Onity® OnPortal™ Lock Management System

User Manual and Training Guide

Copyright © 2022 Carrier. All rights reserved. Onity is a part of Carrier. Other brand and product names are or may be the trademarks of, and are used to identify products or services of, their respective owners.

This document or set of documents discloses subject matter in which Carrier has proprietary rights. Neither receipt nor possession thereof confers or transfers any right to reproduce or disclose the document, any part thereof, any information contained therein, or any physical article or device, or to practice any method or process, except by written permission from, or written agreement with, Carrier.

Disclaimer

The information contained herein is subject to change without notice. Carrier assumes no responsibility for inaccuracies or omissions and specifically disclaims any liabilities, losses, or risks, personal or otherwise, incurred as a consequence, directly or indirectly, of the use or application of any of the contents of this help file.

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99

Table of Contents

TABLE OF FIGURES

Preface

The Onity OnPortal user manual instructions explaining:

- Each function in OnPortal
- How to use OnPortal

The following conventions are used in this document:

Bold	Menu header and items, buttons, checkboxes. Also used for emphasis and/or action items.
Italic	Emphasis of an instructions or point: special terms. File names, path names, windows, panes, tabs, fields, variables, and other GUI elements. Titles of books and various other documents.

Safety Terms and Symbols

These terms may appear in this document.

CAUTION: Cautions identify conditions or practices that may result in security or software issues.

NOTE: *Notes provide additional information.*

TIP: Tips provide helpful suggestions about best practices.

Using OnPortal

Logging into System

Log in based on your login configuration parameters. If you need to revalidate a master user key, follow the steps below.

Revalidate a Card

Step #	Action
1.	If logged in, log out.
2.	Enter the PIN code for this card.
3.	*NEXT EXPIRATION* adds the time increment to the existing expiration date in the *DETAILS* tab.
4.	PIN shows up after saving. Users must change their PIN the first time they revalidate.
5.	Select **OK**.
6.	Present card to encoder when requested.
7.	If prompted to change PIN (prompted first time), enter a *NEW PIN,* select *CONFIRM PIN,* and select **OK**.
8.	Present card to encoder if requested again and it attempts to revalidate.

Reception Tasks

Select the **RECEPTION** menu to manage a guest's stay.

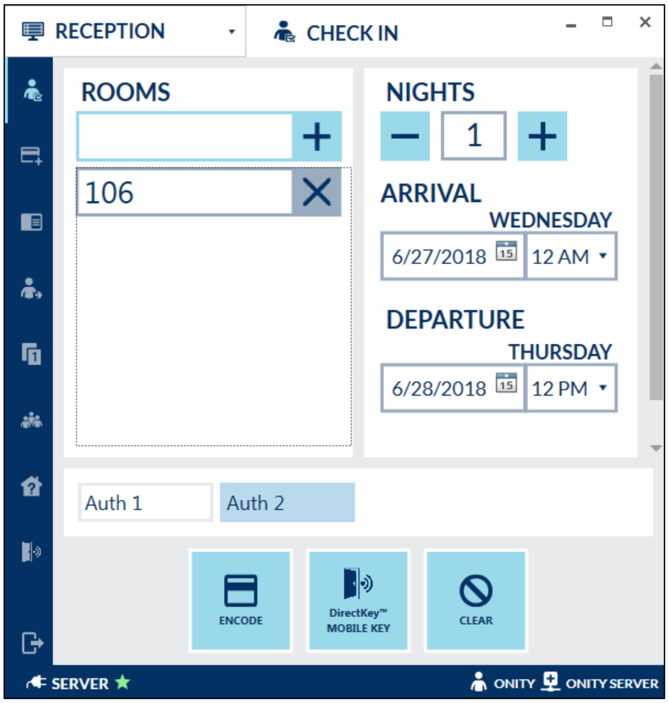
Check In

The *check-in* function is used to create keys for arriving guests OR to create a new set of keys for guests who have lost their existing key. When creating a new guest key with this function, any previous guest keys for the room will be cancelled.

With this function, you may encode a physical keycard, a DirectKey mobile key, or a combination of both.

Step #	Action
1.	Under **ROOMS**, enter a room name, select the + or press the enter key. Up to 3 rooms may be selected if **ARRIVAL** is activated.
2.	Select number of **NIGHTS** and the **ARRIVAL** date (DirectKey requires an arrival date).
3.	Verify that **DEPARTURE** date is correct based upon number of nights.
4.	Across the bottom, select any authorizations for this card. Automatic authorizations will not show at all, only optional authorizations will be shown. A selected authorization will be highlighted.
5a.	Select **ENCODE** to create a card for the guest.
5b.	Select **DirectKey MOBILE KEY** to send a DirectKey. • To send to an unknown key number, send via **EMAIL** and enter valid email address. • To send to a known key number, move slider to **MOBILE KEY NUMBER** and enter number. • Select **SEND MOBILE KEY** to send key device permission to the client. ***NOTE:*** *This option is only available for DirectKey-enabled sites.*
6.	Select **ENCODE** or **DirectKey MOBILE KEY** again for each copy the client desires. Both DirectKeys and physical keys can be made for the same guest.

RETURN TO TABLE OF CONTENTS



ROOMS

106

NIGHTS

1

ARRIVAL

WEDNESDAY

6/27/2018 12 AM

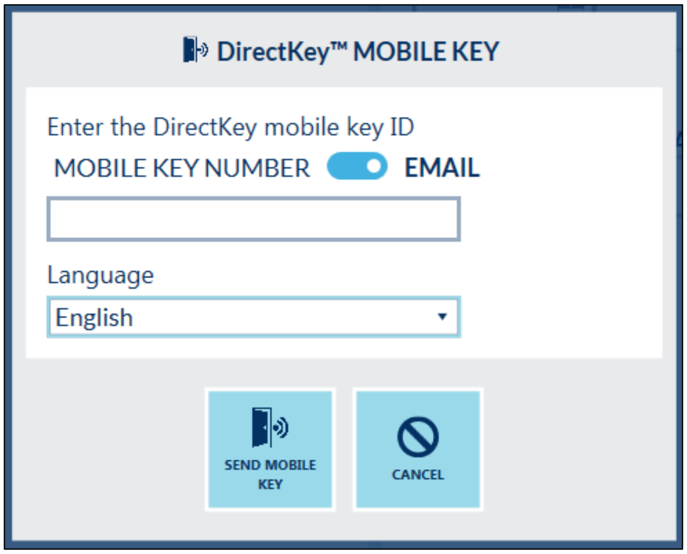
DEPARTURE

THURSDAY

6/28/2018 12 PM

Auth 1 Auth 2

Figure 1 Check-in Screen



Enter the DirectKey mobile key ID

MOBILE KEY NUMBER EMAIL

Language

English

Figure 2 DirectKey^{TM} MOBILE KEY

Copy Card

The *Copy Card* function is used to create additional keycards or DirectKey mobile keys for a guest with an existing key.
CAUTION: Do not create a copy card if the guest key is lost. For a lost card, use the check-in function.

The *Copy Card* function will create a key that will not cancel any existing guest keys.

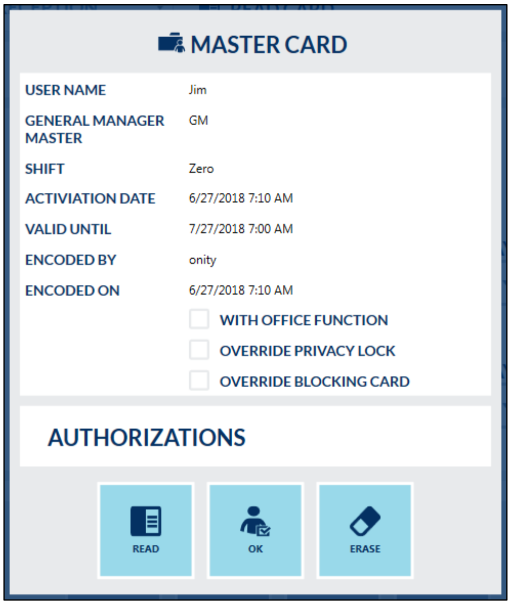
Step #	Action
1.	Select the ***Copy Card*** icon on the left side of the screen.
2.	Either: **ENTER ROOM NUMBER** and select **GO**. *Or:* Select **READ CARD** and read the card to copy. ***NOTE:*** *The system allows details to be changed on a copy card.*
3.	Select the **ENCODE** button to make additional cards or select **DirectKey™ MOBILE KEY** to send additional DirectKeys.
4.	The number that appears on the **ENCODE** button or the **DirectKey™ MOBILE KEY** button is how many current keys of each type are made.

Read Card

The *Read Card* function allows you to read the details from a keycard. It may be used in conjunction with a copy card to find out what an unknown card is or for diagnostic purposes.

Step #	Action
1.	Select the ***Read Card*** icon on the left side of the screen.
2.	Present the card to the encoder when the screen reads “Reading Card.”
3.	There are two results screens: one for master cards/special cards and one for room cards (see Figures 3 and 4 below).

4.	Select: • **ERASE** to erase the card. • **OK** to close the screen. • **READ** to read another card. • **CHECK OUT** to check the person out of the room (only shows on room cards). ***NOTE:*** *On a room card, card reads "Guest" if it is the initial card, copied cards read "Copy x" (up to 4; redundant beyond Copy 4).*



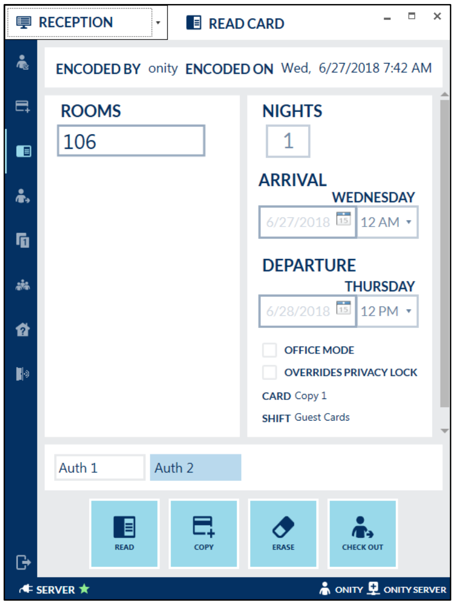
MASTER CARD

USER NAME	Jim
GENERAL MANAGER MASTER	GM
SHIFT	Zero
ACTIVIATION DATE	6/27/2018 7:10 AM
VALID UNTIL	7/27/2018 7:00 AM
ENCODED BY	onity
ENCODED ON	6/27/2018 7:10 AM

□ WITH OFFICE FUNCTION
□ OVERRIDE PRIVACY LOCK
□ OVERRIDE BLOCKING CARD

AUTHORIZATIONS

Figure 3 Master Card Read Screen



RECEPTION
READ CARD

ENCODED BY onity ENCODED ON Wed, 6/27/2018 7:42 AM

ROOMS 106

NIGHTS 1

ARRIVAL WEDNESDAY 6/27/2018 12 AM

DEPARTURE THURSDAY 6/28/2018 12 PM

□ OFFICE MODE
□ OVERRIDES PRIVACY LOCK

CARD Copy 1
SHIFT Guest Cards

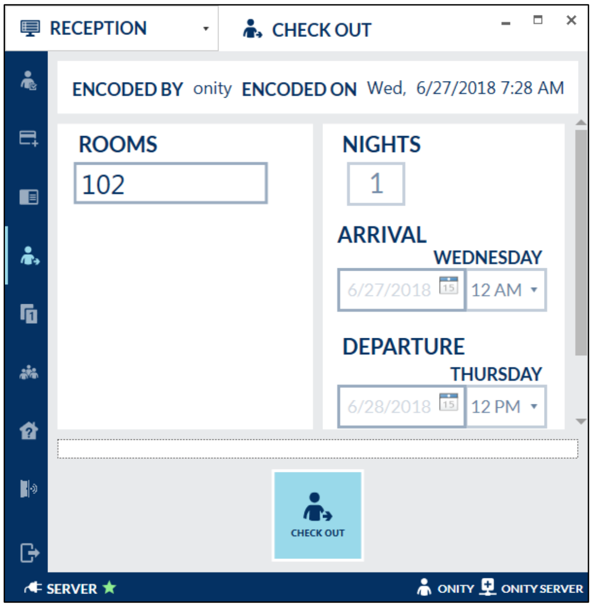
Auth 1 Auth 2

Figure 4 Room Card Read Screen

Check Out

The *Check-out* function does not erase a key; it is used to let the system know that no active guest is using the room. If a key's expiration is still within range, it will still work until that key is canceled in the lock by a new guest card or cancelling card. Using this function will remove the ability to create a copy card for the room.

Step #	Action
1.	Select the ***Check Out*** icon on the left side of the screen.
2.	Either enter a room number and select **GO**, or select **READ CARD** and present the card to the encoder.
3.	When the check-out details screen appears, select **CHECK OUT** at the bottom to complete check out.



ENCODED BY onity ENCODED ON Wed, 6/27/2018 7:28 AM

ROOMS: 102

NIGHTS: 1

ARRIVAL: WEDNESDAY 6/27/2018 12 AM

DEPARTURE: THURSDAY 6/28/2018 12 PM

Figure 5 Check-out Screen

Single Opening

If someone wishes to look at a room before checking in, a site may create a single-opening card for that door. The card will only work one time on the door, hence the name. Only four (4) single-opening cards can be encoded between check-ins.

Step #	Action
1.	Select the ***Single Opening*** icon on the left side of the screen.
2.	A *Single Opening* screen appears, which has the same details as the check-in screen.
3.	Enter a room name under **ROOMS** and press + ADD or “enter” on the keyboard.
4.	In general, leave the nights, arrival and departure times alone. It is very rare that a single-opening card is for the future.
5.	Select **ENCODE** to make the card.

Groups

When a site knows that a large group will arrive at once, it is sometimes more convenient to make all of the cards for that group ahead of time (**maximum of two weeks ahead**). The rooms are checked in when the group is checked in, which we normally configure for automatic check-in (see **CONFIGURATION > PROPERTY**). If the site is not on automatic check-in for groups (all sites SHOULD be), then they have to check in the group manually to keep the card sequence in OnPortal consistent with the card sequence in the lock. Select the *Groups* icon to manage groups.

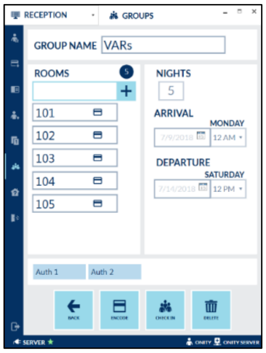
Create a New Group

Step #	Action
1.	Select + ADD at the bottom of the screen to bring up the group details page.
2.	Enter a **GROUP NAME** that describes the group to staff.
3.	For each room being pre-encoded for the group, enter a room name and press enter or the + sign. A list of room names for this group appears below the **ROOMS** area.
4.	A number appears in the circle to the right of **ROOMS** indicating how many rooms have had cards encoded.
5.	Enter the number of **NIGHTS** for the stay.
6.	Enter the **ARRIVAL** date and time.
7.	Verify that the **DEPARTURE** date and time are correct for the number of nights.
8.	Authorizations are a bit different. If any of the rooms has an automatic authorization, that authorization shows selected for all the rooms. Select any remaining optional authorizations desired.
9.	Select **SAVE.**

Encode Group Cards

Group cards can be encoded anytime ***within two weeks*** of arrival. If encoded earlier than two weeks ahead of time, there is a high probability that some or all of the keys will not work upon arrival.

Step #	Action
1.	Select **ENCODE** to bring the up *Group Encoding* screen.
2.	Select the first room to encode. The circle shows the number of cards already encoded for each room.
3.	Select the **NUMBER OF CARDS PER ROOM** to encode.
4.	**CONTINUOUS ENCODING** means once the system starts encoding cards, it goes through and makes cards for all the rooms. Turning it off means the system returns to the main group screen after each card.
5.	Select **ENCODE** to begin encoding group cards.


GROUP NAME VARs

ROOMS 5

101

102

103

104

105

NIGHTS 5

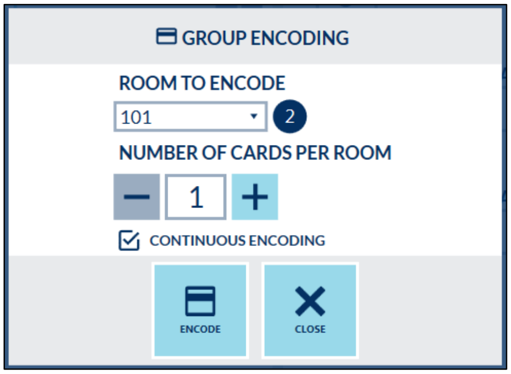
ARRIVAL MONDAY 7/9/2018 12 AM

DEPARTURE SATURDAY 7/14/2018 12 PM

Auth 1

Auth 2

Figure 7 Group Details Screen


GROUP ENCODING

ROOM TO ENCODE 101 2

NUMBER OF CARDS PER ROOM 1

☑ CONTINUOUS ENCODING

Figure 6 Group Encoding Screen

RETURN TO TABLE OF CONTENTS

Managing Groups

The group screen tells the status of a group and contains filters for specific types of groups.

Icon	Meaning	Icon	Meaning
💳	Cards Encoded for this group	✓	Group checked in
💳⊘	Cards Not Encoded for this group	⊘	Group not checked in
3	Number of rooms in the group	!	Group overdue

Manually Check In a Group

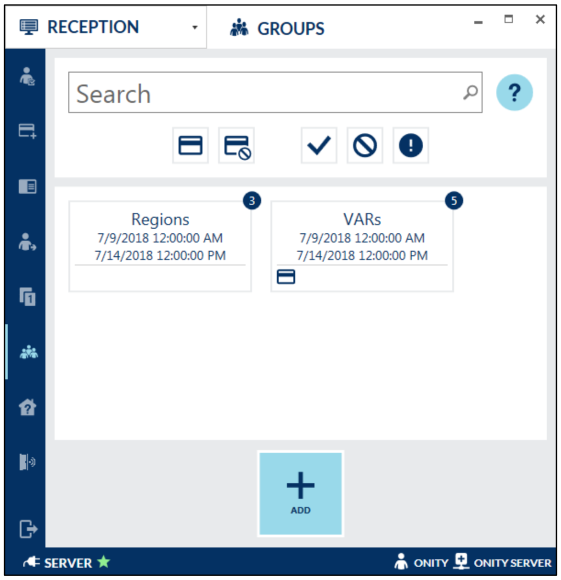
Onity recommends that you set the group check-in to *Automatic*. If you decide to use the manual check-in option, it is imperative that you perform the steps below. Failure to perform check in will cause future guest keys not to work in the locks.

Step #	Action
1.	Select the group to check in.
2.	At the bottom of the screen, select **CHECK IN**.
3.	The button changes to **CHECK OUT** upon successful check in.

Check Out or Delete a Group

If a group cancels, it may be deleted. If the group has checked in, use the check-out function. It is very important that a deleted group's keys be erased to ensure that no issues arise with current or future guest keys.

Step #	Action
1.	Select the group to check out or delete.
2.	For checked-in groups, select **CHECK OUT** to remove the group.
3.	For groups not checked in, check the group in first, then select **CHECK OUT** to delete the group. **CAUTION:** If there's any possibility that any of the keys were used in ANY lock, you MUST check the group in and then check it out.



Regions
7/9/2018 12:00:00 AM
7/14/2018 12:00:00 PM

VARs
7/9/2018 12:00:00 AM
7/14/2018 12:00:00 PM

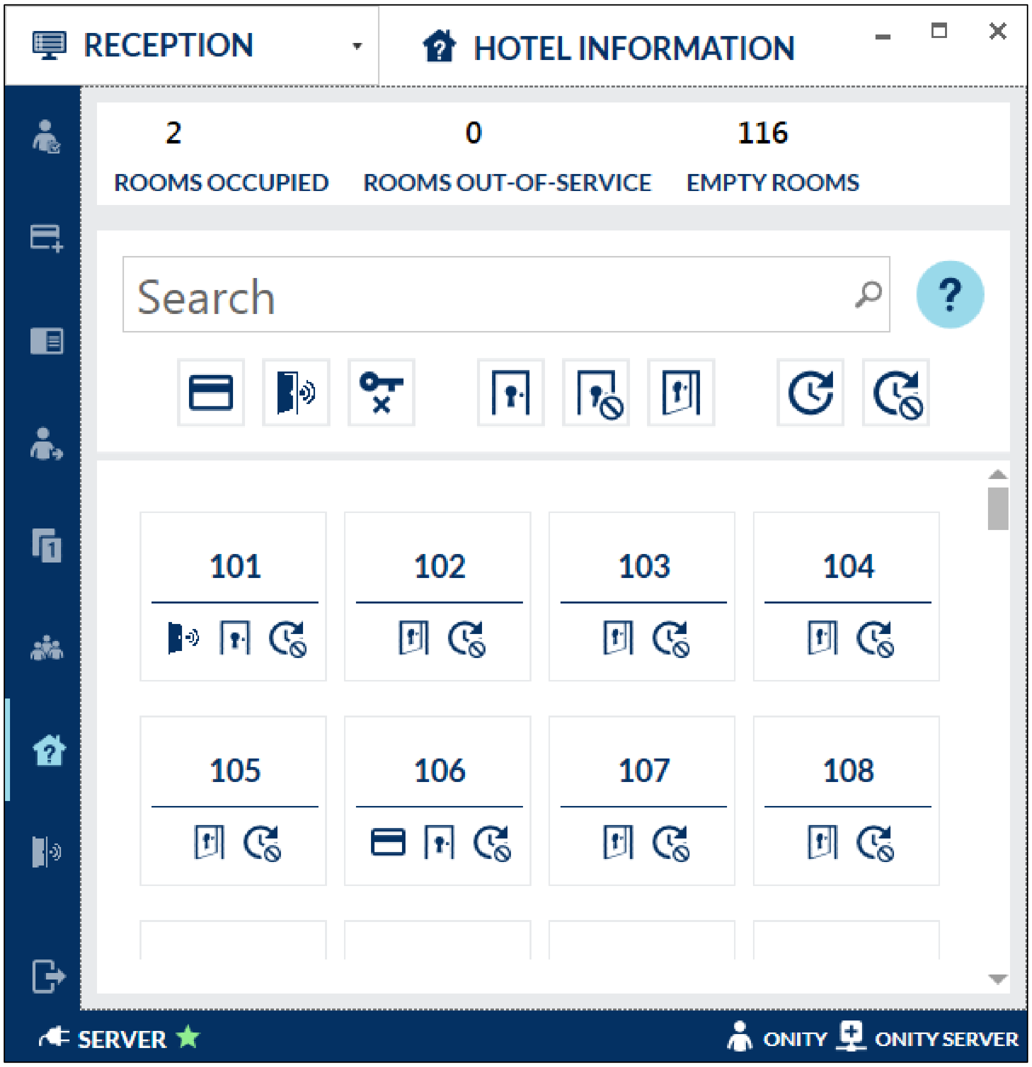
Figure 8 Groups Screen

RETURN TO TABLE OF CONTENTS

Hotel Information

Hotel information gives the site information about the status of their rooms and which type of keys are currently being used for which room currently. Selecting a room gives some room management options, like checking out a guest, copying a card, or managing the mobile key. Select the ***Hotel Information*** icon to view this data.

Icon	Meaning	Icon	Meaning
💳	Encoded cards	🚪⊘	Out of Service
🚪)))	DirectKey mobile key issued	🚪	Vacant
🔑✕	No Key	🕓	Up to Date
🚪	Occupied	🕓⊘	Not Up to Date



2 ROOMS OCCUPIED

0 ROOMS OUT-OF-SERVICE

116 EMPTY ROOMS

Figure 9 Hotel Information Screen

RETURN TO TABLE OF CONTENTS

Manage DirectKey Mobile Keys

Step #	Action
1.	Select ***Manage DirectKey Mobile Keys*** icon on the left.
2.	Select ***Enter Room Number***; enter name of room with a mobile key and select **GO**.
3.	The email address, key serial number, and the date/time (UTC time) of the most current key device permissions for this room appear.
4.	There are two tabs, *Permission* and *Device activity* (see below for information). Available management options: • **RESET** sends another "sign up" email to the end user for download and install instructions. For example, when a guest loses their cell phone and gets a new one during their stay. • **RESEND STAY** instructs Onity servers to send this stay to this device again. • **REFRESH** is used to get the most recent data from the server. It is used when viewing device activity and desiring the most recent activity. • **DELETE STAY** deletes the key device permission from the Onity server.

Permission Tab

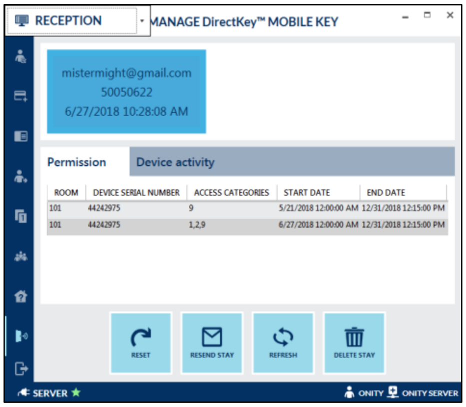
This shows the key device permissions properties in the Onity DirectKey servers.

Heading	Meaning
Room	The explicit room number the key device permission is for.
Device Serial Number	The DirectKey module's serial number for the lock on this room.
Access Categories	Shows which authorizations the key device permission received during creation PLUS the number 9. DirectKey mobile keys MUST have "9" as an access category; this tells the system to give the device permissions to use all of the public doors on a site.
Start Date and *End Date*	Times are shown in local time.

Device Activity Tab

This shows the audit information for the device's usage.

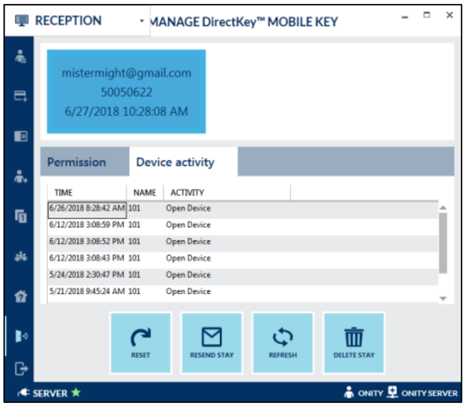
Heading	Meaning
Time	Date/time (in local time) of the activity.
Name	Room name used by the device.
Activity	What the device did.



mistermight@gmail.com
50050622
6/27/2018 10:28:08 AM

ROOM	DEVICE SERIAL NUMBER	ACCESS CATEGORIES	START DATE	END DATE
101	44242975	9	5/21/2018 12:00:00 AM	12/31/2018 12:15:00 PM
101	44242975	1,2,9	6/27/2018 12:00:00 AM	12/31/2018 12:15:00 PM

Figure 10 Permissions Tab Screen



mistermight@gmail.com
50050622
6/27/2018 10:28:08 AM

TIME	NAME	ACTIVITY
6/26/2018 8:28:42 AM	101	Open Device
6/12/2018 3:08:59 PM	101	Open Device
6/12/2018 3:08:52 PM	101	Open Device
6/12/2018 3:08:43 PM	101	Open Device
5/24/2018 2:30:47 PM	101	Open Device
5/21/2018 9:45:24 AM	101	Open Device

Figure 11 Device activity Tab Screen

Maintenance

Select *MAINTENANCE* from the drop-down menu to access the maintenance area.

Portable Programmer

The portable programmer (PP) is the link between the OnPortal software and stand-alone locks on the doors. Typically, a Windows tablet is used, although a laptop is also an option. Once loaded, the PP may be disconnected from the network and used offline. Paired with the PP Adapter, this is the method for programming the locks, reading audits, and performing other diagnostic tasks as detailed below. Once the device is connected to the network again, it will sync with the OnPortal system to pull the lock audits and updated doors list into the database.

The lock data will automatically be deleted at a configured time (typically within 1 day) but the audits will remain in order to be loaded into the database when connected.

If the programmer requires loading, the only option on the screen is *Load Portable Programmer*.

Step #	Action
1.	If not already selected, select **Load Portable Programmer** to load the programmer.
2.	The program loads the locking plan and opens the Portable Programmer screen. ***NOTE:*** *To get the latest information from the server, load the programmer even if it has not yet deleted the data.*

Once the portable programmer has been loaded, the tablet (or laptop) may be disconnected from the network and used in offline mode. You will still be required to log in as an authorized user even in offline mode. Each user may have different permissions for using the portable programmer.

Using the Portable Programmer

Once loaded, the PP contains all the information needed to communicate to the locks. The user must log in to perform any of these functions and must have permission to be allowed to perform each function. Permissions determine not only which functions the user can perform but also which locks the user is allowed to communicate with.

Communicating with Locks

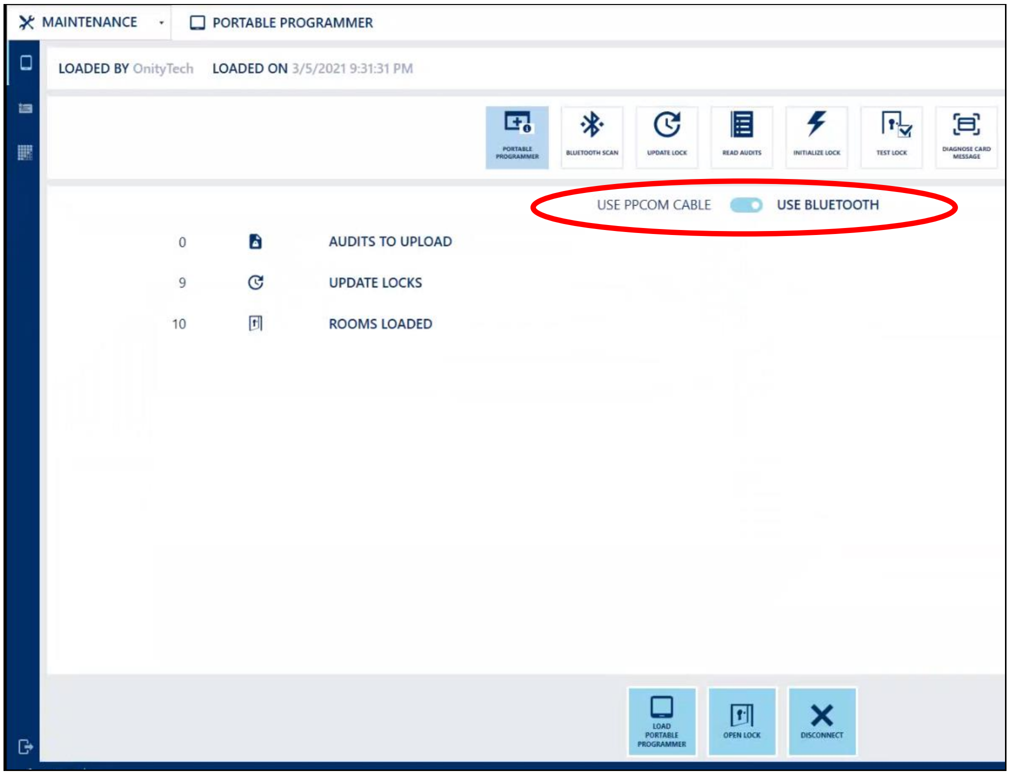
Trillium and HT Locks -- To communicate with a Trillium lock, use the PP Adaptor, which consists of a USB cable, adapter box, and a lock cable connected to the PP tablet.

The PP Adaptor comes with three USB cables with different ends. Select the end that fits your device and connect the PP Adaptor.

The PP adaptor cable for the lock has two ends depending on which type of connection the lock requires. Plug the appropriate end into the lock and connect the other end into the PP adaptor.

Serene Locks (Bluetooth) – Verify that the Bluegiga dongle is plugged in to your device; toggle from PPCOM to **BLUETOOTH SCAN** and select the lock from the maintenance menu. After selecting the lock, press "**SELECT LOCK**" at the bottom of the screen and the lock will beep and its LEDs will flash. If your property has both Trillum and Serene locks installed, select *PPCOM* to program Trillium. To program Serene locks, select *USE BLUETOOTH*. The selected option will appear in **BOLD**.

NOTE: *Use the icons at the top of the screen to select a function and use the icons at the bottom of the screen to perform the function.*



LOADED BY OnityTech LOADED ON 3/5/2021 9:31:31 PM

USE PPCOM CABLE USE BLUETOOTH

0 AUDITS TO UPLOAD

9 UPDATE LOCKS

10 ROOMS LOADED

Figure 12 Portable Programmer

RETURN TO TABLE OF CONTENTS

Opening the lock

RFID Card

(***NOTE:*** *If Serene door lock battery is dead, peel back the rubber cover on the PP Adaptor and attach a 9V battery. Select **Open Lock** at the bottom of the screen.)*

Step #	Action	
1.	Hold RFID card in front of the black rosette surrounding the door handle.	
2.	While holding card in this position, touch card to rosette, then remove card.	
3.	When the green LED light flashes, open the door. ***NOTE:*** *LED light will flash green to indicate lock is open.*	

Bluetooth

Step #	Action
NOTE: *Download the DirectKey^{TM} mobile app or hotel-hosted loyalty app from your mobile app store. If using the loyalty app, user experience may be different from the DirectKey app.*	
1.	Open the DirectKey app.
2.	When physically close to the room, tap the room number on the app. ***NOTE:*** *For Trillium lock, LED light will flash white to indicate it is "awake" and will flash green to indicate lock is open.* ***NOTE:*** *For Serene lock, LED light will flash blue to indicate lock is open.* ***NOTE:*** *If the door lock battery is dead on a Serene lock, plug the emergency battery pack into the bottom of the rosette. (See Appendix C for emergency battery pack instructions.) Then select **BLUETOOTH SCAN** icon at top of screen, then select lock. Select **PORTABLE PROGRAMMER** icon at top of screen and then select **OPEN LOCK** icon at bottom of screen.* ***NOTE:*** *If signal strength is poor (-100), it is recommended that you move closer to the lock to complete programming.*
3.	When the green LED light flashes, open the door.

Update Lock

The *Update Lock* function is used to update any locking plan changes for a door and to update the lock to the current date and time. This function should be used at least two (2) times per year in a region that uses daylight savings time and at least once per year in region that does not use daylight savings time. Also, anytime a change is made to the locking plan of a lock it must be updated.

When you select this function, you will see a list of all the locks that the user has access to, and these can be filtered by update status – locks requiring update and locks updated (this can be filtered by selecting the appropriate filter at the top of the lock list). It is not necessary to select the lock name or number when performing the update as the PP will read the lock name and send the appropriate data.

Step #	Action
1.	Select **UPDATE LOCK** at the top of the screen.
2.	Select **UPDATE LOCK** at the bottom of screen.

Read Audits

The Read Audits function is used to read the event log of the lock. This log may be viewed on the PP or viewed in the OnPortal system once loaded back into the main database.

Step #	Action
1.	Select **READ AUDITS** at the top of the screen.
2.	Select **READ AUDITS** at the bottom of the screen.
3.	You can view any audit collected directly from the PP screen, even when offline. If online, or after the audits have been loaded into the main database, the audits will show more details that are not available offline.
4.	To force an upload audit to the system, select the **Portable Programmer** icon and select **LOAD PORTABLE PROGRAMMER** again. Once the audit information is uploaded to the database, user details will be shown when viewing the logs.

Initialize Lock - Serene

The *Initialize* function is used to program the lock for the first time. When initializing a lock, you must first select the lock name or room number, then click the *Initialize* icon at the bottom of the screen. This will set the lock name, add the locking plan and other parameters for the lock, and set the date and time for the lock. **CAUTION:** The *Initialize* function should only be used to initially program a lock – using this function will erase any audit log contained in the lock. If you just want to update the program of a lock that has already been programmed, use the *Update* function.

The *Initialize* screen also allows you to view locks that have been initialized since the last loading by using the filter icons that can be found just above the list of rooms and under the search bar. This can be used as an aid to help the user know which rooms have been initialized during this use of the programmer. Serene locks that have not been assigned to a room appear with a dash above the serial number. A red exclamation mark will appear in the Maintenance > Portable Programmer > Update screen as seen in Figure 13 when a room needs to be re-initialized.

Step #	Action
1.	Select **BLUETOOTH SCAN** icon at *the top of the screen*. (This scans for all Bluetooth locks within range.) ***NOTE****: The lock with the strongest Bluetooth signal will show up first on the list.*
	Select desired lock from list.
2.	Press **SELECT LOCK** at bottom of screen.
3.	Verify that LED on lock you are initializing lights up.
	Select **INITIALIZE LOCK** icon at top of screen.
4.	Select room name to initialize; it turns blue.
5.	Verify that the name on the programmer matches the name of the door.
6.	Select **INITIALIZE LOCK** icon at the bottom of the screen. Lock lights will flash to indicate that it is being initialized. The LEDs will illuminate; the center LED will display purple, with the left and right rings displaying blue.

Test Lock

The *Test Lock* function is a diagnostic tool to help with troubleshooting a lock. This function will show the lock name and model, battery level, switches, firmware version, lock time and manufacture date of the lock. ***NOTE:*** *You may have to use the left-right scroll bar under the top icons to see the* Test Lock *icon.*

Step #	Action
1.	For Serene locks, select the desired lock on the Bluetooth scan screen, as previously described. For Trillium locks, plug the PP Com cable into the lock.
2.	Select **TEST LOCK** from the menu at the top of the screen.
3.	Select **TEST LOC**K button at bottom of screen to connect with the lock.
4.	Turn the handle, turn the privacy switch, and present a card to the lock to test the various switches of the lock. ***NOTE:*** *A handle and/or privacy switch will show a check if engaged, and a cancel symbol (circle with slash) if not engaged. If you have Serene, the status of the door (open/closed) will also be displayed. If the door is open, a check will be displayed; if the door is closed, the cancel symbol will show.*

5.	Select **STOP TEST** to end the test and break the connection with the lock. ***NOTE:*** *Going to another screen/icon also stops the test.*

Diagnose Card Error

If a card gives an immediate red light or alternating red/green light, the *Diagnose Card Message* will indicate why the lock rejected the card. This is a very useful diagnostic tool to help troubleshoot problems with cards not being granted access to a lock. ***NOTE:*** *You may have to use the left-right scroll bar under the top icons to see the* Diagnose Card Message *icon.*

Step #	Action
1.	Select **DIAGNOSE CARD MESSAGE** at the top of the screen.
2.	Select **DIAGNOSE CARD** at the bottom of the screen.
3.	When prompted to present card, use the card on the lock for Trillium and ADVANCE locks. ***NOTE:*** *For Serene, no card is required. The most recent error will appear.* • *Card Expired* means the lock detected an expired card. • *Card Not Valid* means the lock rejected the sequence number. • *Without Required Authorization* means the card does not contain the correct authorization. • *Card Out of Shift* means that the card is valid for the lock, but not during the time it was used.

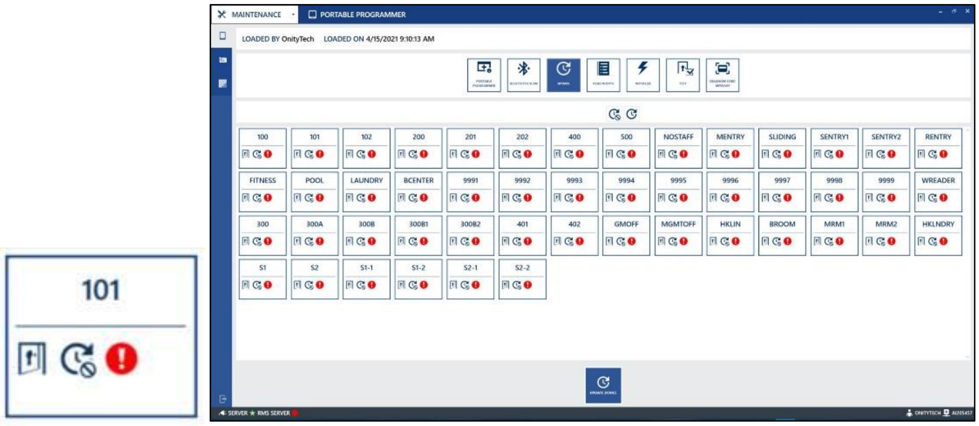
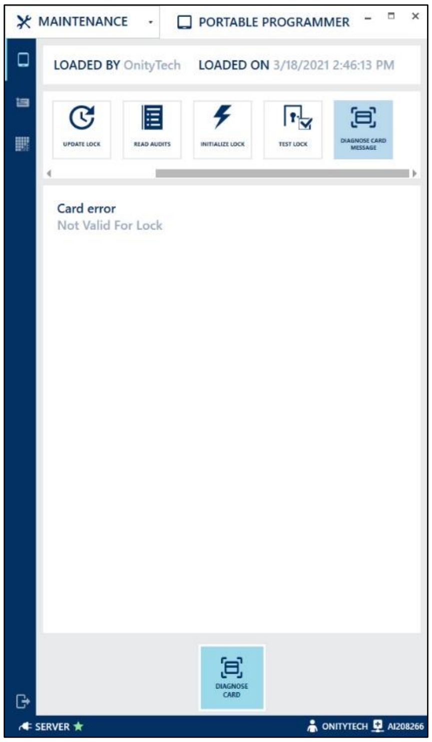


Figure 13 Portable Programmer Screen showing rooms needing initialized



LOADED BY OnityTech LOADED ON 3/18/2021 2:46:13 PM

Card error
Not Valid For Lock

Figure 14 Portable Programmer Screen

RETURN TO TABLE OF CONTENTS

Special Cards

Select the *Special Cards* icon on the left of the screen to show the various special card buttons across the top of the screen.

Button	Usage
GUEST CANCELLING	Cancels the current guest code. A new guest card must be created using the check-in function to create a valid guest card for a room after the cancelling card is used. ***NOTE:*** *The cancelling card is not specific to a room but will cancel the current guest code of any lock in standard mode. This will not cancel guests from a common access door.*
BLOCKING CARD	The blocking card is used to restrict access to only those staff card holders specifically granted the blocking override privilege who also have access to the lock. This is typically used to block access during a maintenance issue or other reason that requires limited access to the room.
SAFE EMERGENCY	Used in conjunction with the room card to open card lock safes when the client forgets what PIN they used.
DIAGNOSTIC	Tests the reader and batteries; shows green if the reader correctly reads the card (does not open) and shows green with a flashing red if batteries are low.
PROGRAMMING AND SPARE	These keys are used as a backup system for anytime the OnPortal system is down (extended power outage, network or PC hardware issues, etc.) It is imperative that current stock of programming and spare cards are kept at the property and accessible during outage times. Onity recommends that these cards be kept in a safe in the front office.
DUPLICATE CARD	For each of the above types of special cards other than the diagnostic card, you have a choice to create a “duplicate” or copy card or create a “new” card. A new card will cancel any previously encoded cards of the same type. The *Duplicate Card* feature is used to make an exact copy of the card type.
NEW CARD	The new card makes a card with a new code sequence. This allows you to cancel the previously encoded cards of the same type. ***NOTE:*** *The previous code will not be cancelled in the lock until either the new card is used or the lock is updated with the portable programmer.*

For most of these special cards, simply selecting *Duplicate* or *New* then ENCODE CARD is all that is required. The exception is the programing and spare cards.

Programming and Spare Cards

This creates programming and/or spare cards. It can create spare cards without creating programming cards.

A *Programming Card* is a special type of card that allows you to create a guest key at the door in times when it is impossible to encode keys through the OnPortal system. When in this situation, take a valid programming card and a spare card to the door, present the programming card (you will see both the red and green lights on the lock), then present the spare card while the lights are still illuminated. The green light will illuminate and the lock will unlock. Hand the spare card to the guest and keep the programming card to use at other doors.

Programming Card

Multiple programming cards may be created to be used by the property in emergency situations. These cards, as well as spare cards, should be carefully guarded at all times and used only during the emergency when no cards can be created by the OnPortal system. Onity recommends that these be kept in a safe in the front office area. If a programming card is lost, you must encode NEW programming cards and update the doors to cancel the previous cards.

CAUTION: The combination of a programming and spare card can open any door on the property configured to work with these types of cards – typically all guest keys. These cards must be carefully guarded and only used in emergency situations.

Step #	Action
1.	Select **PROGRAMMING CARD**.

2.	Select either **DUPLICATE CARD** or **NEW CARD**.
3.	Enter the **NUMBER OF CARDS**; typically Onity recommends one per floor.
4.	Select **ENCODE CARD**.

Spare Card

The *Spare Card* is a keycard encoded with a “random” spare card credential to be used as a guest card when the OnPortal system is unable to encode keys. This card is valid for a lock when used with a programming card as described above. After inserting the programming card, insert the spare card. The lock unlocks and the spare card is given to the guest to use during the system down time.

When programming a spare card to work at the door, all existing guest cards will be canceled. Once the OnPortal system is again able to encode keys, the next guest card will cancel the spare card. If the system is down for a prolonged period of time, any new spare card granted access at a door will cancel the previous one.

Step #	Action
1.	Select **SPARE CARD**.
2.	Enter the **NUMBER OF BATCHES** to do and the **NUMBER OF CARDS PER BATCH**. ***NOTE:*** *Each batch encodes identical data on each card of the batch. Onity strongly recommends that you* ***ENCODE ONLY ONE CARD PER BATCH****. If you encode two cards per batch, you would be creating two identical cards that could be used to give more than one card to guests during the system downtime. However, unless you have a foolproof method of marking the cards as pairs, it is difficult to manage and you run the risk of giving different guests identical cards.* You can make up to 99 “batches” at a time. Onity recommends that you encode twice the number of batches as you have guest rooms and one card per batch. For example, a 100 room-property should create 200 batches of one card each.
3.	Select **ENCODE CARD**.

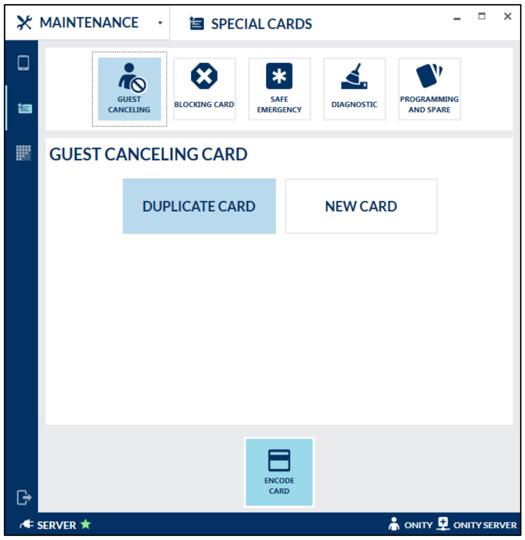


Figure 15 Special Cards Screen

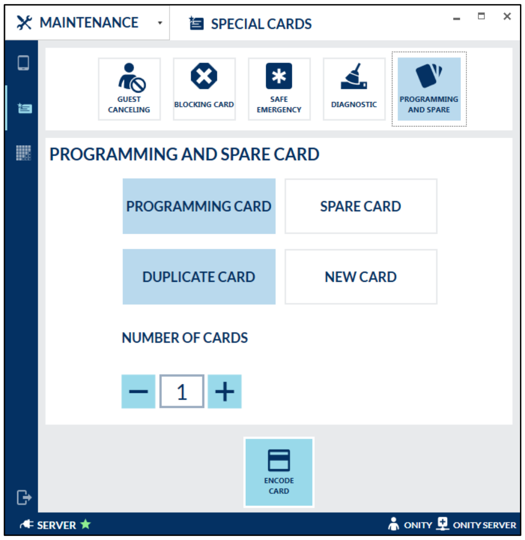


Figure 16 Programming and Spare Cards Screen

Manage Rooms

Allows maintenance staff to put a room out of service, remove a room from out of service, or change a profile. Changing a profile is a specialized function most often used for condo rentals when the cleaning and selling of the rooms are managed by different management companies.

Vacant / Occupied: This selection just allows you to change the room to a certain status apart from the check-in / check-out process.

Out of Service: Removes the option of encoding a guest key for the lock.

Change Lock Profile: Allows the room profile to be changed. This is typically used for condo or timeshare-type facilities where the owner of the condo may hire different management companies to manage rentals, cleaning, etc. This can be used anytime you need to apply a different master keying plan or functionality parameters to a lock.

Step #	Action
1.	Select the ***Manage Rooms*** icon from the left side of screen.
2.	Room names appear with the current profile name below them, and icons indicating room status.
3.	Select either the room number to change or **Select All** the rooms using the ▦ icon in the upper right. (Click **Select All** icon again to de-select all rooms.)
4.	Choose the option for this room: • **Vacant** • **Occupied** • **Out of Service** • **Change lock profile to**
5.	If changing the profile, the system displays all of the profile names after you click **SAVE**; select the correct one, then select **OK**. **CAUTION:** If a profile is changed, the door **must** be updated with the portable programmer.
6.	Select **SAVE** before selecting any other room.

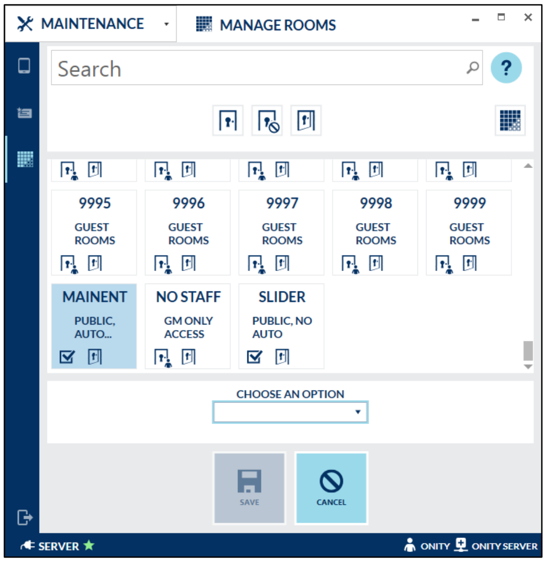


Figure 17 Manage Rooms Screen

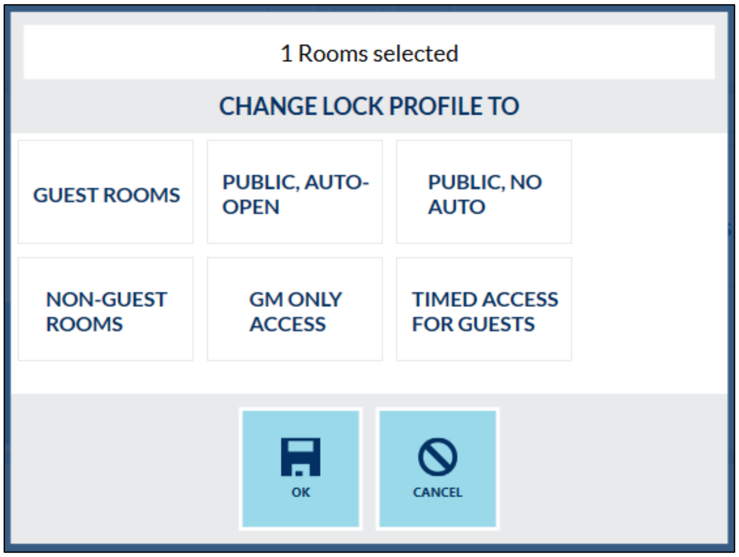


Figure 18 Change Lock Profile To Screen

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99
© 2022 Carrier. Revision 4. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Master Users

The Master Users section allows for management of staff keycards. Each Master User is given a name (may be an actual name or function – this is just a text field), assigned a keying type (determines the access permissions for the keycards and set up in the locking plan), expiration and activation dates and times, and other parameters that determine the user access rights. These are discussed in the subsections below.

Master User

Icons and Filters

The icons below offer a way to filter the Master Users list. Selecting any of these icons in the filters bar will allow you to limit the view to only those users matching the selections.

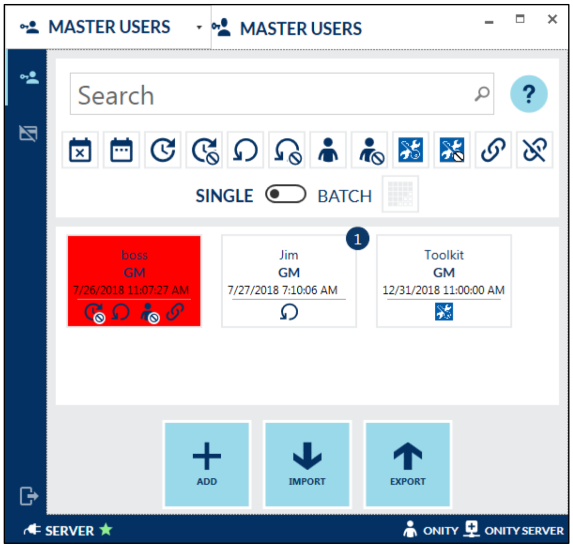
Icon	Meaning	Icon	Meaning
☒	*Expired card*	👤🚫	*Cancelled Master User*
📅.	*Not Expired card*	🛠	*DirectKey Toolkit Linked*
🕒	*Up To Date card*	🛠🚫	*DirectKey Toolkit Not Linked*
🕒🚫	*Not Up To Date card*	🔗	*Operator Linked*
↻	*Revalidation Enabled*	🔗🚫	*Operator Not Linked*
↻🚫	*Revalidation Disabled*	⊙	*Single* or *Batch-edit slider*
👤	*Active Master User*	▦	*Select all master users in this filter*

Creating Master Users

Details Tab

Step #	Action
1.	Select [+ ADD] to add a new Master User and type a name in the Master User textbox at the top.
2.	Fill out the *DETAILS* tab: • **Keying** – Select the master type from the drop-down menu. This menu will show the available master types as setup in the locking plan. Note that an operator creating these master users may be restricted as to what keying types are available. • **Shift** – Each Master User may be assigned to a shift. Up to 8 restricted shifts and an *Always* shift is available as configured in the locking plan. The shift allows access to be restricted to certain doors at certain times. For example, a housekeeper may be assigned a shift that will only allow them into guest rooms between 8am and 5pm, while always allowing access to back-of-house doors. • **Status** ○ **Activation Date**: Optional field that allows you to specify a date and time at which the key will start working. ○ **Expiration Date**: Optional field that allows you to specify when a key will expire. Note that this field is configurable, and the expiration date may be required by your property. ○ **Override Privacy Lock**: if checked, the key will open a lock that it has access to even if the deadbolt / privacy switch is engaged. **TIP:** Onity ***strongly*** suggests you do not put this feature on any user card and that you reserve it for the Emergency Key only.

	○ **With Office Function:** Allows a user card to set doors that it has access to into "Office" or unlocked mode. Requires the door to be configured to allow Office mode. ○ **Override Blocking Card:** Allows a key to open doors that have been blocked using a blocking card. Blocking cards are generally used to block access to doors for maintenance, investigation, or other purposes. This override should be carefully considered before granting access to the user. • **Authorizations:** Select the authorizations to add to the user card. Authorizations are a way to further restrict access within a user type. For example, high-security areas may require this authorization to be added to the card in order to access the area even though the keying type is enabled. A keycard can hold up to all 8 authorizations as configured in the locking plan.

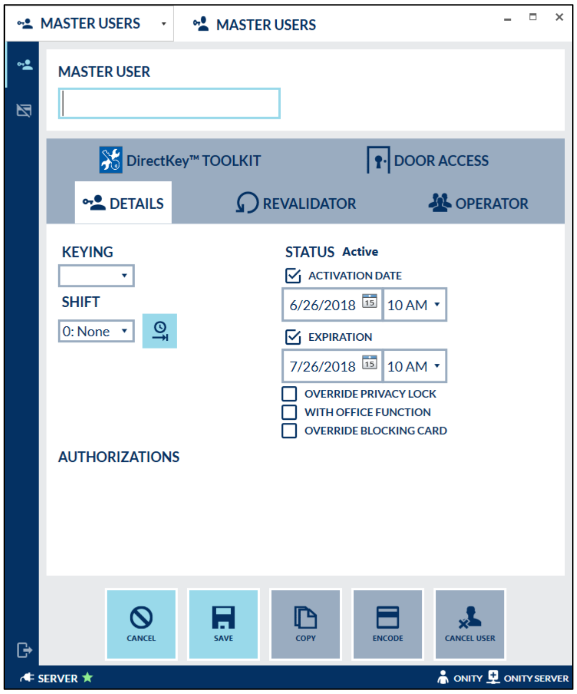


boss
GM
7/26/2018 11:07:27 AM

Jim
GM
7/27/2018 7:10:06 AM

Toolkit
GM
12/31/2018 11:00:00 AM

Figure 19 Master Users Screen showing cancelled Master User



MASTER USER

KEYING

SHIFT 0: None

STATUS Active

☑ ACTIVATION DATE 6/26/2018 10 AM

☑ EXPIRATION 7/26/2018 10 AM

☐ OVERRIDE PRIVACY LOCK

☐ WITH OFFICE FUNCTION

☐ OVERRIDE BLOCKING CARD

AUTHORIZATIONS

Figure 20 Master Users Details Screen

Revalidator Tab

Revalidation is a process that enables a user to update their key without the need to have a manager involved. It allows the property to set a higher level of security by having keycards expire frequently and having users "revalidate" their keycards at certain intervals. If a card is lost, the threat level depends on how much time is left before the key expires.

Revalidating a keycard will update the expiration based on the time increment as well as encoding any other changes onto the card. For example, if a user of the same keying type loses a card, the manager would need to encode a new card for that user but the rest of the keyholders would simply revalidate to get the updated code.

By default, OnPortal disables revalidation when a creating a new user. Select the *REVALIDATOR* tab to enable.

Why Use Revalidation?

Revalidation increases security easily. When implemented with daily revalidation, it can sometimes prevent a site from having to cancel a master user.

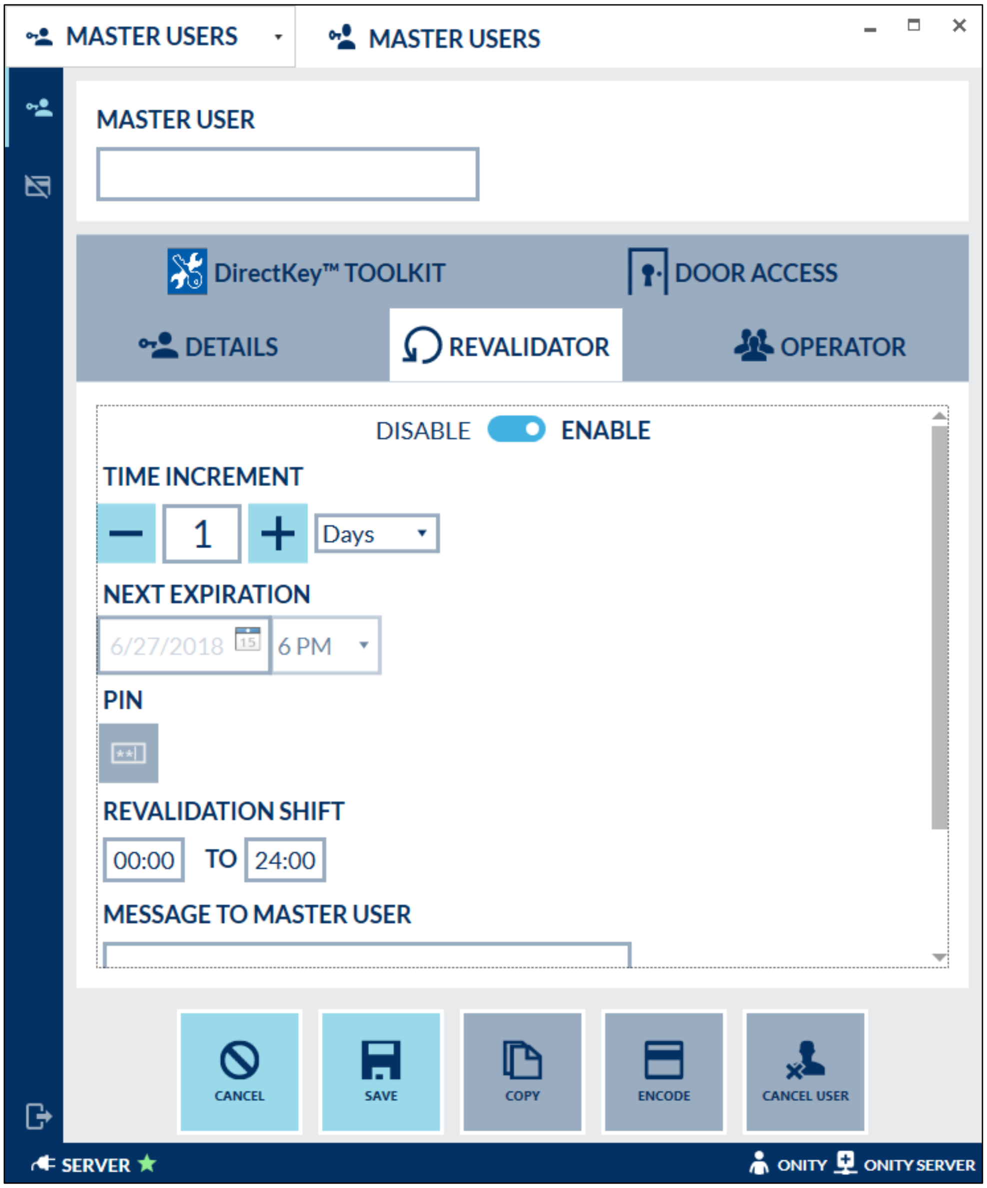
Action	Result
Master card encoded with short expiration period (recommended near end of shift)	The card becomes useless shortly after the employee's shift ends.
Card returns for the next scheduled shift after expiration	The site knows the card was not lost if revalidation occurs.
Employee revalidates card with PIN	System updates the card for the prescribed additional time, with it likely being the employee due to the PIN code. No manager need be involved.

Enabling Revalidation

Step #	Action
1.	Click on User whose card you want to revalidate.
2.	Click on the **REVALIDATOR** tab near the top of the screen.
3.	Move the slider from **DISABLE** to **ENABLE**.
4.	Set the **TIME INCREMENT** for the card. This can be a number of hours, days or months as desired.
5.	*NEXT EXPIRATION* adds the time increment to the existing expiration date in the *DETAILS* tab. This is a reference field only
6.	*PIN* shows up after saving. Users must change their PIN the first time they revalidate.
7.	A user may validate their card during the *REVALIDATION SHIFT*. The revalidation SHIFT is a way to restrict the time of day when the user is able to revalidate a card. This is useful when using the "*Hours*" setting to stop a user from revalidating outside of their work schedule.
8.	An operator may send a *MESSAGE TO MASTER USER.* This message would pop up on the tablet or PC where the user is revalidating their keycard
9.	*MESSAGE COUNT* is the number of times to show the user the message.
10.	Select **SAVE** to generate the default PIN code. **CAUTION:** Never put PIN codes on the card. This is the only time the PIN code appears unless it is being reset. That is why we recommended encoding the card and having the user revalidate it immediately.
11.	Select **SAVE** to generate the default PIN code.

© 2022 Carrier. Revision 4.

RETURN TO TABLE OF CONTENTS



MASTER USER

DISABLE ENABLE

TIME INCREMENT

1 Days

NEXT EXPIRATION

6/27/2018 6 PM

PIN

REVALIDATION SHIFT

00:00 TO 24:00

MESSAGE TO MASTER USER

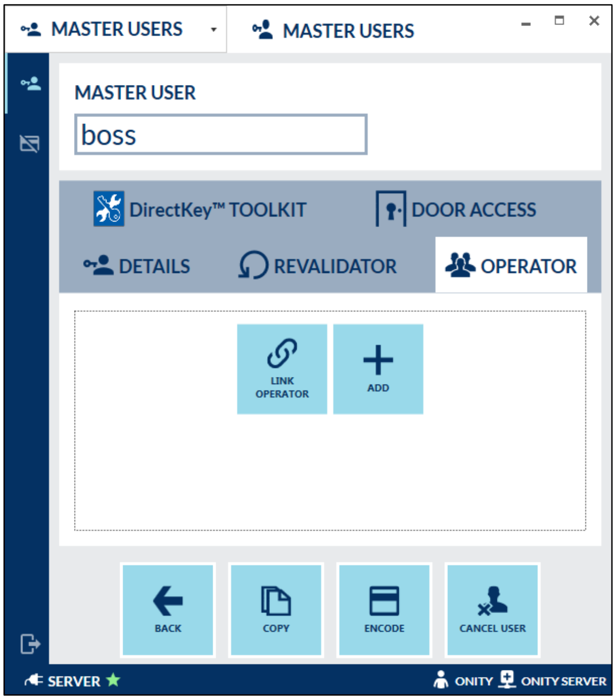
Figure 21 Revalidation Tab Screen

Operator Tab

The *Operator* tab allows you to link a master user with an operator. If a staff member has both Operator access and a Master User card, it is wise to link these together. If that staff member leaves the company and you delete or cancel the master card, the system will also prompt you to delete the operator. This prevents accidentally cancelling a Master User, while leaving their login rights untouched.

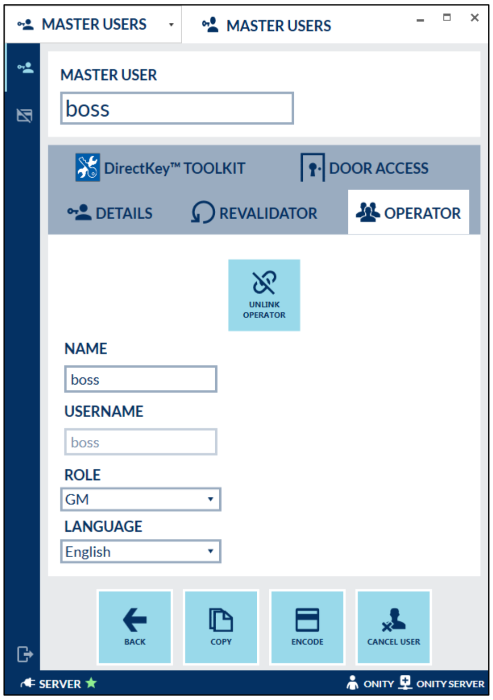
Link a Master User with an Existing Operator

Step #	Action
1.	Select **LINK OPERATOR**; the operator selection screen appears.
2.	Select the operator name to link with this Master User (turns blue when selected).
3.	Select **LINK OPERATOR** in the operator selection screen.
4.	Select **SAVE.**



MASTER USER: boss

Figure 22 Operators Tab Before Link Screen



MASTER USER: boss

NAME: boss

USERNAME: boss

ROLE: GM

LANGUAGE: English

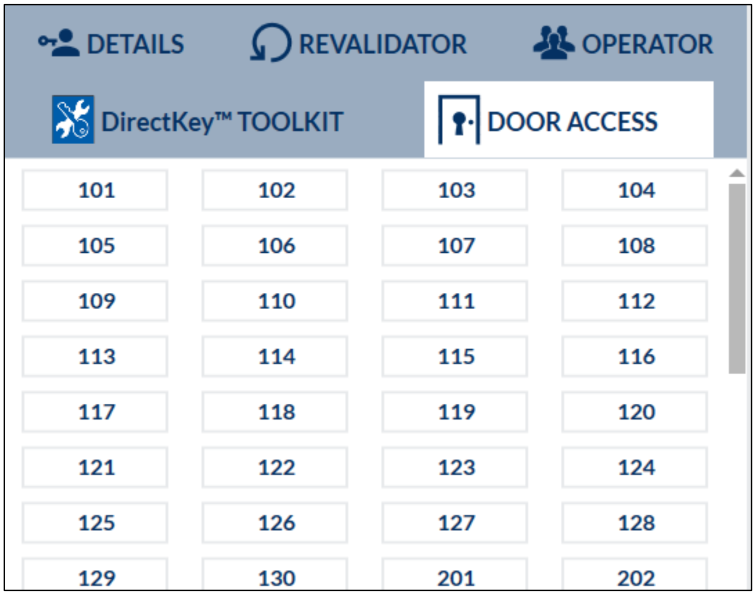
Figure 23 Operators Tab After Link Screen

Adding an Operator while Linking

See steps for adding an operator. The difference is the screen never shows the *PIN* or *PASSWORD.*

Door Access Tab

There is no action to be taken on this tab. It shows all of the doors that this Master User's card may access based upon the master's type and the locking plan.



101	102	103	104
105	106	107	108
109	110	111	112
113	114	115	116
117	118	119	120
121	122	123	124
125	126	127	128
129	130	201	202

Figure 24 Door Access Tab Screen

RETURN TO TABLE OF CONTENTS

DirectKey™ Toolkit Tab

OnPortal gives a site the ability to manage the toolkit without technical support. It is easiest to make the actual DirectKey Toolkit computer into an OnPortal station and set up a toolkit master user on that computer.

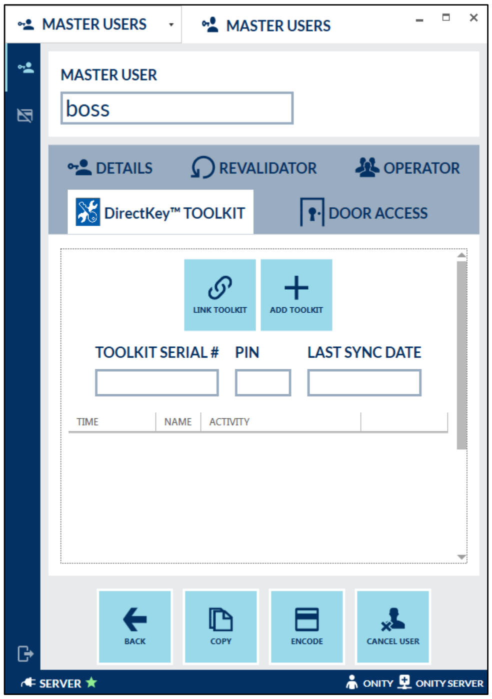
Link a Toolkit to a Master User

Step #	Action
1.	Select the ***DirectKey TOOLKIT*** tab.
2.	There are two options to link the user with a toolkit. When there is an existing toolkit, “link” the existing toolkit with the master user. When the site needs a new toolkit, add a new one.
3a.	Add toolkit steps: • Enter a 4-digit *PIN* code for the toolkit. • Select **+ ADD TOOLKIT**.
3b.	Link toolkit steps: • Enter existing *Toolkit Serial #* to link to. This serial number will be provided by Onity. • Enter 4-digit *PIN* code for the toolkit. • Select **LINK TOOLKIT**.
4.	A window will pop up stating that the program copied the authorization code to the clipboard.
5.	Open the Toolkit program and authorize the toolkit: • Enter the PIN code. • Enter the correct URL: **https://key.directkey.net.** • Paste the 26-digit authorization code. • Verify that the device has Internet access, then submit to authorize the toolkit.

Using the DirectKey Toolkit Tab

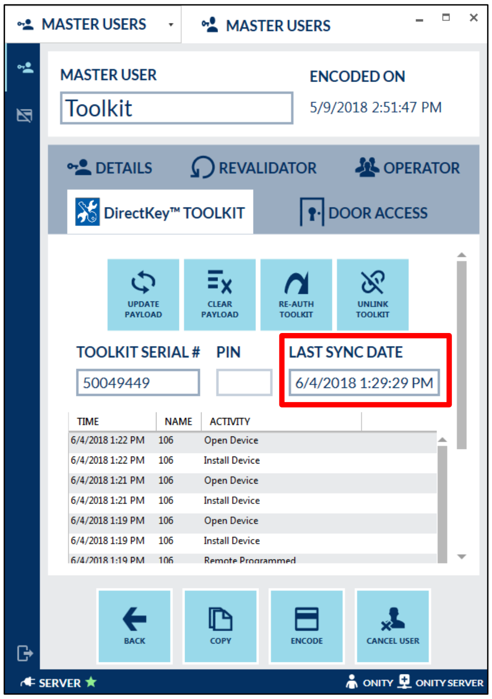
Item	Purpose
UPDATE PAYLOAD	Use this to send a new master card payload to the toolkit electronically.
CLEAR PAYLOAD	Use this to remove the master card payload from the toolkit.
RE-AUTH TOOLKIT	Use this to generate a new authorization code for a toolkit. **CAUTION:** This forces the new code to be entered into the toolkit; there is no turning back after selecting.
UNLINK TOOLKIT	Remove the link between the master user and the toolkit.
TOOLKIT AUDIT	The actions the toolkit performed recently appears in the tab.

RETURN TO TABLE OF CONTENTS



MASTER USER: boss

Figure 25 DirectKey Toolkit Tab, Not Linked



MASTER USER: Toolkit

ENCODED ON: 5/9/2018 2:51:47 PM

TOOLKIT SERIAL #: 50049449

PIN:

LAST SYNC DATE: 6/4/2018 1:29:29 PM

TIME	NAME	ACTIVITY
6/4/2018 1:22 PM	106	Open Device
6/4/2018 1:22 PM	106	Install Device
6/4/2018 1:21 PM	106	Open Device
6/4/2018 1:21 PM	106	Install Device
6/4/2018 1:19 PM	106	Open Device
6/4/2018 1:19 PM	106	Install Device
6/4/2018 1:19 PM	106	Remote Programmed

Figure 26 DirectKey Toolkit Tab, Toolkit Linked

Managing Master Users

OnPortal does not require a copy of a card simply because it expired. OnPortal updates a card's data rather than creating a new card every time.

Expired Cards, Updating (not revalidating)

If a site uses revalidating, the user revalidates their card to update it.

Step #	Action
1.	The user MUST bring the expired card to update it. (If the user does not have the card, it becomes a lost card instead of a card needing updating.)
2.	Select the user from the *Master Users* screen.
3.	Update the expiration date to a date in the future.
4.	Select **ENCODE.**
5.	Present the card to the encoder when prompted. RFID – Just leave the card sitting on the encoding spot. Magnetic stripe – Insert and remove the card as prompted.
6.	The system validates that this is the correct card for this user. Once validated, it prompts for the card again to update it. Present the card to the encoder again.

Cancelling Master Users

When a Master User loses a card, the user should be cancelled. Cancelling a Master User will cause the OnPortal system to increment the code of the master to cancel access for the lost card. With stand-alone locks, it is not sufficient to just cancel the user, the locks must also be updated. There are three ways to do this:

1. Encode one or more Master Cancelling Cards for the keying type of the master – visit every door when the card had access with the cancelling card.
2. Encode a new card for the user that lost the card, have all other users of the same type revalidate their card, and allow the use of the updated cards to update the doors. **CAUTION:** Onity recommends that you proactively update the doors unless the lost card will expire before it is possible to do so. If the card will expire very soon, you can make a decision based on the risk.
3. Load the portable programmer and update the affected locks.

Step #	Action
1.	Select the user to cancel.
2.	Select **CANCEL USER** from the icons at the bottom of the screen. If the user is also an operator, a prompt appears to delete the operator also. **OK** will delete the Operator, **CANCEL** does not delete the operator but does cancel the user.
3.	Go back to the *Master Users* screen; the user should show in red now.
4.	Select the *Master Cancelling Cards* icon from the left side of the screen.
5.	Select the **NAME** of the master type to cancel (should be same master type as the cancelled user).
6.	Select the **ENCODE CARD** button to encode a card. Repeat to create multiple master-cancelling cards for the same master type.
7.	Inform every lock of the cancelled master user. • The easiest way is to use the master-cancelling cards on every lock on the site. Using a master-cancelling card leaves no audit trail in the lock; however, the next time a card of the same type is used, the “new code” tag will be shown. • Load the portable programmer and update all doors. • Encode new master cards for other master users of that type and have them use their cards in every lock.
8.	Encode cards for other affected users. • Select Master Users again. • Select the **Not Up To Date** button across the top of the screen and select a user. • For users with cards, select the user, update the *Expiration* date as needed, and **ENCODE** a new card. The system does not force this to be the existing card and the existing card may be used. • For users linked to a toolkit, select the user, update the *Expiration* date as needed, select the *DirectKey Toolkit tab*, and select **UPDATE PAYLOAD** to send the new payload to the system. ***NOTE:*** *Since there is no physical card encoded for a linked toolkit, the* Not Updated *icon always shows on the toolkit record. To remove it, create a card.*

Deleting a Master User

Step #	Action
1.	Select the cancelled Master User (all red, one cannot delete an active user).
2.	Select **DELETE** icon.
3.	Select **OK** to confirm.
4.	If this Master User has an operator linked, the system prompts to delete the operator. • **OK** deletes the operator and the Master User. • **CANCEL** deletes the Master User but not the operator.

RETURN TO TABLE OF CONTENTS

Security

Roles and Operators are icons on the left under the Security menu. For information on their use, see Operators and Roles under Managing Staff in OnPortal. Select **SECURITY** from the drop-down menu.

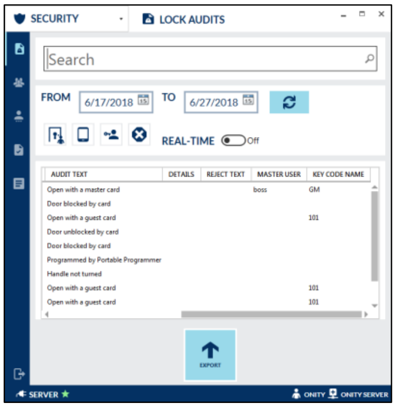
Lock Audits 🔒

Icon	Meaning	Icon	Meaning
Search	Enter a room number to search.	📱	Show only Portable Programmer actions.
FROM	Start dates for these audits.	🔑👤	Show only Master User actions.
TO	End date for these audits.	✖	Show only blocking card usage.
⟳	Refresh, reload audits with changes.	● Off	*REAL-TIME* slider – “On” means there is no *TO* date and no refresh button.
🚪	Show only guest card accesses in audit.		

Reading Lock Audits

NOTE: *Lock audits are periodically archived based on the settings in the system configuration. Archived audits are kept in the folder specified in the configuration as comma-separated values files (.csv); these may be kept as long as needed.*

Heading	Meaning
AUDIT TIME	Time the action occurred according to the lock.
UPLOAD TIME	Time the audit was transferred to the system.
READ TIME	Time when the read was done.
START DATE AND *END DATE*	Room name.
ROOM	What activity occurred.
AUDIT TEXT	For future use.
DETAILS	For future use.
REJECT TEXT	Used for listing the reason a card is rejected by an online wallreader
MASTER USER	Either the room name for a guest card or the Master User name for a master card.
KEY CODE NAME	The key code name is the room number or the master type, if it is a master key.
EXPORT	The audit lock may be exported by clicking the EXPORT icon at the bottom of the screen. This will allow you to save the audit in a .csv file to be viewed externally from the software.



FROM 6/17/2018 TO 6/27/2018

AUDIT TEXT	DETAILS	REJECT TEXT	MASTER USER	KEY CODE NAME
Open with a master card			boss	GM
Door blocked by card				
Open with a guest card				101
Door unblocked by card				
Door blocked by card				
Programmed by Portable Programmer				
Handle not turned				
Open with a guest card				101
Open with a guest card				101

Figure 27 Lock Audits Screen

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99
© 2022 Carrier. Revision 4. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

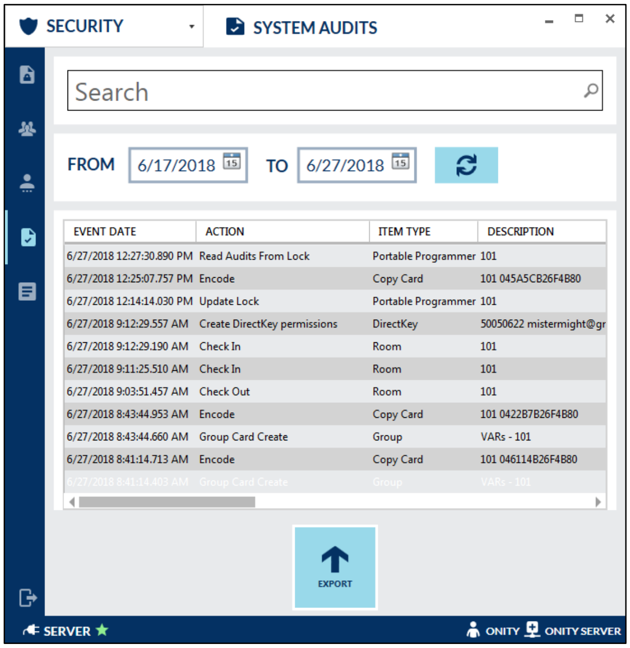
System Audits

The *System Audits* table is an event log for activities performed within the software, such as adding a user, encoding cards, etc.

Step #	Action
1.	Select *System Audit* icon on the left side.
2.	Enter in search criteria if desired; may be a name, room, or action.
3.	Select the date range for the audit.
4.	Press enter or select the refresh icon to display audit with the new criteria.

Reading System Audits

Heading	Meaning
EVENT DATE	Local date and time the action occurred.
ACTION	What the system did.
ITEM TYPE	What type of item did was affected.
DESCRIPTION	Details of this action; displays a name, a number, or both, depending on the action.
OPERATOR	If this action was done by a person, it shows who performed the action.
SEVERITY	What log level this action caused. Options are: INFO, ERR, WARN, DEBUG, and PMS.
SERVER	Which machine was the server when this action occurred.
STATION	What station this action happened on.
ENTRY DATE	Time of the audit log record creation for this action.
ERROR CODE	Any error code associated with this issue.
EXPORT	The *EXPORT* icon at the bottom allows the audit log to be exported to a comma-separated values file (.csv) for archiving or viewing apart from the OnPortal software.



FROM 6/17/2018 TO 6/27/2018

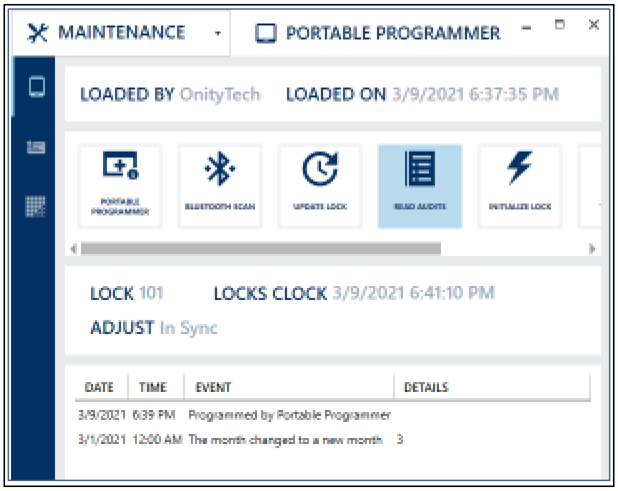
EVENT DATE	ACTION	ITEM TYPE	DESCRIPTION
6/27/2018 12:27:30.890 PM	Read Audits From Lock	Portable Programmer	101
6/27/2018 12:25:07.757 PM	Encode	Copy Card	101 045A5CB26F4B80
6/27/2018 12:14:14.030 PM	Update Lock	Portable Programmer	101
6/27/2018 9:12:29.557 AM	Create DirectKey permissions	DirectKey	50050622 mistermight@gr
6/27/2018 9:12:29.190 AM	Check In	Room	101
6/27/2018 9:11:25.510 AM	Check In	Room	101
6/27/2018 9:03:51.457 AM	Check Out	Room	101
6/27/2018 8:43:44.953 AM	Encode	Copy Card	101 0422B7B26F4B80
6/27/2018 8:43:44.660 AM	Group Card Create	Group	VARs - 101
6/27/2018 8:41:14.713 AM	Encode	Copy Card	101 046114B26F4B80
6/27/2018 8:41:14.403 AM	Group Card Create	Group	VARs - 101

Figure 28 System Audits Screen

RETURN TO TABLE OF CONTENTS

Read Audits - Serene

Step #	Action
1.	Select **Bluetooth Scan** -a list of locks displays.
2.	Select room number.
3.	Click **Select Lock** at bottom of screen.
4.	Select **Read Audits.** Lock LED will illuminate / beep.
5.	The lock audit will display on the screen, as indicated in Figure 28 below.



LOADED BY OnityTech LOADED ON 3/9/2021 6:37:35 PM

LOCK 101 LOCKS CLOCK 3/9/2021 6:41:10 PM

ADJUST In Sync

DATE	TIME	EVENT	DETAILS
3/9/2021	6:39 PM	Programmed by Portable Programmer	
3/1/2021	12:00 AM	The month changed to a new month	3

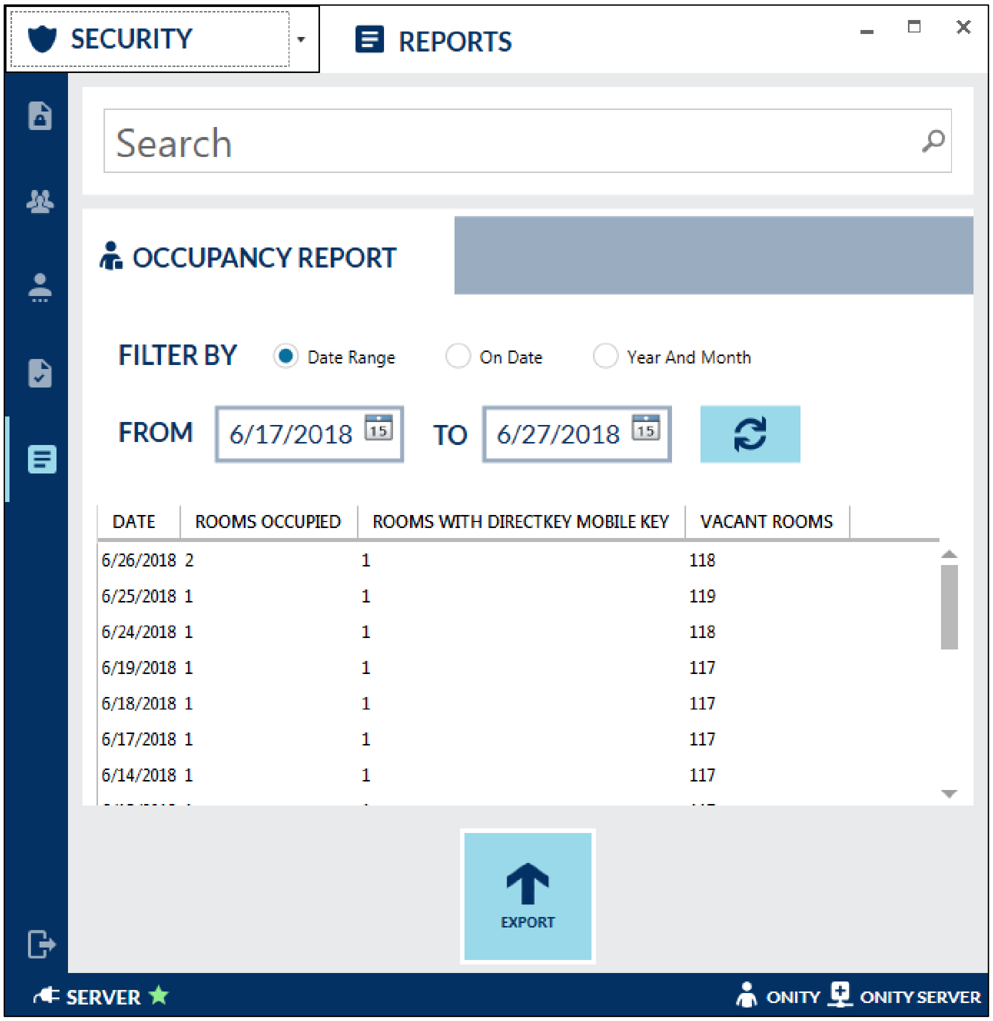
Figure 29 Read Audits screen

RETURN TO TABLE OF CONTENTS

Reports

The only report currently available is the *Occupancy Report*. Occupancy reports display the number of occupied rooms, rooms with a DirectKey, and vacant rooms.

Step #	Action
1.	Select the *Report* icon on the left side of the screen.
2.	Search does not function for *Occupancy Reports;* it is for future reports.
3.	Filter By options: • **Date Range** = Enter *From* and *To* dates. • **On Date** = Enter a specific date. • **Year and Month** = Select the Year and Month for the report range.
4.	Select the refresh icon to apply filters to the report.
5.	**EXPORT** allows the saving of a comma-separated values (.csv) file.



FILTER BY ● Date Range ○ On Date ○ Year And Month

FROM 6/17/2018 TO 6/27/2018

DATE	ROOMS OCCUPIED	ROOMS WITH DIRECTKEY MOBILE KEY	VACANT ROOMS
6/26/2018	2	1	118
6/25/2018	1	1	119
6/24/2018	1	1	118
6/19/2018	1	1	117
6/18/2018	1	1	117
6/17/2018	1	1	117
6/14/2018	1	1	117

Figure 30 Occupancy Report Screen

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99
© 2022 Carrier. Revision 4. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Configuration

The initial property configuration settings are created when the system is initially set up and the locking plan created. This may be completed by Onity prior to installation or done on site during the training process.

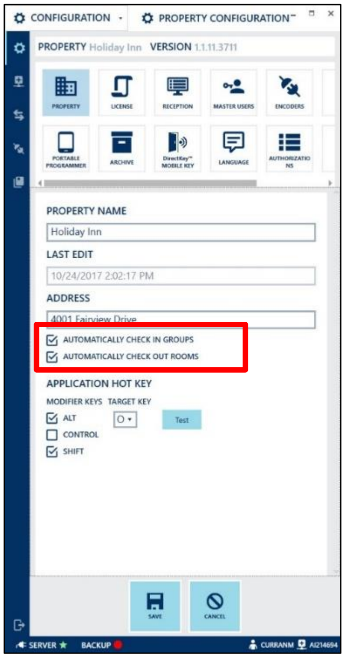
Some of the configuration items will never need to be changed; however, there may be times when changes are required.

Set the Property Configuration

Step #	Action
1.	Select **CONFIGURATION** from the drop-down menu to access the configuration options.
2.	Select the appropriate button at the top of the screen to configure an item.
3.	Icons on the left of the screen are used during station setup.

Property

Step #	Action
1.	Enter the *PROPERTY NAME*. This is a text field and has no effect on the operation of the system but is used to identify the property.
2.	Enter the physical *ADDRESS* of the property. This is also a text field that does not affect the operation of the system.
3.	Most sites prefer to have **AUTOMATICALLY CHECK IN GROUPS** and **AUTOMATICALLY CHECK OUT ROOMS** both checked. Onity strongly suggests leaving these two items checked as indicated in Figure 13 to avoid other issues later. Failure to check in a group with pre-encoded keys will cause subsequent guest keys to fail. The check-out function does not affect system operation but does show the room as vacant again without having to use the check-out function.
4.	Configure the *APPLICATION HOT KEY* if desired. This hot key will quickly minimize or maximize the OnPortal program, which is helpful when multiple windows are open on a machine. When bringing the OnPortal window up, it will return to the last position it was in when minimized.
5.	Select **SAVE.**



PROPERTY Holiday Inn VERSION 1.1.11.3711

PROPERTY NAME
Holiday Inn

LAST EDIT
10/24/2017 2:02:17 PM

ADDRESS
4001 Fairview Drive

☑ AUTOMATICALLY CHECK IN GROUPS
☑ AUTOMATICALLY CHECK OUT ROOMS

APPLICATION HOT KEY
MODIFIER KEYS TARGET KEY
☑ ALT O Test
☐ CONTROL
☑ SHIFT

Figure 31 Property Configuration Screen

RETURN TO TABLE OF CONTENTS

License

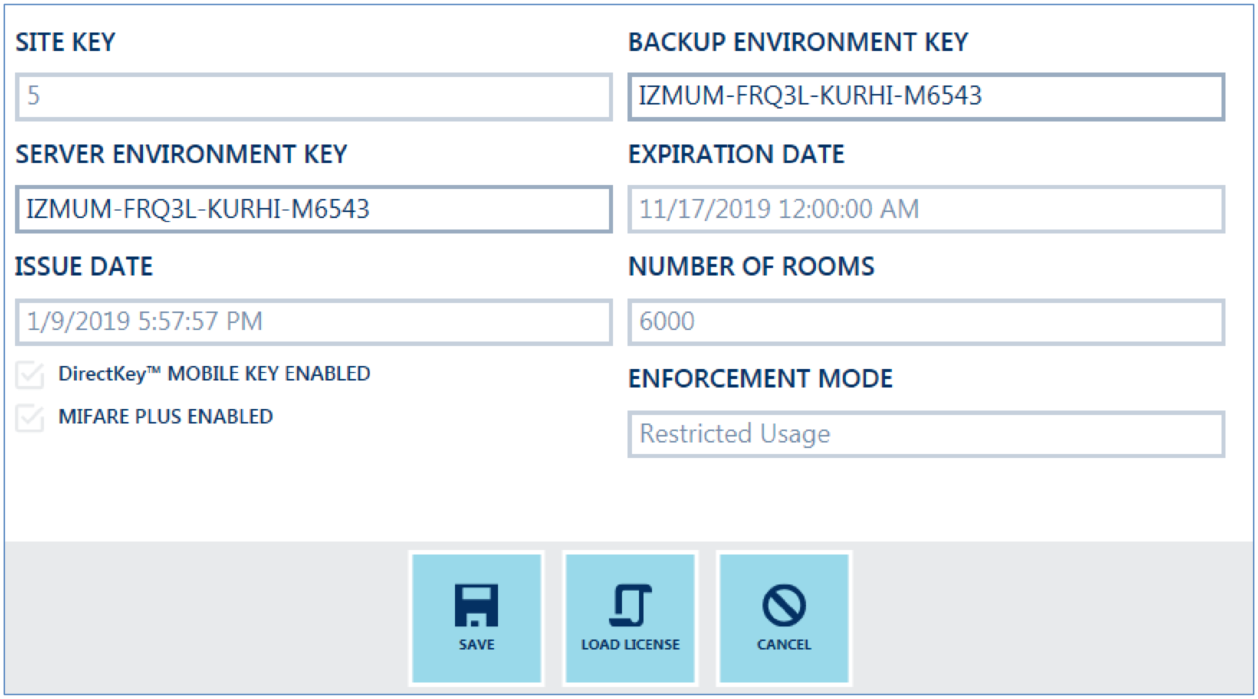
The license section shows the details of the current license, including the following:

1. Site Key – this key should be given to an Onity representative whenever a new license will be generated. This key ties the site to the Onity license server.
2. Server/Backup Environment keys – hardware keys for the server and backup server on the site. These are hardware specific and unique.
3. Site details – the rest of the list shows the details of the license, including the issue date, expiration date, number of allowed rooms, whether or not DirectKey and MIFARE Plus is enabled and the enforcement mode that will be implemented if the license is allowed to expire.

If any changes are needed to the parameters of the site, or the license needs to be renewed, contact Onity to get a new license file.

Step #	Action
1.	Click the LOAD LICENSE icon at the bottom of the screen
2.	Use the BROWSE button to find the new license file
3.	Enter the license password provided to you by Onity
4.	Click IMPORT

If the license and password are correct, the system will be updated with the new license parameters.



SITE KEY: 5

BACKUP ENVIRONMENT KEY: IZMUM-FRQ3L-KURHI-M6543

SERVER ENVIRONMENT KEY: IZMUM-FRQ3L-KURHI-M6543

EXPIRATION DATE: 11/17/2019 12:00:00 AM

ISSUE DATE: 1/9/2019 5:57:57 PM

NUMBER OF ROOMS: 6000

☑ DirectKey™ MOBILE KEY ENABLED

☑ MIFARE PLUS ENABLED

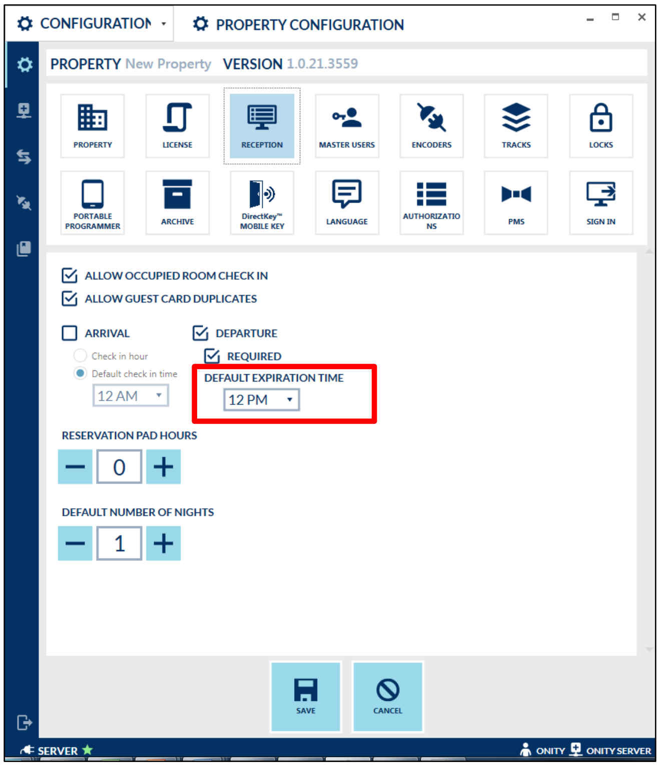
ENFORCEMENT MODE: Restricted Usage

Figure 32 License

RETURN TO TABLE OF CONTENTS

Reception

Step #	Action
1.	**ALLOW OCCUPIED ROOM CHECK-IN:** Selecting this option allows you to check in a new guest even when there is an existing guest key that is still valid. Onity suggests this box be checked.
2.	**ALLOW GUEST CARD DUPLICATES:** Selecting this option allows you to make redundant guest copies. The OnPortal system can uniquely track up to 5 guest card copies. If this option is selected, you will be able to encode as many copies of the guest card as you like, but all cards after the first 5 will be identified as "redundant copy."
3.	**ARRIVAL:** If checked, this requires a start date and time to be encoded on the guest card. This is required if using DirectKey, optional if not. The arrival time can be configured to the hour when the card is encoded (example, a card encoded at 11:30am would have the check-in hour encoded as 11), or to a specific hour of your choosing.
4.	**DEPARTURE:** The default expiration hour for the keycard. On the check-out day, this is the hour past which the key will no longer work in the lock. If using the ARRIVAL option, the DEPARTURE is required. If not using the ARRIVAL option, you have the option to encode keys with no expiration. **ONITY STRONGLY RECOMMENDS REQUIRING EXPIRATION DATE/TIME.**
5.	**RESERVATION PAD HOURS:** When using the arrival date/time, you can pad the arrival hour and expiration hour in order to avoid problems over time with lock time drift or a failure to update the locks for a daylight savings time change. For example, if this field is set to 2, and a guest key is encoded at 11:01am, the start hour encoded on the keycard will be 9am**.** If not padded, the start time would be encoded as 11am. If the lock time is a few minutes behind the OnPortal server, the guest key may not work when initially used for the room. After 11am, the key would begin working. In addition to encoding the card with an earlier hour, the system will also pad the expiration time to be the same number of hours after the default.
6.	**DEFAULT NUMBER OF NIGHTS:** When checking in a guest, the default expiration will be based on this value.
7.	Select **SAVE.**



PROPERTY New Property VERSION 1.0.21.3559

☑ ALLOW OCCUPIED ROOM CHECK IN

☑ ALLOW GUEST CARD DUPLICATES

□ ARRIVAL

○ Check in hour

● Default check in time

12 AM

☑ DEPARTURE

☑ REQUIRED

DEFAULT EXPIRATION TIME

12 PM

RESERVATION PAD HOURS

0

DEFAULT NUMBER OF NIGHTS

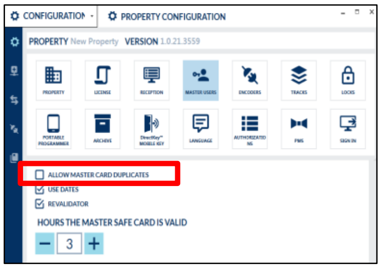
1

Figure 33 Reception Configuration Screen

© 2022 Carrier. Revision 4.

Master Users

Step #	Action
1.	**ALLOW MASTER CARD DUPLICATES:** If checked, copies may be encoded for master cards. These copies are identical to the original card and there is no way to differentiate them. ***NOTE: Onity strongly suggests that this option is unchecked and no master copies are allowed.***
2.	**USE DATES:** Checking this box allows you to encode activation and expiration dates and times on master cards.
3.	**REVALIDATOR:** Allows a master card holder to periodically re-encode the keycard by visiting an OnPortal station, selecting Revalidate, entering their PIN and re-encoding their keycard. This is a security function that will allow you to encode limited-time master cards that must be "revalidated" periodically.
4.	**HOURS THE MASTER SAFE CARD IS VALID:** Only for sites using Onity Card and Keypad safes (OS600). If a guest forgets the PIN used to lock the safe, a hotel staff member may encode a Safe Emergency Card that will be valid only for the number of hours selected in this field. The safe emergency card is used in the safe, followed by the valid guest card to unlock the safe.
5.	Select **SAVE.**



PROPERTY New Property VERSION 1.0.21.3559

☐ ALLOW MASTER CARD DUPLICATES

☑ USE DATES

☑ REVALIDATOR

HOURS THE MASTER SAFE CARD IS VALID

− 3 +

Figure 34 Master Configuration Screen

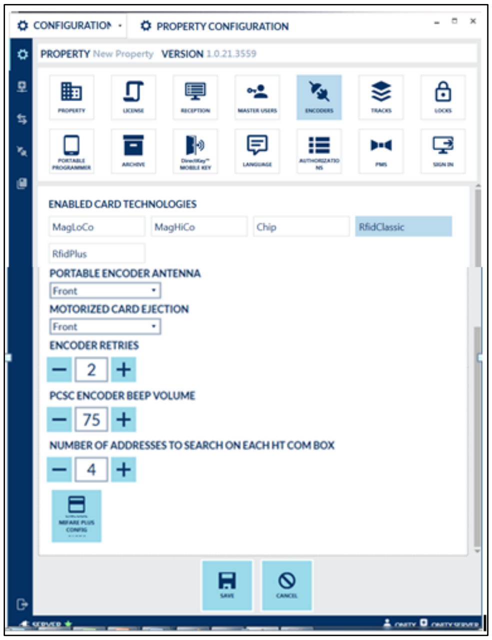
Encoders

The Encoders section is where you can specify parameters based on the type of card technologies and encoders used at the property. ***NOTE:*** *Typically, a property will use only one card technology but you are not limited to this if you are using more than one. For example, if you have magnetic stripe locks and use low-coercivity keycard for guests and high-coercivity keycards for master card holders.*

These options are typically configured by Onity but there may be occasions when changes are required.

Step #	Action
1.	**ENABLED CARD TECHNOLOGIES:** This is driven by the type of locks used by the property as well as the encoders. If using magnetic stripe locks, the encoder determines if you will use Low Coercivity (LoCo) or High Coercivity (HiCo) or a combination of these types. The Onity insertion mag encoders only encode LoCo keycards. Motorized mag encoders may be configured to LoCo or HiCo depending on the needs of the property. Chip cards may be used if the HT28 locks are installed at the property. These are contact smart cards and typically are only used by master card holders. For properties using Trillium or ADVANCE Trillium RFID locks, you have the option to use MIFARE Classic or MIFARE Plus technology. If using MIFARE Plus, the option must be enabled by the license. Also, when using MIFARE Plus, you will need to periodically encode a MIFARE Classic card create the configuration cards. For properties using Serene and Trillium and/or ADVANCE Trillium RFID, MIFARE Classic may not be used; MIFARE Plus must be used. For properties only using Serene, you must use MIFARE Plus or MIFARE Ultralight C technology.

2.	**PORTABLE ENCODER ANTENNA** refers to the small RFID encoder that was part of the OnPoint system. This encoder is configurable to support encoding from the top (the surface above the insertion point) or the front (the surface on the face of the insertion point).
3.	**MOTORIZED CARD EJECTION.** In most cases, leave this as the default. Some kiosk systems using the Onity encoder require the ejection to the rear, but this is rare.
4.	**ENCODER RETRIES.** This is the number of times OnPortal will retry after a failed encode; it should be a minimum of 2.
5.	**PCSC ENCODER BEEP VOLUME.** This is a percentage of the volume level for the OnPortal RFID Encoder; if the site wishes it to be quieter or louder, adjust the number accordingly.
6.	**NUMBER OF ADDRESSES TO SEARCH ON EACH HTCOM BOX.** If the site is using HT22 encoders attached to a HTCOM box, enter the maximum number of encoders attached to any one COM box on site.
7.	Select **SAVE.**



PROPERTY New Property VERSION 1.0.21.3559

ENABLED CARD TECHNOLOGIES: MagLoCo, MagHiCo, Chip, RfidClassic, RfidPlus

PORTABLE ENCODER ANTENNA: Front

MOTORIZED CARD EJECTION: Front

ENCODER RETRIES: 2

PCSC ENCODER BEEP VOLUME: 75

NUMBER OF ADDRESSES TO SEARCH ON EACH HT COM BOX: 4

Figure 35 Encoder Configuration Screen

Encode MIFARE PLUS®-style Config Cards

MIFARE Plus-style configuration cards are required for all sites with Serene locks. To set the locks into MIFARE Plus mode, a configuration card must be encoded and linked to a master card that can open each lock. This master card must be encoded using a MIFARE Classic 1K keycard and the configuration card must be encoded using a MIFARE Plus keycard. Ultralight and Ultralight-C cards cannot be used as the configuration card pair.

If you want to use MIFARE Plus with Trillium or ADVANCE Trillium locks, you must have a master card encoded on a MIFARE Classic 1K keycard that can open all locks on the property, and have at least one MIFARE PLUS 2K or greater keycard. Onity recommends that you name the associated master card “Configuration Master” or something similar remember which card is used with the configuration card to set the locks into MIFARE Plus mode. Note that once the locks are set to MIFARE Plus mode, this configuration master keycard (which is MIFARE Classic) will no longer work in the locks.

NOTE: *To encode the associated master card, you must set the encoder to* RFID Classic *mode in the encoder’s screen in the* configuration *section. See the* Encoders *section. Once card is encoded, you should change the encoder back to* RFID Plus*.*

The configuration card is encoded from within the ENCODERS screen of the CONFIGURATION section. Select the ENCODE MIFARE PLUS CONFIG CARDS icon to begin.

Step #	Action
1.	Select **ENCODE MIFARE PLUS CONFIG CARDS**.
2.	Select an existing master card to use with the config card created.
3.	Select **OK** to encode the MIFARE PLUS config card (must not be a UL-C card).
4.	See the Trillium user guide for instructions on converting a lock to use MIFARE PLUS with configuration cards.

Once the configuration card pair is created, take the pair of cards to each lock in the system and present the cards together to the lock. The lock will give a green light and emit a confirmation tone if successful. To test to ensure the lock entered *MIFARE Plus* mode, use a master card encoded on a *MIFARE Plus* or *UL-C* card. If it successfully opens the lock, the process is complete. The *MIFARE Classic* card used with the configuration card will no longer work in the lock and you will get a delayed red light if you try to use it.

NOTE: *All locks come from the factory in* MIFARE Classic *mode, even if they have been repaired and returned. Any time you install a new lock, you must configure it for* MIFARE Plus *mode.*

Important: Keep the configuration card pair (or pairs) together in a safe place.

Tracks (optional, configure if site is using additional tracks or sectors)

The tracks section allows you set up the method of encoding data on a different track (for magnetic stripe cards) or sectors (for RFID cards). This is typically used for interfacing with point of sale (POS), parking systems, or other non-Onity systems.

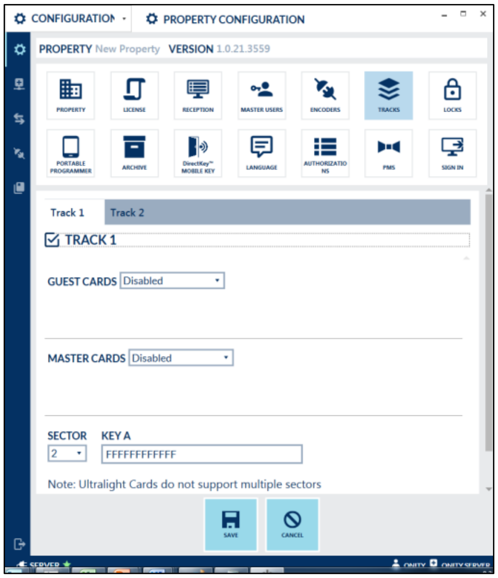
Onity can write default data such as room number, authorizations, and expiration date/time but also can be configured to allow custom data (typically received through the PMS interface). Note that when encoding data on magnetic stripe tracks 1 or 2, Onity writes the data to ISO standards.

Step #	Action
1.	There are two track tabs; check the box for *Track 1* and/or *Track 2* to configure.
2.	Select a **GUEST CARDS** option. **Disabled** = No data on this track. **Prompt for Custom Data** = Forces the system to bring a pop-up to type in custom data based upon the template below. **No Prompt** = Fills the track with the pre-defined data listed in the template, along with any custom data sent from a PMS. ***Pad*** = Software will fill the track with insignificant characters after the encoding data if this is checked.
3.	Select a **FORMAT.** **Guest Standard** = Room, authorizations, expiration date and custom data, depending on the option above. **Micros** = Room, expiration date, and custom data, depending on the option above. **Custom** = Create a proper string for this track under *Template*. Separate each string option with a caret (^) sign. The options are: {Room} {Auths} {Expire} {CustomData} Typically, you will just leave {CustomData} in the template and remove the rest.
4.	Select a **MASTER CARDS** option and **FORMAT** (same as guest cards above).
5.	**SECTOR** - Select which sector you will be writing this data on for RFID cards. ***NOTE:*** *Ultralight and Ultralight-C cards do not have multiple sectors – you must use* MIFARE Classic *or* MIFARE Plus *cards to use this function.*
6.	**KEY A** = Input from the third-party that will be reading this sector is required. Onity recommends that you provide the contact person and information so we may work together to ensure this is set up correctly.

© 2022 Carrier. Revision 4. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

7.	**PMS RETURN SENTINELS** = When checked, Onity will add the ISO standard start and end sentinels to the data sent from the PMS system. If you are using magnetic stripe encoding, Onity suggests you check this box unless the PMS company recommends against it. If using RFID cards, Onity recommends unchecking this box.
8.	Select **SAVE**.



PROPERTY New Property VERSION 1.0.21.3559

☑ TRACK 1

GUEST CARDS Disabled

MASTER CARDS Disabled

SECTOR 2

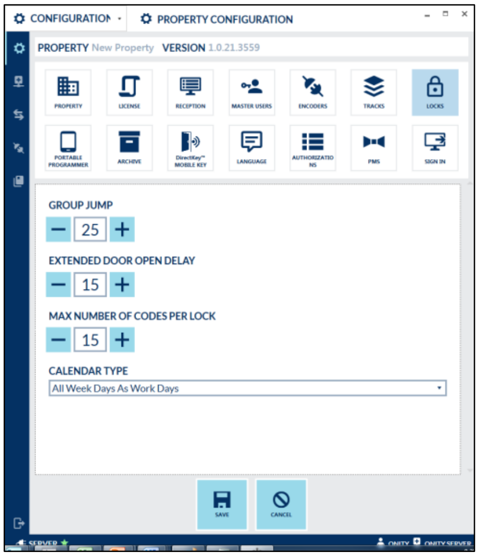
KEY A FFFFFFFFFFFF

Note: Ultralight Cards do not support multiple sectors

Figure 36 Tracks Configuration Screen

Locks

Step #	Action
1.	**GROUP JUMP.** Refers to the future encoding capability of group pre-encoded cards. This should be set to 25 and not changed unless you are specifically told to do so by Onity.
2.	**EXTENDED DOOR OPEN DELAY.** If a room is designated for people with disabilities, the door will remain unlocked for this many seconds. Typically this is higher than the standard opening delay to allow for more time to enter the room. Note that typically locks are configured to lock back as soon as the lever is released.
3.	**MAX NUMBER OF CODES PER LOCK.** Sets the number of master codes allowed to be programmed in the lock for standard doors. Typically this is set to 15 but it may be changed to as many as 250 if needed. Note that most common doors are configured as “selective” mode locks and this limit does not apply to these.
4.	**CALENDAR TYPE.** For most hotels, leave this as *All Week Days* as *Work Days*. If you are using automatic openings and card shifts and you wish these to be configured differently for week days and weekends, you can select a different option and configure the changes and shifts accordingly.
5.	Select **SAVE.**



GROUP JUMP: 25

EXTENDED DOOR OPEN DELAY: 15

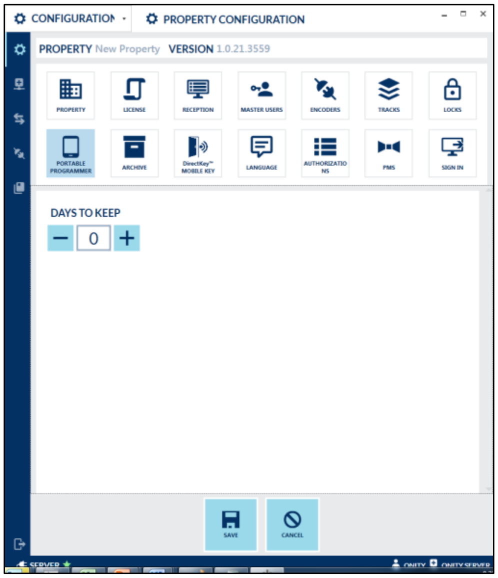
MAX NUMBER OF CODES PER LOCK: 15

CALENDAR TYPE: All Week Days As Work Days

Figure 37 Locks Configuration Screen

Portable Programmer

Step #	Action
1.	**DAYS TO KEEP.** Enter the number of days the tablet or laptop should maintain the lock's data once it has been loaded. After this many days, the data will be automatically erased (audits will remain to be uploaded to the server when connected again). Onity recommends leaving this at zero, which will erase the data at midnight.
2.	Select **SAVE.**



DAYS TO KEEP: 0

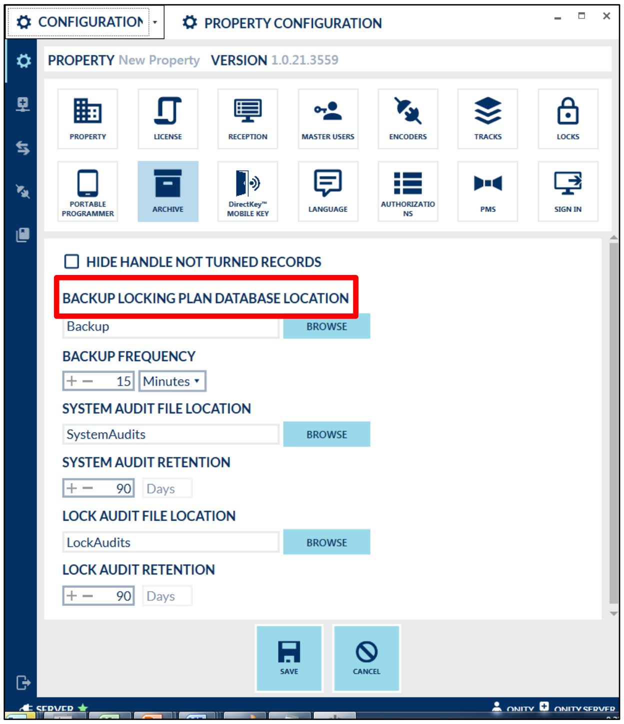
Figure 38 Portable Programmer Configuration Screen

Archive

This section enables you to specify details of database backups as well as audit archives. Specify the location and the frequency (for backups) or number of days to retain (for audit information) in this section.

NOTE: *Moving the audits to archive removes them from the active database and creates a comma-separated values (.csv) file. These are still available for viewing using Microsoft Excel or other .csv file viewer.*

Step #	Action
1.	**HIDE HANDLE NOT TURNED RECORDS.** In most cases, leave this unchecked as this function is only for legacy support for a specific lock module.
2.	*BACKUP LOCKING PLAN DATABASE LOCATION* defaults to the *C:\Onity\OnPortal\FrontDeskClient\Backup* (Provided OnPortal was installed in the C:\ level) folder. Leaving it simply as *Backup* refers to that location. To change location, select the **BROWSE** option and select an appropriate folder.
3.	Select the **BACKUP FREQUENCY** for the locking plan; if unsure, leave default of 15 minutes.
4.	*SYSTEM AUDIT FILE LOCATION* and *LOCK AUDIT FILE LOCATION* behave the same as the Backup location. OnPortal has folders for *SystemAudits* and *LockAudits* under the *FrontDeskClient* folder.
5.	Select how long the system should retain system audits and lock audits next to **Days**. The bigger the number here, the larger the database becomes. Default is 90 days.
6.	Select **SAVE.**



PROPERTY New Property VERSION 1.0.21.3559

□ HIDE HANDLE NOT TURNED RECORDS

BACKUP LOCKING PLAN DATABASE LOCATION: Backup

BACKUP FREQUENCY: 15 Minutes

SYSTEM AUDIT FILE LOCATION: SystemAudits

SYSTEM AUDIT RETENTION: 90 Days

LOCK AUDIT FILE LOCATION: LockAudits

LOCK AUDIT RETENTION: 90 Days

Figure 39 Archive Configuration Screen

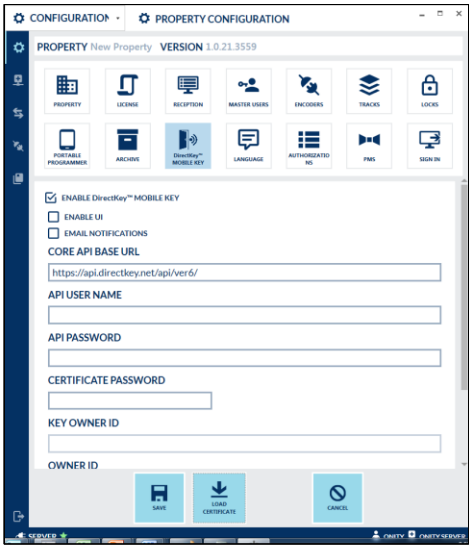
DirectKey™ MOBILE KEY (optional, configure only if site is using DirectKey).

Before setting up Mobile Key, go to **CONFIGURATION > RECEPTION**, and verify that the **ARRIVAL** checkbox has a checkmark in it; if not, fill it in. No DirectKey setup can be saved unless that box is checked.

To properly configure this section, you must work with Onity to get the required information and passwords.

Step #	Action
1.	**ENABLE DirectKey™ MOBILE KEY**, check the box.
2.	If the site will be using OnPortal to generate mobile keys, select **ENABLE UI**.
3.	If selecting **ENABLE UI**, also select **EMAIL NOTIFICATIONS**.
4.	The data and certificate to set this up will come from Onity. Contact the Onity Rep regarding obtaining this certificate and passwords prior to arriving on site. Some regions may leverage the portal page of OnityNET to distribute the certificates and passwords.
5.	The *CORE API BASE URL* = https://api.directkey.net/api/ver6

6.	*API USER NAME*; enter the API User Name received from Onity Rep.
7.	*API PASSWORD*; enter the API Password received from Onity Rep.
8.	*CERTIFICATE PASSWORD*; enter the cert password received from Onity Rep.
9.	Select **LOAD CERTIFICATE** at the bottom of the screen. Transfer the certificate to the server machine. Browse to the location of the certificate. Select the .pfx file. Select **OK**. Upon success, a check appears next to **Certificate Loaded**.
10.	**USE EXPLICIT PROXY** checkboxes. If this computer requires a proxy server to access the Internet and connect to Onity's cloud of servers, check this box. *Proxy Address* = IP Address:PORT NUMBER of the proxy server. *User Name* = Login name that allows access to the Internet. *Password* = Password for the login name. ***NOTE:*** *This information must be obtained from your system administrator.*
11.	Once configured, select **TEST** to test connection to Onity servers. The *KEY OWNER ID*, *OWNER ID*, and *PROPERTY NAME* on the server will fill in after a successful test. ***NOTE:*** *Configuration will not save unless there is a successful test.*
12.	Select **SAVE**.



PROPERTY New Property VERSION 1.0.21.3559

☑ ENABLE DirectKey™ MOBILE KEY

☐ ENABLE UI

☐ EMAIL NOTIFICATIONS

CORE API BASE URL: https://api.directkey.net/api/ver6/

API USER NAME

API PASSWORD

CERTIFICATE PASSWORD

KEY OWNER ID

OWNER ID

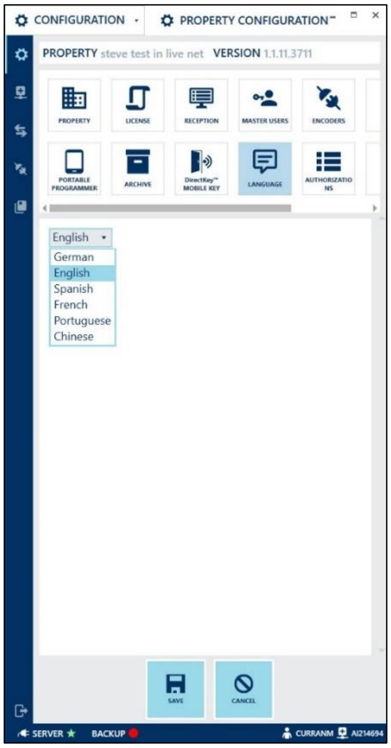
Figure 40 DirectKey™ Mobile Key Configuration Screen

NOTE*: A gray* Enable DirectKey™ Mobile Key *checkbox indicates the license did not have DirectKey enabled. Verify that there is a checkmark for* DirectKey™ Mobile Key Enabled *under* License*; if there is not, a new license is required.*

Language

Select the default language. Each operator may change the language for personal use.

RETURN TO TABLE OF CONTENTS



PROPERTY steve test in live net VERSION 1.1.11.3711

Figure 41 Property Configuration Screen Showing Language Options

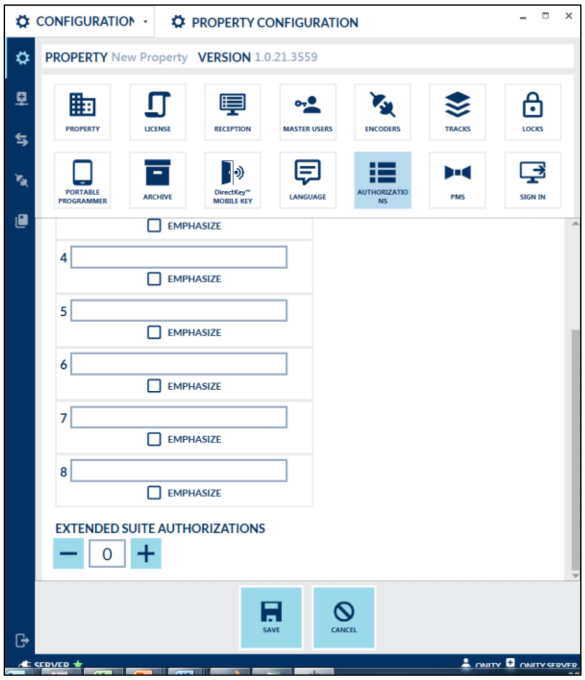
Authorizations

Authorizations are used to restrict access beyond the standard credential and data/time details. For example, a family may wish to have a key for a child but does not want to allow that child to access areas such as the pool or a fitness room. This would be handled by creating an authorization and adding that authorization to the parent's keycards but not adding it to the child's keycard upon check-in. Another use could be for granting access to a concierge level or lounge where you grant this access only to high-level members of your loyalty program.

The OnPortal system allows for up to 8 authorizations. In this section, you are given the option to name the authorization to make it informative to the people encoding the keys. You also are given the option to "emphasize" the authorization, which means it will have a star next to it on the encoding screen.

Authorizations may be optional or automatic. This is set up in the locking plan profile for the locks and not in the configuration section. In the example of the concierge level, any rooms on that level would have the authorization automatically applied while rooms on other levels could be optionally applied.

Step #	Action
1.	Enter a name that identifies this authorization. • Enter a name to identify this authorization. • Select whether to **EMPHASIZE** the authorization (Emphasize means the authorization shows up with a "star" when checking a guest into a room and is just to draw attention to the authorization).
2.	Add any additional authorizations required.
3.	If the site uses Extended Suites to create suite scenarios that require the use of authorizations, those authorizations will not be able to be used for other purposes. The number of extended suites authorizations will be set when the locking plan is created. Onity recommends that you only change this number if specifically instructed to do so by Onity.
4.	Select **SAVE.**



PROPERTY New Property VERSION 1.0.21.3559

□ EMPHASIZE

4

□ EMPHASIZE

5

□ EMPHASIZE

6

□ EMPHASIZE

7

□ EMPHASIZE

8

□ EMPHASIZE

EXTENDED SUITE AUTHORIZATIONS

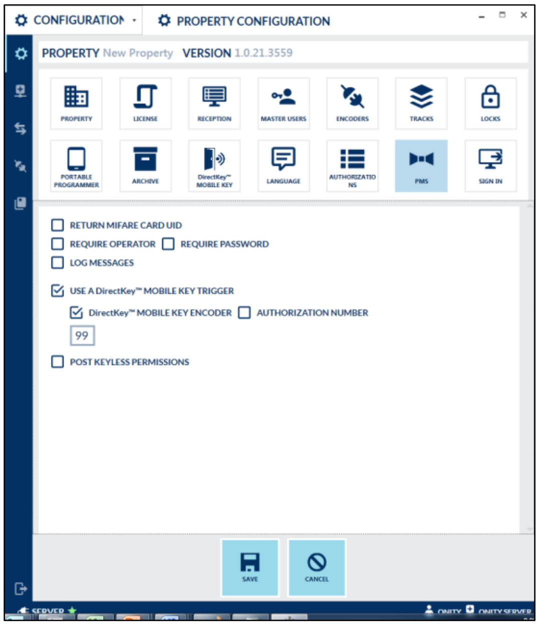
− 0 +

Figure 42 Authorization Configuration Screen

PMS (configure if site is using a PMS interface)

If the OnPortal system will be receiving commands from the PMS, this section (or the next on Cloud PMS) must be configured.

Step #	Action
1.	Leave **RETURN MIFARE CARD UID** unchecked unless the PMS Service requests it. This is a special scenario to be used when a POS or other third-party system will be reading the unique ID from the RFID key.
2.	**REQUIRE OPERATOR** and/or **REQUIRE PASSWORD** should be selected if the PMS will send this information with the PMS command. This is an added security feature that will only allow the commands to be processed if the operator and/or password is correct. Not all systems are set up to send this data.
3.	**LOG MESSAGES** and **LOG FLOW CONTROL** are used for troubleshooting purposes. When turning these on, the PMS messages will show up in the System Audit. Onity recommends that these functions be turned off unless troubleshooting problems with the interface.
4.	**USE A DIRECTKEY™ MOBILE KEY TRIGGER** is only available if enabling DirectKey above. The certificate MUST be loaded and tested under Mobile Key before any of the triggers will function. When to use a **USE A DIRECTKEY™ MOBILE KEY TRIGGER**. If the PMS will send a command to create a DirectKey mobile key, check this box and set the applicable trigger. This may be an encoder number (such as encoder 99) or may be based on a specific authorization. You must work with the PMS company to see exactly what trigger will be used.
5.	**POST KEYLESS PERMISSIONS.** This should only be selected if the DirectKey mobile key will be managed by a third-party system. Checking this box will allow the PMS interface command to request a DirectKey mobile key without sending the email or key serial # associated with the mobile device. If not checked and no email or key serial # is sent with the PMS interface command, a syntax error will be returned. If you are managing the DirectKey mobile key through OnPortal, do not select this box. If you are managing the mobile keys from a third-party system, check this box.
6.	Select **SAVE.**



PROPERTY New Property VERSION 1.0.21.3559

☐ RETURN MIFARE CARD UID

☐ REQUIRE OPERATOR ☐ REQUIRE PASSWORD

☐ LOG MESSAGES

☑ USE A DirectKey™ MOBILE KEY TRIGGER

☑ DirectKey™ MOBILE KEY ENCODER ☐ AUTHORIZATION NUMBER

99

☐ POST KEYLESS PERMISSIONS

Figure 43 PMS Configuration Screen

RETURN TO TABLE OF CONTENTS

Cloud PMS

Utilize the Cloud PMS to check in guests and perform any card operation remotely.

Step #	Action
1.	Under the main drop-down menu, click **CONFIGURATION**.
2.	Under the Configuration menu, click the **ENABLE** slider under *Cloud Configuration*.

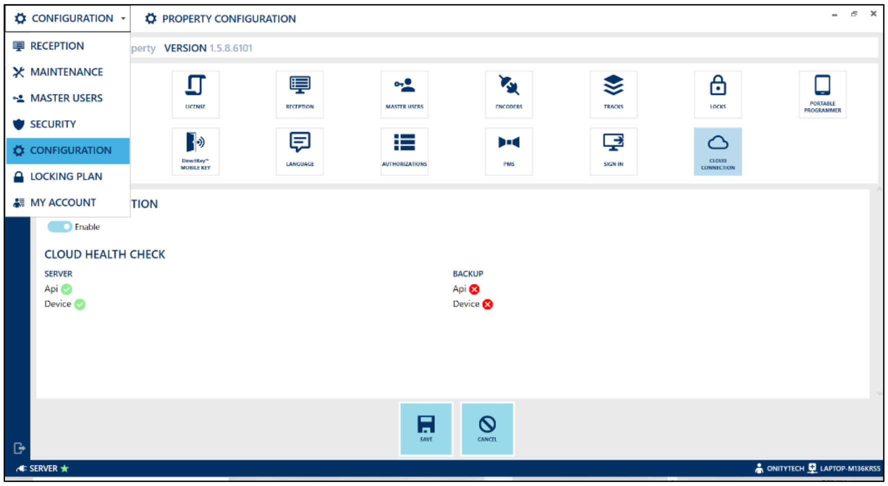


Figure 44 Main Drop-down Menu - Configuration

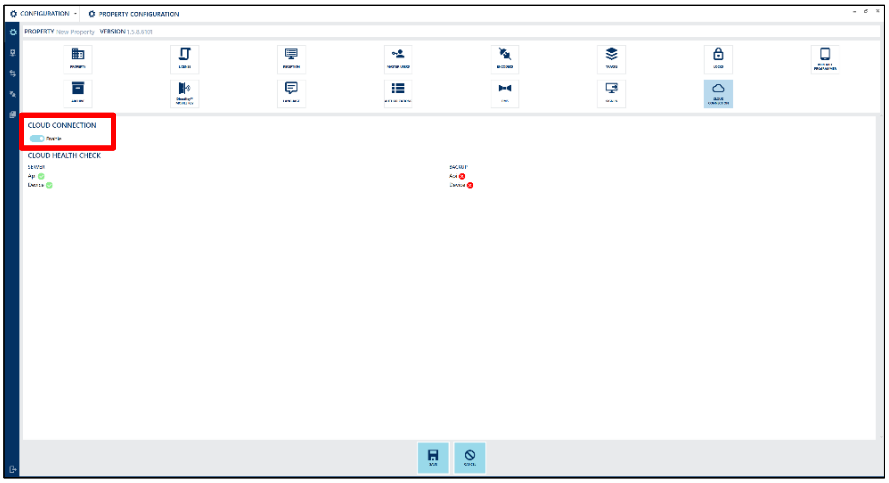


Figure 45 Configuration Slider

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99
© 2022 Carrier. Revision 4. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Sign In

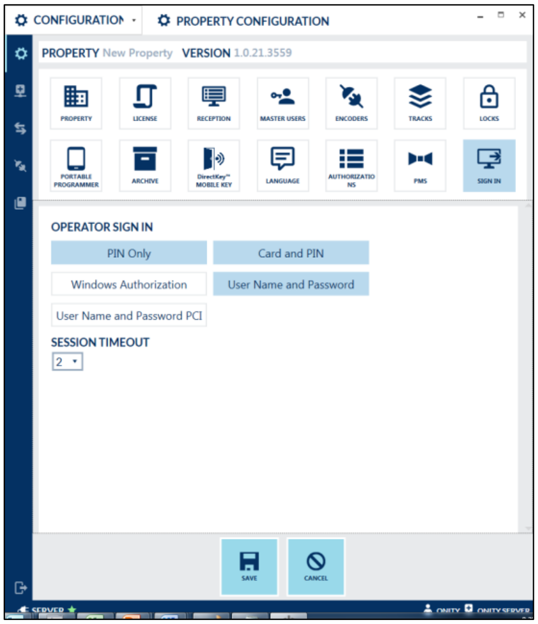
Sign-In Type	Description
PIN Only	A Personal Identification Number (PIN) uses a four-digit login. The system-assigned PIN cannot be changed and is the least secure login method.
Card and PIN	A four-digit PIN with a card to verify the person. This option forces the user to personalize the PIN code. Encoding a new operator card invalidates the old operator card.
Windows Authorization	OnPortal does not present a login screen, it just logs in. This sign-in type requires that the operator name in OnPortal match exactly with the user name in Windows. **CAUTION:** This login type is a potential security risk if the operator has any rights other than *RECEPTION*. For example, suppose the GM uses Windows Authorization to log in, does his work then logs out so that a front desk operator can log in. The operator could simply close the program, re-open it, and be logged in with the same rights as the GM.
User Name and Password	Password is at least 4 characters, contains an uppercase letter, lowercase letter, and a number (symbols are allowed). The system forces the user to change passwords every 180 days and does not allow reuse of any of the last 4 passwords.
User Name and Password PCI	Password is at least 7 characters, contains uppercase, lowercase, and numbers (symbols are allowed). The system forces the user to change the password every 90 days and does not allow use of any of the last 4 passwords.
Onity API User Password	This feature is used with third-party integrations.

Operator Sign-in

Step #	Action
1.	Select the appropriate buttons for the login types the site desires to use.
2.	**SESSION TIMEOUT** is what each *Role* will default to upon creation. Note that actual *SESSION TIMEOUT* for a user is whatever is set for their *Role*.
3.	Select **SAVE.**

Login Lockouts

OnPortal locks out the user for 15 minutes after six invalid sign-in attempts. Another user who is active within the system and has resetting permissions may reset the password to unlock the account.



PROPERTY New Property VERSION 1.0.21.3559

OPERATOR SIGN IN

[✓ PIN Only] [✓ Card and PIN]

Windows Authorization [✓ User Name and Password]

User Name and Password PCI

SESSION TIMEOUT

2

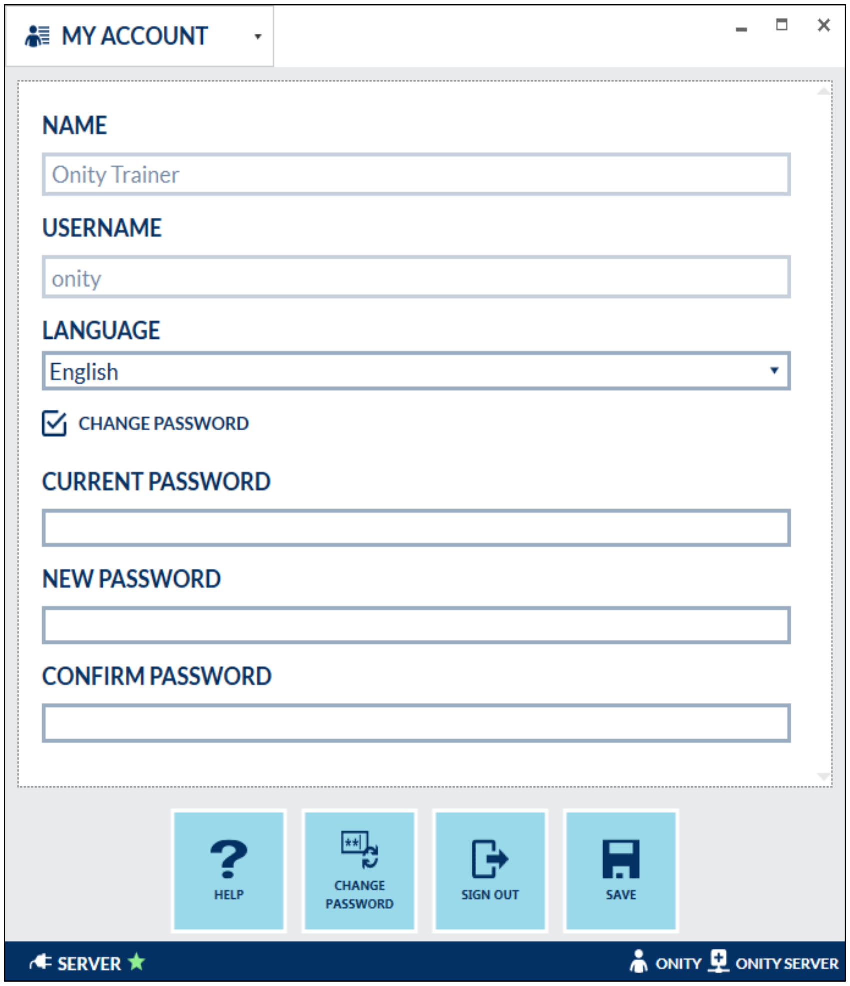
Figure 46 Sign-In Configuration Screen

RETURN TO TABLE OF CONTENTS

My Account

Operators may change their default language and password (where allowed) using the *My Account* section of the software. Note that some login types, such as PIN Only or Windows Authentication, do not allow for password changes.

Step #	Action
1.	Select **MY ACCOUNT** from the drop-down box.
2.	Change **LANGUAGE** if needed.
3.	To **CHANGE PASSWORD**, check box. • Enter the Current Password. • Enter a New Password. • Enter the new password in the *Confirm Password* box. • Select **CHANGE PASSWORD** to change.
4.	Select ? HELP to access help files.
5.	Select **SIGN OUT** to log out of OnPortal.
6.	Select **SAVE** to save a language change.


MY ACCOUNT

NAME: Onity Trainer

USERNAME: onity

LANGUAGE: English

☑ CHANGE PASSWORD

CURRENT PASSWORD:

NEW PASSWORD:

CONFIRM PASSWORD:

Figure 47 My Account Screen

RETURN TO TABLE OF CONTENTS

License Expiration and Renewal

OnPortal uses a software license to provide functionality to a site. The licenses are time-limited and require a new certificate to be downloaded and loaded upon renewal. OnPortal provides warning that the license is going to expire, warns for a while once the license is expired without limiting the site, then, after a grace period, stops providing some functionality to the site. Onity recommends renewing the license prior to the expiration date to avoid losing functionality.

If you have any questions about this process, contact your regional Onity support team.

Requesting a License Renewal

Step #	Action
1.	Log into OnPortal with configuration rights and go to the **CONFIGURATIONS** menu.
2.	Select **LICENSE**.
3.	Note the *Site Key* for this license. This will help the Onity Rep locate the correct license.
4.	Contact Onity to purchase the license renewal. Provide: • Site key • Current name of the site • Current address of the site • Any ownership changes at the site
5.	Once the order is processed, the Onity Rep sends an email with a link to download the new license from Onity.net.

Retrieving the License

Step #	Action
1.	The email should contain instructions to download the license and instructions to load it into OnPortal.
2.	Use the link to go to the Onity.net portal page for this location.
3.	Select **GET LICENSE.**
4.	Save the license in a known location.

Load the License

Step #	Action
1.	Open OnPortal, log in with a user having *CONFIGURATION* permissions (GM, Onity Tech, etc.).
2.	Select **CONFIGURATION** menu.
3.	Select **LICENSE**.
4.	Select **LOAD LICENSE**.
5.	**BROWSE** to the new license file location, select file and select **OK**.
6.	Enter in the characters after the last "\" in the link as the *LICENSE PASSWORD*. For example in the link http://onity.net/portal/3/ojqqy-oadge-x6waz, *ojqqy-oadge-x6wax* is the license password.
7.	Select **IMPORT** to complete loading the license.

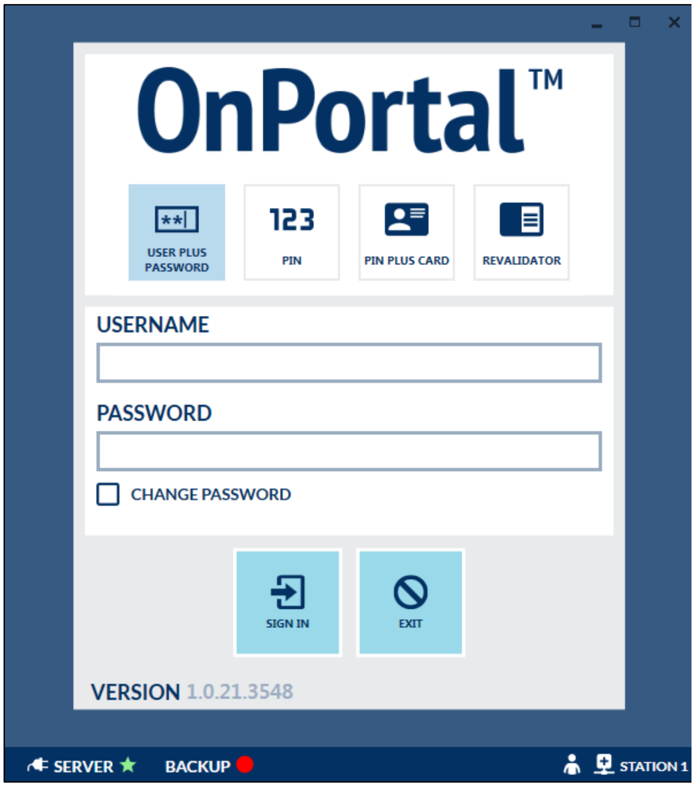
Managing System Status

OnPortal relies on an active network for all remote stations. When a station is not communicating with the server, the first step is to troubleshoot the system's status.

System Status Bar

The "status bar" at the bottom of OnPortal displays information about the status of the system.

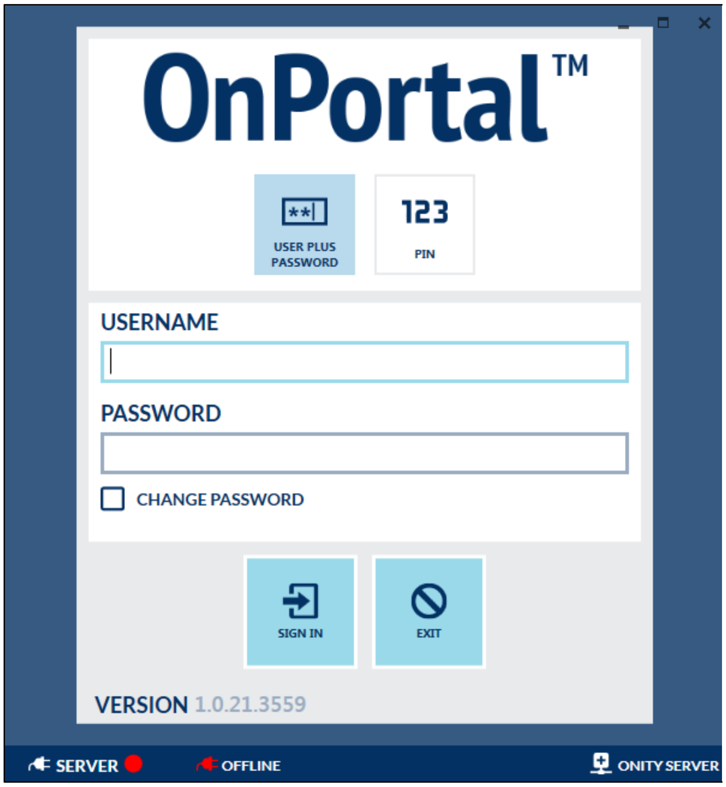
Icon	Meaning
★	Indicates the server is connected and running.
★	Indicates the server is not running or the client is unable to connect to the server.
🟢	Indicates the backup server is connected and running.
🔴	Indicates the backup server is not running or the client is unable to connect to the backup server.
🔌	Indicates the server and backup server status section.
👤	After logging in, the logged-in operator's name shows here.
🖥	Indicates the name of the station in use.
🔌 OFFLINE	Indicates that this system loaded the portable programmer previously but no longer has a connection to the server. This allows logging into a portable programmer, even if the server is down.



VERSION 1.0.21.3548

SERVER ★ BACKUP 🔴 👤 STATION 1

Figure 48 System Status, Backup Service Not Running



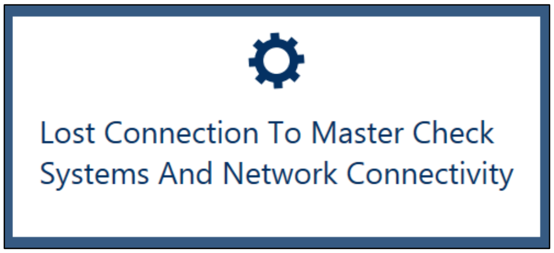
VERSION 1.0.21.3559

SERVER 🔴 OFFLINE ONITY SERVER

Figure 49 System Status, Programmer Loaded, Server Offline

Server Offline

When the main server goes offline, any stations that have the user interface running (and did not load the programmer previously) receive this error message.



Lost Connection To Master Check Systems And Network Connectivity

Figure 50 Server Offline Screen

Causes of Server Offline

Causes	Reason
Date and time mismatch	The date and time on the station are different from the date and time on the server.
Expired certificate	The networking certificates on the backup/stations have expired.
Service stopped	The OnPortal Node Service stopped on the server. The service can be restarted by an administrator of the system in Windows Services (look for OnPortal Node Service) or the server may need to be rebooted. Contact your system administrator in this case.
Computer off	The server machine is off or has lost power.
Firewall blocking	A firewall blocked communication to the server.
Network issue	There is no network connection between the server and this station.

NOTE: *It is always best to attempt to remedy the reason for this message rather than failing the system over to use the backup machine instead. Most of these are network or Windows issues so they may require someone with network/Windows knowledge and administrator rights at the site to remedy the error message.*

Renew Networking Certificates

Before beginning network troubleshooting, try to log in on the server machine. If you are able to log in to the server, the problem is a network issue.

Step #	Action
1.	Go to the **CONFIGURATIONS > STATIONS** screen.
2.	The lower right corner indicates the certificate status among stations.
3.	If the *Days Remaining* is zero or less, select the **RENEW SECURITY** button.
4.	Select **OK** provided the instructions in the message are met.

Restart OnPortal Node Service

The instructions here work on any version of Windows.

Step #	Action
1.	Hold down the key with the Windows logo on it and press the letter “R” at the same time to bring up the run screen.
2.	Type in “services.msc” (without quotes) and select **OK**.
3.	The services window appears, with services listed alphabetically.
4.	Scroll through the list of services and locate *OnPortal Node Service*.
5.	The service status should read “Started” and the startup type as “Automatic (Delayed).”
6.	If the service status is blank, start the service. • On the left upper part of the screen, select **Start the Service**.

7.	The other option available is to **Restart the Service**. Although this implies that the service is running, it does not hurt to try restarting the service if you are unable to log into the server.

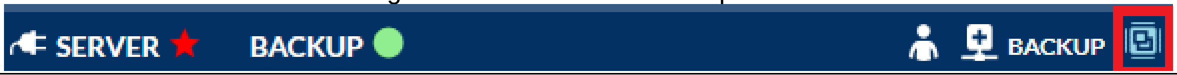
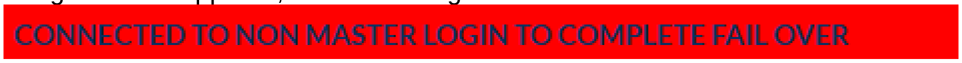
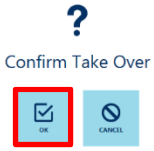
Unable to Get Connection to Main Server

If, after troubleshooting the issue, it appears that the connection will be down for a while, there is a way to make the backup server into the main server. This is called “Fail Over.” There are some important details to test prior to conducting a Fail Over.

Prerequisite	Reason
Stations and Backup Communicating	There is no reason to fail over if the stations cannot communicate with the backup.
OnPortal Node Service runs on Backup machine.	Machines cannot fail over unless the service runs.

Fail Over and Non-Master Login

Again, this option is a last resort. Try to fix the connection issue rather than instantly failing over to the backup server.

Step #	Action
1.	When the “Lost Connection…” error message appears, a new icon shows up in the status bar. Notice the red star for the server indicating no connection to the node service on the server. Indicated below is the **Fail Over** button seen on the lower right of the screen. Select to perform a fail over. 
2.	A login screen appears, with a message in red across the bottom.  CONNECTED TO NON MASTER LOGIN TO COMPLETE FAIL OVER ***NOTE:*** *The role for the user must include the* Config Fail Over *permission under* **CONFIGURATION**. *Perform a login as a user.*
3.	Confirm takeover when prompted 
4.	If using the PMS interface with the listener on the main server, a listener must be created on the backup server or a client PC and the Property Management System must either have the serial connection changed to the new machine or have the IP connection settings modified to reflect the new OnPortal server. Contact your system administrator for this step.

Return Control to Server Machine

Once the connection/computer is running and connecting to the backup and stations again, return control to the main server.

Step #	Action
1.	Start the OnPortal program on the server.
2.	Be patient, as it takes time to load. For a few moments, two green stars appear in the status bar. The server is communicating with the backup machine; once the backup machine becomes the server, the green star turns to a green dot.
3.	Log in if the backup machine shows as a green star. If it is a red star, there is no connection to the backup node service so the problem still exists. Contact your network administrator to troubleshoot connectivity.
4.	Go to **CONFIGURATION > STATIONS** and select the main server machine to bring up the details.
5.	Select **TAKEOVER** in the lower right.
6.	Perform the *Non-Master* login as prompted.
7.	Select **OK** to confirm.

8.	When done, the green star returns to the server machine and a green dot shows on the backup.
9.	Verify that users can log into any remote stations after completing the takeover.

Replacing Existing OnPortal Machines

Since the OnPortal license only works on machines where the environment keys match the license, replacing a server takes a bit more effort than simply installing the program and hooking everything up. The steps required differ whether it is a server, backup, or station.

Main Server Replacement

Visit www.onity.com to find your local Tech Support and they will walk you through the following steps.

Step #	Action
1.	These instructions assume that the system failed over to use the backup machine. If it has not, fail over to the backup machine prior to replacing the server.
2.	Contact an Onity Rep with the *Site Key* (in OnPortal, go to **CONFIGURATION > LICENSE**) to receive an email with a link to the Onity.Net portal page.
3.	Download and install the program up to the Configure Server step as per the instructions in Task 6 in Appendix A, Installing OnPortal.
4.	Run the program on the new machine. • **Copy** the environment key. • Paste it in the *Server Environment Key* on the portal page. • Select **SAVE KEYS** on the portal page.
5.	Download the new license by selecting **GET LICENSE**.
6.	Go to the backup machine. • Open Windows Explorer, and navigate to the install directory of OnPortal (typically *C:\Onity\OnPortal\FrontDeskClient*). • Make a copy of the *Onity.LockingPlan.swf* file. This is the current locking plan used by the system. • Paste or transfer this file to media accessible by the new server (copy to a thumb drive, or transfer via the network to the server machine). ***NOTE:*** *Onity recommends stopping the OnPortal node service on the backup machine after copying the locking plan. This will prevent any other stations from issuing cards or changing the locking plan while the new server is being loaded.*
7.	Finish the *Configure Server* steps in Appendix A, Installing OnPortal for installation using the newly downloaded license, the license password from the portal page link, and the locking plan retrieved from the backup machine. **CAUTION:** Do not forget to rename the server machine before installing.
8.	On the backup machine, close the OnPortal program (if running), open Windows Explorer, and navigate to the OnPortal directory. • Delete the following three files from the FrontDeskClient folder: ○ *LicenseData.bpex* ○ *Onity.LockingPlan.swf* ○ *NodeConfig.json* • Start the program; it will be on the Install screen (start the node service first if stopped). • Finish configuring the backup machine as per the steps under *Configure Backup Server* in Appendix A, Installing OnPortal.
9.	On all stations, close OnPortal program (if running), open Windows Explorer, and navigate to the OnPortal directory. • Delete *NodeConfig.json* file from the *C:\Onity\OnPortal\FrontDeskClient* folder. • Start the program; it will be on an *Install* screen. • Finish station configuration as per the steps under *Install and Configure a Station* in Appendix A, Installing OnPortal.

RETURN TO TABLE OF CONTENTS

Backup Replacement

As when replacing a server, the backup environment key needs to be changed for the system to use the new backup machine.

Step #	Action
1.	Contact an Onity Rep with the *Site Key* for the license and request access to the portal page to replace a backup.
2.	Log into OnPortal with station rights on any machine.
3.	Go to **CONFIGURATIONS > STATIONS.**
4.	Select the existing backup machine. Select **DELETE** to remove the machine from the stations list.
5.	Open the email from Onity containing the link to the portal page and navigate to the portal page. **TIP:** It's a good idea to do this on the new machine.
6.	Download and install the OnPortal program.
7.	Start the program.
8.	Copy and paste the new *Backup Environment Key* to the portal page.
9.	Select **SAVE KEYS**.
10.	Go to the Server machine. • Log into the server with **CONFIGURATION > LICENSE** rights. • Download and load the new license to the server machine. See *License Expiration and Renewal* for steps on downloading and loading the license.
11.	Return to the backup machine.
12.	Finish the configuring the device as a backup as per *Configure a Backup Server* instructions in Task 6 in Appendix A, Installing OnPortal.
13.	No station changes are needed when replacing a backup. The station will be told by the main server of the new backup machine name/location, etc.

Station Replacement

There are no special steps needed to replace a station. It is just like setting up a new station. The only "special" step you might want to take is to delete the old station from the list of stations.

Hardware Setup in OnPortal

All icons for the main subheadings show on the left-hand side of the **CONFIGURATION** section.

Encoders, Setting Up

Install Encoders

Select the ***Encoder*** icon on the left in the **CONFIGURATION** menu. When attaching encoders for the first time, the system must finish installing drivers before scanning for the devices.

On the main encoder screen:

Green checkmark = Encoder is detected by OnPortal and ready to encode cards.
Red X mark = Encoder is not communicating with OnPortal.

If an encoder has a red x on it and is plugged into a computer, you must **SCAN** to find and activate the encoder.

NOTE: *For non-HT22-type encoders, you may connect all of them and perform one scan, then set the default for each station from within the* Stations *section, or you can scan for each encoder as you install it.*

For HT22-type encoders, you must scan for them one at a time.
For IP-type encoders, you may connect all of them and perform one scan, then set the default for each station from within the *Stations* section, or you can scan for each encoder as you install it. For information on installing IP encoders, see Appendix B.

IP Encoders

Step #	Action
1.	Remove DIGI AnywhereUSB 2 Plus hub (“device”) from package.
2.	Connect device to power supply.
3.	Connect device to network using Ethernet cable.
4.	Connect OnPortal Encoder to USB port.
5.	If not already done by Onity tech, configure the DIGI AnywhereUSB 2 Plus hub over IP device. See Installation Guide in Appendix B for details.
6.	Plug the OnPortal encoder into the USB port on the station.
7.	If it is installing drivers, let it finish. (By default, driver files are located in the *C:\Onity\OnPortal\FrontDeskClient\Drivers\ Encoder_Elatec_TWN4_PCSC* folder if needed; Windows 10 drivers are on OnityNET.)
8.	Select **SCAN**.
9.	Upon success, it reads as PC/SC MIFARE Encoder with a green checkmark.

OnPortal RFID Encoders

Step #	Action
1.	Plug the OnPortal encoder into the USB port on the station.
2.	If it is installing drivers, let it finish. (Driver files are located in the *C:\Onity\OnPortal\FrontDeskClient\Drivers\ Encoder_Elatec_TWN4_PCSC* folder if needed; Windows 10 drivers are on OnityNET.)
3.	Select **SCAN**.
4.	Upon success, it reads as *PCSCEncoder* with a green checkmark.

OnPortal Motorized Encoders

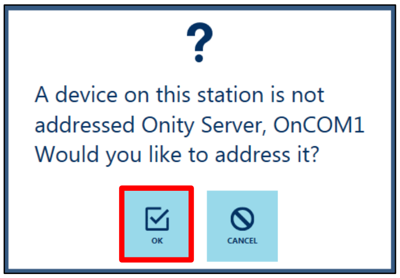
Step #	Action
1.	Plug the OnPortal encoder into the USB port on the station.
2.	If the station installs drivers, let it finish. (Drivers located in *C:\Onity\OnPortal\FrontDeskClient\Drivers\Encoder KDE Motorized* folder if needed.)
3.	Select **SCAN**.
4.	Upon success, it shows as *KDEEncoder* with a green checkmark.

OnPoint Decks

Step #	Action
1.	Plug the OnPoint deck into the USB port on the station.
2.	If it is installing drivers, let it finish. (Driver files are located in the *C:\Onity\OnPortal\FrontDeskClient\Drivers\Encoder_Portable_ADV15* folder if needed.)
3.	Select **SCAN**.
4.	Upon success, it will read as *PortableEncoder* with a green checkmark.

HT22s Connected to a COM Box

All HT22-type encoders must connect through a COM box to the OnPortal system. Hook up the COM box to the computer using the nulled cable, hook up the HT22 using either two-wire or a serial output.

Step #	Action
1.	Prepare the HT22 for addressing. • Press and hold down **EXIT** until it beeps twice to bring up the tech menu. • Scroll to *PROGRAM SELECTION* and press **ENTER**. • Scroll to *REGULAR ENCODER*, press **ENTER**. • Scroll to *HTCOM Settings*. • Press and hold down **CLR** until the HT22 beeps and reads *ADDRESS: CLEARED*. • Press **EXIT** twice to exit the tech menu.
2.	Turn off any other encoders connected to this encoder, or unplug the cable connecting them.
3.	Select **SCAN** to make OnPortal look for encoders. If it finds an unaddressed HT22, a similar screen appears:  A device on this station is not addressed Onity Server, OnCOM1 Would you like to address it?
4.	Select **OK** to address the encoder.
5.	Upon success, the encoder shows as *HT22x* (I, M, P, or R) with a green checkmark indicating it is online.
6.	To add additional HT22s, perform steps 1-5 for each encoder, one at a time.

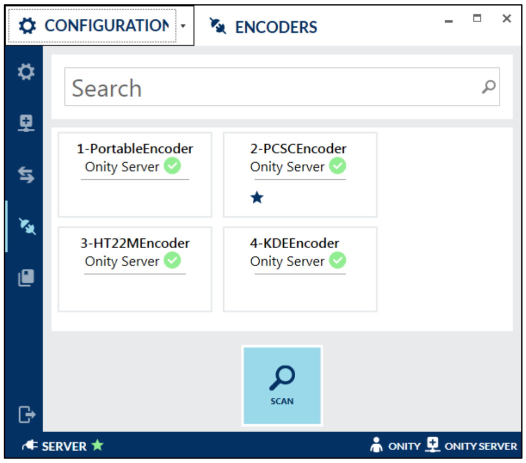
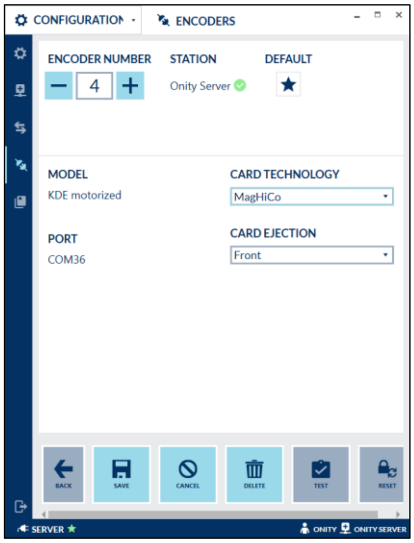


Figure 51 Encoders Screen



ENCODER NUMBER: 4
STATION: Onity Server
DEFAULT: ★
MODEL: KDE motorized
CARD TECHNOLOGY: MagHiCo
PORT: COM36
CARD EJECTION: Front

Figure 52 Encoder Details Screen

Configure Encoders

After installing the encoders to OnPortal, there are a number of configuration tasks to complete.

Step #	Action
1.	Select an encoder to configure.
2.	Use the *Friendly Name* field to identify each encoder easily.
3.	Verify that the **CARD TECHNOLOGY** shown is correct for the encoder and card types in use.
4.	The **ENCODER NUMBER** is very important when interfacing with PMS. This is the number a PMS system sends OnPortal when it wants to use this particular encoder. In general, it can be left on default settings, but if the PMS system needs encoders numbered a certain way, it is OK to change it.
5.	For *Portable Encoders,* verify that the **ANTENNA POSITION** is correct. (**Front** if in a stand, **Top** if on a desk.)
6.	For *KDE Motorized* and *HT22M Encoder*, verify that the **CARD EJECTION** is front (unless otherwise desired).
7.	At the top of the screen, the station denotes the actual client station that the encoder is physically connected to. Note that this encoder may be used as the default encoder for any of the client stations of the system.
8.	The star ★ below DEFAULT at the top of the screen turns blue if this encoder is a default for some station. To make it into the default encoder for the station listed, select the star. ***NOTE:*** *This can also be accomplished from within the* Stations *section. This is a nice way of setting the default encoders for each station without having to be logged into the particular station.*

Stations

Any station installed and configured will show up in this menu. All stations MUST get a default encoder assigned in order to encode keys. Select the *Stations* icon on the left side of the screen to go to the *Stations* screen.

On the main *Stations* screen:

SVC

- *Green checkmark* indicates the OnPortal Node Service is running on the machine.
- *Red X* indicates the OnPortal Node service stopped and that machine cannot encode cards.

UI

- *Green checkmark* indicates the User Interface (OnPortal Program) is open on that station.
- *Red X* indicates the OnPortal Program is not running on that machine.

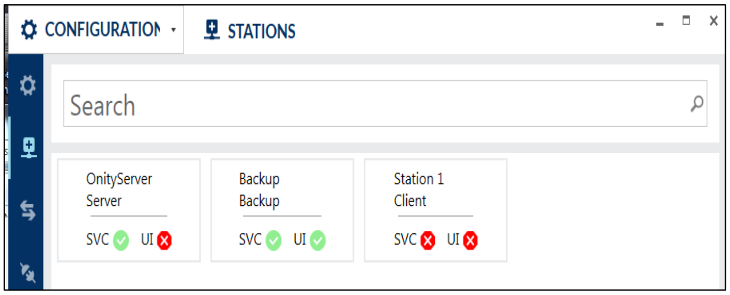


Figure 53 Stations Screen

The following options exist after selecting a station.

Configuring Default Encoders

Step #	Action
1.	Select a **DEFAULT ENCODER** for this station.
2.	Select **SAVE.**

Troubleshooting

Error Message	What's Wrong	How to Correct
Encoder name already exists!	Duplicate encoder name already in the database.	Give the encoder a unique name for proper identification.
Encoder not connected	• DIGI AnywhereUSB 2 Plus hub power cable was unplugged. • Network cable was unplugged. • Card reader USB cable was unplugged. • Check DIGI device software to see if USB encoder is connected. • Network configuration is blocking communication. Contact site IT Department to resolve.	Make sure all three plugs are properly connected; wait to hear a beep sound after reconnecting the cables; try encoding a card again. Go to DIGI device to see if USB encoder is connected. If not, right-click the USB encoder and check “connect device automatically” and then click “**connect device**.”

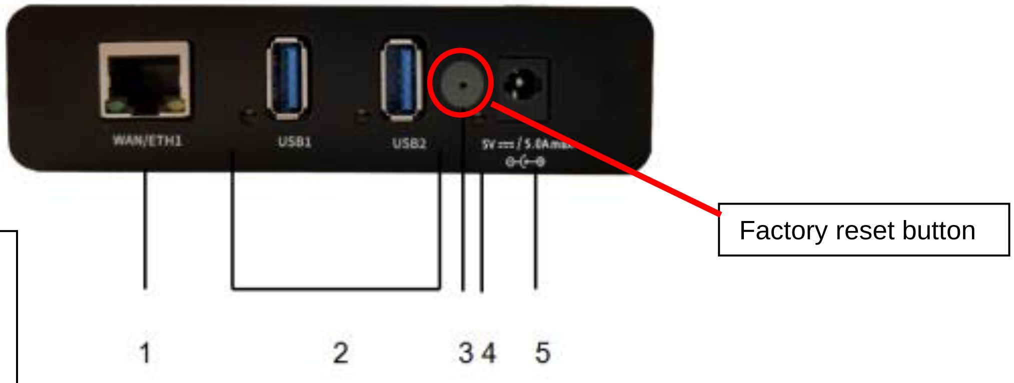
RETURN TO TABLE OF CONTENTS

Other Troubleshooting Tips

If the USB server doesn’t respond when changing from *Static IP* to *DHCP* or from *DHCP* to *Static IP*, restart the USB server.

If there is a power outage or an issue with network and/or USB encoder connectivity, enable the option “Connect Device Automatically” in the USB server application.

If you are unable to assign any other IP when configuring to a static IP, use a small pin or paperclip to push the factory reset button on the DIGI AnywhereUSB 2 Plus hub.



Key

1. Ethernet Connector
2. USB LEDs and Ports
3. Reset Button
4. Power LED
5. Power Connector

Figure 54 DIGI AnywhereUSB 2 Plus Hub

Delete a Station

Always delete the Backup server in *Stations* prior to installing a new machine as the OnPortal Backup Server. If replacing a computer, it is wise to delete the station associated with that computer.

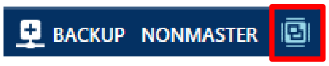
Step #	Action
1.	Select **DELETE**.
2.	Select **OK** on the confirmation screen.

TakeOver Options

An OnPortal license contains the hardware key for both a server and a backup server to ensure the system’s capability to continue operation in the case of a hardware or network failure. There are three scenarios to be considered:

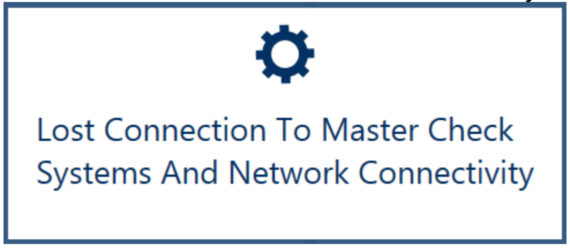
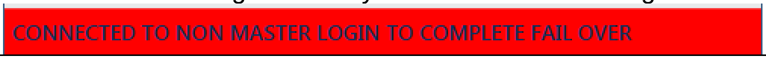
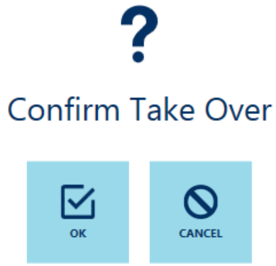
1. Network failure where the backup server is at or near the front desk and needs to be used to encode keys during the downtime.
2. Server maintenance where the main server will be offline for a period of time.
3. Compete server hardware failure – hardware must be replaced.

In scenarios 1 and 3, you will get a “lost connectivity to server” message on all workstations informing you that the server is down. On the backup server, you will have a “Takeover” icon at the bottom next to the PC name that will allow you to take over server responsibilities.



Notice in this case you see BACKUP and NONMASTER, indicating that this machine has not assumed the server role. Click the icon on the right to take over the server role. You will be asked to confirm and enter a password that has authority to take over. ***NOTE:*** *If using Windows Authentication, you will need to contact Onity to get a tech password to perform the takeover. Follow the steps below in the case of an unexpected server failure:*

RETURN TO TABLE OF CONTENTS

Step #	Action
1.	When an OnPortal client has lost connectivity to the server, the following lost connection message is shown.  Lost Connection To Master Check Systems And Network Connectivity Before implementing a “takeover” from the backup server, verify that the problem cannot be easily solved and you really do need to have the Backup Server take over.
2.	Click the ⧉ icon at the bottom right hand of the screen on the Backup Server.
3.	Enter a user name and password with the proper authority to take over the server role. If you do not have one, or are using Windows Authentication, contact Onity. You may need to use an Onity Tech password. At the bottom of the login screen you will see the following:  CONNECTED TO NON MASTER LOGIN TO COMPLETE FAIL OVER
4.	You will be asked to confirm the takeover – click OK  Confirm Take Over
5.	The services will restart and you will be taken to the login screen. If you are using Windows Authentication, exit OnPortal and restart to login.
6.	The Backup Server has now taken over the role of the Main Server. ***NOTE****: You may lose up to 15 minutes of data when the server fails.*

When the server hardware is fixed, or the network issue is corrected, you can “take over” the server role again from the server station. When you first bring the server up, it will start up as the backup server. To take over the server role, navigate to Configuration \ Stations and select the *Takeover* icon. Follow the same steps above to return the server role to the server machine.

A planned takeover of the server role by the backup server can be performed by clicking the *Takeover* icon in in the *Stations* section and following the steps above. This method allows you to plan the timing of the main server maintenance.

If the server machine fails and hardware must be replaced, there are two options:

1. When the new server machine is installed and started, you may let it run as the backup server.
2. To run the new hardware as the server, all stations will need to be reinstalled.

In either case, a new license file is required as the hardware environment key has changed.

RETURN TO TABLE OF CONTENTS

Performing a Server Replacement

Step #	Action999
1.	Take over on the backup server using either the Non-Master login methodology or by going to **Configuration > Stations**, selecting the Backup server, and selecting the “Takeover” option.
2.	Shut down the OnPortal Node service on the existing server if it is still online.
3.	Install OnPortal on the new server.
4.	Upload the new environment key to OnityNet and download a new license. (**TIP:** Verify that the backup machine environment key matches the existing backup key in the license BEFORE downloading it!)
5.	On the backup machine, make a copy of the Onity.FrontDesk.sdf file from the C:\Onity\OnPorta\FrontDeskClient directory for transfer to the new main server. (Shut off the OnPortal Node Service on the backup machine to prevent changes to the locking plan if that is a concern.)
6.	Finish configuring the new server using the new license and the locking plan retrieved from the backup machine. **Note the new server address and port for use in setting up backup and stations later.**
7.	ALL OTHER CLIENTS INCLUDING THE BACKUP SERVER MUST BE REINSTALLED. The fastest way to do this is to go to the C:\Onity\OnPorta\FrontDeskClient folder and delete the following files. (on the standard clients, only the NodeConfig.json file will exist) • LicenseData.bpex • NodeConfig.json • Onity,FrontDesk.sdf
8.	Run the client and follow the process for completing the installation on each machine
9.	Encoders must be reconfigured at this time.

Restart a Station

Restarts the OnPortal node service on the selected machine.

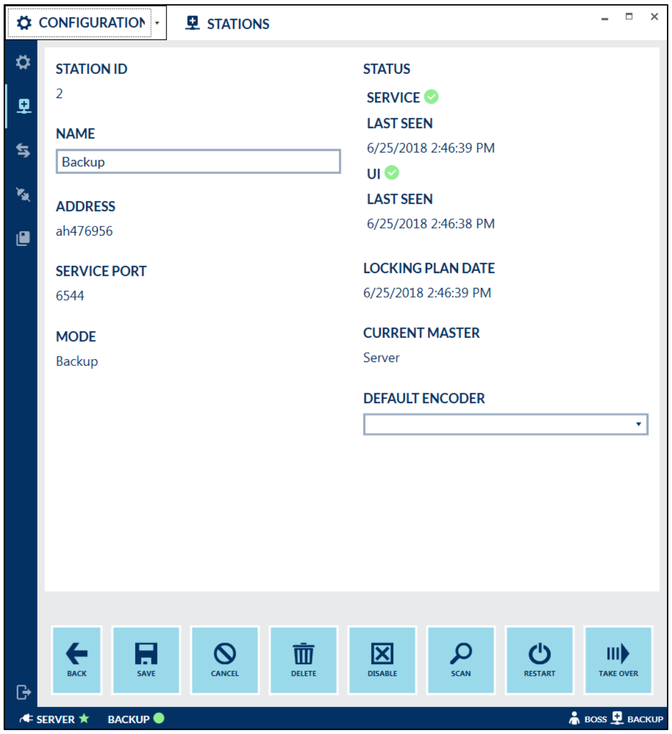
Step #	Action
1.	Select **RESTART**.
2.	Select **OK** on the confirmation screen.

Scan Button

Step #	Action
1.	Select **SCAN**; the system looks for devices (encoders and online readers).
2.	System refreshes list of encoders and readers.

Disable and Enable a Station

Step #	Action
1.	Select **DISABLE** (**ENABLE** if station currently is disabled).
2.	Select **OK** on the confirmation screen.



STATION ID
2

NAME
Backup

ADDRESS
ah476956

SERVICE PORT
6544

MODE
Backup

STATUS

SERVICE ✓

LAST SEEN
6/25/2018 2:46:39 PM

UI ✓

LAST SEEN
6/25/2018 2:46:38 PM

LOCKING PLAN DATE
6/25/2018 2:46:39 PM

CURRENT MASTER
Server

DEFAULT ENCODER

Figure 55 Station Details Screen

RETURN TO TABLE OF CONTENTS

PMS Listeners

PMS listeners allow a Property Management System (PMS) to send guest card encoding commands to OnPortal. Select the PMS listener icon from the left side to display the listeners. Listeners show:

- The station connected with.
- The type of connection in use.
- ▶ indicates a started listener.
- ❚❚ indicates a stopped listener.

A PMS listener may be set up on any of the OnPortal Clients and multiple listeners are available within the system. For example, a property may have a connection to the property management system as well as connections to one or more kiosk systems that send the encoding commands separate from the PMS.

PMS listeners may be configured for serial (RS232) connections or TCP/IP connections.

Setting Up PMS Listeners

The PMS interface in OnPortal may attach to any station, provided that station has a reliable network connection to the server machine. Select the *PMS Listeners* icon on the left side of the configuration screen.

Step #	Action
1.	Select + to create a new listener.
2.	Select an existing listener to edit or start.

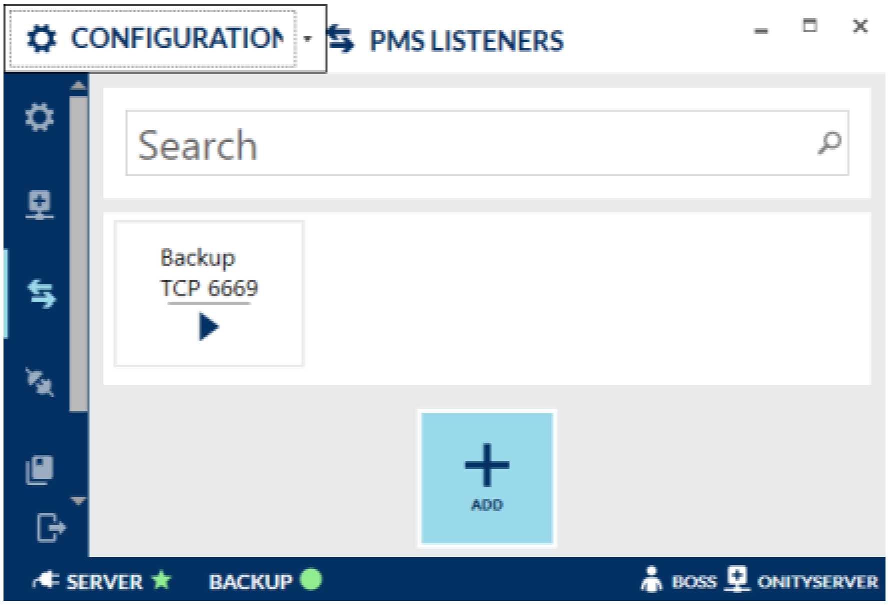


Figure 56 PMS Listeners Screen

PMS REST Listener

Step #	Action
1.	After selecting the **Add** button, verify/change the **TYPE** is/to **REST**.
2.	Enter the *PORT* number given by the PMS for the interface. If unknown, leave at 9090 (Onity default port).
3.	Enter the **API USER** provided by the PMS provider.

RETURN TO TABLE OF CONTENTS

4.	Enter the **API PASSWORD** provided by the PMS provider.
5.	Enter the password again in **CONFIRM PASSWORD.**
6.	Select **SAVE**. **CAUTION:** Once saved, select the listener again, then select *START* to start the listener. Failure to start the listener means it will not listen for PMS commands.

NOTE: The PMS company will need to know the port as well as the computer name or IP address in order to properly route the commands.

PMS on Serial

Step #	Action
1.	After selecting the **Add** button, verify/change the **TYPE** is/to **Serial**.
2.	Enter the *COM PORT* number the serial cable connects to.
3.	Select the **BAUD RATE** provided by the PMS provider. If unsure, set at **9600**.
4.	Select the number of **STOP BITS** the PMS provider uses. If unsure, leave at the default setting of 2.
5.	Verify or set the **PARITY** to **None** unless the PMS provider indicates otherwise.
6.	The **ENFORCE CHECKSUM** option requires the PMS command to send calculate the checksum as part of the command. This is primarily used in serial connections to ensure no part of the message was lost. While not necessary to enforce this checksum with the TCP/IP connection, Onity recommends you always check this box unless specifically instructed not to do so by either Onity or the PMS company.
7.	Select **SAVE**. **CAUTION:** Once saved, select the listener again, then select *START* to start the listener. Failure to start the listener means it will not listen for PMS commands.

PMS on TCP/IP

Step #	Action
1.	After selecting the **Add** button, verify/change the **TYPE** is/to **TCP**.
2.	Enter the *PORT* number given by the PMS for the interface. If unknown, leave at 6669 (Onity default port).
3.	Leave the checkmark on **ENFORCE CHECKSUM**.
4.	Select **SAVE**. **CAUTION:** Once saved, select the listener again, then select *START* to start the listener. Failure to start the listener means it will not listen for PMS commands.

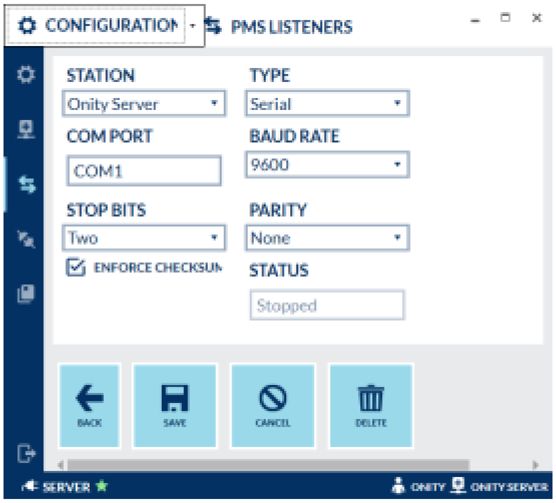
NOTE: The PMS company will need to know the port as well as the computer name or IP address in order to properly route the commands.

Editing PMS Listener

Step #	Action
1.	Select the PMS Listener to edit.
2.	Select **STOP** at the bottom; a running listener cannot be edited.
3.	Perform edits as needed.
4.	**SAVE** changes.

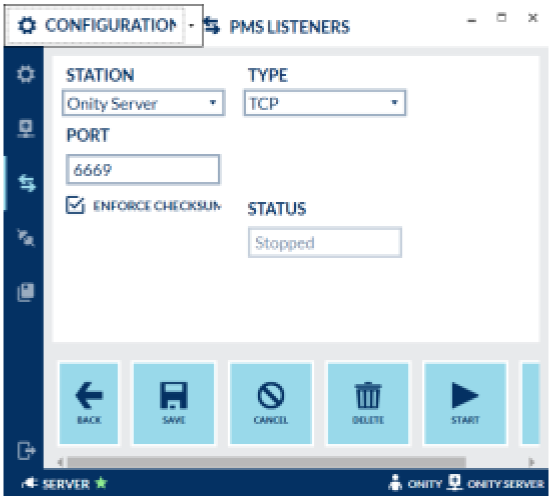
RETURN TO TABLE OF CONTENTS

CAUTION: Once saved, select listener again then select *START* to start listener. Failure to start listener means it will not listen for PMS commands.



STATION: Onity Server
TYPE: Serial
COM PORT: COM1
BAUD RATE: 9600
STOP BITS: Two
PARITY: None
☑ ENFORCE CHECKSUM
STATUS: Stopped

Figure 52 PMS Listener, Serial Configuration Screen



STATION: Onity Server
TYPE: TCP
PORT: 6669
☑ ENFORCE CHECKSUM
STATUS: Stopped

Figure 53 PMS Listener, TCP/IP Configuration Screen

Renew PMS Certificate

A REST PMS Listener has a server certificate that is valid for 365 days. The certificate will be automatically renewed after 180 days. Click **Renew Certificate** to renew the certificate immediately.

***NOTE**: A certificate renewal will trigger an automatic restart of the REST PMS Listener.*

REST API Logging

In PMS Configuration, select **LOG MESSAGES** for REST API to enable this feature.

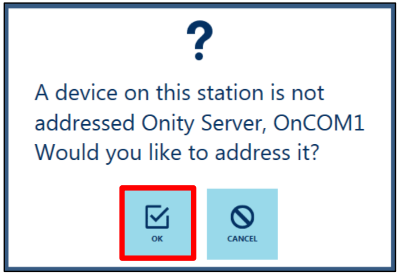
RETURN TO TABLE OF CONTENTS

Online Wall Readers

OnPortal connects to online readers through an HT communication (HTCOM) distributor connected to an OnPortal station. Online readers support up to 8,000 users with audits and have the capability to manage entry and exit readers. Online readers must be addressed in a manner similar to encoders; however, more options are available for online readers such as number of readers, anti-passback functionality, and locking plan. You can also set the opening delay of each reader connected to the system.

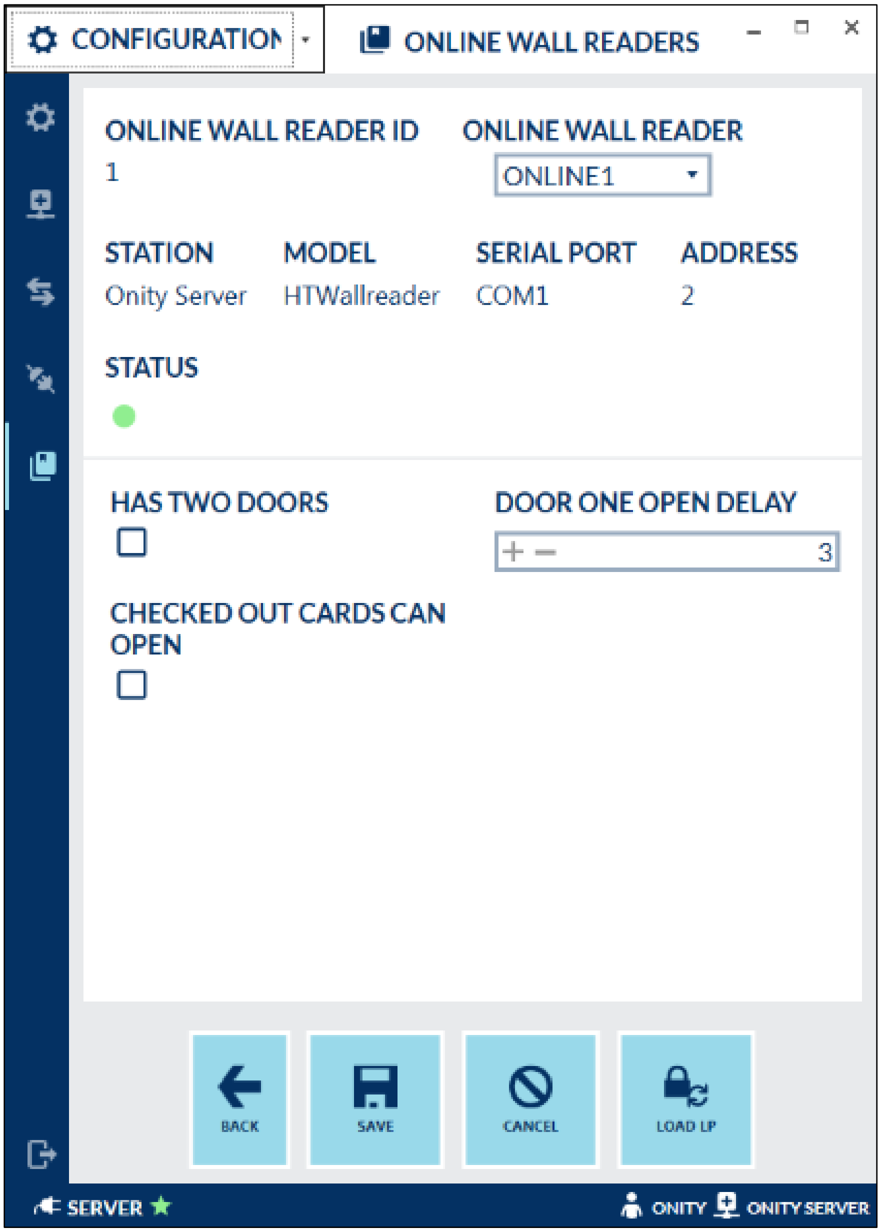
Anti-Passback is a feature that restricts a keycard from accessing the entry door a second time before it is used in the exit door. This is most often used for parking gate readers to ensure that only the cardholder can access the garage. ***NOTE:*** *The requirement for the exit reader can be configured to expire after a certain time.*

Detecting and Addressing

Step #	Action
1.	If the door has the same site code, select **SCAN** and see if it finds the door.
1a.	If it does not, go to the Online Door and press and hold the *CLR* button on the CE-22 board for 5 seconds. Select **SCAN** again.
2.	If found, the system will prompt to address it. Select **OK** to address and open the door details.  A device on this station is not addressed Onity Server, OnCOM1 Would you like to address it?
3.	A configuration screen shows up; configure the online door.

Configuring and Editing

Step #	Action
1.	Select the correct door from the locking plan in the **ONLINE WALL READER** drop-down box. ***NOTE:*** *The online readers must be set up in the locking plan prior to performing this step. This is where the locking plan for the reader is configured.*
2.	Check the box for **HAS TWO DOORS** if two readers are connected to the CE-22 board.
3.	The **CHECKED OUT CARDS CAN OPEN** setting allows a guest card that has been checked out to continue to work in the reader until expiration. This allows a guest to check out of the room and still be able to exit the parking garage (for example) when the exit is controlled by a reader.
4.	Choose a **DOOR** n **OPEN DELAY** for each door ("n" represents 1 or 2). **CAUTION:** If controlling a parking gate, the door opening delay MUST be set to 1 second; otherwise you run the risk of leaving the gate open after the car has passed through.
5.	Select **SAVE**.
6.	Select **LOAD LP** (LP = Locking Plan) to enable cards for that door.
7.	The status indicator should turn green after the locking plan is loaded.



ONLINE WALL READER ID
1

ONLINE WALL READER
ONLINE1

STATION	MODEL	SERIAL PORT	ADDRESS
Onity Server	HTWallreader	COM1	2

STATUS
●

HAS TWO DOORS
□

DOOR ONE OPEN DELAY
+ − 3

CHECKED OUT CARDS CAN OPEN
□

Figure 57 Online Wall Reader Details

RETURN TO TABLE OF CONTENTS

Managing Staff in OnPortal

OnPortal identifies people who log into the software as *Operators* and identifies staff keycards *Master Users*.

Roles

Roles are templates that enforce the permissions for Operators. Roles are in the **SECURITY** menu; select the icon from the left side of the screen.

Default Roles

When a creating a new locking plan, OnPortal creates three default roles. These roles may be modified to fit the needs of your property and additional roles may be configured as needed. Each role is given a name, a sign-in method (such as PIN, User Name and Password, etc.), the permissions that an operator of this role can perform, and a role level. These are discussed in detail below.

To edit a role, select it by clicking on the role name. To add additional roles, click the + ADD icon at the bottom of the screen.

Role	Details
GM	Has permissions for everything in OnPortal except building a locking plan. User Name and Password login type. Role Level of 8. Session Timeout of 3 minutes.
Maintenance	Permissions for **RECEPTION**, **MAINTENANCE**, **SPECIAL CARDS**, and **CONFIGURATION** and all options within those items. User Name and Password login type. Role level of 3. Session Timeout of 3 minutes.
Reception	Permission only for **RECEPTION** tasks. PIN only login type. Role Level of 1. Session Timeout of 3 minutes.

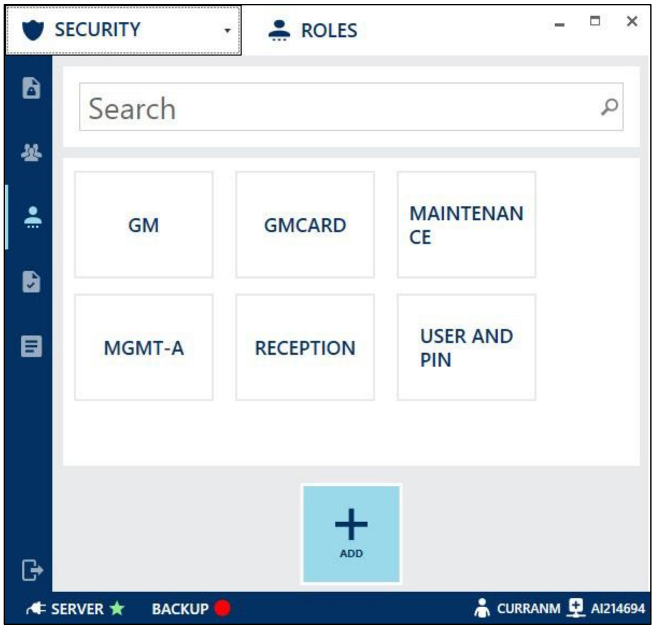


Figure 58 Roles Screen

RETURN TO TABLE OF CONTENTS

Permissions

Permissions determine what menu options a user can see, what cards they can encode, etc. Select permissions by entire categories or by individual functions within the category.

Receptions Permissions	Maintenance Permissions	Special Cards Permissions
• Encode Single-Open Card • Erase Card • Groups • Guest Check-In • Guest Copy Card • Guest Check-Out • Hotel Information • Manage DirectKey mobile keys • Read Card • Use PMS	• Load Portable Programmer • Open Lock • Initialize • Update Lock • Test Card • Test Lock • Read Audits • Allow Programming All Locks • Room Out of Service • Room Change Profile	• Blocking Card • Cancelling Card • Diagnose Card • Encode Safe Emergency Card • Programming Cards • Spare Cards
Master Users Permission	**Security Permissions**	**Configuration Permissions**
• Manage Master Users • Master Cancel Card • Master User Batch Edit **Locking Plan Permissions** • Manage Locking Plan	• Manage Operators • Manager Roles • Activity Log • Reports	• Property Configuration • Station Configuration • Configuration Fail Over • PMS Configuration • Encoder Configuration • Online Wall Reader Configuration

Most permissions are self-explanatory but some need explanation:

- **Allow Programming All Locks** – This is a function of the portable programmer. With the OnPortal system, an operator that has portable programmer permissions may be restricted to only communicating with certain locks. If this box is not checked, you may select which rooms the operator has access to. Additional details are below in the “key codes” subsection.
- **Configuration Fail Over** – User has the rights to “fail over” the system to make the backup server into the main server and vice versa.
- **Manage Locking Plan** – Allows the operator to modify the locking plan of a site. Sites typically do not receive this permission unless they have been Level 9-certified by Onity.

Levels

Role levels determine what roles and permissions someone with the rights to create operators may use. The rules that levels follow are:

Rule	Restriction
1.	Operators may only create or assign a role to operators at their level or below.
2.	Operators may not assign any permission to a new role that they do not have.
3.	Operators will not see roles above their level.
4.	Operators will not see other operators above their level. ***NOTE:*** *OnPortal will warn that it cannot add a user name that already exists; be aware that users may exist that the current operator does not have the rights to see.*

Adding or Editing Roles

Step #	Action
1.	Select + ADD to create a new role or select a role to edit.
2.	Enter a *NAME* that describes the function of this role.
3.	Select *PERMISSIONS* for this role.
4.	Select the **OPERATOR SIGN IN** for this role. Operator sign-in options: • PIN Only (*NOTE*: *With this option, a PIN may only be assigned by the system. This is a security feature to ensure that no one tries to set their PIN to one used by another user.)* • Card and PIN – requires the operator to use a keycard and a PIN. To sign in, enter the PIN and place the key on the encoder (RFID) or insert into the encoder (Mag). This option allows a user to change their PIN. If the operator is also a Master User, the operator and Master User accounts must be linked from within the Master User to allow access to the system and locks via a single card. • User Name and Password – requires a user to enter their user name and password to access the system • User Name and Password PCI – requires the use of a PCI compliant password.
5.	Assign an appropriate **ROLE LEVEL**.
6.	Set the **SESSION TIMEOUT** for this role. **CAUTION:** Remember, this is a security feature so even though it is convenient to stay logged in a long time, it is a security issue if someone walks away and remains logged in
7.	Select **SAVE**.

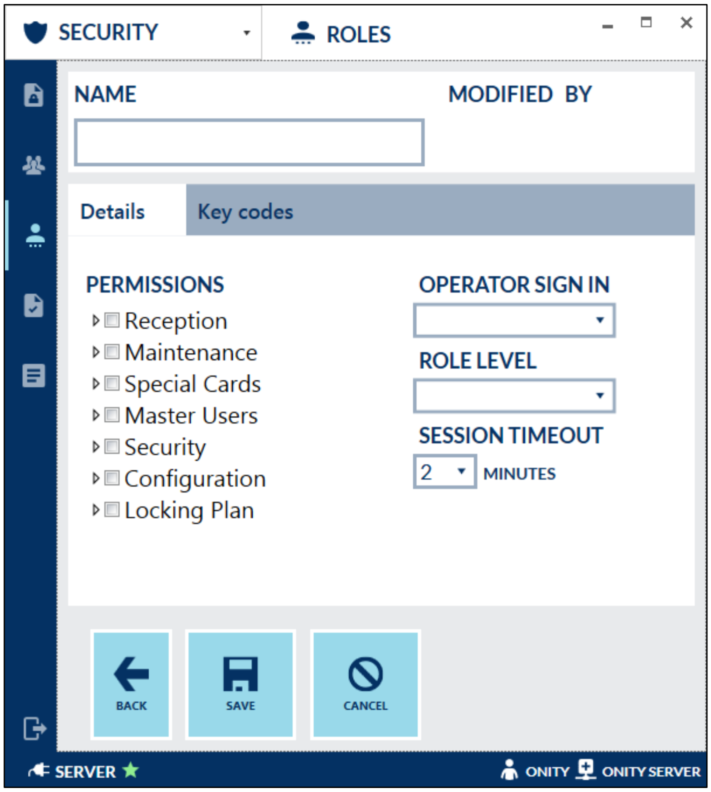


Figure 59 Role Details Screen

Editing Role Key Codes

If a site wishes to prevent someone from encoding a card for a certain type of master user or room, it can remove those key codes from the role. This is also where you remove the ability of an operator to use the portable programmer on certain doors.

Step #	Action
1.	Select the *KEY CODES* tab.
2.	Select any *Master Type* or *Room* to turn it white, indicating that this role will not have permission to create a card for that master/room.
3.	Select **SAVE**. **CAUTION:** If one removes a room/master from their own role, they cannot add it back in. Someone at a higher level with rights to that room/master would have to add it back in.

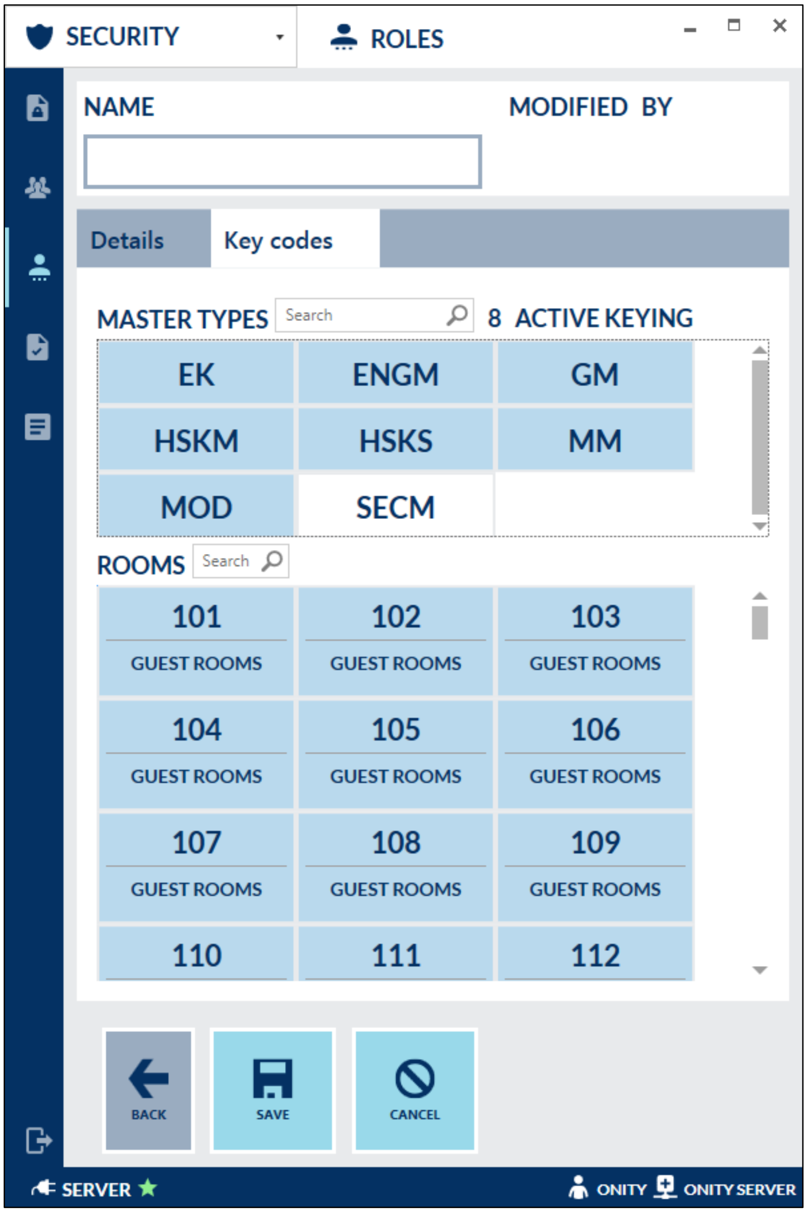


Figure 60 Role Key Codes Screen

RETURN TO TABLE OF CONTENTS

Operators

An *operator* is any user who will log in to the system to either manage or issue cards. To access Operators, go to the ***SECURITY*** menu and select the ***Operators*** icon. After saving an operator, the system allows the *Name* field to be changed but not the *User Name.*

Adding a New Operator

NOTE: *As the system generates a complex default password, it is best to add operators when they are present so they can immediately log out and change their password.*

Step #	Action
1.	Select + ADD to create a new operator.
2.	Enter a *NAME* to identify this user in audits.
3.	Enter the *USERNAME* to use for logging into OnPortal (if expecting to use Windows Authentication, this must be the computer login name for the user).
4.	Select the appropriate **ROLE** and **LANGUAGE**. (*Login Type* fills in based upon the role.)
5.	Select **SAVE**.
6.	OnPortal generates a PIN or Password, depending on the login type. **CAUTION:** Select ⧉ to copy the password to the clipboard, or write down the code.
7.	If the login type is Card plus PIN, select the **ENCODE** button to make the card.
8.	If the operator is present, select the log out icon ⇥ in the lower left. Select **OK** to confirm.
9.	Have the operator log in with their credential and change their password or PIN if applicable

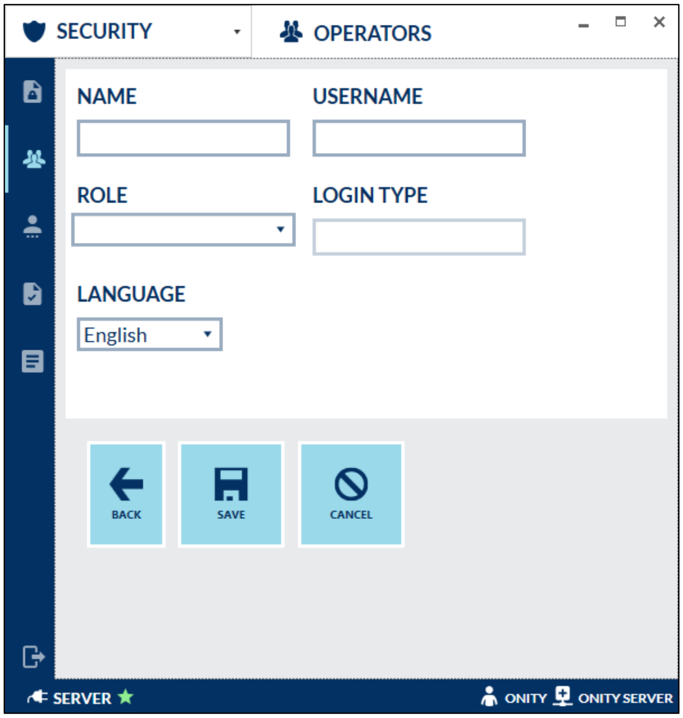


Figure 61 Operator Details Screen

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99
© 2022 Carrier. Revision 4. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Changing Passwords at Log In

Step #	Action
1.	Select the appropriate log-in type at the top of the screen.
2.	Check the box for **CHANGE PASSWORD** or **CHANGE PIN.**
3.	Enter the changed details: • User login: Enter the *USERNAME, PASSWORD, NEW PASSWORD,* and *CONFIRM PASSWORD.* • PIN login: Enter the *PIN, NEW PIN*, and *CONFIRM PIN.*
4.	Select **CHANGE PASSWORD** or **CHANGE PIN** to complete the login.

Delete an Operator

NOTE: *Operators may not delete themselves.*

Step #	Action
1.	Select operator to delete.
2.	Select **DELETE.**
3.	Select **OK.**

Reset the Password of Another Operator

Step #	Action
1.	Select operator.
2.	Select **RESET PASSWORD**.
3.	Copy the password or write it down.
4.	Log out of the system and have the other operator log in and change their password (other than PIN only).

Logging Out of OnPortal

An operator may log out of OnPortal from any of the main screens within the program.

Step #	Action
1.	Select the ***Log Out*** icon ⇨ on the bottom left of any main screen to log out.
2.	Select **OK** to complete the sign out.
3.	Select **OK.**

Appendix A
Installing OnPortal

This document contains technical data subject to the EAR. U.S. Export Control Classification Number: ECCN = EAR99
© 2019 Onity Inc. Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Installing OnPortal

Server Location Recommendations

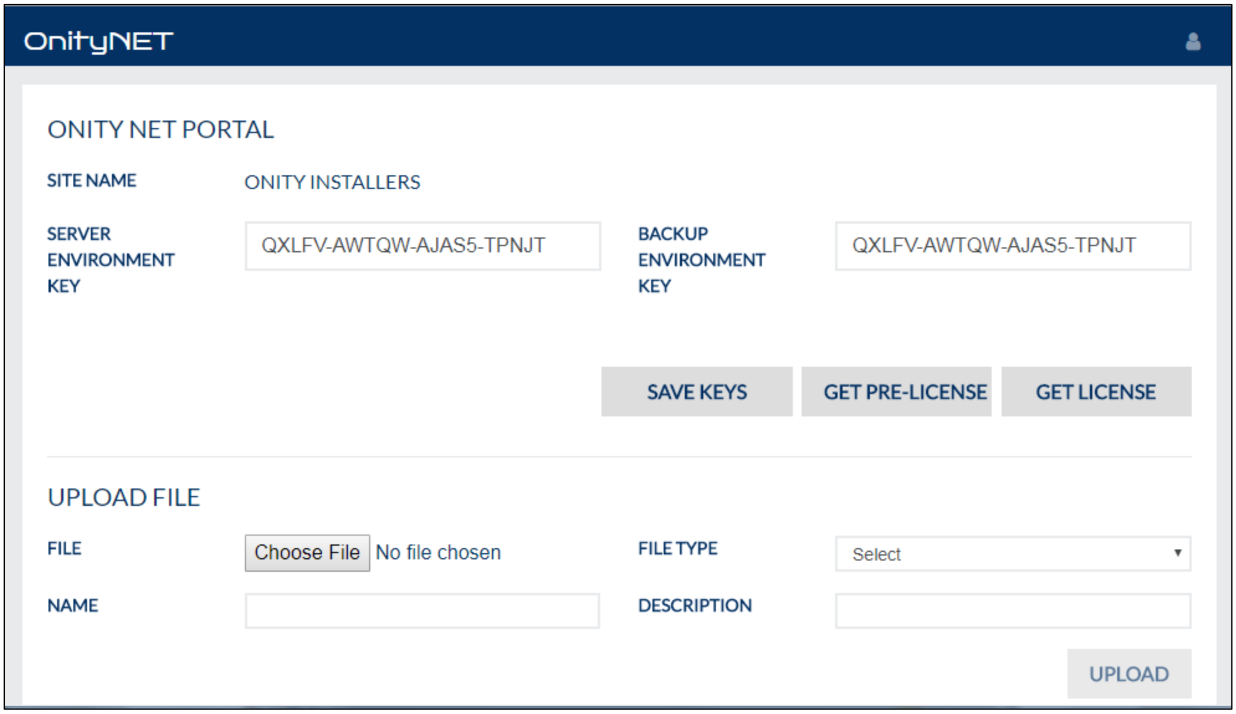
- Main Server: Onity recommends that the server be located in the front desk area so if the site experiences a network problem after installation, staff can still make keys at the main server.
- Backup Server: Locate this at a secure location such as the server room or PMS server room.

Task 1: Go to the *OnityNET* Portal Page

NOTE: You will receive an email from an Onity Rep with a link to the OnityNet Portal Page.

Go to OnityNET (www.onity.net) from the backup machine first when installing it on site. The *Backup Environment Key* needs to be saved prior to downloading the license to the primary server.

Step #	Action
1.1	Using the link provided by the Onity rep in the installer email, go to the OnityNET portal page.
1.2	Links are of the format: http://onity.net/portal/3/ojqqy-oadge-x6waz.
1.3	The characters after the last forward slash "/" are the password for any downloaded certificates from that page (in the example above, *ojqqy-oadge-x6waz*.)



ONITY NET PORTAL

SITE NAME: ONITY INSTALLERS

SERVER ENVIRONMENT KEY: QXLFV-AWTQW-AJAS5-TPNJT

BACKUP ENVIRONMENT KEY: QXLFV-AWTQW-AJAS5-TPNJT

UPLOAD FILE

FILE: Choose File No file chosen

FILE TYPE: Select

NAME:

DESCRIPTION:

Figure 62 The OnityNET Portal page

© 2019 Onity Inc.
Onity Confidential and Proprietary Information

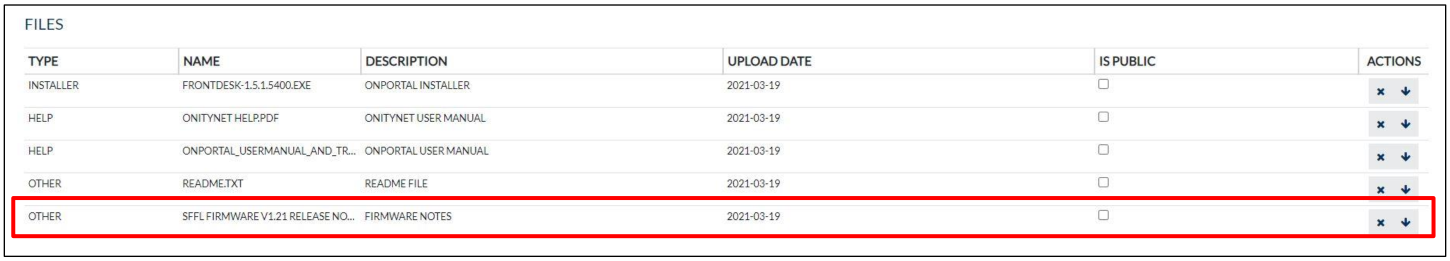
Task 2: Download the OnPortal Installer

NOTE: It is helpful to put the installer file on a thumb drive rather than download from the portal page each time to each machine.

Step #	Action
2.1	In the list of files on the portal page, locate files that are of type *Installer*.
2.2	Locate the *OnPortal –x.x.xx.xxxx* file (where the x's represent the version number), and select the **download arrow** to start the download.
2.3	Save the file on the machine, and if using a thumb drive for other machines transfer the file to the thumb drive.

NOTE: There are more files than the OnPortal installer available on OnityNET; of special importance are:

- SETUPBDE5.EXE – This is the Borland Database Engine installer to use if importing an HT28 locking plan on a machine without HT28 installed.
- ONPORTAL USER MANUAL – This is included in the program as the help file; however, if a site wants a separate copy it is available here.
- ONPORTAL_LEGACY…. – These are the notes created by the programming team explaining what is and what isn't in an import on an HT22 or HT28 system.
- ONITYNET_HELP.PDF – Installation guide for OnPortal.



FILES

TYPE	NAME	DESCRIPTION	UPLOAD DATE	IS PUBLIC	ACTIONS
INSTALLER	FRONTDESK-1.5.1.5400.EXE	ONPORTAL INSTALLER	2021-03-19	□	× ↓
HELP	ONITYNET HELP.PDF	ONITYNET USER MANUAL	2021-03-19	□	× ↓
HELP	ONPORTAL_USERMANUAL_AND_TR...	ONPORTAL USER MANUAL	2021-03-19	□	× ↓
OTHER	README.TXT	README FILE	2021-03-19	□	× ↓
OTHER	SFFL FIRMWARE V1.21 RELEASE NO...	FIRMWARE NOTES	2021-03-19	□	× ↓

Figure 63 Portal Page, OnPortal File Download

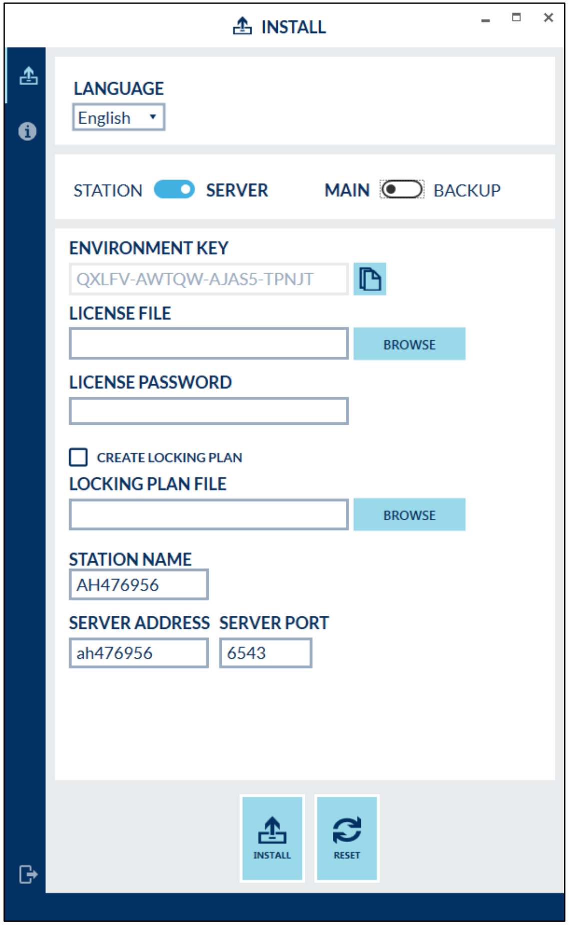
© 2019 Onity Inc.
Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Task 3: Install the OnPortal Program on the Backup Machine and the Server Machine

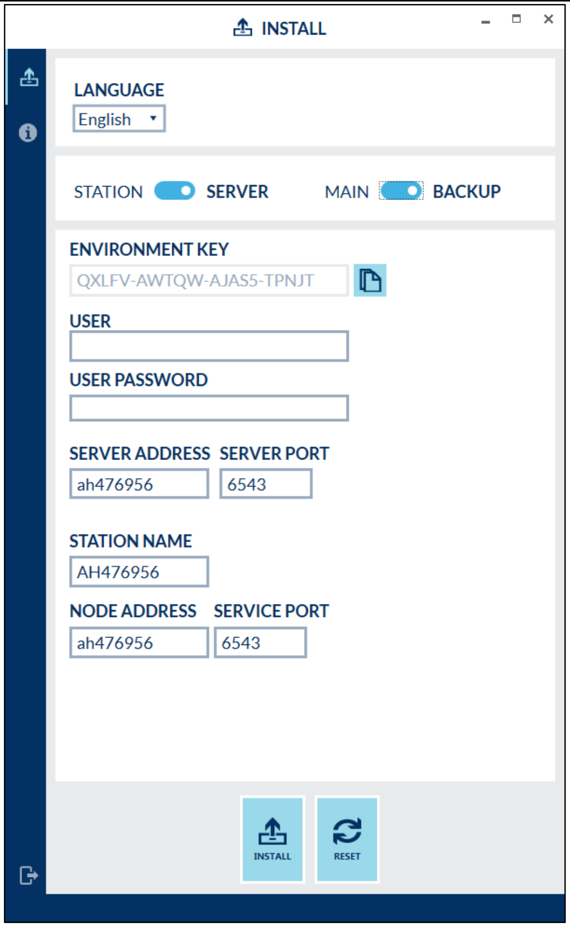
NOTE: Install on the backup machine first; copy the environment key to OnityNET, save it, and then install the main server. Installing in this order means you will not have to switch computers before the next step.

Step #	Action
3.1	Locate the installation file and click *Run as Administrator* to start the program.
3.2	Agree with the license agreement; agree with the prompts to install the program and drivers.
3.3	Once finished, run the OnPortal program.
3.4	It loads to a **STATION** screen; move the slider to **SERVER**.
3.5	If on the backup machine, move the slider from **MAIN** to **BACKUP**.
3.6	Click on the **copy symbol** next to *Environment Key*.
3.7	Return to the portal page on OnityNET.
3.8	Paste the *Backup Environment Key* in the appropriate box.
3.9	Select **SAVE KEYS**.
3.10	Now go to the main server machine, repeat steps 3.1 - 3.9 on the server machine, except set it up as the Main server, and paste into the *Server Environment Key* box.
3.11	Select **SAVE KEYS** after filling in the server environment key.



LANGUAGE: English
STATION / SERVER — MAIN / BACKUP
ENVIRONMENT KEY: QXLFV-AWTQW-AJAS5-TPNJT
LICENSE FILE:
LICENSE PASSWORD:
□ CREATE LOCKING PLAN
LOCKING PLAN FILE:
STATION NAME: AH476956
SERVER ADDRESS: ah476956 SERVER PORT: 6543

Figure 64 Main Server Install



LANGUAGE: English
STATION / SERVER — MAIN / BACKUP
ENVIRONMENT KEY: QXLFV-AWTQW-AJAS5-TPNJT
USER:
USER PASSWORD:
SERVER ADDRESS: ah476956 SERVER PORT: 6543
STATION NAME: AH476956
NODE ADDRESS: ah476956 SERVICE PORT: 6543

Figure 65 Backup Server Install

© 2019 Onity Inc.
Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Task 4: Configure the OnPortal Main Server

NOTE: Always start with the main server machine; you cannot finish the setup on the backup machine until the main server has been set up AND the Windows Firewall Rules have been implemented.

Step #	Action
4.1	After saving both environment keys, download the license file by selecting **GET LICENSE**; save it to a location where you can find it after download.
4.2	On the OnPortal install screen, select the **BROWSE** button next to the license file and select the license file from the location where you saved it in the previous step.
4.3	The *LICENSE PASSWORD* is the 17-character string after the last "/" in the portal link. Copy and paste that into the *LICENSE PASSWORD* box.
4.4	Select the correct locking plan option: • If the site has an existing Onity system, and the goal is to upgrade the system without changing cards or updating locks, an import of their locking plan would meet their needs. Select **CREATE LOCKING PLAN** and **NEW**. • If there is no pre-created plan, select the **CREATE LOCKING PLAN** option and select **NEW**. • If an OnPortal locking plan exists for this site (pre-created using a pre-license), **BROWSE** to the folder where the locking plan is kept and select the file. **CAUTION:** This is the only time you get a chance to change the *STATION NAME* for OnPortal's purposes. The default is the computer's name on the network; naming the machine "Onity Server" or "Onity Backup" makes it very clear which machine is which later when configuring encoders, etc.
4.5	The *SERVER ADDRESS* needs to be the computer's name on the network. OnPortal defaults this value to the computer name on the network. Note the name for future use. **CAUTION:** As of version 1.0.21.3559, computers with names longer than 15 characters will cause an environment key mismatch with the certificate. Have your IT department change the computer name, reboot the computer, restart OnPortal and the environment key will have changed. Upload the new environment key and download the new license.
4.6	The *SERVICE PORT* defaults to 6543. Do not change this unless requested by IT. If it is a different port, write it down for firewall configuration.
4.7	Select **INSTALL** to complete the installation of the main server.
4.8	The machine will take some time to create a new station and start the service but eventually you should see a login screen.

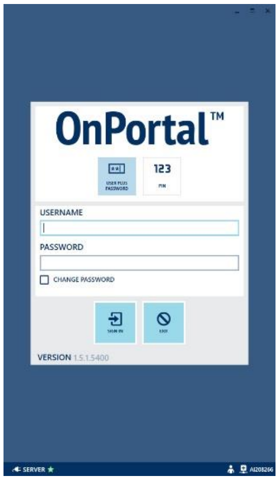


Figure 66 OnPortal Login Screen

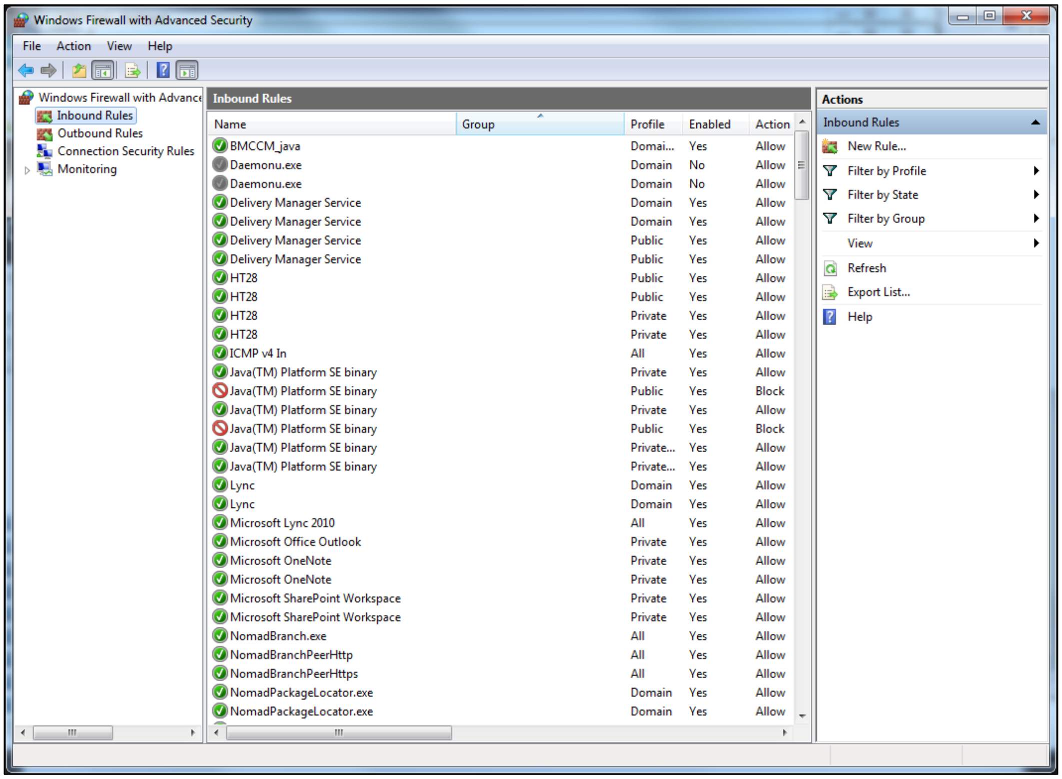
© 2019 Onity Inc.
Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Task 5: Configure the Firewall

CAUTION: Every machine for OnPortal requires that the firewall allow communication to the server. Backup machines and Stations will not communicate with the server unless their firewalls are modified as directed below.

Step #	Action
5.1	On Windows 10, go to Windows Administrative Tools, and select Windows Defender Firewall with Advanced, or select Cortana and type in Windows Firewall. (In any other version of Windows, go to the Control Panel and select Windows Firewall).
5.2	On the left side, select **Advanced Settings**.
5.3	Select **Inbound Rules**.
5.4	On the right, select **New Rule**.
5.5	Select the **Port** radio button for Rule Type, then click **Next**.
5.6	Verify that **TCP** is checked and **Specify local ports** is the port noted in step 4.6 above (default is 6543); click **Next**.
5.7	Select **Allow the connection,** then click **Next**.
5.8	Verify that all three items are checked (Domain, Public, Private), then click **Next.** **CAUTION:** Be careful as it typically defaults to *don't allow* so make sure to allow.
5.9	Name the inbound rule as *OnPortal Inbound Port*, put in a description if you choose and select **Finish**.
5.10	Click on **Outbound Rules**, perform steps 4-9 again except name it as *OnPortal Outbound Port.* **CAUTION:** Be careful on Step 5.8, it typically defaults to *don't allow* so make sure to allow.
5.11	Close the Advanced firewall rules and/or control panel once complete.
5.12	Repeat on *ALL* OnPortal servers and stations.



Inbound Rules

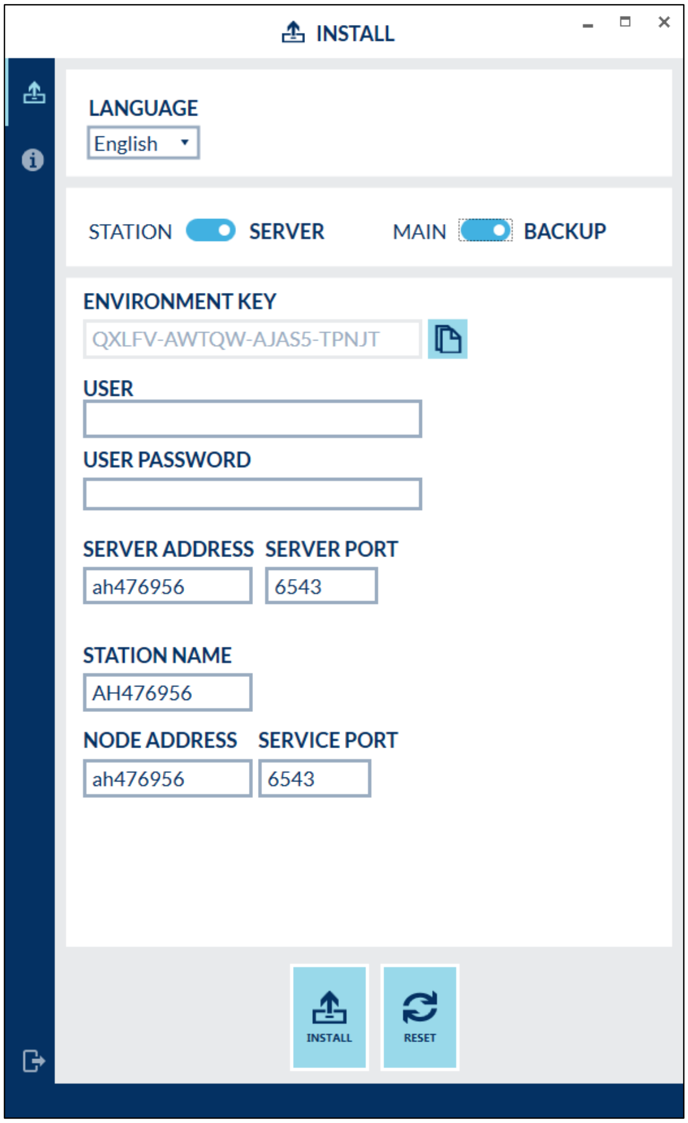
Name	Group	Profile	Enabled	Action
BMCCM_java		Domai...	Yes	Allow
Daemonu.exe		Domain	No	Allow
Daemonu.exe		Domain	No	Allow
Delivery Manager Service		Domain	Yes	Allow
Delivery Manager Service		Domain	Yes	Allow
Delivery Manager Service		Public	Yes	Allow
Delivery Manager Service		Public	Yes	Allow
HT28		Public	Yes	Allow
HT28		Public	Yes	Allow
HT28		Private	Yes	Allow
HT28		Private	Yes	Allow
ICMP v4 In		All	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
Java(TM) Platform SE binary		Public	Yes	Block
Java(TM) Platform SE binary		Private	Yes	Allow
Java(TM) Platform SE binary		Public	Yes	Block
Java(TM) Platform SE binary		Private...	Yes	Allow
Java(TM) Platform SE binary		Private...	Yes	Allow
Lync		Domain	Yes	Allow
Lync		Domain	Yes	Allow
Microsoft Lync 2010		All	Yes	Allow
Microsoft Office Outlook		Private	Yes	Allow
Microsoft OneNote		Private	Yes	Allow
Microsoft OneNote		Private	Yes	Allow
Microsoft SharePoint Workspace		Private	Yes	Allow
Microsoft SharePoint Workspace		Private	Yes	Allow
NomadBranch.exe		All	Yes	Allow
NomadBranchPeerHttp		All	Yes	Allow
NomadBranchPeerHttps		All	Yes	Allow
NomadPackageLocator.exe		Domain	Yes	Allow
NomadPackageLocator.exe		Domain	Yes	Allow

Figure 67 Windows Firewall with Advanced Settings

© 2019 Onity Inc.
Onity Confidential and Proprietary Information

Task 6: Configure Backup SERVER

Step #	Action
6.1	Repeat Task 5: Configure the Firewall on the backup machine.
6.2	For the *USER*, enter "onitytech" (without quotes).
6.3	For the *USER PASSWORD*, enter in the characters after the last "/" in the portal link (same as the license password).
6.4	The *SERVER ADDRESS* is the computer name for the server address in Step 4.5.
6.5	The *SERVER PORT* is the port from step 4.6, usually 6543.
6.6	*STATION NAME* is the name OnPortal calls this machine. Typically Onity suggests using "Backup" or "Onity Backup" so that it is clear to anyone that this is the backup server. **NOTE:** If you want to change the name, you *must* do it here.
6.7	*NODE ADDRESS* is the name of the computer on the network so leave it as is.
6.8	*SERVICE PORT* is the port the backup machine listens on. Allow this port through the firewall on Step 6.1 for inbound if not done already. Outbound traffic will use the *SERVER PORT* number. Usually both ports are 6543.
6.9	Select **INSTALL** to complete.



LANGUAGE: English

STATION ○ SERVER   MAIN ○ BACKUP

ENVIRONMENT KEY: QXLFV-AWTQW-AJAS5-TPNJT

USER

USER PASSWORD

SERVER ADDRESS: ah476956
SERVER PORT: 6543

STATION NAME: AH476956

NODE ADDRESS: ah476956
SERVICE PORT: 6543

Figure 68 Backup Install Screen

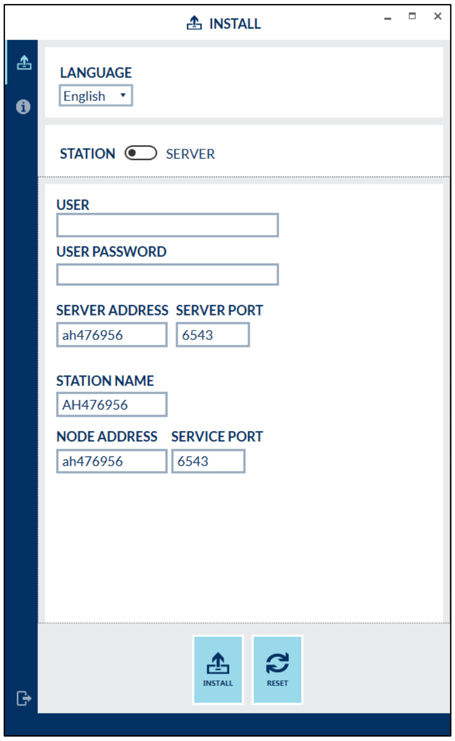
© 2019 Onity Inc.
Onity Confidential and Proprietary Information

RETURN TO TABLE OF CONTENTS

Task 7: Install and Configure Any OnPortal Stations

Installing and configuring stations is very similar to setting up a backup machine. The main difference is that a licensee may have an unlimited number of stations, so there are no environment keys on stations.

Step #	Action
7.1	Install the OnPortal program on the device/machine.
7.2	Configure the firewall first as per Task 5 above.
7.3	Start the OnPortal program.
7.4	Enter “onitytech” as the *USER.*
7.5	Enter the characters after the last “/” in the portal link as the *USER PASSWORD*.
7.6	The *SERVER ADDRESS* is the computer name for the server address in Step 4.5.
7.7	The *SERVER PORT* is the port from Step 4.6, usually 6543.
7.8	Change the *STATION NAME* to something that makes sense for OnPortal usage, like Station 1, Station 2, etc.
7.9	*NODE ADDRESS* is the name of the computer on the network so leave it as is.
7.10	*SERVICE PORT* is the port the station listens on. Allow this port through the firewall on Step 7.2 for inbound traffic. Outbound traffic will use the *SERVER PORT* number. Usually both ports are 6543.
7.11	Click **INSTALL**.



SERVER ADDRESS: ah476956
SERVER PORT: 6543
STATION NAME: AH476956
NODE ADDRESS: ah476956
SERVICE PORT: 6543

Figure 69 Station Install Screen

About the user name and password needed to set up Backups or Stations

These instructions assume that no users are set up in the system yet. As installers become more experienced with OnPortal, it may be easier for them to install on the server and use that machine to create the locking plan and train staff on how to use the program before taking it live. If the site has created operators in OnPortal, and one of those operators has a user ID, password to login AND has the rights to *Configuration > Station Configuration* in their role, then one could use that user ID/Password to set up the backup or any station.

RETURN TO TABLE OF CONTENTS

CAUTION: Closing the zip file is critical. Frequently, people try to run the installer from within the zip extraction program. This will not work and will result in a message saying, "The device driver installation wizard was unable to find any drivers designed for your machine….."

Log in to OnPortal for the First Time

Step #	Action
1.	Open the OnPortal program. Verify that it is on the **USER PLUS PASSWORD** login option.
2.	Enter "onitytech" (without quotes) as the *USER.*
3.	Enter the characters after the last forward slash (\) in the portal link as the *PASSWORD* (This is the tech password, which is the same as the license password during installation).
4.	Select **SIGN IN.**

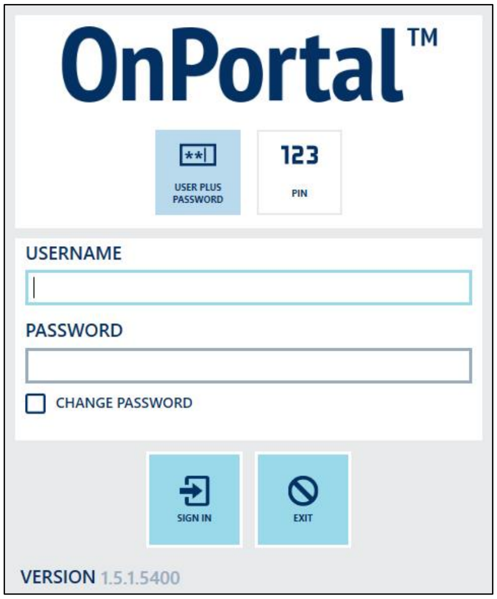


Figure 70 OnPortal Login Screen

RETURN TO TABLE OF CONTENTS

Appendix B
IP Encoder Installation Guide

© 2019 Onity Inc.
Onity Confidential and Proprietary Information

IP Encoder

Installation Guide

1 Purpose

These instructions are applicable to the installation of the Onity IP Encoder, used in conjunction with Onity's OnPortal™ property management system.

1.1 Supported Operating Systems

- Windows 8 or newer
- Windows Server 2012 or newer

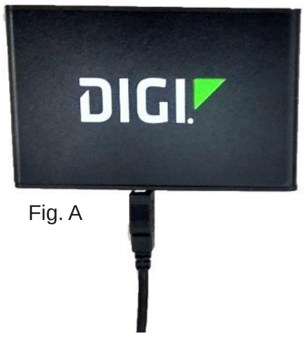


Fig. A

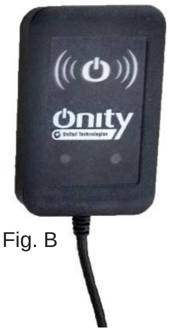


Fig. B

2 Connecting Encoders

2.1 Verify components

Equipment	Description
Included	DIGI AnywhereUSB 2 Plus Hub (Fig. A)
	AC Power Supply: US plug to 5 VDC. 2.5 mm locking barrel plug (3 A max). DIGI PN 76000934
Available Separately	IP Encoder (Fig. B)

2.2 Connect hardware at front desk or at each location an encoder is desired

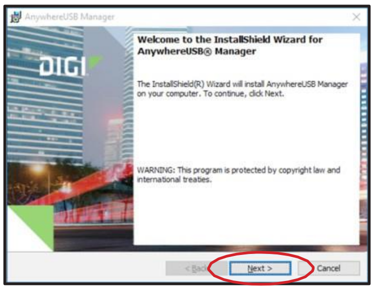
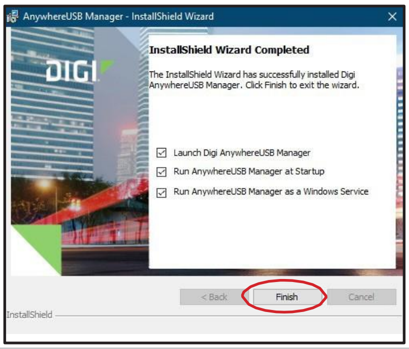
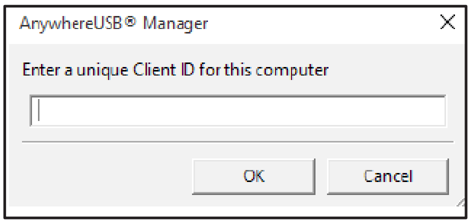
Step	Action
1.	Power the DIGI AnywhereUSB® 2 Plus Hub, using the included power cord.
2.	Connect DIGI AnywhereUSB 2 Plus Hub to a network, using the Ethernet cable.
3.	Connect the OnPortal Encoder / RFID Encoder to the DIGI AnywhereUSB 2 Plus Hub, using the supplied USB attachment.

***WARNING**: This device does not support any USB extension cables.*

2.3 Install AnywhereUSB Manager

***WARNING:** You MUST install AnywhereUSB Manager as a Windows service.*

Step	Action
1.	Visit OnityNet and download the IPEncoder.exe file.
2.	Run the IP Encoder.exe file as an administrator. Note: This requires a 64-bit operating system.

Step	Action
3.	Select **Next**.  **Welcome to the InstallShield Wizard for AnywhereUSB® Manager** The InstallShield(R) Wizard will install AnywhereUSB Manager on your computer. To continue, click Next. WARNING: This program is protected by copyright law and international treaties.
4.	Select **Install**.
5.	Check the box next to ***Run AnywhereUSB as a Windows Service***. The first two boxes on the screen are selected by default, so confirm that all three boxes are checked.
6.	Select **Finish**. You will see the Client ID confirmation dialog box.  AnywhereUSB Manager - InstallShield Wizard DIGI < Back Finish Cancel InstallShield **InstallShield Wizard Completed** The InstallShield Wizard has successfully installed Digi AnywhereUSB Manager. Click Finish to exit the wizard. ☑ Launch Digi AnywhereUSB Manager ☑ Run AnywhereUSB Manager at Startup ☑ Run AnywhereUSB Manager as a Windows Service
7.	Enter a unique Client ID. Use the computer name as the Client ID,  Enter a unique Client ID for this computer
8.	Select **OK**. This launches the AnywhereUSB Manager.

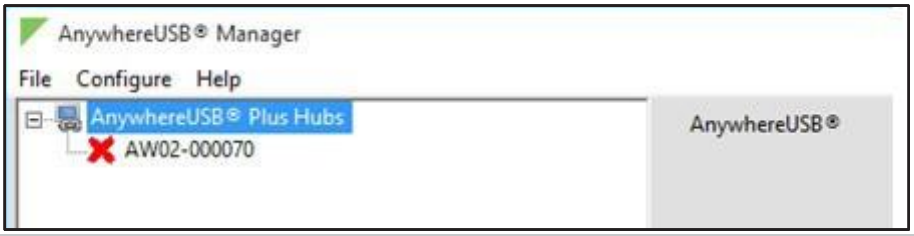
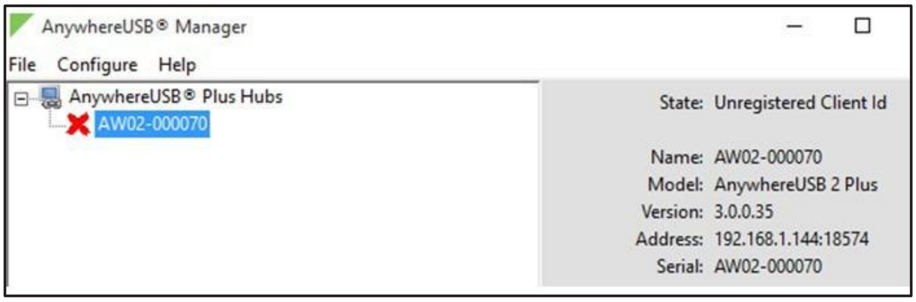
2.4 Verify Initial Connection

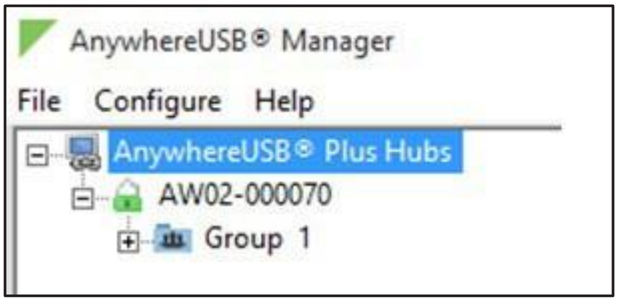
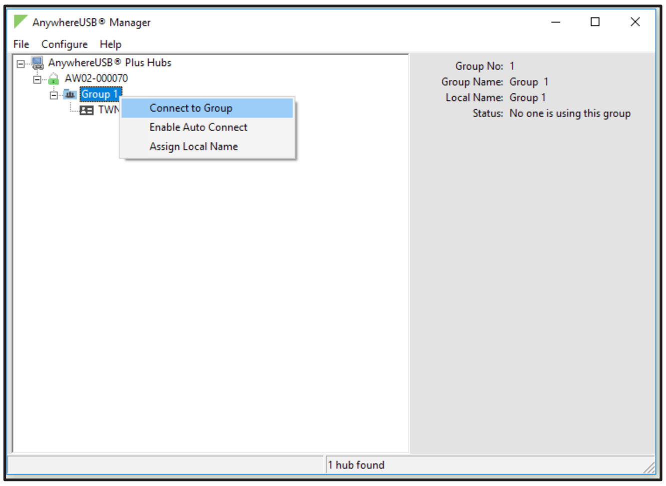
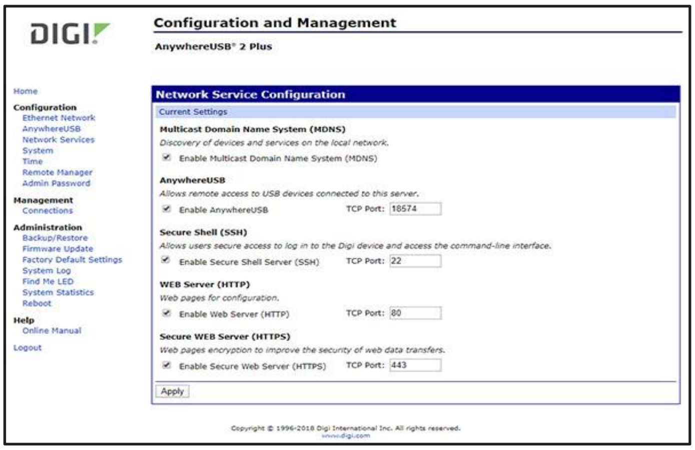
***Note**: Due to smart card limitations in the Microsoft Windows OS, only 5 encocders can be linked per station.*

After you have connected and powered on the hardware and installed the AnywhereUSB Manager, perform the following steps to verify that it is connected.

Step	Action
1.	Verify that your Hub is powered on. (The power LED is solid blue.)
	For Sites with a Static IP Address By default, the IP Encoder has a dynamic IP address. To switch to a static IP address, configure the IP address on the DIGI Hub using the Web UI under *Configuration* > *Ethernet Network.* ***CAUTION**: Verify that the IP Address, Subnet Mask, and Default Gateway are correct. If these are entered incorrectly and saved, the DIGI device will not function and it will need to be factory reset and reconfigured.*
2.	Verify that all ports with connected encoders have solid yellow LEDs.

RETURN TO TABLE OF CONTENTS

Step	Action
3.	If it is not already open, launch the AnywhereUSB Manager.
4.	Expand AnywhereUSB Plus Hubs so that it displays a list of AnywhereUSB Plus Hubs.  AnywhereUSB® Manager File Configure Help AnywhereUSB® Plus Hubs AW02-000070 AnywhereUSB®
5.	Verify that the serial number of the Hub you connected is on the list. You can find the serial number on the Hub’s label.
6.	You will notice that the AnywhereUSB Manager is showing the Hub in an error state, with a red X appearing next to the Hub name. Click on the Hub to update information in the Hub Status pane. The Hub state appears as “Unregistered Client ID.” ***Note:*** *This is a security feature. The Hub administrator needs to allow each new client ID by adding the client ID to the client list.*  AnywhereUSB® Manager File Configure Help AnywhereUSB® Plus Hubs AW02-000070 State: Unregistered Client Id Name: AW02-000070 Model: AnywhereUSB 2 Plus Version: 3.0.0.35 Address: 192.168.1.144:18574 Serial: AW02-000070
7.	You must add the Client ID to the Hub from the Web UI before you can register the Client ID with the Hub. To do so, perform the following steps: a. Right-click on the Hub and select **Open Web UI**. b. When you see the login screen, enter the following: i. User name: admin ii. Password: The password is located on the bottom of the AnywhereUSB Plus Hub. ***Note:*** *The password is case-sensitive and must be entered exactly as it appears on the label.* ***Note:*** *The first time you launch the Web UI, you may see a warning that your internet connection is not private. Continue to access the device and the login screen will appear.* c. Select **log in** and the Web UI will appear. d. Select **AnywhereUSB** from the configuration section and you will see the *AnywhereUSB Configuration* page. e. In the *Client Settings* section, select **Add Client**. A new row labeled “New Client” is added to the client list and the *Settings for Client* section is populated for the new client. f. In the *Client ID* field, enter the Client ID you assigned to your computer when you installed the AnywhereUSB Manager. ***Note****: If you forget the Client ID, it can be viewed under File > Preferences.* g. In the *Description* field, enter a descriptive name for the computer. h. Select the checkbox next to Group 1. i. Select **Apply** to save the Hub settings.
8.	Open the AnywhereUSB Manager. The Manager connects to the Hub.

Step	Action
9.	Expand the Hub to display the groups.  AnywhereUSB® Manager File Configure Help AnywhereUSB® Plus Hubs AW02-000070 Group 1
10.	Expand Group 1 to display the encoders connected to Group 1.
11.	Right-click on Group 1 and select **Connect to Group**. The encoder(s) are now available in Windows. Right-click on Group 1 again and select **Enable Auto Connect**.  AnywhereUSB® Manager File Configure Help AnywhereUSB® Plus Hubs AW02-000070 Group 1 TWN Connect to Group Enable Auto Connect Assign Local Name Group No: 1 Group Name: Group 1 Local Name: Group 1 Status: No one is using this group 1 hub found
12.	Disable Port 22 on the Hub. To do so, in the AnywhereUSB Manager, right-click the Hub and select **Open Web UI.**
13.	Sign in to the web interface.
14.	On the left side under the “Configuration” section, select **Network Services**.
15.	In the “Network Service Configuration” section under “Secure Shell (SSH),” uncheck the checkbox next to “Enable Secure Shell Server (SSH) TCP Port: 22.”  DIGI Home Configuration Ethernet Network AnywhereUSB Network Services System Time Remote Manager Admin Password Management Connections Administration Backup/Restore Firmware Update Factory Default Settings System Log Find Me LED System Statistics Reboot Help Online Manual Logout Configuration and Management AnywhereUSB® 2 Plus Network Service Configuration Current Settings Multicast Domain Name System (MDNS) *Discovery of devices and services on the local network.* ☑ Enable Multicast Domain Name System (MDNS) AnywhereUSB *Allows remote access to USB devices connected to this server.* ☑ Enable AnywhereUSB TCP Port: 18574 Secure Shell (SSH) *Allows users secure access to log in to the Digi device and access the command-line interface.* ☑ Enable Secure Shell Server (SSH) TCP Port: 22 WEB Server (HTTP) *Web pages for configuration.* ☑ Enable Web Server (HTTP) TCP Port: 80 Secure WEB Server (HTTPS) *Web pages encryption to improve the security of web data transfers.* ☑ Enable Secure Web Server (HTTPS) TCP Port: 443 Apply Copyright © 1996-2018 Digi International Inc. All rights reserved. www.digi.com

2.5 Configure the IP Encoder in OnPortal

Note: *Steps 1-8 must be done for each encoder.*

Step	Action
1.	Launch OnPortal.
2.	Sign in.
3.	Navigate to configuration menu using top left drop-down menu. ***Note:*** *On the screen, IP Encoders show as USB servers with a connected OnPortal encoder (shown as "Other").*
4.	Tap the **Encoders** icon on the left.
5.	Tap the **Scan** icon at the bottom of the page. ***Note:*** *While the scan is running, the site will be unable to make keys.*
6.	Once scanned, the encoder(s) should appear on the list.
7.	To locate a specific encoder, select the encoder and tap on the **Test** icon .
8.	Give the encoder a name related to its physical location and click the **Save** icon . Encoders should be named something meaningful to the site. For example, "Front Desk 1" indicates the first front desk encoder. ***Note:*** *Encoder names are limited to 20 characters.*

2.6 Set encoder as a default for a station

Step	Action
1.	In the configuration menu, tap the **Stations** icon on the left.
2.	Select the station that corresponds to the encoder you just named.
3.	From the Default Encoder drop-down menu, select **Encoder**.
4.	Click **Save** .

Note: *To replace an IP Encoder, first* ***copy the station name and encoder name of the encoder you are going to replace****, delete that encoder, then repeat the steps in Sections 2.5 and 2.6 above for the new encoder.*

2.7 Technical Support

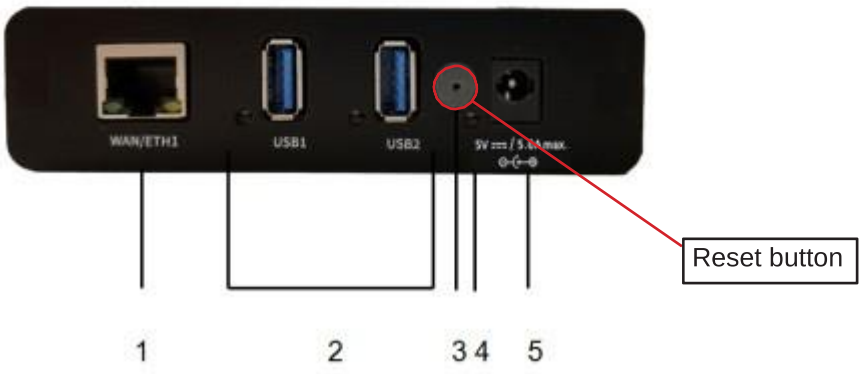
For technical support, call **800-248-6189**.

3 Troubleshooting

Error Message	What's Wrong	How to Correct
Encoder name already exists!	Duplicate encoder name already in the database.	Give the encoder a unique name for proper identification
Encoder not connected.	DIGI AnywhereUSB 2 Plus power cable is unplugged. Network cable is unplugged. Card reader USB cable is unplugged. Check DIGI AnywhereUSB 2 Plus Hub software to see if USB encoder is connected.	Make sure all three plugs are properly connected; wait to hear a beep after reconnecting the cables; try encoding a card again. Go to DIGI AnywhereUSB 2 Plus Hub to see if USB encoder is connected. If not, right-click the USB encoder and check "connect device automatically" and then click "connect device." Verify link lights (around the network jack) to ensure network connection is active.

3.1 Other Troubleshooting Tips

If you are unable to assign any other IP Encoder when configuring to a static IP, use a small pin or paperclip to push the factory reset button on the DIGI Hub.



DIGI AnywhereUSB 2 Plus Hub

KEY
1. Ethernet Connector
2. USB LEDs and Ports
3. Reset button
4. Power LED
5. Power Connector

3.2 Exit the Program

Click the “X” in the upper right corner of the window to minimize the program to the system tray.

4 Environmental Compliance

Onity encoders adhere to environmental regulations established by the current European Union (EU) RoHS, WEEE, and REACH directives.

Onity Inc. declares that our products and packaging do not contain any of the SVHCs, identified by EHCA, in any concentration above 0.1%, and hereby certify that its products are in full compliance with all aspects of Commission Regulation (EU) 2017/999 of 13 June 2017 amending Annex XIV to Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH).

5 Regulatory

Regulatory Statements	
Canada (IC)	This device complies with Industry Canada’s license-exempt RSSs. Operation is subject to the following two conditions: 1. This device may not cause interference; and 2. This device must accept any interference, including interference that may cause undesired operation of the device. Cet équipement est conforme á Ia (aux) norme(s) canadienne(s) d’exemption de licence RSS Industry Canada. Son opération est sujette aux deux conditions suivantes: (1) cet équipement ne provoquera aucune interference el (2) cet équipement doit tolérer toute in interférence pouvant provoquer une opération indésirable de l’equipement..
United States (FCC)	This device complies with Part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: 1. This device may not cause interference; and 2. This device must accept any interference, including interference that may cause undesired operation. Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment. To comply with FCC RF exposure compliance requirements, the device must be installed to provide a separation distance of at least 20 cm from all persons.
European Union (CE)	This Class B digital apparatus conforms to the requirements of the following EU directives: 1. RED, 2.4GHz, Bluetooth Power class 1 (12dBm max) 1. WEEE Directive (2012/19/EC)
Mexico	La operación de este equipo está sujeta a las siguientes dos condiciones: 1. es posible que este equipo o dispositivo no cause interferencia perjudicial y 2. este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

2020 Carrier. Onity is a part of Carrier. Other brand and product names are or may be the trademarks of, and are used to identify products or services of, their respective owners. This document discloses subject matter in which Carrier has proprietary rights. Neither receipt nor possession thereof confers or transfers any right to reproduce or disclose the document, any part thereof, any information contained therein, or any physical article or device, or to practice any method or process, except by written permission from, or written agreement with, Carrier. The information in this document is subject to change without notice. Carrier assumes no responsibility for inaccuracies or omissions and specifically disclaims any liabilities, losses, or risks, personal or otherwise, incurred as a consequence, directly or indirectly, of the use or application of any of the contents of this document. 10106779P1 *EN*

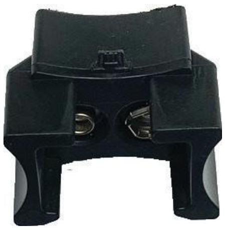
RETURN TO TABLE OF CONTENTS

Appendix C
Emergency Battery Pack

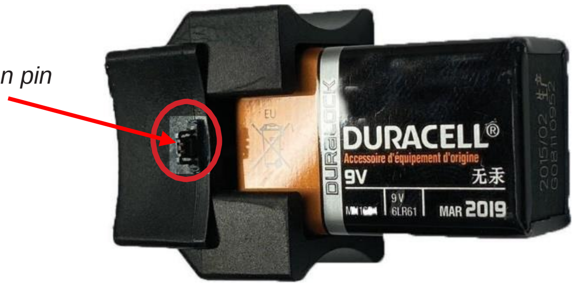
EMERGENCY BATTERY PACK

The Serene Lock is powered by 4 AA batteries. In the event that the batteries in the door have lost power, it may be necessary to open the door using the Emergency Battery Pack.

The Emergency Battery Pack consists of a molded connector and a 9V battery.



Connector only



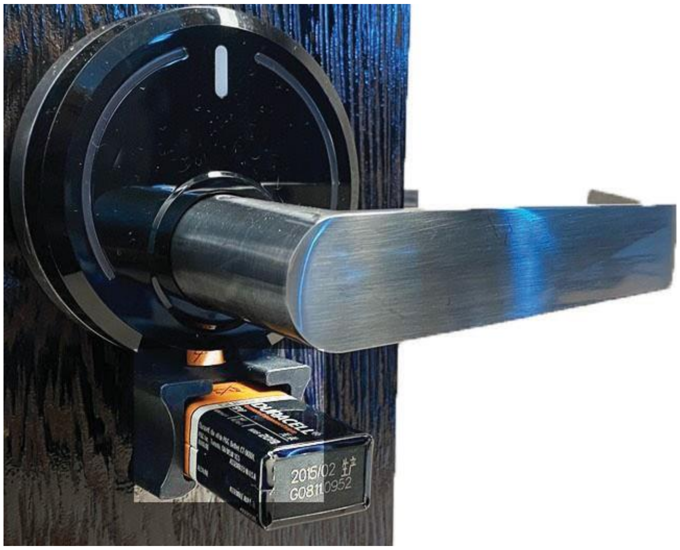
Connection pin

Connector with battery

The Emergency Battery Pack connects to the underside of the exterior rosette, as shown below.

IMPORTANT: *Battery Pack connector pin is fragile. DO NOT FORCE the connection.*

1. To connect Emergency Battery Pack to rosette, press connector flat to the door under rosette.
2. Push up GENTLY to insert connector pin. **DO NOT FORCE**.
3. Once connected, hold onto Emergency Battery Pack (to prevent it from falling) and use valid RFID card/device that will open the door.



Emergency Battery Pack connected to rosette