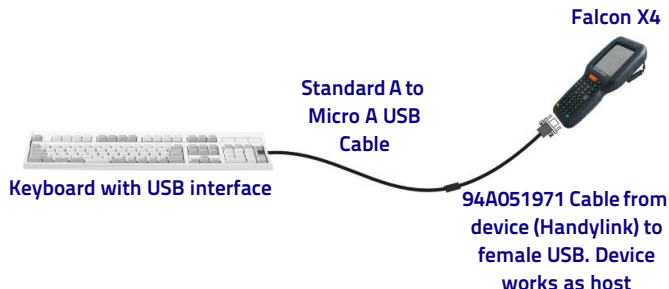
**Falcon X4**

**Standard A to Micro A USB Cable**

**Keyboard with USB interface**

**94A051971 Cable from device (Handylink) to female USB. Device works as host**

**Falcon X4**

**Standard A to Micro A USB Cable**

**USB hard drive/ external memory source**

**94A051971 Cable from device (Handylink) to female USB. Device works as host**

\* 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 using an A to B USB cord (together with a standard USB cable if needed*).



**94A150057**
**Single Slot Dock**

**USB hard drive/**
**external memory**
**source**

**Standard**
**A to Micro A**
**USB Cable**

**94A051969**
**Cable from Micro**
**USB (device or**
**dock) to female**
**USB. Device**
**works as host**

**94ACC1381**
**Power Adapter**
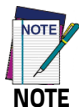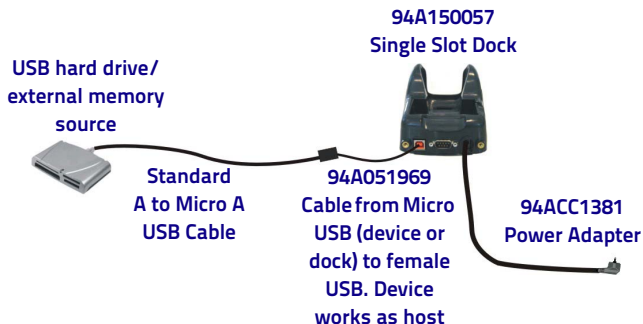


**Falcon X4 works with most of the mentioned USB peripherals. Datalogic cannot guarantee the interoperability of Falcon X4 with all devices on the market.**
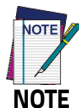


**Connection complies to USB 2.0 standard.**



**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 Falcon X4 to a host computer to transfer data through the RS232 interface.

**Host Computer**

**Falcon X4**

**94A051972 HandyLink Micro RS232 Client Cable**

# 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 Falcon X4 mobile computer into the cradle.

**Host Computer**

**94A150057 Single Slot Dock**

**94A051020 CAB-427 RS232 Null Modem Cable**

**94ACC1381 Power Adapter**
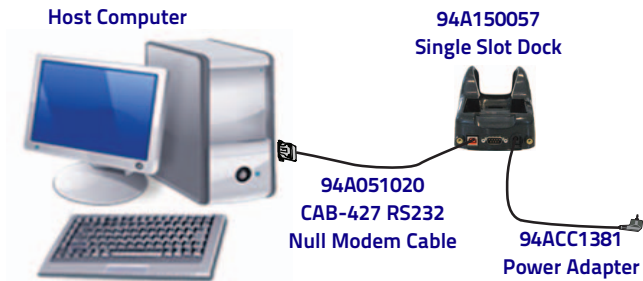
# WLAN Connection

Falcon 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.

For more information on this utility, refer to WCU (Wireless Configuration Utility) on page 55.
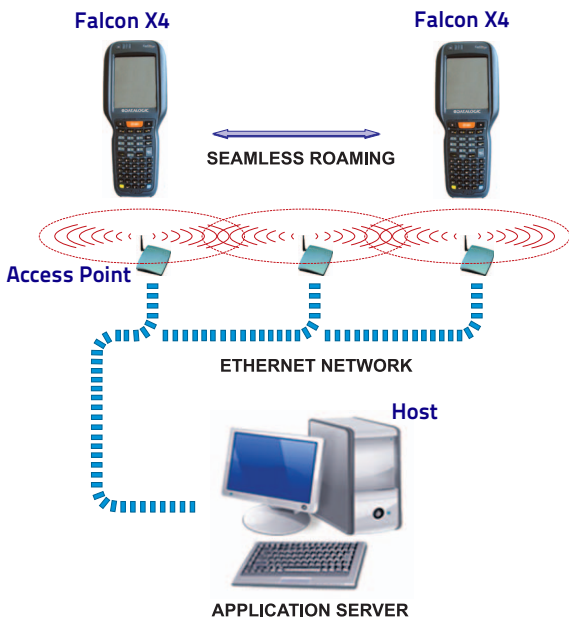
**NOTE**

**802.11 a/b/g/n radio module is on by default, in order to avoid wasting energy, you can switch it off.**

**NOTE**

**Suspending the terminal powers off the 802.11 a/b/g/n radio and drops the radio connection. When the terminal resumes, depending on the radio power mode and security protocol selected, it may take up to 30 seconds for the 802.11 a/b/g/n radio driver to re-associate the radio to the network.**

**NOTE**

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

**NOTE**

**In case of heavy usage the Falcon X4 may get warm; this is normal and does not mean a malfunction.**

# WPAN Connection

Falcon 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.

**Bluetooth® Printer**



**Falcon X4**

| 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 71).** |
| --- | --- |

| 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 Falcon 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: 22.5 x 8.8 x 5.5 cm / 8.9 x 3.5 x 2.2 in<br>6.4 x 4.0 cm / 2.5 x 1.6 in at keyboard<br>Pistol grip: 22.5 x 8.8 x 16.8 cm / 8.9 x 3.5 x 6.6 in |
| Weight | Handheld: 608.0 g / 21.4 oz<br>Pistol grip: 674.0 g / 23.8 oz |
| Display | Reflective TFT daylight readable color display, 320 x 240 pixels, 8.9 cm / 3.5 in diagonal, 65K colors, backlight, touch screen |
| Keyboard | Polycarbonate hard cap keyboards with backlight; 29-key numeric or 52-key alphanumeric with discrete navigation |
| Audio | Integrated microphone, high-volume speaker |
| **Environmental** | |
| Drop Resistance | Withstands drops from 1.8 m / 6.0 ft onto concrete and 1500 random drops from 1.0 m / 3.3 ft according to IEC68-2-32 (Method 2) |
| Particulate and Water Sealing Temperature | IP65<br>Operating: –20 to 50° C / –4 to 122° F<br>Storage: –30 to 70° C / –22 to 158° F |

| Electrical | |
| --- | --- |
| Battery | Removable battery pack with rechargeable Li-ion batteries; 3.7 V 5200 mAh (19.2 Watt hours) |

| 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 wireless technology 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 Ethernet: via single-slot dock (external module) |

| System | |
| --- | --- |
| Operating System | Microsoft Windows Embedded Compact 7 (WEC7)[*] |
| Expansion Slots | Micro Secure Digital slot (SDHC) up to 32 GB, user-accessible |
| Microprocessor | TI OMAP4 @ 1 GHz. |
| Real-Time Clock | Time and date stamping under software control |
| 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 Falcon X4 configurations. The OS swap must be performed at a Datalogic Service Center.

| Software | |
|---|---|
| Applications | Pal Application Library pre-licensed |
| Configuration & Maintenance | Wavelink Avalanche® pre-licensed, SOTI MobiControl, Datalogic xPlatform Utility (DXU) pre-licensed, Datalogic Desktop Utility (DDU) pre-licensed for device lockdown |
| Development | Datalogic Windows SDK™, Wavelink® Studio™, MCL-Collection™ |
| Browser | SureLock locked web browser pre-licensed |
| Terminal Emulation | Wavelink® Terminal Emulation™ pre-licensed (for Pistol Grip models only) |
| 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 |
| Stacked Codes | GS1 COMPOSITE CODES UPC/EAN/JAN Composites, GS1 DataBar Composites and GS1-128 Composite |

| Reading Performance | |
|---|---|
| 2D Imager (Standard Range) | Megapixel sensor for extended range<br>White LED Illumination<br>Optical Resolution: 1D codes: 3 mils; 2D codes: 6.6 mils<br>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<br>Optical Resolution: 2.5 mils (linear codes)<br>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

## Falcon X4 Imager 1D Linear CCD

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

# Falcon X4 Imager 2D SR

| Resolution (mils)/ Barcode Type | Far Guaranteed 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 |

# Falcon X4 Imager 2D DL

| Resolution (mils)/<br>Barcode Type | Far Guaranteed Working<br>Ranges |
| --- | --- |
| 3 mils<br>Code 39 | 6.5 in<br>16.5 cm |
| 5 mils<br>Code 39 | 8.27 in<br>21 cm |
| 10 mils<br>Datamatrix | 7.09 in<br>18 cm |
| 13 mils<br>EAN13 | 12.99 in<br>33 cm |
| 15 mils<br>Datamatrix | 9.06 in<br>23 cm |
| 20 mils<br>Code 39 | 20.87 in<br>53 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%<br><br>EAN 13<br><br>8 012345 000012 |
| 80%<br><br>EAN 8<br><br>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 <br><br>  <br><br> Example |
| Inverse Datamatrix ECC200 <br><br>  <br><br> Example |

# NOTES

# Maintenance

## Cleaning the Device

Periodically clean the Falcon 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.

⚠️ **CAUTION**

**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.
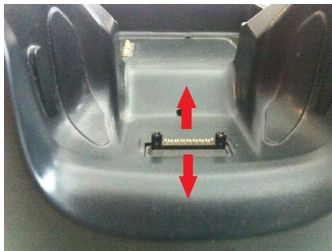


4. Use a dry cloth to remove any dirt near the contacts area and to clean the plastic parts. If the plastic parts of the equipment are very dirty, slightly dampen the cloth with only water.

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

**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.**

**CAUTION**

- 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 Falcon 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 15.

- Use only the components and accessories supplied by the manufacturer for the specific Falcon X4 being used.

- Do not attempt to disassemble the Falcon 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 Falcon X4, disposal must be performed in compliance with the laws in force in your jurisdiction.

- Do not submerge the Falcon 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 Falcon 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)
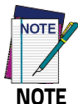
> **NOTE**
>
> **The artwork below may be only a draft. Please refer to the label attached to the product for information about certification marks.**

| 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.

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

**WARNING**

## 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

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

**ATTENZIONE**

**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 descritas 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.

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

**ATENCIÓN**

# 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) $C \in$

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

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

| fi<br>Suomi<br>[Finnish] | Datalogic S.r.l. vakuuttaa täten että Falcon X4 tyyppinen laite on direktiivin 2014/53/EU - 2011/65/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
|---|---|
| sv<br>Svenska<br>[Swedish] | Härmed intygar Datalogic S.r.l. att denna Falcon 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: U4GFX4WB<br>IC: 3862E-FX4WB<br>HVIN: FX4 WB HH<br><br>MADE IN VIETNAM (块/在济津) | FCC ID: U4GFX4WB<br>IC: 3862E-FX4WB<br>HVIN: FX4 WB GUN<br><br>MADE IN VIETNAM (块/在济津) |

# 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

Falcon 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<br>• SISO 20MHz channels bandwidth (HT-20)<br>• MIMO support 20MHz channels bandwidth (HT-20) | 2.4GHz Frequency Bands:<br>2.412 – 2.472 MHz | 19.54 dBm |
| WLAN IEEE 802.11a/n<br>• SISO 20MHz and 40Mhz channels bandwidth (HT-20 and HT-40) | 5GHz Frequency Bands:<br>5.180 – 5.240 MHz<br>5.260 – 5.320 MHz<br>5.500 – 5.700 MHz<br>5.735 – 5.825 MHz (US only) | 16.66 dBm |
| Bluetooth® V4.0 – EDR/LE | 2402-2480Mhz | 9.64 dBm |

# US and Canada

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

# WEEE Compliance



### 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 Falcon 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.

## 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.

## 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.

**ODATALOGIC**

**www.datalogic.com**

822003990          (Rev A)          Jan. 2020