Mobile Connect App

The Gallagher Mobile Connect App delivers secure mobile access combined with the power of Bluetooth® wireless technology.

Secure Mobile Access

Downloadable from the Apple App and Google Play stores, this software provides users with the ability to use their mobile device as an access credential with Gallagher's Bluetooth wireless technology enabled products.

Download on the App Store

GET IT ON Google Play

Mobile Connect interfaces directly with Gallagher Command Centre, and allows users to:

- Open doors with their mobile device just like an access card

- Store access credentials for multiple sites

- Use long range access with Bluetooth® wireless technology

- Store their fingerprint or PIN data on the mobile device, privately and securely using FIDO open standard security

- Interact with building systems

Convenient Credential Management

Set-up and provisioning for users is a simple process, as is the management of mobile credentials within Command Centre. Benefits for the security manager of a site include:

- Eliminating the replacement cost of lost/stolen cards (including the time spent on the administration involved). Users are much less likely to lose their mobile device than an ID card

- Remote provisioning, which allows access to be set up in advance of a user attending a site. Perfect for managing temporary site users (like contractors). Credentials can be scheduled to both begin and expire when needed

- Two factor authentication for added security. If required users can be directed to use a second authorization step (like fingerprint or PIN) on the mobile device to gain access to select areas

Mobile Connect App
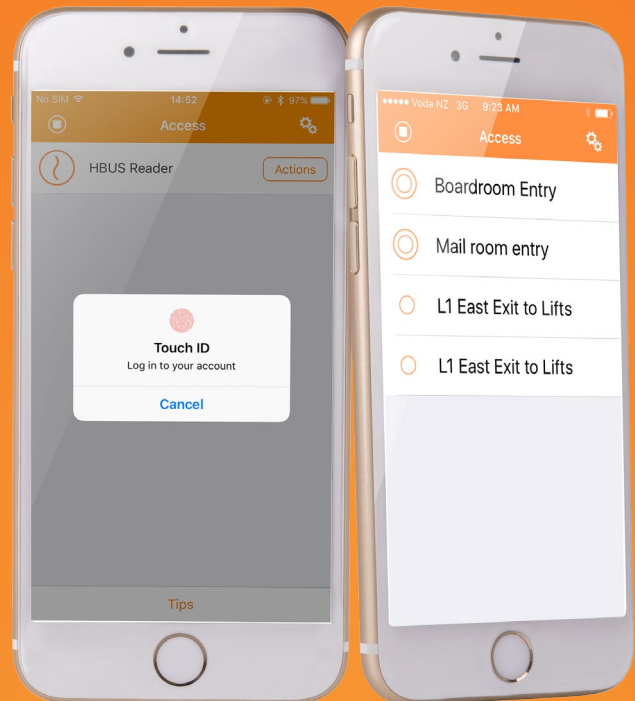
Control your Environment

Mobile Connect makes it possible for users to perform a number of tasks such as arming an Alarm Zone, changing the Access Mode for a door, or turn on lights and air conditioning. This is achieved by allowing outputs to be toggled on or off and means that anything that a system output can do can also be done from Mobile Connect when in range of a Gallagher Bluetooth® wirelss technology enabled reader.
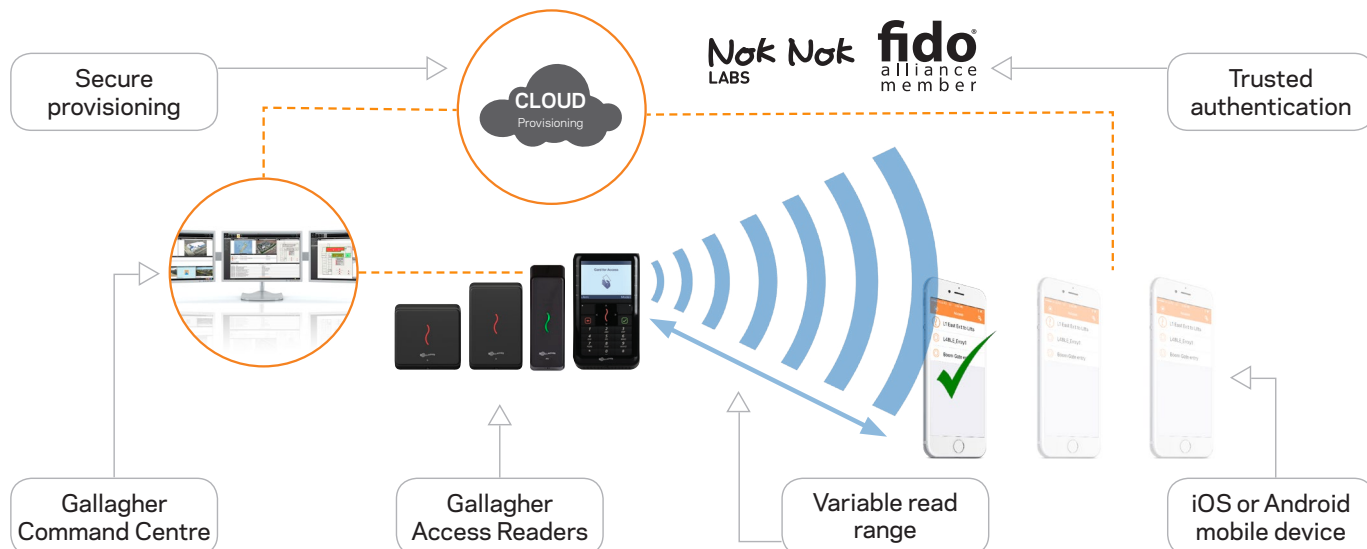
Secure Mobile Credentials

Using the FIDO Certified Nok Nok™ S3 Authentication Suite with the Gallagher platform ensures that user credentials are safe and secure using a globally recognized method of authentication.

Nok Nok LABS

fido® alliance member

GALLAGHER

System Architecture

*Requires Gallagher readers equipped with Bluetooth® wireless technology, Gallagher Command Centre v7.60+, and a suitable mobile device.
†To learn more about FIDO visit *www.fidoalliance.org*

Technical Specifications

Product numbers

Software

2A8570	Mobile Connect Credential (one per user)	2A8571	Mobile Connect Credential - SM Customers	FREE	Mobile Connect App

Readers

C300460	T20 Multi Tech Terminal, Black	C300481	T15 Multi Tech Terminal, White	C300430	T11 Multi Tech Reader, Black
C300461	T20 Multi Tech Terminal, White	C300440	T12 Multi Tech Reader, Black	C300431	T11 Multi Tech Reader, White
C300480	T15 Multi Tech Terminal, Black	C300441	T12 Multi Tech Reader, White		

Mobile Connect App

Product detail	Credential	Mobile Connect Credential (one credential required per user)
	Security	FIDO authentication, using pre-shared asymetric keys with elliptic curve cryptography (P256)
Minimum requirements	iOS:	9.0 and above
	iPhone:	5s and above
	Android:	5.0 and above
	Command Centre:	7.60 and above
	Access Hardware:	Gallagher multi-tech readers with Bluetooth® wireless technology
		Gallagher C6000 Controller
Additional notes		**Cloud provisioning subscription**

Once issued, credentials function indefinitely upon the devices they are sent to. An annual subscription allows for site managers to reissue credentials to users who may need to replace their phones*. Gallagher, in partnership with Nok Nok Labs will endeavour to maintain compatibility with new devices and their associated software updates as they are released.

* A fair use policy applies, allowing an average of four credential issuances per licensed credential. Please discuss additional options with your Gallagher Business Development Manager should you wish to exceed fair use guidelines.

3E4336 - 07/17

security.gallagher.com

GALLAGHER