

 **DATALOGIC**

**DL-AXIST**

Personal Digital Assistant (PDA)



**User's Manual**

## **Datalogic ADC S.r.l.**

Via S. Vitalino, 13  
40012 Lippo di Calderara di Reno  
Bologna - Italy  
Telephone: (+39) 051-3147011  
Fax: (+39) 051-3147205

## **©2016 Datalogic ADC S.r.l.**

An Unpublished Work - All rights reserved. No part of the contents of this documentation or the procedures described therein may be reproduced or transmitted in any form or by any means without prior written permission of Datalogic ADC S.r.l. or its subsidiaries or affiliates ("Datalogic" or "Datalogic ADC"). Owners of Datalogic products are hereby granted a non-exclusive, revocable license to reproduce and transmit this documentation for the purchaser's own internal business purposes. Purchaser shall not remove or alter any proprietary notices, including copyright notices, contained in this documentation and shall ensure that all notices appear on any reproductions of the documentation.

Should future revisions of this manual be published, you can acquire printed versions by contacting your Datalogic representative. Electronic versions may either be downloadable from the Datalogic website ([www.datalogic.com](http://www.datalogic.com)) or provided on appropriate media. If you visit our website and would like to make comments or suggestions about this or other Datalogic publications, please let us know via the "Contact Datalogic" page.

### **Disclaimer**

Datalogic has taken reasonable measures to provide information in this manual that is complete and accurate, however, Datalogic reserves the right to change any specification at any time without prior notice.

Datalogic and the Datalogic logo are registered trademarks of Datalogic S.p.A. in many countries, including the U.S.A. and the E.U. DL-Axist™ and SoftSpot are trademarks of Datalogic S.p.A. or of Datalogic Group companies. The Bluetooth word mark and logos are owned by Bluetooth SIG, Inc. and any use of such marks by Datalogic Group companies is under license. Android™ is a trademark of Google Inc. All other brand and product names are trademarks of their respective owners.

### **Patents**

Patent. See [www.patents.datalogic.com](http://www.patents.datalogic.com) for patent list.



# Table of Contents

<b>Introduction</b> .....	<b>1</b>
Conventions .....	1
Product Presentation .....	2
Available Models .....	3
Out of the Box .....	4
General View .....	5
Front View .....	5
Back View .....	6
Side View .....	7
Top View .....	7
Bottom View .....	7
Accessories .....	8
<b>Battery</b> .....	<b>9</b>
Install the Battery .....	9
Charge the Battery .....	12
Charge with USB .....	12
Charge with the dock .....	14
Replace the Battery .....	19
<b>SD Card/ SIM Card</b> .....	<b>21</b>
Install the microSD Card .....	21
Install the SIM Card .....	24
<b>Getting Started</b> .....	<b>27</b>
Power Button .....	27
Power On .....	27
Suspend Mode .....	27

---

Long Press Power Menu .....	28
Home Screen .....	35
Home Screen Items .....	36
Customize the Home Screen .....	36
Virtual Keyboard .....	38
Applications .....	39
Resetting the Terminal .....	42
Configuration Reset .....	42
Device Reset .....	44
LED Indicators .....	45
<b>Settings .....</b>	<b>47</b>
Overview .....	47
Scanner Settings .....	48
Notification .....	49
Good Read .....	52
Formatting .....	53
Scanner Options .....	56
Wedge .....	59
Symbology Settings .....	61
Global Settings .....	63
Wi-Fi Settings .....	65
Connect to Wi-Fi Network .....	65
Bluetooth Settings .....	70
Enable Bluetooth® .....	70
Connect to Other Bluetooth@ Devices .....	72
Configure, Rename or Unpair Bluetooth@ Devices .....	73
Ethernet Configuration .....	75
NFC Settings .....	77
Enable NFC .....	77
System Upgrade .....	79
Local Upgrade .....	79

---

Recovery Mode .....	84
Advanced Settings .....	85
Suspend Timeout .....	85
Wake-Up Configuration .....	88
Input Configuration .....	88
About Phone .....	96
<b>Datalogic Applications .....</b>	<b>99</b>
Desktop Configuration Utility (DXU) .....	99
How DXU Works .....	100
Installation .....	102
Controls .....	103
Tasks .....	122
SoftSpot™ .....	155
Tap2Deploy .....	158
Create pairing tag .....	161
Advanced Tag Writer .....	165
Settings .....	168
Restart Connection .....	168
About .....	169
<b>Tools.....</b>	<b>171</b>
USB ADB Driver & USB CD-ROM .....	171
SDK Add-on .....	172
Install SDK Add-on .....	172
Install Android™ Studio .....	176
Install Android SDK .....	177
Install ADB Driver .....	178
Create a New Application with Android Studio .....	180
SureLock .....	181
SureFox .....	182
<b>Connections .....</b>	<b>183</b>
USB Connection .....	183

---

---

USB Direct Connection .....	183
USB Dock Connection .....	184
Ethernet Connection .....	185
Ethernet Dock Connection .....	185
WLAN Connection .....	186
MIMO (Multiple-Input and Multiple-Output) .....	187
WWAN Connection .....	188
WPAN Connection .....	190
Near Field Communication (NFC) .....	192
Read NFC Tags .....	192
Wireless and Radio Frequencies Warnings .....	193
<b>Data Capture.....</b>	<b>197</b>
Imager Data Capture .....	197
<b>Technical Features.....</b>	<b>199</b>
Technical Data .....	199
Decode Distances .....	202
<b>Test Codes.....</b>	<b>203</b>
<b>Maintenance.....</b>	<b>211</b>
Cleaning .....	211
Ergonomic Recommendations .....	211
<b>Safety and Regulatory Information .....</b>	<b>213</b>
General Safety Rules .....	213
Power Supply .....	214
Laser Safety .....	215
LED Class .....	223
Audio Safety .....	223
Canadian Statement .....	224
Radio Compliance .....	224
Information for the User .....	227
FCC Compliance .....	228
FCC Interference Statement .....	228

---

---

Industry Canada Compliance .....	231
SAR Compliance .....	234
SAR Information (for European Union) .....	235
FCC SAR values .....	235
Body-worn Operation .....	235
European Union Regulatory Notice .....	236
WEEE Compliance .....	237
<b>Reference Documentation.....</b>	<b>239</b>
<b>Services and Support .....</b>	<b>241</b>
Warranty Terms and Conditions .....	242
<b>Glossary.....</b>	<b>243</b>

---

# NOTES



# Introduction

## Conventions

This manual uses the following conventions:

'PDA', 'terminal', 'device' and 'DL-Axist' refer to the DL-Axist PDA.

'Dock' and 'Single Dock' refer to the DL-Axist Single Slot Dock.

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

## Product Presentation

The DL-Axist PDA combines Datalogic expertise, the latest mobile technologies and user friendly experience in a complete package.

An appealing look and feel and a brilliant full touch 5" HD screen are combined with industrial robustness to survive indoor and outdoor usage. The PDA also leverages an additional protective rubber boot and Gorilla® Glass 3 screen to ensure ruggedness.

The DL-Axist PDA is equipped with a 2D imager allowing quick and easy data capture from high density codes to the standard range distances, along with Datalogic's patented 'Green Spot' technology for good-read feedback with a fast aimer. For applications requiring evidence of task execution or damaged documentation, a 5 MP autofocus camera with a built-in LED flash provides easy documentation with photos. Moreover, this PDA embeds Datalogic's proprietary 'SoftSpot™' technology: a user-definable 'floating soft trigger' to leverage the large touch display, allowing a new triggering experience for the user.

The DL-Axist PDA leverages five embedded wireless technologies: Wi-Fi 802.11 a/b/g/n Cisco CCXv4 certified for quick network access and with superior MIMO technology (ensures higher throughput and better coverage), 3G/4G for real-time wide area voice and data coverage, Enterprise Class Assisted GPS (A-GPS) for location based applications, Bluetooth® wireless technology v4 for fast and low power consuming data connections and NFC for easy and intuitive configuration and pairing.

The embedded Android™ operating system (the leading OS for mobile devices) is complemented by a suite of tools enabling Enterprise level security, fast deployment and easy management, thus helping to maximize the users' ROI.

## Available Models

The DL-Axist is available in different models depending on the options it is equipped with. All options are listed below:

- 944600001 DL-Axist Full Touch PDA, 802.11 a/b/g/n+MIMO, Bluetooth v4 & NFC, 1GB RAM/8GB Flash, Multi-purpose 2D Imager w Green Spot, Android v4
- 944600003 DL-Axist Full Touch PDA, 3G/4G HSPA+ WW/no US, 802.11 a/b/g/n, Bluetooth v4 & NFC, 1GB RAM/8GB Flash, Multi-purpose 2D Imager w Green Spot, Android v4
- 944600005 DL-Axist Full Touch PDA, 3G/4G HSPA+ US, 802.11 a/b/g/n, Bluetooth v4 & NFC, 1GB RAM/8GB Flash, Multi-purpose 2D Imager w Green Spot, Android v4

For further details about the DL-Axist models refer to the web site:

<http://www.datalogic.com>.

For further information regarding Android refer to the website:

[www.android.com](http://www.android.com).

## Out of the Box

The DL-Axist package contains:

- DL-Axist (device)
- Rechargeable battery
- USB charge/communication cable
- Battery Box (for spare battery)
- Quick Start Guide
- Safety & Regulatory Addendum
- EULA sheet

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



**CAUTION**

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

# General View

## Front View



## Back View



## Side View



## Top View



## Bottom View



## Accessories

### Docks

94A150071	DOCK, SINGLE SLOT, DL-AXIST
94A150072	DOCK, ETHERNET SINGLE SLOT, DL-AXIST
94A150074	CHARGER, 4 SLOT BATTERY, DL-AXIST

### Batteries

94ACC0128	BATTERY, STANDARD CAPACITY, DL-AXIST
94ACC0129	BATTERY, EXTENDED CAPACITY, DL-AXIST

### Power Supplies

94ACC0135	POWER SUPPLY, MICROUSB, DL-AXIST
94ACC0136	POWER SUPPLY, SINGLE SLOT DOCK, DL-AXIST
94ACC0137	POWER SUPPLY, 4 BATTERY CHARGER, DL-AXIST

### Various

94ACC0130	STD BATTERY DOOR, DL-AXIST
94ACC0131	EXT BATTERY DOOR, DL-AXIST
94ACC0132	RUBBER BOOT, DL-AXIST
94ACC0133	HANDSTRAP, DL-AXIST
94ACC0134	STYLUS, DL-AXIST (10 PCS)
94ACC0144	CABLE, MICROUSB, DL-AXIST



# Battery

## Install the Battery

To install the battery pack, follow the steps below:

1. Rotate the latches to the open position:



2. Grab the battery cover by the sides and lift it out of the way:



3. Remove the battery pack from the battery box\*. Insert the battery pack into the slot, top (contacts) side first, and press it into place:



4. Insert the battery cover, bottom first, and press it into place:



\* Always use the battery box to carry the battery pack. Do not put the battery pack in your pocket.

5. Rotate the latches to the lock position to lock the cover:



6. Press and release the power button to turn the DL-Axist on.

## Charge the Battery

The DL-Axist battery pack is not initially fully charged. After installing the battery, charge it with the USB cable or with the single dock.

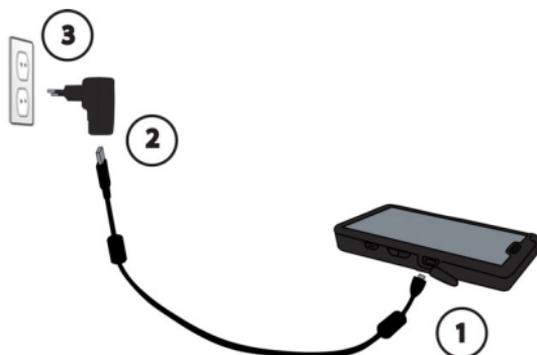


**Charge the battery for a minimum of 4 hours for the standard battery and 8 hours for the extended battery.**

During the charging process the charging LED positioned at the top left side of the display glows red constantly. Once the charging process has been completed, the charging LED glows green constantly.

### Charge with USB

You can use the provided USB charge/communication cable in conjunction with the power supply adapter (p/n 94ACC0135) to charge the terminal from a power outlet. To prevent the risk of short-circuiting, first connect the USB cable to the DL-Axist micro USB port, and then connect the USB cable to the power adapter.





**NOTE**

Use only a Datalogic approved power supply.

## Charge with the dock

The dock provides power to the DL-Axist and allows the charging of the battery.



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



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

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



**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.**

**WARNING**

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 batteries usagées conformément aux instructions.

**NOTE**

Even if the storage temperature range is wider, in order to achieve the longest battery life, store the terminal and the spare batteries between 20 to 30°C (68 to 86°F).

Charging is allowed in the battery temperature range from 0°C to 45°C.

**NOTE**

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

**NOTE**

To maximize operating autonomy, the DL-Axist checks its battery level at all times. If the battery is not sufficiently charged, the DL-Axist will not turn on when the ON/OFF Power button is pressed.

In this case, either substitute with a charged battery, insert the DL-Axist into a powered dock, or plug it into a wall charger.



**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 and/or fire.

Use the battery box to carry the battery pack, do not put the battery pack in your pocket.

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.

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.

**WARNING**

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 terminal.

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 color or shape, or appears abnormal in any other way.

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.



**WARNING**

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.

Before replacing the battery pack, turn off the device or put it in swap battery mode (see "[Swap Battery](#)" on [page 29](#)).

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.

## Replace the Battery

To replace the battery pack, follow the steps below:

1. Turn off the DL-Axist, or put it in **Swap Battery** mode (see [‘Swap Battery’](#) on page -29).
2. Rotate the latches to the open position:



3. Grab the battery cover by the sides and lift it out of the way:



4. Remove the battery by pulling the tab on the bottom of the battery:



5. Insert the new battery pack into the slot (see [‘Install the Battery’](#) on page -9, steps 3 to 6).



## SD Card/ SIM Card

### Install the MicroSD Card

DL-Axist supports microSD memory cards. To access the microSD card slot and insert the card follow the steps below:

1. Turn off the DL-Axist or put it in **Swap Battery** mode (see '[Swap Battery](#)' on page -29
2. Remove the battery pack (see '[Replace the Battery](#)' on page -19, steps 1 to 4).
3. Lift the retaining door:



- Slide the memory card holder to the left to unlock it. Lift the holder:



- Insert the memory card into the holder. Make sure the contacts side is face down:



- Close the holder and shift it to the right to lock it:



7. Close the retaining door.
8. Insert the battery pack into the slot (see [‘Install the Battery’](#) on page -9, steps 3 to 6).

### **Remove the microSD Card**

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

## Install the SIM Card

A SIM card stores the subscriber's personal information, GSM/GPRS radio settings, security keys, contacts, etc. SIM cards can be installed in compatible mobile devices, enabling you to switch devices without losing personal and setup information.

To access the SIM card slot and insert the card follow the steps below:

1. Turn off the DL-Axist or put it in **Swap Battery** mode (see '[Swap Battery](#)' on page -29)
2. Remove the battery pack (see '[Replace the Battery](#)' on page -19, steps 1 to 4).
3. Lift the retaining door:



4. Slide the SIM card holder to the left to unlock it. Lift the holder:



5. Insert the SIM card into the holder. Make sure the contacts side is face down:



6. Close the holder and shift it to the right to lock it:



7. Close the retaining door.
8. Insert the battery pack into the slot (see ['Install the Battery' on page -9, steps 3 to 6](#)).

## Remove the SIM Card

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

# NOTES



# Getting Started

## Power Button

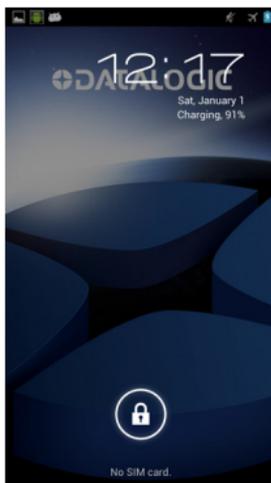
### Power On

The DL-Axist turns on when a charged battery pack is inserted.

### Suspend Mode

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

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

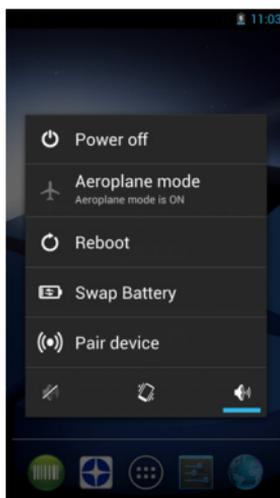


To unlock the home screen, tap and drag the **Lock** icon to the right side of the screen.

To set the timeout limit, see ‘Suspend Timeout’ on page -85.

## Long Press Power Menu

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



### Power Off

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

### Airplane Mode

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

### Reboot

Tap **Reboot** to perform a Soft Reset (see ‘Soft Reset’ on page -44).

## Swap Battery

Swap Battery mode is a low power suspend mode that allows you to replace the battery pack without closing files and applications. It maintains the main memory contents and keeps applications running but does not allow you to operate any of the device's functions.

To switch to Swap Battery mode:

1. Tap **Swap Battery**.
2. Wait for the red Logo indicator to turn off.
3. Replace the battery (see '[Replace the Battery](#)' on page -19).
4. Press and release the power button to resume your session.

## Pair Device

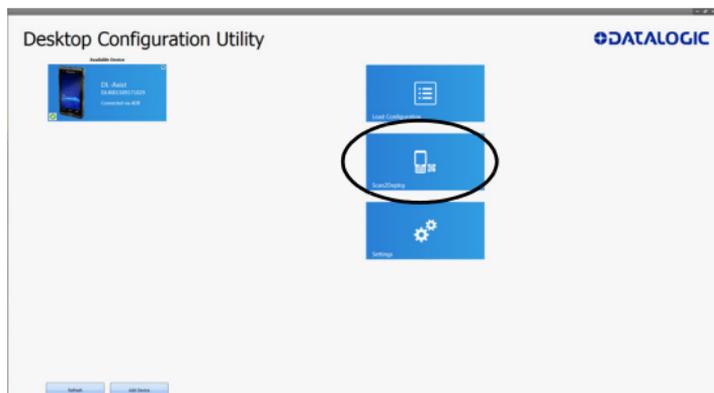
**Scan2Pair** and **Tap2Deploy** allow to start a pairing session with a PC via DXU software.

DXU is the Datalogic system application for device configuration and firmware upgrade from a Windows PC. See "[Desktop Configuration Utility \(DXU\)](#)" on page 99 for further information.

### Scan2Pair

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

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

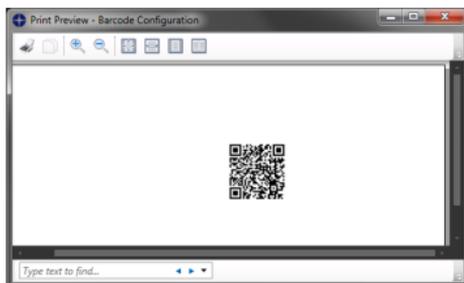


From the **Wi-Fi Configuration** window you can select the barcode type and set the Wi-Fi and pairing configuration data.

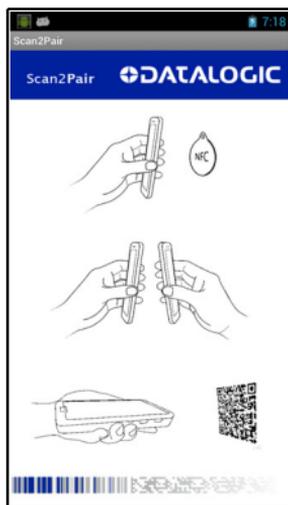
Tap **Print** to create the barcode; tap **Save** to save it on your hard disk:



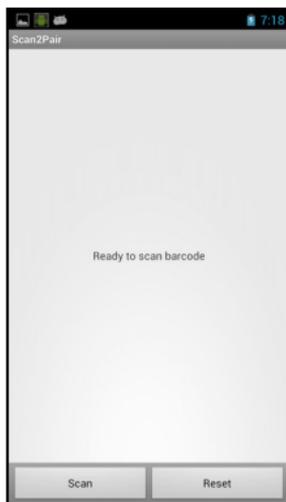
If you select **Print**, the barcode displays on the screen:



From DL-Axist's **Long Press Power Menu**, tap **Pair Device** > **Scan2Pair**. Tap anywhere on the screen:



Tap **Scan** to read the barcode:



### Tap2Deploy (NFC)

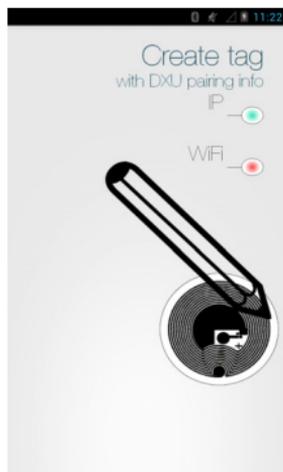
Starts a pairing with DXU by reading an NFC tag containing the configuration data of your PC.

The tag is automatically created by connecting the DL-Axist to your PC using the dock or the USB cable.

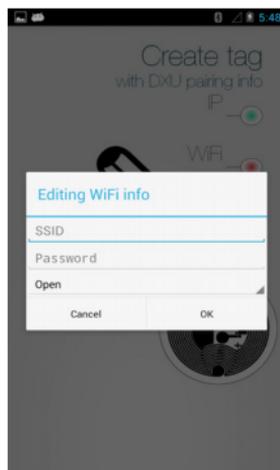
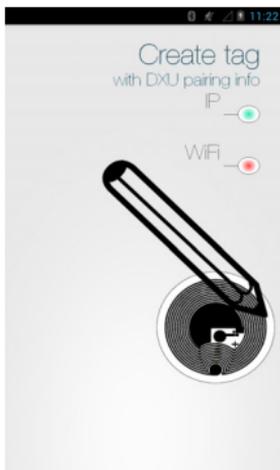
Alternatively, from DL-Axist's **Long Press Power Menu**, tap **Pair Device > Tap2Deploy > Pair with DXU > Create Pairing Tag**:



Tap **IP** to set the IP address and the port number:

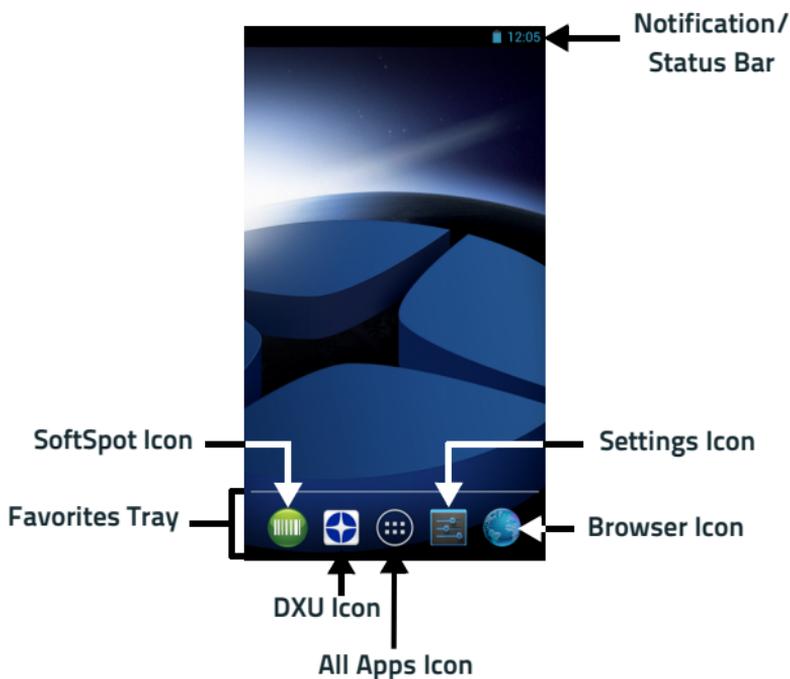


Tap **WiFi** to set the Wi-Fi info:



For further information, see [“Tap2Deploy”](#) on page -158.

# Home Screen



## Home Screen Items

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

## Customize the Home Screen

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

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

### To add an application shortcut:

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

### To add a widget:

1. Tap the **All Apps** icon.

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

**To create a folder:**

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

Tap the folder.

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

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

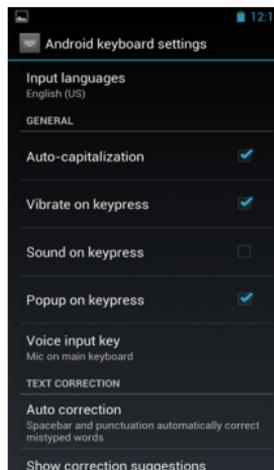
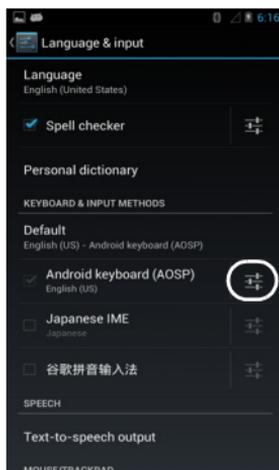
To delete items:

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

## Virtual Keyboard

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

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



## Applications

The **All Apps** screen displays icons for all installed applications. The table below lists the default applications installed on the DL-Axist.

Icon	Description
	AnExplorer - Another Material File Manager you can use to easily find, browse, move, compress, and otherwise manage your apps.
	Browser - Use to access the Internet or intranet.
	Calculator - Provides the basic and scientific arithmetic functions.
	Calendar - Use to manage events and appointments.
	Camera - Take photos or record videos.
	Clock - Use to schedule alarms for appointments or as a wake-up.
	Downloads - Lists all downloads files.
	DXU Agent - Launch to start a pairing with DXU by reading a barcode containing the configuration data of your PC (see ' <a href="#">Desktop Configuration Utility (DXU)</a> ' on page -99).

Icon	Description
	Email - Use to send and receive email.
	Enterprise Agent- Enhances the lockdown functionalities of SureLock and SureFox to ensure advanced device security (see 'SureLock" on page -181 and SureFox on page 182).
	Gallery - Use to view photos stored on the internal storage memory and on the microSD card.
	Movie Studio - Create movie videos.
	Music - Play music stored on the internal storage memory and on the microSD card.
	People - Use to manage contact information.
	Phone - Use to make phone calls.
	Scan2Pair – Enables 2D imager data capture (see 'Imager Data Capture" on page -197).
	Scanner – Enables data capture (see 'Data Capture" on page -197).
	Search - Use the Google search engine to search the Internet and the DL-Axist.

Icon	Description
	Settings - Use to configure the DL-Axist (see ' <a href="#">Settings</a> ' on page -47).
	SoftSpot - A configurable application meant to provide easy access to frequently used functionalities (see ' <a href="#">SoftSpot™</a> ' on page -155).
	Sound Recorder - Use to record audio.
	SureFox - Use to controls web access for the users (see " <a href="#">SureFox</a> " on page 182).
	SureLock - Use to secure and lock your device (see " <a href="#">SureLock</a> " on page 181).
	Tap2Deploy - Use to enable NFC pairing (see ' <a href="#">Tap2Deploy</a> ' on page -158).

# Resetting the Terminal

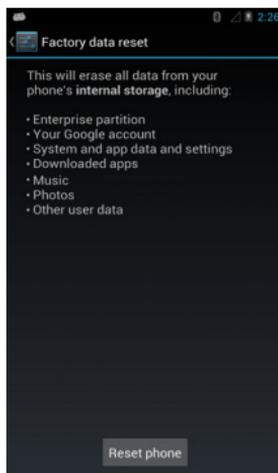
## Configuration Reset

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

### Factory Reset

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

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

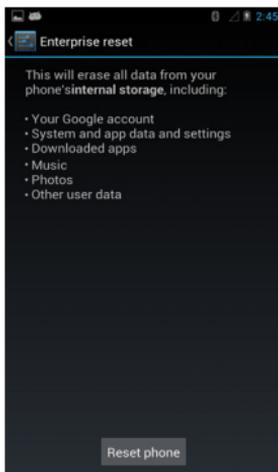


## Enterprise Reset

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

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

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



## Device Reset

Device reset restarts the device.

### Soft Reset

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

1. Press and hold the **Power** button.
2. Tap **Reboot**.
3. The device shuts down and then reboots.

### Hard Reset

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

Simultaneous press and hold the following buttons:

- **Power button**
- **Left trigger**
- **Search button**

## LED Indicators

The LEDs illuminate to indicate various functions or errors on the reader. The following tables list these indications. The good read LED indicator is programmable, and may or may not be turned on (see 'Scanner Settings' on page -48 for more details).

LED	Status	Description
Charging LED	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.
Good Read LED	Red	Light is red from the time the user presses the scan key until the barcode is decoded, until the scanner times out, or until the user releases the scan key.
	Green	Light changes to green when a good decode is completed.

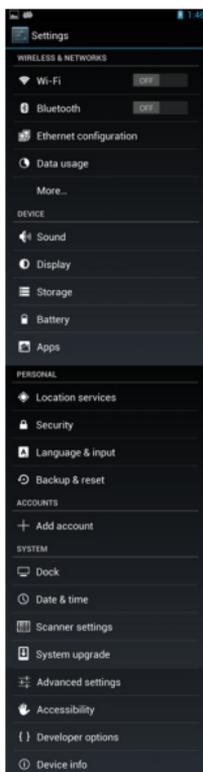
# NOTES



# Settings

## Overview

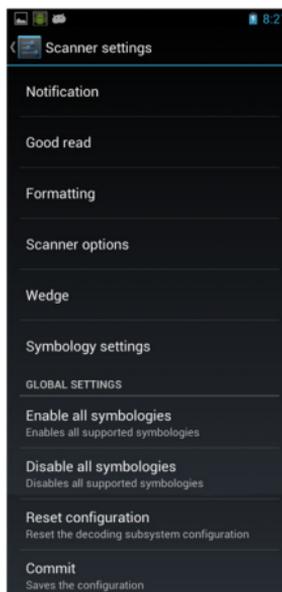
The **Settings** app allows you to check or set system parameters to customize your device. Tap **Settings** or pull down the notification panel and then tap the **Settings** icon next to the date:



## Scanner Settings

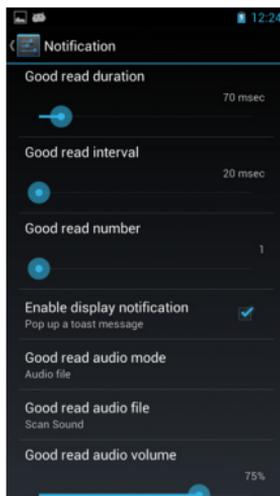
Before you start reading barcodes, use the **Settings** app to view and configure all settings for the scanner.

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



## Notification

Use it to configure the good read LED, green spot, tone and vibration notification:



### Good read duration

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

### Good read interval

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

### Good read number

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

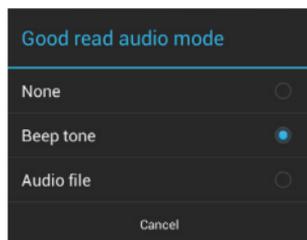
## Enable display notification

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

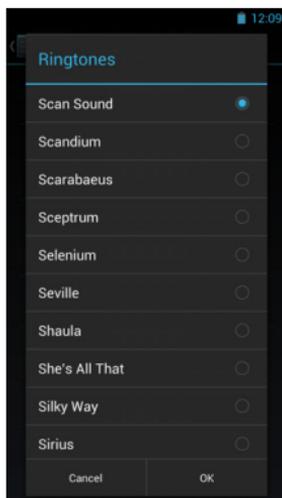
## Good read audio mode

Sets the audio tone to:

- None
- Beep tone
- Audio file



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



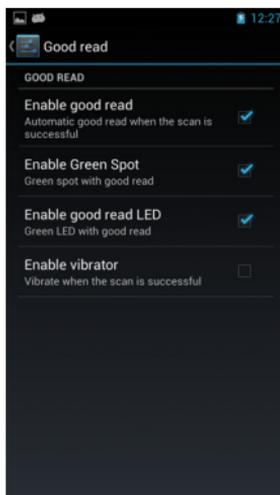
**The Notification settings do not apply to an audio file.**

## Good read audio volume

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

## Good Read

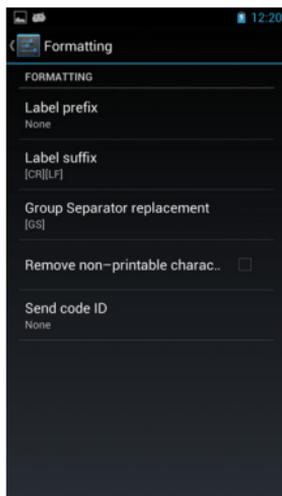
Use it to enable good read notifications (LED, Green Spot, Vibrator):



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

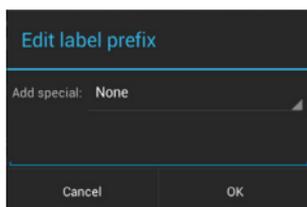
## Formatting

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



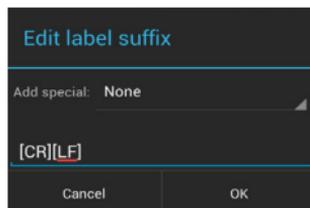
### Label prefix

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



## Label suffix

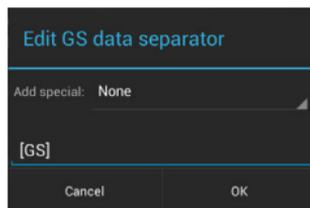
Tap **Label suffix** to enter the characters you will be using as suffix. Tap **Add special** to select a special character to be added in the current cursor position:



## Group Separator replacement

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

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

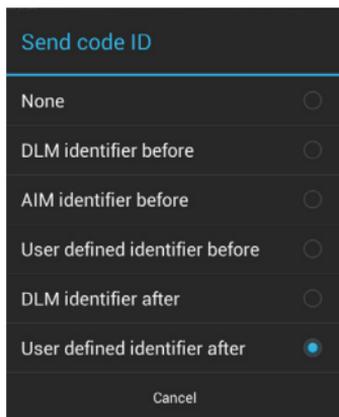


## Remove non-printable characters

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

## Send code ID

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



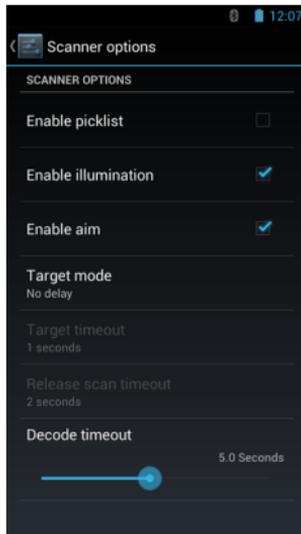
The AIM ID (Association for Automatic Identification and Mobility) is an international barcode identifier. When **AIM identifier before** is enabled, the AIM ID is inserted at the beginning of the decoded barcode.

**DLM identifier** is a Datalogic specific character identifier.

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

## Scanner Options

Tap **Scanner Options** to customize the DL-Axist scanning behavior.



### Enable picklist

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

### Enable illumination

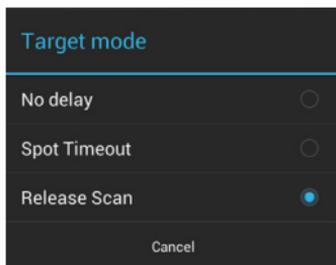
If selected, it causes the scanner to turn on the illumination to aid decoding.

### Enable aim

Enables the laser aim.

## Target mode

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

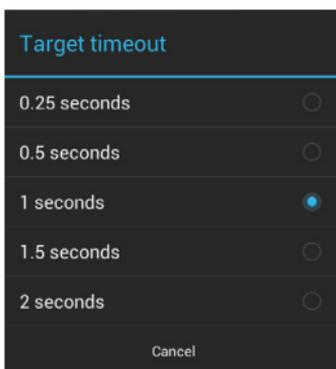


### No delay

Target mode is disabled.

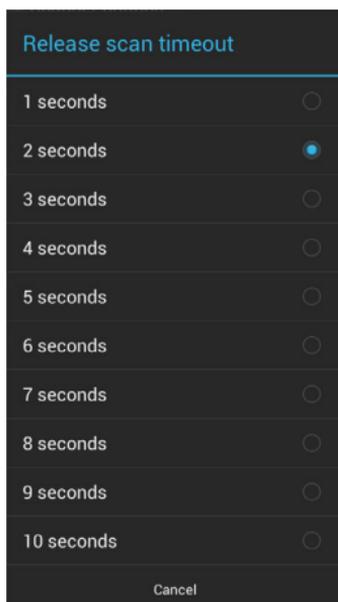
### Spot Timeout

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



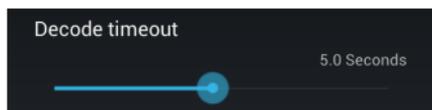
## Release Scan

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



## Decode timeout

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



## Wedge

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



### Enable keyboard wedge

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

### Keyboard wedge only on focus

Provides a safer way to input keystrokes into the foreground app. It allows to send captured data in the form of key events only to the current text area with active keyboard input.

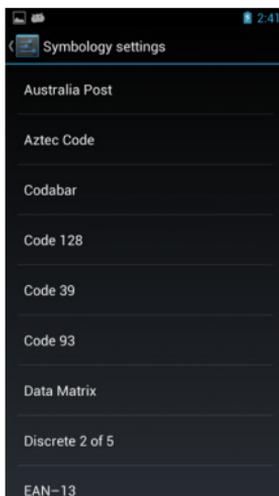
If this setting is not enabled, keystrokes will be always dispatched to the foreground application.

### **Enable intent wedge**

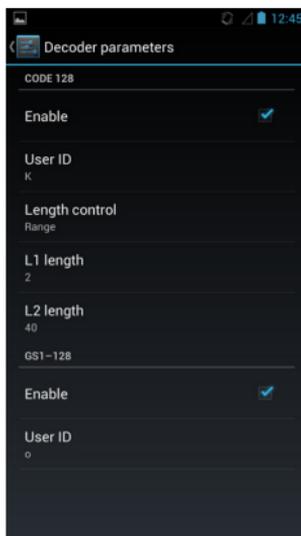
Enables the broadcast of specific intents to the listening applications. The broadcasted intent can have its custom Action, Category and extra content fields. The scanner is enabled whenever the intent option is flagged.

## Symbology Settings

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

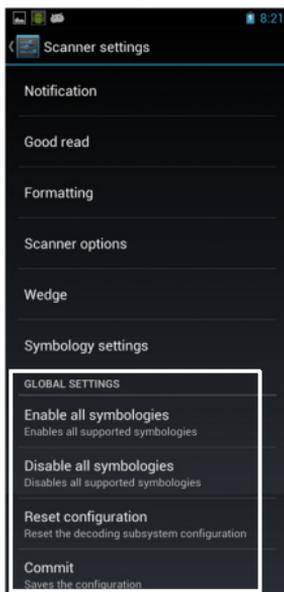


Refer to the sample symbology control panels for examples of the types of fields and options you can modify. The sample below shows the settings of a Code 128 barcode symbology:



## Global Settings

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



### Enable all symbologies

Enables all barcode symbologies.

### Disable all symbologies

Disables all barcode symbologies.

### Reset configuration

Resets back to default scanner configuration settings.

## **Commit**

Saves the configuration settings to a persistent storage. Any change you make is temporary and will be lost when the system restarts, unless you tap **Commit**.

# Wi-Fi Settings

## Connect to Wi-Fi Network

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



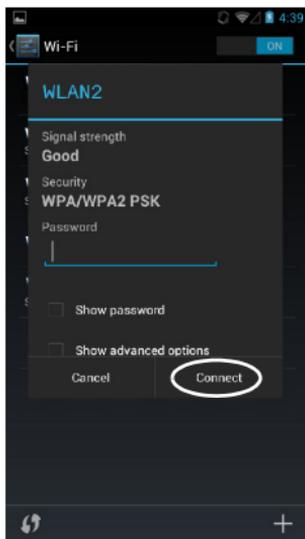
2. Tap **Wi-Fi**. The DL-Axist scans for available wi-fi networks within range and lists them. If the terminal previously connected to a wi-fi network, it automatically reconnects to the same network. Secured networks are indicated with a lock icon:



3. Select the network name you want to connect to from the available network list.
4. If the network is open, tap the profile and then tap **Connect**, or press and hold and then select **Connect to network**:

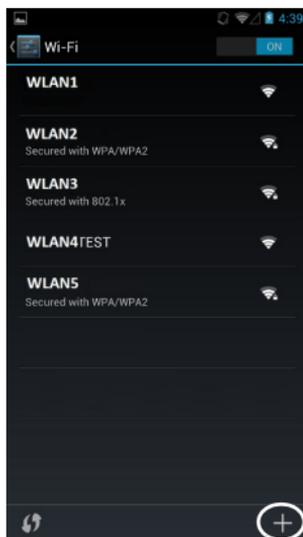


- If the network is secured, a dialog box appears requesting information relevant to the network security protocol (e.g., password, key, or certificate). Enter the required information, then tap **Connect**:

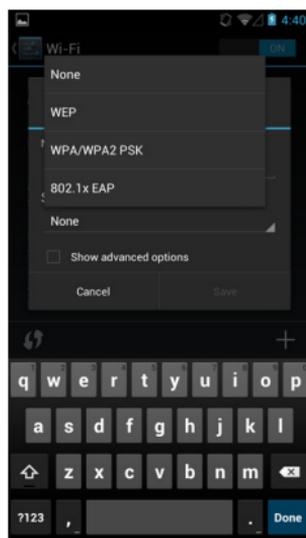
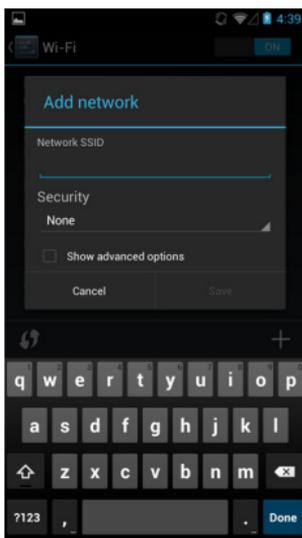


### Add a Wi-Fi Network

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



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



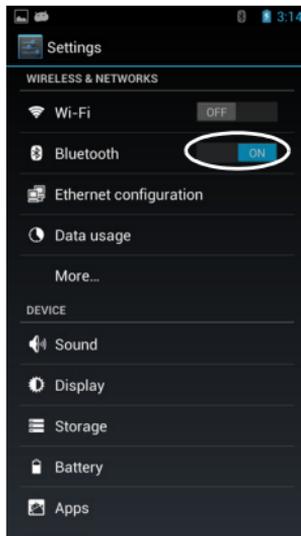
4. Tap **Save**.

# Bluetooth Settings

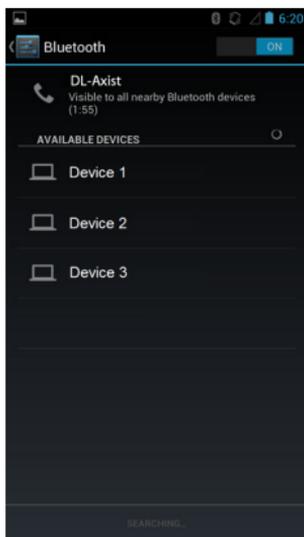
To create a Bluetooth® pairing between your device and another device that has Bluetooth® capabilities, ensure that the two devices are turned on, discoverable, and within close range.

## Enable Bluetooth®

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

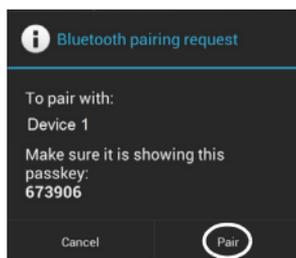


2. Tap **DL-Axist** to make your device visible to other Bluetooth® devices. The device will be discoverable for 2 minutes.



## Connect to Other Bluetooth® Devices

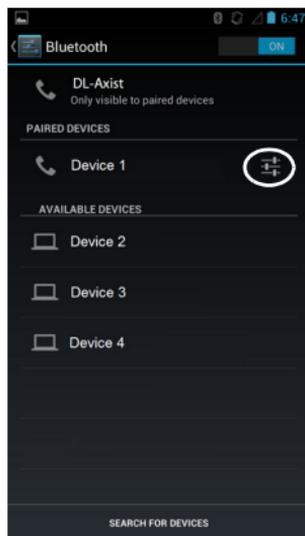
1. Tap **Settings** > **Bluetooth** to search for available Bluetooth® devices. Flick the list and select a device. The **Bluetooth pairing request** dialog box displays on the screen:



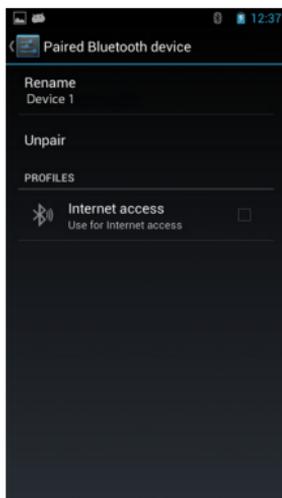
2. Make sure both devices show the same passkey and tap **Pair** on both devices.
3. The selected Bluetooth® device is added to the **Paired Devices** list and a paired connection is established.

## Configure, Rename or Unpair Bluetooth@ Devices

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



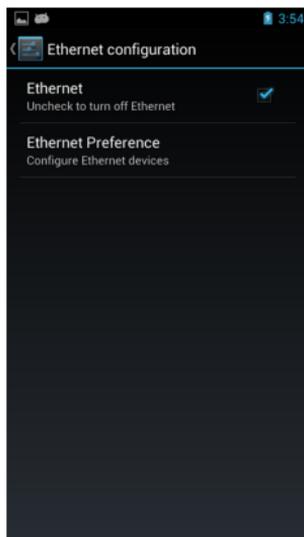
3. Tap **Rename**, **Unpair** or select a different profile from the **Profiles** list available for the paired device:



## Ethernet Configuration

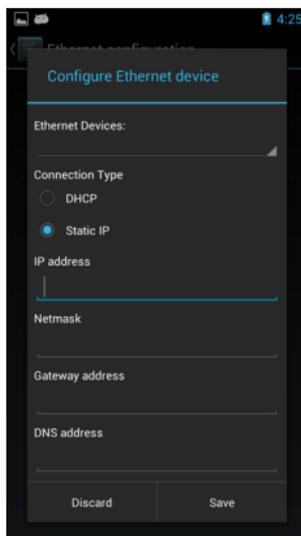
To enable ethernet communication:

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



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

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

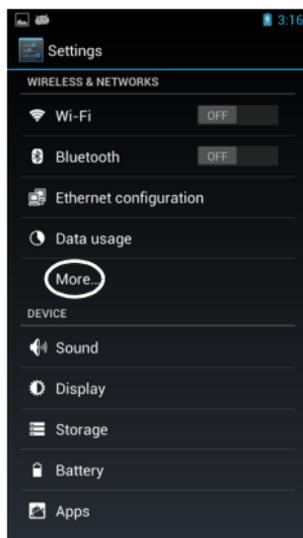


## NFC Settings

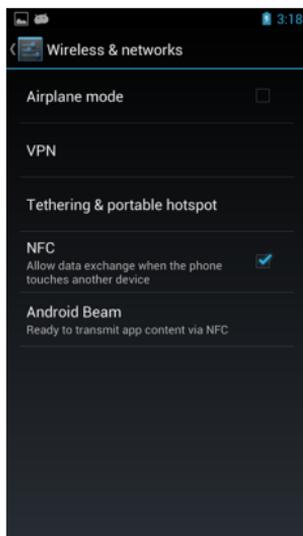
NFC allows data exchanges between the DL-Axist and other NFC devices or tags.

### Enable NFC

1. Tap **Settings** > **More** (under **Wireless & Networks**):



2. Select the **NFC** box to enable short-range wireless data exchange. **Android Beam** is automatically enabled:

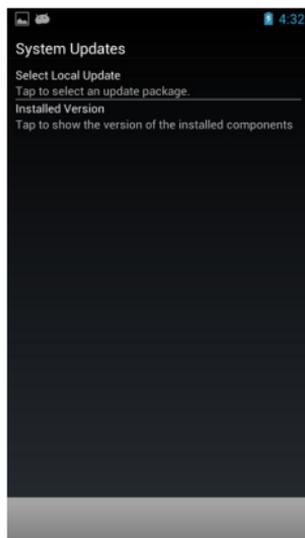


# System Upgrade

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

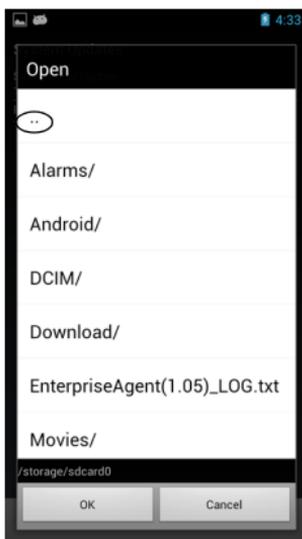
## Local Upgrade

From the **Settings** menu, tap **System upgrade** > **Local upgrade**. The **System Updates** window displays on screen:



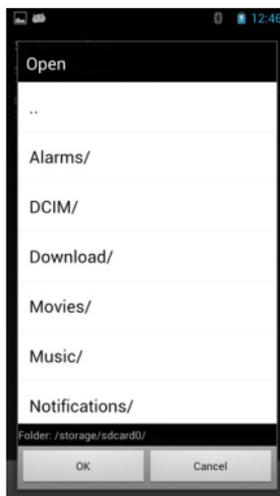
## Select Local Update

Allows you to navigate the file system and select a pre-charged update package:

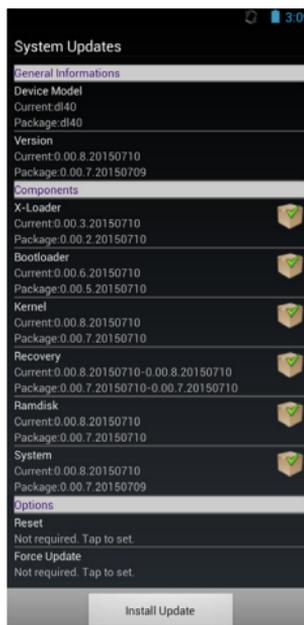


- Tap **sdcard0/** to navigate the internal storage.
- Tap **sdcard1/** to navigate the SD card internal storage.
- Tap **usbdisk/** to navigate the USB disk.

Select the update package you want to install and then tap **OK**:



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



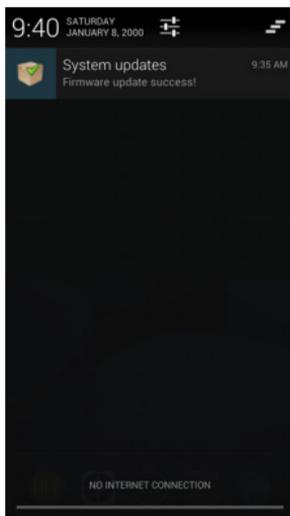
The **General Informations** section shows information about the device model and OS version and the update package version.

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

The **Options** section allows to:

- reset the device after the update (see '[Resetting the Terminal](#)' on page -42)
- force the update of all components, including those already updated.

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



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



**NOTE**

**During the update, ensure that:**

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

**or**

- **the DL-Axist is connected to a power source (USB or dock).**



**NOTE**

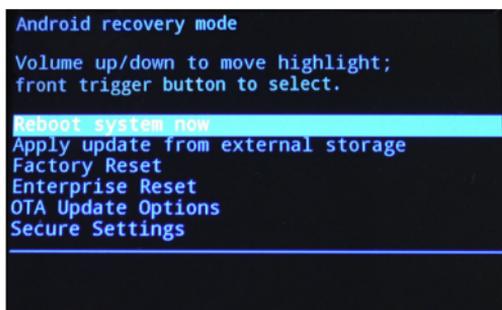
**Update is always done in recovery mode (see “Recovery Mode” on page -84).**

## Recovery Mode

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

To enter **Recovery Menu**:

1. Perform a device reset (see ["Device Reset"](#) on page -44).
2. During reset, press and hold the Search button.
3. The **Recovery Menu** displays on the screen:



4. Use the volume buttons to navigate the menu. You can apply/force updates and perform a configuration reset. Press the front trigger to select.
5. Select **Reboot system now**, then press the front trigger. The device reboots and the reset is complete.



### NOTE

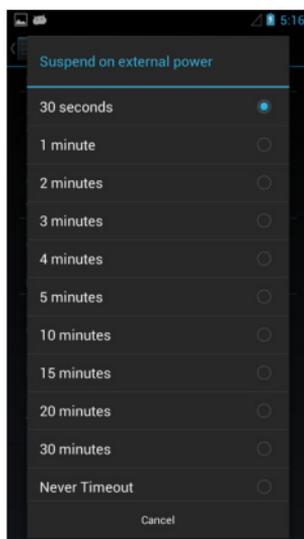
In Recovery mode, you can only apply updates from external storage (see ["Local Upgrade"](#) on page -79).

# Advanced Settings

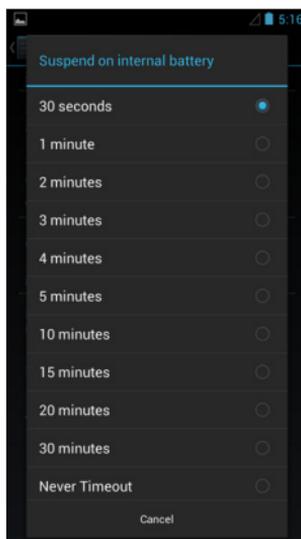
## Suspend Timeout

You have two options to set the suspend timeout (see ‘Suspend Mode’ on page -27 for more information on Suspend Mode):

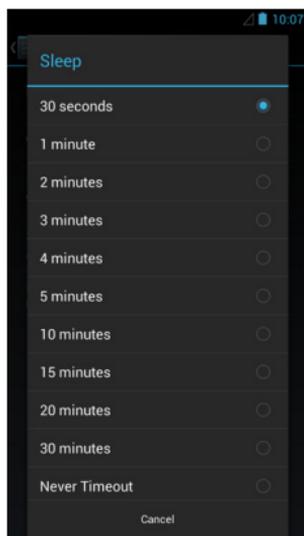
1. Tap **Settings > Advanced settings:**
  - **Suspend on external power** to set the number of seconds without user input activity before the system is suspended while running on external power:



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



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

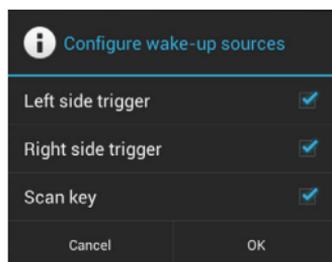


If you use the **Advanced settings** page to set the auto-suspend timeouts, then the **Display** page's **Sleep** control will display the **Suspend on external power** setting the next time you look in the **Display** page.

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

## Wake-Up Configuration

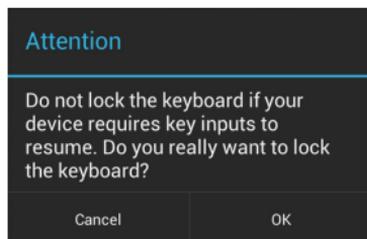
The default wake-up source is the Power button. Tap **Settings > Advanced settings > Configure wake-up sources** to configure other wake-up sources. Possible wake-up buttons are the left, right and front triggers:



## Input Configuration

### Lock Keyboard Input

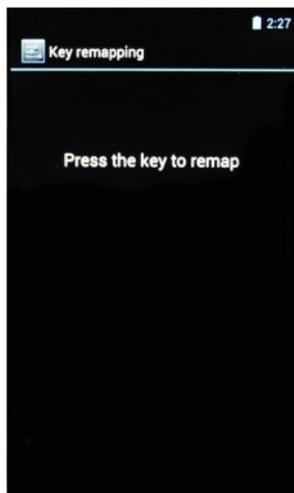
Select **Lock keyboard input** to lock user input from the keyboard. The following pop up windows displays on screen asking for confirmation:



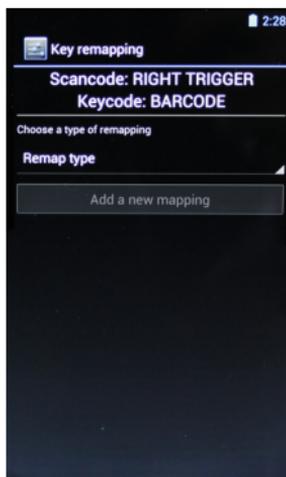
To unlock the keyboard, clear the **Lock keyboard input** check box.

## Key Remapping

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

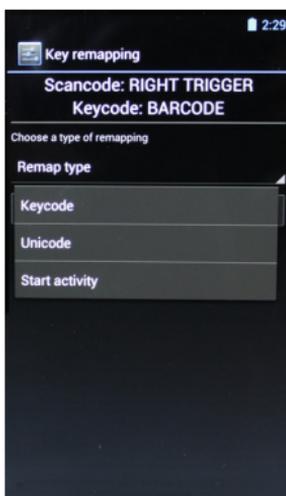


Press the key you want to remap. The following window displays on screen:



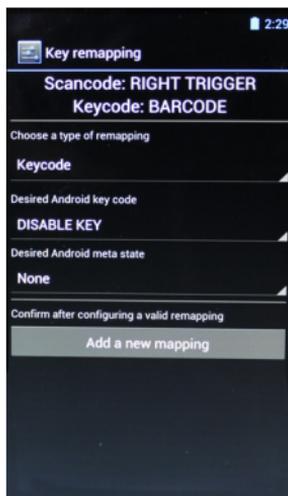
- **Scancode** represents the physical location of a keyboard key.
- **Keycode** represents the value that is mapped to a specific key.

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



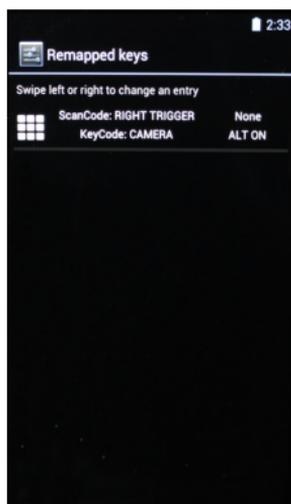
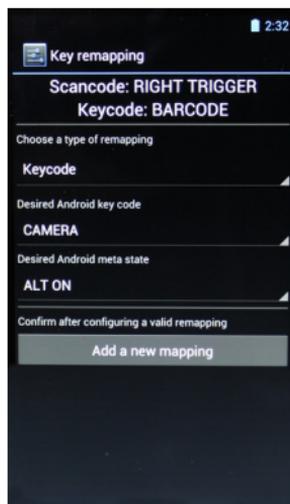
## Keypcode

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



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

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

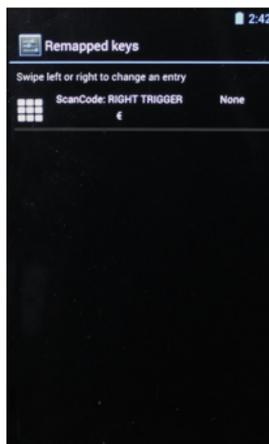


## Unicode

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

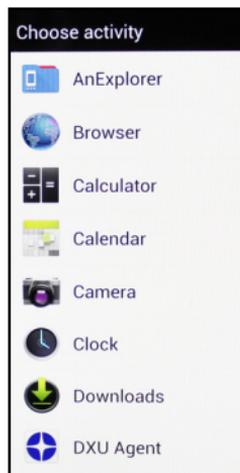
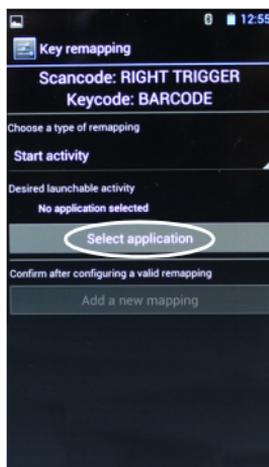


Tap **Add a new mapping**. A window displays showing the new keymap:

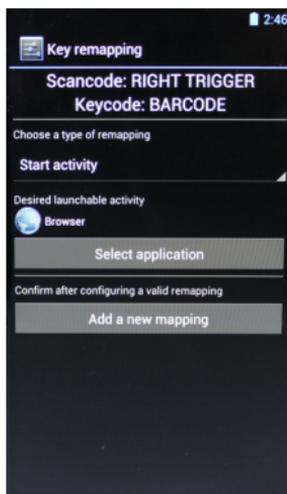


## Start Activity

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

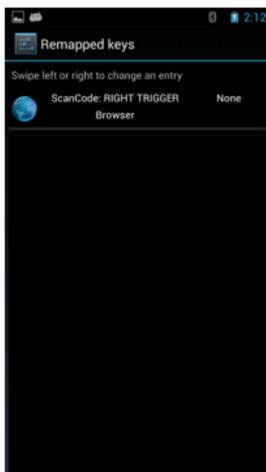


Select the desired application and then tap **Add a new mapping**. A window displays showing the new keymap:



## View all Remapped Keys

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



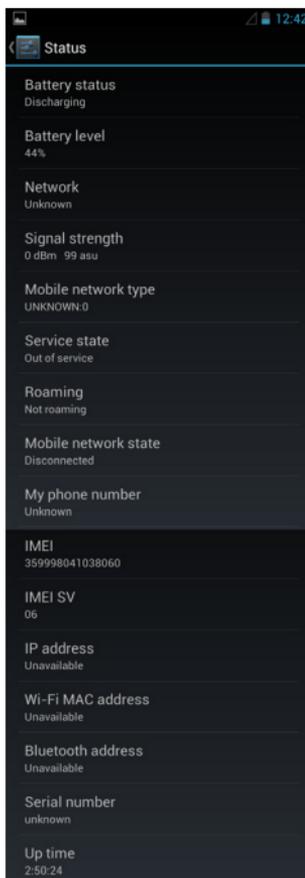
Swipe left or right to edit or remove an entry and reset the key mapping back to default.

## About Phone

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



Tap **Status** to display terminal information including battery, network, roaming, phone number, IMEI, serial number:



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

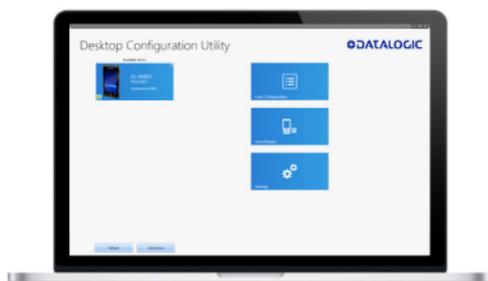
# NOTES



# Datalogic Applications

## Desktop Configuration Utility (DXU)

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



Configure  
devices



Save  
Configurations



Upload  
Configurations



Create  
Scan Codes

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 DL-Axist users can scan to quickly connect to DXU, called Scan2Pair. 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 DL-Axist. 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 DL-Axist 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. DXU supports connecting only to devices in the same subnet as the PC running DXU. When connected to Wi-Fi wireless access points, the DL-Axist can connect to DXU as long as both are on the same subnet. When connected over Ethernet, the DL-Axist can connect to DXU too as long as it connects on the same subnet as your PC. 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 DL-Axist.

### Supported Windows Versions

#### Windows Vista family

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

#### Windows 7 family

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

#### Windows 8 family

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

#### Windows 8.1 family

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

#### Windows 10 family

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

### Unsupported Windows Versions

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

### How to Install DXU

1. Copy the installer file to any convenient location on your PC.
2. Launch the installer.

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

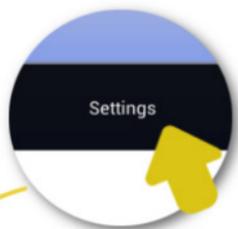
## Controls

### DXU Agent Controls

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

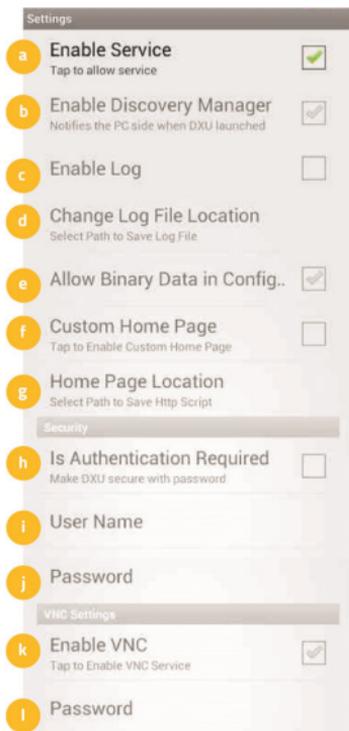
Find these settings in the DXU Agent application on the device.

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



## DXU Agent Settings Window

Here is a brief overview of each of the settings:



### a. Enable Service

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

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

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

### b. Enable Discovery Manager

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

### c. Enable Log

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

### d. Change Log File Location

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

### e. Allow Binary Data in Configuration

This check box allows a few types of binary data to be transmitted from the DL-Axist to DXU, and from DXU to the DL-Axist. The desktop wallpaper file is an example of binary data that can be controlled by DXU. Selecting this check box allows binary data to be sent to or from the binary computer in the configuration file. Clearing this check box

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

f. Custom Home Page

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

g. Home Page Location

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

h. Is Authentication Required

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

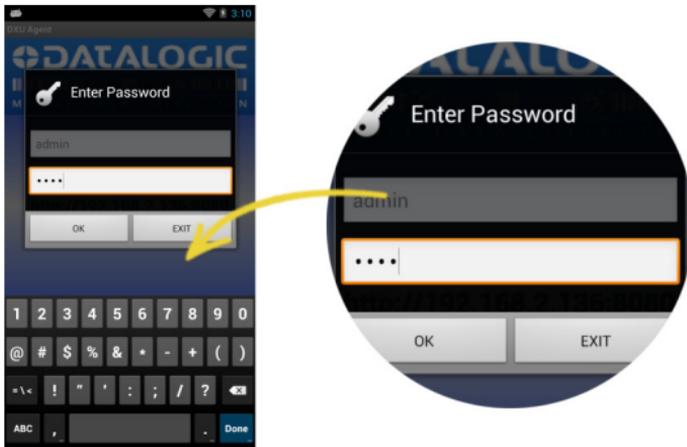
Note that these settings are also enforced by the DXU desktop application when it loads the configuration from the device. The DXU administrator will be prompted to type this user name and password. Once authenticated, the DXU administrator can edit the user name and password in DXU and apply these to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

i. User Name

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

j. Password

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



k. Enable VNC

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

## I. VNC Password

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

### **Advanced Settings**

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

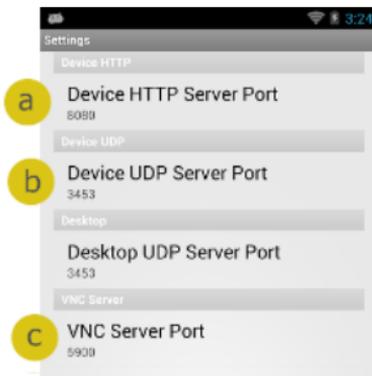
Change these settings only if you understand precisely any advantage you may gain by doing so. Most users will not realize any advantage from changing these port settings.

Find these settings in the DXU Agent application on the DL-Axist.

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

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

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



### a. Device HTTP Server Port

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

### b. Device UDP Server Port

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

### Desktop UDP Server Port

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

### c. VNC Server Port

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

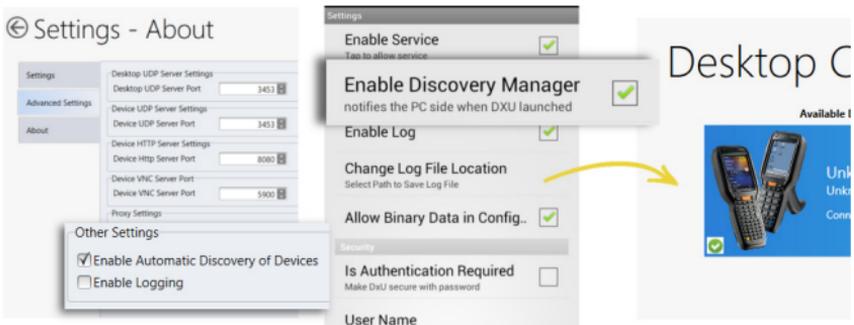
## Version

This page displays the DXU Agent version number.

## DXU Application Controls

### Available Device List and Configuration

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

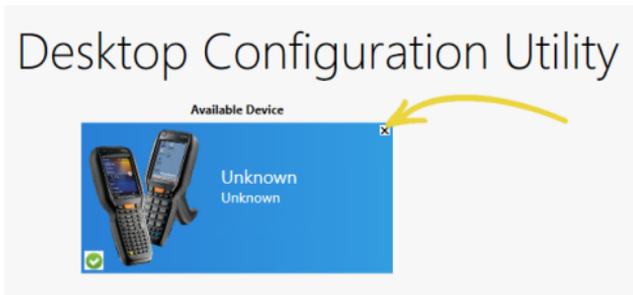


By default, "No Devices Available" will display when no devices announce themselves to DXU either when they connect via USB or when they connect over a network. Simply connecting the DL-Axist to a network, even on the same subnet as the PC running DXU, will not automatically display as being available. The device must try to connect to DXU, which sends an announcement packet to DXU. This can be done by scanning Scan2Pair or Scan2Deploy barcode labels. However, connecting a device to the PC running DXU via USB will automatically display it in DXU. You may also select the "Enable Automatic Discovery of Devices" check box in DXU's Settings view to automatically see any device that connects to the network, but

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

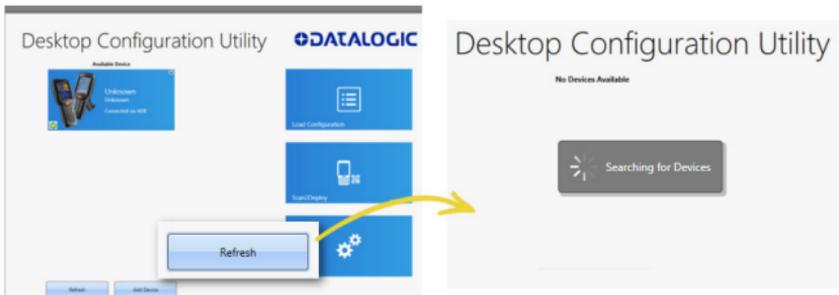
To configure a connected device, you simply click its button under Available Devices to load its configuration into DXU.

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



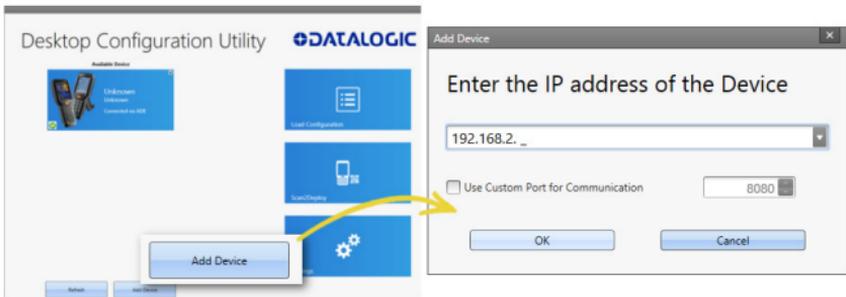
### *Refresh*

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



## Add Device

This button opens the ‘Add Device’ dialog which allows you to type the IP address of a device. This dialog 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 type in the last number of your device’s IP address if it is in the same subnet as your PC.



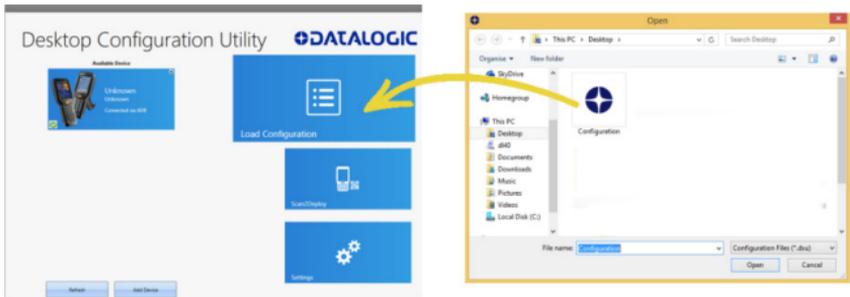
This dialog allows you to manually connect to devices running DXU Agent that are either inside your PC’s subnet or outside it. The limitation is that devices on other subnets must be on a subnet that is routable from your PC’s subnet. Consult with your network expert for more information.

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 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.

### Scan2Deploy

Scan2Deploy allows the DL-Axist running DXU Agent to connect using DXU Agent's Scan2Pair 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 'Scan2Pair' barcode label. This button opens the Scan2Deploy dialog streamlined to create 'Scan2Pair' 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.

The **Scan2Deploy** button located in a device's '**Datalogic Configuration Utility**' view can also automatically connect devices to Wi-Fi access points and to DXU, but this dialog 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 do not have network access to DXU on your PC. When the 'Include Unmodified Changes' check box 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.



### *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'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, 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.**

### *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, this tablets you 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 View**

The **Settings** view is opened by clicking the Settings button on DXU's main view. 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.

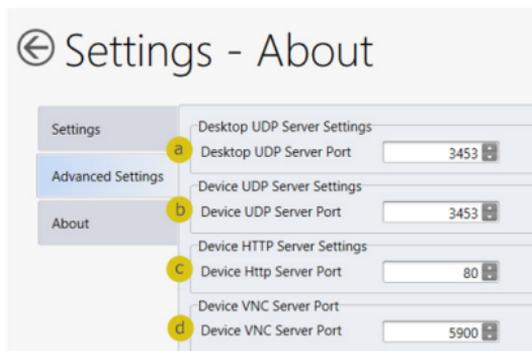


## *Language Tab*

The **Language** tab lets you 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 lets you 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 '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 lets you 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 view, 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, which you can use to update the firmware on your device.

### *Scan2Deploy Button*

Clicking this button opens the Scan2Deploy button. The version of the Scan2Deploy dialog opened from within the 'Desktop Configuration Utility' view lets you 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.

## Tasks

### Connect to a Device via USB

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

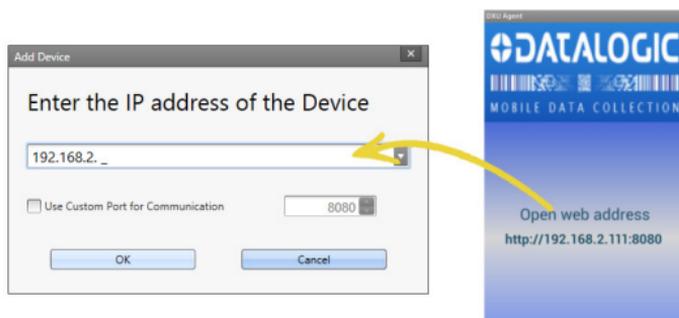
1. Launch **DXU**.
2. Connect your device to your PC with a **USB** cable.
3. Click the device's button in the **"Available Device"** list.

### 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 do this:

1. On DXU's main view, click the **"Add Device"** button;



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

**NOTE**

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

3. Click the **OK** button 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 default settings, do this:

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

**NOTE**

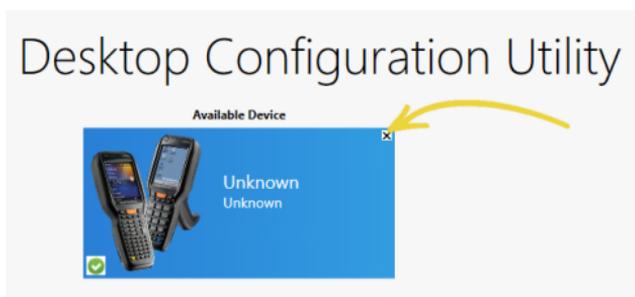
In most cases you should be able to leave other fields with their default values. You may, of course, change those values as needed to work with your network setup.

4. Click the **"Print Preview"** button.
5. Click the **Print** button in the button bar.
6. Since Print dialogs vary by the model or your printer, configure the print job and print as you normally do. Clean up by closing these dialogs.
7. Resume the device and unlock its screen.
8. Launch the DXU Agent application.
9. Tap the **Menu** button, and then select the **Scan2Deploy** command.
10. Scan the barcode.

Your device should appear in DXU's main window in the 'Available Device' list. Click that button to continue configuring your device.

### Deleting a Device from the Available Device List

Simply click the exit button (X) located at top right of the device.



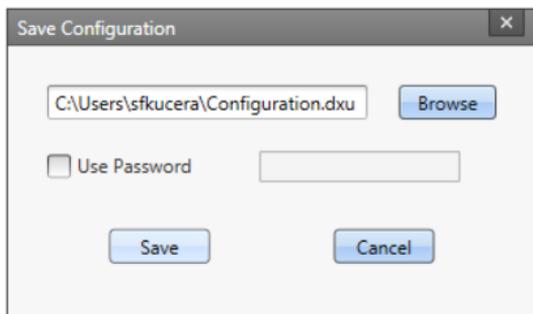
### Configuration Files

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

## Save a Configuration File

To save a configuration file, do this:

1. From within the 'Device Configuration' view, click the 'Save As' button
2. You may type the path and file name in the field, or you can click the **Browse** button to use a standard file dialog to explore to the folder of your choice and type the file name. Unusually, clicking the Save button in the Save As dialog does not actually save the configuration file yet, but instead returns you to the **'Save Configuration'** dialog.

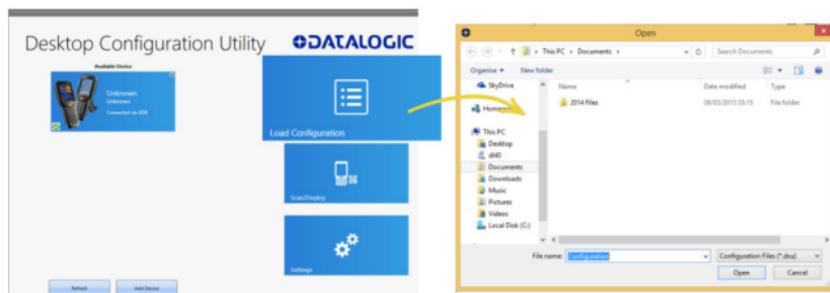


3. Optionally, you may select the **'Use Password'** check box and type a password into the field. This will obligate anyone who opens this configuration file in the future to correctly type the password in order to open the file.
4. Click the **Save** button.
5. Click the **OK** button to dismiss the confirmation dialog.

## Open a Configuration File

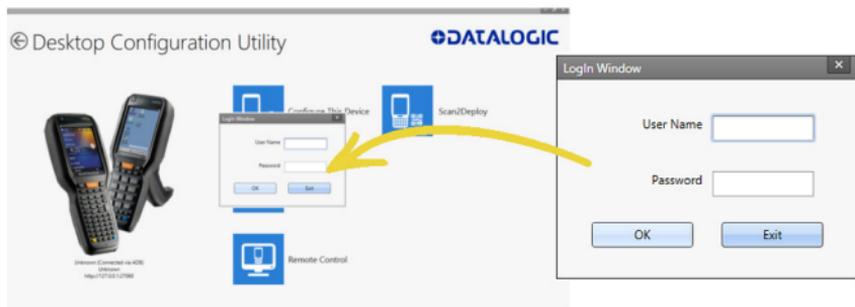
To load a configuration file saved earlier, do this:

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



## Open a Configuration File Which is Authenticated

DXU will display a login prompt when you open a configuration file that requires authentication. DXU will also display a login prompt when connecting to a device with a password set in DXU Agent.



To open a configuration or 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 or device into the **"User Name"** field.
3. Type the password for this configuration or device into the **Password** field.
4. Click the **OK** button.

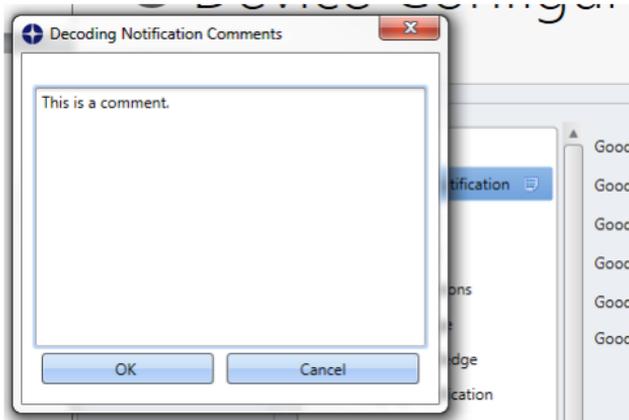
### **Edit a Configuration File Off-line**

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

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" view. 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 the **"Configure This Device"** button.
3. Right-click on any tab, node, or parameter, then select the **"Add comment"** command in the context-sensitive menu.
4. Type your comment.
5. Click the **OK** button to save. A small text balloon will appear next to the item you commented on.

To edit a comment:

1. Right-click on any item with a small comment icon.
2. Select the **"Edit comment"** command in the context-sensitive menu.
3. Edit your comment.
4. Click the **OK** button 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 the **"Configure This Device"** button.
3. If do not have comments in this configuration file, add several.
4. Click the **"Show Comments"** button in the button bar.

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

## Configure a Device On-line

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



To configure a device that is directly connected via USB:

1. Launch DXU.
2. Connect your device to your PC via a USB cable.
3. Click the button for your connected device in the 'Available Device' list.
4. Click the 'Configure This Device' button.
5. Configure any settings you wish.
6. Save changes to a configuration file if you do not wish to apply them to your device.
7. Apply the configuration changes to your device if this is what you want to do.

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

1. Launch DXU.
2. Connect your device to DXU manually, using Scan2Pair labels, or using automatic discovery. (See instructions for these methods in this section.)
3. Click the button for your connected device in the 'Available Device' list.
4. Click the 'Configure This Device' button.
5. Configure any settings you wish.
6. Save changes to a configuration file if you do not wish to apply them to your device.
7. Apply the configuration changes to your device if this is what you want to do.

## Configure a Device Off-line via Scan2Deploy

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



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

1. **Barcode Type:** select the barcode symbology used to print the Scan2Deploy labels. Different symbologies have advantages and disadvantages, so DXU gives you 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 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 the **"Configure This Device"** button.
3. Configure any settings you wish.
4. (Optional) **Save** your configuration.
5. Click the **Back** button to return to the **Desktop Configuration Utility** view.
6. Click the **"Scan2Deploy"** button.
7. Click the **"Device Configuration"** tab.
8. (Optional) Select the **"Include Unmodified Changes"** check box to include all configuration settings in your Scan2Deploy barcodes.
9. (Optional) Select the **"Include Binary Data"** check box to include binary data like the desktop wallpaper image in the configuration barcodes.



**NOTE**

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

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

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

13. Resume your device and unlock its screen.
14. Launch the **DXU Agent** application.
15. Tap the **Menu** button, and then select the **Scan2Pair** command.
16. Scan any label in your Scan2Deploy label set.



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

17. Continue to scan all barcodes until all of them on the list on the screen indicate they have been scanned. 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.
18. Clean up by tapping the **Home** button.

## Configure DXU

There are many ways to configure DXU, such as changing its language, changing the TCP/IP ports used to communicate with DXU Agent on remote devices, enabling automatic discovery of devices, enabling logging, and resetting 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. In DXU's main view, click the **Settings** button.



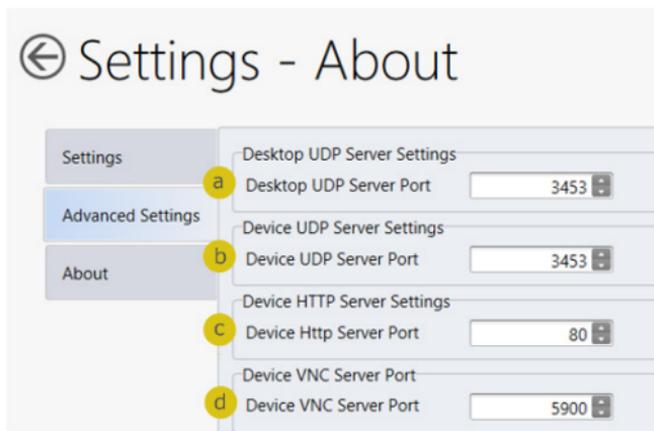
2. Select the language you prefer in the **Language** menu.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to DXU's main view.

## Configure DXU Communication Settings

You can configure the TCP/IP ports used by DXU to communicate with DXU Agent on the DL-Axist. 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. In DXU's main view, click the **Settings** button.
2. Click the **"Advanced Settings"** tab.



3. Edit the port values to match the ports used by 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 DXU's main view).

## Enable Automatic Discovery of Devices

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



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

To enable automatic discovery of devices:

1. In DXU's main view, 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 DXU's main view).

## 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. DXU's default log file location, once enabled, is in your user directory at 'C:\Users\\AppData\Roaming\Datalogic DXU'.

To enable logging:

1. In DXU's main view, click the **Settings** button.
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 DXU's main view).

### Reset Advanced Settings to Defaults

You can reset DXU's Advanced Settings to their default values. To do this:

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

### Enable Logging on the DL-Axist™

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

You can specify where DXU Agent's log file is kept on your device. The default location on Android OS devices is /storage/sdcard0, which is located in the device's on-board flash memory. This

location is a persistent location, so log files stored here are safe if the PDA reboots. If a MicroSD card is used, you may wish to specify that logs be kept on the card if the card has greater capacity than on-board flash. MicroSD cards are also persistent.

To enable DXU Agent logging on your device:

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



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

**NOTE**

6. Select the **"Enable Log"** check box.
7. Select the **"Enable Service"** check box.
8. Clean up by tapping the **Home** button.

To specify where log files are stored on your device:

1. Resume your device and unlock its screen.
2. Launch the **DXU Agent** application.
3. Tap the **Menu** button 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 **“Change Log File Location”** button.
7. Type a valid path on your device into the ‘Change Log File Location’ field, and then tap the **OK** button.
8. (Optional, but desired if you wish to log to this new location) Select the **“Enable Log”** check box.
9. Check the **“Enable Service”** check box.
10. Clean up by tapping the **Home** button.

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

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

### Enable Authentication in DXU Agent

You can ensure that users are prompted to enter a user name and password to open a configuration file in the DXU console or to DXU Agent’s Settings window on a device. This capability is enabled with a single check box in DXU Agent.

To enable authentication:

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



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

6. Select the **"Is Authentication Required"** check box.
7. Select the **"Enable Service"** check box.
8. Clean up by tapping the **Home** button.

To authenticate while opening DXU Agent's Settings window:

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



## Change the User Name in DXU Agent

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

To change the User Name:

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



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

**NOTE**

6. Tap the **"User Name"** button.
7. Delete the contents of the field, and type a new user name.
8. Tap the **OK** button.
9. Select the **"Is Authentication Required"** check box.
10. Select the **"Enable Service"** check box.
11. Clean up by tapping the **Home** button.

### Change the Password in DXU Agent

Editing the password ensures the simplest means to keep untrusted actors out of DXU Agent configuration settings. The default password is '0000.'

To change the Password:

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



#### **NOTE**

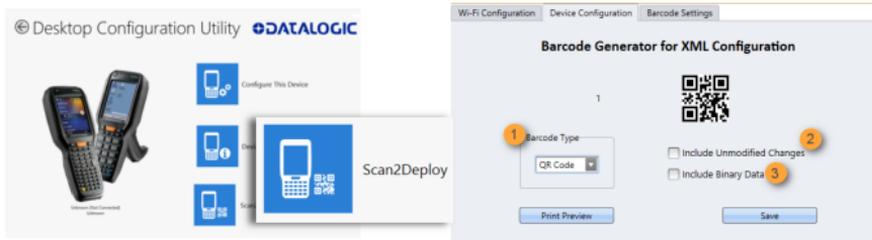
**You must clear "Enable Service" before you can change any setting in DXU Agent.**

6. Tap the **Password** button.
7. Delete the contents of the field, and type a password.
8. Tap the **OK** button.
9. Select the **"Is Authentication Required"** check box.

10. Select the **“Enable Service”** check box.
11. Clean up by tapping the **Home** button.

## Create Scan2Deploy Labels to Fully Configure Remote Devices

The **Scan2Deploy** button located in a device’s **“Datalogic Configuration Utility”** view can automatically connect devices to Wi-Fi access points and to DXU, but this dialog also has another 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 do not have network access to DXU on your PC. When the **“Include Unmodified Changes”** check box 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.



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 the **"Configure This Device"** button.
3. Configure any settings you wish.
4. (Optional) **Save** your configuration.
5. Click the **Back** button to return to the **Desktop Configuration Utility** view.
6. Click the **"Scan2Deploy"** button.
7. Click the **"Device Configuration"** tab.
8. (Optional) Select the **"Include Unmodified Changes"** check box (2) to include all 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 (3) to include binary data like the desktop wallpaper image in the configuration barcodes.



**NOTE**

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

10. (Optional) Select the barcode symbology in the **"Barcode Type"** menu (1).
11. Click the **Save** button to save your barcode label set as a graphic image file.

12. To print, click the **“Print Preview”** button, then click the **Print** button in the button bar, and then finish printing using your printer’s Print dialog.

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 the **Menu** button, and then select the **Scan2Pair** command.
4. Scan any label in your Scan2Deploy label set.



**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 until all of them on the list on the screen indicate they have been scanned. 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. Clean up by tapping the **Home** button.

## 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’s 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 the **"Device Info"** button.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to DXU's main view).

## 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's 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 the **"Device Info"** button.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to DXU's main view).

## Remote Control

Remote Control lets you 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 instead sends an event message in the system as if you had pushed a physical key or tapped a physical button on the touch screen. Remote Control works through the magic of software.



## Unlock the Screen Using Remote Control

You can unlock the screen by dragging your mouse on the Remote Control screen in the same manner as a user swiping on the device's 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 on the network via **Wi-Fi** or **Ethernet**, or scan a **Scan2Pair** label.
3. Click the device's button in the **"Available Device"** list.
4. Click the **"Remote Control"** button.
5. If the device is suspended, with its screen off, click the **Power** button (3) at the bottom of the **Remote Control** window.
6. Click on 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. Some applications have a menu, and others do not, 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 as if you pushed the device's Power button.

## 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 scanner cannot scan if the Camera application is showing its live preview or taking a photograph or recording a video; and the scanner will not scan if none of the device's scan buttons are configured to scan. However, in general if you have your device 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 screen shot of the remote computer and prompts to save it to your PC. The default path that DXU saves screen shots is your user folder.

## Set a VNC Password

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



**The VNC password must match between DXU console and DXU Agent on the device or a connection will not be made.**

## 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 the **Menu** button 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. In the **"VNC Settings"** section, tap the **Password** button.
7. Type a password into the field. It can be numbers, letters, or some punctuation characters.
8. Tap the **OK** button.
9. Select the **"Enable Service"** check box.
10. Clean up by tapping the **Home** button.

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 on the network via **Wi-Fi** or **Ethernet**, or scan a **Scan2Pair** label.
3. Click the device's button in the **"Available Device"** list.
4. Click the **"Remote Control"** button.
5. Type the device's **VNC password** into the field, and then click the **OK** button.

### 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 view. To do this:

1. Open a configuration file or load the configuration from a connected device.
2. Click the **'Configure This Device'** button.

3. Click the 'DXU Configuration' tab.
4. Click the 'General Settings' node in the middle pane.
5. Type a password into 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 DXU's main view).

## Update Firmware

You can update the DL-Axist's firmware from DXU. DXU provides several options, such as performing a 'Silent Install' where no user interaction is required on the device, and performing a 'Force Update' where the firmware is reinstalled even if the device reports that it already has the same version installed. Also, you can specify whether a factory data reset or an enterprise reset is performed after updating the firmware, or if the update will simply reboot the device without performing an update.

**NOTE**

**DXU firmware update is not the only way to update firmware on the DL-Axist. 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 you to perform an image update that does not require any user interaction on the device. If left cleared, the user will be prompted to perform the update, but they have the option to cancel the update. This check box is not checked by default.

## Force Update

This option allows you to 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 inconvenience 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 the condition it would be in if it were just leaving the factory. This reset deletes all user data and settings, deletes 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 connects such as Wi-Fi settings, and it does not reset 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 on the network via **Wi-Fi** or **Ethernet**, or scan a **Scan2Pair** label.
3. Click the device's button in the **"Available Device"** list.
4. Click the **"Firmware Utility"** button.
5. Click the **Browse** button to open a standard file dialog to browse for and select a suitable firmware image file.



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

### NOTE

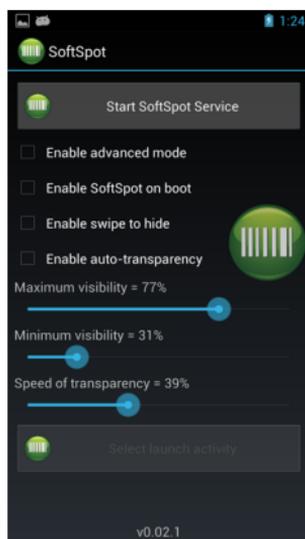
6. Navigate to your firmware image file, select it, and click the **Open** button.

7. (Optional) Select the **"Silent Install"** check box if you wish to perform a firmware update that does not require user interaction on the device.
8. (Optional) Select the **"Force Update"** check box if you wish to force a complete reinstallation of this image on the device.
9. (Optional) Select an option from the **"Reset Type"** menu if you wish to perform a factory data reset after the image update finishes, or if you wish to perform an enterprise reset after the image update finishes, or if you just want to have the device reboot without resetting at all.
10. Click the **Update** button.

## SoftSpot™

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

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



Tap the SoftSpot to scan barcodes.

Double-tap to enable the Continuous Scan mode and scan barcodes consecutively. Tap one more time to stop laser emission.

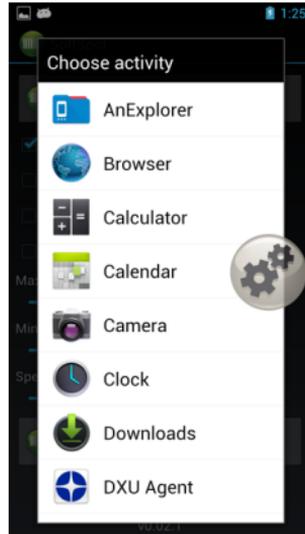
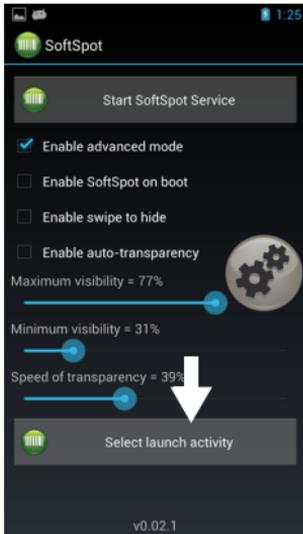
### Start SoftSpot Service

Enables/disables the SoftSpot.

## Enable advanced mode

If selected, allows you to assign the SoftSpot to an application to launch.

Tap **Select launch activity** and then select the application you want to launch with the SoftSpot:



Tap the SoftSpot to launch the selected application.

## Enable SoftSpot on boot

Select it to enable SoftSpot on boot.

## Enable swipe to hide

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

## **Enable auto-transparency**

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

## **Maximum visibility**

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

## **Minimum visibility**

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

## **Speed of transparency**

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

You can also configure the SoftSpot from the DXU. For more details on DXU, see '[Desktop Configuration Utility \(DXU\)](#)' on page -99.

## Tap2Deploy

**Tap2Deploy** application uses NFC technology to establish wireless communication limiting the need of user interaction.

The user interface is intended to be almost touchless, the screen simply shows usage instructions and visual feedback, while the user input is mainly through NFC communication.

The main view shows usage instructions: approaching a device triggers the configuration cloning, while tapping a tag starts the pairing procedure with DXU utility.

This happens automatically as the application is able to discern between reading a tag and talking to a device.

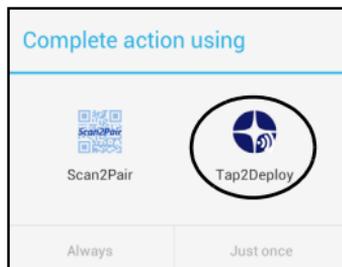
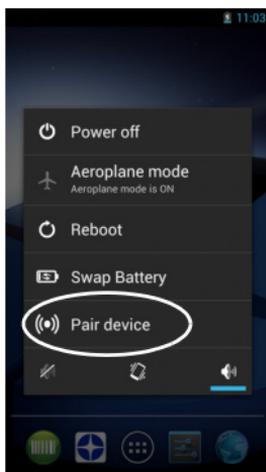


The cloning feature allows the settings of a device to be wirelessly cloned to another device within range.

The cloning process always happens between a device in master mode and a device in slave mode. The master is the device to which the slave will match up. The direction of the cloning is shown by an arrow on the screen: the moving device on the left side of the Clone pane always represents the current device (i.e. where the application is running), while the static one represents the device to get close to. The direction of the arrow and the description label change when the device cloning mode changes (master or slave).

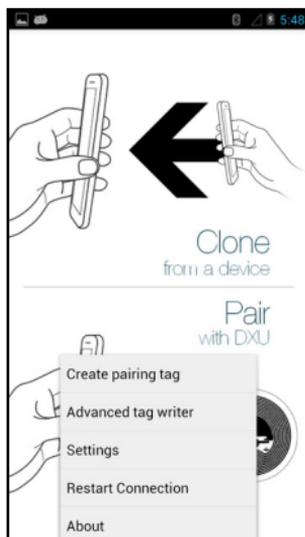
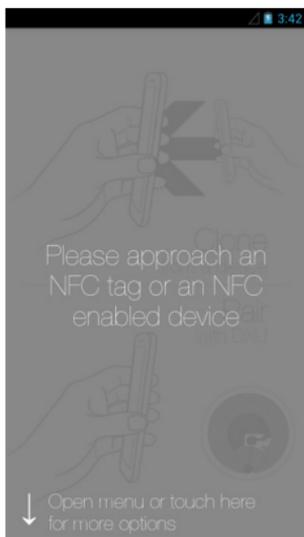
You have two options to access the application menu:

1. Press and hold the **Power** button until the **Long Press Menu** menu displays and then tap **Pair device** > **Tap2Deploy**:



2. Tap **All apps** > **Tap2Deploy**.

Tap the screen anywhere to display a window with further instructions, then tap the bottom of the window 'Open menu or tap here for more options':

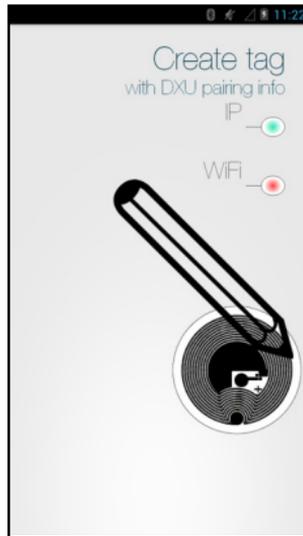


The menu allows to access more features and options.

## Create pairing tag

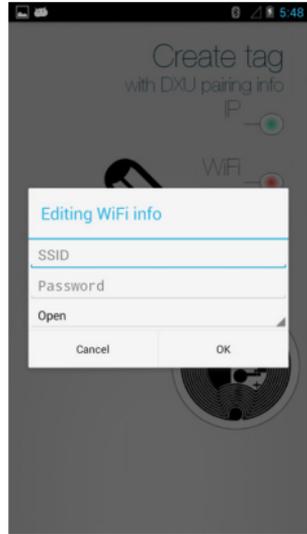
Allows to create a DXU pairing tag, an NFC tag that binds the device to the DXU Desktop application, over a Wi-Fi connection, without any user interaction. The tool is intended to be used by both the device and the DXU desktop application.

The user interface lists the information to be written on the tag. A light on the right side states whether an information is present (green) or not (red):



To create the tag, you need to enter:

- IP and port to access the DXU Desktop application.
- Wi-Fi connection parameters (SSID, password and security).



When the tool is launched from the device, the DXU Desktop IP and port information must be entered by the user. The Wi-Fi SSID, password and security type are automatically set to the actual Wi-Fi connection, unless the device is not connected to any network or there is any problem in fetching such information.

The tag is created if at least one information is available (i.e. writing just the Wi-Fi settings yields a tag for connecting to a Wi-Fi network).

Read the tag to write it. If the **Confirm tag write** is checked in the **Settings** window, a pop up displays asking for confirmation.

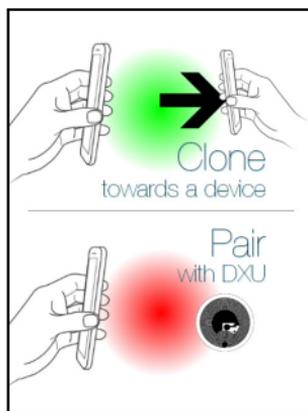
If you need to create a tag with customized content, use the **Advanced tag writer** (see '[Advanced Tag Writer](#)" on page -165).

## Tap2Deploy DXU Plug-in

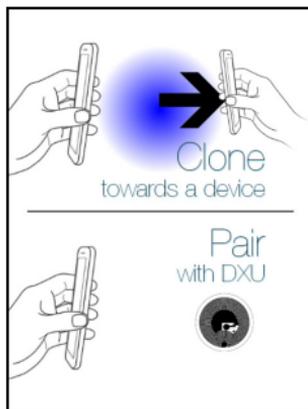
Tap2Deploy is controlled by the DXU Desktop application thanks to a plug-in system. Using the desktop-side plug-in, the user is able to write NFC tags remotely. With this feature the creation of a DXU pairing tag is fully automatic, because the IP and port settings are filled by the application and the user does not need to enter any further information. The plug-in also allows to create custom tags.

### User Feedback

Feedback to the user is provided with red and green colors in the shape of lights that appear on the screen. The example below shows a good cloning and a bad pairing.



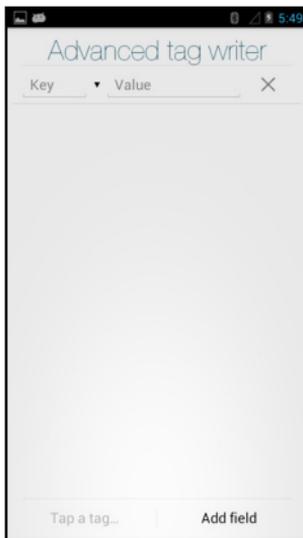
During an operation, the loading status is represented by a pulsing blue light.



## Advanced Tag Writer

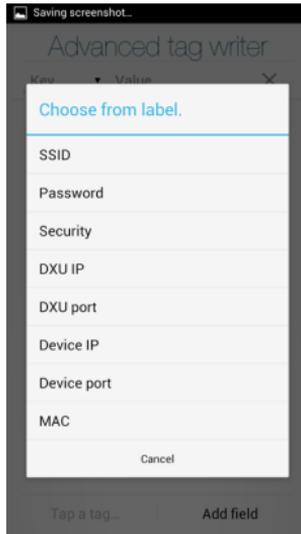
Allows an expert user to create customized tags with JSON content (mime type application/json). It features a simplified editor for creating a JSON object by writing key-values pairs. However, using this tool to create a DXU pairing tag it is highly inconvenient, please use the tag creator or the DXU Desktop plug-in instead.

The **Advanced tag writer** is available from the application menu:



The user interface provides a simplified editor for writing JSON formatted text, as key-value pairs.

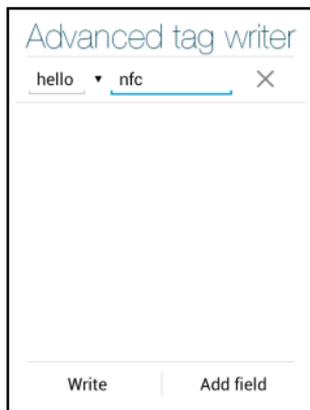
Tap the down arrow to open a dialog for picking predefined JSON keys. These keys are bound to several functionalities in the Tap2Deploy application and are actually used for cloning and pairing features (i.e. the keys may represent Wi-Fi SSID, password, device IP address and others).



Once the editor is filled with the information, you may write the tag simply by tapping it, that is, just approaching it.

If you read a not-empty tag with JSON content (i.e. application/json mime type), the application asks you if you want to edit the content of the tag or to overwrite it with the data in the editor. In case of editing choice, the editor is filled with JSON data from the tag.

If the read tag is empty or the content is not JSON, the tag is written after the confirmation button is tapped. Please notice that the confirmation button appears only when a tag is read and replaces the **tap a tag** button. The write confirmation may be disabled from the **Settings** window.



## Settings

Opens the application settings.



## Restart Connection

Restart a connection that has timed out.

## About

Opens a dialog window showing information about the application, such as version and last update. Use these information when reporting any issue.



# NOTES



## Tools

### USB ADB Driver & USB CD-ROM

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

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

Use the USB CD-ROM to install the Windows drivers and then launch ADB to run a shell using the following tool command prompt:  
**Start/Datalogic Android/Support/Device.**

## SDK Add-on

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

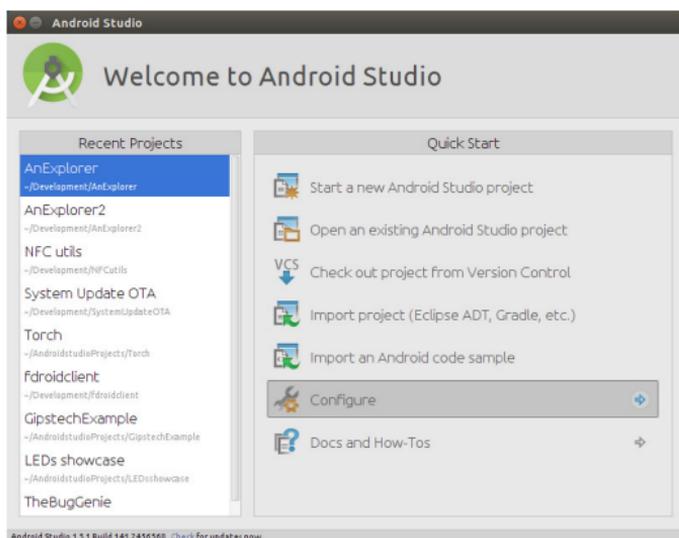
### Install SDK Add-on

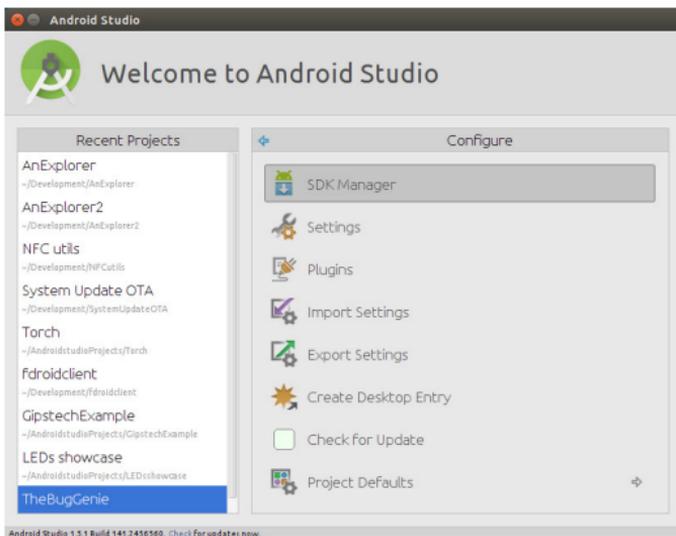
To install Datalogic SDK™ with Android Add-on, please insert the following URL in Android Studio or Eclipse ADT:

<https://datalogicadcsrl.github.io/android-sdk/addon.xml>

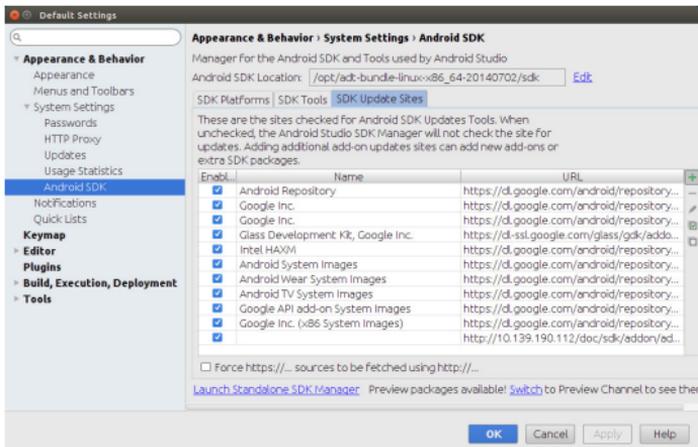
or follow the detailed steps (valid for Android Studio versions released on the stable, there is no support for the beta channel):

1. From Android Studio launch window, click on **Configure > Android SDK Manager** to open Android SDK Manager:



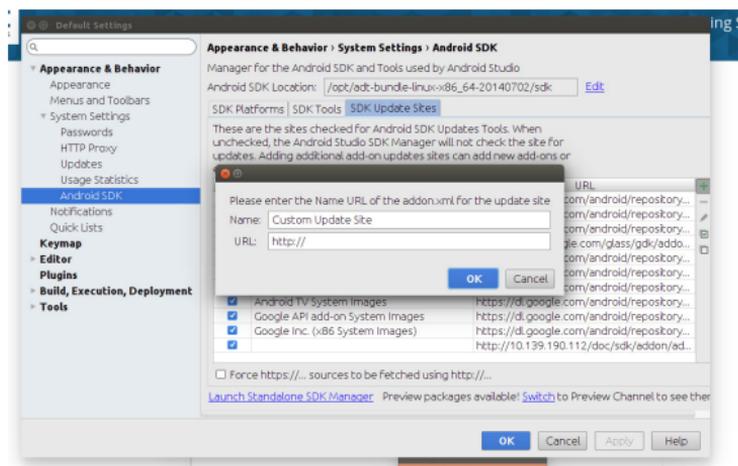


2. Select the tab SDK Update Sites and click the **+** (plus) icon on the right-side toolbar:

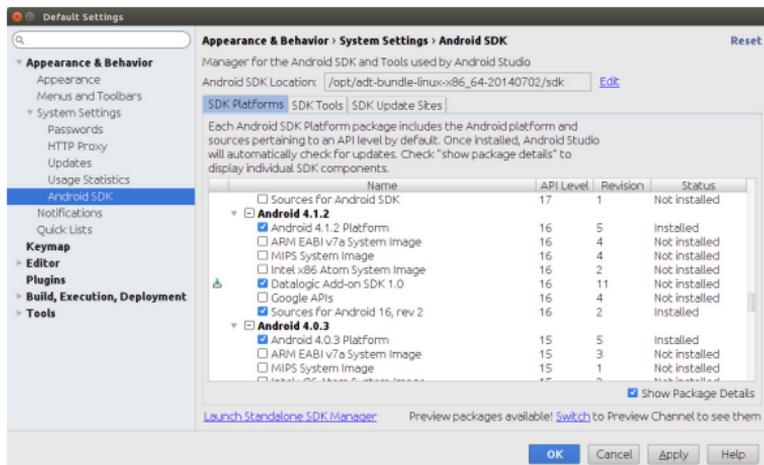


- In the new window insert the following URL, optionally a name and the press **OK**:

<https://datalogicadcsrl.github.io/android-sdk/addon.xml>

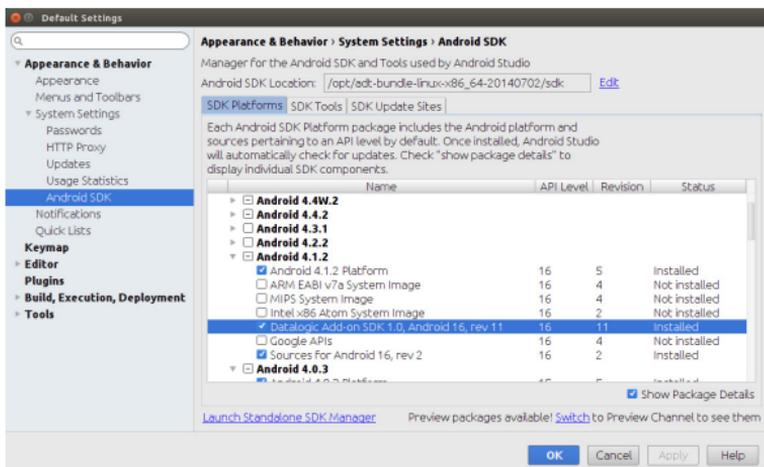


- Now select the tab **SDK Platforms** and check the checkbox on the bottom right **Show Package Details**. Under the section **Android 4.1.2 (API 16) Datalogic SDK Add-on** should appear. To install it, select the Datalogic SDK Add-on checkbox and a small icon on the left should appear:



Please notice that you must also install the Android API platform matching your Android version (i.e. API 16 is required to compile apps for Android 4.1.1).

- Click on the button **Apply** to install the selected packages. Once the installation is complete, the **Status** of the Datalogic SDK Add-on changes from **Not installed** to **Installed**:



## Install Android™ Studio

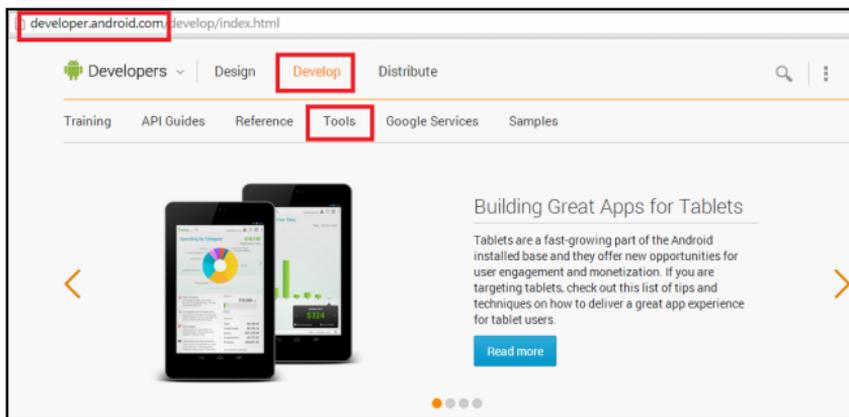
To install Android Studio follow the steps described at:

<http://developer.android.com/sdk/index.html>. No specific version is required.

## Install Android SDK

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

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



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

developer.android.com/sdk/index.html

Develop > Tools > Android SDK

emulator

Download

Installing the SDK

Adding SDK Packages

Android Studio

Workflow

Support Library

Tools Help

Revisions

NDK

ADK

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

GET THE SDK FOR AN EXISTING IDE

SYSTEM REQUIREMENTS

**VIEW ALL DOWNLOADS AND SIZES**

ADT Bundle

Platform	Package	Size	MD5 Checksum
Windows 32-bit	adt-bundle-windows-x86-20140624.zip	377325518 bytes	5655cd8be53c4b27c5242d81943c5a25
Windows 64-bit	adt-bundle-windows-x86_64-20140624.zip	377477237 bytes	0f1fa29a0f229e36ba0fb87bb7ee68d4
Mac OS X 64-bit	adt-bundle-mac-x86_64-20140624.zip	327367424 bytes	7d16e832632598829011f12055a8fe3f2
Linux 32-bit	adt-bundle-linux-x86-20140624.zip	378659422 bytes	692e6135ed459f1e8a10498363f19f67
Linux 64-bit	adt-bundle-linux-x86_64-20140624.zip	378966059 bytes	0f14b4aed1eb1feed778ad6ed76ba01c

SDK Tools Only

Platform	Package	Size	MD5 Checksum
Windows 32 & 64-bit	android-sdk_r23-windows.zip	138459944 bytes	9daba72b3a15a6154fe6ca1ada817553
	installer_r23-windows.exe (Recommended)	90065639 bytes	4564d1f1b30c001c78a22ec40444e5f
Mac OS X 32 & 64-bit	android-sdk_r23-macosx.zip	88015023 bytes	3869e5b9de8d69f9050956866fb7ce8
Linux 32 & 64-bit	android-sdk_r23-linux.tgz	137880976 bytes	fd768c56423e998b3e4aa8895c993bf5

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

About Android | Legal | Support

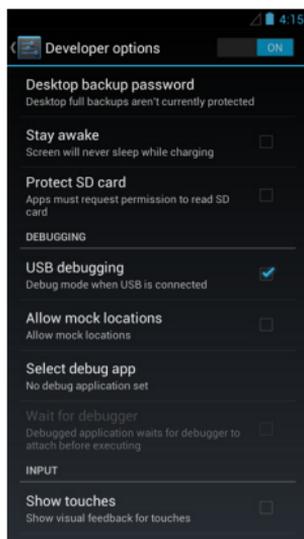
## Install ADB Driver

1. Install Android SDK Manager (see "Install Android SDK" on page -177 for further information).
2. Download and install the Google USB Driver (see <https://developer.android.com> for further information).

**NOTE**

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

3. In order to use ADB with your device connected over USB, you must enable USB debugging in the device system settings. Go to **Settings > Developer options** and select **USB debugging**:



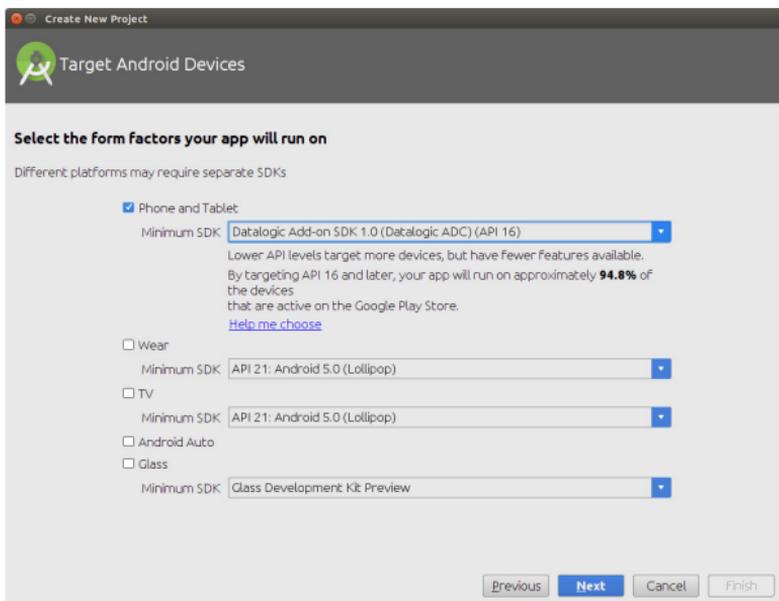
4. Use a CD-Rom Installer to debug the ADB driver and read the DL-Axist as an ADB device.

## Create a New Application with Android Studio

To install Android Studio follow the steps described at:

<http://developer.android.com/training/basics/firstapp/creating-project.html>.

When creating a new project, choose **Datalogic Add-on SDK 1.0** as **Minimum SDK option**:



## SureLock

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

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

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

Refer to the [SureLock Documentation for Android](#) on the 42Gears website for further details on **SureLock**.

## SureFox

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

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

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

Refer to the [SureFox Documentation for Android](#) on the 42Gears website for further details on **SureFox**.



# Connections

## USB Connection

### USB Direct Connection

You can use the supplied USB charge/communication cable to directly connect the DL-Axist to a host computer and transfer data through the USB interface.



**Connection through the cable complies to USB 2.0 standard.**

## USB Dock Connection

The single dock can be connected to the host computer by means of a standard micro USB cable.

Once the host computer has been turned on, insert the DL-Axist into the dock.



### NOTE

Connection through the cable complies to USB 2.0 standard.



### NOTE

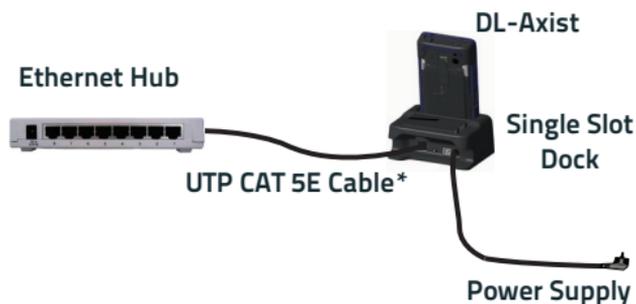
The actual data transfer speed can be appreciably lower than the maximum theoretical speed.

## Ethernet Connection

Use the single dock to build a reading system for the collection, decoding and transmission of barcoded data.

### Ethernet Dock Connection

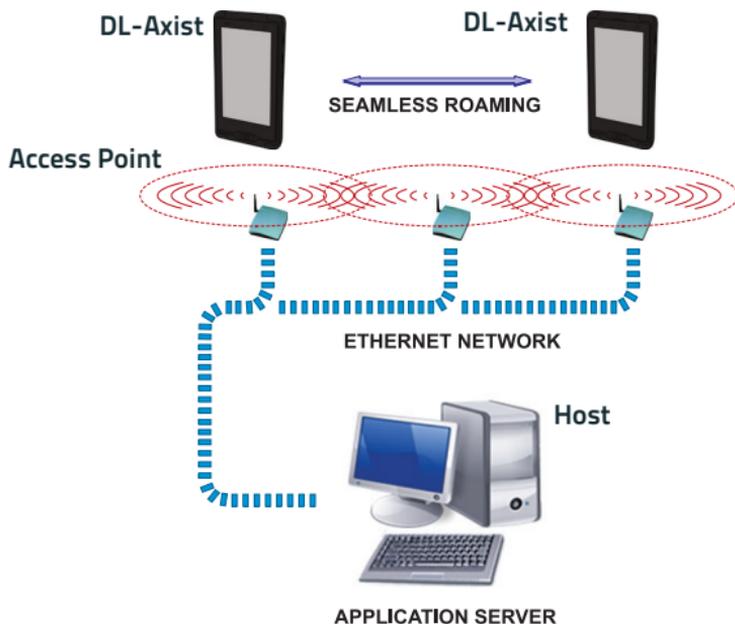
1. Connect the single dock to the power supply.
2. Use the slide switch on the dock to select the ethernet connection.
3. Plug a CAT-5 ethernet cable into the ethernet port on the back of the dock.
4. Plug the ethernet cable into the ethernet hub or a port on the host device.
5. Insert the DL-Axist into the dock.



\* Recommended use

## WLAN Connection

The DL-Axist has a 802.11a/b/g/n WLAN (Wireless Local Area Network) radio and can communicate with other 802.11a/b/g/n, Wi-Fi compliant products including access points, workstations via PC card adapters and other wireless portable devices.



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.).

---

## MIMO (Multiple-Input and Multiple-Output)

DL-Axist supports MIMO technology.

MIMO (multiple-input and multiple-output) is a method for multiplying the capacity of a radio link using multiple transmit and receive antennas to exploit multipath propagation. It is a practical technique for sending and receiving more than one data signal with the same radio channel simultaneously via multipath propagation.

MIMO has become an essential element of wireless communication standards including IEEE 802.11n (Wi-Fi), IEEE 802.11ac (Wi-Fi), HSPA+ (3G), WiMAX (4G), and Long Term Evolution (4G).



### NOTE

**MIMO technology is only available in Wi-Fi models.**



### NOTE

**Ensure your Wi-Fi infrastructure is compatible with MIMO technology to provide the best coverage and speed performance.**

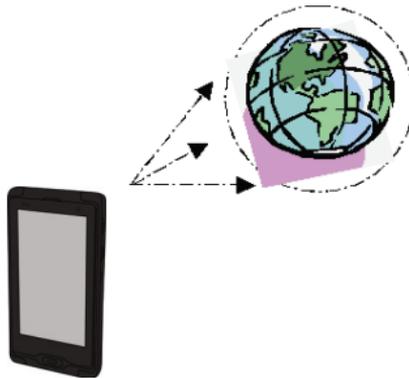
## WWAN Connection

The DL-Axist enhances your connectivity solutions giving you an opening to an international wireless infrastructure that is the global standard. It is optimized for the following two-way communications:

- Voice: GSM voice data (dial-up)
- Data: Available speed depends on the wireless network carrier and their supported packet-data technology in addition to network conditions.

The DL-Axist supports the following bands:

- 2G bands: 850 / 900 / 1800 / 1900
- 3G bands: 2100 / 1900 / 850 / 900.



The signal strength of the connection is indicated by the number of bars that appear in the signal icon located in the Status bar at the top of the screen.



---

In order to use a WWAN Connection you have to install a SIM Card (see 'Install the SIM Card" on page -24).

**NOTE**

**You can use the WWAN radio for simultaneous voice and data communication on a UMTS (3G) network only. On a GSM network, if you want to communicate over the phone (voice), you cannot send data. If you want to send data, you cannot use the phone.**

**NOTE**

**Area coverage and 3G performance may vary, due to environmental conditions, access point types or interference caused by other devices (microwave ovens, radio transmitters, etc.).**

## WPAN Connection

The DL-Axist can communicate with a Bluetooth® device, such as a printer, within a range of 10 m, using the on-board Bluetooth® module.



**NOTE**

In order to extend battery life, the Bluetooth® module is off by default. If you need to have Bluetooth® working, the module must be powered on (see **“Bluetooth Settings”** on page -70).



**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.).**

## Near Field Communication (NFC)

NFC technology allows short-range, wireless data transfer between the terminal and NFC tags or other NFC enabled devices placed in close proximity to the back of the terminal.

DL-Axist support the following modes of operation:

- NFC tag reader/writer mode: the terminal reads and/or writes digital information from or to an NFC tag.
- Peer-to-Peer (P2P) mode: the terminal uses Android Beam and/or Bluetooth@ technology to transfer screen content (e.g., a picture, web page url, or file) between NFC enabled devices.
- NFC card emulation mode - The terminal emulates an NFC card (smart card) that an external card reader can access.

### Read NFC Tags

1. Make sure NFC is enabled (see 'Enable NFC' on page -77).
2. Hold the NFC tag close to the back of the terminal.
3. When an NFC tag is recognized, the terminal emits a sound and the tag data displays on the terminal screen.

See also 'Tap2Deploy (NFC)' on page -32 and 'Tap2Deploy' on page -158.



**Suspend mode and the screen lock temporarily turns the NFC radio off.**

---

## Wireless and Radio Frequencies Warnings



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

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.

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



**WARNING**

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.



**WARNING**

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.



**WARNING**

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.

**WARNING**

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. 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.

# NOTES



## Data Capture

The DL-Axist has an integrated imager that collects data by scanning barcodes.

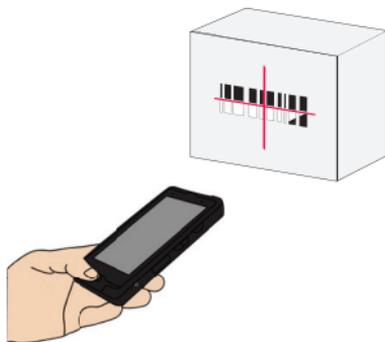
See ‘[Scanner Settings](#)’ on page -48 for instructions on configuring the scanner settings.

### Imager Data Capture

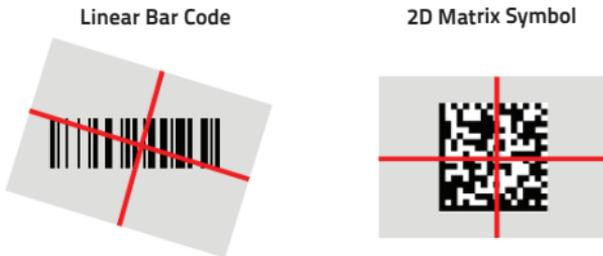
The imager uses digital camera technology to take a digital picture of a barcode, the image is stored in memory and software decoding algorithms are executed to extract the data from the image.

To scan a barcode symbol:

1. Point the scan window at the barcode.
2. Tap **Scan** on the screen or press one of the scan buttons on the DL-Axist. 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.



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



If the scan has been successful:

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

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

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



# Technical Features

## Technical Data

Item	Description
<b>Physical Characteristics</b>	
Dimensions	156.7 x 80 x 19.6 (bottom)/27.1 (top) mm
Weight	350 g with standard battery; 400 g with extended battery pack
Audio	Receiver and speaker Headset
LEDs	1 logo light RGB for good read 1 bi-color LED (red/green) for charger status
Display	Transmissive 5" TFT HD resolution minimum, LED backlight, touchscreen
Camera	5.0M pixels CMOS color camera with autofocus with LED flash light
Power Supply	Removable battery pack with rechargeable Li-ion batteries; Standard Battery: Li-Ion 3200 mAH, 3.8V Extended Battery: Li-Ion 6400 mAH, 3.8V Rechargeable backup battery: 5 mAh, 3.0V

Item	Description
<b>System</b>	
Operating System	Android Jelly Bean 4.1.1
Application Processor	TI OMAP4430 1GHz
System RAM Memory	1GB LPDDR2 RAM
System Flash Memory	8GB eMMC flash memory
<b>Communications</b>	
Interfaces	Micro USB connector: USB 2.0 Client, USB 2.0 Host and Client OTG, also for supplying power
Local Area Network (LAN)	IEEE 802.11a/b/g/n compliant Frequency range: Country dependent, typically 2.4 and 5.2 GHz CCX v4 Security
Personal Area Network (PAN)	Bluetooth® Wireless Technology IEEE 802.15 HCI module, Class II with V2.1 EDR and V4.0 smart ready
<b>Imager Characteristics</b>	
Scanning Rate	60 frames/sec maximum
Optical Resolution	Linear codes 4 mils; 2D codes 5 mil
Aiming Laser	VLD, wavelength 640-660 nm
Barcodes	UPC/EAN, 2 of 5 family, Code 39, Codabar, Code 128, GS1-128, Code 93, MSI, PDF417, MicroPDF417, Data Matrix, QR Code, GS1 DataBar family, Aztec Code, MaxiCode, Pharmacode 39, Trioptic, Composite, US POSTNET, US PLANET, USPS Intelligent Mail, Royal Mail RM4SCC, UPU FICS, Australian Post, KIX Code, Japanese Post

Item	Description
<b>Imager Characteristics (continued)</b>	
Laser Classification	VLD - Class 2 IEC/EN 60825-1. Compliant with 21 CFR 1040-10 except for deviations pursuant to laser notice n. 50, dated June 24, 2007
LED Classification	Exempt risk group IEC/EN 62471
Illumination System	LEDs 600~630 nm
<b>Environmental</b>	
Operating Temperature	- 20° to 50° C (32° to 122° F)
Storage Temperature	- 30° to 70° C (-40° to 158° F)
Humidity	Operating: 10% to 90% relative humidity, non condensing
Drop Resistance	Withstands drops from 1.8 m / 5.9 ft onto concrete (with rubber boot); Withstands drops from 1.2 m / 4.0 ft onto plywood (without rubber boot)
Environmental Sealing	IP67 Standard according to IEC 60529
ESD Level	+/- 8KV direct discharge, +/- 15KV air discharge

## Decode Distances

Depth of Field	Far Guaranteed Working Ranges
Code 39	4.72 in 12 cm
Code 39	8.27 in 21 cm
PDF	6.69 in 17 cm
EAN13	14.57 in 37 cm
Datamatrix	9.25 in 23.50 cm
Code 39	19.29 in 49 cm



## Test Codes

### High Density Codes - 0.25 mm (10 mils)

Code 39



17162

Interleaved 2/5



0123456784

Code 128



test

**High Density Codes (continued) - 0.25 mm (10 mils)**

80%

EAN 13



80%

EAN 8



**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



100%

EAN 8



**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



120%

EAN 8



**2D Codes**

Datamatrix ECC200



Example

Inverse Datamatrix ECC200



Example

# NOTES



## Maintenance

### Cleaning

Periodically clean the DL-Axist with a slightly dampened cloth.

Close all the caps before cleaning.

Do not use alcohol, corrosive products or solvents.

Keep the device dry.

### Ergonomic Recommendations



**CAUTION**

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

- Reduce or eliminate repetitive motion
- Maintain a natural position
- Reduce or eliminate excessive force
- Keep objects that are used frequently within easy reach
- Perform tasks at correct heights
- Reduce or eliminate vibration

- Reduce or eliminate direct pressure
- Provide adjustable workstations
- Provide adequate clearance
- Provide a suitable working environment
- Improve work procedures.



## Safety and Regulatory Information



**Read this manual carefully before performing any type of connection to the DL-Axist PDA.**

**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 9.
- Use only the components and accessories supplied by the manufacturer for the specific DL-Axist being used.

Do not attempt to disassemble the DL-Axist PDA, 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 DL-Axist PDA, disposal must be performed in compliance with the laws in force in your jurisdiction.
- Do not submerge the DL-Axist in liquid products.
- For further information or support, refer to this manual and to the Datalogic web site: [www.datalogic.com](http://www.datalogic.com).

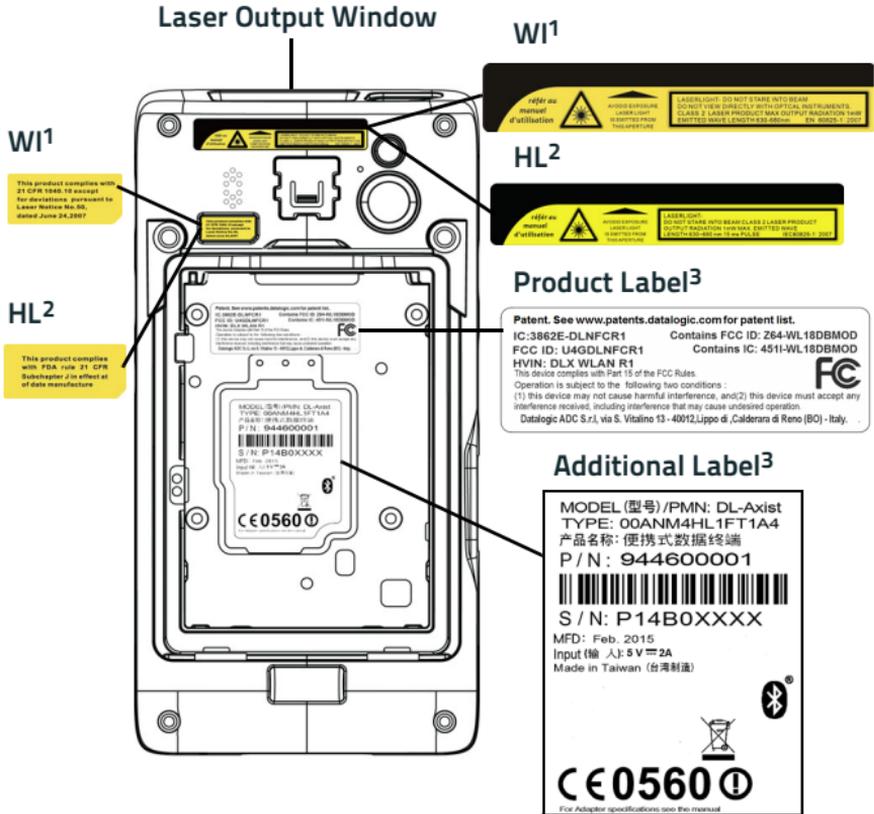
## Power Supply

This device is intended to be connected to a UL Listed/CSA Certified computer which supplies power directly to the DL-Axist or else be supplied by a UL Listed/CSA Certified Power Unit marked 'Class 2" or LPS power source rated 5 V, 2.0 A, which supplies power directly to the DL-Axist via the power connector of the cable.

The adapter package includes three international plug adapters. The adapters must be plugged in the power supply before the power supply itself is plugged on the wall outlet.

# Laser Safety

This information applies to both laser models and the DL-Axist Imager Aiming System. The laser light is visible to the human eye and is emitted from the window indicated in the figure below.



1. For models with Type containing WI.
2. For models with Type containing HL.
3. The label artworks may be only a draft. Refer to the product labels for more precise information.

**NOTE: do not remove the labels.**

LASER LIGHT - DO NOT STARE INTO BEAM  
 CLASS 2 LASER PRODUCT  
 MAX OUTPUT RADIATION 1 mW  
 COMPLIANT WITH EN 60825-1 (2007)

ITALIANO	DEUTSCH	FRANÇAIS	ESPAÑOL
<p>LA LUCE LASER È VISIBILE ALL'OCCHIO UMANO E VIENE EMESSA DALLA FINESTRA INDICATA NELLA FIGURA.</p>	<p>DIE LASER-STRAHLUNG IST FÜR DAS MENSCHLICHE AUGE SICHTBAR UND WIRD AM STRAHLAUS TRITTSFENSTER AUSGESENDET (SIEHE BILD)</p>	<p>LE RAYON LASER EST VISIBLE À L'OEIL NU ET IL EST ÉMIS PAR LA FENÊTRE DÉSIGNÉE SUR L'ILLUSTRATION DANS LA FIGURE</p>	<p>A LUZ LÁSER ES VISIBLE AL OJO HUMANO Y ES EMITIDA POR LA VENTANA INDICADA EN LA FIGURA.</p>
<p>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)</p>	<p>LASERSTRAHLUNG NICHT IN DER STRAHL BLINKEN PRODUKT DER LASERKLASSE 2 MAXIMALE DURCHSCHNITTLIC HE AUSGANGLEISTUNG: 1 mW WELLENLÄNGE: 630-680 nm ENTSPR. EN 60825-1 (2007)</p>	<p>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)</p>	<p>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)</p>

## ENGLISH

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

### STANDARD LASER SAFETY REGULATIONS

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

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



**WARNING**

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



**WARNING**

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

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



**WARNING**

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

## **ITALIANO**

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

### **NORMATIVE STANDARD PER LA SICUREZZA LASER**

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

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



**ATTENZIONE**

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

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



**ATTENZIONE**

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

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



**ATTENZIONE**

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

## **DEUTSCH**

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

### **NORM FÜR DIE LASERSICHERHEIT**

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

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



**ACHTUNG**

Unter keinen Umständen darf versucht werden, die Komponenten im Optikhohlraum zu öffnen oder auf irgendwelche andere Weise zu warten. Das Öffnen bzw. Warten der Komponenten im Optikhohlraum durch unbefugtes Personal verstößt gegen die Laser-Sicherheitsbestimmungen. Das Optiksyst $\ddot{u}$ m 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 Optiksyst $\ddot{u}$ men 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.



**ATENCIÓN**

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

## LED Class

LED illuminator integrated in the DL-Axist models are compliant with exempt risk group requirements according to IEC62471:2006 and EN 62471:2008.

## Audio Safety

To prevent possible hearing damage, do not listen at high volume levels for long periods.



## Canadian Statement

Ne pas regarder le faisceau.

Attention classe 2 lumière laser en cas d'ouverture éviter l'exposition - lumière est émise de la ouverture.

Ce produit est conforme au sous-chapitre J de CFR 21.

Pour le modèle avec TYPE qui contient deux lettres 'WI'.

Rayonnement laser – ne pas regarder dans le faisceau – ne pas regarder avec instrumentation optique - appareil à laser de classe 2 – émission maximale de 1mw – longueur d'onde émise 630 - 650nm – selon EN 60825-1:2007.

Pour le modèle avec TYPE qui contient deux lettres 'HL'.

Rayonnement laser – ne pas regarder dans le faisceau – appareil à laser de classe 2 – émission maximale de 1mw – longueur d'onde émise 630 - 650nm – 15 ms pulse selon IEC 60825-1:2007.

## Radio Compliance

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.

In AP mode, the transmission happens at channel 11.

cs Česky [Czech]	Datalogic ADC S.r.l. tímto prohlašuje, že tento DL-Axist je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES - 2011/65/EU.
da Dansk [Danish]	Undertegnede Datalogic ADC S.r.l. erklærer herved, at følgende udstyr DL-Axist overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF - 2011/65/EU.
de Deutsch [German]	Hiermit erkläre Datalogic ADC S.r.l., dass sich das Gerät DL-Axist in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG - 2011/65/EU befindet.
et Eesti [Estonian]	Käesolevaga kinnitab Datalogic ADC S.r.l. seadme DL-Axist vastavust direktiivi 1999/5/EÜ - 2011/65/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, Datalogic ADC S.r.l. declares that DL-Axist is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC and 2011/65/EU.
es Español [Spanish]	Por medio de la presente Datalogic ADC S.r.l. declara que el DL-Axist cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE - 2011/65/EU.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Datalogic ADC S.r.l. ΔΗΛΩΝΕΙ ΟΤΙ DL-Axist ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK - 2011/65/EU.
fr Français [French]	Par la présente Datalogic ADC S.r.l. déclare que l'appareil DL-Axist est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE - 2011/65/EU.
it Italiano [Italian]	Con la presente Datalogic ADC S.r.l. dichiara che questo DL-Axist è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE - 2011/65/EU.
Latviski [Latvian]	Ar šo Datalogic ADC S.r.l. deklarē, ka DL-Axist atbilst Direktīvas 1999/5/EK - 2011/65/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Lietuvių [Lithuanian]	Šiuo Datalogic ADC S.r.l. deklaruoja, kad šis DL-Axist atitinka esminius reikalavimus ir kitas 1999/5/EB - 2011/65/EU Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart Datalogic ADC S.r.l. dat het toestel DL-Axist in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG - 2011/65/EU.
mt Malti [Maltese]	Hawnhekk, Datalogic ADC S.r.l., jiddikjara li dan DL-Axist jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC - 2011/65/EU.
hu Magyar [Hungarian]	Alulírott, Datalogic ADC S.r.l. nyilatkozom, hogy a DL-Axist megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC - 2011/65/EU irányelv egyéb előírásainak.
pl Polski [Polish]	Niniejszym Datalogic ADC S.r.l. oświadczam, że DL-Axist jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC - 2011/65/EU.
pt Português [Portuguese]	Datalogic ADC S.r.l. declara que este DL-Axist está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE - 2011/65/EU.
sl Slovensko [Slovenian]	Datalogic ADC S.r.l. izjavlja, da je ta DL-Axist v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES - 2011/65/EU.
Slovensky [Slovak]	Datalogic ADC S.r.l. týmto vyhlasuje, že DL-Axist spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES - 2011/65/EU.
fi Suomi [Finnish]	Datalogic ADC S.r.l. vakuuttaa täten että DL-Axist tyyppinen laite on direktiivin 1999/5/EY - 2011/65/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar Datalogic ADC S.r.l. att denna DL-Axist står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG - 2011/65/EU.

## Information for the User

### ENGLISH

Contact the competent authority responsible for the management of radio frequency devices of your country to verify any possible restrictions or licenses required.

### ITALIANO

Contatta l'autorità competente per la gestione degli apparati a radio frequenza del tuo paese, per verificare eventuali restrizioni o licenze.

### FRANÇAIS

Contactez l'autorité compétente en la gestion des appareils à radio fréquence de votre pays pour vérifier d'éventuelles restrictions ou licences.

### DEUTSCH

Wenden Sie sich an die für Radiofrequenzgeräte zuständige Behörde Ihres Landes, um zu prüfen ob es Einschränkungen gibt, oder eine Lizenz erforderlich ist.

### ESPAÑOL

Contacta la autoridad competente para la gestión de los dispositivos de radio frecuencia de tu país, para verificar cualesquiera restricciones o licencias posibles requerida.

# FCC Compliance

## FCC Interference Statement

- 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.
- This device 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 radiated 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.

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

- The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## **IMPORTANT NOTE:**

### **FCC Radiation Exposure Statement**

This model device meets the government's requirements for exposure to radio waves. This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

The exposure standard for wireless devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6W/kg. Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the power required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output.

While there may be differences between the SAR levels of various devices and at various positions, they all meet the government requirement.

The FCC has granted an Equipment Authorization for this model device with all reported SAR levels evaluated as in compliance with

the FCC RF exposure guidelines. SAR information on this model device is on file with the FCC and can be found under the Display Grant section of <http://www.fcc.gov/oet/fccid> after searching on the below:

FCC ID: U4GDLNFCR1

This device is compliant with SAR for general population /uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in IEEE1528-2013 and published RF exposure KDB.

For body worn operation, this device has been tested and meets the FCC RF exposure guidelines for use with an accessory that contains no metal and the positions the handset a minimum of 1.5 cm from the body. Use of other enhancements may not ensure compliance with FCC RF exposure guidelines. If you do not use a body-worn accessory and are not holding the device at the ear, position the handset a minimum of 1.5 cm from your body when the device is switched on.

# Industry Canada Compliance

## IC Statement

This device complies with RSS-247; of the Industry Canada 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.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de classe B est conforme à la norme NMB-003.

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) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and.
- (iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.
- (iv) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands

5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

## **Avertissement**

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment:

(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) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5 250-5 350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5 725-5 825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

(iv) De plus, les utilisateurs devraient aussi être avisés que 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.

## **IMPORTANT NOTE:**

### **IC Radiation Exposure Statement**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 1.5 cm between the radiator & your body. This transmitter must not be co-located or operating in

conjunction with any other antenna or transmitter. IC RF Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 1.5 cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

**Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 1.5 cm de distance entre la source de rayonnement et votre corps.

## SAR Compliance

This product has been tested and found to comply with the following standards:

- IEEE1528-2013: IEEE Recommended Practice for Determining the Peak Spatial-Average Specific Absorption Rate (SAR) in the Human Head from Wireless Communications Devices: Measurement Techniques.
- EN 62311:2008: assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz – 300 GHz).
- EN 62479:2010: Assessment of the compliance of lower power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz).
- RSS102 Issue 5: Radio Frequency (RF) Exposure Compliance of Radiocommunication Apparatus (All Frequency Bands).
- EN50360:2001/A1:2012: Product standard to demonstrate the compliance of mobile phones with the basic restrictions related to human exposure to electromagnetic fields (300MHz – 3GHz).
- EN50566:2013: Product standard to demonstrate the compliance of radio frequency fields from handheld and body-mounted wireless communication devices used by general public (30MHz – 6GHz).
- EN62209-1:2006; Human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices - Human models, instrumentation, and procedures - Part 1: Procedure to determine the specific absorption rate (SAR) for hand-held devices used in close proximity to the ear (frequency range of 300 MHz to 3 GHz).

- EN 62209-2:2010: Human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices - Human models, instrumentation, and procedures - Part 2: Procedure to determine the specific absorption rate (SAR) for wireless communication devices used in close proximity to the human body (frequency range of 30 MHz to 6 GHz).

## **SAR Information (for European Union)**

Head: 0.117 W/kg@10g (CE);

Body: 0.080 W/kg@10g (CE);

This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

## **FCC SAR values**

Head: 0.432 w/kg@1g

Body -Worn: 0.068W/kg@1g

Hand: 0.438 W/Kg@10g

## **Body-worn Operation**

This device was tested for typical body-worn operations. A minimum separation distance must be maintained between the user's body and the handset, including the antenna:

0.5 cm to comply with the RF exposure requirements in Europe  
Third-party belt-clips, holsters and similar accessories used by this device should not contain any metallic components. Body-worn accessories that do not meet these requirements may not comply with RF exposure requirements and should be avoided.

## European Union Regulatory Notice

This device bearing the CE marking is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. This device complies with the following harmonized European standards. The following CE marking is valid for EU harmonized telecommunications products.

CE0560



## WEEE Compliance



### **Information for the user in accordance with the European Commission Directive 2012/19/EC**

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 degli utenti ai sensi della Direttiva Europea 2012/19/EC**

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 concernant la Directive Européenne 2012/19/EC**

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 de acuerdo con la Directiva Europea 2012/19/CE**

Al final de su vida útil, el producto marcado con un símbolo de contenedor de basura 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 Richtlinie 2012/19/EC der europäischen Kommission**

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 Homepage unter <http://www.datalogic.com>.



## Reference Documentation

For further information regarding DL-Axist refer to the SDK Help on-line.

# NOTES



## Services and Support

Datalogic provides several services as well as technical support through its website. Please check our website at [www.datalogic.com](http://www.datalogic.com) under 'Support & Services', then 'Automatic Data Capture', and click on the links indicated for further information including:

- **Downloads**
  - **Manuals** for the latest versions of user manuals and product guides.
  - **Software & Utilities** for the latest firmware release for your product. You can also click on the following link for direct access to this section: [www.datalogic.com/products\\_updates](http://www.datalogic.com/products_updates).
- **Service Program** for warranty extensions and maintenance agreements.
- **Repair Centers** for a list of authorised repair centers.
- **Technical Support Automatic Data Capture** email form to contact our technical support.

## **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.



# 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.

## 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.

## **GSM**

Global System for Mobile communication. It is a standard for digital cellular communications, currently used around the world on as many as seven bands.

## **Host**

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

## **IEC**

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

## **IEEE 802.11**

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

## IP

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

## IP Address

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

## LAN

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

## **Laser Diode**

A gallium-arsenide semiconductor type of laser connected to a power source to generate a laser beam. This laser type is a compact source of coherent light.

## **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.

## **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.

## ROM

Read-Only Memory. Data stored in ROM cannot be changed or removed.

## Scanner

An electronic device used to scan bar code 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 bar code.
- Photodetector - registers the difference in reflected light (more light reflected from spaces).
- Signal conditioning circuit - transforms optical detector output into a digitized bar pattern.

## SDK

Software Development Kit.

## Subnet

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

## **Symbol**

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

## **Symbology**

The structural rules and conventions for representing data within a particular bar code type (e.g. UPC/EAN, Code 39, PDF417, etc.).

## **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.

## **WWAN**

Stands for "Wide Area Network." It is similar to a Local Area Network (LAN), but it is not limited to a single location and it uses Mobile telecommunication cellular network technologies such as UMTS, GPRS, CDMA2000, GSM, CDPD, Mobitex, HSDPA or 3G to transfer data. WWAN connectivity allows a user with a laptop and a WWAN card to surf the web, check email, or connect to a Virtual Private Network (VPN) from anywhere within the regional boundaries of cellular service.

# NOTES

## DECLARATION OF CONFORMITY

**CE 0560**  **16**

Datalogic ADC Srl, Via S. Vitalino, 13  
Lippo di Calderara di Reno (BO) 40012 Italy

dichiara che  
declares that the  
déclare que le  
bescheinigt, daß das Gerät  
declare que el:

### DL-Axist

modelli con funzionalità radio 802.11a/b/g/n+BT+NFC  
models with 802.11a/b/g/n +BT radio feature+NFC  
modèles avec 802.11a/b/g/n +BT radio intègrés+NFC  
Modelle mit 802.11a/b/g/n +BT Radio-funktionalität+NFC  
modelos con funcionalidad radio 802.11a/b/g/n +BT+NFC

sono conformi alle Direttive del Consiglio Europeo sottoelencate:  
are in conformity with the requirements of the European Council Directives listed below:  
sont conformes aux spécifications des Directives de l'Union Européenne ci-dessous:  
den nachstehenden angeführten Direktiven des Europäischen Rats:  
cumple con los requisitos de las Directivas del Consejo Europeo, según la lista siguiente:

### 1999/5/EC R&TTE and 2011/65/EU RoHS

---

La presente dichiarazione di conformità è rilasciata sotto la responsabilità esclusiva del fabbricante ed è basata sulla conformità dei prodotti alle norme seguenti:

This declaration of conformity is issued under the sole responsibility of the manufacturer and is based upon compliance of the products to the following standards:

Cette déclaration de conformité est établie sous la seule responsabilité du fabricant et repose sur la conformité des produits aux normes suivantes:

Diese Konformitätserklärung wurde unter alleiniger Verantwortung des Herstellers ausgestellt und basiert darauf daß das Produkt den folgenden Normen entspricht:

La presente declaración de conformidad se expide bajo la exclusiva responsabilidad del fabricante y se basa en el cumplimiento de los productos con la siguientes normas:

**EN 55022: 2010 + AC:2011 (CLASS B ITE)** *INFORMATION TECHNOLOGY EQUIPMENT RADIO DISTURBANCE CHARACTERISTICS LIMITS AND METHODS OF MEASUREMENTS*

**EN 55024: 2010** *INFORMATION TECHNOLOGY EQUIPMENT IMMUNITY CHARACTERISTICS LIMITS AND METHODS OF MEASUREMENT*

**ETSI EN 301 489-1 V1.9.2:2011:** *ELECTROMAGNETIC COMPATIBILITY AND RADIO SPECTRUM MATTERS (ERM); ELECTROMAGNETIC COMPATIBILITY (EMC) STANDARD FOR RADIO EQUIPMENT AND SERVICES; PART1: COMMON TECHNICAL REQUIREMENTS*

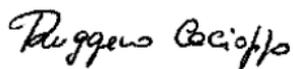
<b>ETSI EN 301 489-3 v1.6.1:2013</b>	<i>ELECTROMAGNETIC COMPATIBILITY AND RADIO SPECTRUM MATTERS (ERM); ELECTROMAGNETIC COMPATIBILITY (EMC) STANDARD FOR RADIO EQUIPMENT AND SERVICES; PART 3: SPECIFIC CONDITIONS FOR SHORT-RANGE DEVICES (SRD) OPERATING ON FREQUENCIES BETWEEN 9 KHZ AND 246 GHZ</i>
<b>ETSI EN 301 489-17 v2.2.1:2012</b>	<i>ELECTROMAGNETIC COMPATIBILITY AND RADIO SPECTRUM MATTERS (ERM); ELECTROMAGNETIC COMPATIBILITY (EMC) STANDARD FOR RADIO EQUIPMENT; PART 17: SPECIFIC CONDITIONS FOR 2,4 GHZ WIDEBAND TRANSMISSION SYSTEMS, 5 GHZ HIGH PERFORMANCE RLAN EQUIPMENT AND 5,8 GHZ BROADBAND DATA TRANSMITTING SYSTEMS</i>
<b>ETSI EN 300 328 v1.8.1:2012</b>	<i>ELECTROMAGNETIC COMPATIBILITY AND RADIO SPECTRUM MATTERS (ERM); WIDEBAND TRANSMISSION SYSTEMS; DATA TRANSMISSION EQUIPMENT OPERATING IN THE 2,4GHZ ISM BAND AND USING WIDE BAND MODULATION TECHNIQUES; HARMONIZED EN COVERING ESSENTIAL REQUIREMENTS UNDER ARTICLE 3.2 OF THE R&amp;TTE DIRECTIVE</i>
<b>ETSI EN 301 893 V1.7.1:2012</b>	<i>BROADBAND RADIO ACCESS NETWORKS (BRAN);5 GHZ HIGH PERFORMANCE RLAN;HARMONIZED EN COVERING THE ESSENTIAL REQUIREMENTS OF ARTICLE 3.2 OF THE R&amp;TTE DIRECTIVE</i>
<b>EN 60950-1:2006 AMENDMENT A11:2009 AMENDMENT A1:2010 AMENDMENT A12:20111 AMENDMENT A2:2013</b>	<i>INFORMATION TECHNOLOGY EQUIPMENT - SAFETY - PART 1: GENERAL REQUIREMENTS</i>
<b>EN 50360:2001+A1:2012</b>	<i>PRODUCT STANDARD TO DEMONSTRATE THE COMPLIANCE OF MOBILE PHONES WITH THE BASIC RESTRICTIONS RELATED TO HUMAN EXPOSURE TO ELECTROMAGNETIC FIELDS (300 MHz - 3 GHz) HUMAN EXPOSURE TO RADIO FREQUENCY FIELDS FROM HAND-HELD AND BODY-MOUNTED WIRELESS COMMUNICATION DEVICES - HUMAN MODELS, INSTRUMENTATION, AND PROCEDURES - PART 1: PROCEDURE TO DETERMINE THE SPECIFIC ABSORPTION RATE (SAR) FOR HAND-HELD DEVICES USED IN CLOSE PROXIMITY TO THE EAR (FREQUENCY RANGE OF 300 MHz TO 3 GHz)</i>
<b>EN 62209-2:2010</b>	<i>HUMAN EXPOSURE TO RADIO FREQUENCY FIELDS FROM HAND-HELD AND BODY-MOUNTED WIRELESS COMMUNICATION DEVICES - HUMAN MODELS, INSTRUMENTATION, AND PROCEDURES - PART 2: PROCEDURE TO DETERMINE THE SPECIFIC ABSORPTION RATE (SAR) FOR WIRELESS COMMUNICATION DEVICES USED IN CLOSE PROXIMITY TO THE HUMAN BODY (FREQUENCY RANGE OF 30 MHz TO 6 GHz)</i>
<b>EN 50566:2013</b>	<i>PRODUCT STANDARD TO DEMONSTRATE COMPLIANCE OF RADIO FREQUENCY FIELDS FROM HANDHELD AND BODY-MOUNTED WIRELESS COMMUNICATION DEVICES USED BY THE GENERAL PUBLIC (30 MHz - 6 GHz)</i>
<b>EN 62479:2010</b>	<i>ASSESSMENT OF THE COMPLIANCE OF LOW POWER ELECTRONIC AND ELECTRICAL EQUIPMENT WITH THE BASIC RESTRICTIONS RELATED TO HUMAN EXPOSURE TO ELECTROMAGNETIC FIELDS (10 MHz TO 300 GHz)</i>

EN50581:2012

*TECHNICAL DOCUMENTATION FOR THE ASSESSMENT OF ELECTRICAL AND  
ELECTRONIC PRODUCTS WITH RESPECT TO THE RESTRICTION OF HAZARDOUS  
SUBSTANCES*

LIPPO DI CALDERARA DI RENO, MARCH 1, 2016

RUGGERO CACIOPPO  
PRODUCT QUALITY LEADER  
DATALOGIC SPÀ

A handwritten signature in black ink, reading "Ruggero Cacioppo". The signature is written in a cursive, flowing style.

# NOTES



# **DATALOGIC**

[www.datalogic.com](http://www.datalogic.com)

©2016 Datalogic ADC S.r.l. ■ All rights reserved.  
Datalogic and the Datalogic logo are registered trademarks of  
Datalogic S.p.A. in many countries, including the U.S.A. and the E.U.

**Datalogic ADC S.r.l.**

Via S. Vitalino, 13 | Lippo di Calderara di Reno  
40012 BO | Italy | Telephone: (+39) 051-3147011  
Fax: (+39) 051-3147205



822001850

(Rev A)

May 2016