Application Note

NFC-Windscreen and NFC-InCar Readers

Part Number APP-0015
Revision A October 2019
Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2019</td>
<td>1.0.0</td>
<td>Initial version.</td>
</tr>
<tr>
<td>October 2019</td>
<td>A</td>
<td>Initial Lantronix document. Added Lantronix document part number, logo, contact information, and links.</td>
</tr>
</tbody>
</table>

For the latest revision of this product document, please check our online documentation at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).
# Table of Contents

1. Introduction ................................................................................................. 5
   1.1 What is NFC and how does it work? .................................................. 5
   1.2 What is needed to get started with NFC readers? ............................ 5
   1.3 Hardware setup ................................................................................... 5
      1.3.1 Connecting device to your PC .................................................. 6
      1.3.2 Installing the Lantronix Workbench software and loading the configuration into the device ...................................................... 6
      1.3.3 Connecting the NFC reader to device with CA31 and powering up the device .... 8
      1.3.4 Testing the NFC readers on the FOX3-2G/3G/4G series .............. 8


1 INTRODUCTION

This guide shows how to install the NFC reader series, configure your FOX3-2G/3G/4G series, connect it to the one of Lantronix vehicle telematics devices and monitor activities on your remote server.

1.1 What is NFC and how does it work?

Near-field communication (NFC) is a set of short-range wireless technologies and a set of communication protocols that enable two electronic devices to establish communication by bringing them within 4 cm of each other. NFC always consists of a NFC reader and a NFC tag; the reader actively generates an RF field that can power a passive tag. NFC tags contain data and are typically read-only. Once the tag is activated by the reader, small amounts of data between the two devices can be transferred when held a few centimeters from each other. NFC operates as one part of a wireless link at the same frequency (13.56 MHz) on ISO/IEC 18000-3 as HF RFID readers and tags. The FOX3-2G/3G/4G series are vehicle telematics devices supporting NFC connectivity for applications like: secure vehicle access control, contactless key, vehicle and driver identification in-car access, car-sharing, and car-rental applications.

1.2 What is needed to get started with NFC readers?

The following components should be available to operate with NFC readers:

1. FOX3-2G/3G/4G series device with firmware version 3.x.x and a data SIM card
2. Device configuration to control the activities of one of the NFC readers
3. CA31b for in-vehicle installation: Main port extended installation cable with 2x4pin connector, 6 x open ends and 2x2pin UCOM connector to connect one of the NFC reader to the 1st serial port of the FOX3-2G/3G/4G series.
4. CA69 for accessory installation: Accessory port cable with 6pin (2x3) connector, open ends and 4pin (2x2) UCOM connector to connect one of the NFC reader to the 2nd serial port of the FOX3-2G/3G/4G series (not available on LITE models).
5. NFC-Windscreen reader or NFC-InCar reader
6. RFID-TAGS-TYPE-A from Lantronix (tags compatible with NFC readers )
7. Workbench software to load the configuration into the FOX3-2G/3G/4G and BOLERO40 series device.
8. Power source from +12 to +32 VDC (e.g. 12 VDC in your vehicle)

1.3 Hardware setup

This chapter explains how to connect and get started with FOX3-2G/3G/4G series device and NFC reader:

1. Connect FOX3-2G/3G/4G to your PC with the help of Control-box or USB cable.
2. Install the Workbench software and load the configuration into your FOX3-2G/3G/4G series device.
3. Connect one of the NFC readers and power up the FOX3-2G/3G/4G series device.
4. Start testing the device configuration.
5. To install the NFC reader in your vehicle, first pull off the protective foil on the adhesive pad on the back of casing and then stick it on a cleaned and dried surface.
6. For more information about the NFC readers, please refer to the flyer available on our website.
1.3.1 Connecting device to your PC

To connect your FOX3-2G/3G/4G series device to your PC use either the Control-box (included in the promotion kit) or a USB cable* (USB 2.0 Cable A-Male to Mini-B-5pin-Male), connect it to the USB port on the device and install the USB driver. The USB driver can be downloaded from our website:

https://www.lantronix.com/support/.

* Please note that, when using the USB cable for device configuration you have to apply extra power to the FOX3-2G/3G/4G series.

If you are going to use the Control-box for connection of FOX3-2G/3G/4G series device to a PC, go to our website https://www.lantronix.com/products/fox3-series/ and download the document “FOX3/-3G PROMOTION-KIT Getting Started” – then refer to the chapter 3.1.2 in that document.

![Figure 1: Use the Control-box for connection of a FOX3-2G/3G/4G series device to a PC](image)

1.3.2 Installing the Lantronix Workbench software and loading the configuration into the device

To be able to communicate with the FOX3-2G/3G/4G series device and load a configuration onto the device, you need to install the Workbench software. Go to the following link to download it:

https://www.lantronix.com/products/workbench/

System requirements for using the Workbench software:

(a) PC with 700 megahertz or higher processor Intel Pentium II or compatible processor recommended,
(b) 512 megabytes (MB) of RAM or higher recommended (512MB minimum supported; may limit performance and some features),
(c) 90 megabytes (MB) of hard disk space available (recommended 2 gigabytes),
(d) Keyboard and Mouse.

After downloading the Workbench software, double click on the file to install it. An install shield will guide you through the installation. Integrated online help can be found once the installation is completed.
1. After completing the installation, double-click on **Workbench.exe** to start it. Open a new **COM Port** from the Toolbar (1), on the **COM Port view** (2), choose the port where FOX3-2G/3G/4G is connected (go to Device Manager > Ports > USB Serial Port (COMxx), where xx is the COM port to use), define the port settings (**115200** bps, **8** Data bits, **No** Parity bit, **1** Stop bit, **None** Flow control) and finally, click the connect (play) icon (2.1) to open that COM port. You can also get an online help in HTML format if you click the "Help" button on the upper-right hand corner.

2. Open a new **Console** from the Toolbar (3), click on the **Console1** (4), then go to **Connection view** and click on **COMPort** (5).

3. Open a new **Editor** from the Toolbar (6), click on the **Editor1** (7), then go to **Connection view** and click on **Console1** (8).

4. To load the configuration or send commands to the FOX3-2G/3G/4G series device, type them in the **Editor** (9), then click on **Start sending configuration** (10) or double-click with the left mouse key on each configuration line individually, in the **Editor** (9).

5. Now, copy the configuration lines from one of the tables in chapter **Error! Reference source not found.** or **Error! Reference source not found.** below and past them in the **Editor** (9) and perform the step 4 above.
1.3.3 Connecting the NFC reader to device with CA31 and powering up the device

After the device has been successfully configured, connect one of the NFC readers as shown in pictures below. First, plug in the 8pin connector of one of these cables (CA1 or CA69) to the 8pin connector of the FOX3-2G/3G/4G series device. Then connect the 2x2 connector of the connection cable to the 2x2 connector of CA31 or CA69.

Finally, connect the IN+, GND wires of the cable CA31 to an external power source ranging from +12 to +32 VDC (e.g. 12 VDC in your vehicle) and apply power to the device

---

Figure 3: Connection of NFC-Windscreen to the 1st serial port via CA31

Figure 4: Connection of NFC-Windscreen to the 2nd serial accessory port via CA69

1.3.4 Testing the NFC readers on the FOX3-2G/3G/4G series

This section describes how to test the FOX3-2G/3G/4G series with one of the NFC readers. After loading the configuration examples given in the sections 1.3.4.1 and 1.3.4.2 into the FOX3-2G/3G/4G series device, connecting the NFC reader and applying power, to test the NFC reader just touch a valid NFC card to the reader. The green LED will flash for 2 seconds. If you touch an invalid card to the reader the red LED will flash for 2 seconds. If you would like to control a door by an output then use the configuration line in chapter with the IO1 wired to the door locking system.
1.3.4.1 Device configuration when connecting the NFC reader to 1st serial port

The table below shows how to configure your FOX3-2G/3G/4G series device if NFC reader is connected to the 1st serial port. If you would like to connect the NFC reader to 2nd serial accessory port, please use the configuration in the section 1.3.4.2 below. For more details about the PFAL commands related to the NFC, refer to section below 0.

$PFAL,Cnf.Set,AL0=SYS.NFC.eCARD="0A921027":Msg.send.Serial1,0,"authorized_access=&(NFCUID)"&Msg.send.TCP,8,"nfc_authorized_access=&(NFCUID)"&SYS.NFC.LED2,hPulse,2000

**AL0**: It sends the ID of the passed NFC card with the test "authorized_access" together with the GPS position to the server. It also outputs this information on the 2nd serial port.

$PFAL,Cnf.Set,AL1=SYS.NFC.eCARD="1AAD1027":Msg.send.Serial1,0,"unauthorized_access=&(NFCUID)"&Msg.send.TCP,8,"nfc_unauthorized_access=&(NFCUID)"&SYS.NFC.LED1,hPulse,2000

**AL1**: It sends the ID of the passed NFC card with the test "unauthorized_access" together with the GPS position to the server. It also outputs this information on the 2nd serial port.

$PFAL,SYS.NFC.Enable=Serial0
$PFAL,Sys.Device.Reset

At the end send this command to activate the NFC on the 1st serial port of device and reset the device.

<table>
<thead>
<tr>
<th>Data transferred to the server</th>
<th>$authorized_access:0A921027*18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,,*00</td>
</tr>
<tr>
<td></td>
<td>$unauthorized_access:1AAD1027*0C</td>
</tr>
<tr>
<td></td>
<td>$GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,,*00</td>
</tr>
</tbody>
</table>

Table 1: Identification of specific NFC card, output data on 2nd serial port

If you would like to work with whitelist and store all IDs with access into a whitelist inside the device then use the configuration lines below:

$PFAL,Sys.WhiteList.Set0="7A848E0B"
$PFAL,Sys.WhiteList.Set1="A21148E0B"
.....
$PFAL,Sys.WhiteList.Set2999="B32175465"

Create a whitelist of authorized cards by their IDs. Once the whitelist is created, the FOX3-2G/3G/4G series will only accept the card IDs available in this whitelist. To edit a card ID in the whitelist use the same command with new ID.

$PFAL,Cnf.Set,AL0=SYS.NFC.eCARD=whitelist:Msg.send.Serial1,0,"nfc_authorized_access=&(NFCUID)"&Msg.send.TCP,8,"nfc_authorized_access=&(NFCUID)"&SYS.NFC.LED1,hPulse,2000

**AL0**: It sends the ID of the passed NFC card with the test "authorized_access" together with the GPS position to the server. It also outputs this information on the 2nd serial port.

$PFAL,Cnf.Set,AL1=SYS.NFC.eCARD=!whitelist:Msg.send.Serial1,0,"nfc_unauthorized_access=&(NFCUID)"&Msg.send.TCP,8,"nfc_unauthorized_access=&(NFCUID)"&SYS.NFC.LED2,hPulse,2000

**AL1**: It sends the ID of the passed NFC card with the test "unauthorized_access" together with the GPS position to the server. It also outputs this information on the 2nd serial port.

$PFAL,SYS.NFC.Enable=Serial0
$PFAL,Sys.Device.Reset

At the end send this command to activate the NFC on the 1st serial port of device and reset the device.

<table>
<thead>
<tr>
<th>Data transferred to the server</th>
<th>$authorized_access:7A848E08*13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,,*00</td>
</tr>
<tr>
<td></td>
<td>$unauthorized_access:1AAD1027*0C</td>
</tr>
<tr>
<td></td>
<td>$GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,,*00</td>
</tr>
</tbody>
</table>

Table 2: Identification of NFC cards available in Whitelist, output data on 2nd serial port
If you would like to control a door by an output then use the configuration line in chapter with the IO1 wired to the door locking system:

```
$PFAL,Sys.WhiteList.Set0="7A848E0B"
$PFAL,Sys.WhiteList.Set1="A21148E0B"
......
$PFAL,Sys.WhiteList.Set2999="B32175465"
```

Create a whitelist of authorized cards by their IDs. Once the whitelist is created, the FOX3-2G/3G/4G series will only accept the card IDs available in this whitelist. To edit a card ID in the whitelist use the same command with new ID.

```
$PFAL,Cnf.Set,AL0=SYS.NFC.eCARD=whitelist:Msg.Send.Serial1,0,"nfc_authorized_access=&(NFCUID)"&Msg.Send.TCP,8,"nfc_authorized_access=&(NFCUID)"&IO5.Set=hpulse,1000&SYS.NFC.LED1,hPulse,2000
```

**AL0**: It unlocks and locks the vehicle doors (depending on the vehicle type) using the IO1 wired to the door locking system and sends the ID of the passed NFC card with the test “authorized_access” together with the GPS position to the server. It also outputs this information on the 2nd serial port. It there is needed 2 outputs for unlock and lock the vehicle doors and 1 input to know the state of the door locking system then use these configuration lines and wire IO1 to unlock signal and IO2 to lock signal on the door locking system. The IO0 should be wired to the status of the door locking system – locked = 0V, locked=12V (Note: depending on the vehicle type the pulse duration may be longer than 1000 milliseconds):

```
$PFAL,Cnf.Set,AL0=SYS.NFC.eCARD=whitelist:Msg.Send.Serial1,0,"nfc_authorized_access=&(NFCUID)"&Msg.Send.TCP,8,"nfc_authorized_access=&(NFCUID)"&IO0.Set=hpulse,1000&SYS.NFC.LED1,hpulse,2000
$PFAL,Cnf.Set,AL1=SYS.NFC.eCARD=whitelist:Msg.Send.Serial1,0,"nfc_authorized_access=&(NFCUID)"&Msg.Send.TCP,8,"nfc_authorized_access=&(NFCUID)"&IO6.Set=hpulse,1000&SYS.NFC.LED2,hpulse,2000
$PFAL,Cnf.Set,AL2=SYS.NFC.eCARD=!whitelist:Msg.Send.Serial1,0,"nfc_unauthorized_access=&(NFCUID)"&Msg.Send.TCP,8,"nfc_unauthorized_access=&(NFCUID)"&SYS.NFC.LED2,hpulse,2000
```

**AL1**: It sends the ID of the passed NFC card with the test “unauthorized_access” together with the GPS position to the server. It also outputs this information on the 2nd serial port.

```
$PFAL,SYS.NFC.Enable=Serial0
$PFAL,Sys.Device.Reset
```

At the end send this command to activate the NFC on the 1st serial port of device and reset the device.

<table>
<thead>
<tr>
<th>Data transferred to the server</th>
<th>authorized_access:7A848E0B*13</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,*,&quot;*0</td>
<td></td>
</tr>
<tr>
<td>unauthorized_access:1AAD1027*0C</td>
<td></td>
</tr>
<tr>
<td>GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,*,&quot;*0</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3**: Identification of authorized NFC cards in Whitelist for door locking system

### 1.3.4.2 Device configuration when connecting the NFC reader to 2nd serial port

The table below shows how to configure your FOX3-2G/3G/4G series device if NFC reader is connected to the 2nd serial port. If you would like to connect the NFC reader to 2nd serial accessory port, please use the configuration in the section **1.3.4.1** above.

```
$PFAL,Cnf.Set,AL0=SYS.NFC.eCARD="0A921027":Msg.send.Serial0,0,"authorized_access=&(NFCUID)"&Msg.send.TCP,8,"nfc Authorized_access=&(NFCUID)"&SYS.NFC.LED2,hpulse,2000
```

**AL0**: It sends the ID of the passed NFC card with the test “authorized_access” together with the GPS position to the server. It also outputs this information on the 1st serial port.

```
$PFAL,Cnf.Set,AL1=SYS.NFC.eCARD="1AAD1027":Msg.send.Serial0,0,"unauthorized_access=&(NFCUID)"&Msg.send.TCP,8,"nfc_unauthorized_access=&(NFCUID)"&SYS.NFC.LED1,hpulse,2000
```

**AL1**: It sends the ID of the passed NFC card with the test “unauthorized_access” together with the GPS position to the server. It also outputs this information on the 1st serial port.

$PFAL,SYS.NFC.Enable=Serial1
$PFAL,Sys.Device.Reset
At the end send this command to activate the NFC on the 2\textsuperscript{nd} serial port of device and reset the device.

| Data transferred to the server | $\text{authorized\_access}=0\text{A921027}\ast 18$  |
|                              | $\text{GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,},*00$  |
|                              | $\text{unauthorized\_access}=1\text{AAD1027}\ast 0\text{C}$  |
|                              | $\text{GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,},*00$  |

Table 4: Identification of specific NFC cards, output data on 1\textsuperscript{st} serial port

If you would like to work with whitelist, you have to create a whitelist of authorized cards into a device with the configuration lines below:

```
$\text{PFAL, Sys.WhiteList.Set0}="\text{7A848E0B}"$
$\text{PFAL, Sys.WhiteList.Set1}="\text{A21148E0B}"$

.......
$\text{PFAL, Sys.WhiteList.Set2999}="\text{B32175465}"$
```

Create a whitelist of authorized cards by their IDs. Once the whitelist is created, the FOX3-2G/3G/4G series will only accept the card IDs available in this whitelist. To edit a card ID in the whitelist use the same command with new ID.

```
$\text{PFAL, Cnf.Set, AL0=SYS.NFC.eCARD=whitelist:Msg.send.Serial0,0,"nfc\_authorized\_access=&(NFCUID)\"&Msg.send.TCP,8,"nfc\_authorized\_access=&(NFCUID)\"&SYS.NFC.LED1,hPulse,2000}$

\textbf{AL0}: It sends the ID of the passed NFC card with the test “authorized\_access” together with the GPS position to the server. It also outputs this information on the 1\textsuperscript{st} serial port.

```
$\text{PFAL, Cnf.Set, AL1=SYS.NFC.eCARD=!whitelist:Msg.send.Serial0,0,"nfc\_unauthorized\_access=&(NFCUID)\"&Msg.send.TCP,8,"nfc\_unauthorized\_access=&(NFCUID)\"&SYS.NFC.LED2,hPulse,2000}$

\textbf{AL1}: It sends the ID of the passed NFC card with the test “unauthorized\_access” together with the GPS position to the server. It also outputs this information on the 1\textsuperscript{st} serial port.

```
$\text{PFAL, SYS.NFC.Enable=Serial1}$
$\text{PFAL, Sys.Device.Reset}$
```

At the end send this command to activate the NFC on the 2\textsuperscript{nd} serial port of device and reset the device.

| Data transferred to the server | $\text{authorized\_access}=7\text{A848E0B}\ast 13$  |
|                              | $\text{GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,},*00$  |
|                              | $\text{unauthorized\_access}=1\text{AAD1027}\ast 0\text{C}$  |
|                              | $\text{GPRMC,083157.000,A,5040.4185,N,01058.8433,E,2.42,169.88,250618,},*00$  |

Table 5: Identification of NFC cards available in Whitelist, output data on 1\textsuperscript{st} serial port
### 1.3.4.3 PFAL commands implemented for NFC in the AVL firmware 3.x.x

The table below shows the list of PFAL commands/events/dynamic entries implemented in AVL firmware 3.x.x for the NFC functionality.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS.NFC.Enable=&lt;Serial0</td>
<td>Serial1&gt;</td>
</tr>
<tr>
<td>SYS.NFC.Disable</td>
<td>Disables the NFC reader</td>
</tr>
<tr>
<td>SYS.NFC.Reset</td>
<td>Resets the NFC reader</td>
</tr>
<tr>
<td>SYS.NFC.LED[1..3],[&lt;Low</td>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE.NFC=&lt;Serial0</td>
<td>Serial1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Events/states</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS.NFC.eCARD=&quot;ID&quot;</td>
<td>Verifies whether or not the scanned card is the same with defined one.</td>
</tr>
<tr>
<td>SYS.NFC.sCARD=&quot;ID</td>
<td>None&quot;</td>
</tr>
<tr>
<td>SYS.NFC.eCARD&lt;comp&gt;whitelist</td>
<td>NFC event with a set of comparator (&quot;=&quot;&quot;,&quot;!=&quot;) to compare a scanned NFC card with the tag IDs available on the whitelist.</td>
</tr>
<tr>
<td>SYS.NFC.eLOST[&lt;comp&gt;whitelist]</td>
<td>NFC event with a set of comparator (&quot;=&quot;&quot;,&quot;!=&quot;) to compare a NFC card UID which is no longer detected but available on the whitelist. For example the fuel cards which normally are always inside the reader, the event occurs when it is removed.</td>
</tr>
<tr>
<td>SYS.NFC.sCARD&lt;comp&gt;whitelist</td>
<td>NFC state with a set of comparator (&quot;=&quot;&quot;,&quot;!=&quot;) to compare a scanned NFC card with the tag IDs available on the whitelist.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dynamic entries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;{(NFCUID)}</td>
<td>Reports the UID (manufacturer code) of the NFC card</td>
</tr>
</tbody>
</table>

*Table 6: PFAL commands for NFC readers*