SOFTWARE MANUAL

ProxessIQ™ Software & Proxess Sync™ Mobile App Configuration

Equipment & Network Needs

In preparation for the system software download and hardware installation & configuration:

Here are the Computer & other required system components:

- **Minimum Computer Spec** (for each ProxessIQ™ server and client), Windows 10+ Pro, Intel 12th Gen 2GHz, 1 USB input, 8GB RAM, 256GB hard drive, 40GB free disk space.
- For **Larger Systems**; 12 Generation Intel Core i7, 16MB RAM, 512GB HD, .NET 4.8.
- *It is strongly recommended to pre-install Microsoft SQL Express 2022 on the Server PC prior to downloading the ProxessIQ™ software. Consult Proxess for very large systems.*
- Network or Internet connection for the PC, depending on the Proxess Sync™ connection method
- Common WiFi connection to ProxessIQ™, or mobile plan with connection to the ProxessIQ™ network
- ProxessIQ™ software Download link: www.proxess.com/downloads
- USB Enrollment Reader
- Apple or Android Smart Phone
- Proxess Sync™ Download link
- Router for DNS comms to controllers, or switches for static IP & WiFi comms
- USB-to-Serial cable for custom controller configuration

Ports to be opened for client and IP controller communications:
- TCP 8008-8011 (client-to-server software comms), TCP 8031 (controller comms to the software) & UDP 8032 (controller beaconing)
- Note: The IP Controllers/Gateways may be configured to communicate over ethernet and/or WiFi

Website URLs to be **white-listed**:
- Bi-directional communications for Mobile Keys: Outbound for initialization and changes and Inbound for audits and events & Notifications: https://pmcs.proxess.com
- "Dumb" remote synchronization app, which can be enabled & disabled with a click in the software anytime that it is to be used: https://proxy1.proxess.com
- The back-up: https://proxy2.proxess.com

Email to be **white-listed**, for Mobile Key& Notifications receipt:
- DoNotReply@email.Proxess.com

Firewall Settings

Please prepare/enable your firewall to accept the following.

This is a summary of the firewall rules that the Proxess software installer attempts to create:

```
<fire:FirewallException Id="ProxessControllerCommunication"
    Name="Proxess Controller Communication"
    Protocol="tcp"
    Port="8031"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessControllerBeacon"
    Name="Proxess Controller Beacon"
    Protocol="udp"
    Port="8032"
    Scope="localSubnet"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessServerSecureCommunication"
    Name="Proxess Server Secure Communication"
    Protocol="tcp"
    Port="8009"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessServerOpenCommunication"
    Name="Proxess Server Open Communication"
    Protocol="tcp"
    Port="8011"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessIdentityServer"
    Name="Proxess Identity Server"
    Protocol="tcp"
    Port="8008"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
```

This is

- **Software Installation:** Instructions for downloading and installing the ProxessIQ™ software; both server & clients.

- **Licensing:** Add and upgrade licenses for ProxessIQ software and Mobile Credentials/Keys.
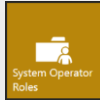
- **System Operator Roles:** Define the grouping for view\edit\delete rights for each software module.
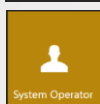
- **System Operators:** Add operators into an Operator Role. Modify\personalize their role.
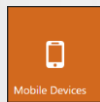
- **Mobile Devices:** Add mobile phones which will operate the Proxess Sync simple configuration App.

- **IQ Mobile / Proxess Sync™:** Sign in and enable the Proxess Sync™ simple configuration App on your Apple or Android Mobile Phone.
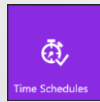
- **Time Schedules:** Create the days and times that locks and doors will operate with credentials and remain locked or unlocked.
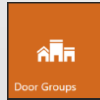
- **Door Groups:** Create groups of Doors, for more easily assigning access rights to users.
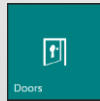
- **Doors:** *Adding, programming & editing* wireless locks and online doors.
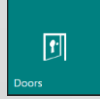
- **Doors & Door Groups:** *Mass-Adding*\Modifying\Deleting Doors & Door Groups using a .csv spreadsheet
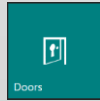
- **Doors:** *Controlling* Online & Bridged doors.
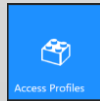
- **Access Profiles:** Create groupings combining Time Schedules with Doors and Door Groups.

This is

- **Controllers:** Define online\checkpoint doors\readers.

- **Users:** Add\Modify\Delete credential holders and their **PHYSICAL** credentials (cards, keychain fobs, stickers, watches), including custom Advanced Searches.

- **Users:** Add\Modify\Delete credential holders and their **MOBILE** credentials (Apple & Android phones).

- **Users:** **Mass-Adding**\Modifying\Deleting Users & Credential using a .csv spreadsheet

- **Database Exports:** Exporting data from the SQL database, supplementing the "Export" buttons in Users, Doors & Door Groups

- **Encoding & Deleting:** Using the **ProxessIQ Software** to Encode & Delete credentials

- **Encoding & Deleting:** Using the **Proxess Sync** phone app to Encode & Delete credentials

- **Calendars:** Schedule Holidays and special events, years in advance.

- **Credentials:** Simpler management utility for credentials, after a User is created in Users menu, including custom Advanced Searches

- **Notifications:** Set Email alerts based on virtually any system event.
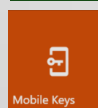
- **Mobile (Phone) Keys:** Administrative management of Mobile Keys/Credentials (Note: Issuance typically occurs in the Users menu).

This is

ProxessIQ™ Quick Start Guide - 3
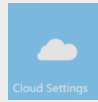
- **Cloud Settings:** Communications management between ProxessIQ server and the Mobile Credential Cloud.

- **System Schedules:** Aggressive Event & Audit pulling

- **Settings:** Define system and operational attributes, including for door, reader, LED and credential operations.

- **Logs:** All User & Door event logs are available here and may be searched using multiple custom Boolean rules , with custom Advanced Searches.

- **User Interface:** Arrange and hide Module icons and UI color schemes.

Click on a Menu item for Instructions
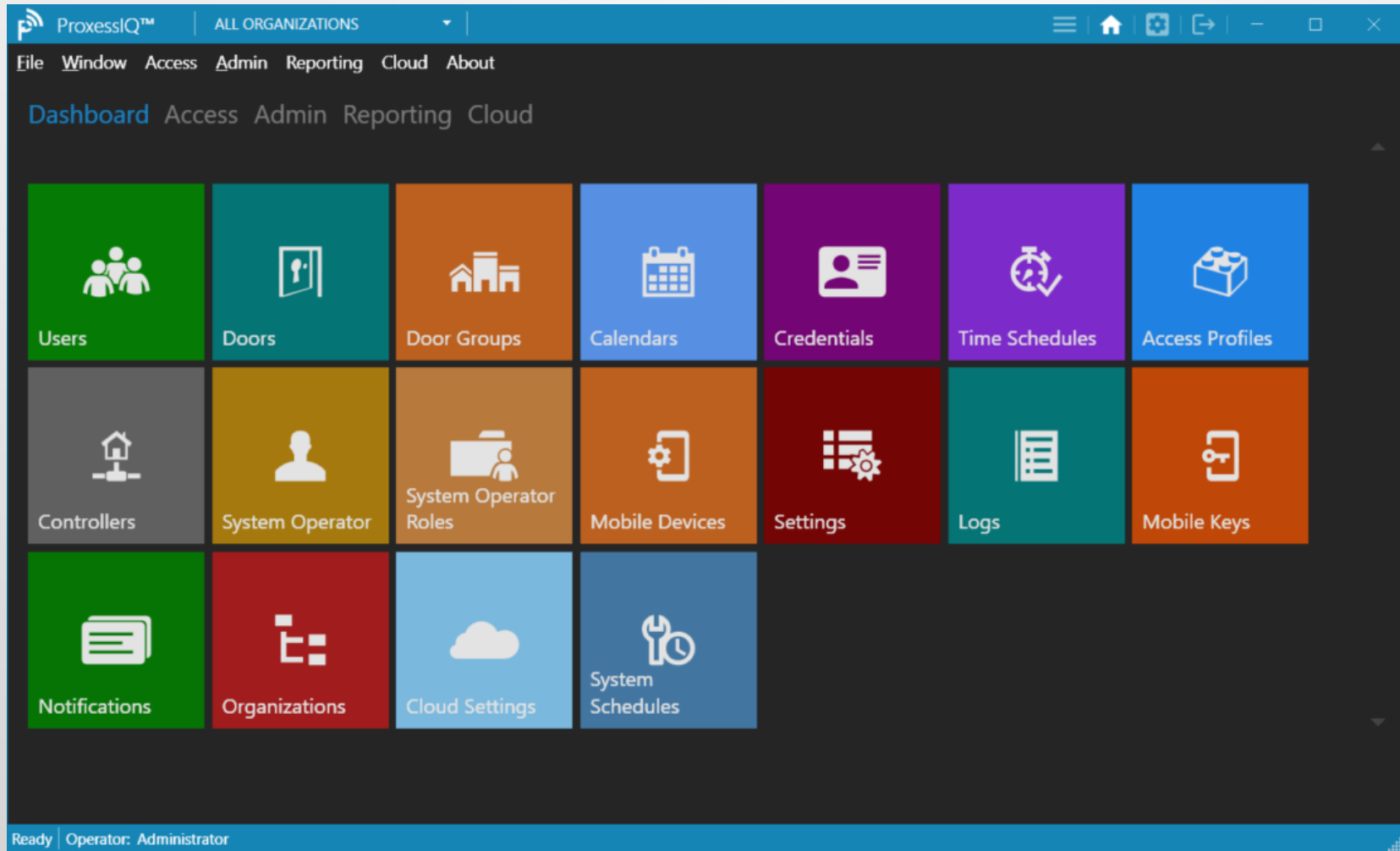
SOFTWARE
DOWNLOAD & INSTALLATION

Which software do I download for a Basic system?

From the links provided at www.Proxess.com/Downloads if your system is described on this page, then on the computer that will be your primary (the "server") you will download and install "**Proxess-Server-Installer-LocalDB-Bundle.exe"**. On all other computers (unlimited), you will only install "**Proxess-Installer-Client.msi"**

Follow the instructions in this section if this describes your system.

There will be only 1 (one) computer (laptop or desktop) used for configuration and data entry.

OR

There is 1 (one) main computer (laptop or desktop) used for data entry and one (1) or more additional computers may be used for configuration and data entry, either now or in the future.

PC SPEC (minimum):
Intel Core i5, 2GHz
8MB Cache
8GB RAM
256GB Hard Drive

Primary computer ("Server"):
Install "**Proxess-Server-Installer-LocalDB-Bundle.exe"**

Additional computers ("Clients"):
Install "**Proxess-Installer-Client.msi"**

Locate the download link provided at www.Proxess.com/Downloads or which has been emailed or otherwise provided to you by the Proxess support staff or sales team.

For basic and small-to-medium sized systems that choose to use the Proxess built-in "LocalDB" database (a Microsoft database product), you will install the file from the top section (in the version depicted below, 1.5.2.1) "ProxessIQ_Server_Installer_LocalDB_**Bundle**.exe".

This file will install both the server and client (system programming user-interface) applications onto the computer. This "bundle" can only be installed on one computer per system, but the Client download files can be loaded onto several other computers, which will be used as administration workstations.

Click on "**Proxess-Server-Installer-LocalDB-Bundle.exe"** and, if prompted, click on "Download" on the screen that opens.

www.Proxess.com/Downloads

Note on Upgrading Versions:
When upgrading the version of your ProxessIQ™ software, be certain to upgrade the server as well as all the clients to the same version, or there could be functions that do not operate properly.

Note: 1.4 versions are for support of Legacy systems **Only**

Alternatively, for systems where the server computer will Not be used as an administrative terminal, click on the 1.5.x **Server** file (instead of the Bundle). All the subsequent administrative workstations will have the Client file installed, as discussed above.

Per the previous page, click on "**Proxess-Server-Installer-LocalDB-Bundle.exe"** to begin the file download.

There are 3 automated wizards that will guide you through each the **download bundle,** the **server** installation and the **client** installations. At the completion of all 3, the Server program, ProxessIQ™ Control Center will launch.

This is the **Download Bundle** installation wizard:

Follow the windows that open and prompts that appear on this page. Depending on your computer's settings, some of these windows may not appear and can be ignored.

The icon below may blink in your computer's taskbar. If so, click on it to proceed.
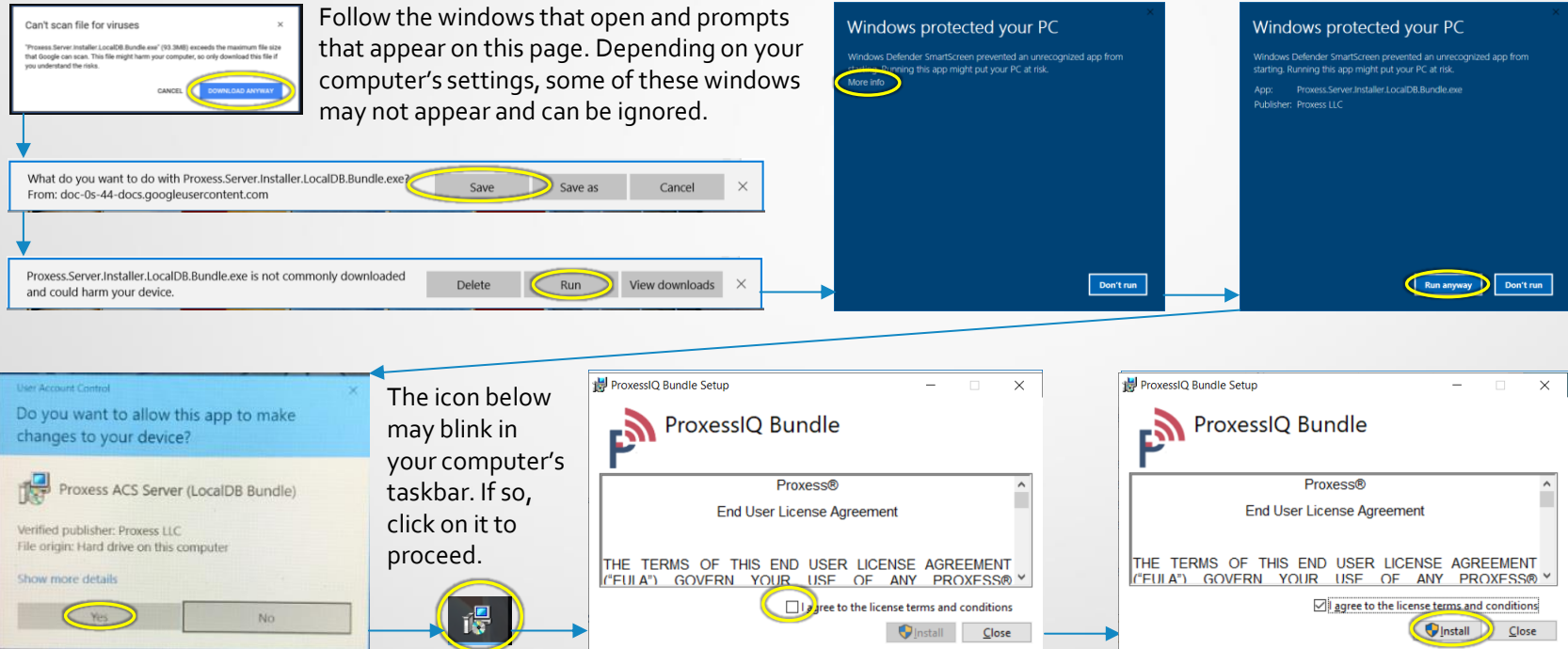
This is the **Server Installation** installation wizard:
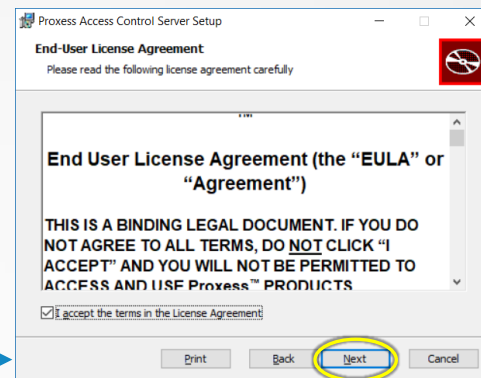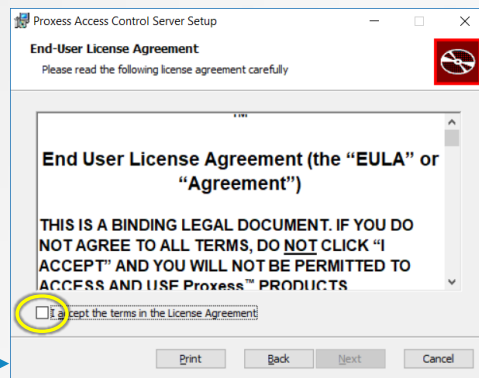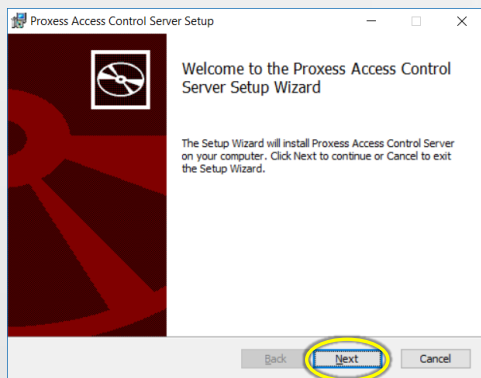
Continue following the windows that open and the prompts that appear on this page.

Note: Only click "Existing" if you are upgrading the version of your ProxessIQ™ system.
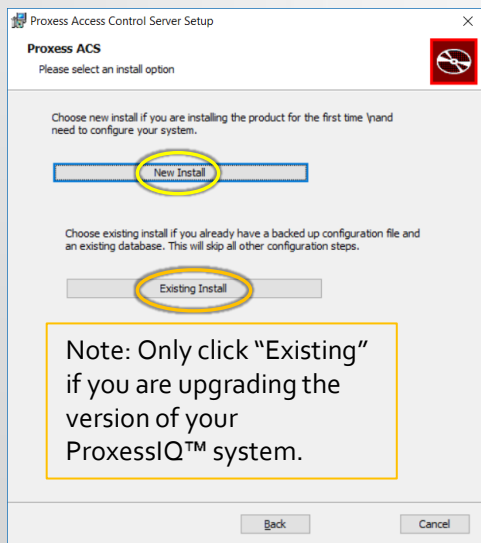
Click "New Install". Only click "Existing Install" if you are upgrading the current version of your system.
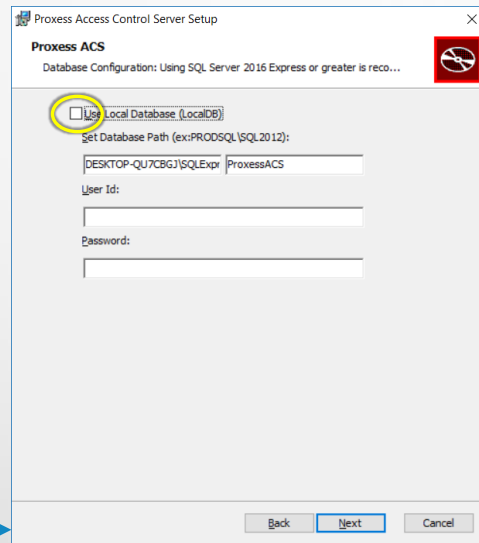
Check the box to Use LocalDB and do not change the path that appears.
Only set a different path if you have already installed SQL Express and will take responsibility for its maintenance.
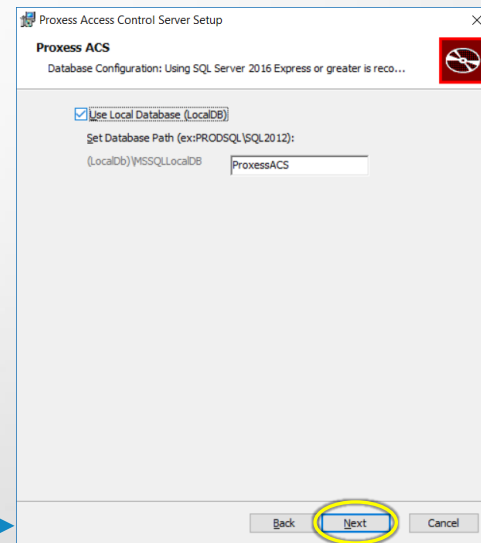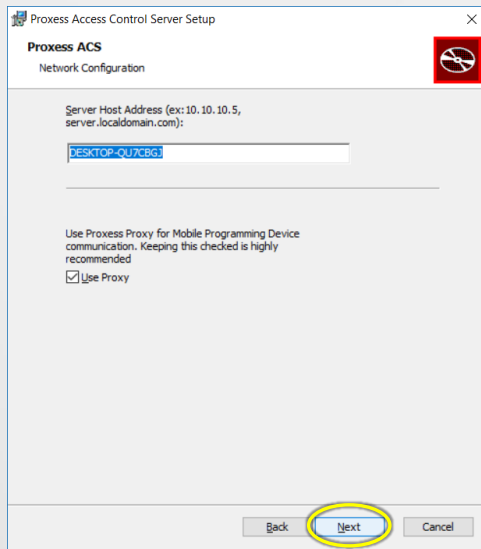
Do not change the default server address or name, unless you are prepared take responsibility for the resulting network connectivity.
Leave "Use Proxy" checked.
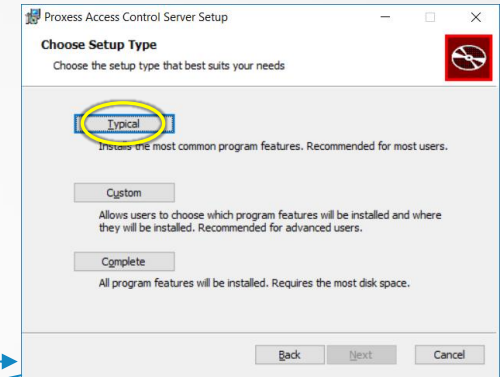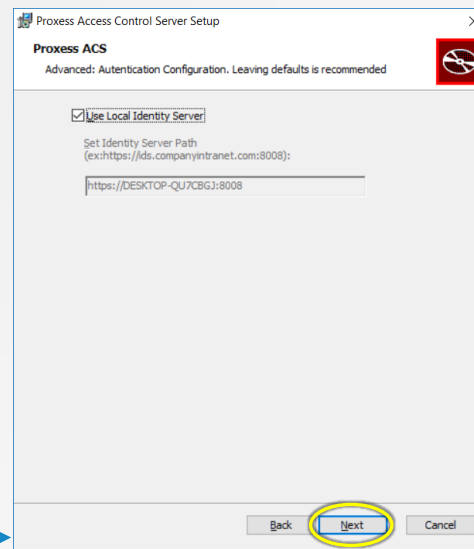
Select "Typical", unless otherwise discussed with Proxess.
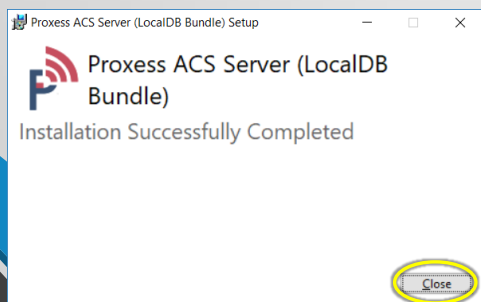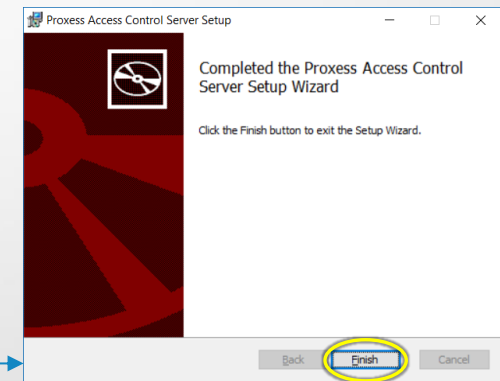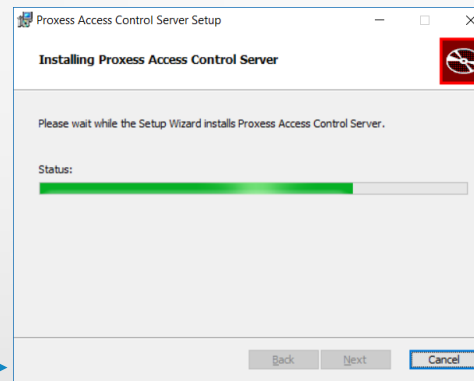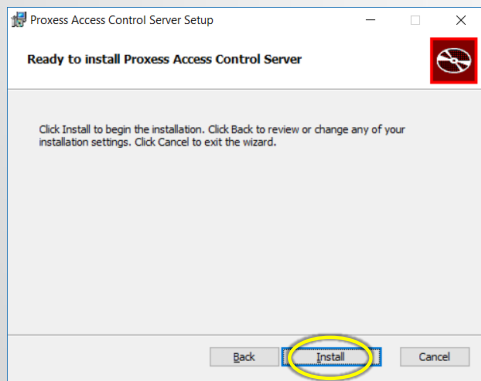
Initializing the Server

Recently added

ProxessIQ

ProxessIQ Control Center

Type here to search

User Account Control

Do you want to allow this app to make changes to your device?

Proxess Configuration Manager

Verified publisher: Proxess LLC
File origin: Hard drive on this computer

Show more details

Yes   No

PROXESSIQ™ CONTROL CENTER

Server Status
Server Settings
Self-Signed Certificates
Identity Server Config
Service Configuration
Certificate Bindings
Active Directory Config
Web API Config

Server Status

Start Proxess Service   Stop Proxess Service

Server Status: Running
Server Version: 1.5.2.101

Client Configuration

Get Client Configuration File   ☐ Include Root Certificate Export

Backup Utilities

Create Local Database Backup   Backup Server Config

Logs

View Server Logs   Export Server Logs

Additional Details

Server Location: C:\Program Files (x86)\Proxess\Server\
Database Server: (LocalDb)\MSSQLLocalDB
Database Name: ProxessIQ

Both the "Server" and "Client" portions of the software have now been installed on your computer.
It is good practice to follow the steps on this page, which will assure that the essential Server services are running on this computer.

Press the Windows™ icon on the keyboard or click on the Windows™ icon on the left side of the Taskbar on the bottom of your screen. Locate and click on the "ProxessIQ™ Control Center", which will be in both the "Recently Added" section of the pop-up list of programs, as well as under the "P" section down below. If prompted with the window requesting to make changes to your computer, click "Yes".
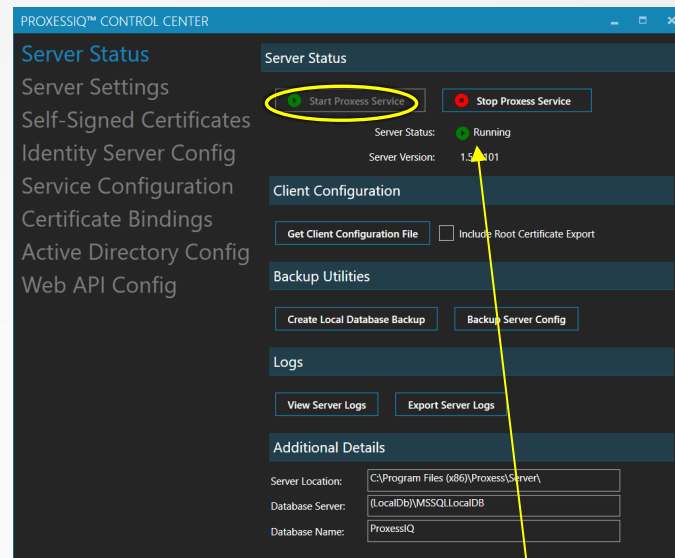
The above screen will open. If the Server Status is shown as "Stopped" then click on "Start Proxess Services".

PROXESSIQ™ CONTROL CENTER

Server Status
Server Settings
Self-Signed Certificates
Identity Server Config
Service Configuration
Certificate Bindings
Active Directory Config
Web API Config

Server Status

Start Proxess Service   Stop Proxess Service

Server Status: Running
Server Version: 1.5.2.101

Client Configuration

Get Client Configuration File   ☐ Include Root Certificate Export

Backup Utilities

Create Local Database Backup   Backup Server Config

Logs

View Server Logs   Export Server Logs

Additional Details

Server Location: C:\Program Files (x86)\Proxess\Server\
Database Server: (LocalDb)\MSSQLLocalDB
Database Name: ProxessIQ

Usually within several seconds (and upwards of about a minute) after clicking "Start Proxess Services" the Server Status will change to "Running". We will now proceed to initiate the software.
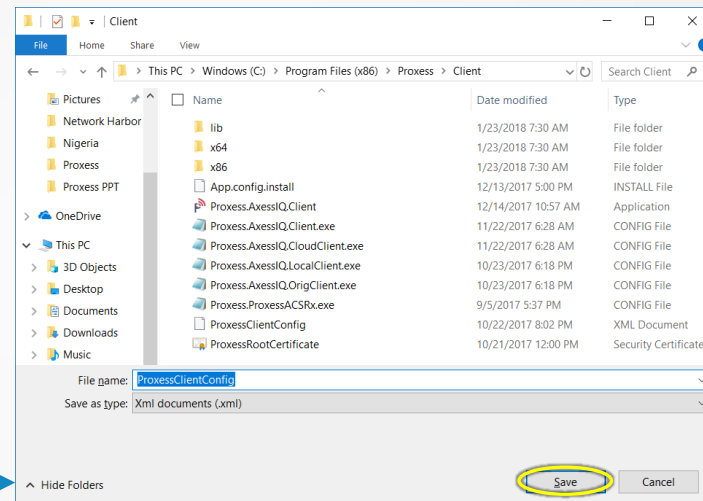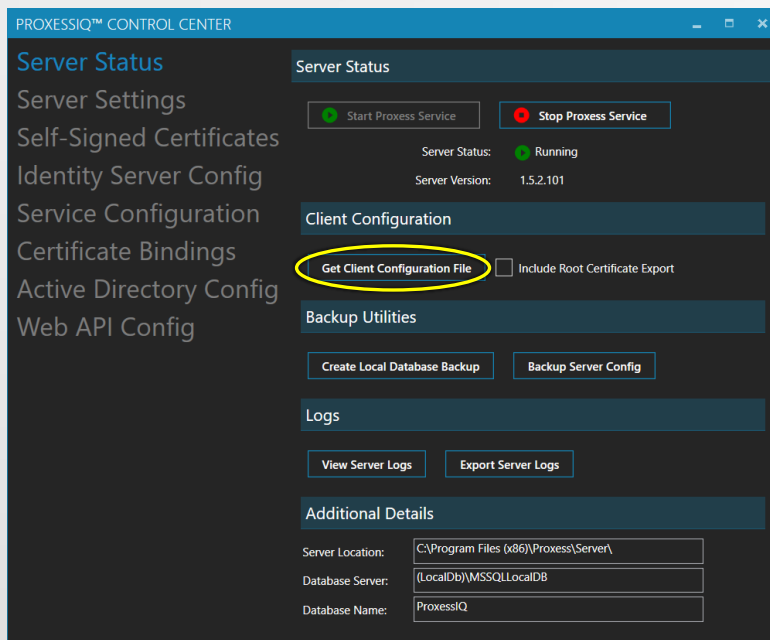
Click the "Get Client Configuration File" button.
On the "Save As" screen, navigate to the following (preferable) folder location to save the file in:
"This PC \ Windows (C) \ Program Files (x86) \ Proxess \ Client".
Click the "Save" button.
Click on the "x" on the top right of the ProxessIQ™ Control Center window to close the application.
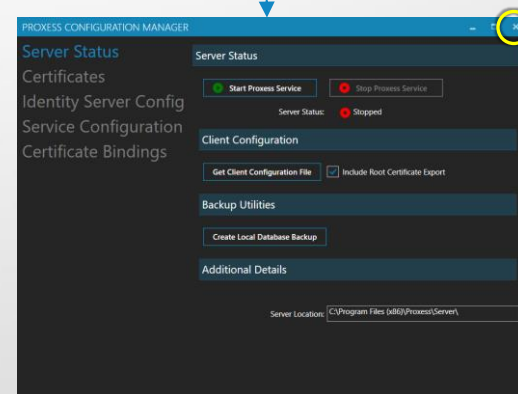
Note: It is important to keep the Proxess Services Running at all times and especially to enable it to automatically start-up upon a restart of the computer.

Initializing the Client
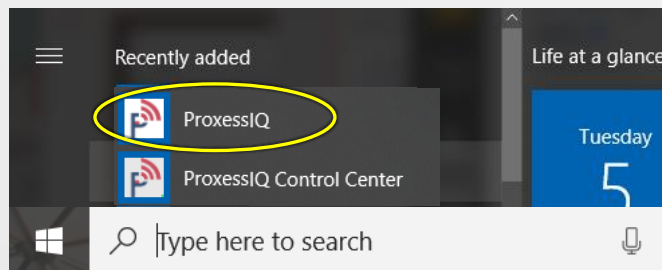
Click the "Windows" icon on your computer and select the "ProxessIQ" program and allow the app to make changes to your device.
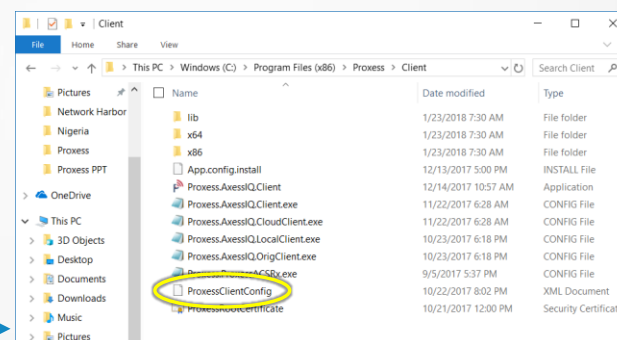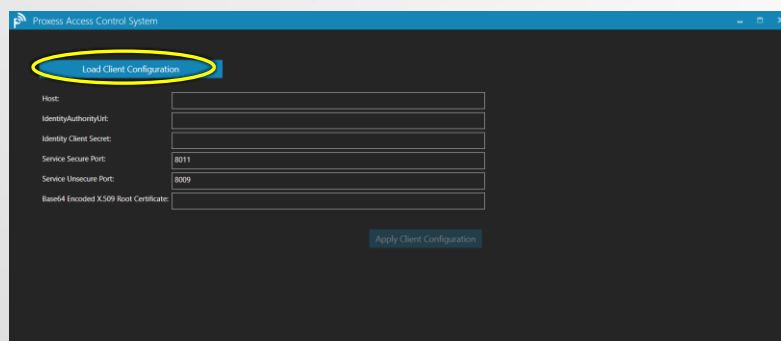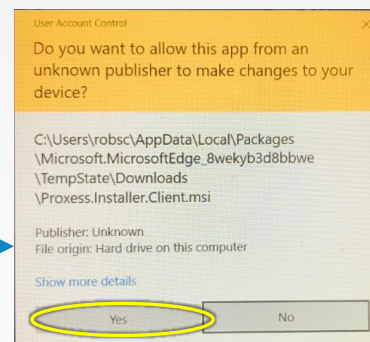
NOTE: Other than as stated here, do not make any changes to these screens. Click the "Load Client Configuration" button on the first screen. If you have not yet pasted it into the Client folder, you will be asked to search for the Configuration file, which may be found in the file folder you saved it in. Click on it.
On the next screen (below), click the "Apply Client Configuration" button.
The Login screen will open. Enter "**administrator**" and "**proxess**".
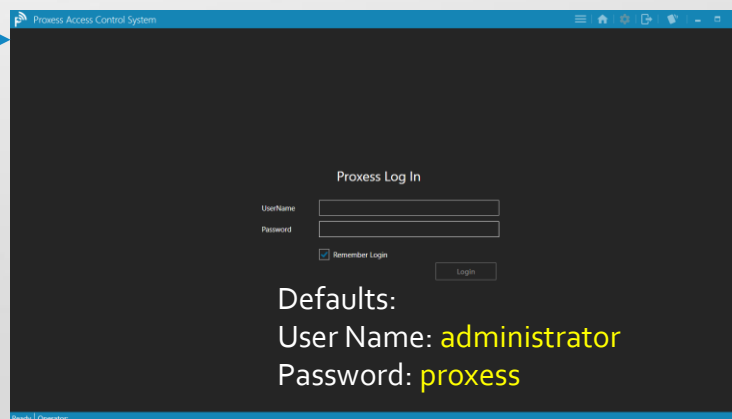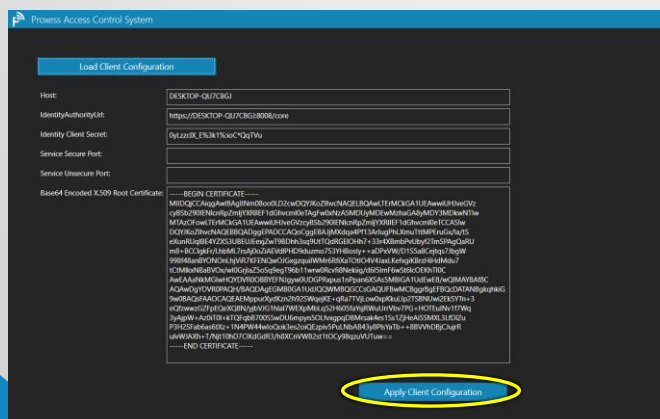
Defaults:
User Name: administrator
Password: proxess

You will now be prompted to change your password, which is strongly recommended, but not required.
One option is to get familiar with the software and configure it and get a second administrator trained before changing the default password.
Please do not take either of these options lightly and be certain to **SAVE YOUR PASSWORD** !!
The ProxessIQ™ software will now open.
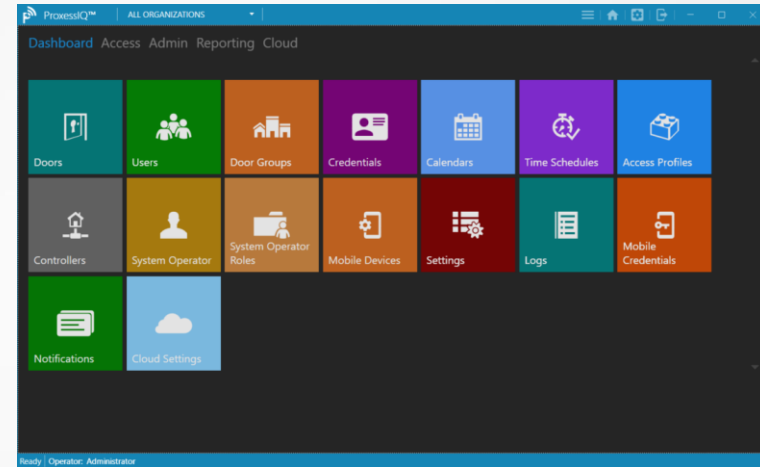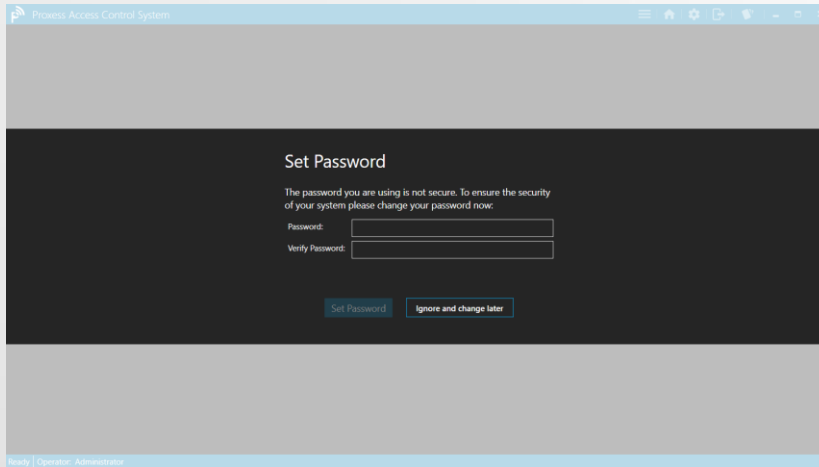
After installing the ProxessIQ™ software, you may add the icon
to your taskbar and\or desktop.

The following section will guide you through adding a License Key for ProxessIQ and for Mobile Credentials/Keys.

Assuring Software Clients Connect to the Server

Resolving Local Host Names

When using the computer name for a server's host name, any client trying to access the server will need to be able to resolve that host name. In a local network environment this happens automatically through either local DNS (typically in a domain environment) or through NetBIOS name resolution. If you are attempting to connect to the server's host name outside of your local network environment, these name resolution methods will not be available. The simplest approach for creating this mapping is to **create an entry for the host name in the local host file of the client computer that is attempting to reach the server**.

The Windows Host file is located at c:\Windows\System32\Drivers\etc\hosts. To make edits to this file, you will need to open the file with a simple text editor (like Notepad) with administrator privileges (Right-Click and select Run as administrator). The host file does not have an extension (.txt) so you will need to select "All Files (*.*)" in the file Open dialog. Once the host file is open, you will need to create a new line that contains the routable IP address followed by the computers host name. Assuming this is outside the internal network, this will need to be the public IP with proper routing/NAT rules setup. For example, if your public IP is "123.456.0.100" and your server's host name is "myservername", the host file entry should look like this:

123.456.0.1   myserversname

A robust alternative to this is to use a registered domain name with a public DNS record for your server's host name.

NAT/Port Forwarding

To connect to a server inside a local network from outside of the local network, you will need to set up the appropriate NAT or Port Forwarding rules on your gateway /firewall. These rules need to provide a path from the public IP (provided by your ISP) to the internal network IP for all ports required for communication to the AxessIQ server. The default ports that are used for this communication are 8008, 8009, and 8011. Setting up NAT/Port Forwarding rules will be specific to your gateway manufacture. Please refer to the manufactures documentation for setting this up.

Example documentation for setting up port forwarding on a Comcast gateway can be found here:
https://www.xfinity.com/support/articles/port-forwarding-xfinity-wireless-gateway

Assuring Software Clients Connect to the Server

When the Computer Host Name Changes

When the Host Name is changed (on purpose or accidentally…) you will need to:
- Edit all the values in the ProxessIQ Configuration File, changing the old to the new name
- Reload the config file, or change it manually in the "Load Client Config File" screen
- In ProxessIQ Control Center, change the old to the new Host Name in the Certificate Bindings

When a computer changes from a Wired to a WiFi connection:
- When a computer changes from a wired to a wireless (WiFi) connection, be certain to delete the localhost IP address listen in C://Windows/System32/drivers/etc/hosts

Software Licenses for:
ProxessIQ™
&
Mobile Credentials/Keys

The following are the separately licensable modules and features.
Please see your RSM or contact the Proxess HQ.

Licensing Information

American School District

administrator@proxess.com

FEATURE	VALUE
UserModule	unlimited
DoorModule	unlimited
AdvancedDoorFeatures	enabled
OrganizationModule	3
AuditPullSchedules	enabled
DeviceActions	enabled
ExtendedUnlockSchedules	enabled
WebAPI	enabled
RemoteManagement	enabled

Update License **Close**

When prompted to provide a license file in a ProxessIQ™ system and in order to add mobile credentials/keys to your system, a Proxess employee or authorized dealer will email a license package, as a .zip file.

LicensPackage_Customer-ABC_4-19-24_344051f8.zip
7 KB

The following instructions will show you how to download the .zip file and Extract and Save both files within it and note that location.

The first file we will address is the .lic validation and feature license for the ProxessIQ software.

This file may be added when prompted upon your login to the software, via this notification on the bottom bar of the software:
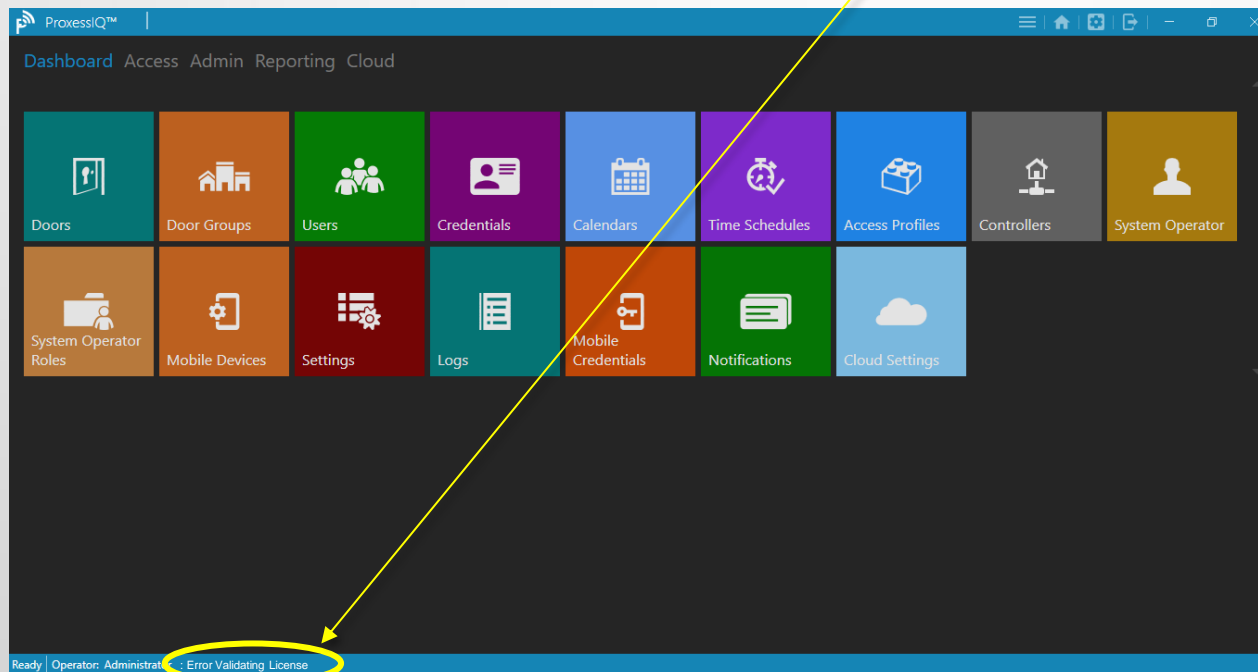
Install the license file using the following instructions.

Click on the Menu ("Hamburger") button in the top bar of the software.
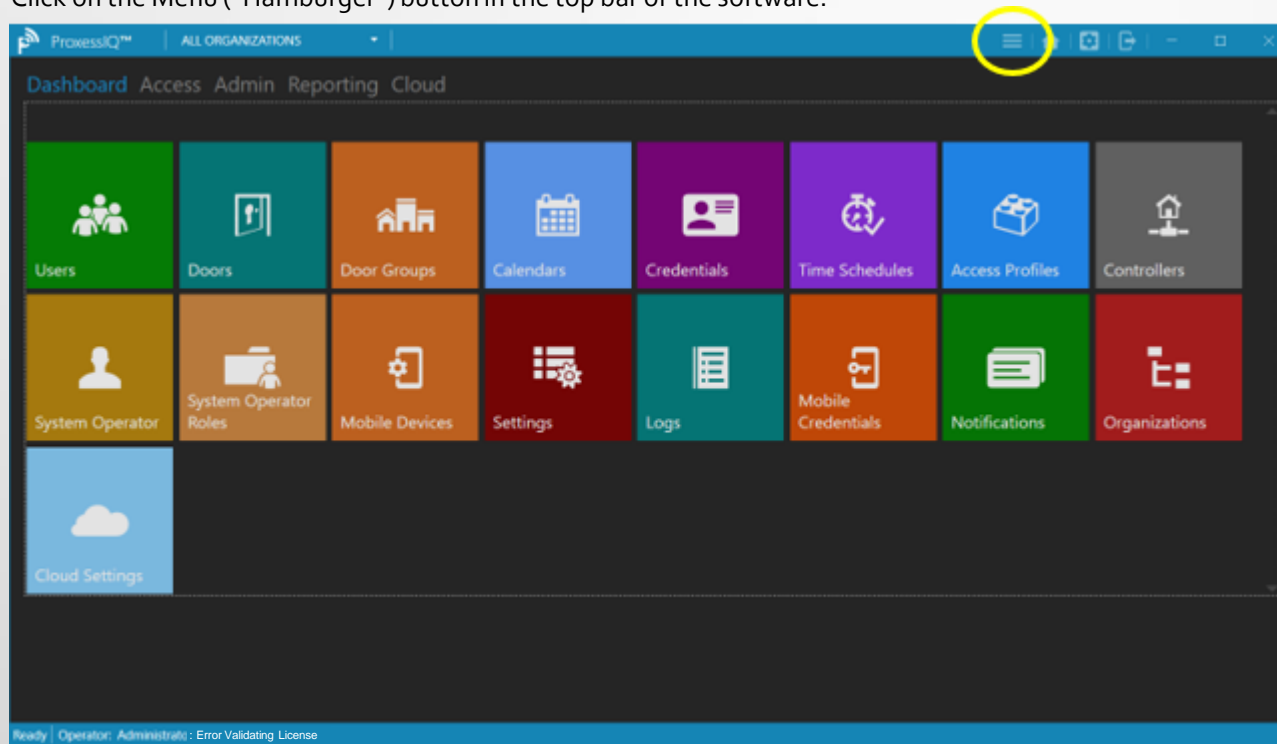
In the white menu items that appear, Click on "About".

Click "Licensing"

Click "Update License"
(In a New System)

...OR...
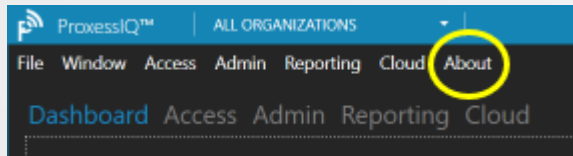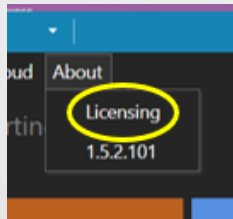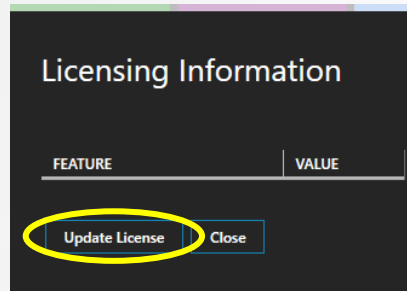
Click "Update License"
(Updating an Existing System)

Locate the file location you save the .lic file to and double click on it.
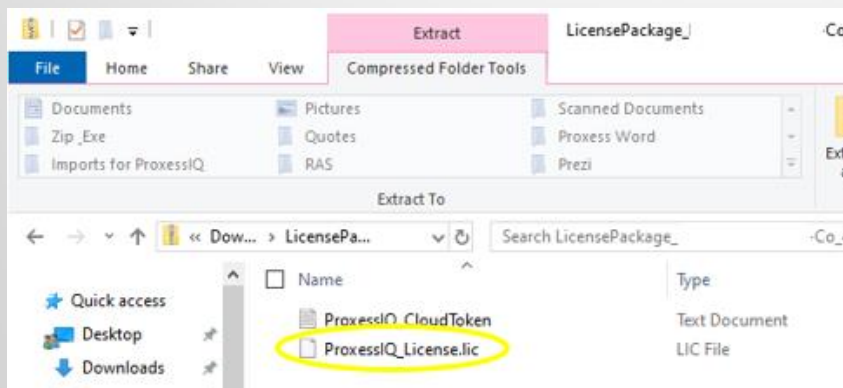
Your ProxessIQ software will now be licensed with the attributes that were purchased and you can return to the program to continue programming your system.

The second file you extracted from the .zip will provide you information to enable mobile credential operation.

Locate the file location you save the .lic file to and double click on "ProxessIQ_CloudToken".
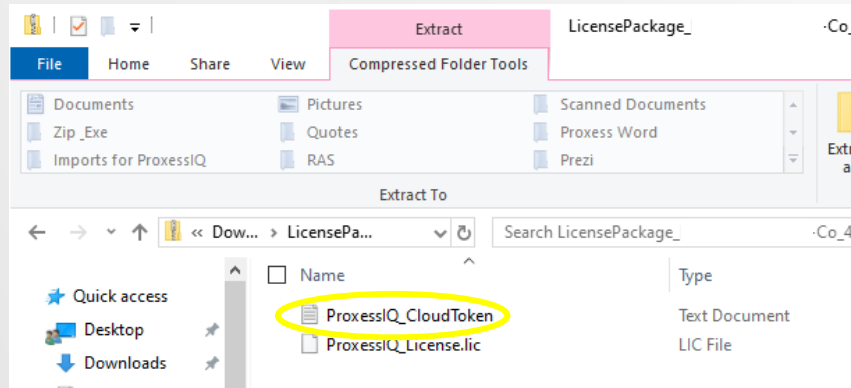
Allow this file to open in Notepad, or a similar program.
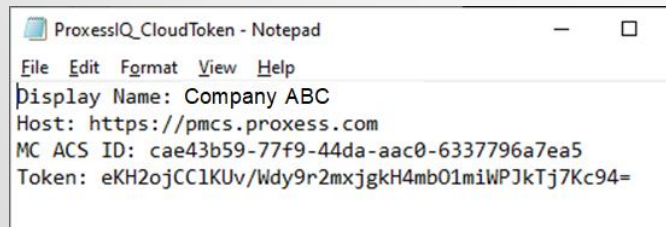
Once the data is entered, as explained below, your system will be provisioned with the number of mobile credentials your customer has purchased.

Future mobile credential purchases will simply be added by the Proxess support team in the cloud and applied to your system, without further action by the ProxessIQ™ Operator.

From the ProxessIQ dashboard, click on Cloud Settings .
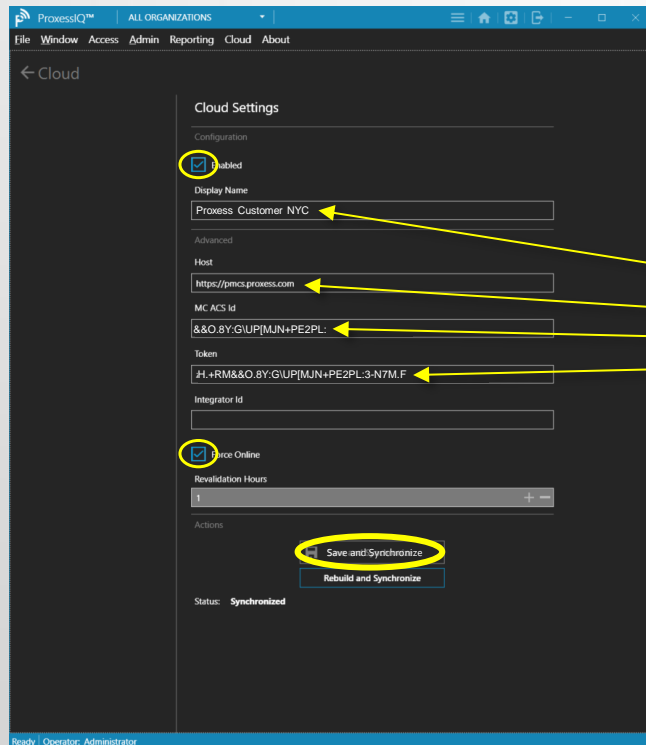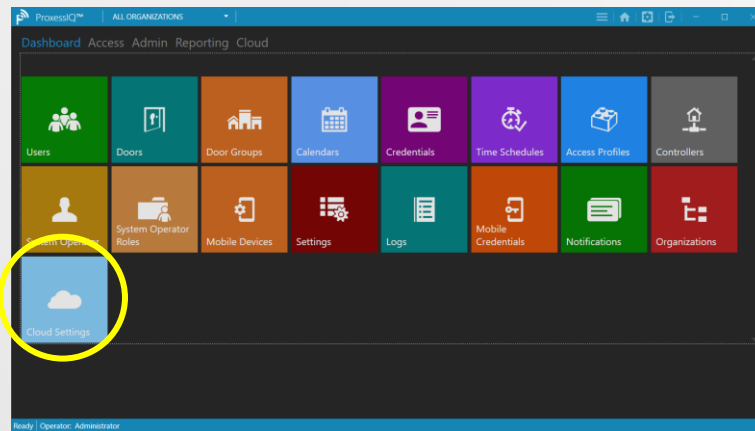
Check the "Enabled" box.
Copy each line of text file (including all the special characters, but not any extra spaces) and paste them into the appropriate fields.
Leave the "Forced Online" box checked.
Then click "Save and Synchronize" until "Synchronized" is shown.


```
ProxessIQ_CloudToken - Notepad                    —     □

File  Edit  Format  View  Help
Display Name: Company ABC
Host: https://pmcs.proxess.com
MC ACS ID: cae43b59-77f9-44da-aac0-6337796a7ea5
Token: eKH2ojCClKUv/Wdy9r2mxjgkH4mbO1miWPJkTj7Kc94=
```
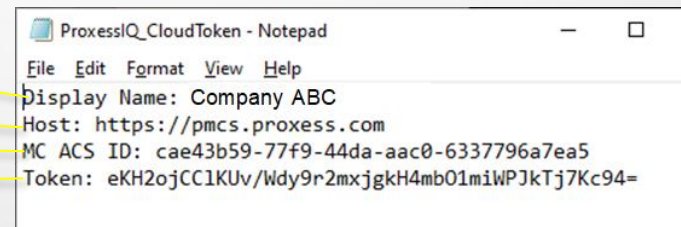
You may now click the back arrow or the Home button and resume your system programming.

Begin Programming ProxessIQ™

NOTE: The programming sequence from the Quick Start Guide (pages 3&4) will be the order followed throughout this operator manual.

Each module has dependencies on the previous modules, so attempting to configure a system out of this order may not be the most efficient, as it may result in the need to go back to the prescribed order to fill in various missing data entry fields.

Opening the ProxessIQ Client Administrative Interface
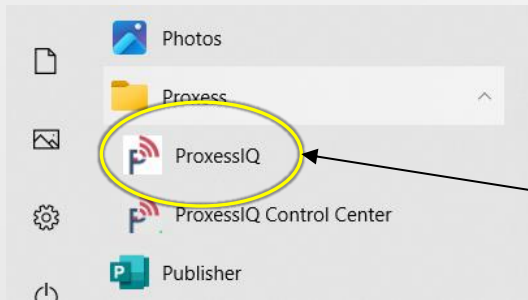
Click on the ProxessIQ icon from the Windows Program list,
Computer Desktop or Task Bar

Proxess Log In

UserName rschorr
Password ••••••••

☑ Remember Login
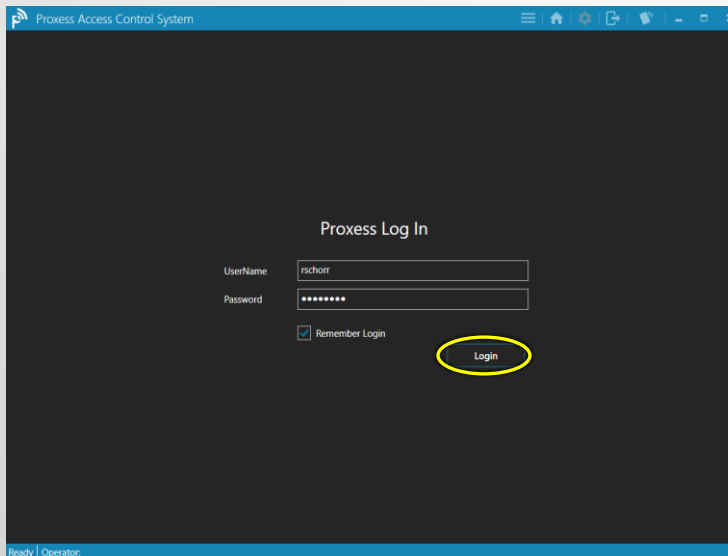
Login

The Login screen will appear after a short background start-up. Enter the default operator credentials you have been given. For security, be sure to immediately delete these credentials and add new personal credentials. Click on Login.
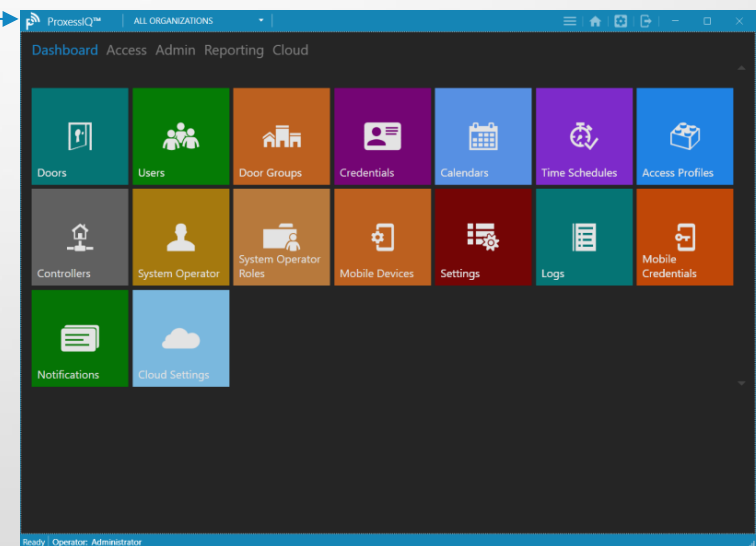
The Dashboard \ Home Screen will appear. In a later section we will show how to add the shortcut menu and change the background and icon colors, order and visibility. Click on the Module/Menu (the large icons) you wish to enter.

OPERATOR ROLES
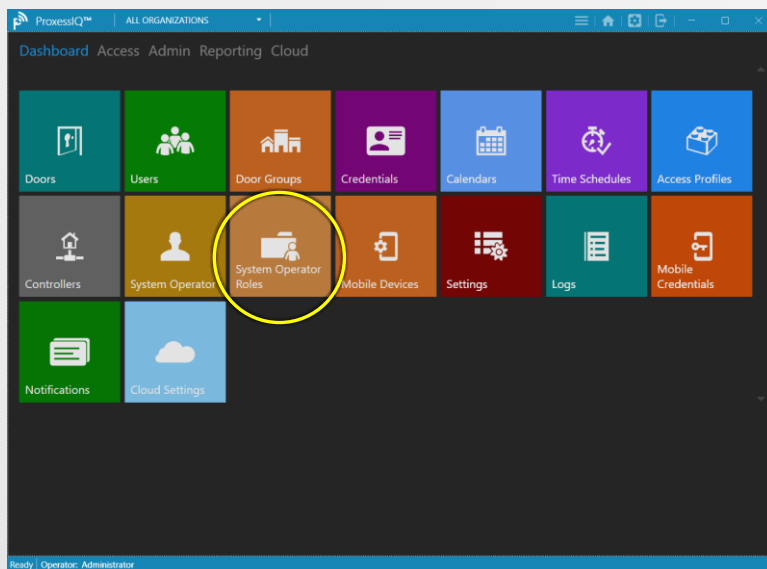
Operator Roles define what Modules (the large icons) Operators will have access to and what actions they will be able to perform once in that section. Click "System Operator Roles".
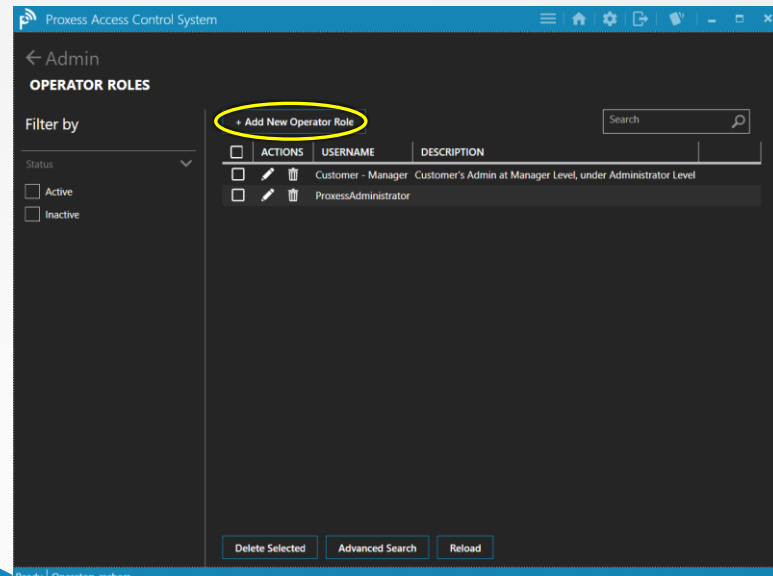
Options on this page allow editing and deleting existing Roles and filtering down a longer list of Roles using the Filter checkboxes for Active and Inactive Roles, on the left side of the page. Click "Add New Operator Role" to do so.
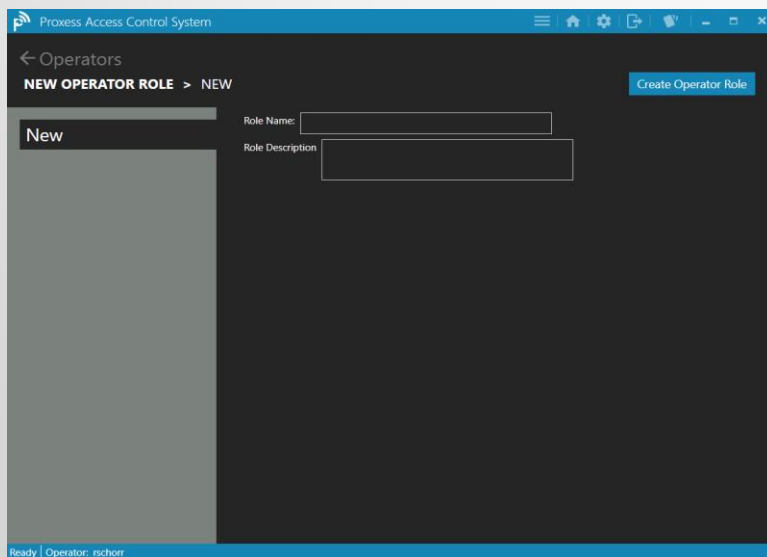
The following screen will open, for creation of the new Operator Role.
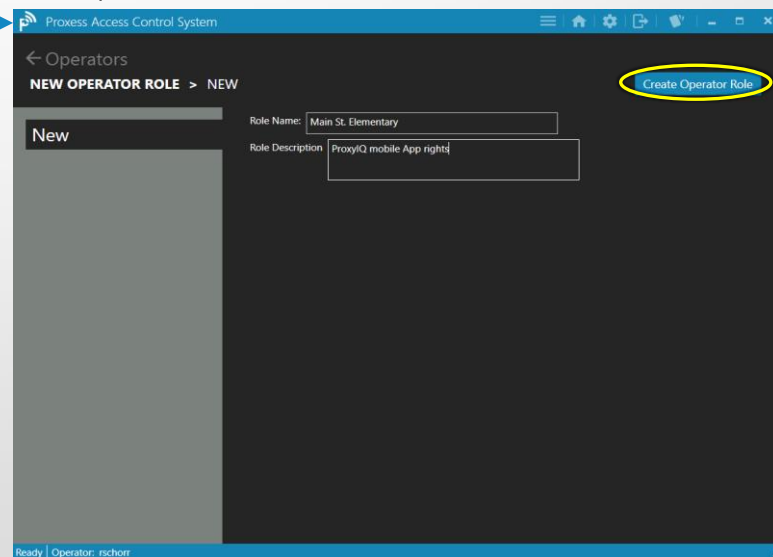
Enter a descriptive name for the Role, considering all the future possible names that may be in your system, to avoid future naming conflicts. You may add any descriptions that may assist you and the team. Click on the Create button when complete.
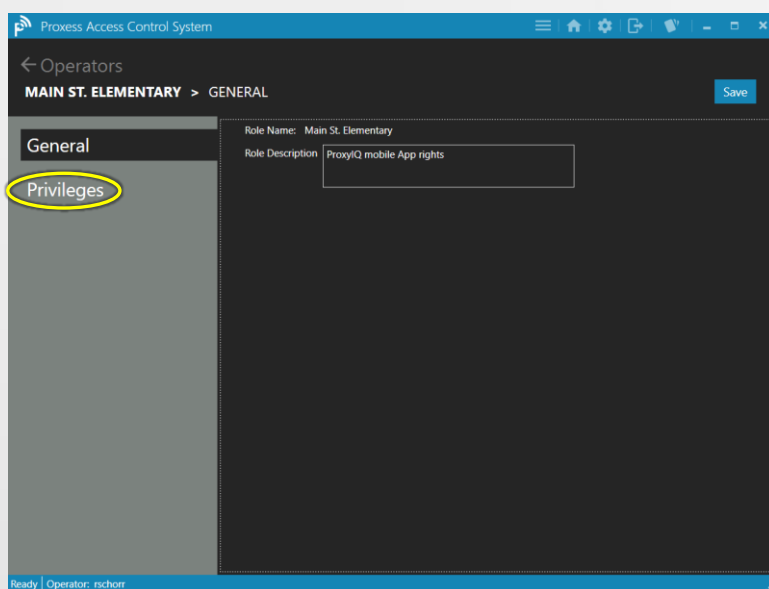
Once the new Role has been created, click on the Privileges button to define their modules and rights access.
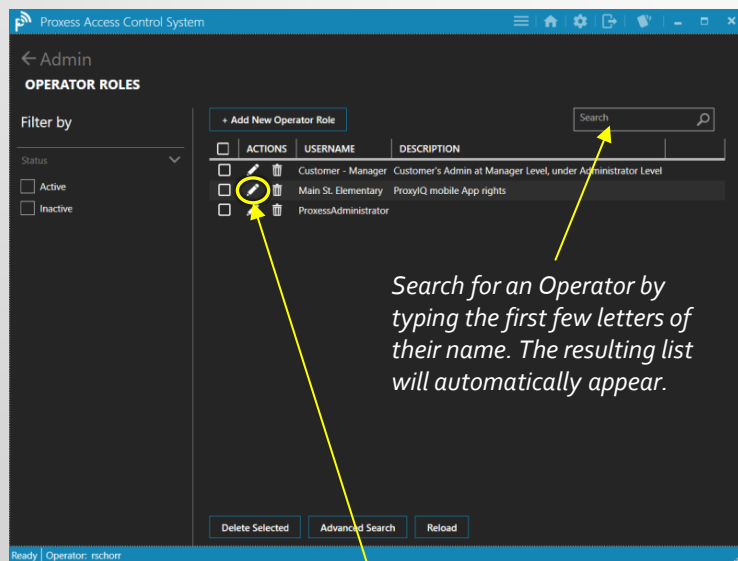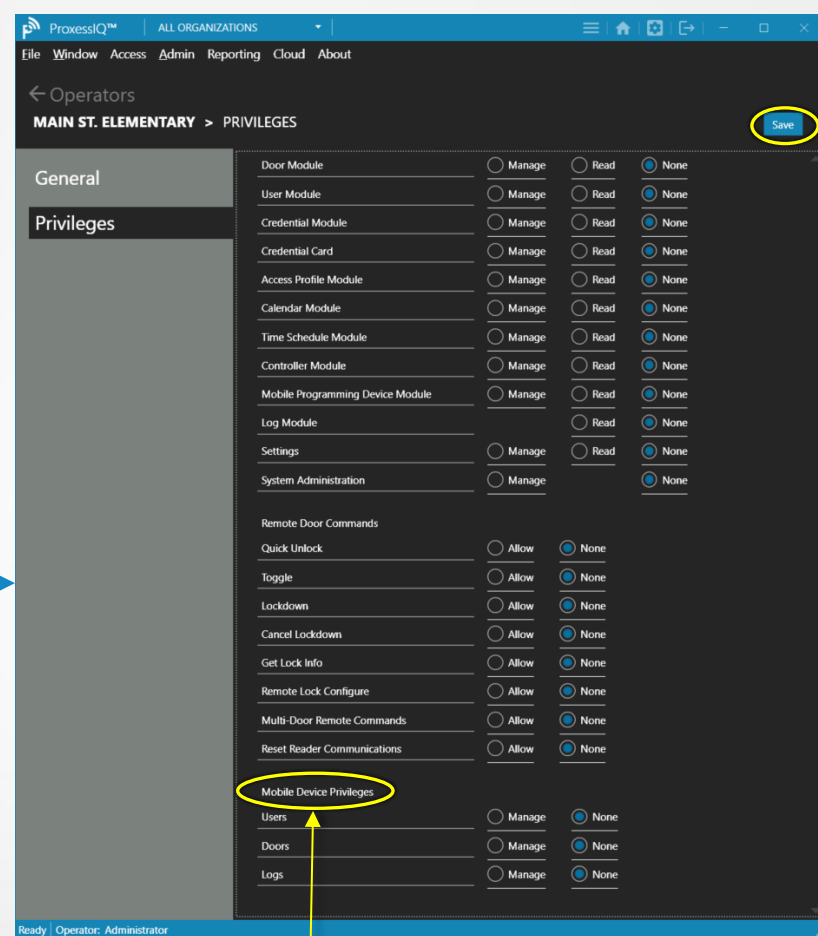
Search for an Operator by typing the first few letters of their name. The resulting list will automatically appear.

To review or edit any Role, click on the above icon. Other options on this page allow deleting existing Roles and filtering down a longer list of Roles , using the Filter checkboxes, for Active and Inactive Roles, on the left side of the page, or searching by name.

For each of the listed ProxessIQ™ software modules, click the radio button for the rights this Role will have once an Operator with this Role logs in. "Manage" allows editing and "Read" only allows viewing within each module. Click "Save" when complete. **Note** that the **Mobile Device Privileges** apply to the entire IQ Mobile phone administration app.; "Users" allow the device holder to encode and wipe credentials, "Doors" allows the device holder to see, bind, unbind & synchronize locksets and Logs allows the device holder to view the system Event Logs from their phone. **Note:** Be sure to apply the appropriate Operator Role to each phone in the "Mobile Devices" menu.
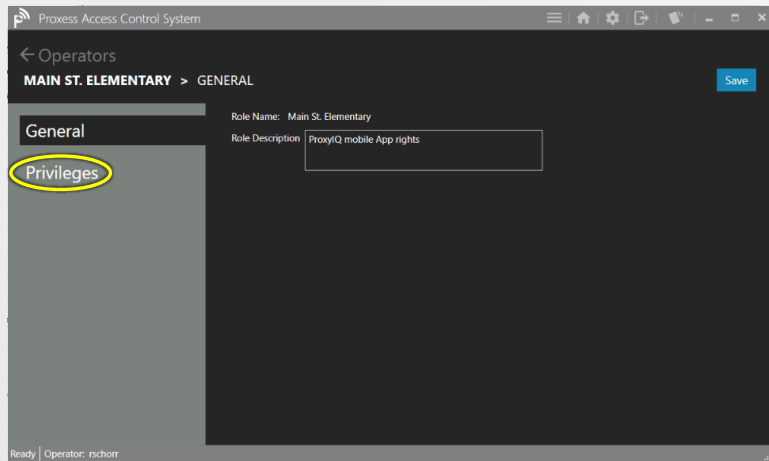
The Role you selected will appear. You may change any notes you wish. Click on the Privileges label to review those rights.
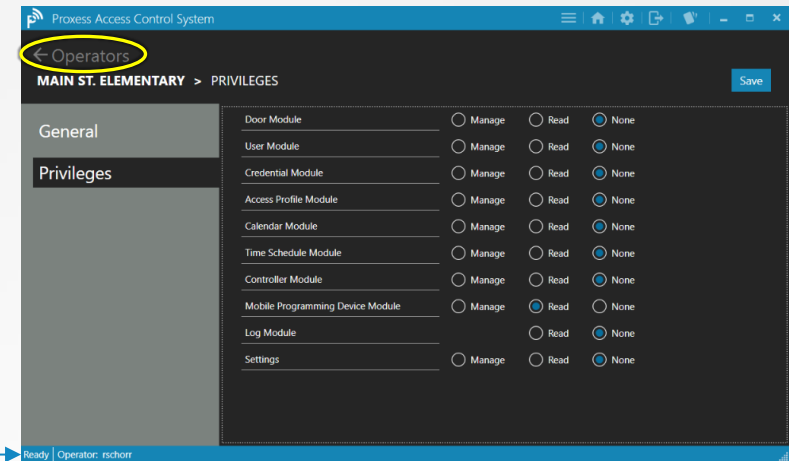
For each of the listed ProxessIQ™ software modules, click the radio button for the rights this Role will have, once an Operator with this Role logs in. "Manage" allows editing and "Read" only allows viewing within each module. Click "Save" when complete and "Operators" to return to the main Operator Roles screen.
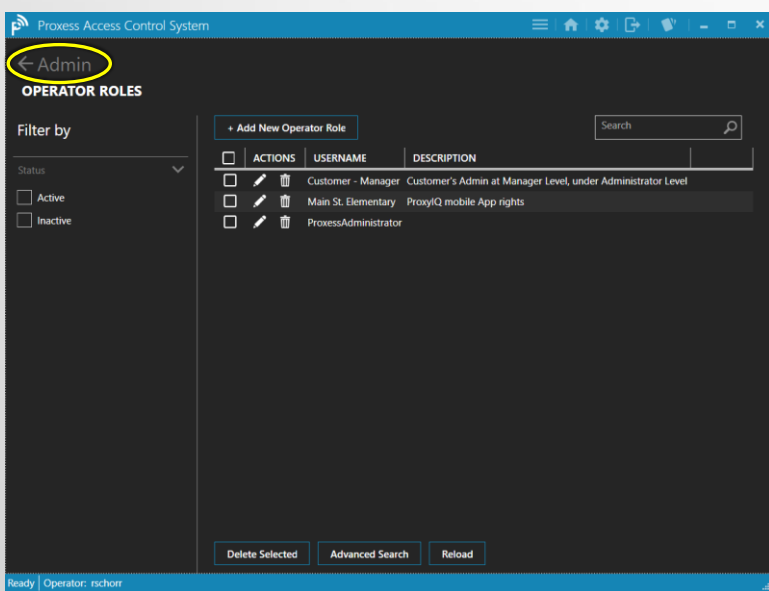
The main Operator Roles screen appears. Click on the "Admin" tag to return to your Home view.
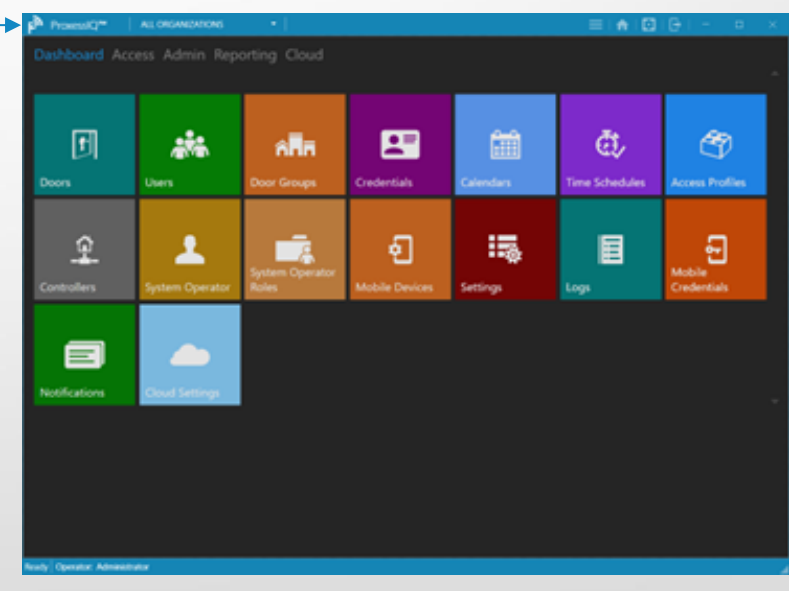
You will be returned to your Home Screen \ Dashboard.

OPERATORS
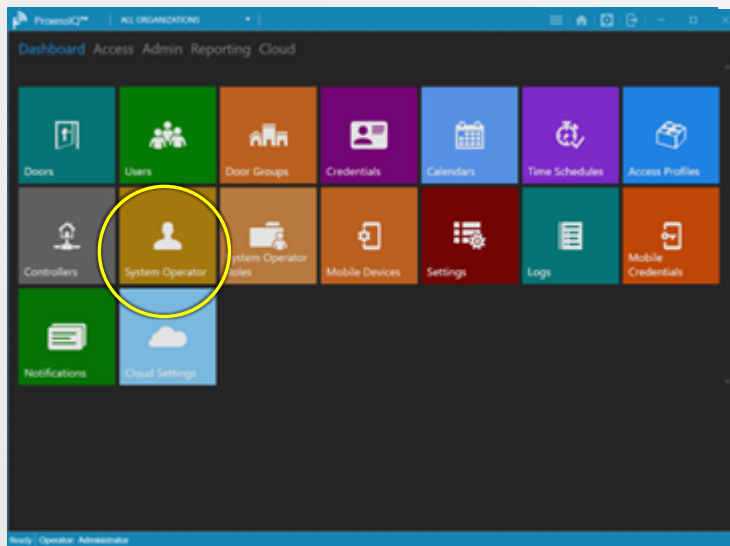
From the Home Screen (Dashboard) click on the System Operators icon, where you will be able to add and modify individual operators\programmers, including assigning them to one or more Operator Groups.
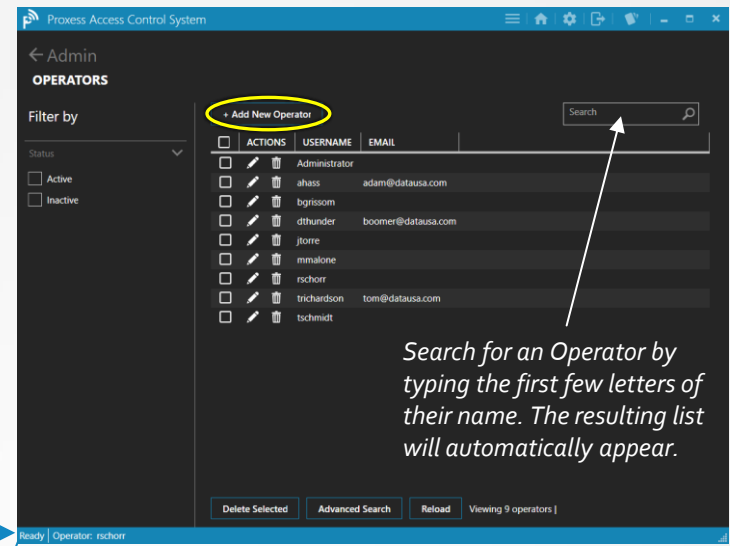
Click on "Add New Operator" to perform this action. Other options on this page allow editing and deleting existing Operators and filtering down a longer list of Operators , using the Filter checkboxes, for Active and Inactive Operators, on the left side of the page. Or, search for a specific Operator by typing the letter you know of the name of that person.

Search for an Operator by typing the first few letters of their name. The resulting list will automatically appear.
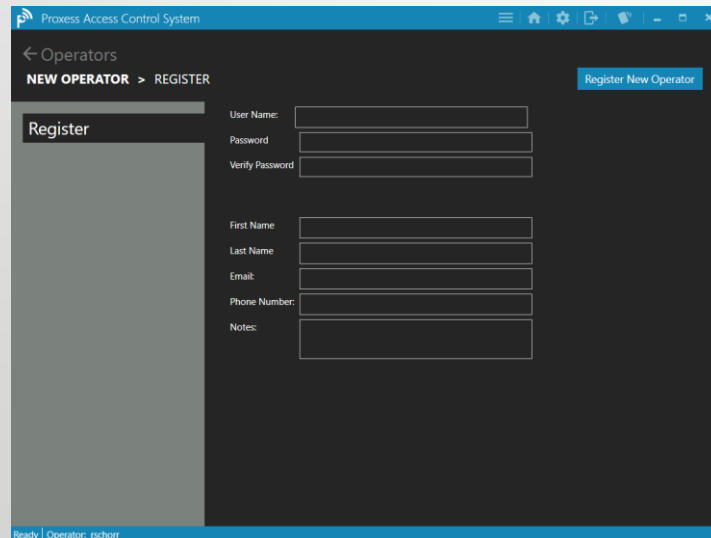
The main New Operator screen appears, showing the mandatory and optional fields. You may click on the "Operators" tag to return to the main Operators list.
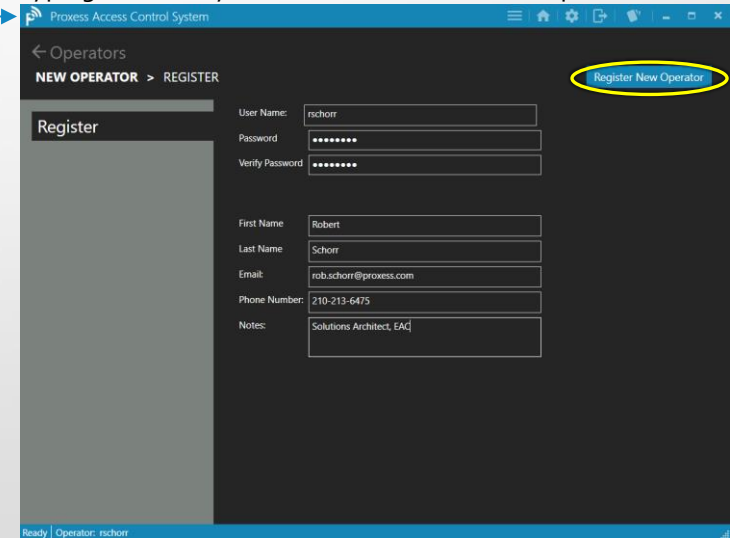
Create a case-sensitive User Name and Password, ensuring to verify the password exactly. No spaces are permitted in these fields. Enter a first and last name and a valid email, for use in later modules. The phone number and notes are optional. Click Register when complete.

The details for the Operator which you have just registered will appear. You may edit these details, including clicking on "Change Password" to do so, or click "Save".

Click on the Roles button to assign this individual to a category of rights within the software.

The existing list of Operator Roles that have been allocated to this Operator is displayed, which may be deleted. To add more Roles, click the dropdown arrow to reveal the full list of Operator Roles.

Select an additional or initial Operator Role to apply to this Operator.
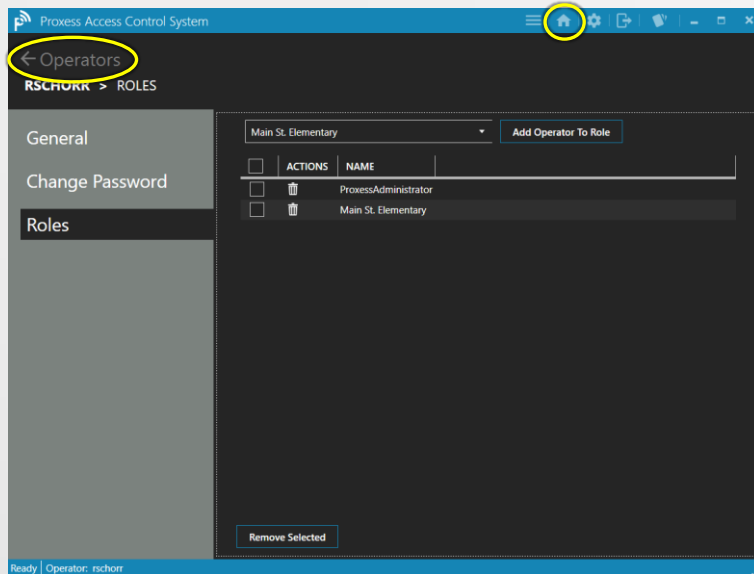
The new Role added to this Operator now appears in the list of previous Roles for the Operator. To return to the Home Screen \ Dashboard, click on the Home icon on the top task bar. To return to the list of Operators page, click on "Operators".
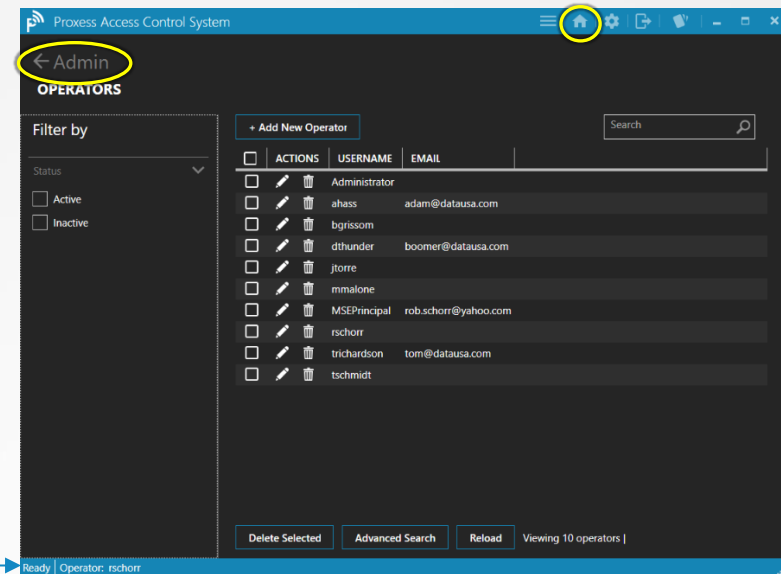
This is the list of all the Operators, including the one that was just added. To return to the Home Screen \ Dashboard, click on either the Home icon on the top task bar, or the "Admin" tab at the top left of the page.
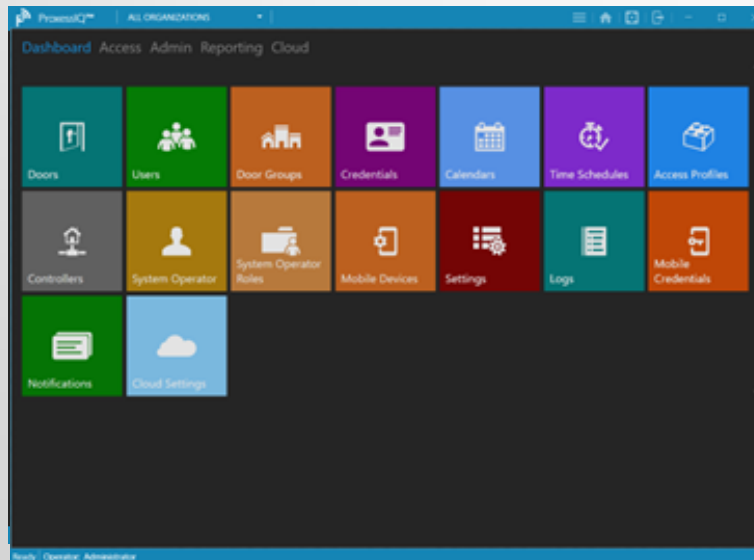
You have returned to the Dashboard \ Home Screen.

MOBILE DEVICES

This section will show you how to add administrative phone app users, using the IQ Mobile phone app, to the system, for the purposes of initializing Bluetooth locks, exit trim devices and controllers.
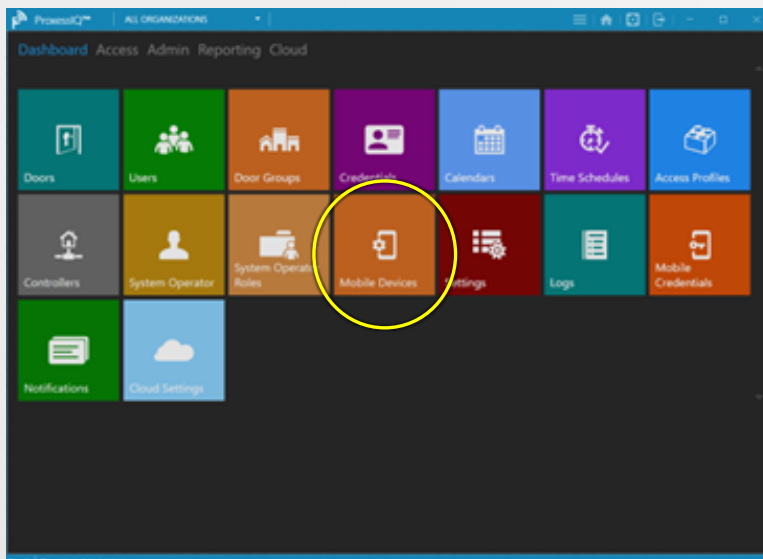
Mobile Devices - 1

To add a new (and manage existing) mobile phone to be used as an in-the-field programming device click on the "Mobile Devices" module icon.
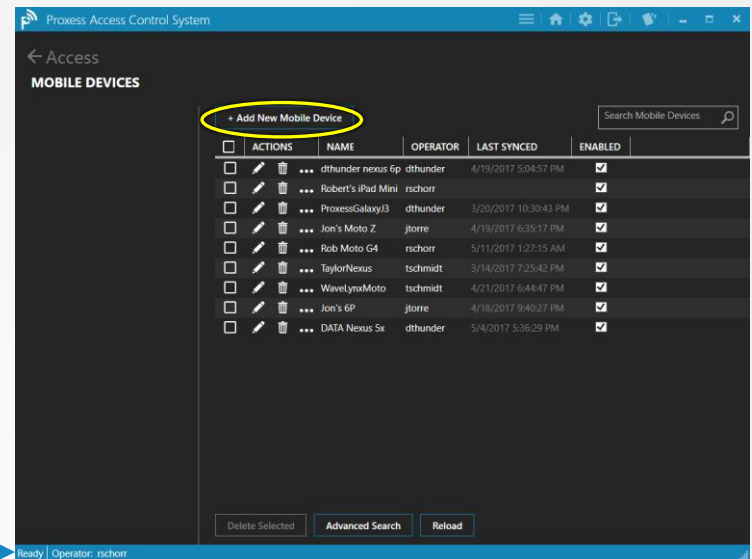
This is the list of all the registered mobile phone Apps in the system. Click "Add New Mobile Device" to do so. To return to the Home Screen \ Dashboard, click on either the Home icon on the top task bar, or the "Access" tab at the top left of the page.
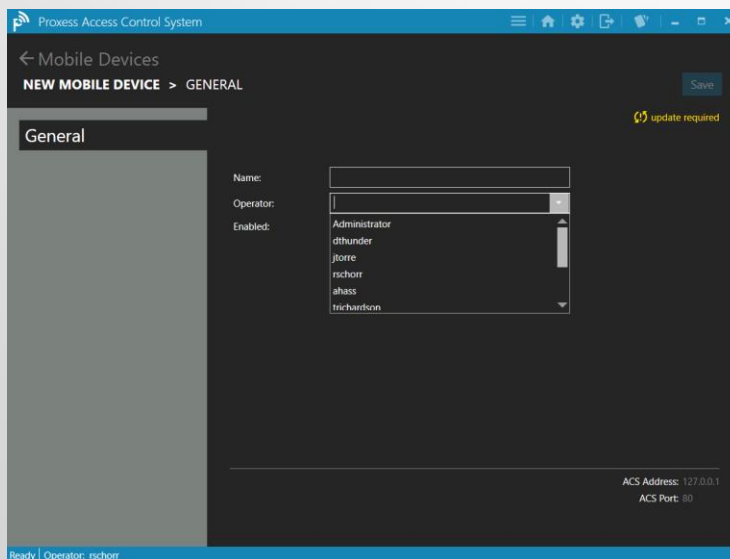
Enter a name for the mobile phone to be added. **Note:** Be certain to select the responsible Operator for this App from the drop-down list, as discussed I the Operator Roles section.
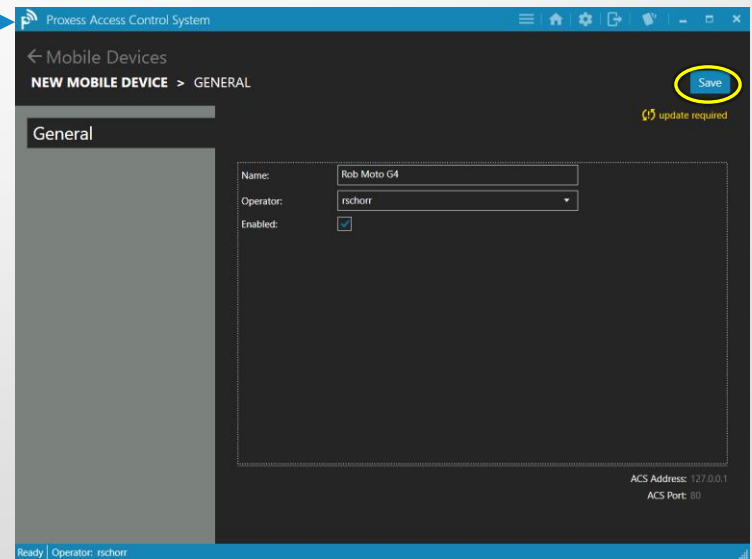
Check the Enabled box and click "Save".

Proxess Access Control System
Mobile Devices
NEW MOBILE DEVICE > GENERAL   Save
                                                        update required
General

Name: Elliot
Operator: rschorr

Mobile Device Saved
The mobile device changes have been saved
                                                Ok

ACS Address: 127.0.0.1
ACS Port: 80

Ready | Operator: rschorr

Click "OK".

Proxess Access Control System
Mobile Devices
ROB MOTO G4 > GENERAL   Save
                                                        update required
                                           Last Synced: 5/11/2017 1:27:15 AM
General

                    Scan with Proxess Mobile App

                                                        Scroll
                                                        down

ACS Address: cloud1.proxess.com
ACS Port: 0

Ready | Operator: rschorr

A unique 2-dimensional bar code will be generated and displayed for use in the next module, "Mobile Phone App". Click "Save", though you may scroll down to view the other communications data.

Proxess Access Control System
Mobile Devices
ROB MOTO G4 > GENERAL   Save
                                                        update required
                                           Last Synced: 5/11/2017 12:00:16 PM
General

Device Communication Codes
Com Code: .2#=-)*!s>;;l_y
Key Code: 7M&o)%g|#!m%@[-.
                Reset Communication Codes

Proxy Settings
Installation Id: 9999876-1111-4e65-a065-00fd65531f18
Naming Convention: https://p[0]proxessproxy.azurewebsites.net/
Is Dynamic: ☑
Preferred Proxies: 1, 2

Mobile Device Registration
Registered Device Id: 1dd624b7-3f5c-4d55-84ab-525139612cfd
                Remove Mobile Device

ACS Address: cloud1.proxess.com
ACS Port: 0

Ready | Operator: rschorr

No changes are encouraged or required to be made. Click "Save" to continue.

Proxess Access Control System
Access
MOBILE DEVICES

+ Add New Mobile Device   Search Mobile Devices

ACTIONS	NAME	OPERATOR	LAST SYNCED	ENABLED
✎ 🗑 ...	dthunder nexus 6p	dthunder	4/19/2017 5:04:57 PM	☑
✎ 🗑 ...	Robert's iPad Mini	rschorr	4/21/2017	☑
✎ 🗑 ...	ProxessGalaxyI3	dthunder	3/20/2017 10:30:43 PM	☑
✎ 🗑 ...	Jon's Moto Z	jtorre	4/19/2017 6:35:17 PM	☑
✎ 🗑 ...	TaylorNexus	tschmidt	3/14/2017 7:25:42 PM	☑
✎ 🗑 ...	WaveLynxMoto	tschmidt	4/21/2017 6:44:47 PM	☑
✎ 🗑 ...	Jon's 6P	jtorre	4/18/2017 9:40:27 PM	☑
✎ 🗑 ...	DATA Nexus 5x	dthunder	5/4/2017 5:36:29 PM	☑
✎ 🗑 ...	Rob Moto G4	rschorr	5/11/2017 12:00:16 PM	☑

Delete Selected   Advanced Search   Reload

Ready | Operator: rschorr

The list of all the registered mobile devices in the system will appear. You may enable, view, edit or delete any device you have access to in the list. To return to the Home Screen \ Dashboard, click "Access" or the Home icon in the top task bar.

MOBILE PHONE ADMIN APP
IQ Mobile (formerly Proxess Sync™)
INITIALIZATION

This section will show you how to add an administrative phone app, IQ Mobile™ to the system.

Have your Apple or Android phone ready.

IQ MOBILE phone app Modules:

Lockset Synchronization
- Audit retrieval
- Initialization
- Time Schedule changes
- Functional changes
- Remote support

Physical Credential Encoding
- Encoding
- Updating
- Wiping & deleting

Full Users Module
- Create & manage Users
- Create & manage physical and mobile credentials

Door Control
- Door unlocks, toggling, status updates
- Lockdown

Audit Logs
- System event and audit logs for investigation

Settings
- Reset authentication codes for remote users
- Add & delete additional systems

iPhone Download

Go to the App Store and search for "Proxess". Select the "Proxess IQ Mobile™" Management App and download it to your phone.

For lockset communication, assure Bluetooth is turned on in the Settings app.

For ProxessIQ™ synchronization, ensure WiFi and\or Mobile Communication is turned on.

IQ Mobile

Click the Proxess icon to open the App.

Mobile App Screenshot

Allow the app to use the camera on your phone.

PC Software Screenshot

The app will open and ask you to confirm you will allow it to sue the camera on your phone. Confirm this and the above scanner image will open. Point your phone's camera to view the QR code that appears in the screen in the software when your new Mobile Device was added, shown in the image on the right.

NOTE: There are a few ways to scan the QR code in the software with the mobile phone being added:

- The first is to bring the phone to the software, open the "Mobile Devices" module and click the edit button for the mobile device being added where the QR code will then appear. With the scanner screen open, hold the phone over the code and all of the connection data will automatically populate as shown in the image below on the left. This connection data will match what is on that software page.
- If the phone is not near the software, a screenshot can be taken of the QR code and emailed to the person with the phone to scan it (from either the email screen or a printed copy) in the same manner as above.
- The third way is to manually enter all the data into the phone whether the phone is local or remote.

Name this as the system you are connecting to.

At the bottom of the screen, you may click "Test Connection" to verify the setup was successful.

Click Done to return to the Proxess Sync™ Home screen for this system.

NOTE: In order to assure the Test works, it is necessary to verify that the phone has connectivity to the ProxessIQ™ software, wherever it is located, via either the customer's WiFi or the mobile phone network. These are matters for resolution between the customer and the integrator and are not the responsibility of Proxess.

Proxess' **IQ Mobile** is an application suite providing a combination of remote observation and control of your ProxessIQ™ system.

The following modules are contained within the app and their visibility on the dashboard, per operator, are defined within the Operator Roles menu and with the Operator privilege they are assigned in the Mobile Devices menu.
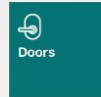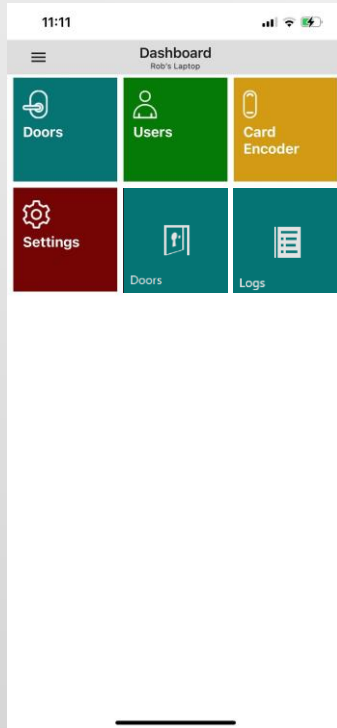
This low-risk module displays all the locks and Mini-IQ controllers that have been entered into from the PC software client. Here, Doors may be initialized, Synchronized, Updated, Reset and have their Audits retrieved.
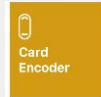
The Card Encoder module is a low-risk module for operators who will only need to encode and update physical credentials, which have been entered into the software from a PC client and for which they have been granted visibility for.

The Settings module provides for resetting the authentication codes for operator devices and allows users to add & delete additional ProxessIQ™ systems.
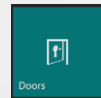
This module provides the Door Control functionality from the main Doors screen in the ProxessIQ™ PC client software. This includes Quick Unlock, Toggle, Lockdown, Refresh, reader status, Battery %
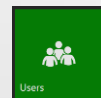
This provides the complete functionality of the Users module General and Credentials tabs from the ProxessIQ™ PC client software. The IQ Mobile app holder can add, edit and delete users and their credentials, including the ability to encode and update them from this module.
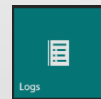
The Logs module provides investigation of all system events and audit logs.
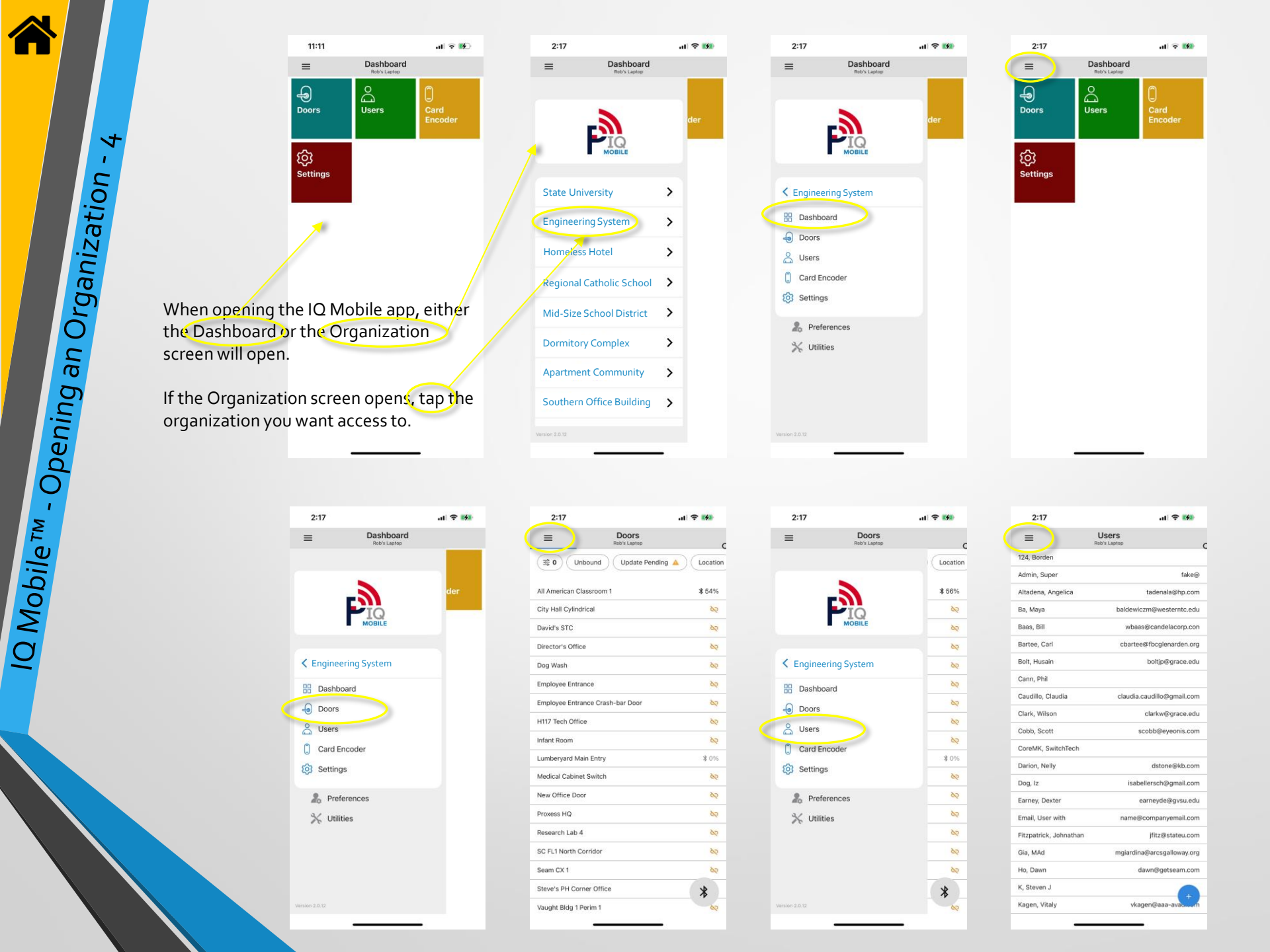
When opening the IQ Mobile app, either the Dashboard or the Organization screen will open.

If the Organization screen opens, tap the organization you want access to.
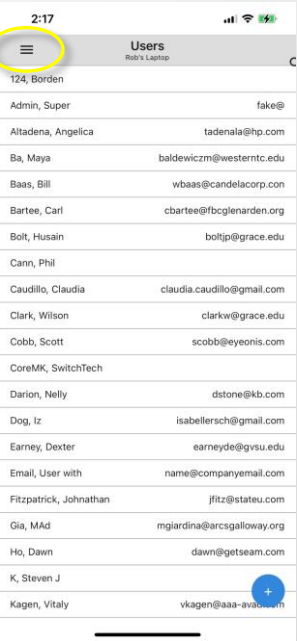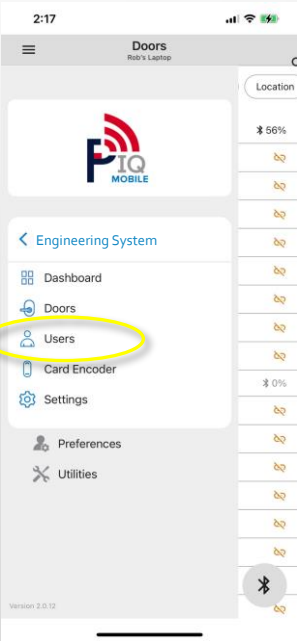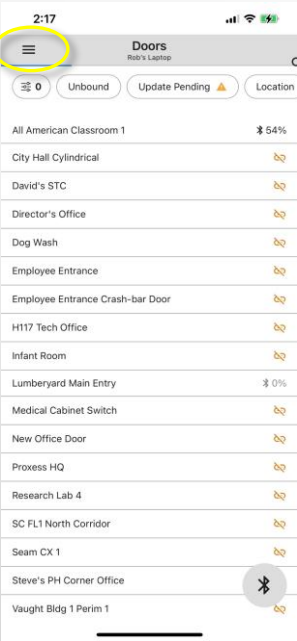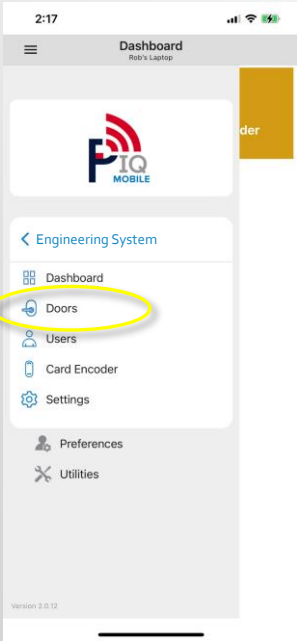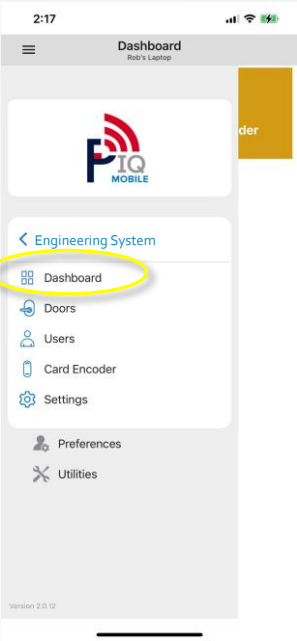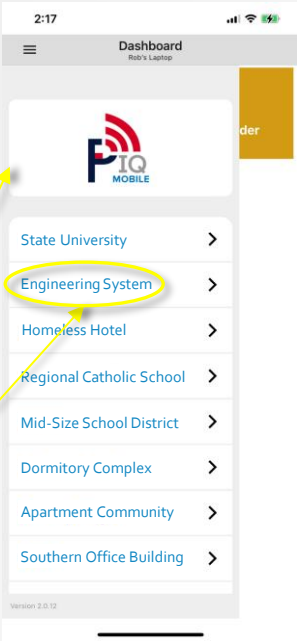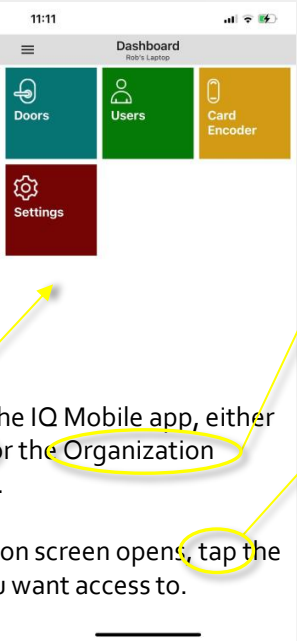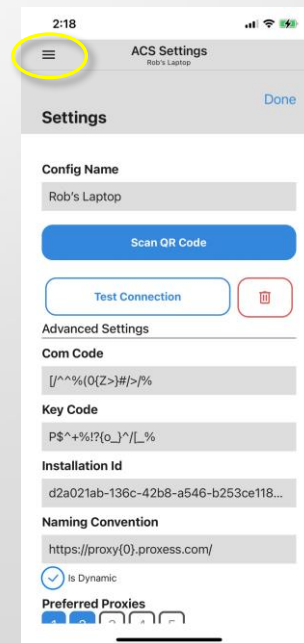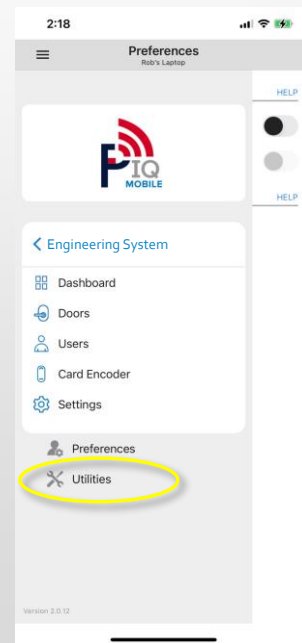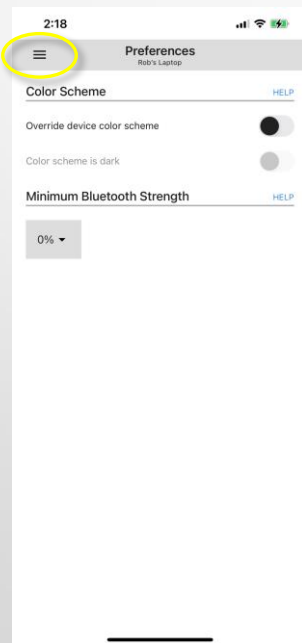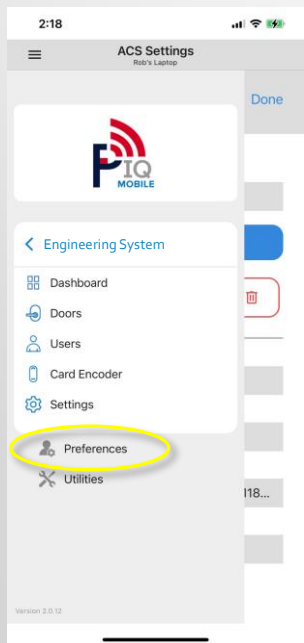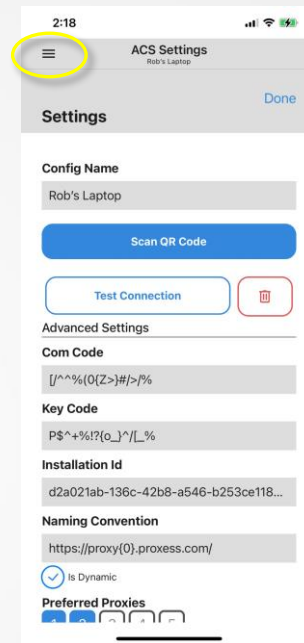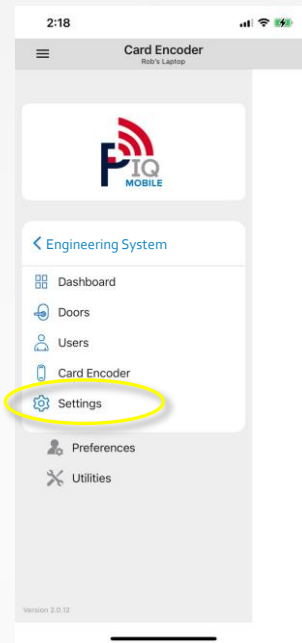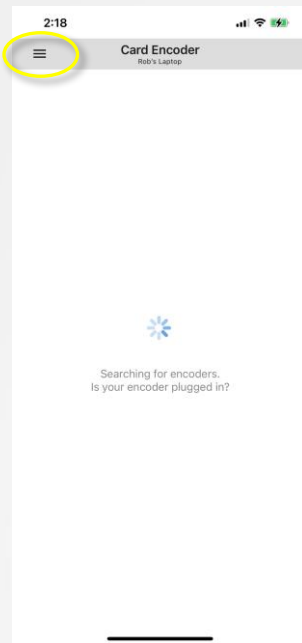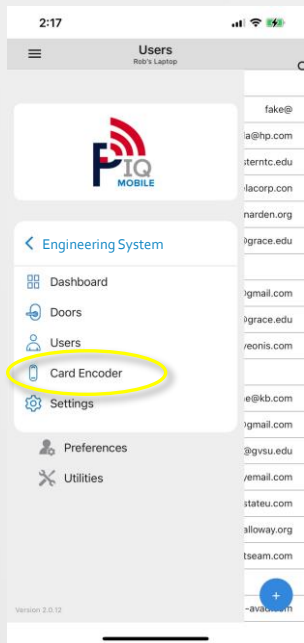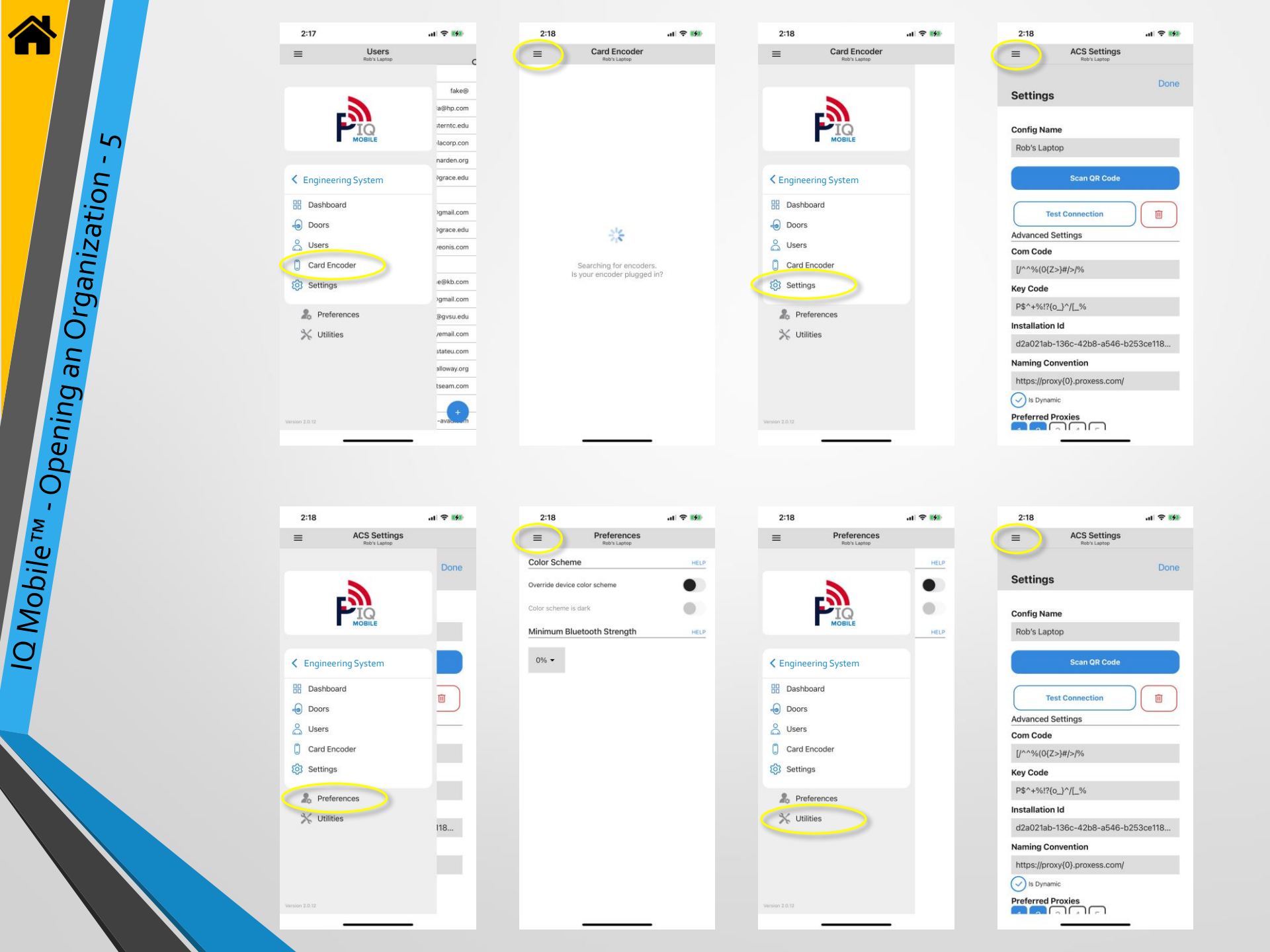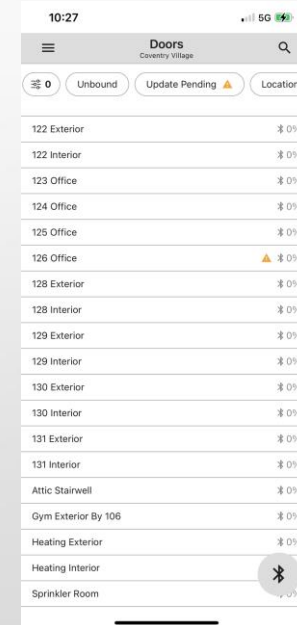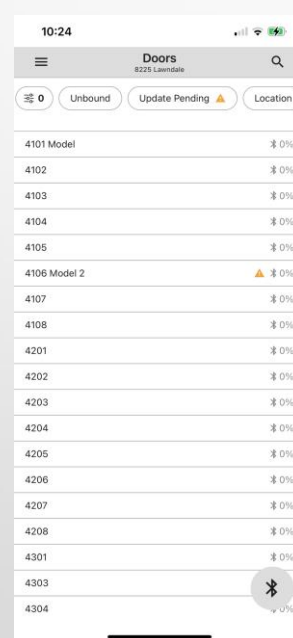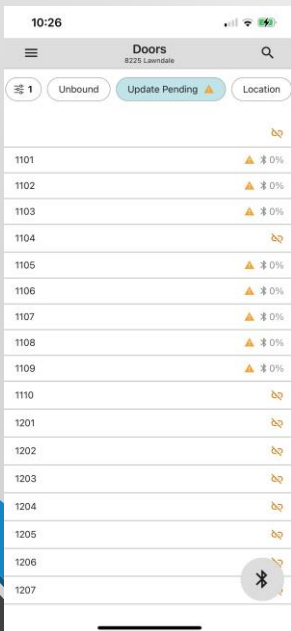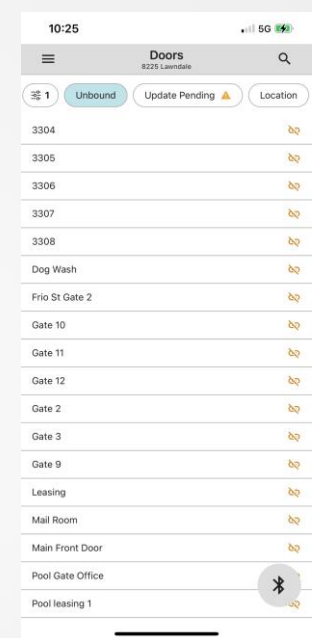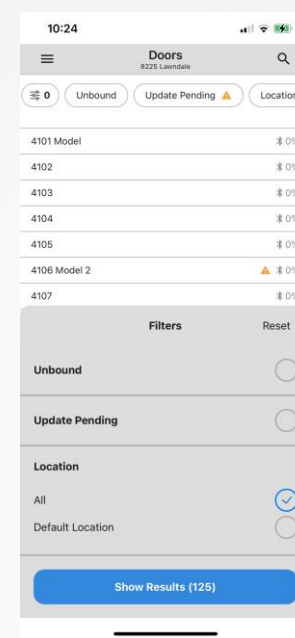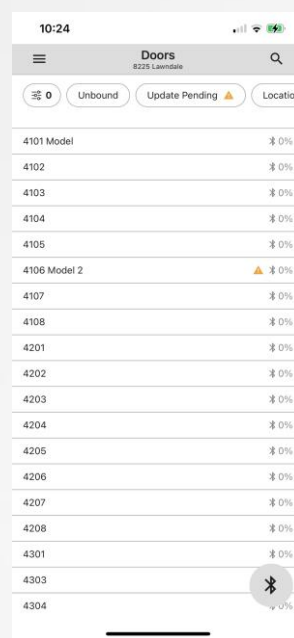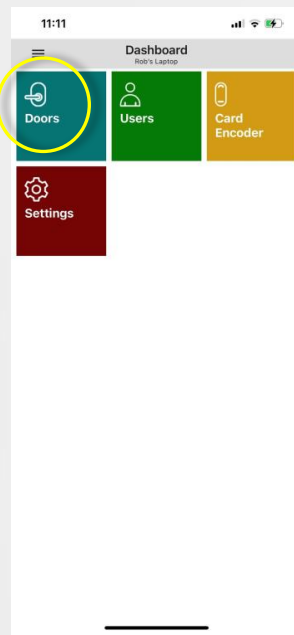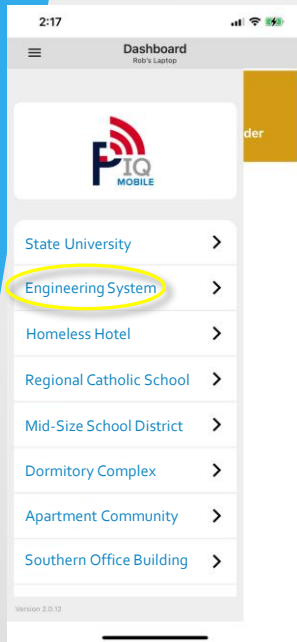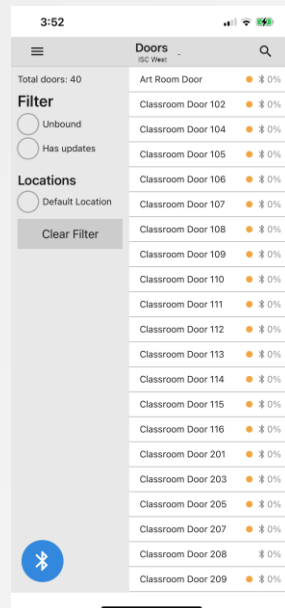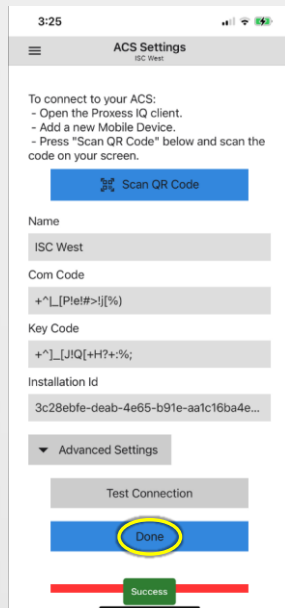
...OR....
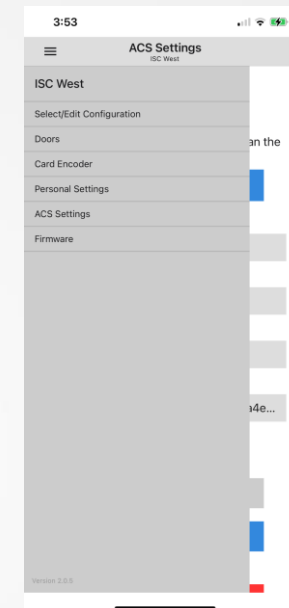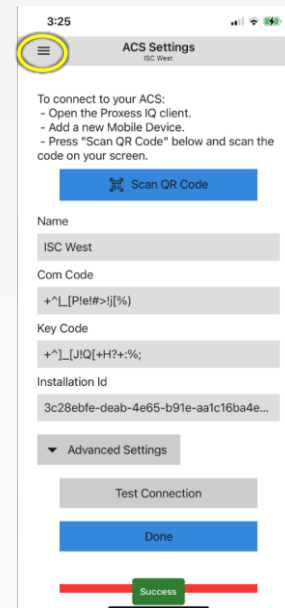
When you click Done, you will be brought to the Doors screen for that system. By checking the radio buttons on the left, you will cull the list to see only doors in a certain location, or doors that have not be bound or connected to this system.

You may also click on the Menu/Hamburger button, which will take you to the overall Menu for Proxess Sync.
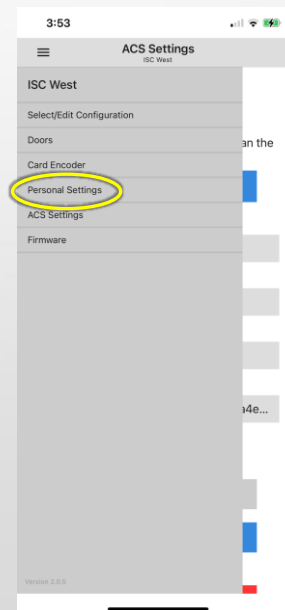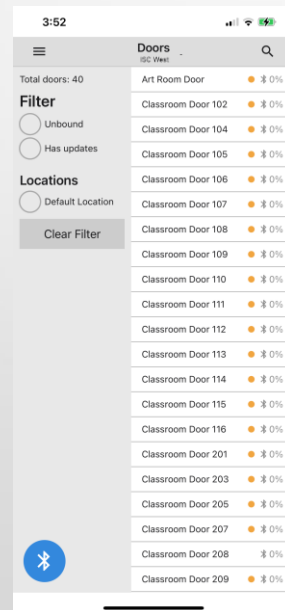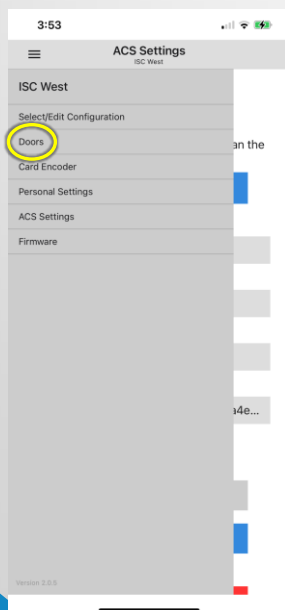
Minimum Bluetooth signal strength from your phone to a lock for it to show up in Proxess Sync to be viewable to be sync'd.

Click on Doors to bring you to the Doors screen.

Click on Personal Settings to bring you to the that screen.
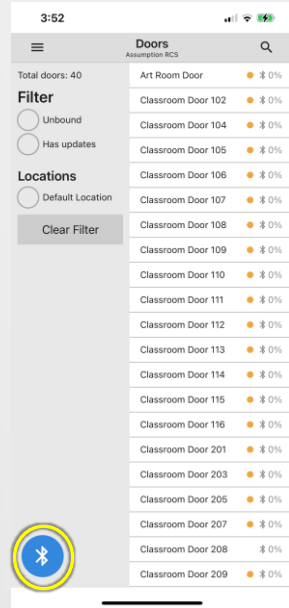
...OR....
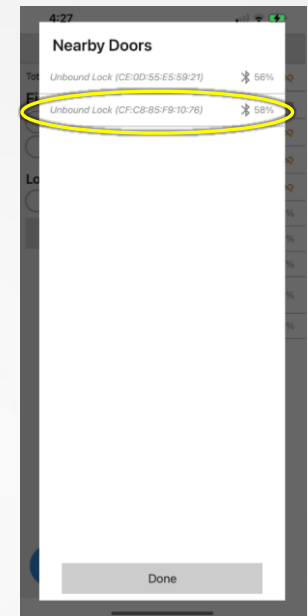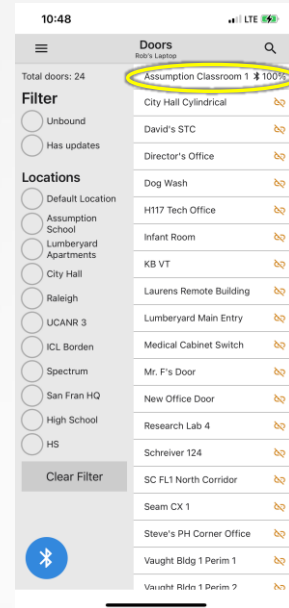
As an alternative to clicking on the Door name to initialize/ sync it, Click on the Bluetooth icon and all the nearby doors will appear. The % indicates the Bluetooth signal strength of each lock. Place your phone near the front-facing plastic of the lock

So, from either screen view you wish, select a Door to connect with, ensuring you select the one with the greatest signal strength. For a first-time lock initialization, be sure to select an "Unbound" lock.
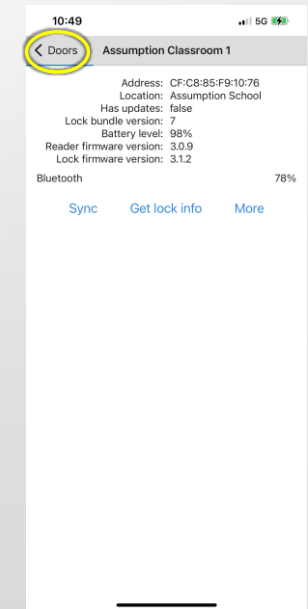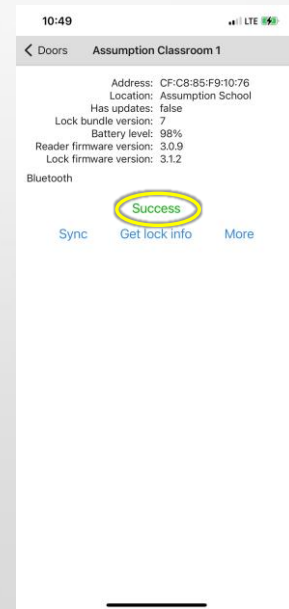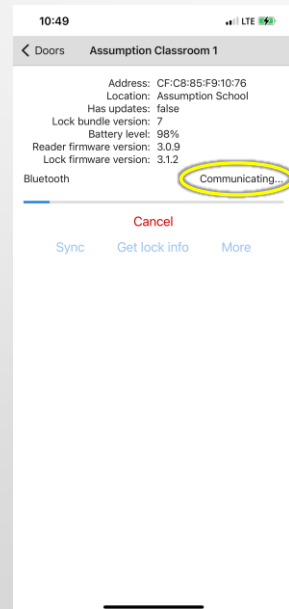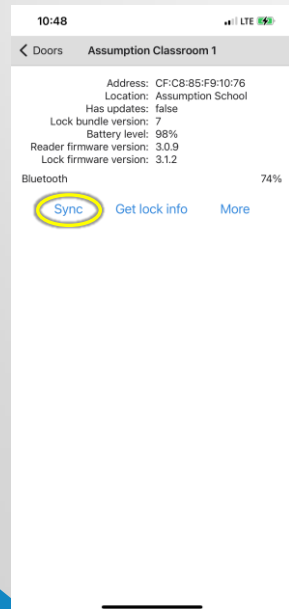
Click Sync to initialize or update a lock.

Success will be displayed and you can return to the Doors screen.

Android

For lockset communication, assure Bluetooth is turned on.

For ProxessIQ™ synchronization, ensure WiFi and\or Mobile Communication is turned on.

Go to the Google Play Store and search for "Proxess". Select the "Proxess IQ Mobile™" Management App and download it to your phone.

Click the Proxess icon to open the App.

Proxess Sync

STATUS   SYNC   DOORS

Status

Last synced: Tuesday, May 9, 2017 11:19 PM

There are 16 doors to update.

Proxess Sync

ACS Settings

Lock Sync Settings

Firmware

Export Log

STATUS

Status

Last synced: Tuesda

There are 16 doors to update.

Connect to ACS

Directions
In the ACS, add a Mobile Programming Device to a System Operator. Add the com code and key code below.

SCAN QR CODE

Com code

Key code

Proxy installation Id

Proxy naming convention

Is dynamic

The screen on the left will appear the first time the App is opened. Future openings of the App will display the last screen viewed from the last time the App was closed. Click the icon circled. Then click "ACS Settings" from the menu. The screen on the right appears. To initiate the App, click on "Scan QR Code". To continue, you must now open the ProxessIQ software and go to the "Mobile Devices" module and click on the Edit icon for the device you will now add.

Mobile App Screenshot
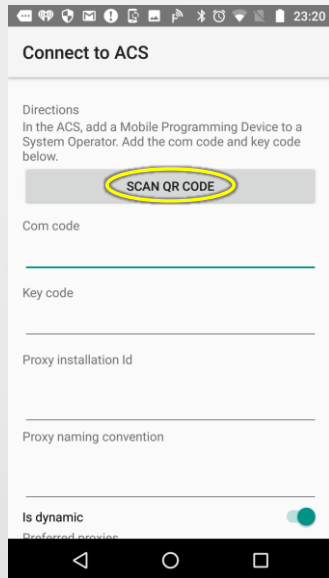
Mobile App Screenshot
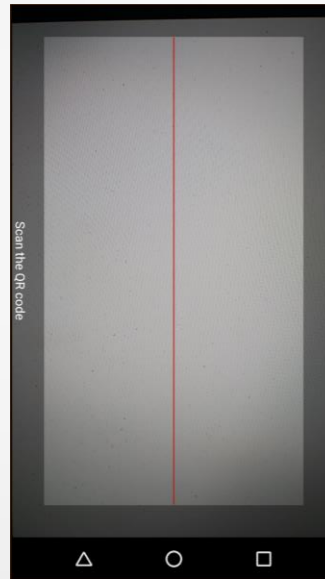
PC Software Screenshot

The screen on the left opens. Click the "SCAN QR CODE" button and the scanner screen in the center opens. This is a scanner, which uses your phone's camera to view the QR code that has appeared in the screen in the software where your new Mobile Device was added, shown in the image on the right.

NOTE: There are a few ways to scan the QR code in the software with the mobile phone being added:

- The first is to bring the phone to the software, open the "Mobile Devices" module and click the edit button for the mobile device being added where the QR code will then appear. With the scanner screen open, hold the phone over the code and all of the connection data will automatically populate as shown in the image below on the left. This connection data will match what is on that software page.
- If the phone is not near the software, a screenshot can be taken of the QR code and emailed to the person with the phone to scan it (from either the email screen or a printed copy) in the same manner as above.
- The third way is to manually enter all the data into the phone whether the phone is local or remote.

At the bottom of the phone screen, you may click "Test Connection" to verify the setup was successful.
Click the Back button on the phone to return to the Proxess Sync™ Home screen.

NOTE: In order to assure the Test works, it is necessary to verify that the phone has connectivity to the ProxessIQ™ software, wherever it is located, via either the customer's WiFi or the mobile phone network. These are matters for resolution between the customer and the integrator and are not the responsibility of Proxess.

NOTE: Bear in mind that Proxess Sync™ is a passive and un-hackable App in that the programming is done only from the ProxessIQ™ software. The App is simply presented to the locksets and the operator will simply need to click a button for the programming changes to be synchronized with the locksets.

If the access control software has changes to be synchronized, that note will appear here.
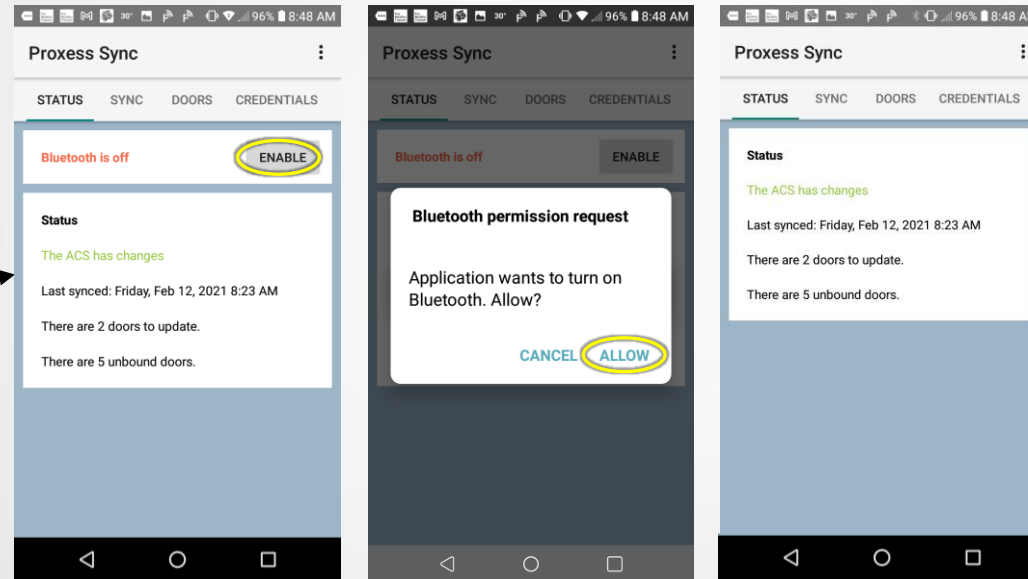
To use the Proxess Sync™ App to update locksets and gather their audit trail data to send to the ProxessIQ™ software, open the App and click on "Status" in the top menu. If Bluetooth on your phone is off, click "Enable" to turn it on or the phone will not be able to communicate with the locksets and no updating or downloading will take place.

NOTE: Before you will be able to proceed, it is also necessary to verify the phone has connectivity to the ProxessIQ™ software wherever it is located, via either the customer's WiFi or the mobile phone network. These are matters for resolution between the customer and the integrator and are not the responsibility of Proxess.

Sync with the Access Control System
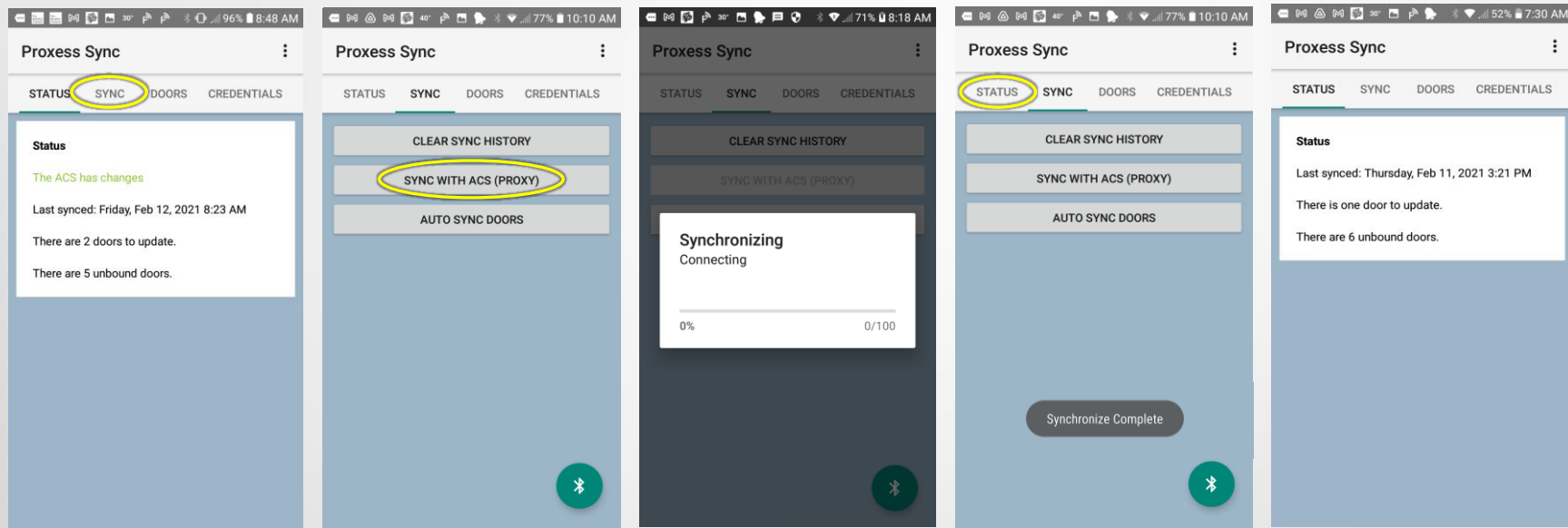
To perform any desired updates on the locksets, updates first need to be delivered to this phone. At this point, the phone does not need to be near any lockset. Click "Sync" from the top menu. The second screen above appears. Click "Sync with ACS" and the status bar will update you with progress and a note when the synchronization is complete.

Must Initialize a Lockset Prior to First Synchronization
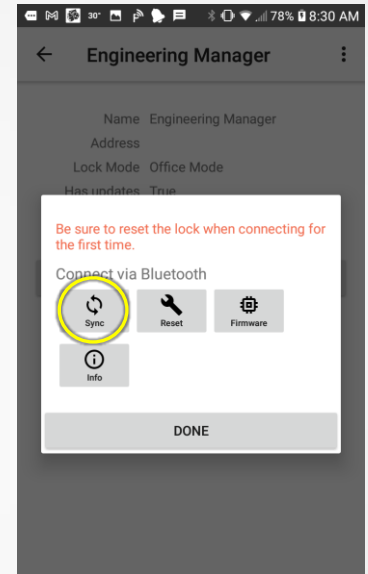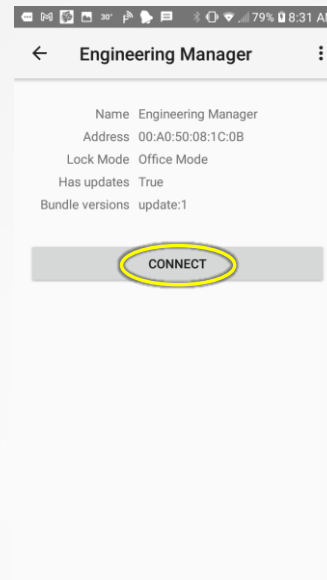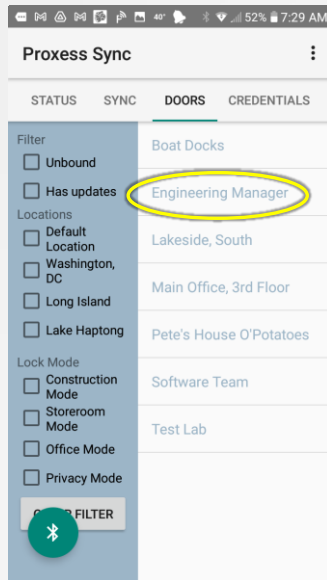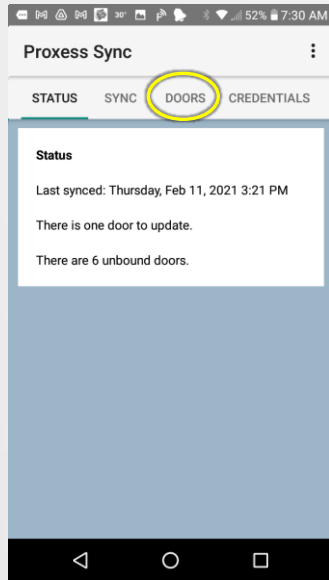
To initialize a lockset click on "Doors" from the top menu. To see the door you are looking for, check the box for the location your lockset resides in. That list of doors will appear. Click on the lockset name to be initialized and the menu for that door will appear. Click on "Connect" and then "Sync" on the following screen. Stand close to the lock so that the lock with the highest signal strength % is in front of you. Click on that Available lockset.
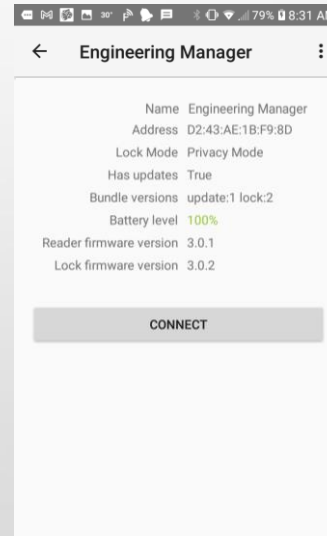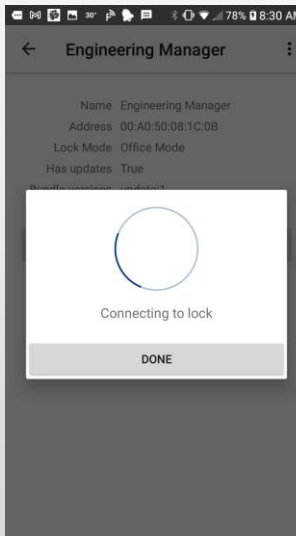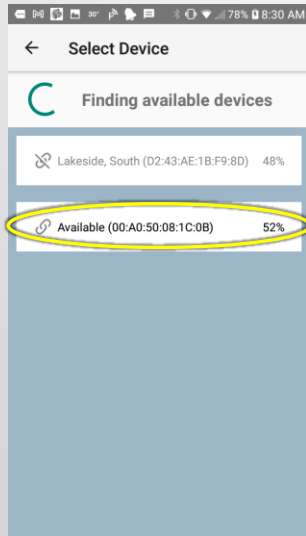
The status bar will appear and then the *Synchronization Complete* bar will appear. The configuration is complete and you may return to other screens in the App or connect to it again to update the firmware.

Automatically Sync with all (desired) Locksets
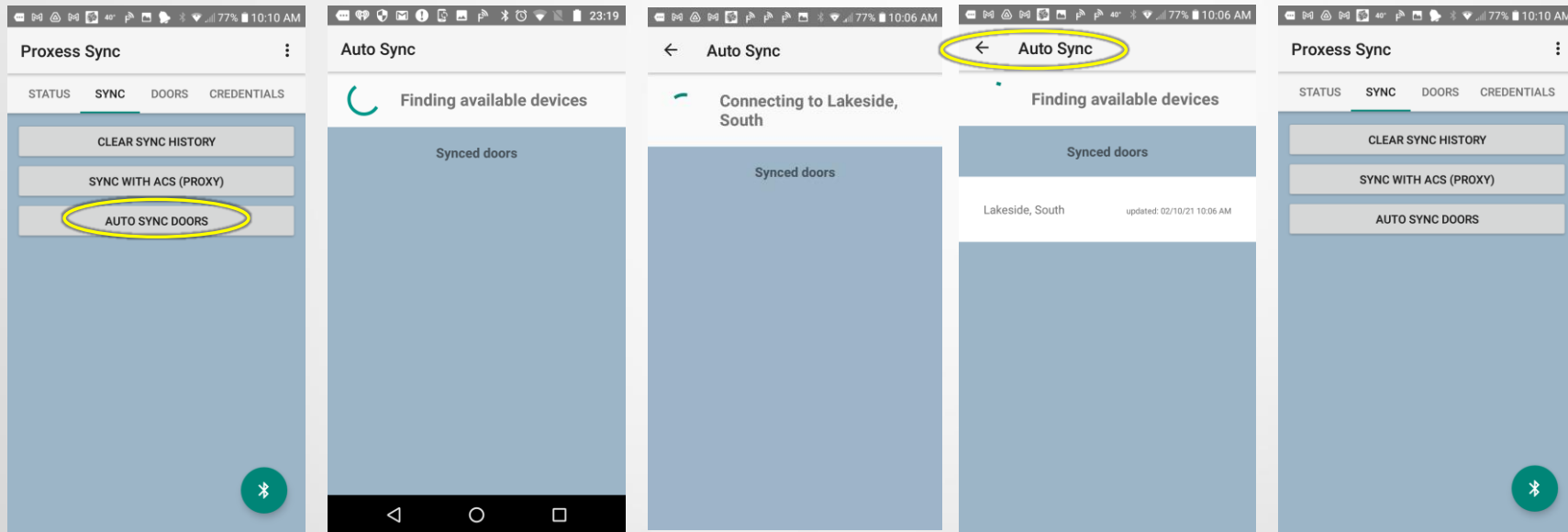
Once the ACS sync is complete and you are ready to update the locksets, click "Auto Sync Doors" and proceed to the first door to be updated. The 2nd (second) image will be shown as the App begins looking for locksets. The App will automatically begin the handshake, verification and update process when the 3rd image appears, usually within about 20 feet of a lock. However, it is highly recommended to remain close to a lock for it to sync quickly and completely, which is not just more reliable, but will also help to reduce the battery usage on the lock. The App will show when the update has completed. You may proceed to the next lockset(s) to be updated without the need to click on further buttons.

When complete, click the back arrow at the top of the screen to return to the main menu.

NOTE: During the update process, audits will be collected from the locksets and as long as there is connectivity to the ProxessIQ™ software, those audits will be uploaded to the software and will be immediately available in the system Event Log. Otherwise, you will need to tap "Sync with ACS" again to push the audits to the software.

Manually Sync with a Specific Lockset (1 of 2)
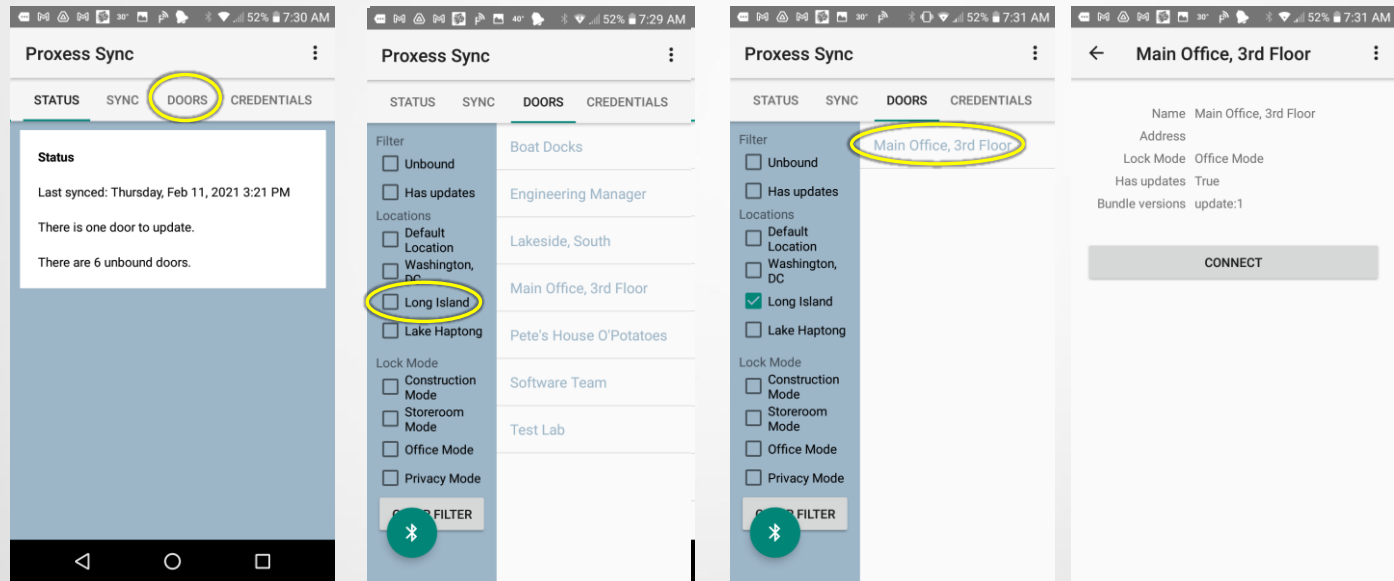
To manually perform any desired update on one specific lockset at a time, follow the instructions to "Sync with ACS" from the beginning of this section.

From the Home screen of the App, click on "Doors" from the top menu. To see the door you are looking for, check the box for the location your lockset resides in. That list of doors will appear. Click on the lockset name to be updated and the menu for that door will appear.

Manually Sync with a Specific Lockset (2 of 2)
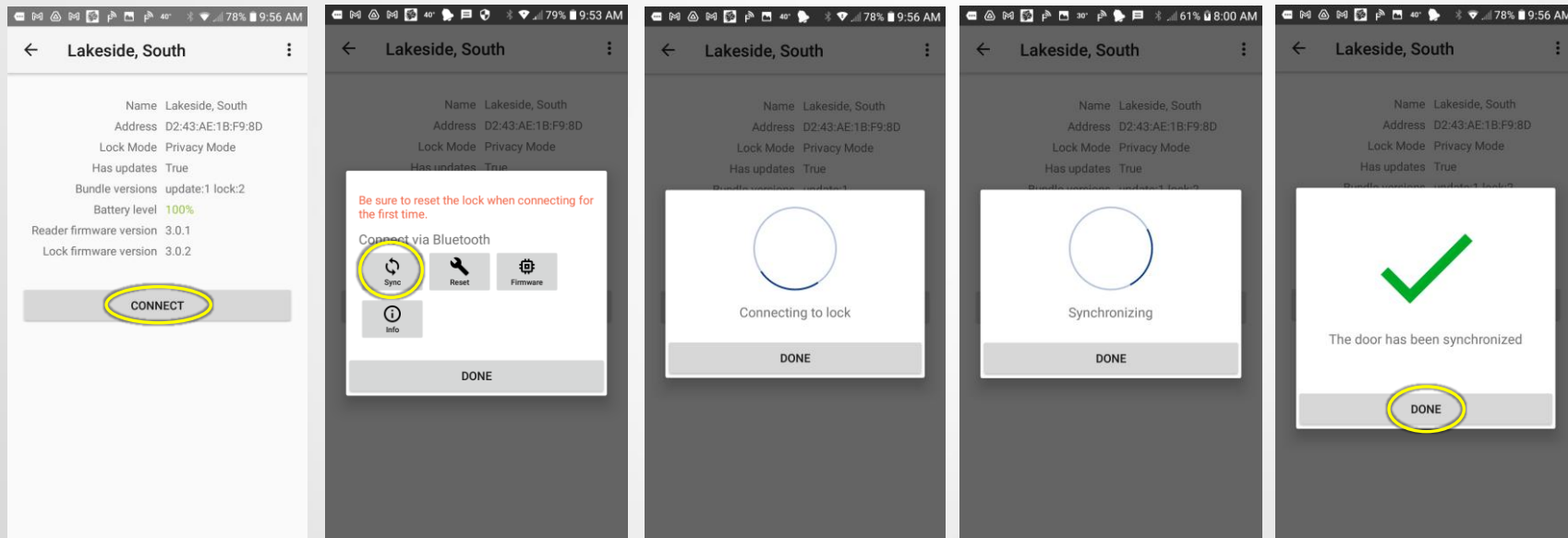
Proceed to the selected door and click "Connect" and the "Sync". The App will automatically begin the handshake, verification and update process. This can be accomplished, usually within about 20 feet of a lock. However, it is highly recommended to remain close to a lock for it to sync quickly and completely, which is not just more reliable, but will help to reduce the battery usage on the lock. The status will display as above. Click "Done".

NOTE: During the update process, audits will be collected from the locksets and as long as there is connectivity to the ProxessIQ™ software, those audits will be uploaded to the software and will be immediately available in the system Audit Log. Otherwise, you will need to tap "Sync with ACS" again to push the audits to the software.

MOBILE PHONE APP
FIRMWARE UPDATES & SYNCHING
with LOTS of DOORS AROUND
For both Apple & Android phones

iPhone

Firmware Updates for Locks, Readers & Controllers
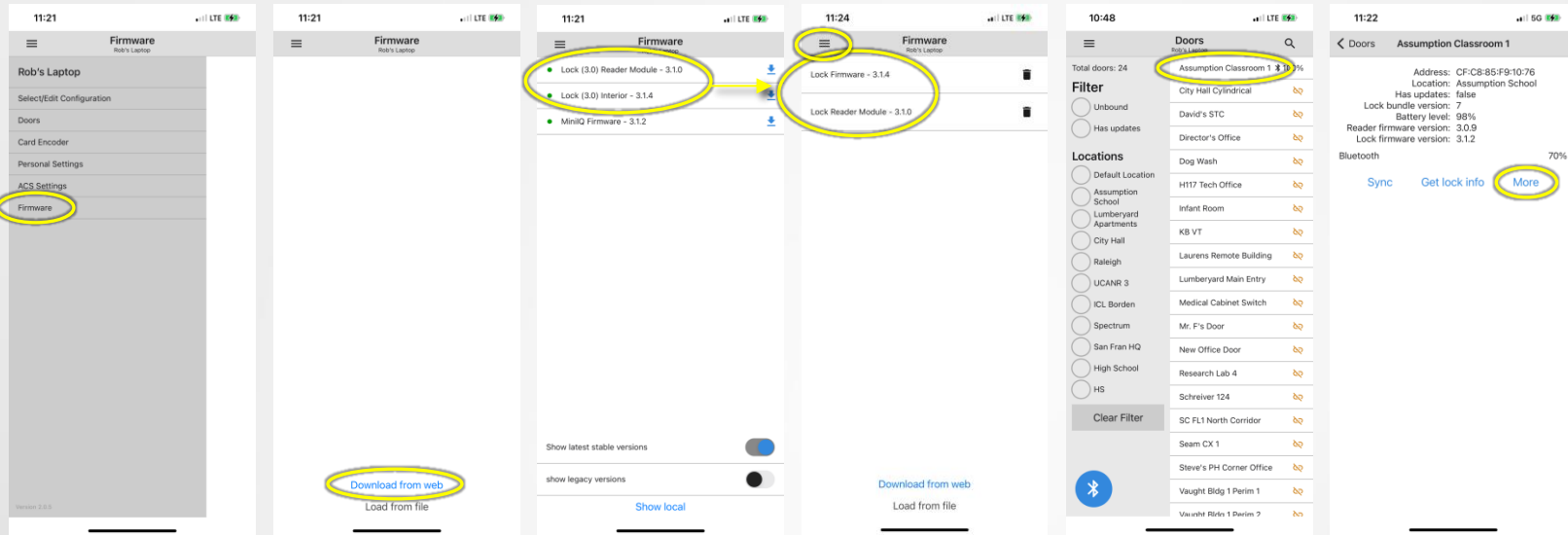
In Proxess Sync, click on the Menu button and then "Firmware" and then "Download from web". For a lock, download both the "Lock Interior" and "Lock Reader Module" files. They will show as loaded onto the phone. Click on the Menu button and click on the door/lock you want to update. Click "More" and then "Firmware". Select the first of the two firmware files and watch the update progress and then repeat the firmware update for the second file.

Finally, click "Reset and rebuild bundles" and watch the reset progress. The lock will be Reset and is upgraded. Go back to the Doors screen.
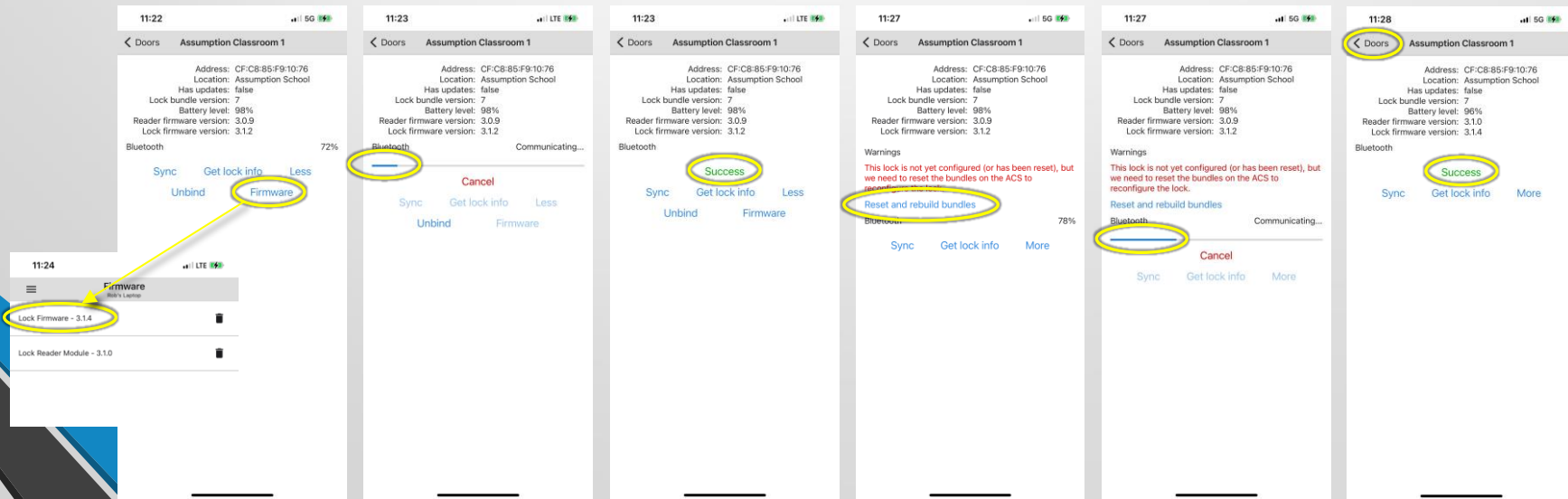
Synching When there are LOTS of Doors Around
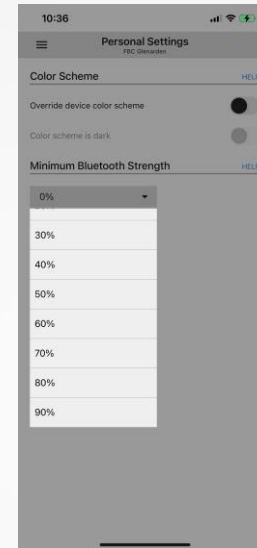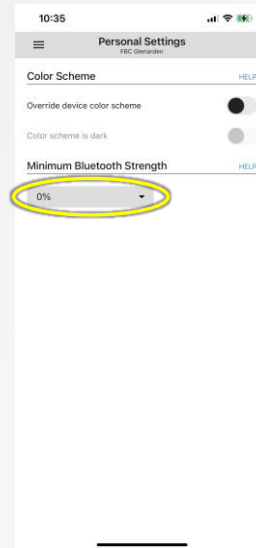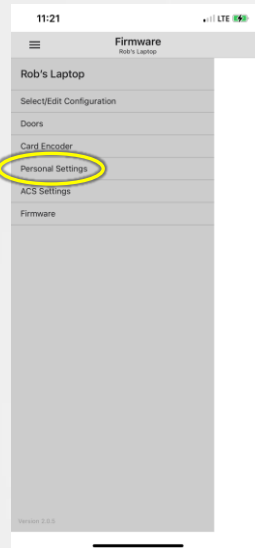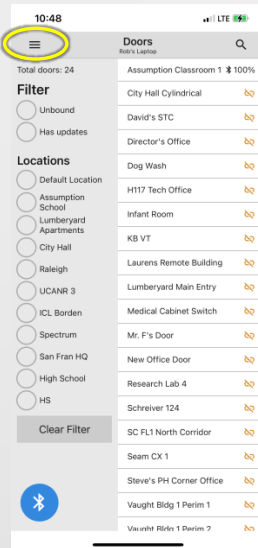
From the Home screen of the App, click on the icon highlighted in the image on the left; also known as the Menu or Hamburger button. The menu in the second image will appear. Click "PersonalSettings". The image on the right will open. The two features shown allow you to select the audit retrieval details for each phone. The first radio button allows the phone to automatically pull the audits off the locksets when they are synchronized. The second radio button authorizes the phone to delete the audit logs off of the locksets once they are uploaded into the App.
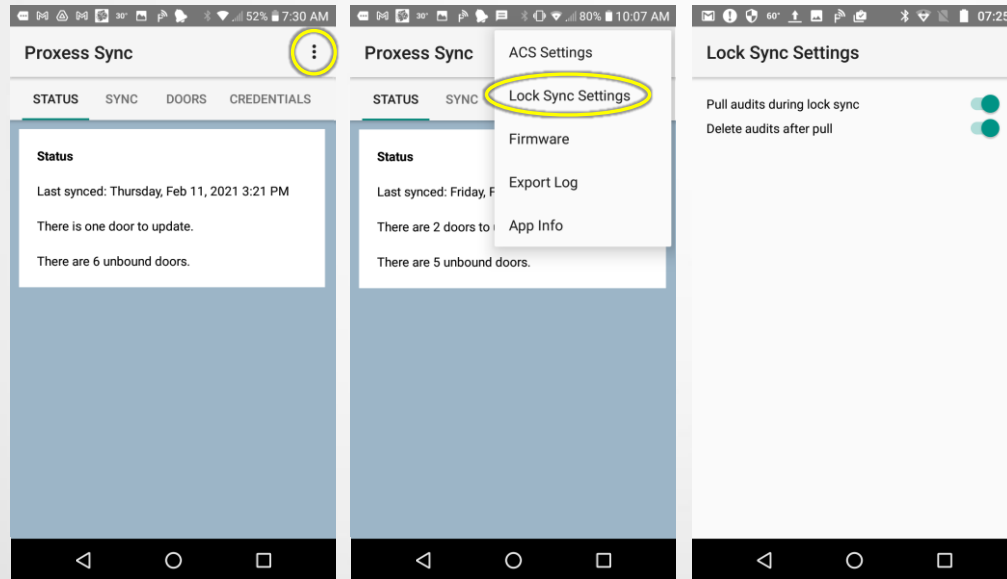
Sync Settings

From the Home screen of the App, click on the icon highlighted in the image on the left. The menu in the middle image will appear. Click "Lock Sync Settings". The image on the right will open. The two features shown allow you to select the audit retrieval details for each phone. The first radio button allows the phone to automatically pull the audits off the locksets when they are synchronized. The second radio button authorizes the phone to delete the audit logs off of the locksets once they are uploaded into the App.

Lockset Firmware Uploading (Preparation)
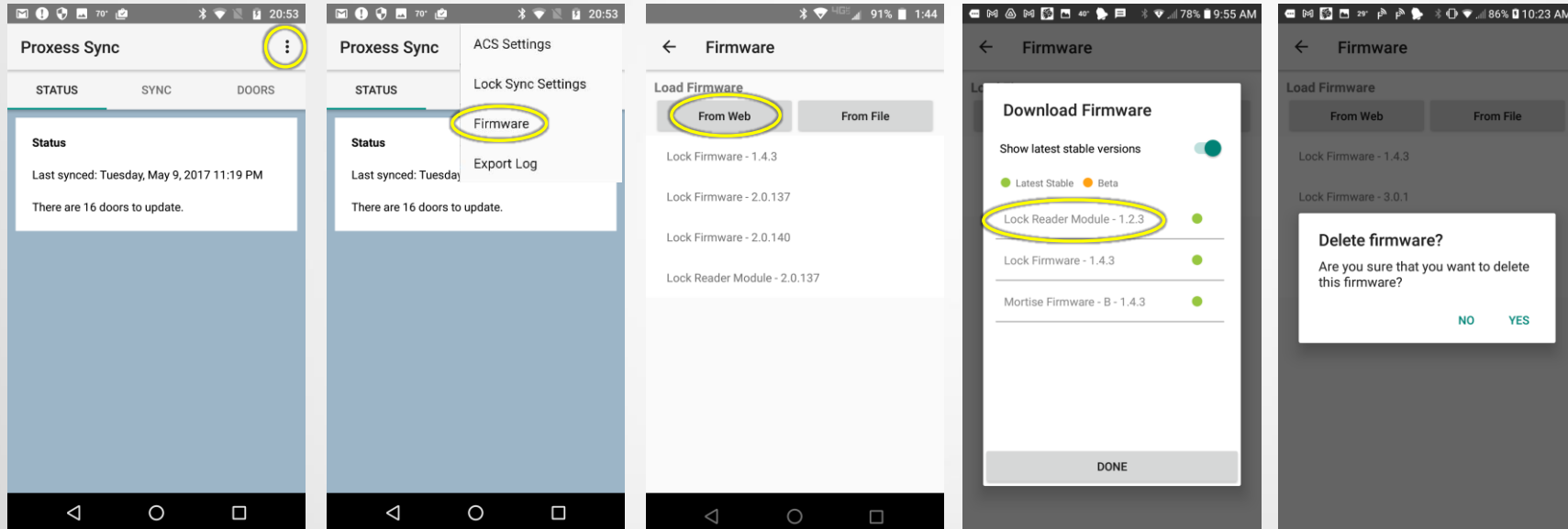
There are two (2) sets of firmware on each lockset, one for controller operations and one for the reader PC board.
Note: For the Cylindrical locksets, only download the Lock Firmware file. For the Mortise locksets, only download the Mortise Firmware file. The reader module firmware is the same for both Cylindrical and Mortise locksets.
To retrieve the latest versions, click the 3-dot icon highlighted above and then select "Firmware". If the file(s) you need have already been downloaded to the phone (as they will be shown in the above list), then you may just click on it to begin the download process to the lockset (only one file at a time may be downloaded). Once you are done with the firmware, or if there is an obsolete firmware shown in the list, you may press and hold that item and tap "Yes" when asked to delete that firmware version.

Lockset Firmware Downloading –
From Web & Device
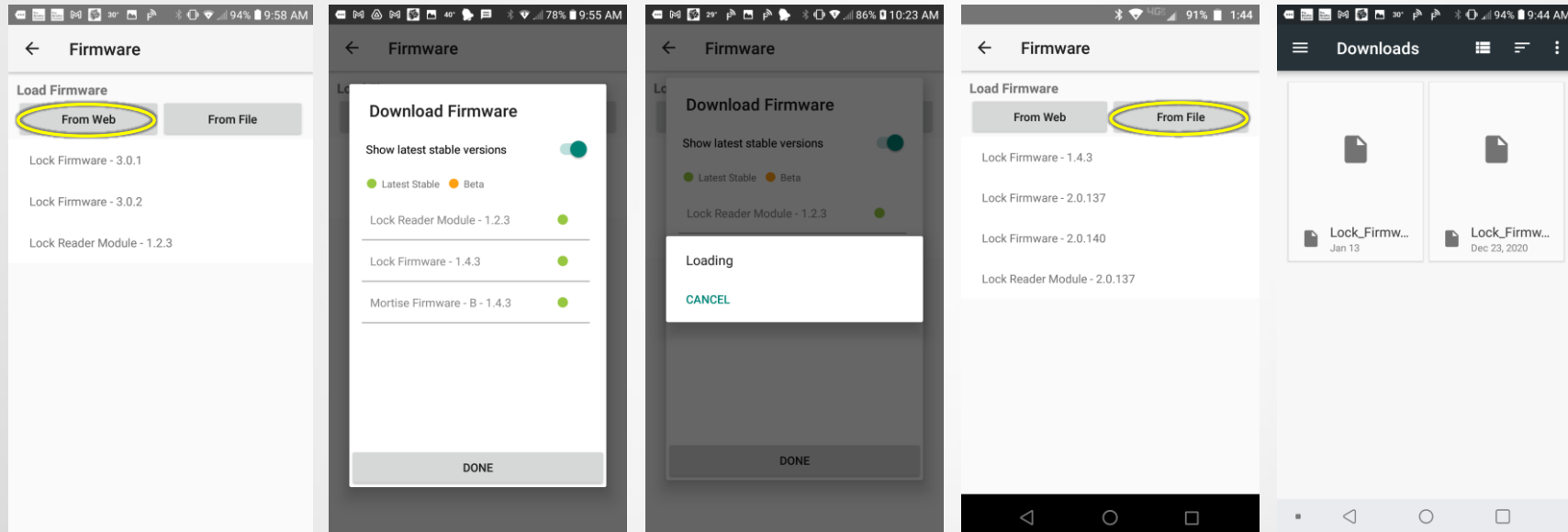
On the Settings-Firmware page, you may load firmware onto (the proper folder in) your device from either the Proxess website, or your device. To load firmware from the Proxess website, just tap "From Web" and the available firmware (that is Not already on your device) will be listed. If allowed, you will be able to tap and select a Beta version. Tap (one at a time) each of the firmware files you need and they will automatically download onto your phone and will then appear in the list.

On the Settings-Firmware page, to load firmware onto the proper folder in your device from a general file folder on your device (You may have received the firmware as an email attachment, for instance), tap "From File". Tap (one at a time) each of the firmware files you need and they will automatically download onto your phone and will then appear in the list.

Lockset Firmware Downloading (Execution)
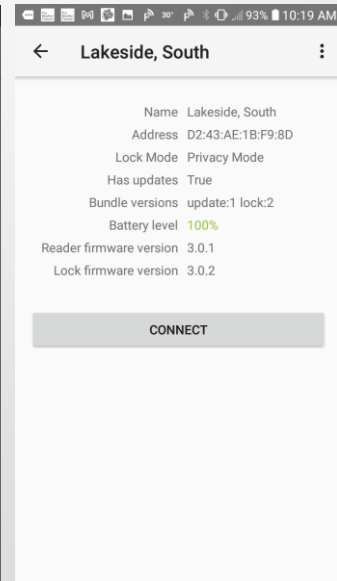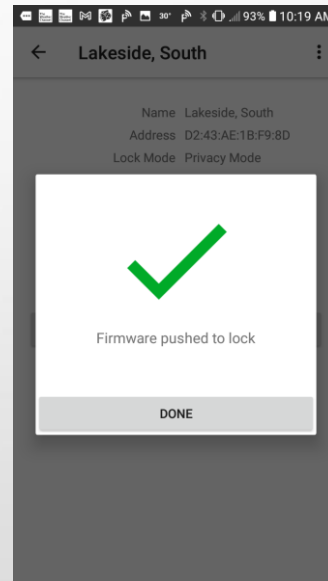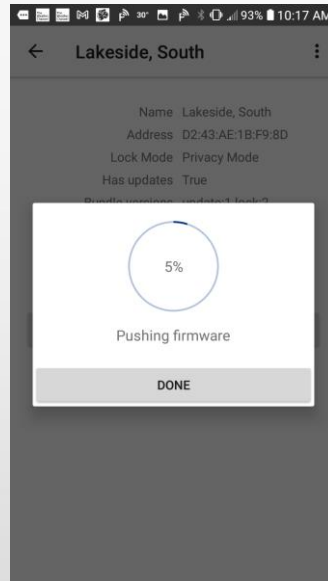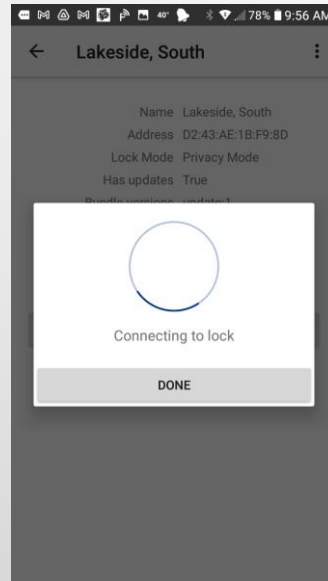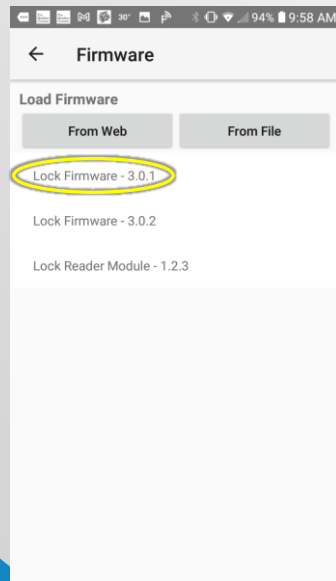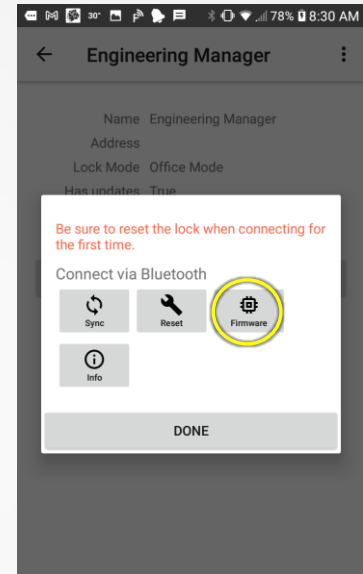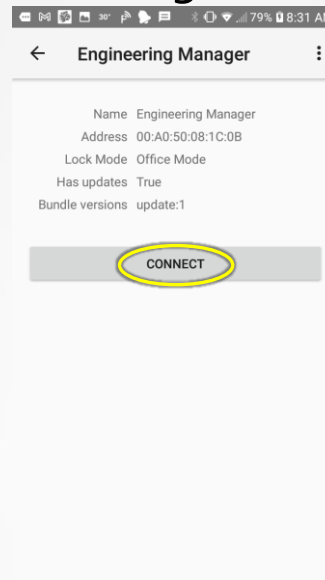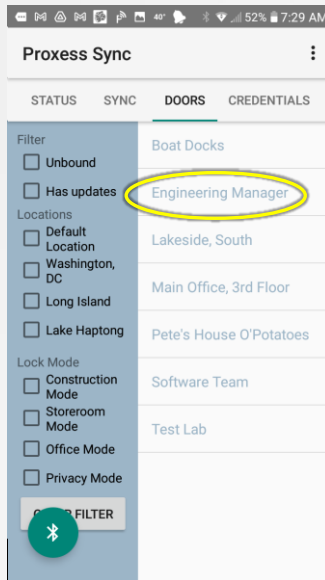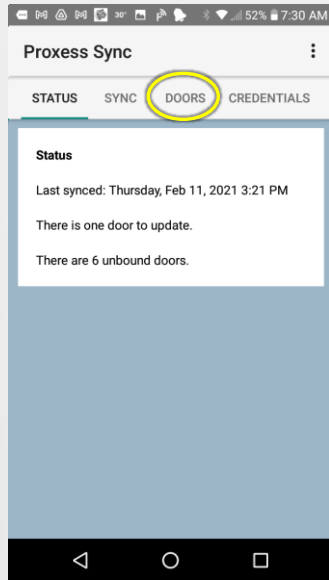
To perform the lockset firmware update, select "Doors" from the top menu. Select the location in which the lockset is located and then select the door from the resulting list. Click "Connect" and then tap "Firmware". Select the firmware from the list you wish to update onto the lockset. The lockset will connect and begin pushing the firmware. When completed, the updated firmware versions and battery life will display. The lock will reset, returning it to Construction Mode and then must be re-synch'd using this app to work with the credentials programmed into this system.

Proxess Sync App Message Log Export
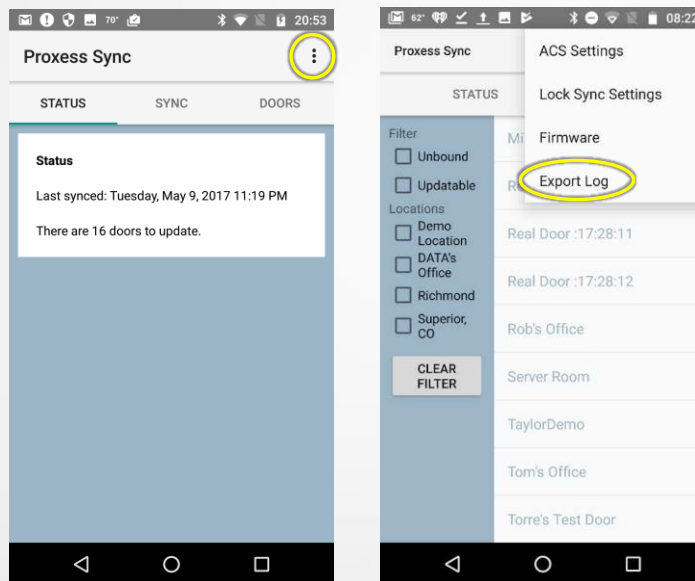
For advanced diagnostics, usually upon request from the Proxess Technical Support team, the Proxess Sync™ App maintains a support message log, which can be exported and emailed to Tech Support.
From the Home Screen of the App, click on the icon above and then click on "Export Log" from the resulting menu. Email the file that is downloaded into the phone's file directory.

TIME SCHEDULES
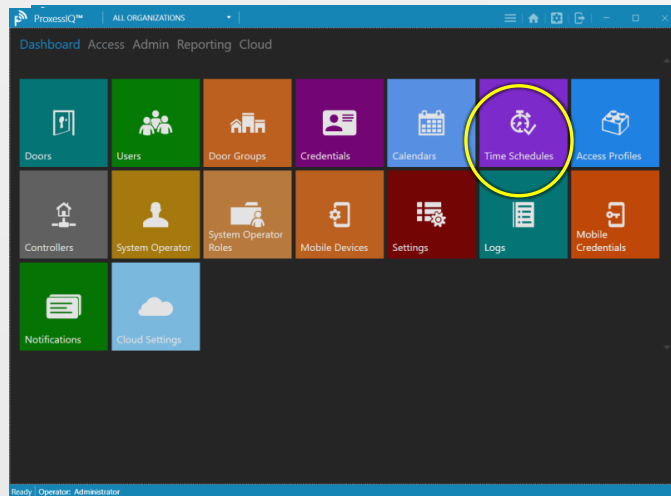
From the Home screen \ Dashboard, click "Time Schedules".
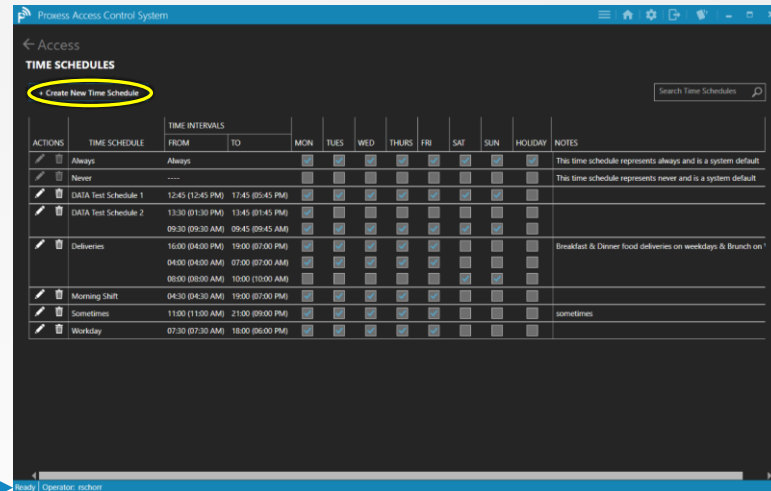
Click "Create New Time Schedule". You may use the Search box in the top right to find specific Time Schedule names if the list is longer than what is seen in the current view. You may edit or delete any existing schedule by clicking on its icon on the left side.
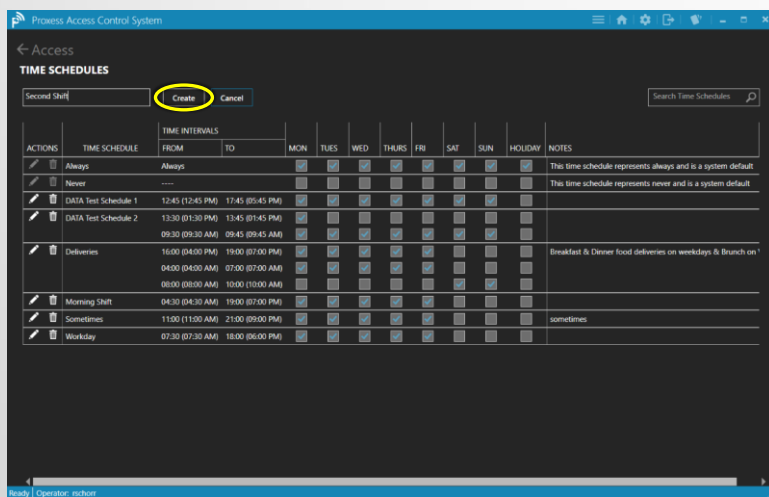
Type in a name for the new Time Schedule and click "Create".
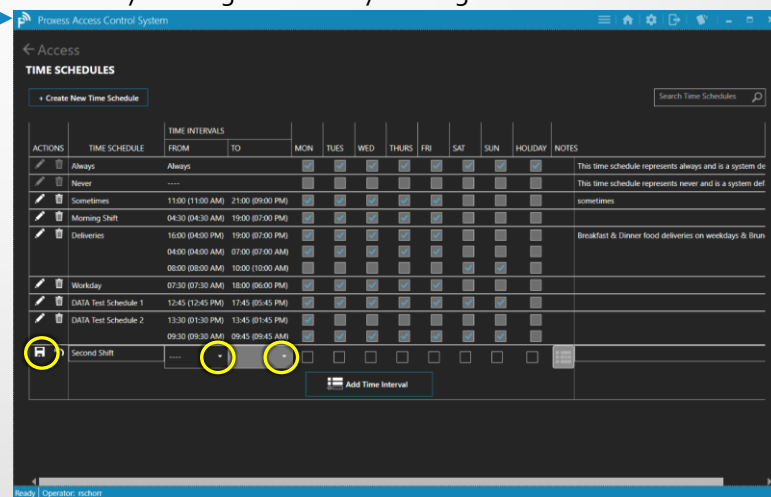
The new Time Schedule will appear at the bottom of the list. To select the overall time for it click the dropdown buttons for both the "From" and "To" columns. Select the days of the week in which this will be in effect and whether it will apply during Holidays. Optionally, add a note to describe the use of this schedule. Click the "Save" icon on the left side of the screen.
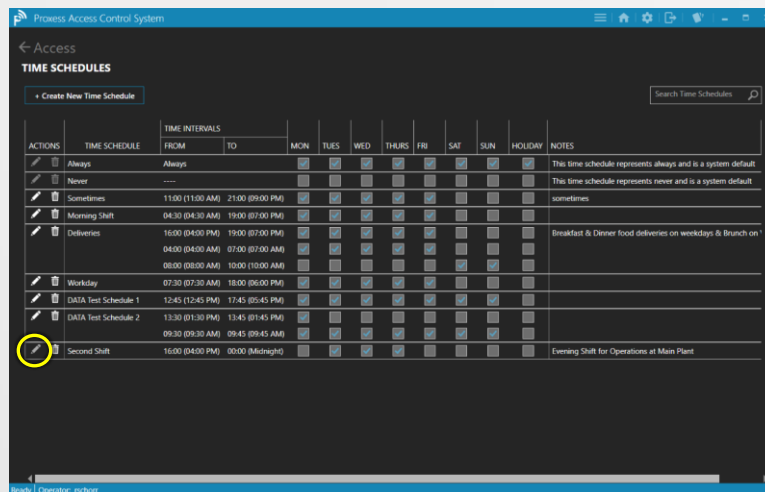
To make changes, or to add Time Intervals, click the Edit icon.
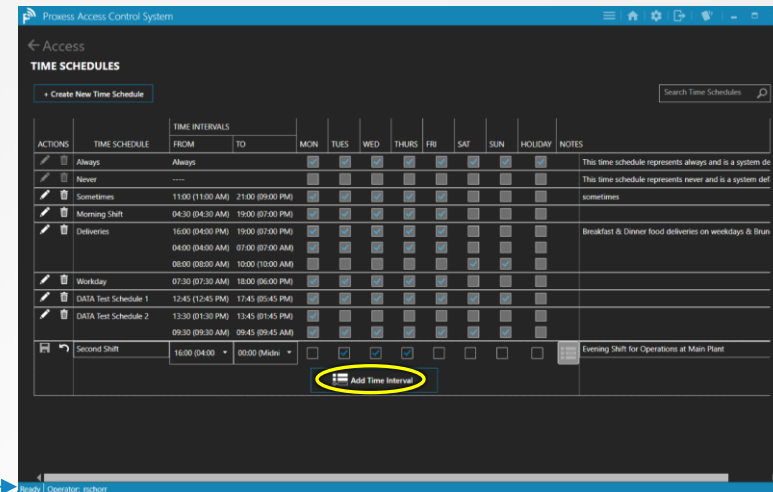
Click the "Add Time Interval" icon.
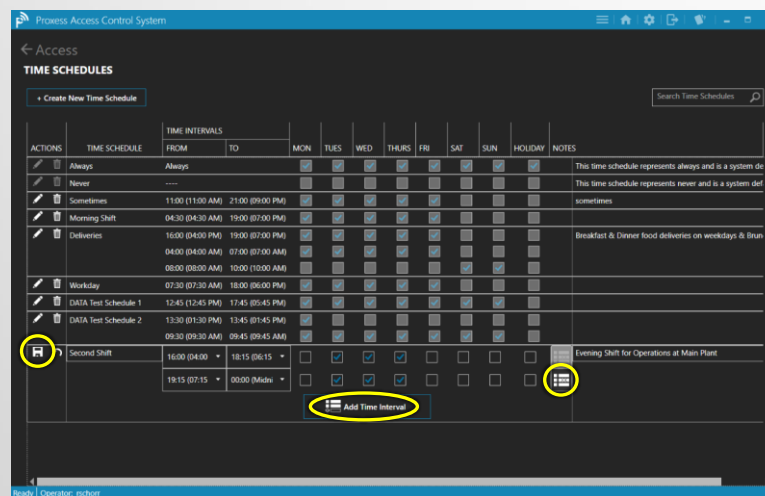
Add the second Time Interval and adjust the overall interval you previously entered. This could be used for a lunch period, for instance. In this case, the cards would grant access in the working areas during these intervals, but would deny access during the gaps between the intervals. Click the Save icon on the left, the Delete Interval icon on the right, or the Add Time Interval button.
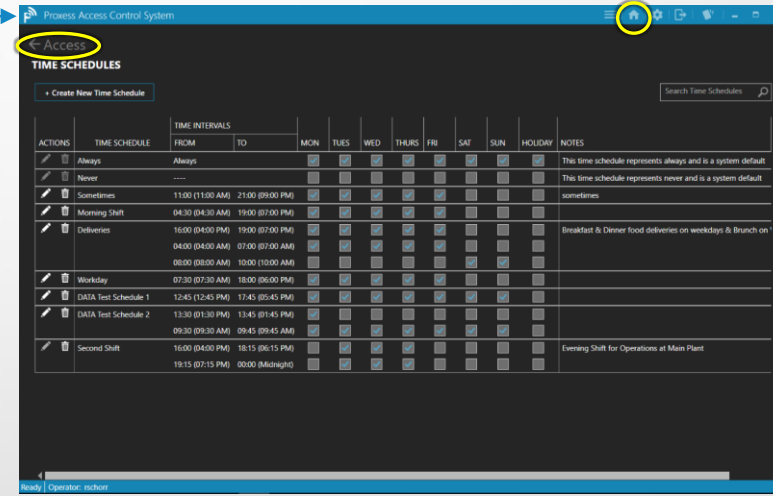
This is the screen you will see if you clicked Save. To return to the Home Screen \ Dashboard, click either "Access" or the Home icon in the top taskbar.

1-Minute & 5-Minute Increments for Time Schedules

For following Bell schedules, etc.
Enabled by each Client/Workstation

This is a licensable feature, available upon request from the Proxess sales team.
- Once licensed, each workstation can select it's time increment.
- The ProxessIQ default is 15-minute increments and may be set to either 1 or 5-minute increments.
- Be mindful that it may be annoying to spin through small time increments, so it may be better to set all your non-small increment time schedules first and then change over to the smaller increment for just those schedules that need it.

Up to 24 total Time Intervals can be added within a single Time Schedule. You can **only** add more than 4 Time Intervals for use as an **Unlock** Schedule, such as to abide by school Bell Schedules.

When selecting times, you can type the number for the hour and it will be highlighted and/or you may scroll to the time you want.

Time Schedules - 4

DOOR GROUPS

Before proceeding to create Door Groups, please review our online tutorial, which will greatly simplify your data entry and ongoing maintenance:

www.proxess.com/Proxess/media/Proxess/Documents/ProxessIQ-Manual-without-Hidden-Slides_3.pdf?ext=.pdf
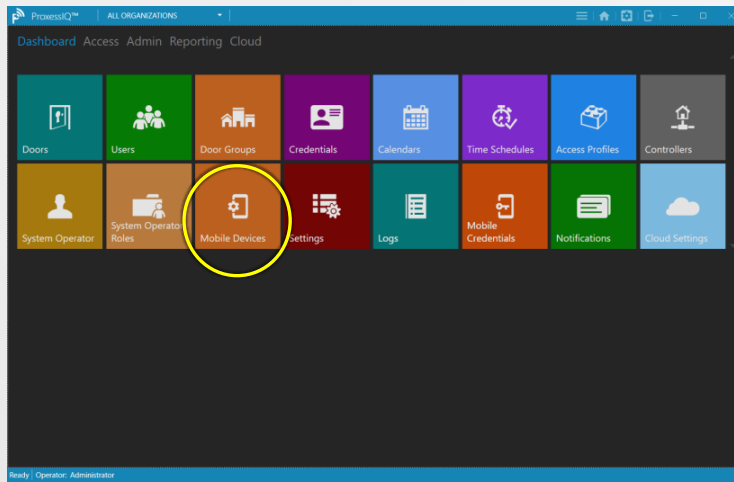
From the Home screen \ Dashboard, click "Door Groups".
Before adding Door Groups , consider adding any custom Time Schedule and Access Profiles you desire.

Click "Add New Door Group" to do so. You may also use the Search box in the top right to find existing Door Group names, if the list is longer than what is seen in the current view. You may edit or delete any existing Door by clicking on its Pencil/Edit icon on the left side.

Enter the name for the new Door Group. "External ID" and "Notes" are not mandatory and are just for the administrator's reference. Checking the "Auto Enroll" box will cause all future doors that are added into the software to be enrolled into this Door Group. Click "Save" to do so.

Click on "OK".

Click on the "Doors" tab to add the Doors that will become a part of this new group.

Click "Add New Door Group" to do so. You may also use the Search box in the top right to find existing Door Group names, if the list is longer than what is seen in the current view. You may edit or delete any existing Door by clicking on its Pencil/Edit icon on the left side.

Enter the name for the new Door Group. "External ID" and "Notes" are not mandatory and are just for the administrator's reference. Checking the "Auto Enroll" box will cause all future doors that are added into the software to be enrolled into this Door Group. Click "Save" to do so.

Click on "OK".

Click the drop-down arrow and from the list that appears, select the first Door you wish to add to this Door Group. Then click the "Add" button.
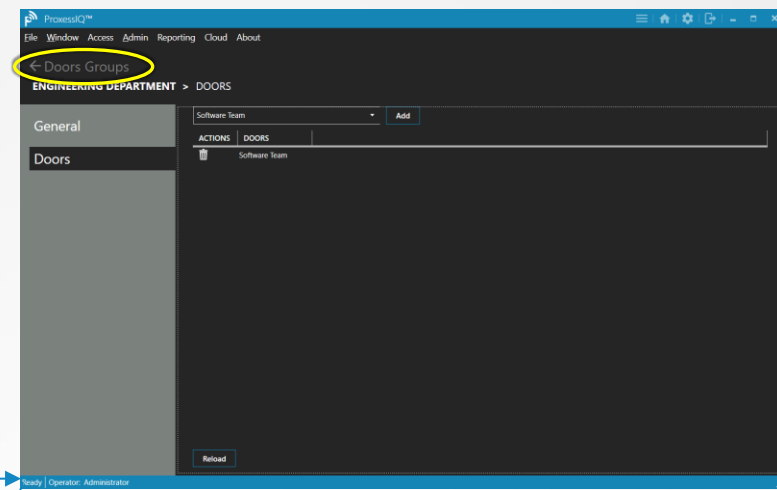
The door will now appear in this list. You can continue to add doors to this new Door Group and Delete doors from this group. Once you have added all the doors desired for this group, you may return to the main Door Groups screen.
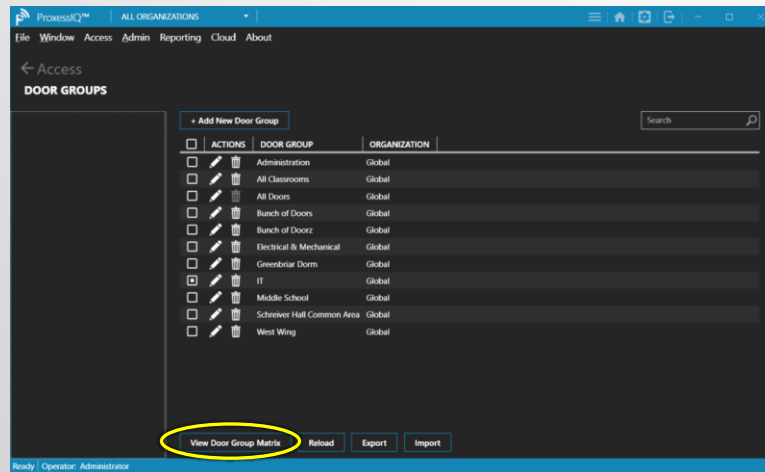
Click the View Door Group Matrix button.
The complete matrix of all your doors and Door Groups will appear, for verification of your programming efforts.

You may now return to programming in other sections of ProxessIQ.
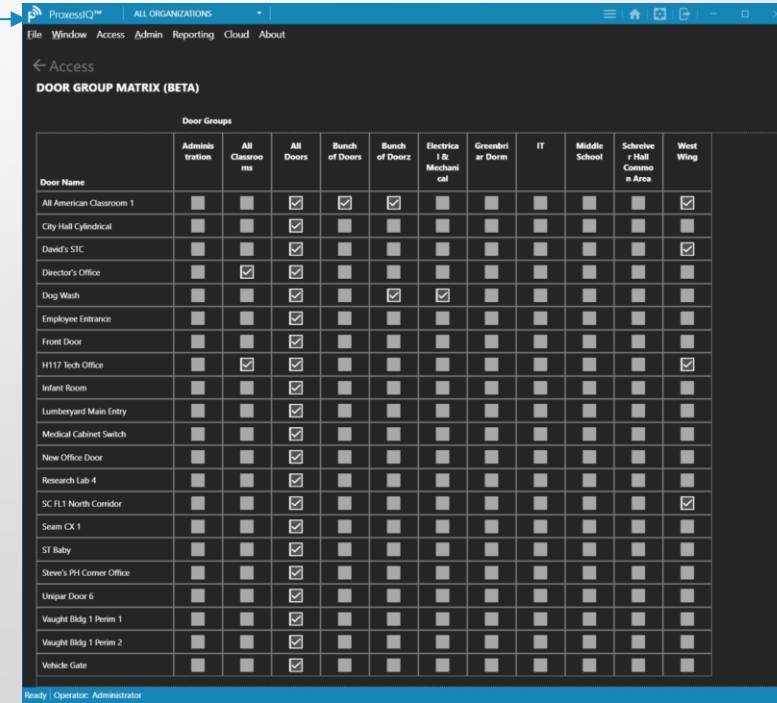
DOORS

Creating, Synchronizing & Configuring
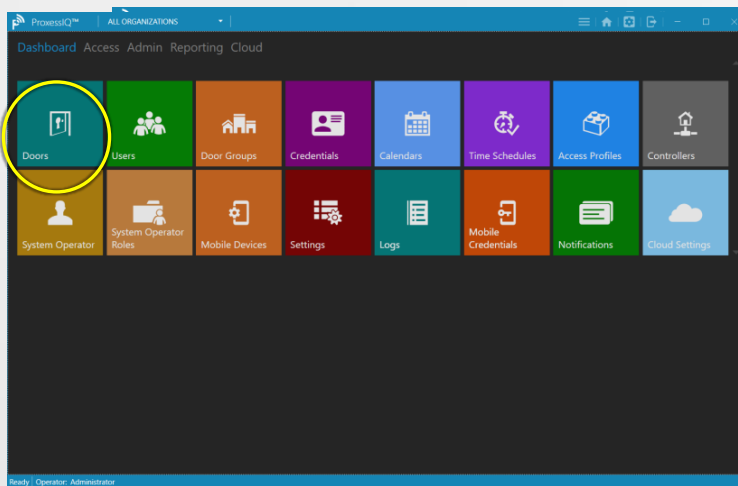
From the Home screen \ Dashboard, click "Doors". Before adding Doors, consider adding any custom Time Schedule and Access Profiles you desire.
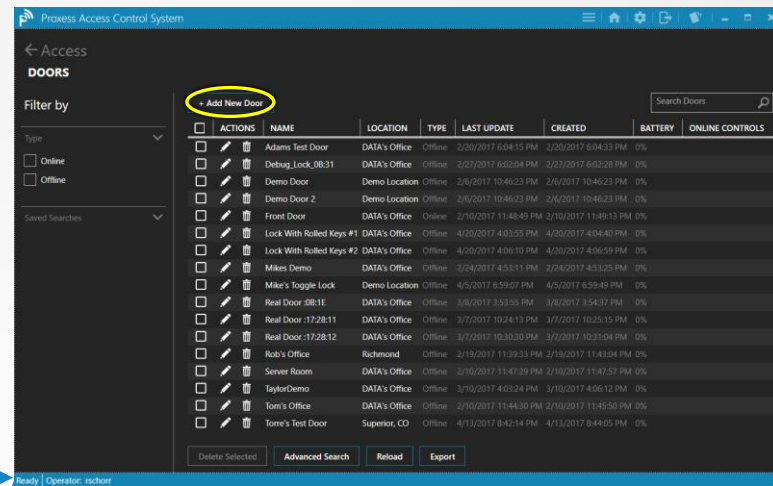
Click "Add New Door" to do so. You may also use the Search box in the top right to find existing Door names, or Filter the list by "Online" or "Offline" types using the checkboxes on the left if the list is longer than what is seen in the current view. You may edit or delete any existing Door by clicking on its icon on the left side. We will go over Advanced Searches at the end of this section.
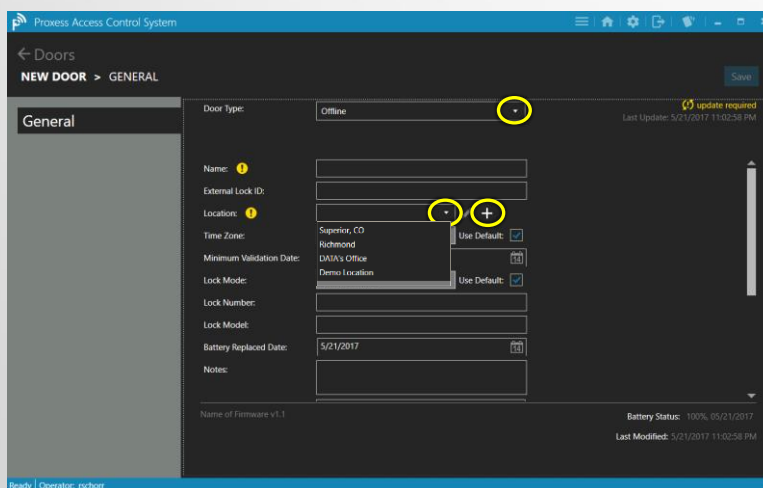
Select if the door will be online or offline. This selection will let the software know how to attempt to connect with this door for updates and on-demand commands. If you select "Online" you will need to add a Controller in a later section to connect it with.
Type in a name for the new Door and select a location from the dropdown arrow as shown above. To create a New Location, click the "+" shown above.
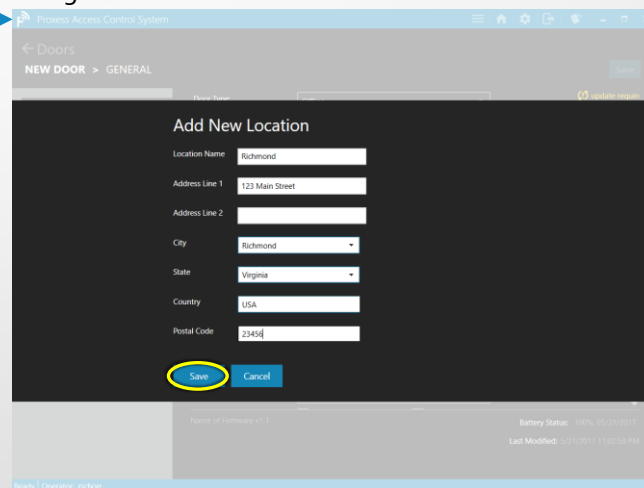
The "Add New Location" screen appears. Enter a "Name", and any other information you desire. Click the "Save" button to complete the action.

Adding & Editing Doors - 1

Continue entering information for the door. Add the Time Zone the door resides in and a Validation date for the door, which is typically used in the education and office leasing markets. A battery replacement date can also be put on a calendar. Select the appropriate Holiday Calendar and the Unlock Schedule when the door would not require a card for entry. A cardholder with a "First person In" card may be enforced before the door unlocks if the box is checked. The door may be put in a Toggle mode of operation during a specific time schedule. A Card-only schedule can be set for those doors where combination reader-keypads are installed. Finally, enter the times a door remains in the Unlocked position after a valid swipe, in the Extended Unlocked position, is Held Open and is Held Open-Extended and set. "Default" values may be found in the "Settings" module and in the "Door Defaults" tab. Click "Save" when done. Click "Doors" on the screen on the right.

Click "Advanced Search".

The Advanced Search bar appears. Click the first dropdown arrow to select the field or item you want to more granularly search. Click the second dropdown arrow and a context-sensitive list of information will appear to select from.

Initialize a Lockset (1 of 2)

NOTE: Once a new lockset Door has been created in the software, it **MUST** be initialized for operation using the Proxess Sync™ mobile App. **This initialization process is detailed here and it may be done at this step in the programming process,** or anytime until you need the door to be in service.
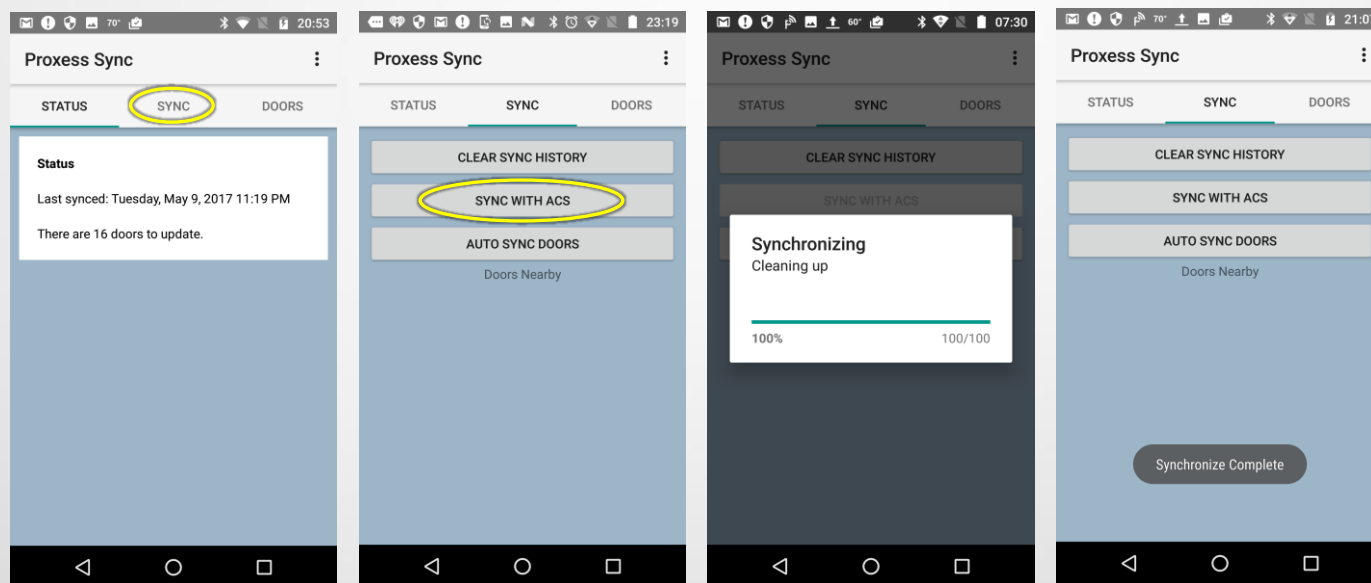
To perform any desired updates on the locksets, updates first need to be delivered to this phone. At this point, the phone does not need to be near any lockset. Open the Proxess Sync™ mobile App and click "Sync" from the top menu. The second screen above appears. Click "Sync with ACS" and the status bar will update you with progress and a note when the synchronization is complete.

Adding & Editing Doors - 4
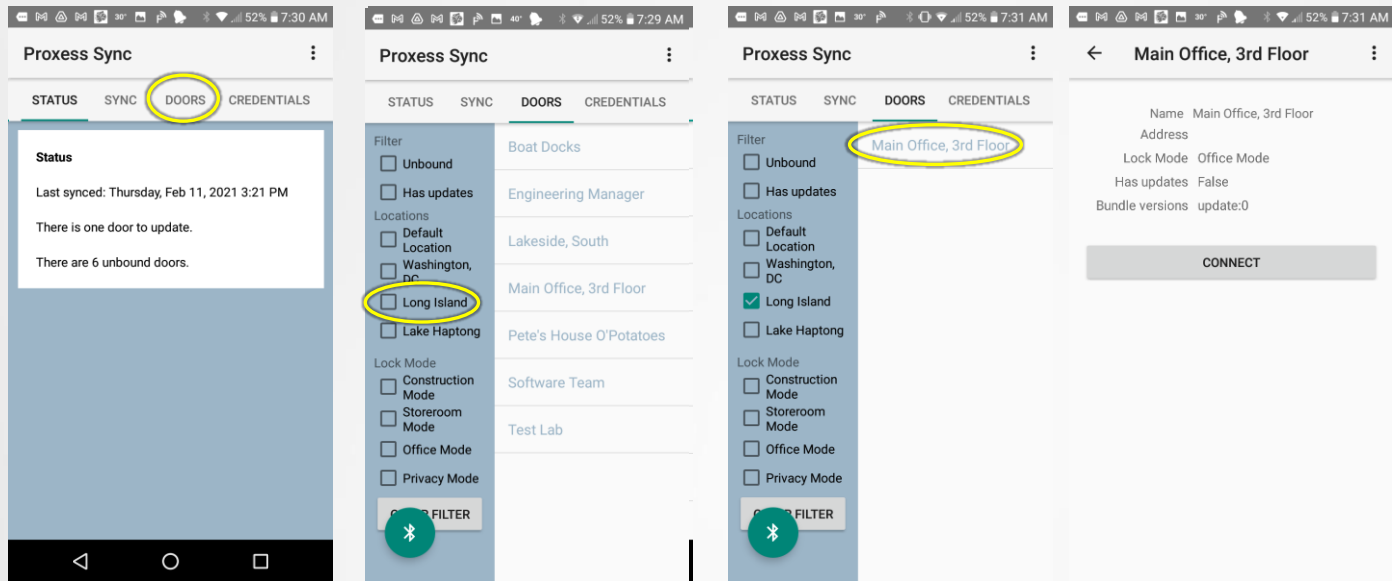
To initialize a lockset click on "Doors" from the top menu. To see the door you are looking for, check the box for the location your lockset resides in. That list of doors will appear. Click on the lockset name to be initialized and the menu for that door will appear. Click on "Connect".
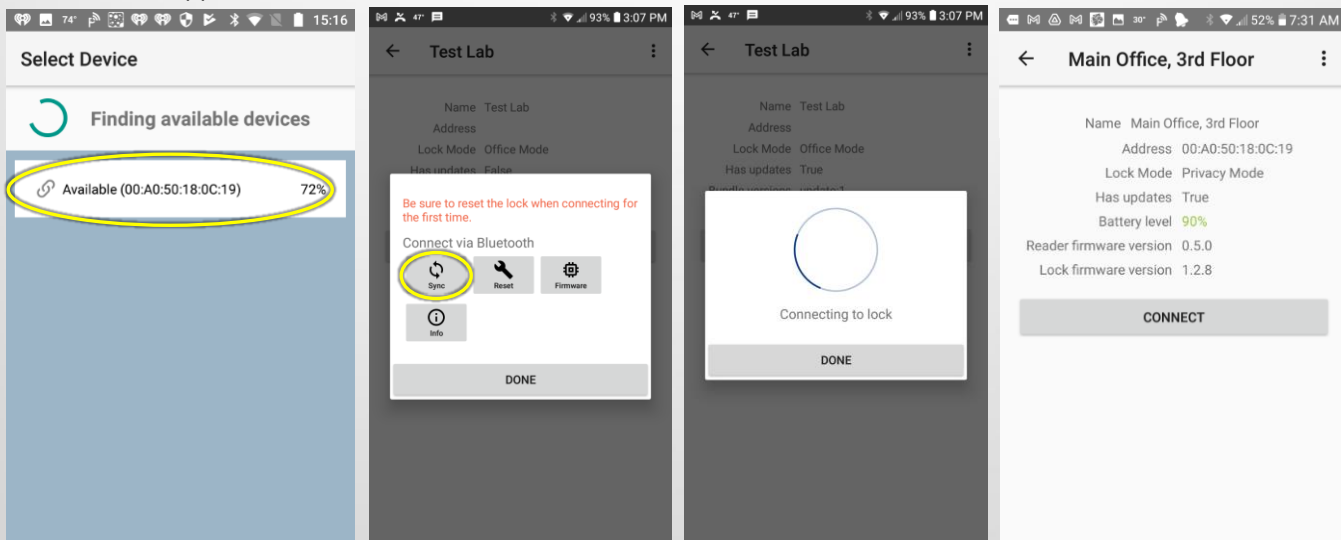
If the select device screen appears, click on the device with the greatest signal strength. Click the "Sync" button and once initialized, the battery level and firmware version for the lock's boards will display. The initialization is complete and you may return to other screens in the App or simply close it.

Replacing or Resetting a Door
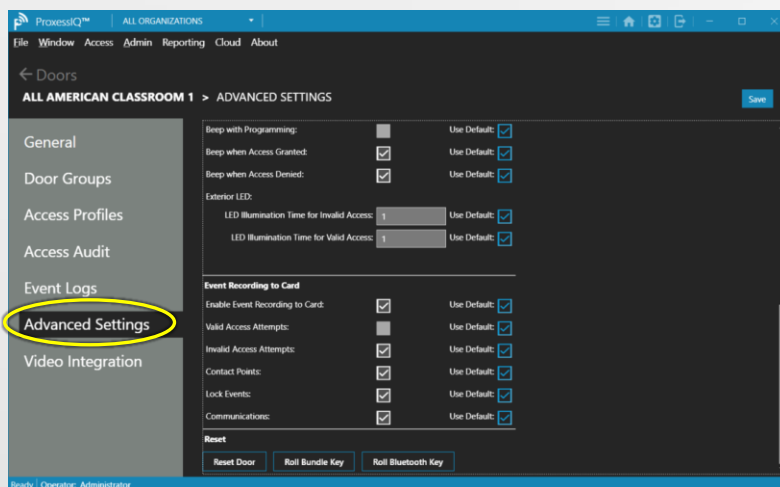
When a lock needs to be replaced or reset to its factory configuration, go to the Advanced Settings tab and click on the "Reset Door" button.
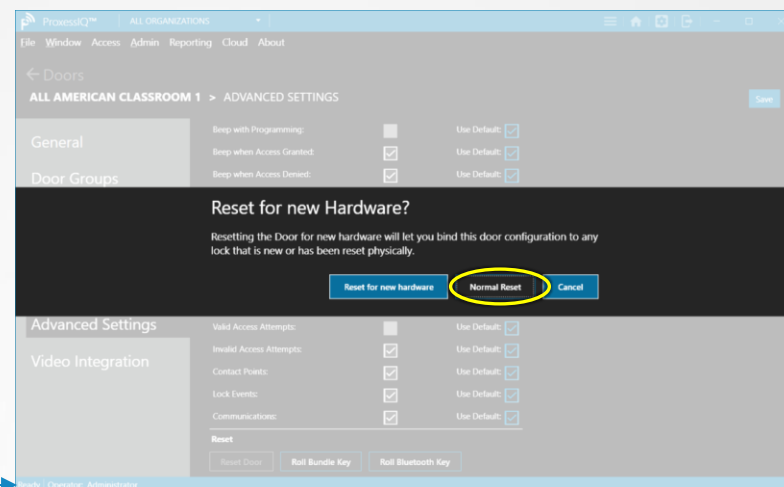
If you are just resetting the original lock, perhaps after repairing the wiring or after a firmware upgrade, click on "Manual Reset". Click Cancel to stop this process.
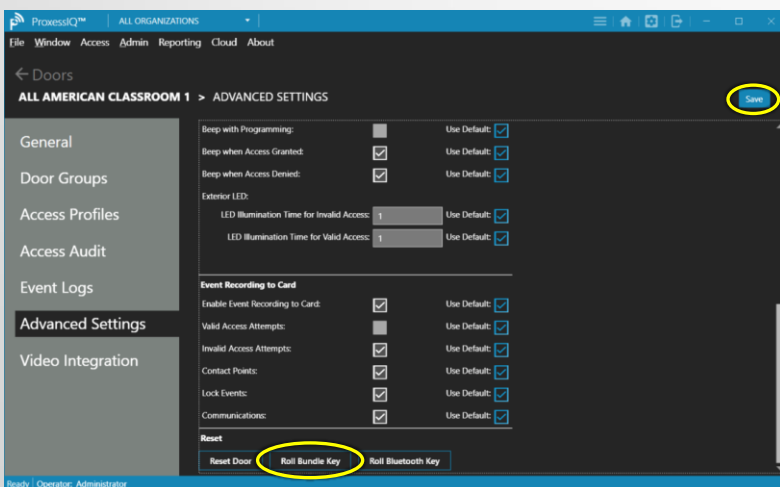
It is not necessary unless the IQ Mobile/Sync app requests it, but it is good practice to also click "Roll Bundle Key". If the IQ Mobile app requests it, you will then need to click "Roll Bluetooth Key". Then click "Save"
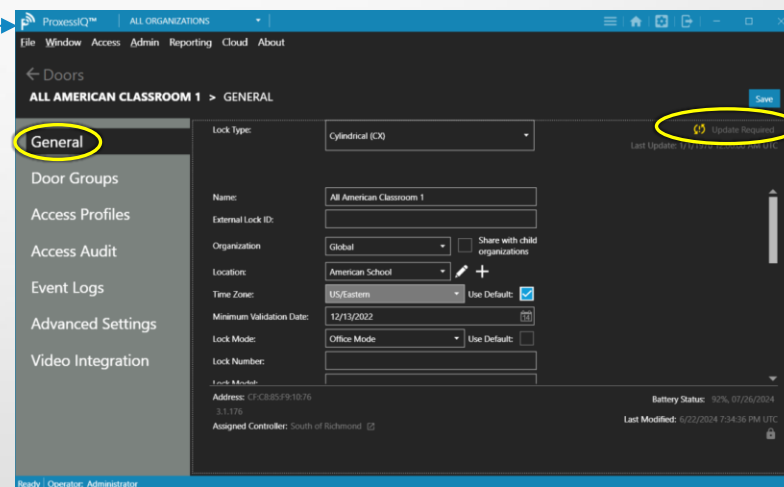
Go back to the General tab and you will notice the lock has changes, which will require you to now go to the lock and Reset and re-synchronze it.

To reset the lock, remove the battery cover, the lever and the trim screws.

Remove the trim off of the backplate while holding onto the bottom half of the trim, pulling it straight off (as in, not on an angle).

Press the blue reset button 3 times in rapid succession (3 times within 3 seconds) and the lock will go into a flash sequence.

Reconnect the lock, by first carefully placing the trim back onto the backplate, pressing straight into the door (not on an angle), assuring the white connector (2 rows of 8 pins) at the bottom of the trim snaps into place.

As the lock is reconnected, you can listen for the motor to re-spin, assuring the lock is ready to be synchronized.
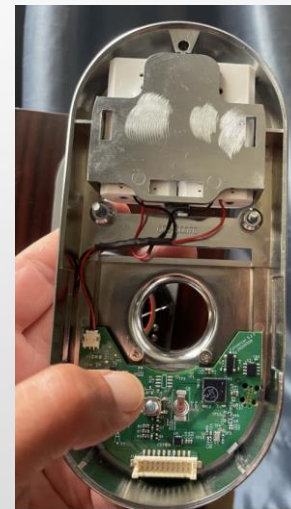
Re-Synchronizing or Resetting a Door with Proxess IQ Mobile /Proxess Synch
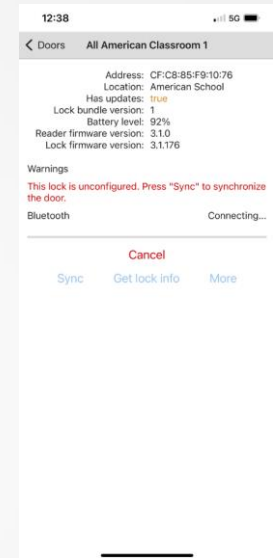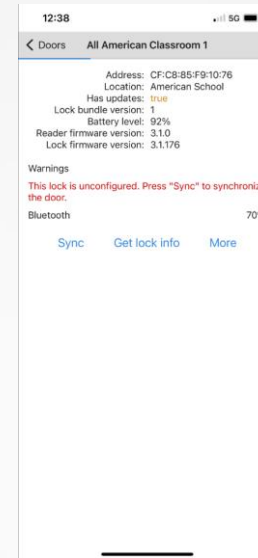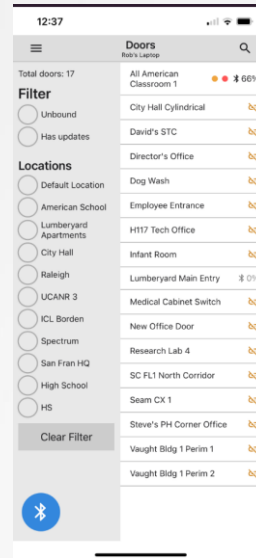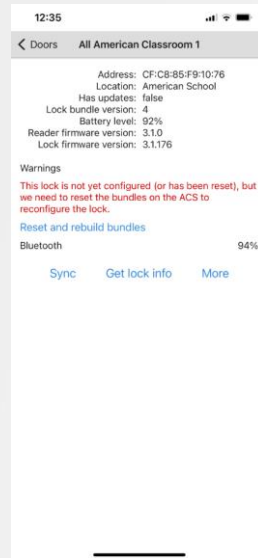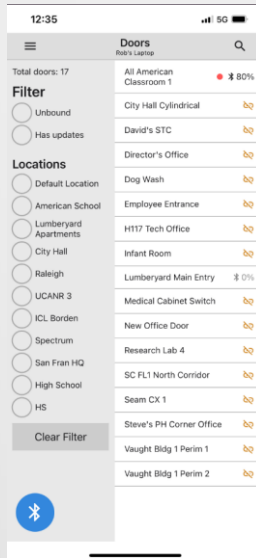
Once the lock has been reset in the software and the lock has been physically reset, open the ProxessIQ Mobile/Proxess Sync app on your phone.
On the Doors screen you will note a red dot by any door that has been reset and that needs to be re-synched.
Follow the screenshots on this page to complete the reset process for the lock.
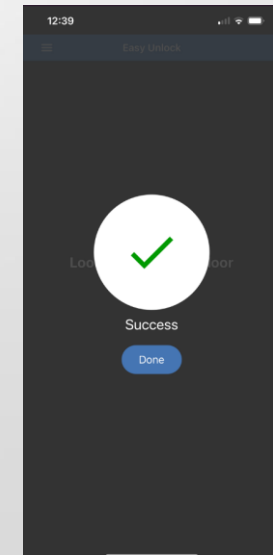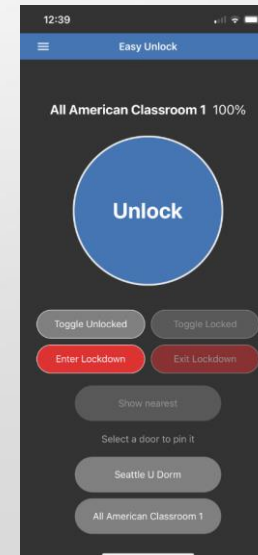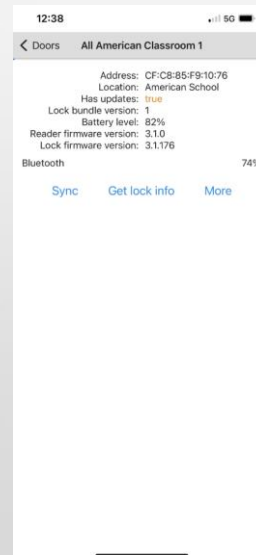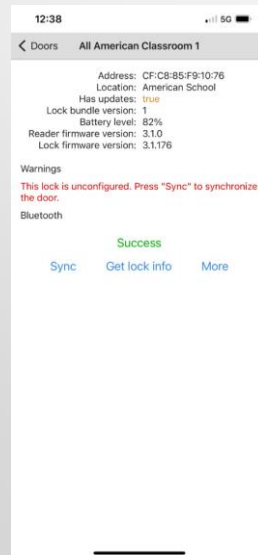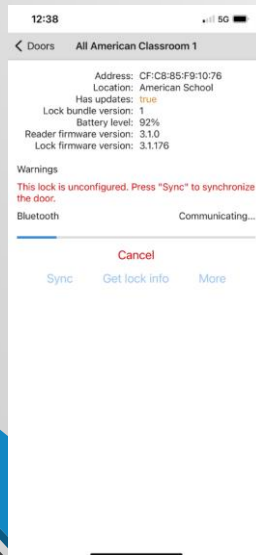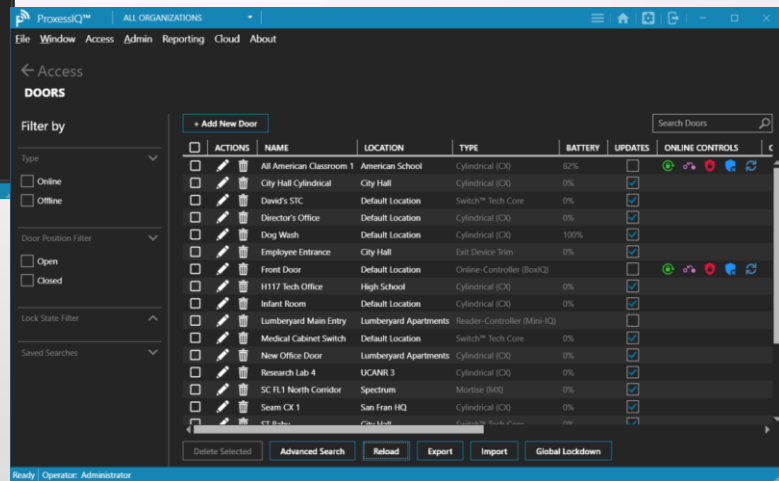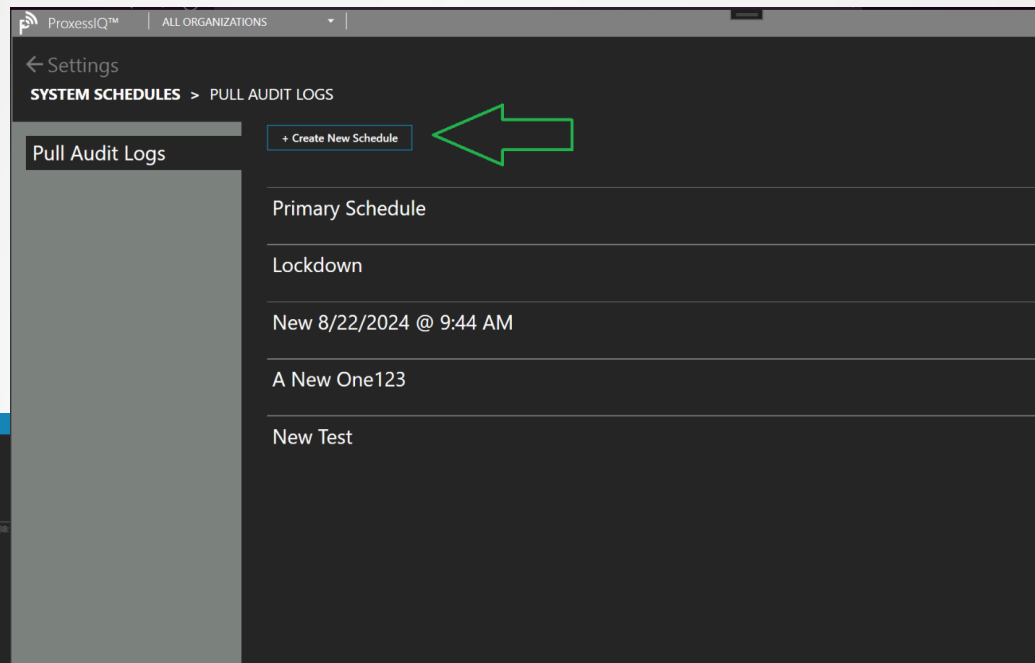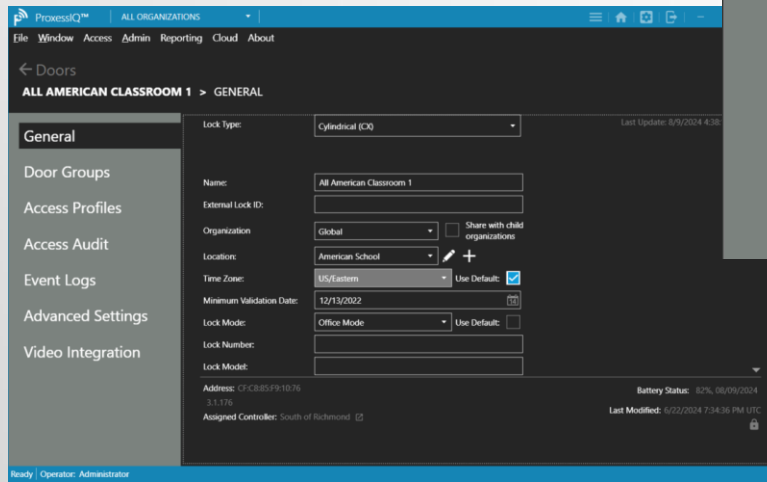
To the first search filter\criteria you have just entered, additional filters can be applied by clicking "Add Filter" and then selecting whether they are to be searched with all conditions needing to be met ("AND") or just one of the conditions needing to be met ("OR"). When all your desired filters have been added, click "Search" and the resulting list appears. Go back to the Main Screen \ Dashboard by clicking "Access".

Click the "Doors" module and then click the edit icon for the door to continue editing properties for.

Click the "Door Groups" tab. Note that you may also add Door Groups from the Door Groups menu on the Home page.

To add a new Door Group, type the name you want in the "Enter New Door Group" field and then click the "Create New Door Group" icon.
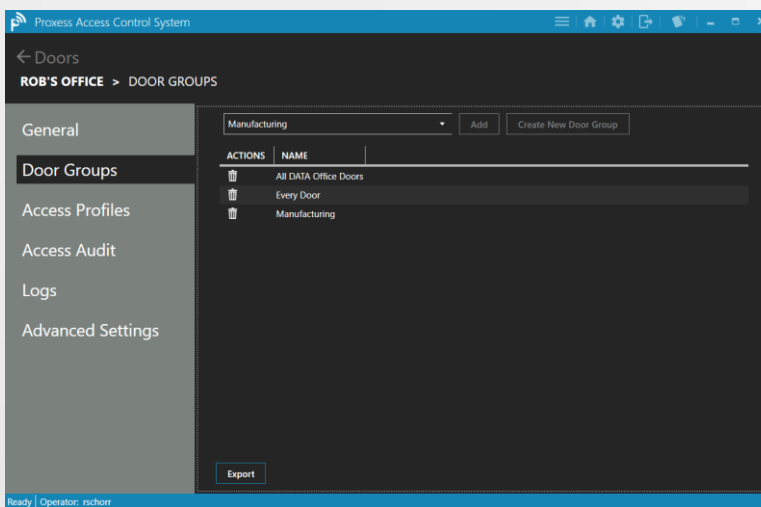
The new Door Group you have created will appear in the list for that Door and will become available to all other Doors in the system.
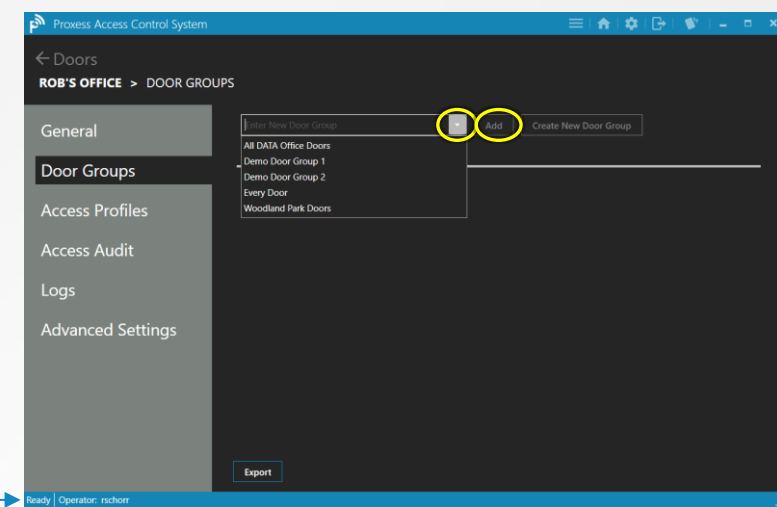
To add a Door Group for this Door to belong, click the dropdown icon and select a Door Group. Then click "Add". You can add a Door to as many Door Groups as you want.
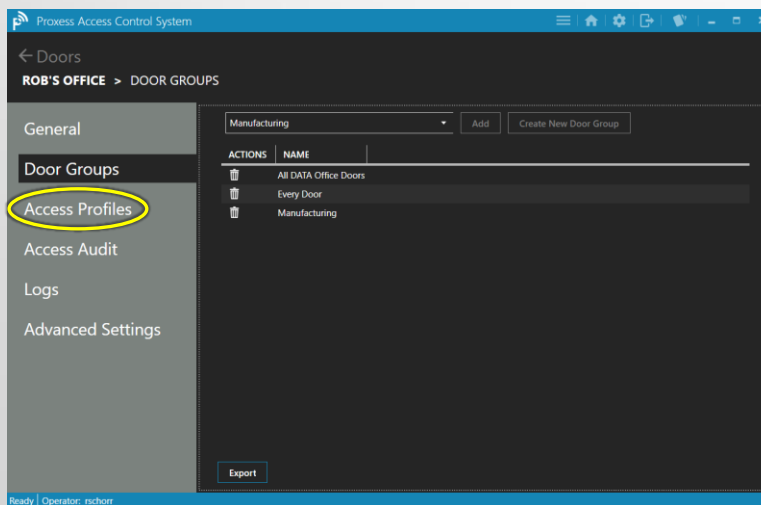
Click the "Access Profiles" tab.
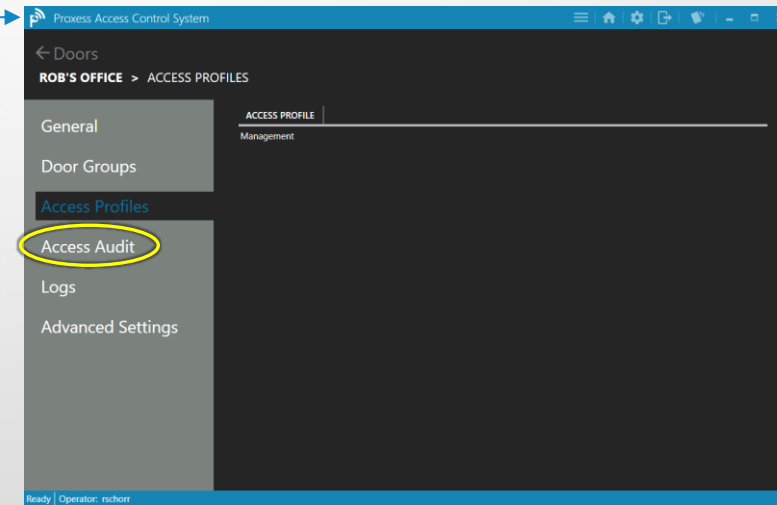
Any Access Profile that this Door is a part of will appear in this list. It is not necessary for a Door to be part of an Access Profile. If there is no Door listed, you may go back to the Dashboard \ Home Screen and click on the "Access Profiles" module to add this Door to an existing Access Profile or create a new one. Click on "Access Audit".

Each of the individual Cardholders\Users that have access to this Door will appear in this list. For any of the Users, click on their "View" icon.

This Access Audit view shows the relationship between the cardholder and their credentials and the door's record that we are in.

The insert on the bottom right of the screen allows you to see the entire relationship tree and the slide bar at the top of this insert can be moved to widen or narrow the main screen view.

Click "X" in the top right to close this view and return to the list of doors.

For a list of all the recorded Events at this Door, click "Logs".

Though you may scroll through this list, you may instead select a starting and ending date and time range for the events to be displayed making the resulting list more pertinent.
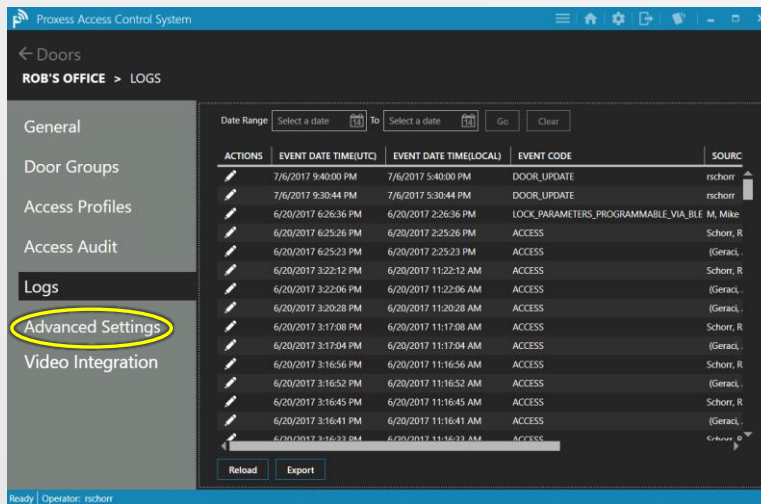
Click on the "Advanced Settings" tab.
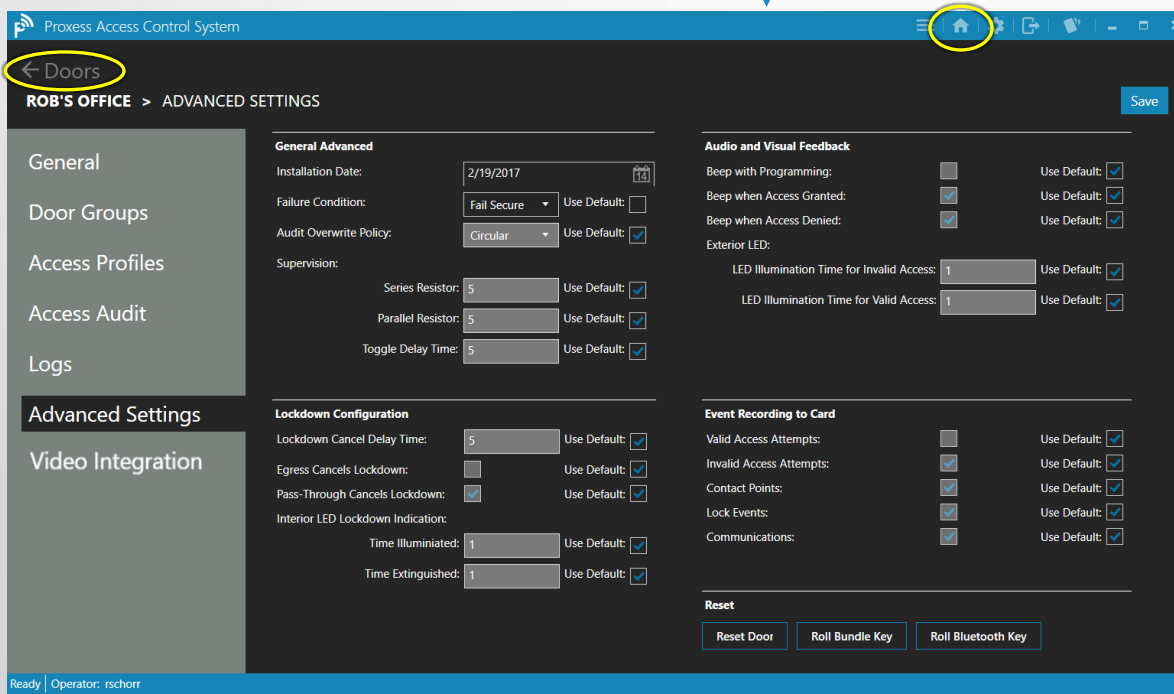
Everything in the "Advanced Settings" tab is initialized in a default mode with all the "Defaults" being edited in the "Settings" module. To change any setting, first un-check its "Use Default" box. A lockset is able to be set to Fail in a Secure, Unsecure\Safe or As-is mode. To return to the Home Screen \ Dashboard, click the "Doors" tab on the top left and then click "Access", or click the Home icon on the top right taskbar.
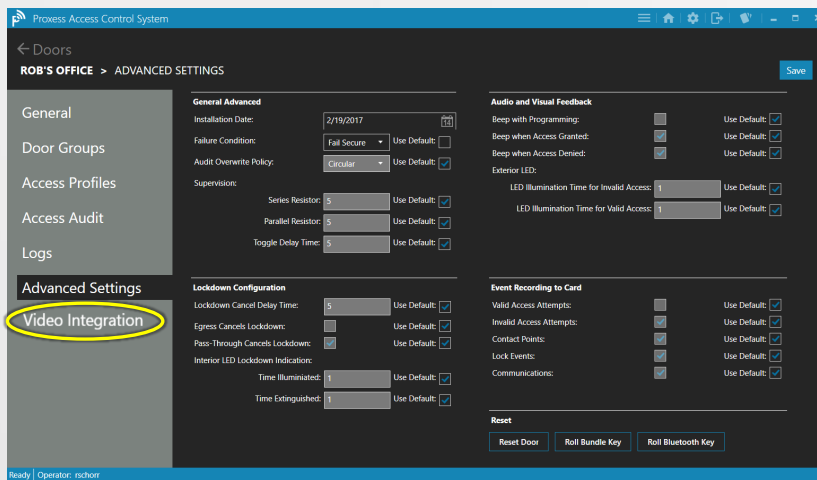
Click on the "Video Integration" tab.
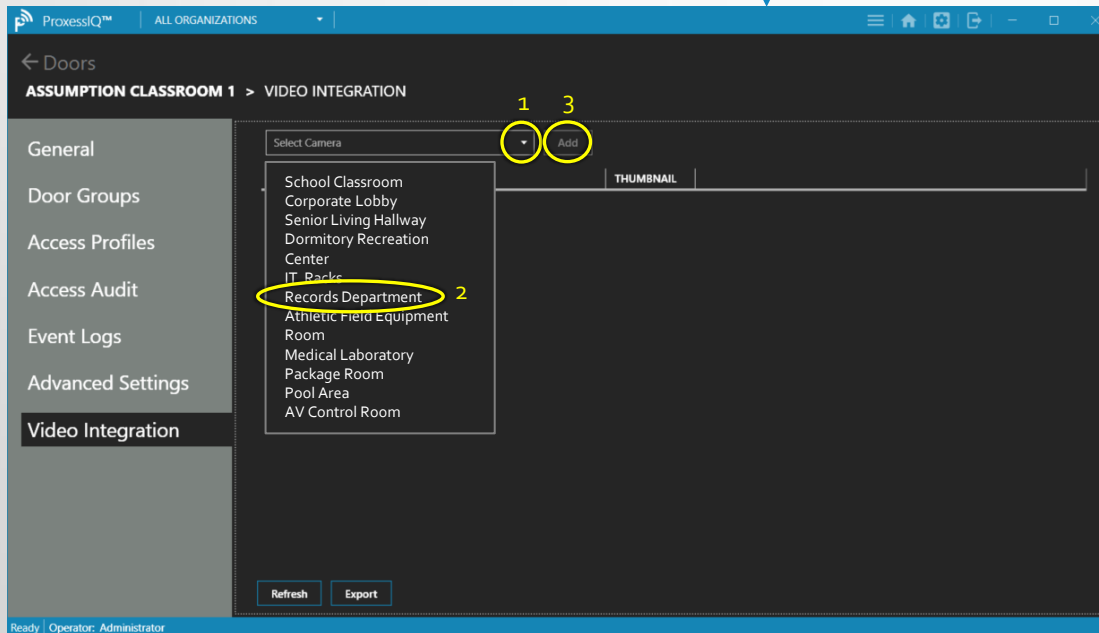
From this page you will select the cameras you wish to associate with and record video clips with for any event that occurs at this Door.

Click on the drop-down arrow (1) and all of the cameras that are connected to the NVR/VMS entered into the config file will automatically appear here. You may select (2) four (4) cameras to be associated with any event from this camera by selecting the first camera and clicking the "Add" button (3) and repeating the process for the cameras you need.

In this case, 3 cameras have been associated with this door. As a visual reference only, the static thumbnail image from each camera will appear. Updated thumbnail images can be obtained by clicking the "Refresh" button.
Note: Proxess does not display, record or store video clips. They exist solely on the NVR/VMS. Thus, for real-time and archived video event viewing, please use the NVR/VMS client software.

Doors with one or more cameras affiliated with its events will display a video camera icon.
Double-click on the camera icon to view the thumbnail images of the cameras, at three (3) seconds before the time of the event occurrence.
For further video information, go to the NVR/VMS event log.

Configuring Video Integration

Proxess currently integrates with Hanwha Wisenet WAVE 5.0

To configure the Hanwha video integration, you must have Admin privileges on the Proxess Server computer:
On that computer, go to c:/Program Files (x86)/Proxess/Server.
Locate and open, with Admin privileges, the Notepad file "Proxess.Service.Host.Console.exe", which is about 5k in size.

Change the lines that are there and add the information below that is not already in the file, precisely, per the below
<add key="videointegrationenabled" value="true" />
<add key="videointegrationtype" value="1" />
<add key="videointegrationhost" value="https://localhost:7001" />
<add key="videointegrationforcessltrust" value="true" />
<add key="videointegrationusername" value="admin" />
<add key="videointegrationpassword" value="SuperSecurePassword" />

Save that file and you may now close it.
Inside ProxessIQ™, in the Doors menu and the Video Integration tab for a selected door, the camera list will now automatically populate with all cameras that are connected to the NVR/VMS.

DOORS & DOOR GROUPS
Spreadsheet Adding & Editing

How to MASS-Add and edit Doors & Door Groups using .csv spreadsheets

Mass Adding and Editing **Doors,** using a .csv spreadsheet
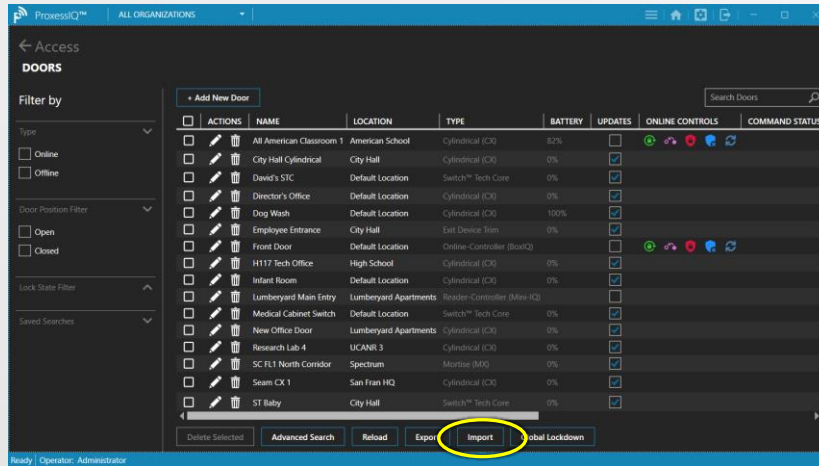
To make mass Door additions, changes or deletions, no program is simpler or more flexible than Microsoft Excel or Google Sheets.

Proxess can import a .csv formatted file from those programs or Notes, etc., with an unlimited number of Doors entered, for Door, Door Group & Access Profile entry, deletion or changes.

We will now explain the columns of detail that can be added, their format requirements and how to perform the imports and exports.

For reference, these are the overall views of all the fields that can be imported & exported and we will enlarge them and explain each field on the following pages.

Import List snapshot:

Export List snapshot:

Mass Adding and Editing **Doors,** using a .csv spreadsheet

Note: The column order may not be altered from the below and the exact headers must appear, as shown.

A	B	C	D	E	F	G	H	I	J	K
ExternalId	Name	Notes	LockType	CalendarName	UnlockTimeScheduleName	EnableButtonToggle	EnableButtonLockdown	LockdownRequiresHandle	EgressCancelsLockdown	DeadboltEnablesLockdown

ExternalID: Not required to be entered by the end user. Will otherwise be automatically assigned by the system. This is a unique identifier and may not be changed, or the entry will be treated as a second/additional user entry. The User's existing ExternalID must be included here for subsequent data imports, where you wish to have that record updated. **Note:** Therefore, this **SHOULD** be entered for the initial import.

Name: Name of the Door that will be automatically entered into the database. If one is already entered with this name, and no ExternalID is entered into column A, then an additional Door will be added to the system with the attributes in this line. If this spreadsheet is meant to update an existing Door name in the system, then be certain the name is spelled correctly and the ExternalID is included in column A. No minimum or maximum characters

Notes: No minimum or maximum characters. May be used as a "custom" field for searching and for mass updates via the import sheet.

LockType: Must specifically be listed as either "Cylindrical", "Mortise", "Exit Trim", "Mini_IQ" or "Controller".

CalendarName: 24 maximum characters. This is the Calendar and associated Holidays (days on which credentials that do not have the Holiday box checked will not work) the Door will follow.

UnlockTimeScheduleName: No minimum or maximum characters. This is the name of the Time Schedule that the Door will follow to go into the Unlocked (no credential required for entry) position. This Time Schedule must already have been manually entered into the system, as it will not be automatically created by this import spreadsheet.

EnableButtonToggle: Enter "TRUE" if you will allow the interior trim button to "toggle" the door lock status (change it from locked to unlocked and from unlocked to locked), each time it is quick-pressed/pushed. Enter "FALSE" if you do not want this door's button to perform this operation.

EnableButtonLockdown: Enter "TRUE" if will allow the interior trim button to be long-pressed/pushed (for a variable 3-to-6 seconds in the software) and have the lock go into the Lockdown mode. Enter "FALSE" if you do not want this door's button to perform this operation.

LockdownRequiresHandle: Enter "TRUE" if, for a Lockdown to be performed on the lock, you wish for both the interior trim button to be pressed/pushed, while simultaneously holding the exit lever down. Enter "FALSE" if you do not.

EgressCancelsLockdown: If a door is in Lockdown, by any means, any time the handle is used to exit or open the door, the Lockdown will be cancelled and the lock will return to the state appropriate to the day and time.

DeadboltEnablesLockdown: Only for a mortise lock with a deadbolt, enter "TRUE" if you want this lock to go into Lockdown when the deadbolt is thrown from the inside. Enter "FALSE" if the deadbolt will only lock the door.

Spreadsheet Import Utility- 2

Mass Adding and Editing **Doors,** using a .csv spreadsheet

Note: The column order may not be altered from the below and the exact headers must appear, as shown.

L	M	N	O	P	Q	R	S
BatteryReplace Date	DoorGroupList	AccessProfileList	AccessProfileTime ScheduleName	AssignedController ExternalID	OrganizationGuid	ShareWithChildren Orgs	ForceUpdate

BatteryReplaceDate: Not required to be entered by the end user. An informative entry field for maintenance purposes. If done on a large number of locks at a time, it makes sense to use this spreadsheet to enter the date for all the locks.

DoorGroupList: The Door Group(s) that this Door is a part of. If more than one will be listed, they must be separated by a "|", with no additional spaces on either side, or the Door Group will be interpreted as not being spelled correctly and it will not be added. An unlimited number of Door Groups can be entered. No minimum or maximum characters.

AccessProfileList: Name of the Access Profile(s), which **must first be manually added** by the system administrator in the Access Profiles menu. No minimum or maximum characters. Up to 24 APs can be added into this cell (which is the maximum number of Direct Privileges [a combination of Doors & Door Groups] that a single credential may have), separated by a "|". Be careful not to include any extra spaces, or the AP will be interpreted as not being spelled correctly.

AccessProfileTimeScheduleName: Enter the exact name of the Time Schedule (which must first be manually entered into the Time Schedules menu) that this aggregation of doors will operate during.

AssignedControllerExternalID: Enter the exact External ID of the Controller this Door has been connected via Bluetooth with, in the Offline Doors tab of the Controller. Leave this cell blank if the Door has not been connected with a Controller.

OrganizationGuid: If this system has a license for the Partitioned Database / Organizations feature, enter the exact Organization GUID that this Door is apart of.

ShareWithChildrenOrgs: If this system has a license for the Partitioned Database / Organizations feature, enter "TRUE" if this Door can be used by / shared with sub-organizations. Otherwise, enter "FALSE".

ForcedUpdate: Enter "TRUE" if this Door already exists and the information in this row should be used to update the existing record in the software with this import. Otherwise, enter "FALSE".

Mass Adding and Editing **Door Groups,** using a .csv spreadsheet
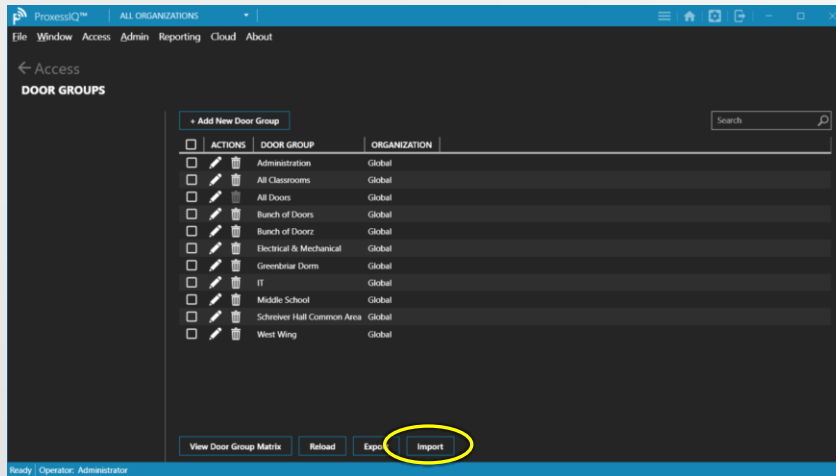
To make mass Door Group additions, changes or deletions, no program is simpler or more flexible than Microsoft Excel or Google Sheets.

Proxess can import a .csv formatted file from those programs or Notes, etc., with an unlimited number of Door Groups entered, for Door, Door Group & Access Profile entry, deletion or changes.

We will now explain the columns of detail that can be added, their format requirements and how to perform the imports and exports.

For reference, these are the overall views of all the fields that can be imported & exported and we will enlarge them and explain each field on the following pages.

Import List snapshot:

	A	B	C	D	E	F	G	H	I	J	K
1	ExternalId	DoorGroupName	Notes	DoorList	AccessProfileList	AccessProfileTimeScheduleName	AssignedC	EnableAutoEnroll	OrganizationGuid	ShareWithChildrenOrgs	ForceUpdate
2		Bunch of Doorz		Classroom 110|Office 25|Package Room	Teachers	School Day		FALSE	00000000-0000-00(	FALSE	TRUE
3		Freshman Dorm		Fresh Perim N|FPS|Laundry|Bike Room	Freshers	24/7		TRUE	00000000-0000-00(	FALSE	TRUE
4											

Door Groups csv Import 08-14-24   +

Export List snapshot:

	A	B	C
1	Door Group	Organization	
2	Administration	Global	
3	All Classrooms	Global	
4	All Doors	Global	
5	Bunch of Doors	Global	
6	Bunch of Doorz	Global	
7	Electrical & Mechanical	Global	
8	Greenbriar Dorm	Global	

Export of DoorGroups_   +

Mass Adding and Editing **Door Groups,** using a .csv spreadsheet

Note: The column order may not be altered from the below and the exact headers must appear, as shown.

A	B	C	D	E	F	G	H	I	J	K
ExternalId	DoorGroupName	Notes	DoorList	AccessProfileList	AccessProfileTimeScheduleName	AssignedControllerExternalID	EnableAutoEnroll	OrganizationGuid	ShareWithChildrenOrgs	ForceUpdate

ExternalID: Not required to be entered by the end user. Will otherwise be automatically assigned by the system. This is a unique identifier and may not be changed, or the entry will be treated as a second/additional user entry. The User's existing ExternalID must be included here for subsequent data imports. **Note:** Therefore, this **SHOULD** be entered for the initial import.

DoorGroupName: Name of the Door Group that will be automatically entered into the database. If one is already entered with this name, and no ExternalID is entered into column A, then an additional Door Group will be added to the system with the attributes in this line. If this spreadsheet is meant to update an existing Door name in the system, then be certain the name is spelled correctly and the ExternalID is included in column A. No minimum or maximum characters

Notes: No minimum or maximum characters. May be used as a "custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.) field and for mass updates via the import spreadsheet.

DoorList: The Door(s) that are included within this Door Group is a part of. If more than one will be listed, they must be separated by a "|", with no additional spaces on either side, or the Door Group will be interpreted as not being spelled correctly and it will not be added. An unlimited number of Doors can be entered. No minimum or maximum characters.

AccessProfileList: Name of the Access Profile(s), which **must first be manually added** by the system administrator in the Access Profiles menu. No minimum or maximum characters. Up to 24 APs can be added into this cell (which is the maximum number of Direct Privileges [a combination of Doors & Door Groups] that a single credential may have), separated by a "|". Be careful not to include any extra spaces, or the AP will be interpreted as not being spelled correctly.

AccessProfileTimeScheduleName: Enter the exact name of the Time Schedule (which must first be manually entered into the Time Schedules menu) that this aggregation of doors will operate during.

AssignedControllerExternalID: Not currently used

EnableAutoEnroll: Enter "TRUE" if this Door Group will be automatically added to every new User. Enter "FALSE" is it won't.

OrganizationGuid: If this system has a license for the Partitioned Database / Organizations feature, enter the exact Organization GUID that this Door is apart of.

ShareWithChildrenOrgs: If this system has a license for the Partitioned Database / Organizations feature, enter "TRUE" if this Door can be used by / shared with sub-organizations. Otherwise, enter "FALSE".

ForcedUpdate: Enter "TRUE" if this Door already exists and the information in this row should be used to update the existing record in the software with this import. Otherwise, enter "FALSE".

DOORS

Controlling Online & Bridged Doors
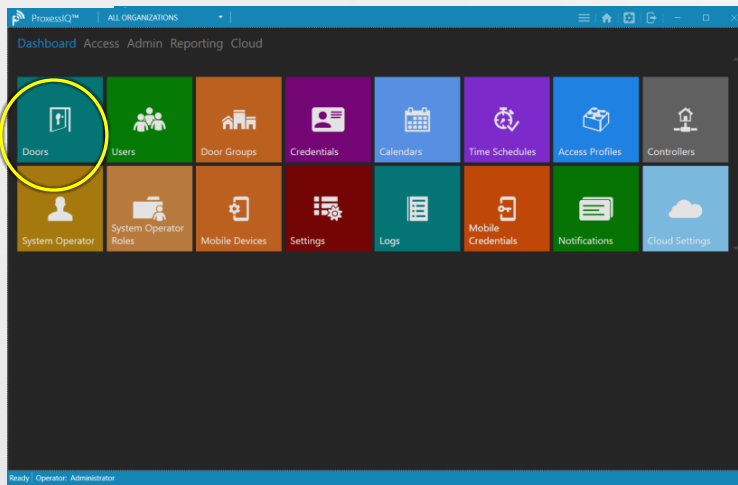
We will now review the real-time/online door controls. From the Home screen \ Dashboard, click "Doors". "Online" Doors are BoxIQ PoE controllers, as well as any lock or Mini-IQ that is bridged to it.
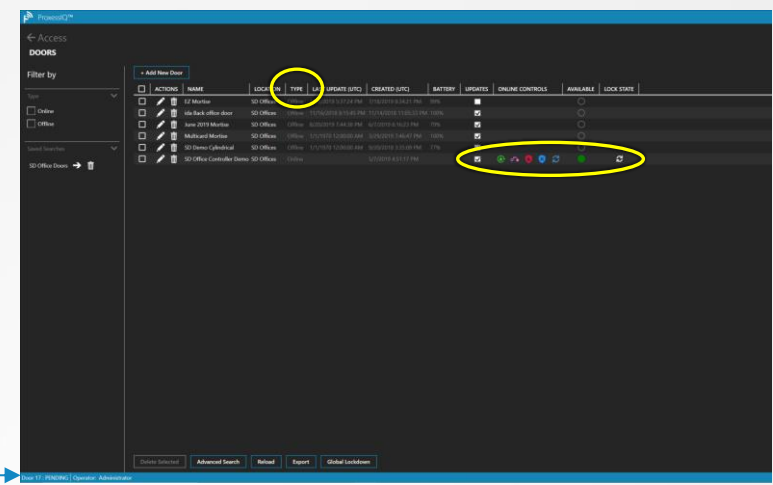
This is the User Interface for online doors and circled (on the right) are the available door controls. You can sort so that Online doors appear at the top of the list of doors by clicking on "Type", circled at the top of the screen.

Click this icon to Lockdown this door and this icon to cancel the Lockdown.

Click this icon to Toggle this door to an unlocked state. Click the icon again to Toggle it back to the state it was in.

Click this icon to Refresh the state of the lock.

This icon shows that the door has been programmed, but it is now offline.

Click this icon to perform a Quick/Momentary Unlock this door. The open time is as programmed into the Settings screen in the *Doors* module.

This icon shows that the lock has been and is unlocked.

This icon shows that the lock has been and is now locked.

More Status Icons

This icon shows that Reader #1 is Connected.

This icon shows that the Door is Open.
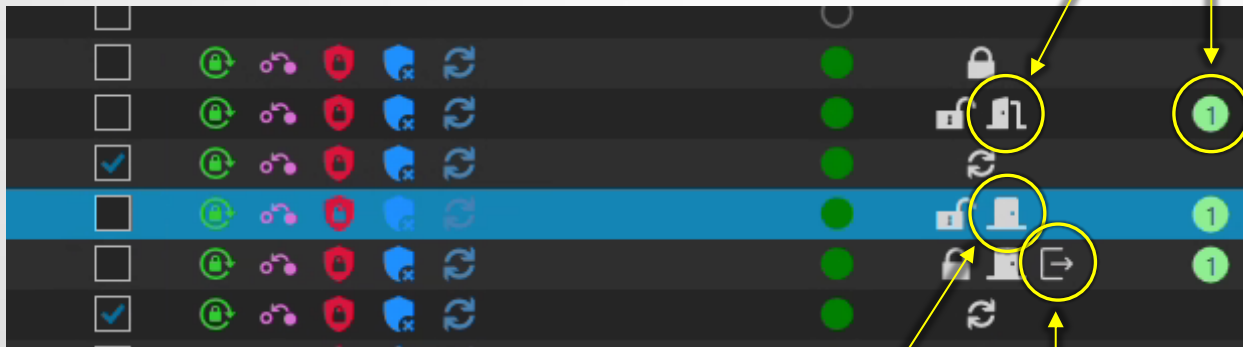
This icon shows that the Door is Closed.

This icon shows that the Request-to-Exit input has been activated.

Global and Grouped Lockdowns

Only the Global Lockdown button appears on this page.
Grouped Lockdowns can be configured and performed from within the **Notifications** menu.

Controlling Online & Bridged Doors - 4
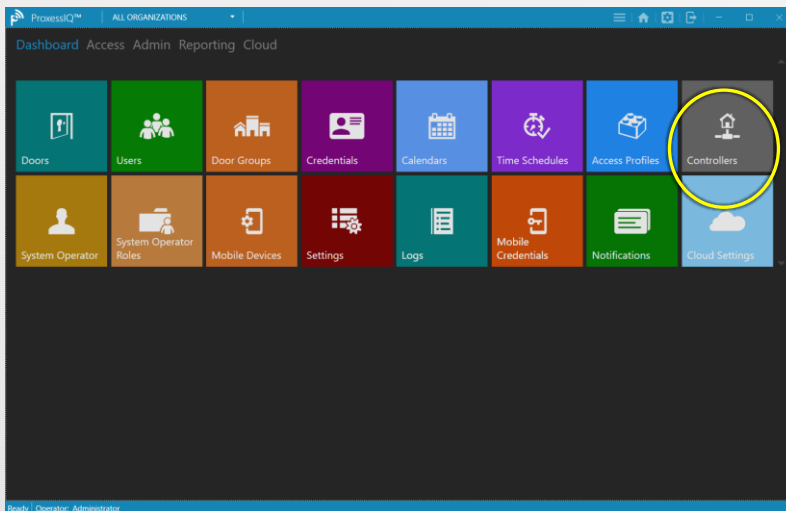
CONTROLLERS

To add a controller to the system, click on the "Controller" module icon. After adding a Controller, you will then be able to select entry & exit readers that you have added into the "Doors" module to connect.
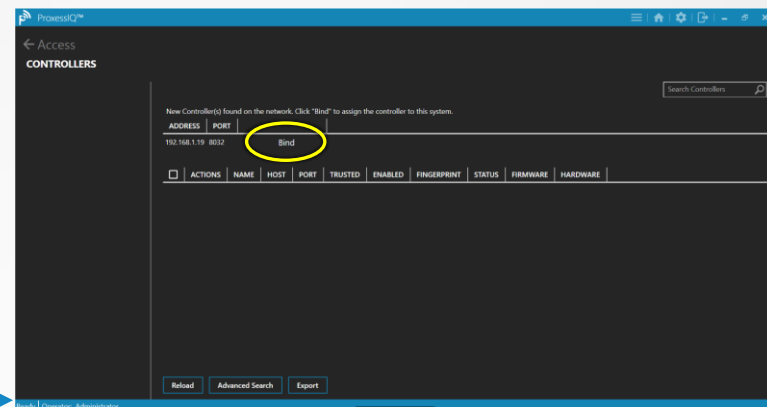
Any controller that is connected, within the guidelines of our BoxIQ Connectivity document located here on our website: www.proxess.com/documents/BoxIQConnect will automatically appear in this window. To avoid confusion, it is best to connect and configure one controller at a time.
Click "Bind" to connect the newly discovered controller with ProxessIQ
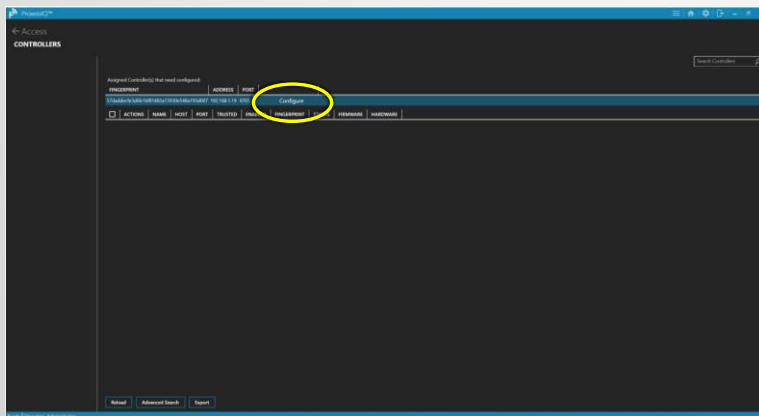
Now click "Configure" to have the software configure this controller for its proper function within this software instance.
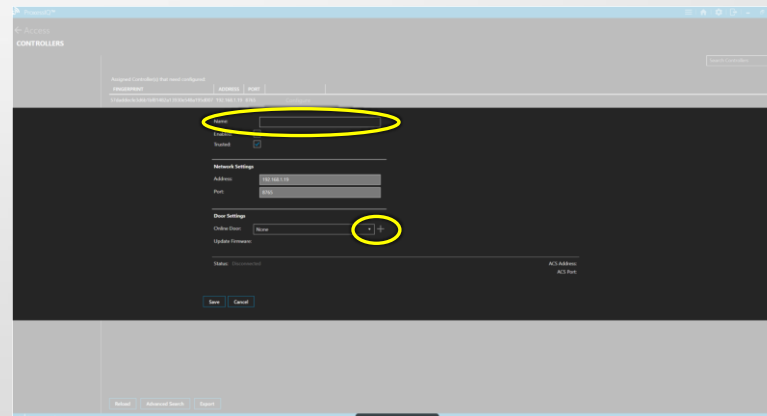
Type a name for this controller.
Next, click on the drop-down arrow above.
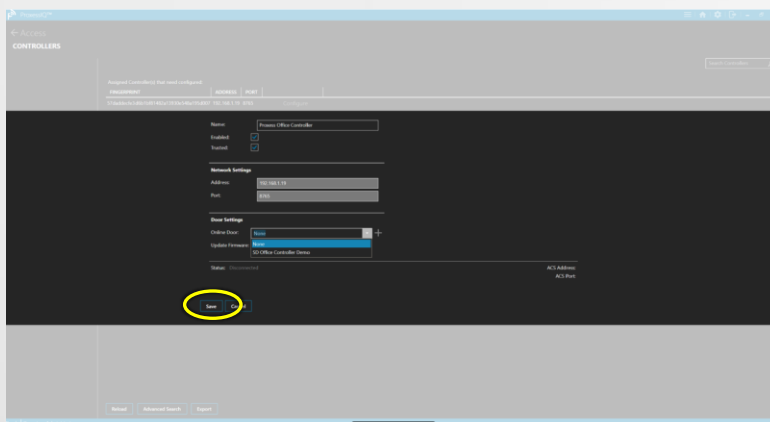
Select any reader that you have already entered in the "Door" module to be connected to this controller. Then click "Save".
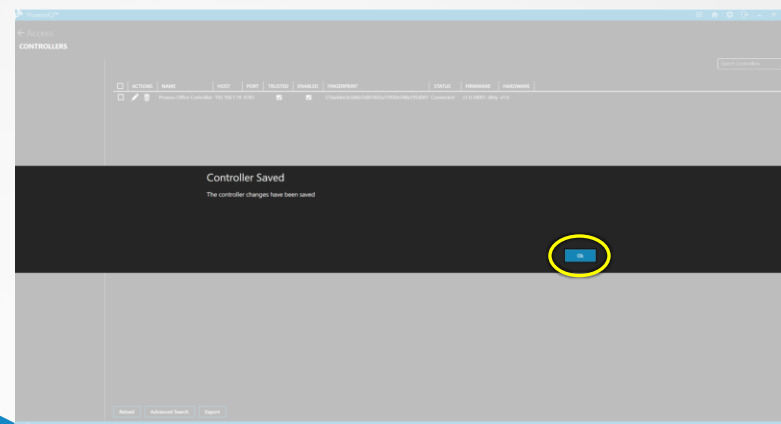
Click "OK" on the verification screen.
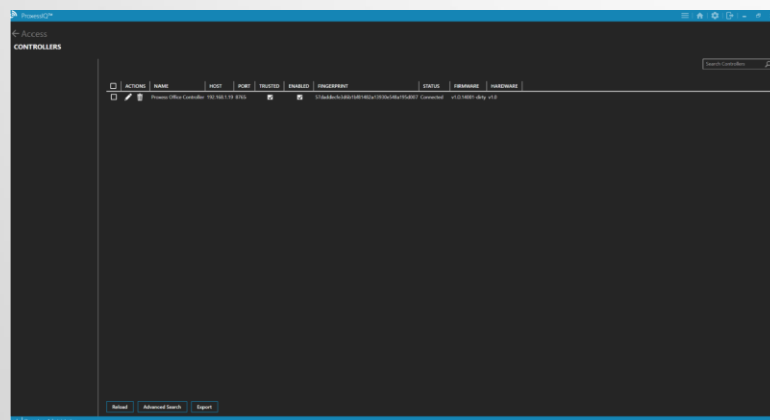
The Controller is now bound, configured enabled and shown as Connected and operational.

Mobile Credential Note: In order for this attached, online Door (as it is called in the software)/reader (the physical device that is wired to the controller) to be fully operational for Bluetooth Mobile credentials, you must now remove the power from the controller and then reapply it (i.e. power-cycle the controller). A Bluetooth address will now appear at the bottom left of the General Door tab of this connected reader and mobile credentials will operate.

Controller Error Messages
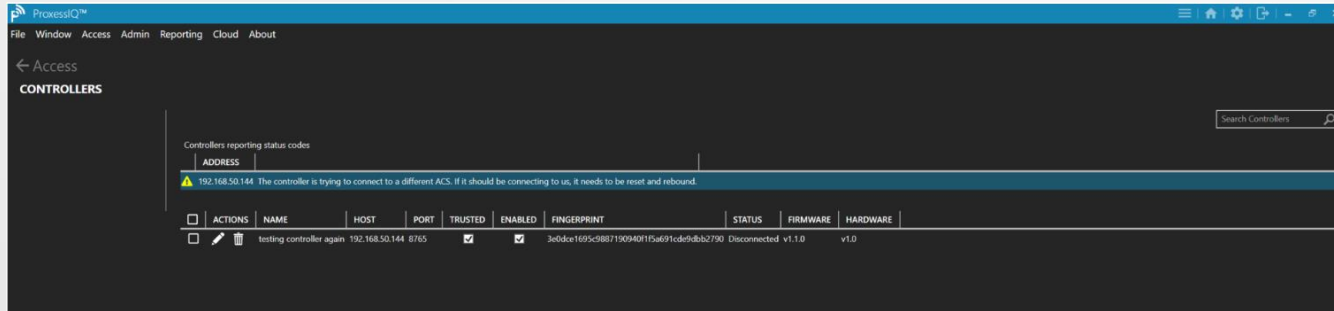
Note: It is unlikely, but possible to receive this Controller screen error message. For instance, if a controller from another system is placed on the network for your system (in a dealer's lab, for instance), your software will note the above, prompting your investigation and possible resetting of that controller for it to be bound into your system.

All Controller Related Status and Error Messages that may appear in blue highlight, as above:
- Controllers reporting status codes
- New Controller(s) found on the network. Click "Bind" to assign the controller to this system.
- The Controller is unable to reach the Proxess service. Check inbound TCP firewall rules.
- The Controller is timing out during key exchange. This is likely caused by poor network performance.
- The controller is trying to connect to a different ACS. If it should be connecting to us, it needs to be reset and rebound.
- Unknown, the status code is not supported. Update to receive information about this Controller.
- Unknown, the Controller has suffered a fault.

Port & Network Scanning for Controllers

To search for Proxess controllers on a network, it will be quickest to scan Port 8032 for its UDP beacon, as it is unlikely that there would be other devices doing the same.

If you are scanning the entire network for a Proxess Controller, you should expect to see "Texas Instruments" (the blue highlighted devices below) or sometimes a Ring device appear. That will give you the MAC address , which you can then use to SSH into it and configure its IP address.

THUNDER-LAPTOP4	10.23.10.174	Plugable Technologies	8C:AE:4C:BD:11:FD
10.23.10.4	10.23.10.4	Raspberry Pi Foundation	B8:27:EB:3A:00:FE
Lutron-01e8c00e	10.23.10.123	Texas Instruments	60:64:05:6D:1B:29
10.23.10.105	10.23.10.105	Texas Instruments	38:D2:69:B3:C3:CB
10.23.10.191	10.23.10.191	Texas Instruments	54:4A:16:95:8F:46
10.23.10.176	10.23.10.176	Texas Instruments	38:D2:69:A1:3F:92
10.23.10.195	10.23.10.195	Universal Global Scientific Industrial...	3C:E1:A1:5E:94:68

	Allowed	2.4G		Chime Pro Ring-Chime Pro	10.0.0.50	D8:A9:8B:A6:0E:6D
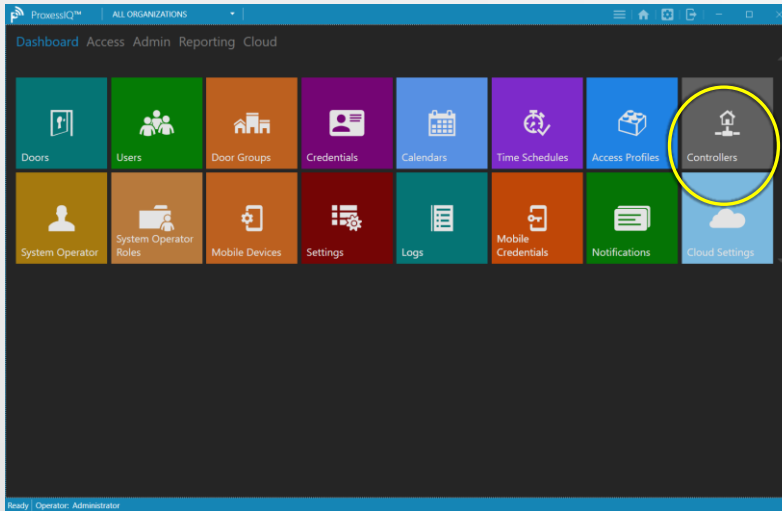
To add a door controller to the system, click on the "Controller" module icon. After adding a Controller, you will then be able to select entry & exit readers that you have added into the "Doors" module to connect.
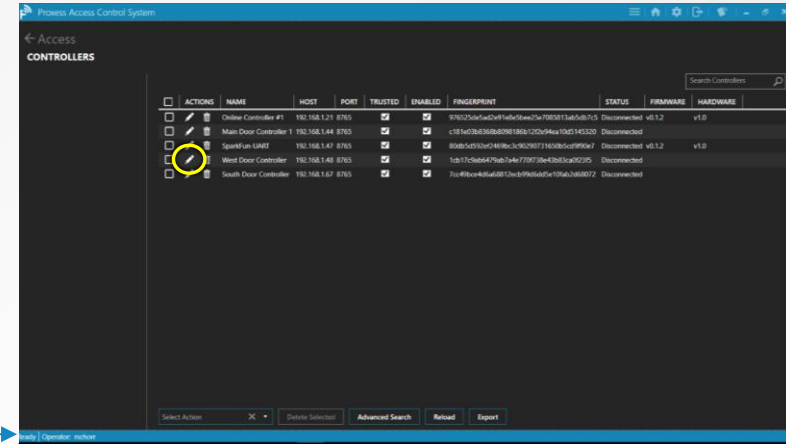
Now we will show how to add readers to a controller that is already in the system, click its *Edit* icon shown above.
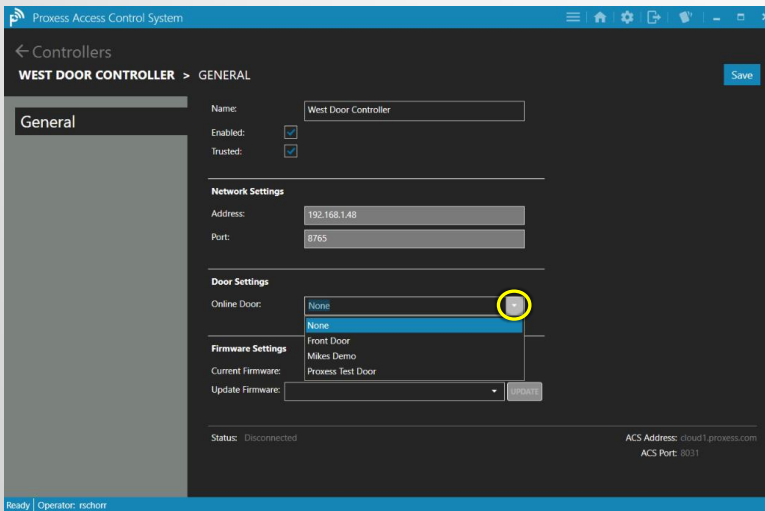
Add any door that has been defined as "Online" in the "Door Type" field of the *Doors* module may be connected to this controller by clicking this arrow and selecting it from the drop-down list.
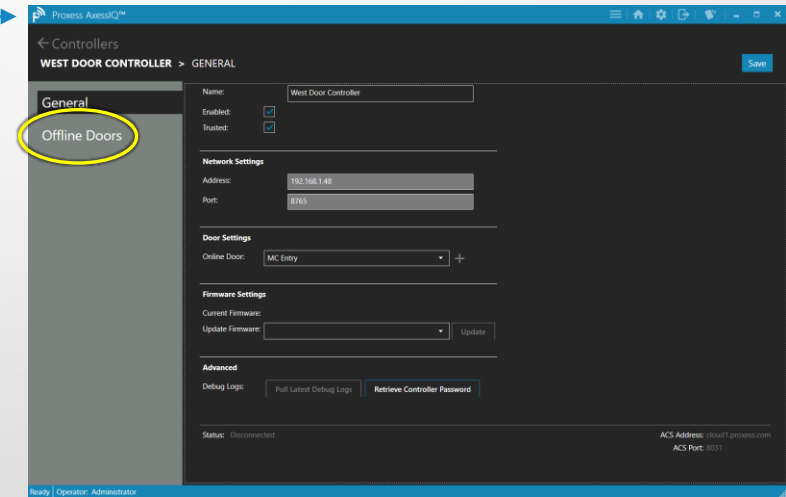
The Controller screen now shows the reader that has been attached to that Controller.
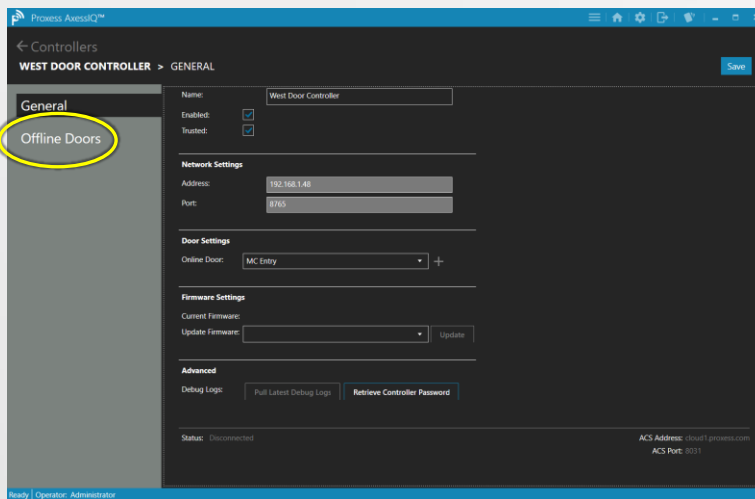
Now click on "Offline Doors" to bind cylindrical locksets, mortise locksets and Mini-Controllers to the Controller.
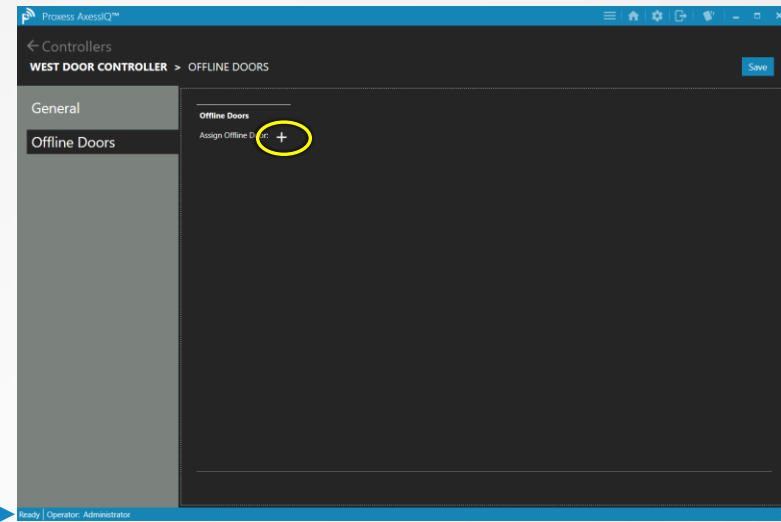
Up to eight (8) locksets and mini-controllers can be bound to a single controller.
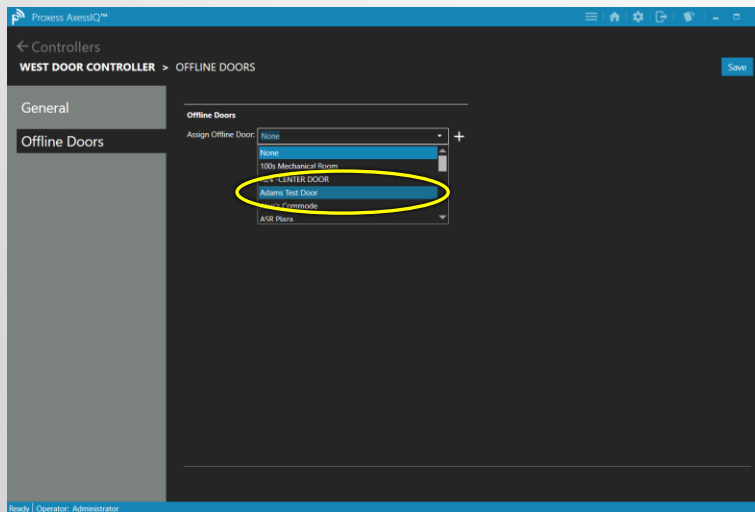
Add any door (i.e. Lockset and Mini-Controller) that has been defined as "Offline" in the "Door Type" field of the *Doors* module may be connected to this controller selecting it from the drop-down list.
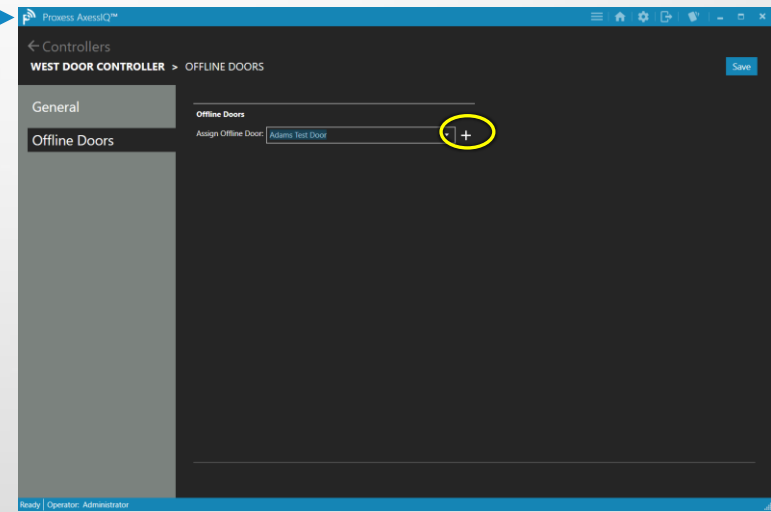
˙Up to eight (8) total locksets and mini-controllers can be connected to a controller.
A lockset or M-C can only be connected to one (1) controller.
Take care to select locksets or M-Cs to be connected that can easily be "seen" and controlled by the software, in the "Doors" module.

Customize Inputs & Outputs on a Controller

Find the MAC Address of a Controller with Putty

Within Putty, while connected to the serial connector of a controller from a laptop;
- Go to the command prompt and modify the command line to the below:
- "root@varsomam33:/usr/bin# ifconfig"
- Press Enter and its MAC/Hardware address will appear, as in the underlined

```
root@varsomam33:/usr/bin# ifconfig
eth0      Link encap:Ethernet  HWaddr 38:D2:69:A1:6B:26
          inet addr:192.168.50.79  Bcast:192.168.50.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2386791 errors:0 dropped:676 overruns:0 frame:0
          TX packets:1788712 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:258854126 (246.8 MiB)  TX bytes:156454190 (149.2 MiB)
          Interrupt:177
```

SYSTEM SCHEDULES

Setting up aggressive schedules for pulling Logs/Audits and Events from Offline locks & Mini-IQs.

Note: These doors must be connected to a gateway/online controller to deliver their information back to the software.

Note: Available on version 1.5.4.1 and greater systems.

System Schedules – For Aggressive Event Gathering from Locks
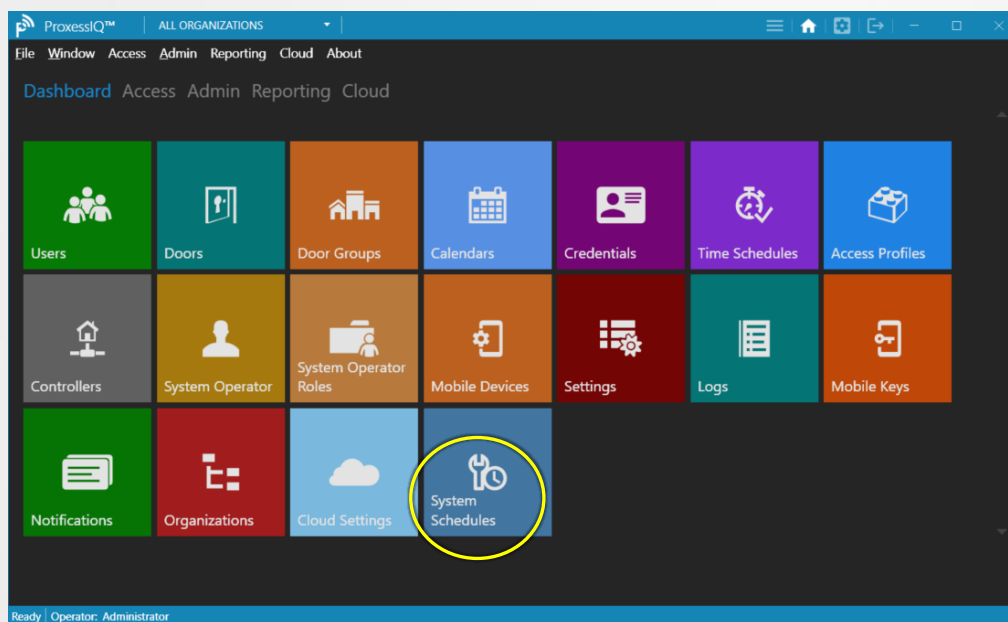
This menu allows you to set schedules for the retrieval of audits, transactions and events from locks and Mini-IQs that have been connected to a gateway.

From the Dashboard, click on the System Schedules icon.

Sometimes, the System Schedules menu will not appear on the Dashboard. In that case, click on "Admin" and those menus will appear.
Right-click on System Schedules and click "Pin to Dashboard".
Now you can return to the full Dashboard and that icon will appear.
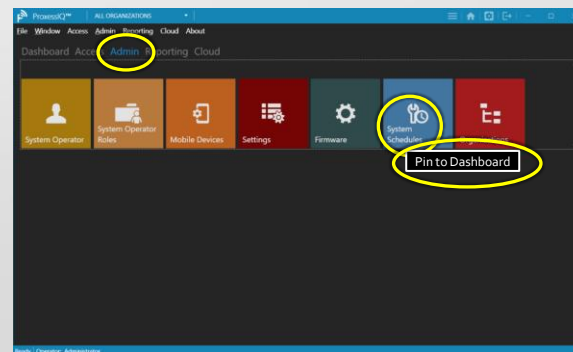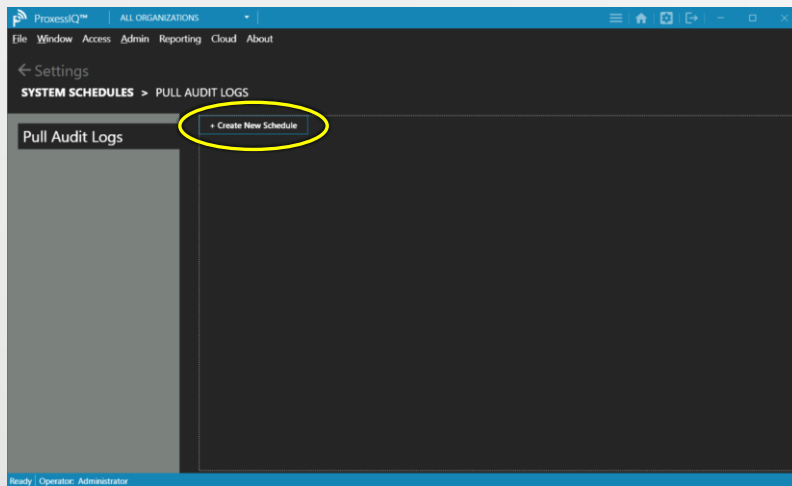
Click "Create New Schedule"
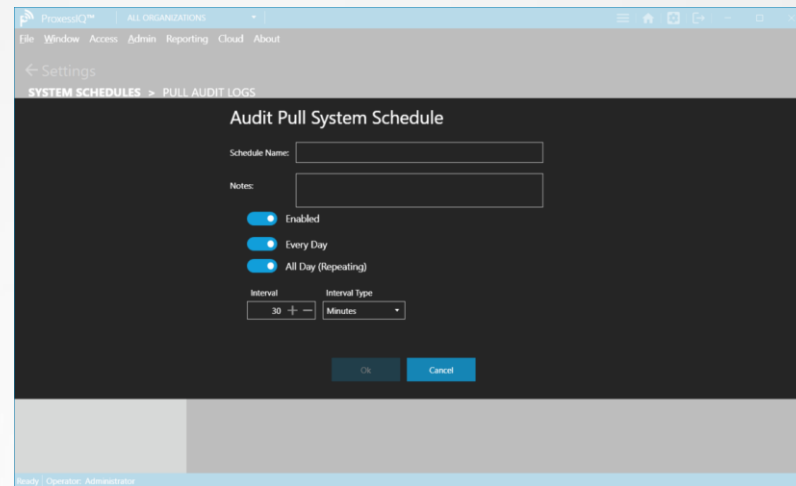
Enter a name for the schedule. Leave "Enabled" check to make it active. Uncheck it to deactivate the implementation of the schedule. Uncheck "Every Day" to limit the days to aggressively pull audits & events from the doors. Leave "All Day Reporting" checked to set a time period to be pulling audits & events from the doors.
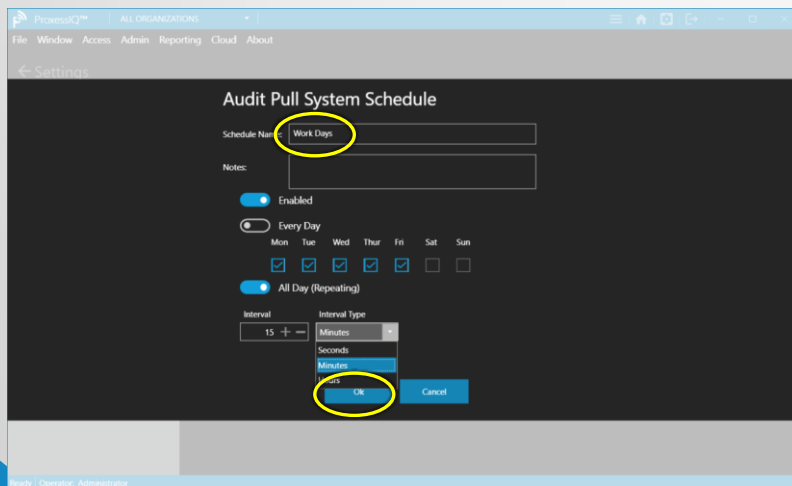
In this example, we named the schedule "Work Days" and checked Mon-Fri for the events to be pulled from the locks, on a schedule of every 15 minutes. At pull-rates greater than 5 minutes, there could be noticeable battery use over time.
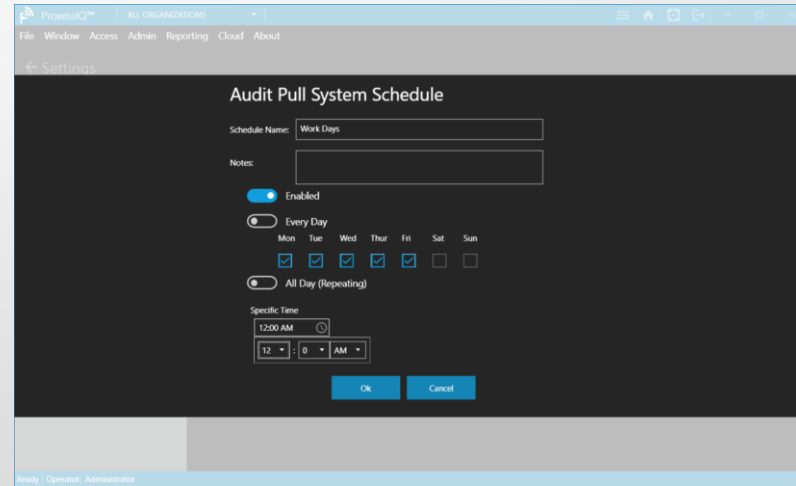
You can also uncheck the "All Day Reporting" box and select a time each day for the logs/audits/events to be pulled down. Click "OK" to save this Schedule.
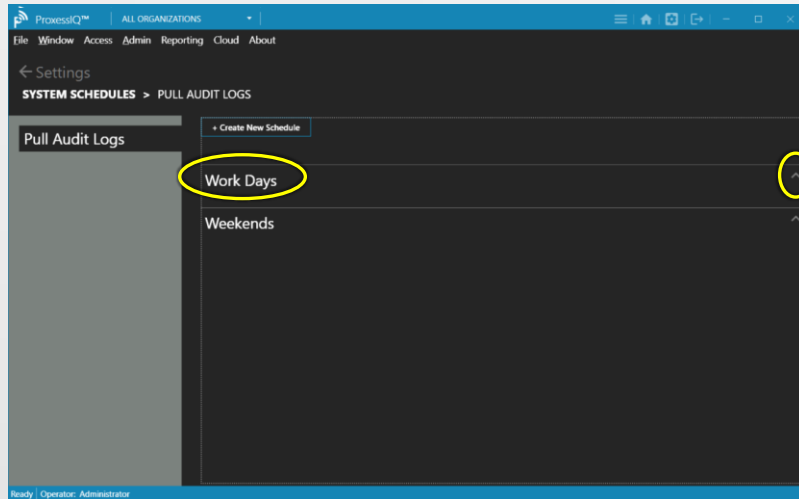
Your list of schedules will appear here. Select one to view it by clicking on either its name, or the drop-down arrow.
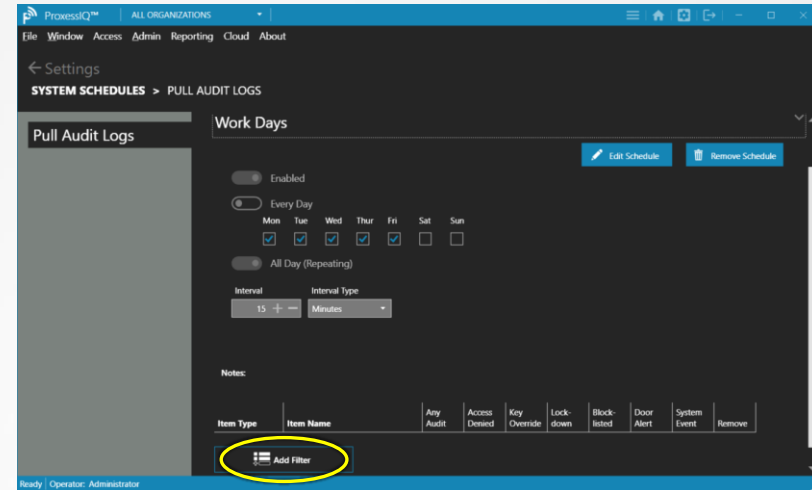
You will now need to define the list of events that you wish to have pulled from and the locks & Mini-IQs to be involved. Click "Add Filter".
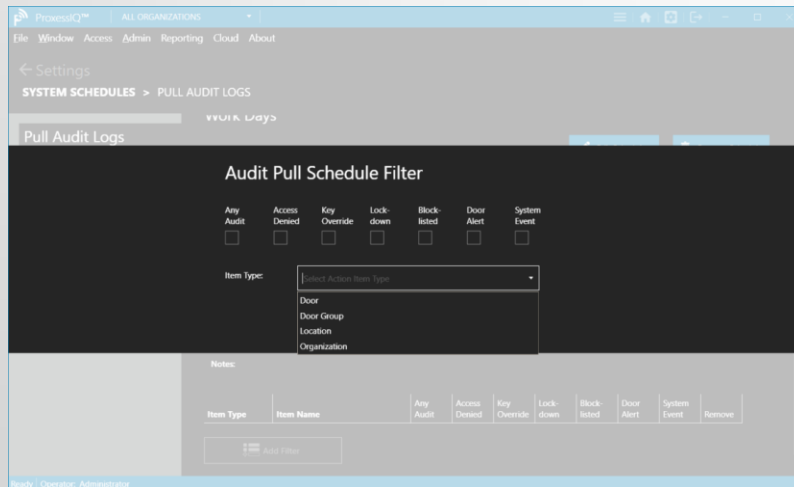
First, check the boxes of any audit or event that you wish to have delivered to the software on this schedule and then select the affected Door, Door Group, Location or Organization. Consider that you can make several schedules for the same time frame and have different audits with different pull times for each one..
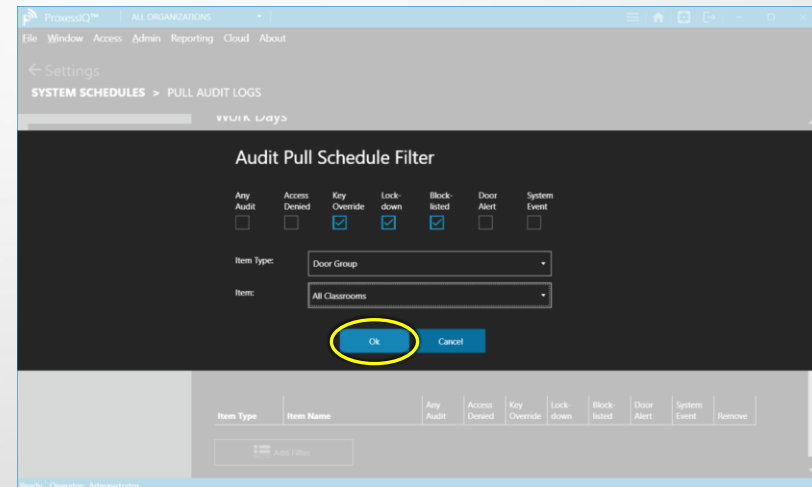
In this case, we selected Key Override, Lockdown & Blocklist events to be sent from the All Classrooms Door Group, during the Word Day schedule, of every 15 minutes. Click "OK".
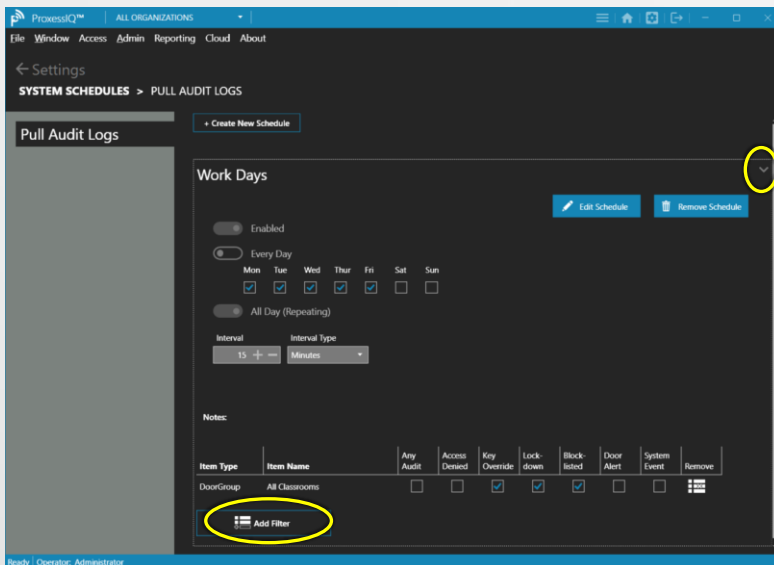
You can now add additional filters for other audits to be pulled from either the same or different doors, by clicking on "Add Filter".
Click on the Collapse arrow to return to the full list of schedules.
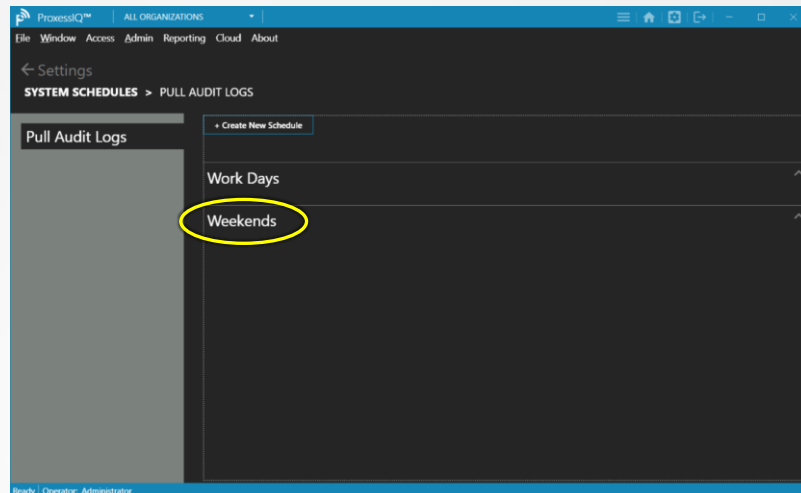
To View, Edit or Remove a schedule, click on its name.
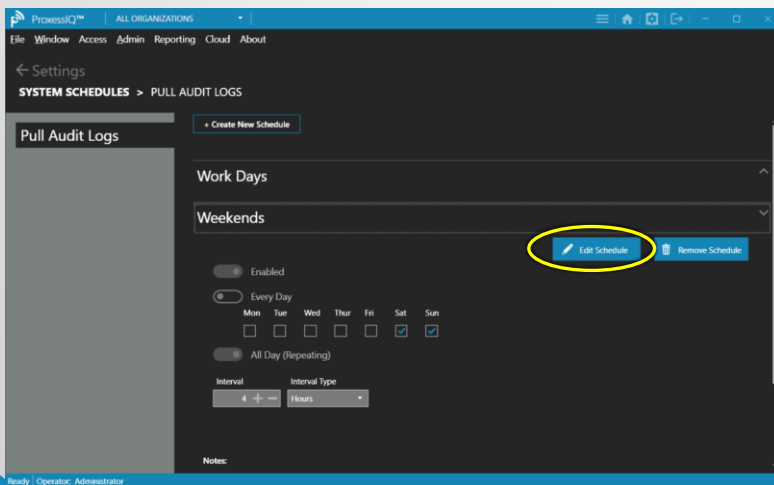
To edit, click "Edit Schedule".
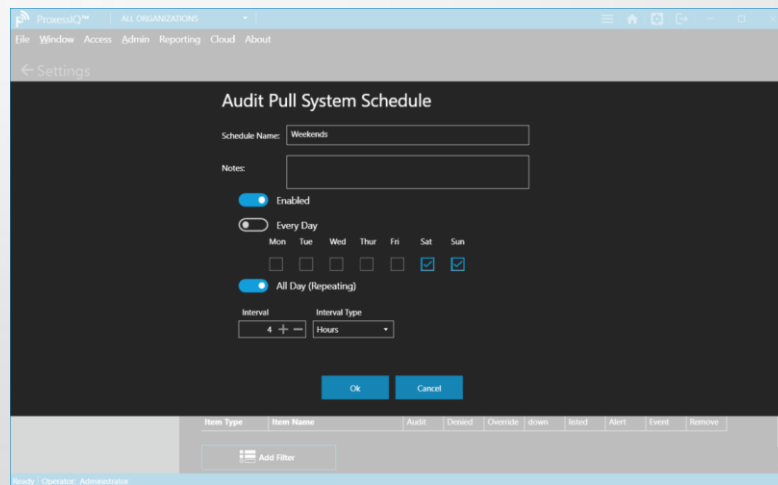
When you are done making adjustments, click "OK" and you will be returned to the main System Schedules page.

ACCESS PROFILES

Access Profiles combine Time Schedules and Doors (and Door Groups) together and can then be assigned to Users.

The **benefit** to the operator is to minimize keystrokes when assigning rights to each card. Ideally, spending time up front to create thoughtful Access Profiles could result in just a single right being assigned to each credential, as opposed to numerous Door Groups and Doors needing to be added to every credential.

NOTE: Access Profiles must be entered manually using the ProxessIQ software, as they will Not be automatically added using the User, Door & Door Group import spreadsheets.
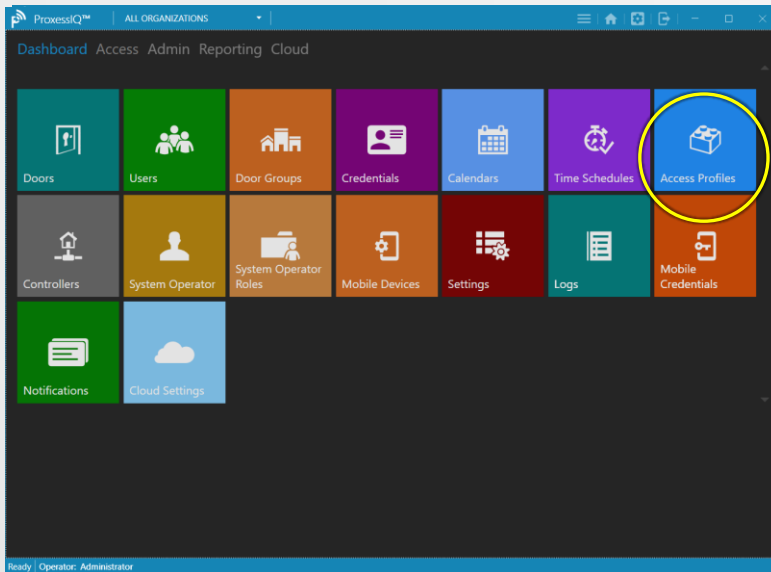
Access Profiles combine Time Schedules and Doors (and Door Groups) together and can then be assigned to Users. To create or edit them, click the "Access Profiles" icon.
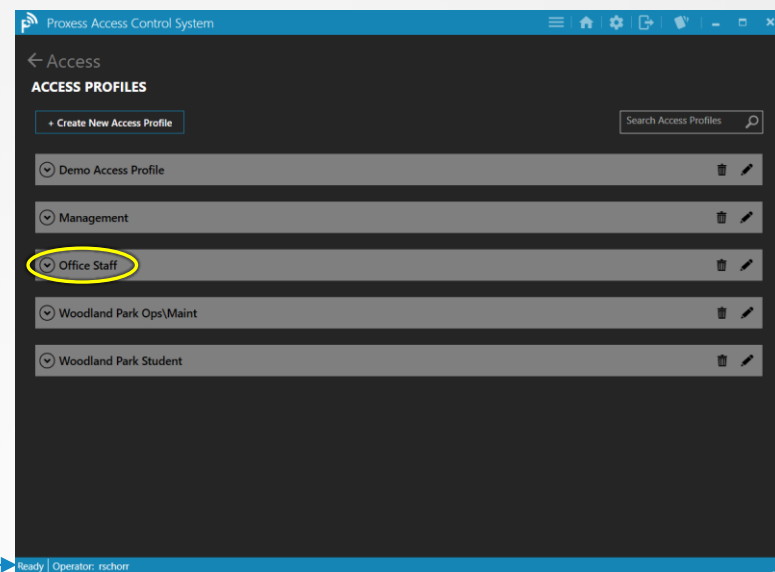
For a quick edit note, if there is one, click an existing Access Profile.
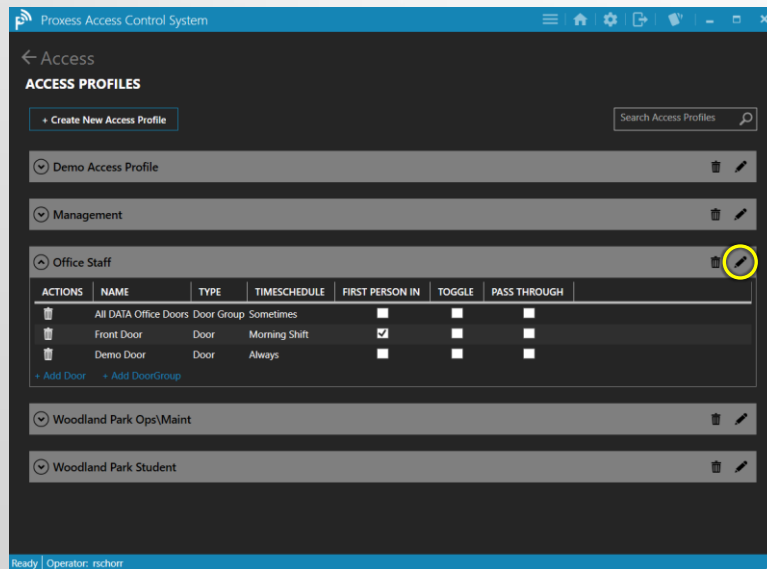
Click the Edit icon.
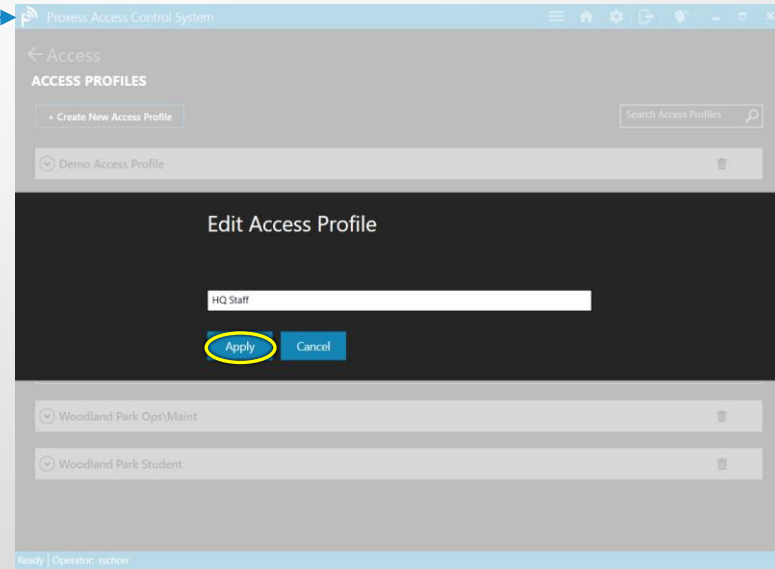
Change the name and click "Apply".
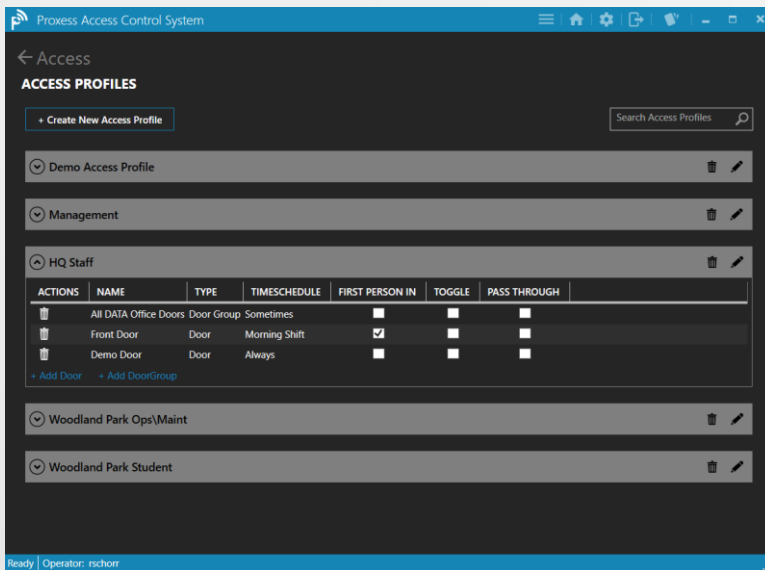
The new Access Profile name appears.
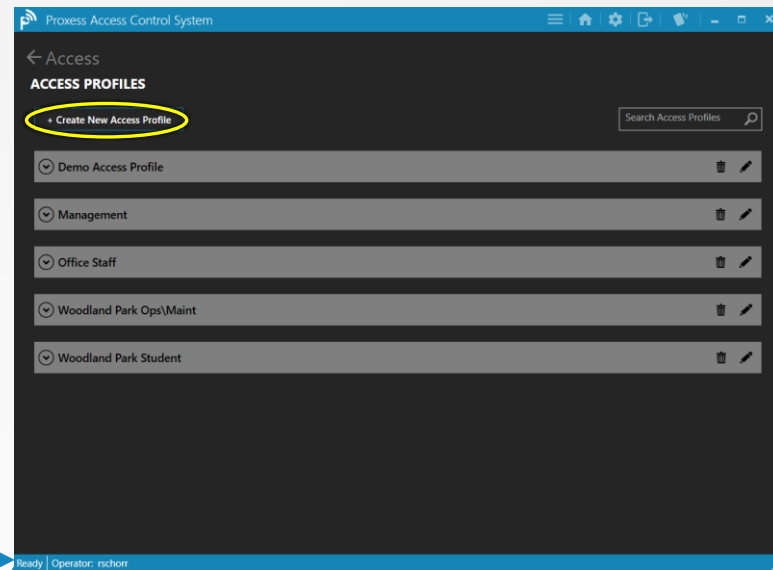
Click "Create New Access Profile".
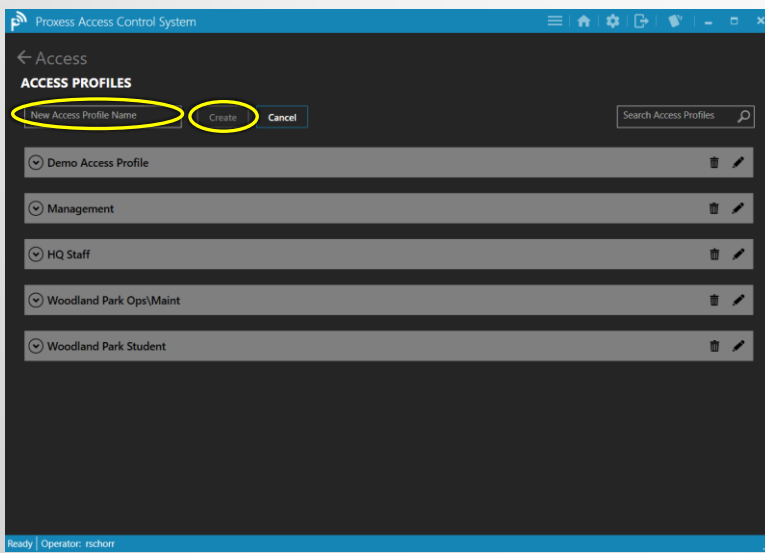
Enter a name for the new Access Profile and then click "Create".
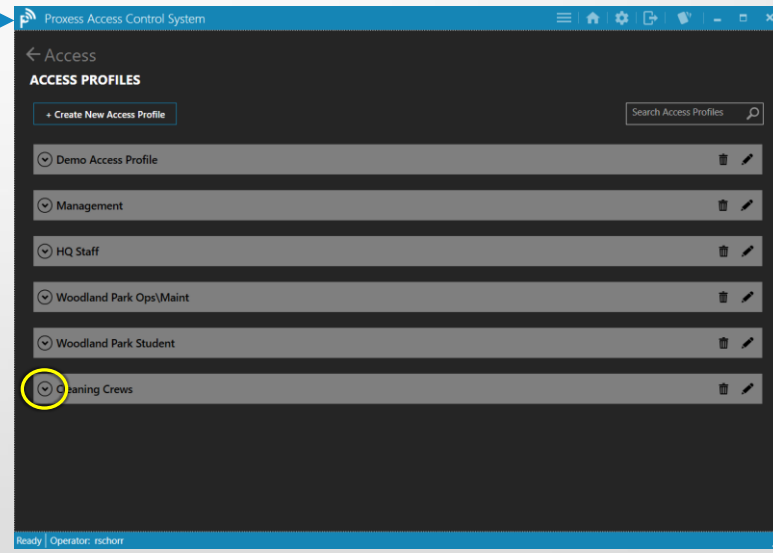
The new Access Profile appears. Click the dropdown arrow to view and edit the details.
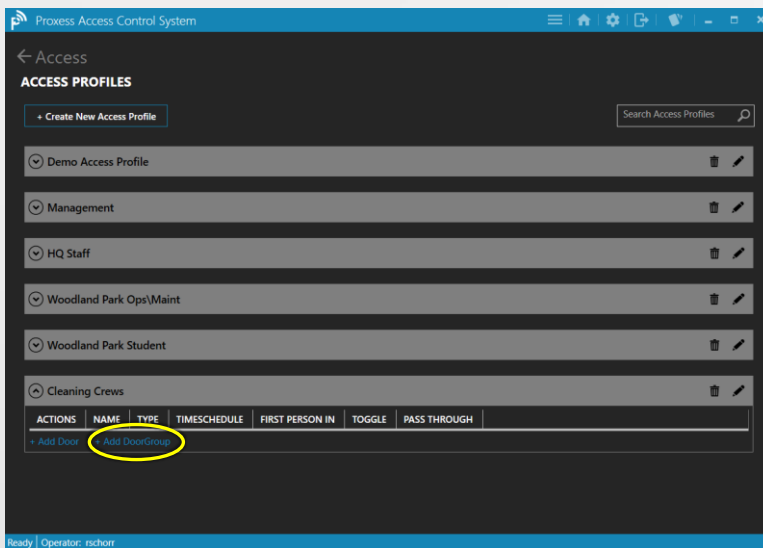
To add a Door Group to the new Access Profile, click "Add Door Group".
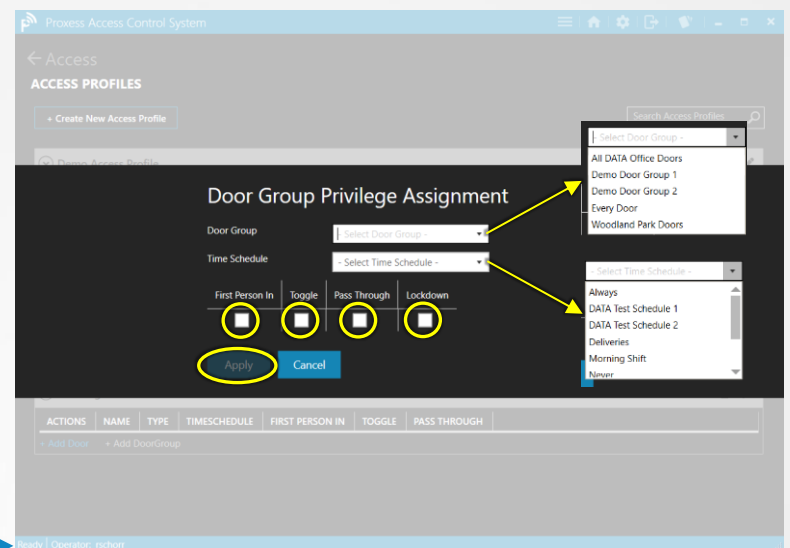
Use the dropdown arrows to select the Door Group to add along with the corresponding Time Schedule that those doors will operate within. Check any of the features that can be used at those doors by appropriately designated cardholders\Users and click "Apply".
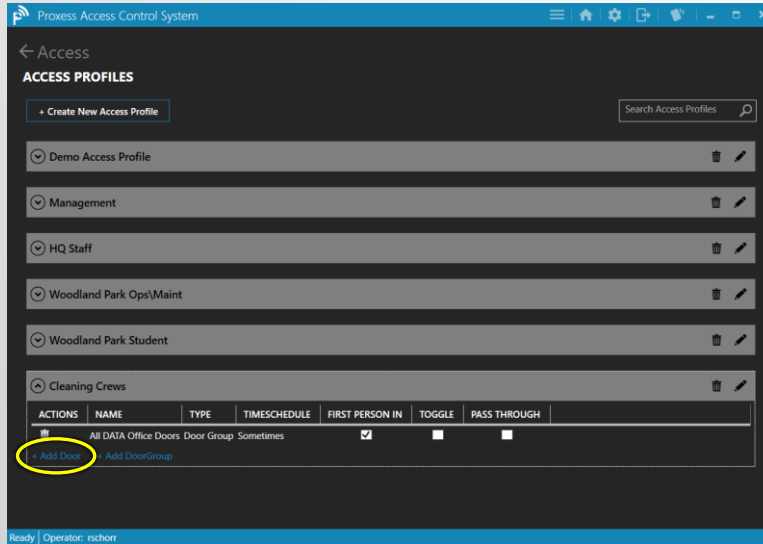
After adding a Door Group and returning to this screen, click "Add Door".
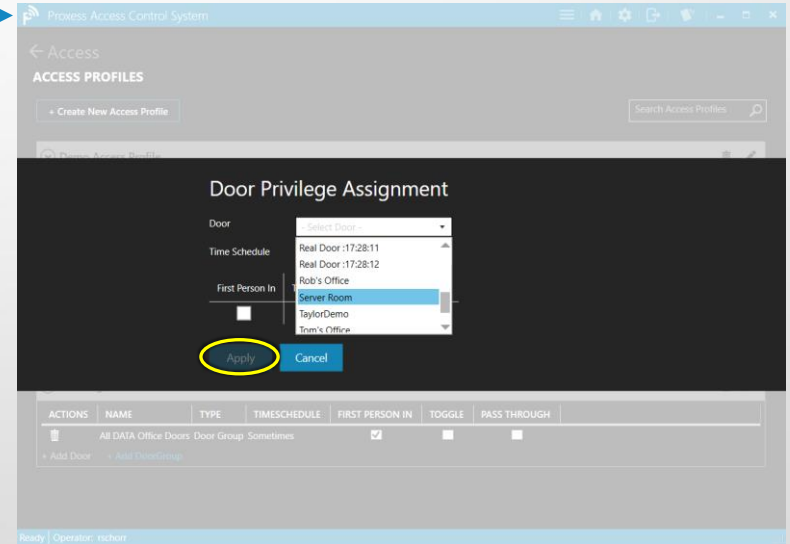
After clicking the "Add Door" button from the main Access Profile screen, select the Door and its corresponding Time Schedule and check off the features that can be used at those doors by appropriately designated cardholders\Users and click "Apply".
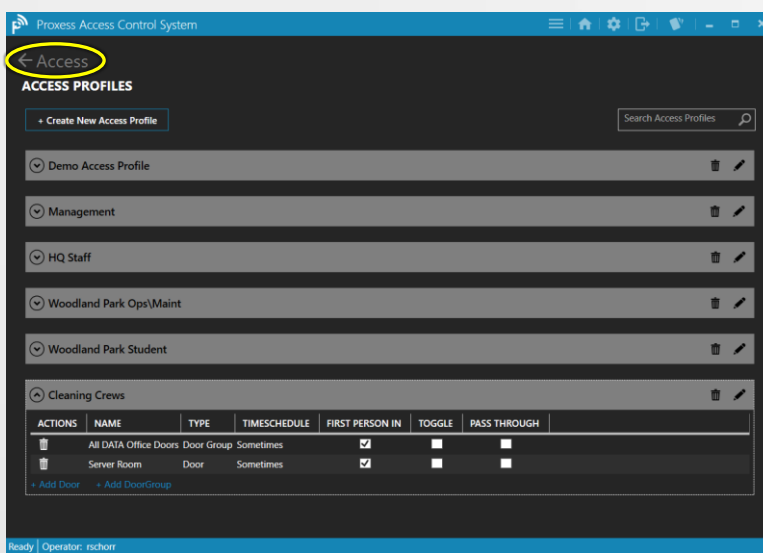
This is the screen you will see after you click Save. To return to the Home Screen \ Dashboard, click either "Access" or the Home icon in the top taskbar.

USERS
Adding & Editing

PHYSICAL Credentials (including cards, fobs and coin & portrait stickers) are addressed in this section.
Mobile Credentials are addressed in the following section.
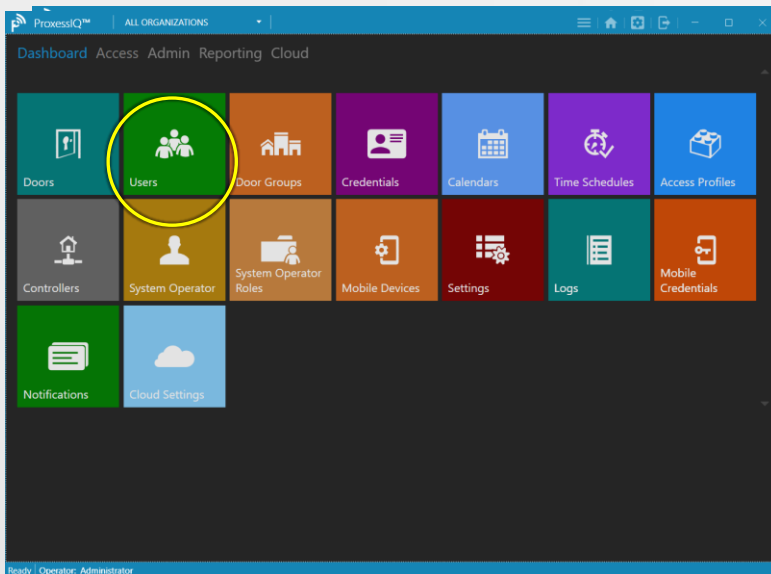
The Users module is where we add and edit new Users\Cardholders and credentials. Their rights to access doors and door groups are also definer here. Click the "Users" icon.

Addressed at the end of this chapter.
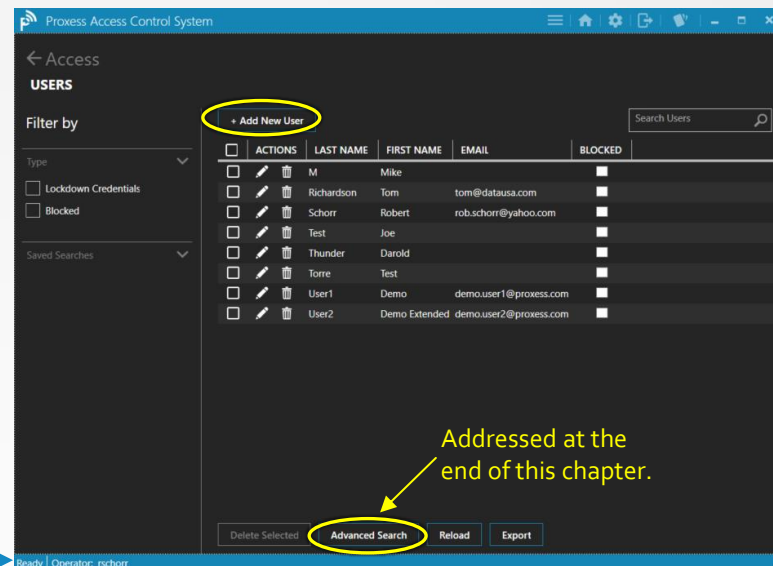
From the main Users screen you can edit, delete and block individual cardholders. The list can be filtered\sorted by checking one or both of the boxes on the left: "Lockdown" and "Blocked" and Users can be searched for by typing letters in their name in the Search box. Click "Add New User" to do so.
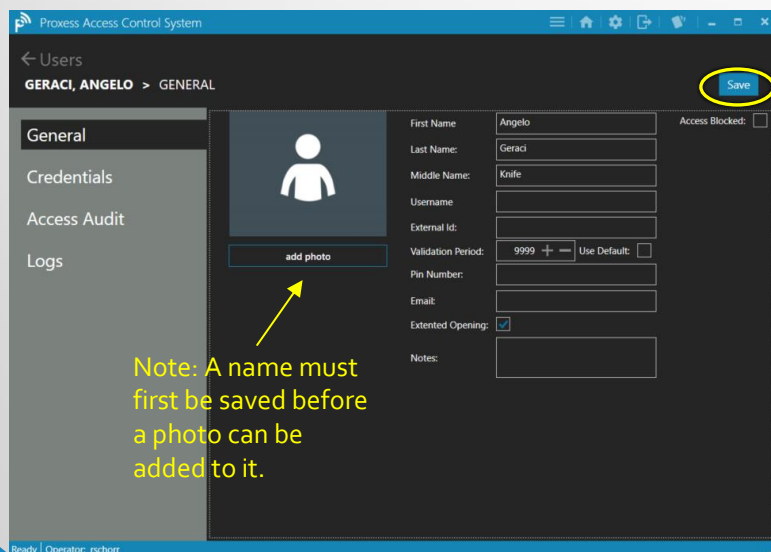
Note: A name must first be saved before a photo can be added to it.
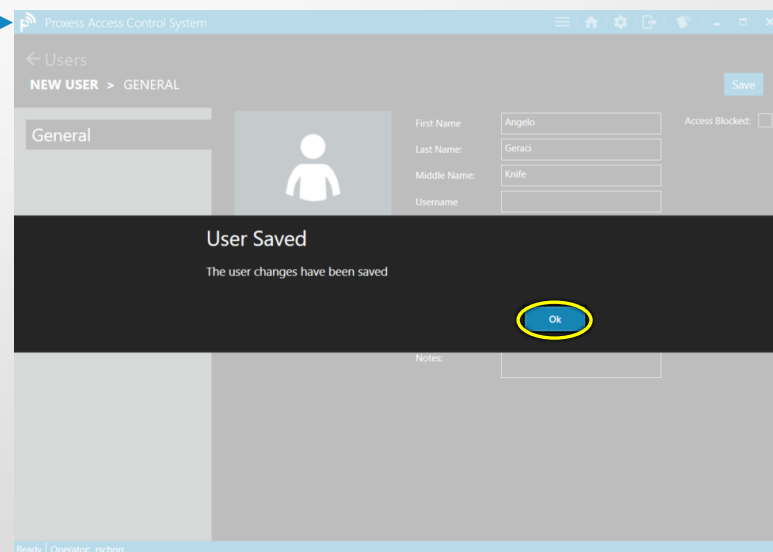
Add the essential new user information, including just their first and last name. Optional information includes the "Validation Period", the number of days a credential has to check-in at an online reader, before access is denied (leave this high for offline systems) and an Extended Opening checkbox, for the wheelchair bound, for example. The Pin is used if an online, wall-mounted reader\keypad is used in the system. The User Name and Email are only needed if this User will also be assigned software Operator rights. Click "Save" to continue.

Now that the new user has been saved, we can assign a card\credential to them. This can be done now, or anytime in the future, by returning to their record, going to the Users module and clicking on the edit icon for their name.

For now, click "Credentials" to proceed.

For this User, click "Add New Credential". As many credentials as desired may be issued to a User.

Select the Activation Date, which is usually left as the current date, but may be set at a future date. Select the Expiration Date of the card, which may be on an annual basis, by semester for schools, or at 90 days for evaluations of new hires. Select the Status of this credential and check the box if it is to be Blacklisted (disallowing access with the *credential*, as opposed to disallowing access of the *user*). You may give a "Name" to this card, such as Vehicle Tag, or Phone Sticker. If you wish to change the "Revalidation Date", return to the "General" tab after saving. Click "Save".

The rights for this credential to access various doors may now be selected. This is done by selecting one or more "Access Profiles" and\or one or more "Door Groups" and individual "Doors". These have been set up in their respective programming modules. Click "Add Access Profile", if desired.

To choose an Access Profile, click the dropdown arrow, or "Cancel" to return to the previous screen.

Select the desired Access Profile from the list and click "Apply".

To add a door for this credential to have access to, click "Add Door".

Click the dropdown arrow to select the first individual Door and then the Time Schedule for the credential to have access to it. Check the appropriate boxes to allow this credential to have First Person In rights, Use this door in a Toggle function, Pass Through\Enter a door that is in Lockdown mode and permit the credential to release a door in Lockdown. (?)

Click "Apply" to proceed, or "Cancel" to return to the previous screen.

Repeat this procedure for all the additional doors and Door Groups that this credential will have access to and then, as long as the new card is on the enrollment reader, click "Write to Card".

The "Stamped ID" of the card will now be shown towards the top of the screen, along with the selected Revalidation Date. Click "Save" to complete the process.
The card programming process is now complete.

From the previous screen, this verification screen appears. Click "OK".

Though the credential programming is complete, we will now show a visualization what we have programmed, as it is listed above. Click on the "Access Audit" tab.
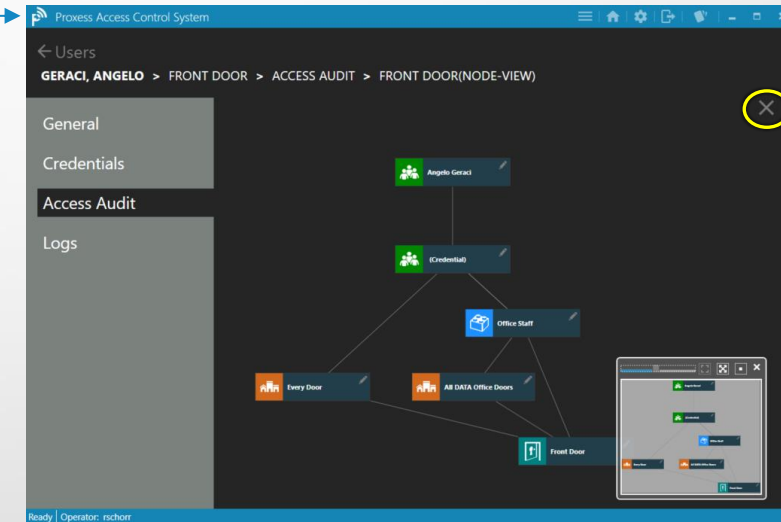
Each of the individual doors this Cardholder\User has access to will appear in this list. For any of the doors, click on its "Views" icon.

This Access Audit view shows the relationship between the cardholder and their credentials and the door selected on the previous screen.
The insert on the bottom right of the screen allows you to see the entire relationship tree and the slide bar at the top of this insert can be moved to widen or narrow the main screen view.
Click "X" in the top right to close this view and return to the list of doors.
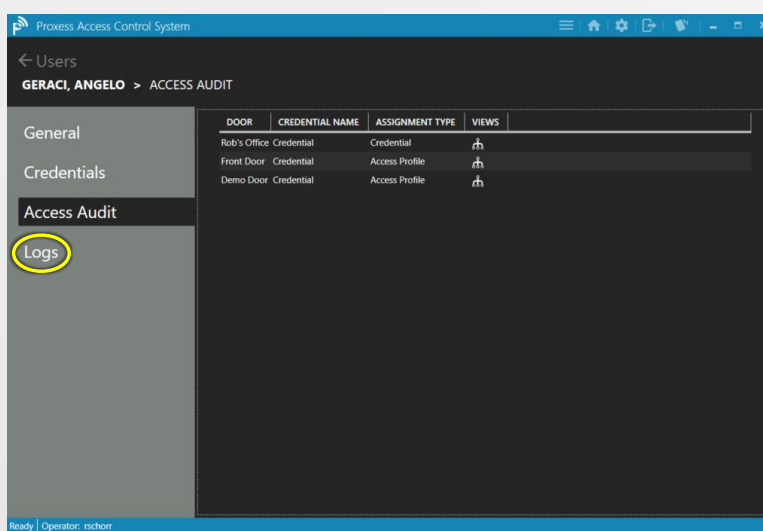
For a list of all of the recorded Events for a User, click "Logs".
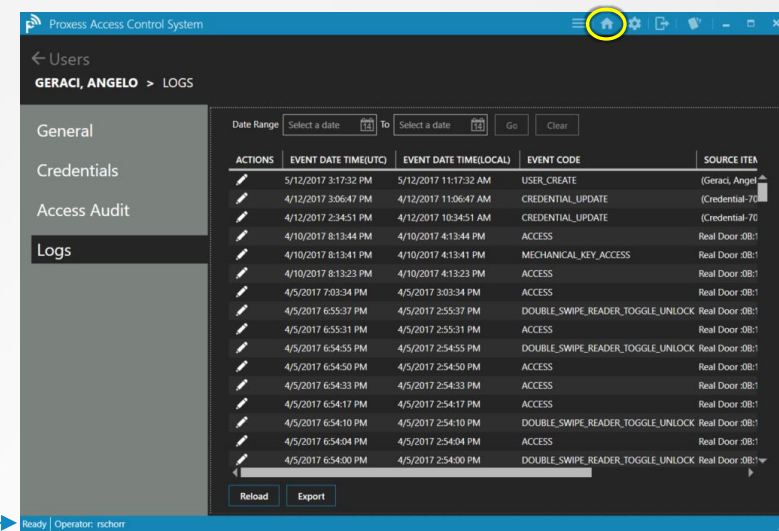
The Log lists every stored Event from that door. This list may be Exported as an Excel file by clicking the "Export" button at the bottom.

This list may be scrolled and may also be searched and shortened, by selecting a "Date Range" from the top of the page. Again, the resulting list may be Exported by clicking the "Export" button.

To return to the full list of Users, click "Users" at the top left.

To return to the Home Screen\ Dashboard, click the Home icon

Advanced Searches of Users

Within each User record

Must cancel "X" an Advanced Search, or the User menu will continue to only show those results.

Advanced Searches of Users

Within each User record

Name this search for your future use and click "OK".
Your new custom search will now appear in this list, for later execution by this and other operators.
When you have completed your Search, you must click "X" to bring you back to the full list of Users, or the User menu will continue to only show those Search results.

Advanced Searches of Users

You are now returned to the full list of Users.
You may execute on that saved search again any time, by clicking on the arrow next to its name.

You may Export the search results to a .csv for further manipulation and click the "X" and return to your normal system work.

USERS
Adding & Editing

==Mobile Credentials== are addressed in this section.
PHYSICAL Credentials (including cards, fobs and coin & portrait stickers) are addressed in the previous section.

Prior to entering and delivering mobile keys to Users, consider communicating to them the expected email they will receive and the installation process. This will result in fewer support calls and a better user experience.

The following is an example from a Proxess customer you may use as a model. An editable copy will be sent upon request,

From: paul.hevesy@proxess.com <paul.hevesy@proxess.com>
Date: Thursday, May 11, 2023 at 5:56 PM
To: Robert Schorr <rob.schorr@proxess.com>
Subject: Proxess Mobile Key Welcome Email

Dear [End User Staff & Team Members] -

This email is to inform you of our exciting new security system designed to more effectively control access to our facilities that will allow you to use your mobile phone as your key!

Your new "key" is an app that needs to be downloaded to your phone. Our new system will leverage Bluetooth from your phone to grant you access.

HERE ARE THE STEPS YOU WILL NEED TO FOLLOW:

STEP 1: Download the "Proxess Mobile Credential" App TODAY from the appropriate app store here:

IMPORTANT: Once you download the app to your phone please **DO NOT TAKE** any further action until you have received an email invitation from "Proxess (no reply)" to your company/personal email.

STEP 2: Once the new security system is fully installed and programmed, you will be added to the system as a user. As part of the process, you will receive an email invitation from "Proxess (no reply)" to your company/personal email that looks like the image below.

You have been invited to Proxess Mobile by Proxess Texas Demo

Proxess (no-reply) <no-reply@proxess.com>
To: sample@proxess.com

Today at 4:41 PM

Proxess

Invitation

You have been invited to use Proxess Mobile by Proxess Texas Demo. Proxess Mobile enables users to use their phones as access credentials.

1. Download the Proxess Mobile app from the appropriate app store.

2. Once the app is installed, open the link below on your mobile device.

Here are some things to note:

- You must use this email address to retrieve your credentials. If you need to use a different email address you must have the ACS administrator change your address in the system.
- The link below expires in 30 minutes and can only be used once.
- You must be able to click the link from the mobile device running the mobile credential app for authentication to work.

Don't worry, you can request a new email to be sent from the app. If you uninstall the app you will need to request another link.

→ OPEN THIS LINK ←

STEP 3: While using your mobile phone to locate the email invitation, open the Proxess (no reply) email and scroll to the bottom of the email and tap "OPEN THIS LINK"

This will authenticate your mobile key by taking you directly to the Proxess Mobile Key app on your phone.

That's it! In a separate communication you will receive further information on how to use your new mobile key!

NOTE: You can also watch a How To Download Your Proxess Mobile Credential For The 1st Time video here

Now that the new user has been created and saved, we can assign a card\ credential to them. This can be done now, or anytime in the future, by returning to their record, going to the Users module and clicking on the edit icon for their name.
For now, click "Credentials" to proceed.

For this User, click "Add New Credential".
As many credentials as desired may be issued to any User.

The Credential status screen appears.
You may (but do not need to) add a name for this User's credential.
Check the box to identify it as a Mobile Credential.
Click "Save"

You may now assign Privileges (a.k.a. access rights) for this Mobile Credential, as defined in the previous section.
In this case we will assign the Privilege for this credential to access the Door Group Engineering Department, during the Time Schedule Always and the individual Door Lakeside, South , also during the Time Schedule Always.
When you are done, click "Save" and the mobile credential email invitation will be delivered to the recipient.
Toggle & Lockdown views will be shown in a few pages from here.
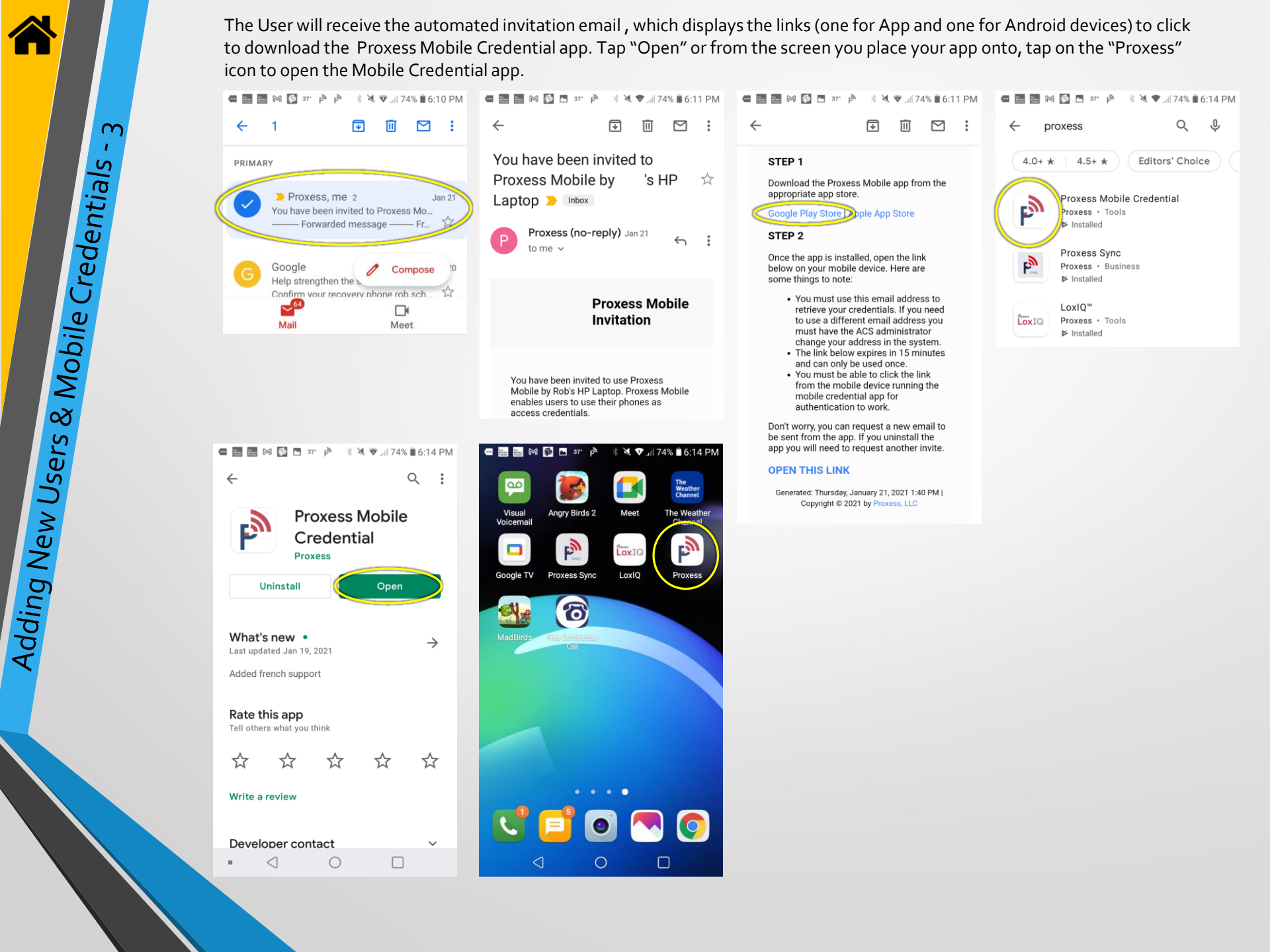
The User will receive the automated invitation email , which displays the links (one for App and one for Android devices) to click to download the Proxess Mobile Credential app. Tap "Open" or from the screen you place your app onto, tap on the "Proxess" icon to open the Mobile Credential app.
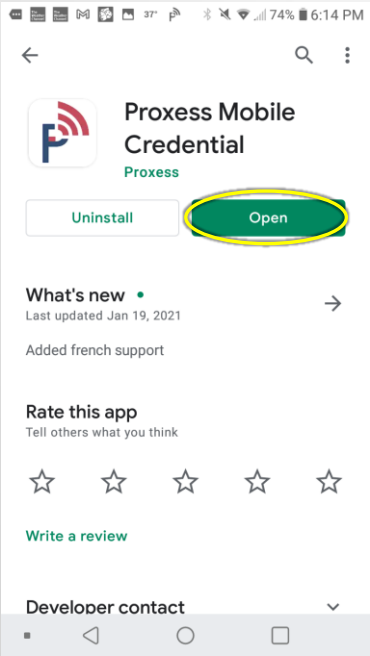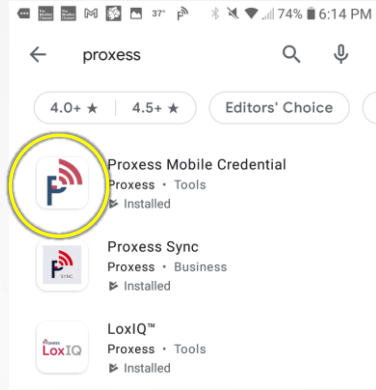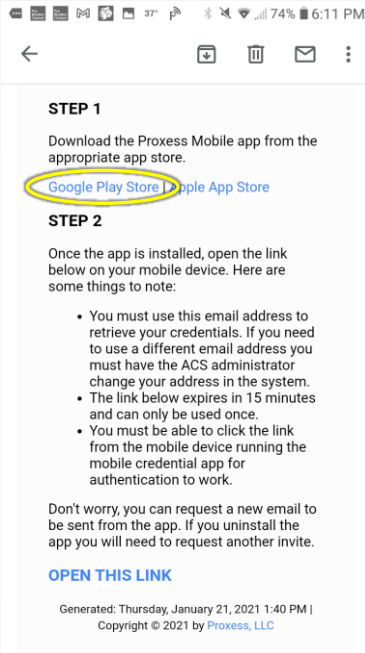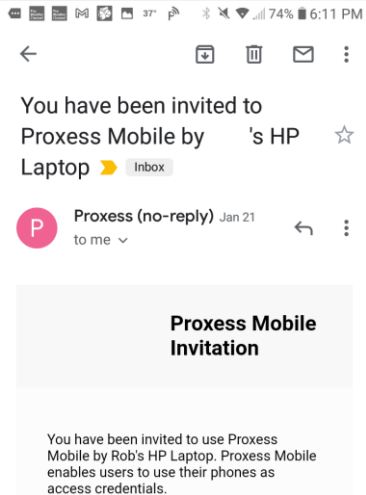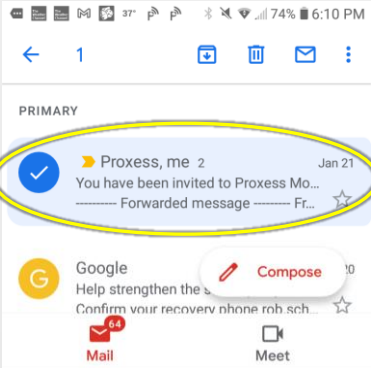
The Mobile Credential app will open in "Easy Unlock" mode, where it will automatically find and display the door with the greatest signal strength (usually the closest door as well). Tap the "Open" button for the door you wish to access and it will unlock. For the best user experience, open your app on your approach to the door, so the app has already displayed the door and you have already tapped Open, prior to your arrival at the door handle.
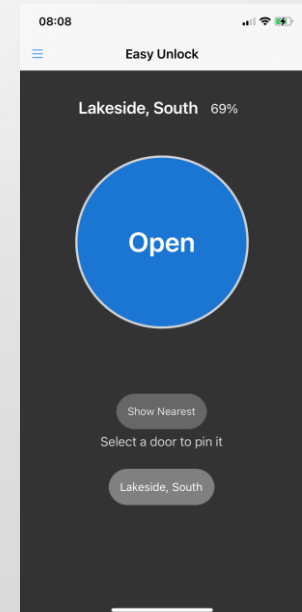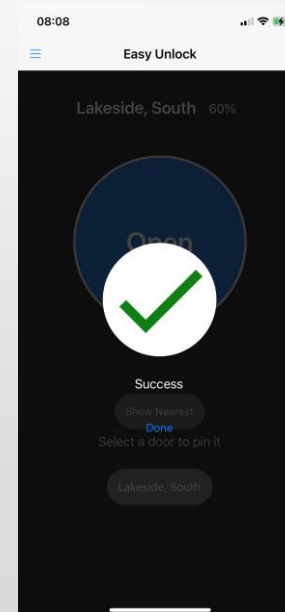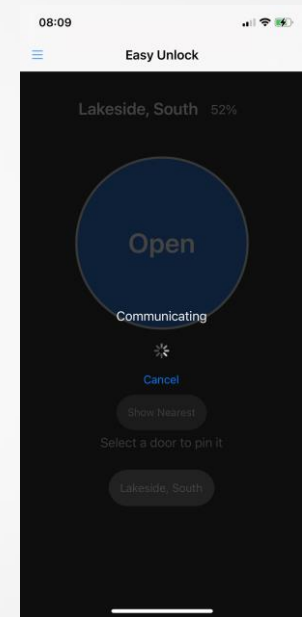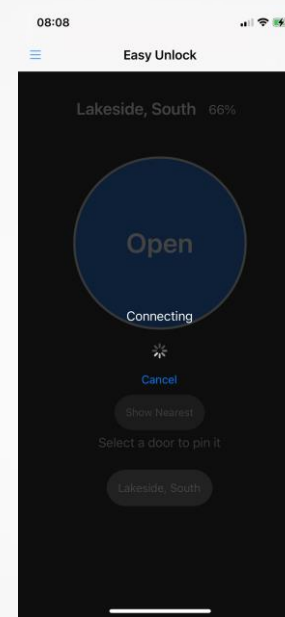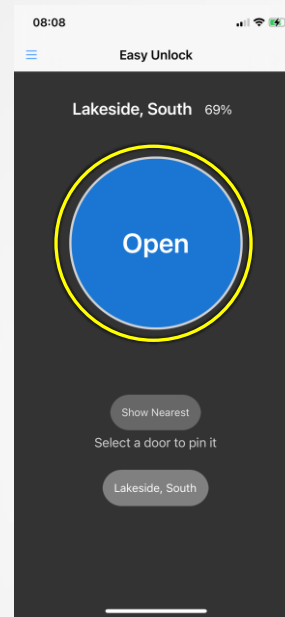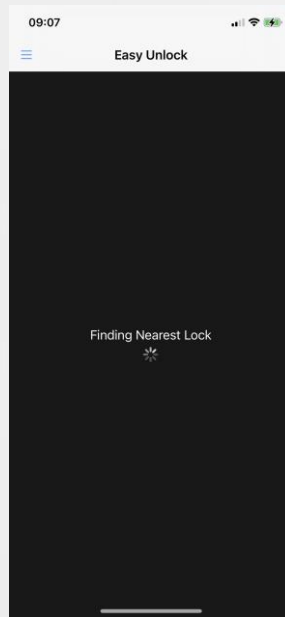
When creating a Mobile Credential, you may assign Toggle rights. In this case, the "Toggle Unlocked" and "Toggle Locked" buttons will display. Toggled locks remain Unlocked (no credential required to enter) until either Toggled Locked or until the next Time Schedule occurs requiring the lock to be in the locked (valid credential required to enter) state.

When toggled into the Unlocked mode, the mobile credential will not display the "Open" button. Once the lock is toggled back to the Locked mode the "Open" button will again display.
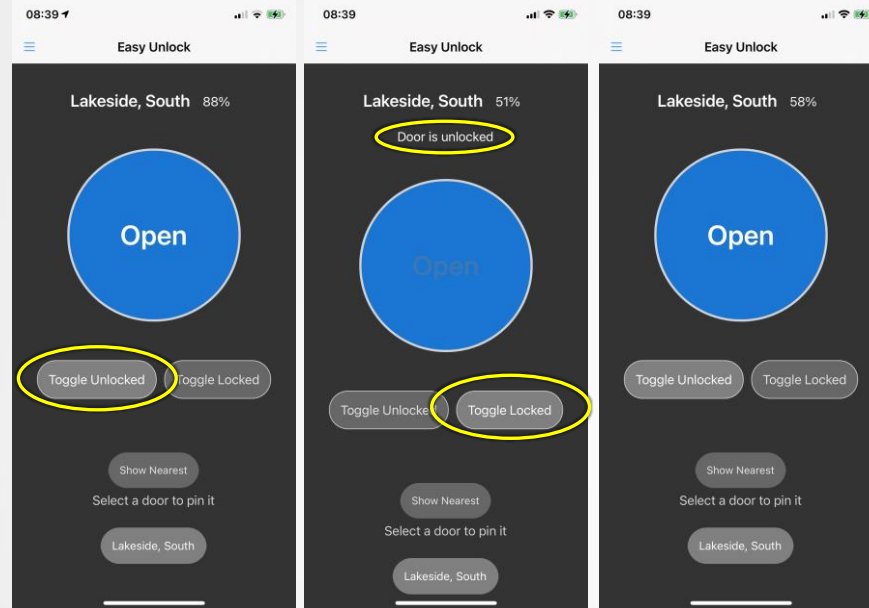
When creating a Mobile Credential, you may assign Lockdown rights. In this case, the "Enter Lockdown" and "Exit Lockdown" buttons will display. You can also assign normal, Toggle and Lockdown rights on the same Mobile Credential (see image to the right).

When the lockset has entered the Lockdown mode, a note in red will display. Once removed from the Lockdown mode the note will be removed.
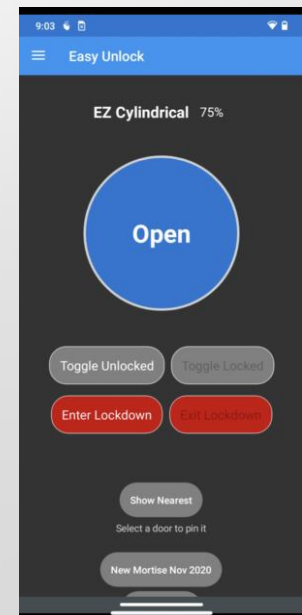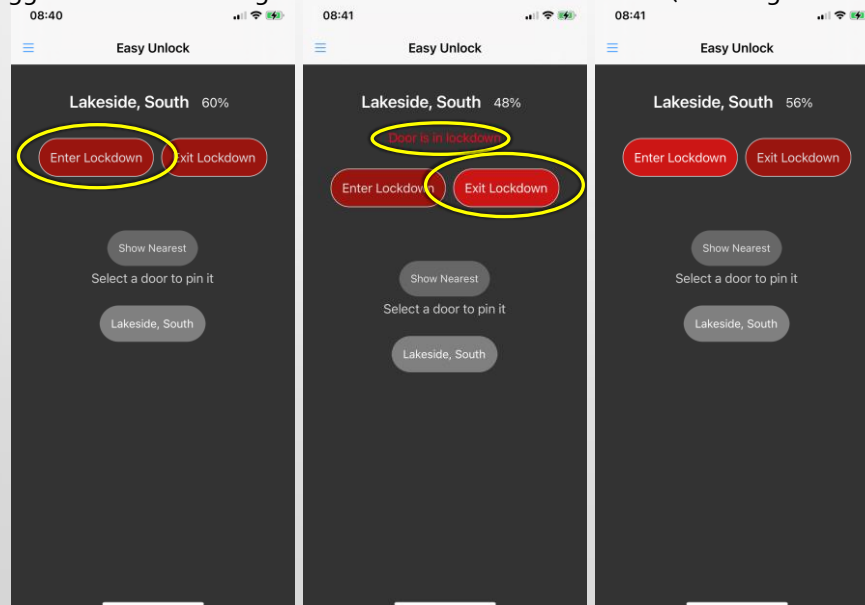
By default, the Mobile Credential will open in the "Easy Unlock" mode. In this mode, the app will automatically locate and display the door with the greatest signal strength... Tap the hamburger icon in the top left to being up the mode menu. Click on the "Access" mode and all of the Organizations that you have rights for access will be listed. Tap on the organization you want to see your rights for.

Your credential name will display, along with the list of doors that you have access to. For applications allowing temporary offline operation, there is a 5-minute check-in requirement for the mobile credential to get online to reverify its rights and the countdown is shown in green text. When the credential rights expire a note in red appears "Invalid (Needs to be refreshed)". Bring the phone online (via WiFi or a mobile network) and the rights will be renewed for five (5) more minutes. Click the hamburger icon to return to the Easy Unlock operation.
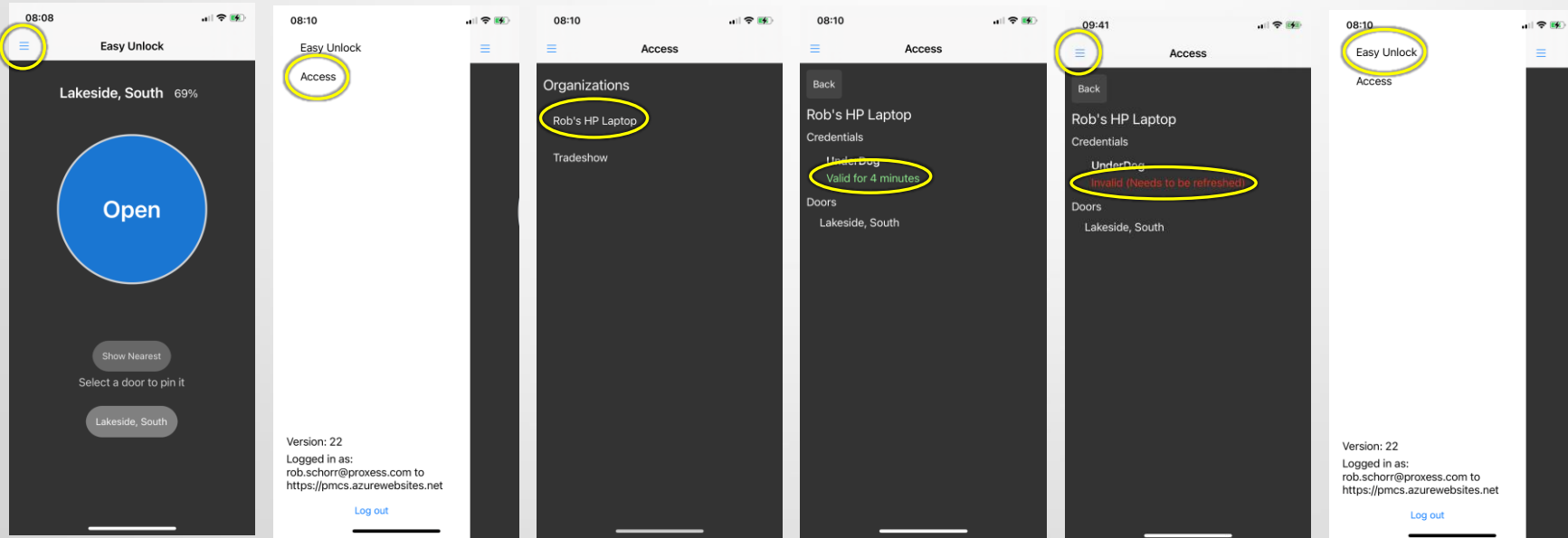
USERS
Spreadsheet Adding & Editing

How to MASS-Add and edit Users & Credentials using a .csv spreadsheet

Mass Adding and Editing Users, using a .csv spreadsheet

To make mass User additions, changes or deletions, no program is simpler or more flexible than Microsoft Excel or Google Sheets.

Proxess can import a .csv formatted file from those programs or Notes, etc., with an unlimited number of Users entered, for mass-card entry, deletion or changes.

We will now explain to columns of detail that can be added, their format requirements and how to perform the imports and exports.

For reference, these are the overall views of all the fields that can be imported & exported and we will enlarge them and explain each field on the following pages.

Import List snapshot:

Export List snapshot:

Mass Adding/**Importing** and Editing Users, using a .csv spreadsheet

Import List snapshot (**Page 1 of 3**):

Note: The column order may not be altered from the below and the exact headers must appear, as shown.

A	B	C	D	E	F	G	H	I	J	K
ExternalId	FirstName	LastName	MiddleName	UserName	Email	PinCode	Extended Opening	Notes	Organiza tionGuid	ShareWith ChildrenOrgs

ExternalID: Not required to be entered by the end user. Will otherwise be automatically assigned by the system. This is a unique identifier and may not be changed, or the entry will be treated as a second/additional user entry. The User's existing ExternalID must be included here for subsequent data imports. Therefore, this **SHOULD** be created & entered in this initial import list.

FirstName: No minimum or maximum characters

LastName: No minimum or maximum characters

MiddleName: No minimum or maximum characters May be used for "Custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.)

UserName: No minimum or maximum characters. May be used for "Custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.).

Email: No minimum or maximum characters. This is the email that will receive Notifications and Mobile Keys

PinCode: Not currently used

ExtendedOpening: Enter "TRUE" if this credential-holder will receive the extra time to open the door and "FALSE" is they won't.

Notes: No minimum or maximum characters. May be used for "Custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.)

OrganizationGuid: Not required to be entered by the end user. Will otherwise be automatically assigned by the system, uniquely for each the "Global" and "Child" Organizations. This is a unique identifier and may not be changed, or the credential will not be added correctly and may be unusable. The User's existing OrganizationGuid must be included here for subsequent data imports. "Organizations" is a separately licensed feature.

ShareWithChildrenOrgs: Enter "TRUE" if this credential may be seen and managed by Operators of downstream/Child Organizations.

Import List snapshot (**Page 2 of 3**):

Note: The column order may not be altered from the below and the exact headers must appear, as shown.

L	M	N	O	P	Q	R	S	T	U	V
Credential Name	CredentialActivation DateTime	CredentialExpiration DateTime	EnableMobile Credential	Access ProfileList1	Credential PrintedNumber	Credential Status	BlockList Credential	Remove User	Force Update	ImportStatus
Tom Mobile	5/18/2023 0:00	5/18/2026 0:00	TRUE	Bldg1		Other	FALSE	FALSE	FALSE	ReadyForImport

CredentialName: Not required to be entered by the end user. Especially when multiple credentials are issued to a User, individually naming each credential allows for more obvious and quicker recognition and sorting in the Event Logs. Especially important where there may be multiple credentials delivered to a single room/dorm/household. No minimum or maximum characters

CredentialActivationDateTime: The day & time this credential will begin to operate on its doors. This format must be followed precisely for the date and time (Military format: hours:minutes)

CredentialExpirationDateTime: The day & time this credential will cease operating on its doors and will need to be re-encoded on an ENR enrollment reader in order to begin working on doors again. This format must be followed precisely for the date and time (Military format: hours:minutes)

EnableMobileCredential: Enter "TRUE" if this credential will be a mobile key (mobile phone credential). Otherwise enter "FALSE", or leave it blank.

AccessProfileList1: Enter all the APs (Access Profiles) for this credential. Separate each AP with a "|" (e.g. "Building Amenities|Athletic Center"). A maximum of 24 Aps can be entered into this cell and thus applied to a single credential, for a maximum of 24 total privileges (which is the maximum number of Direct Privileges [a combination of Doors & Door Groups] that a single credential may have). **NOTE:** Aps MUST be **entered manually** using the ProxessIQ software and will NOT be auto added.

CredentialPrintedNumber: The number printed on the physical credential. This is purely a visual reference and for easier look up and in the future will be used for using 3rd part credentials.

CredentialStatus: Enter Active, Returned, Damaged, Lost, Deactivated, Other. Leave it blank for no change to be made to the database.

BlocklistCredential: Enter "TRUE" if this credential must be denied and never allowed access, until an Admin resets it.

RemoveUser: Enter "TRUE" is this User is to be deleted from the database & not just deactivated. Enter "FALSE" otherwise.

ForceUpdate: Enter "TRUE" if there are changes to the User that you are certain you wish to have update the existing database record…Otherwise, enter "FALSE". If there is an existing Credential for the User, the User will be removed from the search list, but their credential will remain in the Credential menu until it is deleted. Then the credential and user will both be gone.

ImportStatus: Enter "ReadyforImport" if this User may be added or updated at this time. Otherwise, if, for instance, their rights area still being determined, enter "FALSE".

Spreadsheet Import Utility- 3

Mass **Exporting** of Users, using a .csv spreadsheet

Export List snapshot (**Page 1 of 1**):

For reference, these are the overall views of all the fields that will be exported.
Once you download it and open it with Excel or Sheets, you may make your global changes
Do not make any additional user additions in the software until you have made changes to this export and
have then re-imported it.
Note: The column order may not be altered from the below and the exact headers must appear, as shown.

ExternalId	Last Name	First Name	Middle Name	Email	Username	Organizations	Notes	PinCode	ExtendedOpening
684f1dca-a3c0-4	Altadena	Angelica		tadenala@hp.com		Global			FALSE
368c6807-55d9-4	Caudillo	Claudia		claudia.caudillo@gmail.com		Global			FALSE

ExternalID: This field will automatically be assigned by the system – if it was not already entered by the customer. This is a unique identifier and may Not be changed, or the next time it is imported, it will be treated as a second/additional user entry. Thus, the User's existing ExternalID must be included here for subsequent data imports.

FirstName: No minimum or maximum characters

LastName: No minimum or maximum characters

MiddleName: No minimum or maximum characters May be used for "Custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.)

Email: No minimum or maximum characters. This is the email that will receive Notifications and Mobile Keys

UserName: No minimum or maximum characters. May be used for "Custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.).

Organizations: Multiple Organizations can be entered here, using the "|" character (e.g. Global|Building 1).

Notes: No minimum or maximum characters. May be used for "Custom", sortable data (Staff, Student, Administrator, Leadership, Building, Department, etc.)

PinCode: Not currently used

ExtendedOpening: Enter "TRUE" if this credential-holder will receive the extra time to open the door and "FALSE" is they won't.

Note: When using sortable fields, you may sort by the group you wish to make a field change to and then copy & paste that parameter change to just the credentials in that group. Then you may re-import this spreadsheet.

How to make mass changes to the rights for a User Group:

- *Instant Holiday calendar addition:* Give Holiday access to only the group you want to keep allowing access to. Extend the Holiday for as long as desired.

- *Instant Access Profile change:* Delete a "Door Group A" from the AP, which the Users you want to exclude have access to. Leave a duplicate "Door Group B" which only the Admin team have access to. Add "Door Group A" when the event is over.

- *Export & Import spreadsheet:* Export all users of a particular group (e.g. Admin, Leadership, Teachers, Coaches, HS Teachers, Staff, Contractors), using a custom field (e.g. MN, UN, Notes). Change their AP according to their updated rights/restrictions(e.g. Days, Doors, MK operation) & re-import the file.

SQL SERVER
DATABASE EXPORTS

In addition to the "Export" button in Users, Doors & Door Groups, you can export more information from SQL

Note: This is not a training guide for SQL and is just referential for those already familiar with SQL on where to locate the Proxess data.

Open SQL Server Management Studio & Connect to the ProxessIQ™ Database
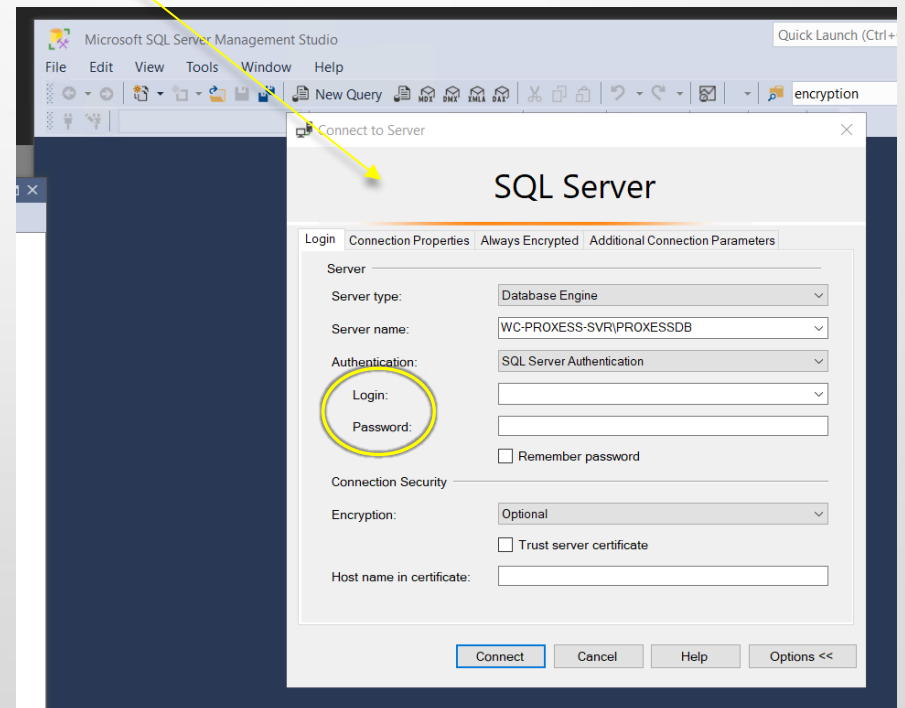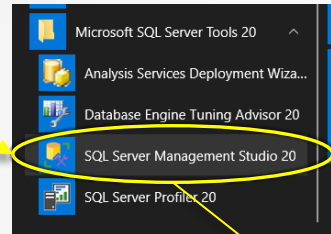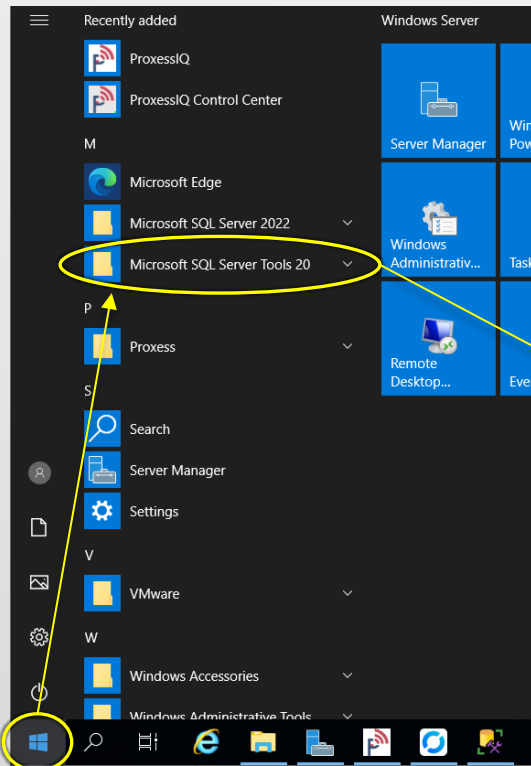
Locate the Database Login & Password

Open SQL Server Management Studio & Connect to the ProxessIQ™ Database

If You Cannot Find the Proxess Database Name or Password
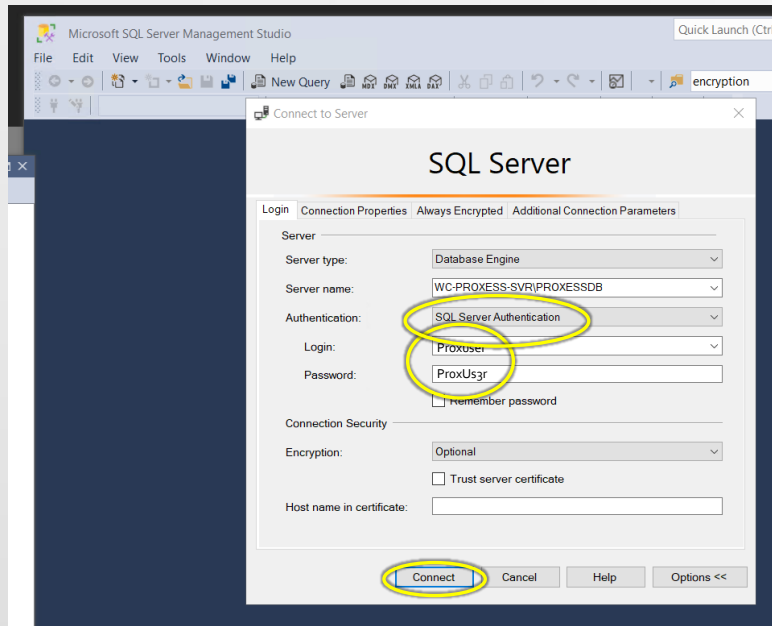
OR
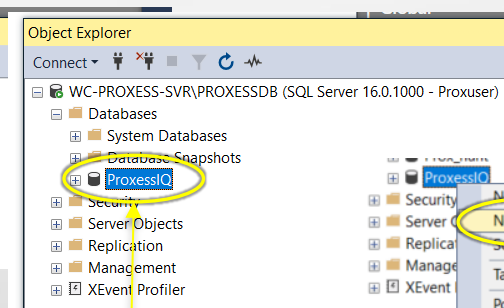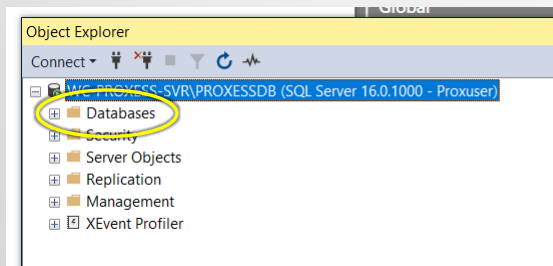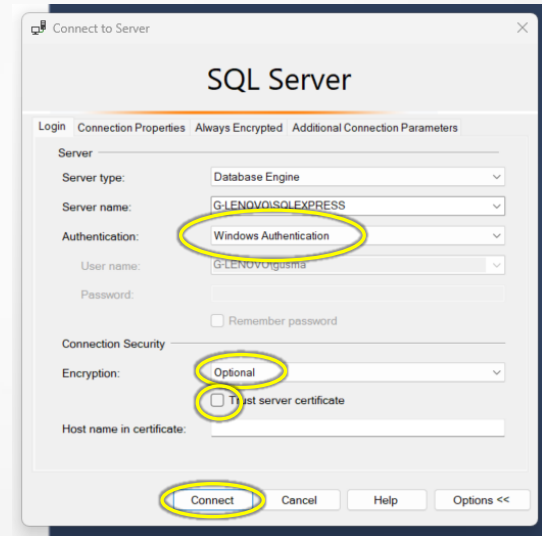
Right
-Click

SQL Database Exports - 5

dbo.Credentials
Columns
- CredentialId (PK, int, not null)
- CryptoCredentialId (varbinary(max), null)
- CryptoExternallyPrintedNumber (varbinary(max), null)
- EncodedId (decimal(20,0), not null)
- StampedId (nvarchar(max), null)
- ExternalId (nvarchar(max), null)
- Name (nvarchar(max), null)
- Notes (nvarchar(max), null)
- Blacklist (bit, not null)
- ExpirationDate (datetime, not null)
- ActivationDate (datetime, not null)
- RevalidationDate (datetime, not null)
- CreatedDateTime (datetime, not null)
- ModifiedDateTime (datetime, not null)
- CredentialStatus (int, not null)
- DeleteFlag (bit, not null)
- UserId (FK, int, not null)
- HasChanges (bit, not null)
- MPDId (int, not null)
- EnableMobileCredential (bit, not null)
- CardLastWrittenDate (datetime, not null)
- ExternalData (nvarchar(max), null)

SQLQuery5.sql - WC-PROXESS-SVR\PROXESSDB.ProxessIQ (Proxuser (58))* - Microsoft SQL Server Management...

Quick Launch (Ctrl+Q)

File   Edit   View   Query   Project   Tools   Window   Help

encryption

ProxessIQ   ▶ Execute

SQLQuery5.sql - WC...sIQ (Proxuser (58))*   SQLQuery4.sql - WC...sIQ (Proxuser (60))*   SQLQuery3.sql - WC...sIQ (Proxuser (61))*

```sql
SELECT [CryptoExternallyPrintedNumber], [ExternalId], [Name]
FROM [dbo].[Credentials]
```

100 %

Results   Messages

	CryptoExternallyPrintedNumber	ExternalId	Name
35	0x0000000000123309	1006	Marilyn Lacy card
36	0x0000000000123221	1009	David Adams card
37	0x0000000000123222	1010	Drew Adams card
38	0x0000000000123223	1011	Janice Aderibigbe ca...
39	0x0000000000123224	1012	Stella Afolabi card
40	0x0000000000123225	1013	Lawrence Aitch card
41	0x0000000000123226	1014	Olubukola Akinsipe c...
42	0x0000000000123227	1015	Anthony Alexander c...
43	NULL	1016	Lemar Ali card
44	0x0000000000123240	1017	Leaza Allen card
45	0x0000000000123228	1018	Jenise Anthony card
46	0x0000000000123229	1019	Audranette Arrington ...
47	0x0000000000123230	1020	Mark Ashe card
48	0x0000000000123231	1021	Garrett Askew card

Query executed successfully.   WC-PROXESS-SVR\PROXESSDB (1...   Proxuser (58)   ProxessIQ   00:00:00   526 rows

dbo.Doors
  Columns
    DoorId (PK, int, not null)
    ExternalId (nvarchar(max), null)
    LockModel (nvarchar(max), null)
    DeleteFlag (bit, not null)
    CreatedDateTime (datetime, not null)
    ModifiedDateTime (datetime, not null)
    LastUpdateDateTime (datetime, not null)
    MinimumValidationDate (datetime, not null)
    UpdateRequired (bit, not null)
    Name (nvarchar(max), null)
    LocationId (FK, int, not null)
    TimeZone (nvarchar(max), null)
    Notes (nvarchar(max), null)
    LockNumber (nvarchar(max), null)
    DoorType (int, not null)
    LockMode (int, null)
    UnlockTime (int, null)
    UnlockTimeExtended (int, null)
    DoorHeldOpenDetectTime (int, null)
    DoorHeldOpenDetectTimeExtended (int, null)
    FirstPersonIn (bit, null)
    CalendarId (FK, int, null)
    UnlockTimeScheduleId (FK, int, null)
    ToggleEnableTimeScheduleId (FK, int, null)
    CardOnlyTimeScheduleId (FK, int, null)
    DefaultDoorState (int, not null)
    BatteryLastChanged (datetime, not null)
    InstallationDate (datetime, not null)
    FailCondition (int, null)
    AuditOverwritePolicy (int, null)
    SupervisionSeriesResistor (int, null)
    SupervisionParallelResistor (int, null)
    ToggleMaxDelayTime (int, null)
    LockDownMinDelayTime (int, null)
    EgressDisableLockdown (bit, null)
    PassThroughCancelsLockdown (bit, null)
    InteriorLEDLockdownTimeOn (int, null)
    InteriorLEDLockdownTimeOff (int, null)
    ExteriorLEDInvalidAccessOnTime (int, null)

    ExteriorLEDValidAccessOnTime (int, null)
    BeepWithProgramming (bit, null)
    BeepWhenAccessGranted (bit, null)
    BeepWhenAccessDenied (bit, null)
    RecordValidAccessAttempts (bit, null)
    RecordInvalidAccessAttempts (bit, null)
    RecordContactPoints (bit, null)
    RecordLockEvents (bit, null)
    RecordCommunications (bit, null)
    ControllerId (FK, int, null)
    ControllerOrder (int, not null)
    EnableNocAudits (bit, null)
    BatteryFailureThreshold (int, null)
    BatteryLowPercent (int, null)
    BatteryCriticalPercent (int, null)
    OrganizationId (FK, int, null)
    OrganizationGuid (uniqueidentifier, not null)
    LockType (int, not null)
    ButtonToggleEnabled (bit, null)
    ButtonLockdownEnabled (bit, null)
    LockdownRequiresHandle (bit, null)
    LockdownGestureTimer (int, null)
    DeadboltEnablesLockdown (bit, null)
    RelayOption (int, null)
    DoorPositionSwitchOption (int, null)
    RequestToExitOption (int, null)
    MotorEnabled (bit, null)
    EncryptReaderCommunications (bit, null)
    ShareWithChildrenOrgs (bit, null)
    DoorHeldOpenAlarmSetting (int, null)
    DoorForcedOpenAlarmSetting (int, null)
    HardwareVariant (int, not null)
    EnableDPS (bit, not null)
    ExternalData (nvarchar(max), null)
    MotorRuntimeOverride (int, null)
  Keys

SQLQuery2.sql - WC-PROXESS-SVR\PROXESSDB.ProxessIQ (Proxuser (59))* - Microsoft SQL Server M

File   Edit   View   Query   Project   Tools   Window   Help

New Query

ProxessIQ   Execute

SQLQuery2.sql - WC...sIQ (Proxuser (59))*   SQLQuery1.sql - WC...sIQ (Proxuser (51))*

```sql
SELECT [ExternalId], [Name]
FROM [dbo].[Doors]
WHERE [ExternalId] != ''
```

100 %

Results   Messages

	ExternalId	Name
1	ff623d6f-ef3c-43bd-ac76-cc15213bf545	MC 115 Class
2	822f2cbc-7885-4256-95c5-9bf5abe88730	MC 116 Class
3	75716419-271b-4f7c-aff7-653f2087bd22	MC 117 Library
4	d164e22b-1f82-4067-89d0-18bf03b5dcdc	MC 118 Class
5	0486fee8-3652-4f1a-9d6d-250a554d9492	MC 121 Class
6	1ef48bc4-56ed-4b3b-8aad-d35556b7be15	MC 122 Class
7	3597651f-8789-4e33-9882-21ede718aa4d	MC 123 Class
8	2f4f1839-3480-4a2a-bb5f-efff3b8125c8	MC 124 Class
9	1a033510-b72b-43fd-814e-0382378f699c	MC 125 Class
10	fbcg 4001	Construction Basement
11	fbcg 4002	Construction Front
12	fbcg 1001	EC 104 Telephone Room
13	fbcg 1002	EC 112
14	fbcg 1003	EC 112 A

Query executed successfully.   WC-PROXESS-SVR

SQL Database Exports - 8

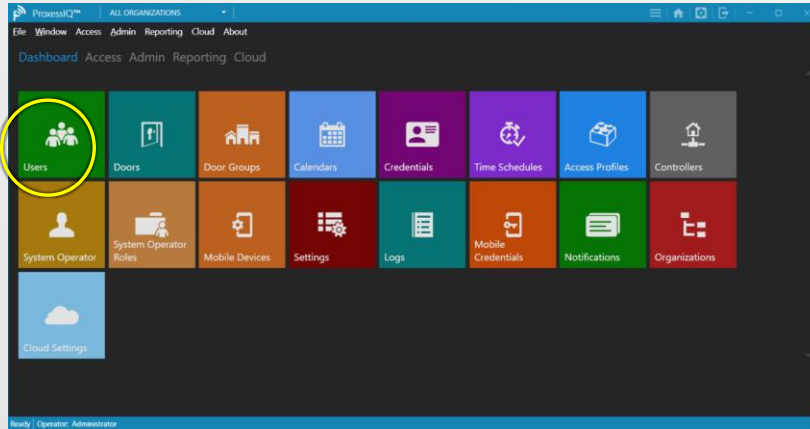# USERS

Encoding & Wiping Cards/Fobs/Wristbands/Stickers

with the **ProxessIQ™ Software**

Encoding Physical Credentials using the ProxessIQ™ Software
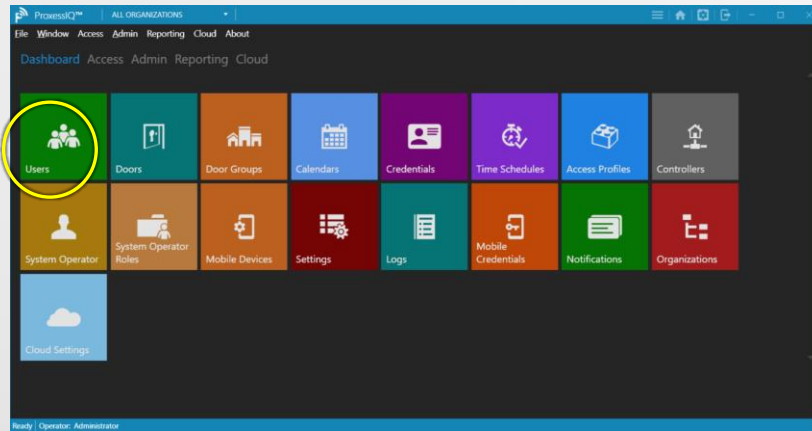
A credential (card, keyfob, sticker, watchband) must first be created in the software and then it can be encoded with the software, by plugging a n Enrollment Reader (ENR) into a USB port (USB 3.0 is optimal) the local PC that the client software is installed on. Note that the enrollment reader will not work on a virtual client.

Go to the Users menu.
Add a User and then add a Credential (as shown in a prior section).
Assign the rights to be assigned to that credential and click "Save".
The "Write to Card" button will become illuminated, enabling the encoding process.
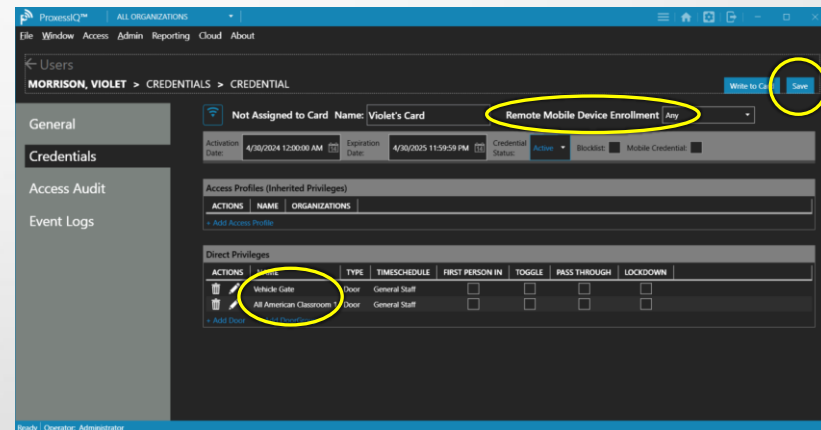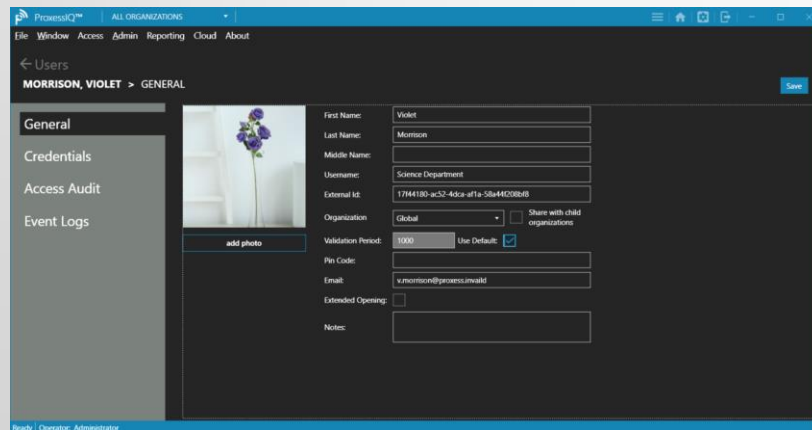
NOTES for SUCCESSFUL CREDENTIAL ENCODING, READING & DELETING

- Ensure the enrollment reader (ENR) is connected to a USB 3.0 (preferably) port on the administrator computer.
- Always keep credentials 6" away from the ENR until you are ready to place one on the ENR (the ENR will try to read credentials that are close).
- Then, immediately place and hold the credential on the ENR until the read or encode or wipe (delete) sequence is complete. Waiting to place a credential will result in a time-out error on the software.
- Then, immediately remove the credential from the ENR.
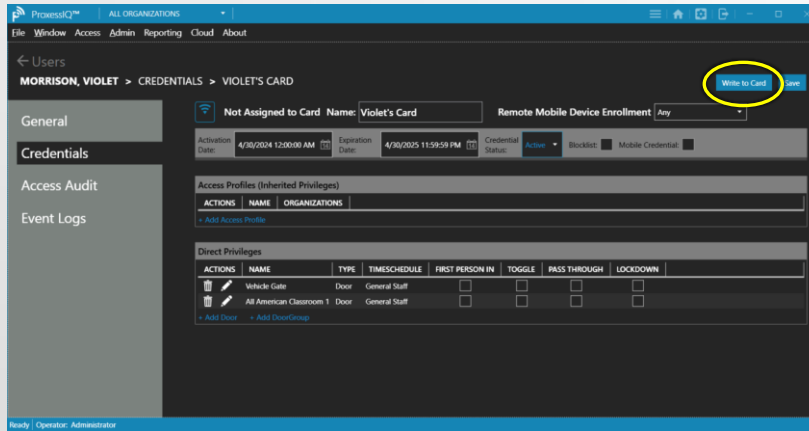
- If you are certain the credential (card/keyfob/sticker/watch) to encode has not already been encoded, then click on "Write to Card"
- Immediately place and hold the credential on the ENR until the blue LED appears and the screen to the right appears
- This shows the credential has been encoded with the rights shown and to card number shown.
- Remove the card from the ENR.
- You may now use the card on all of the doors that it has programmed for, during the allowed days and times.
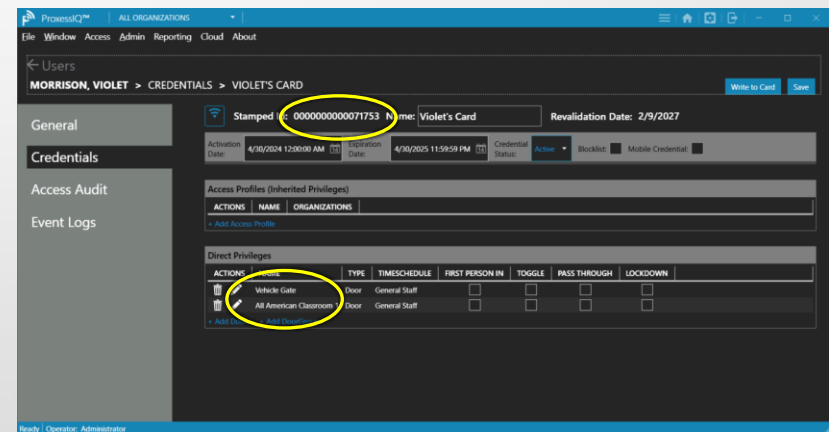
Verifying and Deleting (Wipe) a Credential
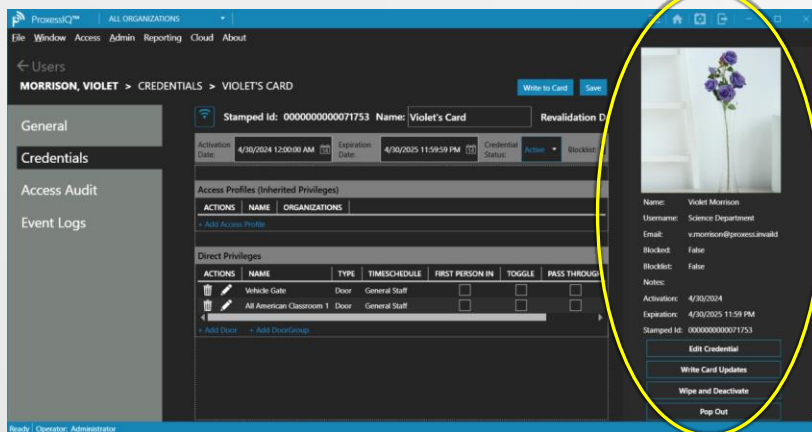
To Wipe/Delete a credential, or if you are uncertain if the credential (card/keyfob/sticker/watch) to encode has already been encoded:

- Place and hold the credential on the ENR until the blue LED appears and the above pop-up window appears.
- Remove the card from the ENR.
- In this case, this card has been encoded with Violet's rights.
- Click "Wipe and Deactivate"
- Immediately place the card on the ENR until it Beeps and the LED turns green.
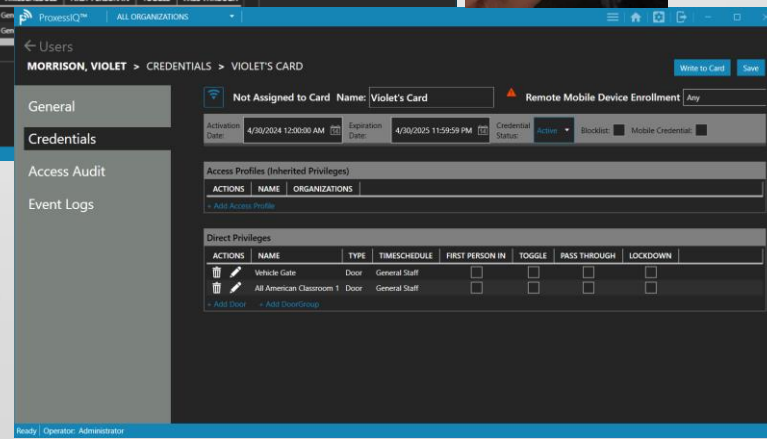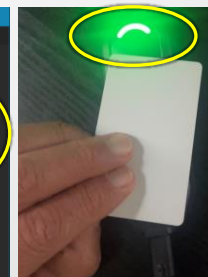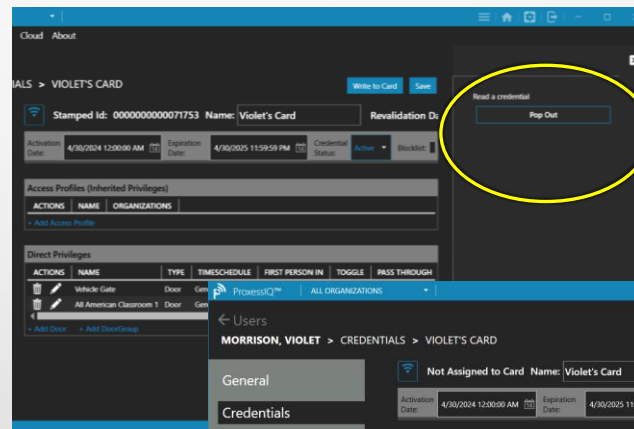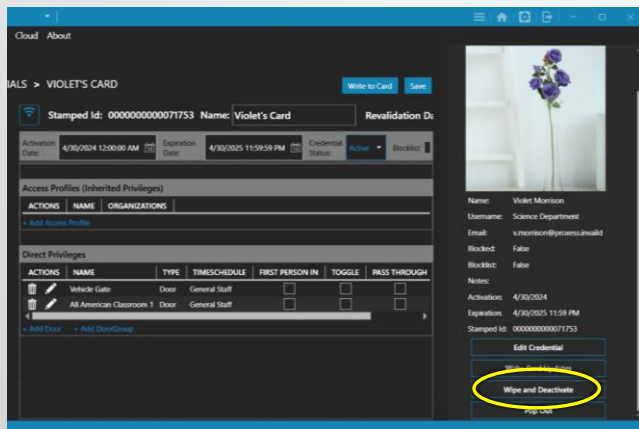
Verifying and Deleting (Wipe) a Credential
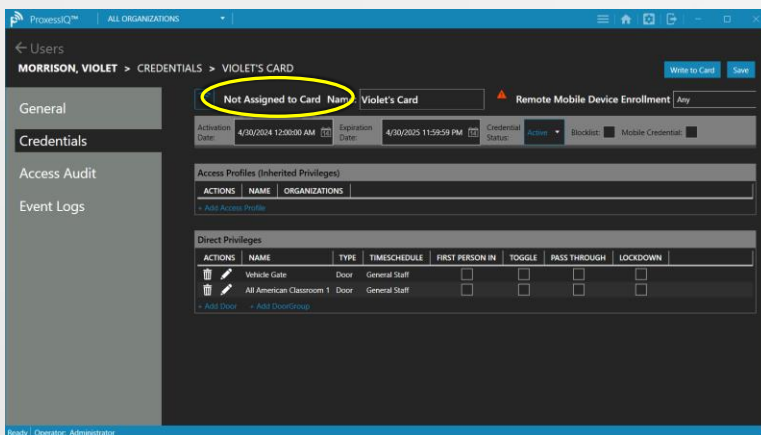
When the screen is next refreshed, it will note that this user is "Not Assigned to Card".

Better Practice to Delete (Wipe) Rights from a Credential
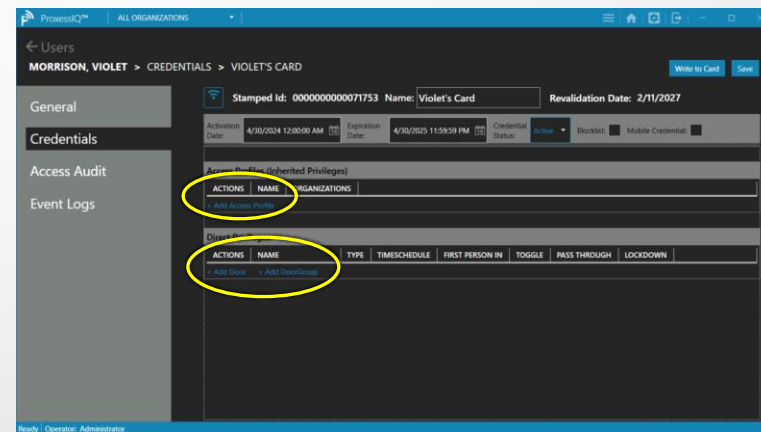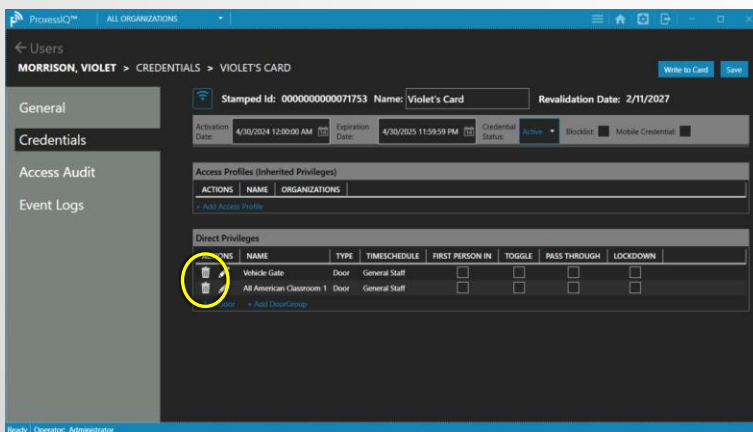
It is always better to first delete the rights for a credential, by clicking on the Trash Can icons, leaving the credential with no rights.
If the card is ever presented at an online reader, it will automatically be updated to have No door entry rights and will not be allowed into the door.

Note: If further action is desired, it is best Not to just delete a credential....**First**, Wipe the credential on an enrollment reader, or delete its Privileges/rights and have it presented to an online controller's reader, which will have its rights wiped.
Note: It is also a best practice to have each card's Validation be configured to as few days as possible, ensuring that even if a rouge credential is presented to an offline lock, it will be rejected.
Note: If there no online doors, then check the Blocklist box for the credential and the Proxess Sync app must be presented to each offline lock that they had the rights to.

Can I Encode this Random Card & Assign it to Someone?
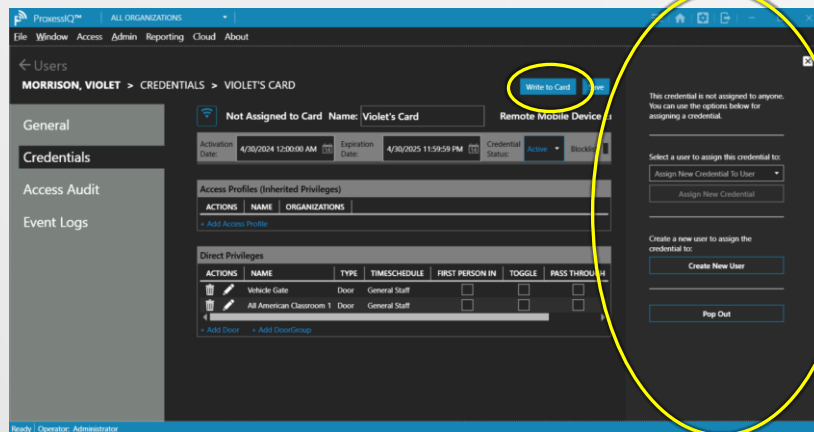
- If you are uncertain if the credential (card/keyfob/sticker/watch) to encode has already been encoded, then first place and hold the credential on the ENR until the blue LED appears and the above pop-up window appears.
- Remove the card from the ENR.
- In this case, this card is not assigned to anyone
- You may now click "Write to Card" and place the card on the enrollment reader to encode it, resulting in the below screen, showing its success.
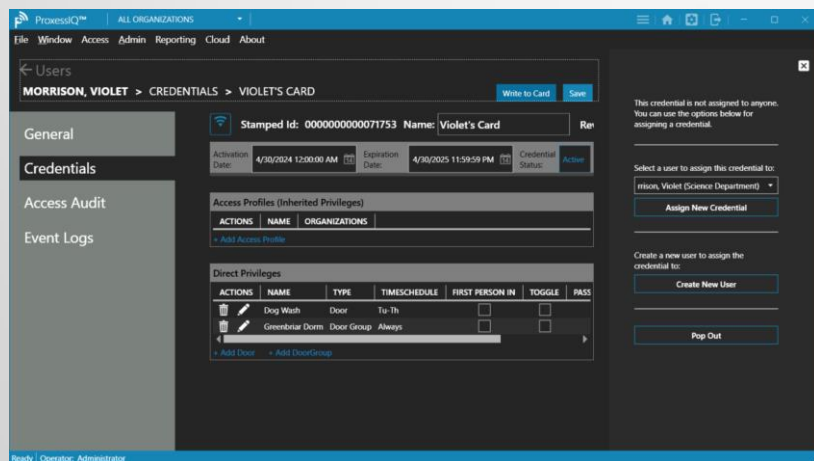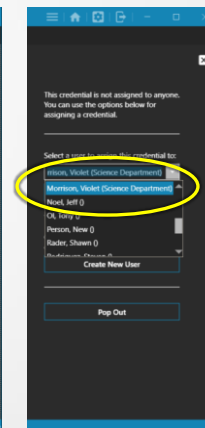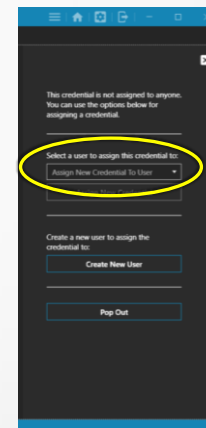
Another way to Encode a Card

You may choose to first enter Users in the system and then select an un-encoded Credential to encode under that User, Remember that a User is typically a person and a several Credentials can be assigned to each User.
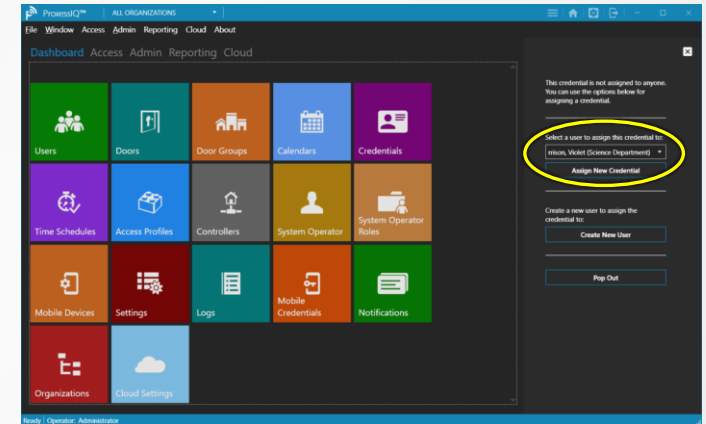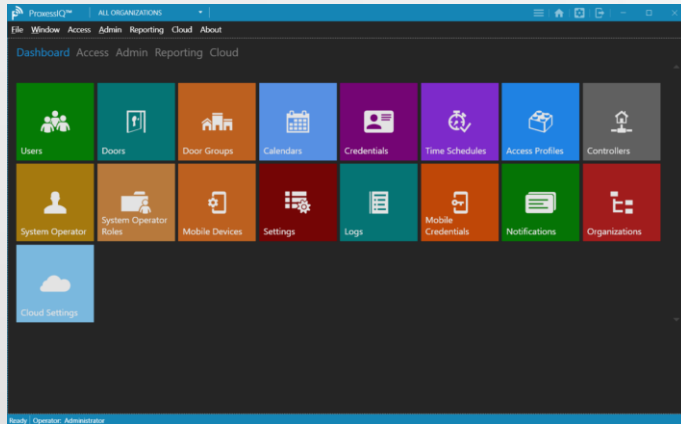
From any screen in the system, take an unencoded card and place it on to the ENR. The light will turn blue and the pop-up window will appear.

Select a User's name that you have already entered into the system and click "Assign New Credential".
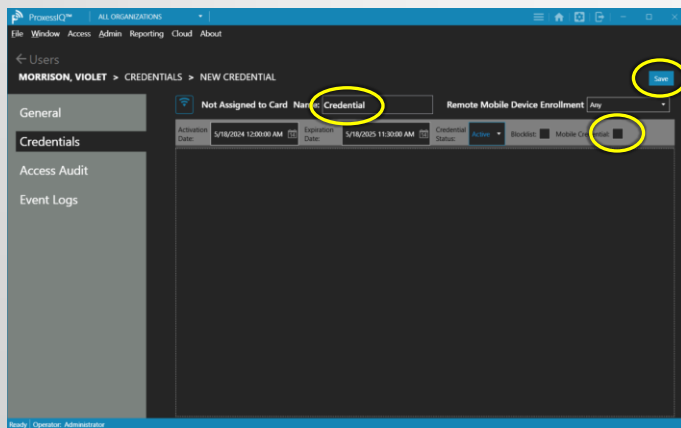
The Add New Credential window opens. Optionally add a Name for it, in this case check the "Mobile Credential" box and click "Save".
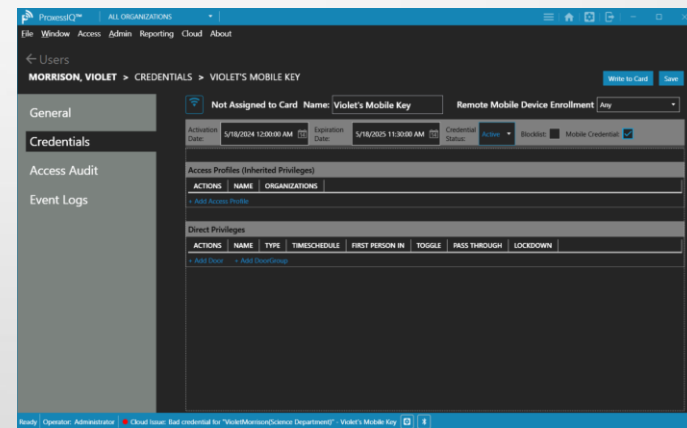
Enter the information for their new credential (a mobile phone key in this case) and add their access rights as described in previous sections.
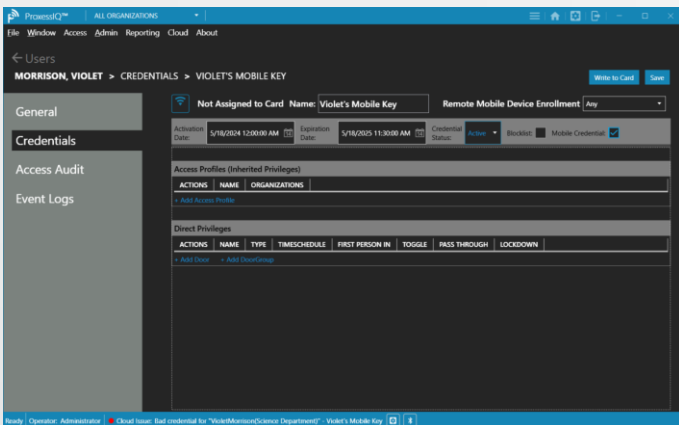
Enter the information for their new credential (a mobile phone key in this case) and add their access rights as described in previous sections.
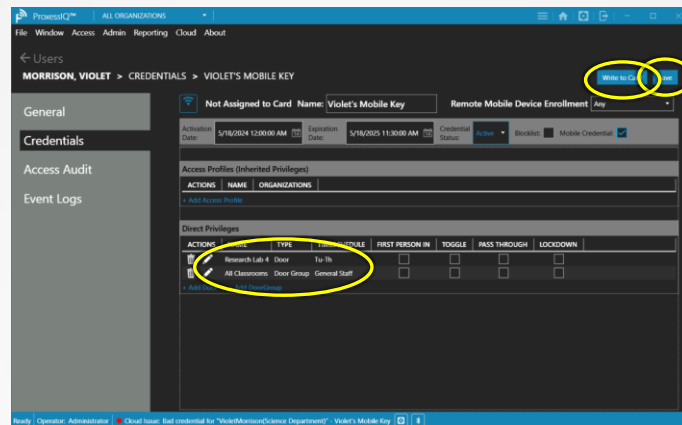
Select their Door and Door Group Privileges. Remember to keep all credentials away from the ENR until this point. Now click "Save" and then click "Write to Card".
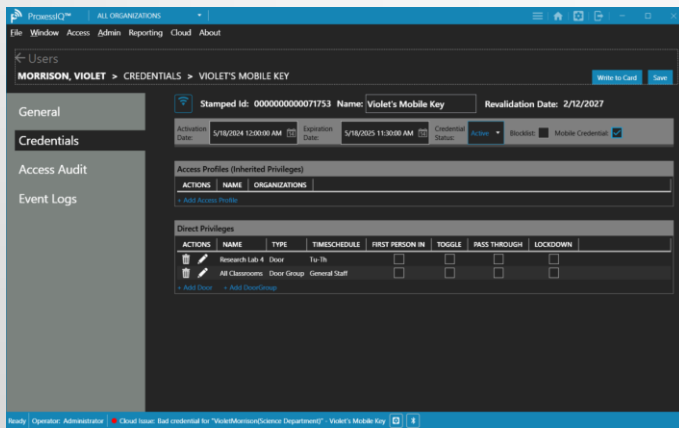
Promptly place and hold a credential on the ENR (enrollment reader) until it beeps and it will have been encoded.

Pop-Out Window: Another way to Encode a Card
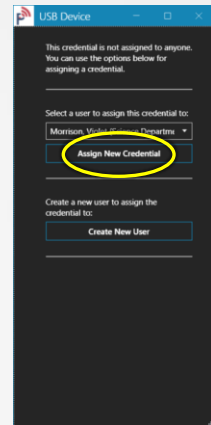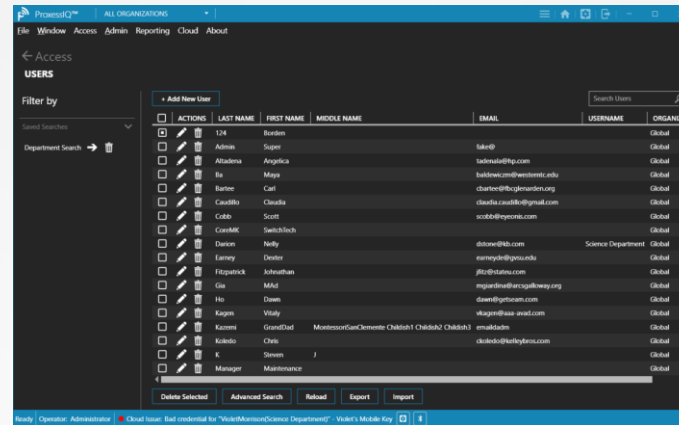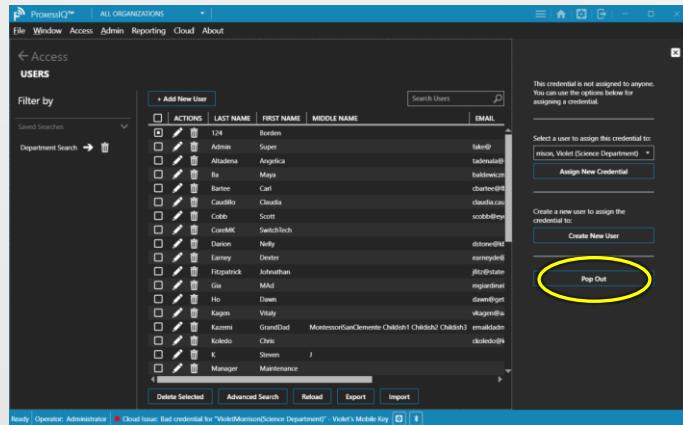
Using the Pop-out window is an easy way to enroll/encode multiple credentials, after their User names have been added.
From any screen, place an unencoded/blank credential on the ENR (enrollment reader) and then click "Pop Out".
You will now have a separate window for encoding credentials. Click "Assign New Credential" and select the User from the drop-down list.
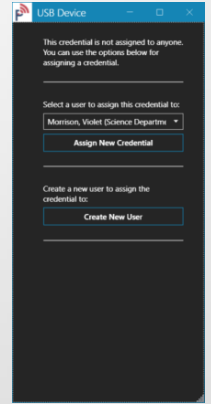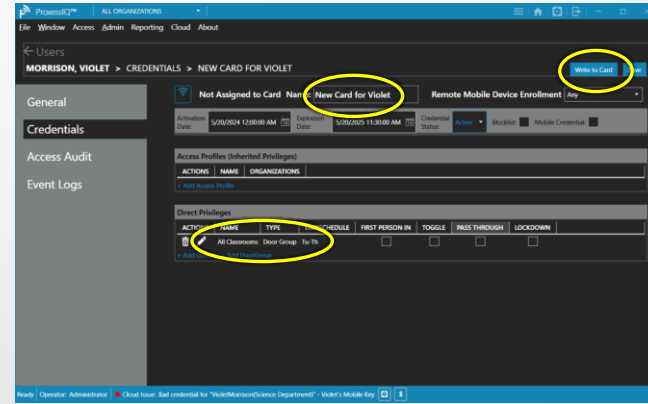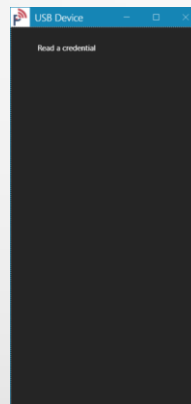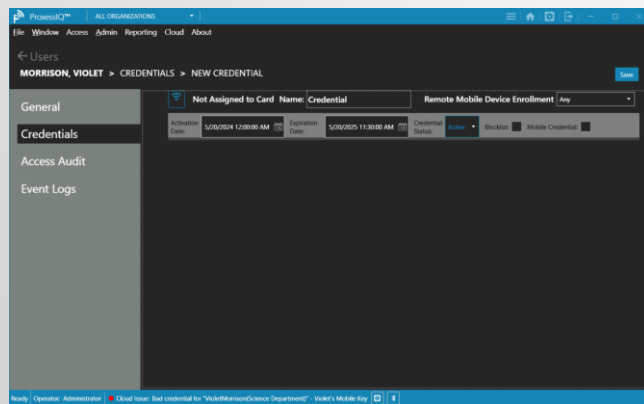
A New Credential window for the selected User will open.

Create a name for and add access rights for the credential, click "Save" and the click "Write to Card" and the card information will display.

Place the next blank/ unencoded credential on the ENR and repeat the process..

USERS

Encoding & Wiping Cards/Fobs/ Wristbands/Stickers

with the **ProxessSync app**

Encoding Physical Credentials using the Proxess Sync app

Any card that has been created in the software can be encoded in the field by any allowed Mobile Device (see this section in this manual) with the Proxess Sync app.

Go to the Users menu.
Add a User and then add a Credential (as shown in a prior section).
Assign the rights to be assigned to that credential.
Select a Mobile Device (or All of them) that will be allowed to create or edit this card.
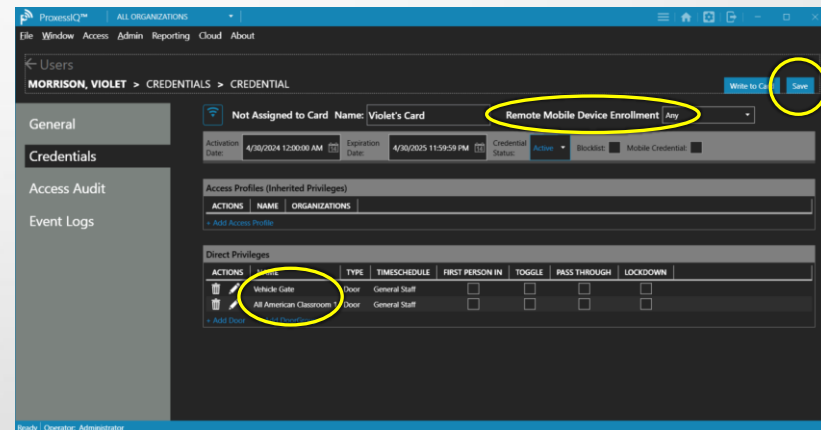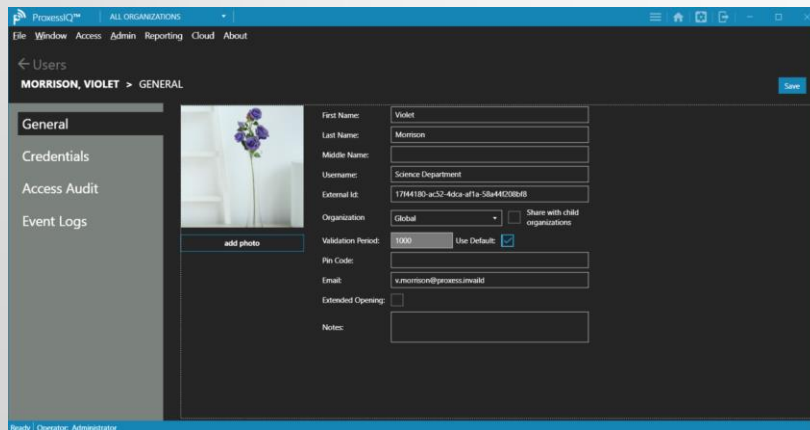
Encoding Physical Credentials using the Proxess Sync app

Open the Proxess Sync app on your phone
Plug an Enrollment Reader (ENR) into a power source: A wall plug, a USB (A or C) port of a PC, or your phone or tablet (Android and iPhone 15 and above)

Tap the Menu ("Hamburger") icon.
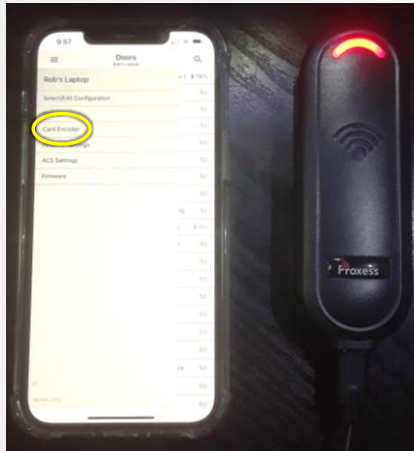
Tap "Card Encoder" and make sure the Enrollment Reader (ENR) is within 12" for the initial connection. The screen will state that it is looking for the ENR. Once connected, the ENR can be up to 20' away.
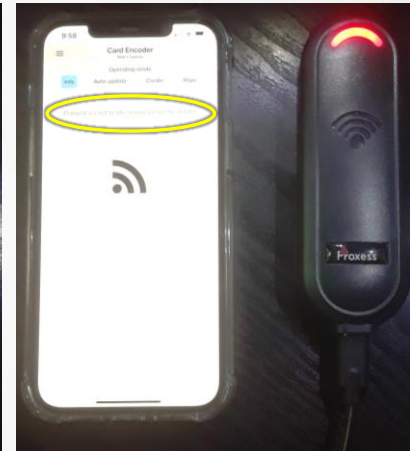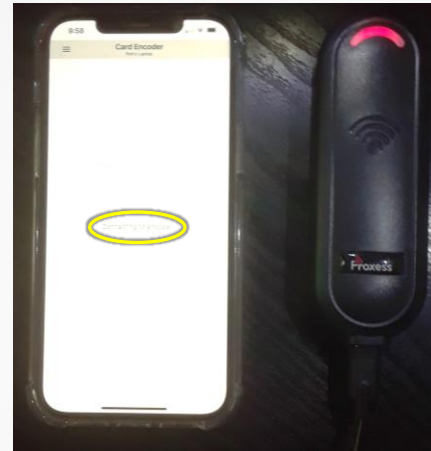
Once bound to an ENR, the screen will state it is ready for a credential to be presented.
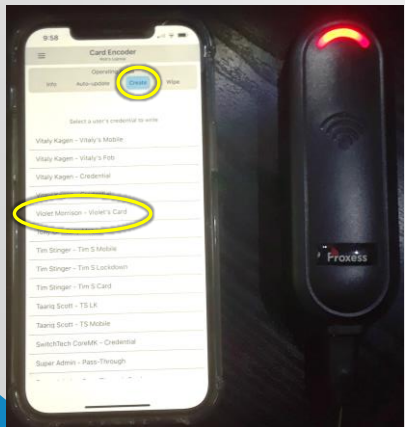
Tap the "Create" button and a list of all Credentials that this operator is allowed to encode is presented. Tap on the name whose credential you will encode and you will be prompted to place the credential on the ENR.
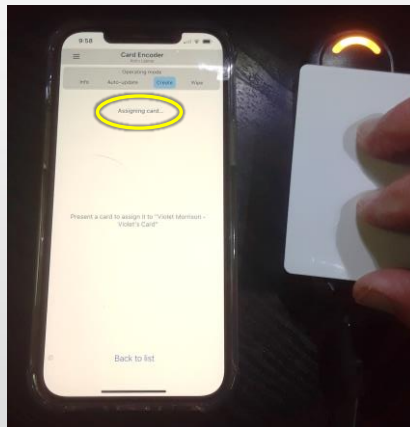
Place the card on the face of the ENR for the entire enrolment process, until the LED turns green.
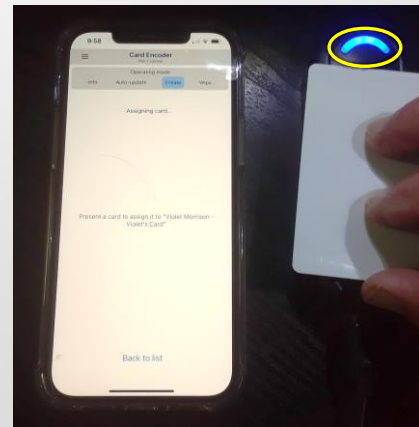
The blue LED shows the card is being encoded to that User's Credential. Please Remove the card from the ENR.

Verifying & Wiping Physical Credentials using the Proxess Sync app

To Verify a credential or to see who a credential belongs to, Click on the "Info" button. Then place a card onto the reader surface. The blue LED shows the card is being read and/or written to.
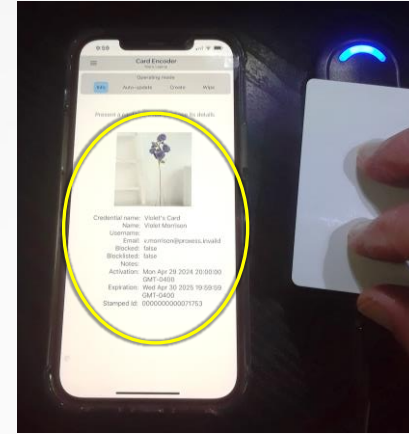
The credential information, including any stored photo of the User, will appear. Please Remove the credential from the reader.

To Wipe & Delete a credential, Click on the "Wipe" button. Then place a card onto the reader surface. The blue LED shows the card is being read and/or written to.

The screen will state that the credential has been successfully wiped. Please Remove the credential from the reader.

CALENDARS
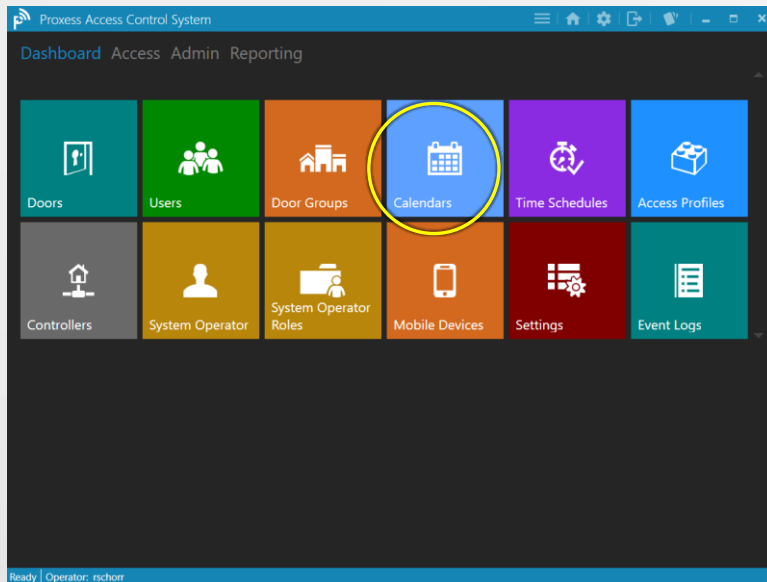
Click the icon for the "Calendars" module. Calendars are where you add traditional Holidays and other specialty days. Specialty days can be planned in advance (e.g. weddings at a church, sports games at a school) , or added on-demand (e.g. weather related event).
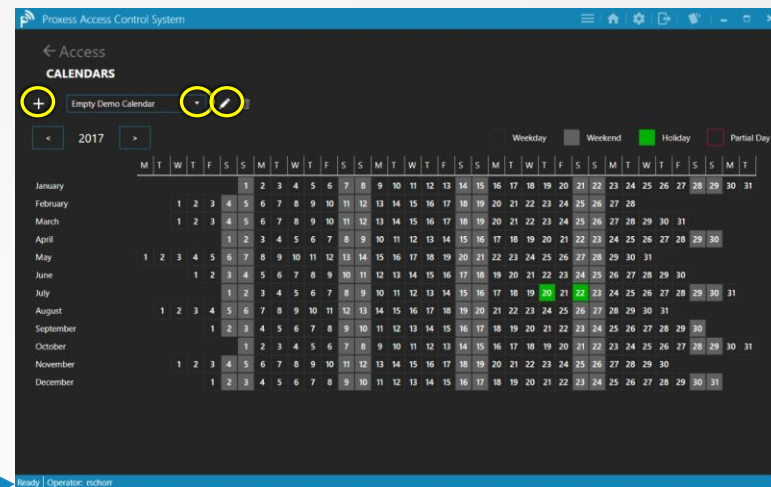
The Default calendar will appear, if this is a new system. Since a customer may have multiple locations, with each location abiding by different calendars, you may create multiple Calendars and apply a different Calendar to each lockset and door. Click the dropdown arrow to select a Calendar to view and the edit icon to do so. At this time click "+" to create a new Calendar.
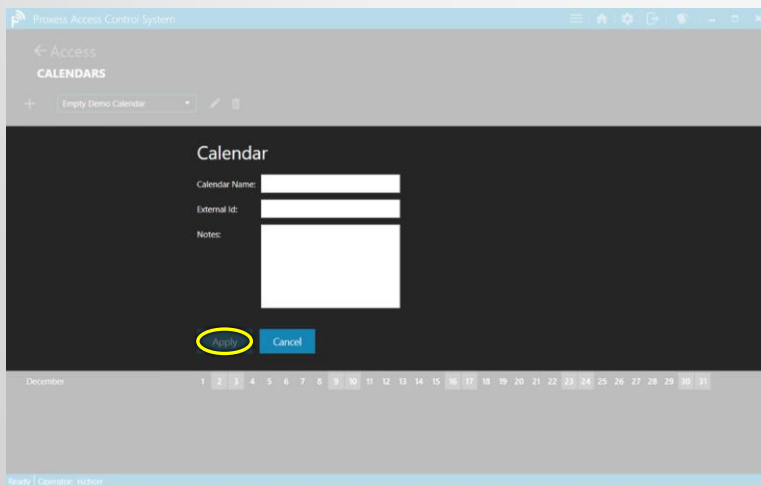
Enter the name for the new Calendar. This is the name that will appear in all the Doors selection screens. The External ID is optional and is an alternate reference that the customer may have. Enter any further notes you may have. Click "Apply" to continue.
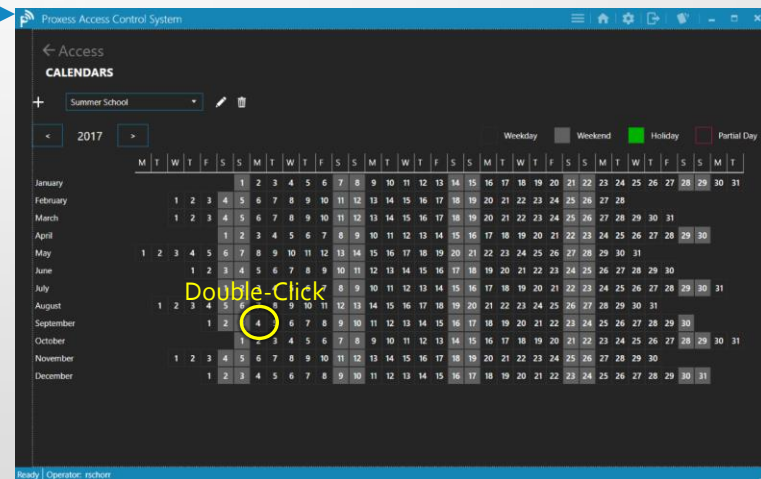
The Calendar you just created appears. To begin adding days for a Door to operate\function differently than normal\programmed, click on any day for the current year that is displayed (2017 in this case). To add a Calendar Event, Double-click on any day.

Calendars - 1

The page to create a new Calendar Event appears. Enter the Event Name you want along with any optional clarification Notes. Select the Start and End days and times for this special Door operation to occur and click "Apply" to save this new event.

The new Holiday\Event now appears, highlighted in green. Note that a Holiday is the most common type of Event and is therefore the term used in the software and the two words are equal to this program. To view the detail of this Holiday\Event click on the green highlighted date.

The Holiday\Event detail appears at the bottom of the Calendar. To edit the Event, Double-click on the green highlighted date.

You can now make adjustments to the Holiday, or click "Cancel" to return to the previous screen and then click the Home icon on the top taskbar to return to the Home Screen \ Dashboard.

USER INTERFACE FLEXIBILITY
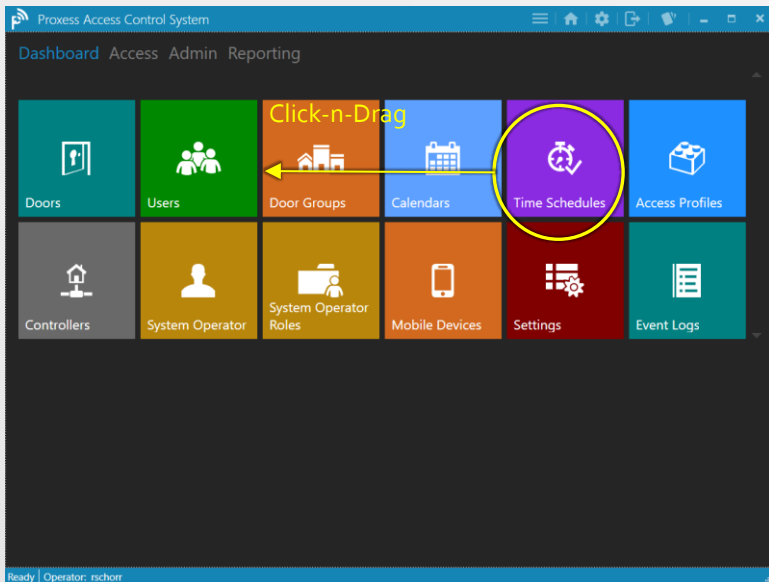
The Dashboard \ Home Screen \ User Interface may be customized in several ways. First, you may click-and-drag any module to another part of the screen, thus rearranging the module icons.

By clicking on the icon highlighted on the top taskbar…

…The file shortcut menu will appear and remain at the top of the page throughout the system, until you again click on the same icon on the top taskbar.
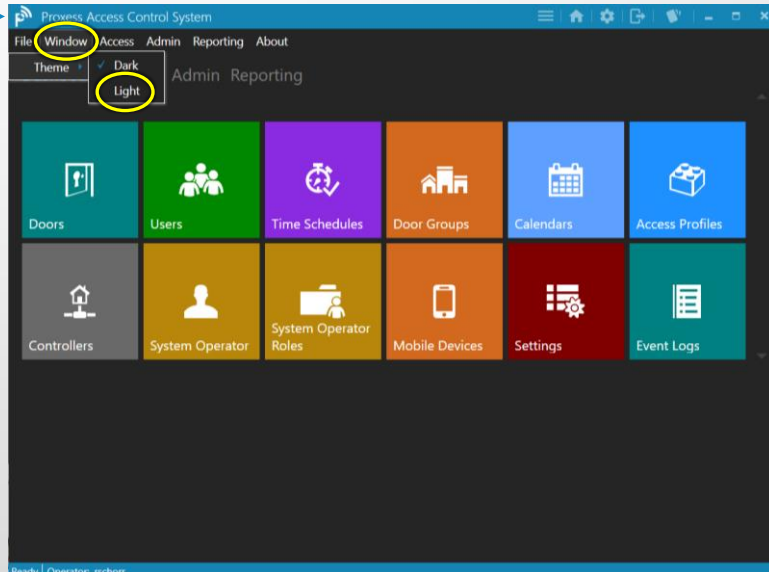
Click on the "Window" button, highlight "Theme" and then click on "Light".

ProxessIQ™

Dashboard Access Admin Reporting Cloud

Cntrl+Shift+D	Cntrl+Shift+G	Cntrl+Shift+U	Cntrl+Shift+A	Cntrl+Shift+T	Cntrl+Shift+R	Cntrl+Shift+E	Cntrl+Shift+O
Doors	Door Groups	Users	Access Profiles	Time Schedules	System Operator Roles	Audits/Events	System Operator
Calendars	Controllers	Settings	Mobile Devices	Credentials	Mobile Credentials	Notifications	Cloud Settings
Cntrl+Shift+Y	Cntrl+Shift+B	Cntrl+Shift+S	Cntrl+Shift+M	Cntrl+Shift+C	Cntrl+Shift+I	Cntrl+Shift+N	Cntrl+Shift+G

Ready   Operator: Administrator

From anywhere within the ProxessIQ program, the above Hot-Key shortcuts may be used to jump into that menu.

User Interface Flexibility - 3
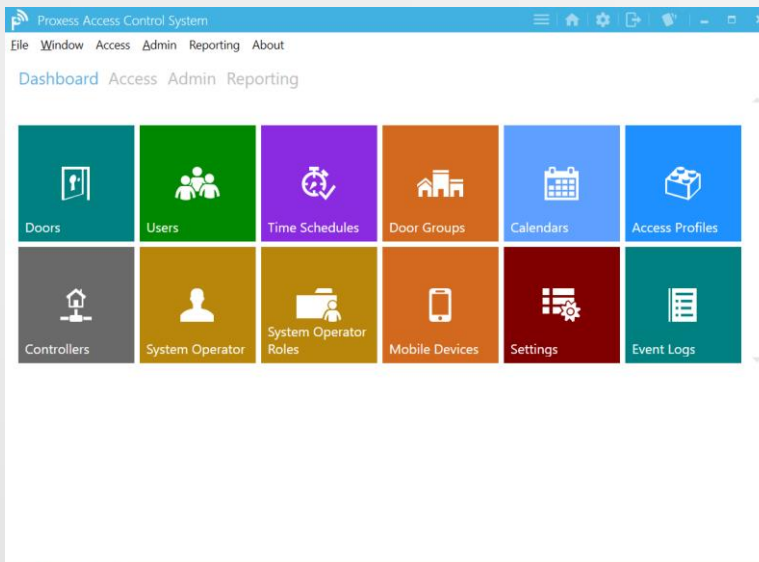
The screen background is now changed to white and will remain so throughout the system until the background is changed back to "Dark".
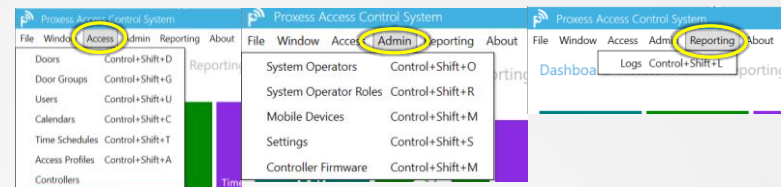
As an alternate to using the module icons on the Dashboard, the file shortcut menu can be used to quickly navigate from and to any other module with a single click.
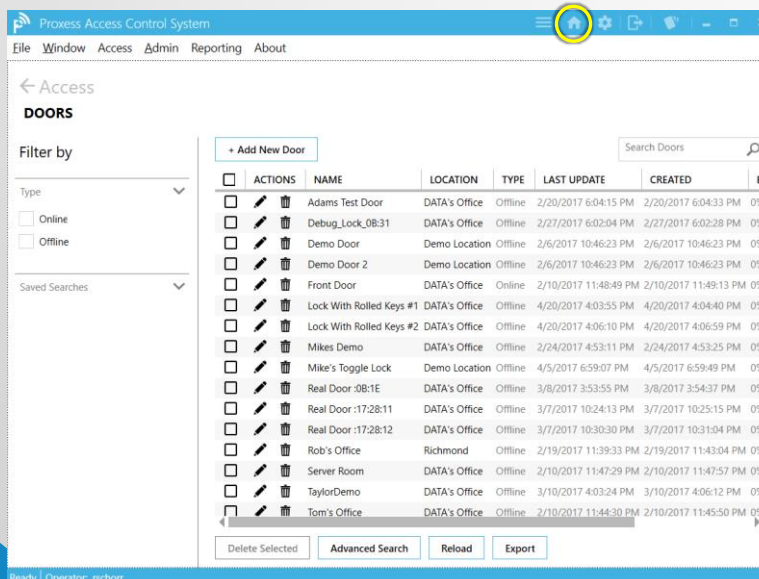
The Home icon is used from any screen in the system to bring you back to the Dashboard \ Home Screen.
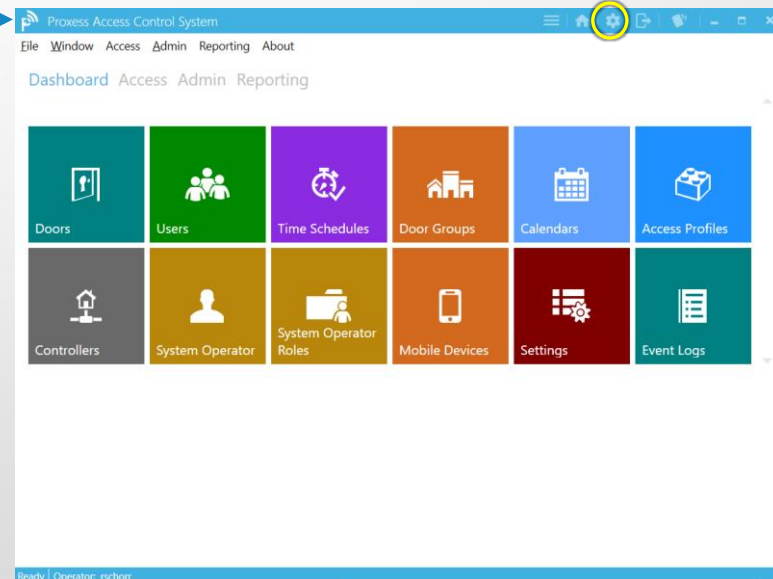
From any screen in the system, you can shortcut to the "Settings" module with a click on the icon shown in the top taskbar.
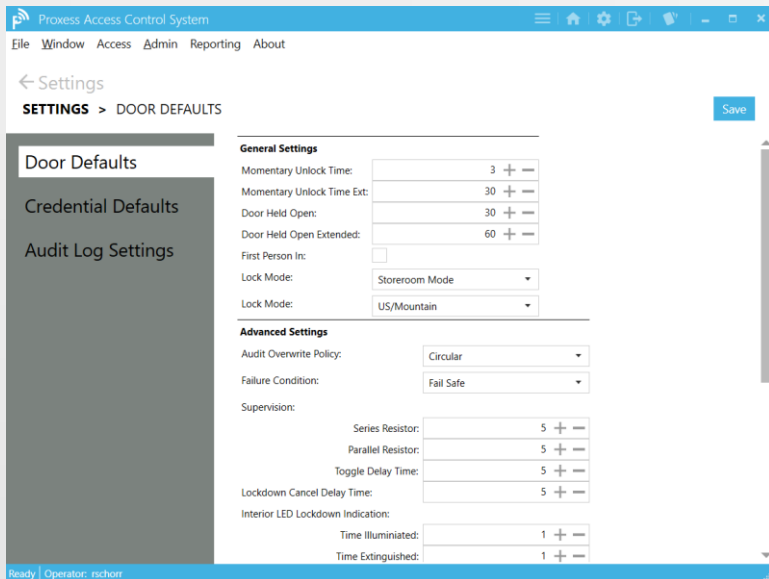
The "Settings" module opens. Now return to the Home Screen \ Dashboard.
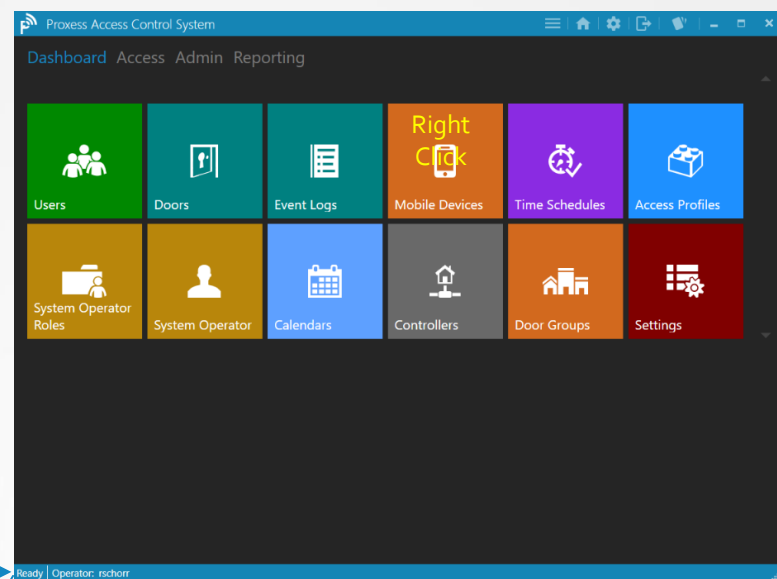
Right-click on a module icon.
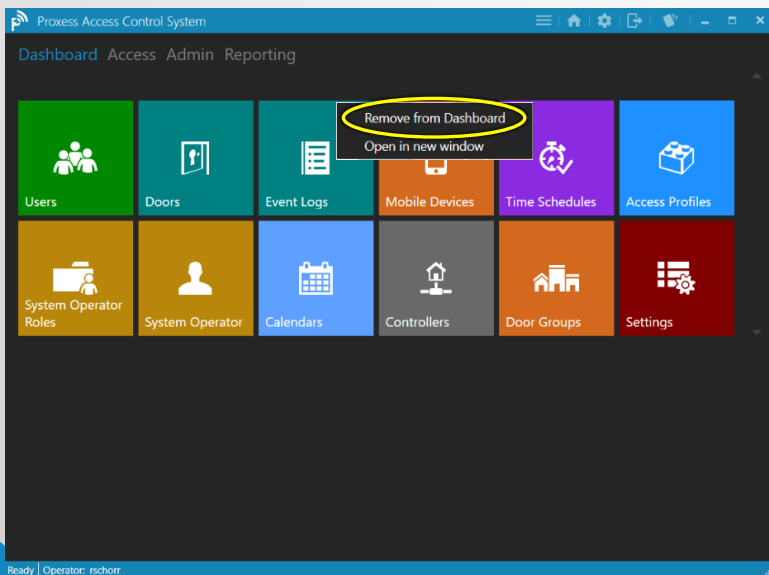
You may "Remove" the icon from the Dashboard or open it in a new window (Is this working right?).
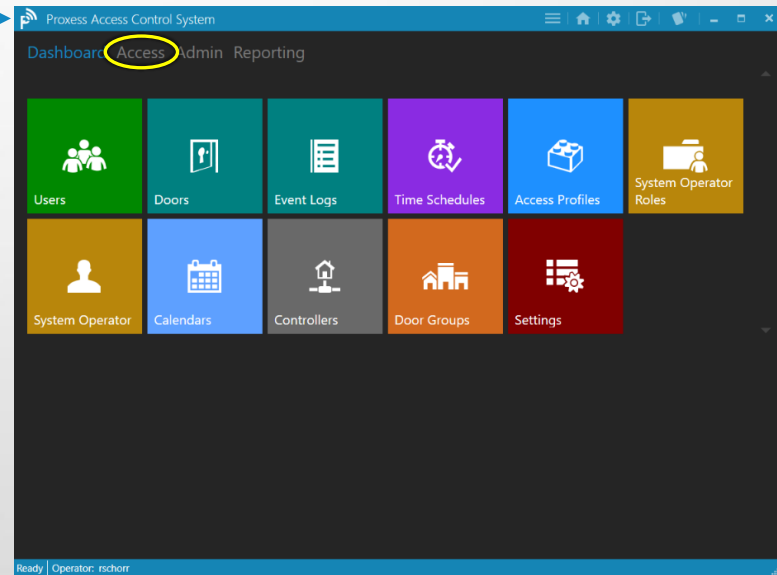
Click on "Access" in the top menu.
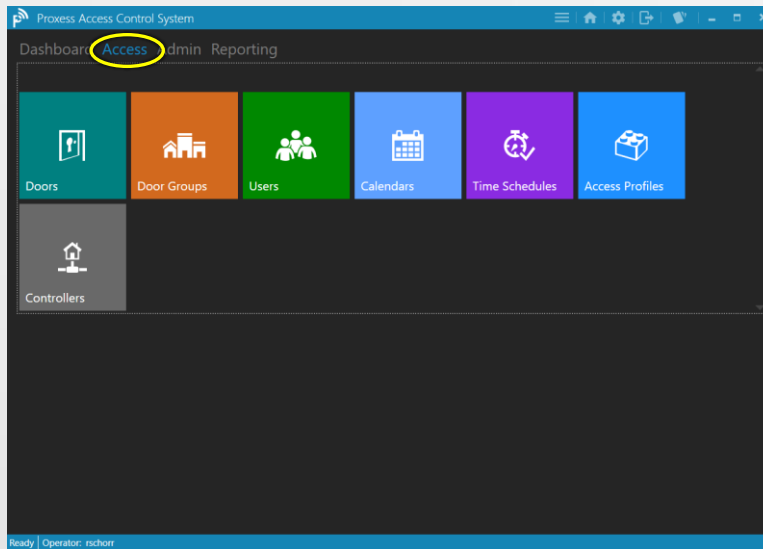
These are the module icons that appear when you click on "Access".
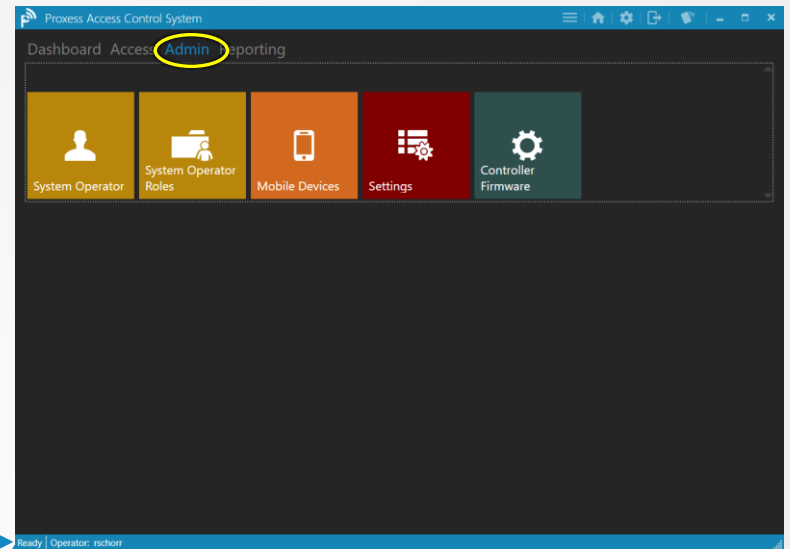
These are the module icons that appear when you click on "Admin".
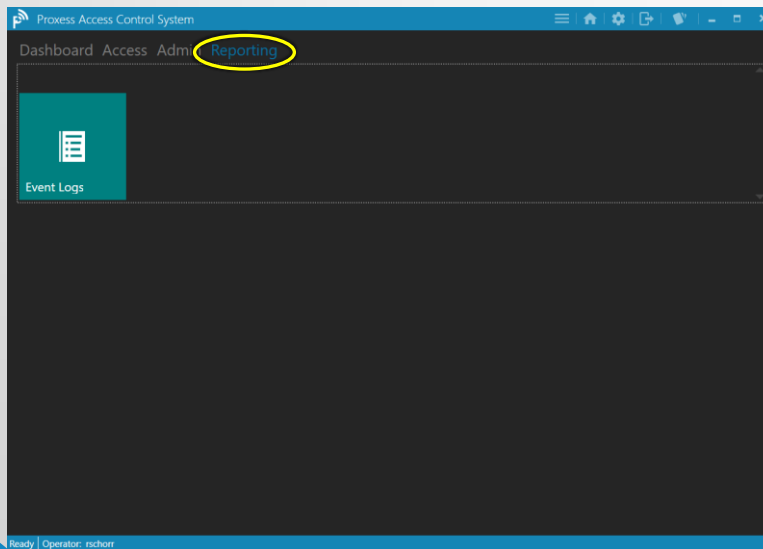
These are the module icons that appear when you click on "Reporting".
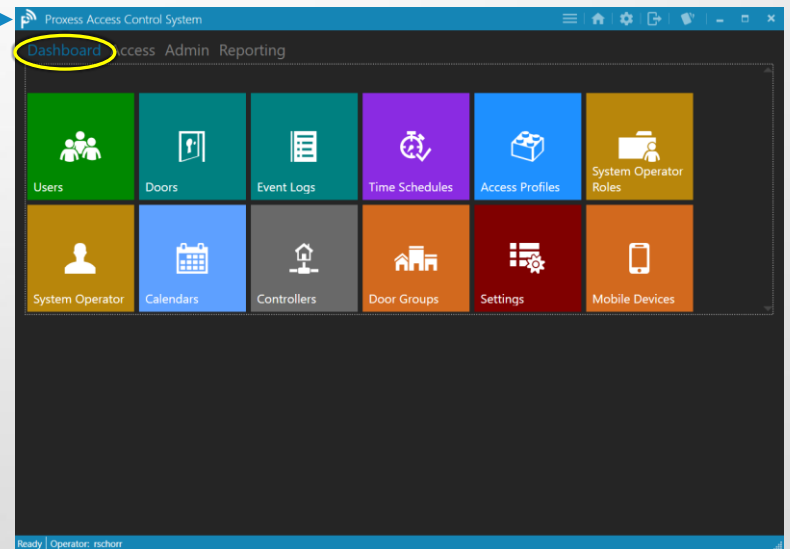
These are the module icons that appear when you click on "Dashboard".
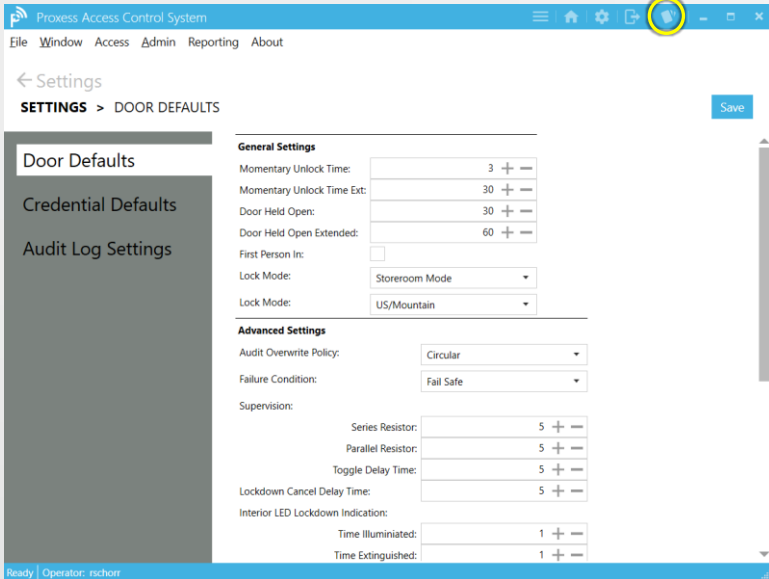
From any screen in the system, click on the icon shown in the top taskbar
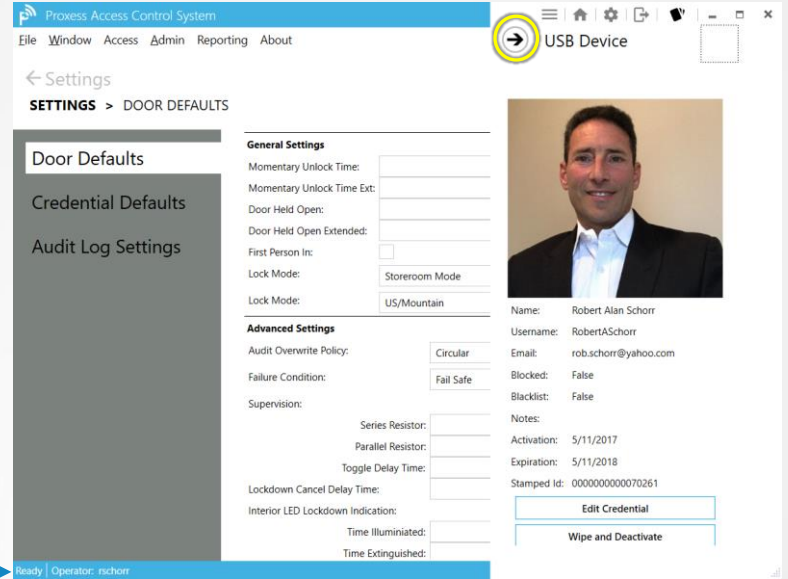
The most recent credential that was placed on the enrollment reader will pop-up.

USING the
ENROLLMENT READER within
ProxessIQ™

Go to any screen in the software
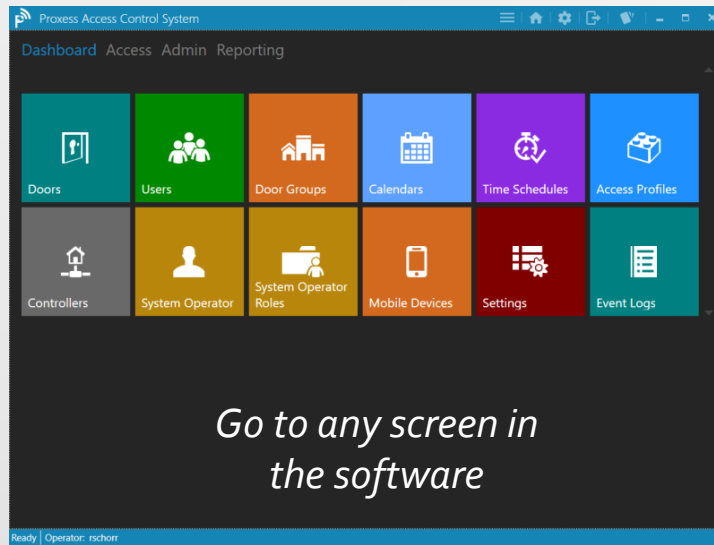
Place a new card on the enrollment reader

This pop-up window appears
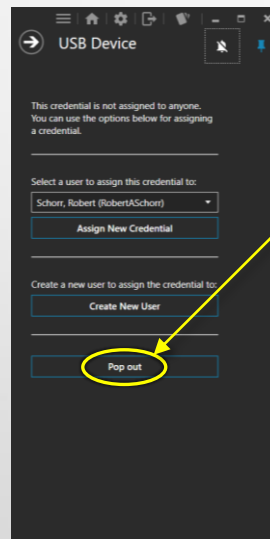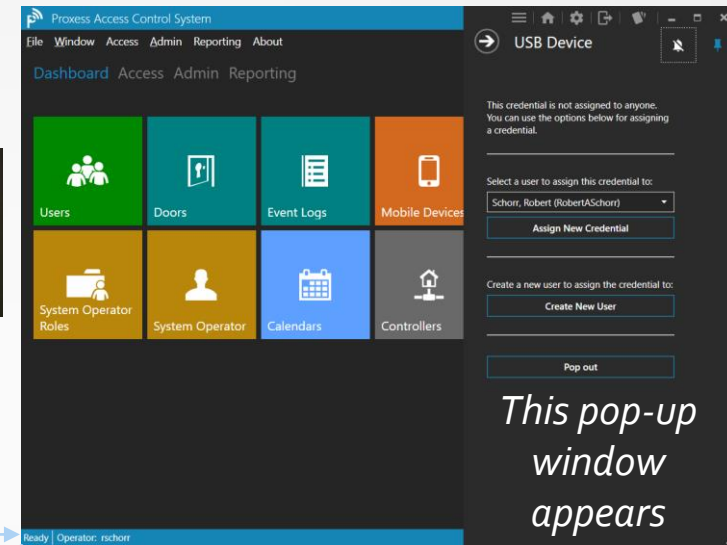
The pop-up window presents several options for the operator.

The operator may click the "Pop out" button, which will undock this window from the main ProxessIQ™ application. It may then be dragged anywhere on the desktop, so that the user can continue programming other screens in the ProxessIQ™ system and return their focus to the new card when they are ready.

At that time, the operator may leave the card on the enrollment reader and proceed with the process of creating or assigning this card.

Assign a Credential to an Existing User
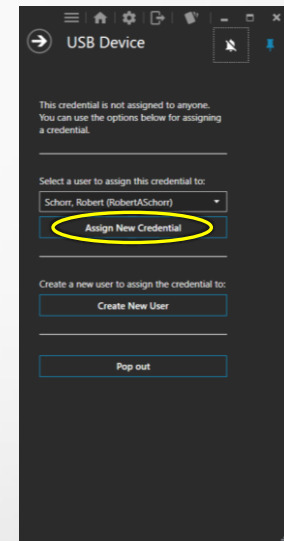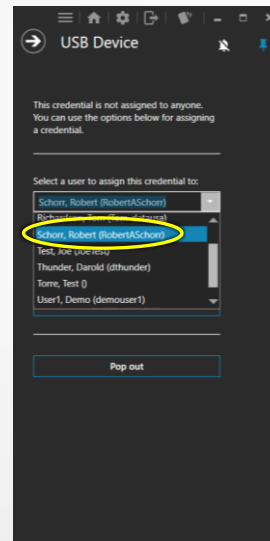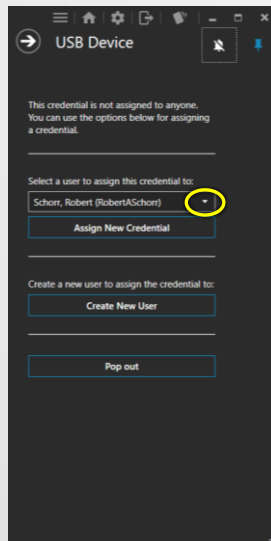
The Operator may assign the credential that is currently on the enrollment reader to an Existing User.

First, click on the drop-down arrow and then select an existing user\cardholder from the list. You may scroll down the list using the scroll bar, or begin typing letters of their name which will bring up all the matching results as you type. Select the desired name and then click on the "Assign New Credential" button to complete the task.

NOTE: Users may have more than one credential. The user selected may have only their information entered and this may have been the first credential assigned to them, or they may already have another credential.

Adding a New User
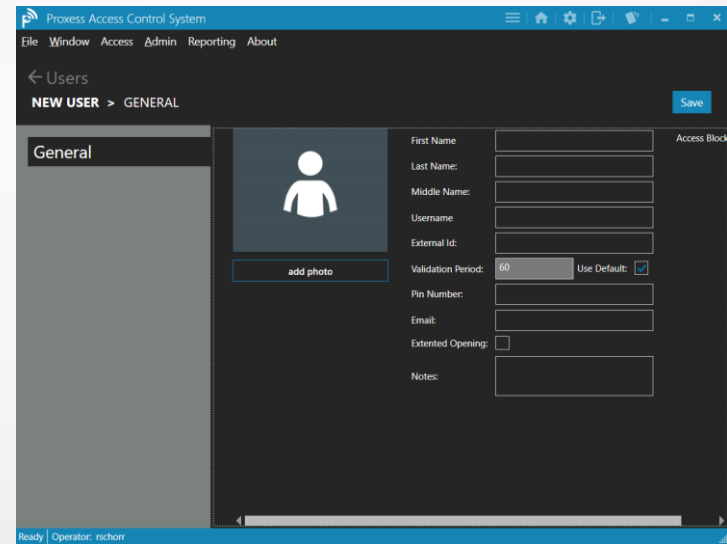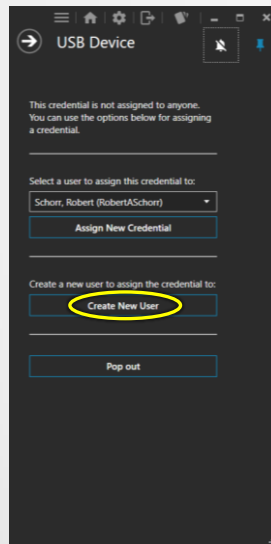
With the card on the enrollment reader, the Operator may create a New User record for it.

Click on the "Create New User" button and the new user information screen will open. We will cover the remainder of this process in the next section.

Whose card is this?
&
Deleting a Credential
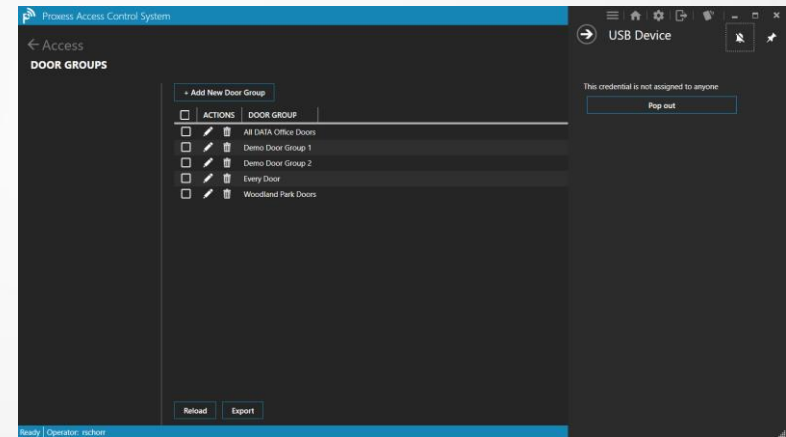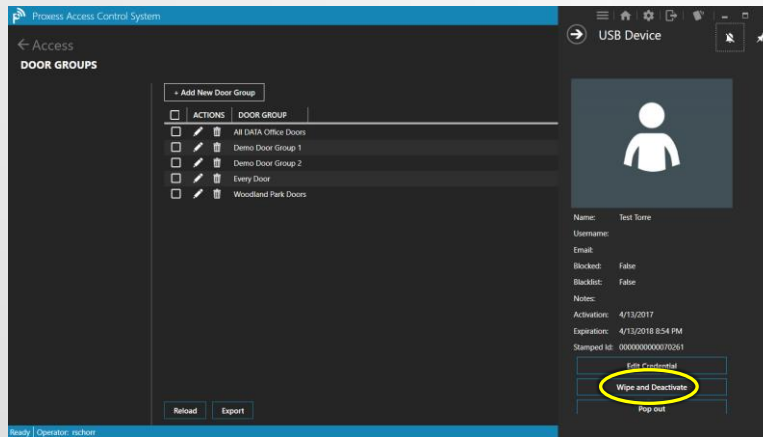
To find out who a card belongs\has already been assigned, place it on the enrollment reader while in any screen in the software.

The pop-up window appears along with their basic cardholder and card information which includes their stored photo. Three (3) button choices are also presented.

The operator may click "Edit Credential" to be brought to the edit screen for that user and may click "Pop out" to move the window freely on their desktop.

The operator may also decide to assign this credential to a new user or simply wipe the existing information off the card. To do so, click "Wipe and Deactivate".

The screen on the right will appear and the card is now free to be assigned to anyone.

Attempting to Enroll an Existing Card
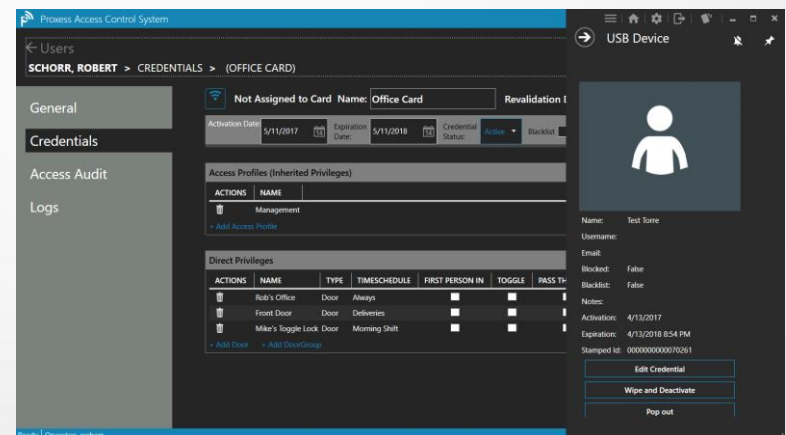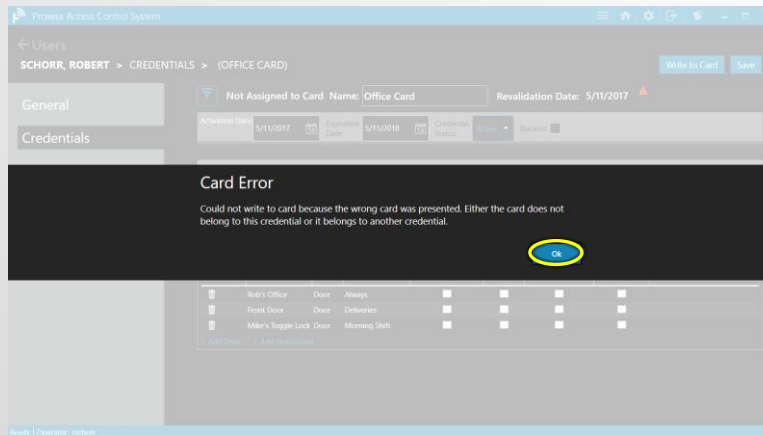
After a user has been added to the system, placing a credential on the enrollment reader and attempting to enroll or encode one that has already been programmed and assigned to someone else (from this system or any other system) will result in the above "Card Error" screen appearing.
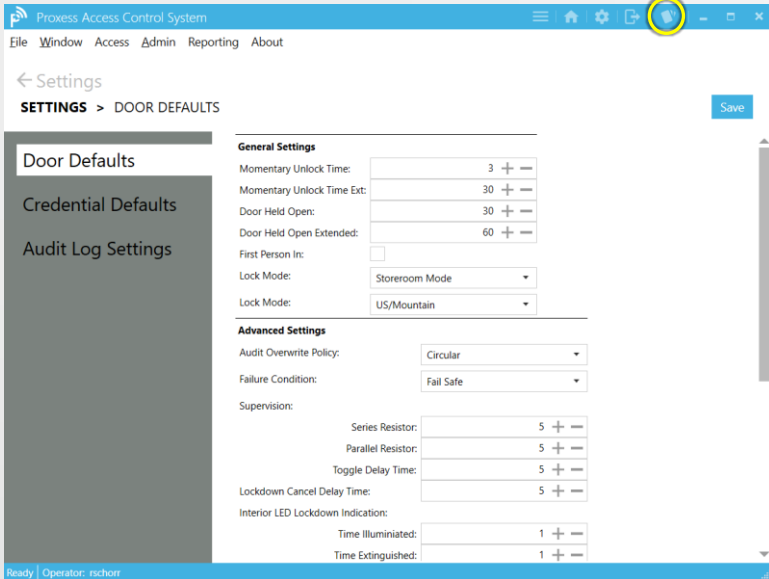
From any screen in the system, click on the icon shown in the top taskbar
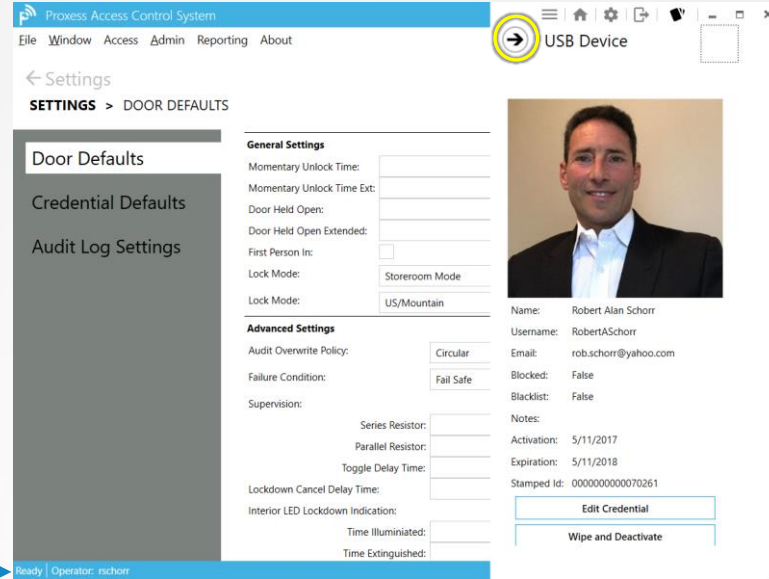
The most recent credential that was placed on the enrollment reader will pop-up.

CREDENTIALS
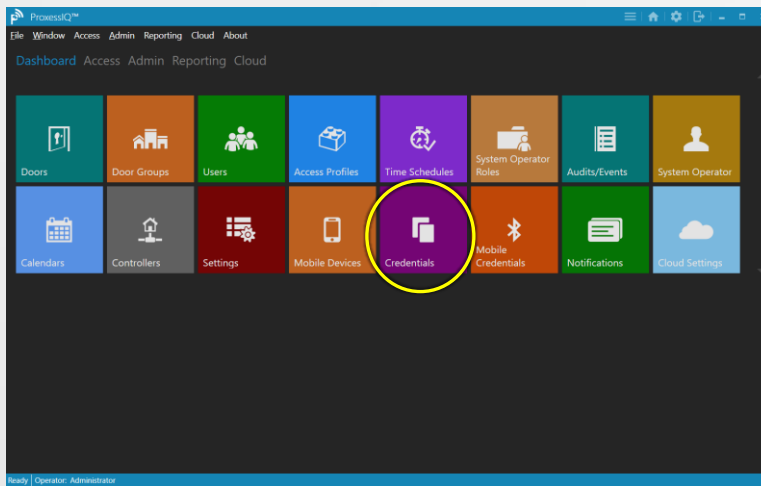
From the Home screen \ Dashboard, click "Credentials".
A User must first be created/entered from the Users menu.
Once a User has been created, Credentials may be created in either the Users or Credentials menus. The Credentials menu is a simpler management tool, as all of the credentials are in a single list, whereas in the Users menu, you must first navigate into a specific User's record and then exit from that User before managing another User's credential.
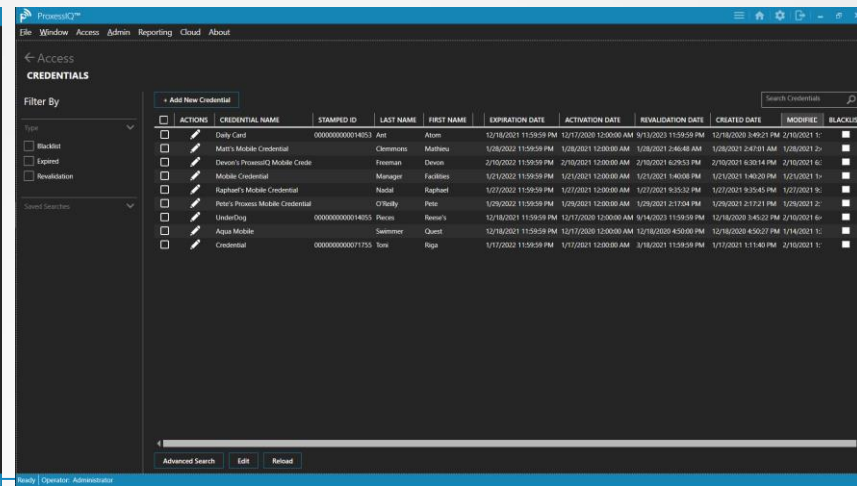
Your existing Credentials (even multiple credentials associated with a single User) will be listed.
Credentials may be edited, as previously instructed in the Users section.
Credential records may be sorted by clicking on the headers at the top of the list (Credential Name, Stamped ID, etc...).
Credentials may be Blacklisted from this menu.
New Credentials may be added , as previously instructed in the Users section.
Advanced Searches, with multiple levels using Boolean Algebra, can be created, executed and saved for future use.
Click ...

Must cancel "X" an Advanced Search, or the User menu will continue to only show those results.

Credentials - 2

Advanced Searches of Users

Within each User record

Credentials - 3

Name this search for your future use and click "OK".
Your new custom search will now appear in this list, for later execution by this and other operators.
When you have completed your Search, you must click "X" to bring you back to the full list of Users, or the User menu will continue to only show those Search results.

Advanced Searches of Users

You are now returned to the full list of Users.
You may execute on that saved search again any time, by clicking on the arrow next to its name.

You may Export the search results to a .csv for further manipulation and click the "X" and return to your normal system work.

NOTIFICATIONS
&
Upgrade to TRIGGERS & ACTIONS

The first part of this section provides instruction on creating and configuring basic system triggers and their associated actions and Notifications that can be provided.

The second part of this section instructs on the enhanced options for triggering both software and hardware-based actions and Notifications. Enhanced Notifications are a software licensed feature and are accompanied by the additional capabilities for custom defining the inputs and outputs on controllers, for use within advance Notifications.
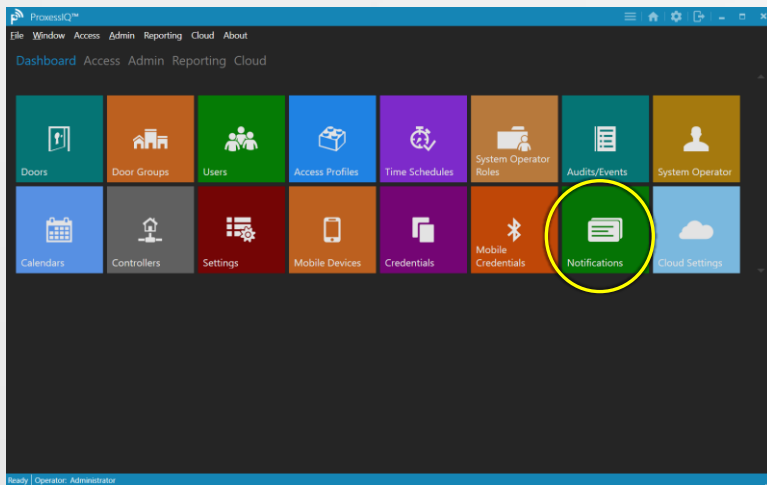
From the Home screen \ Dashboard, click "Notifications".
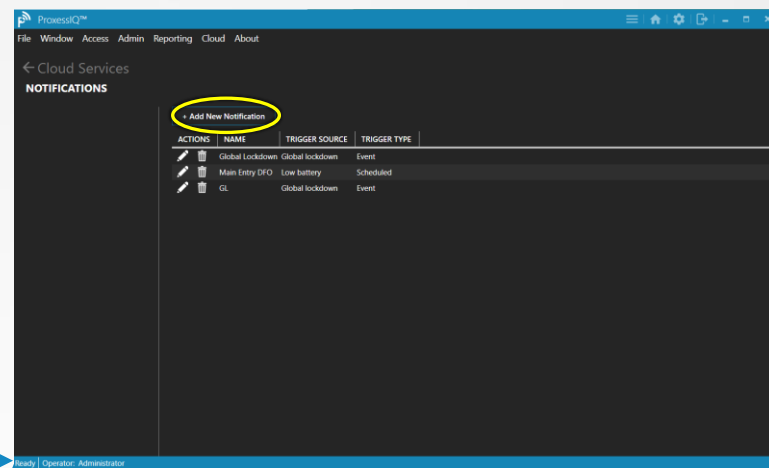
Your existing Notifications will be listed. Click "Add New Notification" to do so. You may click on the column titles (Name, Trigger Source and Trigger Name) to sort by them in alphabetical order. You may edit or delete any existing Notification by clicking on its Pencil/Edit icon on the left side.

Note: "Low Battery" & "Expiring Credentials" are good preventative Notifications to set, to receive emails in advance of the resulting poor user experiences.
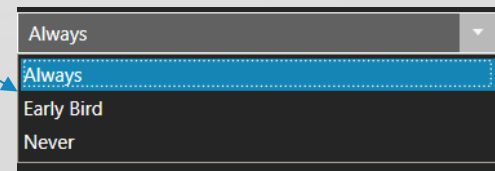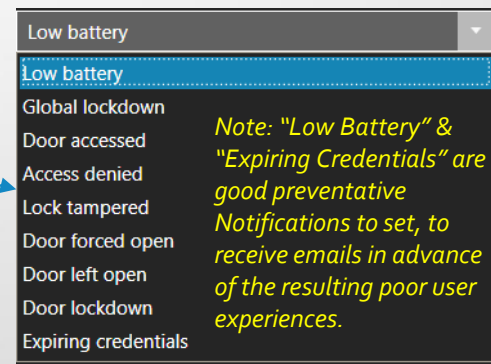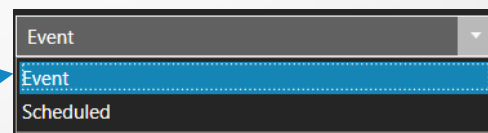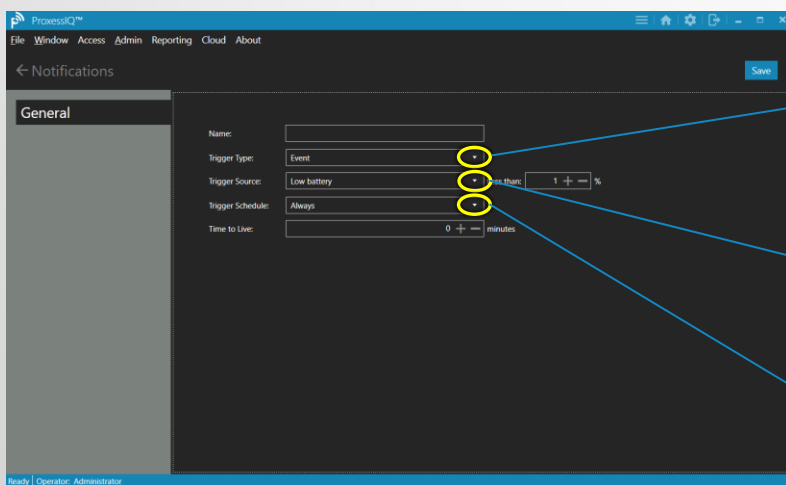
Enter the name for the new Notification. The "Trigger Type" for initiating a Notification is either an instantaneous Event, or one that is Scheduled. The "Trigger Source" list is shown on the right. "Trigger Schedule" is provided to allow different people to receive emails at different times and days. "Time to Live" is the number of minutes you want the Notification to remain valid. In other words, it is the number of minutes from activation until the Notification will expire. Selecting "O" means that the Notification will **Not** expire and will persist until it is attended to. Only one email will be sent per event.

Notifications - 1

Note: In the following example we will create a Scheduled Notification. For Notifications with the "Trigger Type" selected as an "Event", individual Users/Recipients may be added to be emailed either always, or just for specific days of the week and times of the day.

As an example, we will name a new Notification, "Preventative Battery Maintenance". We will select it to be a scheduled event, notifying on any-and-all locksets that have a "Low Battery" level of 30% (This should give you 1 to several months, depending on usage, advance notice before the low-battery LED begins blinking on the locksets). The default time for a scheduled notification is once per week. Click the edit button to change this.

Let's have this email sent out every 4 weeks (click the + & - to change), at 8AM (click there to change), beginning on the date of your choice (click there to change). Click "OK".

Click on "Save".

This shows the new Notification has been saved. Click "OK".

To select someone to receive an email for this Notification (either on a schedule or as it is received in the software), Click "Add a New Recipient".

Select the recipient's name from the drop-down list of Users and then "User Email" from the next drop-down list. Additional options may become available for selection in this list. Click OK".

The recipient now appears in the list for this Notification. You may return to the Notifications menu by clicking "← Notifications".

Notifications - 3

Note: In the following example we will create an Event based Notification. The primary difference from a Scheduled Notification is this: With an Event based Notification, individual Users/Recipients may be added to be emailed either always, or just for specific days of the week and times of the day.
From the main Notifications page, Click on "Add New Notification" and this page will open.

As an example, we will name a new Notification, "Local Lockdown". This will provide an email from an individual Lockset being put into the Lockdown mode. We will select it to be an "Event" based Trigger Type, with a Trigger Source as a "Door Lockdown", with the email being sent to the Users we will next select, during the "Early Bird" Trigger/Time Schedule. Click "Save".

Click "Add New Recipient".

Select the recipient's name from the drop-down list of Users and then "User Email" from the next drop-down list. Additional options may become available for selection in this list. Click OK".

Here is a User, with their email, to receive Mobile Keys, as well as Notifications

As it is for any typical User, they have a Mobile Key for door entry.

For this User to receive Notifications as a Text to their phone, Create another User for them. Enter their email as their email-as-text format.

This second User does Not get a credential assigned to them.

Here are both of their User records.
Any Notification can be sent to one or both of this person's User emails.

Mobile phones with **AT&T** and **T-Mobile** service plans can receive emails-as-texts, with the full data contents as are provided in standard emails. In the case of a Lockdown, the information includes the name of the initiator, their phone number and the door they put into lockdown. Texts are generally much quicker than emails and are easier to set as a notification to phones, even when locked. They are therefore generally a better emergency method than emails, though consideration should be given when utilizing them as the sole emergency notification strategy. Generally, a Proxess local or vicinity lockdown occurs at the onset of an event and the turnaround time for the email and text notifications to arrive at the recipients' phones will precede the initiation of mass staff, student, etc. texting, calling and streaming, which will then likely saturate both cell and WiFi networks.

Email-as Text Format: **AT&T** 1234567890@txt.att.net and **T-Mobile** 1234567890@tmomail.netnet

UPGRADE to TRIGGERS & *ACTIONS*

Note: This is a licensed capability. Please contact your Proxess sales representative for an upgrade.

Notifications - 5

Notifications - 6

The recipient now appears in the list for this Notification.
You may return to the Notifications menu by clicking
"   Notifications".

The recipient now appears in the list for this Notification.
You may return to the Notifications menu by clicking
"← Notifications".

MOBILE (Phone) KEYS

(a.k.a. Mobile Credentials)
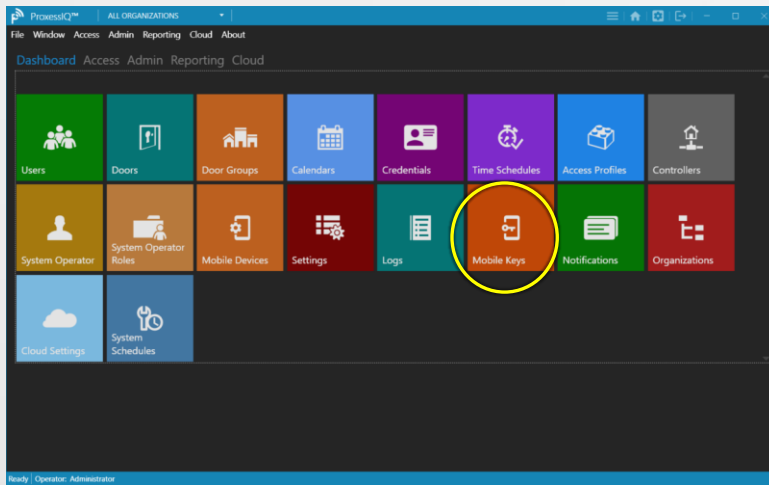
Click on the "Mobile Keys" menu to specifically view and manage Mobile Keys.
Note that Mobile Keys are created and issued in the Users section and this section is more of a shortcut to managing and debugging them.

Total Mobile Keys allotted to your system.

Total Mobile Keys being used now.

Direct link to edit this credential.

To Enable (blue) / Disable (unchecked) Mobile Keys.

Global Dis/Enable

Incorrect Email
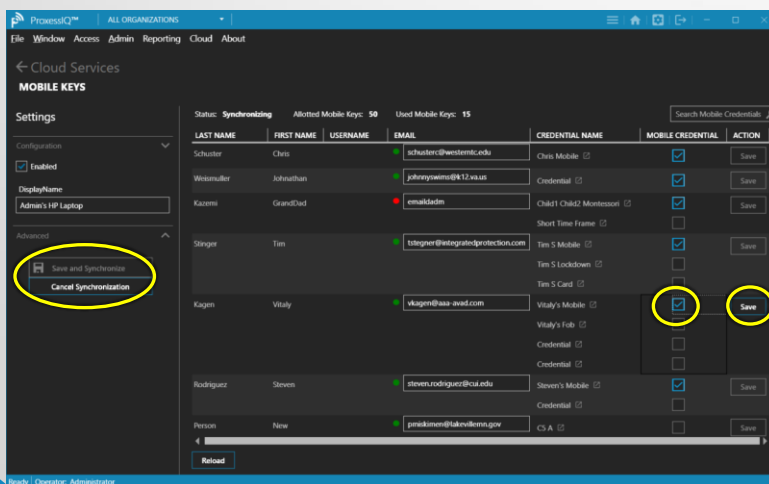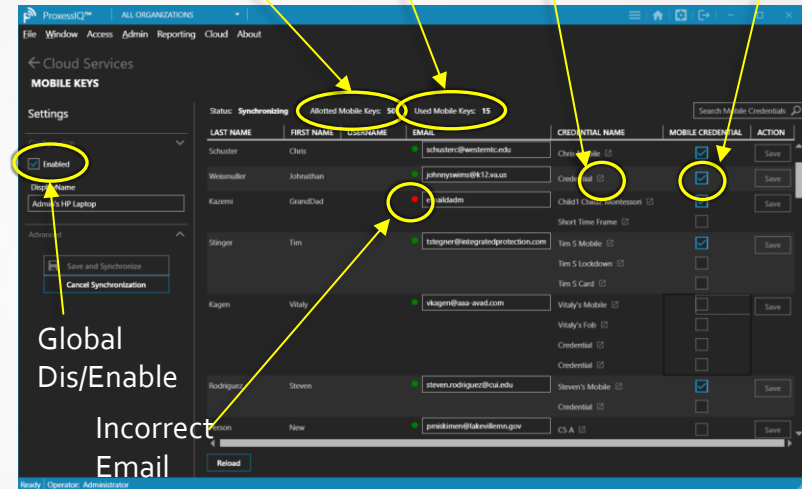
To enable a previously dormant Mobile Key, click its box to give it a blue check and click "Save". The system will Synchronize
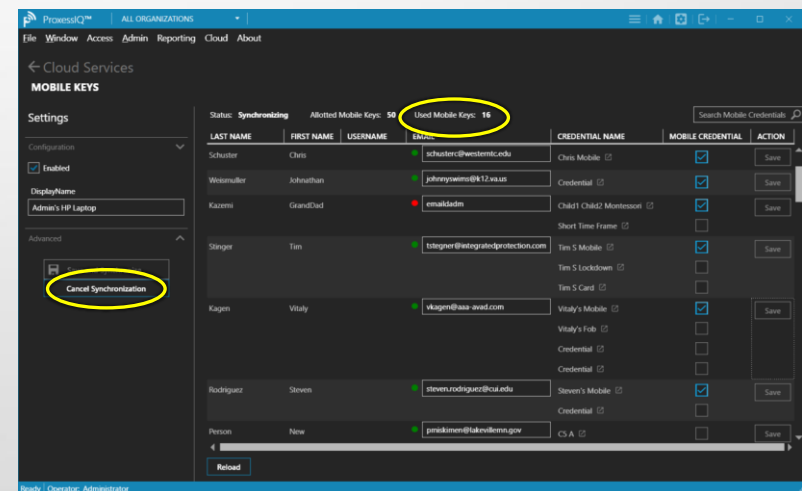
Once Synchronized, the number of Used Mobile Keys will increment by 1 (to 16 in this case). The same will happen in reverse, if you uncheck an MK to disable it.

CLOUD Settings

Enabling the use of Mobile Keys in Proxess**IQ**™

From the ProxessIQ dashboard, click on Cloud Settings .
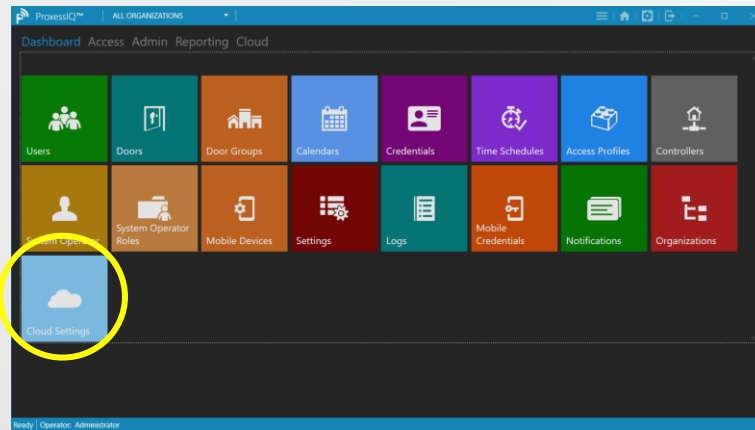
Extract the files from the license zip you have received and open the ProxessIQ_CloudToken text file..
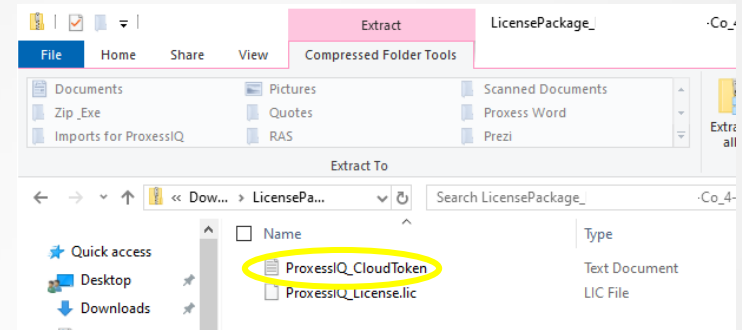
In the Cloud Settings menu, check the "Enabled" box.
Copy each line of text file (including all the special characters, but not any extra spaces) and paste them into the appropriate fields.
Leave the "Forced Online" box checked.
Then click "Save and Synchronize" until "Synchronized" is shown.

ProxessIQ_CloudToken - Notepad

File Edit Format View Help

Display Name: Company ABC
Host: https://pmcs.proxess.com
MC ACS ID: cae43b59-77f9-44da-aac0-6337796a7ea5
Token: eKH2ojCClKUv/Wdy9r2mxjgkH4mbO1miWPJkTj7Kc94=
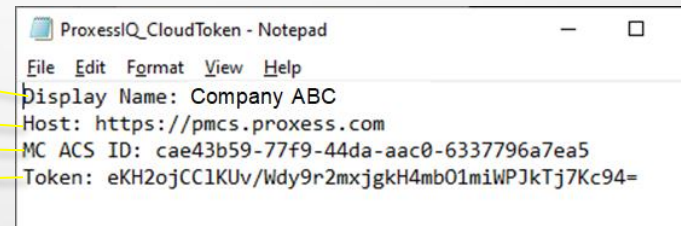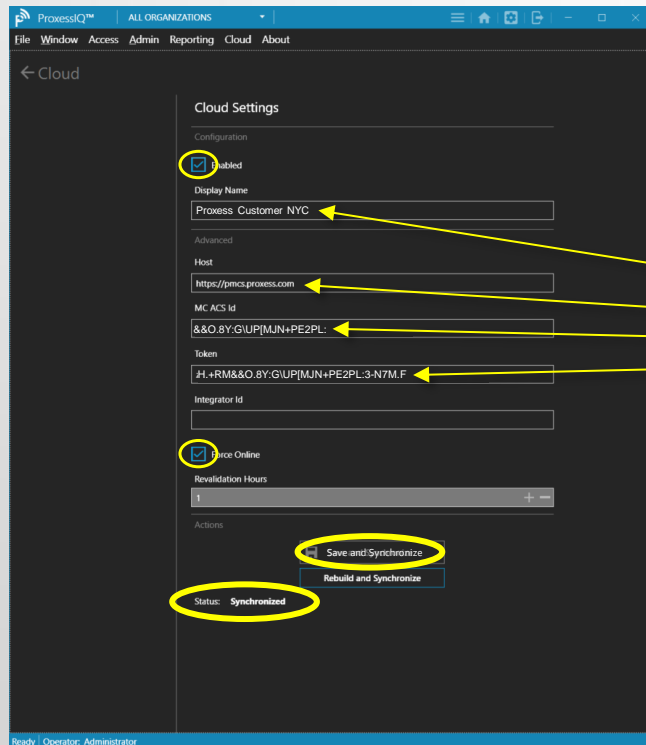
This will check the license against the Proxess Mobile Key issuance cloud and allow the use of mobile keys in your system.
As you use and purchase mobile keys over time, those quantities will be displayed in the Mobile Keys menu.

You may now click the back arrow or the Home button and resume your system programming.

LOGS

All User & Door event logs are available here and may be searched using multiple custom Boolean rules.
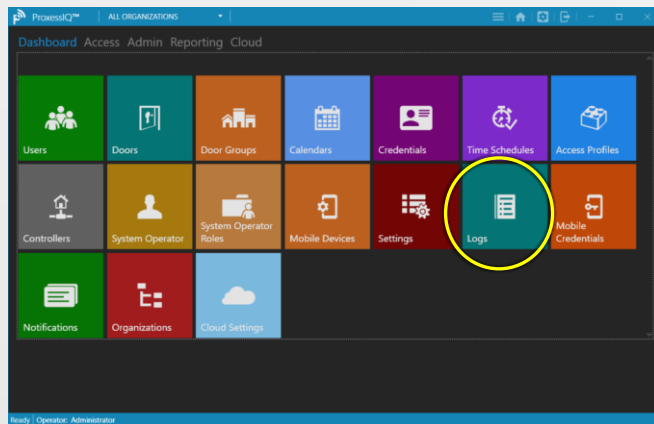
Click on the "Logs" menu.

The combination of all User & Door Logs/events are available here and may be searched using multiple custom Boolean rules.

As a reminder, a single User's or Door's events/Logs may also be found under their individual records.

This is the initial screen. On the left is the list of saved custom searches you or other Operators may have created. You can simply click the name of the one you want to execute or the trash icon of the one you may want to delete.

SEARCH SOURCES	EVENT CODE TYPE	EVENT SOURCE TYPE
Event Date Time	Valid Access	LockAudit
Source Item Name	Invalid Access	Door
Source Details	Contact Point (Physical Input)	Door Group
Event Code	Lock Event	User
Event Code Type	Event Group Door Alerts	Credential
Event Source Type	Communications	Operator
	Item Created	Controller
	Failed	OperatorMPD
	Item Removed	AccessProfile
	Item Deleted	Calendar
	Item Relationship Added	TimeSchedule
	Item Relationship Removed	AuditLog
	Item Updated	OperatorRole
	Accessed	Other

EVENT CODE NAME

Access	Alert Door Forced Open	Controller Create
Entry	Alert Door Forced Open Cancel	Controller Update
Exit	Communication Lost to Proxess Host	Controller Remove
Access Under Duress	Communications Restored to Proxess Host	Controller Create Fail
Entry Under Duress	Communications Lost to Reader	Controller Update Fail
Exit Under Duress	Communications Restored to Reader	Controller Remove Fail
Access Under Lockdown	Door Create	Controller Password Accessed
Entry Under Lockdown	Door Create Fail	Controller Connecting
Exit Under Lockdown	Door Update	OperatorMPD Create
Double Swipe Reader Toggle Unlock	Door Update Fail	OperatorMPD Update
Double Swipe Reader Toggle Cancel	Door Remove	OperatorMPD Remove
Mechanical Key Access	Door Remove Fail	OperatorMPD Create Fail
Lockdown Initiated	Door Delete	OperatorMPD Update Fail
Lockdown Cancelled	Door Group Create	OperatorMPD Remove Fail
Card Format Not Supported	Door Group Create Fail	AccessProfile Create
Invalid System ID	Door Group Update	AccessProfile Update
Antipassback Violation	Door Group Update Fail	AccessProfile Remove
Credential Not Yet Activated	Door Group Remove	AccessProfile Create Fail
Credential Has Expired	Door Group Remove Fail	AccessProfile Update Fail
Revalidation Period Has Expired	Door Group Delete	AccessProfile Remove Fail
No Access Granted To This Door	Door Group Delete Fail	Calendar Create
Access Not Permitted At Time Of	Door Group Assignment Add	Calendar Update
Presentation	Door Group Assignment Remove	Calendar Remove
Repeated Invalid Attempts	User Create	Calendar Create Fail
Rex Active	User Create Fail	Calendar Update Fail
Rex Secure	Upser Update	Calendar Remove Fail
Rex Fault Short	User Update Fail	TimeSchedule Create
Rex Fault Open	User Remove	TimeSchedule Update
Tamper Active	User Remove Fail	TimeSchedule Remove
Tamper Secure	Credential Create	TimeSchedule Create Fail
Power On Reset	Credential Update	TimeSchedule Update Fail
Factory Default Reset	Credential Remove	TimeSchedule Remove Fail
Lock Parameters Programmable VIA BLE	Credential Create Fail	AuditLog Clear All
Lock Database Programmable Via BLE	Credential Update Fail	AuditLog Row Removal
Low Battery Warning	Credential Remove Fail	OperatorRole Create
Critical Battery Warning	Operator Create	OperatorRole Update
Battery Failure As Is	Operator Update	OperatorRole Remove
Time Changed	Operator Remove	OperatorRole Create Fail
Batteries Replaced	Operator Create Fail	OperatorRole Update Fail
Alert Door Held Open	Operator Update Fail	OperatorRole Remove Fail
Alert Door Held Open Cancel	Operator Remove Fail	Unknown Event

SETTINGS

These tabs show the default settings used throughout the ProxessIQ™ software. Each of them can be customized to your preferences, by site, reader, cardholder and operator.

Unless changed, all new devices (i.e. controllers, readers, …), operators and cardholders will be defaulted to the attributes on these tabs.

To change the default settings usage, you may either uncheck the appropriate box on these tabs (which will change all future defaults) or you may uncheck the individual box next to the field that you are configuring elsewhere in the software (which will affect only that device or person).

ORGANIZATIONS

A.k.a. Partitioned Database & Landlord-Tenant
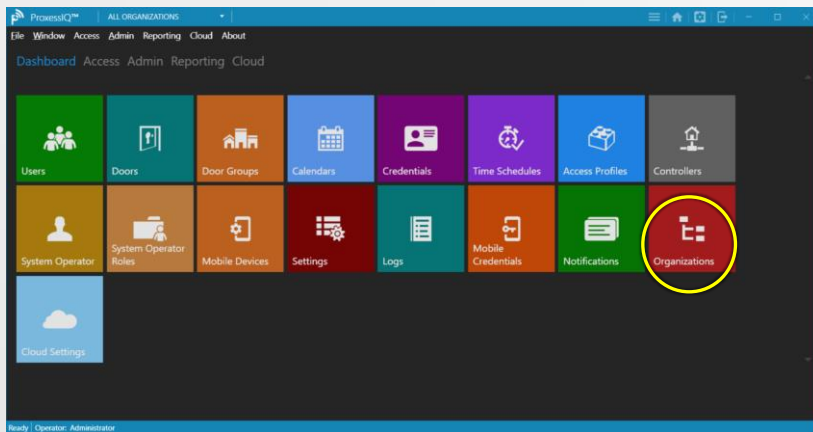
LOCKDOWN CONFIGURATIONS

Configuring Various Lockdown Operations
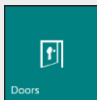
Define the Lockdown parameters for a Door, including the use of the Lockdown button on the Lock and requiring the use of the Lever for a Lockdown.
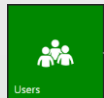
Create Physical Cards & Fobs for First Responders.

Create Mobile Keys for First Responders.
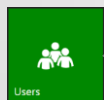
Create and enable Mobile Keys to perform Lockdowns from across the room.
1st Responders receive Door #, Initiator Name & Phone #
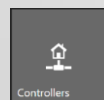
Connect locks and BLE controllers to gateways to place them into Lockdown, whenever another specific system event occurs (defined in Notifications).
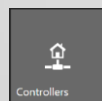
Custom define an external Input and/or Output in Controllers, for their use in Notifications.

Lockdown Capabilities

Local:
At the door

First Responder Cards:
Passthrough /Welfare Check

Go Mobile:
Did the 1st 1st Responder take the keybox key?!

Vicinity:
Across the room

Within the Threat Radius

Inside Verification
External Notification

Regional/Grouped:
Down the hall

Global:
Across Campus

Linked:
Proxess Initiated
3rd Party Initiated

Lockdown Card:

Panic Button:
Wearable or Wall Mounted

AV Notification:
Campus, Hall & Classrooms

With the addition of a gateway, local Lockdown events can automatically go to the software and create a Grouped or Global Lockdown

Initiate Global Lockdown from dedicated button on Doors menu
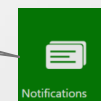
Configure a Global or Grouped Lockdown to occur due to any system-defined event.

Athletic Field

Initiate Lockdown from Athletic fields. No Wiring
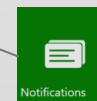
Configure any system event or external device to perform any number of system and external events.
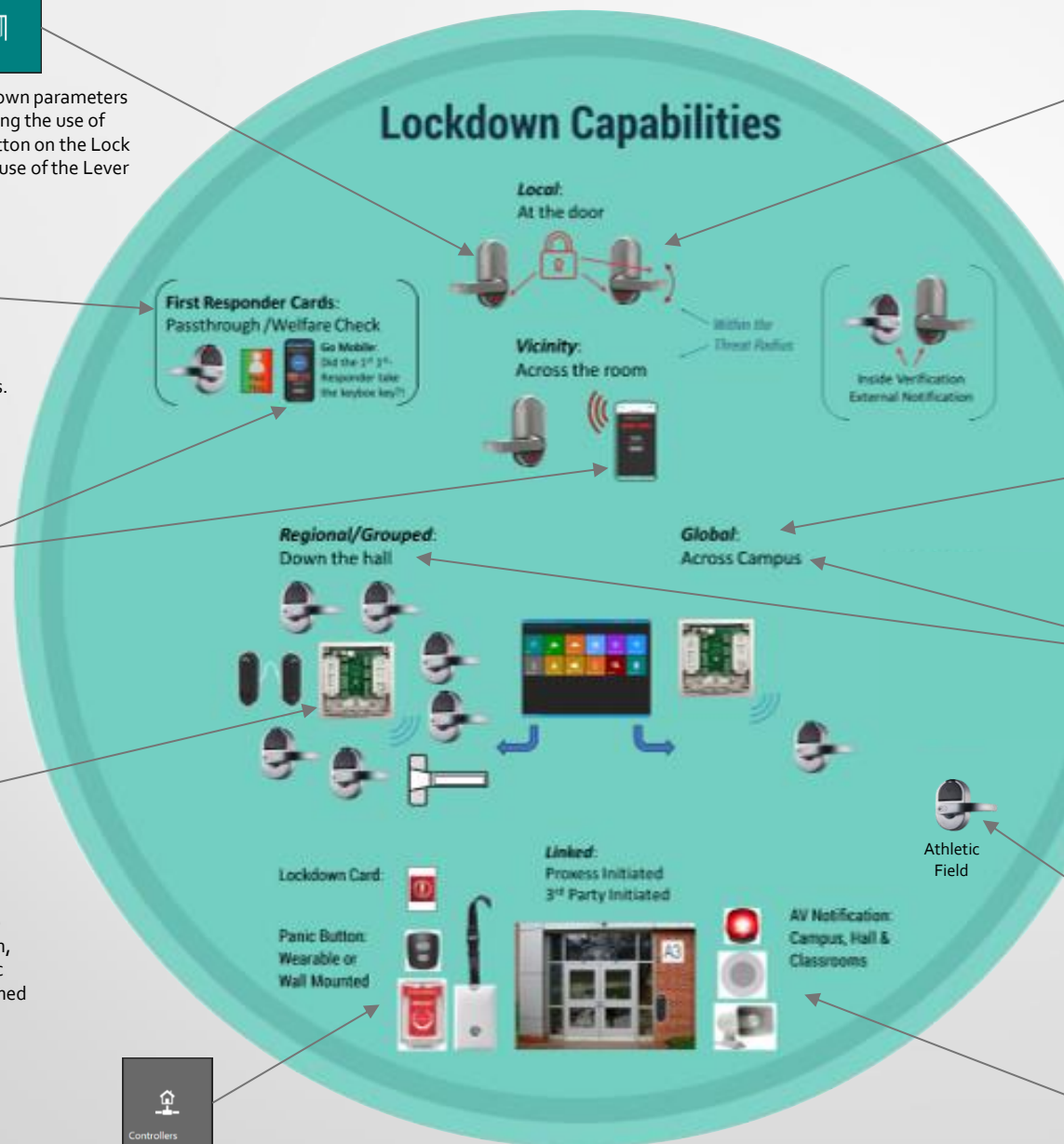
LEDs for DEBUGGING LOCKS & CONTROLLERS

Information & Debugging LED/Light Sequences

Cylindrical / Mortise / Exit Trim

- Rainbow (all colors in sequence)-startup sequence when lock is powered on or restarts
- White- when interior button pushed, one flash white means lock is in construction mode (unprogrammed)
- Green- access granted
- Red-Access denied
- Blue-Data communication issue happening
- Triple red- battery low (or when toggled locked)
- Triple green- toggled unlocked
- Yellow- bad/defective/uninitialized credential
- Teal-Bluetooth timeout
- Purple- communication issue with lock reader board

Information & Debugging LED/Light Sequences

<u>Mini-IQ</u>

- Rainbow (all colors in sequence)-startup sequence when lock is powered on or restarts
- Green- access granted
- Red-Access denied
- Blue-Data communication happening
- Triple red- battery low (or when toggled locked)
- Triple green- toggled unlocked
- Yellow- bad/defective/uninitialized credential
- Purple/white (reader light will be half illuminated purple & half white)- error pushing firmware, reader will restart on its own within a few minutes (do not reset power)
- Yellow- bad/defective/uninitialized credential
- Pulsing red – reader cannot communicate with Mini-IQ board

Information & Debugging LED/Light Sequences

Reader (BoxIQ)

- Rainbow (all colors in sequence)-startup sequence when lock is powered on or restarts
- Green- access granted
- Red-Access denied
- Blue-Data communication happening
- Triple red- battery low (or when toggled locked)
- Triple green- toggled unlocked
- Yellow- bad/defective/uninitialized credential
- Purple/white (reader light will be half illuminated purple & half white)- error pushing firmware, reader will restart on its own within a few minutes (do not reset power)
- Yellow- bad/defective/uninitialized credential
- Pulsing red – reader cannot communicate with BoxIQ
- Stuck on solid blue – Can happen after firmware updates, reader is waiting for a command from a controller. Any action will set the reader lights to normal

API
CONFIGURATION

API Configuration - 9

ProxessIQ™ API

AccessProfile — Show/Hide | List Operations | Expand Operations
AuditLog — Show/Hide | List Operations | Expand Operations
Calendar — Show/Hide | List Operations | Expand Operations
Controller — Show/Hide | List Operations | Expand Operations
Credential — Show/Hide | List Operations | Expand Operations
Door — Show/Hide | List Operations | Expand Operations

GET /api/door/getdoors — Returns a list of all active doors

Response Class (Status 200)
OK

Model | Example Value

```
[
  {
    "UnlockTime": 0,
    "UnlockTimeExtended": 0,
    "DoorHeldOpenDetectTime": 0,
    "DoorHeldOpenDetectTimeExtended": 0,
    "FirstPersonIn": true,
    "CalendarId": 0,
    "UnlockTimeScheduleId": 0,
    "ToggleEnableTimeScheduleId": 0,
```

Response Content Type application/json

Try it out!

Try it out!   Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii11Zn
```

Request URL

```
https://desktop-une0fp0:8015/api/door/getdoors
```

Response Body

```
[
  {
    "UnlockTime": 5,
    "UnlockTimeExtended": 30,
    "DoorHeldOpenDetectTime": 30,
    "DoorHeldOpenDetectTimeExtended": 60,
    "FirstPersonIn": false,
    "CalendarId": 1,
    "UnlockTimeScheduleId": 2,
    "ToggleEnableTimeScheduleId": 1,
    "CardOnlyTimeScheduleId": 1,
    "ToggleMaxDelayTime": 5,
    "LockDownMinDelayTime": 5,
    "EgressDisableLockdown": false,
    "PassThroughCancelsLockdown": true,
    "RecordValidAccessAttempts": false,
    "RecordInvalidAccessAttempts": true,
    "EnableNocAudits": true,
    "BatteryFailureThreshold": 0,
```

Response Code

```
200
```

Response Headers

```
{
  "content-length": "39403",
  "content-type": "application/json; charset=utf-8",
  "date": "Fri, 11 Oct 2024 22:45:15 GMT",
  "server": "Microsoft-HTTPAPI/2.0"
}
```