KASAccess User Manual / Product Guide

Setting up KASAccess

To start using KASAccess, you need to obtain login credentials from KAS. This can be done by contacting their customer service via phone or email. Once you receive your login details, you can log into KASAccess and access the dashboard, which provides an overview of the system and information about the locks associated with your account.

Instructions:

1. Call +61 7 5500 5580 or send an email to support@kas.com.au.
2. Inform the customer service representative that you need an account for KASAccess.
3. Follow any instructions given by the representative, such as providing your contact information and any relevant company details.
4. KAS support staff will process your request and generate your login credentials.
5. Once your account is created, KAS support staff will respond to your request with your login credentials.
6. Visit the KASAccess website and enter your login credentials (username and password) to log in.
7. After successfully logging in, you will be presented with a dashboard that provides an overview of the system. Take some time to familiarize yourself with the information and features available.
8. Within the dashboard, you will find details about the locks associated with your account, such as their status, usage history, and any alerts or notifications.

Remember to keep your login credentials secure and refrain from sharing them with unauthorized individuals.

Creating a Key

To create a key in KASAccess, you need to follow a series of steps. These include accessing the "Keys" section, entering the required information such as pincode or RFID number, selecting or entering an identifier for the key user, setting the start and end dates and times, selecting locks or lock groups, and monitoring the key status for successful addition to the locks.

Instructions:

1. Access the "Keys" section: From the left menu in KASAccess, expand the "Access and Passage" menu and click on "Keys."
2. Click "Add": On the "Keys" page, click the "Add" button located at the top of the page.
3. Enter pincode or RFID number: In the "Pincode" field, enter a 4-6 digit pincode or a 10-digit RFID number for the key.
4. Select or enter an identifier: Choose an existing identifier from the "Select a Key User" dropdown or enter a new identifier in the "Guest Identifier" field. The identifier should be unique and reflect t
5. Set start and end dates and times: Specify the desired start and end dates and times for the key using the provided windows. By default, the start date/time will be set to the current time, but you can a
6. Select locks or lock groups: Choose the locks to which you want to add the pincode or RFID card. You can either select specific locks or opt for a pre-configured "Group" of locks from the dropdow
7. Configure KAS Lift Controllers (if applicable): If you are using KAS Lift Controllers, modify the floors for which access should be granted and save the changes.
8. After completing the above steps, you will be redirected to the keys list. Initially, the key's status will show as "Queued" in the right-hand column of the table. Refresh the page periodically to see the
9. As the keys are processed and written to each lock sequentially, their status will change from "Queued" to "Pending" and eventually to "Success." Refresh the page to observe the status updates.
10. If a key fails to add to a lock, it will display an "Error" status. Hover your mouse over the red error badge to view the error message and identify the problem. In case of a "Notice" status, hover over

Remember to save any changes and ensure the accuracy of the entered information before creating the key in KASAccess.

Adding a Bluetooth Key

Adding a Bluetooth key in KASAccess is a straightforward process. By default, when you create a regular pincode or RFID key, a corresponding Bluetooth key is automatically generated for the same lock(s). However, if you specifically want to create a Bluetooth-only key, you can do so by selecting the "is BT Only Key" checkbox on the "Keys > Add" page. After creating the key, instruct the guest to download the KASAccess Mobile app and log in using their identifier and the default one-time password. Once logged in, the guest can use the app to unlock their room.

Instructions:

1. From the left menu, Access and Passage > Keys, click the "Add" button at the top of the page.
2. Just above the "Pincode" field, there will be a checkbox labelled "is BT Only Key." Check this box to create a Bluetooth-only key.
3. Proceed with the same steps mentioned earlier for creating a new key, including entering the necessary details such as pincode or RFID number, selecting or entering an identifier, setting start and en
4. Instruct the guest to download the KASAccess Mobile app from either the Google Play Store (for Android) or the iPhone App Store (for iOS).
5. Ask the guest to log into the app using their identifier and the default one-time password "defaultpass" (all in lowercase).
6. Once logged in, the app will prompt the guest to change their password. They need to enter a new password and repeat it. Passwords must be at least 8 characters long and include a combination of n
7. When the guest is in front of their room door, opening the app will display a Bluetooth icon next to the name of their door. As they approach, the Bluetooth icon should turn from grey to blue.
8. Once the Bluetooth icon turns blue, the guest can press the dark blue "unlock" button in the app to immediately unlock their room door.

Note: Ensure that the guest is aware of the proper usage of the KASAccess Mobile app and how to access and utilize the Bluetooth key functionality.

Using Bluetooth Unlock

Guests with the KASAccess mobile app can utilize Bluetooth Unlock functionality to conveniently unlock their doors. The process differs slightly for Android phones and iPhones. For Android, guests need to enable Auto Unlock in the app settings and hold their phone to the lock for automatic unlocking. On iPhones, guests can enable Auto Unlock in the phone settings and open the KASAccess app for automatic unlocking. Voice assistants can also be used to trigger the app and unlock the door, enhancing the user experience.

Instructions for Android Phones:

1. If not already logged in, the guest should open the KASAccess app and log in.
2. Tap on the account tab located at the bottom right.
3. Click on "Open Settings" and navigate to the desired settings page.
4. Enable the switches for "Auto Unlock when within range" and "Auto Close app after successful unlock."
5. Instruct the guest to close the app.
6. Wait for 20 seconds: Wait for 20 seconds after activating the Auto Unlock feature.
7. The guest can now open the KASAccess app, hold it to the lock, and wait for the lock to be discovered (1-10 seconds). The door will automatically unlock, and the app will close. Voice commands li

Instructions for iPhones:

1. Ensure that the KASAccess app is closed.
2. Open the phone settings app (with the gear icon).
3. Scroll down and locate the KASAccess menu, then tap on it.
4. Select the option "Auto Unlock when within range" within the KASAccess menu.
5. Close the phone settings app.
6. When the guest opens the KASAccess app, it will automatically unlock any door for which they have been granted keys, provided the phone is within Bluetooth range.
7. (Optional) Guests can create a shortcut in the "Shortcuts" app to automatically open KASAccess and unlock the door. For example, create a shortcut named "Open KASAccess" that opens the KASA
8. With the shortcut set up, guests can use their iPhone's voice assistant (e.g., "Hey Siri, open KASAccess") while within Bluetooth range of the lock to automatically open the app and unlock the door.

Ensure that guests are familiar with the Bluetooth Unlock feature and the specific steps required for their phone type to maximize convenience and security.

Lock Settings for Bluetooth Access

Bluetooth access is enabled by default on each lock in KASAccess. If you do not want to provide Bluetooth access to guests, simply refrain from sharing their identifier. However, if you wish to adjust Bluetooth sensitivity or define locks as close range or long range, you can modify the settings. This can be done through the KASAccess Admin Console by accessing the property settings for Bluetooth range sensitivity. Close range and long range sensitivity values can be adjusted to control the distance at which Bluetooth access is granted. Locks can be categorized as either close range or long range based on your preferences. It is recommended to set different sensitivities for different types of locks (e.g., guest rooms, car park boom gates). Changing lock definitions can be done within the "Doors and Locks" menu, specifically the "ACRs and Locks" section.

Instructions:

1. Access KASAccess Admin Console: Log in to the KASAccess Admin Console using your credentials.
2. Select "Properties": From the menu, choose the "Properties" option.

3. Choose your property: Locate and select the name of your property from the list.
4. Navigate to "BT Range Sensitivity Setting": Within the property settings, find the section labelled "BT Range Sensitivity Setting."
5. Adjust sensitivity values: Set the close range and long range sensitivity values based on your requirements. Here is a guide for reference:
    - Close range: A value of 35 requires the phone to be held directly against the lock. 42-45 allows for 2-3 cm proximity. 50-60 is suitable for 10-20 cm proximity. A value of 100 enables access f
    - Long range: Recommended values are 50 for close range and 100 for long range sensitivity. Adjust as per your preferences.
6. Define lock types: Determine whether each lock should be considered close range or long range based on its location and purpose. This distinction affects which sensitivity value the lock observes.
    - To modify lock definitions, go to the "Doors and Locks" menu on the right side of the admin console.
    - Select "ACRs and Locks" and choose the lock name you wish to edit.
    - Check the "BT long range sensitivity" checkbox to designate the lock as long range. Leave it unchecked for close range.
7. Save changes: After adjusting the settings and defining lock types, ensure to save the changes made.

Consider the specific requirements and characteristics of your property while configuring Bluetooth access and sensitivity settings.

Checking Battery Levels

In KASAccess, battery levels of battery-operated locks can be monitored to ensure timely replacement of batteries. To accurately check battery levels, the system needs to be calibrated for your specific locks. By adjusting the settings under the Properties menu for your property, you can configure the battery notification threshold, battery reference max, and battery reference min. Battery levels are automatically updated by KASAccess at regular intervals and can also be refreshed manually. Monitoring the "Low Battery Alert" widget on the KASAccess Dashboard allows you to identify locks with low battery levels and promptly replace batteries to avoid access issues.

Instructions:

1. Access KASAccess Admin Console: Log in to the KASAccess Admin Console using your credentials.
2. Select "Properties": From the menu, choose the "Properties" option.
3. Choose your property: Locate and select the name of your property from the list.
4. Adjust battery settings:
    - Set the Percentage (%) notification threshold to 15. This is the battery level at which you will be alerted to consider battery replacement.
    - Set the Battery reference max to 100. This value represents a fully charged battery.
    - Set the Battery reference min to a value that corresponds to the minimum acceptable battery level for your locks. Note that this value is not the battery percentage itself but a reference value u
5. Save changes: After adjusting the battery settings, save the changes made.
6. Monitor "Low Battery Alert" widget: On the KASAccess Dashboard, keep an eye on the "Low Battery Alert" widget. This widget will display locks with low battery levels that require battery replac
7. Update battery levels:
    - Battery levels are automatically updated by KASAccess every 30 minutes.
    - Battery levels will also be updated when a pincode or RFID card is used to access a door.
    - To manually update battery levels, click the "Status" button on the Locks table page and then refresh the page.
8. When locks appear in the "Low Battery Alert" widget, promptly replace the batteries to ensure uninterrupted access for guests or residents.
9. If you replace a lock's batteries, it may take up to 30 minutes for the automatic battery level service to check and update the value. Be patient if the value does not update immediately.
10. If you need the battery level to update right away, you can perform one of the following actions:
    - Click the "Status" button on the Locks Table page and refresh your browser.
    - Use a pincode or RFID card to unlock the door. The battery value should be updated within 60 seconds.

Note: It is recommended to use the same type of batteries in all locks for consistent performance and battery reference values.

Lock Groups

Lock groups in KASAccess allow property owners to conveniently manage access to common doors shared by multiple guests or staff members. By creating a lock group and adding specific locks to it, you can easily assign keys to both individual guest rooms and the locks within the group. This simplifies the process of granting access to common areas such as the front door, pool gate, laundry, and more. Lock groups can be configured through the "Doors and Locks" > "Lock Groups" menu in KASAccess.

Instructions:

1. Log in to the KASAccess Admin Console using your credentials.
2. From the left menu, select the "Doors and Locks" option.
3. Locate and click on the "Lock Groups" menu.
4. Create a lock group:
    - Click on the "Add" button or a similar option to create a new lock group.
    - Provide a name for the lock group that reflects its purpose or location (e.g., "Common Doors").
5. Add locks to the group:
    - On the right side of the screen, you will see a list of available locks.
    - Select and add each lock that should belong to the lock group by clicking on them.
    - Alternatively, you may have the option to drag and drop the locks into the group.
6. After adding the desired locks, click the "Save" or similar button to create the lock group.
7. Assign keys to the lock group:
    - Proceed to add a new key as you would normally.
    - From the "Select Lock(s) or Lift(s)" menu, choose the guest's room lock.
    - In the "Select Groups" menu below, select the lock group you created earlier.
    - Click "Save" to add the key to both the guest's room lock and the locks within the selected lock group.
8. If you have additional lock groups or keys to assign, repeat steps 4 to 7 as needed.
9. To make changes to lock groups, return to the "Lock Groups" menu under "Doors and Locks". From there, you can edit existing lock groups, add or remove locks, or create new groups as necessary.

Note: Lock groups streamline access management by allowing you to assign keys to both individual locks and multiple locks within a group simultaneously. This is particularly useful for common doors shared by multiple guests or staff members.

Deleting Keys

1. Log in to the KASAccess Admin Console using your credentials.
2. From the menu or navigation options, locate and click on the "Keys" table.
3. Select the key(s) to delete:
    - To delete a single key: Locate the specific key you want to delete and select the checkbox on the left side of its row.
    - To delete multiple keys: Use the available filters at the top of the page to narrow down the list of keys. Once you have applied the desired filters, select the checkbox at the top of the leftmost
4. After selecting the key(s) you wish to delete, locate the red "delete" button at the top of the page and click on it.
5. A confirmation prompt or dialog box may appear asking you to confirm the deletion. Carefully review the selected keys before confirming the deletion.
6. If prompted, confirm the deletion by clicking "OK" or a similar option.

Note: It's important to exercise caution when deleting keys, as this action permanently removes the access privileges associated with the key. Ensure that you have selected the correct key(s) for deletion. Using the available filters can help you delete multiple keys efficiently, but make sure to double-check the selection before confirming the deletion.

Deleting Keys with Filters

This section provides instructions on how to delete keys with filters using the "KasAccess" system. It covers the process of searching for specific keys based on PIN, RFID, or Bluetooth, selecting and deleting the desired keys.

Instructions:

1. Enter the PIN, RFID, or Bluetooth identifier you wish to search for in the "search" field.
2. Click the search button to initiate the search process.
3. Once the search results are displayed, navigate to the leftmost column and click the checkbox at the top to select all the results.
4. After selecting the desired keys, locate and click the delete button at the top of the page.
5. Confirm the deletion action when prompted to remove the selected keys.

Note: The process of deleting Bluetooth-only keys follows the same steps as deleting PIN codes or RFID keys.

The Queue Table

The Queue table in "KasAccess" provides real-time status updates on key or command processing as they are sent to locks. This section explains the purpose of the Queue table, its connection to the keys table, and how to interpret and troubleshoot key-related issues using the Queue table. It also describes the different icons and colors used to represent key status.

Instructions:

1. Access the Queue table through the right-hand side menu in the "KasAccess" system.
2. The Queue table displays rows of individual PINs or RFID numbers along with the corresponding locks they are being added to.
3. On the right column of the Queue table, observe small square dots indicating key activity.
4. If a specific RFID or PIN number and lock are not visible in the Queue table, it means they haven't landed in the queue yet. Be patient as it may take approximately 5 to 10 minutes for very large sets
5. Examine the right-hand column of small square colored dots to determine the status of each key:
    - Yellow dots: Represent attempts by the KASAccess system to write a key to a lock.
    - Green dots: Indicate successful key additions to locks.
    - Red dots: Signal an error that has occurred after all attempts to add the key to the lock have failed.
6. To diagnose a problem with a lock, hover over the red dot of a failed key to obtain detailed information.
7. Rectify the problem, if possible, and click the retry button next to the red dot to reinsert the key and lock into the list for processing.
8. A successfully added key to a lock will display a green status in the Queue table and appear in the Keys table with a "Success" icon.
9. If a key fails to be added due to an error, it will be shown in the Keys table with a red error icon.
10. When a key is in the queue but not yet listed in the Queue Table, it will appear in the Keys table with a light blue "Queued" icon.
11. Once a key is added to the Queue table for processing, it will be displayed in the Keys table with an orange "Pending" icon.

Note: The Queue table provides valuable information for diagnosing lock-related problems and tracking the status of keys being added to locks in the KASAccess system.

The Gateways Table

The Gateways table in "KasAccess" provides essential information about gateways and their connection to locks. This section explains the purpose of the Gateway table, the importance of a solid internet connection for gateways, and how to utilize the table for diagnosing lock-related issues. It also covers renaming and deleting gateways, as well as interpreting signal levels for optimal performance.

Instructions:

1. Access the Gateways table on the left-hand side of the "KasAccess" system.
2. The table contains a list of gateways, their names, and a status button.
3. Click on the status button of a gateway to view a list of locks connected to that gateway.
4. To rename a gateway, click on the "Gateway Serial" in the Gateways list. Provide a familiar name, such as "Floor 10 East."
5. Clicking on the Gateway Serial also allows you to delete a gateway if needed.
6. The locks list within the Gateway table provides valuable information for diagnosing lock problems and their connection to the gateway.
7. The locks list displays the lock name, the last time the lock was seen by the gateway, and the last signal level reported by the lock to the gateway.
8. Note that the signal level is measured in decibels (dB), with negative values indicating a poorer quality connection.
9. For example, a -100 dB signal is of poorer quality compared to a -50 dB signal.
10. If the signal level is consistently too low, especially below approximately -90 dB, you may experience intermittent issues with activities like setting PIN codes, remote unlocking, and setting clocks.
11. To achieve optimal results, aim for each lock to have a signal level higher than -85 dB.

Note: The Gateways table provides important information about the connection between gateways and locks, helping to diagnose problems and maintain a stable connection.

Configuring Ipassan Locks for Use with KASAccess

This section provides instructions on configuring Ipassan locks for use with the "KASAccess" system. It covers adding API credentials, syncing access profiles, and integrating Ipassan profiles with KASAccess. Additionally, it explains how to add Ipassan doors to lock groups for simplified key management.

Instructions:

1. Create an API user in Ipassan Manager by following Ipassan's instructions. Grant the API user privileges to add and remove access profiles and users.
2. In KASAccess, navigate to "Doors and Lock" > "Ipassan Profile" on the left-hand side.
3. Click on the "Configure Ipassan" button located in the top right of the screen.
4. Enter your API URL, username, and password (all required) in the provided fields.
5. Click the "Save" button to save the API credentials.
6. Click the green "Retrieve / Refresh Profiles" button. This action retrieves a list of all Ipassan profiles added through Ipassan Manager.
7. Select the desired Ipassan profiles to add to KASAccess and click "Save."
    - Note: If there are multiple pages of profiles, click "Save" after making a selection on each page.
8. The Ipassan profiles will now appear in the profiles list within KASAccess.
9. Take note of the number of doors each Ipassan profile contains in the profile table.
10. When adding keys, the Ipassan access profiles will appear in the locks list.
11. To simplify key management, you can add Ipassan doors to lock groups, similar to adding KAS locks to a lock group.
12. Create a lock group called "Common doors" (or any desired name) and add both Ipassan doors and KAS doors to this group.
13. This grouping allows for easier key addition to multiple doors simultaneously.

Note: By configuring Ipassan locks in KASAccess, syncing access profiles, and utilizing lock groups, you can effectively manage and control access to Ipassan doors within the system.

Fault Diagnosis with KASAccess

This section explains the process of diagnosing problems with locks using KASAccess. It highlights the use of the Queue Table and the Locks Table for fault diagnosis. The instructions cover filtering the Queue Table, reviewing the chronology of events, interpreting icons and colors, and addressing errors. Additionally, it provides information on checking the battery level of locks using the Locks Table and accessing battery reference values in the Events table.

Instructions:

1. To diagnose lock problems, access either the keys list or the Queue Table in KASAccess.
2. The Queue Table is the recommended place for diagnosing lock errors as it provides a complete timeline of the key-to-lock process.
3. Use filters in the Queue Table to assist in the diagnosis:
    - Adjust the date filter if needed to extend the search period.
    - Add an RFID number, pincode, or Key Identifier to the search field and click "Search."
4. Review the displayed information on the screen to see the chronology of events related to the lock, including key additions or deletions and lock responses.
5. Mouse over the yellow or red icons on the right-hand side for additional information about each process.
6. Green icons indicate successful execution of a command, while red indicates a failed command.
7. Multiple red or yellow dots indicate retry attempts. A green dot after yellow dots indicates a successful retry, while a red dot indicates failure.
8. Mouse over the red dot to display an error message indicating the problem that needs to be addressed before attempting a manual retry using the adjacent "Retry" button.
9. For example, an error message like "No gateway" suggests a communication issue between the lock and the gateway, possibly due to low signal strength or depleted batteries.
10. To check the current battery level of a lock, access the Locks Table by clicking on "Doors and Locks" > "ACRs and Locks Menu."
11. The last reported battery level will be displayed in the middle "Battery" column of the Locks Table. Note that this is a calculated value.
12. To obtain the "battery reference" value, click on the "Events" button corresponding to the lock of interest. This will provide the date at which the battery level was last updated.
13. It's important to note that battery levels will only appear in the Events table if the lock has been opened with a pincode or RFID card.

Note: By utilizing the Queue Table, Locks Table, and associated filters, you can effectively diagnose lock-related issues in KASAccess. Understanding the icons, colors, and error messages helps identify and resolve problems, while checking the battery level provides insights into the lock's power status.

Restricting admin access to specific locks

This section provides step-by-step instructions for adding secondary admin users and restricting their access / management to specific locks in your system. This is accomplished by restricting the Staff role according to your specifications and then excluding locks from their management in the users menu.

Instructions:

1. From the "User Configurations" menu on the left select Roles.
2. Select the "Staff" Role to edit the menu visibility.
3. Edit the visibility according to your requirements and save.
4. From the User Configurations menu on the left select the "Users" menu.
5. Create a user and assign the roll of "Staff".
6. Fill out other fields as required.
7. Down the bottom, under the menu "Select Locks to Exclude" select one or more locks to exclude from the users management capacity.

KAS Neo Lock Installation

This section provides step-by-step instructions for installing a KAS Neo lock on a standard fire door. It covers the selection of the correct tubular latch, the direction of the lock's spindle, attaching the front part of the lock, mounting the back plate, securing the power cable, and testing the lock before closing the door.

Instructions:

1. Ensure you have the correct tubular latch that matches the center hole of your lock handle. KAS tubular latches come in backset sizes of 60 mm, 70 mm, and 127 mm. Generic latches won't retract en
2. Take note, generic latches will not retract far enough for use with KAS Neo Locks. If you're replacing an existing tubular latch, remove it and replace it with a KAS tubular latch of the appropriate s
3. Before installation, pay attention to the direction of the spindle on the front part of the Neo lock. The small arrow on the spindle should point directly upwards or downwards based on the handle dire
4. Install the front part of the lock on the door. Thread the battery wire through the center hole of the door and insert the spindle into the corresponding hole in the tubular or mortise latch.
5. Attach the back mounting plate to the rear side of the door. Pass the power cable through either hole in the back plate and secure it with the provided screws.
6. Ensure the power cable is not squashed or pinched, as this may affect the reliable operation of the door. Avoid over-tightening the back plate, as it may cause the door to bind. Tighten only enough to
7. The front of the Neo lock and back plate should now be firmly in place but not overtightened.
8. Insert the power cable into the rear half of the lock and secure the rear half to the back plate using the remaining three screws.
9. Install the batteries in the lock.
10. IMPORTANT: Do not close the door yet**. Test the lock to ensure it unlocks correctly before closing the door.** This step ensures that any potential issues can be addressed without the door being cl

Fire Door Installation

When installing a KAS Neo lock on a fire door, additional steps must be taken to comply with fire safety regulations. A Fire Door Kit, including intumescent material, is required to enhance the fire door's effectiveness. The installation process is similar to that of a regular door, with attention given to the direction of the square spindle on the lock to ensure proper operation.

Instructions:

1. Obtain a Fire Door Kit specifically designed for the KAS Neo lock installation on fire doors.
2. Prepare the fire door by following the necessary fire safety guidelines and regulations.
3. Take the two pieces of intumescent material from the Fire Door Kit.
4. Locate the hole drilled for the Neo Lock handle on the fire door.
5. Install the intumescent material inside the hole, ensuring it is placed securely and evenly.
6. The intumescent material expands when exposed to heat during a fire event, enhancing the fire door's performance.
7. Proceed with the installation of the KAS Neo lock on the fire door following the same steps as for a regular door, ensuring the square spindle direction is facing directly up or down, but not sideways
8. Securely attach the front part of the lock to the fire door, taking care to align the spindle correctly.
9. Complete the installation process as described in the previous section.

Note: Installation on a fire door requires the use of a Fire Door Kit and the inclusion of intumescent material. Ensure the arrow on the square spindle is facing directly up or down during the installation process. By following these guidelines, you will ensure compliance with fire safety regulations and maintain the proper operation of the KAS Neo lock on the fire door.

Management Codes

Management codes are special codes known only to property managers. These codes allow property managers to program new PIN codes or RFID cards onto the lock face without the need for gateways. However, the management code itself cannot be used to directly access the lock. It is essential to keep the management code secret and change it from the default code as soon as the lock is installed.

- The management code is a confidential code that enables property managers to add new PIN codes or RFID cards to the lock without the use of gateways.

- **Keep the management code secure:** It is crucial to treat the management code as highly confidential information. Only property managers should have knowledge of this code.
- **Change the default management code:** Upon lock installation, it is recommended to change the default management code immediately. This ensures that unauthorized individuals cannot access the
- **Use the management code for programming:** To add new PIN codes or RFID cards to the lock, access the lock's programming interface using the management code. This allows property manager
- **Do not use the management code for direct access:** Remember that the management code itself cannot be used to directly access the lock. It is solely for the purpose of programming new PIN cod
- **Maintain strict control over the management code:** Limit the number of individuals who have knowledge of the management code and regularly review and update access privileges as needed.
- **Periodically change the management code:** To enhance security, consider changing the management code periodically. This helps prevent unauthorized access in case the code is compromised.
- **Document the management code securely:** Store the management code in a secure location, such as a password-protected digital file or a locked physical storage, ensuring that only authorized indi

Note: The management code is a vital tool for property managers to manage access to the lock. By keeping the management code confidential, changing it from the default code, and using it solely for programming purposes, property managers can ensure the security and integrity of the lock system.

To change the management code in the KAS Neo lock, follow these steps:

1. Start with the default management code: **888888#.
2. Enter the default management code followed by the number five: **888888#5.
3. Input the new 4 to 6 digit code that you want to set as your new management code. For example, let's say you want to set the code as 12345. Enter the new management code: **888888#5 12345#.
4. Ensure that you enter the commands in quick succession to prevent the lock from timing out during the process.
5. Once you've entered the new management code, it will replace any instances where the default management code (**888888#) was previously used. For example, if you were instructed to enter **88

Remember to keep your new management code secure and change it periodically for enhanced security.

Gateways

Gateways in KASAccess are devices used for communication between KASAccess and KAS Neo locks and devices. They can connect to the internet via Ethernet or Wi-Fi and use a sub-1 Gigahertz wireless signal to communicate with the locks. Placing the gateways within approximately 15 meters of the locks is recommended for optimal signal strength. Gateways can be powered via Power over Ethernet (POE) or with a 240V power transformer. Configuring Wi-Fi access for each gateway is done individually through the KASAccess App. The gateway's status lights indicate its connectivity and readiness for use.

Summary:

- **Purpose of Gateways**: Gateways serve as communication devices between KASAccess and KAS Neo locks and devices, enabling remote management and control.
- **Powering the Gateway**: Gateways can be powered through Power over Ethernet (POE) using a compatible switch or with a 240V power transformer. Ensure proper power supply based on your setu
- **Gateway Placement**: Place the gateway within approximately 15 meters of the locks you want it to communicate with, ensuring a clear line of sight for optimal signal strength.
- **Gateway Configuration**: Before configuring a gateway, it must be added to your KASAccess Account via the KASAccess App. If the gateway is new, power it on and select the Setup > Bluetooth S
- **Resetting the Gateway (if necessary)**: If you are migrating from a Generation 1 Console to KASAccess, you may need to reset the gateway before activating it. Hold down the small black button on
- **Configuring Wi-Fi Access**: After selecting the gateway in the KASAccess App, choose the "configure" option. Enter the Wi-Fi SSID and password, ensuring correct capitalization. Save the configu
- **Gateway Status Lights**: The internal status light on the gateway indicates its connectivity. A flashing red light indicates no internet connection, possibly due to incorrect Wi-Fi credentials or no inter
- **Naming the Gateway**: It is recommended to name the gateway during installation for easy identification. In the KASAccess App, navigate to Gateways, select the specific gateway, choose the "conf

Note: Gateways play a crucial role in enabling communication between KASAccess and KAS Neo locks. Proper placement, power supply, and configuration of gateways ensure reliable connectivity and efficient management of the lock system.

Stand Alone Mode

Operating your lock through codes on the face of the lock (Stand Alone).

To add a code to the face of the lock, follow these steps:

1. Dial the management code or **888888# into the face of the lock. If your management code is set to "1234," you would dial **1234#.
2. Enter the position number. For example, if you want to assign the backup code to position 01, enter "6" and then “01" after the management code. 6 tells the lock you want to add a pin code, 01 is th
3. Enter a 4-digit code of your choice. Let's use "7711" as an example. Dial "7711#" after entering the position number from the previous step.
4. A full example of the above steps is **888888# 6 01 7711#

5. The backup code has now been set. You can use this code at any time, even without the presence of a gateway or internet access. It serves as a backup in emergency situations.

Please note that codes or cards entered directly into the lock face do not rely on the lock's internal clock and will always work, regardless of the time. The only scenario in which they will not work is when the lock's batteries are completely drained.

The following instructions provide a summary as to the settings which can be changed at the face of the lock. Follow the same format as the example above to make changes as required.

Please note if you have changed the management code, <Management Code> should be replaced with your new management code when executing the following commands.

- Single Opening Mode
  - Either 1 card or 1 pin code will open the door.
  - **Enable Single Opening Mode:** ** <Management Code> # 141 #
- Dual Opening Mode
  - Requires both RFID Card and pincode to be presented for the same User IDs.
  - **Enable Dual Opening Mode:** ** <Management Code> # 142 #

Features

- Free Passage Mode
  - **Enable Free Passage:** <User Pin Code> # or <Swipe RFID Card> and press and hold # for 3 seconds after the lock is opened.
  - **Disable Free Passage:** Wake the keypad, press and hold * for 3 seconds or present any valid card to the lock.
- Keypad Lockout
  - The keypad will lockout for 1 minute if a pin code was entered incorrectly 3 times.

Management Instructions - Local

- Management Code
  - Default Management Code: 888888
  - **Set Management Code:** ** <Management Code> # 5 <New Management Code> #
- Pin Code
  - **Set Pin Codes:** ** <Management Code> # 6 <User ID> <User Pin Code> #
  - **Delete Individual User Pin Code:** ** <Management Code> # 7 <User ID> #
  - **Delete All User Pin Codes:** ** <Management Code> # 666 #
- RFID Card & Fob
  - **Set User RFID Card:** ** <Management Code> # 2 <User ID> # <Swipe RFID Card>
  - **Delete User RFID by ID:** ** <Management Code> # 3 <User ID> #
  - **Delete All User RFID:** ** <Management Code> # 444 #
  - **Delete User RFID by Reading Card:** ** <Management Code> # 8 # <Swipe RFID Card To Delete>
  - **Delete User RFID by Continuously Reading Cards**: ** <Management Code> # 888 # <Swipe Card 1> <Swipe Card 2> ...

Factory Reset

- **Factory Reset By Keypad:** ** <Management Code> # 199 #

Further ACR Customizations

- Standalone/Console Mode Only
  - **Location Light Off:** ** <Management Code> # 151 #
  - **Location Light Remains On:** ** <Management Code> # 152 #
  - **Keypad Enters Sleep Mode:** ** <Management Code> # 161 #

- **Keypad Always Remains On:** ** <Management Code> # 162 #
- **Pin Code Input Delay Time:** 0.5 seconds - ** <Management Code> # 171 #
- **Pin Code Input Delay Time:** 1.0 second - ** <Management Code> # 172 #
- **Pin Code Input Delay Time:** 1.5 seconds - ** <Management Code> # 173 #