TOC

Onity® OnPortal™ Lock Management System

Installation Guide

Copyright

Disclaimer

The information contained herein is subject to change without notice. UTC 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.

Preface

The Onity OnPortal Lock Management System Installation Guide includes instructions explaining:

- How to use the OnityNET site
- How to install the OnPortal software
- How to configure the OnPortal software

The following conventions are used in this document:

Bold	Menu items and buttons.
Italic	Emphasis of an instruction or point; special terms. File names, path names, windows, panes, tabs, fields, variables, and other GUI elements. Titles of books and various documents.
Blue italic	(Electronic version.) Hyperlinks to cross-references, related topics, and URL addresses.
`Monospace`	Programming or coding sequences.

Safety terms and symbols

These terms may appear in this manual:

WARNING: Warnings identify conditions or practices that may result in personal injury.

CAUTION: Cautions identify conditions or practices that may result in damage to the equipment or other property.

Note*: Notes provide additional information that precedes the procedure step.*

Welcome To OnityNET

OnityNET is the internal online system to help Onity Installers set up customers with the OnPortal Lock Management system. OnityNET requires a valid sign in ID and password and administrative privileges to install the system. OnityNET and OnityNET Portal are used together to complete the secure transfer of software and site information to the customer.

- Create and manage sites, customers, and users
- Download OnPortal software and license
- Generate tech passwords
- Upload locking plans and other essential files

About Business Units

Business Units are Onity employees located in:

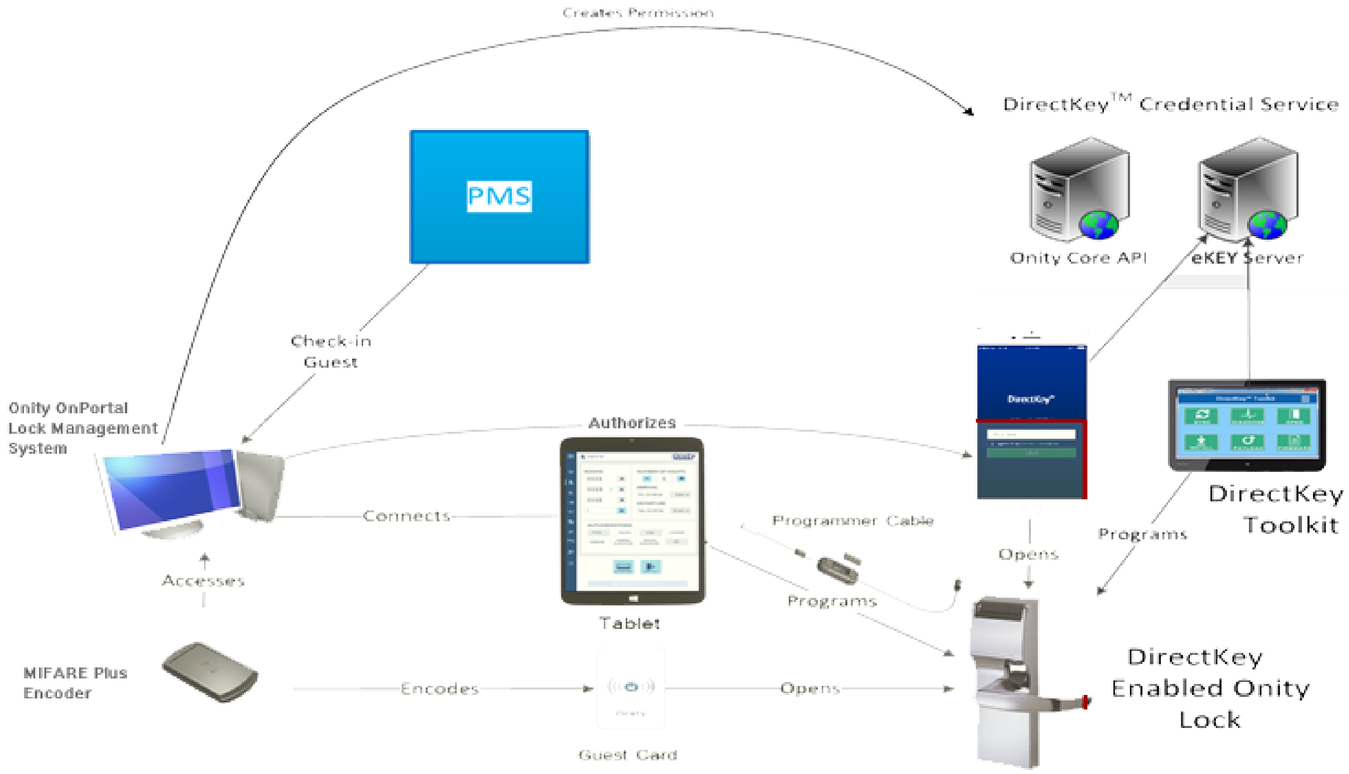
- Asia
- Australia
- Europe, the Middle East and Africa (EMEA)
- Latin America (LATAM)
- North American Region (NA)

About Onity OnPortal

The Onity OnPortal Lock Management System software offers stand-alone and online access management from a personal computer.

The operational speed of this software (in a networked environment) is determined by network speed, available bandwidth, and other applications utilizing the same network portals concurrently. Refer to the site network administrator with speed and connectivity issues.

Process Flow



DirectKey Mobile App

With the Property Management System (PMS) or OnPortal Lock Management System (OnPortal), a guest is checked into the site. OnPortal sends the information to the DirectKey Credential Service. OnPortal authorizes the DirectKey app to open the assigned lock.

Without DirectKey Mobile App

With the PMS or OnPortal, a guest is checked into the site. OnPortal authorizes the encoder to encode a key card for the assigned lock.

OnityNET

When installing OnPortal at a site, use the internal Onity site, www.onity.net, with your login and password to obtain:

- Site-specific documentation (Locking Plan, Keying Form, etc.)
- Software installer
- Pre-licenses and licenses
- Tech Passwords

Installers receive an email from Onity that includes an installer link and password. This allows the installer to download the pre-license and license, software, and locking plan (if applicable) for the site. The password is required to import the license.

OnityNET

OnityNET (www.onity.net) is a website interface for licensing and operational support of Onity OnPortal.

- Site-specific documentation (Locking Plan, Keying Form, etc.)
- OnPortal software installer
- OnPortal pre-licenses and licenses
- OnPortal Tech Passwords

OnityNET Portal

OnityNET Portal is a secure website interface designed for Onity Installers and is used to house site licenses. An email is sent to the installer with the installer link that grants the installer access to support a single site.

- Site-specific documentation (Locking Plan, Keying Form, etc.)
- OnPortal software installer
- OnPortal pre-licenses and licenses

System Requirements

The operating system must run using one of these systems. The disk space requirements will increase as data is added to the program. A mouse and a modem are required for communications. The software may be run on a local area network (LAN). Verify your system meets the minimum hardware and software requirements.

Compatibility Requirements

OS Compatibility	Server Compatibility
Windows 10 32 bit and 64 bit Windows 8.1 32 bit and 64 bit Windows 7 Service Pack 1, 32 bit and 64 bit	Windows Server 2016 Windows Server 2012

Server Requirements

Recommended	
CPU	x64
Clock Speed	3GHz or faster multi-core
RAM	8 GB
Disk Space	5 GB
Color Display Area	1280x1024 pixels
Dedicated Serial Ports	2
Minimum	

CPU	x86 or x64
Clock Speed	1GHz or faster
RAM	2 GB
Free Disk Space	50 MB
Color Display Area	1024x768 pixels
Dedicated Serial Ports	1

Client Requirements

Recommended	
CPU	x64
Clock Speed	3GHz or faster multi-core
RAM	8 GB
Free Disk Space	5 GB
Color Display Area	1280x1024 pixels
Dedicated Serial Ports	2
Minimum	
CPU	x86 or x64
Clock Speed	1GHz or faster
RAM	2 GB
Free Disk Space	50 MB
Color Display Area	1024x768 pixels
Dedicated Serial Ports	1

Tablet Requirements

Recommended	
CPU	x64
Clock Speed	3GHz or faster multi-core
RAM	8 GB
Disk Space	5 GB
Color Display Area	1366x768 pixels
Dedicated Serial Ports	2

Minimum	
CPU	x86 or x64
Clock Speed	1GHz or faster
RAM	2 GB
Disk Space	50 MB
Color Display Area	1024x768 pixels
Dedicated Serial Ports	1

Tool and Equipment Requirements

Item
Installer Email
OnityNET Sign In and Password
Internet Access
Site System Administrative Rights

Skill Requirements

Function	Skills
Software Installation	Computer Technician
System User, Admin	General

Maintenance Requirements

Product	Description
Locks	Update locks once a year for areas that do not observe Daylight Saving Time (DST). Update locks twice a year for areas that do observe DST.
System Backup	Back up the OnPortal system daily.

Reference Information

Sign into www.onity.com to find general product documentation. Sign into www.onity.net to find site specific and sensitive information. Contract trainers and others do not need to sign into OnityNET.

Document Nomenclature	Document #	Intended Audience	Location
Onity OnPortal Lock Management System Installation Guide	10104944P1	Master Users and Operators	eBuisness website
Onity OnPortal Quick Guide	10104940P1		eBuisness website
DirectKey App Quick Guide	10104739P1	Guests using DirectKey	eBuisness website
Site Survey	Site-specific	Installers	OnityNET
Keying Form	Site-specific	Installers	OnityNET
Locking Plan	Site-specific		OnityNET
Firmware	None		OnityNET
MSI	None		OnityNET

Install Process Overview

Installers must have administrative rights on the main computer to install OnPortal.

***Important**: Use the link and Tech Password provided in the installer email to sign in to OnityNET. The tech password is at the end of the link string after the last forward slash (ex: http://onity.net/portal/23/ojqqy-oadge-x6waz). When using the link, no sign in is required.*

Double-click on the installation program and choose the default directory. Continue through the installation and accept the license agreements, etc.

Install the program on the backup server before configuring the server to get the license key of the backup machine.

OnPortal Components

See the Hardware Connections section for more details.

Software

OnPortal and OnityNET may need to be open at the same time to copy and paste the environment key from OnPortal to OnityNET when creating the license. A license key and tech password is required to continue to install OnPortal on the site server. The license file requires a password to decrypt it for the system.

Step #	**Action**
1.	Open your email with the sign in and password for OnityNET from Onity.
2.	Click **Get Installer** to download the file.
3.	Download ***FrontDesk-x.x.x.x.x.msi*** to the local machine.
4.	Run the *FrontDesk-x.x.x.x.x.msi* file as an Administrator to install and start an OnPortal window service.
5.	Install all the drivers, as required.

6.	Double-click the OnPortal desktop icon (no admin rights required).
7.	On the OnPortal INSTALL screen, choose **SERVER**.
8.	Create a new site.
9.	Copy the environment key from the OnPortal INSTALL screen to the OnityNET ENVIRONMENT KEY field in the LICENSE tab.
10.	Create the license key and password, see Download License.
11.	In OnPortal, next to the *LICENSE* field, click **BROWSE** and in *Downloads*, choose the license.
12.	Add the license password.
13.	Create a locking plan (NEW or DEMO) or click **BROWSE** to choose the existing locking plan.
14.	Download the OnPortal software.
15.	Add the OnPortal license and password.
16.	Click **INSTALL**.

Standard Work Checklist

An OnityNET sign in ID and password are required to perform these steps.

✓	Steps to Do
	Create or verify customer.
	Create the customer site.
	Create the license details.
	If upgrading from a previous Onity system, set the site code.
	Copy or enter MIFARE Plus Keys.
	Download OnPortal pre-license, if applicable.
	Download OnPortal license.
	Download the pre-license or email link to trainer, if applicable.
	Download the OnPortal license and import it into the OnPortal server on site.
	Upload files to OnityNET
	Download the files to the site.
	Create a tech password.
	Download the OnPortal software.
	After the OnPortal files are downloaded, download the drivers, as required.
	Install the OnPortal software.
	Create the locking plan.

Pre-Install Process Checklist for Installers

These steps should be done by the Onity Product Manager.

✓	Steps to Do
	Verify required products are at the site.
	Verify required people have been contacted.
	Log into OnityNET.
	Create a customer.
	Create the customer site.
	Enter the license details.
	Create a Tech Password.
	Download OnPortal Pre-license.
	Email the password and URL to the assigned Onity Trainer.

About Customers

A customer is typically the parent company of the site. A customer may have many sites under it. Customers and sites may have different account numbers.

Create Customers

The customer must be created before the site can be created.

1. Sign into OnityNET.
2. Click **CUSTOMERS**.

***Note**: Filter by account number to check if the customer already has an account number, if so, note the number for later, if not, continue to create new customers.*

3. Click the add (+) icon next to *CUSTOMERS*.
4. Add the following information: name, account number, business unit, email, contact number, address, city, state, zip code, and country.
5. Click **CREATE**.

Edit Customers

The customer details can be modified.

1. Sign into OnityNET.
2. Click **CUSTOMERS**.
3. From the customer list select a customer.
4. Apply filters as required for quick searching.

5. Edit the information.
6. Click **SAVE**.

Delete Customers

1. Sign into OnityNET.
2. Click **CUSTOMERS**.
3. From the customer list, click the **X** next to the customer.
4. Click **OK** to confirm.

See also:

Create Sites

About Customers

About Sites

A site is the actual location of the property for a customer. A site is always connected to a customer. Customers must be created first before a site is created. The site and customer may be the same, but you still need to set up both.

In the *SITES* section, click the column headings to sort columns in ascending and descending order.

Create Sites

The customer must be created before the site can be created.

1. Sign in to OnityNET.
2. Click **SITES**.
3. Click the add (+) icon next to *SITES* to create a site.

***Note**: To connect the site to a customer, click SEARCH in the Customer section. In the Customers popup select desired customer. Filters are available for quick searching.*

4. To the *Name* field, add the property name from the *Keying Form*.
5. From the drop-down menu, choose the customer.
6. From the drop-down menu, choose the system type.
7. In the *ACCOUNT NUMBER* field, add the account number from billing system.
8. Add the customer email, phone number, address, country, location code (optional) and notes (optional).
9. Click **CREATE**.

Edit Sites

The site details can be modified. The Site ID cannot be modified.

1. Click **SITES**.
2. From the customer list select customer.
3. Apply filters as required for quick searching.

4. Edit the information.
5. Click **SAVE**.

Delete Sites

1. Click **SITES**.
2. From the site list, click the **X** next to the site.
3. Click **OK** to confirm.

See also:

About Customers

Create Customers

Create License

Create Tech Password

About License Tab

The *LICENSE* tab (within the SITES tab) provides details about the license configuration.

Term	Description
Environment key server	The environment key for the main OnPortal server.
Environment key backup	The environment key for the backup On Portal server.
Grace Period	This is how long the software will continue to work on an expired license.
Provide Warning	Between 1 week and 90 days warning notice of when the license will expire.
Number of rooms	Enter how many rooms are on the property for licensing.
Expiration date	The date the license expires.
Enforcement mode	What will happen when the license expires.
DirectKey enabled	Allow DirectKey mobile keys to be made.
Use MIFARE Plus	Check this when the property uses MIFARE Plus cards.
MIFARE Plus Keys Copy	Copy MIFARE Plus keys from a different site.
MIFARE Plus Keys Enter	Enter MIFARE Plus keys if known.
Site Code Copy	Copy Site Code from a different site.
Site Code Enter	Enter Site Code if known.
Change site code	Copy and enter site codes.
Password	This is the license password. This password is required to open the license. ***Note**: Passwords must be between 8 and 32 characters, have at least one uppercase and lowercase letter, one special character, and one alphanumeric character.*

Term	Description
Download Pre-License	Allows for OnPortal to operate as stated in the license details without environment keys for 30 days.
Download License	Allows for OnPortal to operate as stated in the license details, environment keys are required.

Create the Onity OnPortal License

Environment Keys are unique per machine. Only enter the site environment keys in OnityNET.

1. Using OnityNET, in the top navigation bar, click **SITES**.
2. Click the site.
3. Below the *SITE DETAILS*, click the **LICENSE** tab.
4. From the OnPortal software, copy the environment key and paste it into the appropriate section of the site in OnityNET.
5. From the drop-down menu, choose the grace period.
6. From the drop-down menu, choose amount of time to provide a warning.
7. Enter the number of rooms and expiration date.
8. From the drop-down menu, choose the enforcement mode.
9. Check **DIRECTKEY ENABLED** or **USE MIFARE PLUS**, as required.
10. Click **CREATE**.

See also:

Copy and Enter Site Codes

About Files Tab

This are is where site plans, locking plans, installer files, and firmware updates are uploaded. OnityNET allows for the storage of site specific files.

- Keying Form
- Site Survey
- Locking Plan
- Firmware
- Installer
- Other
- Help

See also:

Upload Site Files

Download Site Files

Delete Site Files

Upload Site Files

Files can be added to OnityNET and saved for a specific site for future access.

***Note**: These instructions are for adding specific site files to OnityNET and is different than global files. Adding and deleting global files can only be done by an Administrator in the MAINTENANCE section and are not site specific.*

1. In the top navigation bar, click **SITES**.
2. Click the site.
3. Below the *SITE DETAILS*, click the **FILES** tab.

***Note**: If using Internet Explorer the file button says "Choose file". If using Chrome the file button says "Browse...".*

4. In the *UPLOAD FILE* section, click **Browse...**, choose a file, and click **Open**.
5. Choose a file type.
6. Enter a file name.
7. Enter a description.

Note: If the file will be accessible from the OnityNET Portal then the IS PUBLIC box must be enabled for the file.

8. Click **UPLOAD**.

See also:

About Sites

Download Site Files

Delete Site Files

Create Tech Password

Download Site Specific Files

These instructions are to download specific site files that have already been added to OnityNET. Adding and deleting global files (not site specific) can only be done by an Administrator in the *MAINTENANCE* section.

1. Sign in to OnityNET.
2. Click **SITES**.
3. From the site list select the site.
4. Below the *SITE DETAILS*, click the **FILES** tab.
5. Click the down arrow icon next to the file to download.

See also:

Delete Site Files

Create Tech Password

Upload Locking Plan to OnityNET

1. Sign into OnityNET.
2. Locate the site.
3. Select the **FILES** tab under the site details.
4. Select **Choose File**, locate and select the locking plan backed up in Step 9.
5. For file type, select **Locking Plan**.
6. Enter a name and description for the file.
7. Select **UPLOAD**.

Import Locking Plans

About Tech Passwords

Tech Password

Tech Passwords are for Onity Installers, Tech Support, etc. A customer will not get the tech password. The password is also imbedded in the URL that is used.

The password can be set up to 30 days in the future. It is best to set the password for the least amount of days as possible.

1. Click the **TECH PASSWORD** tab.
2. Add the date the password is valid for.
3. Click **GENERATE**.
4. Copy the tech password to a text editor and open the URL in a new window.

URL

The URL to installer workspace. The installer will get the environment keys for the main system and backup system and add it here. There is one license for the site, but can be used for both environment keys. Use the URL and tech password to download the pre-license.

Generate Tech Password and URL

Tech passwords are for any Onity support personnel who require access to a customer's OnPortal system. The password can be set up to 30 days in the future. It is best to set the password for the least amount of days as possible.

Get a Tech Password

A *Tech Password* is required to download the OnPortal license.

1. In the top navigation bar, click **SITES**.
2. From the site list, click the site.

3. Below the *SITE DETAILS*, click the **TECH PASSWORD** tab.

***Note**: The maximum date for the tech password to expire on is 30 days from current day.*

4. Enter the date or use the calendar to add a password end date.
5. Click **GENERATE**.
6. In the *PASSWORD* section, copy and distribute the tech password as necessary.

OnityNET Portal

When a tech password is generated a URL is also generated. This URL has access to the OnityNET Portal. There are several actions, listed below, that can be completed on the OnityNET Portal page.

Modify and Save Site Environment Keys

1. Access OnityNET Portal.
2. In the *SERVER ENVIRONMENT KEY* or *BACKUP ENVIRONMENT KEY,* enter keys as displayed in OnPortal install.
3. Click **SAVE KEYS**.

Download Pre-License or Full License

The tech password will be the license password for all licenses downloaded from the OnityNET Portal.

1. Access OnityNET Portal.
2. Click **GET PRE-LICENSE** or **GET LICENSE**.

Download Global and Public Files

1. Access OnityNET Portal.
2. Click the down arrow icon to download a file.

See also:

About Users

Create Users

About Users

There are three (3) types of user roles in the OnityNET system.

- Users (general system use, not able to modify other users)
- Dealer (general system use, not able to modify license information)
- Administrators (full access to system)

There are several main features to help utilize the system. Depending on user permissions, different features may be available.

See Also:

Create Users

Reset User Password

Create Users

1. Sign into OnityNET.
2. Click **USERS**.
3. Click the add icon next to *USERS*.
4. Add the following information: first name, last name, username, email, business unit, and role.
5. Click **CREATE**.

See also:

About Users

Reset User Password

Reset User Password in OnityNET

To reset another user password, follow the steps below. To reset your personal sign in password, go to Reset Your User Password.

1. Sign in to OnityNET.
2. Click **USERS**.
3. From the user list select the user.
4. Click **EMAIL TEMPORARY PASSWORD**.

See also:

About Users

Create Users

About Maintenance Tab

There are four (4) tabs in the OnityNET *MAINTENANCE* tab. Only users with an administrator role have access to the MAINTENANCE tab.

GLOBAL FILES	Uploaded files are available for download from any site and OnityNET Portal.
SYSTEM LOGS	Displays system logs. Includes the entry date, username, action, category, etc.
HEALTH CHECK	Displays the machine name, version, database connection, and event log.
REPORTS	Displays site information regarding all of the sites that have license expiration dates in the next 90 days.

See also:

Upload Global Files

System Logs Tab

Health Check Tab

Reports Tab

Upload Global Files

These files will be accessible from every site and every OnityNET Portal.

1. Sign into OnityNET.
2. Click the **MAINTENANCE** tab.

***Note**: The GLOBAL FILES tab is selected by default. If using Internet Explorer the file button says "Choose file". If using Chrome the file button says "Browse...".*

1. In the *UPLOAD FILE* section, click **Browse...**, choose the file, and click **Open**.
2. Choose a file type.
3. Add the file name.
4. Enter a description.
5. Click **UPLOAD**.

See also:

About Maintenance Tab

Delete Global Site Files

Adding and deleting global files can only be done by an administrator in the *MAINTENANCE* section.

1. Sign in to OnityNET.
2. Click **SITES**.
3. From the site list select the site.
4. Click **MAINTENANCE**.
5. In the *FILES* section, click the **X** icon next to the file to delete the file.
6. Click **OK**.

See also:

Create Tech Password

Upload Site Files

System Logs Tab

In *MAINTENANCE*, the *SYSTEM LOGS* tab displays system logs and can be filtered by entry date, username, action, category, etc.

1. Click **MAINTENANCE**.
2. Click **SYSTEM LOGS**.
3. Use the fields to filter information.
4. Click **FILTER**.

See also:

About Maintenance Tab

Health Check Tab

In *MAINTENANCE*, the *HEALTH CHECK* tab displays the machine name, version, database connection, and event log. This is information only and no action can be taken on this tab.

Reports tab

In *MAINTENANCE*, the *REPORTS* tab displays site information regarding all of the sites that have license expiration dates in the next 90 days. This is information only and no action can be taken on this tab.

Reset Your User Password

To reset your personal sign in password, follow the steps below. To reset another user password, go to Reset User Password.

1. Sign into OnityNET.
2. Click your sign in at the far right of the top navigation bar.
3. Click **RESET PASSWORD**.
4. Add the new password twice.
5. Click **RESET**.

Sign Out of OnityNET

1. Click your sign in at the far right of the top navigation bar.
2. Click **LOGOUT**.

Hardware Connections

OnPortal Encoder

1. Install the OnPortal encoding deck drivers onto the system, if required.
2. Attach the OnPortal encoder deck to the computer USB port.

HT22 Encoders

1. Attach an Onity Communications Distributor (COM box) to the OnPortal computer for HT22 encoders.
2. Attach an encoder for each station to the COM box.
3. Press and hold the **EXIT** button on the encoder until it beeps and the menu displays.
4. Use the arrow buttons to scroll through the menu to **Program Selection** and press **ENTER**.

***Note**: Use the Regular encoder mode if making keys from the OnPortal UI or a PMS interface. Use the Terminal mode if you plan to use the keypad of the HT22 encoder to create the keys.*

5. Scroll to **Regular Encoder** and press **ENTER**.
6. Press **EXIT** and release.
7. Clear the addresses out of each encoder that is connected to a station.

***Note**: If only one encoder is addressed, OnPortal can be on the one HT encoder. Leaving multiple cleared encoders on will result in multiple encoders having the same address. However, once they are all addressed, multiple encoders can be left on at the same time.*

8. Turn off all encoders except the first one.

OnPoint Encoder

1. Remove existing OnPoint decks from the OnPoint app for each station.
2. Install the OnPoint encoding deck drivers onto the system, as required.
3. Using a full size USB to Mini USB adapter, attach the OnPoint encoder deck.

Install Station Encoders

When adding the encoder in OnPortal, let driver that are installing finish before continuing.

1. Plug the OnPortal encoder into the USB port on the station.
2. Click **SCAN**.
3. Click the encoder.
4. Click **TEST**.
5. Click **SAVE**.

See also:

Create Edit Site Configuration Options

Download OnPortal

Download the Onity OnPortal files. This can also be done from the deployment portal (URL sent to the trainer).

1. In the top navigation bar of OnityNET, click **SITES**.
2. Click the site.
3. Below the *SITE DETAILS*, click the **FILES** tab.
4. In the *FILES* section, click the MSI file download icon.

See also:

Download License

Download OnPortal Pre-License

To download the Onity OnPortal license the license details for the site must first be saved. Downloading a license can also be done from the OnityNET Portal. A pre-license does not require environment key(s) and is only valid for 30 days.

1. Sign in to OnityNET.
2. Click **SITES**.
3. From the site list select the site.

***Note**: Below the SITE DETAILS, the LICENSE tab is displayed by default. Passwords must be between 8 and 32 characters, have at lease one uppercase and lowercase letter, one special character, and one alphanumeric character. This license password is required for the OnPortal installation.*

4. In the *DOWNLOAD LICENSE* section, enter a license password.
5. Click **DOWNLOAD PRE-LICENSE**.
6. When prompted to save, select the location.

See also:

About Files Tab

Upload Site Files

Delete Site Files

Download OnPortal License

To download the Onity OnPortal license the license details must first be saved. Downloading a license can also be done from the OnityNET Portal.

1. In the top navigation bar of OnityNET, click **SITES**.
2. From the site list, click the site.

***Note**: Below the SITE DETAILS, the LICENSE tab is displayed by default. Passwords must be between 8 and 32 characters, have at lease one uppercase and lowercase letter, one special character, and one alphanumeric character. This license password is required for the OnPortal installation.*

3. In the *DOWNLOAD LICENSE* section, enter a license password.
4. Click **DOWNLOAD LICENSE**.
5. When prompted to save, select the location.

See also:

Download OnPortal Pre-License

About Files Tab

Reset OnPortal Locking Plan

1. Click **LOCKING PLAN**.
2. Select **RESET**.
3. Select **OK**.

OnPortal restarts and prompts for site license files.

OnPortal Download Steps

As an option, pre-install the OnPortal license (used for remote regions). These instructions are very similar to the *Download and Installation* section below. Instead of clicking LICENSE, click PRE-LICENSE. Then, when physically at the site to install the license, follow the steps in the section below.

Use the link and Tech Password provided in the installer email to sign in to OnityNET. The tech password is at the end of the link string after the last forward slash (ex: http://onity.net/portal/23/ojqqy-oadge-x6waz).

Download the program or install it from the USB supplied. Double-click on the installation program and choose the default directory. Continue through the installation and accept the license agreements, etc.

Install the program on the backup server before configuring the server to get the license key of the backup machine.

***Important**: If importing a locking plan from an encoder, do not click on the FINALIZE button. The FINALIZE button randomizes the sequence codes for all of the locks which forces the hotel to re-initialize all the locks to work again. Onity would use this for the hotel that loses a portable programmer, or a backup server, and may suffer security breaches. System Build uses this button at the end of building a locking plan from a template to assure that the sequence numbers do not match the template.*

Download and Installation

***Note**: Place the installer and locking plan in a folder for easy access when new tablets are added to the system.*

1. Create a folder on the computer and add the installer and locking plan files.
2. Navigate to OnityNET on the property site server for OnPortal.
3. Click the link provided in the email.

***Note**: The Onity tech password is included at the end of the link to the installer page and expires.*

4. Click **GET INSTALLER** and download the file.
5. Click **GET LOCKING PLAN**, if available, and download the locking plan to the server.
6. Run the installation program on the server.
7. Select the default directory unless instructed otherwise.
8. Continue through the installation and accept the license agreements, click **Finish**.

Note: The backup server should be in a secure location.

9. On the backup server, use the same link, and download the installation program to that machine.
10. Run the installation program on the backup server.
11. On the desktop, click the OnPortal icon to start the program on the server and backup computers.
12. At the top of the screen, slide the button to **SERVER** on both computers.

Download and Set Up the License File

The OnPortal server requires a valid license file to work. License files require the environment key for the server, the environment key for the backup computers, and an expiration date. A license file is not portable from one computer to another.

1. On the backup computer, in OnPortal, click the copy link next to the *ENVIRONMENT KEY* field.
2. In OnityNET, paste in the *BACKUP ENVIRONMENT KEY* field, and click **SAVE KEYS**.
3. On the main server computer, in OnPortal, click the copy link next to the *ENVIRONMENT KEY* field.
4. In OnityNET, paste in the *ENVIRONMENT KEY* field, and click **SAVE KEYS**.
5. Click **GET LICENSE** to download the license.
6. Allow access through Windows Firewall on all computers, laptops, and tablets using OnPortal.

Main Server Installation

Before starting the OnPortal installation, Installers must have:

- Administrative rights on the main server computer to install OnPortal
- Received an email with the tech password (the license password is the tech password)
- Access through Windows Firewall is enabled

The license password is the tech password.

1. Double-click or tap on the OnPortal icon.
2. At the top of the screen, verify **MAIN** is selected for server type.
3. Click **Browse** next to the *LICENSE FILE* field and find the downloaded license (example: Property Name-license-v0.bpex).

***Note**: There are two (2) locking plan choices; with a downloaded locking plan or without a downloaded locking plan. For the OnPortal locking plan downloaded from OnityNET option, do not check CREATE LOCKING PLAN, use the Browse button to locate the plan and import (.sdf file extension). For the no locking plan option, click CREATE LOCKING PLAN. Click NEW to create a new plan for a site, or importing an existing locking plan from another Onity system. DEMO is for sales and teaching without a locking plan. Installers /Trainers will not use this feature.*

4. In the *NODE NAME* field, enter **Onity Main Server** (this cannot be changed later).

***Note**: The server address is the network name for the computer. Leave this as it is, unless the property IT department chooses a static IP address for this computer, then enter the static IP address.*

5. Record the main server address to use when installing backup servers and stations.
6. Leave the server port default unless instructed otherwise by the property IT department.
7. Record the port number.
8. Allow the port through the Windows Firewall.
9. Click **INSTALL**.

Backup Server Installation

1. Enter in the user ID and password for the backup computer (tech password will work during installation).
2. Enter in the server address (computer name of the server on the network or IP address if static) and the port the OnPortal configured server.
3. Name the node **OnPortal Backup Server**.

***Note**: The node (station) address and service port tell the server what network computer to make the backup. The node address may be a computer or static IP address.*

4. Click **INSTALL**.

Client Server Installation

1. Verify the *INSTALL* screen slider is positioned to **STATION**.

***Note**: This may be the onitytech username and tech password provided during install, or post install, use an operator usename and password.*

2. Enter the username and password.

***Note**: To find the server address and port, go to the server and log into OnPortal. Click the CONFIGURATION menu in the drop down in the upper left. Click STATIONS and the server name displays above the station labeled SERVER.*

3. When configuring the server, enter in the address of the server and the server port.

***Note**: Each client name will be unique. As an example, for the next client, name it OnPortal Client 2, OnPortal Client 3, and so on.*

4. Name the client **OnPortal Client 1**.
5. Use the default for the NODE ADDRESS.
6. Use the default for the port unless directed otherwise.
7. Click **INSTALL** to configure the machine as a client.
8. Sign in with a valid operator.

See also:

Pre-Install Process Checklist

Download License

Download OnPortal

Windows Firewall

Upload Locking Plan to OnityNET

Upload Site Files

Create a Locking Plan

Create Customers

Create Sites

Windows Firewall

To allow the OnPortal to pass through Windows® Firewall on all computers, laptops, and tablets that use the OnPortal system.

1. Open the *Control Panel* on the computer for the server.
2. Click **Windows Firewall**.
3. Click **Advanced Setting**s.
4. Click **Inbound Rules**.
5. On the right, click **New Rule**.
6. For the *Rule Type*, click **Port**, then click **Next**.
7. Verify TCP is checked and specify local port (default is 6543), then click **Next**.
8. Click **Allow the connection**, then click **Next**.
9. Keep Domain, Private, and Public checked unless you know exactly how the network is configured, then click **Next**.
10. Name the inbound rule as *OnPortal Inbound*, add a description, and click **Finish**.
11. Click Outbound Rules, perform steps 5-9 again.
12. Name the inbound rule as *OnPortal Outbound*, add a description, and click **Finish**.
13. Close the *Advance firewall rules* and *Control Panel* once complete.
14. Repeat steps 1-13 on all backup servers and client stations (laptops, desktops, or tablets).

Copy and Enter Site Codes

When one site must have the same site code as a different site, it is possible to copy the site code. A site code can be entered for any site where the code is known and must stay the same (any Onity upgrade).

Copy

***Caution**: Adding the wrong site code will disrupt site activity.*

1. Click **SITES**.
2. Click a site.
3. In the LICENSE tab and SITE CODE section, click **COPY**.
4. Click the site to copy the site code from.
5. Click the site to copy the site code to.

Enter

***Caution**: Adding the wrong site code will disrupt site activity.*

1. Click **SITES**.
2. Click a site.
3. In the LICENSE tab and SITE CODE section, click **ENTER**.
4. Enter the site code.
5. Click **SAVE**.

See also:

Copy and Enter MIFARE Plus Keys

Copy and Enter Site Codes

When one site must have the same site code as a different site, it is possible to copy the site code. A site code can be entered for any site where the code is known and must stay the same (any Onity upgrade).

Copy

***Caution**: Adding the wrong site code will disrupt site activity.*

1. Click **SITES**.
2. Click a site.
3. In the LICENSE tab and SITE CODE section, click **COPY**.
4. Click the site to copy the site code from.
5. Click the site to copy the site code to.

Enter

***Caution**: Adding the wrong site code will disrupt site activity.*

1. Click **SITES**.
2. Click a site.
3. In the LICENSE tab and SITE CODE section, click **ENTER**.
4. Enter the site code.
5. Click **SAVE**.

See also:

Copy and Enter MIFARE Plus Keys

Create or Edit Site Configuration Options

These are the OnPortal locking plan steps used to create and edit the site *CONFIGURATION* options. The OnPortal system is already installed on the server and ready to be configured.

PROPERTY CONFIGURATION

PROPERTY

This shows the property name, last edit, and address. Set up to automatically check-in and check-out groups.

1. In the menu drop-down, click **CONFIGURATION**.
2. Click **PROPERTY**, and add the property name and address as it appears in *OnityNET* and the *Keying Form*.
3. Check to allow occupied room check in.
4. Check to allow guest card duplicates.
5. Add the arrival and departure default hours.
6. Enter the default number of nights for stays.
7. Click **SAVE**.

LICENSE

Shows information about the license: environment key, issue date and expiration date, number of rooms, the enforcement mode and if the DirectKey mobile keys are enabled. Click LOAD LICENSE to add the OnPortal license.

RECEPTION

This section show options on check-in functions. Use these defaults unless the customer specifies something different on the *Keying Form*.

1. Click **RECEPTION**.
2. Enable **ALLOW OCCUPIED ROOM CHECK IN**.
3. Enable **ALLOW GUEST CARD DUPLICATES**.
4. Click ARRIVAL and verify the default arrival time is 12 AM.
5. Enter in the default departure time listed on the *Keying Form*.
6. Check the **REQUIRED** box.
7. Verify the default number of nights is 1.
8. Click **SAVE**.

MASTER USERS

Shows the options to encode master cards (copies, start date, expiration date, and revalidation).

1. Click **MASTER USERS**.
2. Verify **ALLOW MASER CARD DUPLICATES** is unchecked.
3. Enable **USER START DATE** and make it required.
4. Verify **START DATE REQUIRED** is unchecked.
5. Enable **USER EXPIRATION DATE**.
6. Enable **REVALIDATOR**.
7. Click **SAVE**.

ENCODERS

Use to add encoder technologies and encoder audio volume.

When using the RFID compact encoder to disable the smart card plug and play service: *gpedit.msc -> Local Computer Policy -> Computer Configuration ->Administrative Templates -> Windows Components -> Smart Card : "Turn on SmartCard Plug and Play service" = "Disabled"*.

In general, do not encode MIFARE Plus config cards unless the site meets all of the following conditions.

- All locks and wall readers are Trillium style locks
- MIFARE Plus cards are used for keys
- A MIFARE Classic 1K or larger card, and a MIFARE Plus card greater than 2K to use to create configurations cards
- Customer wants to use MIFARE Plus immediately

1. From the main drop-down menu, click **CONFIGURATION**.
2. Click **ENCODERS**.
3. Click the correct card technologies for the site.

***Note**: If using the ADV15R encoder, choose the location of the portable encoder antenna. If using the motorized encoder, choose the position on the encoder from where the card ejects.*

4. From the drop-down menu, choose the encoder antenna position.
5. From the drop-down menu, choose the motorized card ejection position, if applicable.
6. Enter the number of times the encoder will retry the function.
7. Enter the maximum volume for the PCSC encoder beep volume.
8. Enter the number of addresses to search on each HT COM box and add 1 to the total.
9. Select **SAVE**.
10. Click **ENCODE MIFARE PLUS CONFIG CARDS** if applicable.
11. Click **SAVE**.

TRACKS

In the *CONFIGURATION > PROPERTY CONFIGURATION* section, the *TRACKS* icon is used to add additional multi-track and multi-sector encoding to track 1 and track 2. If the site uses additional tracks on Magnetic stripe cards, or sectors on MIFARE type cards (Ultralight cards are not used), set up key card tracks.

1. Click *CONFIGURATION*, and then **TRACKS**.
2. Click **TRACK 1** and/or **TRACK 2** to configure.
3. In the *GUEST CARDS* drop-down menu, choose **DISABLED**, **PROMPT FOR CUSTOM DATA**, or **NO PROMPT**.
4. In the *MASTER CARDS* drop-down menu, choose **DISABLED**, **PROMPT FOR CUSTOM DATA**, or **NO PROMPT**.
5. Choose a format from the drop-down menu.
6. Use the default for *KEY A*, unless the lock/system that will be using this sector requests a specific key.
7. Verify **PMS RETURN SENTINALS** is unchecked, unless the PMS system requests it.
8. Click **SAVE**.

Disabled	No data on this track.
Prompt for Custom Data	A pop-up displays to type in custom data, based upon the template.
No Prompt	Adds to the track pre-defined data listed in the template and custom data sent from a PMS.
Sector	For MIFARE and MIFARE Plus cards that have multiple sectors (Ultralight and Ultralight-C do not), select the sector to be used.

LOCKS

Set the group jump, extended opening delay, max masters per lock, and the calendar type.

1. Click **LOCKS**.
2. Use the default for *GROUP JUMP* (25).
3. Set the amount of seconds for the extended opening delay for ADA locks.
4. Add the maximum number of card codes allowed per lock.
5. Use the default for *CALENDAR TYPE* (all weekdays as workdays).
6. Click **SAVE**.

PORTABLE PROGRAMMER

In the *CONFIGURATION > PROPERTY CONFIGURATION* section, the *PORTABLE PROGRAMMER* icon is used to set the days to keep data.

1. Click **PORTABLE PROGRAMMER**.
2. Verify the default for *DAYS TO KEEP* is at 0 (recommended).
3. Click **SAVE**.

ARCHIVE

Use the defaults, the installer configures this on site based upon the system folder.

1. Click **ARCHIVE**.
2. Click to hide the records for locks that have had the cards read to open the door but the handle was not turned.
3. Click **BROWSE**, find the backup folder and click **OK**.
4. Choose the backup frequency and click *Minutes*, *Hours*, or *Days* from the drop-down menu.
5. Click **BROWSE**, find the system audit folder and click **OK**.
6. Choose the number of days to retain the system audit.
7. Click **BROWSE**, find the lock audit folder and click **OK**.
8. Choose the number of days to retain the lock audit.
9. Click **SAVE**.

DIRECTKEY MOBILE KEY

In the *CONFIGURATION > PROPERTY CONFIGURATION* section, the *DirectKey MOBILE KEY* icon is used to set up the DirectKey Mobile Key. This must be configured on site.

1. Click **DirectKey MOBILE KEY**.
2. Check to enable DirectKey mobile keys.
3. Check to enable the OnPortal system user interface.
4. Check to enable email notifications.

***Note**: The Core API Base URL depends if it is an Onity-hosted mobile key solution, or a hotel-hosted mobile key solution. For an Onity-hosted solution, the API user name and password and the certificate password is required. The Onity URL is https://api.directkey.net.*

5. Add **the CORE API BASE URL**.
6. Add the API user name.
7. Add the API password.
8. Add the certificate password.
9. Click **LOAD CERTIFICATE**.
10. Click **BROWSE**, to locate the certificate and select the .pfx file.
11. Click **OK**.

***Note**: 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.*

12. If the computer requires a proxy server, check **USE EXPLICIT PROXY**.

***Note**: The Key Owner ID, Owner ID, and Property Name on the server will fill in after a successful test.*

13. Click **TEST** to test the connection to Onity servers.
14. Click **SAVE**.

LANGUAGE

The LANGUAGE icon is used to change the language for the system user interface. Use English while building the plan. Once done, switch to the language for the client prior to uploading plan to OnityNET.

1. Click **MY ACCOUNT**.
2. From the *LANGUAGE* drop-down menu, click a language.
3. Click **SAVE**.

AUTHORIZATIONS

In the *CONFIGURATION > PROPERTY CONFIGURATION* section, the *AUTHORIZATIONS* icon is used to add authorizations to extended suites.

Authorizations must be configured before creating the lock profiles. There will be some default authorizations. Authorizations numbers correspond to the boxes (1 is the upper left box, and 8 is the lower right box).

Add Authorizations

To add an authorization, drop the number of extended suite authorizations by 1.

1. From the main drop-down menu, click **CONFIGURATION**.
2. Click **AUTHORIZATIONS**.
3. Enter an authorization name (based on the Keying Form).

***Note**: When EMPHASIZE is enabled, a confirmation pop-up displays when the user adds authorizations. The default for this feature is disabled.*

4. Click to emphasize the authorization, if required.
5. Repeat steps 3 and 4, as required to enter in all of the authorizations required based on the Keying Form.
6. Click **SAVE**.

Remove Authorizations

To remove authorizations, increase the number of extended suite authorizations or to erase all and start from scratch, select 8.

1. From the main drop-down menu, click **CONFIGURATION**.
2. Click **AUTHORIZATIONS**.
3. In *EXTENDED SUITE AUTHORIZATIONS*, click the plus (+) icon until the authorization is removed.
4. Click **SAVE**.

PMS

Configure the PMS feature if the site will use a PMS with OnPortal. The PMS listeners are set up in CONFIGURATION > PMS listeners.

1. Click **PMS**.
2. Disable **RETURN MIFARE CARD UID** to use MIFARE Plus cards and DirectKey.
3. Disable REQUIRE OPERATOR and REQUIRE PASSWORD for audits.
4. Click to log messages and to log the flow control.
5. Click to use a mobile key trigger.

***Note**: For Hilton properties, do not enable DirectKey mobile key. For other properties, follow the instructions that come with the DirectKey certificate.*

6. Click **DirectKey MOBILE KEY ENCODER** and add the value.
7. Click to have a mobile key authorization number.
8. Check the box to post keyless permissions.
9. Click **SAVE**.

SIGN IN

Selected items highlight in blue (unselected items are white). Any operator with *Config_Property* rights will be able to change the sign in types. See About Sign In Types and Lockouts.

1. Click **SIGN IN**.
2. Click the sign in types.
3. Click the amount of time until a session times out (in minutes).
4. Click **SAVE**.

STATIONS

In *CONFIGURATION/STATIONS* set the default encoder for a station to allow a tablet to make keys on an encoder connected to a different PC.

To renew the security certificate for communication between all OnPortal stations, click *RENEW SECURITY*.

1. Click ***CONFIGURATION/STATIONS***.
2. Click the station.
3. Change the name if required.
4. In the *DEFAULT ENCODER* drop-down menu, select a station.
5. Click **SAVE**.

Click *SCAN* to scan for nearby devices and *RESTART* to restart the station.

PMS LISTENERS

Use the *ENCODERS* icon on the left side menu to add and configure PMS Listeners (station, type, COM port, baud rate, stop bits, parity, etc.).

1. Click **PMS LISTENERS** in the left side menu.
2. Click **ADD**.
3. Use the drop-down menus or enter the information, if different on the *Keying Form*.
4. Click **SAVE**.

ENCODERS

Use the *ENCODERS* icon on the left side menu to search for connected encoders and make defaults. For HT22 encoders see Install HT22 Encoders.

1. Click **ENCODERS** on the left side menu.
2. Click **SCAN**.
3. Click the encoder.
4. Change the encoder number as required.
5. Click the *DEFAULT* star icon to make this encoder the default.
6. Choose the card technology.
7. Click **SAVE**.
8. Click **TEST**.

ONLINE WALL READERS

Use the *WALL READERS* icon on the left side menu to configure wall readers.

1. Click **WALL READERS** on the left side menu.
2. Click **SCAN**.
3. Choose the wall reader.
4. Change the information listed, if different on the *Keying Form*.
5. Click **SAVE**.

About Sign In Types and Lockouts

Sign In Types

OnPortal uses various types of sign in options.

Term	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.
PIN and Card	A four-digit PIN with a card to verify a person. This option forces the user to personalize the PIN code. Lost cards may be challenging.
Windows Authentication	The sign in screen is not provided if the user is logged into the Windows computer and is an operator in the OnPortal system. If signed into OnPortal with another type of login, close the program and re-open it to get all the rights of the Windows user. This type of login would work best for the Reception level operators.
User Name and Password	Reasonably secure login, the user name is not case-sensitive, the password is case-sensitive. The user can personalize their password. Password do not expire and have requirements. Initial password is usually complex and typically requires a copy and paste for the first login. Password Requirements: • At least 4 characters (a capital letter, lowercase letter, number, or a symbol) • Contains both alpha and numeric characters (symbols allowed) • Users to change passwords at least every 180 days • Cannot be any of the previous 4 passwords
User Name and Password PCI	Most secure login, the user name is not case-sensitive, the password is case-sensitive. The user can personalize their password. Password do not expire and have requirements. Initial password is complex and typically requires a copy and paste for the first login. Password Requirements: • At least 4 characters (a capital letter, lowercase letter, number, or a symbol) • Contains both alpha and numeric characters (symbols allowed) • Users to change passwords at least every 180 days • Cannot be any of the previous passwords
SESSION TIME OUT	The amount of time until the session times out.

Lockouts

OnPortal locks out the user for 15 minutes after six (6) invalid sign in attempts. Another user that is active within the system and has resetting permissions may reset the password to unlock the account.

Add a Master User In OnPortal

1. From the drop down menu choose **MASTER USERS**.
2. Click **ADD**.
3. Enter the name or title.
4. From the *KEYING* drop-down menu, choose the master type.
5. From the *SHIFT* drop-down menu, choose the shift type.
6. Click **ACTIVATION DATE** and add the dates and time.
7. Click **EXPIRATION** and add the dates and time.
8. Click any overrides.
9. Click the authorizations.
10. Click **SAVE**.

If the master user also has an operator sign in, you have the option to link the user to the operator. The **DOOR ACCESS** tab displays a list of the doors the master users has access to but it cannot be edited.

Link the Master User and Operator

1. Click **OPERATOR** tab.
2. Slide **ENABLE** to allow the link.
3. Click **LINK OPERATOR**.
4. Under the *OPERATORS* section, click the operator and then **LINK OPERATOR**.
5. After all fields are filled in, click **ENCODE**.

Cancel a Master User Card

1. From the drop down menu choose **MASTER USERS**.
2. Choose a user.
3. Click **CANCEL USER**.
4. Click **OK**.

Cancel the Code in the Locks

1. From the sidebar menu click **MASTER CANCEL CARDS**.
2. Click the master type.
3. Click **ENCODE CARDS** at the bottom.
4. Using the master cancel card, visit each lock to cancel the master code from that lock.
5. Re-encode all users of the same master type.

***Note**: You can encode a new card for the user that was lost; reactivate the user and encode the new card.*

Add Operators in OnPortal

1. From the drop down menu choose **SECURITY**, then click **OPERATORS**.
2. Click **ADD**.
3. Enter the information.
4. Click **SAVE**.

A password is generated for the user. If the user role is set to *PIN Only*, this is the password that is used. If the user role is set to *User Name and Password* or *PIN and Card*, the user will be asked to change the password at the next log in.

See also:

About Sign In Types and Lockouts

Create a Locking Plan

Use the *Keying Form* (get from OnityNET) to configure keys and locks. The *LOCKING PLAN OVERVIEW* lists:

- Door count
- Lock profiles
- Master key codes
- Master user count
- System audit count
- Lock audit count
- Timetable count

Initial OnPortal System Startup

1. Run the OnPortal program with administrator rights.
2. On the *INSTALL* screen, click **SERVER** at the top.
3. Browse and select the pre-license file (naming convention: SiteName-prelicense.bpex).
4. Enter in the tech password generated for the license password.
5. Click **CREATE LOCKING PLAN**.
6. Verify **NEW** is selected.

Note*: The Node Name, Server Address and Port are the names of the computer and the default port.*

7. Click **INSTALL** to finish.

Create locking plans by starting with the timetable setup, then create master types, lock profiles, and locks. Setting up each step in this order makes the next step easier.

Note*: If the locking plan specifies holidays other than the defaulted calendar type, then configure the calendar first.*

Configure the Calendar

Use the *CALENDAR* feature to set shifts and dates on the system. Leave all as work days unless timetables and shifts will work differently on weekends and holidays. Or, set the weekends to be weekend days and then choose which days are considered holidays.

Note*: Daylight Saving Time is pulled from the operating system and does not need to be configured on the calendar.*

1. Click **LOCKING PLAN**.
2. Click **CALENDARS** (at the bottom of the left menu).
3. Double-click on a date to add holidays, as required.
4. Click **SAVE**.
5. Repeat these steps at least 6 times to put six years of calendars into the system.
6. Click **SAVE**.

Add Timetables

Set shifts to be able to restrict card access to a time range, and Automatic changes to automatically open at a specific times and lock back at a specific times. All shifts are 24 hour access unless the shifts are modified. Add any non 24-hour shift as required from the Keying Form. The hours use military time (11:00 AM, 12:00 AM, 13.00 PM, etc.).

Add to Shifts Table

1. Click **LOCKING PLAN**.
2. Click **TIMETABLES** (at the top of the left menu).
3. Click **SHIFT**.
4. Click in field 8 and type Guest Rooms.
5. Click on fields 1-7 and add shifts as listed in the Keying Form for this site.
6. Click **SAVE**.

Add Workday/Weekend/Holiday Shifts

1. Click **ADD**.
2. Add the description.
3. In the *WORK DAY* tab, click the drop-down menu for SHIFTS and click the shift then click the plus sign (+).
4. Add the start and end for the first period.
5. If auto time changes are required for this shift, choose *Open* or *Close* and the hour.
6. Click **SAVE**.
7. Repeat steps 3-6 for weekend shifts and holiday shifts.
8. Click **SAVE**.

Master Types

In *MASTER TYPES* define what the master types are, not where they have access.

Create

1. Click **LOCKING PLAN**.
2. Click **MASTER TYPES**.

***Note**: To edit a default master user, select on the abbreviation in the box then adjust the name and description.*

3. Click **ADD**.

***Note**: Only add master types listed on the Keying Form. In a locking plan, there should not be master types that are not used on a room designated in the keying form.*

4. From the Keying Form, enter the *Master Type Designator* as the name.
5. From the Keying Form, enter the *Master Type Name* as the description.
6. Click **SAVE**.
7. Remove any default master types not used.

Delete

1. Click on the master type.
2. Click **DELETE**.
3. Click **OK**.

Lock Profiles

Lock profiles allow system build to easily create rooms that will have the same time table, authorizations, and master keying. If more than one room will have the same of those, then a profile is the best way to create the rooms. Configuring time tables, authorizations, and masters prior to lock profile creation saves editing steps.

Create lock profiles before creating the rooms.

1. Click **LOCKING PLAN**.
2. Click **LOCK PROFILES** on the left-side menu.
3. Click **ADD**.
4. Enter a profile name.
5. From the *RELATED TIMETABLE* drop-down menu, click the timetable.
6. From the drop-down menu for *REQUESTED AUTHORIZATION*, as required.
7. In the *DETAILS* tab, copy the profile name to the description.
8. Change **FUTURE GUEST CARD** to 50.
9. Verify **FUTURE MASTER CARD** is 10.
10. Verify *OFFICE MODE* is not checked.
11. Enable **PROGRAMMING CARD**.
12. Set *OPENING DELAY* to 6 seconds.
13. Enable **OPEN ON WITHDRAW**.
14. Enable **CLOSE ON LEVER**.
15. Disable **SHOW LOW BATTERY**.
16. From the *CARD AUTHORIZATIONS* drop-down menu, add card authorizations a guest card automatically gets when encoded.
17. From the *CARD OPTIONAL AUTHORIZATIONS* drop-down menu, add all optional card authorizations.
18. From the *SHIFT* drop-down menu, click the shift.
19. Disable **OVERRIDES PRIVACY LOCK**.
20. Click **SAVE**.
21. Click the **KEYING** tab.
22. Click all master types that apply to this lock profile.
23. Click **SAVE**.

***Note**: It saves time to create a profile for those doors that share the same timetable, requested authorizations, and keying information. A lock profile is not needed if only one door in a locking plan has a unique set of time tables, requested authorizations, and keying information. Once a lock profile has been created, it is quicker to create the rest of them by using the COPY command.*

a. Click **COPY**.
b. Change the profile name and description on the *DETAILS* tab.
c. All of the details copied from the profile are the same. Change any authorizations, etc. required for this new lock profile.
d. Click the **KEYING** tab.
e. Highlight master types and click **DELETE** to remove or highlight to add master types.
f. Click **SAVE**.

24. Repeat steps to create all needed guest room profiles.
25. Create additional profiles based upon information in the *Keying Form*.

26. Delete all unused lock profiles.

Rooms

To create rooms, see Create Edit Rooms.

Finalize and Backup the Locking Plan

1. Click **LOCKING PLAN**.
2. Click **FINALIZE** to randomize the key codes for all the locks.
3. Click **BACKUP** to create a file to upload to OnityNET.
4. Browse for the folder to save the backup.
5. Click **OK**.

Upload Locking Plan to OnityNET

1. Log into OnityNET.
2. Locate the site.
3. Click the **FILES** tab under the site details.
4. Click **Choose File**, locate and select the locking plan backed up in Step 9.
5. From the *FILE TYPE* drop-down menu, click **Locking Plan**.
6. Enter a name and description for the file.
7. Select **UPLOAD**.

Reset OnPortal for the Next Site

1. Go to **Locking plan overview**.
2. Click **RESET**.
3. Click **OK**.
4. Verify OnPortal restarts and prompts for site license files.

Reset OnPortal Locking Plan

1. Click **LOCKING PLAN**.
2. Select **RESET**.
3. Select **OK**.

OnPortal restarts and prompts for site license files.

Create or Edit Rooms

Create and edit single rooms or in a batch.

- Batch edit multiple doors on multiple floors to create ADA rooms
- Batch edit multiple doors with similar individual characteristics
- Create *Selective*, *Related* or *Extended suite* rooms
- Create foyer doors, etc.

Add a Single Room

1. Click **ADD**.

***Note**: The room type cannot be changed after saving. It is important to set room type first and correctly before enter anything, see the Room Types section below for more information.*

2. From the *ROOM TYPE* drop-down menu, choose the room type first.
3. Enter a room name.
4. From the *LOCK PROFILE* drop-down menu, choose the lock profile.
5. Change the details for the room type, as required, see the *ROOM TYPES* section below for more information.
6. Click **SAVE**.

Edit a Single Room

1. Click the room to edit.
2. Change the details, as required.
3. Click **SAVE**.

Create ADA Rooms

Americans with Disabilities Act (ADA) is the term used to describe a room that is accessible for those with disabilities. This includes a delayed time that the door stays unlocked when opening. Various ways exist to make a room into an ADA room. Any door may be an ADA door, and any room type may be an ADA door.

1. Click **LOCK PROFILES** to designate all rooms in that profile are ADA rooms or go into **ROOMS** edit the room and change the profile to the ADA profile.
2. Click the profile or room to edit.
3. Change the value in *OPENING DELAY* to **15**.
4. Click the wheelchair symbol next to *OPENING DELAY*.
5. Click **SAVE**.

Edit a Batch Room

Batch edits can only change fields with the EDIT icon next to them.

1. In *LOCKING PLAN*, click **Rooms** and click all the rooms to edit.
2. Click **EDIT** at the bottom of the screen.
3. Verify the door names selected appear at the top of the screen.
4. Click the **EDIT** icon in front of the field and edit the field, as required.
5. Click **SAVE**.

Room Types

Room types may have different requirements when creating or editing. In the following information, is for a room that is being added using the ADD icon.

***Note**: The room type cannot be changed after saving. It is important to set room type first before enter anything.*

SELECTIVE

If you copy a *SELECTIVE* room after adding in the children, the copy gets all of the children automatically. Best practice is to create copies for each public door, and adjust the profile, timetable, and authorizations as required.

1. When creating rooms, from the *ROOM TYPE* drop-down menu, choose the room type first.

***Note**: Using a profile that is for foyer doors, for example, is unwise because they usually have no master types assigned to them.*

2. Verify the lock profile has *Master Keying* for the lock.
3. Click the **CHILD ROOMS** tab.
4. Click the **EDIT** icon next to *Search*.

***Note**: Selecting a lock profile includes all of the guest rooms, suites, and sub-suites linked to that profile.*

5. In the room selection screen, click each individual room or select a lock profile.
6. Click **SAVE** on the *CHILD ROOMS* tab.
7. Click **SAVE** on the *ROOM DETAILS* tab.

RELATED

1. From the *ROOM TYPE* drop-down menu, choose **RELATED**.

***Note**: The characters used are: $ = A card lock safe is in the room, * = Card locked wet bar or refrigerator, and % = Other card locked hardware.*

2. Enter in one character to signify the related room the following Onity standard characters.
3. Click a lock profile.
4. Choose the timetable, authorizations, and if it needs a to use a programming card.
5. Select the default master card that can access the lock.
6. Click the **CHILD ROOMS** tab.
7. Click **EDIT**.
8. Click each individual room or select a lock profile.
9. Click **SAVE** on the *CHILD ROOMS* tab.
10. Click **SAVE** on the *ROOM DETAILS* tab.

FOYER

1. From the *ROOM TYPE* drop-down menu, choose **FOYER**.
2. Enter in the room name.
3. From the *LOCK PROFILE* drop-down menu, choose the lock profile (Foyer).
4. Choose the timetable, authorizations, and if it can have office mode.
5. Click **SAVE**.

Create ADA Lock Profile

Create

1. Click **LOCKING PLAN**.
2. Click **ROOMS**.
3. Click **ADD** to create the room details.
4. Next to *OPENING DELAY*, click wheelchair icon and add or decrease the opening delay time.
5. Click **SAVE**.

Edit

1. Click **LOCKING PLAN**.
2. Click **ROOMS**.
3. Slide the Single bar to **Batch**.
4. Click rooms to edit.
5. Click **EDIT**.
6. Next to *OPENING DELAY*, click the **EDIT** icon.
7. Click the wheelchair icon and add or decrease the opening delay time.
8. Click **SAVE**.

Batch Edit Rooms in OnPortal

Batch edits can only change fields with the *EDIT* icon next to them.

1. In *LOCKING PLAN*, click **Rooms** and click all the rooms to edit.
2. Click **EDIT** at the bottom of the screen.
3. Verify the door names selected appear at the top of the screen.
4. Click the **EDIT** icon in front of the field and edit the field, as required.
5. Click **SAVE**.

Create Rooms Within a Lock Profile

All master keying in OnPortal is done within a lock profile. Create every room possible using the following method. For sites with less than an expected 1000 rooms + master users, use *Selective* lock types for public doors, which allows for master canceling (foyer doors do not). For selective locks, related locks, and extended suites, note which lock profile to use based upon the master types needed or create an individual profile for those doors. **Best Practice**: Create a *Selective-No Auto* profile for doors without an automatic opening, and a *Selective-Auto* profile for doors with an auto opening. The majority of public doors should be *Selective* doors (create those named doors under ROOMS and select the appropriate profile).

1. Click **LOCKING PLAN** and **LOCK PROFILES**.
2. Click a guest room lock profile.
3. Click the **ROOMS** tab.
4. Click the plus (+) sign to add in successive room numbers.

***Note**: First, use to add a single named room to a profile. Second, use to create successive doors that have a prefix. Most hotels do not require a root to the names. An example of a root is if the Keying Form shows room names like B101-B160, the root would be B.*

5. In *ROOT OF NAMES*, enter the name of the room.

***Note**: Verify the room type before saving the rooms, the room type cannot be changed except by deleting the room and adding it back in correctly. **REGULAR** = Any door that opens only for a card made for it or the door's master keying. **FOYER** = Do not use for sites with less than 1000 rooms and master users. **SUITE** = Doors that must allow a set of cards for a door behind them to enter. Suites and sub-suites are listed on the Keying Form. If SUITE is selected, the number of sub-suites is required.*

6. Choose a room identifier.

NUMERIC	These numbers appear immediately after the root of names. Check the box for NUMERIC. Enter the first consecutive room number for this profile in the FROM box. Enter in the last consecutive room number for this profile in the TO box.
ALPHA	The alpha letters appear immediately after the root of names. Check the box for ALPHA. Enter in the first letter of the alphabet used in the FROM box. Enter in the last letter of the alphabet used in the TO box. FROM A to D will

	create rooms 100A, 100B, 100C, and 100D with 100 as the root.
FIXED	The text becomes a suffix to the root of names. Check the box for FIXED. Enter in the text that will appear as a suffix on all the doors. Click VIEW to view the room names generated by the selections. If the rooms names are correct, click SAVE.
NUMERIC + ALPHA	It does not matter which order you check the boxes. If both are checked the root of names, followed by a number, followed by the alpha, the next room has the next alpha until all alphas are used, then the number steps one and begins with the alphas again.
NUMERIC + FIXED	Same as NUMERIC, except every room has the FIXED text as a suffix to the name.
ALPHA + FIXED	Same as ALPHA, except every room has the FIXED text as a suffix to the name.
NUMERIC + ALPHA + FIXED	Same as NUMERIC + ALPHA except every room has the FIXED text as a suffix to the name.

7. Click **SAVE**.
8. Repeat steps to create rooms on other profiles.
9. Click **SAVE**.

Error Codes

This area lists some error codes and their resolutions. See the *Onity OnPortal Lock Management System Installation Guide, 10104944P1* for more error codes.

Error Code	What this means and actions to take
Administrator Privilege Required	Administrator privileges are required. Sign in as an administrator.
APICall_ClientCertInvalid	The API call client certification is invalid. Verify the or reinstall the certificate.
APICall_InvalidURL	The API call has an invalid URL. Verify the URL and retry. If the error continues, call Tech Support.
APICall_ReturnType InCorrect	The API call return type is incorrect.
APICall_Server CertInvalid	The API call server certification is invalid. Verify the or reinstall the certificate.
APICall_Unauthorized	The API call is not authorized.
APICall_Unsuccessful	The API call was unsuccessful.
APICall_Unsuccessful_ NotServer	The API call was unsuccessful, not the server.
Authentication_ NotFound	Authentication was not found.
Authorization_ NameRequired	The authorization name is required. Add the authorization name and

	retry.
Authorization_ NotFound	Authorization was not found.
Backup_Already Installed	Backup is already installed. No action required.
Backup_Failed	The backup has failed.
Card_InvalidCode	The card code is invalid.
Card_MasterCard DoesNotExist	The master card does not exist.
Card_NoRooms	
Card_NoSafe EmergencyCard	
Card_NotFound	
Card_Redundant GuestCardNot Allowed	
Card_RFIDSector NotSupported	The RFID card sector is not supported.
Card_TooMany Rooms	There are too many rooms for this card.
Card_TooManySingle OpenCards	There are too many single open cards.
Card_UnIdentified	This is an unidentified card.
ChangePassword _Invalid	The password change is invalid. Try to change the password again using the password requirements. Passwords must have 8 to 32 characters, and at least one: uppercase letter, lowercase letter, number, and symbol.
Configuration_ EncoderReset Unsuccesful	The encoder reset was not successful.
Configuration_ EncoderTest Unsuccesful	The encoder test was unsuccessful.
Configuration_ No Master Users With Encoded Cards Have Been Found_You Must Have An Existing Master User Card Before CreatingA_MIFARE Plus Configuration Card	There were no master users with encoded cards found. An existing master user card is required before creating a MIFARE Plus configuration card.
Configuration_PleaseProvideA_NameForTheNode	Provide a name for the node/station.
Configuration_ PleaseSelect A CardTechnology ForThe Encoder	Choose a card technology for the encoder.
Configuration_SaveOr CancelCurrent Encoder Details_ ToAddNnewEncoder	Save or cancel the current encoder details to add a new encoder.
Configuration_Test Failed_ Please Check Your Configuration	The test failed, check your configuration.
Configuration_ The License You Are Importing Is For A_ Different site Code _You Must Be An Onity Tech To Make This Change	The license you are importing is for a different site code and you must be an Onity Tech to make this change.
Configuration_ There IsNo WallreaderSelected	A wall reader must be selected.
Configuration_TheSelected WallreaderDoes NotCurrentlyHave A_WallreaderSetings ThusYouMay NotUpdateIt	The wall reader does not have the settings feature and cannot be updated.

Convert_DateTime	Convert the date and time.
CTCom_Wrong_Port	The wrong port was used for CT communication.
DB_Blank	The database is blank.
DB_PasswordNotSet	The database password has not been set up.
Device_HTCOM_FailedToAddress	The HT device communication address has failed.
DeviceScan_InProgress	A device scan is in progress.
DirectKey_ConfigNotTested	The DirectKey configuration was not tested.
DirectKey_DatesRequired	The mobile key dates are required.
DirectKey_EmailConfirmError	The mobile key email confirmation failed.
DirectKey_EmailInvalid	The guest email address to set up the DirectKey mobile key is invalid.
DirectKey_ GetAccess CategoriesFailed	The Get Access Categories function failed for the DirectKey.
DirectKey_GetAuthCodeFailed	Getting an authorization code for the DirectKey failed.
DirectKey_GetDeviceNamesFailed	The DirectKey device name has failed.
DirectKey_ GetKeyDevice ActivityFailed	The DirectKey Get Key Device Activity function has failed.
DirectKey_ GetKeyDevice PermissionsFailed	The DirectKey Get Key Device Permissions function has failed.
DirectKey_ GetMyAccountFailed	The DirectKey Get My Account function has failed.
DirectKey_GetOwnersFailed	The DirectKey Get Owners function has failed.
DirectKey_InvalidCert	The DirectKey Invalid Cert function has failed.
DirectKey_InvalidKeySerialNumber	The DirectKey Invalid Key Serial Number function has failed.
DirectKey_KeyNotCreated	The DirectKey was not created.
DirectKey_KeyNotFound	The DirectKey was not found.
DirectKey_KeyOwnerNotFound	The DirectKey mobile key owner was not found.
DirectKey_NotConfigured	The DirectKey mobile key is not configured.
DirectKey_NotConfigured_AccessCategories	The DirectKey access categories are not configured.
DirectKey_PermissionDeleteFailed	The DirectKey Permission Delete function failed.
DirectKey_PermissionPostFailed	The DirectKey Permission Post function failed.
DirectKey_PropertyNotConfigured	The property was not configured for the DirectKey mobile key.
DirectKey_PropertyNotFound	DirectKey Property was not found.
DirectKey_Push Notification RequestFailed	The DirectKey Push Notification Request function failed.
DirectKey_ResetKeyFailed	The DirectKey Reset Key function failed.
DirectKey_SendInviteFailed	The DirectKey Send Invite function failed.
DirectKey_StayDatesRequired	The Stay Dates for the DirectKey mobile key are required.
DirectKey_StayEmailRequestFailed	The DirectKey Stay Email Request function has failed.

DirectKey_UINotSupported WithKeylessPermissions	DirectKey UI doe not support keyless permissions.
DK_APIException	The DirectKey API call failed.

See also:

Troubleshooting

Troubleshooting

System Set Up

Issue	Explanation or Action
HT22 locking plan import	Some customer databases have back office rooms names with 8 character lengths. In OnPortal, back office room names are trimmed to 7 characters when imported HT22 LP. If we try to perform any PP action for room names greater than 7 character, an error *Data for this room not loaded* displays after importing HT22 LP to OnPortal. Re-initialize all rooms with names greater than 7 characters.
System says it is not connected	A cable may have been disconnected. Verify all of the connections to the system are secure.

Encoder Driver

Issue	Explanation or Action
Window 10 machine not detecting the USB encoder device	When SecureBoot is enabled, the driver doesn’t work with windows 10. There is currently a fix being worked on from the manufacturer.

See also:

Error Codes

Glossary

C

Customers

A customer is typically the parent company of the site. A customer may have many sites under it. Customers and sites may have different account numbers.

D

DirectKey

DirectKey mobile application and Bluetooth enabled locks allow a user to open the lock with a smart phone using secure Bluetooth communication

F

Files Tab

This are is where you can upload site plans, locking plans, installer files, and firmware updates.

L

License

A license is required for the operation of the OnPortal system.

O

Operators

Operators have access to the software management (Installers, System administrators)

P

Pre-License

A pre-license is required if the customer information is set up prior to the installation of the OnPortal system. A pre-license will enable a site to operate OnPortal for 30 days.

R

Regular Encoder

Use Regular encoder mode to make keys from the OnPortal UI or a PMS interface.

S

Site code

The site code is a unique set of letters and numbers used to match keys with the customer lock system.

Sites

Sites are defined as the property location for a customer.

T

Terminal Encoder mode

Use Terminal encoder mode to use the keypad of the HT22 encoder to create the keys.

Index