

inVUE



User Manual

A guide to:

- ✓ **Using the *Web Portal*** (web application)
- ✓ **Using the *Mobile App*** (Android & iOS)

Release: April 14, 2023



Contents

About this manual	5
Who should read this manual	5
Help beyond this manual	5
Glossary	6
Frequently Asked Questions and Helpful Tips.....	7
LIVE Access Web Portal	14
About LIVE Access.....	14
Pro vs. Lite	14
Pro	14
Lite.....	14
Overview of the Web Portal, functionality	16
Audit.....	17
Dashboard.....	18
Users.....	19
Roles.....	24
Zones	25
Devices.....	26
Keys	26
KAS/OKM.....	27
Settings.....	29
LIVE Access Mobile App	31
About the App.....	31
Installing the App	31
Supported Mobile Platforms.....	31
Login with Single Sign On (SSO) → Home Screen → Logout (Android).....	32



Login without Single Sign On (SSO) → Home Screen → Logout (Android & iOS)	33
Operate a Device: Unlock → Unlatch → Latch → Lock (Android & iOS)	34
Authorized Devices in Range (Android)	36
Authorized Devices in Range (iOS)	38
Update Device Settings (Android)	39
Enroll Devices, 1 at a time or in bulk (Android)	40
Update Firmware (Android)	42
Request a Remote Unlock, by an unauthorized user (Android)	43
Remote Unlock from the App (Android)	44
Remote Unlock from the Web Portal & Remote Bridge (Android)	45
Device Not Found (screens explained) (Android)	47
Operation / Interaction Error States (Android)	49
Features unique to certain Devices	50
Glossary of Features	50
Package Protection – IR3	50
RAC Lock	51
Padlock	51
LIVE Locks	51
Setting up a new Environment	53
New Environment Setup Parameters	53
Setting up a Site – 1 st or adding a new one	53
About the IR Ecosystem	54
The IR3 Ecosystem	54
The IR4 Ecosystem	54
Setting up the IR3 Ecosystem	55
Products in the IR3 Ecosystem	55



IR3 OneKEY	55
Key Authorization Station (KAS).....	55
Installing the KAS and the IR3 OneKEY	55
Setting up the IR4 Ecosystem.....	56
Products in the IR4 Ecosystem	56
IR4 OneKEY	56
OneKEY Manager (OKM)	56
Installing the OKM and the IR4 OneKEY	56



About this manual

This manual details how to use LIVE Access as well as how to install the hardware and troubleshoot common issues. Each section prescribes prerequisites, if any, to help avoid pitfalls.

IMPORTANT:

- **Pro Tip:** download this manual and open it in a PDF viewer so that you can search it for specific terms. However, this manual is updated with each new release of the software so, when possible, reference it through the UI each time, not a locally saved copy.
- **Yellow highlighted text** indicate new functionality or updated instructions since last revision.

Who should read this manual

This manual is written for system administrators, operations managers, device outfitters, and IT and support persons.

Help beyond this manual

If you are not able to find the solution in this user manual then, review the FAQs which can be found under the 3-dot menu on the top-right.

If you still need help, then submit a Service Request to get our Customer Service Team's attention. Our Customer Service team is ready to help.

Important: Please submit one Service Request per issue.

Below are two ways to submit a Service Request (use the one that works for you):

1. [Click here](https://invue.zendesk.com/hc/en-us/requests/new?ticket_form_id=360001497494) or copy and paste this link in a browser:
https://invue.zendesk.com/hc/en-us/requests/new?ticket_form_id=360001497494
2. Scan the QR code with your smartphone:



Once you have navigated to the form:

1. Enter the requested information and "Submit" the request
2. Look for a confirmation email and use that email going forward for all correspondence on the issue

Important: submit one request per issue.



Glossary

Term or Acronym	Definition
LIVE Access (LA)	System used by the customer to manage the environment (Users, Devices, etc.) and view results of Users' operations. <i>LIVE Access</i> was formerly known as <i>Access Manager</i> .
OneKEY	An InVue 'key' which is programmable from LIVE Access to enable authorized Users' to Operate Devices.
Device	Generic term used to describe InVue Smart Locks Operated using the OneKEY or the Mobile app.
IR4	InVue's new-generation ecosystem which introduced real-time data transfer from the OneKEY to the cloud.
OKM (IR4)	OneKEY Manager, part of the IR4 ecosystem. Required for checking in and checking out an IR4 OneKEY.
IR3	InVue's previous-generation ecosystem which boasted the ability to capture and record User's interactions with Devices using the IR3 OneKEY.
KAS (IR3)	Key Authorization Station, part of the IR3 ecosystem. Required for checking in and checking out an IR3 OneKEY.
User	Any human actor who interacts with the InVue products, such as Smart Locks, KAS or OKM, OneKEY or the Mobile App, etc.
Operate	Refers to actions, such as Lock and Unlock, performed on Devices by a User.
Auto-locking	Certain InVue Devices come with the capability to auto-lock about 10 seconds after the Device was unlocked by a User so that the User does not have to manually lock the Device. The Devices are considered 'auto-locking'.
Latch	An action performed by a User (such as pull/push, turn, or lift) to activate the Device's internal mechanism to enable the physical opening of secured furniture (eg. a door, cabinet, or drawer) after a Device has been unlocked.
Site	The physical business location where a Device is installed and Operated by an authorized User.
Corporate Hierarchy (CH)	This is the logical hierarchy in which the Sites are organized. The CH provides a way to filter (narrow down the search for) Sites. Example: a Site may roll up to a Region which rolls up to a District. Or, to see this from the top down: Districts break down into Regions and Regions break down into Sites. Labels for Region, Division, and Site are customizable to meet customer's needs.
SoR	System of Record where source data is saved for permanent record.
SSO	Single Sign On – an integration with the customer's authentication system which prevents the user from having to enter credentials each time to log in to the web portal or the mobile app.



Frequently Asked Questions and Helpful Tips

FAQ	Steps / Description / Helpful Tips	Media
<p>Trouble logging into the LIVE Access Web Portal</p>	<p>Check your Username and Password to ensure accuracy. User ID is not case-sensitive but be sure it is entered as provided.</p> <p>If you are still experiencing issues, contact your company's LIVE Access administrator to have your password reset.</p>	<p>None</p>
<p>Trouble logging into the LIVE Access Mobile App</p>	<p>Check your Username and Password to ensure accuracy. User ID is not case-sensitive but be sure it is entered as provided.</p> <p>If you are still experiencing issues, contact your company's LIVE Access administrator to have your password reset.</p>	<p>None</p>
<p>What smart devices are compatible with the LIVE Access mobile app?</p>	<p>Currently, the LIVE Access mobile app works on Android devices with Android OS 10 and above and on Apple devices with iOS 12 and above.</p>	<p>None</p>
<p>How do I download the LIVE Access mobile app?</p>	<p>The LIVE Access mobile app is available from the Google and Apple app stores. Search for "InVue LIVE Access".</p>	<p>None</p>
<p>What is the maximum number of Devices LIVE Access can handle?</p>	<p>Unlimited; there is no limit to the number of Devices that can be enrolled in LIVE Access.</p>	<p>None</p>
<p>What is the maximum number of Users LIVE Access can handle?</p>	<p>Unlimited; there is no limit to the number of Users that LIVE Access can handle.</p>	<p>None</p>
<p>What is the projected lifespan of the LIVE Lock? How many cycles? How does that translate to years of operation?</p>	<p>LIVE Locks have been designed and tested to achieve 50,000 open/close cycles, which equates to 28 cycles a day for 5 years. Based on data that InVue collected from our customers, 98% of cabinets/fixtures average 12 cycles a day.</p>	<p>None</p>
<p>How long should a fresh set of batteries last? How many cycles?</p>	<p>Batteries are designed to provide 2 years of operation based on a minimum of 12 open/close cycles a day.</p>	<p>None</p>
<p>Do you need the LIVE Access mobile app to operate a LIVE Lock?</p>	<p>LIVE Locks are designed to work optimally with a mobile/smart device. As such, if you plan to use a smart device to operate the locks, then yes, you need the LIVE Access mobile app. However, LIVE locks can also be operated with a OneKEY similar to other InVue Smart Locks.</p>	<p>None</p>



FAQ	Steps / Description / Helpful Tips	Media
Does the LIVE Access mobile app have the SDC like the OneKEY?	LIVE Locks do inherit the SDC from the OneKEY (just like normal SmartLocks) but the mobile app does not utilize the SDC. The mobile app communicates with the LIVE Lock using other proprietary technologies.	None
Is the 4-second unlock time configurable?	The 4-second unlock timer, known as the auto-relock window, will be configurable in LIVE Access. Admin users will be able to set this value between 3 and 30 seconds.	None
What types of LIVE Locks are available now? What do I need to install them?	LIVE Locks come in three body types: CAM, SLIDER and PLUNGER. Each lock requires its own adapter kit which will be available under a separate order code. Refer to the installation instructions for more details.	None
How do you enroll LIVE Locks in LIVE Access?	The enrollment process is very easy with LIVE Locks. Reference the User Manual for detailed installation instructions.	None
What kind of batteries are required with LIVE Locks?	LIVE Locks come with two cells already installed. For replacement, please replace with the batteryCR123A - commonly available in all regions.	None
What if someone opens the battery compartment and steals the batteries?	The battery compartment is secure and can only be opened with a tool provided by InVue. However, if the batteries are removed from the LIVE Lock, you can use an authorized OneKEY to unlock the LIVE Lock.	None
What happens if the batteries are completely drained or removed? Can I still operate the lock?	Yes. LIVE Locks can still operate with a OneKEY (leveraging the power transfer.	None
How can I check the battery level on each of the LIVE Locks?	The battery status of each LIVE Lock can be seen in real time in both the LIVE Access mobile app and the web app.	None
What is the threshold for the battery indicator changing from green to red?	Approximately 20%.	None
Do I have to select one of the LIVE Locks within range on the app before approaching to unlock it?	No, you simply walk up to the LIVE Lock you wish to open and tap your mobile device to the top of the lock.	None
Can you unlock multiple LIVE Locks in a row without locking the previous locks?	The behavior of the LIVE Lock with the mobile app is the same as it is with the OneKEY. The ability to restrict/allow a user from/to open multiple locks is managed by the "Restricted Mode" permission which can be set in the individual user's profile in the web app.	None



FAQ	Steps / Description / Helpful Tips	Media
Can another store associate lock a LIVE Lock that was left open by another associate? How will that show in LIVE Access?	LIVE Locks auto-lock in 4 seconds but they can be left unsecured (unlatched). If so, another associate can secure (latch) the lock at any time. LIVE Access (mobile and web app) will show the status of each lock through each state (locked & unlocked, secured and unsecured) in real time.	None
Is tapping my phone to the LIVE Lock the only option to unlock a LIVE Lock?	No, in addition to tapping, you can also leverage the 2D barcode printed on each lock, which is normally hidden by a plastic cap. Simply remove the plastic cap to expose the 2D barcode. You can now use the scanning functionality of a Zebra device or the camera on any mobile device. Also, remember that you can also use the OneKEY.	None
What happens if I lose connectivity with my mobile device? Can I still operate the LIVE locks?	In order to use the LIVE Access mobile app, the mobile device requires an internet connection (WIFI or LTE). So, if you lose complete internet access, the app will display a message informing you of the same and prevent you from operating a lock. You can however use a OneKEY to access the lock. Note that you can still check-out a key from the OneKEY manager even when the internet connection is interrupted.	None
Is it secure to use an app to access the LIVE Locks?	Yes. First, we use advanced encryption technology so that the LIVE Locks are only visible when using the LIVE Access mobile app. Second, you have the option to immediately deactivate a mobile app user via the LIVE Access web app in case of suspicious activity. Third, when interacting with a OneKEY, we continue to rely on InVue's proprietary IR communication protocol.	None
Can you remotely unlock a LIVE Lock?	Yes, but the ability to remotely unlock a LIVE Lock is only available by permission. Reference the User Manual for details on this functionality.	None
Can our customer integrate the LIVE Access functionality in their own app for their customers?	Not yet. The ability for our customers to integrate the LIVE Access functionality in their own software platforms will be available in 2022.	None
Is the LIVE Locks firmware upgradeable?	Yes, via the LIVE Access mobile app. Reference the User Manual for details.	None
How does Notifications work? How do I set up for myself?	Start by navigating to the USERS page in the Web Portal. Then, hover over your own User record – this should reveal the 3-dot context menu on the right edge of the record row. Select “Notifications” from the menu. Check out the video for this and remaining instructions.	< QR to video >
Can I setup Notifications for another user?	No, each User can only set up their own Notifications. You can, however, view the setup of other user's Notifications.	None
Can any user setup Notifications?	Only ADMIN type of users can set up Notifications.	None



FAQ	Steps / Description / Helpful Tips	Media
<p>What is the max number of transactions a OneKEY (any version) can store?</p>	<p>About 1600 audit records.</p> <p>To put it in perspective, on a 8-hr shift, a user would need to interact with a Pod every 18 seconds to reach that limit. A Pod only creates data exchange (no power transfer)</p> <p>If a user is only interacting with a smart lock (which involves both power exchange and data transfer), he/she would be limited to 350 powered presses anyway. And to reach that 350 powered press limit, the user would need to interact with a smart lock every 82 seconds on a 8-hr shift.</p>	<p>None</p>
<p>Cannot check out a OneKEY</p>	<p>What you see:</p> <ul style="list-style-type: none"> • Green light on front rapid flashing. <p>This indicates that the KAS is not able to communicate with the customer’s network (back-end) but network connection is active.</p> <p><u>Resolution:</u></p> <ul style="list-style-type: none"> • Ensure all cables are installed correctly. • Power Cycle the KAS. <p>Contact your internal IT Team and request that they check the data port to ensure connectivity and settings.</p>	
<p>Factory Reset an OKM</p>	<p>To fully reset the OKM to factory defaults:</p> <ul style="list-style-type: none"> • Select the sprocket icon on the main screen. • Follow the on-screen instruction to factory reset the OKM. <p>Note: you will need the OKM Enrollment PIN to access this feature.</p>	<p>None</p>
<p>Upgrade the Firmware of an OKM</p>	<p>Firmware updates happen automatically on the OKM when InVue publishes a update. Currently, customers do not have a way to opt-in or opt-out of the upgrade process.</p>	<p>None</p>
<p>What is the maximum number user/sales associate can OKM support?</p>	<ul style="list-style-type: none"> • The OKM can accommodate up to 2,000 users 	<p>None</p>
<p>What is the maximum number of Devices that an OKM can handle?</p>	<ul style="list-style-type: none"> • The OKM is designed to hold up to 2,000 assets. An asset is anything that shows up in LIVE Access as a device: smart lock, POD, etc... 	<p>None</p>



FAQ	Steps / Description / Helpful Tips	Media
<p>What is the maximum number of transactions an OKM can store when offline?</p>	<p>The OKM can store up to 60,000 key-transactions (records). The OKM has been designed to work with LIVE Access and would only operate off-line mode on exceptional basis. But if off-line, the OKM has been designed to keep an accurate log of last 2 weeks of transactions. That is a very conservative estimate as it assumes very heavy use.</p> <ul style="list-style-type: none"> As a side note, transaction size can vary greatly. It can be very low like “arm/disarm” of a POD, lock/unlock of a SML while other transactions can be more data-intensive such as key checking/checkout, user changes or asset changes. 	<p>None</p>
<p>What is the max number of OKMs that LIVE Access can support?</p>	<p>There is no set limit to number of OKMs connected to an LIVE Access instance. The limitation would come from the 2,000 assets or 2,000 users being linked to that site environment.</p>	<p>None</p>
<p>Is a Manager’s PIN related to a specific OKM or a store environment?</p>	<p>The manager PIN is related to the customer’s environment, ie. instance of LIVE Access. All OKMs for a given instance, operate with the same Manager PIN.</p>	<p>None</p>
<p>When you checkout/check-in a OneKEY LIVE, are those events transmitted through LoRa from the Key or from the OKM only?</p>	<p>Interactions with the LIVE OneKEY go directly to the cloud via the LoRA Gateway. When a OneKEY is checked in on a OKM, the data goes from the OKM to the cloud. A reconciliation occurs at the Cloud level eliminating all duplicates.</p>	<p>None</p>
<p>What is the maximum number of Devices that a KAS can handle?</p>	<ul style="list-style-type: none"> The OKM is designed to hold up to 2,000 assets. An asset is anything that shows up in LIVE Access as a device: smart lock, POD, etc... 	<p>None</p>
<p>Enrollment of a KAS fails, the green light is slow blinking</p>	<p>What you see:</p> <ul style="list-style-type: none"> Red light on top of KAS Green light is slow flashing. <p>A slow blinking green light indicates that the KAS is NOT connected to the customer’s network. This issue is most likely dealing with the Customer’s on-Site network.</p> <p><u>Resolution:</u></p> <ul style="list-style-type: none"> Ensure all cables are installed correctly and securely. Contact your internal IT Team and request that they check the data port to ensure connectivity and settings. If the connection appears clear on the customer’s end, try to install the back up unit to help rule out a potential hardware issue. 	<p>None</p>



FAQ	Steps / Description / Helpful Tips	Media
Factory Reset a KAS	<p>To fully reset the KAS to factory defaults:</p> <ul style="list-style-type: none"> • Unplug the KAS from both Power and Ethernet. • Hold down the *, CLR, Out buttons firmly and plug in the power cable. • The light on the top of the KAS will flash Red and Blue. • Once the light stops flashing, the KAS is factory reset. 	None
Upgrade the Firmware of a KAS	<p>Firmware upgrade is not possible in the KAS. If the KAS is not functioning as expected, initiate a return and replacement with InVue Customer Service.</p>	None
Enrollment fails, the KAS is not taking the KAS PIN	<p>What you see:</p> <ul style="list-style-type: none"> • Red light on top of KAS • Green light on front is rapid flashing. <p>This indicates that the KAS is not able to communicate with the customer's network (back-end) OR that the PIN used for enrollment is incorrect, or not being entered correctly.</p> <p><u>Resolution:</u></p> <ul style="list-style-type: none"> • Verify that the PIN being used is correct. • When entering the PIN, please work intentionally, firmly pressing each button (light on the top of the KAS will flash each time) allowing for a 1 second pause between digits. • Allow for the KAS to sit, fully installed for 10 minutes, and try again. • Power cycle the KAS and try again. • Factory reset the KAS (see separate FAQ) • Attempt the installation on the back up unit to help rule out a potential hardware issue. • Contact your internal IT Team and request that they check the data port to ensure connectivity and settings. • If the issue persists, call InVue for more assistance. 	



FAQ	Steps / Description / Helpful Tips	Media
<p>The OneKEY makes an error sound (NAK NAK) when placed on the KAS</p>	<p>What you see:</p> <ul style="list-style-type: none"> • Red light on top of KAS • Green light is solid on the front. <p>This indicates that the KAS is not able to communicate with the customer’s network (back-end) OR that the KAS has not been assigned to the Customer’s LIVE Access environment.</p> <p><u>Resolution:</u></p> <ul style="list-style-type: none"> • Follow directions for enrolling the KAS into the LIVE Access Customer environment per the LIVE Access installation guide. Call InVue for more assistance. • Allow for the KAS to sit, fully installed for 10 minutes, and try again. 	<p>None</p>
<p>Is it possible to connect the KAS or OKM to the LoRa Gateway with an ethernet cable so the KAS or OKM has network connection through the gateway?</p>	<p>No, because the LoRa Gateway does not have a LAN Ethernet port. The Ethernet port on the LoRa Gateway is a WAN port for connecting the gateway to the Internet. To connect a KAS or OKM to internet using a LoRa Gateway, you must fit a WiFi dongle on the KAS or OKM and connect it wirelessly (via WiFi) to the gateway.</p>	<p>None</p>
<p>Is it possible to connect the KAS or OKM to an LTE Router with an ethernet cable so the KAS or OKM has network connection through the router?</p>	<p>Yes, as long as the LTE Router has a LAN port into which the KAS or OKM can be connected for access to the internet.</p>	<p>None</p>



LIVE Access Web Portal

About LIVE Access

LIVE Access is a system (application) for managing access to merchandise that is secured by an InVue Smart Lock (“Devices”). LIVE Access does this by allowing you to create Zones, which are logical groups of Devices, and Roles, which are logical groups of Zones, and assigning these Roles to Users; thereby granting permission to Users to Operate (lock or unlock) Devices. View <https://invue.com/software-analytics/live-access.cfm> to learn more.

Pro vs. Lite

LIVE Access is available in two configurations: **Pro** and **Lite**. Below is a brief description of available functions of each.

Pro

Pro is available with a paid license and offers the full functionality as described in this manual.

The **Pro** version has the following functionality:

- Audit log to view real-time activity
- Dashboard to view historical trends
- Export historical data
- View the Site Report
- Unlimited Roles
- Unlimited Zones
- Unlimited Users (ADMIN and USER)
- Unlimited Sites
- Enroll unlimited KAS/OKM and register unlimited Devices

Lite

Lite is a limited functionality version. **Lite** is typically offered as a starter system for a 6-month period only, after which, the customer is expected to convert to **Pro**; exceptions are provided by special approval.

The **Lite** version has the following restrictions:

- Audit log to view real-time activity
- Dashboard is not visible, no access
- Cannot export data



- Cannot view the Site Report
- Limited to one (1) Role, which is set by the system administrator
- Limited to one (1) Zone, which is set by the system administrator
- Limited to one (1) ADMIN user per Site
- Limited to one (1) USER user per Site
- No restriction on number of Sites, KAS/OKM, and Devices



Overview of the Web Portal, functionality

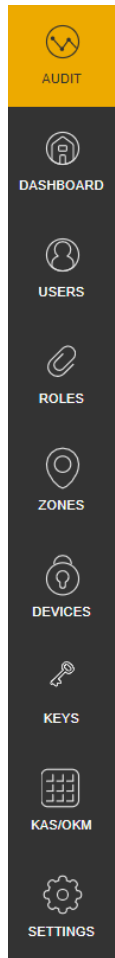
- The application allows the User to manage the environment and view data in real time.
- **The application menu** comprises of the following:
 - ✓ 3-DOT menu (⋮) on top-right of the screen offers: Logout, this User Manual, and Language selection.
 - ✓ AUDIT: view transactions in real-time. This is the default view when you first sign in.
 - ✓ DASHBOARD: view data of the operational KPIs in a graphical format.
 - ✓ USERS: show registered Users and allow management of each.
 - ✓ ROLES: allow configuration of permissions to each User.
 - ✓ ZONES: allow grouping of Devices which can then be assigned to Roles.
 - ✓ DEVICES: show registered Devices and allow management of each.
 - ✓ KEYS: view the status of all keys checked out.
 - ✓ KAS/OKM: show registered KASs and/or OKMs and allow management of each.
 - ✓ SETTINGS: configure settings applicable to the enterprise/company.
- **Note**: a User’s permissions dictate which menu items are visible.

Configure the environment in the following order to avoid having to jump around:

1. SETTINGS ← start here
2. set up ZONES
3. set up ROLES
4. then, for each Site (business location):
 1. enroll each KAS/OKM and activate at least one OneKEY
 2. enroll DEVICES, and finally
 3. associate Devices → ZONES → ROLES → USERS
5. Finally, see activity on the DASHBOARD and AUDIT pages



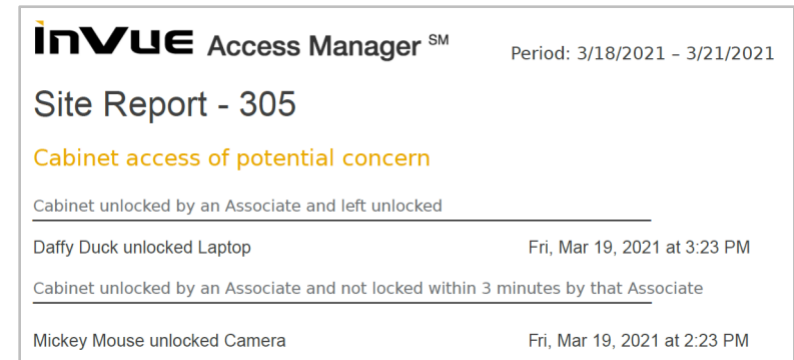
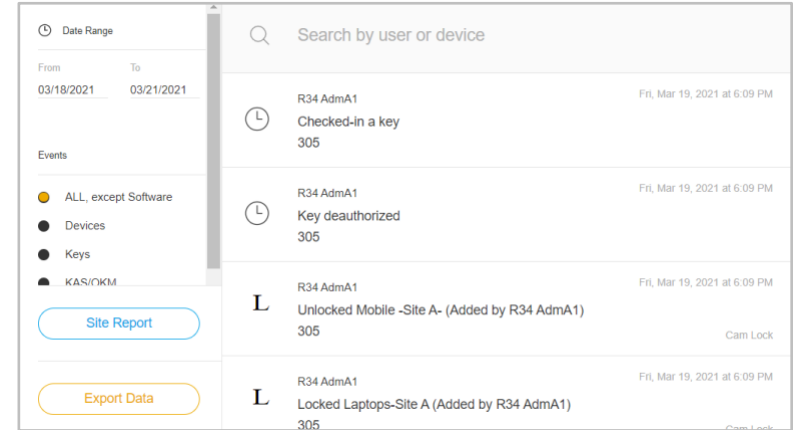
Each step (menu item) is explained in detail on the following pages, in menu order.





Audit

- **About:** displays the history of activities such as key check-outs and check-ins, all interactions with InVue Devices, and any changes made within the software, provides a way to export the data for independent analysis, and provides access to the Manager’s report.
- **Functionality:**
 - ✓ Select a filter (including date and CH) to control the category of information displayed.
 - ✓ **Site Report:**
 - This option is only visible when the signed-in User has selected a Site from the Site picker (button in the header of the page on the top-right of the screen).
 - The report is an easy-to-digest collection of potentially concerning activity from the selected Site. Admin Users who have not been assigned to a Site must first select a Site.
 - This report is specific to a Site and shows a detail account of the following:
 - Cabinet access of potential concern:
 - Cabinet unlocked by a User and left unlocked
 - Cabinet unlocked by a User and not locked within 3 minutes by the same User
 - Unauthorized attempts:
 - Attempt to access a Device that is not included in the User's profile
 - Key activity of potential concern:
 - User that has more than one active key
 - User that did not check in their key within 1 hour after their shift ended
 - Disarm of a POD that was not alarming
 - ✓ **Data Export:**
 - Export data for the selected date range and KPI. Data is exported in CSV format.
- **Noteworthy:**
 - ✓ This page shows both User interactions with Devices, Keys, KAS/OKM, and Software in a chronological order; the most recent transaction is on top.

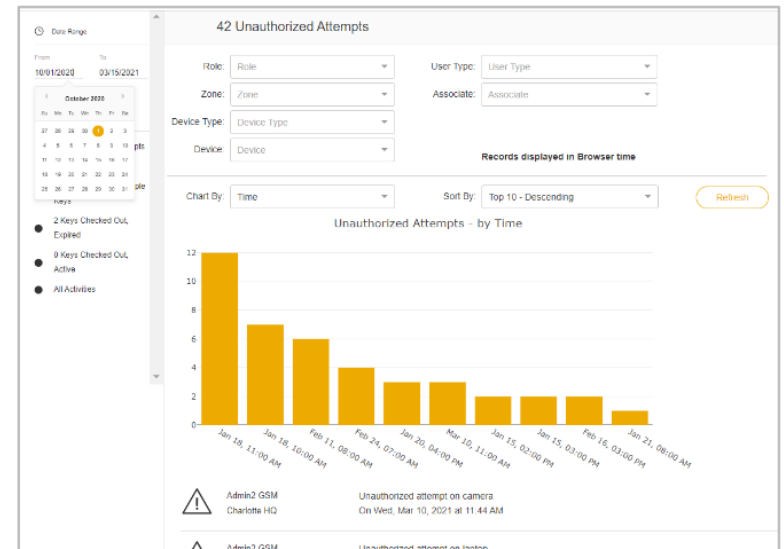




- ✓ For Users of the IR3 OneKEY: records of User’s interactions are displayed after the Keys are checked in.
- ✓ For Users of the IR4 Batch OneKEY: records of User’s interactions are displayed after the Keys are checked in.
- ✓ For Users of the IR4 LIVE OneKEY: records of User’s interactions are displayed in near-real-time.

Dashboard

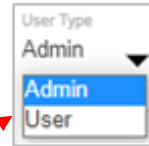
- **About:** an interactive reporting tool to view current and historical data.
- **Functionality:**
 - ✓ View historical data for various KPIs in a graphical and tabular form.
 - ✓ Select the KPI then select one or more filters (date range, roles, zones, devices, etc.) then select how you want to display the graph.
- **Noteworthy:**
 - ✓ To download the data so that you can conduct the analysis in your own BI tool, see the *Audit* page.





Users

- **About:** a User is any person (human resource) who is configured to register and/or Operate a Device.
- **Functionality:**
 - ✓ Manage Users (select type of User, view details, define and/or change data, delete, disable access w/o deleting, or assign to Role(s)).
 - ✓ There are two types of User accounts: ADMIN and USER (see image on right).
 - ✓ Each User's access to data and assets (users, devices, keys, okm, etc.) is governed by their assignment to a Site or any part of the Corporate Hierarchy (CH, for example *Region, Division, or Site*).
 - ✓ Context Menu: move the mouse over the record to reveal the 3-dot context menu on the right side of the row. This menu contains the following options:
 - *Audit*: select to see the audit trail of activity performed by the selected User.
 - *Notifications*: select to set up your own notifications or view other users' set up of notifications. You can only enable/disable and modify your own notifications.
 - *Delete*: select to delete the record.
 - ✓ Pro Tip: you can narrow the list of Available Roles by entering search criteria.



New User ✕

User Type User ▼	Account Enabled Yes ▼
First Name	Key/App Session (hours) 8 ▼
Middle/Friendly Name	Restricted Mode Yes ▼
Last Name	Enroll KAS/OKM/Device No
Employee ID	Manage Devices No ▼
PIN *****	Remote Operation No ▼
Level of Access No Site Selected Select Level of Access	

Search available roles

Available Roles	Selected Roles
<div style="display: flex; align-items: center;"> <div> <p style="margin: 0;">Test User</p> </div> <div style="margin-left: auto; border: 1px solid gray; padding: 5px;"> <ul style="list-style-type: none"> <li style="padding: 5px; margin-bottom: 5px;">Audit <li style="padding: 5px; margin-bottom: 5px;">Notifications <li style="padding: 5px;">Delete </div> </div>	

Context Menu

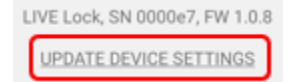
- **Noteworthy:**
 - ✓ A User must be assigned to one or more Roles.
 - ✓ A User can only be assigned to a Role, not to a Zone or a Device.
 - ✓ There is no limit to the number of Users which can be registered in a system.
 - ✓ Each User Type's Permissions are explained in the **Permission Matrix table**.
 - ✓ **Pro Tip:** record the PIN of every User that is entered into the system in a safe and secure location. If a PIN is forgotten and/or not recorded, generate a new one by selecting the User and clicking *Reset PIN*. An Admin User can choose to "Export Users" which shows the currently assigned PIN for each User, along with other relevant data.
- **Types of User Accounts:**
 - ✓ User Type: **ADMIN**
 - An **ADMIN** user is the highest authority User in the system.
 - An ADMIN type of user can log in to the Web Portal and operate Devices using the OneKEY and/or the Mobile App.



- To create this user, select User Type = ADMIN. When you select “Save”, you will be prompted to create a separate account for signing in to LIVE Access (enter a User ID and password).
- ✓ **User Type: USER (aka. Operator or PIN User)**
 - This type of User is intended for associates whose only function is to operate InVue Devices (Smart and LIVE Locks). For example, access a cabinet fitted with an InVue Device (lock) that is securing high-value merchandise or critical equipment.
 - To create this user, select User Type = USER.
 - A USER type of user can not log in to the Web Portal; they can only operate Devices using the OneKEY and/or the Mobile App.
 - This User type should always be assigned to the CH (cannot be a Global user); however, they can be created with a *Region* or *Division* assignment; that is, without a specific *Site* assignment.
- **User Permissions:** within a user’s profile or when creating a new user, several permission levels exist:
 - ✓ **Account Enabled:** Controls a user’s ability to access authorized assets
 - If YES is selected, the user will have immediate access to the Devices that are associated with the Roles you select. A user can:
 - Login to the Web Portal (ADMIN user type ONLY – refer to the permission matrix below)
 - Login to the Mobile App
 - Check OUT a OneKEY
 - If NO is selected, the user will not be able to access any Devices until this drop down is enabled.
 - If this permission is changed to NO while the user is logged in to either the web portal OR mobile App OR has a OneKEY checked out, the following will occur:
 - Web Portal: An ADMIN user’s current session will continue but after logging off the web portal, they will not be able to login again.
 - Mobile App: The user’s session will end (will be logged out) within 15 seconds.
 - OneKEY checked out:
 - BATCH OneKEY: A user’s current session will continue but after checking IN the key (returning to OKM/KAS), they will not be able to check OUT a key again until the Account Enabled permission = YES.
 - LoRa/LIVE OneKEY: user’s current session will be terminated after the next key interaction, and they will not be able to check OUT a key again until the Account Enabled permission = YES.
 - ✓ **Key/App Session (hours):** Controls the number of hours a OneKEY will remain active after it is checked (typically, this can be the length of the user’s shift).
 - Note, a OneKEY will remain active until checked IN or the key/app session time has been reached.



- ✓ **Restricted Mode:** Users are prohibited from operating more than one lock at a time.
 - If YES is selected, a user will not be able to operate a second lock until the prior lock is LOCKED.
 - If using a OneKEY, an audible reminder (continuous beeps), will alert the user
 - If using the mobile app, a user will not be allowed to exit the Unsecured screen of the first lock (lock that is left unsecured).
 - If NO is selected, restricted mode is not activated, and a user may operate more than one lock at a time.
 - Note, this setting can be set at the enterprise level; it can be further customized per user (on the USERS page).
- ✓ **Enroll KAS/OKM/Device:** An ADMIN user's ability to enroll KAS/OKM or Devices using the mobile App
 - If YES is selected, an ADMIN user can:
 - Have visibility to the KAS/OKM page on the web portal that allows them to administer new and existing KAS/OKM's.
 - See the Enroll Devices menu option on the mobile app, which allows ADMIN user's to enroll LIVE Locks in bulk.
 - Enroll a single device on the mobile app by using NFC or the mobile app Camera ONLY IF the device is new to the environment.
 - See the Firmware Update (FW) menu option on the mobile app, which allows ADMIN user's to update the FW of LIVE Locks in bulk.
 - Update FW of a single device from the Secured page by clicking on the FW version (which will be linked).
 - If NO is selected, a user cannot:
 - Administer new and existing KAS/OKM's in the web portal
 - Enroll LIVE Locks on the mobile app
 - Administer FW updates to LIVE Locks
 - If NO is selected AND IF Manage Devices AND Remote Operation are also NO, a user will not be able to open the '# in range, # authorized' view in the mobile app (a.k.a. Authorized Devices/AD List).
- ✓ **Manage Devices:** This gives a user the ability to name or rename the Device, view details, or assign the Device to a Zone.
 - If YES is selected:
 - User will be able to open the AD List on the mobile app and see list of all Devices they have access to.
 - This includes LIVE Locks as well as Smart Locks.
 - User will be able to select a Device from the AD List on the mobile app; this will display the Secured screen with the Update Device Settings link.
 - LIVE Locks only
 - User will be able to update the Device Name, Description, and assigned Zone of a single Device by clicking on the Update Device Settings link in the mobile app.
 - LIVE Locks only
 - If NO is selected:
 - The "# authorized and in range" on the mobile app will represent only the # of LIVE Locks the user is authorized to access based on roles assigned to the user (will not show all LIVE Locks within range).





- If NO is selected AND if Enroll KAS/OKM/Device and Remote Operation are also NO, User will not be able to open the “# in range, # authorized” view (a.k.a. Authorized Devices/AD List). This will be greyed out.
- ✓ **Remote Operation:** Controls a user’s ability to unlock a Device without scanning with NFC or Camera and to turn their phone into a remote bridge.
 - If YES is selected:
 - A user will be able to select a Device from the AD List on the mobile app and will be allowed/able to unlock the selected LIVE Lock without scanning via NFC or Camera as long as they are within BLE range of the selected LIVE Lock.
 - A USER, user type will see the Remote Bridge menu option on the mobile app. Selecting this menu option will open a Remote Bridge, thus turning the user’s mobile device/phone into a remote bridge utilizing internal BLE.
 - An ADMIN user type will be able to remotely unlock a LIVE Lock from the DEVICES page.
 - If NO is selected:
 - An ADMIN user type will not be able to remotely unlock a LIVE Lock from the DEVICES page.
- If NO is selected AND if Enroll KAS/OKM/Device ad Manage Devices are also NO, User will not be able to open the “# in range, # authorized” view (a.k.a. Authorized Devices/AD List). This will be greyed out.

• **Permission Matrix: permissions by type of installation (PRO or LITE) for each User Type are explained in the following table.**

✓ A User can be one of two "levels":

- **Global:** a user who is not assigned to a level of the CH (Region, Division, or Site). Level of Access = “No Site Selected”.
 - Only ADMIN users can be configured as **Global**.
- **Non-Global:** a user who is assigned to a level of the CH (Region, Division, or Site). Level of Access = specifies a level, including down to a Site.



ACCOUNT PERMISSIONS - what the user can do: ['Yes' = full functionality 'read only' = page will be visible but non-editable 'Hide' = the function will be hidden; applies to menu button and the page]						
Permission	User Type >	ADMIN (PRO) - global user -	ADMIN (PRO) - non-global user -	USER (PRO) - non-global user -	ADMIN (LITE) - site user -	USER (LITE) - non-global user -
Allow Global access (no CH selected)		Yes	No	No	No	No
OneKEY Check Out		Yes	Yes	Yes	Yes	Yes
Mobile App Log In		Yes	Yes	Yes	No	No
Web Portal Log In		Yes	Yes	No	Yes	No
AUDIT, view page		Yes	Yes	n/a	Yes	n/a
View Transactions		Yes	Yes	n/a	Yes	n/a
Site Report (a Site must be selected)		Yes	Yes	n/a	Hidden	n/a
Export		Yes	Yes	n/a	Hidden	n/a
DASHBOARD, view page		Yes	Yes	n/a	Hidden	n/a
USERS, view page (see below for details)		Yes	Yes	n/a	Yes	n/a

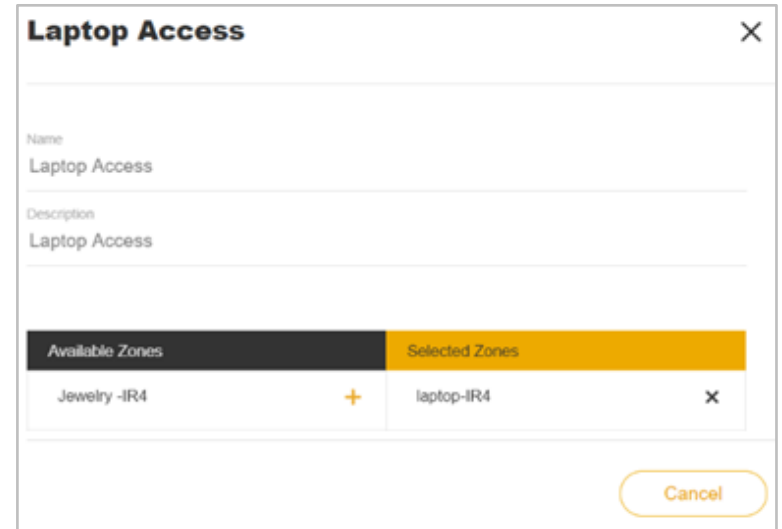


ACCOUNT PERMISSIONS - what the user can do: ['Yes' = full functionality 'read only' = page will be visible but non-editable 'Hide' = the function will be hidden; applies to menu button and the page]						
Permission	User Type >	ADMIN (PRO) - global user -	ADMIN (PRO) - non-global user -	USER (PRO) - non-global user -	ADMIN (LITE) - site user -	USER (LITE) - non-global user -
User Types that can be managed		ALL	ALL	n/a	Admin and User	n/a
Add User		Yes	Yes	n/a	Hidden	n/a
Edit User		Yes	Yes	n/a	Reset PIN only	n/a
Delete User		Yes	Yes	n/a	Hidden	n/a
Assign Level of Access (LoA)		same or lesser than own	same or lesser than own	n/a	read only	n/a
Assign Permissions		same or lesser than own	same or lesser than own	n/a	read only	n/a
Update own information		PIN & Password	PIN & Password	n/a	PIN & Password	n/a
Import/Export		Yes	Yes	n/a	Hidden	n/a
Configure Notifications		Yes, own	Yes, own	n/a	No	n/a
ROLES , view page		Yes	Yes	n/a	Hidden	n/a
Add/Edit/Delete/Import		Yes	No	n/a	Hidden	n/a
ZONES , view page		Yes	Yes	n/a	Hidden	n/a
Add/Edit/Delete/Import		Yes	No	n/a	Hidden	n/a
DEVICES , view page (see below for details)		Yes	Yes	n/a	Yes	n/a
Add/Delete/Disable/Remote Unlock		Yes	Yes	n/a	Yes	n/a
Edit		Yes	Yes	n/a	Yes	n/a
KEYS , view page		Yes	Yes	n/a	Yes	n/a
Delete		Yes	Yes	n/a	Yes	n/a
Deactivate		Yes	Yes	n/a	Yes	n/a
KAS/OKM , view page		Yes	Yes	n/a	Yes	n/a
Add/Delete/Connect/Disconnect		Yes	Yes	n/a	Yes	n/a
Edit/Connect/Disconnect		Yes	Yes	n/a	Yes	n/a
SETTINGS , view page		Yes	Hidden	n/a	Hidden	n/a
Restricted Mode (default = Yes)		Yes	Hidden	n/a	Hidden	n/a
PIN Length (default = 5)		Yes	Hidden	n/a	Hidden	n/a
Automatic Logout (default = 4 hours)		Yes	Hidden	n/a	Hidden	n/a
Firmware update Management		Yes	Hidden	n/a	Hidden	n/a
Customer Profile		Yes	Hidden	n/a	Hidden	n/a
Upload Corp. Hierarchy – Non-SaaS		Yes	Hidden	n/a	Hidden	n/a
Upload Corp. Hierarchy – SaaS		Hidden	Hidden	n/a	Hidden	n/a



Roles

- **About:** a Role specifies the User permissions, or access to locks assigned to various Zones.
- **Functionality:**
 - ✓ Manage Roles (name or rename the Role, view details, or delete).
 - ✓ Add Roles in bulk by uploading an Excel workbook.
 - ✓ Manage the Role-Zone relationship.
 - ✓ Context Menu: move the mouse over the record to reveal the 3-dot context menu on the right side of the row. This menu contains the following options:
 - *Duplicate*: select to create a clone of the selected Role.
 - *Delete*: select to delete the record.
- **Noteworthy:**
 - ✓ Roles are common across the company; not Site-specific so you will always see all Roles.
 - ✓ A good practice is to not change or delete a Role which you did not create as it may adversely affect other Users.
 - ✓ It is possible to give access to an entire enterprise using one (1) Role by selecting every Zone; however, this is not recommended due to the loss of granular access control and resulting data which can help to optimize operations.
 - ✓ The *New Devices Zone* comes preinstalled and cannot be deleted. It works as a collection point for any newly registered, unassigned Devices and should be assigned to the Site Manager.
 - ✓ There is no limit to the number of Roles which can be created.
 - ✓ There is no limit to the number of Zones which can be assigned to a Role.
 - ✓ At least one Role is required.





Zones

- **About:** a Zone is a logical grouping of Devices, grouped for the purpose of managing Users’ permissions.
- **Functionality:**
 - ✓ Manage Zones (name or rename the Zone, view details, or delete).
 - ✓ Add Zones in bulk by uploading an Excel workbook.
 - ✓ The number in parenthesis at the end of the Zone name indicates the number of Devices in the selected Site that are associated with the Zone. **IMPORTANT:** zero (0) Devices does not mean that the Zone has no Devices associated with it; it could be that there are Devices in that Zone that are associated with other Sites which you do not have visibility to.
 - ✓ Devices associated with the selected Zone are displayed on the Zone details page (visible when you select a Zone).
 - ✓ Context Menu: move the mouse over the record to reveal the 3-dot context menu on the right side of the row. This menu appears only if the Zone has 1 or more Devices associated, it contains the following options:
 - *Delete:* select to delete the record.
- **Noteworthy:**
 - ✓ Zones are common across the company; not Site-specific so you will always see all Zones.
 - ✓ A good practice is to not change a Zone which you did not create as it may adversely affect other Users.
 - ✓ A Zone can be deleted only if zero (0) Devices are associated with it. While the system allows you to delete a Zone which shows zero (0) Devices – even fir there are non-visible Devices associated to it, once you select to “delete”, a message will appear informing that the Zone cannot be deleted because there may be other Devices associated which you do not have access to.
 - ✓ There is no limit to the number of Zones which can be created.
 - ✓ There is no limit to the number of Devices which can be assigned to a Zone.
 - ✓ At least one Zone is required.

Low Security ✕

Name
Low Security

Description

Registered Devices

- Display Camlock (Site: 313)
- Display L410 (Site: 313)
- Display L430 (Site: 313)
- Display L440 (Site: 313)
- Display Padlock (Site: 201)
- Door handle (Site: 201)

Test Zone

Context Menu

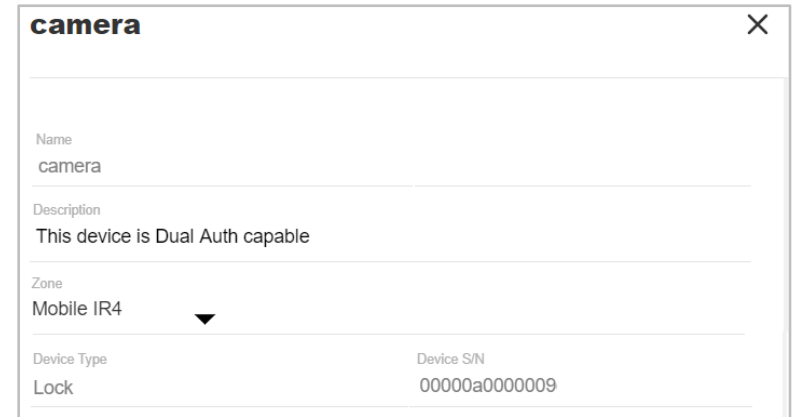
Delete

⋮



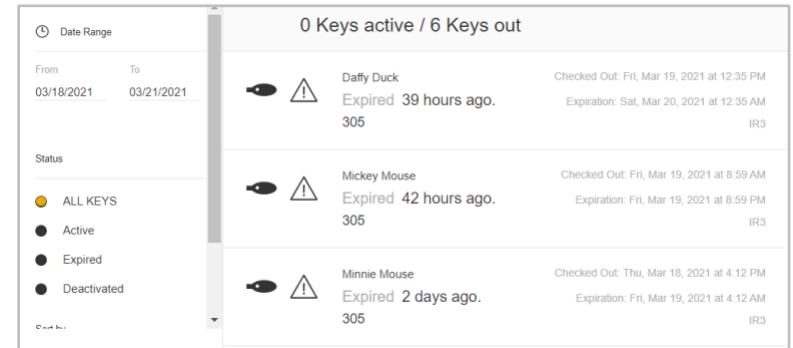
Devices

- **About:** a Device is any InVue mechanism which can be Operated with a OneKEY or the Mobile App, such as a Cam Lock, Smart Lock, or Package Protection.
- **Functionality:**
 - ✓ Devices appear on this page automatically once they have been successfully registered using a OneKEY or the Mobile App.
 - ✓ Manage Devices (name or rename the Device, view details, or delete).
 - ✓ Manage the Device-Zone relationship.
 - ✓ Context Menu: move the mouse over the record to reveal the 3-dot context menu on the right side of the row. This menu contains the following options:
 - *Audit*: select to see the audit trail of users' activity performed with the selected Device.
 - *Delete*: select to delete the record.
- **Noteworthy:**
 - ✓ A Device can be assigned to only one (1) Zone.
 - ✓ A device can only be assigned to a Zone, not to a Role or a User.
 - ✓ There is no limit to the number of Devices which can be registered in a system.





Keys

- **About:** a Key is any InVue mechanism which can be used to Operate a Device, typically, this is a OneKEY.
- **Functionality:**
 - ✓ For active IR3 OneKEY: displays Keys which have been checked out but not yet checked in or expired
 - ✓ For active IR4 Batch OneKEY: displays Keys which have been checked out but not yet checked in or expired
 - ✓ For active IR4 LIVE OneKEY: displays Keys which have been checked out but not yet checked in, expired, or deauthorized

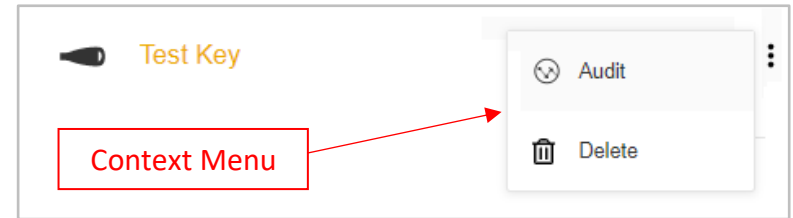




✓ For deauthorized IR4 LIVE OneKEY: displays Keys which have been checked out and deauthorized. A broken key icon  is displayed next to the Key icon . An Admin User can Deauthorize the key such that it ceases to allow operations.

✓ **Context Menu:** move the mouse over the record to reveal the 3-dot context menu on the right side of the row. This menu contains the following options:

- *Audit:* select to see the audit trail of activity performed by the selected Device.
- *Deactivate:* option is visible only if the OneKEY is a LIVE/LoRa key and the key is active (not expired or checked in). Select to remotely deactivate the selected LIVE/LoRa OneKEY.
- *Delete:* select to delete the record.




• **Noteworthy:**

- ✓ This page shows the number of keys that are currently active in the Site, as well as the total number of keys that are currently checked out. The list reflects only keys that are currently checked out, whether they be active or expired. When a key is checked back in to the system, the entry is removed from the list.
- ✓ With this information, the Administrator can see which employees currently have a key checked out and which employees, if any, have checked out more than one key. It also displays the check-out time and expiration time, when the key will deauthorize itself.
- ✓ Keys expire at the end of an employee’s shift. If a Key is not returned, or checked in to the system, then it will appear in this log as Expired, giving a Manager the opportunity to follow up with the employee on the location of the expired key. If a key is not checked in within one hour after a shift has ended, then the event is recorded in the Manager’s Report to aid in training.
- ✓ There is no limit to the number of Keys which can be registered in a system.
- ✓ Unlike other assets, a OneKEY cannot be named.

KAS/OKM

• **About:**

- ✓ a KAS, or Key Authorization Station, is an InVue device which is used to authorize the use of an IR3 OneKEY. An IR4 OneKEY will not work with the KAS.
 -  is the icon for a KAS.
- ✓ an OKM, or OneKEY Manager, is an InVue device which is used to authorize the use of an IR4 OneKEY. An IR3 OneKEY will not work with the OKM.



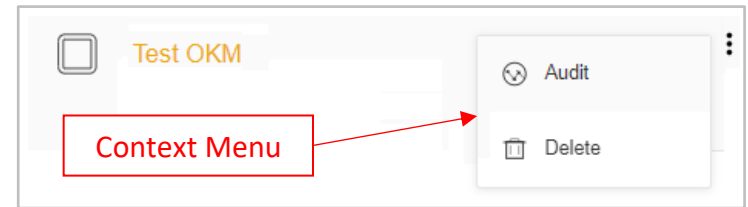
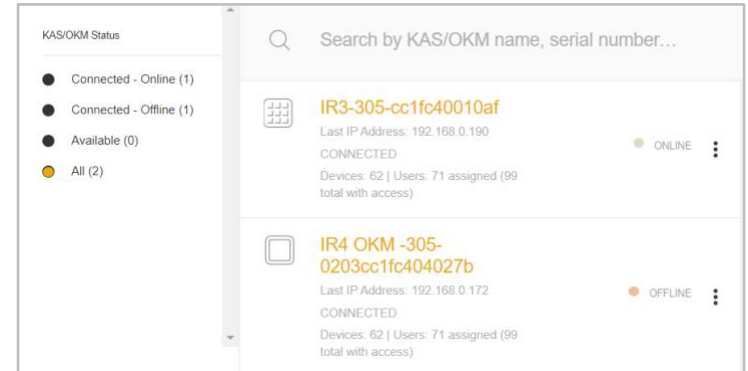
-  is the icon for an OKM.

• **Functionality:**

- ✓ Displays all KAS or OKM registered in the system.
- ✓ Manage KAS or OKM (name or rename the device, view details, or delete).
- ✓ For KAS and OKM functionality, see the appropriate section under *InVue Products*.
- ✓ Context Menu: move the mouse over the record to reveal the 3-dot context menu on the right side of the row. This menu contains the following options:
 - *Audit*: select to see the audit trail of activity performed by the selected KAS or OKM.
 - *Delete*: select to delete the record.

• **Noteworthy:**

- ✓ There is no limit to the number of KAS or OKM which can be registered in a system.
- ✓ In order to use a OneKEY to Operate a Device, at least one KAS or OKM is required.





Settings

- **About:** Choices made here apply to the environment; as such, you may find it helpful to set these preferences before continuing with the setup of all other areas.
- **Functionality:** you can manage the following parameters:
 - ✓ **Restricted Mode:**
 - This feature is especially useful for new Users who are learning the system.
 - Business Rule: Enables the ability to provide an audible reminder when a lock is left UNLOCKED and restricts a User of the key from operating a second lock until the prior lock is LOCKED.
 - Activate for All New Users: enables the Rule by default for new Users created from the time this setting is set or changed. This setting can be further customized per User (on the USERS page).
 - Volume: select between *Low* and *High* at which the key makes an audible sound. For example, select a “High” setting if the work environment is loud so that the User can hear the audible alert.
 - Delay: specify how many seconds after the Rule is violated before the audible alarm is activated in the key. “0” (zero) seconds = no delay.
 - Duration: specify how long the audible alarm should sounds.

Restricted Mode ✕

Restricted Mode (1) enables the ability to provide an audible reminder when a lock is left UNLOCKED and (2) restricts a user of the key from operating a second lock until the prior lock is LOCKED. This setting is at the enterprise level; it can be further customized per user (on the USERS page). "Activate for All New Users" enables the audible alert by default when creating a new user.

Enable Restricted Mode

Activate for All New Users

Volume **HIGH** LOW

Delay **0s** 30s 60s 2m

Duration **30s** 60s 2m 4m

Cancel



✓ **PIN Length:**

- Change the length of PINs used to check out a OneKEY using the KAS or OKM.
- PIN length: can be from 5 to 8 digits and applies to all new Users created from the time the PIN length is set or changed.
- It is a good idea to set your preferred default for the PIN length before entering all of the Users for your Sites.
- PIN Length can be changed any time. If you decide later to change the PIN length, existing PINs will continue to work, but all new PINs issued will follow the new setting. For example, if a Site’s PIN length is set to 5-digit and it is changed to 7-digit, existing Users will be able to continue using their existing 5-digit PINs while all new Users and Users with newly reissued PINs will receive a 7-digit PIN.
- In an IR3/IR4 hybrid environment, a User’s PIN works with both the IR3 and the IR4 key.

✓ **Automatic Logout:**

- Change the amount of time the User who is signed in to the Web Portal (LIVE Access) may be idle before being automatically logged out of the application.

✓ **Customer Profile:**

- Shows the settings for the customer’s environment, including:
 - Customer Name, Customer logo, Customer ID (used to log in to the Mobile App), KAS/OKM Enrollment PIN, and KAS/OKM TCP Port.

• **Noteworthy:**

- ✓ This SETTINGS menu item is only visible to Admin Users who do not have a Site assigned.

PIN Length ✕

Change the length of PINs used to check out Access Manager Keys from the Key Authorization Station. Unique PINs are randomly generated by the Operations Manager.

PIN Length

Cancel

Automatic Logout ✕

Change the amount of time the user may be idle before being automatically logged out of the application.

Idle Auto-logout Time

3m	5m	10m	15m	30m
1h	2h	4h	6h	Never

Cancel



LIVE Access Mobile App

About the App

The mobile app is available in both Android and iOS but with the following differences:

- Android app:
 - ✓ Supported version: 2.3.0 and newer
 - ✓ Available functionality: allows user to operate Devices, Enroll Devices, Name and re-Zone Devices, update Firmware of LIVE Locks, Remote Operation, and supports SSO (Single-Sign-On).
- iOS app:
 - ✓ Supported version: 1.0.1 and newer
 - ✓ Available functionality: only allows user to operate Devices (does not support any other functions which are listed above under Android).

Installing the App

- The app can be installed from the respective app store (Google Play or Apple).
- Search for “InVue LIVE Access”



Supported Mobile Platforms



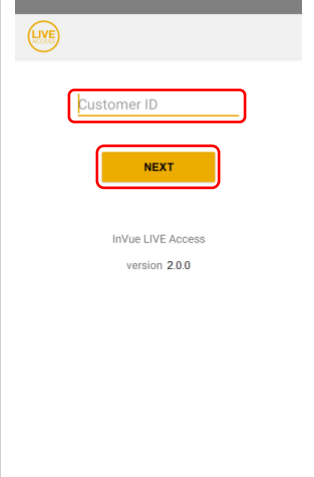

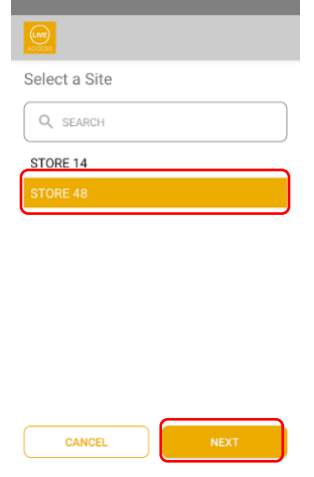
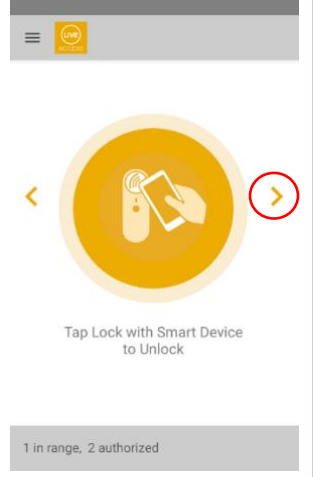
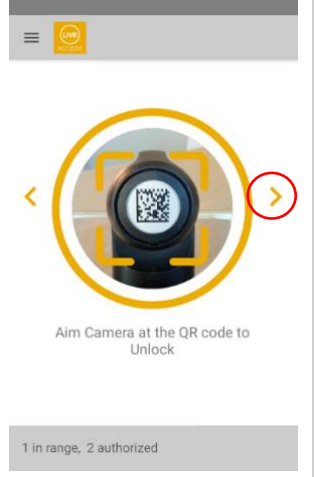
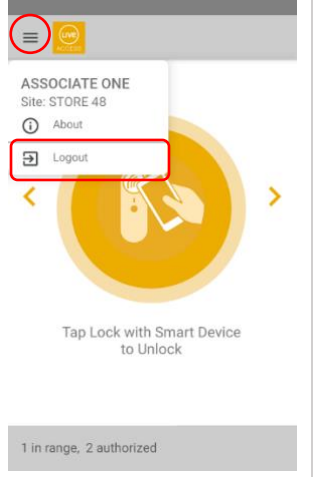
Android 10 and above (avoid low-cost devices)



iOS 12 and above | iPhone 8 and above

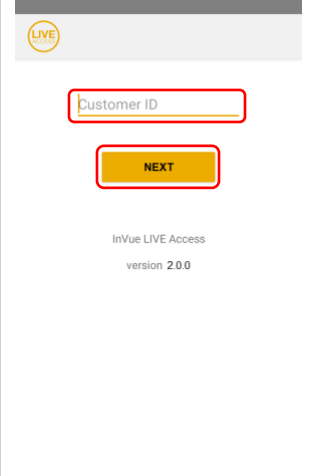
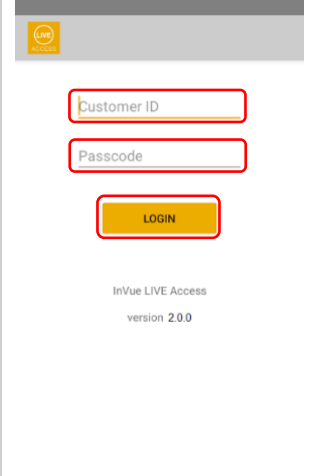
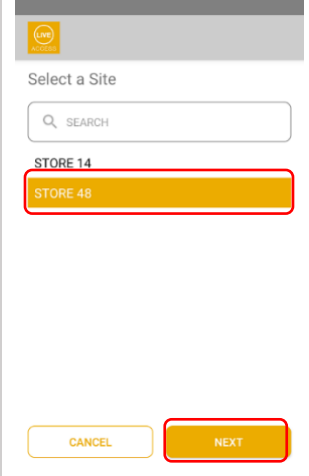
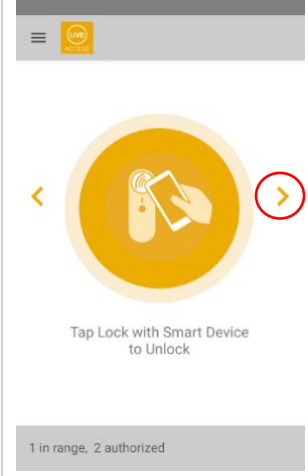
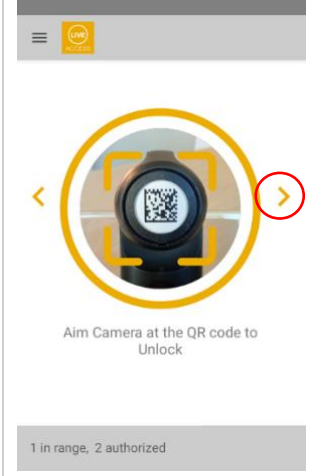
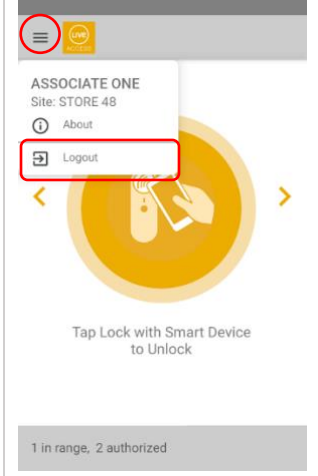


Login with Single Sign On (SSO) → Home Screen → Logout (Android)

Login	Continue Login with SSO	Select a Site	NFC Scan (aka: Home Screen)	2D Barcode Scan	Logout
					
<p><i>Customer ID</i> is unique to the environment/customer; this will be provided by InVue.</p> <p>Select <i>NEXT</i> to enter further credentials. System will check if the customer is configured for SSO (Single Sign On).</p>	<p>If SSO is configured, user will see a page similar to this – a custom SSO login page.</p> <p>This page is customer-specific so the look and function of the page will be different for each customer.</p> <p>Enter the required credentials and Sign In.</p>	<p>This screen is only seen if the User has access to more than one Site.</p> <p>User cannot switch to a different Site while logged in. To switch Sites, User has to log out and back in.</p>	<p>Use the smart-device's NFC scanner (if available).</p> <p>Please note: If you have access to only one site, this will be the first screen visible after logging in.</p>	<p>Using the arrows, a User can toggle between the NFC scanner (shown on previous screen) or a User can use the smart device's camera or laser scanner (if available).</p>	<p>User can log out manually by selecting the option from the menu.</p> <p>User is automatically logged out after 30 minutes of inactivity.</p>



Login without Single Sign On (SSO) → Home Screen → Logout (Android & iOS)

Login	Continue Login, no SSO	Select a Site	NFC Scan (aka: Home Screen)	2D Barcode Scan	Logout
					
<p><i>Customer ID</i> is unique to the environment/customer; this will be provided by InVue.</p> <p>Select <i>NEXT</i> to enter further credentials. System will check if the customer is configured for SSO (Single Sign On).</p>	<p>If SSO is NOT configured, user will see the Passcode field appear and the button text will change to <i>LOGIN</i>.</p> <p><i>Passcode</i> is same as the user's PIN which is used to check out a OneKEY; this will be provided by the system 1.</p>	<p>This screen is presented only if the User has access to more than one Site.</p> <p>User cannot switch to a different Site while logged in. To switch Sites, User has to log out and back in.</p>	<p>Use the smart-device's NFC scanner (if available).</p> <p>Please note: If you have access to only one site, this will be the first screen visible after logging in.</p>	<p>Using the arrows, a User can toggle between the NFC scanner (shown on previous screen) or a User can use the smart device's camera or laser scanner (if available).</p>	<p>User can log out manually by selecting the option from the menu.</p> <p>User is automatically logged out after 30 minutes of inactivity.</p>



Operate a Device: Unlock → Unlatch → Latch → Lock (Android & iOS)

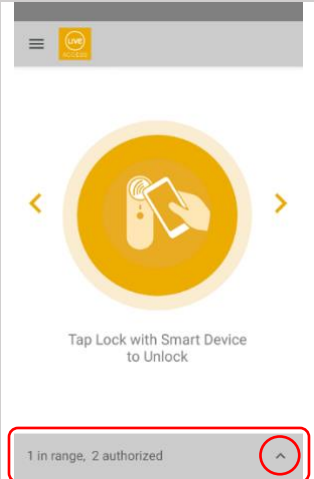
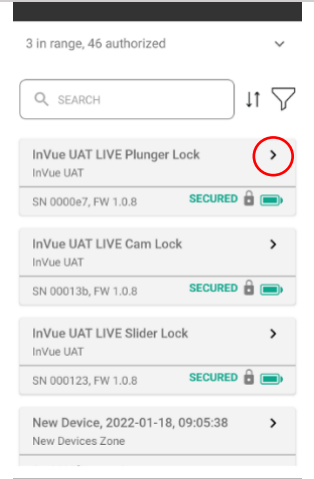
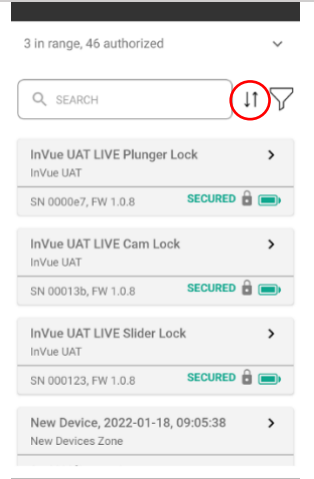
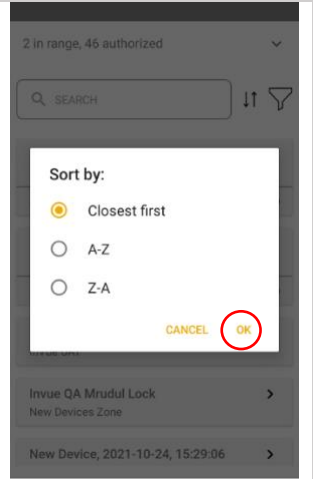
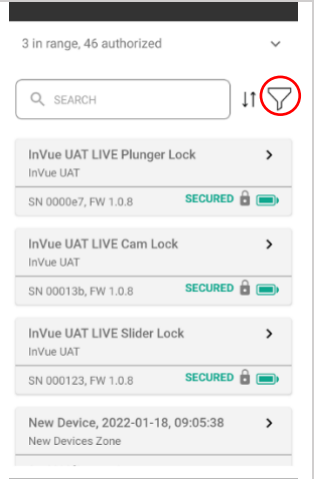
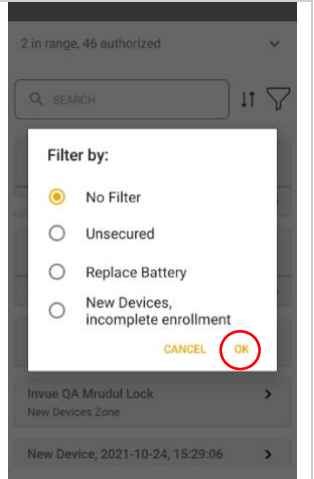
Home Screen	Unlocked	Unsecured	Locked	Secured	Time Expired
<p>Tap Lock with Smart Device to Unlock</p> <p>1 in range, 2 authorized</p>	<p>OPEN the Cabinet within 4 seconds</p> <p>InVue UAT LIVE Plunger Lock InVue UAT UNSECURED GOOD LIVE Lock, SN 0000e7, FW 1.0.8</p>	<p>Secure the Lock</p> <p>InVue UAT LIVE Plunger Lock InVue UAT UNSECURED GOOD LIVE Lock, SN 0000e7, FW 1.0.8</p>	<p>Locked</p> <p>InVue UAT LIVE Plunger Lock InVue UAT SECURED GOOD LIVE Lock, SN 0000e7, FW 1.0.8</p>	<p>Touch the circle to Unlock</p> <p>InVue UAT LIVE Plunger Lock InVue UAT SECURED GOOD LIVE Lock, SN 0000e7, FW 1.0.8</p>	<p>Time Expired</p> <p>Tap or Scan again to Unlock</p> <p>InVue UAT LIVE Plunger Lock InVue UAT SECURED GOOD LIVE Lock, SN 0000e7, FW 1.0.8</p>
<p>Home Screen enables the user to operate the lock by scanning it with NFC:</p> <p>Android: NFC is always engaged so touch the smart phone to the top of the LIVE Lock to engage the Unlock.</p> <p>iOS: touch the circle in the app to engage NFC then touch the smart phone to the top of the LIVE Lock</p>	<p>The green circle animation runs for a maximum of 4 seconds. User will be able to unlatch the Device (and open the cabinet/fixture) during these 4 seconds.</p> <p>If the User does not unlatch the Device, the Device will auto-lock and therefore return to a SECURED state.</p>	<p>The “Unsecured” screen appears if the User Unlatches the Device. This screen remains visible until the Device is returned to a SECURED state.</p>	<p>The “Locked” screen appears for a split-second to inform the User that the Device is SECURED.</p>	<p>The “Secured” screen is the final step of the unlock-lock process.</p> <p>From this screen, the User is able to operate the Device by touching the Secured circle one more time within 5 seconds after the first iteration.</p> <p>However, if user has the Remote Operation permission, they can operate the same lock multiple times without rescanning it until</p>	<p>A user with the Remote Operation permission will not see this screen.</p>



Home Screen	Unlocked	Unsecured	Locked	Secured	Time Expired
<p>to engage the Unlock.</p> <p>If the number “in range” = 0, User will not be able to operate any Devices.</p>				<p>they exit this page; the <i>Time Expired</i> screen will not appear.</p>	



Authorized Devices in Range (Android)

Home Screen	In Range and Authorized	Sort	Select Sort Criteria	Filter	Select Filter Criteria
					
<p>Numbers “in range” and “authorized” refresh every 5 seconds.</p> <p>User must have one or more of the following permissions:</p> <ul style="list-style-type: none"> • Enroll KAS/OKM/ Devices • Manage Devices • Remote Operation <p>to open the list to view the Devices (this is configurable in a User’s profile).</p>	<p>Once the list is opened, the list will only refresh when a swipe-down is performed or when a <i>Sort or Filter</i> is invoked.</p> <p>Users with one or more of the following permissions:</p> <ul style="list-style-type: none"> • Manage Devices • Remote Operation <p>will see a “>” icon indicating that they can select a Device.</p>	<p><i>Closest First</i> is the default.</p> <p>If no LIVE Locks are present, then A-Z is the default sort order.</p>		<p><i>No Filter</i> (= view all) is the default</p>	



Home Screen	In Range and Authorized	Sort	Select Sort Criteria	Filter	Select Filter Criteria
	Users with the following permission: <ul style="list-style-type: none"> • Manage Devices will see <u>all</u> Devices, including LIVE Locks and non-LIVE Locks such as SmartLocks, PODs, etc. 				



Authorized Devices in Range (iOS)

Home Screen	In Range and Authorized	Sort	Select Sort Criteria	Filter	Select Filter Criteria
<p>Numbers “in range” and “authorized” refresh every 5 seconds.</p> <p>Any User will be able to open the list and view the Devices; regardless of special permissions.</p>	<p>Once the list is opened, the list will only refresh when a swipe-down is performed or when a <i>Sort or Filter</i> is invoked.</p>	<p><i>Closest First</i> is the default. If no LIVE Locks are present, then A-Z is the default sort order.</p>		<p><i>No Filter</i> (= view all) is the default</p>	

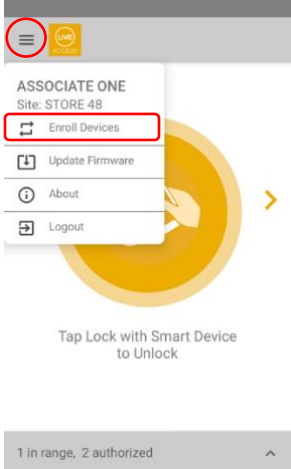
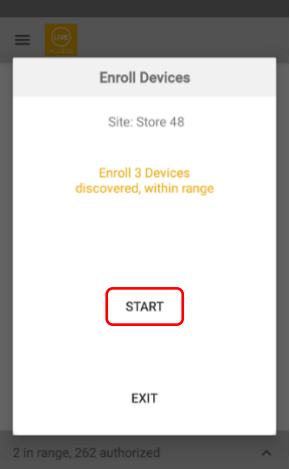
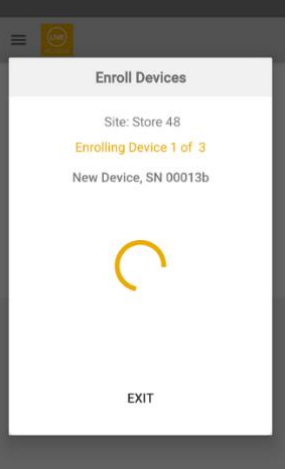
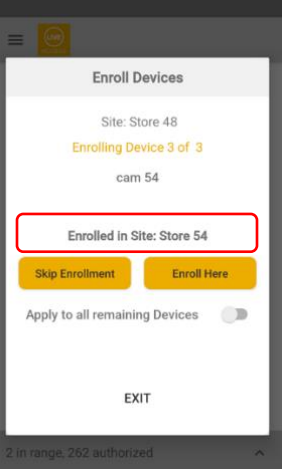
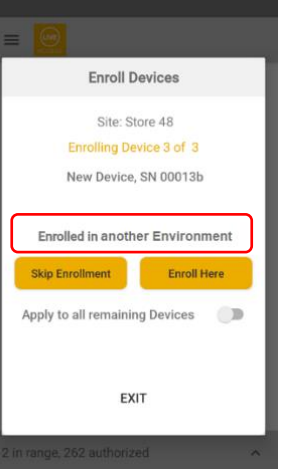
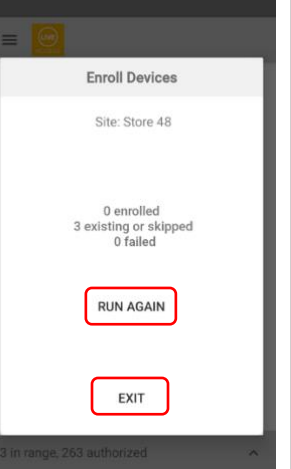


Update Device Settings (Android)

Update Device Settings	Select to Update Settings	Current Settings	Update and Save	Updated Device Settings
<p>Users with the following permission:</p> <ul style="list-style-type: none"> • Manage Devices can select a Device to update its settings. <p>User will be able to manage settings of <u>all</u> Devices, including LIVE Locks and SmartLocks, if given permission.</p>	<p>The “<u>UPDATE DEVICE SETTINGS</u>” link will appear in the Device Info section.</p> <p>Selecting this link opens the Settings page.</p>	<p>Settings page displays the current Device settings.</p>	<p>Update the needed fields, then SAVE changes, then touch the BACK (<) button to return to the <i>Secured</i> page.</p> <p>It may take up to 30 seconds for the Device Info to reflect the changes.</p>	



Enroll Devices, 1 at a time or in bulk (Android)

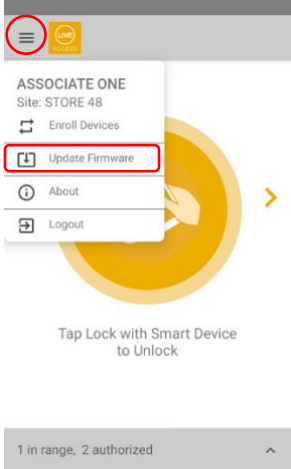
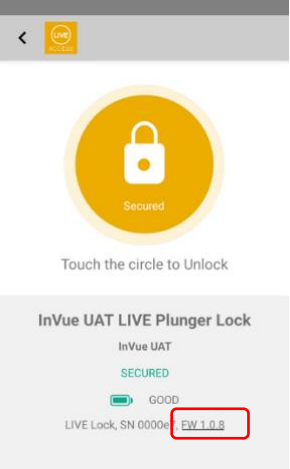
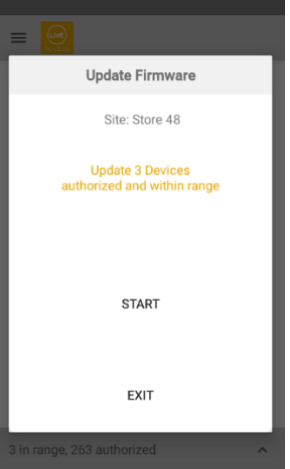
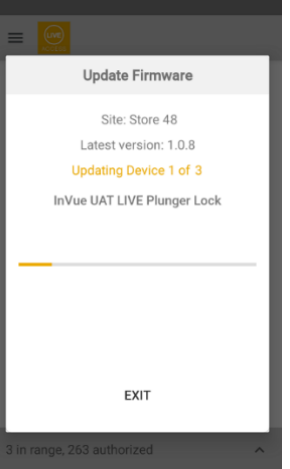
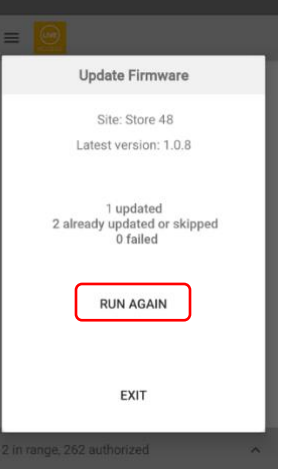
Home Screen	Start Enrollment	Enrolling Each Device	If already Enrolled in a different Site of same Env	If already Enrolled in a different Environment	Summary
					
<p>Users with the following permission:</p> <ul style="list-style-type: none"> Enroll KAS/OKM/ Devices <p>will see the “<i>Enroll Devices</i>” menu item.</p> <p>Selecting the menu item opens the “<i>Start Enrollment</i>” page.</p> <p>All Devices that are discovered and within range will be processed.</p>	<p>Confirm the correct Site is selected for Enrolling.</p> <p>System shows the number of Devices discovered within the range of the smart phone. This is the maximum number of Devices which will be processed.</p> <p>Start the Enrollment process by selecting “START”.</p>	<p>Enrollment process takes 1 – 5 seconds per Device so it is normal for the human eye to not catch the enrollment of each Device.</p> <p>If the process takes beyond 60 seconds for a lock, that may indicate an underlying issue related to communication between the Device and the app. In this</p>	<p>If a Device is already Enrolled in a different Site of the User’s enterprise, User is prompted to specify if the Device should be Enrolled in the currently selected Site. If chosen to “<i>Enroll Here</i>”, the Device will be removed from the “other” Site and Enrolled in this Site.</p>	<p>If a Device has:</p> <ul style="list-style-type: none"> FW version 1.0.9 or higher <u>and</u> was previously Enrolled in another Environment. <p>the User is prompted to specify if the Device should be Enrolled in their Environment. If chosen to “<i>Enroll Here</i>”, the Device will</p>	<p>Summary page detailing the number of Devices processed.</p> <p>Enrollment can be RUN AGAIN; thus avoiding the need to EXIT and restart.</p>



Home Screen	Start Enrollment	Enrolling Each Device	If already Enrolled in a different Site of same Env	If already Enrolled in a different Environment	Summary
		<p>case, try to run Enrollment again (exit and restart). If the issue persists, note the Serial Number of the Device where it hangs then contact support.</p>	<p>Select “<i>Apply to all remaining Devices</i>” to not be prompted again for a similar case with remaining Devices.</p>	<p>be added to the user’s Environment. IMPORTANT: The Device will not be removed from the “other” Environment.</p>	



Update Firmware (Android)

Home Screen	Update FW of Selected Device	Start FW Update	Update Firmware	Summary	
					
<p>Users with the following permission:</p> <ul style="list-style-type: none"> Enroll KAS/OKM/ Devices <p>will see the “Update Firmware” menu item.</p> <p>Selecting the menu item opens the “Start FW Update” page.</p> <p>All Devices that are authorized and within range will be processed.</p>	<p>Users with the following permission:</p> <ul style="list-style-type: none"> Enroll KAS/OKM/ Devices <p>will see the FW version link.</p> <p>Clicking on the link opens the “Start FW Update” page.</p> <p>Only the selected Device will be processed.</p>	<p>Confirm the correct Site is selected for Updating the FW.</p> <p>System shows the number of Devices authorized and within the range of the smart phone. This is the maximum number of Devices which will be processed.</p> <p>Start the FW Update process by selecting “START”.</p>	<p>Updating FW takes about 30 seconds per Device.</p> <p>During the FW Update and for 10 to 20 seconds following the update, the Device will not appear in the “in range, authorized” list and therefore will not operate using the App.</p>	<p>Summary page detailing the number of Devices processed.</p> <p>FW Update can be run again by selecting “RUN AGAIN”; thus avoiding the need to “EXIT” and restart.</p>	



Request a Remote Unlock, by an unauthorized user (Android)

Home Screen	Not Authorized	Request Remote Unlock	Wait up to 120 Seconds	Remotely Unlock
				<p>An ADMIN User can remotely unlock the Device from the LIVE Access Web Portal, Devices Page.</p>
<p>User attempts to operate a Device as per normal process.</p>	<p>If the User does NOT have permission to operate the scanned Device, user is presented with the option to “Request a Remote Unlock”.</p> <p>User must touch the circle to begin the process of initiating the request.</p>	<p>User must “CONFIRM” to initiate the request.</p>	<p>System allows 120 seconds (2 minutes) for an authorized User of the Web Portal to remotely unlock the Device.</p> <p>The App User must wait next to the Device for the Remote Unlock to function.</p>	<p>User’s App will show the Device Unlock sequence.</p> <p>Note: during normal operations, the <i>Unlocked</i> screen displays for 4 seconds but, to allow the requester more time to react to a remote unlock, this screen will display for approximately 10 seconds.</p>

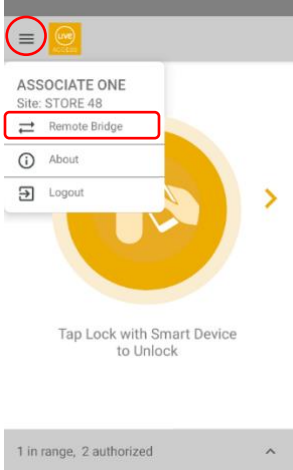
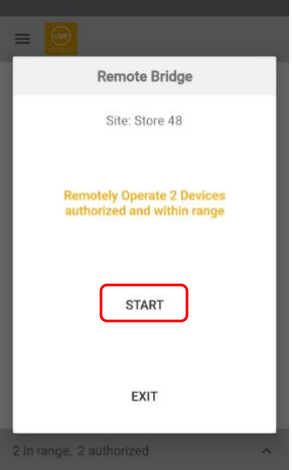
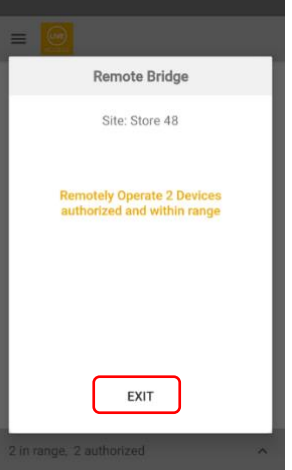
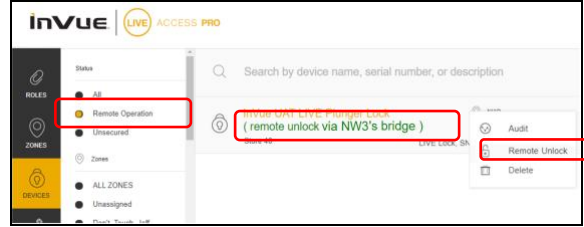


Remote Unlock from the App (Android)

In Range and Authorized	Secured	Unlocked	Unsecured	Locked	Secured
<p>Users with the following permission:</p> <ul style="list-style-type: none"> Remote Operation <p>will be able to select a Device from the list to operate the Device without first scanning it.</p> <p>Selecting a Device will open the “Secured” page.</p>	<p>User must touch the circle to operate the Device.</p> <p>User must be within range of the Lock to Remotely Unlock.</p> <p>If User is <u>not</u> within range of the Device, the circle will <u>not</u> be actionable.</p>	<p>Note: during normal operations, the <i>Unlocked</i> screen displays for 4 seconds but, to allow the requester more time to react to a remote unlock, this screen will display for approximately 20 seconds.</p>			<p>User is able to repeatedly operate the Device by touching the <i>Secured</i> circle after each iteration (<i>Time Expired</i> screen will not appear).</p>



Remote Unlock from the Web Portal & Remote Bridge (Android)

Remote Bridge	Start Remote Bridge	Remote Bridge Open	Advertise in Web Portal, Devices page and Remote Unlock
			
<p>A User Type = USER with the following permission:</p> <ul style="list-style-type: none"> Remote Operation will see the “Remote Bridge” menu item. <p>Selecting the menu item opens the “Remote Bridge” page.</p>	<p>Confirm the correct Site is selected for the Remote Bridge.</p> <p>Start the Remote Bridge process by selecting “START”.</p> <p>Remote Bridge will be able to operate Devices that are within range and in the User’s access.</p>	<p>While the Remote Bridge is active, in the Web Portal, each Device will display that it is available for remote unlock via this User’s bridge.</p>	<ol style="list-style-type: none"> Sign in to the Web Portal with a User Type = ADMIN On DEVICES page, select Status = <i>Remote Operation</i> <ul style="list-style-type: none"> This will display all Devices available for remote unlock To unlock a Device remotely, navigate to the 3-dot context menu and select “Remote Unlock” <ul style="list-style-type: none"> This menu item is only available to a User Type = ADMIN with the <i>Remote Operation</i> permission Selecting this menu item will send a message to the Remote Bridge to unlock the Device The Device will unlock then relock in 20 seconds



Remote Bridge	Start Remote Bridge	Remote Bridge Open	Advertise in Web Portal, Devices page and Remote Unlock
			<ul style="list-style-type: none"> • During this time, the Device can be unlatched, cabinet can be opened, then closed, and the Device can be latched. <p>All activity is recorded and visible on the Audit page.</p>



Device Not Found (screens explained) (Android)

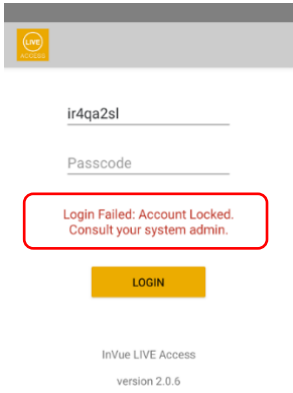
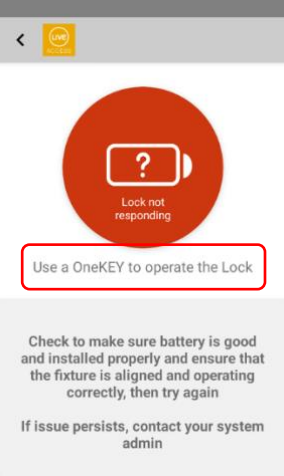
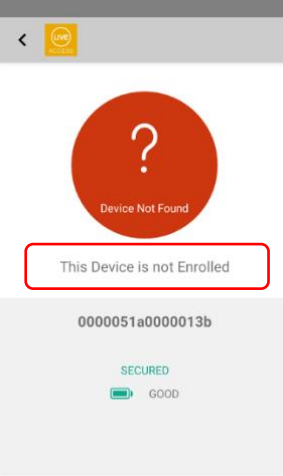
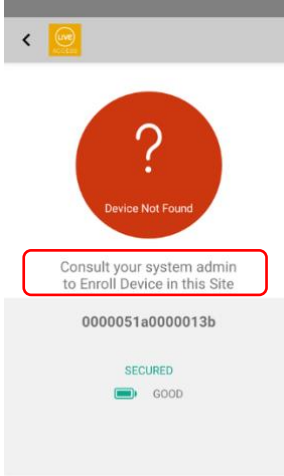
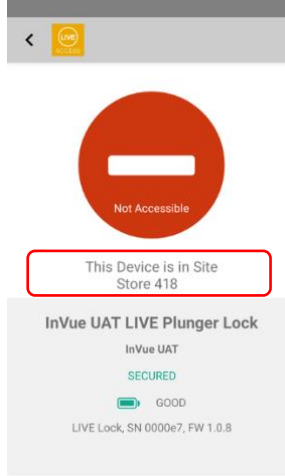
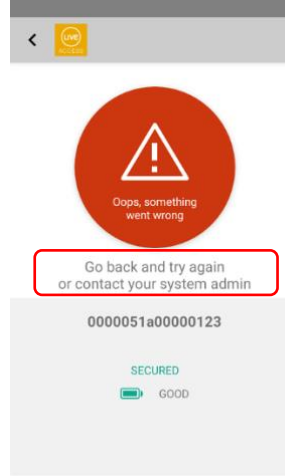
	Device Not Found	Previously Enrolled in a different Environment	New and all others	Device in Another Site	
<p>If the Device is not enrolled in the User's environment, they will be presented with the "Device Not Found" screen.</p>					<p>The Enrollment process is the same whether enrolling 1 Device at a time or multiple (in bulk).</p> <p>See the <i>Enroll Devices</i> workflow for details.</p>
	<p>A User does not have the permission:</p> <ul style="list-style-type: none"> Enroll KAS/OKM/Devices <p>will see the "This Device is not Enrolled" message.</p>	<p>A non-SuperAdmin User who has the permission:</p> <ul style="list-style-type: none"> Enroll KAS/OKM/Devices <u>and</u> the Device has FW version 1.0.9 or higher <u>and</u> was previously Enrolled in another Environment. 	<p>A User who has the permission</p> <ul style="list-style-type: none"> Enroll KAS/OKM/Devices <u>and</u> the Device is New (from factory, in box) or has been reset to Factory Defaults* <p>they will see the "Touch the circle to Enroll this Device" message.</p>	<p>Message seen when the Device is Enrolled in another Site of the User's Environment.</p> <p>To Enroll the Device in the User's current Site, delete the Device (from the Web Portal) then rescan it.</p>	



	Device Not Found	Previously Enrolled in a different Environment	New and all others	Device in Another Site	
		<p>they will see the “<i>Consult your system admin to Enroll Device in this Site</i>” message.</p> <p>A SuperAdmin will not see this message; they will be able to Enroll this Device.</p>	<p>This User can proceed to Enroll the Device.</p> <p>* only InVue can reset a lock to Factory Default.</p>		



Operation / Interaction Error States (Android)

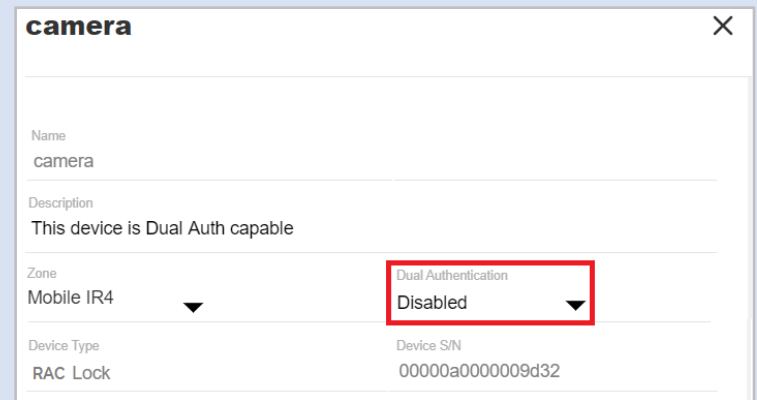
Account Locked	Device Not Responding	Device Not Found	Previously Enrolled in a different Environment	Device is in Another Site of the same Environment	Oops, something went wrong
					
<p>Message seen if User's account is locked.</p> <p>Account can be unlocked from the Web Portal by an authorized Admin User.</p>	<p>Message seen if the Device (Lock) is not responding to scanning (NFC or 'QR' Code).</p> <p>Steps to correct the situation are provided on-screen.</p>	<p>Message seen when the Device is not found in the User's Environment (Customer's instance of LIVE Access) <u>and</u> the User does not have the permission to "Enroll".</p>	<p>Message seen when the Device is Enrolled in another Environment (<u>not</u> this Customer's instance of LIVE Access).</p> <p>A special user has to complete this type of enrollment.</p>	<p>Message seen when the Device is Enrolled in another Site of the User's Environment.</p> <p>To change the Enrollment of this Device to the User's current Site, first delete the Device (from the Web Portal) and then rescan it.</p>	<p>Message seen when a Device is scanned but something went wrong (an undermined error occurred).</p>



Features unique to certain Devices

Glossary of Features

Term or Acronym	Definition
Auto-locking	Device auto-locks 10 seconds after it is unlocked.
IR3/IR4 Compatibility	All IR4 compatible Devices are backward compatible with IR3; however, the features supported by IR4 are not backward compatible with IR3. Which means, to take advantage of the features offered by IR4, an upgrade to IR4 is required.
Dual Authentication (DA)	<p>When a Device is capable of Dual Authentication (DA), a setting appears on the Device's <i>Edit</i> page to <i>Enable/Disable</i> the DA function. You can <i>Enable</i> this setting to take advantage of this functionality.</p> <ul style="list-style-type: none"> If <i>Enabled</i>: <ul style="list-style-type: none"> ✓ Two different Users have to Operate this Device within 10 seconds (aka. the DA Operating Window) in order to unlock it. ✓ Both Users must have authorization to Operate the Device and the second User must Operate the Device within the authorized operating window (default = 10 seconds). If either condition is violated, the Device will not unlock. ✓ Only one authorized User is required to lock the Device. If <i>Disabled</i>: <ul style="list-style-type: none"> ✓ The Device behaves like any other smart lock in that it will only require one User to unlock it.



Package Protection – IR3

Package Protection is a category of security devices designed to protect retail merchandise. Products include Spider Wraps, Locking Hooks, Stop Locks, etc.. Picture of the various Devices and their typical implementation can be seen on www.invue.com.

Features specific and/or unique to this Device:

- Compatible with IR3 OneKEY
- These Devices are not serialized; therefore, each Device is recorded as a “Legacy Device” and basic information such as Device Type or Zoning is not available



- By default, all Users are authorized to Operate these Devices (if control over authorization is required, see “Package Protection with IR4”)

RAC Lock

The RAC Lock is a special Device designed to secure Server Racks such as those found in Data Centers. A picture of the Device and its typical implementation are shown here. Visit <https://invue.com/products/rac-lock-data-center> to learn more.



Features specific and/or unique to this Device:

- Compatible with IR4 OneKEY only
- A OneKEY is required to unlock and relock the Device; not auto-locking
- Each Device is serialized, thereby enabling Zoning and access tracking
- Supports *Dual Authentication* which can be configured at the device-level from the Devices page

Padlock

The Padlock is designed to secure any fixture for which a standard padlock is applicable. A picture of the Device and its typical implementation are shown here. Visit <https://invue.com/products/padlock> to learn more.



Features specific and/or unique to this Device:

- Compatible with IR3 and IR4 OneKEYs
- A OneKEY is required to unlock the Device; auto-locking
- Each Device is serialized, thereby enabling Zoning and access tracking
- This Padlock is indoor and outdoor compatible
- Supports *Dual Authentication* which can be configured at the device-level from the Devices page

LIVE Locks

LIVE Locks are a category of smart locks designed to secure retail merchandise. Products include the Plunger, Slider, and Cam locks. Visit <https://invue.com/products/live-locks.cfm> to learn more.



Features specific and/or unique to this Device:

- Auto-Locking
- Compatible with IR3 and IR4 OneKEYs and the Mobile App
- Each Device is serialized, thereby enabling Zoning and access tracking



- Unlock the Device using a smartphone/device equipped with NFC, a Camera, and/or a barcode reader (such as a laser scanner)



Setting up a new Environment

Like any new product, LIVE Access has to be configured to work and behave as you need it to. Before the environment is released to you (our customer) we may ask you a few questions, such as:

- ✓ Do you want to allow your associates to open multiple cabinets (which will be secured by InVue Devices)? If Yes, then a few more questions will follow.
 - This is a key input to configuring the *Restricted Mode*
- ✓ How long a PIN length do you prefer for your associates to check out keys?
 - Select a PIN length of 5, 6, 7, or 8 digits
- ✓ The system provides the ability to assign permissions (authorizations) per User, by default. Will you want to disable this?
 - This is a key input to configuring access to *Zones*

Answers to these and more questions will be used to update settings on the *Settings* page which apply to the entire environment and all Users.

New Environment Setup Parameters

As a sign of handing you the keys to your new environment, you will receive the following by email from our team:

- URL to access the environment: typically this is in the format: `https://<customer name>-sso.invue-am.com`
- KAS/OKM Enrollment PIN: PIN used to enroll each new KAS or OKM; this PIN is unique to the customer's environment
- KAS/OKM Network Port: Your IT dept. will need this Port # for configuring network access through the company's firewall
- Admin ID: User ID of the Admin account (the ID is case sensitive)
- Admin Password: Password of the Admin account (the password is case sensitive)
- Admin PIN: PIN unique to the Admin user, used to check out a OneKEY, login to the Mobile App, and to register and Operate Devices

Keep this information handy but secured.

Setting up a Site – 1st or adding a new one

Before adding any data, Devices, or Users to the system, ensure that the Settings are acceptable and applicable for how you plan to use the software and the Devices.



About the IR Ecosystem

The IR ecosystem consists of IR3 and IR4 products (such as the locks and keys and LIVE Access, the software you will use to manage the environment. IR3 products include the IR3 OneKEY and the Key Authorization Station (KAS). IR4 products include the IR4 Batch OneKEY, IR4 LIVE OneKEY, and the OneKEY Manager (OKM). All InVue Smart Locks are compatible with both the IR3 and IR4. Following pages provide step-by-step detail to install the various components of each product line.

You can learn more about the IR Ecosystem on <https://www.InVue.com>.

The IR3 Ecosystem

IR3 is InVue’s first OneKEY which introduced the time-out feature whereby the OneKEY times out at the end of the User’s shift. The key also introduced the ability to read and record transaction data, allowing managers to view all operations performed by each User in chronological order.

- The IR3 ecosystem introduced new functionality over the previous IR2 version of the OneKEY by capturing and storing transaction records in the key. These records are saved to the cloud in LIVE Access when the key is docked on a KAS.
- Pictures of the KAS and the IR3 OneKEY are shown →



The IR4 Ecosystem

IR4 is InVue’s newest OneKEY which introduced the ability to communicate User interactions in real-time and deactivate the key, also in real-time.

- The IR4 key comes in two versions:
 1. One version of the IR4 key preserved the functionality of the IR3 key (to save records on the key until it is docked and checked in) – this is called the **IR4 Batch key**
 2. The second version of the IR4 key introduced the functionality to connect wirelessly to the cloud and, therefore, send user-interaction data in real-time to LIVE Access – this is called the **IR4 LIVE key**
 - To take advantage of the real-time-connectivity feature, connection to a LoRaWAN network is required.
- Both the Batch and the LIVE keys look the same.
- Pictures of the OKM and the IR4 OneKEY are shown →





Setting up the IR3 Ecosystem

Products in the IR3 Ecosystem

IR3 OneKEY

The OneKEY is used by a User to Operate (lock or unlock) a Device. Each time a User presses the button on the OneKEY, the OneKEY records the interaction on on-board storage. Then, when the OneKEY is docked on a KAS, the KAS reads the data from the OneKEY and sends it to LIVE Access. The IR3 OneKEY is referred to as a 'batch' key because it stores records in a on-board storage until it is checked-in.



Key Authorization Station (KAS)

A KAS, or Key Authorization Station, is a network-connected device which facilitates communication between the OneKEY and LIVE Access. Operationally, when a User checks out a OneKEY, they do it by docking a OneKEY on the KAS and entering their assigned PIN #. Similarly, at the end of their shift or once they are done using the OneKEY, a User docks the OneKEY on the KAS to check it in, thus initiating a process where the KAS reads the data off of the OneKEY and send the data to LIVE Access.



Installing the KAS and the IR3 OneKEY

Below are two ways to view the installations instructions:

1. [Click here](https://invue.com/wp-content/themes/invue/instructions/one-key/IR3/index.html) or copy and paste this link in a browser:
<https://invue.com/wp-content/themes/invue/instructions/one-key/IR3/index.html>
2. Scan the QR code with your smartphone →
 Optional: you will have the ability to print the instructions.





Setting up the IR4 Ecosystem

Products in the IR4 Ecosystem

IR4 OneKEY

The OneKEY is used by a User to Operate (lock or unlock) a Device. Each time a User presses the button on the OneKEY, the OneKEY records the interaction on on-board storage. Then, when the OneKEY is docked on an OKM, the OKM reads the data from the OneKEY and sends it to LIVE Access. The IR4 OneKEY comes in two SKUs: one connects wirelessly to the cloud and, therefore, send data in real-time to Access Manage, known as the 'LIVE' key, and the other, referred to as the 'batch' key, acts much like the IR3 key in that it does not connect wirelessly to the cloud.



OneKEY Manager (OKM)

An OKM, or OneKEY Manager, is the next-generation of the KAS. The OKM is also a network-connected device which facilitates communication between the OneKEY and LIVE Access. Operationally, when a User checks out a OneKEY, they do it by docking a OneKEY on the OKM and entering their assigned PIN #. Similarly, at the end of their shift or once they are done using the OneKEY, a User docks the OneKEY on the OKM to check it in, thus initiating a process where the OKM reads the data off of the OneKEY and send the data to LIVE Access.



Installing the OKM and the IR4 OneKEY

Below are two ways to view the installations instructions:

1. [Click here](https://invue.com/wp-content/themes/invue/instructions/one-key/IR4/index.html) or copy and paste this link in a browser:
<https://invue.com/wp-content/themes/invue/instructions/one-key/IR4/index.html>
2. Scan the QR code with your smartphone →
 Optional: you will have the ability to print the instructions.

