



Inigma set up guide using the inigma app

Version 1.0

Prepared by Maria Wilson

Henry Squire & Sons Ltd





Inigma set up guide using the inigma app

Introduction

Inigma users interact with the inigma system either via the inigma app or the inigma website. The inigma app is the interface that all users interact with in order to manage their account and to operate some of the devices. The inigma app is the vital part of the inigma system due to its Bluetooth capability allowing communication between the Class 1 powered devices, such as the inigma key fob, the inigma bike locks and inigma integrator, and the inigma server via the inigma app. The inigma app is used to unlock inigma bike locks and other Bluetooth locks.

Class 2 unpowered devices such as the inigma cylinders and padlocks, however, require the inigma key fob to operate these locks. The inigma app bridges the communication between the inigma server and these devices by synchronising the inigma key fob with the inigma app. This action updates the validity and status of the key fob and locks and whether the user has access rights or not at that time and provides an audit log of these communications.



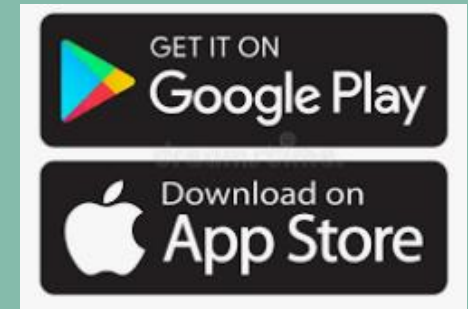


Inigma set up guide using the inigma app

Downloading the inigma app

First time users of the inigma system are required to download the inigma app to their mobile device. The mobile app compatibility policy for the inigma system is to support all major operating systems to the latest-but-one version. At the time of writing, supported mobile platforms are:

- Android V7+
- iOS/iPadOS V12.4+



Mobile platforms are supported using the Xamarin/MAUI cross platform framework which includes support for Android, iOS and iPadOS.

The inigma app is available for Android from Google Play and for iOS/iPadOS from the App Store.





Inigma set up guide using the inigma app

Account Registration

To register for an account users must:

- provide a valid email address
- create a secure password
- create a secure PIN

Users can register online or via the app by selecting the **register** option. To complete the registration and account authentication process, the user must activate a link sent via email. The link is delivered as an encrypted token that is only valid for 30 minutes. Instructions are provided for the user to verify their email address, which completes the process and generates an **account recovery code**. **It is important that this is saved securely on the user's device.**

Once the registration process is completed the user can sign into their inigma account.





Inigma set up guide using the inigma app

Account sign in

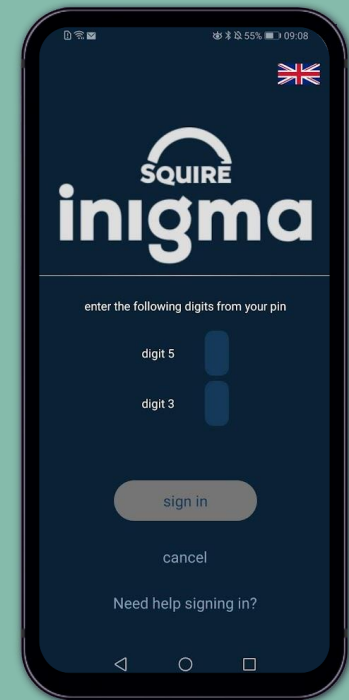
Users sign in to inigma app using the 2-step verification:

- step 1 - user email address and password
- step 2 - 2 randomly selected digits from their 6-digit PIN

The **activate** view is the first page displayed. This is one of the three main views that can be selected from the inigma app's menu bar displayed at the bottom of the screen:

- activate
- devices
- settings

The **activate** view is also used to synchronise Bluetooth devices with the app.





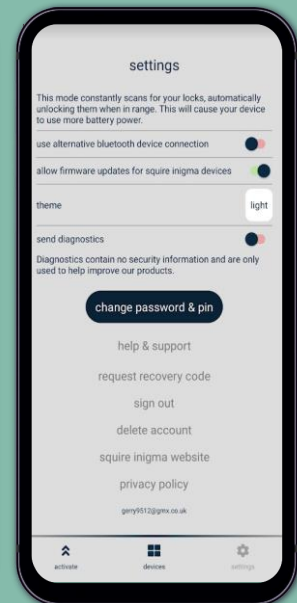
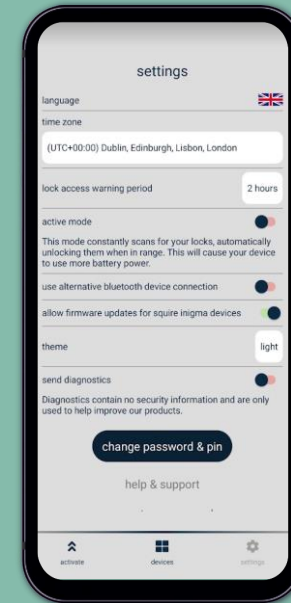
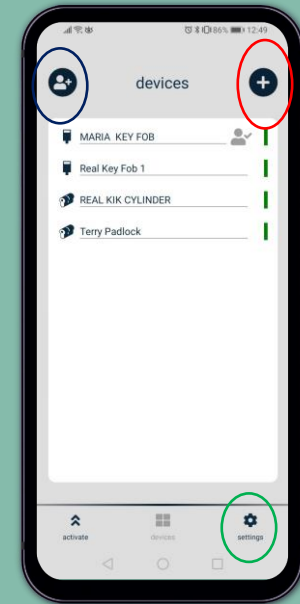
Inigma set up guide using the inigma app

Devices and Settings

The **devices** view displays a grid where the account holder's owned, delegated, shared, and assigned devices are displayed. New devices can be added here via the **+add** button.

Only when an account holder **owns** their own device, then they can add delegates to their account via the **+ add delegate** button.

The **settings** view provides the account holder with a variety of functions and features to help them manage their account. The settings view is comprehensive as it covers a wide area of functionality.





Inigma set up guide using the inigma app

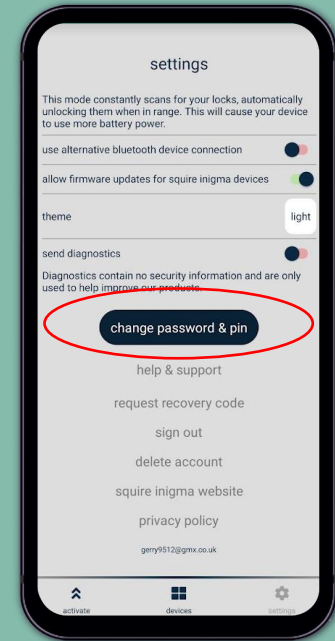
Password Management

Users have the option to change their password, PIN or both if these credentials are forgotten or through choice. This is found under the **settings** menu.

The inigma app provides a **Need help with signing in?** option on the **sign in** view when the user has forgotten one or both of their credentials.

Options:

- reset password with PIN
- reset PIN with password
- reset password & PIN with account recovery code





Inigma set up
guide using
the inigma app

Management of inigma devices

Class 1 – Powered Devices – Bluetooth Devices



- **Special Purpose Locks** - Bike Locks: BL1, BL1 Diamond, IC1 Integrated Chain lock, FL1 Folding lock
- **inigma key fob**
- **inigma integrator unit**

Bluetooth locks are opened and operated primarily using the inigma app on the user's mobile phone and the user's smartphone is effectively their "key".





Inigma set up guide using the inigma app

Management of inigma devices

Class 2 – Non-Powered Devices – Keyed Locks

In the case of keyed locks, the mobile application communicates with the inigma key fob, and the key fob is used to power and communicate with the keyed lock.

If access is permitted, the light on the inigma key fob illuminates green and access is given. If access is denied, the light on the inigma key fob illuminates red and no access is given.

The lock decides.



- **Special Purpose Locks** – Padlock – WS75 Container Lock
- **General Purpose Locks** – Stronghold Padlocks – SS100, SS80, SS65, SS50, SS50 Marine, SS45
- **Cylinder Locks** – Stronghold Cylinders – HC2, DC10, DC12, DC16, KC7, SOC
- **Cylinder Locks** – SmartKnob Cylinders – SC1, SC2, SC3, SC4, SC5 (in design)
- **Mortice Locks** – Handle Sets – Maxi (in design)





Inigma set up guide using the inigma app

Activation of Devices

The activation of inigma devices depends on which class of device they are.

Class 1 - powered devices with Bluetooth connectivity, can only be activated using the inigma app.

Class 2 - non-powered devices, can be activated either using the inigma app or on the inigma website.

Waking-up the inigma key fob

The inigma key fob is woken up by holding it securely between your first or middle finger and your thumb, with the nozzle pointing downwards. Firmly double tap the top of the key fob and the light illuminates with a solid amber light which remains illuminated for about 12 seconds.

x2





Inigma set up guide using the inigma app

Charging the key fob

The inigma key fob is charged using the inigma key fob charger. Plug the charger into the charging cable. Gently push the key fob into the charger and turn to the right until it stops and is locked in place. A charging light will illuminate on the key fob to indicate the status of the key fob charge:

- Slow amber fade in-out - key fob battery charging
- Slow green fade in-out – key fob battery charged

The time taken to charge the key fob depends on the level of the battery before charging. An average charge takes about 40 minutes from completely empty to full charge.

When a key fob battery level falls below the critical level or is fully discharged, the key fob light will not illuminate straightaway as it requires a certain level of charge to display the charging light. Once the key fob has enough battery power, the charging light is displayed.

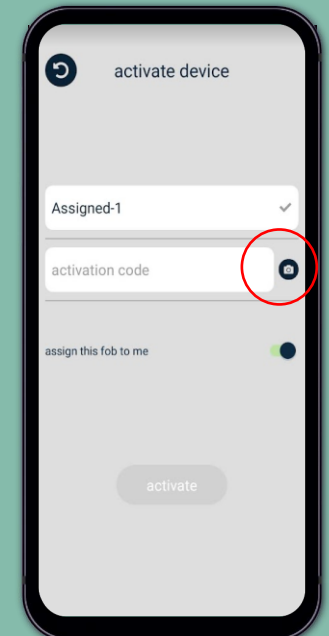
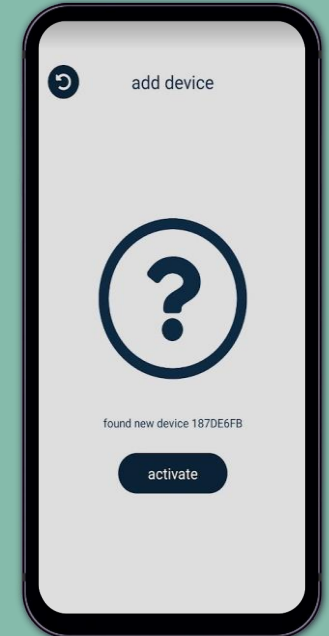




Inigma set up guide using the inigma app

Adding an inigma key fob to an inigma account via the inigma app

1. Bluetooth devices such as bike locks and key fobs can only be added to a user's account via the inigma app because of its BLE capability.
2. Ensure that Bluetooth is activated, sign into your inigma account – go to the **devices** view.
3. Click the **+** button - **select device** view is displayed.
4. Select the option to add a powered Bluetooth device to your account.
5. Wake the key fob and click the **activate** button.
6. The inigma app scans for your key fob and the *"scanning"* status is displayed.
7. Once the inigma app has located the key fob then the *"found new device"* status is displayed with a unique code associated with the key fob.
8. Click the **activate** button again and the **activate device** view displayed.
9. Complete the name field, enter the activation code received with the key fob, or use **the camera to scan the QR code** then click **activate**.
10. The key fob displays an *"activating"* transition view and then returns to the **devices** view where the grid has been updated and displays the newly added key fob.

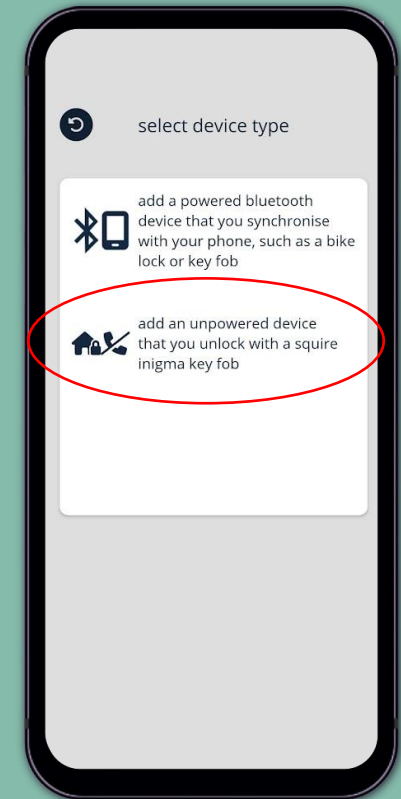




Inigma set up guide using the inigma app

Adding an inigma lock/padlock to an inigma account via the inigma app

1. Go to the **devices** view.
2. Click the **+** button.
3. Select the option to add an unpowered device to your account.
4. Complete the name field, enter the activation code received with the lock or scan the QR code using the camera icon then click **activate**.
5. The lock/padlock displays an “*activating*” transition view and then returns to the **devices** view where the grid has been updated and displays the newly added lock.








Inigma set up guide using the inigma app

Inigma devices grid

The devices grid provides the user with an overview of all the devices that are associated with their account and displays the following information to quickly distinguish between them:

- **device icon** – key fob, bike lock etc
- **device name** – friendly name chosen by user
- **association with the device** – owned, delegated, shared or assigned
- **status of the device** – coloured ribbons (see device access legend)
- **battery warning** – low (amber) and critical (red) icons

association with device

-  this device has been delegated to you
-  this device has been shared with you
-  this device has been assigned to you

status of device

- device access legend
- full access
 - validity expires within 120 minutes
 - validity expired
 - access lost within 120 minutes
 - no access
 - not synchronised

battery warning

amber – battery level threshold is below 40%



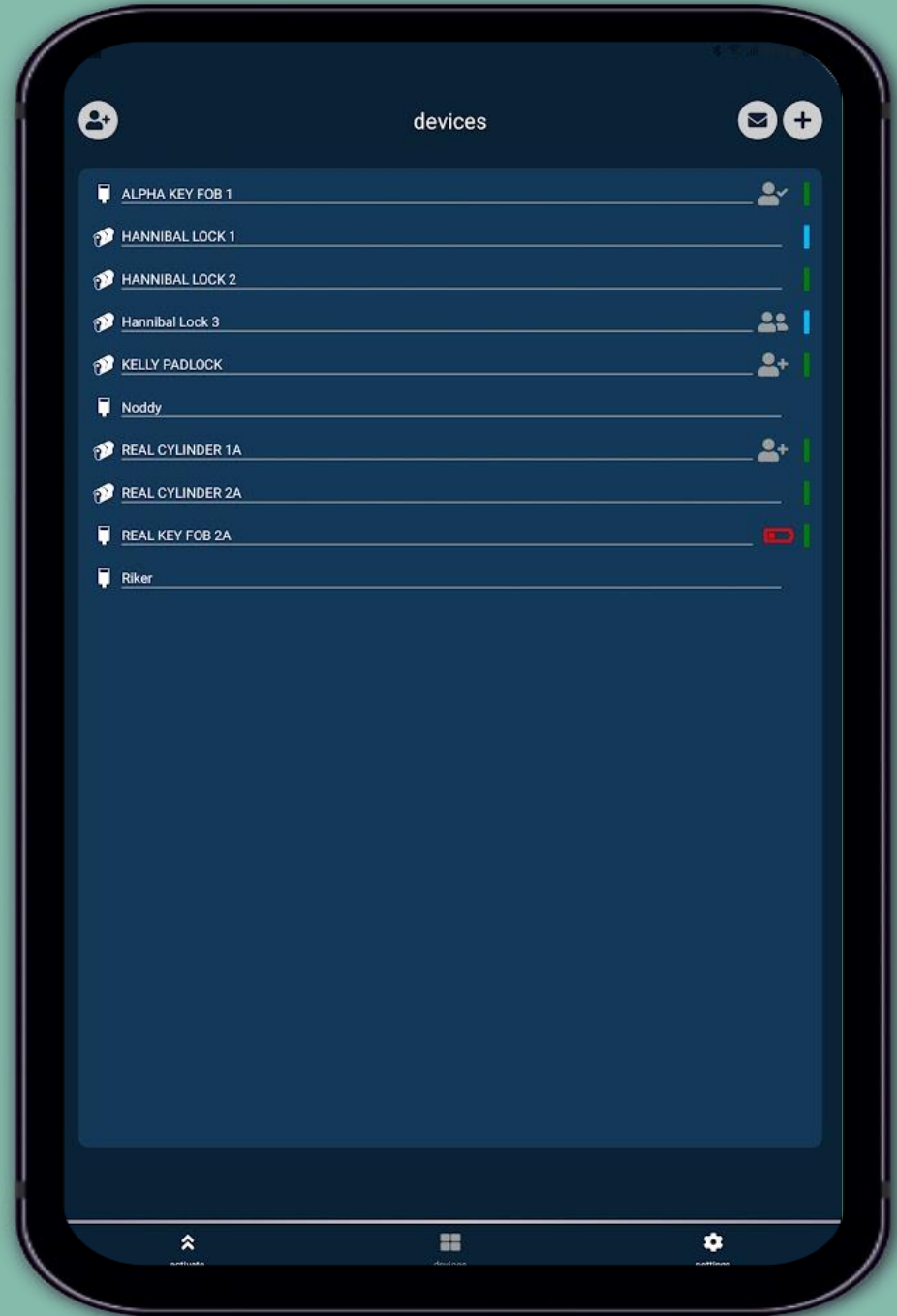
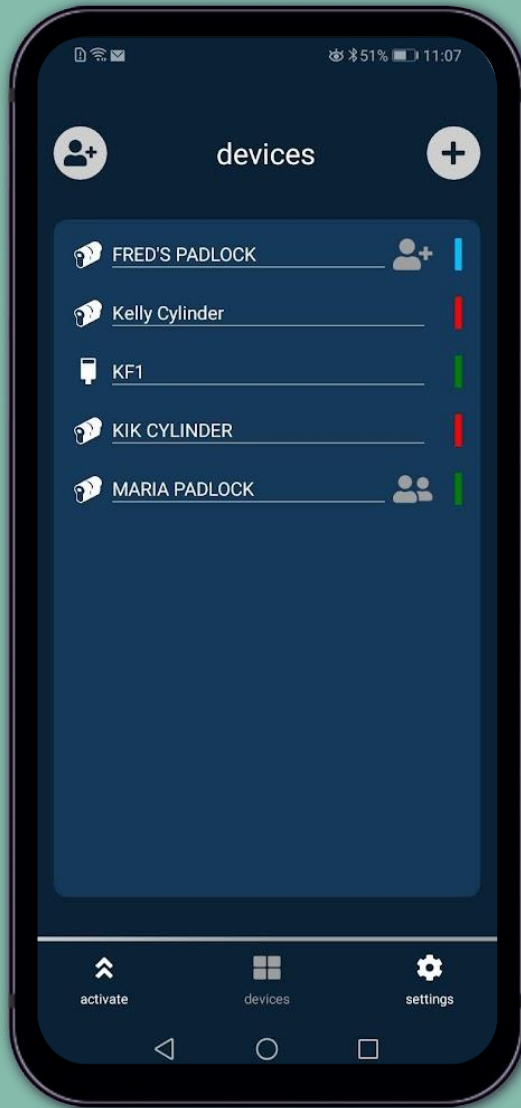
red – battery level threshold is below 25%





Inigma set up guide using the inigma app

Inigma devices grid





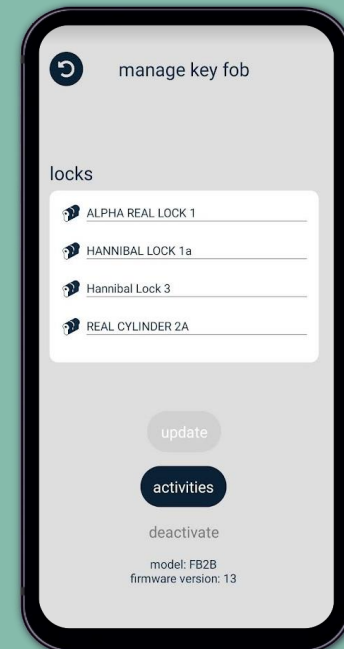
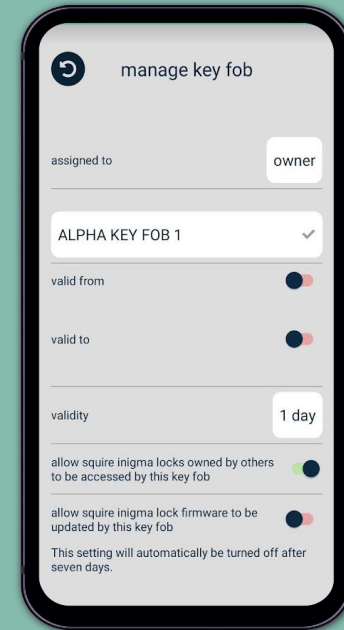
Inigma set up guide using the inigma app



Manage key fobs

Key fobs can be viewed and edited in the following ways on the **manage key fob** view by selecting a key fob from the devices grid:

- **assigning key fob** to the owner, other or be unassigned (view & edit)
- **name of device** (view & edit)
- **valid from and to date and time** (view & edit)
- **validity** (view & edit)
- **interoperability on/off** (view & edit)
- **permission to allow firmware to be updated by the key fob on/off** (view & edit)
- **notes** - only visible if activated by organisation administrators and when activated the user can view, add, append, or edit notes depending on the notes setting.
- **list of locks that can be accessed by the key fob** (view & access locks via the grid, links to **manage lock** view, schedule, and validity)
- **update** when selected, saves changes to the page
- **activities** (view audit log for the key fob)
- **deactivate** (deactivate device and generation of the reactivation code)
- **model number and firmware version** (read only)





Inigma set up guide using the inigma app

Manage Key Fobs – validity and access

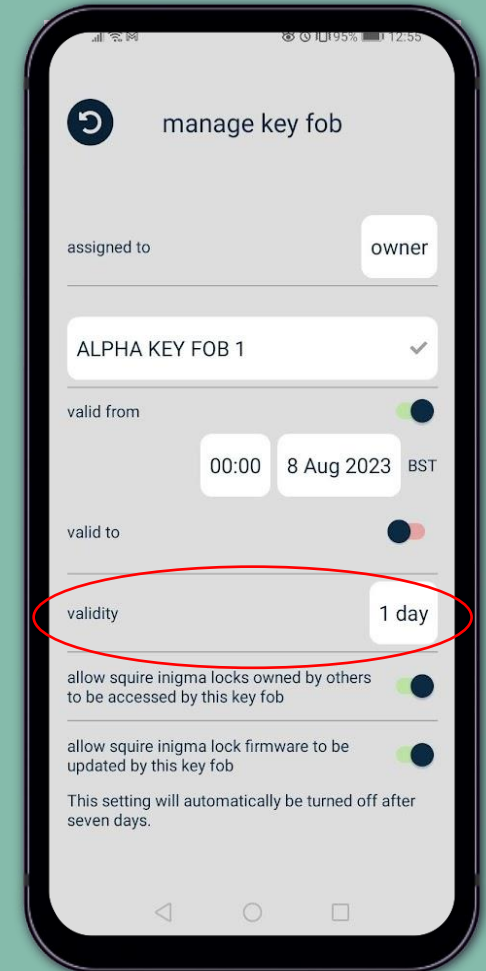
- **valid from/valid to** - sliders control the dates and times that the key fob is active. There are 4 possible scenarios:
 - **both switched off** – no access restrictions
 - **valid from on only** – restricted access before from date and time
 - **valid to on only** – restricted access after to date and time
 - **both switched on** – date and time settings on both will dictate the access from and to

The **validity** field is displayed on the manage key fob view and is set per key fob. Default validity is set to 1 day but can be changed in increments from 1 hr to 4 weeks.

Validity is renewed every time the key fob synchronises with the app.

Device grid ribbons display the status of each device and act as a guide for users.

If the key fob is not synchronised to renew validity, then access will be denied by the locks with an alert – 5 short flashes and beeps emitted from the key fob.



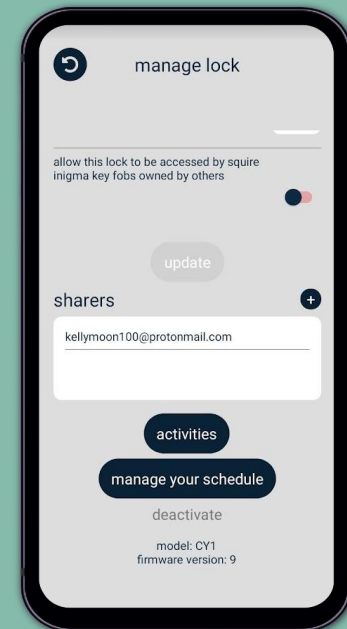
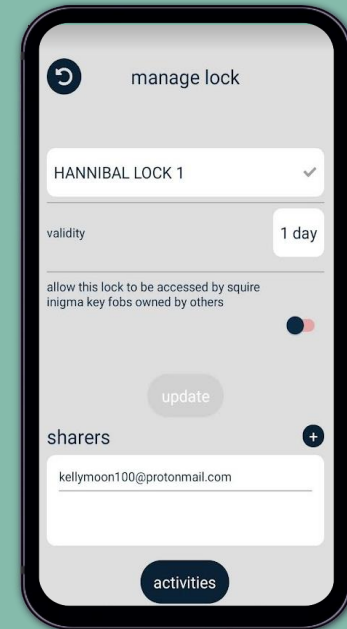


Inigma set up guide using the inigma app

Manage Locks

Locks can be viewed and edited in the following ways on the **manage lock** view by selecting a lock from the devices grid:

- **name of device** (view & edit)
- **validity** (view & edit)
- **interoperability on/off** (view & edit)
- **list of sharers** that share the device and option to add more with a link to each sharer to **manage sharer** view, where the schedule and validity is managed, and the sharer can be removed (view & edit)
- **activities** (view audit log for the lock)
- **manage your schedule** link to manage own schedule for the device (view & edit)
- **deactivate** (deactivate device and generation of the reactivation code)
- **model number and firmware version** (read only)





Inigma set up guide using the inigma app



Manage locks – validity and access

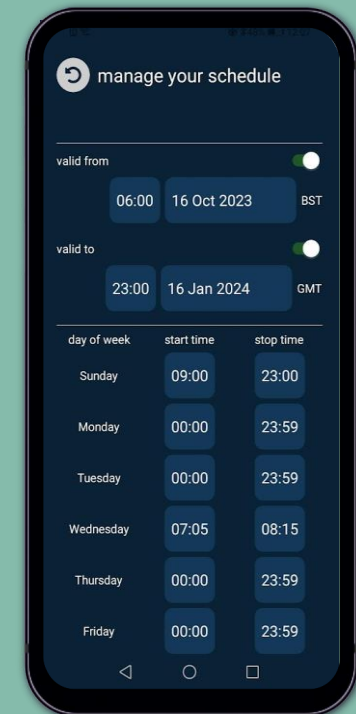
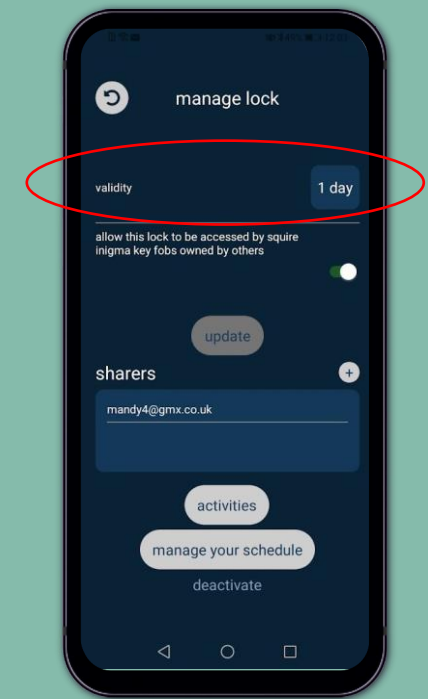
- **validity** – field is displayed on the manage lock view and is set per lock. Default validity is set to 1 day but can be changed in increments from 1 hr to 4 weeks.

Validity is renewed every time the key fob synchronises with the app.

If the key fob is not synchronised to renew validity, then access will be denied by the locks with an alert – 5 short flashes and beeps emitted from the key fob.

Device ribbons display the status of each device and act as a guide for users.

- **manage your schedule** - links to the **manage your schedule** view for the lock. The owner or delegate can set their own schedule using the valid from and to dates and times and extend scheduling to specific days of the week with their own start and stop times. This remains fully editable and can be updated as soon as the **update** button has been selected.





Inigma set up guide using the inigma app

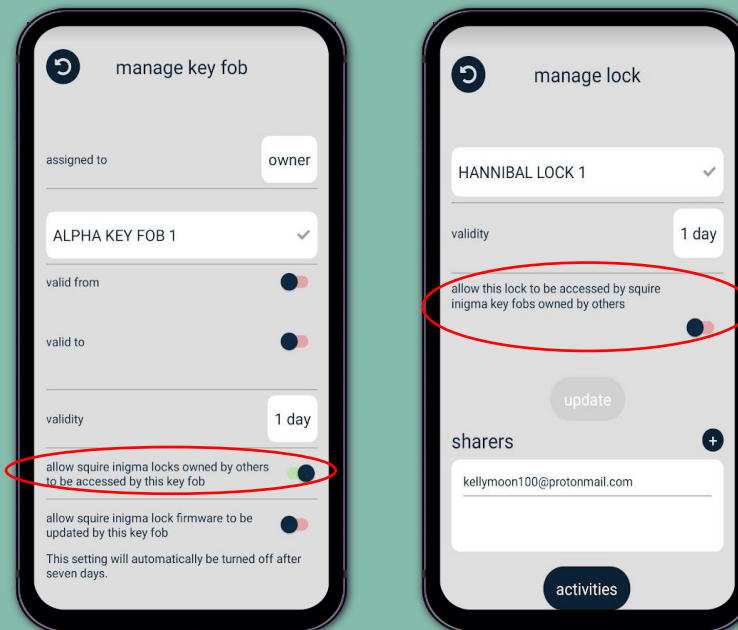


Interoperability

Interoperability is one of the key features for managing inigma key fobs and inigma locks. Interoperability is controlled by a switch *“allow squire inigma locks owned by others to be accessed by this key fob”* on the **manage key fob** view and by *“allow this lock to be accessed by squire inigma key fobs owned by others”* on the **manage lock** view.

The rules for interoperability are:

- Interoperability works on hardware actuators and locks that are hardware actuated.
- Interoperability must be activated on both a key fob and lock for them to be interoperable.
- When interoperability is not activated on one or both devices, either key fob or lock or both, the connection is not viable, and interoperability is not possible. However, the owner of the key fob can use their key fob with locks owned by them.
- When interoperability is activated on both key fob(s) and lock(s), the user can see all the hardware actuated locks that are owned by them, delegated to them, or shared with them.
- When interoperability is not activated the user is only able to see their own hardware actuated locks.





Inigma set up guide using the inigma app

Management of Users

Users of the inigma app fall into 4 main categories:

- owners
- delegates
- sharers
- assignees

All types of users are required to register for an inigma account which gives them access to the inigma app and website.

Owners

The definition of an owner in the inigma system, is a user who registers for an inigma account and activates their own device(s). The owner of a device has full control of that device and can manage it via the inigma app or inigma website

A device owner has the option to add delegates to their account and select which devices to delegate to them. A device owner also has the option to add sharers to one or more devices either owned by or delegated to them on their account. A device owner can add and revoke delegation and add or remove sharers of these devices at any time. A device owner can also assign key fobs owned by them or delegated to them, to themselves, other users, or choose to have them unassigned.

The owner of a device manages their own schedule for each device they own and for each device that is shared with another user.





Inigma set up guide using the inigma app

Delegates

 this device has been delegated to you

The definition of a delegate in the inigma system, is a user who has been delegated, by the owner of another account, some or all of their devices and to manage those devices as if they were the owner themselves. A delegate does not own the device, but once delegated, they have the same control of the devices as a device owner.

A delegate can share delegated devices with other users or assign delegated key fobs to themselves, another user or unassign them. Like the device owner they can add and remove device shares, edit key fob assignment and they can also revoke delegation for themselves which would then remove all the delegated devices from that owner from the delegate's account.

The "*can add hardware*" and "*can remove hardware*" permissions, on the **manage delegate** view, extend/limit the permission for the delegate to add or remove hardware on behalf the account holder.

The delegate of a device can manage their own schedule for that device and manage the schedule for any sharer of that device.

The inigma app identifies devices that are delegated to the user with an icon.





Inigma set up guide using the inigma app

Sharers

 this device has been shared with you

The definition of a sharer in the inigma system, is a user who has been shared one or more inigma locks, (not key fobs) by the device owner or delegate. A sharer does not own the locks, and once shared, they do not have the same control of the locks as a device owner or delegate.

The device owner or delegate can remove the sharer from the device at any time which removes the device from the sharer's account, and they would no longer have access.

A sharer can view the shared lock in their devices' grid, which is identified with a sharer icon, and they can view the schedule for their use of the shared lock. They do not have permission to edit the shared device, but they can remove the shared device from their account by selecting the **remove** button which would remove the device from their account.





Inigma set up guide using the inigma app

Assignees



this device has been assigned to you

The definition of an assignee in the inigma system, is a user who has been assigned a **key fob** from an owner or delegate of the key fob. A key fob owner/delegate must assign the key fob to themselves to be able to use it with locks owned, delegated, or shared with them. When an assignee is not the owner or delegate, they do not have the same control as an owner or delegate.

An assignee, who is not the owner or delegate, is able to view the key fob in their account, which is identified with an *"assigned to"* icon and view the schedule for their use of the assigned key fob. They do not have permission to edit the assigned key fob, except for switching firmware updates on and off, but they can remove the assignment which would remove the key fob from their account and the assignment of the device. This action would change the status of the key fob to unassigned and an email would be sent the key fob owner.

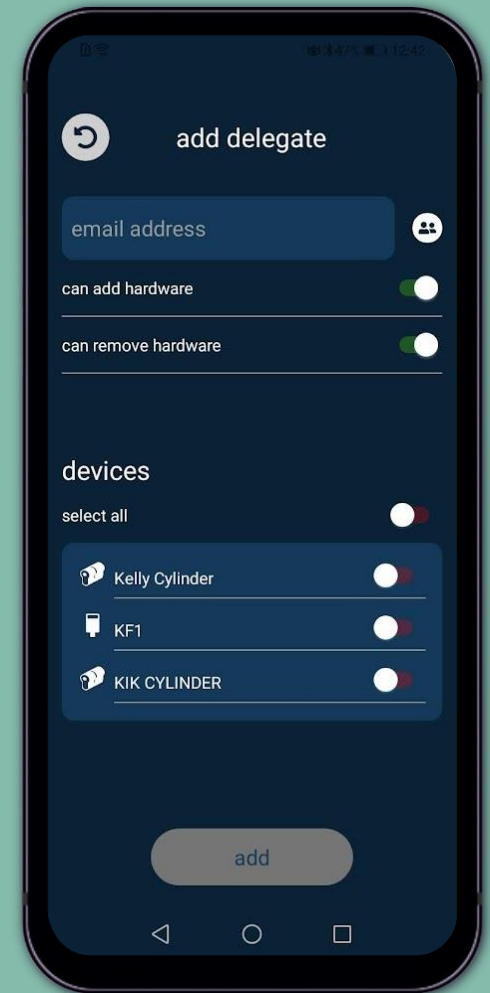




Inigma set up guide using the inigma app

Add a Delegate

1. A delegate can only be added to an owner's account if the owner owns one or more devices. The inigma app does not display the **+add delegate** button if there are no owned devices displayed. The process of adding a delegate is as follows:
2. Open the **devices** view and select the **+add delegate** icon. This opens the **delegates'** view. If there are delegates already active on the user's account, then they will be displayed in the grid identified by their email address.
3. Select the **+add** icon, this opens the **add delegate** view.
4. The **add delegate** view consists of 4 fields:
 - **email address** – blank to be completed by user
 - **can add hardware** – activated/deactivated = delegate can/cannot activate new devices for the owner
 - **can remove hardware** – activated/deactivated = delegate can/cannot deactivate devices for the owner
 - **devices** - only inigma devices owned by the user are displayed in the devices grid. The default setting for each device is deactivated. The user must select 1 or more devices to delegate to the new user by activating each device using the switch control.
 - **add** - when the email field is completed and one or more devices selected, the add button is activated and adds the new delegate to the delegate's grid.
5. Once the process is completed, the new delegate is displayed in the **delegates** grid where they can be selected and managed.
6. The new delegate receives an email informing them of the delegation of devices and the delegated devices are displayed in their devices grid with the delegate icon.





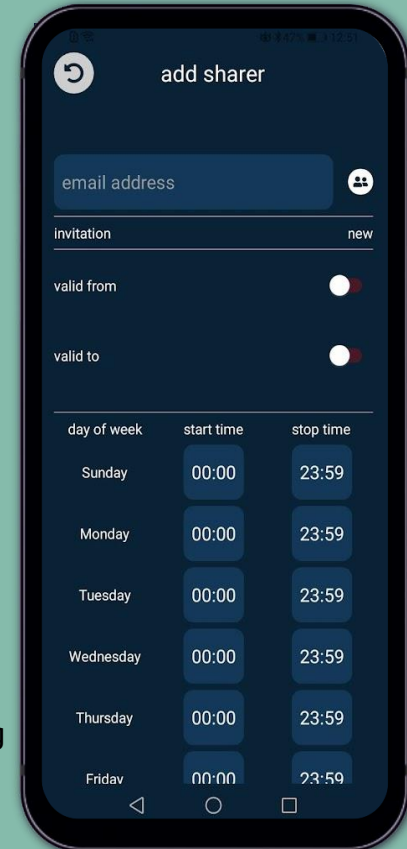
Inigma set up guide using the inigma app



Add Sharer to an inigma lock

A sharer can only be added to a lock if you are an owner or delegate of a lock. The inigma app displays the option to add a sharer when a lock is selected from the user's devices grid. The process of adding a sharer is as follows:

1. Open the **devices** view and select the owned or delegated device to add the sharer to. This opens the **manage lock** view and any existing sharers are displayed in the sharers grid and are identified by their email address.
2. Click the **+add** button, this opens the **add sharer** view.
3. The **add sharer** view consists of 6 fields:
 - **email address** – blank ready to be completed by the user
 - **invitation status** – new, pending or accepted – new when creating a new share
 - **valid from/valid to** - sliders control the dates and times that the key fob is active. There are 4 possible scenarios:
 - both deactivated – no access restrictions
 - valid from activated only – restricted access before from date and time
 - valid to activated only – restricted access after to date and time
 - both activated – date and time settings on both will dictate the access from and to
 - **days of the week/start and stop times** – the user can schedule the daily access to the device via inputting the start and stop times for each day. Clicking the start or stop time fields activates an analogue clock or digital clock tool where the user can set the times.
 - **add** – activated when changes are made and when selected all changes are saved.
5. Once the process is completed, the new sharer is displayed in the **sharers** grid where they can be selected and managed.
6. The new sharer receives an email informing them of the sharing of devices, and the shared devices are displayed in their devices grid with the shared icon.



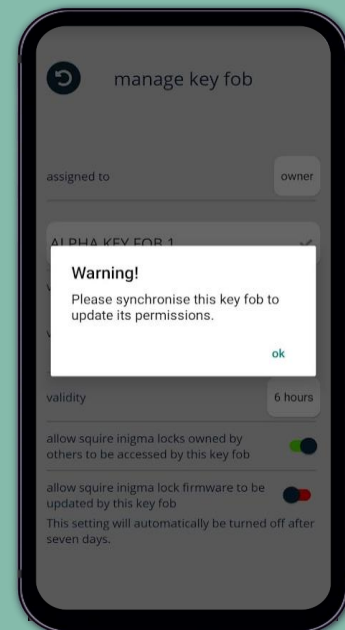
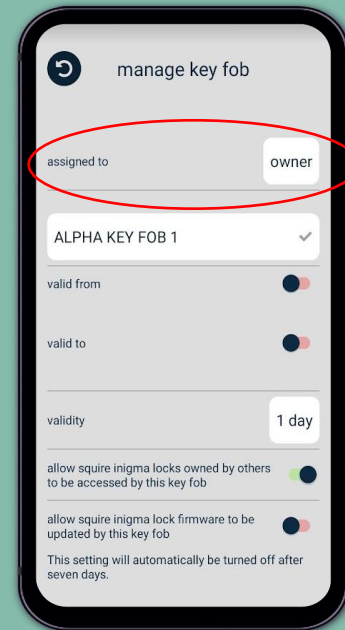


Inigma set up guide using the inigma app

Assign another user to an inigma key fob

1. A user can only assign a key fob to another user if they are an owner or delegate of the key fob. The inigma app displays the option to assign a key fob to another user on the **manage key fob** view. The process of assigning a key fob is as follows:
2. Open the **devices** view and select the owned or delegated key fob to assign to another user. This opens the **manage key fob** view.
3. The **assigned to** field has 3 options (4, if the user is a delegate) accessed via a drop-down menu:
 - **unassigned** – key fob cannot be used with any lock
 - **owner** – key fob can be used with locks owned by the user, delegated to, or shared with the user if interoperability is activated on both devices
 - **other** – activates an email field to identify an assigned user, this user can only use the key fob with locks owned, delegated and shared with them if interoperability is activated on each device, depending on device ownership
 - **self** – this option is only displayed when the user is a delegate for the device so the user can set it to themselves, as the owner is someone else

1. The user can set the **valid from** and **valid to** dates and times before or after updating the key fob assignment.
2. The user clicks **update** and once synchronised the app displays a warning window to *“Please synchronise this key fob to update its permissions”*. The key fob must synchronise with the inigma app via the **activate** view to update the changes made to ensure that the new permissions are fully communicated.





Inigma set up guide using the inigma app

Adding users to an account who are not already inigma account holders

When a user is delegated, shared, or assigned an inigma device they receive an email notifying them of the device delegation, share, or assignment. If the recipient does not already have an inigma account, the email received provides the information required to support the new user to set up an inigma account so that they are able to use the shared, delegated, or assigned devices.

Removing Users

Owners can remove delegates via the **manage delegate** view.

Owners and delegates of devices can remove sharers via the **manage sharer** view.

Owners and delegates of key fobs can remove the assignee via the **manage key fob** view.

Delegates, sharers, or assignees can revoke the delegation (all devices for that organisation), the sharing of one or more devices, or the assignment of a key fob via the **manage lock/key fob** view.

These action trigger emails to the users to inform them of the change of use for the devices.





Inigma set up guide using the inigma app



Settings

The settings option is displayed on the menu bar in the inigma app and navigates the user to the settings view. From here there several settings that can be configured by the account holder to personalise their inigma app. The options below may not all be visible, and the user's email address is also displayed.

Language – 7 languages (English, German, French, Dutch, Italian, Polish, Spanish)

Time Zone – changes only take affect once every 5 days

Assign key fobs to me – new key fobs are assigned to the user when activated
Lock access warning period – changes how much warning a user is given on the devices' grid's ribbons

Active mode – Bluetooth locks can be unlocked when woken without viewing the app
User alternative Bluetooth device connection – alternative Bluetooth communication method

Allow firmware updates for squire inigma devices – allows the app to update the firmware of all devices

Theme – light or dark

Change password & PIN

Request recovery code

Sign out

Squire inigma website – link to the Squire inigma website

Privacy Policy – link to the Henry Squire Ltd privacy policy

Help & Support – links to a new view with support information, device access legend, device ownership legend and link to email squire support

Delete Account – deletes a user's inigma account if all devices have been deactivated or removed



Inigma set up guide using the inigma app

Key fob Alerts – lights and sounds

The inigma key fob has a range of light sequences and sounds that indicate its status:

Not In Use

- No light = asleep

At Any Time

- Cycle red, amber, green rapidly = battery lock out mode – you must charge the key fob as the key fob will be locked out

In a Charger

- Slow amber fade in-out = battery charging
- Slow green fade in-out = battery charged

In a Cylinder

- Two short green flashes with beeps = lock access granted
- One short red flash with beep = lock access denied
- 5 short red flashes with beeps = expired validity – you must synchronise the key fob with the app
- Flash amber rapidly = battery low warning, displayed after the key fob has interacted with a lock – you must charge the key fob
- Continuous rapid red flashing with beeping = key fob lockout mode – affected lock must be locked before the key fob can be used in another lock, synchronise the key fob with the app to identify which lock it is
- Continuous amber light = cylinder firmware update waiting to be sent to lock – you must be familiar with the firmware update process to continue, or wait until the light goes out and continue without updating the firmware

After Double-Tap Wake

- Steady amber = key fob ready to synchronise with the inigma app
- Short pulse amber = message transfer from key fob to inigma app during fob synchronisation

When Dropped

- Long amber flash mostly on = dropped key fob detection, accompanied by a rapid alarm for about 12 seconds – synchronise the key fob with the app to renew the key fob's validity

