Kwikset UNITE™ Software Reference Guide

INTRODUCTION

The Kwikset UNITE™ software and web-enabled platform provides convenient and efficient access control for your multifamily property. The Kwikset UNITE™ software platform is an intuitive cloud-based web and mobile solution. Property managers can use the desktop dashboard for quick and easy access control or the mobile app for on-the-go management. Residents may enjoy simple and secure access to their homes through the mobile app. With Kwikset UNITE™ software, you're in control of your property.

TABLE OF CONTENTS

Version History

Version	Date	Summary of Changes
1.00	28AUG2024	Initial Release

GENERAL UNITE ACCOUNT AND SOFTWARE

I. Software and Application Access

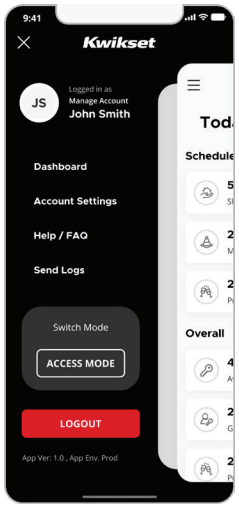
A. Kwikset UNITE is an invitation-based multifamily property management ecosystem. The initial invitation into the system stems from a Kwikset team member in contact with the initial property owner, developer, or system integrator. Once system access has been handed over to this initial party, additional invitations are processed and handed out by them to subsequent users throughout the property's hierarchy.

B. The UNITE mobile application may be found in the iOS and Google Play Stores here:

1. Note: All users within the UNITE ecosystem may use this mobile application to engage with the system regardless of user authority.
2. Users may log into the interface via the credentials that they were presented with when invited into the system.

C. The UNITE Property Management Web Portal may be found here: Multi Family (KwiksetUnite.com)

1. Note: The UNITE Property Management Web Portal is only for Property Manager user types within the system. It is used to engage with and manage the property and is therefore not available to residents.
2. Users may log into the interface via the credentials that they were presented with when invited into the system.



(Fig. 1.1)

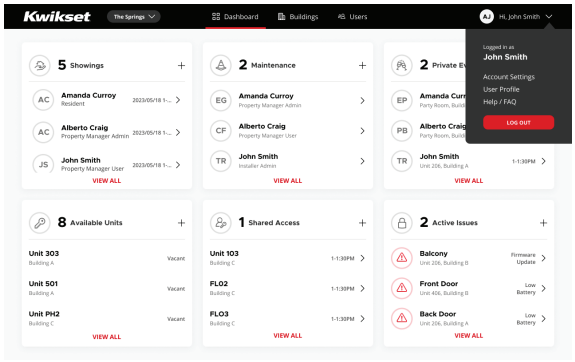
II. Log Out

A. UNITE Mobile Application

1. Users may find the log out function of the UNITE Mobile Application within the drop down menu in the upper left hand corner of the landing page. *(Fig. 1.1)*

B. UNITE Property Manager Web Portal

1. Users may log out of the UNITE property Manage Web Portal by selecting the circle with their initials present in the upper right hand section of the interface. *(Fig. 1.2)*
2. From this menu selection, the option to Log Out will be present.

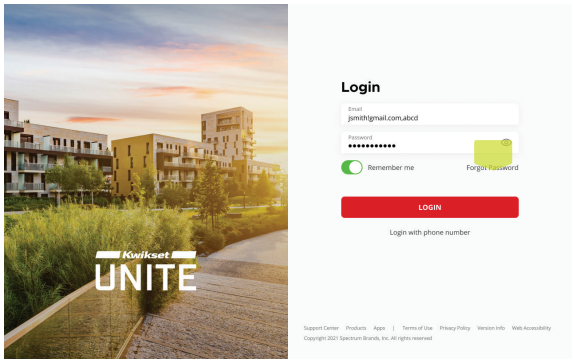


(Fig. 1.2)

III. Forgot Password

A. UNITE Property Management Web Portal

1. Users of the Property Management Web Portal that may have forgot their password may recover access via the following process:
   a. Visit Multi Family (KwiksetUnite.com)
   b. Enter the Email address associated with the account in question.
   c. Click the “Forgot Password” link located on the lower right hand side below the Password entry field. *(Fig. 2.1)*

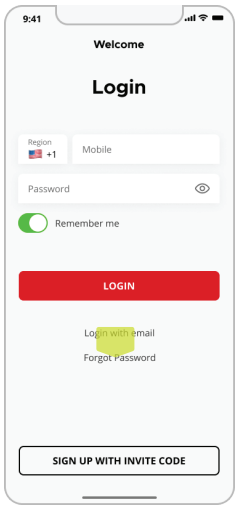


(Fig. 2.1)

   d. This will trigger a verification process, whereas a code will be sent to the email on file.
   e. Confirm the code, and a prompt to reset the password will be triggered.

B. UNITE Mobile Application

1. Users of the UNITE Mobile Application that may have forgot their password may recover access via the following process:
   a. Open the UNITE Mobile Application.
   b. Enter the Email address associated with the account in question
   c. Click the “Forgot Password” link located on the lower right hand side below the Password entry field. *(Fig. 2.2)*
   d. This will trigger a verification process, whereas a code will be sent to the email on file.
   e. Confirm the code, and a prompt to reset the password will be triggered.



(Fig. 2.2)

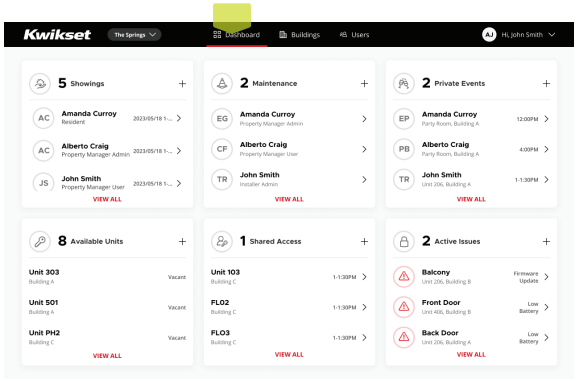
IV. Navigation

UNITE Property Manager Web Portal

A. Upper Control Bar

1. Site Selection

a. Property Managers within UNITE may be invited to as many different properties as their role requires. While one may have multiple accounts, UNITE offers the ability for users to maintain access to multiple sites from a single account and interface. *(Fig. 3.1)*



(Fig. 3.1)

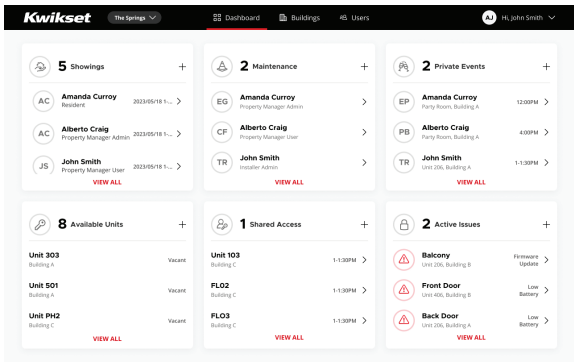
b. From the Upper Control Bar, one will see the name of their property listed in the upper left section to the right of the “Kwikset” branding.

i. If one have access to multiple sites, they may click the property name and a drop down list of their other sites will present itself.

ii. One may select the site that they wish to view, and the system will route the user to the dashboard and all subsequent site information for that property.

2. Dashboard

a. The Dashboard is the landing page for property managers within UNITE, and the user interface will always default the Dashboard upon logging in. As the UNITE Property Manager Web Portal is only accessible by Property Managers within the property, this dashboard is designed to quickly and easily relay all of the information which those responsible for the day-to-day operations of the site may need. *(Fig. 3.2)*

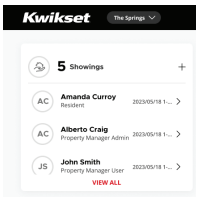


(Fig. 3.2)

b. Included within the Dashboard are interactive tiles intended to communicate various scheduled aspects of interest within the property. These tiles include:

i. Showings

- The Showings tile communicates the name of users tagged to view a unit onsite. It includes the time of their tour event within a chronological list of other showings in the short-term future. *(Fig. 3.3)*
- Users may be conveniently tagged to the “Showings” tile during initial configuration or via their respective user profile detail page at any time.



(Fig. 3.3)

ii. Maintenance

- The Maintenance tile may be used to tag users within the system to a maintenance event onsite. Whether it be a worker onsite or a resident with an issue, tagging a user to the Maintenance tile signifies that there is an upcoming event requiring attention.
- Users may be conveniently tagged to the “Maintenance” tile during initial configuration or via their respective user profile detail page at any time. *(Fig. 3.4)*

iii. Private Events

- Property Managers may tag users to the Private Events tile to denote unique access rights for users which are above or beyond their normal. It is intended to help easily visualize and organization onsite events such as parties or special events. *(Fig. 3.5)*
- Users may be conveniently tagged to the “Private Events” tile during initial configuration or via their respective user profile detail page at any time.

iv. Available Units

- This tile will show units which do not have Resident or Installer access rights associated with them. They are vacant units. *(Fig. 3.6)*

v. Shared Access

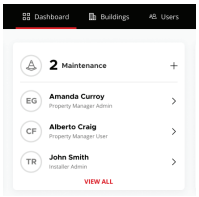
- This tile will show units in which access rights for Resident Users have been shared by Resident Admins. The intention is to communicate units in which users have been added by users other than Property Management. *(Fig. 3.7)*

vi. Active Issues

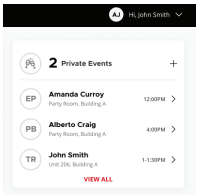
- Ongoing issues with components of the system will be communicated here. This is meant to share system-wide updates on urgent issues requiring attention. *(Fig. 3.8)*

vii. Remaining Invitations

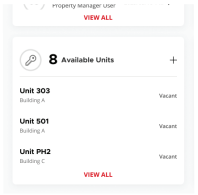
- This will share the remaining number of invitations allocated to the site. Each site begins with 250 invitations by default, with this number decreasing for each user invited into the stem by a Property Manager or Installer. Invitations can be added to a site by contacting Kwikset sales personnel. *(Fig. 3.9)*



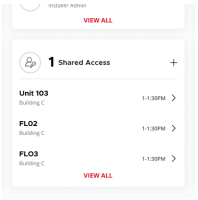
(Fig. 3.4)



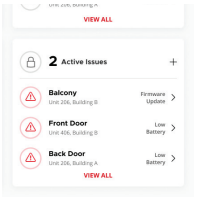
(Fig. 3.5)



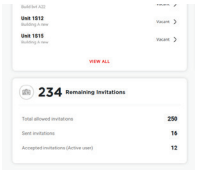
(Fig. 3.6)



(Fig. 3.7)



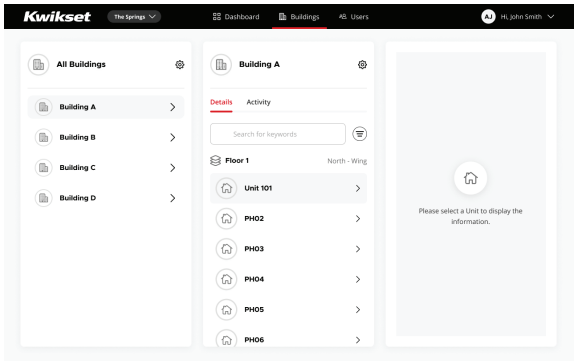
(Fig. 3.8)



(Fig. 3.9)

c. Buildings

i. Navigation to this section of the interface enables users to engage with the physical configuration of the site. From here, users are able to add, edit, and delete all building related configuration details enabled by their user authority. *(Fig. 3.10)*



(Fig. 3.10)

ii. The user flow of this portion of the interface operates from left to right, with users being able to expand upon details of their site by opening selecting aspects of their buildings.

iii. At any point in their engagement with the Buildings section, users may select the "gear" icon to switch from a viewing mode to a configuration mode. They will then be able to make changes to the site's configuration as they see fit.

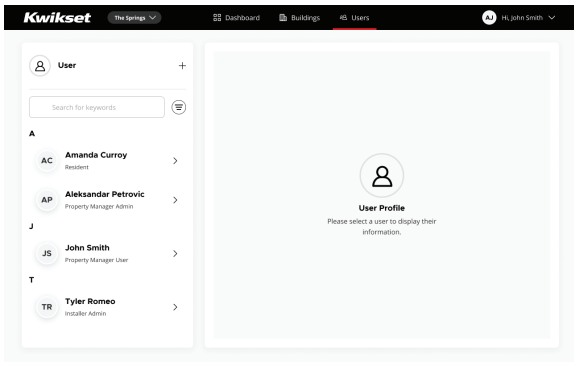
B. Users

1. Account Settings and Help/FAQs

a Users may access their Account Settings and User Profile by clicking on the circle with their initials present in the upper right-hand section of the page.

i. Account Settings

- From the Accounts Settings selection, the user will be to view and modify aspects of their UNITE experience such as accessibility and personal information. *(Fig. 3.11)*

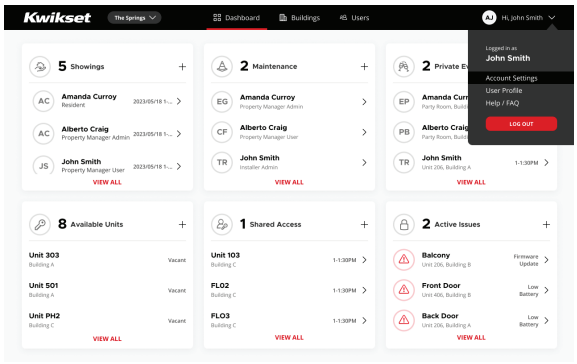


(Fig. 3.11)

ii. User Profile

- From the User Profile selection, users will be able to view their respective access right, history, and credential information.

2. General interface assistance may be accessed via the Help/FAQ section of this menu. *(Fig. 3.12)*



(Fig. 3.12)

Kwikset UNITE™ USERS

USERS

I. User Types and Authority

A. User access rights within the system, including exposed functionality, are organized within the following user types:

	Consumer/Property Manager Web Portal & App Level Users										
	Property Manager				Installer				Resident		
User Types	Property Manager Admin		Property Manager User		Property Manager Admin		Property Manager User		Admin		User
Interface	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Mobile
User Management											
Logout	X	X	X	X		X		X		X	X
Recover Own Password	X	X	X	X		X		X		X	X
Change Own Password	X	X	X	X		X		X		X	X
Management Profile Overview Home Page (i.e. view Dashboard)	X	X	X	X							
Installer Overview Home Page (i.e. start on building overview)						X		X			
Tenant Overview Home page (i.e. End-User Dashboard)										X	X
Add new users to the Customer Account Management Portal											
Edit users in the Customer Account Management Portal											
Delete users from the Customer Account Management Portal											
Access Management											
Lock/Unlock devices which they are authorized for	X	X	X	X		X		X		X	X
Delete UNITE account											
Add Property Manager Admin	X	X									
Edit Property Manager Admin	X	X									
Delete Property Manager Admin	X	X									
Add Property Manager User	X	X									
Edit Property Manager User	X	X									
Add Installer Admin	X	X	X	X							
Edit Installer Admin	X	X	X	X							
Delete Installer Admin	X	X	X	X							
Add Installer User	X	X	X	X		X					
Edit Installer User	X	X	X	X		X					
Delete Installer User	X	X	X	X		X					
Add Resident Admin	X	X	X	X							
Edit Resident Admin	X	X	X	X							

* This specific item is broken down into more detailed in the subsequent sheet entitled “User Profile Access.” It is with a number of specific rules per user type so it needed to be outlined in more detail.

	Consumer/Property Manager Web Portal & App Level Users										
	Property Manager				Installer				Resident		
User Types	Property Manager Admin		Property Manager User		Property Manager Admin		Property Manager User		Admin		User
Interface	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Mobile
Access Management (continued)											
Delete Resident Admin	X	X	X	X							
Add Resident	X	X	X	X						X	
Edit Resident	X	X	X	X						X	
Delete User account	X	X	X	X						X	
Edit Property Manager Admin Access Rights	X	X									
Edit Property Manager User Access Rights	X	X									
Edit Installer Admin User Access Rights	X	X	X	X							
Edit Installer User Access Rights	X	X	X	X		X					
Edit Resident Admin Access Rights	X	X	X	X							
Edit Resident User Access Rights	X	X	X	X						X	
Assign physical credential to a Property Manager Admin	X	X									
Edit physical credential of a Property Manager Admin	X	X									
Delete physical credential from a Property Manager Admin	X	X									
Assign physical credential to a Property Manager User	X	X									
Edit physical credential of a Property Manager User	X	X									
Delete physical credential from a Property Manager User	X	X									
Assign physical credential to an Installer Admin	X	X	X	X							
Edit physical credential of an Installer Admin	X	X	X	X							
Delete physical credential from an Installer Admin	X	X	X	X							
Assign physical credential to an Installer User	X	X	X	X		X					
Edit physical credential of an Installer User	X	X	X	X		X					
Delete physical credential from an Installer User	X	X	X	X		X					
Assign physical credential to a Resident Admin	X	X	X	X							
Edit physical credential of a Resident Admin	X	X	X	X							
Delete physical credential from a Resident Admin	X	X	X	X							
Assign physical credential to a Resident	X	X	X	X							
Edit physical credential of a Resident	X	X	X	X							
Delete physical credential from a Resident	X	X	X	X							
View User Profile (own)*	X	X	X	X		X		X		X	X

* This specific item is broken down into more detailed in the subsequent sheet entitled “User Profile Access.” It is with a number of specific rules per user type so it needed to be outlined in more detail.

	Consumer/Property Manager Web Portal & App Level Users										
	Property Manager				Installer				Resident		
User Types	Property Manager Admin		Property Manager User		Property Manager Admin		Property Manager User		Admin		User
Interface	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Mobile
Access Management (continued)											
View User Profile (others)*	X	X	X	X		X		X		X	
View / Sort User*	X	X	X	X		X		X		X	
Search User	X	X	X	X		X		X		X	
Add Group	X	X	X	X		X					
Edit Group	X	X	X	X		X					
Delete Group	X	X	X	X		X					
Filter by Group	X	X	X	X		X		X		X	
Property Details											
Add Site											
Edit Site	X	X									
Delete Site											
Add Building	X	X	X	X		X		X			
Edit Building	X	X	X	X		X		X			
Delete Building	X	X	X	X		X		X			
Add Floor	X	X	X	X		X		X			
Edit Floor	X	X	X	X		X		X			
Delete Floor	X	X	X	X		X		X			
Add Unit/Access Point	X	X	X	X		X		X			
Edit Unit/Access Point	X	X	X	X		X		X			
Delete Unit/Access Point	X	X	X	X		X		X			
Site Toggle (i.e. switch between sites in the system)	X	X	X	X		X		X			
View Buildings	X	X	X	X		X		X			
View all Event History/Activity for all user groups for the Units that they are assigned to	X	X	X	X		X		X		X	
View all Event History/Activity for all user groups for the Access Points that they are assigned to	X	X	X	X		X		X			
Device Management											
Add a Unit Lock	X	X	X	X		X		X			
Edit a Unit Lock	X	X	X	X		X		X			
Delete a Unit Lock	X	X	X	X		X		X			
View Unit Lock Details	X	X	X	X		X		X		X	

* This specific item is broken down into more detailed in the subsequent sheet entitled “User Profile Access.” It is with a number of specific rules per user type so it needed to be outlined in more detail.

	Consumer/Property Manager Web Portal & App Level Users										
	Property Manager				Installer				Resident		
User Types	Property Manager Admin		Property Manager User		Property Manager Admin		Property Manager User		Admin		User
Interface	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Web	Mobile	Mobile
Device Management (continued)											
Add an Access Point Device	X	X	X	X		X		X			
Edit an Access Point Device	X	X	X	X		X		X			
Delete an Access Point Device	X	X	X	X		X		X			
View Access Point Device Details	X	X	X	X		X		X			
Perform a Device Firmware Update	X	X	X	X		X		X			
Perform a Device Factory Reset	X	X	X	X		X		X			
Test Locks at the factory level											
View lock settings, lock name	X	X	X	X		X		X		X	
Edit lock settings, lock name	X	X	X	X		X		X			
View lock settings, secure mode	X	X	X	X		X		X			
Edit lock settings, secure mode	X	X	X	X		X		X			
View lock settings, operation window	X	X	X	X		X		X			
Edit lock settings, operation window	X	X	X	X		X		X			
View lock settings, lock sound	X	X	X	X		X		X		X	
Edit lock settings, lock sound	X	X	X	X		X		X		X	
View lock settings, User Access	X	X	X	X		X		X		X	
Edit lock settings, User Access	X	X	X	X		X		X		X	
View lock settings, Activities	X	X	X	X		X		X		X	
Edit lock settings, Activities	X	X	X	X		X		X		X	
View lock settings, Block Credential	X	X	X	X							
Edit lock settings, Block Credential	X	X	X	X							
View lock settings, Lock Info	X	X	X	X		X		X		X	
Edit lock settings, Lock info	X	X	X	X		X		X			
View lock settings, Firmware Updates	X	X	X	X		X		X			
Edit lock settings, Firmware Updates	X	X	X	X		X		X			
View lock settings, FAQ	X	X	X	X		X		X		X	
Edit lock settings, FAQ	X	X	X	X		X		X			
Other											
Notification of Error States (as per authority level)	X	X	X	X		X		X		X	
Access to FAQ in UI (as per authority level)	X	X	X	X		X		X		X	X

* This specific item is broken down into more detailed in the subsequent sheet entitled “User Profile Access.” It is with a number of specific rules per user type so it needed to be outlined in more detail.

Property Manager Admin

The Property Manager Admin has all privileges for the property, buildings, and units, and thereby all locks and devices in the property. Property Manager Admin's have the privilege to add and manage properties, buildings, and units in the system. User management and control for each User type is also fully accessible for the Property Manager Admin. This user has full control to add, edit, or remove access for other Property Manager Admins, in addition to all other user types. The ability to modify other Property Manager Admins at the same authority level make this user type unique. This functionality is enabled to assist with the hand-off of properties from one site owner to another. As locks and devices are commissioned into a site, the Property Manager Admin for that site will automatically be assigned full access. They will also have full visibility to all features and elements within the Kwikset UNITE EAC platform. This user type has access to both the Property Management Portal and the UNITE mobile app.

Property Manager User

Property Manager User has the next highest level of privileges. Property Manager Users can add and manage at the building level, down to units, locks (entry points), and devices, while also controlling access rights for the user groups beneath them in the user hierarchy. Property Manager Users cannot add or edit a User at or above their level (i.e. they may only edit the following user types: Installer Admin, Installer User, Resident Admin, and Resident User). Property Manager Users cannot add, edit, or delete sites. This user type has access to both the Property Management Portal and the UNITE mobile app.

Resident User

A Resident User is the lowest authority level within the system. It is a user type that may only view, lock, and unlock the units/access points that they have been assigned to. They do not have the ability to modify any system parameters. They only have access to the UNITE mobile app.

II. Inviting a User and Getting them Started

A. Users may be invited and configured within the system via the following process:

1. Via the Property Management Web Portal
    a. Login to the Portal. User will be navigated to the Dashboard screen.
    b. Tap on the Users option from the upper control bar.
    c. Tap on the "+" icon in the upper portion of the left most "Users" tile. An "Add User" pop up will appear
    d. Enter the email id of the user to be added/invited and Tap on the "continue" Button.
        i There is a search function on this pop up if the user is unsure whether they already have account. One may search out existing accounts via this entry field, but may otherwise continue with a new email account.
    e. Enter the first and last name of the User, select "Continue", then select the User type from the following page.
        i. User type descriptions may be found in the previous section of this reference guide.

f. Property Managers will have comprehensive access rights over the entire site. If inviting a non-Property Manager user type, one may assign access via the presented building hierarchy.
    i. Users may select the time parameters for this user once access rights are assigned. If “skip” is selected, the user will be a permanent user within the system.
        • There is also the ability to repeat schedules in this window as outlined in the pop up window once toggled.
    ii. The selected access rights, with the associated scheduling parameters, will be reflected on the next page.
g. With authority and access rights configured, the invitation is ready to be sent. Enter a valid Phone number and tap on “Share Access with User” Button from this final page.
h. The user will be added into the selected UNITE site, with their information reflected within site details immediately.
    i. The invited user will receive an email containing the information to access their invitation and create their account. They will also receive an informative SMS informing them of this.

2. Via the UNITE Mobile Application:
    a. Login to the App. The user will be navigated to the Dashboard landing page.
    b. Tap on the “Users” icon on the lower portion of the dashboard.
    c. Tap on the “+” icon in the upper left hand portion of the Users section. The user will be redirected to the “New User” page.
    d. Enter the email id of the user to be added/invited and Tap on the “Continue” Button.
    e. Enter the first and last name of the User and select the User type from the drop down.
        i. User type descriptions may be found in the previous section of this reference guide.
        ii. Toggle “Set this User as an Admin” option to set or remove the user type as an Admin type.
        iii. Property Managers will have comprehensive access rights over the entire site. If inviting a non-Property Manager user type, one may assign access via the presented building hierarchy.
            • Users may select the time parameters for this user once access rights are assigned. If “Continue” is selected with no revision, the user will be a permanent user within the system.
            • There is also the ability to repeat schedules in this window as outlined once engaged.
            • The selected access rights, with the associated scheduling parameters, will be reflected on the next page.

f. With authority and access rights configured, the invitation is ready to be sent. Enter a valid Phone number and tap on “Share Access with User” Button from this final page.

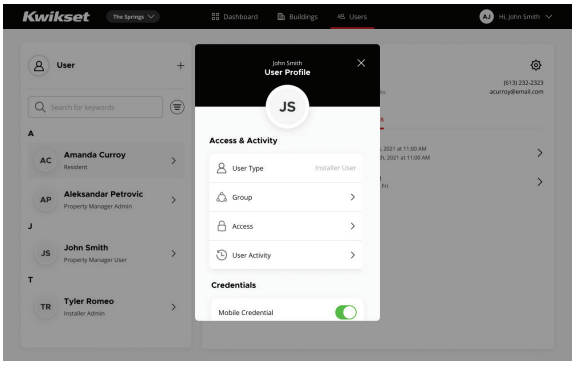
g. The user will be added into the selected UNITE site, with their information reflected within site details immediately.

i. The invited user will receive an email containing the information to access their invitation and create their account. They will also receive an informative SMS informing them of this.

III. Display and Edit User Information

A. Via the Property Manager Web Portal

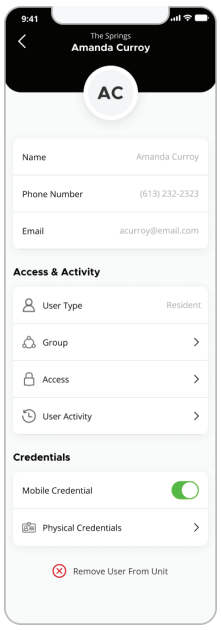
1. Property Managers may view and edit the information and configuration of other users via the “Users” section. *(Fig. 4.1)*
2. From the Dashboard, select the “Users” option from the Upper Control Bar.
3. Via the list of users on the left hand side of the page, select the user to view or edit.
4. From the user’s detail page now populating the right hand portion of the page, Property Managers may view that user’s access rights.
5. To edit any configuration details of this user, one may select the icon of a gear in the upper right hand corner of the user’s detail page.



(Fig. 4.1)

B. Via the UNITE Mobile Application

1. Property Managers may view and edit the information and configuration of other users via the “Users” section.
2. From the Dashboard, select the “Users” icon on the bottom of the page.
3. Via the list of users, select the user to view.
4. One may then view and edit any details of that user. *(Fig. 4.2)*



(Fig. 4.2)

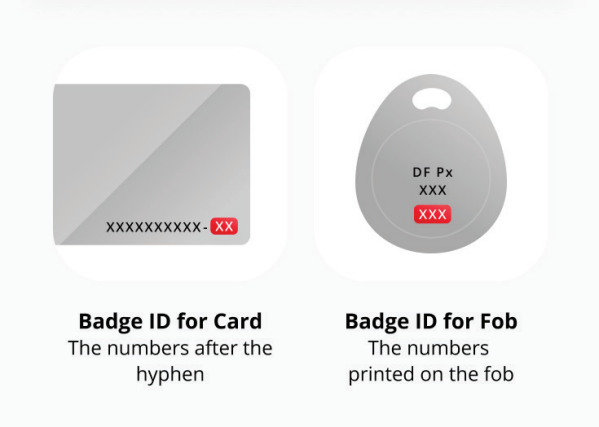
IV. Adding Physical Credential

A. Prerequisites:

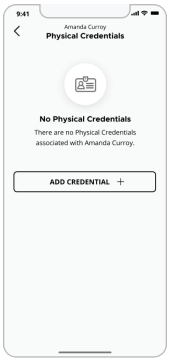
1. When assigning a physical credential to a user, that user needs to be in the system and have access rights for the locks that will be linked to the credential.
2. A credential enroller is onboard every UNITE lock. Property Managers must be within Bluetooth range of a lock in order to enroll a physical credential.
3. The fob or card being used must be a UNITE credential with Badge ID present on the face of the credential.

B. Things to note:

1. Any commissioned lock in a site may be used for the physical credential enrollment process. UNITE features a seamless enrollment process that does not require the user to engage with the lock gaining access rights from the credential. This means that user may enroll a physical credential, hand it off to the receiving user, and that user may go to the lock in question without having to engage with it prior.
2. The physical credential process may only be performed via the UNITE Mobile Application, as it requires a secure connection with a UNITE lock.
3. The Badge ID will be written on the lower right hand corner of the lock.
4. For Cards, the Badge ID may be up to five digits, and will be found to the right of the hyphenated numbers present on the card. *(Fig. 5.1)*
5. For fobs, the Badge ID will be on the bottom row of the numbers printed on the fob. *(Fig. 5.2)*
6. Credentials may be overwritten or reused, both for the same user or for others, as much as desired.



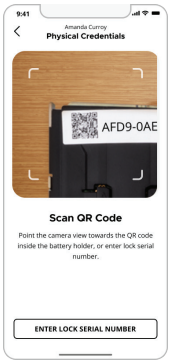
(Fig. 5.1) *(Fig. 5.2)*



(Fig. 5.3)

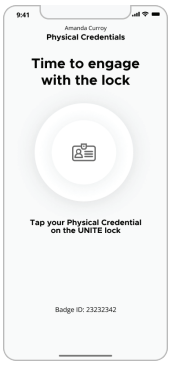
C. Enrollment Process

1. Login to the Unite Mobile Application and navigate to the Users section.
2. Select User's Profile for which the Card/Fob will be encoded. (It can be either done directly from Users tab or from the Users list inside Unit details under a Building). *(Fig. 5.3)*
3. Scroll to the "Physical Credentials" option in that user's profile.
4. Tap on the "Add Physical Credential" Button.
5. Enter a reference name for the credential and enter the Badge ID from on the fob or card, then select "Continue."
6. Either scan the QR code of the lock being used for this process, or enter in the lock's serial number. This is just the lock being used to enroll the credential, with no access rights being transferred at this stage. *(Fig. 5.4)*
7. Select the access rights desired for the credential, and select "Continue."

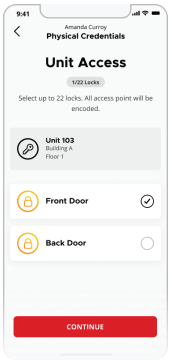


(Fig. 5.4)

8. Acknowledge the “Before you Start” notices, and select “Continue.” One will be presented with a notice confirming that the credential will be overwritten. This means that any access rights already on the credential will be erased and a new configuration will be written onto the credential. Select “Continue” to acknowledge.
9. It is now time to present the credential to the lock. Hold the credential up to the lock and hold it up to the lock (within 5mm, but touching the face plate is preferred) until a blue gear icon lights up on the lock. Keep the credential in place until the gear icon turns green. *(Fig. 5.5)*
    a. Notice: A red flashing LED means that the credential was not initially read correctly. If this occurs, please pull the credential back and present it again.
    b. Notice: If the gear icon turns from blue to red, then the enrollment process did not complete properly. The credential may initially function as desired, but unexpected behavior may result. Please re-encode the credential by selecting the credential and re-starting the process if this occurs to ensure optimal performance.
10. The credential is now enrolled, and will be displayed in that user’s list of physical credentials, and will be represented in the site’s audit trail with that user. *(Fig. 5.6)*



(Fig. 5.5)



(Fig. 5.6)

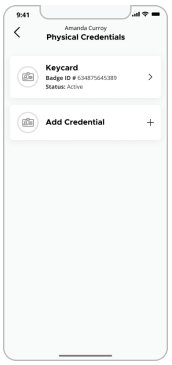
V. Lock or Unlock using Fob or Card

A. Prerequisites:
1. The lock in question has been fully commissioned into the site Activated Lock.
2. The user has access rights to the lock in question.
3. The user has a physical credential encoded with access rights for the lock in question.

B. Engagement Process:
1. Present the credential within 5mm of the lock to the location between the “Kwikset” logo and the turn piece.
2. If access rights are correctly encoded, the lock will recognize the credential and flash a green light with an accompanying beep sound.
3. The turn piece may then be turned clockwise to lock the device or counter-clockwise to unlock. *(Fig. 5.7)*
4. By default, the Operation Window, being the time for which the turn piece remains engageable, is set to five seconds. This Operation Window may be revised within the lock’s settings under the “Buildings” section, up to a maximum of 30 seconds.

(Fig. 5.7)

5. Once the Operation Window closes, a red LED will flash on the lock. After that lock/unlock will not be possible unless scanned again.



(Fig. 5.8)

VI. Blocking Physical Credential

A. To remove a card or fob, the physical credential must be added to a "Block List" within each respective lock. UNITE locks maintain a list of authenticated credentials, and this list must be edited to block an existing credential from maintaining access.

1. Important notes:

a. One must update each lock's blocklist to ensure that the physical credential's access rights are properly removed

b. Blocking a physical credential may only be completed via the UNITE Mobile Application, as the process requires a secure connection to the lock via the application.

B. Process for Blocking a Physical Credential:

a. Login to the UNITE Mobile Application and navigate to the Users section.

b. Select the User's Profile associated with the card or fob that needs to be blocked. (It can be either done directly from the Users section or via the list of users associated with a unite within the Buildings section).

c. Scroll to the "Physical Credentials" option in the user's detail page.

d. Select the Physical Credential that needs to be blocked. *(Fig. 5.8)*

e. Tap the Add to Block List button on the card details screen and click Yes on the Confirmation fly-out. *(Fig. 5.9)*

f. Select the card that needs to be blocked from the pending list of Blocklist screen and tap on setup central card button. *(Fig. 5.10)*

   i. A “Central Card” is a credential that is encoded with the data needed to update a lock’s blocklist. Any standard user credential (card or fob) may be configured as a “Central Card.” This updater type credential enables users block credentials regardless of whether the credential being blocked is physical accessible.

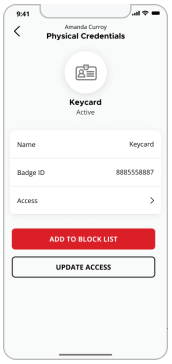
g. Enter the Badge ID of the central card to be used for blocking and click the “Add” button.

h. Scan the QR code of the lock being used as the encoder for blocking the physical credential and click the “Continue” button. *(Fig. 5.11)*

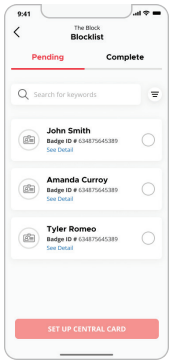
i. Engage the central card with the lock once a beep is heard from the lock. As with adding a credential, a gear icon will light blue and then green to confirm that the process has successfully completed. *(Fig. 5.12)*

j. With the “Central Card” created and encoded, one must now present this card to each lock where access is being removed.

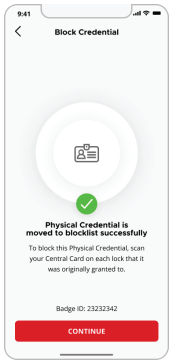
   i. Important Note: credentials are not blocked until all necessary locks have been presented with this “Central Card.”



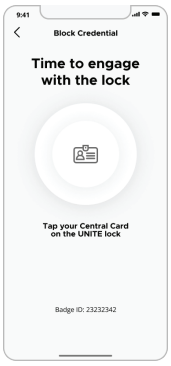
(Fig. 5.9)



(Fig. 5.10)



(Fig. 5.11)



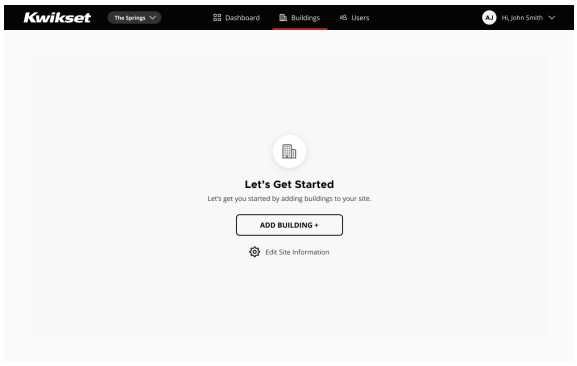
(Fig. 5.12)

CONFIGURATION

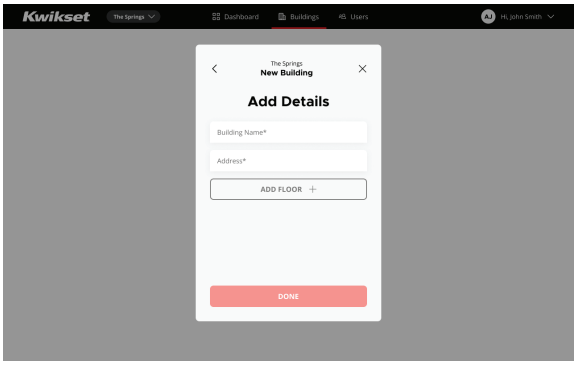
I. Add and Configure a Building Favorites

A. Only Property Managers and Installers may add/edit/delete buildings within a site. No user may add or delete a site, as this is only able to be performed by Kwikset account personnel.

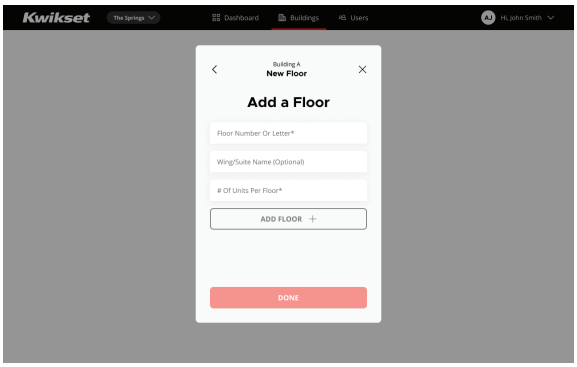
1. Via the Property Management Web Portal
   a. Login to the Property Management Portal and select the “Buildings” section from the Upper Control bar on the Dashboard.
   b. Tap on the icon of a gear located in the upper right hand corner of the “All Buildings” list populating the left hand side of the page. This will present an “Edit Site” pop up.
   c. Tap on “Add Building +” Button. *(Fig. 6.1)*
   d. Enter a Name and Address for the building. *(Fig. 6.2)*
   e. Tap on “Add Floor +” Button to add a floor, or “Done” to create the Building within the site. *(Fig. 6.3)*
      i. The ability to create a placeholder is unique within UNITE, and enables the user to create a building before they possess all of the final construction details of that building. At any point in the configuration process, users may select “Done” to save the configuration data within the system with the option to come back later to complete the configuration process.
      ii. Each building must possess at least one floor before units and devices may be assigned. Upon selected the “Add Floor +” option, users will be presented with the “Add a Floor” page.



(Fig. 6.1)

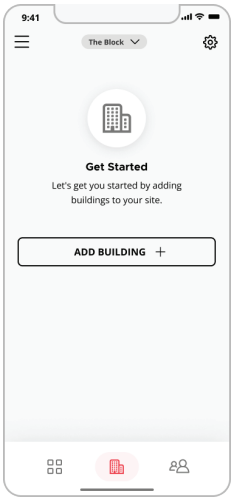


(Fig. 6.2)



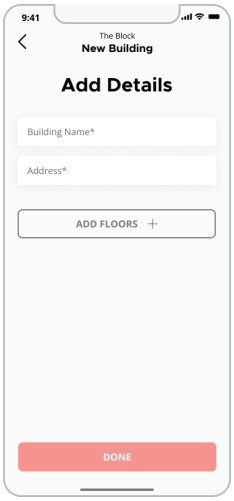
(Fig. 6.3)

f. A Floor Number/Letter and the number of units on the floor are required information to create a floor.
    i. There is also an option to create a “Wing” in this “Add a Floor” process. The concept of a “Wing” enables floors to be configured with custom subsections for additional ease of use and organization of audit data. Examples of “Wings” include East & West, or Floor 1A & Floor 1B. “Wings” are completely optional, so users may disregard this entry field and leave it blank if they do not wish to use it.
    ii. Select “Done” to finalize the floor’s configuration data.
g. Once all floors are entered, one may return to the “Buildings” section of the portal be pressing the “Return” icon located in the upper left hand corner of the page and then selecting “done” when they return to the buildings list.

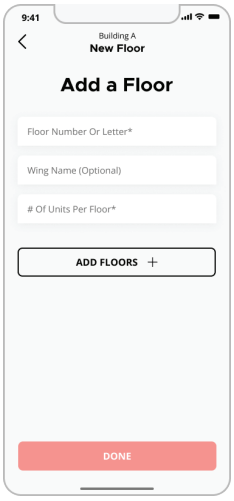


(Fig. 6.4)

2. Via the UNITE Mobile Application
a. Login to the Unite mobile application and select the “Buildings” icon from the bottom of the dashboard.
b. Tap on the icon of a gear located in the upper right hand corner of the page, and select the “Edit Site” prompt from the list.
c. Tap on “Add Building +” Button. *(Fig. 6.4)*
d. Enter a Name and Address for the building. *(Fig. 6.5)*
e. Tap on “Add Floor +” Button to add a floor, or “Done” to create the Building within the site. *(Fig. 6.6)*
    i. The ability to create a placeholder is unique within UNITE, and enables the user to create a building before they possess all of the final construction details of that building. At any point in the configuration process, users may select “Done” to save the configuration data within the system with the option to come back later to complete the configuration process.
f. Each building must possess at least one floor before units and devices may be assigned. Upon selected the “Add Floor +” option, users will be presented with the “Add a Floor” page.
g. A Floor Number/Letter and the number of units on the floor are required information to create a floor.
    i. There is also an option to create a “Wing” in this “Add a Floor” process. The concept of a “Wing” enables floors to be configured with custom subsections for additional ease of use and organization of audit data. Examples of “Wings” include East & West, or Floor 1A & Floor 1B. “Wings” are completely optional, so users may disregard this entry field and leave it blank if they do not wish to use it.
    • Select “Done” to finalize the floor’s configuration data.
h. Once all floors are entered, one may return to the “Buildings” section of the application be pressing the “Return” icon located in the upper left hand corner of the page until they reach their desired location.



(Fig. 6.5)

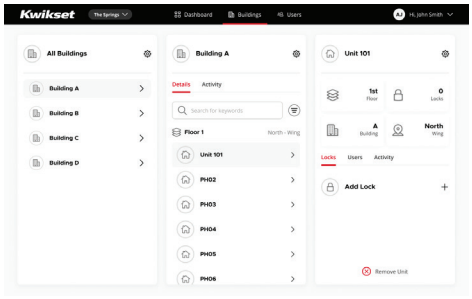


(Fig. 6.6)

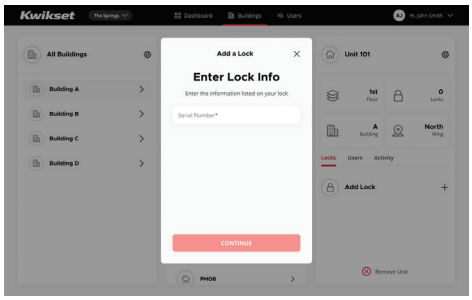
II. Add and Commission Locks Within a Site

A. Via the Property Manager Web Portal

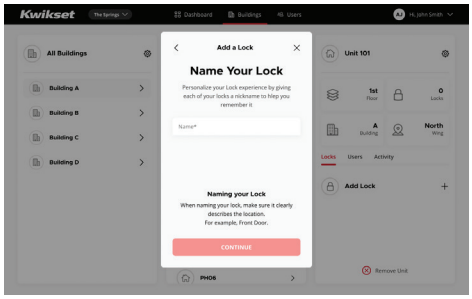
1. Important to note: Locks may be pre-commissioned from the Property Manager Web Portal, but final onsite commissioning of the lock must be completed via the UNITE Mobile Application.
    a. UNITE Locks include a proprietary secure channel that establishes a high level of protection over the communication pathway of the lock. The UNITE Mobile Application is required to establish this secure channel.
2. To pre-commission a lock, one must first login to the Property Manager Web Portal and select the "Buildings" section from the Upper Control Bar.
3. Find the location for the lock in question working form left to right by selecting a building, then select the unit to which one would like to add a lock to.
4. Click on 'Add Lock +' in the unit details screen location on the right hand tile of the page. *(Fig. 7.1)*
5. Enter the lock's Serial Number, select "Continue". *(Fig. 7.2)*
6. Name the lock, select "Continue". *(Fig. 7.3)*
7. One will be presented with the "Congrats" page confirming that the lock has been added to the unit. *(Fig. 7.4)*
    a. This page will remind the user that the lock requires onsite installation. Pre-commissioning is complete, with the next step being for the installer to connect to the lock via the UNITE mobile application and complete the onsite portion of the installation process as outlined in the "Via the UNITE Mobile Application" portion of this guide. *(Fig. 7.5)*



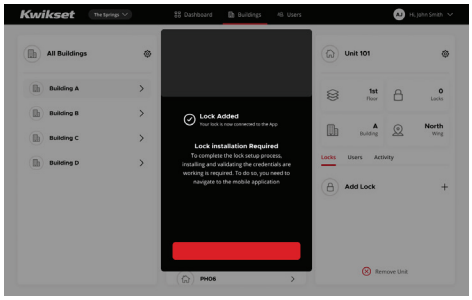
(Fig. 7.1)



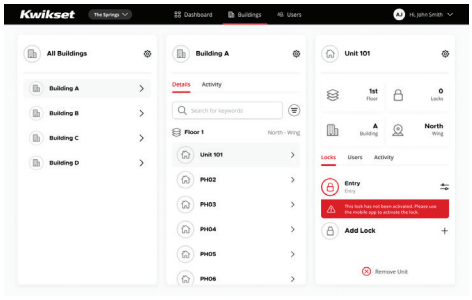
(Fig. 7.2)



(Fig. 7.3)



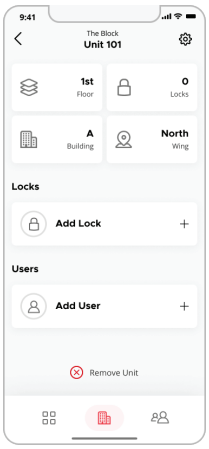
(Fig. 7.4)



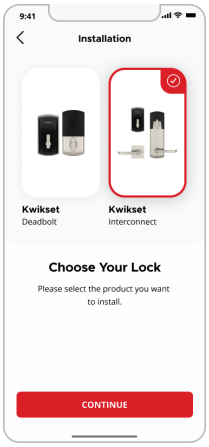
(Fig. 7.5)

B. Via the UNITE Mobile Application

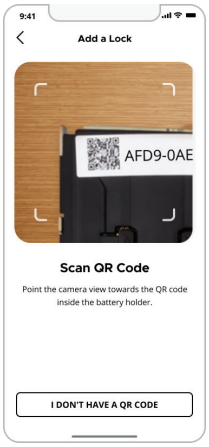
1. Login to the Unite mobile application and select the “Buildings” icon from the bottom of the dashboard.
2. Select a building, then select the unit to which a lock will be added.
3. Click on ‘Add Lock +’ in the unit details screen. *(Fig. 7.6)*
4. Select the lock type which needs to be added from the “Choose Your Lock” screen and click Continue. *(Fig. 7.7)*
5. A PDF Instruction Manual is accessible if needed, otherwise select the “Skip and Continue” option and a milestone screen will be displayed with “Lock Installed” marked as completed.
    a. This assumes that the lock has been installed, but for those pre-commissioning the locks there is no negative impact on the process imparted here by skipping the physical installation portion of the lock.
6. Note the “Before you Start” information, and then select “Continue”
7. Scan the QR code provided on the lock. *(Fig. 7.8)*
    a. There is also a “I Don’t Have a QR Code” option if the QR code is missing or damaged. Selecting this will enable the user to manually enter in the Serial Number of the lock.
8. Confirm the serial number and select “Continue”.
9. Enter the name for the lock and click “Continue”. *(Fig. 7.9)*
10. This will present the “Lock Added Successfully” page, which will confirm that the lock’s serial number is now associated with the Site and Unit selected. Click “Continue”. *(Fig. 7.10)*
11. The lock’s technical activation process will now start. This process may take up to two minutes, during which the page will display progress reports of the various steps which the lock needs to complete to come onboard.
    a. Please do not turn off the phone or close the app during activation.
12. The lock’s blue settings icon will blink during this stage and a beep sound will be heard from the lock with a green indication when activation is completed.
13. Once activation is completed, the milestone screen will be presented again displaying “Lock Added and Activated” marked as completed.



(Fig. 7.6)

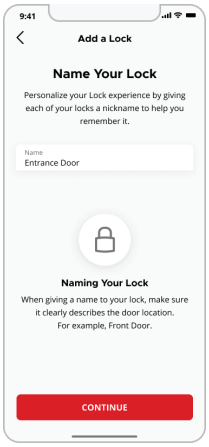


(Fig. 7.7)

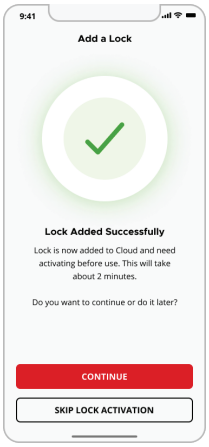


(Fig. 7.8)

14. Click “Continue”. If updated firmware for the lock is available, one will be presented with the option to update the lock or skip. If no new firmware is available, a “firmware is up to date” message will be displayed.
    a. It is strongly recommended to update the lock’s firmware if a new update is available. In addition, certain updates may not offer the option to skip due to the importance of the update. Kwikset will communicate all firmware version information to customers.
15. Click “Continue” and the “Milestone” screen will be displayed with “Firmware Update” marked as completed. Click “Continue.”
16. The user will be presented with the “Test Lock” page. This the user’s opportunity to confirm that all installation and activation processes were correctly processed. Click on the lock button on this page to lock/unlock to engage the lock, and then turn the turn piece on the lock after hearing the beep sound. Once operation is confirmed, users may select “Continue” to move forward.
17. The “Milestone” screen will now be displayed with “Test Lock” marked as completed. The commissioning process is now complete and the user may select “Continue” to exit.
18. The lock’s information will now be linked to the unit with all subsequent audit and access information displayed under that unit’s detail page.



(Fig. 7.9)



(Fig. 7.10)

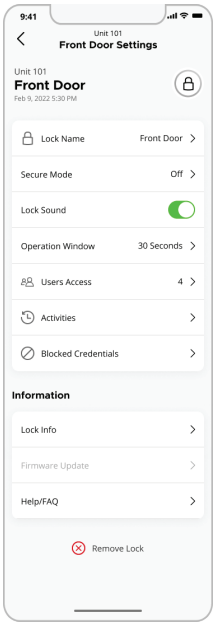
III. Remove a Lock From a Site

A. Important Note:

1. UNITE locks are offline devices. One must either connect to a lock via the UNITE mobile application or physical factory reset the device to fully remove it from a site.

B. Via the Property Manager Web Portal

1. Log into the UNITE Property Manager Web Portal.
2. Navigate to the Buildings section of the portal, and then locate the lock that one wishes to remove from the site.
3. Go into the lock’s settings page, via the icon on the far right of the locks tile.
4. Scroll to the bottom of the lock’s settings, and select “Remove Lock”. *(Fig. 8.1)*
5. Confirm that the lock is to be removed.
6. The lock will now be removed from the site, but one still needs to deactivate the lock at the device level as UNITE locks are offline in nature.



(Fig. 8.1)

7. To finalize deactivation, physically go to the lock and factory reset it.
    a. To factory reset a UNITE lock, please perform the following process:

Manual Factory reset

1. Insert battery to power up the lock.
2. Status LED light displays GREEN 3s.
   Rotate the interior turnpiece back and forth to extend and retract bolt 3x within 5s.
3. Wait for programing LED light to alternate BLUE and RED continuously.
4. Within 10s, rotate the interior turnpiece back and forth 3x.
5. Successful manual factory reset will be indicated by programming LED light displaying solid Green for 3s, accompanied by an audible beep.
6. Fail/ Time out all LED lights will remain off.

- Important Note: the lock will continue to operate as normal, albeit without reporting to the UNITE audit trail, until it has been deactivated. Please ensure that the entire process is completed.

C. Via the UNITE Mobile Application

1. Log into the UNITE Mobile Application.
2. Navigate to the Buildings section of the app, and then locate the lock that one wishes to remove from the site.
3. Go into the lock's settings page, via the icon on the far right of the locks tile.
4. Scroll to the bottom of the lock's settings, and select "Remove Lock".
5. Confirm that the lock is to be removed.
6. The lock will now be removed from the site, but one still needs to deactivate the lock at the device level as UNITE locks are offline in nature.
7. To finalize deactivation, physically go to the lock and factory reset it.
    a. To factory reset a UNITE lock, please perform the following process:

Manual Factory reset

1. Insert battery to power up the lock.
2. Status LED light displays GREEN 3s.
   Rotate the interior turnpiece back and forth to extend and retract bolt 3x within 5s.
3. Wait for programing LED light to alternate BLUE and RED continuously.
4. Within 10s, rotate the interior turnpiece back and forth 3x.
5. Successful manual factory reset will be indicated by programming LED light displaying solid Green for 3s, accompanied by an audible beep.
6. Fail/ Time out all LED lights will remain off.

- Important Note: the lock will continue to operate as normal, albeit without reporting to the UNITE audit trail, until it has been deactivated. Please ensure that the entire process is completed.

IV. Add Lock to Favorites

A. Important Notes:

1. In order to engage with a lock in Access Mode, one must assign the lock as a Favorite. The purpose of favoriting a lock is to prioritize which locks are presented to the user due to the many devices onsite.
2. Locks may only be engaged with via the UNITE Mobile Application due to the need for the lock to securely connect with the application to authenticate access rights.

B. Add a Lock to Favorites

1. Login to the App as Property Manager or Installer. By default, the user will be directed to the Dashboard of the "Manage Mode." To engage with locks, and thus add them to one's favorites, one must switch to the "Access Mode." To enter "Access Mode," navigate to the menu via the icon in the upper left hand corner, and select "Access Mode".
    - Note: Residents do not possess the ability to favorite locks, as they will only be presented with the locks that they have access to.
    - Note: Residents to not have access to "Manage Mode".
2. From the "Access Mode" dashboard, either select "View all Access," or if locks have already been entered, swipe right until the "View All Access" tile is present .
3. Search out the desired lock by navigating through the building's configuration presented.
4. Select the "Heart" icon to favorite the lock. This is a toggle, and may be reengaged by selecting it again.
5. The lock will now be present on the landing page of "Access Mode" for this user.

C. Remove Lock From Favorites

1. Via the "Access Mode" dashboard, swipe right to the "View All Access" tile.
2. Search out the desired lock to remove from Favorites by navigating through the building's configuration presented.
3. Select the "Heart" icon to remove the lock from Favorites. This is a toggle, and may be reengaged by selecting it again.
4. The lock will now be removed from the landing page of "Access Mode" for this user.

V. Settings

A. Firmware Update

1. Note:

a. Firmware Updates will be pushed out periodically to the UNITE ecosystem as required throughout the lifecycle of the UNITE ecosystem. While locks will automatically check for new firmware versions during commissioning, it is also important to update locks in the field as new firmware versions are released. This process will cover the process of updating locks which have already been commissioned into a site.

b. Firmware Updates may only be performed via the UNITE Mobile Application as a secure connection with the application is required to pass date down to the lock.

2. Prerequisites:

a. The lock must be running an outdated firmware version. I.e. if the lock is up to date then the interface will not present the "Update Firmware" option.

b. Both the battery in the lock and the smart device must be above 25%. This is to ensure that neither battery dies midway through an update.

c. The lock must remain within Bluetooth range of the smart device running the UNITE Mobile Application until the firmware update process is completed.

d. Firmware Update Process:

i. Log into the UNITE Mobile Application, and navigate to the lock in question via the "Buildings" section of the application.

ii. One will see a "New Firmware Available" message associated the lock.

iii. Navigate to the lock's settings page via the icon located in the right hand section of the lock's tile.

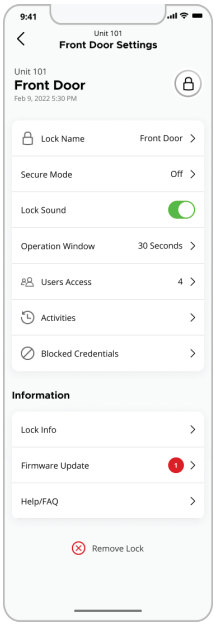
iv. Scroll down to the "Firmware Update" option, and select it. *(Fig. 9.1)*

v. Confirm the necessary acknowledgments and begin the firmware update process. *(Fig. 9.2)*

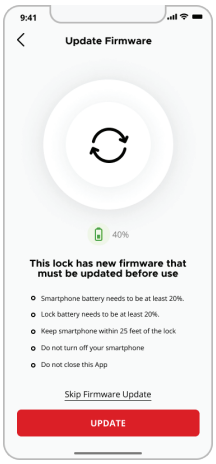
vi. The UNITE backend will then complete the firmware update process via an automated process.

vii. Continue this process for all other necessary locks. *(Fig. 9.3)*

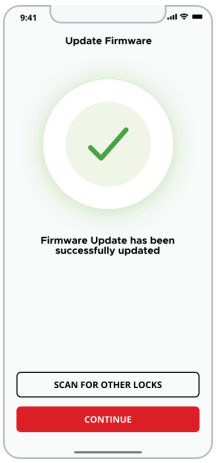
viii. Firmware version may be confirmed via the lock's settings page via the "Lock Info" option.



(Fig. 9.1)



(Fig. 9.2)

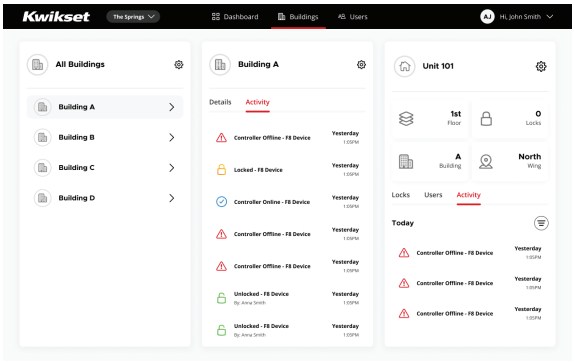


(Fig. 9.3)

REPORTING

I. Event History

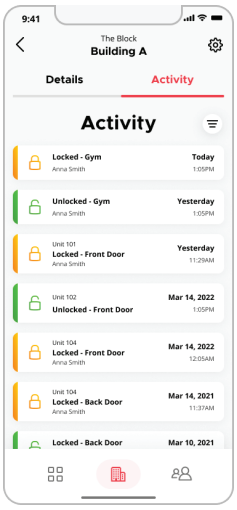
A. UNITE maintains an extensive audit trail which is conveniently organized into multiple views in largely the same manner for both the Property Manager Web Portal and the UNITE Mobile Application.



(Fig. 10.1)

B. Building View

1. Log into the Property Manager Web Portal or UNITE Mobile Application and navigate to the "Buildings" section.
2. Select the desired Building from the list of Buildings on the left hand side of the Portal, or via the Buildings list in the application.
3. Within the Portal's middle Building Overview tile, select "Activity" from the options in the upper section of the tile, or from the top of the page within the UNITE Mobile Application. *(Fig. 10.1)*
4. The Building's audit trail of event activity will be displayed in reserve chronological order.



(Fig. 10.2)

C. Device View

1. Device view is a Continuation of Building View.
2. Instead of selecting "Activity" from the Building's Overview page, simply select the unit that one wants to view.
3. Select the lock that one wants to view.
4. Select "Activity" from the right hand lock details page in the Portal, or scroll to the "Activities" option in the lock's detail page within the application. *(Fig. 10.2)*
5. The Building's audit trail of event activity will be displayed in reserve chronological order.

D. User View

1. Log into the Property Manager Web Portal or UNITE Mobile Application and navigate to the "Users" section.
2. Select the desired user
    a. Users of the portal may select the gear icon in the upper right hand corner of the page, and then scroll down to the "User Activity" option to view the user's audit trail activity in reverse chronological order.
    b. User of the UNITE Mobile App may simply scroll down to "User Activity" option to view the user's audit trail activity in reverse chronological order.

Kwikset UNITE™ Software Reference Guide

KwiksetUnite.com · 1-800-327-LOCK
© 2024 Assa Abloy, Inc., Kwikset is a trademark of Assa Abloy, Inc., Lake Forest, CA 92610 • 1853405-11/24