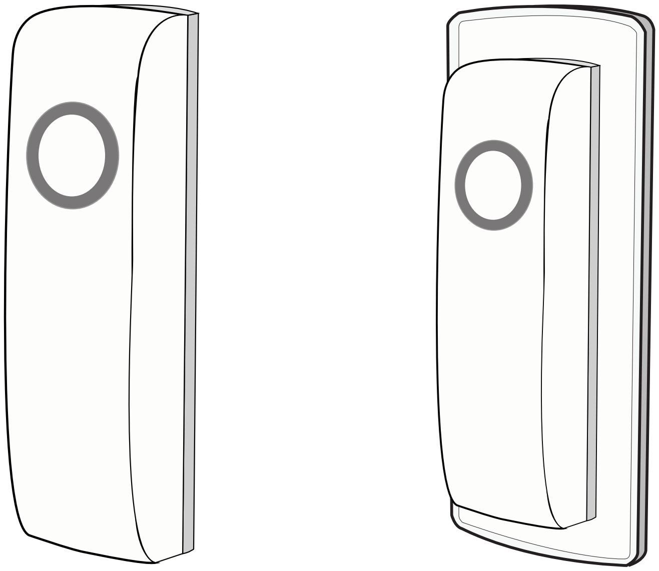
Linear®

# BluePass

## 2-N-1 BluePass Multi-Tech Reader Manual



# User's Guide

NORTEK
SECURITY & CONTROL
USA & Canada (800) 421-1587 & (800) 392-0123
(760) 438-7000 - Toll Free FAX (800) 468-1340
www.nortekcontrol.com

P/N: 10019180 X14

## Contents

## Overview

The Linear BluePass Multi-Tech Reader provides a simple and convenient way to leverage state of the art BLE mobile credentials for access control. Whether a new site installation or an upgrade of an existing system, realizing the power of mobile credentials is a very simple process. In this guide, we will walk you through setting up and configuring the necessary to get started.

There are several major components in the Linear BluePass ecosystem solution illustrated in this guide:

1. The Linear BluePass Portal – This is a web based portal used by the dealer/installer/facility administrator to manage mobile credentials.

   Portal functionality includes:

   a. Redeem your Credential-To-Go™ cards for mobile credential credits.

   b. Define top level Organizations in which end-users have access to via mobile credentials.

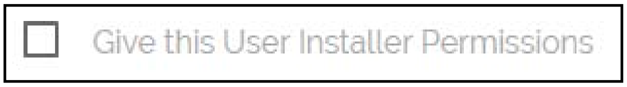
   c. Issue mobile credentials to end-users for access to an Organization.

   d. Manage existing BLE credentials, their associated Wiegand IDs, and view reports on the number of credential credits remaining for issuance.

2. The Linear Wallet Mobile Application – This mobile app is available for both iOS and Android.
   The app serves two purposes:

   a. Intended for use by end-users of an organization to gain entry to a protected area using a BluePass Multi-Tech Reader. It displays virtual credentials assigned for use when the app is opened. Under normal circumstances, the app runs silently in the background of the user's mobile device, transmitting the end-user BLE credential to the reader when the user activates the reader's capacitive touch sensor, typically by touching the reader.

   b. The Installer Permission Credential + The Linear Wallet APP – To gain entry to a protected area using BluePass, as well being designed specifically for the dealer/installer to configure and manage BluePass Multi-Tech Readers installed at the Organizations they manage. This permission is granted by checking the installer Permission box located at the bottom of the "Add User" page.



□ Give this User Installer Permissions

This Permission allows the Administrators/Installers to:

   c. Enroll (assign) your reader to a specific Organization configured in the Dealer Portal account.

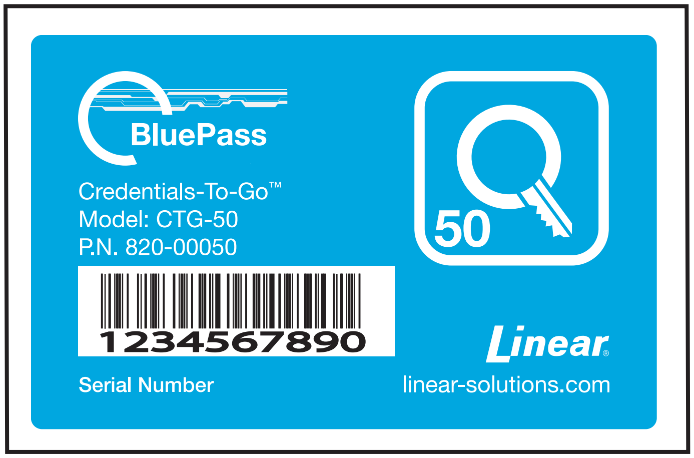
      i. Change setup configurations of individual reader hardware, such as BLE range requirements for acceptance of access requests, and the reader power setting for LED intensity and animations.

      ii. In-field firmware upgrades and advanced version reporting.

3. The Linear BluePass Multi-Tech Reader – This is the physical reader hardware that supports a standard mullion-style or U.S. single-gang mounting installation. The reader uses standard 26 to 37-bit Wiegand formats and supporting legacy 125 KHz prox cards, as well as the Linear BluePass Mobile Credential. The reader is configured using the Linear Dealer/Installer Mobile Application during installation.

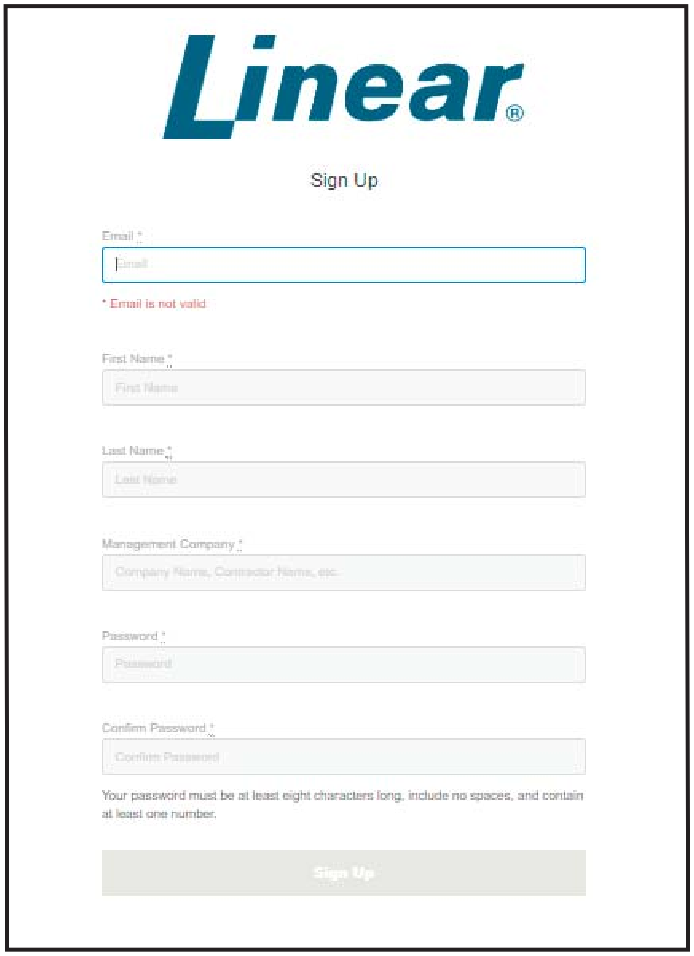
## Setting up Your Dealer Portal Account

To begin, a Credential-To-Go™ card must be purchased. Once a card is obtained, set up your dealer/installer account login by visiting https://bluepasscloud.io.



## Setting up Your Dealer Portal Account (*Continued*)

1. Click on the link at the bottom of the login page titled, “Are you a new user? Sign Up.”
2. Enter your e-mail address, first name, last name, dealer name, and a password. Be sure to follow the password guidelines as listed on the sign-up page.



Your password must be at least eight characters long, include no spaces, and contain at least one number.

3. Click Sign Up.
4. The dealer/installer account is now set up.

Now that the dealer/installer account is established, some Organizations must be set up within the portal the dealer/installer for managing the BluePass Credentials and Readers.

## Setting up Readers within your Organization

### Organization

An Organization is the top-level entity in the Access Control hierarchy and represents the end-user company the system is being installed into.

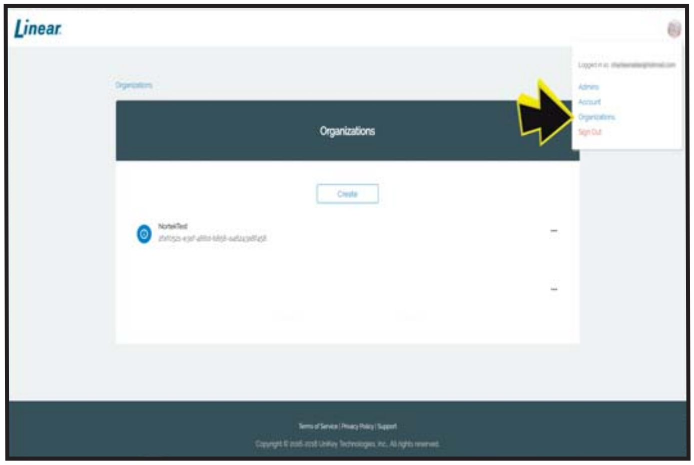
### Reader

A reader is assigned to an Organization. The user’s credentials are presented to the reader and passed along to the Access Control System for validation. If the access request is valid, entrance is granted at that reader access point.

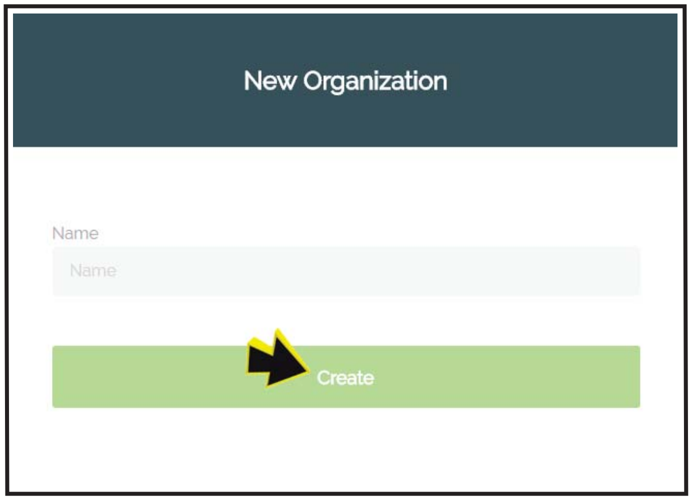
### Creating Your First Organization

You must first add credentials, followed by assigning installer credentials, which allow a reader to be assigned.

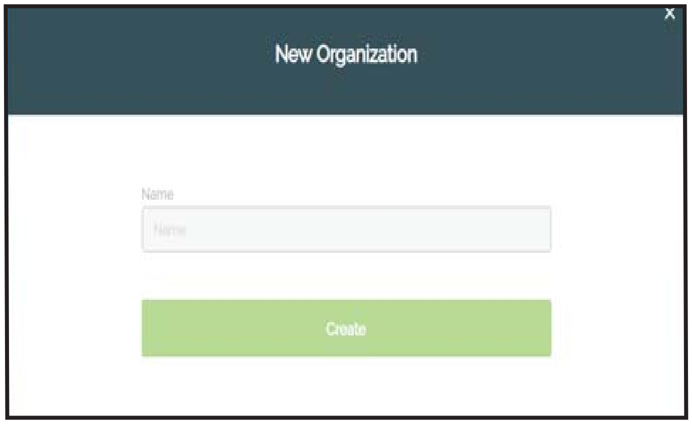
1. In the upper right hand corner of the portal, select “Organizations.”



2. You are now on the “Organizations” page. Click “Create.”



3. You are now on the “New Organization” page. In the “Name” field, enter the name of the Organization you wish to create.

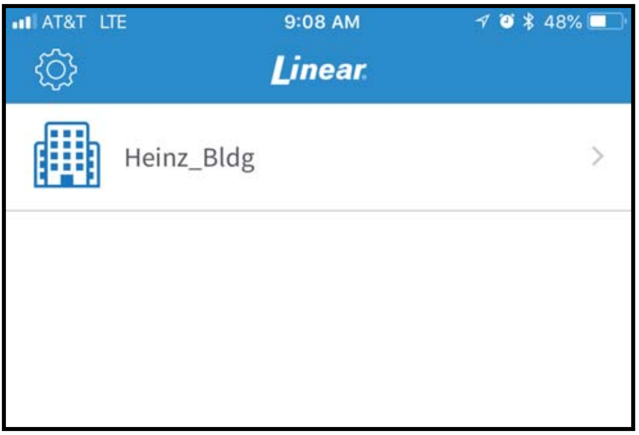


Now that you have at least one Organization created, it is time to install readers at the actual facility.

## Setting up Your First Reader

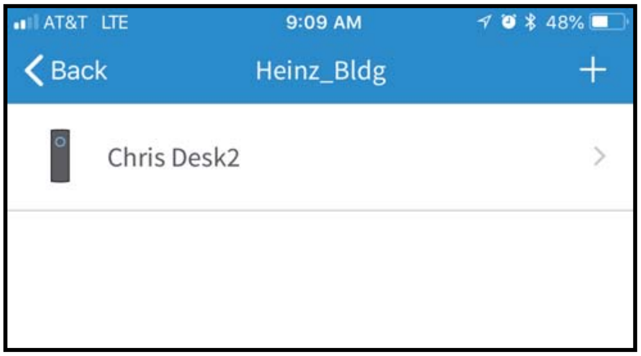
You must now add credentials then assign an installer credentials which allows a reader to be assigned.

1. Using the enclosed Getting Started guide found in your reader packaging, follow all wiring and safety precautions to connect the reader to your access control panel.
2. Once wired and mounted to the protected area, the reader should be illuminated with a solid amber ring animation. This animation indicates that the reader is powered, but not yet configured to use BluePass Mobile Credentials. The reader can, however, fully function as a standard 26 to 37-bit 125 KHz prox reader that is compatible with cards and fobs commonly found in the marketplace.
3. From the Linear BluePass Web Portal you will need to issue at least one credential with "Installer Permissions" (This credential type will be needed for all steps below.)
4. After following the steps to Accept the BluePass credential with "Installer Permissions," open the Linear Wallet Mobile Application and press the ">" located to the left of the Organization Name.

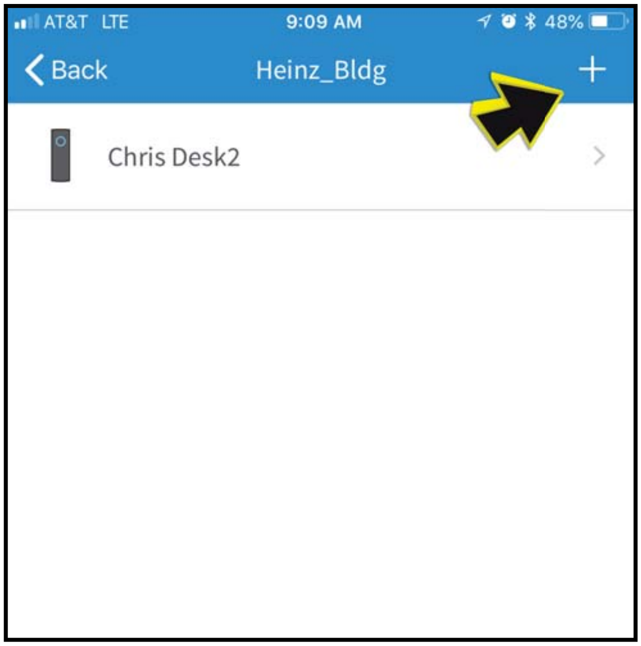


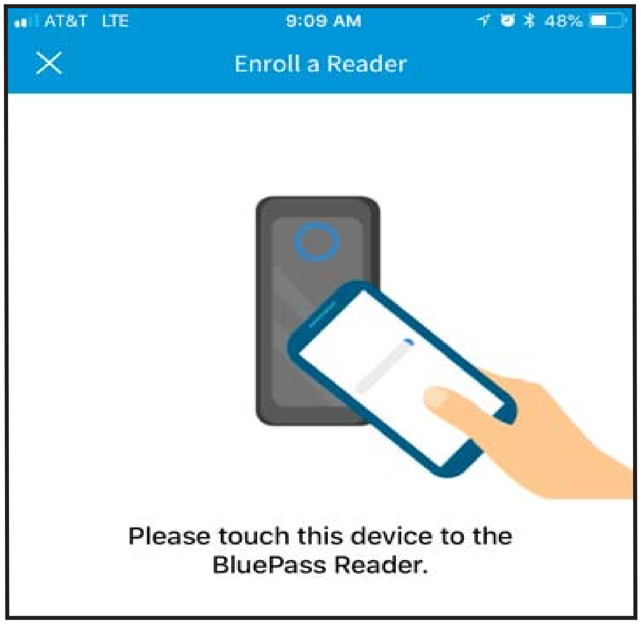
**Notes:**

- If this is the first reader you have assigned to this Organization, you will now see a blank list.
- If you previously assigned readers to this Organization, you will see the names of all the readers you previously configured that are currently assigned to this Organization.



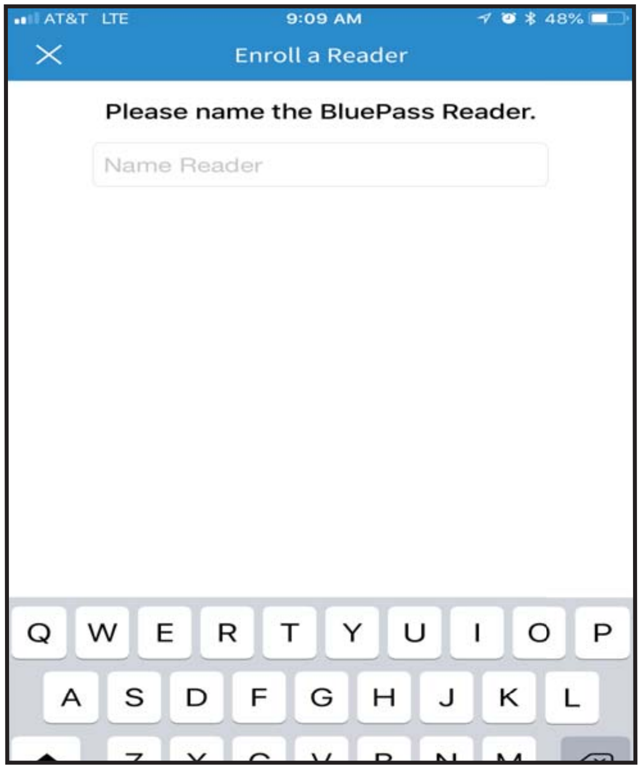
5. In the upper-right of your screen, click on the "+" icon to add a new reader to this Organization.





Please touch this device to the BluePass Reader.

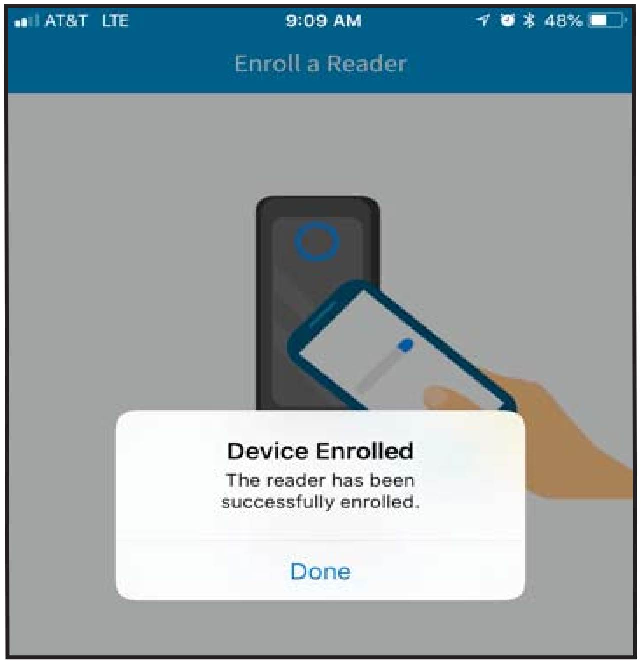
6. Enter a name for the reader or door that the reader is installed for. We suggest a descriptive name that will make management easier, such as "West Entrance Door" or similar. It is also advised that the name used matches the name of the door within the access control system (if applicable), so that two different names do not exist for the same door or entrance. Whatever name is chosen will be displayed in the list of readers for that Organization later.



Please name the BluePass Reader.

Name Reader

7. After naming your reader, click submit and you will receive a message telling you enrollment of your reader was successful.

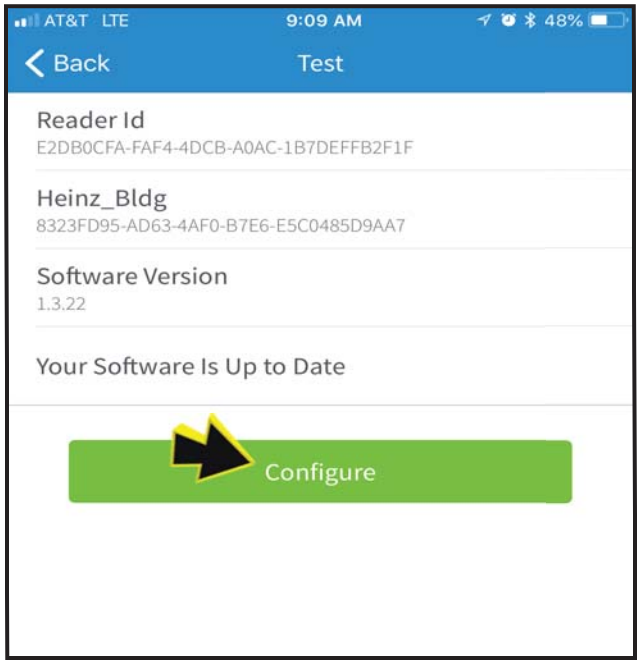


Device Enrolled

The reader has been successfully enrolled.

- You can now check for any available firmware updates for this reader. If an update is available, follow the prompts to successfully do so. Continue to maintain a close physical connection between the mobile device and reader, as the firmware update process can take several minutes to complete.
- You can now also configure your reader.

8. Tap the "Configure" button.



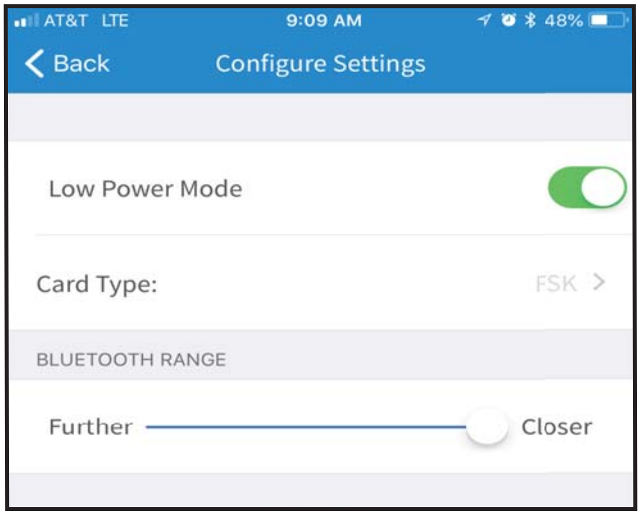
Reader Id
E2DB0CFA-FAF4-4DCB-A0AC-1B7DEFFB2F1F

Heinz_Bldg
8323FD95-AD63-4AF0-B7E6-E5C0485D9AA7

Software Version
1.3.22

Your Software Is Up to Date

9. On the reader configuration page, there are two options:



Low Power Mode

Card Type: FSK

BLUETOOTH RANGE

Option 1 - Sets the BLE range restrictions. This determines whether the end-user's mobile device must be presented to the reader or if it can remain in their pocket. This is a very important consideration, as it is advisable to set the range to be as short as possible for building entrances that are in close proximity to employees' work spaces or break areas.

- If the reader's Bluetooth reception strength is set too high, it may inadvertently pair with an employee's mobile device and allow unauthorized entry into the building simply by waiving a hand over, or touching, the reader.
- For maximum security, it is advisable to have to the reader's Bluetooth signal reception strength set to the most minimal level, requiring the end-users to present their mobile device to the reader in order to request access.

Entrances where security is less of a factor:

Interior doorways

- Locations where other employees are working far from the doorway
- Bluetooth reception strength may be adjusted to allow users to request access without having to present their mobile device to the reader.(This will vary Phone to Phone)

Option 2 - Controls the power mode which affects the LED intensity and animation scenes.

- Choose the power mode settings you would like for the reader and then select “BACK.”
- Future capabilities will be available in subsequent versions for the administrator app, including the ability to disable the 125 KHz RFID antenna for an added layer of security.

The reader should now have a solid blue animation indicating it is ready to process BluePass Credentials.

## Performing a Factory Reset on the Reader

A factory reset is performed in order to clear the reader of existing organizations and corresponding end-user credentials, as well as to clear any firmware updates initiated on the reader since manufactured. Access to any specified organization will need to be re-established, and firmware will need to be reinstalled to the latest version before using the reader

1. To locate the reset button on the reader, dismount from the installation points. the reset button is located on the back of the reader, as depicted in Figure 1.
2. Disconnect the reader from the power source.
3. Begin holding down the reset button; while holding the reset button, reconnect the reader to the power source. Please note that the card-present line must be connected to ground during this step.
4. Give the reader a minimum of 10 seconds to reset, and release the reset button.
5. The LED on the front of the reader will momentarily be off while the reader reconfigures.
6. After the reader has completed the factory reset, the LED ring will momentarily flash white, then change to amber.
7. The reader’s enrollment has now been cleared, along with any firmware updates that have been initiated since it was manufactured.

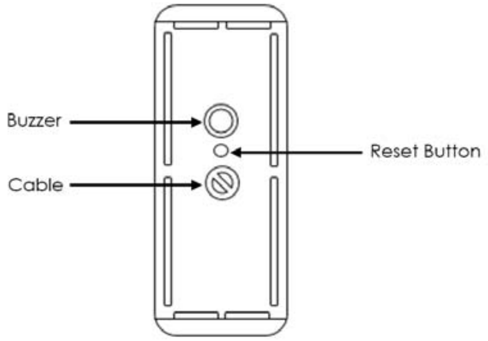
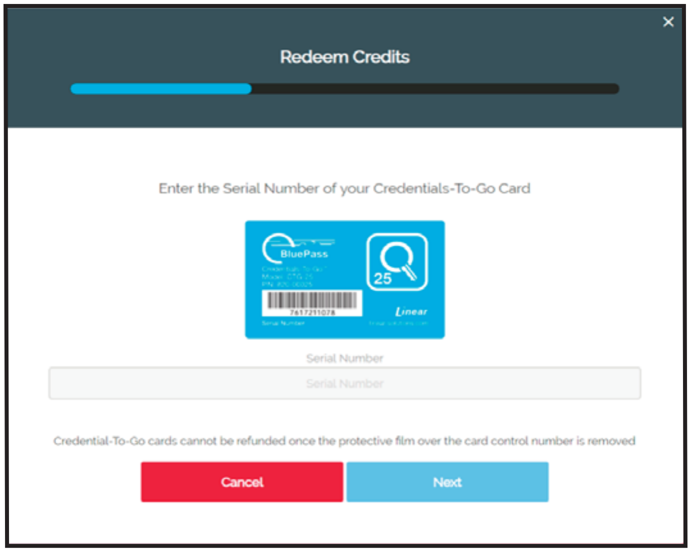


**Fig. 1** Reset button is located on the back of the reader between the buzzer and the cable.

## Issuing Your First BluePass Credential

Now that you have configured at least one reader for an Organization you are ready to send your first BluePass Credential to an end-user for access.

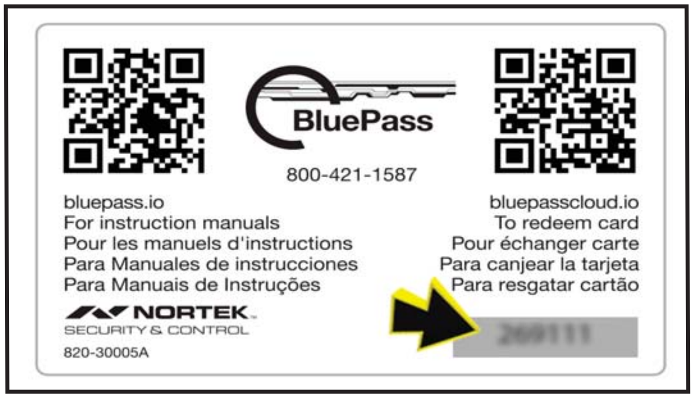
1. Create or locate a valid Wiegand credential in the Organization’s access control panel and take note of the ID and Reader Group Code values.
2. Login to the Dealer Portal using your previously configured username and password.
3. Locate the intended Organization and click on the ellipsis to open the pop up menu. Select “View/Add Users.” On this page, click on “Redeem Credits.”



Enter the Serial Number of your Credentials-To-Go Card

Credential-To-Go cards cannot be refunded once the protective film over the card control number is removed

4. Enter the serial number from your previously purchased Credential-To-Go™ card and click “Next.”



BluePass

800-421-1587

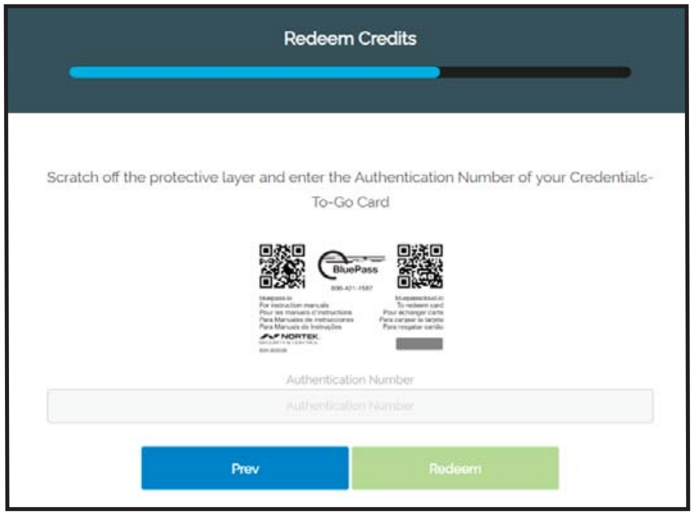
bluepass.io
For instruction manuals
Pour les manuels d'instructions
Para Manuales de instrucciones
Para Manuais de Instruções

bluepasscloud.io
To redeem card
Pour échanger carte
Para canjear la tarjeta
Para resgatar cartão

[redacted]

NORTEK
SECURITY & CONTROL
820-30005A

5. Enter the authentication number on the back of the card by scratching off the protective film and entering it into the Blue Cloud Portal.



Redeem Credits

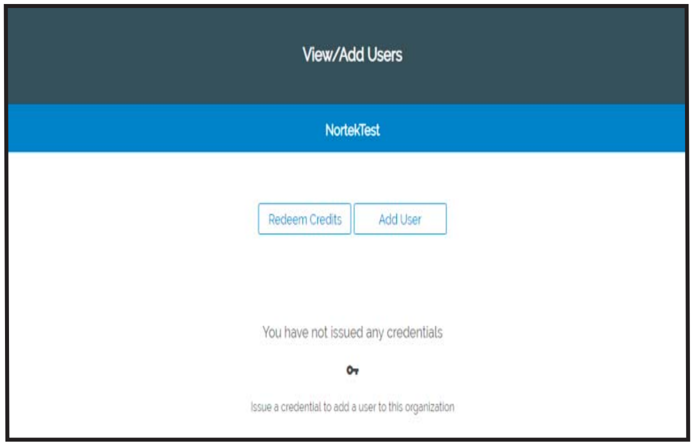
Scratch off the protective layer and enter the Authentication Number of your Credentials-To-Go Card

Authentication Number

6. Select the redeem button.

Your account has now been credited with mobile credential credits.

7. Select "Issue Credential." In the "View/Add Users" page, click on "Add User."



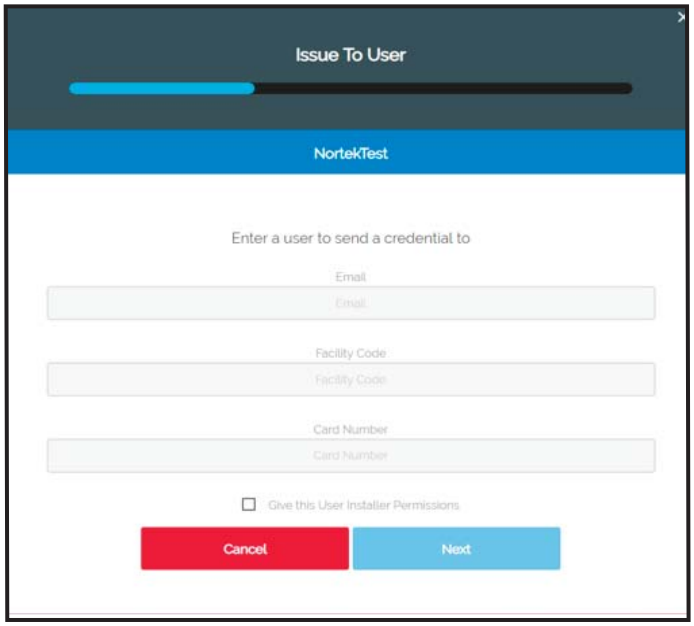
View/Add Users

NortekTest

You have not issued any credentials

Issue a credential to add a user to this organization

8. Enter the email address, facility code, and card number for the user you would like to issue the mobile credential and click "Next."



Issue To User

NortekTest

Enter a user to send a credential to

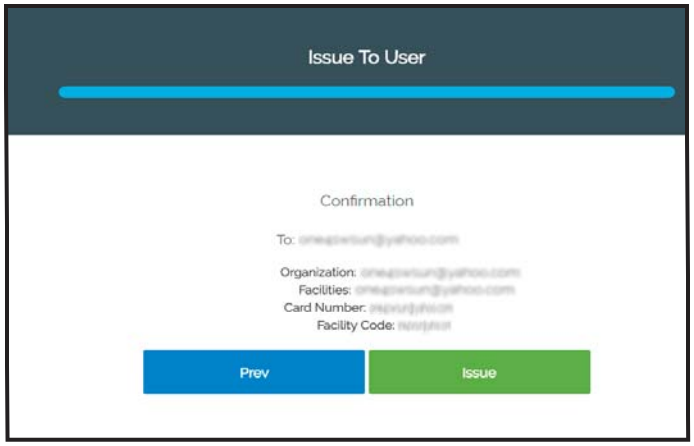
Email

Facility Code

Card Number

□ Give this User Installer Permissions

9. Confirm the information is correct and click the "Issue" button. The end-user will receive an invitation e-mail with instructions for installing and using their BluePass Mobile credential.



Issue To User

Confirmation

To: [redacted]

Organization: [redacted]
Facilities: [redacted]
Card Number: [redacted]
Facility Code: [redacted]

## Accepting Your First BluePass Credential as an End-User

1. The email from the administrator will provide two links, one for downloading the BluePass App, and the other for downloading the BluePass Credential.
2. Download and install the BluePass App from the iOS App Store or the Android Play Store as appropriate for your device's operating system.
3. Use the other link provided in the e-mail to obtain your BluePass Mobile Credential.
4. A dialog box will appear asking if you would like to open the link using the BluePass Application
5. Select "Open." The BluePass Wallet App will open and after a brief period of time a virtual "access card" will appear in your Wallet App.

6. Once the access card icon has appeared in your BluePass Wallet App, you may present your phone to the reader. The light ring will display a blue spinning animation indicating that the reader is actively searching for nearby BluePass Credentials. You will then hear a beep indicating that the Wiegand ID has been transmitted securely from the mobile device to the reader followed by a green flash LED animation sequence once access is granted by the on-site access control panel.

## Frequently Asked Questions

**How much power does the BluePass Reader use?**

- 100 - 200 mA typical, 225 mA max peak @ 12 VDC low-power mode. Bright light power mode available.
- High power mode - 120 mA @ 12 VDC

**What voltage does the reader require?**

- +5.5 - 16 VDC at the reader. Regulated power supply and 12 VDC at the reader is recommended for best operation.

**What prox cards does the reader support?**

- The reader supports HID™ compatible 26 - 37-bit 125KHz Wiegand formats
  Other bit formats will be supported in the future with OTA reader firmware updates.

**What card technologies are supported?**

- 125 KHz Prox and Bluetooth Low Energy

**Which RFID modulations are supported?**

- EM4102 (ASK modulation)
- ISOProx II (HID™ Prox II H10301 compatible FSK modulation)

**Does the reader support RS-485/OSDP?**

- Not at this time.

**How can it replace an existing reader?**

- Swapping of an existing 26 to 37-bit 125 KHz reader with a new BluePass Reader and is simple and easy with common Wiegand wiring.

**What do I do if I am replacing a single-gang reader with this mullion reader?**

- The mullion reader comes with a U.S. single-gang adaptor plate. The mounting holes are aligned with the most common mullion readers on the market.

**Does the reader require any special access control panel features to work?**

- No. The Reader is compatible with most preexisting access control panel that supports standard Wiegand protocol input/output.

### Mobile Applications

**What phones/devices are supported?**

- Any Apple device running iOS 10.0 or higher
- Android devices running Android v5.0 (Lollipop) or higher that supports BLE peripheral mode.

**Does the Linear App have to be running in the foreground or “active” to enter a door?**

- No, as long as the app has been launched after the phone is powered on, it can run silently in the background without any further interaction by the user needed to enter a door, except for presenting the phone to the reader.

**Do I have to present my phone to the reader to enter a door?**

- The allowed distance between reader and mobile device is configurable by the facility manager on a per reader basis. The range can be restricted such that a user must present the mobile device to the reader much like a legacy prox card. Alternatively the range setting can be relaxed allowing the user to simply wave their hand near the reader and leave the mobile device in their pocket, backpack, or purse when requesting access.
- We strongly recommend that in most cases the BLE range settings of the readers be set to the shortest range possible to prevent inadvertent access into the building and for the highest level of security.

**How do I receive Bluetooth Credentials to a building?**

- You will receive an email from your facility manager to download the mobile application and mobile credential. Select the link for each step to successfully download the app and accept the credential.

**How do I get the mobile app?**

- Typically, you will download the apps via the App Store for iOS and the Play Store for Android.

**Do I have to have an internet connection to enter a door using a mobile key?**

- No, once you have accepted the BluePass Mobile Credential on your mobile device it is securely stored on the device and requires no network connectivity to request access to a door. Only Bluetooth is required.

**Are mobile keys secure?**

- The BluePass Mobile Credential uses the CORE™ platform which features a robust security architecture. It is based on the largest mobile key platform in the world with more than 135 million access transactions to date. Credentials feature AES128 encryption using a PKI implementation that meets or exceeds industry standard best practices.

**As a facility manager, how do I issue, modify or revoke mobile credentials for my users?**

- Facility managers have access to a simple web portal that allows them to redeem credential credits using Credential-To-Go™ cards, create new end-users, or modify existing end-users. These actions take effect immediately on the end-user mobile device.

**Note:** Additional FAQ information can be found by visiting https://bluepasscloud.io.

## Troubleshooting

| Issue | Corrective Action |
|---|---|
| The reader will not read cards and fobs. | Check cards and fobs to ensure they are HID™ compatible 26 to 37-bit 125 KHz RFID. |
| End-user was issued credentials and replaced their mobile device with a newer model. They downloaded the app and used their original e-mail invite link to reinstall credentials on their new device. The installation was unsuccessful. | BluePass mobile credentials are only good for the life of the original mobile device. Once a new device is purchased, new credentials are required, even if the phone number has not changed. |
| I installed the system in a multi-tenant residential condominium complex. The property management company wants to re-use mobile credentials from departing tenants, reissuing them to the new tenants moving in. Is there an option in the dashboard to repurpose the same credentials without having to buy them each time this happens? | No. BluePass Credentials are tied to specific mobile devices. The only way the property management firm could do this is if they owned the mobile devices, repurposing the device from a departing tenant to a new tenant. A more viable and less expensive option would be to use BluePass Bluetooth fobs. |
| Our customer wants to fully migrate away from 125 KHz cards and fobs, turning off that portion of the reader so it will only read the Bluetooth-based credentials. Can I turn off that portion of the reader? | Currently, you cannot turn off the 125 KHz portion of a reader. |
| My customer has a home access control system and has programmed it so he can use the same fob that he uses to access the building at his work, he simply programmed the same legacy credential ID number from his fob into his home system. This makes it convenient, requiring him to only need one credential. Does the BluePass system allow for the same thing? | No. The system is specific to each organization. Your customer's home reader will not read the employer's BluePass credential at all. The customer will need to have two BluePass credentials; one for home and one for work. When the customer replaces their mobile device, two new credentials will need to be purchased. |

## Certifications

FCC 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.

2. This device must accept any interference received, including interference that may cause undesired operation.

Product can be used without license conditions or restrictions in all European Union countries, including Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Luxembourg, The Netherlands, Portugal, Spain, Sweden, and the United Kingdom, as well as other non-EU countries, including Iceland, Norway, and Switzerland.

Intertek

Nortek Security and Control LLC reserves the right to change specifications without notice.