



FAQs

Question (Q): What is BluePass™?

Answer (A): BluePass™ is the brand name Nortek has created for our BLE-Based Mobile Credential Reader, Cloud-based credential management and issuance service, and smart-phone applications.

Q: What are the components of BluePass?

A: Components consist of:

- BluePass Reader – Reads 125kHz HID Compatible, 26 - 37 bit and BluePass BLE-based mobile credentials.
- BluePass Credentials - are purchased via our patent pending Credentials-To-Go™ (“CTG”) redemption card. Purchased at your local supplier and instantly redeemable, CTG cards are sold in packages of 5, 25, 50 and 100 credential credits.
- BluePass Cloud – a software management tool for dealers and system administrators who can create an account to issue and manage credentials.

Q: How does the BluePass reader and credential work?

A: The BluePass reader has three antennas, the first is capacitive touch. When the reader is touched or a hand or body part is near the reader it senses a user. When this occurs the reader turns off the capacitive touch and turns on two credential antennas - BLE and 125kHz. The user then should present the credential (card, fob and or phone). Depending on several factors, such as the BLE range settings of the reader and make/model of phone, the signal strength may allow the reader to read the credential without having to present the phone to the reader. All smart-phones have different BLE performance, depending on model and manufacturer, so some may have to be presented to the reader, while others can remain in a pocket or purse while you simple touch the reader.

Q: What is the best way to use the system?

A: Touch the reader and present your physical credential (key fob) or touch reader with phone or with hand and phone in pocket.

Q: How are credentials redeemed and issued?

A: BluePass Cloud provides a function called “redemption”. This step allows the administrator to enter information found on a Credentials-To-Go™ card. These numbers, when properly entered, apply the amount purchased on the redemption card to the account credential bank.

Issuing a credential is easy. The system allows for the addition of one card or a flat file import of many cards. In this step, the administrator can define the card format and code. Each recipient of a mobile credential is e-mailed an invitation to obtain the credential. In this invitation step, the recipient first downloads the app and that enables the acceptance of the credential. BluePass Cloud maintains a list of all invites and the current status of the issuance.

Q: What options do we have to add credentials into BluePass Cloud?

A: The system offers the ability to issue one BluePass credential at a time or a bulk load of credentials via a CVS flat-file import. The easiest way to determine the input data position (flat file format) is to hit "Export," which will provide the column headings for the alignment of the user data to import.

Q: What happens if the person you sent a BluePass credential does not receive it?

A: The BluePass administrator can log into their cloud account and see the status of the credential invitation. The administrator now can resend or revoke the credential. If this occurs, we recommend the recipient reviews their spam mail box as it may have been filtered out.

Q: Why are there two types of credentials that can be sent?

A: Type one is a "Standard" credential and all this provides is the basic functionality of a credential, allowing the user to present the phone to the reader to gain access into a building.

Type two is an "Installer" credential. This credential is important to the BluePass Eco-System as it provides additional functionality within the BluePass app allowing the installer to set up, calibrate the reader's BLE range, control of the reader's LED brightness (power mode), and perform over-the-air reader firmware upgrades. Additional functionality may be provided in the future. Unlike competitive offerings, you do not need to purchase a configuration card to manage the reader, as it is all done with the app.

Q: Why do you need to enroll readers into the organization?

A: Part of the system's security layer is the enrollment of readers to a specific organization. A layer of the ecosystem encryption is built around SSID of the readers in the system. This means that every reader enrolled under each organization has a unique ID and this ID establishes ownership of each reader to a specific organization. Only credentials associated with that specific organization's readers will work. This added layer of security - on top of BLE security standards - ensures that the credential data is secure.

Q: What is an organization?

A: An "organization" is considered an installation. It could consist of one or many locations. We provide the option to support multiple organizations as a dealer may elect to issue credentials to customers and/or end-user organizations may want separate credentials and encryption in different areas of their facilities.

Q: What if BluePass Cloud is not working. Will my credential work?

A: Once the application is installed and a credential is accepted onto your smart device, the smart device does not need to be on-line. The cloud service is only to manage and distribute credentials. For example, you may have been in an elevator or basement where cell service did not work. The BluePass App will still work, as it is not dependent on being connected to a cell or Wi-Fi service. You only need Internet access to download the app and accept the credentials that have been issued to you. Once accepted they are securely stored on the smart-phone and there is no further need for an Internet connection.

Q: If I lose my phone - or get a new phone - do I need to get a new BluePass credential issued?

A: Yes, the credential is tied to the life of each phone. To issue a credential to a new phone simply e-mail another invitation to the user of the new phone.

Q: What if I need help understanding how to design a system with BluePass?

A: Linear offers both an “access” hot line and e-mail submission address. Our staff is uniquely knowledgeable on design, wiring for both telephone entry, access control and gate products. E-mail your request or information to: Appdesk@nortekcontrol.com or call our dedicated phone line: 888-944-5897.

Q. Is BluePass Cloud a cloud-based access control system?

A. No, it is not. The BluePass reader has the same basic purpose and functionality of other readers with regards to passing a user’s unique ID number to a system that controls access into an organization’s facilities. The BluePass Cloud only functions as a cloud-based credential distribution and management system and a method to store credential inventory, in the form of credential credits. It does not directly control access into a building.

Q. Is this reader compatible with other systems in the market or specific to only Linear branded Access Control panels?

A. The reader is Wiegand-based and therefore backwards compatible with the vast majority of installations around the globe. Almost any Access system that is 26 to 37-bit 125kHz HID compatible (H10304 compatible) can be upgraded to BLE reader and credential technology with BluePass.

Q. Do I need to create multiple BluePass Cloud accounts to allow my end-user customers to distribute and manage their own credentials?

A. There are two primary use cases for setting up a BluePass Cloud account.



The first use case is for a dealer who will **exclusively** manage credential issuance for multiple organizations (end-user organizations). In this case, the dealer creates an account and then will create multiple organizations under the dealer's e-mail address or user name account. Once the

organization is set up, the dealer can issue credentials to each individual for that organization. Note that one account can manage many organizations but there is only one user and password per account. The dealer should not share this log in information as the user can see all organizations information.

The second use case occurs when **the dealer sets up the account with the end user's email address and generic password**. The dealer then goes into the account and issues themselves an installer credential, sets up the readers, and as part of the service, possibly issues credentials. *When they transfer all the systems over to the end-user, they should inform the end users to change the password. Should the end user want the dealer to have access, they can provide the user name and password and elect to change after the assistance is provided.*

Q: Can a user share their credentials with someone else?

A: No. After a user's credentials are imported into the BluePass app, they cannot be shared with anyone. The credentials are assigned to that user and can't be imported to another device.

Q: I'm an admin and one of my end-users complained that they didn't get the BluePass credential email. What do I do?

A: First, confirm that their email address is correct in the User List in the admin portal. If their email is incorrect, revoke the original credential and send a new one. If the email is correct, have the user check their spam folder to make sure the email didn't end up there. If it isn't found in the spam or deleted folder, you can reissue the credential using the admin portal. This will resend the original credential invitation email to them.

Q: I plan to get a new iPhone soon and want to know if my BluePass credential will move to the new phone.

A: Moving from one mobile phone to another requires the admin to send a new credential to you that you will import into the BluePass app on your new phone.

Q: I'm a BluePass administrator. What do I need to do when someone leaves our company?

A: Removing a user is a two-step process: 1.) First and foremost, remove access rights for the end-user's card number from the access panel and 2.) Revoke the user's BluePass credentials in the admin portal.

Q: Nothing happens when I tap on the blue ring of the BluePass reader. I figured it's a button and that's what I'm supposed to tap. What's wrong?

A: The top portion of the BluePass reader including the blue ring does not have the electronics behind it that scans for user taps. The active tap scan area is the rectangular front of the reader below the blue ring.

Q: **I have an iPhone and I routinely shut down apps manually because someone told me that it will make my battery last longer. I figured out that the BluePass app doesn't work when I do that. Why is that?**

A: If you manually shut down the BluePass iOS or Android app, it is not running any longer and it can't process the BluePass credential validation that is triggered when you tap the reader. It's a misconception that shutting down iOS apps increases battery life. The BluePass app utilizes very little battery on the device and the app should be left running at all times.

Q: **I'm an admin and I need to know if we can add more readers to our organization after the initial installation? What do my users need to do to use new readers?**

A: Simply install and enroll new readers in your existing organization, and your existing users will automatically get updated credentials with permissions to the new readers behind the scenes.

Q: **I'm an admin and we have an area in our company that only select employees are allowed to access. How do I set that up using BluePass readers?**

A: Just like you would do with any other reader - by setting up access levels and rights in the access control panel. Remember BluePass is simply a Wiegand-based reader not an Access Control system.

Q: **How do I remove installer permissions for a user who is still with our company, but is not responsible for managing the BluePass readers now?**

A: Revoke the existing credential for that user and send a new credential that doesn't include the installer permission.

Q: **Will the BluePass app only work with smart-phone? What about other devices like tablets?**

A: The BluePass app can be loaded and function on most mobile devices such as iOS and Android based tablets as well as phones.

Q: **I have Installer rights for my organization and I have some end-users who have to present their phones to the readers while others can simply keep their phones in their pockets or purse and just touch the reader to gain access? The end-users who have to present want the**



same ability to leave their phones in their pockets. Can I just simply boost the BLE range of the reader to a higher level?

A. If you boost the range higher for the end-users that have to present their phones to the reader then the range will be even further for the users who can currently keep their phones in their pockets, so this could pose a risk of inadvertent entry from distance or from inside the building. As a general rule, we strongly recommend keeping the BLE range set to the factory default for the highest security level possible, which allows the majority of phones to function with the reader.

Q: Does the BluePass reader work with all phones that have Bluetooth?

A. BluePass works with various phone models and iOS and Android operating systems and we have attempted to provide interoperability to the most current and popular phones in the market, but there are some older phones that are not supported. Please go to our web site for a current list of compatible phone models and operating systems. Bluetooth fobs and/or stick on proximity tags applied to the back of an end-user's phone can provide BluePass reader interoperability, if the end-user does not want to purchase a newer phone.