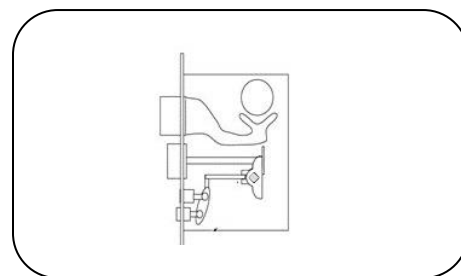
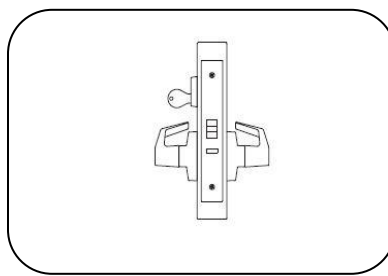
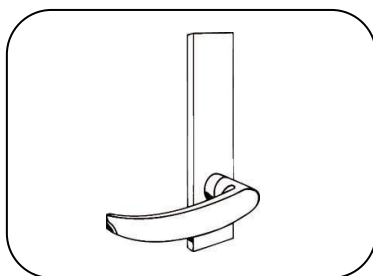


LEAPIN Digital Keys Ltd



NB IoT Smart Access Control Systems



LDK400 Manual



© 2019 LEAPIN Digital Keys Ltd.

The information contained in this document produced by LEAPIN Digital Keys Ltd is solely for the addressee for the purposes for which it has been prepared. LEAPIN Pty Ltd undertakes no duty or accepts any responsibility to any third party who may rely on this document. All rights reserved. No sections or elements of this document may be removed from this document, reproduced, electronically stored or transmitted in any form without the prior written permission of LEAPIN Digital Keys Ltd.

About This Manual

Copyright 2018 by LEAPIN Digital Keys Pty Ltd.
2/11 York Street, Sydney, Australia 2000
Telephone: + +44 1706 577 991
<https://www.digitalkeys.io/>

Edition: 20191303

Version: 1.0

Document number: **LDK400_1.0.DOCX**

This issue replaces all previous issues. All previous issues are invalid. The information in this manual can be changed without prior notice.

Passing on or copying this document, using and providing information on its contents is prohibited unless expressly permitted. Infringements shall be subject to compensation claims. All rights reserved in the case of patent award or listing of a registered design.

The arrangement of information for this document is to the best of our knowledge and belief. LEAPIN Digital Keys assumes no guarantee for the accuracy or completeness of the contents of this document. In particular, LEAPIN Digital Keys cannot be made liable for consequential damages which are due to erroneous or incomplete information. As mistakes can be made despite our best possible efforts, we would be very thankful for any corrections which you may find necessary.

Safety and warning instructions

- This manual outlines the commissioning, installation and operation of a NB IoT Smart access control solution LDK400 model.
- This equipment may only be used for the purpose specified by the manufacturer.
- This manual should be kept accessible.
- Illegal changes and the use of spare parts as well as accessories that have not been sold or recommended by the manufacturer of this unit can cause fires, electric shocks and injuries. Such measures lead to an exclusion of liability, and the manufacturer accepts no responsibility.
- Repairs may only be carried out by the manufacturer or accredited distributor/re-seller.
- Basis for the guarantee of the manufacturer is the version of the warranty policy for the unit at the time of purchase. No liability is accepted for inappropriate, incorrect manual or automatic setting of the parameters for the device, or its improper use.
- The distributor/re-seller in conjunction with the lock purchaser (if required), is responsible for ensuring that the device is assembled and mounted according to the recognised technical guidelines as well as other valid regulations in the country of use

Contents

Introduction	5
The technology	5
Operation.....	5
Deadbolt security	5
Flexibility.....	5
The system concept.....	6
The security concept	6
Parts Overview.....	7
Instructions on installation.....	9
Mounting	10
General information.....	12
Capacitive wake-up button	12
Programming	12
Operator guidance	13
LED light display	13
Information on unlocking.....	13
Time Zones.....	13
NFC Tokens/cards.....	13
Battery replacement	13
Battery Notifications/monitoring.....	14
Care and maintenance	14
Metal Key override.....	14
Technical Data	15
PART 2 - DIGITAL KEYS MANAGEMENT SOFTWARE USER GUIDE.....	17
LOGGING INTO THE DIGITAL KEYS MANAGEMENT SOFTWARE	17
HOME PAGE.....	17
CREATE NEW USERS	17
Create New User (Individual).....	19

CREATE NEW DIGITAL KEYS..... 20

UNLOCK ANY DOOR..... 23

DELETE DIGITAL KEY 25

VIEW LOCK EVENTS/LIVE AUDIT 26

LOCK STATUS REPORT 27

PART 3 - DIGITAL KEYS MANAGEMENT APPS USER GUIDE..... 30

 DOWNLOAD AND LOG IN 30

 USING YOUR DIGITAL KEYS TO UNLOCK OVER NB IOT NETWORK 31

 REQUEST DIGITAL KEYS 33

 MAKE NFC CARDS/TOKENS 36

Introduction

This manual outlines the functions of the NB IoT Smart access LDK400 door locking systems, how to install and use the product.

The technology

The NB IoT Smart access LDK400 door locking system is mounted on the door leaf like a book binding, and screwed together for any doors with thickness 32-55mm.

The NB IoT Smart access LDK400 door locking system is operated completely independent of any external cable connections (product is battery powered with 4 standard AA batteries) and can be installed and operated on the majority of commercially available doors.

The operation of the NB IoT Smart access LDK400 door locking system occurs via NB IoT technology, combined with NFC technology, and with cloud-based software and smartphone apps.

In order to unlock the lock, any smartphone which can connect to the internet, which has also been authorized, can be used. Smartphones which have NFC inbuilt (most Android phones) which have also been authorized, can be held in front of the lock to gain access (within 2-4 centimeters) from black cover with NB IoT logo stamp. NFC tokens/keycards, which have been authorised can also be used for unlocking. With these authorized devices/tokens, a mechanical coupling is activated for a few seconds that allows the LDK400 to be opened and closed using the door handle.

Operation

After the NB IoT Smart access LDK400 door locking system has recognised a valid digital key, a mechanical coupling is produced for several seconds between the door locking system and the mortise lock. The mortise lock can be closed in the same way as mortise locks with profile cylinders. The door locks when it is closed. Operation is single-handed.

Deadbolt security

The NB IoT Smart access LDK400 door locking system the door can be 'deadbolt' locked and is not just left on the latch. To unlock the door, the bolt and latch are operated via the NB IoT Smart access LDK400 door locking system turn knob to release the door. The deadbolt can also be turned for use from the inside of the door.

Flexibility

The NB IoT Smart access LDK400 door locking system is an autonomous door locking system that can manage an unlimited number of users, on any time-limitable digital keys, and an unlimited number of locks per account. With this, individual time-limited access rights can be assigned to every user. The fact that every digital key can be authorised for every lock, means a high degree of flexibility is reached. Various access profiles can be set within the locking system.

If a digital key on a NFC card/token or smartphone is lost, the digital key can be deleted, and replaced with another digital key, without making it necessary to physically attend to the NB IoT Smart access LDK400 door locking system.

The system concept

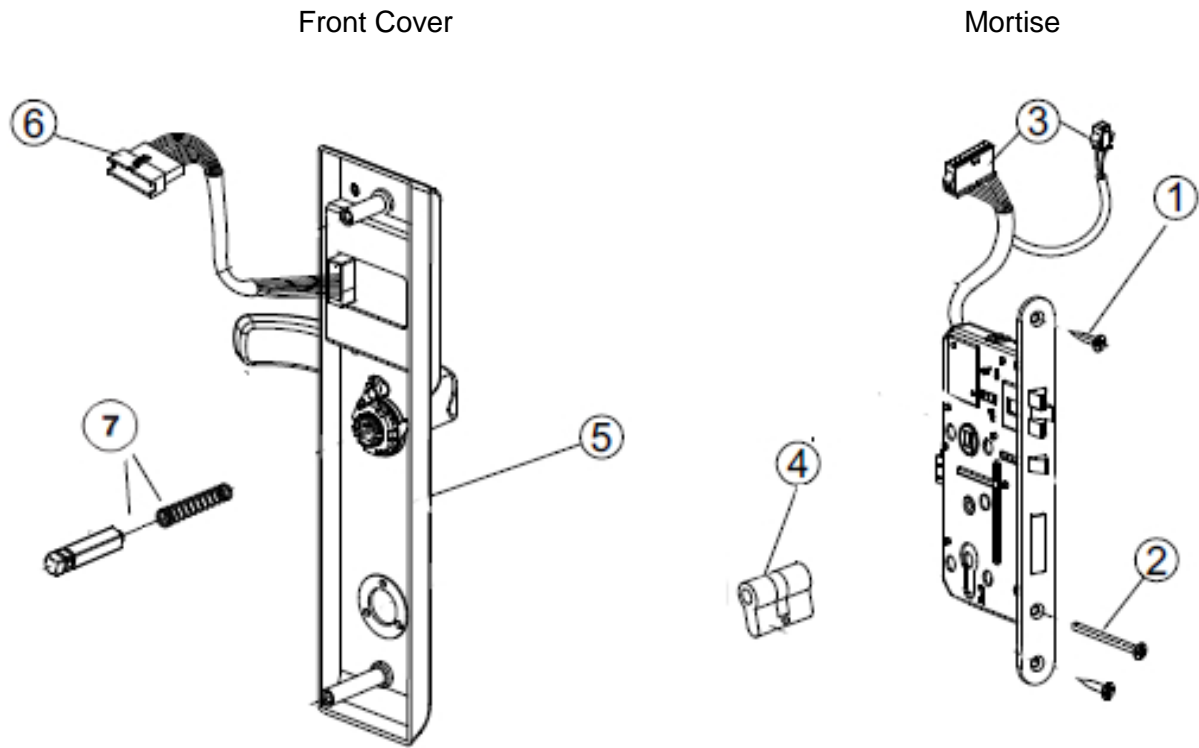
The NB IoT Smart access LDK400 door locking system is complemented by;
Digital Keys Management Cloud Based Software
Digital Keys Apps (Android and iOS available for unlimited downloads from online app stores)
Digital Keys NFC keycards and tokens (2 cards provided). Please check with your local distributor to purchase more.

The security concept

NB IoT is part of the mobile network, fully managed with standardized security to guarantee the credential and integrity of all data running through it. NB IoT has passed security protocols as outlined by 3GPP, the organisation responsible for managing the mobile network.

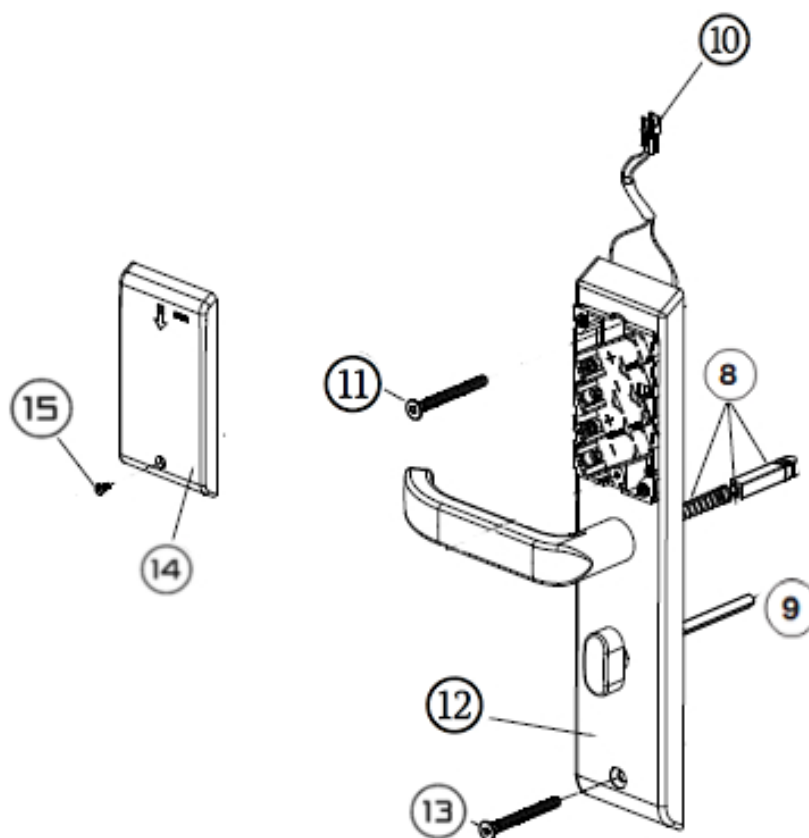
The NB IoT module chipset included in our NB IoT smart locks applies 2048 bit RSA encryption. All communications are running on HTTPS 128 bit military grade encryption between all the vertical applications including software and hardware. Between the telco's mobile network, and the IoT device management platform a layer of Internet Protocol Security (IPSEC) is provided. The Telecommunication company on some occasions, also provides a dedicated VPN for further security and reliability.

Parts Overview



1. Screws for mounting mortise to inside of door
2. Screw for securing metal key cylinder in place
3. Power cord connector for connecting to battery pack (smaller connector) and cord for connecting to PCB which is housed inside the lock covers black box (larger connector)
4. Metal Key cylinder (for metal key emergency override)
5. Front cover case
6. PCB connection cord for connecting to mortise
7. Square Spindle with spring

Back Cover



8. Square spindle and spring

9. Deadbolt Spindle

10. Battery connector cord (plugs into mortise cord connector)

11. Top screw for attaching lock to door (keep screwing until lock sits flush with door)
can work with thicknesses from 32mm-55mm

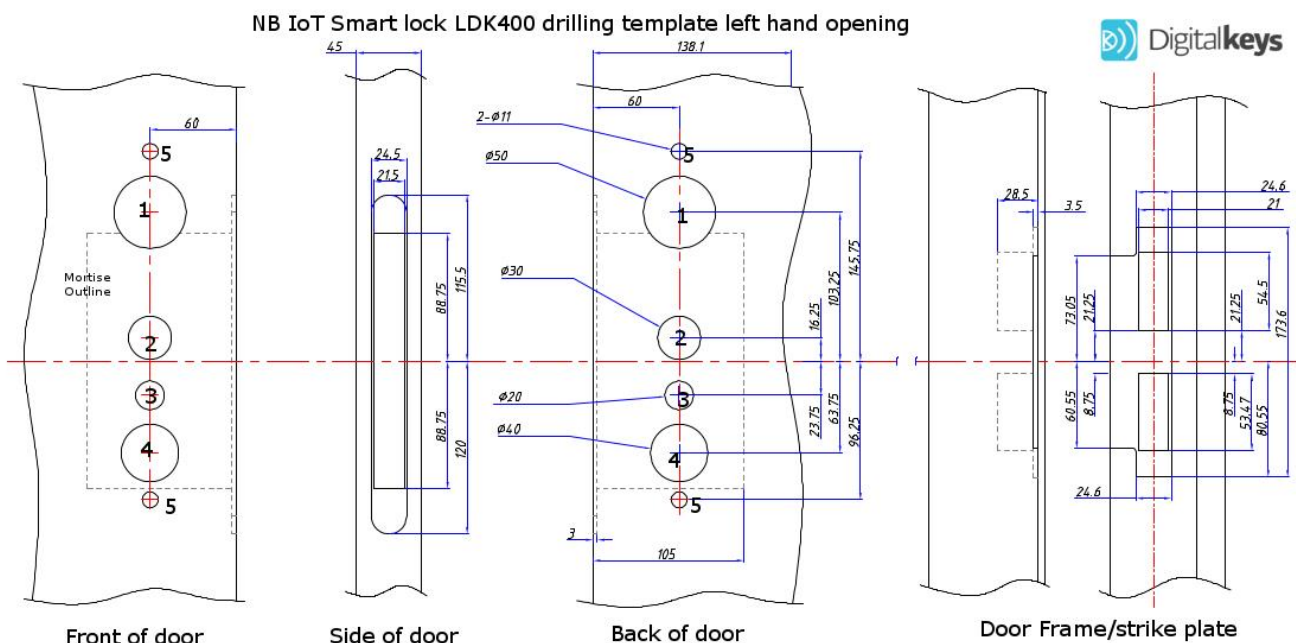
12. Lock casing

13. Bottom screw for attaching lock to door

14. Battery cover

15. Battery cover screw (black 3mm)

Instructions on installation

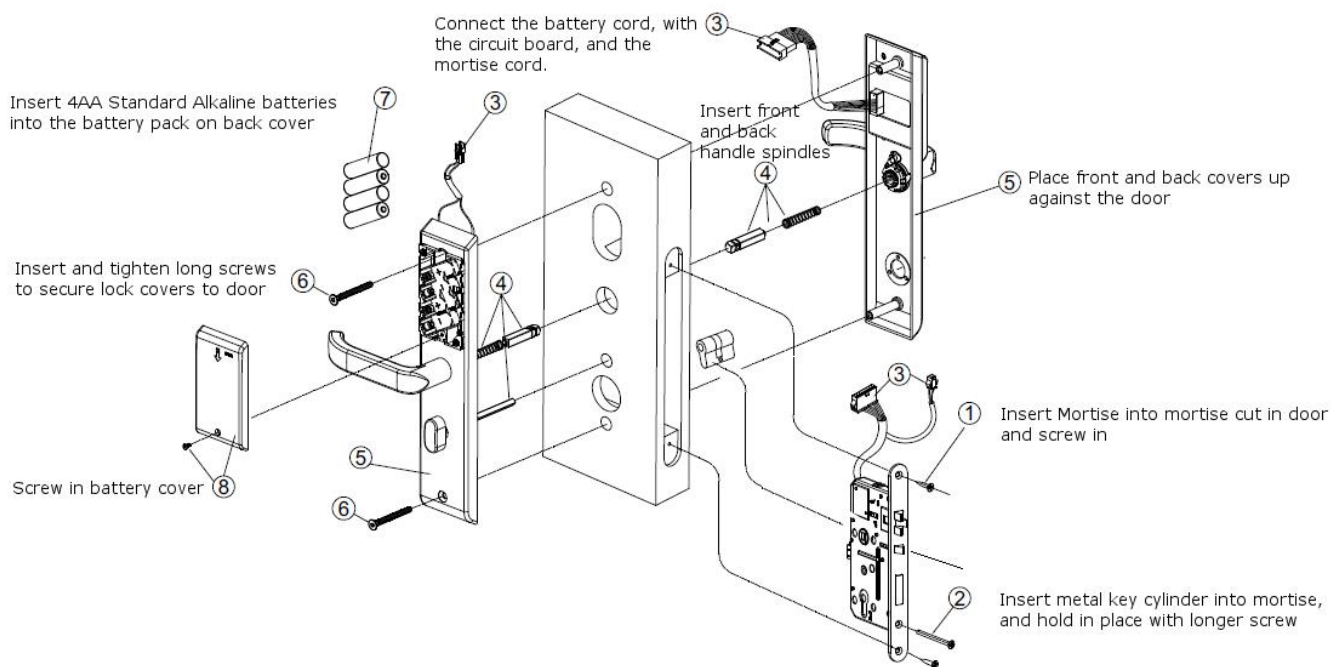


As per the diagram above, the following bore holes should be present in the door:

1. A bore hole with a dimension of 50mm (for cords to pass through)
2. A hole for the handle spindles with a dimension of 30mm
3. A hole for the deadbolt spindle 20mm
4. A hole for the metal key cylinder 40 mm
5. Punch holes for holding lock to door with a dimension of 11mm

NOTES: Holes can be drilled with the aid of a drilling template (pdf template can be found at digitalkeys.io). Metal drilling template can be ordered. Locks with left hand and right hand opening are available. Please advise your local distributor/re-seller about which type you require at time of purchase order.

Mounting



1. Insert the mortise into the cut in the door, and screw in with small mortise screws. **IMPORTANT;** Please make sure a small dot is at the top of the square whole in the mortise for the handle before installing. If this dot is at the side or bottom of the lock, the lock will not lock (see images on next page - page 10)
2. Screw in metal key cylinder with long screw (cylinder should already be placed inside the mortise, if not insert into the hole) metal key cylinder can be replaced with a cylinder of choice.
3. Thread the battery, PCB, and mortise connector cords together through large hole in door, and join cords together
4. Insert front and back spindle's and springs into mortise and push into back of handle holes, and insert deadbolt long spindle into spindle hole and mortise
5. Push front and back covers up against the door, until it sits flush with the door (make sure all the spindles sit in place)
6. Screw top and bottom screws together until the lock sits flush against the door
7. Insert batteries
8. Insert small black screw (use check/allen key to tighten - not provided)

NOTES: a nano SIM should already be fitted into the PCB (if not please get in touch with your local distributor or send an email to info@digitalkeys.co).

Door handle direction (left or right) needs to be requested from distributor when an order is placed (can work for left or right hand swinging doors, but distributor needs to be notified first)



LEFT: Correct positioning of handle spindle hole, before inserting spindle
RIGHT: Incorrect positioning of handle spindle hole.

General information

Capacitive wake-up button

The NB IoT smart lock LDK400 uses a capacitive wake-up button which must be pressed to unlock the lock. The wake-up button wakes the lock up and prepares it to receive unlock commands over the NB IoT network, from smartphone unlocking, and from digital keys management software unlocking. The wake-up button exists to conserve battery energy so the lock is not always on, waiting to receive commands. The capacitive wake-up button is located on the NB IoT logo - see below where green arrow is pointing (the button is the entire area inside the rectangle, and not the words, 'NB IoT'). The capacitive wake-up button does not need to be pressed for NFC phone unlocking and NFC card unlocking.



Programming

The programming for the NB IoT smart lock, can be carried out with the Digital Keys Management Software, and the Digital Keys apps (Digital Keys apps are FREE to download from the online app stores Android and iOS). The programming is described in part 2 and part 3 of this manual. When using NFC phones and NFC tokens/cards, programming of the lock is carried out over the NB IoT network on the first time the phone or token/card is presented to the door for unlocking. For all future unlocks with NFC, this will be done locally, and commands do not need to be sent over the NB IoT network everytime. When NFC is used to unlock, the NB IoT is still used for live audits, live battery status, and live notifications.

Operator guidance

Operation is supported by the blue LED display, as well as by acoustic signals - a buzz sound occurs when the lock has successfully received its command, and the lever handle can then be pulled down to unlock the door.

LED light display

The NB IoT smart lock LDK400 has a blue LED light built in.

There are only 2 different status offered by the LED lights as follow;

1. Flashing blue - lock is awake (after wake-up button is pressed or new batteries inserted) and is connecting to the network (new batteries) or awaiting a command such as an unlock command.
2. Solid blue light - lock has successfully received an authorized unlock command, and is now unlocked, so you can pull handle down to unlock.

Information on unlocking

To unlock the lock, please follow the instructions below;

1. Hit unlock button on the app (follow instructions on the app, which says that the unlock command has been sent, and you should touch NB IoT logo to wake up the lock to unlock it).
2. Touch NB IoT logo to wake-up lock.
2. Blue light flashes whilst unlock command is finalized
3. A buzz noise occurs, blue lights stop flashing and stays on.
4. Pull handle down to unlock.

There is a pause of a few seconds between pressing the wake-up button and the lock making the buzz noise/flashing blue light indicating the handle is ready to be pulled down and lock opened.

When unlocking with NFC (NFC phones and tokens) there should not be any delay in the lock being ready to be opened by pulling the handle down. NFC phones and tokens must be held within 4 centimeters from the NB IoT logo.

Time Zones

The NB IoT smart locks use local internet time, which can be set when the locks are first set-up and commissioned by local distributors. Locks can be programmed to work for a minimal 30 minute timeslot. When the programmed time for the digital keys expires, the unlock icon will disappear from the digital keys app.

NFC Tokens/cards

The NB IoT smart locks only work with special Digital Keys NFC cards/tokens. The product will not work with any NFC cards bought online from third parties, or from non-certified NB IoT smart lock re-sellers. 2 NFC tokens are provided in every pack. Please contact Digital Keys or your local distributor/re-seller if you require more keycards/tokens.

Battery replacement

1. Loosen the small screw on the bottom of the black cover on the back of the lock, with a chuck/allen key

2. Open the battery compartment and remove the batteries.
3. Place new 4 standard AA batteries correctly into the compartment - any standard AA batteries (alkaline) can be used.
4. Close the battery compartment and screw shut again.

Note: No digital keys are deleted during the battery changeover.

Battery Notifications/monitoring

A live battery status is shown in the digital keys management software (please see section 2 User guide for more information). Account administrators can set up email notifications for when battery status gets below 10%.

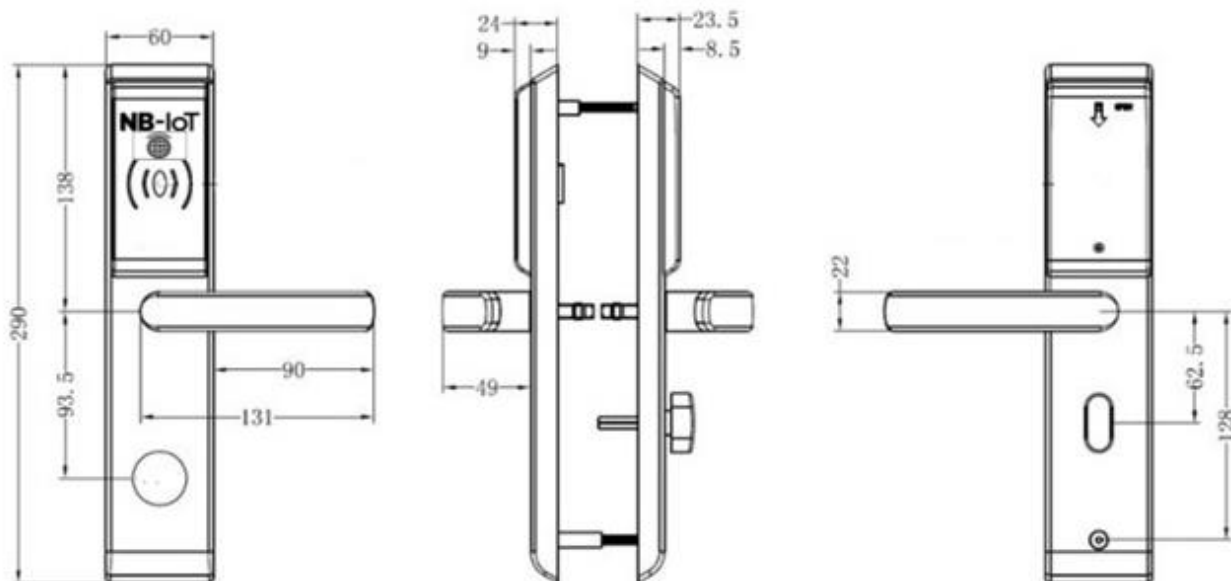
Care and maintenance

The NB IoT smart locks LDK400 are maintenance-free. At no time may they be oiled or greased with lubricants containing mineral oil. Cleaning may only be carried out with non-stick, residue-free cleaning and disinfection agents. No abrasive cleaning agents, or acids may be used for care and maintenance. Equally, pressure washers may not be used. Although the LDK400 is weatherproof we don't suggest the use of a high pressure hose to spray product, as it can lead to damage and liability exclusion.

Metal Key override

Each lock is delivered with a standard mortise lock cylinder (EU/AU) and other countries compatible. The cylinder can be replaced with most other cylinders. We recommend the use of metal keys in the case of emergencies. Use of metal keys will not show up in the lock events audit trail.

Technical Data



Display elements:

Acoustic signal:

Battery:

Battery life:

1 x LED blue

Signal transmitter

4AA standard alkaline batteries

approx. 2 years or approx. 20.000 operations

Temperature range;	-50 to 60°C
Relative humidity:	20 to 95% RH
External Panel dimensions:	L95mm x W62mm x H26.8mm
Surface housing including handles:	Stainless steel
Door thickness:	32 to 55mm, further door thicknesses optional (please check with distributor/re-seller for longer screws for larger thickness
NB IoT Module:	Quectel BC28 NB IoT module Band 5 Asia, Band 20 EU, B1, B3, B8, B28
SIM card	NB IoT nano SIM (global roaming or local)

PART 2 - DIGITAL KEYS MANAGEMENT SOFTWARE USER GUIDE

LOGGING INTO THE DIGITAL KEYS MANAGEMENT SOFTWARE

Please advise with LEAPIN Digital Keys, or your local distributor/re-seller who the account administrator will be for the digital keys management software (provide email, name etc). When the software account is first set up, the nominated account administrator, will receive an email from info@digitalkeys.co, inviting them to set up their username and password to access their account as administrator. An account administrator can also choose to create new users and user types for the digital keys management software at anytime. Whenever a new user is created in the system to use the digital keys management software they will receive an email from info@digitalkeys.co inviting them to set up a username and password.

NOTE: Please check all inboxes including SPAM for the email invite from info@digitalkeys.co

Click “EU Sign in” button at top of digital keys home page and enter your username and password to access the software (EU users) or click “ASEAN log in” for users in Asia/Pacific region.

HOME PAGE

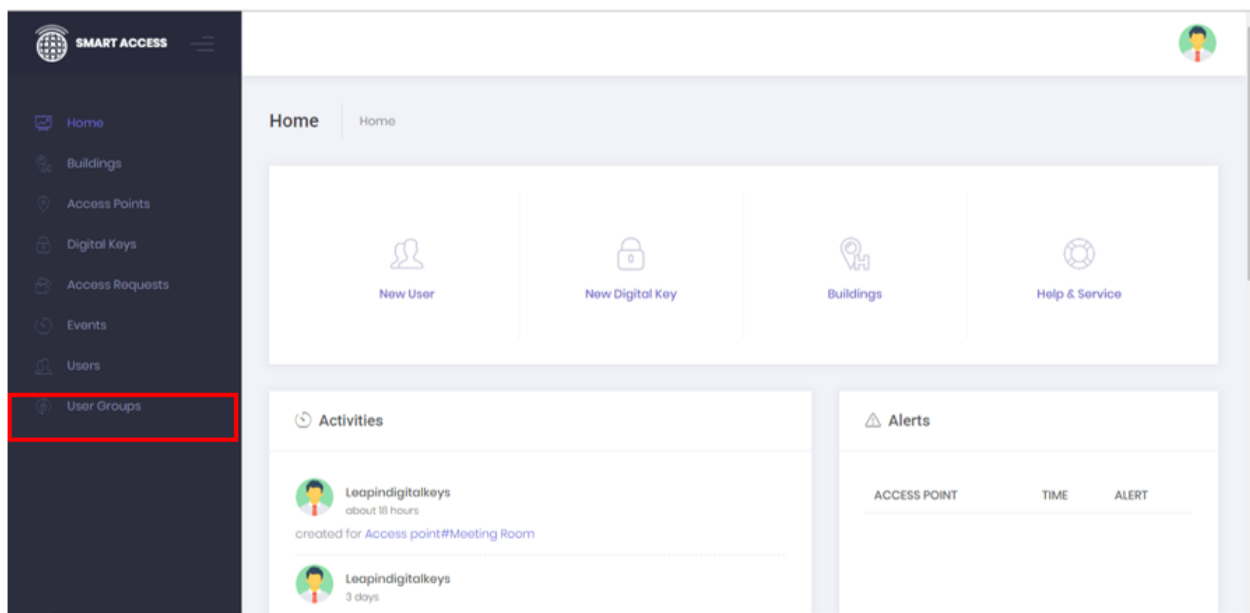
The Home page provides shortcuts to the features of the Digital Keys Management Software and also displays live notifications of all activities of the account holders locking system, including new keys being generated, locks being unlocked, and digital keys being deleted. Live 'Alerts' are also featured on the home page for any locks in the account system, such as when the battery status gets below 10%. Notifications of alerts can also be sent to account manager phone or a selected users phone.

CREATE NEW USERS

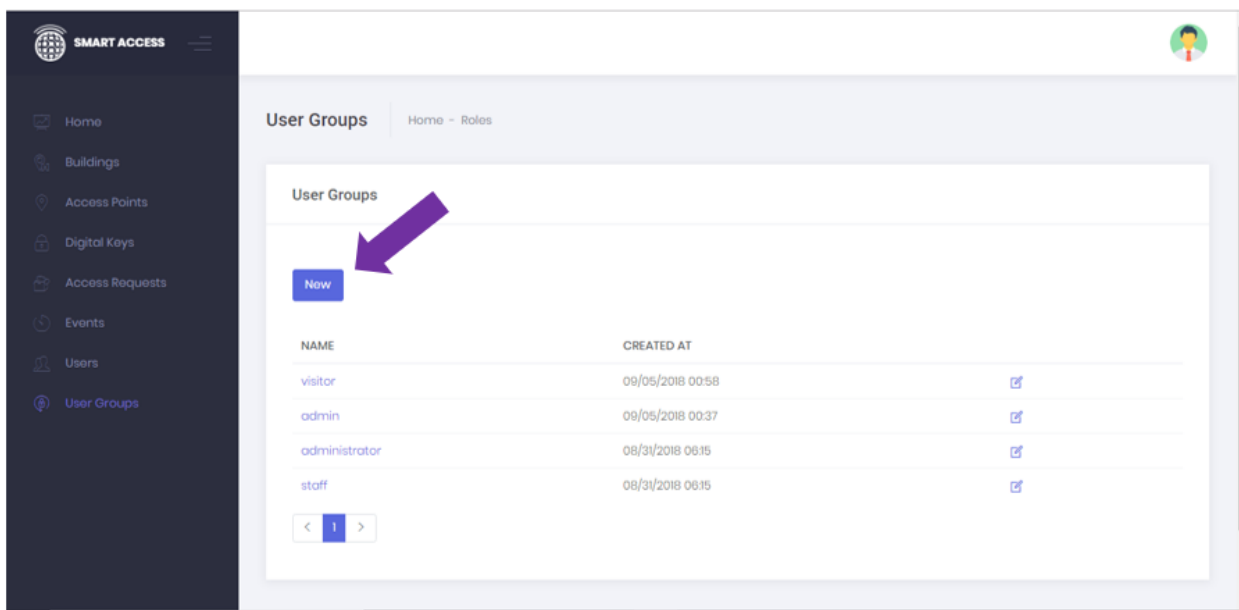
The Create Users feature enables the account administrator to add permanent or semi-permanent users, in addition to being able to great 'user groups' such as visitors or contractors. When using the user groups this only has to be done once, and then digital keys can be created for these user group types, without having to go through the process of entering all the users details each time.

Create New User Group

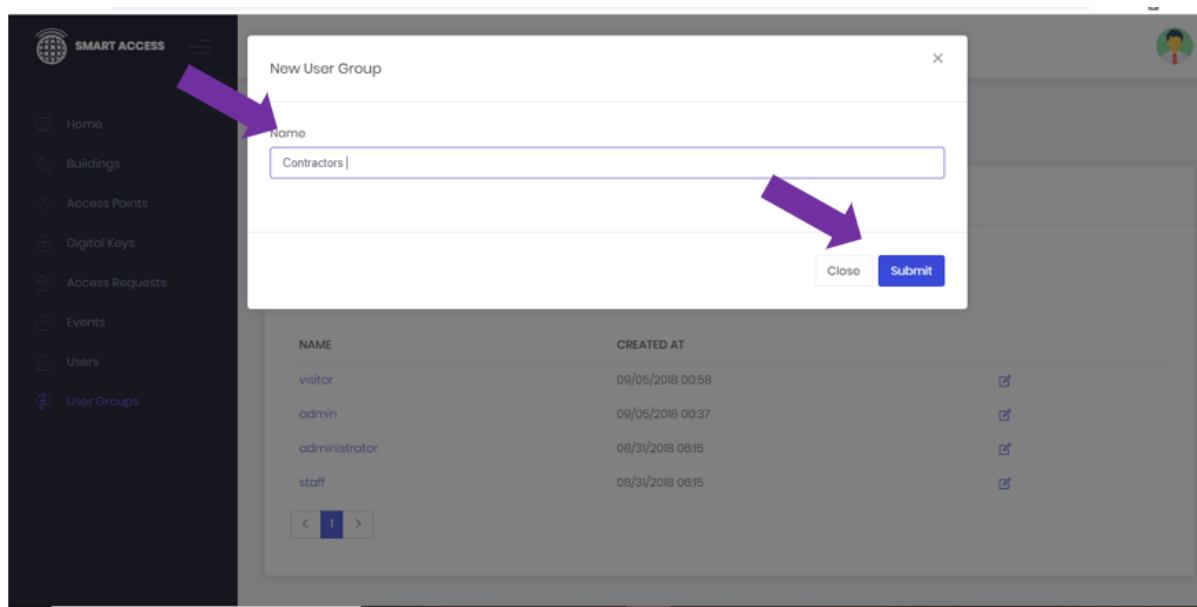
1. Create new 'User Group' by selecting User Groups on left hand side menu



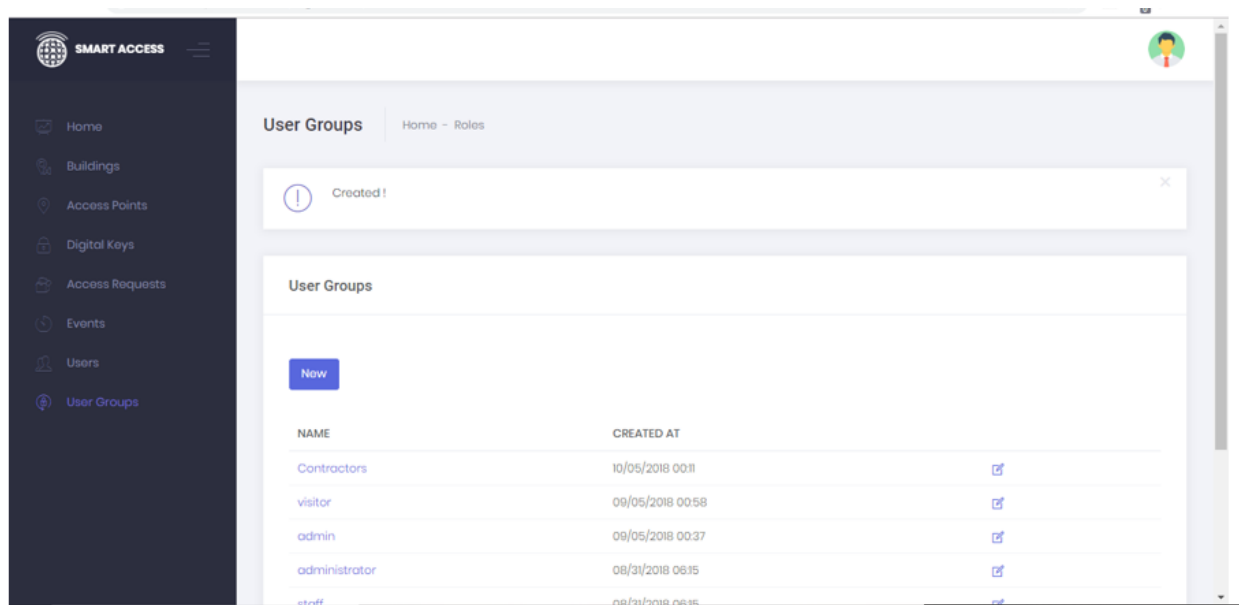
2. Select 'New' button



3. Enter the name of the new user group in the box e.g 'contractors', or 'visitor' and click submit.

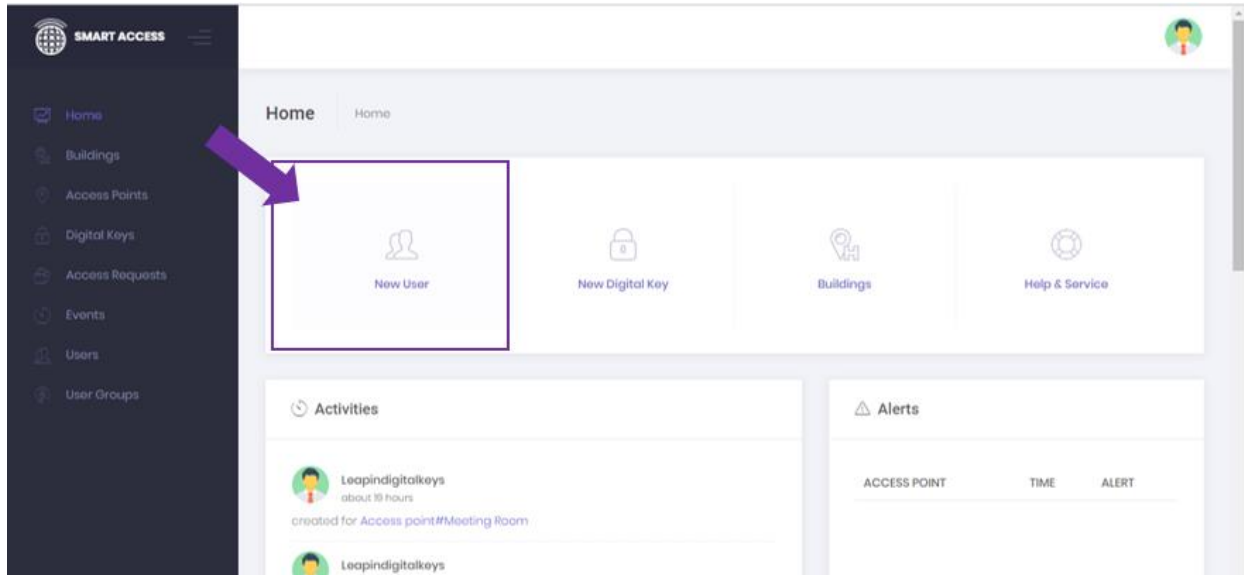


4. A 'created' confirmation message is returned, and you can see the new user group you named in the table.

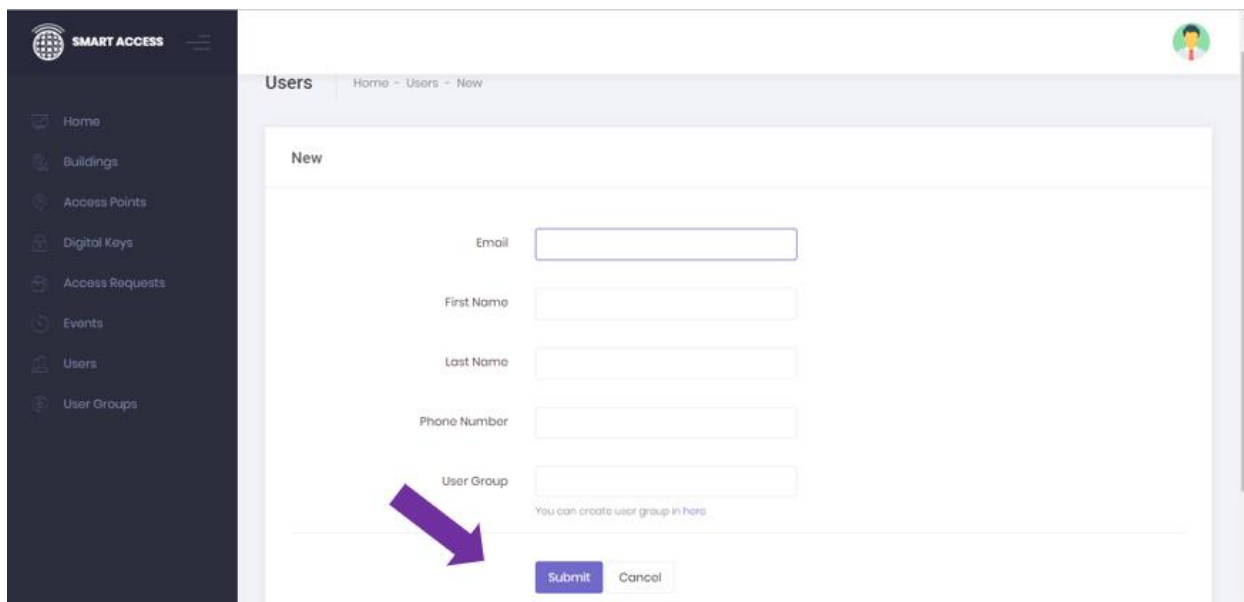


Create New User (Individual)

1. Select 'New User' from the box on the home page.



2. Enter the users details into the form, and click 'Submit' button when finished.

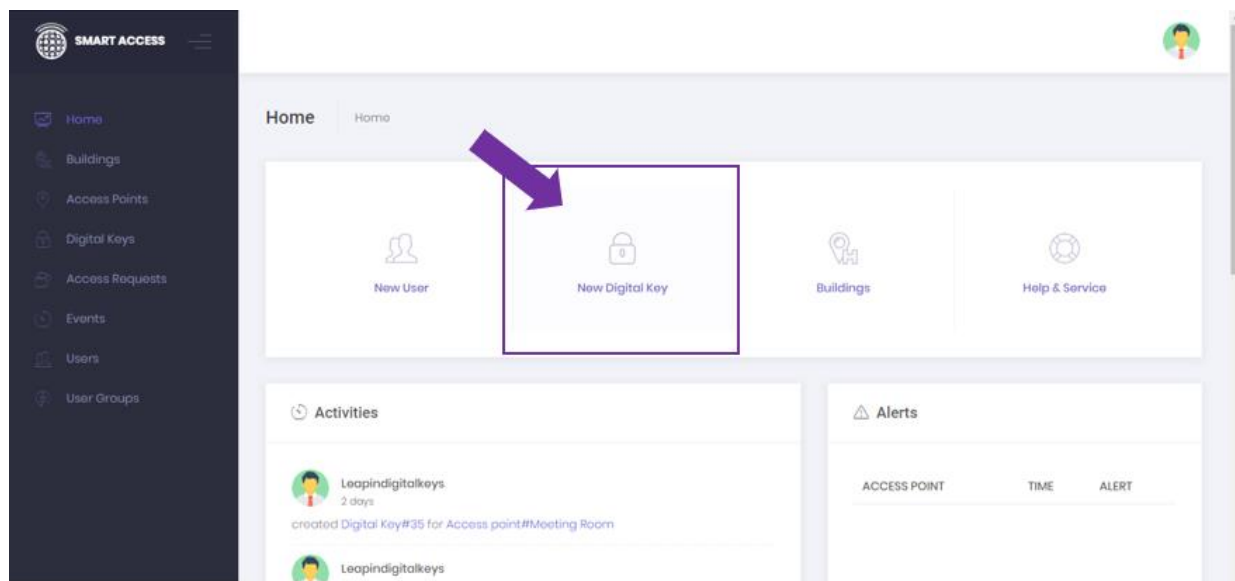


3. A 'created' confirmation message is returned, and the user is listed now in the users table. The users name, or user group can now be selected when generating a time-sensitive digital key as outlined in the next section.

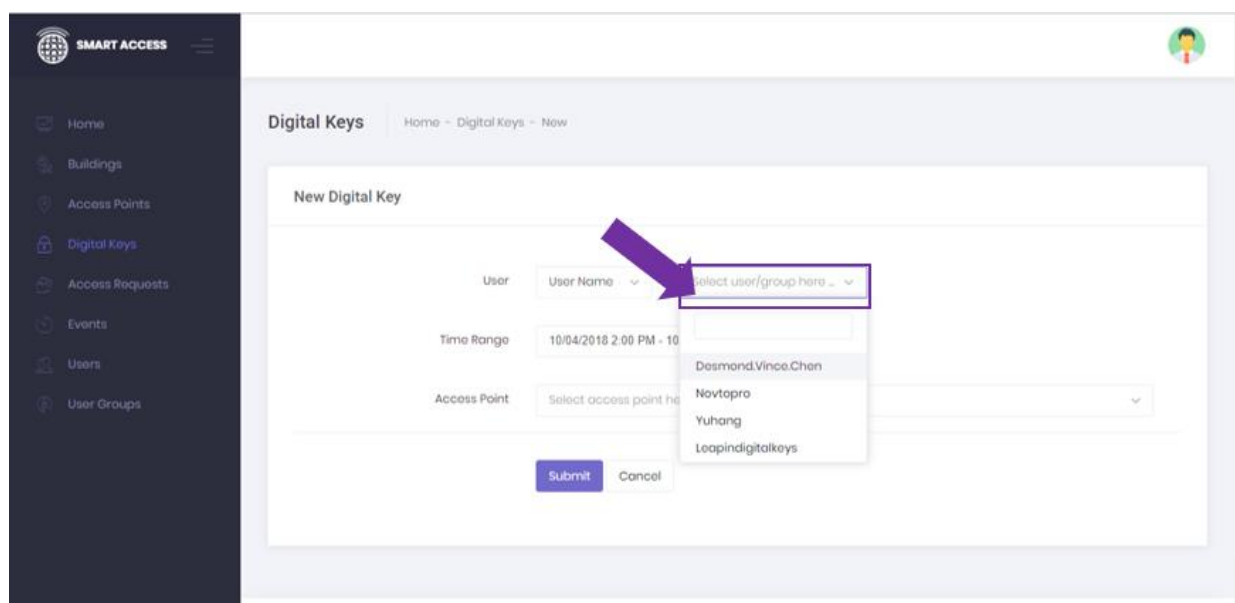
CREATE NEW DIGITAL KEYS

Account Managers can create time-sensitive Digital Keys for anyone, anywhere at anytime from within the Digital Keys Management Software, as outlined below.

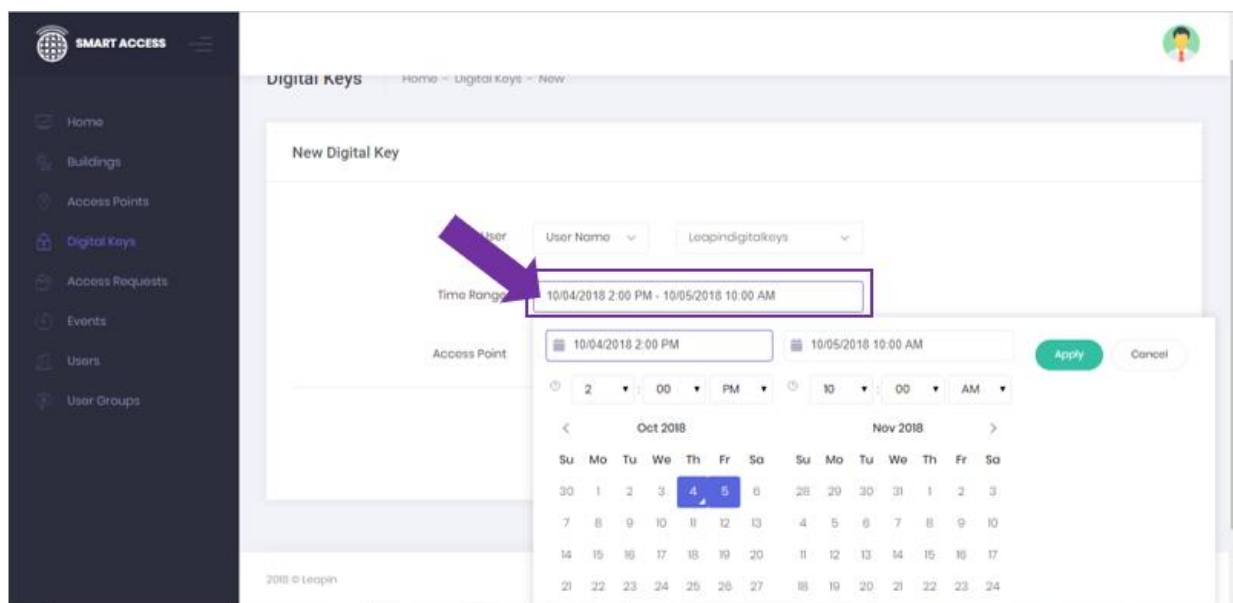
1. Click on the 'New Digital Key' box on the homepage



2. Select user name or user group from drop down menu.



3. Select the date and time you want the digital key to work for.



SMART ACCESS

Digital Keys Home - Digital Keys - New

New Digital Key

User User Name Leapindigitalkeys

Time Range 10/04/2018 2:00 PM - 10/05/2018 10:00 AM

Access Point 10/04/2018 2:00 PM 10/05/2018 10:00 AM Apply Cancel

2 00 PM 10 00 AM

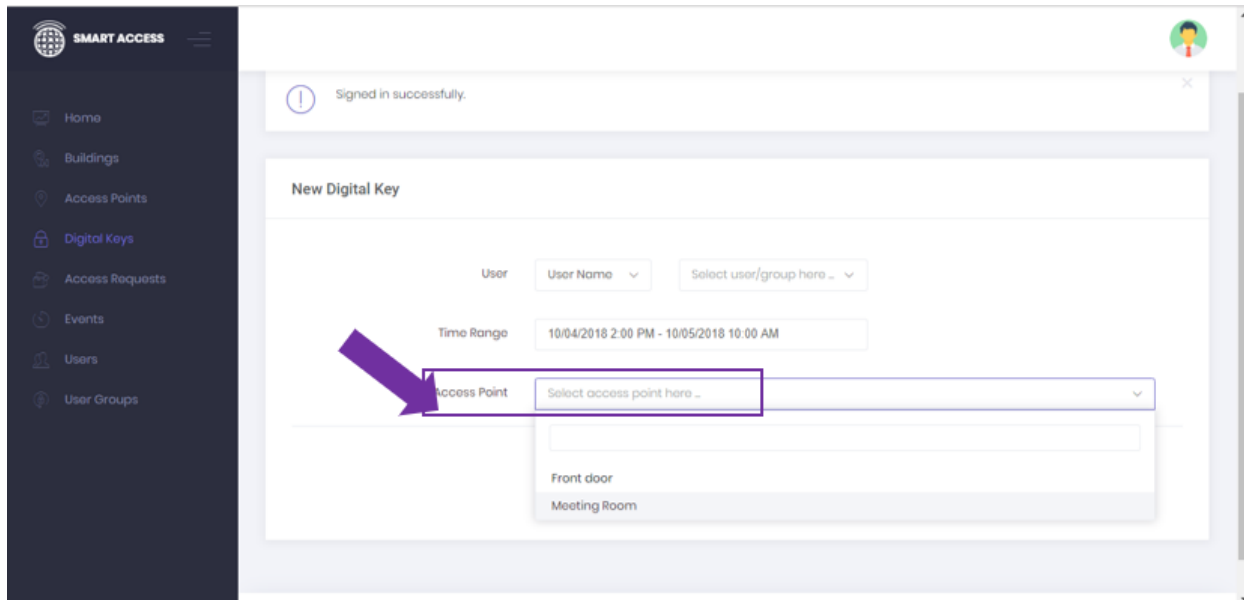
Oct 2018 Nov 2018

Su	Mo	Tu	We	Th	Fr	Sa
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

2018 © Leapin

NOTE - The Digital Keys are pre-set with default times to work from 2pm on the first date of choice, to 10am on the final date of choice. You can easily change these times by selecting in the time box.

4. Select the access point (that is room/lock) for where you want to make the digital key work for from the drop-down menu as shown below.



SMART ACCESS

Signed in successfully.

New Digital Key

User User Name Select user/group here ..

Time Range 10/04/2018 2:00 PM - 10/05/2018 10:00 AM

Access Point Select access point here ..

Front door

Meeting Room

5. Click the submit button

Signed in successfully.

New Digital Key

User:

Time Range:

Access Point:

6. A message will appear on the next screen that says created, and the digital keys will appear in the 'created digital keys table' (this is a list of all digital keys that have been created/in use) - if the dates for the digital key created is current, the digital key will display as “ACTIVE”. The user will then receive their digital key immediately on the digital keys app in the form of an unlock button in a tab with the access point selected. If a digital key has been created for a time in the future, it will display in the list of digital keys as “UPCOMING”. Digital Keys that have expired are displayed in the table as “INACTIVE”

Created !

Digital Keys

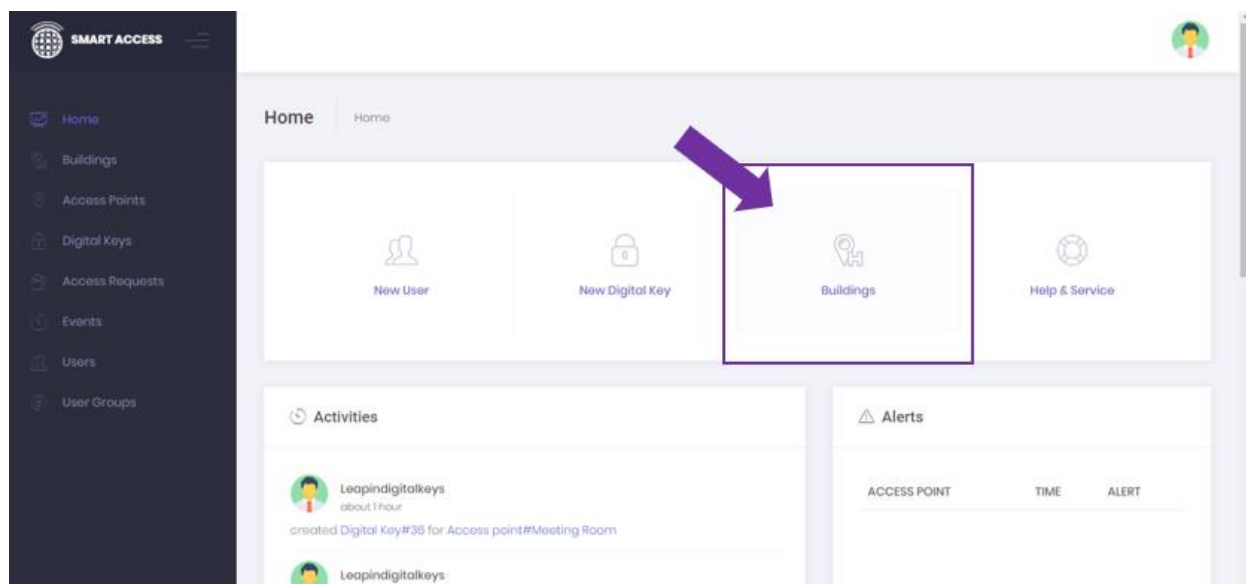
Search...

OWNER TYPE	OWNER NAME	STATUS	ACCESS POINT	DATE RANGE	CREATED AT
User	Leapindigitalkeys	INACTIVE	Meeting Room	10/04/2018 - 10/05/2018	10/04/2018 05:34
User Group	visitor	ACTIVE	Meeting Room	10/01/2018 - 10/11/2018	10/02/2018 08:01
User	Novtopro	INACTIVE	Front door	10/06/2018 - 10/13/2018	10/02/2018 07:52

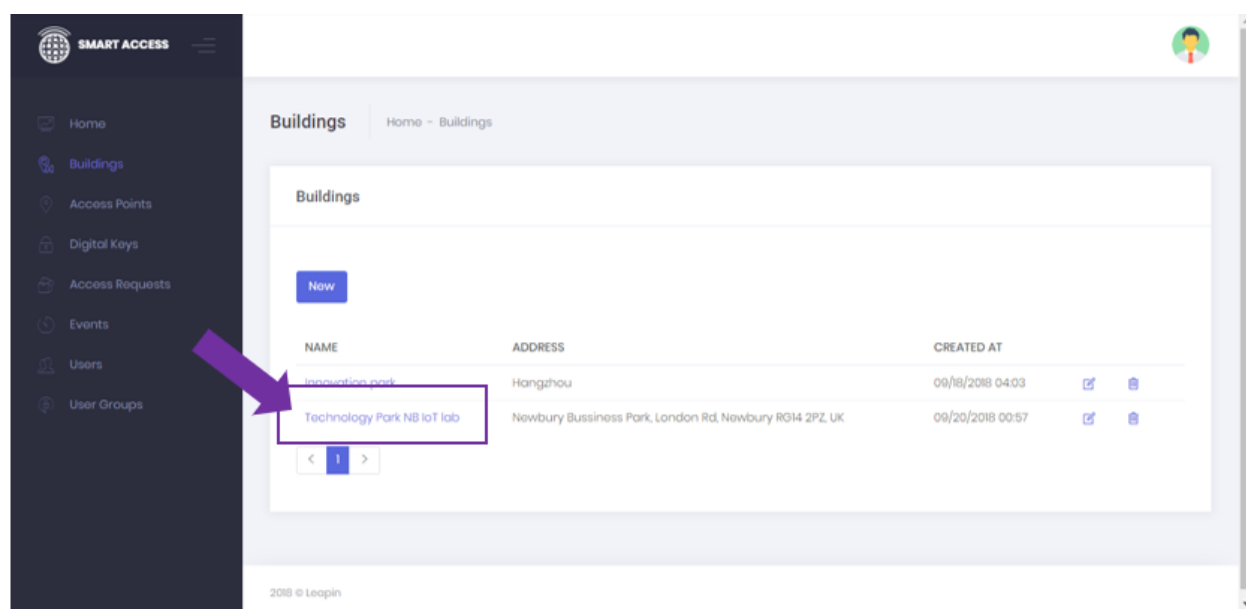
UNLOCK ANY DOOR

The 'Unlock Door' feature enables authorized users to unlock their locks/doors at anytime as outlined below.

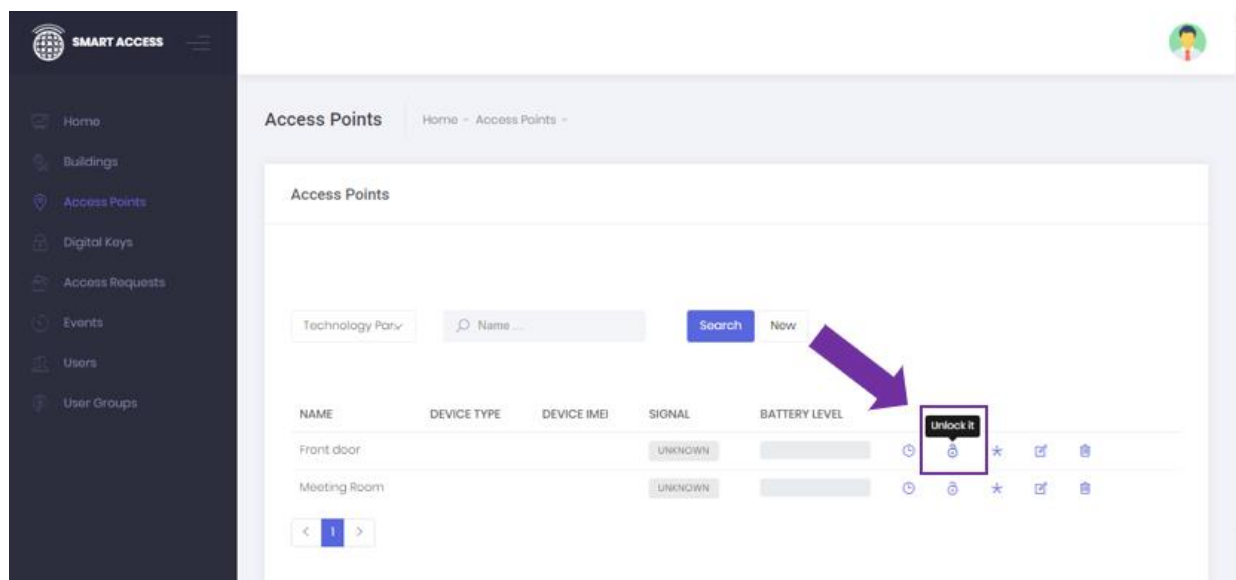
1. Select buildings box on the home page (to drill down to the lock you want to unlock)



2. Select the Building name of where the lock is that you want to open



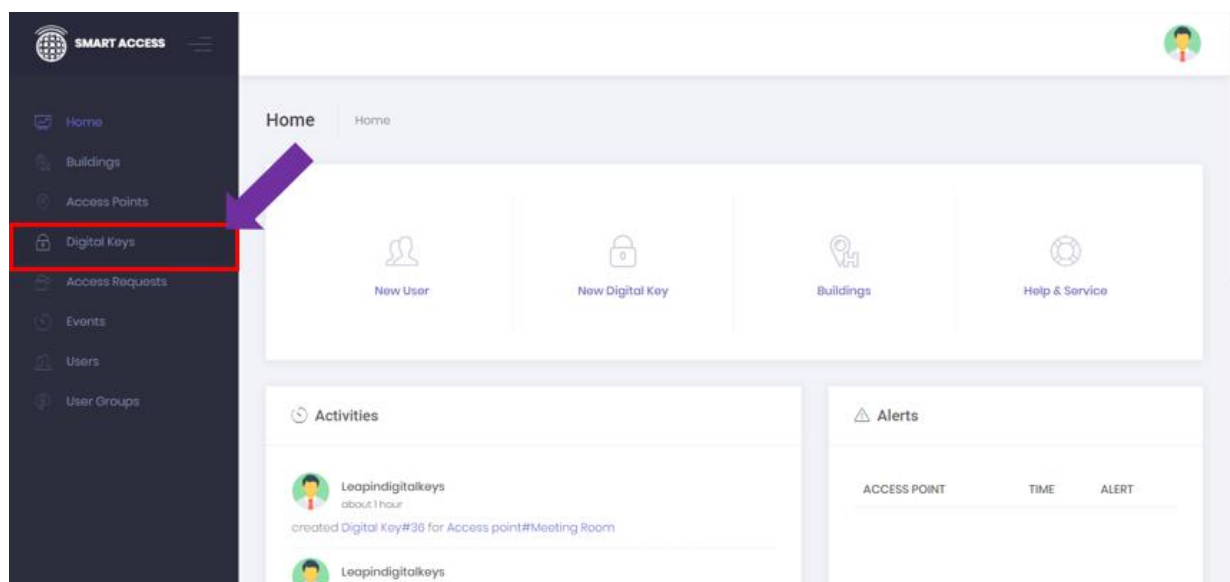
3. Click the 'unlock' button of the lock/access point you want to unlock. Lock will open.



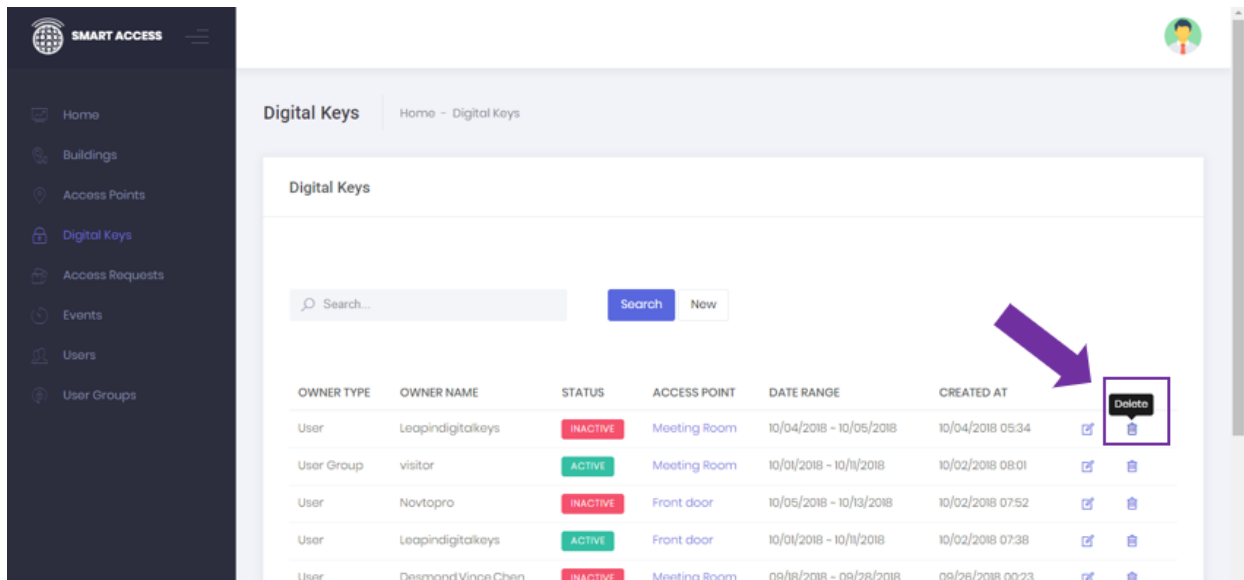
NOTE: After you hit unlock, someone will need to be at the door to touch the 'wake-up button' on the lock (NB IoT logo) which wakes it up, so it can unlock.

DELETE DIGITAL KEY

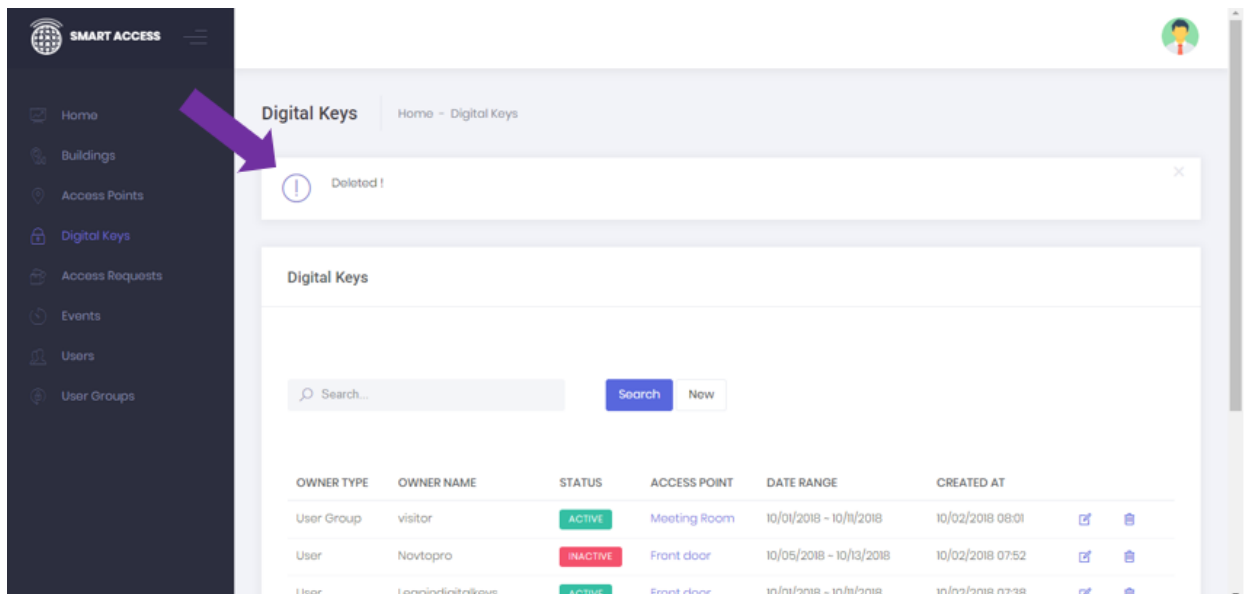
The Delete Digital Key feature enables authorized users to delete a users digital key at any time. To delete a digital key select Digital Keys from side menu bar as shown below.



1. All the Digital Keys created will be listed in a table. Select the 'Delete/rubbish bin' icon, to delete the digital key.



2. A message will appear at the top of the screen confirming the digital key has successfully deleted.



Of course to delete a digital key, you need to first generate a digital key – see previous section titled 'Generate time-sensitive digital key'.

VIEW LOCK EVENTS/LIVE AUDIT

The Live Audit feature shows who opened which door(lock/access point) at which time. The Live Audit is useful for tracking movements of users throughout buildings, and for arriving and leaving sites -for knowing who has entered a room/space at what time – similar to a time-card punch-in system.

The screenshot shows the SMART ACCESS web interface. On the left is a dark sidebar menu with options: Home, Buildings, Access Points, Digital Keys, Access Requests, Events (highlighted with a red box and number 1), Users, and User Groups. The main content area is titled 'Events' and contains a table of access events. The table has columns: ACCESS POINT (highlighted with a red box and number 2), BUILDIN, DEVICE MODEL, USER (highlighted with a red box and number 3), UNLOCK METHOD (highlighted with a red box and number 4), and TIME (highlighted with a red box and number 5). The table lists several events, all for 'Front door' at 'Innovation park' using device model 'vi000' and user 'Desmond.Vince.Chen', unlocked via 'app' at various times on 10/07/2018.

ACCESS POINT	BUILDIN	DEVICE MODEL	USER	UNLOCK METHOD	TIME
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:27
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:27
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:27
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:24
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:24
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:24
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:21
Front door	Innovation park	vi000	Desmond.Vince.Chen	app	10/07/2018 08:21

The features of the audit include

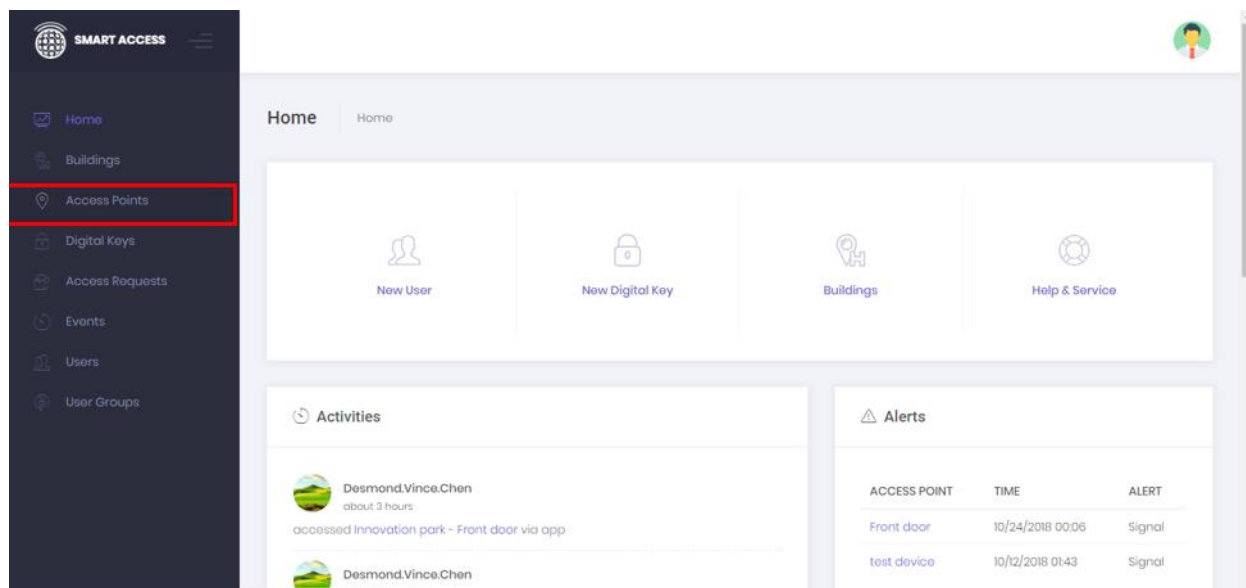
- 1 Events menu bar
- 2 Access point – lock/room name
- 3 User – lock opened by user with users name as identifier
- 4 Unlock Method – NFC unlock (by NFC on phone or NFC token), APP unlock on Digital Keys smartphone app (over NB IoT network), SOFT on Digital Keys management software
- 5 Time - the time the lock was unlocked

NOTE: The unlock event automatically updates into the table within a few seconds of someone unlocking the door. This a view only feature.

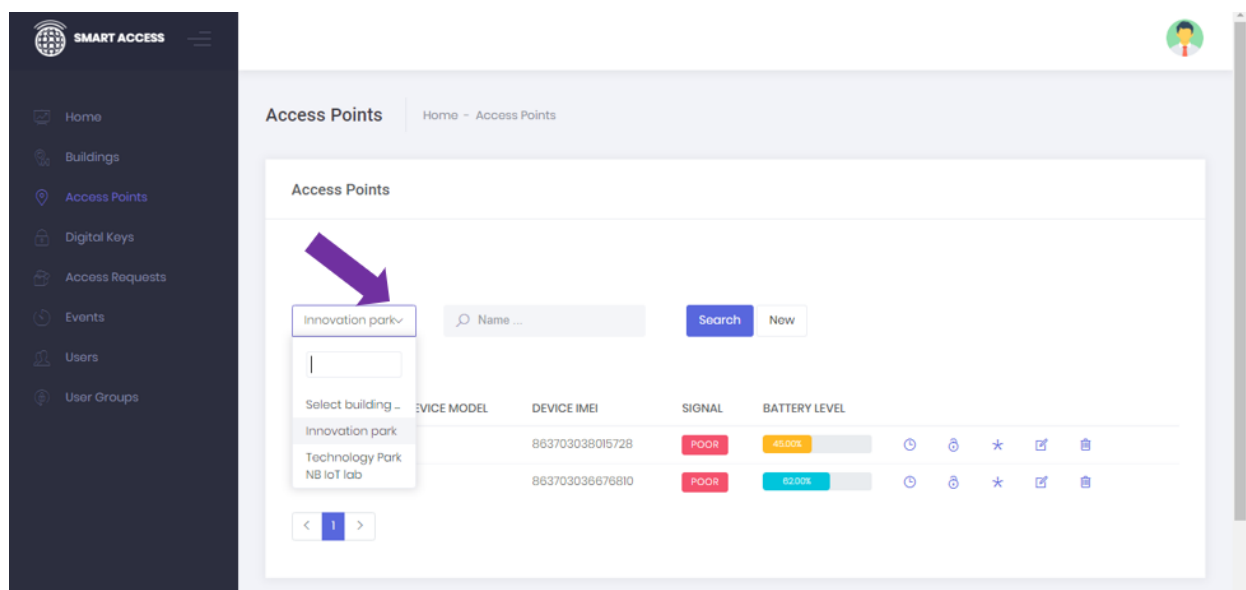
LOCK STATUS REPORT

You can view the status of the lock at anytime including seeing the battery status, and the signal strength/see that lock is online.

1. Select 'Access Points' from the side menu bar.



2. Select the building from the drop down menu



3. The locks and their signal strength and battery levels will be displayed as outlined below.

Signal strength is defined as;

POOR = NB IoT Network ECL2











FINE = NB IoT Network ECL1

EXCELLENT = NB IoT network ECL0^

*Extended Coverage Level as defined by the 3GPP - the authority charged with managing the global mobile phone network)

^Recommended Signal Strength for NB IoT Smart locks

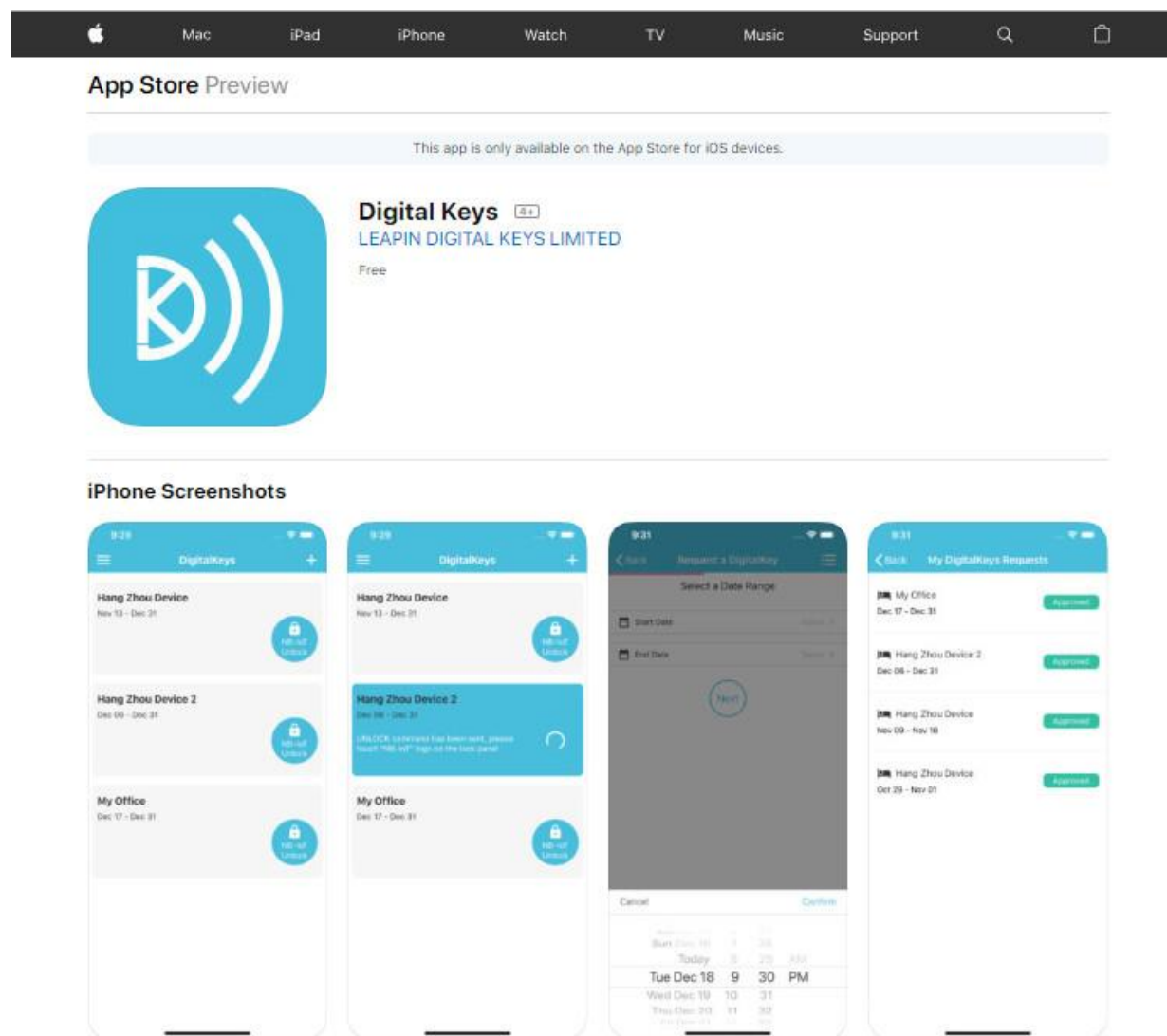
The screenshot displays the SMART ACCESS web application interface. On the left is a dark sidebar with navigation links: Home, Buildings, Access Points (highlighted), Digital Keys, Access Requests, Events, Users, and User Groups. The main content area is titled 'Access Points' and features a search bar with a dropdown menu showing 'Innovation park', a search input field, and buttons for 'Search' and 'New'. Below this is a table listing access points with columns for NAME, DEVICE MODEL, DEVICE IMEI, SIGNAL, and BATTERY LEVEL. Two entries are visible: 'Front door' and 'test device'. The 'test device' entry shows a 'POOR' signal and an 82.00% battery level. Each entry has a set of action icons to its right. At the bottom left of the main area is a pagination control showing '< 1 >'. The footer of the page indicates '2018 © Leapin'.

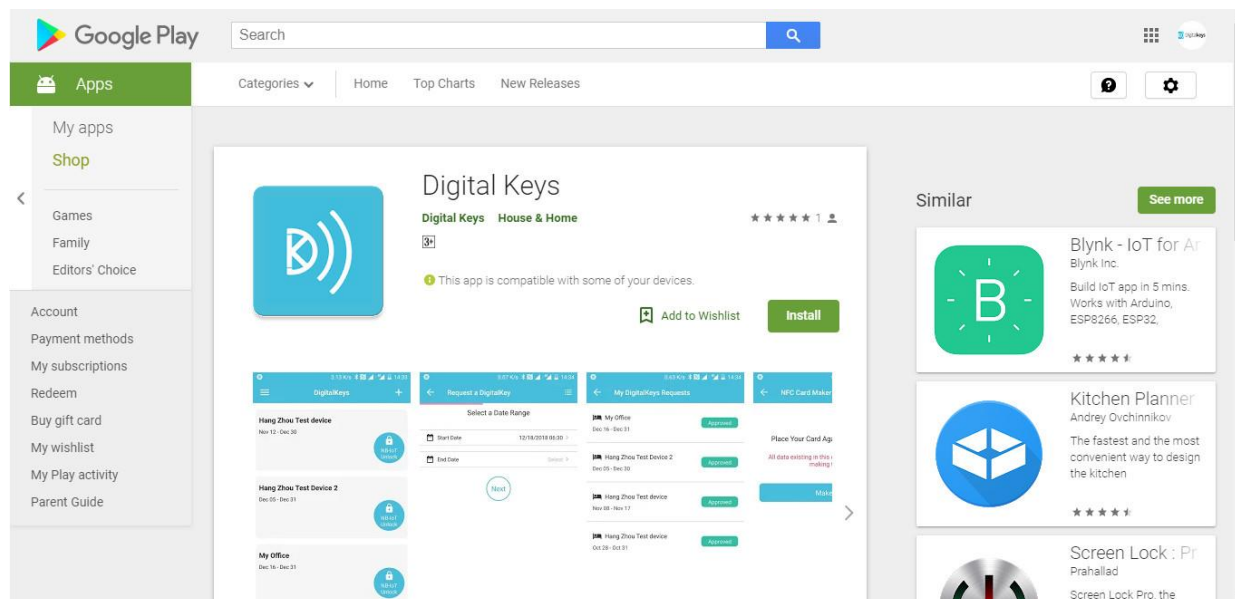
NAME	DEVICE MODEL	DEVICE IMEI	SIGNAL	BATTERY LEVEL	
Front door		863703038015728	POOR	45.00%	    
test device		863703038676810	POOR	82.00%	    

PART 3 - DIGITAL KEYS MANAGEMENT APPS USER GUIDE

DOWNLOAD AND LOG IN

Download the Digital Keys Universal App from the online stores, and hit 'sign-up' and follow instructions to sign-up. If you are account administrator, or you have been given access to the Digital Keys Management account, please use the same email and password you used for signing in to the Digital Keys Management Software.



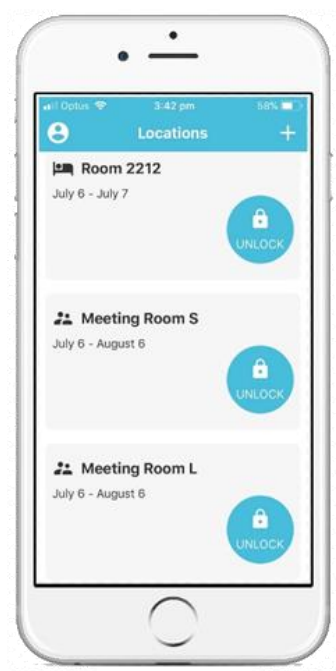


USING YOUR DIGITAL KEYS TO UNLOCK OVER NB IOT NETWORK

Sign into the digital keys app (only need to do this once, or after a new digital key is generated for you).



When you sign in, you list of digital keys which has been created for you by your account administrator will appear - e.g see below. Touch the 'unlock button' for the door you want to unlock.



Wait 1-3 seconds for unlock command to go over NB IoT network/query device status.



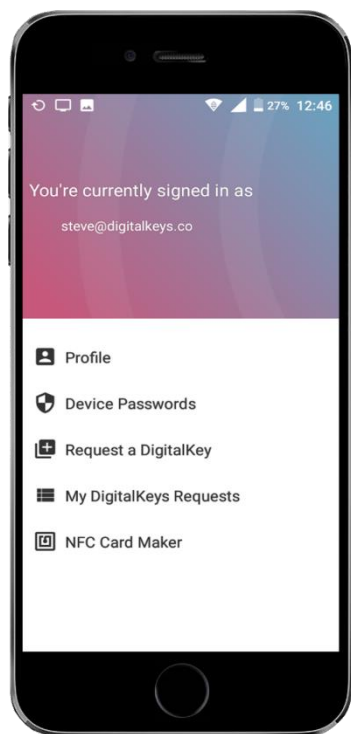
After 1-3 seconds a message will appear saying, 'Done touch the NB IoT logo on lock to open it' - see below. Your door will be unlocked and you can enter.



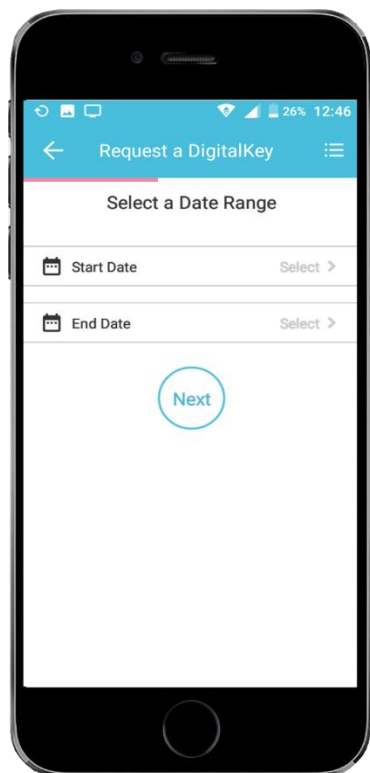
REQUEST DIGITAL KEYS

You can request at anytime a digital key from inside the digital keys app. Upon making a request for a digital key, after choosing date/time and lock, your account administrator will receive an email asking to approve your request. The account administrator can approve the request simply by hitting an approve button inside their email. The idea of this function is to make management of the locks and system the most efficient it can be, so the account administrator does not have to worry about logging into the software and generating new digital keys each time for authorised users. The end-user can 'generate the digital key' themselves inside the app and all they have to do to get access to a lock is to seek the approval of the account administrator, by getting them to hit one button inside their email.

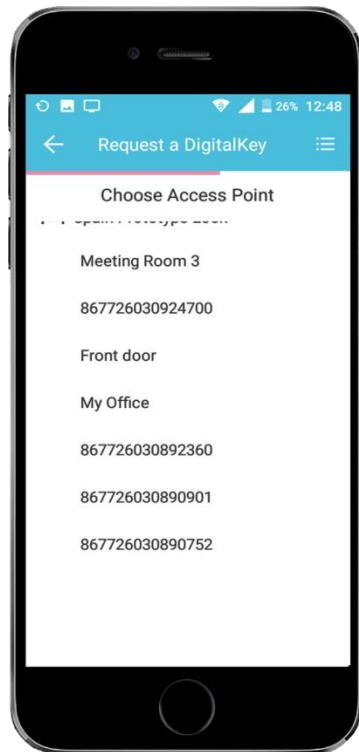
1. To make a request for a digital key, firstly select 'Request a Digital Key' from the menu bar - as shown below (swipe right for menu list)



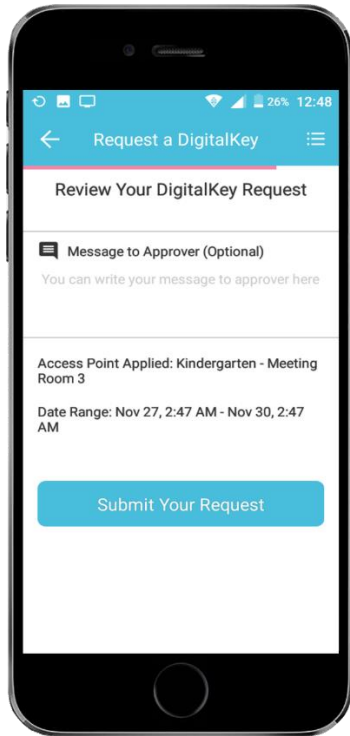
2. Select the date and time for the digital key to work.



3. Choose from the list the locks/access points which you want a digital key for. This list will be made available for you to choose from when the distributor/re-seller/account administrator first sets you up as a regular user in the digital keys management software account. If the lock you want access to is not on the list, then please follow up with your account administrator.



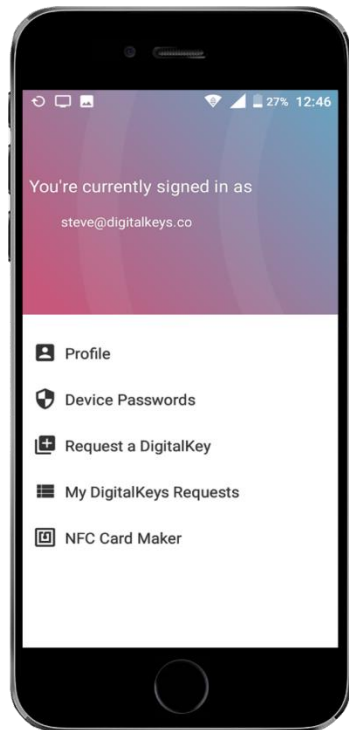
4. Review your Digital Key request, and if you like, give a message to your account administrator stating why you need the digital key for the date/time you have requested. For example you could say, "I'm opening the shop tomorrow as John is on leave, and so I need the digital key, or "I need to get to the server room tomorrow between 2-3pm to upload some updates of the software", or whatever reason it is you need to get a digital key. After you hit the 'Submit your request' button, your account administrator will immediately receive an email, and if they approve by hitting the one button in the email, then your digital key will appear within a few seconds. You will need to refresh the screen if you have the app open to see your new digital key(s).



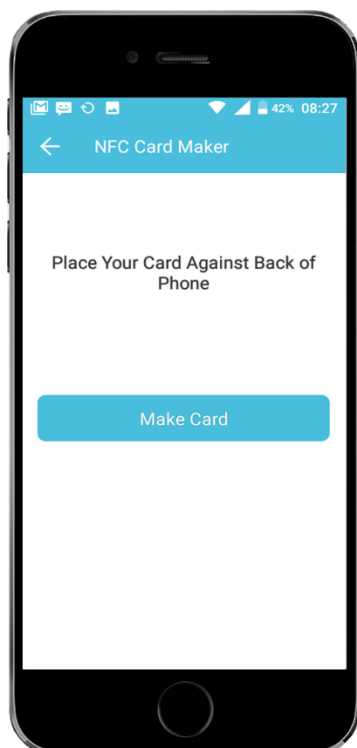
MAKE NFC CARDS/TOKENS

If you would like to use your NB IoT smart access control solution just like a typical keycard system, such as those commonly used in hotels and offices, then follow the steps below to make a NFC card/token work for a specific lock/room for a specific time period for a specific person.

1. Generate the digital key in the digital keys management software (as outlined above) or make a digital keys request in the app (see section above).
2. Select the NFC card maker menu item.



3. Place one of our supplied NFC card/tokens* to the back of the phone (Android phone operating system version 5.0 and above) and hit the 'Make Card' button. The digital key will then copy to the card/token, and you are ready to use the card/key for the time/date/lock you are authorised to access. You can write to this card 100,000 times, and you cannot copy the digital keys from this card once it has been written.





2/11 York Street, Sydney, Australia 2000

<https://www.digitalkeys.io/>

info@digitalkeys.io