How does ENGAGE technology manage electronic credentials?

ENGAGE technology can provide tenants the freedom and flexibility to use their building ID inside their office suite. Electronic credentials, which are easily issued on cards or smart phones, reduce the need for IT or building management service calls related to lockouts and re-keying. Access privileges can be quickly assigned and revoked electronically by an administrator, making them ideal for employees, contract workers, visitors, and service providers.

NDE Series wireless locks are compatible with most proximity and smart cards including aptiQ™ and aptiQmobile™.

Is there a limit to the number of openings I can deploy with ENGAGE technology?

ENGAGE cloud-based web and mobile apps can support up to 100 NDE wireless locks, allowing you to easily accommodate growth and expansion as needs change. For applications that exceed 100 openings, NDE Series wireless locks can be managed with software from one of our access control alliance partners. Consult your access control software provider for additional details regarding support and availability.

Can I use Schlage NDE Series wireless locks in my existing access control system?

Yes, NDE Series wireless locks will be supported by many of our access control alliance partners. Consult your access control software provider for additional details regarding support and availability.

Do I need Wi-Fi at each lock to use ENGAGE technology?

Schlage NDE Series wireless locks are Wi-Fi enabled but can be updated if Wi-Fi is not available at each lock. Changes to lock configuration and access privileges made through the cloud-based web and mobile apps can be sent to the lock anytime from the ENGAGE mobile app when in Bluetooth Low Energy (BLE) range.

How will ENGAGE technology impact my network?

If you have access to google.com from your location, no further firewall or network modification is required. The NDE Series locks will be dynamically assigned IP addresses on your network once commissioned with the ENGAGE mobile app. Worried about network traffic? Don't be. NDE Series wireless locks with ENGAGE technology provide you with the best of both worlds—an offline lock with the online features and control you expect. You determine how you want updates sent to the lock. Connect your locks to Wi-Fi for automatic daily updates directly from the cloud or send updates wirelessly while at the lock from the ENGAGE mobile application. The size of a full 5,000 user database door file with 2,000 audit events is smaller in size than an average email. NDE Series wireless locks with ENGAGE technology provide maximum capabilities with minimal network traffic.

What if my network goes down?

NDE Series wireless locks with ENGAGE technology allow you to leverage the convenience of once daily online updates without tying your physical security to your network up time. They operate as offline locks with access rights and audit events stored in the lock until it is time to communicate for daily updates.

Do I need a bridge or some other piece of equipment for this to work?

No. You need a Phillips head screwdriver and an ENGAGE mobile app compatible smart phone or tablet. If you want the convenience of automatic daily updates you will need a Wi-Fi internet connection at the lock.

Does my team need special training?

ENGAGE™ technology was designed to be simple and intuitive to use. If the members of your team can use a smart phone and a web browser, you can leverage ENGAGE™ technology in your business with minimal training. To get you started, a series of "How To" videos are available at www.AllegionEngage.com.

How do I get my team involved?

Anyone can be invited to assist with administration of your site through the web and mobile applications at one of three levels of authority:

Administrator: The site Administrator has full access to the database and lock configuration settings. The Administrator is able to add and remove users, connect to locks to send updates, retrieve and view lock audits, and initiate and view the results of the lock self-diagnostic test. The Administrator is able to delegate authority by inviting or removing other Administrators, Managers and Operators.

Manager: The Manager shares the same authority as the Administrator but is able to delegate authority by inviting or removing only Operators.

Operator: The Operator is the most limited role. The Operator is able to connect to locks to send updates, retrieve audits and initiate the self-diagnostic test. The operator cannot make modifications to the database.

What are the device, operating system and web browser requirements for ENGAGE technology?

The free ENGAGE mobile application is required to commission NDE Series wireless locks.

Download on the App Store

Mobile OS compatibility

- iOS 7.1 or later

Mobile device compatibility

- iPhone 4S and newer
- iPad 3rd generation and newer
- iPad Air 1st generation and newer
- iPad Mini 1st generation and newer
- iPod Touch 5th generation and newer

ANDROID APP ON Google play

COMING SOON

Mobile OS compatibility

- Andriod 4.4 (Kit Kat) or later

Mobile device compatibility

- HTC 1 M8 (recommended)
- Samsung S5 (recommended)
- Moto X (recommended)
- Nexus 7 (recommended)
- Nexus 4
- Nexus 6
- Nexus 9
- Galaxy Tab S
- Galaxy Tab 4
- LG G3

Browser compatibility

- Chrome 38.0 or later
- Internet Explorer 11.0 or later
- Firefox 33.0 or later
- Safari for Mac OS X 10 +

How secure is ENGAGE technology?

ENGAGE technology was designed from the ground up with security in mind. ENGAGE technology leverages industry leading security practices and encryption to provide our customers with a secure, dependable experience. Hosted in state-of-the-art redundant data centers across the globe, our cloud solutions provide IT professionals with the confidence they need to support their business 24/7.

Application and infrastructure hosting: ENGAGE technology is built and hosted on the Microsoft Azure cloud platform. Azure provides a secure, state-of-the-art, high availability, fault tolerant solution to our customers world-wide.

Encryption keys and security standards: By design, ENGAGE is the core element of the product security plan. It creates and manages the encryption keys for the system, records the commissioning device of each lock, and is the interface to any 3rd party systems. It is able to register devices and locks, and can provide OEM license management for partners.

Mobile devices are used to configure and manage the lock. They are widely available and not proprietary. Carefully planned measures have been taken to safe guard the system against a hacked mobile device. The mobile device is required to 'check in' with ENGAGE daily to receive updated encryption keys. This mandatory 'check in' is used to eliminate the use of static encryption keys between the ENGAGE mobile application and the lock and provides an added layer of security. The mobile device never receives any keys that are used to communicate between the ENGAGE web services and the lock. This ensures that all communications between the ENGAGE web services and the lock are secure.

CLOUD-BASED BLE encryption: All Bluetooth Low Energy (BLE) communications are encrypted using AES 256 bit encryption. This is executed by temporary key given to the lock by the ENGAGE™ web services.

TLS encryption: The ENGAGE web services secure communications to the ENGAGE mobile application and OEM Partner systems using TLS 1.0. The ENGAGE web services leverage a server certificate from 3rd party authority. The lock downloads and stores the associated CA certificate. The lock will then perform server authentication only via a USER ID & PASSWORD combination.

Wi-Fi encryption: The Schlage NDE Series wireless locks with ENGAGE technology support WEP, WPA/WPA2-Personal and WPA2-Enterprise (PEAP) wireless security protocols to encrypt the Wi-Fi communications between the lock and wireless router.

We have created two videos that provide more detail about cloud-based security:

WATCH NOW

What Makes Cloud-based Products Secure: Certificates

This video explains how digital certificates provide protection against spoofing attacks.

WATCH NOW

What Makes Cloud-based Products Secure: Encryption

What makes cloud-based products secure? Learn how encryption defends against sniffing attacks.