DATALOGIC

Rhino™ II

Rugged Vehicle Mount Computer

User's Manual

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

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

Disclaimer

Datalogic has taken reasonable measures to provide information in this manual that is complete and accurate, however, Datalogic reserves the right to change any specification at any time without prior notice. Datalogic and the Datalogic logo are registered trademarks of Datalogic S.p.A. in many countries, including the U.S.A. and the E.U.

Rhino is a trademark of Datalogic S.p.A. and/or its affiliates.

The Bluetooth® word mark and logos are owned by Bluetooth SIG, Inc. and any use of such marks by Datalogic Mobile, Inc. is under license.

Wi-Fi is a registered certification mark of the Wi-Fi Alliance.

Microsoft, Windows Embedded Standard 7, Windows 10 IoT and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other brand and product names may be trademarks of their respective owners.

Patents

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

Table of Contents

Introduction

Conventions

This manual uses the following conventions:

"Mobile computer", "Vehicle Mount Computer", "VMC" and "Rhino II" refer to Rhino II vehicle mount computer.

WEC7 refers to the Windows Embedded Compact 7 operating system.

WES7 refers to the Windows Embedded Standard 7 Pro operatingy system.

Win10 IoT refers to the Windows 10 IoT operating system.

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

Product Presentation

The Rhino II vehicle mount computers, available in both 10" and 12" display sizes, set the standard for ruggedness in the warehouse. A sealed design tested to IP65/IP67 ensures operation in the toughest environments. A dedicated freezer-rated model with integrated display heater allows use in and out of cold storage. The capacitive touch models feature 3 mm anti-glare armored glass, while still allowing use of gloves.

Tailored for warehouse management, the Rhino vehicle computer increases productivity through reduced errors during receiving, putaway, picking and shipping activities. Adding a handheld bar code scanner such as Datalogic's PowerScan™ allows for quick data entry and location confirmations.

The Rhino vehicle computer is equipped with an internal isolated power supply, ignition sense to automatically control the power, and an optional battery backup for the ultimate protection against data loss. The Rhino vehicle computer fits different mounting and space constraints. Mounting options include various brackets and RAM mounts for the vehicle computer along with ABCD or QWERTY external keyboards. A dedicated software keyboard includes a multitude of layouts and languages, adapting the Rhino computer to a minimum footprint and global applications.

The Rhino II computer offers a choice of Windows Embedded Compact 7 (WEC7), Windows Embedded 7, or Windows 10 IoT Enterprise operating systems. Included are various Datalogic Utilities and on the WEC7 models, Wavelink® Avalanche™ and Terminal Emulation are pre-loaded and pre-licensed, allowing the Rhino computer to maximize return-on-investment (ROI) through easy deployment, device and maintenance management.

Available Models

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

- Internal power supplies: 12-24VDC and 24-48VDC
- Screen sizes: 10" and 12"
- Operating Systems: Windows Embedded Compact 7, Windows Embedded 7 Pro, Windows 10 IoT and Android 6
- Freezer Model (WEC7 10" only)

For further details about the Rhino II models refer to the web site: http://www.datalogic.com.

The currently available models are:

- 943200008 10" Rhino II Win10 IoT 12VDC
- 943200006 10" Rhino II WES7 12VDC
- 943200004 10" Rhino II WEC7 12VDC
- 943200007 10" Rhino II Win10 IoT 24-48VDC
- 943200005 10" Rhino II WES7 24-48VDC
- 943200003 10" Rhino II WEC7 24-48VDC
- 943200002 10" Freezer Rhino II WEC7 12VDC
- 943200001 10" Freezer Rhino II WEC7 24-48VDC
- 943200022 12" Rhino II Win10 IoT 12VDC
- 943200020 12" Rhino II WES7 12VDC
- 943200018 12" Rhino II WEC7 12VDC
- 943200021 12" Rhino II Win10 IoT 24-48VDC
- 943200019 12" Rhino II WES7 24-48VDC
- 943200017 12" Rhino II WEC7 24-48VDC

Out of the Box

The Rhino II package contains:

- Rhino II vehicle mount computer
- Installation guide
- Power cable length = 2.9m (9.5')
- Bag - 4 mounting screws and washers for use with RAM mounts
- Bag - rubber cable slot seals and cable ties
- Bluetooth USB adapter (only for WES7 and Win10 IoT models)
- Safety & Regulatory Addendum
- Wavelink Avalanche Insert (WEC7 models only)
- Wavelink Terminal Emulation insert (WEC7 models only)
- End User License Agreement (EULA) Sheet

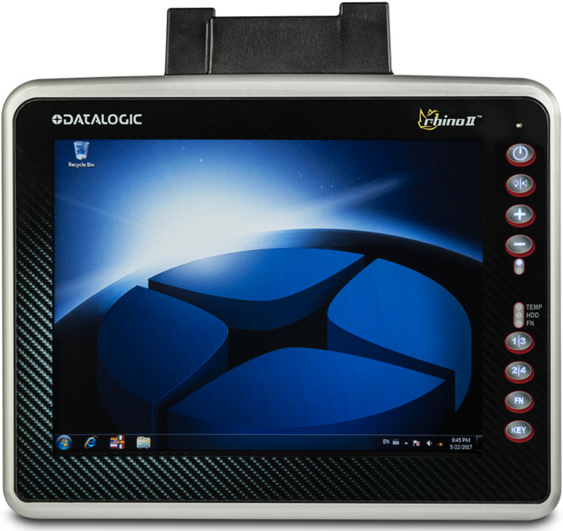
Remove all the components from their packaging; check their integrity and compare them with all the packing documents.

CAUTION

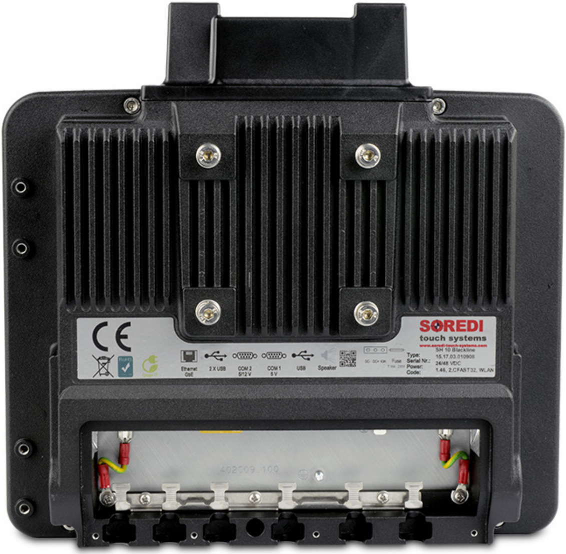
Keep the original packaging for use when sending products to the technical assistance center. Damage caused by improper packaging is not covered under the warranty.

General View

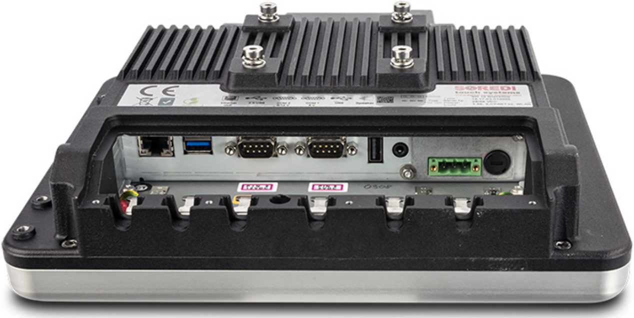
Front View



Back View


SOREDI
touch systems
Ethernet GbE
2 X USB
COM 2 5/12 V
COM 1 5 V
USB
Speaker

Bottom View



Accessories

Keyboards

95ACC1330	External Keyboard QWERTY
95ACC1374	Compact Keyboard, External, QWERTY
95ACC1331	External Keyboard, ABCD

Cable Covers

94ACC0173	Cable Cover, 5 poles, w 2.9m power cable (for quick disconnect)
94ACC0160	Speaker Cable Cover

Mounts

94ACC0172	Fixed Mounting Bracket, 130 degree
94ACC0155	Keyboard External Mounting Bracket
94ACC0175	Quick Change V Mount
94ACC0035	RAM Mount 4" rail base
94ACC0034	RAM Mount with round base
94ACC0156	Scanner holder
94ACC0154	Vehicle Mounting Bracket, 10 degree

Power Supplies

94ACC1061	AC/DC Power Brick
94ACC0165	DC Power Cable, 2.9M
94ACC0041	External 72-80 VDC Voltage Converter

⚠ CAUTION

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

Getting Started

Power On

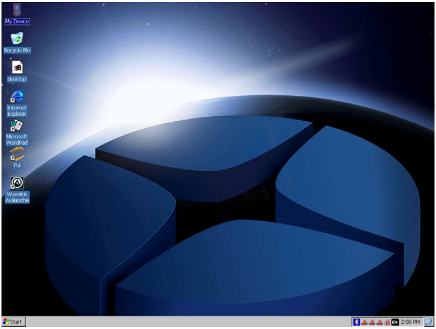
The Rhino II turns on based on its current startup mode settings (see Startup/Shutdown Modes on page 17).

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

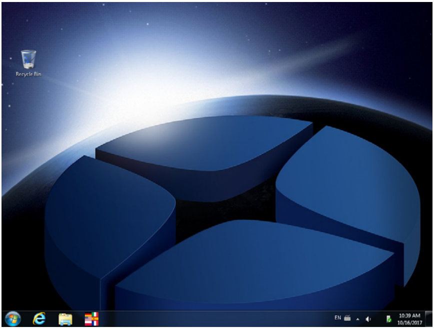
The VMC shuts down based on its current shutdown mode settings (see Startup/Shutdown Modes on page 17).

Desktop Window

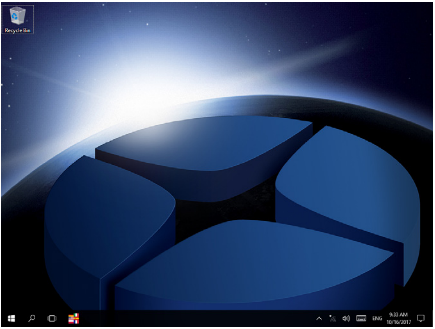
As soon as the mobile computer is on, the WEC7, Win10 IoT or WES7 desktop appears on the screen. Wait a few seconds before starting any activity so that the mobile computer completes its startup procedure.



WEC7 Desktop



WES7 Desktop



Win10 IoT Desktop

Adjusting the Screen Brightness

To adjust the screen brightness:

- Press the + button to increase the brightness.
- Press the - button to decrease the brightness.

Adjusting the Volume

To adjust the volume, press the FN button first

- Press + button to increases the volume. The computer will play the Default Sound at the new volume setting.
- Press the - button to decreases the volume. The computer will play the Default Sound at the new volume setting.

Using the Accessories

Using an External Keyboard

You can use many standard USB compatible keyboards. Datalogic recommends the use of a sealed/ruggedized key-board:

- Sealed/rugged keyboards are available from Datalogic including: full sized QWERTY, ABCD, or mini QWERTY USB keyboards
- The keyboard attaches to one of the two USB ports on the Rhino. It is automatically detected and prepared for use.

For information on installing the rugged keyboard and its mount, see the Rhino II Installation manual.

Using a Barcode Scanner

Your can use either a USB or serial scanner with the Rhino II computer. Be sure to order your scanner with the ap-propriate cable.

Connecting a USB Scanner

1. Remove the cable compartment cover plate.
2. Plug the cable into one of the USB ports. Depending on the scanner you are attaching, you may hear a series of beeps and the Good Read light may flash.
3. Choose a rubber plug for the scanner cable with the appropriate sized hole. Run the cable through the hole, then insert the plug into a slot on the terminal.
4. If desired, use a nylon tie-wrap to secure the cable to the post inside the cable compartment. Replace the cable compartment cover

5. The scanner should now be ready for use. To test, run any program that accepts keyboard input and perform a scan. If the data does not display in the application, consult the user manual for the scanner.

Connecting a Serial Scanner

COM1 provides 5VDC on pin 9, COM2 provides 12 VDC. Verify which voltage the scanner requires and connect to the appropriate COM port.

1. Remove the cable compartment cover plate.
2. Plug the cable into the desired COM port. Depending on the scanner you are attaching, you may hear a series of beeps and the Good Read light may flash.
3. Choose a rubber plug for the scanner cable with the appropriate sized hole. Run the cable through the hole, then insert the plug into a slot on the terminal.
4. If desired, use a nylon tie-wrap to secure the cable to the post inside the cable compartment. Replace the cable compartment cover
5. Configure the serial wedge program for the selected port and baud rater. See Setting Up Serial Scanning on page 127. The scanner should now be ready for use. To test, run any program that accepts keyboard input and perform a scan. If the data does not display in the application, consult the user manual for the scanner.

Resetting the Terminal

There are two reset methods for the Rhino II.

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

A clean boot restores the Rhino II to a clean configuration: both the Registry and the file system returns to a clean status that conforms to factory default (WEC7 only).

Warm Boot

To perform a warm boot, power down the terminal.

Clean Boot (WEC7 Only)

To perform a clean boot, do the following steps:

1. Launch a DOS prompt in Administrator mode
2. Change directory to \Windows
3. Run CleanBoot.cmd. CleanBoot can take up to 5 minutes, please wait for the VMC to reboot.

LED Indicators (WES7/Win10IoT)

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

LED	Status	Description
Top Blue (Top)	Solid	Wi-Fi connected
Blue (Center)	-	Not used
Blue (Bottom)	Solid	FN toggled on
Red	Solid	High Temperature Warning
Yellow	Solid	HD Access

LED Indicators (WEC7)

LED	Status	Description
Blue	Solid	FN toggled on
Red	Solid	High Temperature Warning
Yellow	Solid	HD Access

Startup/Shutdown Modes

The Rhino II has 3 modes of controlling Startup and Shutdown. The mode is set by commands in the "\Utilities\UtilConfig.cfg" file. Each mode controls how the Ignition Sense power connector wire (IGN) and the Rhino II's front panel Power button (PWR) work together. In the default mode (mode 1), IGN must be at a voltage greater than 10 VDC and PWR must be pressed and held for a specified period to power up the VMC. Shutting down in this mode may be accomplished by removing the positive voltage from IGN or pressing the PWR button, either must be for a specified time to shutdown.

The other common mode (mode 0) allows IGN or PWR to control the Startup/Shutdown. In this mode connecting IGN to positive voltage will power up the VMC, and disconnecting it will power down. Similarly powering up via PWR then pressing PWR again will power back down. If using PWR to control the VMC in this mode, IGN should NOT be switched or tied to + power. When using this mode you should either be exclusively using IGN to control the VMC, or PWR but not mixing the two.

NOTE: If the VMC is powered up via IGN, but powered down via PWR, it will immediately begin to power back up.

The final mode (mode 3) is seldom used. In this mode, the VMC will power up anytime there is power applied. Both IGN and PWR are ignored in this state.

When the VMC is being powered down by IGN, it will typically display a countdown screen advising the user the remaining time before the terminal shuts down. The shutdown time as well as whether the countdown is displayed are both controlled by the configuration file.

Configuration (in \Utilities\UtilConfig.cfg):

- PowerOnMode=1 Sets the Startup/Shutdown mode.
  - 0 = IGN or PWR
  - 1 = IGN and PWR
  - 3 = AutoOn
- IgnOffDialog=01 Display the shutdown timer window when IGN is turned off.
  - 0 = Do not display the window.
  - 1 = Display the shutdown timer window.
- IgnOffDlgType=2 Size of the shutdown timer window if enabled.
  - 0 = Full screen display, no user interaction is allowed (not recommended).
  - 1 = Medium size display, user may move the window and interact with the system.
  - 2 = Small size display, user may move the window and interact with the system.
- IgnStartTimeSec=3 Seconds after IGN goes high before the VMC begins booting.
- IgnOffDelayTimeSec=15 Seconds after IGN disconnects before the VMC shuts down.
- DelayPowerKey=100 Milliseconds PWR must be pressed before the VMC begins booting.

Front Panel Keys

There are four programmable buttons on the right side of the terminal. The programming is set by command lines in the "\Utilities\UtilConfig.cfg" file. The buttons are PWR, 1/3, 2/4 and KEY. The 1/3 and 2/4 buttons are actually programmable as two keys each, giving a total of six available keys. In normal operation these will generate the specified 1 key and 2 key values. If the FN key is pressed to set the VMC into function mode, pressing the same keys will generate the specified 3 key and the 4 key values. When FN is pressed, the blue function LED with display. Pressing 1, 2 or FN will turn the LED off and turn off function mode. By default, the buttons have the following functions:

- PWR – Starts & shutdowns the terminal depending on the current Startup/Shutdown mode.
- 1 – Up arrow.
- 2 – Down arrow.
- 3 – Escape key.
- 4 – Return key.
- KEY – Display/remove the soft keyboard from the screen.

Normally the PWR and KEY buttons should not be reprogrammed, but they are available if required.

Configuration (in \Utilities\UtilConfig.cfg). The listed values are the default values from the factory. Setting PWR and KEY to blank causes them to execute Startup/Shutdown and Softkeyboard respectively. The VK values for each key are listed in the SoftKeyboard section of this document. Multiple values can be entered for a key by using comma to separate the values. For example, the definition Frontkey_S1=#EXT=VK_TAB,VK_RETURN would cause the S1 key to transmit tab, then a return key.

- Frontkey_PWR=

- Frontkey_S1=#EXT=VK_UP
- Frontkey_S2=#EXT=VK_DOWN
- Frontkey_S3=#EXT=VK_ESCAPE
- Frontkey_S4=#EXT=VK_RETURN
- Frontkey_KEY=

The S1-S4 keys can also be used to launch executables. Just give the fully qualified name after the equal sign. For example:

Frontkey_S1=\Windows\pword.exe

will launch the WordPad program when the 1 key is pressed.

The Rhino II also provides the ability to lock the individual front panel keys. There are two keywords to control the state of the keys when the function mode is off (HWKeyLockFNOff) and when the function mode is on (HWKeyLockFNOn). Each of the keywords is an 8 bit mask, using one bit each to control the individual keys. Bits 0-7 are:

- PWR (1)
- BL (2)
- + (8)
- - (16)
- S1 (32)
- S2 (64)
- FN (128)
- KEY (256)

Setting the specific bit to a 1 will lock the respective key. For example, setting HWKeyLockFNOff=66 would disable the BL (2) and S2 (64) buttons when the function mode is not set. Setting HWKeyLockFNOn=256 would disable the KEY (256) button when the function mode is set.

NOTE

Be aware that if you are attempting to control the PWR button, you can lock the Rhino II. Disabling the PWR button at the same time you have the startup mode set to IGN and PWR will block the Rhino II from being able to be powered up.

Screen Blanking

The Rhino II has the ability to blank the screen when positive voltage is applied to a designated COM port pin. This is typically used to blank the screen when a vehicle is in motion, a requirement is some countries. For the Rhino II, an external sensor must be used that will either provide a positive voltage when the vehicle moves, or closes a relay in the same circumstance. If using a relay, then the positive voltage from pin 9 of the selected COM port should be wired as input to the relay. The output from the sensor or relay should be wired to pin 1 (DCD) or pin 6 (DSR) of the selected COM port. The screen blanking cable from Datalogic (p/n 94ACC0157) is wired to pin 9 (pink) and pin 6 (grey).

Configuration (in \Utilities\UtilConfig.cfg):

Locate (or add) the line ScreenBlankBits=X in the [General] section of the file. X should be set to the appropriate value from the list:

- 1 – COM1: DCD (pin 1)
- 2 – COM1: DSR (pin 6)
- 4 – COM2: DCD (pin 1)
- 8 – COM2: DSR (pin 6)

Deleting the ScreenBlankBits line from the cfg file will turn off screen blanking.

Keyboard Configuration File

The Configuration file is a text file built in sections to provide the definitions for the keyboard layouts. Comments can be marked at beginning of a line with a semicolon (;).

Section [Common]

In this section general settings will be defined.

Certain settings can be overridden explicitly within the definition sections of the actual keyboard data for the respective keyboard. These settings are explained separately in a 2nd table.

General Settings

Keyname	Parameter – Info
ImagePath	Directory name for all used Bitmaps within this Cfg. The specified directory is always searched in the list of the specified CFG file. A complete path specification is not supported.
KBShowOnStart=X	With this parameter a fixed specified Keyboard will be shown automatically after the start. X stands for the Keyboard-Number from the Keyboard-Config. For example, KBShowOnStart=1 always shows the Keyboard from the Cfg-Section [Keyboard_01]. If no keyboard should be visible at the start, X can be set to a invalid Number, e.g. 100 or the parameter can be left out.
SysAdminPwdKB	Specifies the defined keyboard number for a password keyboard.
SysAdminMenKB	Specifies the defined keyboard number for a SysAdmin-Menu-Keyboard.

Keyname	Parameter – Info
RotateScreen	With this you can specify the angle of rotation which is set by the key function VKX_KB_SCRROTATE. A maximum of four values are possible (0=Default-Systemstartup, 1=90°, 2=180°, 3=270°). For rotation minimum 2 values must be defined. For example RotateScreen=0,1 is defined, it will be toggled between these two angles. If the Key isn't existing or empty, all 4 values will be set one after another.

Pre Settings for Keyboards

These settings apply here for all following keyboard definitions, however, they can be explicitly overridden in the keyboard definition for special cases.

Keyname	Parameter – Info
FrameImage	*BitmapName.bmp,FrameSizeX,FrameSizeY* Bitmap for the Keyboard-Frame and to set the background. FrameSizeX defines the left and right distance to the keys. FrameSizeY defines the upper and lower distance to the keys. A keyboard without frame can be defined.
TitleBar	*0 (=Default)* With 1 the Windows title bar can here be activated for special cases.
Title	Here, any string can be defined as titles for TitleBar, e.g. "Soft Keyboard".

Keyname	**Parameter – Info**
AlphaValue	*0 (=Default – no Transparency)* Here values of 10 (almost completely transparent / invisible) to 250 (almost opaque) are accepted.
TransparentCol	*0 (=Default – not transparent respectively invisible color)* Here, a color can be set that is completely invisible in the output, i.e. the background is completely visible. This will, for example, be used to produce Window frames round corners or to paint the icons used regardless of the background color of the buttons. Usually, purple is mostly used. The colors are always in RGB notation, Example: "TransparentCol=255,0,255".
ZoomFactor	Here a maximum 10 zoom values are specified, separated by commas. The values are always specified as a percentage (e.g 200 = twice as large as normal). The starting size of a keyboard is always 100% in accordance with the key sizes specified in the keyboard definition, etc. The value 100 must not be specified separately in the Zoom list - it is automatically inserted at the beginning.
RepeatKeys	0=Off, 1=On (Default), on default the Repeat function is activated. For special Keyboards with special functions this Repeat function is mostly not desired.
AutoMove	0=Off (Default), 1=On, allows freely moving Keyboards with finger. Therefore you must press anywhere on the Keyboard and immediately start to move (wipe) it around. If this function is activated, which results in a slight delay (~ 100 ms) when releasing (or pressing) the key. If you tap the key only briefly, the key function is executed without further delay on release.

Keyname	**Parameter – Info**
AutoSnap	0=Off, 1=On (Default), the Snap function – means the snapping on the screen corners and if there is enough space also centred on the edges – only works in conjunction with the option AutoMove=1. To trigger the automatic snapping, with a short wipe the keyboard must be moved to the right direction. Only at short wiping movements (< 500 ms) the Snap function is activated If the movement of the keyboard takes longer, you can move it to any position (without snapping). The screen sizes are not supported for snapping.

Section [VolumeTouchCtrl]

This section defines the graphics used in the touch screen volume control.

Background	The bitmap displayed as the background of the volume control.
Pointer	Bitmap used to indicate the current volume.
MuteIcon	When the speaker is muted, this bitmap will be displayed.

Section [Fonts]

In this section all fonts used with the keyboard (max. 40) will be defined.

Keyname	**Parameter**
Fontname	*font name, width, height, Text (3 cols),Shadow (3 cols), shadow offset (2 cols), format*

The various fields can be assigned as follows:

Fontname	For this keyname any name can be given, according to the use of fonts. If the font definition will be used later for the keys, the font must be specified in this section.
Font name	Name of the desired and installed Windows system font.
Width	**Width** 0 will be used as default, so the font is displayed in its natural width. For special cases the character width will be stretched or compressed.
Height	The height of the font in pixels.
Text- R,G,B	In these 3 fields, the red, green, blue values for the font colors are defined. For all RGB fields values from 0-255 allowed.
Shadow - R,G,B	In this 3 fields the R,G,B values for shadow colors are defined.
Shadow offset X,Y	Shadow offset in pixels. Setting offset to 0 = no shadow.
Format	If specified, font formatting may be set to italic (I) and/or bold (B).

Example:

```
FontDef = Arial, 0,26, 0,0,0, 190,190,190, 2,2, B
FontMini = Tahoma, 0,14, 0,0,0, 190,190,190, 0,0, IB
FontSymbol = Wingdings, 0,29, 0,0,0, 190,190,190, 0,0, B
```

Section [Keys]

In this section the general and for all keyboards valid definition for the layouts of the single keys will be specified.

Max. 40 individual Key-Layouts can be created.

Keyname	**Parameter**
KeyName	*FontName, BMPNormal, BMPActive, TxtMode, IconMode, FrmXL,FrmYL, FrmTxtNormL,T,R,B, FrmTxtActL,T,R,B, FrmIconNormL,T,R,B, FrmIconActL,T,R,B*

The various fields can be assigned as follows:

KeyName	This KeyName can arbitrarily be named. If the key will be used later on the keyboard, the corresponding defined *KeyName* must be specified.
FontName	The Fontname from the [Fonts] section to be used.
BMPNormal	Bitmap for normal key display (not pressed).
BMPActive	Bitmap for active key display (pressed).
TxtMode	Here the orientation for the text output can be determined, per default the text will be displayed always horizontal and vertical centered in the key. L=left-aligned, R=right-aligned, T=top, B=bottom. Combinations like e.g. 'LT' or 'LB' are allowed.
IconMode	Orientation for Icon-Positioning, identical to *TxtMode*.
FrmXL, FrmYL	Here special frame values for the allocation of Bitmaps (*BMPNormal + Active*) can be set to create bigger or smaller Buttons. Normally it isn't necessary and the values should be left empty.

FrmTxtNormL,T,R,B	Position frame for the text output in normal keys. With the values L=Left,T=Top,R=Right,B=Bottom substituting the distances of the text output to the side edge. This is necessary so that the text will not be written over the 3D-Frame of a key by left-aligned output.
FrmTxtActL,T,R,B	Position frame for the text output at active/pressed keys. The frame for the active Display will be specified in 1-3 Pixel (depends on key size). In this case the effect of a pressed key will appear.
FrmIconNormL,T,R,B	Position frame for the Icon output of normal keys.
FrmIconActL,T,R,B	Position frame for the Icon output of active/pressed keys.

Section [Keyboard_XX]

This section provides the actual definition of the keyboards. Max. 20 Keyboards (XX = 01-20) are possible for each Cfg-File. A Keyboard Definition is only recognized as valid if at least the line **"L01_Norm"** is defined in the section (see description below).

With horizontal screen orientation (Landscape), the default definitions are read, for example, **[Keyboard_01]**.

In vertical orientation (Portrait-Mode), first the system tries to read the keyboard definition from the Section **[Keyboard_XX_Portrait]**, for example from **[Keyboard_01_Portrait]**.

If nothing is defined in the Portrait-Section (at least **L01_Norm**) or the section doesn't exist, the default landscape will be used.

General Settings

Keyname	**Parameter – Info**
Name	Individual Name for the Keyboard. This name can be shown optional in the Title bar (or can be eventually be used later to control the keyboards).
DefaultKeyName	Here the KeyName layout from the [Keys] section will be specified, which will be used for all keys.
DefaultKeySize	XLength,YLength Standard-Key size for this Keyboard in Pixels.
Position	XPos,YPos Start position of the keyboard in pixels. Should the keyboard be moved by the user, this new position is stored in the registry for each keyboard and used in subsequent starts.
CloseOnClick	0=Off (Default), 1=On, this mode automatically closes the keyboard after pressing or executing a button.

Keyname	Parameter – Info
CloseToggle	0=Off (Default), 1=On, an open keyboard with this mode, by a repeated call (e.g. carry out by a key or a HW-Key) can be closed again.
CloseOnTimer	0=Off, Value >= 1000 specifies a timeout value in milliseconds for this keyboard. If the timer runs out, the keyboard will be automatically closed. A keystroke on the keyboard will start the timer each time again.

Definition of Keyboard-Layouts

The definition of the keyboard layout is done in single lines. For each line 3-Cfg Keys are possible, according to the status of the special keys. Max. 20 key lines can be defined per keyboard.

The overall size of the keyboard is automatically calculated based on the contained buttons.

Keyname	Parameter – Info
LXX_Norm	Definition of the Key row XX for the normal key status.
LXX_Shift	Definition of the Key row XX for the status at pressed Shift-Key.
LXX_AltGr	Definition of the Key row XX for the status at pressed AltGr-Key.

For XX any number from 01-20 can be specified.

The Syntax is always the same, e.g.: **LXX_Norm=Key1¦Key2¦Key3¦...¦**

It is important that even the last keymust always must be terminated with the vertical bar character '¦'.

The number of keys within a row is not explicity limited, but no more than 300 keys per keyboard can be defined. Overlapping keys will not be checked, the definition must be correct at any time.

Syntax of a Key Definition

The syntax of a key is constructed as: "**`#Command;VK_CODE;Text¦`**"

Single Fields and Commands will be separated through a Semicolon (;).

Each Key must be finished with the vertical bar character ("¦" Ascii-Code=124).

Special Commands will be introduced with the Character "#".

Should one of these reserved characters be indicated in the text or as a key code, the Hex-Code must be used:

- " | " = "0x7C"
- "#" = "0x23"
- ";" = "0x3B"

The fields "**`#Command`**" and "**`Text`**" are optional, so that a minimum definition can look like: "A | "

The generated Key code as well as the label of the key is defined with "A". This works with single characters only. For other special keys, special "Virtual Keycodes (VK)" are defined. (See table below).

If in a text for a key the combination "0x0A" is used, it will enforce a word-wrap in the label of this key.

Example: "Row 1 **0x0A** Row 2"

However the possibility of vertical centering will be lost if using word-wrap.

Commands for Key Definitions

Important: Position fixes and changes are evaluated only in the "LXX_**Norm**" line. The Shift and AltGr-definition position changes are ignored, as it could otherwise lead to conflicting data.

#ICON=<file>	Set Bitmap-Icon for this Key. This icon can also be used for different color designed keyboards, it should be drawn on transparent background. If <file> has no file ending automatically ".bmp" is appended.
#KDEF=<key>	Enables a new Key-layout <key> (from Section [Key]) for this and all subsequent keys of that row. For new lines, the layout is always automatically reset to the *DefaultKeyName*.
#KUSE=<key>	Sets the key layout <key> (from Section [Key]) explicitly for the current key.
#KUSE2=<key>	Sets a 2nd Key-Layout for a 2nd Text.
#KXL=<Size>	Change the length of the actual Key to <*Size*>. **<Size>** is evaluated as a floating point number and returns the size relative to **DefaultKeySize**. Example: "1" corresponds exactly to *DefaultKeySize*, "1.5" 150% of the size and "2" 200% of the default size.
#KYL=<Size>	Change the height of the actual key to <*Size*>.
#YADD=<Size>	Change the general Y-Position for the key positioning. When setting the first key, for example all following lines/keys can be deducted from the upper keys.
#SP=<Size>	Adds an appropriate distance before the current key.
#EXT=<name>	Allows the definition of several key codes with one key. For a detailed description see the following section.
#VXT=<name>	Allows the direct definition of key codes for one key. The format is identical to #EXT certainly with #VXT the data's can directly be written into the Key definition, the bypass over a Key in the [ExtendedKeys]-Section is here not necessary.

#EXEC=<exedef>	Executing of Windows-Shell-Commands. In <exedef> defined Name must indicate a definition from the Section [Execute]. In the Execute section all commands must be defined and grouped together to perform.

#KUSE2 for Creative Inscriptions

With #KUSE2 a complete 2nd Layout for a key from the section [Keys] can be set. #KUSE2 must be always at the end of the Keydefinition. The first Keytext should be explicit defined with 'Text'.

The fields *BMPNormal*, *BMPActive* of the KUSE2-Layouts will always be ignored.

#KUSE2 always applies only to the definition of a current key.

Example:

L05_Norm = ...|VK_F1;"F1";#KUSE2=<*Layout2*>;"This is the KUSE2 Text :-)"|...

L05_Norm = ...|VK_F1;"F1";#KUSE2=<*Layout2*>;"This is 0x0A two lines added"|...

Keycodes definition with #EXT

If you want to assign a key with multiple codes, this is done by means of **#EXT** definition within a key definition. Using #EXT only the symbolic name of the definition is indicated. The actual definition of each key code will be executed in the section **[Extended Keys]**:

DefName1=Key1,Key2,Key3,.....

DefName2=Key1,Key2,Key3,.....

In the section a maximum of 20 different strings can be defined with multiple key codes. The maximum length of the symbolic name DefName is 50 characters. In a definition (in a row) a maximum of 100 key codes may be defined. As a separator between different codes a comma is used. To generate a comma, this can be done through the name VK_COMMA.

To assign a keyboard key with Ctrl-Alt-Delete, the following definition must be specified:

DefName=#CTRL_ALT_DEL

Before releasing a Key sequence, all other Keys will be "released" to prevent problems with mixing of keystates like Shift, Control and Alt.

Example:

```
[ExtendedKeys]
MyTestString  = This is a test!
TextExt1      = @
TestExt2      = VK_ALTGR,q
Special       = VK_ESCAPE,VK_F1, This was ESC and
F1

[Keyboard_XX]
L01_Norm      =
^|#EXT=MyTestString;1|2|3|4|5|6|7|8|9
L01_AltGr     =     |   |#EXT=Special;²|³|   |   |
|{|[|]|}|\|
```

Like in the above example TestExt+2 shown, Keys can be generated through different definitions.

If you have problems with specific combinations try explicitly the respective left and right code definitions of Special Keys, e.g. VK_LCONTROL, VK_RSHIFT, etc. ...

Status keys as VK_SHIFT, VK_CONTROL, etc. ... always affect only the directly following 'real' key. For example should F5 are pressed with Shift and F6 with Shift + Control, it must be specified as follows:

```
Special       =
VK_SHIFT,VK_F5,VK_SHIFT,VK_CONTROL,VK_F6
```

Section [Execute]

In this Section programs for availability with Soft Keys can be defined. Using a key definition with EXEC# = <ExecDefineName>, the key can launch the defined program.

Execute Assignments are only allowed for normal user keyboards. In Soft-Keyboards, for example appears in UAC-, System- or Login-Screens, the execution of any Program is permitted. To prevent a possible mixing or problems with the KB-definition, the following settings allow defining a separate logon keyboard.

The Section Keyboard also includes other general settings and is described in SorediService documentary.

File: SoftConfig.cfg

Section: [Keyboard]

Settings:

LogonKeyboardCfg=<...Path...LogonKeyboardConfig.cfg>

The format of the definitions in the Execute section looks like this:

ExecName = ProgramName,Callparameter,Directory

Example:

```
[Execute]
InternetAddress=‘www.google.de‘
ElevatedApp=^calc.exe
Network=control,netconnections
CtrlPanel=control
AdminTaskMan=runas.exe,/user:administrator taskmgr.exe.
```

System-Admin and Password-Keyboard

The system admin menu or keyboard is always linked with the upstream password entry.

The behaviour is defined as follows:

- If the SysAdmin-Menu is **not active** at pressing the KEY-Button, always the entry password dialog appear.
- If the SysAdmin-Menu is **active** at pressing the KEY-Button the normal Keyboards like usually will be fade in or fade out.
- If the SysAdmin-Menu will be exit, all normal open Keyboards will be closed automatically.

Both keyboards in the [Common] section of the Keyboard Config be activated as follows:

SysAdminPwdKB=Num

SysAdminMenKB=Num

For Num the Number of the corresponding Keyboard-configuration will be specified.

These Special-Keyboards, always should be specified after the normal Keyboards.

If the Password-Keyboard for example is defined in the Section [Keyboard_10] the above entry would look like: SysAdminPwdKB=10.

Attention:

With SysAdmin....KB defined Keyboards, means Keyboards which will be started at UAC/System- and Login-Sessions will NOT be read in and therefore they don’t have any meaning.

Password Keyboard

The Password-Keyboard can be configured like any other Keyboard. A complete Keyboard (incl. Letters) can be configured below the entry field.

The Password-Keyboard appears after pressing onto the KEY-Button, if the SysAdmin-Menu is not open. Another push on the KEY-Button deletes the password keyboard from the screen.

When configuring the password keyboards 2 Key codes are of particular importance:

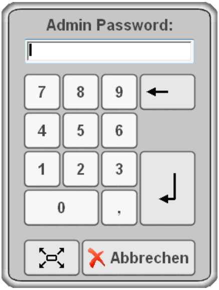
VK_ESCAPE = Escape (deletes the KB from Screen)

VK_RETURN = input (entry) ready

After receiving VK_RETURN the Password will be proved.

If the password is wrong a error message appears.

If the password is correct, the SysAdmin-Keyboard will open.



Special Settings Password Keyboard

Special Keys for configuration of password keyboards in the [Keyboard_XX] Section:

Key	Default	Info
KeyDialog=DlgInputLine	-	To enable the Password entry, this key is mandatory with the assigned registry.
KeyDlgPassword=X	-	For X any password can be defined. It is only important, that all characters of the password must be defined and shown in the Password-Keyboard.
KeyDlgText=Text	Password Input	For Text any text can be entered, which will prompt the PID input via the input line.
KeyDlgFont=FontDef	-	Here a Font definition from the Section [Fonts] can be given. The Text from KeyDlgText is then output with this.
KeyDlgColor=R,G,B	-	Here the Color value of a typical Keyboard-Background-Color should be specified. In this case the displayed Pwd-Dialog will be output in the same color. For the silver-grey Soft-Keyboard it is for e.g.: 198,198,198.
KeyDlgPwdErr=ErrText	Invalid Password !	For ErrText any Error-Message can be defined. This will be shown after a wrong Pwd-Input in the MsgBox. A line break can be specified with "\ n".

Key	Default	Info
KeyDlgPwdBlock=X	5	For X any number can be specified. This gives a fixed waiting time in minutes. If a wrong password is entered 3 times the Password-Dialog cannot be called up for the duration of the specified waiting period. If a 0 is specified, it will not be blocked.
ExcludeChain=1	0	With 1 this Keyboard will not be considered at fading in/out of the normal Input-Keyboards.
StartupHide=1	0	With 1 this keyboard is prevented from displaying at startup - regardless of the previous state.

SysAdmin-Menu Keyboard

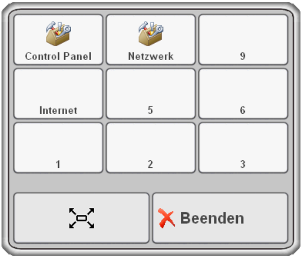
The Admin Menu Keyboard displays after successful password entry through the above password keyboard. For proper function this menu keyboard is configured according to the following section.

This Menu-Keyboard contains always a special Key to Exit. This Key must be defined with the Keycode **VKX_KB_HIDE**.

Example: |#KXL=1.5;**VKX_KB_HIDE**;#ICON=Cancel;"Cancel"|

During this Menu-Keyboard is open, over the KEY-Buttons of the unit all other Keyboards can fade in/out normally.

If the Menu-Keyboard will be Exit, all other „normal' open Keyboards will exit as well and after pressing the KEY-Button the Password-Menu appears again.



Special Settings SysAdmin-Menu Keyboard

Special Keys to configure System-Admin Keyboards in the [Keyboard_XX] Section:

Key	Default	Info
ExcludeChain=1	0	With 1 this Keyboard will not be considered at fading in/out of normal Input-Keyboards.
StartupHide=1	0	When 1 this Keyboard will be prevented from being shown at start – independent from the previous Status.
NormalWin=1	0	With 1 the Admin-Menu will be set in a way, that it looks like a normal Window and for example at Start/Click on a different Application moves to the background.
PushForeground=0	1	When 1 the Admin-Menu is pevented from automatically moving back in the foreground again.
ShowInTaskbar=1	0	Because the Admin-Menu might be behind other Apps, it should be visible in the Taskbar (if shown) to activate it again.
Title=<Keybd.Title>	-	Name of keyboards which will be shown in the Taskbar.
ElevateAdmin=X	0	With this setting (ElevateAdmin=1) the Admin-Menu-Keyboard can be started in the Elevated-Mode. In this case all other Keyboards opened with KEY-Buttons are in the elevated Mode.

Otherwise, the keyboard can be configured as a normal keyboard with any buttons. This keyboard has the opportunity to create Keys with executable programs or batch jobs.

Virtual Keycodes

Special Function Codes

The following Function codes can be used to define Keys for special functions.

VKX_KB_MOVEBUT	Moving function for the Keyboard.
VKX_KB_ZOOM	Zoom function for the keyboard. By pressing this key, the next Zoom level will be activated. (See ZoomFactor on page 25)
VKX_KB_SWITCHTO=<kbdnum>	Switches the keyboard to <kbdnum>.
VKX_KB_HIDE	Deletes the actual keyboard from the screen.
VKX_KB_KBOPEN=<kbdnum>	Open the dedicated keyboard. The actual keyboard remains unchanged displayed (unless it isn't defined with the Mode CloseOnClick).
VKX_KB_SCRROTATE	Rotates the screen orientation by 90°. The orientation actually will not be stored. After restart the unit will display again the default orientation.
VKX_KB_UPDO	Change the Keyboard-Position from the upper edge downward and vice versa. The vertical X-Position will not change.
VKX_KB_KEYLIGHT	After pressing on this Button the lighting mode of the HW-Keys will be switched between the 4 possibilities.
VKX_KB_VOLUMEDLG	Open the dialog to set the volume.

VKX_KB_HWKEYLOCK	Blocks the HW-Toolbar completely (default). This changing will not stored.
VKX_KB_HWKEYSCAN	Turns the whole HW-Toolbar for scanning on. This changing will not stored.
VKX_KB_HWKEY_NORM	Release the HW-Toolbar for normal use.

General Keyboard Codes

VK_SEPARATOR
VK_BACK
VK_TAB
VK_CLEAR
VK_RETURN
VK_SHIFT
VK_CONTROL
VK_MENU
VK_PAUSE
VK_CAPITAL
VK_ESCAPE
VK_SPACE
VK_PRIOR
VK_NEXT
VK_END
VK_HOME
VK_LEFT
VK_UP
VK_RIGHT
VK_DOWN
VK_SELECT

VK_F2
VK_F3
VK_F4
VK_F5
VK_F6
VK_F7
VK_F8
VK_F9
VK_F10
VK_F11
VK_F12
VK_F13
VK_F14
VK_F15
VK_F16
VK_F17
VK_F18
VK_F19
VK_F20
VK_F21
VK_F22
VK_F23

VK_PRINT
VK_EXECUTE
VK_SNAPSHOT
VK_INSERT
VK_DELETE
VK_HELP
VK_LWIN
VK_RWIN
VK_APPS
VK_NUMPAD0
VK_NUMPAD1
VK_NUMPAD2
VK_NUMPAD3
VK_NUMPAD4
VK_NUMPAD5
VK_NUMPAD6
VK_NUMPAD7
VK_NUMPAD8
VK_NUMPAD9
VK_MULTIPLY
VK_ADD
VK_SEPARATOR

VK_F24
VK_NUMLOCK
VK_SCROLL
VK_LSHIFT
VK_RSHIFT
VK_LCONTROL
VK_RCONTROL
VK_LMENU
VK_RMENU
VK_NUMRET
VK_CIRCUMFLEX
VK_SHARP_S
VK_ACCENT
VK_PLUS
VK_GER_UE
VK_GER_OE
VK_GER_AE
VK_NUMSIGN
VK_COMMA
VK_POINT
VK_SMALLER

VK_SUBTRACT
VK_DECIMAL
VK_DIVIDE
VK_F1

VK_MINUS
VK_ALTGR

Upgrading the Rhino II WEC7 Firmware

When you upgrade the Rhino II software, you are updating the operating system (OS), the radio drivers and the Datalogic specific software.

There are three steps involved to upgrade your Rhino II computer:

1. Download the upgrade cab file from the Datalogic website.
2. Make the upgrade file accessible to the Rhino II computer. This can be done by;
    a. Attaching a USB External storage device, such as a USB Memory Drive, USB External Hard Disk, or USB External Card reader.

    b. Downloading the file via an Ethernet connection to put the upgrade file onto the internal disk.

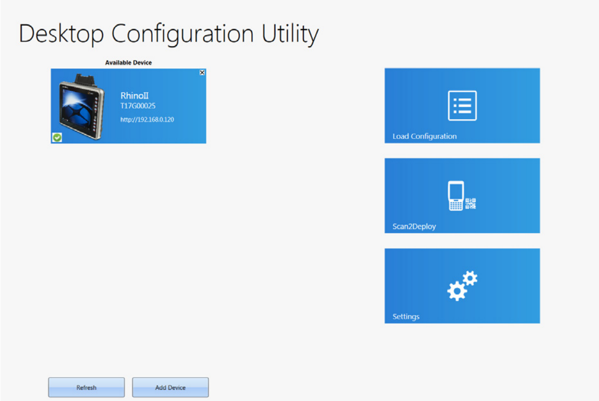
    c. Using a shared drive on the network.
3. Double click on the .cab file to install the new firmware.

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 Rhino II that connects either directly to a PC via USB or remotely over a network, either via Ethernet or Wi-Fi. DXU reports information about currently connected devices.



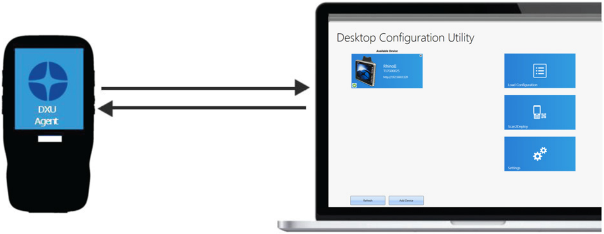
DXU can configure a wide variety of device parameters, including the touch screen and the keyboard, interfaces such as Wi-Fi, Bluetooth, USB, and Ethernet, device settings such as date, time, time zone, and power management, and security settings such as password access. DXU can also configure communication 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 Rhino II users can scan to quickly connect to DXU, called Scan2Deploy. DXU also offers the capability to create barcodes that can completely configure the device by scanning specific configuration barcodes alone, without connecting to DXU via USB or via a network. This feature may prove helpful for configuring devices that operate in environments that forbid the use of networked computers.

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

How DXU Works

DXU is really two applications working together. The DXU desktop application runs on a Windows PC, providing convenient UI to configure the Rhino II. 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 Rhino II 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 to devices on your network.

Ask your network specialists for more information.

Installation

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

Supported Windows Versions

Windows Vista family

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

Windows 7 family

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

Windows 8 family

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

Windows 8.1 family

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

Windows 10 family

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

Unsupported Windows Versions

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

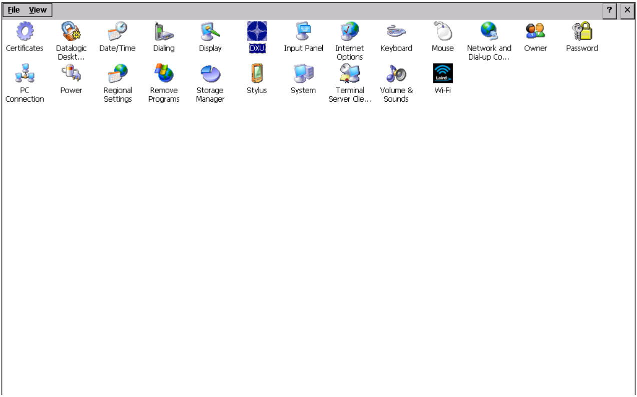
How to Install DXU

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

Controls

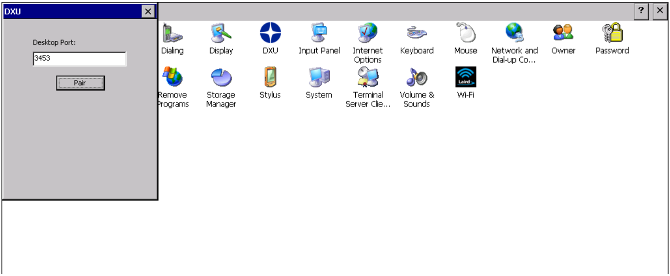
DXU Agent Controls

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



The following options are available in the DXU control panel:

1. **Desktop Port** number – needs to match setting on DXU Desktop. Requires warm boot for change to take effect.
2. **Pair** – Button to broad case UDP packets to automatic discovery of device by DXU Desktop.



Desktop Port: 3453

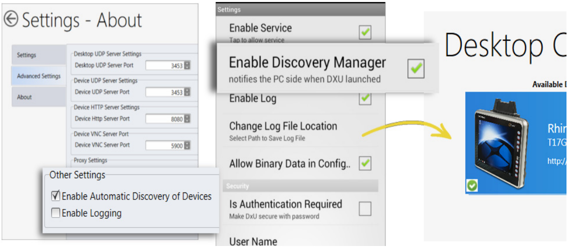
Version

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.



Settings - About

Settings
Advanced Settings
About

Desktop UDP Server Settings
Desktop UDP Server Port 3453

Device UDP Server Settings
Device UDP Server Port 3453

Device HTTP Server Settings
Device Http Server Port 8080

Device VNC Server Port
Device VNC Server Port 5900

Proxy Settings

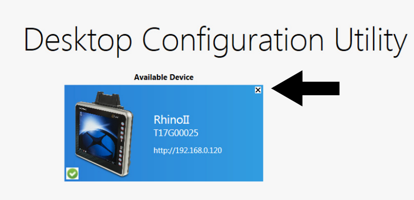
Other Settings
☑ Enable Automatic Discovery of Devices
☐ Enable Logging

Settings
Enable Service ☑
Tap to allow service
Enable Discovery Manager ☑
notifies the PC side when DXU launched
Enable Log ☑
Change Log File Location
Select Path to Save Log File
Allow Binary Data in Config.. ☑
Security
Is Authentication Required ☐
Make DxU secure with password
User Name

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 Rhino II to a network, even on the same subnet as the PC running DXU, will not automatically display as being available. The device must try to connect to DXU, which sends an announcement packet to DXU. This can be done by scanning Scan2Deploy barcode labels. However, connecting a device to the PC running DXU via USB will automatically display it in DXU. You will need to enter the DXU control panel on the device and press the Pair button in order to Automatic Discovery of Devices to properly function.

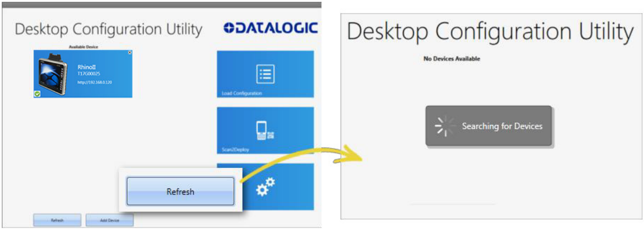
To configure a connected device, you simply click its button under Available Devices to load its configuration into DXU.

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



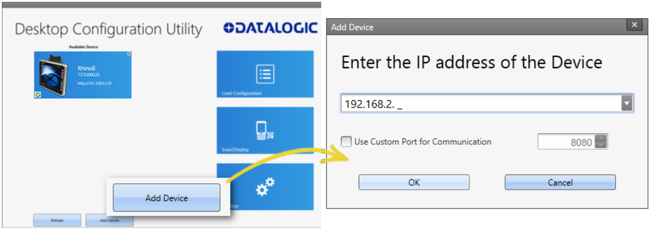
Refresh

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



Add Device

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



Enter the IP address of the Device

192.168.2. _

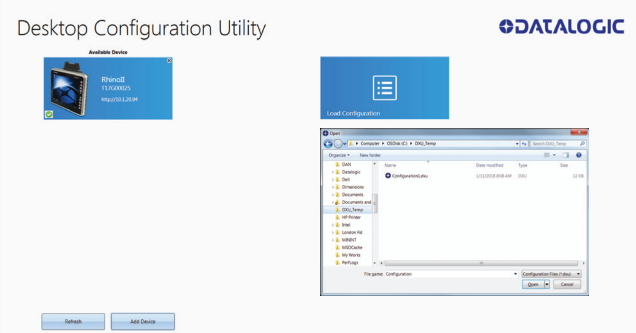
□ Use Custom Port for Communication 8080

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

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

Load Configuration

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



Name	Date modified	Type	Size
Configuration1.dxu	1/11/2018 8:08 AM	DXU	12 KB

File name: Configuration

To load a configuration:

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

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

Simplified Deploy

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

In order for Simplified Deploy to function:

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

Manifest File

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

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

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

Manifest File Format

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


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


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

WEC7 Example

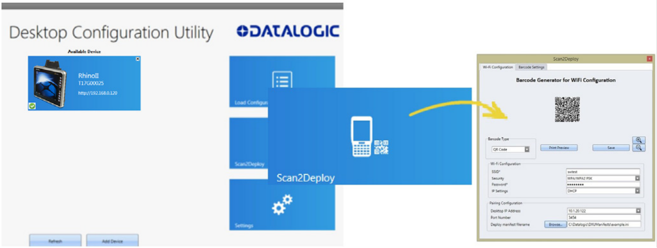
```
[update] firmware.img


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


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

Scan2Deploy

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



Barcode Type: QR Code

Wi-Fi Configuration
SSID*: swtest
Security: WPA/WPA2 PSK
Password*: ••••••••
IP Settings: DHCP

Pairing Configuration
Desktop IP Address: 10.1.20.122
Port Number: 3454
Deploy manifest filename: C:\Datalogic\DXUManifests\example.ini

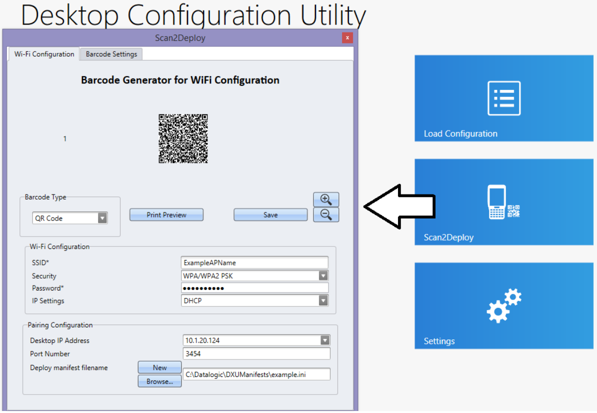
The **Scan2Deploy** button located on the main DXU page does not require an active connection to a device to create a Scan2Deploy barcode label. This button opens the Scan2Deploy dialog box streamlined to create Scan2Deploy labels that can automatically connect a device to a Wi-Fi access point on your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

Printing a Simplified Deploy Barcode

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

To print this barcode, from DXU desktop:

1. Launch **Scan2Deploy**.



Barcode Generator for WiFi Configuration

Barcode Type: QR Code

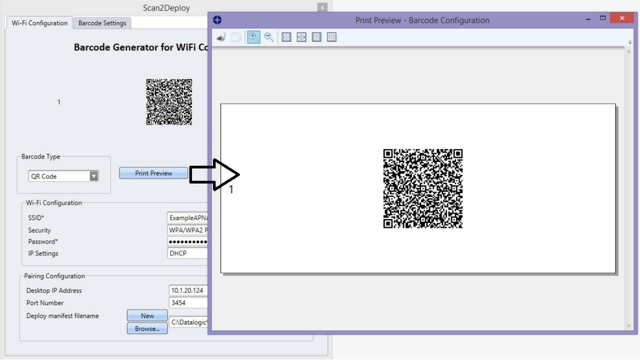
Wi-Fi Configuration

SSID*: ExampleAPName
Security: WPA/WPA2 PSK
Password*: ••••••••••
IP Settings: DHCP

Pairing Configuration

Desktop IP Address: 10.1.20.124
Port Number: 3454
Deploy manifest filename: C:\Datalogic\DXUManifests\example.ini

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



Barcode Type: QR Code

Wi-Fi Configuration

SSID*: ExampleAPNa

Security: WPA/WPA2 P

Password*: ••••••••••

IP Settings: DHCP

Pairing Configuration

Desktop IP Address: 10.1.20.124

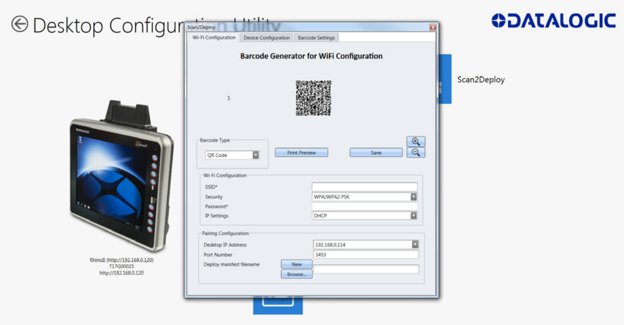
Port Number: 3454

Deploy manifest filename: C:\Datalogic\

Printing Custom Configuration Barcodes

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

While it is possible to generate a Simplified Deploy barcode using this window, it has the additional flexibility presented in the **Device Configuration** tab, which allows printing barcodes to configure the device without the need of the PC with DXU desktop being accessible from the Wi-Fi network.



Barcode Generator for WiFi Configuration

Barcode Type: QR Code

Wi-Fi Configuration
- Security: WPA/WPA2 PSK
- IP Settings: DHCP

Pairing Configuration
- Desktop IP Address: 192.168.0.114
- Port Number: 3453
- Deploy manifest filename

Wi-Fi Configuration Tab

Barcode Type Menu

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

QR Code

Aztec

Data Matrix

PDF417

Code 128

QR Code, Aztec Code, and Data Matrix are 2D barcodes that offer high data density and larger capacity, but require 2D scanners to scan them. PDF417 is a stacked linear barcode that offers moderate data density and larger capacity than linear symbologies. Code 128 is a linear symbology that can be scanned by laser scanners, but its data capacity is low, which may result in a great many individual labels to be scanned in order to fully configure a device remotely.

Print Preview

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

Save Button

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

Wi-Fi Configuration Controls

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

WARNING

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

Pairing Configuration Controls

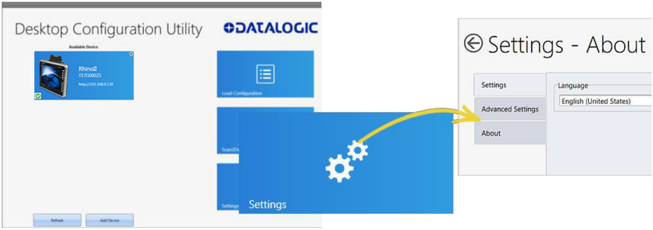
These fields let you configure your connection to the PC you are running DXU on. These fields are filled in automatically, but you can change them to deliberately connect to another IP address where another instance of DXU is running, for example.

Barcode Settings

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

Settings Window

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



Desktop Configuration Utility

Available Device

RhinoII
T17G00025
http://192.168.0.120

Settings - About

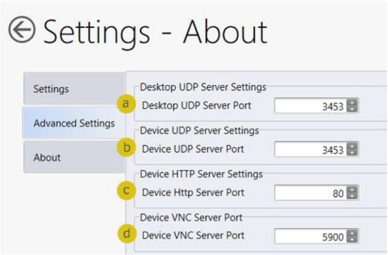
Language: English (United States)

Language Tab

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

Advanced Settings Tab

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



Settings - About

Desktop UDP Server Settings
Desktop UDP Server Port: 3453

Device UDP Server Settings
Device UDP Server Port: 3453

Device HTTP Server Settings
Device Http Server Port: 80

Device VNC Server Port
Device VNC Server Port: 5900

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

About Tab

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

Desktop Configuration Utility View

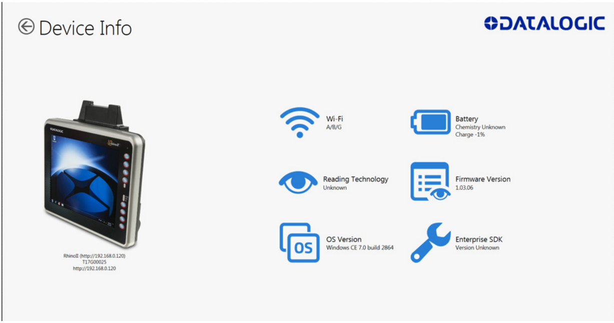
This is the view you see when you click on a device's button in the **Available Device** list. It displays a large picture of your device's model, along with the model name and serial number.

Configure this Device Button

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

Device Info Button

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



RhinoII (http://192.168.0.120)
T17G00025
http://192.168.0.120

Wi-Fi
A/B/G

Battery
Chemistry Unknown
Charge -1%

Reading Technology
Unknown

Firmware Version
1.03.06

OS Version
Windows CE 7.0 build 2864

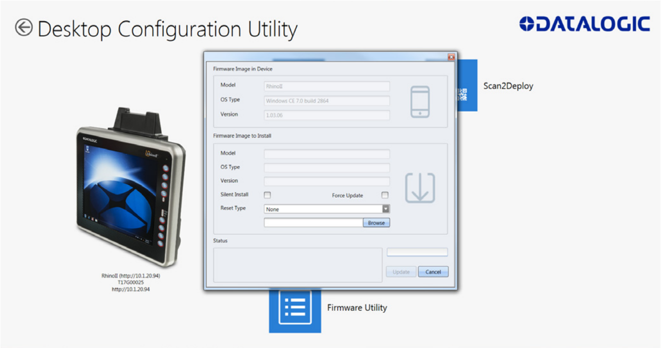
Enterprise SDK
Version Unknown

Remote Control Button

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

Firmware Update Utility Button

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



Desktop Configuration Utility

Firmware Image in Device

Model: RhinoII
OS Type: Windows CE 7.0 build 2864
Version: 1.03.06

Firmware Image to Install

Model:
OS Type:
Version:
Silent Install □ Force Update □
Reset Type: None

Status

Scan2Deploy Button

Clicking this button opens the **Scan2Deploy** dialog box (see see 'Printing Custom Configuration Barcodes" on page -65). Use it to create Scan2Deploy barcode sets that can fully configure a device without network access to DXU on your PC, containing all configuration settings in one set of barcodes and applying them by scanning the labels - all without the need to use Simplified Deploy.

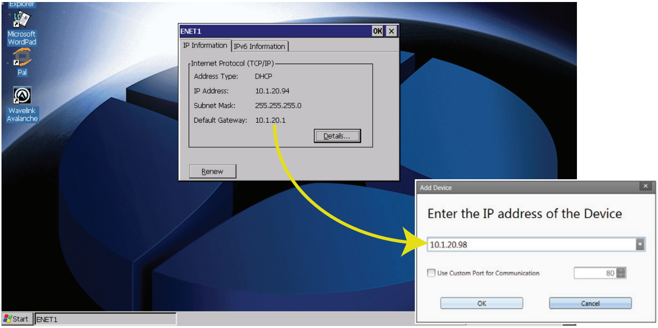
Tasks

Connect to a Device via Network Manually

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

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

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



Internet Protocol (TCP/IP)

Address Type: DHCP

IP Address: 10.1.20.94

Subnet Mask: 255.255.255.0

Default Gateway: 10.1.20.1

Enter the IP address of the Device

10.1.20.98

□ Use Custom Port for Communication 80

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

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

3. Click **OK** to complete.

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

NOTE

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

Connect to a Device via Network Using Scan2Pair

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

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

NOTE

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

4. Click **Print Preview**.
5. Click **Print** in the button bar.
6. Since **Print** dialog boxes vary by the model of your printer, configure the print as you normally do. Close these dialog boxes to exit.
7. Click **Start menu** > **Programs** > **Device Tools** > **Scan2Deploy**.

NOTE

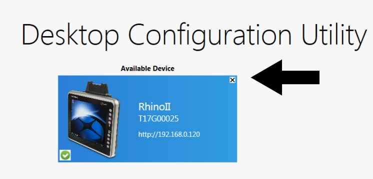
Scan to Configure, also under Device Tools, allows you to configure a Wavelink Avalanche barcode to configure.

8. Scan the barcode.

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

Delete a Device from the Available Device List

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



Desktop Configuration Utility

Available Device

RhinoII
T17G00025
http://192.168.0.120

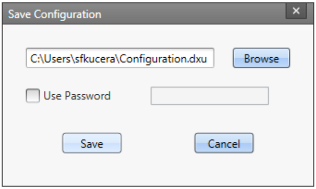
Configuration Files

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

Save a Configuration File

To save a configuration file, follow the steps below:

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



C:\Users\sfkucera\Configuration.dxu

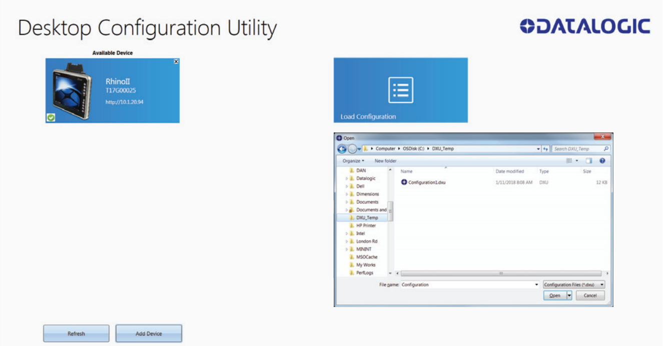
□ Use Password

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

Open a Configuration File

To load a configuration file previously saved, do this:

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



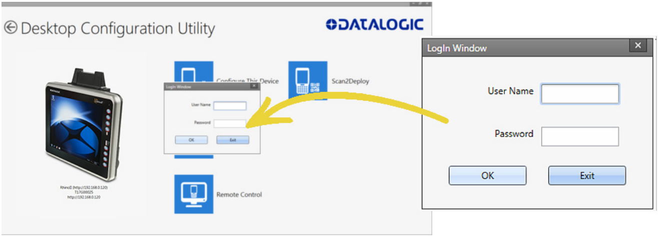
Name	Date modified	Type	Size
Configuration1.dxu	1/11/2018 8:08 AM	DXU	12 KB

File name: Configuration

Configuration Files (*.dxu)

Open a Configuration File Which is Authenticated

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



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

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

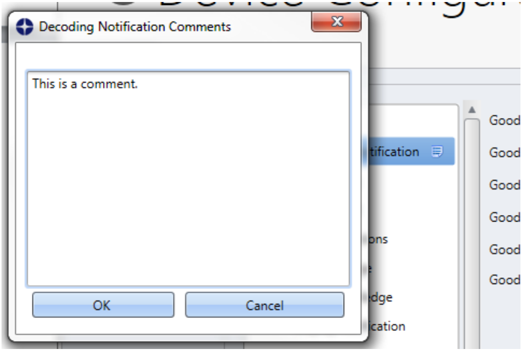
Edit a Configuration File Off-line

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

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

Add Comments to Configuration Settings

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



This is a comment.

To add a comment:

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

To edit a comment:

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

4. Click **OK** to save.

Show Comments

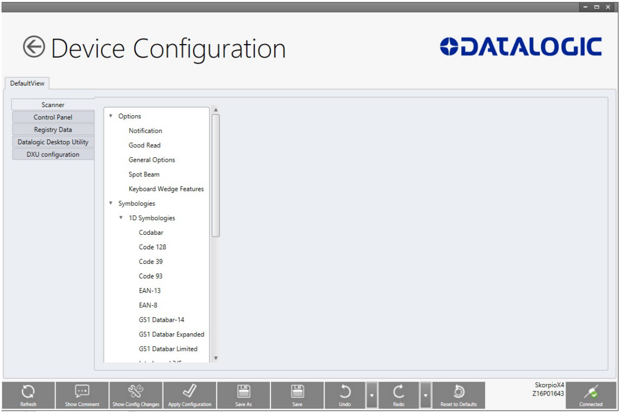
You can show all comments in a configuration file in one handy table by doing this:

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

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

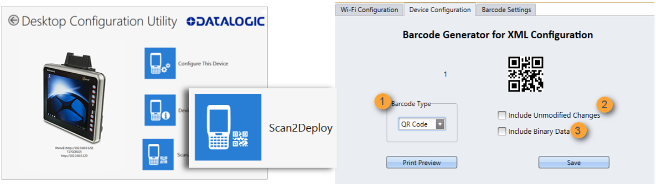
Configure a Device On-line

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


Device Configuration
DATALOGIC
DefaultView
Scanner
Control Panel
Registry Data
Datalogic Desktop Utility
DXU configuration
Options
Notification
Good Read
General Options
Spot Beam
Keyboard Wedge Features
Symbologies
1D Symbologies
Codabar
Code 128
Code 39
Code 93
EAN-13
EAN-8
GS1 Databar-14
GS1 Databar Expanded
GS1 Databar Limited
Refresh
Show Comment
Show Config Changes
Apply Configuration
Save As
Save
Undo
Redo
Reset to Defaults
SkorpioX4
Z16P01643
Connected

Configure a Device Off-line via Scan2Deploy

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



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

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

QR Code

Aztec

Data Matrix

PDF417

Code 128

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

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

To create a **Scan2Deploy** label set:

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

NOTE

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

10. (Optional) Select the barcode symbology in the **Barcode Type** menu.

11. Click **Save** to save your barcode label set as a graphic image file.
12. Click **Print Preview**, then click the **Print** button in the button bar and complete using your printer's **Print** dialog box.

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

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

NOTE

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

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

Configure DXU

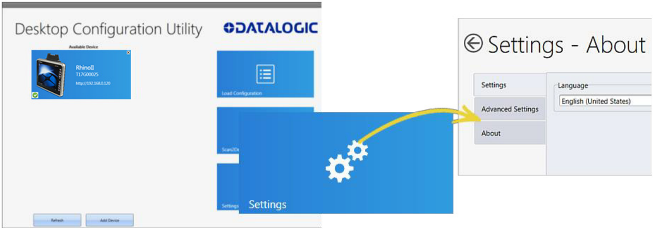
You can change DXU's language and the TCP/IP ports used to communicate with DXU Agent on remote devices, enable automatic discovery of devices, enable logging, and reset DXU's settings back to their default values.

Configure DXU's Language

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

To change DXU's language:

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



Language: English (United States)

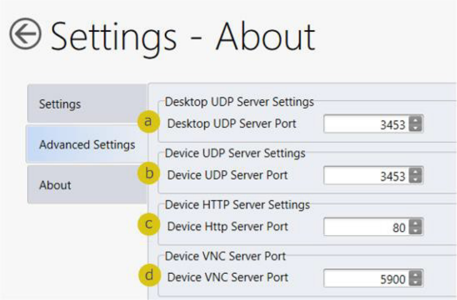
2. Select the language you prefer in the **Language** menu.
3. Click the **Back** button (a leftward pointing arrow in a circle) to return to **DXU** main window.

Configure DXU Communication Settings

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

To configure DXU's UDP and TCP ports:

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



Desktop UDP Server Settings
Desktop UDP Server Port 3453

Device UDP Server Settings
Device UDP Server Port 3453

Device HTTP Server Settings
Device Http Server Port 80

Device VNC Server Port
Device VNC Server Port 5900

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

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

Enable Automatic Discovery of Devices

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

WARNING

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

To enable automatic discovery of devices:

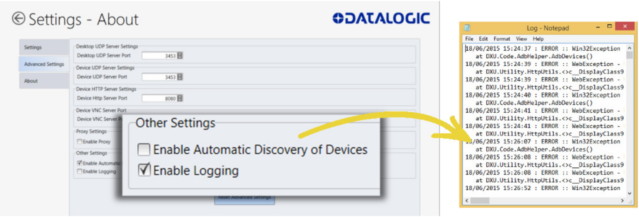
1. From the **DXU** main window, click the **Settings** button.
2. Click the **Advanced Settings** tab.
3. Select the **Enable Automatic Discovery of Devices** check box.
4. Click the **Back** button (a leftward pointing arrow in a circle) to return to the **DXU** main window.

Enable Logging on the DXU Console PC

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

To enable logging:

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



Desktop UDP Server Settings
Desktop UDP Server Port 3453

Device UDP Server Settings
Device UDP Server Port 3453

Device HTTP Server Settings
Device Http Server Port 8080

Device VNC Server Port
Device VNC Server P

Proxy Settings
☐ Enable Proxy

Other Settings
☑ Enable Automatic
☐ Enable Logging

Other Settings
☐ Enable Automatic Discovery of Devices
☑ Enable Logging

```
18/06/2015 15:24:37 : ERROR :: Win32Exception
   at DXU.Code.AdbHelper.AdbDevices()
18/06/2015 15:24:39 : ERROR :: WebException -
   at DXU.Utility.HttpUtils.<>c__DisplayClass9
18/06/2015 15:24:39 : ERROR :: WebException -
   at DXU.Utility.HttpUtils.<>c__DisplayClass9
18/06/2015 15:24:40 : ERROR :: Win32Exception
   at DXU.Code.AdbHelper.AdbDevices()
18/06/2015 15:24:41 : ERROR :: WebException -
   at DXU.Utility.HttpUtils.<>c__DisplayClass9
18/06/2015 15:24:41 : ERROR :: WebException -
   at DXU.Utility.HttpUtils.<>c__DisplayClass9
18/06/2015 15:26:07 : ERROR :: Win32Exception
   at DXU.Code.AdbHelper.AdbDevices()
18/06/2015 15:26:08 : ERROR :: WebException -
   at DXU.Utility.HttpUtils.<>c__DisplayClass9
18/06/2015 15:26:08 : ERROR :: WebException -
   at DXU.Utility.HttpUtils.<>c__DisplayClass9
18/06/2015 15:26:52 : ERROR :: Win32Exception
```

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

Reset Advanced Settings to Defaults

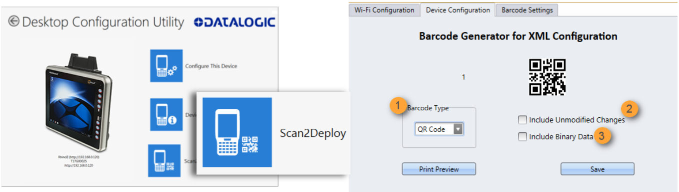
To reset the DXU's Advanced Settings to their default values follow the step below:

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

Create Scan2Deploy Labels to Fully Configure Remote Devices

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

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



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

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

NOTE

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

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

NOTE

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

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

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

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

NOTE

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

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

View Device Info for a Connected Device

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

To view information about the device you are connected to:

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

View Device Info Recorded in a Configuration File

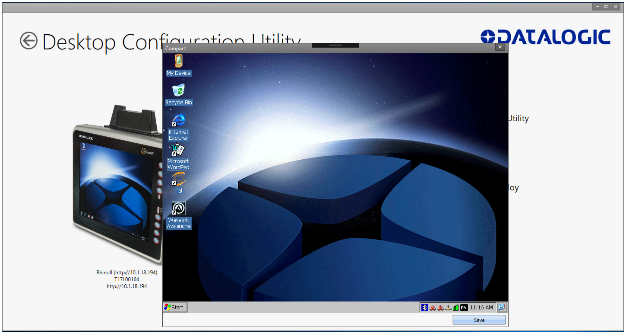
You can view information about the device from which a configuration file was extracted. This information includes the capabilities of the device's Wi-Fi radio, the type of barcode scanner it has, the OS version, the battery type and state of charge, the firmware version and the version of the Datalogic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

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

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

Remote Control

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



Unlock the Screen Using Remote Control

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

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

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

Save a Screenshot of Remote Device

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

Set a VNC Password

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

NOTE

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

Set a VNC Password in DXU Agent

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

To set or edit a VNC password in DXU Agent:

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

NOTE

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

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

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

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

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

Set or Edit the VNC Authentication Password from DXU

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

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

NOTE

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

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

Update Firmware

You can update the Rhino II's firmware from DXU. DXU provides the following options:

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

NOTE

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

NOTE

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

Silent Install

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

Force Update

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

Factory Data Reset After Installing Firmware

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

Enterprise Reset After Installing Firmware

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

Update Firmware on a Connected Device

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

To perform a firmware update with DXU:

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

NOTE

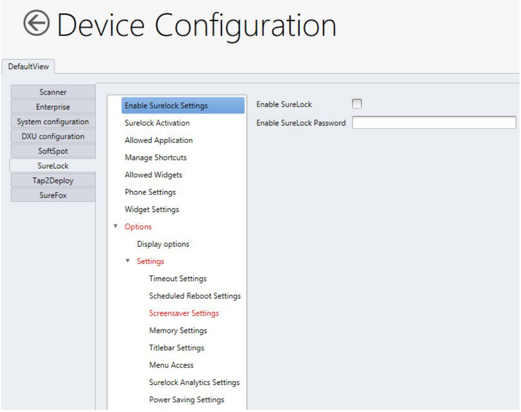
DXU will automatically filter your view of file types to those that are compatible with your device.

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

Configuring SureLock and SureFox

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

1. The EULA on the device must first be accepted. This can be performed by first launching **SureLock** or **SureFox** on the device and accepting the EULA. Future versions of DXU Desktop will allow you to remotely accept this EULA just once for your entire installation.
2. The **Enable SureLock Password** and/or **Enable SureFox Password** fields must have the current password. The Default password is "0000".

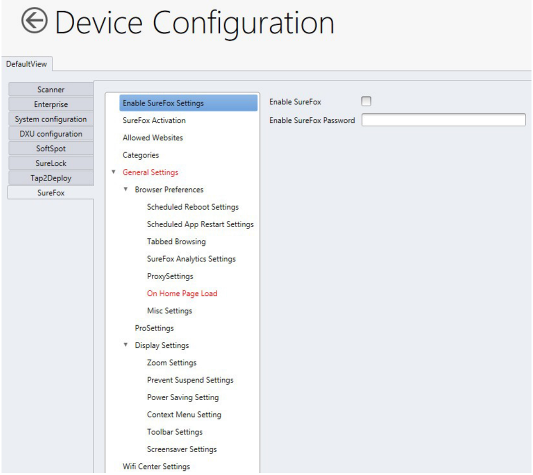


Device Configuration

Enable SureLock ☐

Enable SureLock Password

SureLock



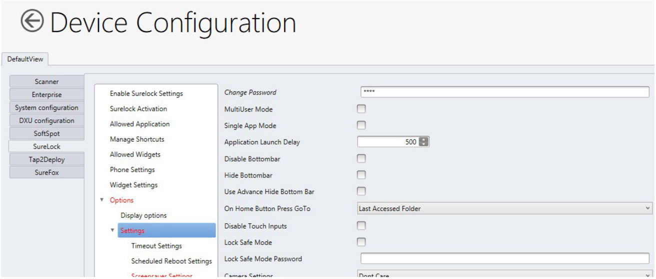
Enable SureFox □

Enable SureFox Password

SureFox

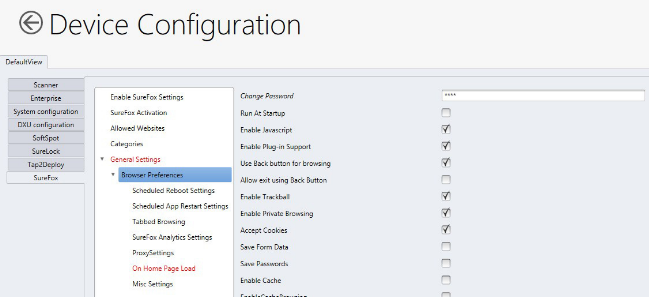
Change the SureLock and/or SureFox Password

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



Change Password ****
MultiUser Mode □
Single App Mode □
Application Launch Delay 500
Disable Bottombar □
Hide Bottombar □
Use Advance Hide Bottom Bar □
On Home Button Press GoTo Last Accessed Folder
Disable Touch Inputs □
Lock Safe Mode □
Lock Safe Mode Password
Camera Settings Dont Care

SureLock



Change Password ****
Run At Startup □
Enable Javascript ☑
Enable Plug-in Support ☑
Use Back button for browsing ☑
Allow exit using Back Button □
Enable Trackball ☑
Enable Private Browsing ☑
Accept Cookies ☑
Save Form Data □
Save Passwords □
Enable Cache □
EnableCacheBrowsing □

SureFox

Command Line DXU Execution

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

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

Usage

DXU command line options are:

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

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

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

  Applies Simplified Deploy to device ofspecific IP address

To output a log file, add the optional parameter:

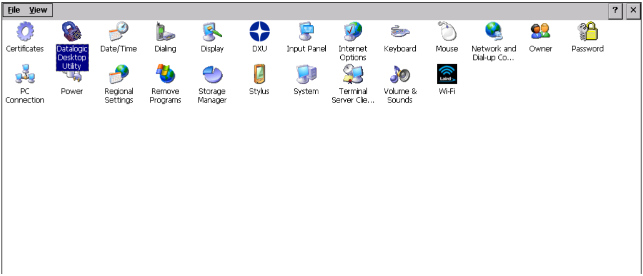
`-log <logfilename>`.

Datalogic Desktop Utility

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

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

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

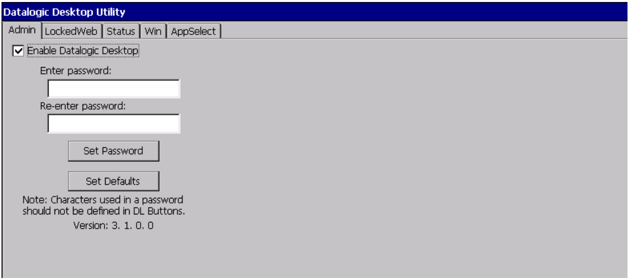


You can also open the DDU by pressing the appropriate key shortcut. The default is "Alt+6".

NOTE

You can change the key combination and specific keys (such as <F1>-<F10>) by using DL Buttons. See Desktop Configuration Utility (DXU) on page 51 for more information.

Administrative Options (Admin tab)



Note: Characters used in a password should not be defined in DL Buttons.

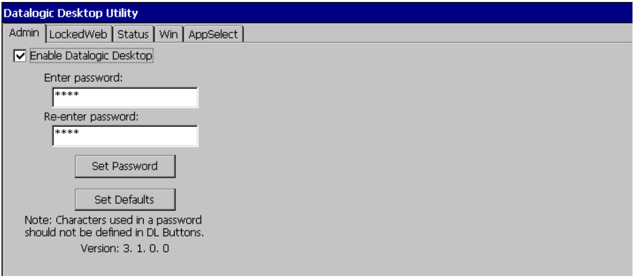
Version: 3. 1. 0. 0

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

Set a Password

To set a password, follow the steps below:

1. Enter a password in the Enter password text box. By default the password is "1234". A password can consist of all standard keyboard characters.
2. Re-enter the password in the second text box.
3. Tap **Set Password** to enable the password.



Datalogic Desktop Utility

☑ Enable Datalogic Desktop

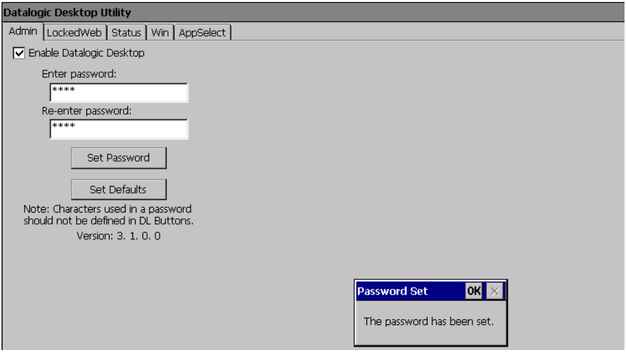
Enter password: ****

Re-enter password: ****

Note: Characters used in a password should not be defined in DL Buttons.

Version: 3. 1. 0. 0

4. Tap **OK** to close the **Password Set** dialog box.



Datalogic Desktop Utility

☑ Enable Datalogic Desktop

Enter password: ****

Re-enter password: ****

Note: Characters used in a password should not be defined in DL Buttons.

Version: 3. 1. 0. 0

Password Set

The password has been set.

NOTE

Be sure to record the Password for future reference.

NOTE

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

CAUTION

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

Change a Password

To change to a new password:

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

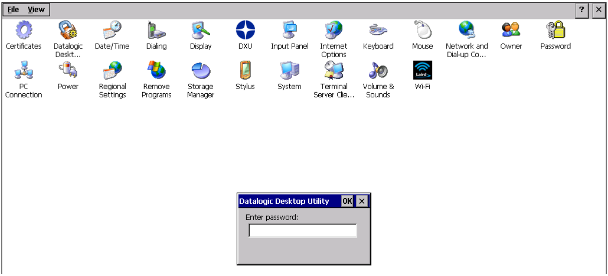
Remove a Password

To remove a password:

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

Password Request Dialog Box

Once the password is set, the next time you launch the **Datalogic Desktop Utility**, the DDU password dialog box opens:



1. Type in your password using either the keypad on the unit, or using the stylus on the soft input panel (SIP). If you enter an incorrect password, the system will prompt you to input the correct one.
2. Tap OK to verify the password, or tap X to cancel.

Locked Web Browser Options (LockedWeb Tab)

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

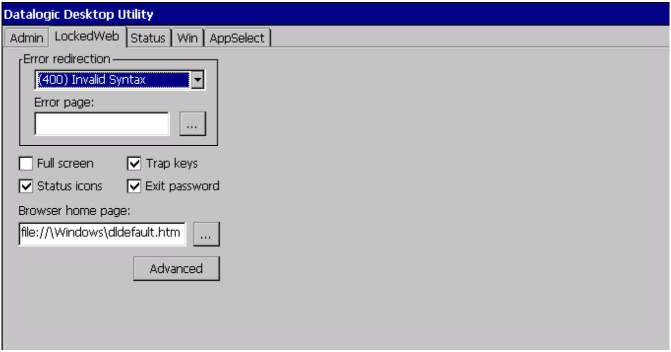
NOTE

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

For further information about Locked Web Browser commands and metatags, see Locked Web Browser Options (LockedWeb Tab) on page 108.

Error Page Redirection

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



Datalogic Desktop Utility

Admin | LockedWeb | Status | Win | AppSelect

Error redirection: (400) Invalid Syntax

Error page: ...

□ Full screen ☑ Trap keys

☑ Status icons ☑ Exit password

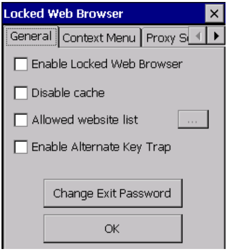
Browser home page: file://\Windows\dldefault.htm ...

Advanced

Error Redirection Options	
Error Type	The **Error Type** drop-down list displays available Error Types: (400) Invalid Syntax, (403) Request Forbidden, (404) Object Not Found, (406) No Response Format, (410) Page Doesn't Exist, (500) Internal Server Error, (501) Server Can't Do That, Generic Error, Network Disconnected.
Error Page	Edit this textbox to associate a website or html file with the specified error.
Other Options	
Full Screen	Sets the web browser in full screen mode.
Status Icon	Enables or disables the status icons view (see Status Icons Options (Status Tab) on page 113). The status icons can be configured on the **Status** tab of DDU.
Trap Keys	When selected: ▪ all key presses will be trapped by the Locked Web Browser to prevent the user from accessing unsafe parts of the system. For example, pressing "Ctrl + O" to open a file will not work; ▪ safe key presses (e.g. Alpha numeric) will still get processed by the Locked Web Browser as normal. For example entering a number in a text field on a web page; ▪ DL Buttons keys will not work in the LockedWeb Browser; ▪ all Locked Web Browser command keys will work (e.g. "Ctrl + O" to exit). When not selected: ▪ all keys will be processed normally by the system and the browser; ▪ DL Buttons keys will work normally; ▪ all Locked Web Browser command keys will work (e.g. "Ctrl + O" to exit).

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

Advanced Settings

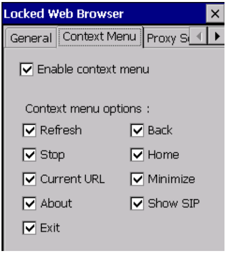


☐ Enable Locked Web Browser

☐ Disable cache

☐ Allowed website list

☐ Enable Alternate Key Trap



☑ Enable context menu

Context menu options :

☑ Refresh ☑ Back

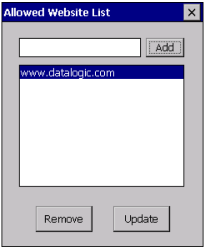
☑ Stop ☑ Home

☑ Current URL ☑ Minimize

☑ About ☑ Show SIP

☑ Exit

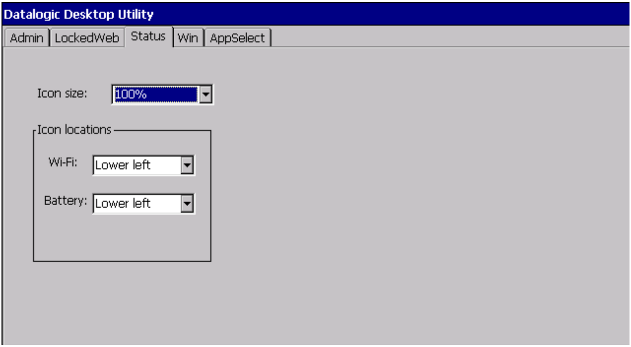
Advanced Locked Web Browser Options	
General	
Enable Locked Web Browser	Enables the Locked Web Browser when Internet Explorer is launched.
Disable Cache	Prevents the browser from loading the local intranet page from cache instead of navigating to the **Network Disconnected** error redirection page.

Advanced Locked Web Browser Options	
Allowed Website List	Restricts browsing only to files and URLs in the **Allowed Website List** (accessed by the ... button). The following dialog box appears:  Tap **Add** to add allowed URLs to the white list. Other sites will be restricted when the option is enabled. Domain names must be exactly specified.
Change Exit Password	Allows to change the password required to exit the Locked Web Browser (when the **Exit password** option is selected on the **LockedWeb** tab in DDU).
Context Menu	
Enable Context Menu	Enables the context menu accessed by a touch screen tap in the Locked Web Browser.
Refresh	Adds a **Refresh** item to the Locked Web Browser context menu.
Stop	Adds a **Stop** item to the Locked Web Browser context menu. Selecting during navigation stops the downloading of a page.
Current URL	Adds a **Current URL** item to the Locked Web Browser context menu. Selecting the item pops up a dialog displaying the URL for the current web page.
About	Adds an **About** item to the Locked Web Browser context menu. Selecting the item pops up the **About** dialog.
Back	Adds a **Back** item to the Locked Web Browser context menu. Selecting the item allows to navigate to the previous page.

Advanced Locked Web Browser Options	
Home	Adds a **Home** item to the Locked Web Browser context menu. Selecting the item allows to navigate to the IE home page.
Minimize	Adds a **Minimize** item to the Locked Web Browser context menu. Selecting the item minimizes the Locked Web Browser and allows access to other programs.
Show SIP	Adds a **Show SIP** item to the Locked Web Browser context menu. Selecting the item toggles the show state of the SIP.
Exit	Adds an **Exit** item to the Locked Web Browser context menu. Selecting the item exits the Locked Web Browser with an optional password (set in the Locked Web Browser Advanced options).

Status Icons Options (Status Tab)

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



Icon size: 100%

Icon locations

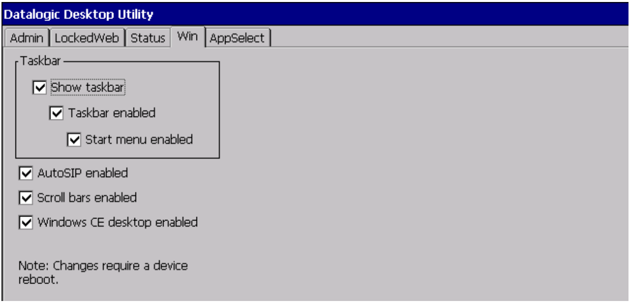
Wi-Fi: Lower left

Battery: Lower left

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

Windows Controls (Win Tab)

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



☑ Show taskbar

☑ Taskbar enabled

☑ Start menu enabled

☑ AutoSIP enabled

☑ Scroll bars enabled

☑ Windows CE desktop enabled

Note: Changes require a device reboot.

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

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

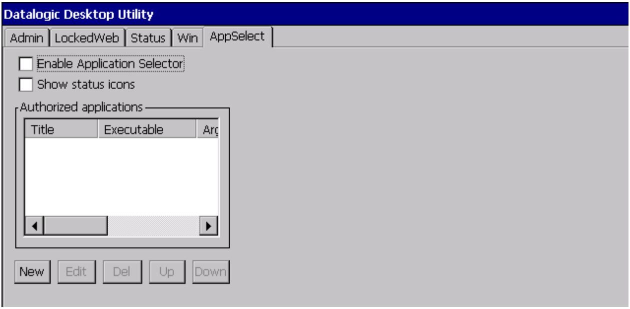
NOTE

Changes require a device reboot.

AppSelector Options (AppSelect Tab)

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

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



□ Enable Application Selector

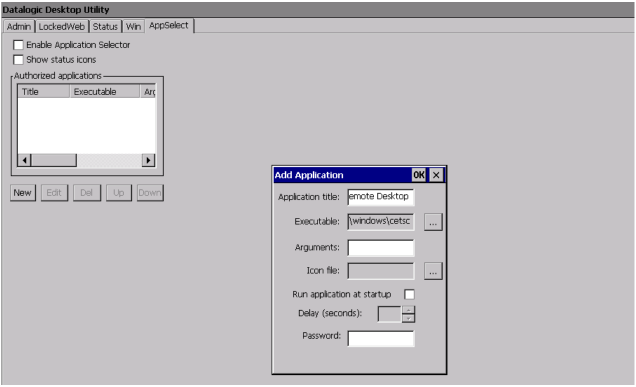
□ Show status icons

Application Selector Options	
Enable Application Selector	Select to enable the application selector.
Show status icons	Select to enable the status icons view (see Status Icons Options (Status Tab) on page 113). The status icons can be configured on the **Status** tab of DDU.
Authorized applications	List of applications that the user can access.
Application Selector Commands	
New	Tap to create a new application entry.
Edit	Tap to edit the selected entry.
Del	Tap to delete the selected entry.
Up/Down	Tap to move an entry up or down in the ListView.

Add Application

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

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



Datalogic Desktop Utility

□ Enable Application Selector
□ Show status icons

Add Application

Application title: emote Desktop

Executable: \windows\cetsc

Arguments:

Icon file:

Run application at startup □

Delay (seconds):

Password:

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

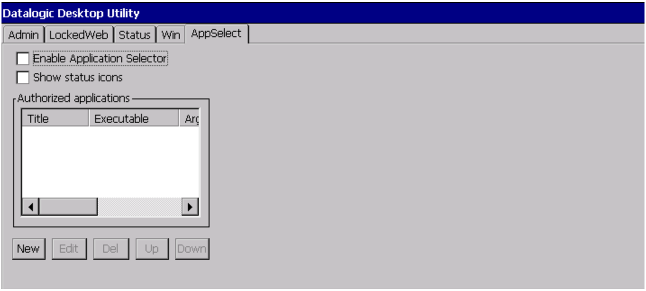
Command	Description
Browse	Tap ... to browse for the desired icon file. The results of this search are displayed in the **Icon file** textbox.
Run Application at Startup	Select to force the application to auto start when the Application Selector starts up. Applications will be started in the order listed in the authorized application list.
Delay	Enter a delay duration in seconds in the combo box. This option delays auto start of application(s) to allow drivers to load before starting applications.
OK	Tap to add/save changes.
X	Tap to cancel.

App Selector (Application Selector)

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

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

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



☐ Enable Application Selector

☐ Show status icons

The administrator can customize this list as shown in AppSelector Options (AppSelect Tab) on page 116. Additionally, the page template can be modified to display a different background. Contact your Datalogic representative for more information on this feature.

To run an application, tap its name.

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

Locked Web Browser

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

NOTE

Configuration is set up through the DDU control panel. See Locked Web Browser Options (LockedWeb Tab) on page 108 for more information.

Locked Web Browser Special Metatags

General Metatag Comments

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

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

</head> tag set.

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

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

In particular, the special metatags allow it to:

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

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

Trigger Metatag

DL_Triggers – "Enable" or "Disable" all triggers

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

Example:

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

GetSerialNumber Meta-tag

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

Content – name of function to pass serial number to.

Example:

<meta http-equiv="DL_GetSerialNumber" content=

"Javascript:CustomerFunction">

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

Reboot – Warm Boot Device Metatag

DL_Reboot – Warm boot device.

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

Example:

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

Exit Metatag

DL_Exit – Exit the Locked Web Browser.

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

Example:

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

Decoding Metatags

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

DL_Code_39 DL_Code_128 DL_Code_I25 DL_Code_S25 DL_Code_M25 DL_Code_CODABAR DL_Code_93 DL_Code_UPCA DL_Code_UPCE DL_Code_EAN13 DL_Code_EAN8 DL_Code_MSI DL_Code_MSR DL_Code_GS1_14 DL_Code_GS1_LIMIT DL_Code_GS1_EXP DL_Code_PDF417 DL_Code_DATAMATIX

DL_Code_MAXICODE

DL_Code_TRIOPTIC

DL_Code_PHARMA39

DL_Code_RFID

DL_Code_MICROPDF417

DL_Code_COMPOSITE

DL_Code_QRCODE DL_Code_AZTEC

DL_Code_POSTAL

Examples:

<meta http-equiv="DL_Code_39" content="Disable">

<meta http-equiv="DL_Code_I25" content="Enable">

Key Press Metatags

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

Example:

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

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

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

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

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

NOTE

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

Scanning Metatags

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

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

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

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

Example:

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

PAL and PAL Communicator

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

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

For further information refer to the Pal & Pal Communicator User's Guide, downloadable from our website (see Support Through the Website on page 155).

Setting Up Serial Scanning

To use a serial scanner with the Rhino II, a wedge utility must be executed to convey the serial input to the keyboard input. By doing this, the scanner data will be presented to the application as if it had been typed on the keyboard. On the Rhino II WEC7 units the wedge utility is \Windows\DLWedgeCE.exe, which should be copied to \Windows\StartUp directory in order to automatically launch when the terminal is rebooted.

On all other Rhino IIs the utility is c:\Program Files (x86)\Device Tools\Keywedge.exe. To automatically launch keywedge you will want to follow the instructions for automatically launching applications for the loaded operating system. Search for 'add program to startup windows" on the internet then select the instructions for Windows 7 or 10 as appropriate.

Wedge parameters may be changed by the user if desired using a registry edit utility such as regedit. The parameters are stored as strings in the registry, under the key HKEY_CURRENT_USER\SOFTWARE\DATALOGIC\MWWEDGE. To add any desired parameters, use the registry editor on the PC to add or edit the string value. The default value for each setting is listed in bold below. The following parameters are available:

CommPort REG_SZ Sets the serial port to be monitored for input. Legal values are **COM1**: or COM2:.

CommBaud REG_SZ Sets the baud rate to be used on the serial port. Legal values are 1200, 9600, 19200, 38400, 57600 or **115200**.

Suffix REG_SZ Decimal value of the character to be added to the end of the scanned data. For example, to add a carriage return to the end of the scan set the suffix to 13. By default no suffix is set.

Prefix REG_SZ Decimal value of the character to be added to the beginning of the scanned data. For example, to add a 's' to the beginning of the scan set the prefix to 115. By default no prefix is set.

Terminator REG_SZ Sets the decimal value of the character that indicates a complete scan has been received. For example, to look for a tab as the end of the scan, set terminator to 9. The default is **13** (CR).

KeepTerm REG_SZ **Y** or N, used to determine if the terminator character defined above should be retained and processed as a part of the scan data or if it should be dropped from the scan. If the terminator is retained, note that the suffix character (if any) will be added after the terminator is processed.

CopyPaste REG_SZ Y or **N**, used to determine if the input should be placed in the keyboard buffer (default) or pasted into the current screen. If using CopyPaste mode, KeepTerm should normally be set to no. CopyPaste mode is much faster than keyboard input, but might not work on all screens (those that don't support the normal ctrl-v paste command).

PasteDelay REG_SZ An optional delay used with the CopyPaste option above to prevent overflowing the windows copy buffer. This value is the number of milliseconds to pause after pasting a scan.

Communications

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

Setting Up Ethernet Communications

Ethernet communications usually do not require special configuration. The Rhino II default settings are configured to use DHCP to automatically get an IP address from a DHCP server. To change these settings select Start -> Settings -> Network and Dialup Connections. Then select DM9CE1 and set the parameters to work with your network.

NOTE **Windows Embedded CE does not have native support for allowing direct Network browsing (No "Network Neighborhood") or for allowing network clients to access the Rhino II (Rhino II will not show up in "Network Neighborhood").**

Setting Up 802.11 Radio Communications

The Rhino II has an internal 802.11 a/b/g radio from Laird. Under WEC7 and WES7, the Rhino II uses the Laird Connection Manager to configure the radio. Go to http://www.lairdtech.com for latest version of the Laird Manager guide. Running Windows 10 IoT, the radio is managed by the standard built in Microsoft wireless manager.

Laird also has white papers on a verity of topics from security to difference in radio types. See the Lairdtech.com Web site for access to these white papers.

Setting Up Bluetooth Radio Communications

The WEC7 Rhino II has an internal Bluetooth radio from Laird. The Rhino II uses the Laird Connection Manager to configure the radio. Go to http://www.lairdtech.com for latest version of the Laird Manager guide.

Running WES7 or Windows 10 IoT, the Bluetooth radio is attached in the connection compartment to a USB port.

It is managed by the standard built in Microsoft Bluetooth manager.

Wireless and Radio Frequencies Warnings

WARNING

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

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

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

Persons with pacemakers:

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

WARNING

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

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

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

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

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

WARNING

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

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

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

NOTES

Technical Features

Technical Data

Physical Characteristics	
Construction	Coated aluminum, no fan design
Dimensions	27.8 x 22.3 x 6.4 cm / 10.9 x 8.8 x 2.5 in
Weight	3.4 Kg / 7.5 lb (10 inch Freezer Models) 3.6 Kg / 7.9 lb (10 inch Standard Models) 4.7 Kg / 10.4 lb (12 inch Standard Models)
Display	Resistive/Freezer Model: 10.4 inch SVGA 800x600, 400 NITS; Capacitive/Standard Models: 10.4 inch XGA 1024 x 768, 350 NITS 12.1 inch XGA, 1024 x 768, 500 NITS
Function Buttons	4 programmable keys (S1-S4)
Mounting	VESA: 75 mm pattern
Screen Blanking	Optional
Speakers	Optional: downward facing, waterproof
Touchscreen	Resistive, 4 Wire (WEC7/Freezer model only); Capacitive (all OS); 3 mm, non-reflecting, hardened glass; Gloves support
Video Output	1 x HDMI port (top) [Win7/10 only]
Voice Support	Wireless via Bluetooth v4 (10 inch Freezer Models)

Environmental	
Humidity	10 to 90% at 40 °C / 104 °F; non-condensing
Temperature	Operating: -20 to 55 °C / -4 to 131 °F (without heater, Capacitive models); -30 to 55 °C / -22 to 131 °F (with heater, minimal condensation using freezer-rated model - 10” only)
Shock & Vibration	Class 5M3 at EN 60721-3-5: 1998 (landcrafts)
Particulate and Water Sealing	IP65/IP67

Electrical	
Backup Battery	Optional backup battery for up to 30 min. runtime; 2,500 mAh @ 10.8 VDC; 27 Wh; Battery charging: 0 to 50 °C / 32 to 122 °F Battery operating: -20 to 50 °C / -4 to 122 °F
Power supply	Choice of 12 VDC; 24/48 VDC isolated internal power supplies
Light Indicators	On front bezel

Wireless Communications	

Local Area Network (WLAN)	Wi-Fi: 802.11a/b/g/n (2.4 GHz and 5 GHz);
	Cisco CCX v4;

Personal Area Network (WPAN)	Bluetooth Wireless Technology 4.0
Antennas	Diversity antennas under top cap; Optional cab mount antenna

Interfaces	
Interfaces	1 x Ethernet 10/100/1000 Mbps; RJ45; USB: 2 x USB 2.0 Type A (bottom) 1 x USB 3.0 Type A (bottom) [Win7/10 only] 1 x USB 2.0 Type A (top) Serial: 2 x RS-232 (bottom); COM1: 5 V on pin 9; COM2: 5/12 V on pin 9
Interface Slots	1x Mini-PCIe, half or full size slot (full size used for Wi-Fi) 1x CFast for SSD (Win 7/Win 10) 1x SD Card slot for SDHC card (WEC7)
System	
Operating System	WEC7, Windows Embedded Standard 7 or Windows 10 IoT Enterprise 64 bit

Processor	Freescale NXP ARM Quad Core:
	1 GHz (WEC7 Standard models);
	800 MHz (WEC7 Freezer models);
	Intel Atom E3826 Dual Core 1.46 GHz (Win7/10)

Memory	WEC7: 1 GB RAM; Win7/10: 4 GB RAM
Storage	WEC7: 32 GB SDHC; Win7/10: 32 GB CFast SSD
Software	

Configuration & Maintenance	WEC7: Datalogic DXU, DDU, SDK, SureFox Locked Browser;
	WEC7: Wavelink Avalanche pre-installed and pre-licensed;
	Win7/10: Datalogic Aladdin™ pre-loaded

Development	Datalogic Windows CE SDK™
Terminal Emulation	Wavelink Terminal Emulation™ pre-installed and pre-licensed (WEC7 models)
Soft Keyboards	Includes QWERTY layouts for English, German, Italian, Spanish, Polish; Azerty French layout; Function Key layout (F1-F12)

Safety & Regulatory	
Agency Approvals	The product meets necessary safety and regulatory approvals for its intended use.
Certifications	Certified for CE/FCC; RoHS compliant
Regulatory	US, Canada, EU countries
Warranty	
Warranty	1-Year Factory Warranty.

Troubleshooting the Rhino II

If you send the Rhino II in for service, it is your responsibility to save the computer data and configuration. Datalogic is responsible only for ensuring that the hardware matches the original configuration when repairing or replacing the computer.

Problems While Operating the Rhino II

Problem	Solution
You press **Power** and nothing happens	▪ *Make sure you are connected to a power supply.* ▪ *Make sure the brightness is not set all the way to the darkest or lightest setting. Press the + key until you reach the desired brightness level.* ▪ *Make sure you are pressing the Power button for at least the minimum duration set in the configuration (default 3 seconds).* ▪ *If the Rhino II will not reboot, contact Datalogic or your local Datalogic service representative for help.*

Problem	**Solution**
The Rhino II appears to be locked up and you cannot enter data.	▪ Press and hold Power to turn off the Rhino II and then turn it back on. ▪ If the Rhino II will not reboot, contact Datalogic or your local Datalogic service representative for help.

Problems with Wireless Connectivity

Problem	**Solution**
When you turn on the Rhino II after it was suspended for a while (10 to 15 minutes or longer) and it no longer sends or receives messages over the network.	*The host may have deactivated or lost your current terminal emulation session. In a TCP/IP direct connect network, you need to turn off the "Keep Alive" message (if possible) from the host so that the TCP session is maintained while a Rhino II is suspended.*
The network connection icon in the taskbar appears to be communicating, but the host computer is not receiving any data from the Rhino II.	In a TCP/IP network, there may be a problem with the connection between the access point and the host computer. Check with your network administrator or use your access point user's manual.

Problem	Solution
The Rhino II is not communicating with the access point.	▪ The Rhino II is not connected to the access point. Make sure the access point is turned on and operating. You may also be using the Rhino II out of range of an access point (no green bars). Try moving closer to an access point to reestablish communications. ▪ Make sure the Rhino II is configured correctly for your network. The radio parameters on the Rhino II must match the values set for all access points the Rhino II may communicate with. ▪ The radio initialization process may have failed on the 802.11 radio. Try rebooting the Rhino II. ▪ If you have tried these possible solutions and nothing happens, you may have a defective radio card. For help, contact Datalogic or your local Datalogic service representative.

NOTES

Maintenance

Cleaning the Device

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

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

Ergonomic Recommendations

⚠ CAUTION

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

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

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

Safety and Regulatory Information

NOTE

Read this manual carefully before performing any type of connection to the Rhino II.

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 Safety and Regulatory Addendum.
- Use only the components and accessories supplied by the manufacturer for the specific Rhino II being used.
- Do not attempt to disassemble the Rhino II, 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 Rhino II, disposal must be performed in compliance with the laws in force in your jurisdiction.
- Do not submerge the Rhino II in liquid products.
- For further information or support, refer to this manual and to the Datalogic web site: www.datalogic.com.

Power Supply

The device is intended to be supplied by an external DC power appropriate to the installed power supply (12-24VDC or 24-48VDC)

and/or by UL Listed/CSA Certified Power Unit LPS/SELV power source which supplies power directly to the unit via the attached power connector.

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

Marking and European Economic Area (EEA) CE

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

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

Simplified EU Declaration of Conformity

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

Statement of Compliance

cs Česky [Czech]	Datalogic S.r.l. tímto prohlašuje, že tento Rhino II je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU - 2011/65/EU.
da Dansk [Danish]	Undertegnede Datalogic S.r.l. erklærer herved, at følgende udstyr Rhino II overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU - 2011/65/EU.
de Deutsch [German]	Hiermit erklärt Datalogic S.r.l., dass sich das Gerät Rhino II in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU - 2011/65/EU befindet.

et Eesti [Estonian]	Käesolevaga kinnitab Datalogic S.r.l. seadme Rhino II vastavust direktiivi 2014/53/EU - 2011/65/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
es Español [Spanish]	Por medio de la presente Datalogic S.r.l. declara que el Rhino II cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU - 2011/65/EU.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Datalogic S.r.l. ΔΗΛΩΝΕΙ ΟΤΙ Rhino II ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU - 2011/65/EU.
fr Français [French]	Par la présente Datalogic S.r.l. déclare que l'appareil Rhino II est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU - 2011/65/EU.
it Italiano [Italian]	Con la presente Datalogic S.r.l. dichiara che questo Rhino II è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU - 2011/65/EU.
Latviski [Latvian]	Ar šo Datalogic S.r.l. deklarē, ka Rhino II atbilst Direktīvas 2014/53/EU - 2011/65/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo Datalogic S.r.l. deklaruoja, kad šis Rhino II atitinka esminius reikalavimus ir kitas 2014/53/EU - 2011/65/EU Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart Datalogic S.r.l. dat het toestel Rhino II in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU - 2011/65/EU.
mt Malti [Maltese]	Hawnhekk, Datalogic S.r.l., jiddikjara li dan Rhino II jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU - 2011/65/EU.
hu Magyar [Hungarian]	Alulírott, Datalogic S.r.l. nyilatkozom, hogy a Rhino II megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU - 2011/65/EU irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym Datalogic S.r.l. oświadcza, że Rhino II jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU - 2011/65/EU.

pt Português [Portuguese]	Datalogic S.r.l. declara que este Rhino II está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU - 2011/65/EU.
sl Slovensko [Slovenian]	Datalogic S.r.l. izjavlja, da je ta Rhino II v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU - 2011/65/EU.
Slovensky [Slovak]	Datalogic S.r.l. týmto vyhlasuje, že Rhino II spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU - 2011/65/EU.
fi Suomi [Finnish]	Datalogic S.r.l. vakuuttaa täten että Rhino II tyyppinen laite on direktiivin 2014/53/EU - 2011/65/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar Datalogic S.r.l. att denna Rhino II står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU - 2011/65/EU.

Information for the User

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

FCC ID/IC Warning

FCC Label Compliance 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.

To assure continued FCC compliance:

1. Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil radio est conforme au CNR d'Industrie Canada. L'utilisation de ce dispositif est autorisée seulement aux deux conditions suivantes: (1) il ne doit pas produire de brouillage, et (2) l'utilisateur du dispositif doit être prêt à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

Exposure to Radio Frequency Radiation

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body

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 20 cm de distance entre la source de rayonnement et votre corps.

Europe

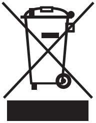
This device is used at a distance greater than 20 cm from body.

Radio Technologies and Frequency Bands

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

	RF Module	Frequency Bands	Max Transmission Power
1	BT/SRD	2400 - 2479 MHz	10mW
2	WLAN	2412 - 2472 MHz	100mW
3	WLAN	5150 - 5350 MHz	200mW
4	WLAN	5470 - 5725 MHz	200mW

WEEE Compliance



Information for the user

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

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

Informazione per gli utenti

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

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

Information aux utilisateurs

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

Pour obtenir des informations complémentaires concernant l'élimination, veuillez contacter le fournisseur auprès duquel vous avez acheté le produit ou consulter la section consacrée au site Web http://www.datalogic.com.

Información para el usuario

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

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

Benutzerinformation bezüglich

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

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

Reference Documentation

For further information regarding Rhino II refer to the SDK Help on-line.

Support Through the Website

Datalogic provides several services as well as technical support through its website.

Log on to www.datalogic.com and click on the **SUPPORT** link which gives you access to:

Downloads by selecting your product model from the dropdown list in the Search by Product field for specific Data Sheets, Manuals, Software & Utilities, and Drawings;

Repair Program for On-Line Return Material Authorizations (RMAs) plus Repair Center contact information;

Customer Service containing details about Maintenance Agreements;

Technical Support through email or phone.

Warranty Terms and Conditions

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

NOTES

Glossary

Access Point

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

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.

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.

Density (Barcode Density)

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

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.

Firmware

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

Flash Memory

Non-volatile memory for storing application and configuration files.

Host

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

Laser

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

Light Emitting Diode (LED)

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

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.

RF

Radio Frequency.

Scanner

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

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

SDK

Software Development Kit.

Symbology

The structural rules and conventions for representing data within a particular barcode 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.

WLAN

A Wireless Local Area Network links devices via a wireless distribution method (typically spread-spectrum or OFDM radio), and usually provides a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.

WPAN

A Wireless Personal Area Network is a personal area network - a network for interconnecting devices centered around an individual person's workspace - in which the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about 10 meters - in other words, a very short range.

www.datalogic.com

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

822002330 (Rev A) January 2018