

## The aPod II Access Control System Administrator's Guide



## Table of Contents

<b>Introduction .....</b>	<b>7</b>
<b>Login .....</b>	<b>8</b>
Access the Login Page .....	8
On Site Access .....	8
Remote Login.....	9
Browser Window.....	9
Bookmark the aPod II URL.....	10
Enable JavaScript.....	11
Logout.....	11
Automatic Logout.....	12
<b>System Navigation .....</b>	<b>13</b>
Hypertext Search .....	16
<b>Configure and Manage the System .....</b>	<b>18</b>
Administrators.....	18
Add an Administrator .....	18
Assign a temporary password .....	19
Custom temporary password .....	19
Assign administrator permissions .....	21
The Remote Login permission .....	21
Edit or Delete an Administrator.....	22
Audit Logs .....	23
Password .....	24
Preferences .....	25
The Browser Interface Language.....	25
Alarm Audio Alerts.....	26
Door Open Chimes.....	26
Schedules in Monochrome.....	26
Enable Email Security Alerts.....	27
Doors .....	28
Schedules.....	29
Modify the door locking schedule.....	29
Weekdays, weekends, and holidays .....	31
Daylight Savings Time.....	31
Automatic locking and unlocking .....	32
Replicating door schedules.....	32
Schedule with the 'By Door' Access Authorization Method.....	33
Schedule with the 'Door by Schedule' or 'By User Groups' Access Authorization Methods .....	36

- Holidays ..... 39
- Options ..... 40
  - Alarm annunciation ..... 40
  - Door Forced alarms ..... 41
  - Door Held Open alarms..... 41
  - The unlock operation ..... 43
  - Scheduled unlock ..... 44
  - PIN functionality ..... 45
  - Dual Custody Mode..... 47
- Doors – Advanced Options..... 48
  - Hardware ..... 48
    - Enrolling a Secondary controller ..... 49
    - The locking and reader hardware ..... 49
    - The input points ..... 51
    - The output points ..... 56
  - IP..... 57
    - IP Settings..... 58
    - Time Server..... 59
- Areas..... 60
- Dates ..... 61
  - Modify your holidays list ..... 61
  - Edit the perpetual calendar. .... 62
  - Add a new holiday. .... 64
    - Schedule a shutdown period ..... 64
  - Override Daylight Savings Time dates ..... 65
  - Non-Statutory Religious Holidays ..... 67
- Backup ..... 68
  - Backup Types ..... 69
    - Standard backup..... 69
  - Events backup..... 70
- Restore ..... 71
  - Restore from Backup. .... 71
  - Restore to Defaults..... 73
- Archive Events and the Administrators Audit Log ..... 75
  - The archiving procedure..... 75
  - Review the Archives ..... 77
- System-wide Settings ..... 78
  - Site Name and Site Address..... 78
  - Time Zone..... 78
  - Daylight Savings..... 79
  - Add Dates ..... 79
  - Custom Applications ..... 79
  - Language ..... 79

- Access Authorization ..... 79
  - By Door..... 80
  - Door by Schedule ..... 80
  - User Groups..... 80
- Pin Length and Pin Strength ..... 80
- Administrator Temporary Password..... 80
- Elevators..... 81
- Primary Internet IP and Port..... 81
- Remote Login Setup ..... 81
- Remote HTTP Port (TCP)..... 81
- Date and Time ..... 81
- Selected Locale ..... 84
- Primary IP Address ..... 84
- The Engineering Page..... 85
- Cards..... 89

**Monitor and Control the System ..... 91**

- Home - Dashboard ..... 91
  - Door security status..... 93
    - Cancel alarms..... 93
  - Door locked/unlocked status and open/closed status ..... 94
    - Override door schedules..... 94
    - User controlled schedule overrides..... 94
    - Scheduled locked intervals..... 95
    - Scheduled unlocked intervals ..... 95
    - Pending unlocked intervals ..... 95
    - Unlock override..... 96
    - Lock override ..... 96
    - Lockout override ..... 96
    - Fire system unlock ..... 96
    - User controlled unlock override..... 97
    - User controlled lock override ..... 97
  - Input point status ..... 97
    - Secure state..... 98
    - Point active state..... 98
    - Alarm State..... 98
    - Alarm Conditional input..... 99
    - Alarm Panel input ..... 99
    - High Security (Supervised) input points ..... 99
  - The event log..... 100
    - The Access Denied response..... 102
- Reports ..... 103
  - Report Type ..... 103
  - Report Filters..... 104

Database Reports .....	106
Report Format .....	107
Custom Report Header .....	110
<b>Manage Users.....</b>	<b>111</b>
Add a User.....	112
User Options.....	112
<i>Assisted Access</i> .....	112
<i>Suspend</i> .....	112
<i>3X Lock/Unlock</i> .....	113
<i>3X Arming</i> .....	113
<i>Keypad Options</i> .....	113
<i>Silence Alarms</i> .....	114
<i>Pending unlock</i> .....	114
<i>Deny Entry if Armed</i> .....	115
Enroll the Access Token .....	115
Enter the Card ID Number manually.....	117
Enroll an unmarked card .....	117
Give a User Temporary Access .....	118
Assign PIN's .....	120
<i>PIN length and PIN strength</i> .....	120
<i>Assign PIN's</i> .....	121
<i>Managed PIN's</i> .....	122
<i>Temporary PIN</i> .....	123
CARD+PIN MODE .....	124
ID+PIN MODE .....	124
Change the PIN at a Keypad Reader .....	126
Assign Access Permissions to Users .....	128
By Door .....	129
Door by Schedule.....	130
By User Groups .....	131
<i>Create the User Groups</i> .....	131
<i>User Group Schedules</i> .....	134
<i>User Group Holidays</i> .....	136
Importing User Data.....	137
Introduction.....	137
The Procedure .....	137
<b>Advanced Options.....</b>	<b>147</b>
Update the Software.....	147
New software notification .....	151
Remote Login .....	152
Step 1 - Identify the system .....	152

- Step 2 - Configure communications..... 153
  - Configure the aPod II Controller. .... 154
  - Configure the router. .... 154
- Remote Login Portal ..... 156
- Manage the remote login permission..... 157
- Proxy Servers and Firewalls ..... 158
- Systems with a static Internet address ..... 158
- Alarm Panel Interface..... 159
  - Overview ..... 159
  - Features of the aPod II Alarm Panel Interface ..... 160
  - Arm the Alarm Panel with Your Access Token ..... 161
  - Assign authority for Arming the Alarm Panel ..... 162
  - Delayed arming ..... 163
  - Disarm the Alarm Panel ..... 164
    - Authorization to Disarm the Alarm Panel..... 165
  - Disarm with Grant Access ..... 166
  - Remote Arming and Disarming..... 166
  - Arming/Disarming Security Alerts ..... 168
  - Piezo Siren Annunciation ..... 168
- Anti-passback ..... 169
  - Introduction..... 169
  - Configure Logical Anti-Passback ..... 169
    - Step 1 – Define areas for anti-passback. .... 169
    - Step 2 – Configure the second reader..... 171
    - Step 3 – Select the anti-passback mode of operation. .... 172
    - Step 4 – Assign the access readers to an anti-passback area..... 173
  - Reset anti-passback. .... 175
- Automatic Door Opener Interface ..... 177
- Fire Alarm Unlock Operation ..... 178
  - Cancelling the Fire Alarm..... 179
- Lockdown Operation ..... 181
  - Introduction..... 181
  - Implementation ..... 181
  - Configure the Lockdown Doors ..... 186
    - Define a Lockdown Area ..... 186
    - Assign Doors to the Lockdown Area ..... 187
- Occupancy Counter by Area..... 188
  - Overview ..... 188
  - Multiple access points ..... 188
  - Tailgating ..... 189
  - Free egress ..... 189
  - Occupancy count display ..... 190

Occupancy count reset .....	191
Software configurations .....	192
Time Zone Mode .....	196
Custom Apps .....	198
<b>Appendix 1 – Specifications.....</b>	<b>199</b>
<b>Appendix 2 - The aPod II System Network Topology.....</b>	<b>203</b>
A LAN Distributed System.....	203
A Multi-Site Distributed System .....	204

**Disclaimer:**

The example company, persons, places, and email addresses used in this Guide are fictitious and used for descriptive purposes only. Any resemblance to real companies, persons, places, or email addresses is purely coincidental.

**Version 3.20 - Issue date: June 11, 2021**

**Regulatory Notifications for the aPod II Door Controller:**

**Industry Canada ICES-003 compliance statement:**

**ICES-003 Class A Notice - Avis NMB-003, Classe A**

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

**Federal Communications Commission Part 15 compliance statement:**

**NOTE:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.





## Introduction

Your aPod II Access Control System will greatly improve the security of your building. Electric locks activated by access tokens will determine where people can go and at what time. Doors to restricted areas can remain locked without imposing any inconvenience on personnel who need access. As an administrator of this system, you will be responsible for some or all the following tasks which will integrate the use of this system into your normal daily activities.

- Designate other Administrators and specify which functions they can control.
- Establish time schedules for each access door. Time schedules determine when the door is unlocked or if locked, which level of access permission is required to unlock it.
- Add, modify, and delete Users (also known as card holders).
- Assign or modify access permissions to Users and give them an access token. Access permissions determine which doors a User can unlock and at what time.
- Provide instruction to Users on system operation. For most Users this is a trivial task but for some Users, such as security guards, additional training may be required.
- Print and examine reports to investigate security issues.
- Periodically backup the system database and restore it if necessary.

The aPod II Access Control System provides a Browser Interface which makes these tasks easy to perform. This Administrator's Guide is your resource for using the Browser Interface.

Browser-based software applications eliminate the task of distributing and installing software. The entire program is contained within the aPod II Primary Controller's web server and can be accessed from anywhere on your local area network or from anywhere there is Internet access, with any device that uses a browser, including PC's, tablet computers and smartphones.

The Login chapter describes how to set up your browser and bookmark the link to the aPod II system for easy, one-click access. The Remote Connect section describes how to configure your system for secure remote access from anywhere on the Internet.

Software updates for your aPod II Access Control System are free. You can easily update the software in your system using the simple and fail-safe process described in the Advanced Options chapter of this guide. The version number of the guide corresponds to the version number of the software.





## Login

### Access the Login Page

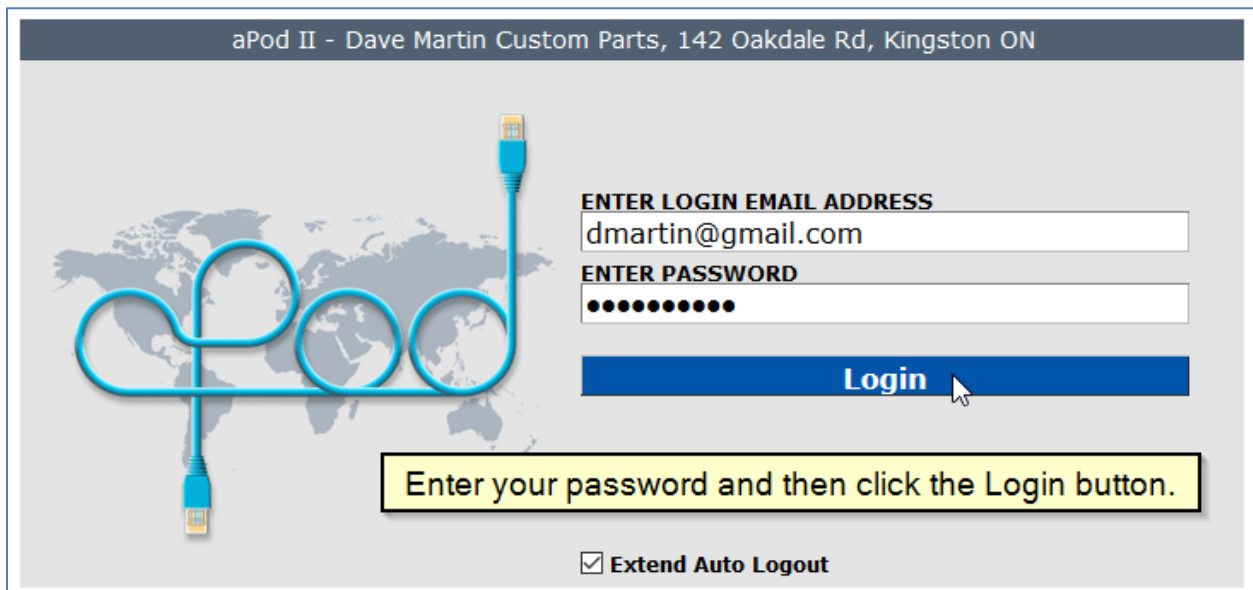
#### On Site Access

Use a browser to log into the system. Any common browser (e.g., Edge, Firefox, Chrome, and Safari) will work with any common computer operating system (e.g., Windows XP, Vista, Windows 7, 8 and 10, MAC OS and Linux).

Open the browser, enter “http://apod.local” into the address bar, and click the go button or press the “Enter” key to navigate to the System Login page. This will always work if the aPod II Primary Controller is on the same subnet or VLAN (*Virtual Local Area Network*) as your PC. In large facilities there may be more than one subnet. If your PC and the Primary Controller are on different subnets and are not connected with a VLAN, then you will need to enter the IP address of the Primary Controller to access it. In this case, your IT Department rep will give you this address.

For more information about subnets and VLAN’s, refer to Appendix 2 - The aPod II System Network Topology.

On your first login, enter your **LOGIN EMAIL ADDRESS** and your **PASSWORD** and then click the Login button to open the aPod II Home page. Your **LOGIN EMAIL ADDRESS** will be stored in a cookie and displayed automatically on subsequent logins.



## Remote Login

The aPod II Access Control System provides the ultimate in remote connectivity. It can be managed from anywhere there is Internet access with any device that uses a browser, including PC's, tablet computers and smart phones.

Open the browser and use a bookmark or a connection link on the Online Security Technologies web portal to access the [Login](#) page for your system. The method you use will depend on the Remote Login configuration mode. Please refer to page 152 for instructions on how to setup Remote Login.

## Browser Window

When you login to the aPod II system, the Browser Interface is opened in a new window. The browser tab displaying the [Login](#) page remains open but changes to the display shown below.

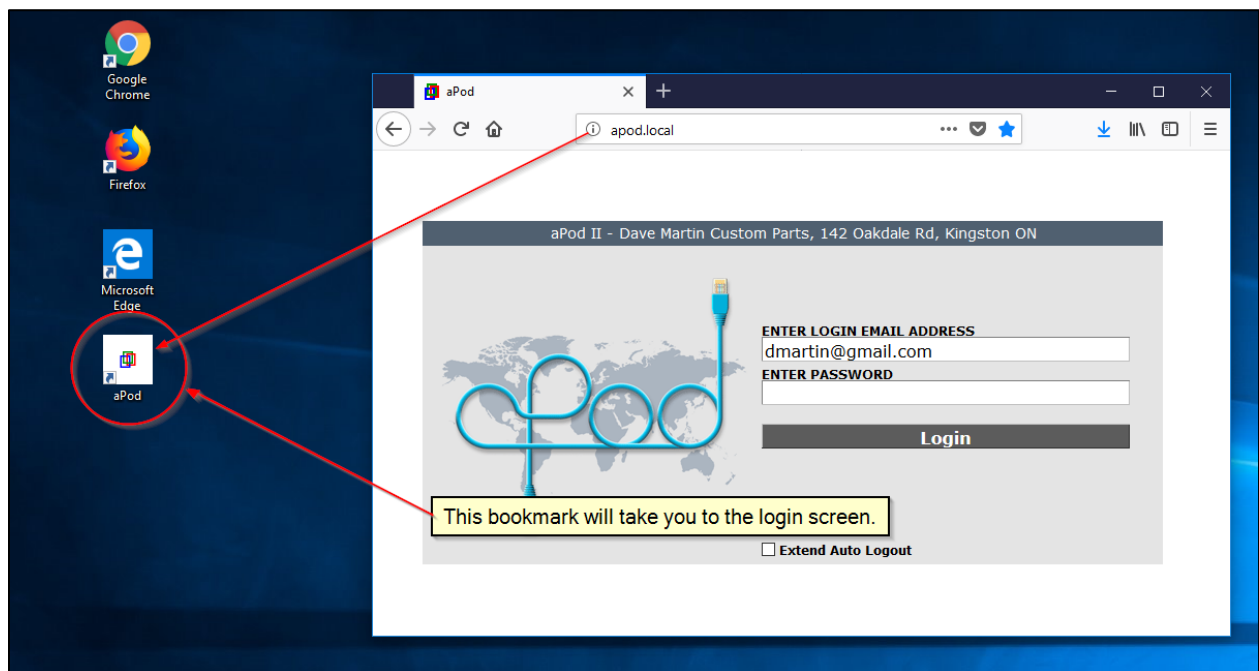
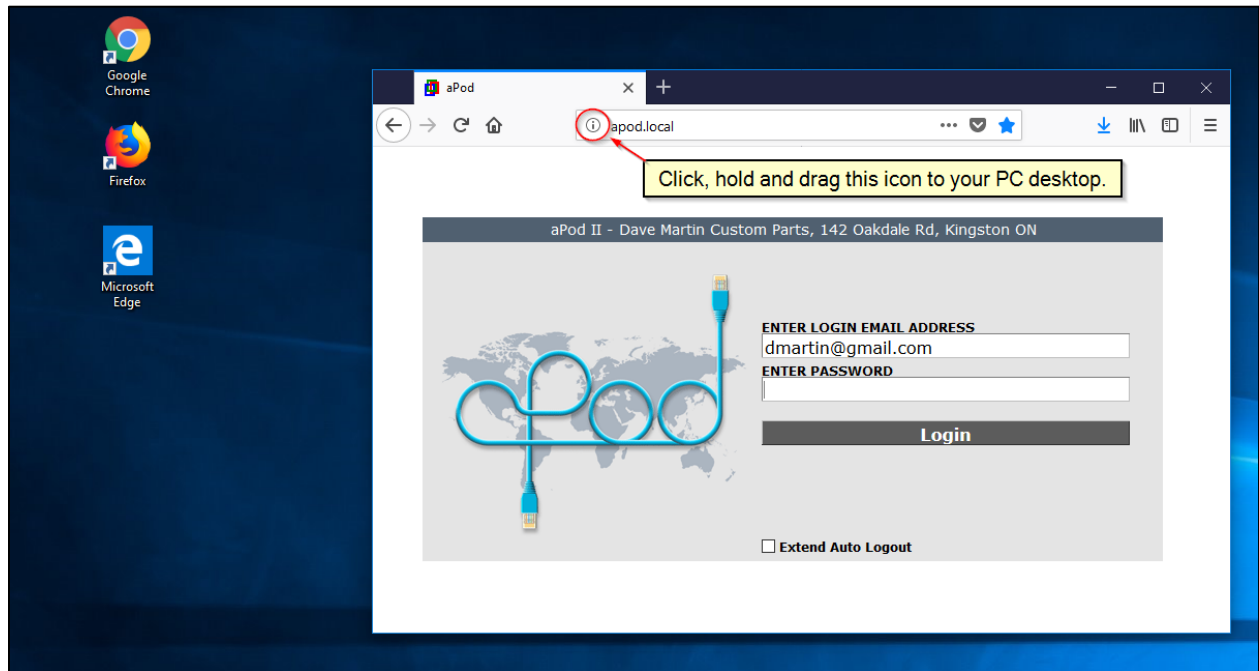


When switching from one application to another on your PC, if you open this tab, click the "Show aPod" button to display the aPod II Browser interface. When you logout of the aPod II Browser Interface, the above display reverts to the standard [Login](#) page.

**Note:** This function is not available in Firefox. Use the Windows Alt-Tab function to recall the active aPod II Browser Interface window.

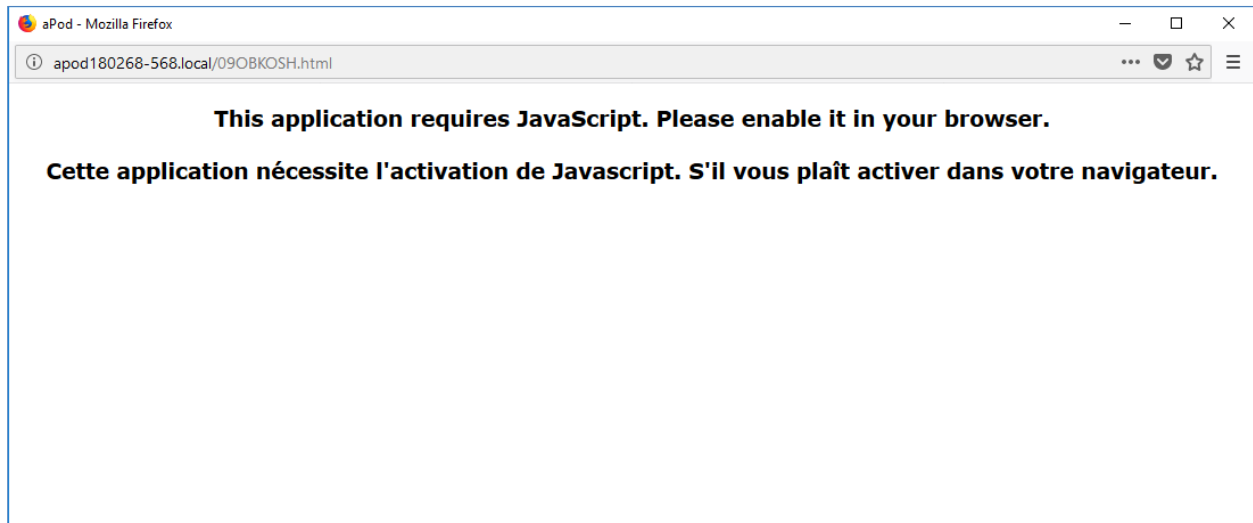
## Bookmark the aPod II URL

Bookmark the aPod II Login page for quick access. You may want to place a shortcut on your desktop. Downsize the aPod II Login window to partially expose your desktop. Drag the icon that precedes the URL onto the desktop, and you now have a shortcut that will take you directly to the Login page.

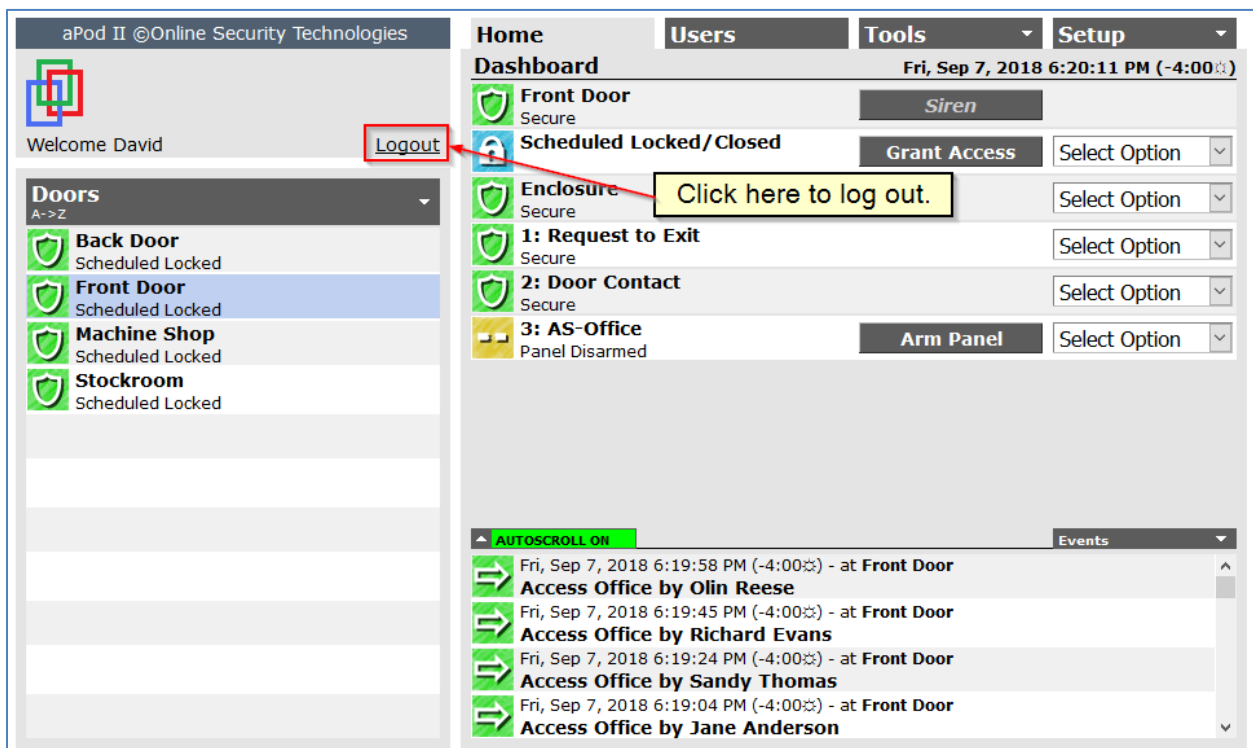


## Enable JavaScript

JavaScript is enabled by default in all browsers. If it is turned off in your browser, you will see the following message when you try to login. You must enable JavaScript to use the aPod II Browser Interface.



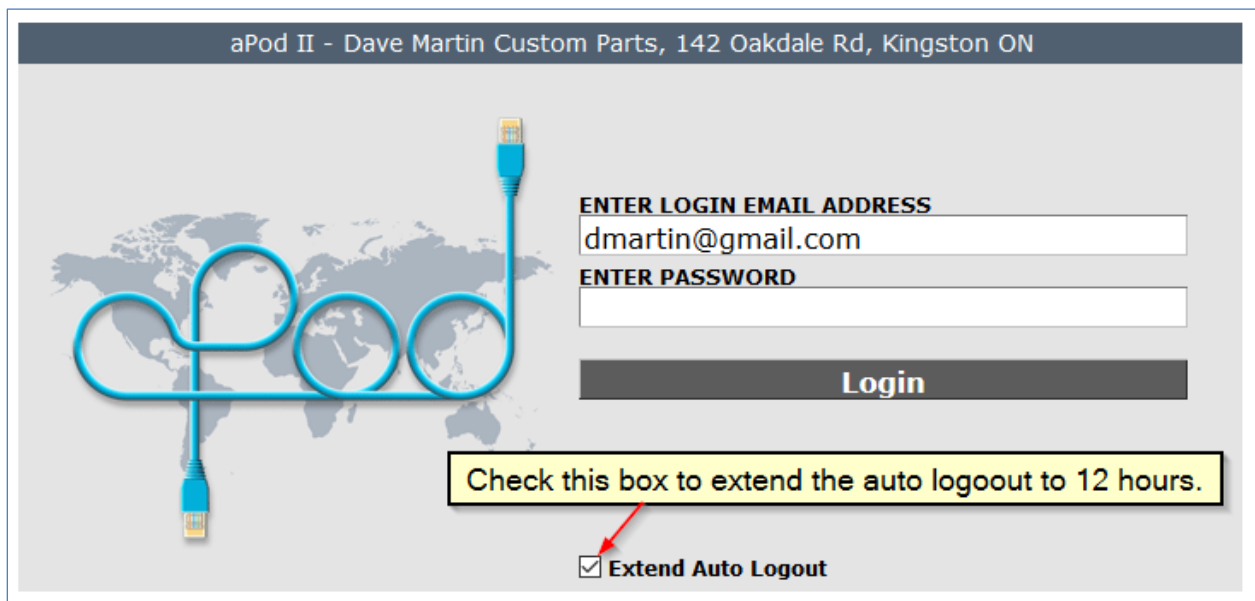
## Logout



## Automatic Logout

The aPod II system will log you out automatically if there has been no page activity for ten minutes. Click the “Extend Auto Logout” checkbox on the Login page to extend the time out period to 12 hours. This will allow the aPod II browser window to remain open during an entire normal workday and will allow continuous system monitoring.

The aPod II browser session will automatically close at the end of 12 hours but to maintain security you should log out whenever you leave your workstation.



aPod II - Dave Martin Custom Parts, 142 Oakdale Rd, Kingston ON

ENTER LOGIN EMAIL ADDRESS  
dmartin@gmail.com

ENTER PASSWORD

Login

Check this box to extend the auto logout to 12 hours.

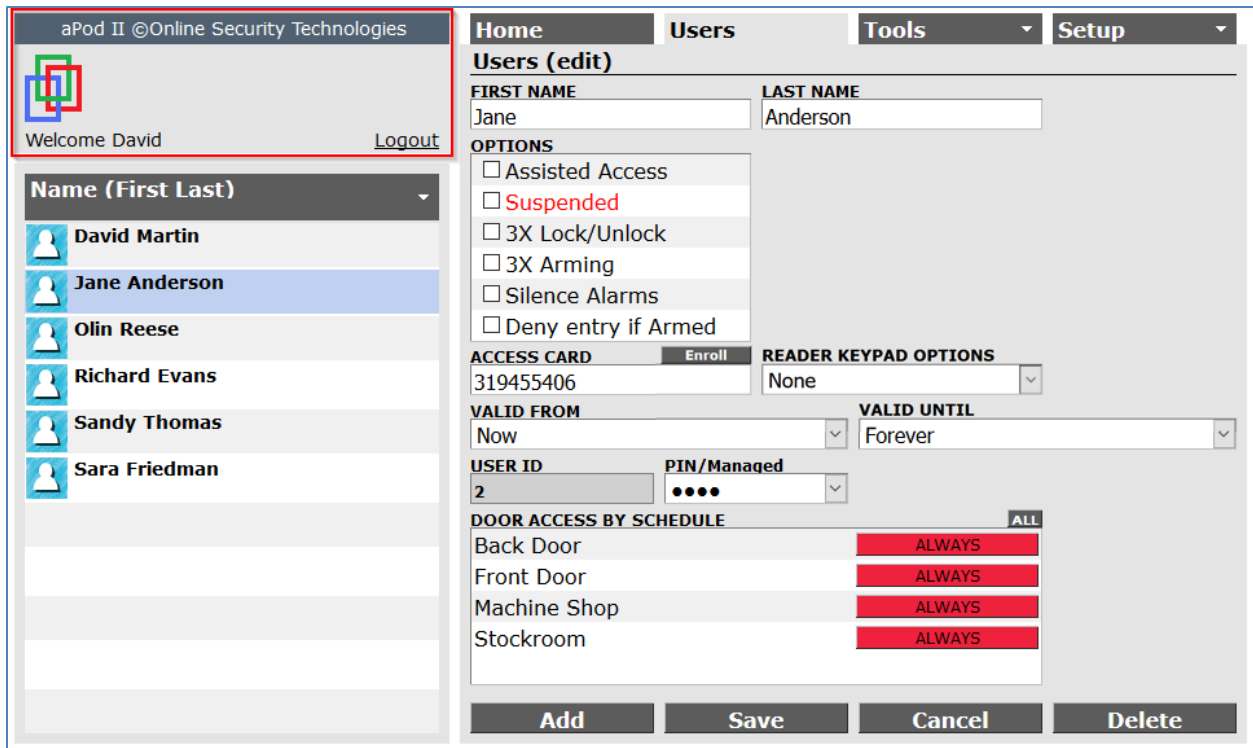
Extend Auto Logout



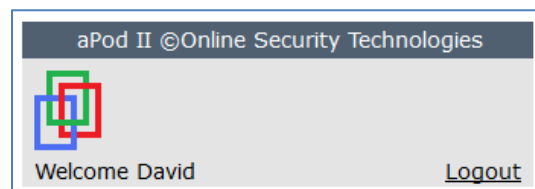
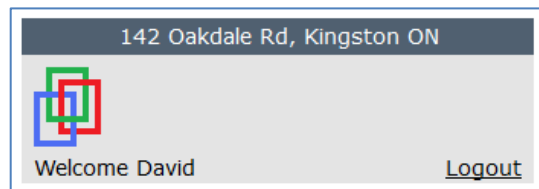
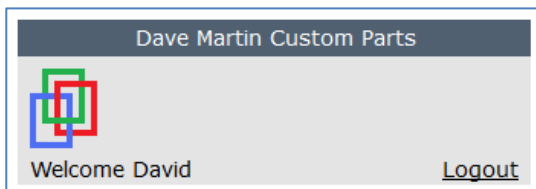
## System Navigation

The aPod II Browser Interface is intuitive and easy to use. Only relevant information is displayed. Many advanced features are turned off by default and when they are turned on additional configuration fields will be activated as needed. Similarly, all functions that are not allowed by an administrator's permission set are hidden.

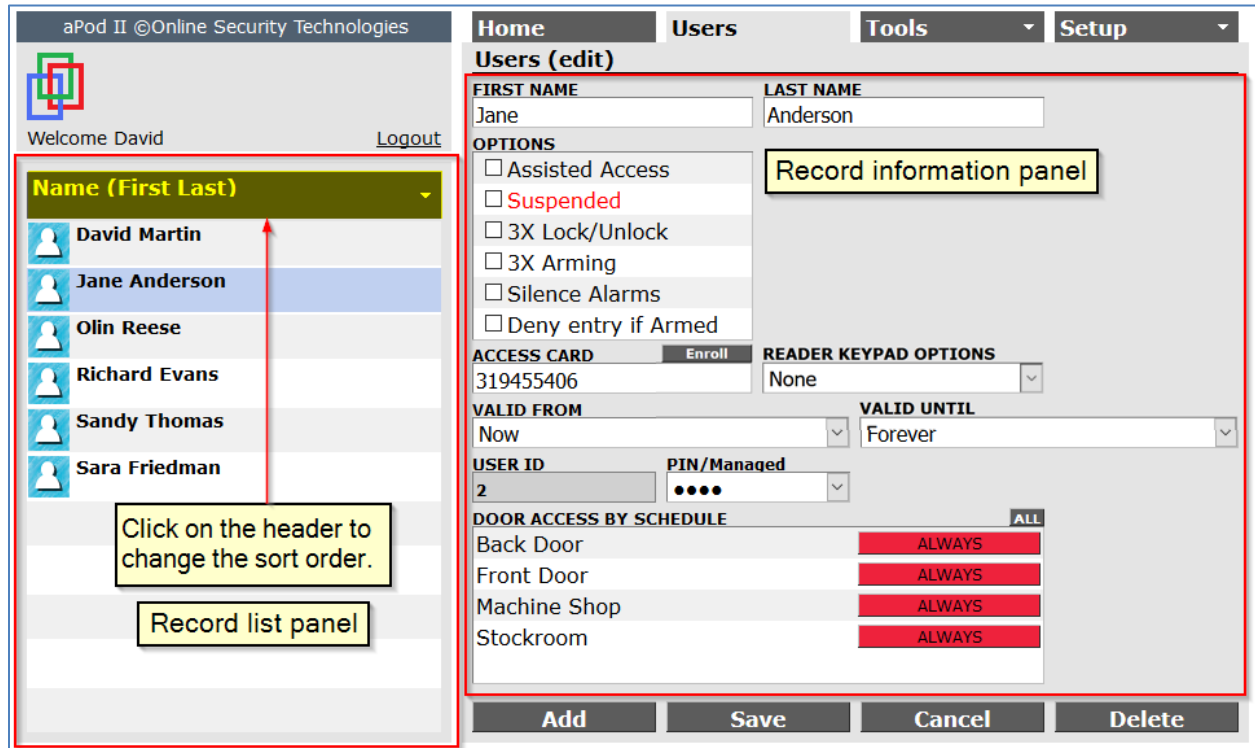
The aPod II Browser Interface is organized into five functional areas. The *header panel* identifies the active administrator and displays a logout link.



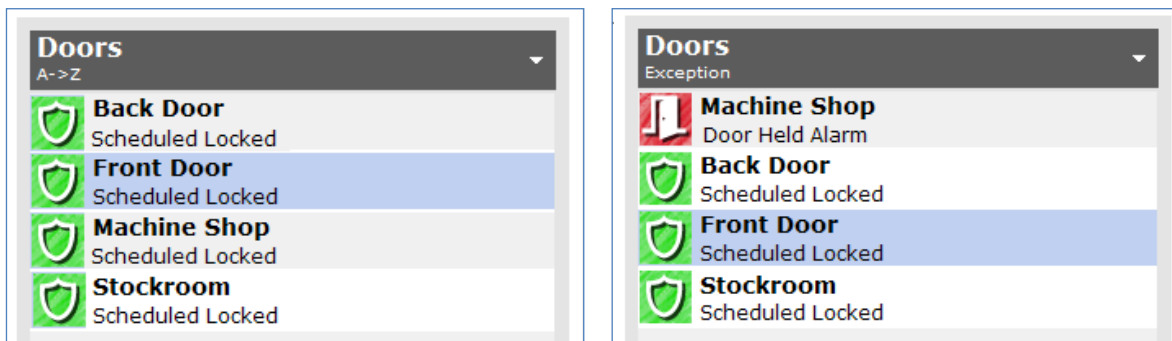
The header displays the system name, the system address, and the product name in a continuous cycle.



Some pages (for example, Doors, Users and Dates) display multiple records. These records are listed in the *record list panel*. Click on any record to highlight it and display its details in the *record information panel* on the right. The *record information panel* is displayed in edit mode by default.



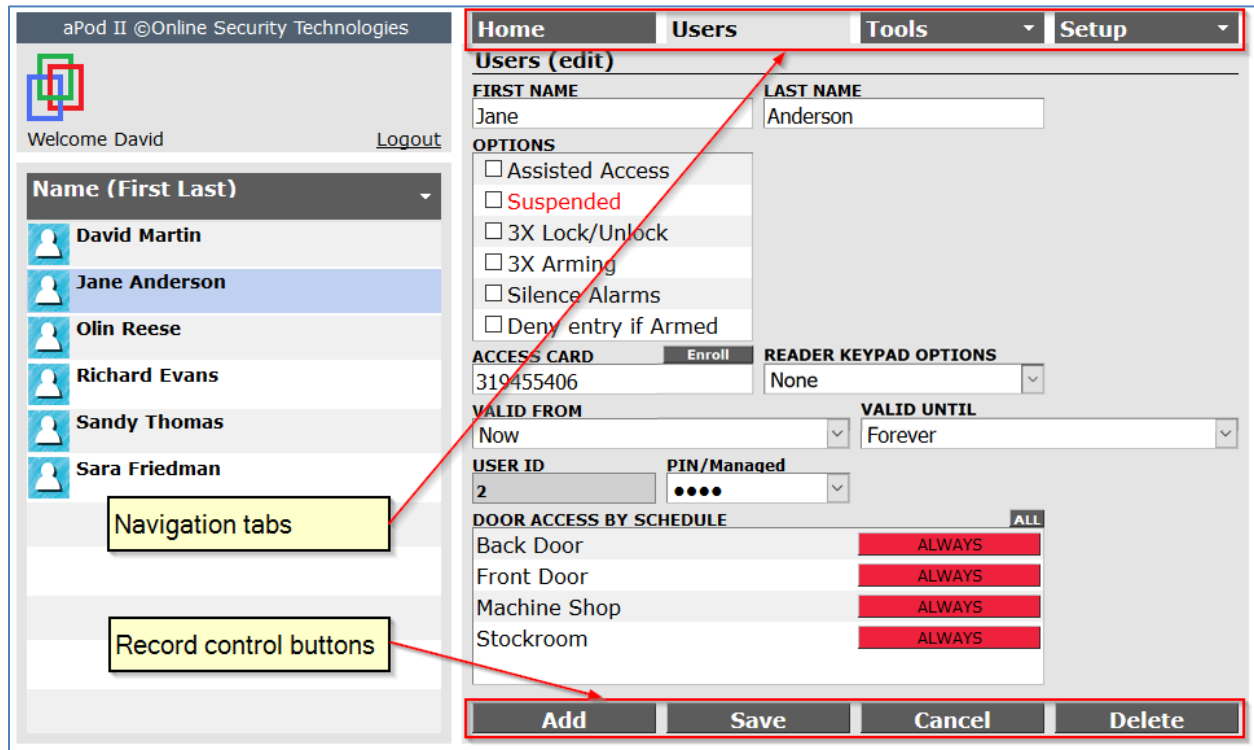
At the top of the *record list panel* is a header which displays the active sort order. Click the header to allow alternative sorts of the list. For example, Doors on the Home page are normally sorted by name. You can sort them by alarm status with doors in alarm on the top and secure doors at the bottom. The sort order for alarm status is listed on page 92.



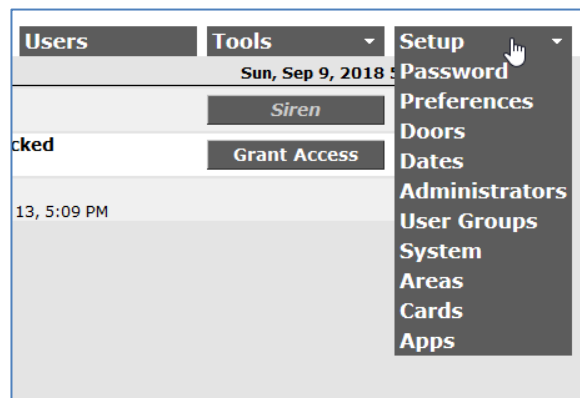
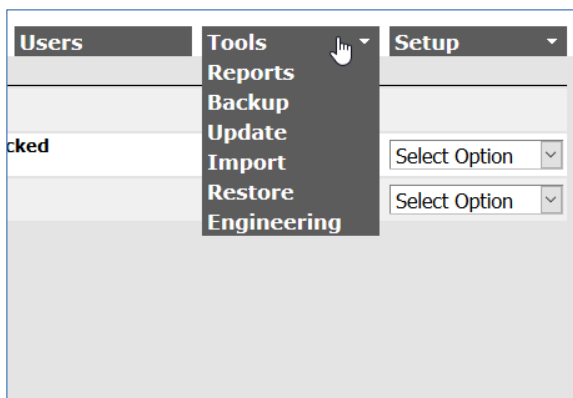
# Online Security Technologies

...security evolution

The system navigation menu is on top of the record information panel. The aPod II Browser Interface will only display menus and submenus that are allowed by the administrator's permission set. The active menu tab is highlighted. The record control buttons are on the bottom of the record information panel.



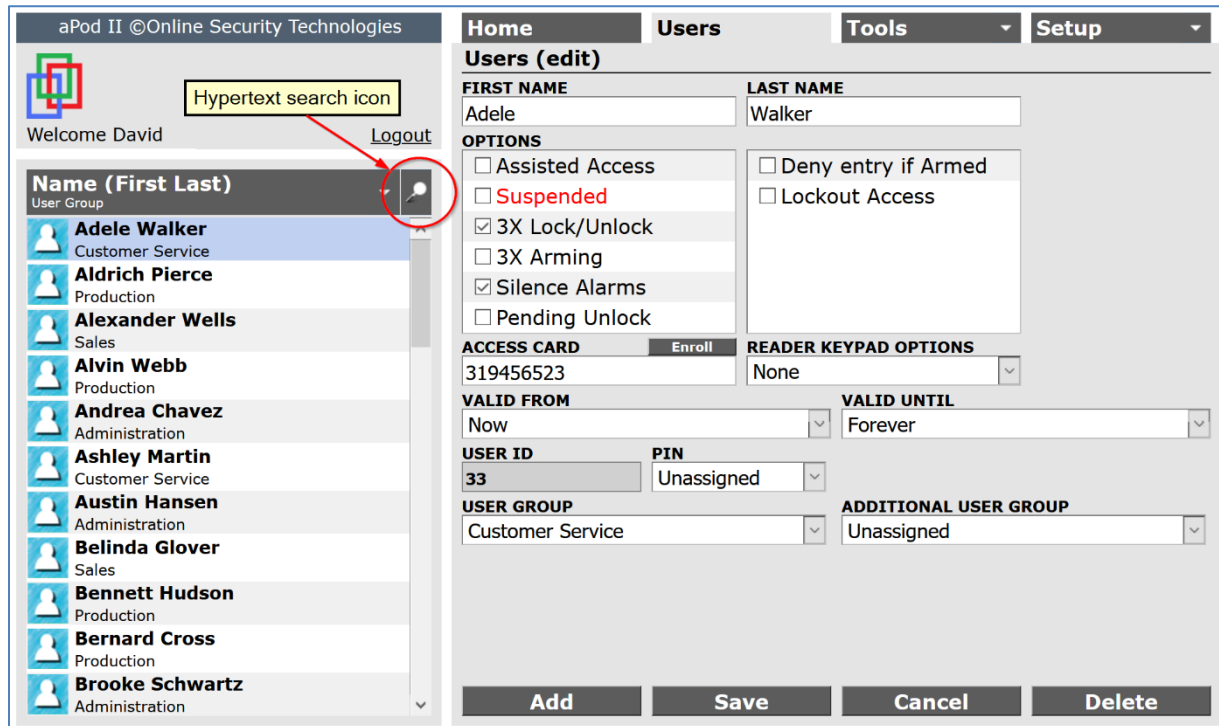
The Tools and Setup tabs display sub-menus which are shown below.



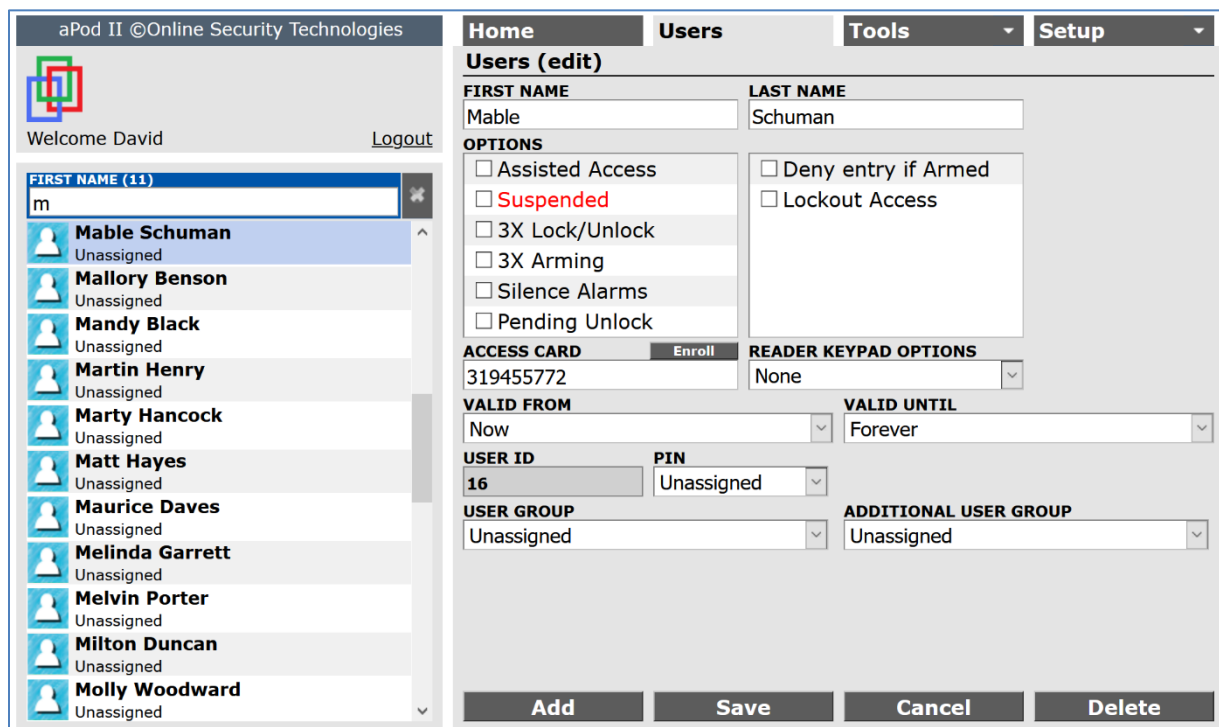


## Hypertext Search

Hypertext search is available on any page that has a record list which exceeds a single page display. Click the search icon to open the search box.



With each text entry the first matching record is displayed.



If a character is entered that creates a string that cannot be matched, the text entry box will flash red three times and then reset the string to its previous matching value. This quickly identifies that the target search is not in the list.

The screenshot shows the 'Users (edit)' interface. On the left, a list of users is displayed with a search bar containing 'mu'. The user 'Mable Schuman' is selected. The main form contains the following fields and options:

- FIRST NAME:** Mable
- LAST NAME:** Schuman
- OPTIONS:**
  - Assisted Access
  - Suspended**
  - 3X Lock/Unlock
  - 3X Arming
  - Silence Alarms
  - Pending Unlock
  - Deny entry if Armed
  - Lockout Access
- ACCESS CARD:** 319455772
- READER KEYPAD OPTIONS:** None
- VALID FROM:** Now
- VALID UNTIL:** Forever
- USER ID:** 16
- PIN:** Unassigned
- USER GROUP:** Unassigned
- ADDITIONAL USER GROUP:** Unassigned

Buttons at the bottom: Add, Save, Cancel, Delete.

**Note:**

There is no hypertext search for access card ID. The owner of a card can be easily determined by badging the card at a reader and then checking the event log.



## Configure and Manage the System

### Administrators

#### Add an Administrator

Administrators configure and manage the aPod II Access Control System through the Browser Interface. The first administrator is assigned by the Quick Start Wizard during the initial system configuration and is automatically given full authority. You can assign additional administrators on the Administrators page under the Setup tab.

The screenshot shows the 'aPod II @Online Security Technologies' web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The 'Setup' dropdown menu is open, showing options like 'Password', 'Preferences', 'Doors', 'Dates', 'Administrators', 'User Groups', 'System', 'Areas', 'Cards', and 'Apps'. The 'Administrators' option is highlighted. The main content area is titled 'Administrators (add)'. It contains the following fields and sections:

- FIRST NAME**: Text input field.
- LAST NAME**: Text input field.
- LOGIN EMAIL ADDRESS**: Text input field.
- PASSWORD**: Text input field with the value 'g8StV95y0e'.
- ADMINISTRATOR PERMISSIONS**: A list of checkboxes for various permissions:
  - Remote Login
  - Manage Users
  - Silence Alarms
  - Bypass Inputs
  - Grant Access
  - Override Door Schedules
  - Run Reports
  - Arm/Disarm Alarm Panel
  - Full Authority
  - Manage Schedules
  - Manage Door Options
  - Manage IP Parameters
  - Manage Administrators
  - Backup the system
  - Restore the system
  - Update Software

At the bottom of the form, there is a yellow box with the text 'Click the Add button to create a new record.' and four buttons: 'Add', 'Save', 'Cancel', and 'Delete'. The 'Add' button is highlighted with a red box.

Enter the administrator's **FIRST NAME** and **LAST NAME**. These are used for identification and are displayed in the audit log. Both names are required and the combined first and last names must be unique.

Enter the **LOGIN EMAIL ADDRESS** for the new administrator. An email address is used for the login ID because it is unique and easy to remember. The **LOGIN EMAIL ADDRESS** will also receive automatic security alerts from the aPod II System if this option is selected.

## Assign a temporary password

A temporary password is generated automatically when you add a new administrator and is valid for 24 hours. Give the login credentials (i.e., the **LOGIN EMAIL ADDRESS** and the temporary password) to the new administrator *who must change their password on the first login*.

The temporary password can only be viewed when first generated. Examining the **PASSWORD** field at a later stage will just show its status, i.e., “Expires (date and time)”, “Unassigned”, “Assigned” or “Expired”.

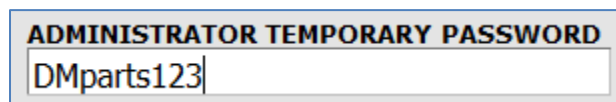
If a temporary password expires or is lost or forgotten, simply repeat the process and generate a new one. A new temporary password is generated every time you click the **Assign Temporary Password** button.

## Custom temporary password

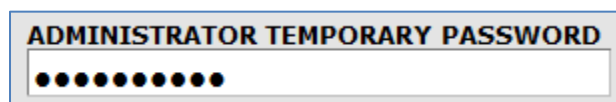
By default, temporary passwords are random strings of ten alphanumeric characters with a mix of uppercase letters, lowercase letters and numerals. The aPod II System allows the creation of a fixed temporary password that is easier to remember but is still unique to your own system.

Use the **ADMINISTRATOR TEMPORARY PASSWORD** field on the System page to enter a strong password. A strong password must have a minimum of 10 characters and at least one uppercase letter, one lowercase letter and one numeric character.

Click on the password field to show the password. Click off the password field to hide the password.



ADMINISTRATOR TEMPORARY PASSWORD  
DMparts123



ADMINISTRATOR TEMPORARY PASSWORD  
●●●●●●●●●●

You may edit or delete the custom temporary password at any time. If you delete the custom temporary password, random passwords will be generated as described above.

System configuration page showing the Administrator Temporary Password field highlighted in red. A callout box indicates: "Create a temporary password that is specific to your system and easy to remember."

<b>SITE NAME</b> David Martin Custom Parts	<b>SITE ADDRESS</b> 142 Oakdale Rd, Kingston ON
<b>TIME ZONE</b> Eastern Time (GMT-5:00)	<b>DAYLIGHT SAVINGS</b> Enabled
<b>CUSTOM APP #1</b> [Empty]	<b>ADD DATES</b> [Add dates]
<b>CUSTOM APP #2</b> [Empty]	
<b>LANGUAGE</b> English (en)	
<b>ACCESS AUTHORIZATION</b> By User Groups	<b>PIN LENGTH</b> 4 Digits
<b>ADMINISTRATOR TEMPORARY PASSWORD</b> DMParts123	<b>PIN STRENGTH</b> Standard
<b>PRIMARY INTERNET IP</b> 64.228.89.95	<b>PORT (UDP)</b> 5268
<b>REMOTE LOGIN SETUP</b> Automatic (DDNS)	<b>ELEVATORS</b> None
<b>PC's DATE/TIME</b> Sun, May 2, 2021 8:25:04 AM	<b>REMOTE HTTP PORT (TCP)</b> 25268
<b>SELECTED LOCALE</b> Ontario	<b>aPod's DATE/TIME</b> Sun, May 2, 2021 8:25:01 AM
	<b>PRIMARY IP ADDRESS</b> 192.168.2.164

The custom temporary password is automatically assigned to a new administrator.

Administrators (add) page showing the Password field highlighted in red. The Assign Temporary Password button is visible. The Administrator Permissions section is checked.

<b>FIRST NAME</b> [Empty]	<b>LAST NAME</b> [Empty]
<b>LOGIN EMAIL ADDRESS</b> [Empty]	
<b>PASSWORD</b> Dmparts123	<b>Assign Temporary Password</b> [Assign Temporary Password]
<b>ADMINISTRATOR PERMISSIONS</b>	
<input checked="" type="checkbox"/> Remote Login	<input checked="" type="checkbox"/> Full Authority
<input checked="" type="checkbox"/> Manage Users	<input checked="" type="checkbox"/> Manage Schedules
<input checked="" type="checkbox"/> Silence Alarms	<input checked="" type="checkbox"/> Manage Door Options
<input checked="" type="checkbox"/> Bypass Inputs	<input checked="" type="checkbox"/> Manage IP Parameters
<input checked="" type="checkbox"/> Grant Access	<input checked="" type="checkbox"/> Manage Administrators
<input checked="" type="checkbox"/> Override Door Schedules	<input checked="" type="checkbox"/> Backup the system
<input checked="" type="checkbox"/> Run Reports	<input checked="" type="checkbox"/> Restore the system
<input checked="" type="checkbox"/> Arm/Disarm Alarm Panel	<input checked="" type="checkbox"/> Update Software

## Assign administrator permissions

It is often necessary to add an administrator with limited authority. By default, new administrators have full authority to manage system functions. Restrict the authority of an administrator by de-selecting the specific permissions.

ADMINISTRATOR PERMISSIONS	
<input checked="" type="checkbox"/> Remote Login	<input checked="" type="checkbox"/> <b>Full Authority</b>
<input checked="" type="checkbox"/> Manage Users	<input checked="" type="checkbox"/> Manage Schedules
<input checked="" type="checkbox"/> Silence Alarms	<input checked="" type="checkbox"/> Manage Door Options
<input checked="" type="checkbox"/> Bypass Inputs	<input checked="" type="checkbox"/> Manage IP Parameters
<input checked="" type="checkbox"/> Grant Access	<input checked="" type="checkbox"/> Manage Administrators
<input checked="" type="checkbox"/> Override Door Schedules	<input checked="" type="checkbox"/> Backup the system
<input checked="" type="checkbox"/> Run Reports	<input checked="" type="checkbox"/> Restore the system
<input checked="" type="checkbox"/> Arm/Disarm Alarm Panel	<input checked="" type="checkbox"/> Update Software

New administrators can add additional administrators if they are given the “Manage Administrators” authority, but they can only assign permissions that they own.

Administrators cannot change their own permissions with one exception. They can change their own “Remote Login” permission if they have “Full Authority” or if they have both the “Manage Administrators” and “Manage IP Parameters” permissions.

The “Restore the System” permission is only available if you have “Full Authority”.

## The Remote Login permission

Enable **REMOTE LOGIN** to allow a new administrator to access the system from the Internet.

**Note:** To make this option functional, the Remote Login feature must be configured. Please refer to page 152 for instructions on how to setup Remote Login.

When all required fields have been configured, save the record.

The screenshot shows the 'Administrators (add)' form in the Online Security Technologies web interface. The form is titled 'Administrators (add)' and is located under the 'Users' tab. The form contains the following fields and options:

- FIRST NAME:** Sara
- LAST NAME:** Friedman
- LOGIN EMAIL ADDRESS:** sara@onlinesecuritytech.com
- PASSWORD:** DMParts123
- ADMINISTRATOR PERMISSIONS:**
  - Remote Login
  - Manage Users
  - Silence Alarms
  - Bypass Inputs
  - Grant Access
  - Override Door Schedules
  - Run Reports
  - Arm/Disarm Alarm Panel
  - Full Authority
  - Manage Schedules
  - Manage Door Options
  - Manage IP Parameters
  - Manage Administrators
  - Backup the system
  - Restore the system
  - Update Software

At the bottom of the form, there are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'. The 'Save' button is highlighted with a red box, and a yellow callout box with an arrow points to it containing the text 'Save the record.'

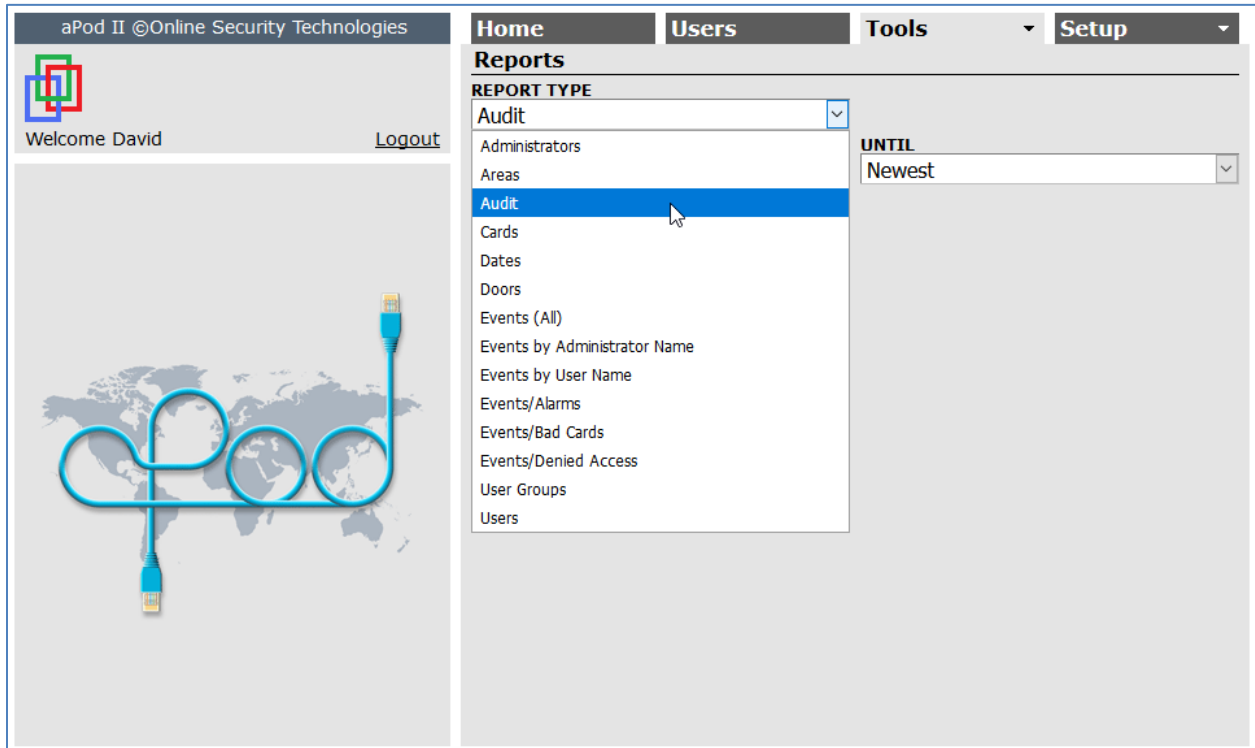
## Edit or Delete an Administrator

Within the restrictions described below, you can change an administrator's information and permissions at any time or delete an administrator.

- Administrators cannot edit or delete their own record.
- Administrators with "Full Authority" can edit or delete the record of any other administrator.
- Administrators with the "Manage Administrators" permission, can edit or delete the record of other administrators with equivalent or lesser authority.

## Audit Logs

The aPod II System tracks all actions taken by an administrator. All configuration changes are captured in the audit log and all control actions are captured in the event log. These logs may be viewed or printed by using the Reports page under the Tools menu.





## Password

Use the [Password](#) page to change your password. Passwords are case sensitive.

Only strong passwords are allowed. Passwords must have a minimum of 10 characters and at least 1 uppercase, 1 lowercase and 1 numeric character.

The screenshot shows the 'aPod II ©Online Security Technologies' web interface. The user is logged in as 'David' and is on the 'Password' page. The page title is 'Password' and it contains the following text: 'Passwords must have a minimum of 10 characters and uppercase, 1 lowercase and 1 numeric character.' Below this text are three password input fields: 'OLD PASSWORD', 'NEW PASSWORD', and 'CONFIRM NEW PASSWORD', each with a masked password of ten dots. A red box highlights a 'Valid password' message in a grey box below the input fields. Below this is a yellow box labeled 'Password status indicator'. At the bottom of the form are 'Save' and 'Cancel' buttons. The left sidebar shows a 'Logout' link and a world map graphic with a blue cable forming the shape of the letters 'OS'. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The 'Setup' dropdown menu is open, showing options like 'Password', 'Preferences', 'Doors', 'Dates', 'Administrators', 'User Groups', 'System', 'Areas', 'Cards', and 'Apps'.

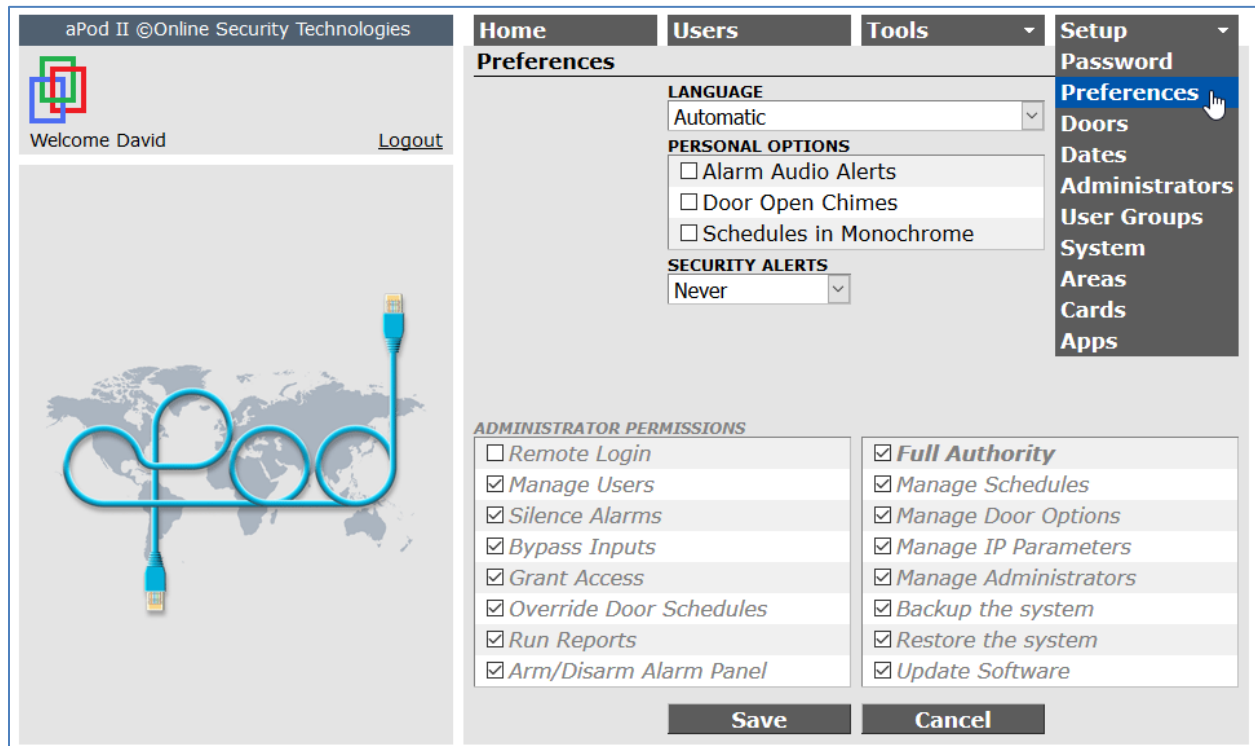
Enter your old password and then enter and confirm your new password. A password status indicator will appear below, showing either:

- Valid password, or
- Invalid password

When you save your new password the Browser display will change to the [Home](#) page.

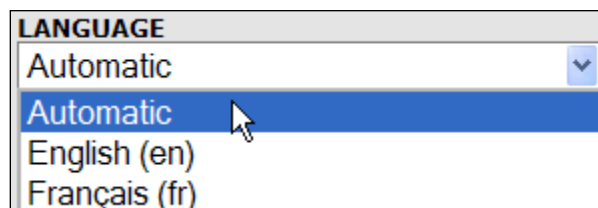
## Preferences

Every administrator can set certain display and system operation options according to their own personal preference. These settings are on the [Preferences](#) page. The default values are shown below.



### The Browser Interface Language

The aPod II System has built-in support for the French language.



'Automatic' is the default language setting. With this selection, the language of the aPod II Browser Interface will be set to the language used by the Browser.

If a specific language is selected, the Browser Interface will always be displayed in that language regardless of the language used by the Browser. When a different language is selected, the Browser Interface will switch to the new language as soon as the change is saved.

## Alarm Audio Alerts

A system alarm will trigger an audio alert on the Administrator's PC when this feature is enabled. This can enhance the reporting of alarms because the reader buzzer is often not loud enough unless you are near the door and a siren may not be installed. Cancelling the system alarm will also cancel the PC alert tone.

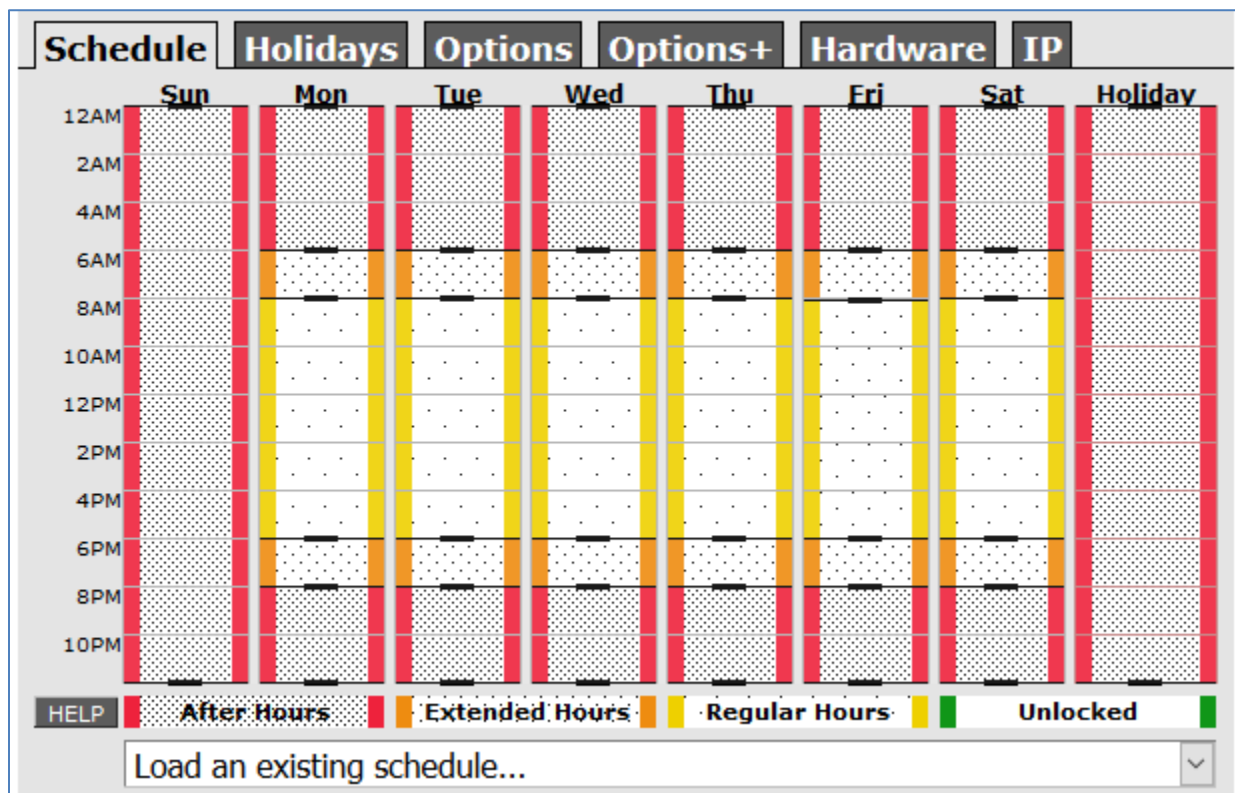
## Door Open Chimes

When this feature is enabled, the opening of a door will trigger door chimes on the Administrator's PC. Door chimes must also be enabled for each door individually on the [Setup](#)→[Doors](#)→[Options](#) page.

## Schedules in Monochrome

The graphical scheduling in the aPod II System uses colors to distinguish intervals with different 'locked states' and required levels of access authority. This makes it easy to view and understand the entire weekly schedule on a single display. Select the 'Schedules in Monochrome' option to augment the color scheme with background patterns.

The background patterns would improve the scheduling display for anyone that has a degree of color blindness in their vision. This option is turned off by default.

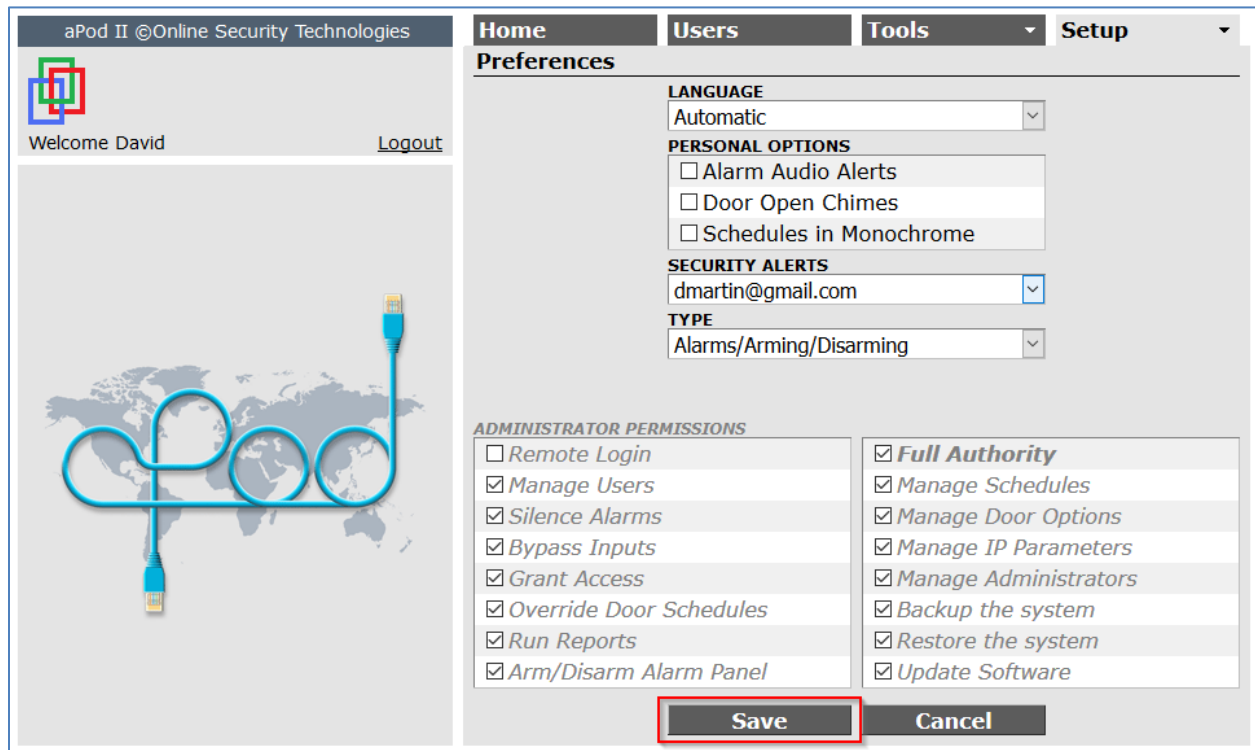


## Enable Email Security Alerts

The aPod II Access Control System can email security alerts to administrators if they choose to receive them. Alerts are sent to the administrator's **LOGIN EMAIL ADDRESS**. A security alert is transmitted when the system detects an alarm condition. This would include events such as 'door forced open', 'door held open', 'input point alarm' or 'system tamper alarm'.

If an alarm panel interface has been installed the aPod II System can send an alert whenever the panel is armed or disarmed. Alerts for arming and disarming are optional and can be configured using the **TYPE** drop-down list. This setting is only displayed if an alarm panel interface is configured, and security alerts are enabled.

Save the record when you have configured the administrator preferences.



## Doors

There are many options for configuring the operation of your aPod II door controller. The configuration options are divided into tabs on the Doors page which is accessed from the Setup menu. The settings that an administrator can access will depend on their administrator permissions as described on page 21. The Hardware and IP configurations are described in the Advanced Options section on page 85.

Click **Add** to create a record for a new door. Edit the **DOOR NAME** field and click **Save**.

Select the door of interest from the list on the left and then navigate to the various options using the configuration tabs.

The screenshot displays the 'Doors (edit)' configuration page in the aPod II web interface. On the left, a 'Door selection list' contains four entries: 'Back Door', 'Front Door', 'Machine Shop', and 'Stockroom'. The 'Front Door' entry is selected. The main area shows the 'Doors (edit)' form with the 'DOOR NAME' field set to 'Front Door'. Below the form are configuration tabs: 'Schedule', 'Holidays', 'Options', 'Options+', 'Hardware', and 'IP'. The 'Schedule' tab is active, showing a grid with time slots from 12AM to 10PM and days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday). The grid indicates 'After Hours' (red) for most days, 'Regular Hours' (yellow) for Monday through Friday, and 'Unlocked' (green) for Monday through Friday. A legend at the bottom identifies the colors: red for After Hours, orange for Extended Hours, yellow for Regular Hours, and green for Unlocked. There is a 'Load an existing schedule...' dropdown and buttons for 'Add', 'Save', 'Cancel', and 'Delete' at the bottom.

Click **Delete** to delete a record. The aPod II system will not allow you to delete the record for the Primary Controller.

## Schedules

The Schedule tab on the Doors page is a graphical representation of the setting of the door lock status on a weekly basis. You modify this schedule to create time intervals for which the aPod II controller will automatically lock or unlock the door, or for locked doors, restrict access for some Users but not others.

### Modify the door locking schedule

Modify the schedule for one or more days by using your mouse “click and drag” functions and then click **Save**. Hover over a time interval to display the start/stop times.

The screenshot displays the 'aPod II @Online Security Technologies' web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The main content area is titled 'Doors (edit)' and shows the 'Front Door' selected. A sidebar on the left lists other doors: 'Back Door', 'Front Door', 'Machine Shop', and 'Stockroom'. The central 'Schedule' tab is active, showing a weekly grid from Sunday to Saturday. The vertical axis represents time from 12AM to 10PM. The grid is divided into colored vertical bars representing different access states: red for 'After Hours', orange for 'Extended Hours', yellow for 'Regular Hours', and green for 'Unlocked'. A mouse cursor is hovering over a green bar on Tuesday, with a tooltip displaying '9:00AM..6:00PM'. A yellow callout box with a red arrow points to the tooltip, containing the text: 'Hover over the time interval to display the start/stop times.' Below the grid is a legend for the colors and a dropdown menu for 'Load an existing schedule...'. At the bottom are buttons for 'Add', 'Save', 'Cancel', and 'Delete'.

Create a time interval by dragging down one of the pulsing bars on the top edge or by dragging up one of the pulsing bars on the bottom edge. (The drag operation is click, hold, move, and release.) When you hover over the edge bar, the cursor will change to an up/down arrow cursor to indicate that you have captured the edge. As you drag the edge, the time defined by its location will be displayed beside the cursor. This will allow you to precisely define a scheduling interval in 5-minute increments. Use this same technique to modify intervals. Drag an edge off the column to delete an interval. You can create up to seven intervals per day.

Drag edge bars to desired start and stop locations for time intervals.

Edge bars

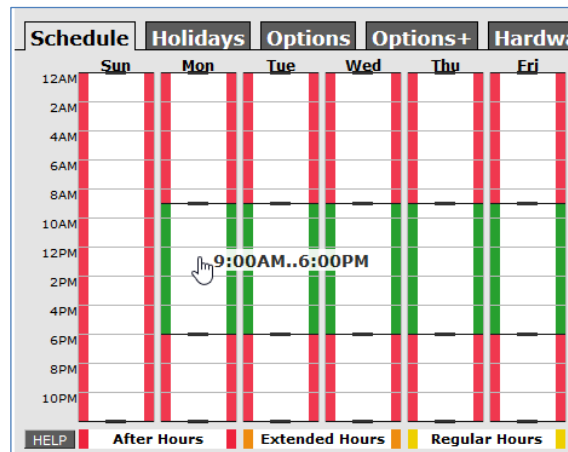
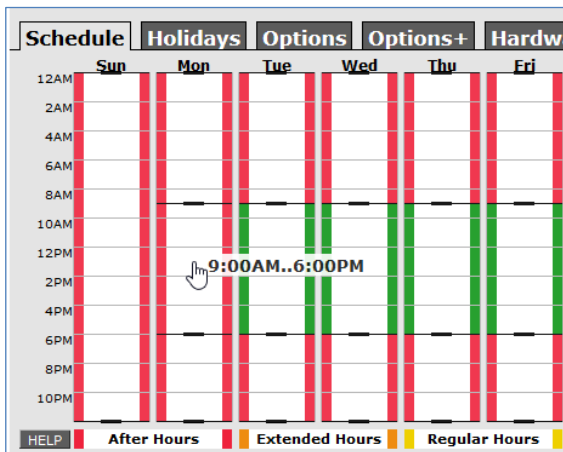
9:00AM

HELP After Hours Extended Hours Regular Hours Unlocked

Load an existing schedule...

Add Save Cancel Delete

Clicking an interval area will rotate its lock status through available options.



## Weekdays, weekends, and holidays

The schedules configured for the five weekdays and two weekend days will repeat every week. The schedules configured for holidays will be activated for any day of the week that is pre-defined as a holiday. When your locale was selected in the Quick Start Wizard during the initial system set up, the aPod II system pre-configured all the statutory holidays for your jurisdiction in a perpetual calendar. There is no need to designate any specific day as a holiday.

The selected holidays are listed under the Doors→Holidays tab. Refer to page 39 for more information about the Holidays page. You can edit the list of holidays on the Dates page which is described on page 61 .

The screenshot displays the 'Doors (edit)' configuration page for the 'Front Door'. The 'Holidays' tab is selected, showing a grid of the door's schedule. The grid has columns for each day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and a 'Holiday' column. The time slots range from 12AM to 10PM. The schedule is color-coded: red for 'After Hours', orange for 'Extended Hours', yellow for 'Regular Hours', and green for 'Unlocked'. The 'Holiday' column is currently empty. A callout box points to the 'Holiday' column with the text: 'The schedule configured in the 'Holiday' column will be activated on days listed under the 'Holidays' tab.'

## Daylight Savings Time

Your schedules will automatically be adjusted for Daylight Savings Time. When your locale was selected in the Quick Start Wizard during the initial system set up, the aPod II system pre-configured Daylight Savings Time for your jurisdiction in a perpetual calendar.

If the rules for Daylight Savings Time change in your jurisdiction, you can edit the DST dates as described on page 65.



## Automatic locking and unlocking

When a 'door locked' schedule begins the door will always lock automatically and immediately. You have several options to configure the way a door will unlock when a 'door unlocked' schedule begins. The default option is 'Pending next Entry'. With this option the door will remain locked after the start of the unlock schedule until someone opens the door with a valid token. This ensures that an automatic unlock schedule will not compromise the security of your premises. For more information, refer to the Scheduled Unlock section under [Doors](#)→[Options](#) on page 44.

## Replicating door schedules

When a door schedule is created in the aPod II System it is added to a library of schedules and can be selected for use on any other door. Once selected, it can be modified for minor changes if required. This simplifies the process of setting up door schedules in a multi-door system.

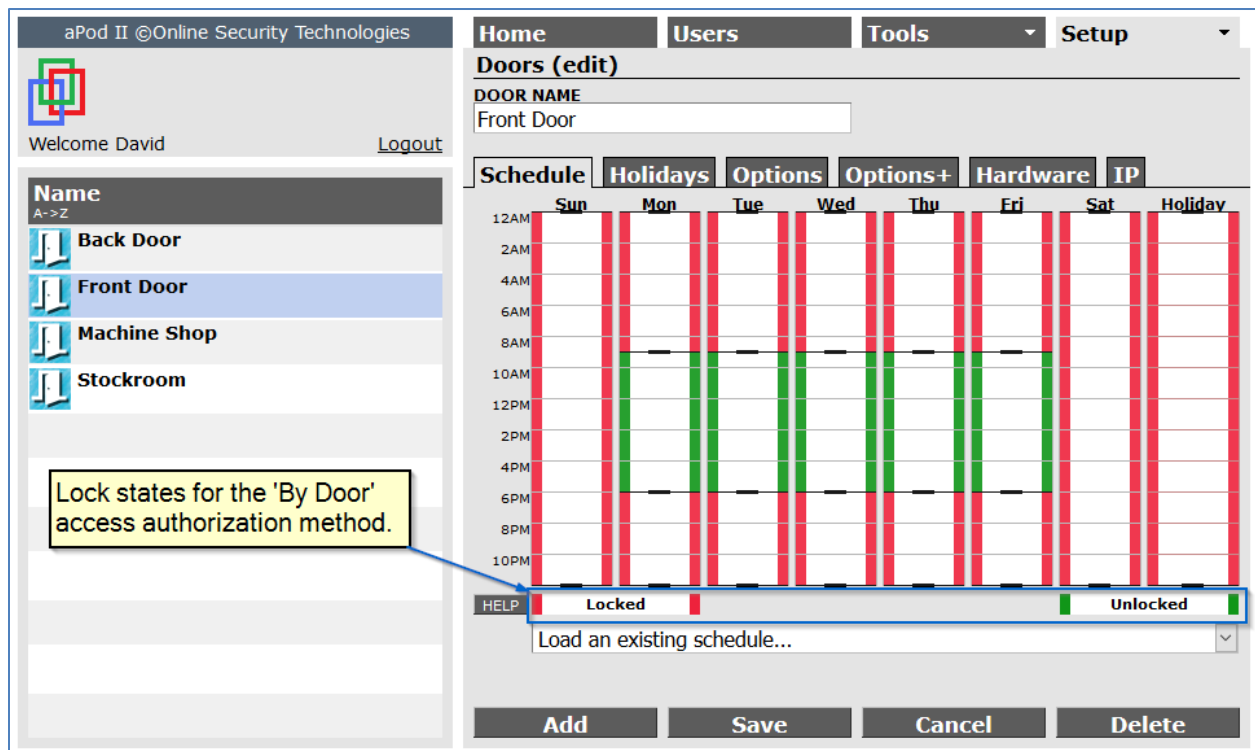
The schedule selection list includes several pre-set schedules in addition to the schedules created by Administrators.

The screenshot shows the 'aPod II ©Online Security Technologies' interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The main title is 'Doors (edit)'. Below this, there is a 'DOOR NAME' field containing 'Front Door'. The interface is divided into several tabs: 'Schedule', 'Holidays', 'Options', 'Options+', 'Hardware', and 'IP'. The 'Schedule' tab is active, displaying a calendar grid with time slots from 12AM to 10PM. The grid shows a schedule for the 'Front Door' with red bars indicating locked periods and green bars indicating unlocked periods. A legend at the bottom of the grid identifies the colors: red for 'After Hours', orange for 'Extended Hours', yellow for 'Regular Hours', and green for 'Unlocked'. A dropdown menu is open, showing a list of available schedules. A red arrow points from a yellow box labeled 'Schedule selection list' to the dropdown menu. The dropdown menu includes options like 'Load an existing schedule...', 'Locked', 'M-F 8AM-6PM', 'M-F 6AM-|-|-7PM', 'M-F 6AM-|-|-7PM', and options to replicate the schedule from other doors like 'Back Door', 'Machine Shop', and 'Stockroom'.

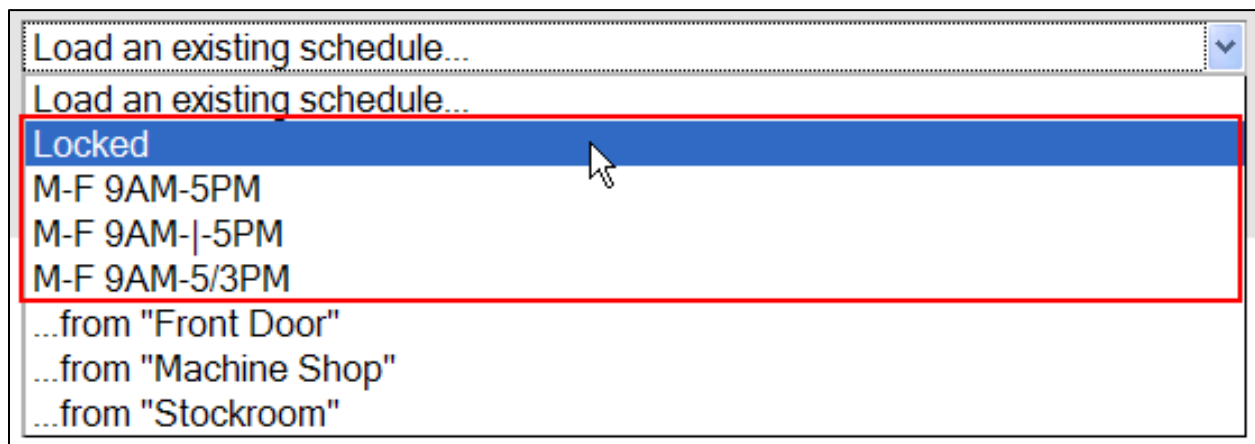
## Schedule with the 'By Door' Access Authorization Method

There are three available methods for assigning access permissions to Users (cardholders). The most appropriate method will depend on the size and complexity of your access control system. These methods are described in detail in the Assign Access Permissions chapter on page 128. The method that you choose will affect your options for configuring a door schedule.

When the default and simplest access authorization method (By Door) is configured, there are only two possible lock states, that is "Locked" and "Unlocked".



There are four pre-set unlock schedules available.



## Always locked ("Locked") – the default schedule

The screenshot shows the 'Doors (edit)' interface for the 'Front Door'. The 'DOOR NAME' field contains 'Front Door'. The 'Schedule' tab is active, displaying a grid where all cells are red, indicating the door is locked. The grid has columns for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday, and rows for times from 12AM to 10PM. A legend at the bottom shows a red bar for 'Locked' and a green bar for 'Unlocked'. A dropdown menu is set to 'Load an existing schedule...'. Buttons for 'Add', 'Save', 'Cancel', and 'Delete' are at the bottom.

## Monday to Friday, 9 a.m. to 5 p.m. ("M-F 9AM-5PM")

The screenshot shows the 'Doors (edit)' interface for the 'Front Door'. The 'DOOR NAME' field contains 'Front Door'. The 'Schedule' tab is active, displaying a grid where the cells for Monday through Friday between 9AM and 5PM are green, indicating the door is unlocked. All other cells are red, indicating the door is locked. The grid has columns for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday, and rows for times from 12AM to 10PM. A legend at the bottom shows a red bar for 'Locked' and a green bar for 'Unlocked'. A dropdown menu is set to 'Load an existing schedule...'. Buttons for 'Add', 'Save', 'Cancel', and 'Delete' are at the bottom.

Monday to Friday, 9 a.m. to 5 p.m., locked during the lunch hour ("M-F 9AM-|-5PM")

The screenshot shows the 'Doors (edit)' configuration page for 'Front Door'. The 'Schedule' tab is active, displaying a grid from 12AM to 10PM. The door is locked (red) from 12AM to 9AM and from 5PM to 10PM. It is unlocked (green) from 9AM to 12PM and from 12PM to 5PM, with a red bar at 12PM indicating a lunch break. The interface includes a sidebar with door names, a top navigation bar, and buttons for 'Add', 'Save', 'Cancel', and 'Delete'.

Weekends included ("M-F 9AM-5/3PM")

The screenshot shows the 'Doors (edit)' configuration page for 'Front Door' with the 'Weekends included' schedule. The 'Schedule' tab is active, displaying a grid from 12AM to 10PM. The door is locked (red) from 12AM to 9AM and from 5PM to 10PM on all days. It is unlocked (green) from 9AM to 5PM on all days, including weekends. The interface includes a sidebar with door names, a top navigation bar, and buttons for 'Add', 'Save', 'Cancel', and 'Delete'.

## Schedule with the 'Door by Schedule' or 'By User Groups' Access Authorization Methods

Four lock states are available when the 'Door by Schedule' or the 'By User Groups' access authorization methods are configured. In addition to 'Unlocked' there are three states for a locked door which are defined by 'Regular Hours', 'Extended Hours' and 'After Hours'. These time-oriented states allow you to program *when* a User is allowed access through a locked door. For example, an employee may be allowed to access the workplace through a back door during normal business hours but would not be granted access on the weekend.

Create time intervals to define after hours, extended hours, and regular hours for the time that a door will remain locked. You can then restrict access by Users to the appropriate schedule by assigning the 'After Hours', 'Extended Hours' or 'Regular Hours' privilege to their cards. This is accomplished on the Users page which is discussed later in the guide. Refer to page 128.

The time-oriented lock states have cumulative access permissions. If a User has 'After Hours' access permission, they automatically have 'Extended Hours' access permission. Similarly, if a User has 'Extended Hours' access permission, they automatically have 'Regular Hours' access permission.

The screenshot displays the 'Doors (edit)' interface. On the left, a list of doors includes 'Back Door', 'Front Door', 'Machine Shop', and 'Stockroom'. The 'Front Door' is highlighted. A yellow callout box points to the legend at the bottom of the schedule grid, containing the text: 'Lock states for the 'Door by Schedule' and the 'User Groups' access authorization methods.'

Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday
12AM	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours
2AM	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours
4AM	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours
6AM	After Hours	Extended Hours	Extended Hours	Extended Hours	Extended Hours	Extended Hours	After Hours	After Hours
8AM	After Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	After Hours	After Hours
10AM	After Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	After Hours	After Hours
12PM	After Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	After Hours	After Hours
2PM	After Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	After Hours	After Hours
4PM	After Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	Regular Hours	After Hours	After Hours
6PM	After Hours	Extended Hours	Extended Hours	Extended Hours	Extended Hours	Extended Hours	After Hours	After Hours
8PM	After Hours	Extended Hours	Extended Hours	Extended Hours	Extended Hours	Extended Hours	After Hours	After Hours
10PM	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours	After Hours

Legend: After Hours (red), Extended Hours (orange), Regular Hours (yellow), Unlocked (green)

As with the simpler, 'By Door' access authorization method, pre-configured templates are available to assist in setting up the door schedules.

## Always locked ("Locked") – the default schedule

The screenshot shows the 'Doors (edit)' interface for the 'Front Door'. The 'DOOR NAME' is 'Front Door'. The 'Schedule' tab is active, displaying a grid with columns for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and a 'Holiday' column. The rows represent time slots from 12AM to 10PM. All cells in the grid are colored red, indicating the door is 'Always locked'. A legend at the bottom identifies the colors: red for 'After Hours', orange for 'Extended Hours', yellow for 'Regular Hours', and green for 'Unlocked'. A dropdown menu shows 'Load an existing schedule...'. Buttons for 'Add', 'Save', 'Cancel', and 'Delete' are at the bottom.

## Business hours for most employees ("M-F 8AM-6PM")

The screenshot shows the 'Doors (edit)' interface for the 'Front Door'. The 'DOOR NAME' is 'Front Door'. The 'Schedule' tab is active, displaying a grid with columns for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and a 'Holiday' column. The rows represent time slots from 12AM to 10PM. The grid shows a schedule where the door is 'Always locked' (red) on all days from 12AM to 8AM and from 6PM to 10PM. From 8AM to 6PM, the door is 'Regular Hours' (yellow) on Monday through Friday, and 'After Hours' (red) on Saturday and Sunday. A legend at the bottom identifies the colors: red for 'After Hours', orange for 'Extended Hours', yellow for 'Regular Hours', and green for 'Unlocked'. A dropdown menu shows 'Load an existing schedule...'. Buttons for 'Add', 'Save', 'Cancel', and 'Delete' are at the bottom.

Unlocked during business hours plus early and late intervals ("M-F 6AM-I-I-7PM")

The screenshot shows the 'Doors (edit)' interface for the 'Front Door'. The 'Schedule' tab is active, displaying a grid with time slots from 12AM to 10PM and days from Sun to Sat. The legend indicates: After Hours (red), Extended Hours (orange), Regular Hours (yellow), and Unlocked (green). The schedule shows 'Unlocked' status from 6AM to 7PM on Monday through Friday, with 'Extended Hours' (yellow) from 6AM to 8AM and 6PM to 7PM. 'After Hours' (red) covers the rest of the time slots. A legend at the bottom identifies the colors: After Hours (red), Extended Hours (orange), Regular Hours (yellow), and Unlocked (green). A dropdown menu below the legend contains the text 'Load an existing schedule...'. Buttons for 'Add', 'Save', 'Cancel', and 'Delete' are at the bottom.

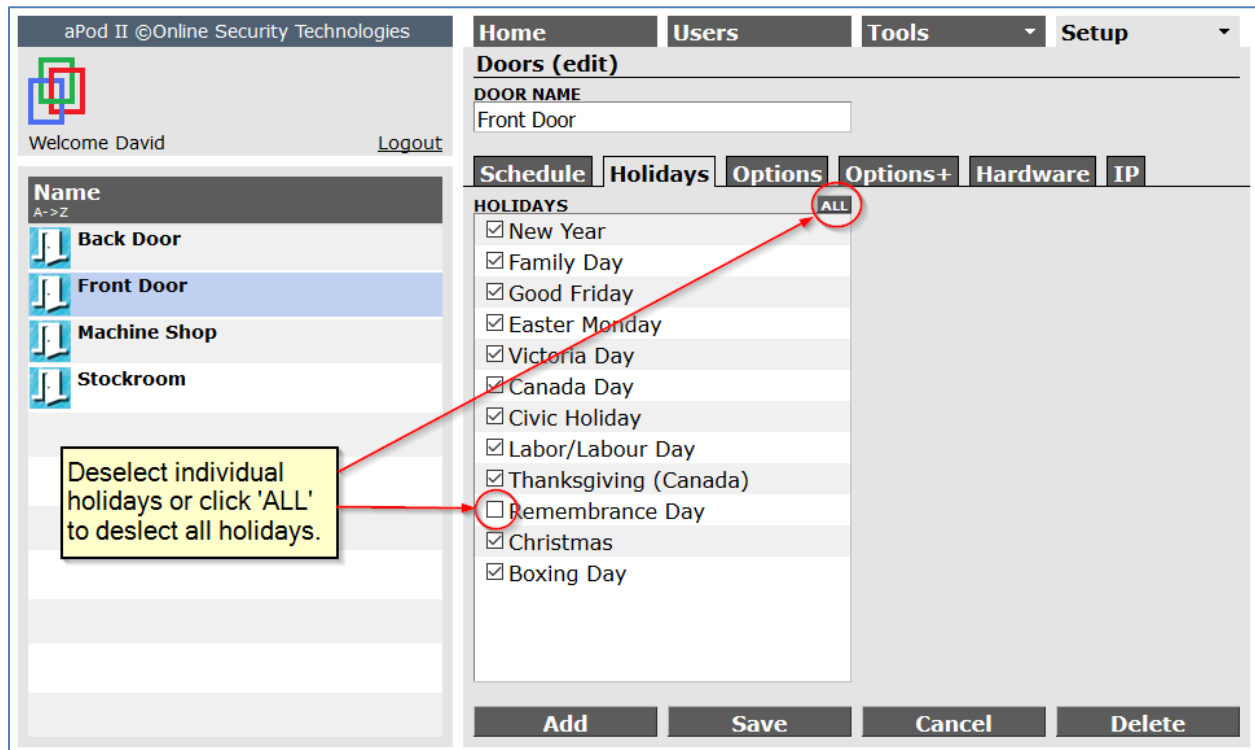
Unlocked during business hours plus early, late and lunch intervals ("M-F 6AM-I-I-I-7PM")

The screenshot shows the 'Doors (edit)' interface for the 'Front Door'. The 'Schedule' tab is active, displaying a grid with time slots from 12AM to 10PM and days from Sun to Sat. The legend indicates: After Hours (red), Extended Hours (orange), Regular Hours (yellow), and Unlocked (green). The schedule shows 'Unlocked' status from 6AM to 7PM on Monday through Friday, with 'Extended Hours' (yellow) from 6AM to 8AM and 6PM to 7PM. A lunch interval is shown as a gap in the 'Unlocked' status from 12PM to 1PM. 'After Hours' (red) covers the rest of the time slots. A legend at the bottom identifies the colors: After Hours (red), Extended Hours (orange), Regular Hours (yellow), and Unlocked (green). A dropdown menu below the legend contains the text 'Load an existing schedule...'. Buttons for 'Add', 'Save', 'Cancel', and 'Delete' are at the bottom.

## Holidays

When your locale was selected in the Quick Start Wizard during the initial system setup, the aPod II system pre-configured all possible statutory holidays for your jurisdiction in a perpetual calendar. The selected holidays are listed under the Doors - Holidays tab and are sorted according to their calendar dates. You can edit this list on the Dates page. Please refer to page 61.

For any selected holiday, the holiday schedule defined on the Schedule tab will automatically be activated.



Check any holiday to select/deselect it or click the **ALL** button to select/deselect all holidays.

### Important notes:

Each door is assigned its own holiday schedule. You should review and edit the list of holidays for any door whose lock schedule on a holiday is different from its normal lock schedule.

The aPod II System will display a message to alert you to an upcoming holiday when you first login to the Browser Interface. The message is displayed three days prior to the holiday and finally, on the day of the holiday.



## Options

A door under electronic access control is a major component in your building's security system but it must also be convenient and easy to use. The aPod II system provides many options which allow you to optimize the operation of the door for your circumstances.

The screenshot shows the aPod II web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The main content area is titled 'Doors (edit)' and shows the configuration for the 'Front Door'. The 'Options' tab is selected, displaying various settings:

ALARM DURATION	UNLOCK DURATION	EXTENDED UNLOCK	DOOR OPEN CHIMES
1 minute	5 seconds	+3 seconds	Disabled

Other settings include:

- DOOR FORCED PROCESSING: None
- DOOR HELD OPEN PROCESSING: None
- SCHEDULED UNLOCK: Pending next Entry
- CARD+PIN MODE: Never Required
- ID+PIN MODE: Never Allowed
- DUAL CUSTODY MODE: Never Required

Buttons at the bottom include 'Add', 'Save', 'Cancel', and 'Delete'. A sidebar on the left lists other doors: Back Door, Front Door (selected), Machine Shop, and Stockroom.

### Alarm annunciation

The aPod II door controller will turn on the buzzer in the access reader to annunciate alarms. You can also connect a siren to the controller for a much louder alarm signal which may be appropriate for a high security door.

Use the **ALARM DURATION** drop-down list to choose how long the siren will sound in the event of an alarm if it is not manually cancelled. The default is 1 minute. It can be set to as little as 15 seconds and as long as 15 minutes.

The image shows a close-up of the 'ALARM DURATION' drop-down menu. The menu is open, showing a list of options:

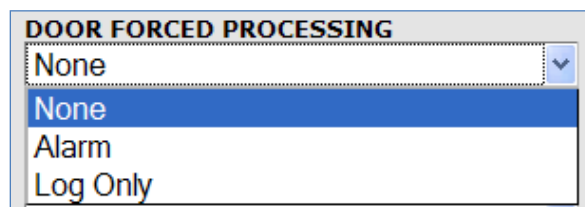
- 15 seconds
- 20 seconds
- 30 seconds
- 45 seconds
- 1 minute (highlighted)
- 90 seconds
- 2 minutes
- 3 minutes
- 5 minutes
- 8 minutes
- 10 minutes
- 15 minutes

## Door Forced alarms

The 'door forced' alarm is generated when the 'door open' signal is tripped without a 'door unlock' command from the aPod II door controller. This might occur for example, if someone opens a locked door with a key rather than their access token or if someone turns the knob and exits without using a Request to Exit device. It might also mean that someone has forced the door and broken into your facility.

'Door forced' alarms are not generated when a door is unlocked. If a door contact is not installed 'door forced' alarms cannot be detected.

Use the **DOOR FORCED PROCESSING** drop-down list to choose one of the following options.



The **DOOR FORCED PROCESSING** options are described below.

- **None** – 'Door forced' alarm conditions are ignored. This is the default.
- **Alarm** – The alarm will sound, and the event will be recorded in the event log.
- **Log Only** – The alarm will not sound but the event will be recorded in the event log.

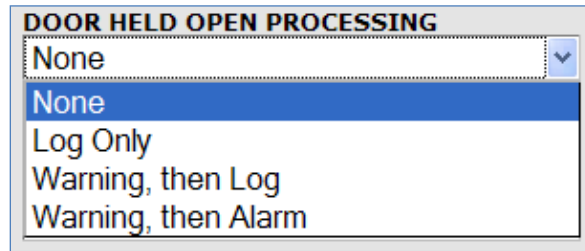
Leave 'door forced' alarms turned off if the door is monitored by an intrusion detection system. In this circumstance, you will avoid nuisance alarms and true alarms will be managed by the intrusion detection system when it is armed, and no one is in the facility.

## Door Held Open alarms

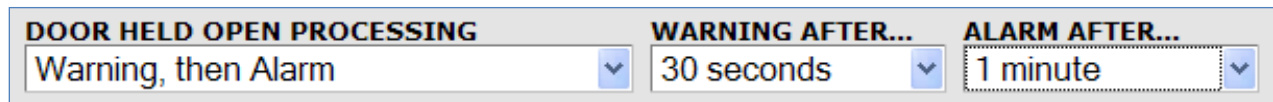
A 'door held open' event is triggered when a door is not closed within a reasonable period after the door has been opened. Normally a locked door should not be held open because this would compromise the security of your facility.

'Door held open' alarms are not generated when a door is unlocked. If a door contact is not installed 'door held open' alarms cannot be detected.

You can customize the way the aPod II door controller responds to a 'door held open' condition. Use the **DOOR HELD OPEN PROCESSING** drop-down list to choose one of the following options.



If you select an option other than 'None' two additional drop-down lists appear which allow you to configure the **WARNING AFTER...** delay and the **ALARM AFTER...** delay.



The **WARNING AFTER...** delay is the time that must elapse after the door has been held open before the access reader buzzer sounds a warning. The default setting is 30 seconds. The **WARNING AFTER...** timer begins when the door unlock cycle has ended.

The **ALARM AFTER...** delay is the time that the warning buzzer will sound before the 'door held open' alarm is recorded and if configured, the siren is activated. The default setting is 1 minute.

**Note:** Closing the door will cancel the warning buzzer but not the Siren if it has already been activated. Refer to page 93 for information about turning off the Siren.

The **DOOR HELD OPEN PROCESSING** options are described below.

- **None** – If the door is held open, the aPod II controller will ignore it. This is the default.
- **Log Only** – The alarm event is logged but no warning buzzer or siren will sound.
- **Warning, then Log** – If the door is held open for the time set in the **WARNING AFTER...** field, the aPod II controller will pulse the reader buzzer to sound a warning. After a second delay, as set in the **ALARM AFTER...** field, the alarm event is logged but the siren will not sound.
- **Warning, then Alarm** – If the door is held open for the time set in the **WARNING AFTER...** field, the aPod II controller will pulse the reader buzzer to sound a warning and then after a second delay as set in the **ALARM AFTER...** field, it will turn on the siren.

**Note:** If a door is held open when the door is unlocked, there will be no 'door held open' event. If the door is re-locked, as would occur at the end of an unlock schedule for example, and the door is left open, a 'door held open' event will be processed according to the selected configuration.

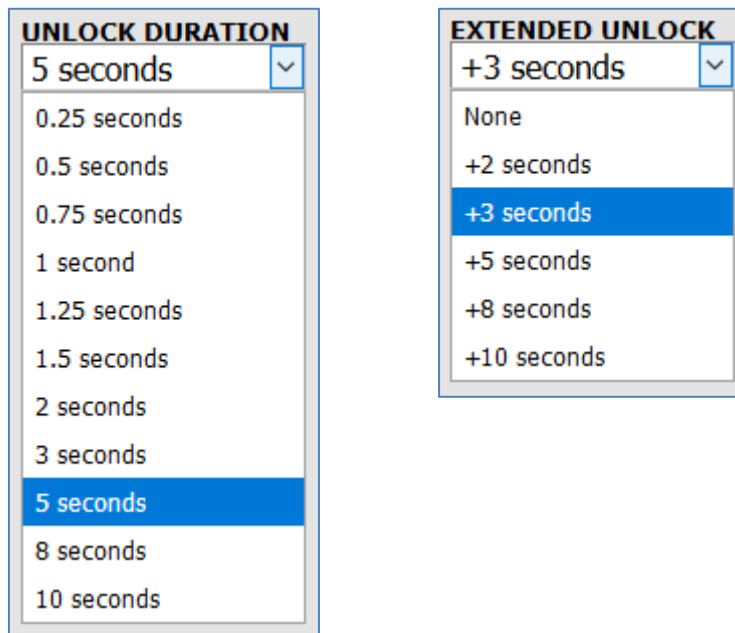
## The unlock operation

Use the **UNLOCK DURATION** drop-down list to choose how long the door will remain unlocked after the unlock command is triggered by a valid credential or a Request-To-Exit device. The default is 5 seconds but can range from 0.25 seconds to 10 seconds. Short unlock times may be required when interfacing a turnstile.

Use the **EXTENDED UNLOCK** drop-down list to configure additional unlock time for users who may require it. You assign this attribute by selecting the 'Assisted Access' option on the Users page. Refer to page 112. The default is +3 seconds.

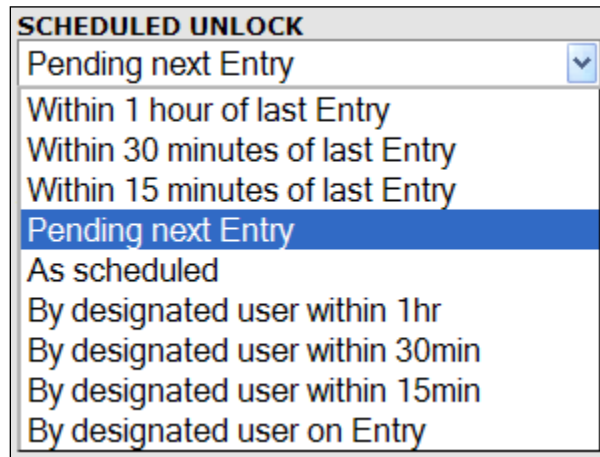
Total unlock time is **UNLOCK DURATION + EXTENDED UNLOCK**.

**Note:** The extended unlock time is also used when granting access. Please refer to page 94.



## Scheduled unlock

When a 'door locked' schedule begins the door will always lock automatically and immediately. You have several options to configure the way a door will unlock when a 'door unlocked' schedule begins.



- **Pending next Entry** – The door will remain locked after the start of the unlock schedule until someone opens the door with a valid token, or the door is unlocked by clicking the **Grant Access** button on the Home page. This ensures that an automatic unlock schedule will not compromise the security of your premises. *This is the default option.*
- **As scheduled** – The door will unlock immediately at the start of the unlock schedule. This would be appropriate where there is always someone present, for example, a security guard or if the door is used by visitors or customers and allows access to a common area of the building.
- **Within 1 hour (or 30 minutes, or 15 minutes) of last Entry** – These options are similar in operation to the **Pending next Entry** option but will also unlock the door if someone has opened it with a valid token within the indicated preceding time interval. This would be appropriate for opening a door for business on schedule when a responsible User has arrived before the starting time.
- **By designated user (within 1 hour, or 30 minutes, or 15 minutes, or on Entry)** – These options are like the options described above, but the door will remain locked after granting access unless the user has been assigned the "Pending Unlock" option.

When any "By designated user" option is selected in the **SCHEDULED UNLOCK** drop-down list, the "Pending Unlock" option is displayed on the Users page.

The screenshot shows the 'Users (edit)' form for user David Martin. The form includes fields for First Name (David) and Last Name (Martin). Under the 'OPTIONS' section, the 'Pending Unlock' checkbox is highlighted with a red box. A yellow callout box points to this checkbox with the text: 'Displayed if 'pending unlock' is by 'designated user''. Other options include 'Assisted Access', 'Suspended', '3X Lock/Unlock', '3X Arming', and 'Silence Alarms'. The 'ACCESS CARD' field contains the number 319455405. The 'VALID FROM' field is set to 'Now' and the 'VALID UNTIL' field is set to 'Forever'. The 'USER ID' field contains the number 1. The 'DOOR ACCESS BY SCHEDULE' section shows access for 'Back Door', 'Front Door', 'Machine Shop', and 'Stockroom', all set to 'ALL'.

## PIN functionality

If an access reader with a keypad is installed at the door, Users can be assigned a PIN (*personal identification number*) and you have the option of using one of two additional access modes.

- **CARD+PIN MODE** – This mode requires a PIN in addition to a valid access token to unlock the door. The card plus PIN mode provides a higher level of security. Anyone that attempts to access the facility with a stolen card would not know the PIN and would not be granted access.
- **ID+PIN MODE** – This mode only requires the User to enter their **USER ID** plus their **PIN** to unlock the door. The PIN only mode eliminates the requirement to issue and manage access tokens. If tokens are used, the PIN only mode will allow a User to unlock the door with just their ID+PIN if they have forgotten their token.

The **USER ID** is system generated and cannot be edited. Although a **PIN** may not be unique the **USER ID** is unique for each User, and therefore, the combined USER ID+PIN is always unique.

The **CARD+PIN MODE** and **ID+PIN MODE** drop-down lists determine when these access modes are used. The default values are “Never Required” and “Never Allowed” respectively.

**Note:** By default, all PIN configuration fields are inactive. PIN functionality is activated when either the **CARD+PIN MODE** option or the **ID+PIN MODE** option is changed to an active mode for any door in the system. When this occurs, the PIN configuration fields on the System page and the Users page are activated.

The available **ID+PIN MODE** options are logically determined by the **CARD+PIN MODE** options. For example, when a card plus a PIN is required, you cannot unlock the door with just a PIN so that option is excluded.

If the simple “By Door” access authorization method is used, there are only two options for **CARD+PIN MODE**. “Always Required” means **ID+PIN MODE** is automatically set to “Never Allowed”.

<b>CARD+PIN MODE</b>	<b>ID+PIN MODE</b>
Always Required	Never Allowed
Never Required	
Always Required	

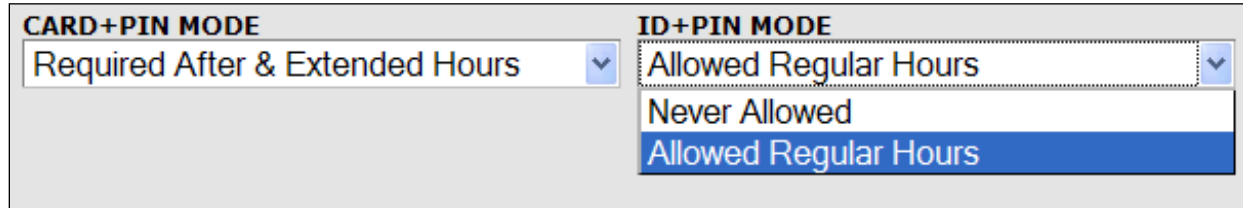
“Never Required” means ID+PIN MODE is optional.

<b>CARD+PIN MODE</b>	<b>ID+PIN MODE</b>
Never Required	Always Allowed
	Never Allowed
	Always Allowed

When “Door by Schedule” or “By User Groups” access authorization methods are used, the **CARD+PIN MODE** drop-down list provides additional scheduling options. For example, you can assign the card plus PIN requirement to “after hours” when security takes precedence over convenience.

<b>CARD+PIN MODE</b>	<b>ID+PIN MODE</b>
Never Required	Always Allowed
Never Required	
Required After Hours	
Required After & Extended Hours	
Always Required	

PIN-only mode will automatically be excluded when card plus PIN is specified. For example, if card plus PIN is required during 'extended hours' and 'after hours', then the PIN-only mode will only be allowed during 'regular hours'.

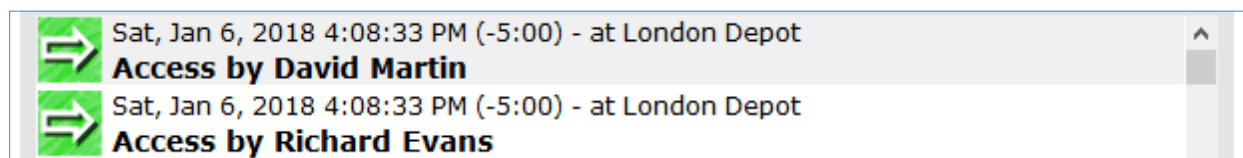


## Dual Custody Mode

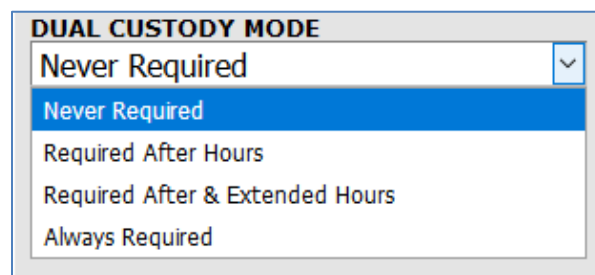
When the Dual Custody Access mode is enabled, two different employees with a valid access permission must badge their access token consecutively to unlock the door or access point. If either employee is denied access for any reason, such as "not authorized for the time schedule" or "access denied when the alarm system is armed", the Dual Custody access is not granted. The Dual Custody access mode can be combined with the other high security access modes to further reduce the risk of false entry.

After the first successful Card Only or Card plus Pin action, the reader LED will retain the "locked" colour but will flash the "unlock" colour once per second while waiting for the second cardholder to badge in. The reader buzzer will also chirp in unison with the "unlock" flash. This continues for 15 seconds after which the unlock request times out and must be repeated.

A successful Dual Custody unlock request is recorded in the Event log with two entries with the same time stamp.



When "Door by Schedule" or "By User Groups" access authorization methods are used, the **DUAL CUSTODY MODE** drop-down list provides additional scheduling options.





## Doors – Advanced Options

### Hardware

**Note:** There are no administrative tasks associated with this page.

The Hardware tab on the Doors page provides configuration options which are normally set by your service provider when the system is first installed. They can be modified at any time if your access requirements change.

The aPod II door controller has many operational features and functions. Configuration fields that are not used are hidden so the appearance of the Doors→Hardware page will change a little depending on how the controller is configured.

Every aPod II system has one Primary Controller. In a multi-door system, there can be 1 to 99 additional door controllers which are automatically configured as Secondary Controllers.

There are four functional areas in the detailed information panel of the Hardware page.

The screenshot shows the 'Hardware' configuration page for a door named 'Back Door'. The page is part of the 'aPod II' system interface by Online Security Technologies. The user is logged in as 'David'. The page has several tabs: 'Home', 'Users', 'Tools', and 'Setup'. The 'Hardware' tab is selected. The configuration fields are as follows:

- DOOR NAME:** Back Door
- SERIAL NO.:** 075359, Master
- STRIKE:** Normal (1.)
- READER #2:** Not Used (2.)
- READER LED:** RBG OST
- INPUT #1:** Door
- CIRCUIT #1:** Normally Closed
- NAME #1:** Door
- INPUT #2:** Alarm Panel (3.)
- CIRCUIT #2:** Normally Closed
- NAME #2:** AS-Machine Shop
- INPUT #3:** None
- INPUT #4:** None
- INPUT #5:** None
- INPUT #6:** None
- OUTPUT #1:** Siren (4.)
- OUTPUT #2:** Panel Arm/Disarm

At the bottom, there are 'Add', 'Save', and 'Cancel' buttons. A legend in the bottom left corner explains the numbered callouts:

1. Strike hardware configuration
2. Reader hardware configuration
3. Input points configuration
4. Output points configuration.

The Doors→Hardware page for the Primary Controller will differ from that of the Secondary Controllers in that there is no Enroll function and no Delete button. The Primary Controller is always the first controller that is brought online and is configured with the Quick Start Wizard. The Primary Controller cannot be deleted. In a multi-door system, Secondary Controllers are added to the system and enrolled using the enroll function on the Doors→Hardware page.

The aPod II controller supports up to six optional input points and a second reader. The second reader requires input points 5 and 6 for its Wiegand inputs. If a second reader is configured, input points 5 and 6 are hidden. Similarly if either input point 5 or 6 is used, the second reader option is hidden.

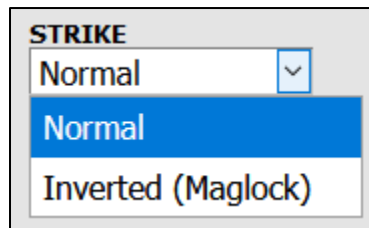
### *Enrolling a Secondary controller*

When a Secondary controller is enrolled in the system, its serial number will be displayed in the **SERIAL NO.** field. *Enrolling a Secondary controller is an installation or service function and is not normally an administrative task.*

### *The locking and reader hardware*

#### **Strikes versus maglocks**

The **STRIKE** drop-down list is used to configure the door locking mechanism. 'Normal' is used for strikes and 'Invert (Maglock)' is used for maglocks. The default is 'Normal'.

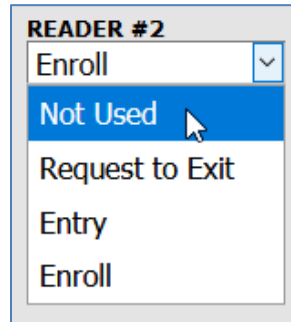


The aPod II controller can drive a sustained strike/maglock output of 500 mA provided the *total* current draw does not exceed 700 mA. This condition is met for all the common door hardware configurations. The power available is enough for almost all strikes and some lighter duty maglocks.

If more power is required than allowed by the aPod II power specification, the aPod II controller output should be used to drive a relay to switch a supplementary power supply.

## Reader #2

A second reader can be connected to an aPod II controller. The **READER #2** drop-down list to choose the correct configuration according to its use.

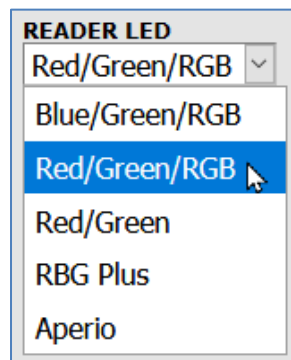


There are three options.

- **Not Used** – A second reader is not used. This is the default mode.
- **Request to Exit** – The exit reader is used to grant an egress. It is recorded in the event log. Any valid card will be granted egress without the need for a PIN.
- **Entry** – An interior door may have a reader on either side. With this option access can be restricted from both directions.
- **Enroll** – A second reader which can be desk or counter mounted and used to enroll the tokens for new Users. Refer to page 115 for more information.

**Note:** When a second reader is configured, input points 5 and 6 are used for the reader Wiegand signals and are not available for additional optional inputs.

## Card reader LED colors



The **READER LED** drop-down list is used to configure the colors of the reader LED in the locked and unlocked states.

There are five options.

- **Blue/Green/RBG** – This option is only available with a proximity reader that supports a tri-colour LED. The reader LED is blue when the door is locked and green when the door is unlocked.
- **Red/Green/RBG** – This option is only available with a proximity reader that supports a tri-colour LED. The reader LED is red when the door is locked and green when the door is unlocked. This is the default option.
- **Red/Green** – This option may be selected for any reader. The reader LED is red when the door is locked and green when the door is unlocked.
- **RBG Plus** – This option is only available with a reader that supports independent control of a tri-colour LED. Select this option if the Alarm Panel Interface has been installed. The reader LED is blue, when the door is locked, and the area is disarmed. It is red when the door is locked, and the area is armed. The reader LED is green when the door is unlocked. This visual feedback of the armed/disarmed status is optional and can be suppressed by selecting another **READER LED** setting.
- **Aperio** – This option is selected when interfacing an Assa Abloy Aperio wireless lock system with an AH20 Wiegand interface hub. The AH20 hub must be configured to use both the green and red reader LED lines from the aPod II controller.

## The input points

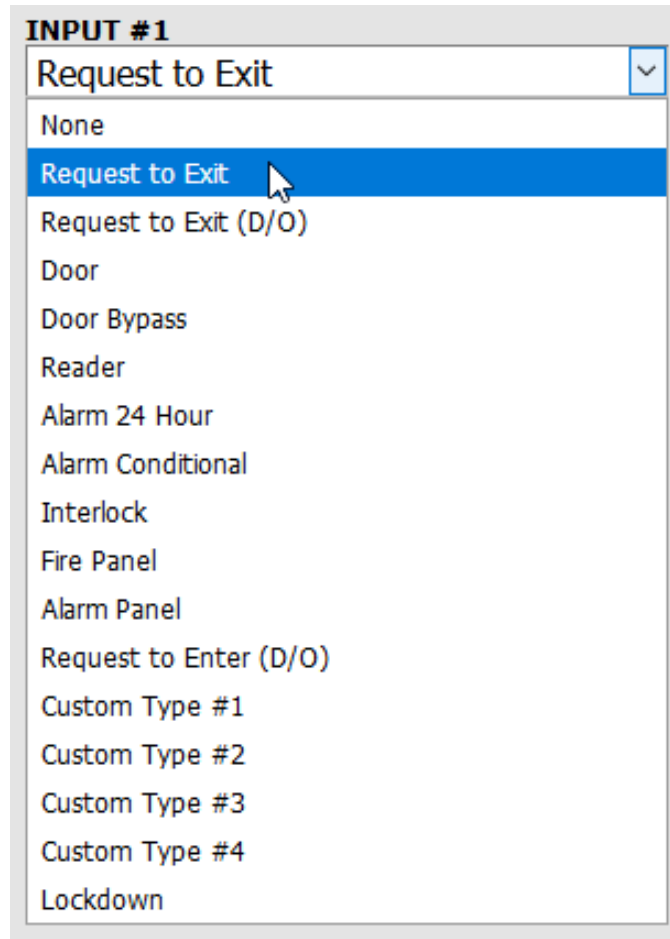
The aPod II controller supports up to six optional input points. There are several ways to configure an input depending on how it will be used. The configuration is accomplished using the following three configuration fields.

INPUT #4	CIRCUIT #4	NAME #4
Alarm 24 Hour	Normally Closed	Locker #3

As mentioned previously, input points 5 and 6 are not available when a second reader is configured. The **CIRCUIT** and **NAME** fields are hidden if the **INPUT** field is set to 'None'.

## Input Type

The **INPUT** field is used to select the *type of input* and its associated function. There are twelve standard input types and provision for four custom input types in the **INPUT** drop-down list in addition to the setting of 'None'.



- **None** – The input is not used, and the circuit is ignored. This is the default setting for all inputs.
- **Request to Exit** – The input is connected to a pushbutton or a request to exit PIR (*passive infrared*) detector and when triggered, releases the strike. The total unlock time is the **UNLOCK DURATION** plus the **EXTENDED UNLOCK** time. These settings are configured on the Setup→Doors→Options page. Refer to page 43. This input type does not activate an automatic door opener.

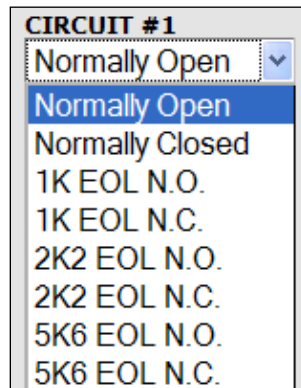
- **Request to Exit (D/O)** – The input is connected to a request-to-exit pushbutton or PIR and when triggered, releases the strike for the **UNLOCK DURATION** plus the **EXTENDED UNLOCK** time and activates an automatic door opener.
- **Door** – The input is connected to a door position switch (door contact) and is used to monitor the open/closed status of the door.
- **Door Bypass** – Also known as “Free Egress”, this input allows the door to be opened manually from the inside without triggering the door forced alarm and without activating the strike. It would typically be used with a request-to-exit PIR or an emergency exit device with a built-in contact. If the door is opened without this input or a valid ‘grant access’ command, the *door forced alarm* is triggered.
- **Reader** – This input is connected to the reader tamper circuit and triggers an alarm if activated.
- **Alarm 24 Hour** – This input is connected to an alarm point and will always trigger an alarm if activated.
- **Alarm Conditional** – The activation of this input depends on one of two conditions.
  - This input may be used in conjunction with the aPod II alarm panel interface. In this case, the conditional input is connected to an alarm point and will only trigger an alarm if the area it resides in is armed.
  - If the conditional input is connected to an alarm point that is not part of an area managed by the alarm panel interface, it will only trigger an alarm if it occurs during an ‘After Hours’ or ‘Extended Hours’ time period in the door schedule.
- **Interlock** – When activated this input will prevent the door from opening. The most common application is the two-door mantrap in which either door will not unlock unless the other door is closed. In this case, the input is connected to the Door Contact point of the other door.
- **Fire Panel** – This input is connected to an alarm output from the fire alarm panel. When triggered it will sound an alarm, unlock the door, and send a command to other aPod II controllers to unlock their doors. A fire panel alarm output can be connected to any input on any aPod II controller, and it will unlock all doors in the event of a fire alarm. Refer to page 178 for more information.
- **Alarm Panel** – This input is connected to a programmable output on an alarm panel which indicates the armed/disarmed status of the panel in “away” mode.

- **Request to Enter (D/O)** – This input is connected to the exterior pushbutton of an automatic door opener. When the door is locked, this input is disabled, and the automatic door opener is only activated after the door is unlocked by a valid card swipe. The total unlock time is the **UNLOCK DURATION** plus the **EXTENDED UNLOCK** time. When the door is unlocked, this input will activate the automatic door opener.
- **Custom Type #1 to #4** – The aPod II system provides four custom input points which by default have an undefined function. Custom input points can be used if required by the installation of a custom application. Custom apps provide non-standard features that are needed to address specific customer requirements. Refer to page 177 for more information.
- **Lockdown** – An emergency lockdown can be triggered by this input point which would typically be connected to a panic button, key switch, or wireless button. For more information about the Lockdown function, please refer to page 178.

## Input Circuit Type

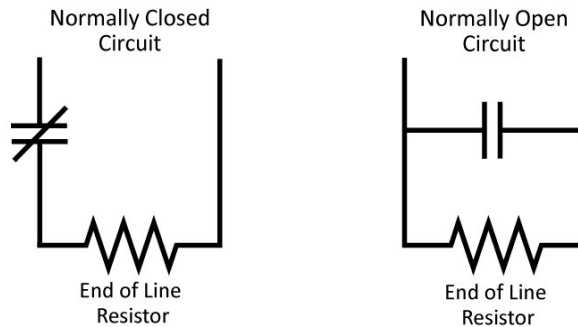
Use the numbered **CIRCUIT** fields to select the *type of circuit* for each input.

There are eight different circuit types in the **CIRCUIT** drop-down list.



The terms ‘normally open’ and ‘normally closed’ refer to the non-activated state of the input. A request to exit switch input is an example of a normally open circuit. Pressing the switch button closes the circuit, activates the input, and releases the door strike. A door contact is an example of a normally closed circuit. The door contact circuit is closed when the door is closed which is its normal state. Opening the door opens the circuit and activates the input.

The first two options, 'Normally Open' and 'Normally Closed' are unsupervised circuits. The remaining options are supervised circuits which use an end of line (EOL) resistor to detect line faults in the field wiring which may occur accidentally or could be the result of sabotage.



Normally Closed Circuit	Normally Open Circuit
A cut line triggers an input alarm	A cut line triggers a tamper signal
A bypassed sensor triggers a tamper signal	A bypassed sensor triggers an input alarm

Your service provider will configure supervised circuits according to the value of the EOL resistor used in the circuit. Three options are available: 1kΩ, 2.2KΩ and 5.6KΩ. The reporting of a tamper alarm is *schedule dependent*.

If a line fault is detected during an unlock schedule, unlock pending or Regular Hours, the 'Tamper' status condition is displayed, and the reader buzzer is activated. At all other times, the line fault is treated like an input alarm. The 'Alarm' status condition is displayed, and the reader buzzer and siren are activated.

### Input Name

Use the numbered **NAME** fields to customize the input label.

<b>INPUT #4</b>	<b>CIRCUIT #4</b>	<b>NAME #4</b>
Alarm 24 Hour	Normally Closed	Locker #3

These input point labels will appear in the event log and on the Home page. Up to 30 characters are allowed. If a custom name is not supplied, the input type is used as a label.



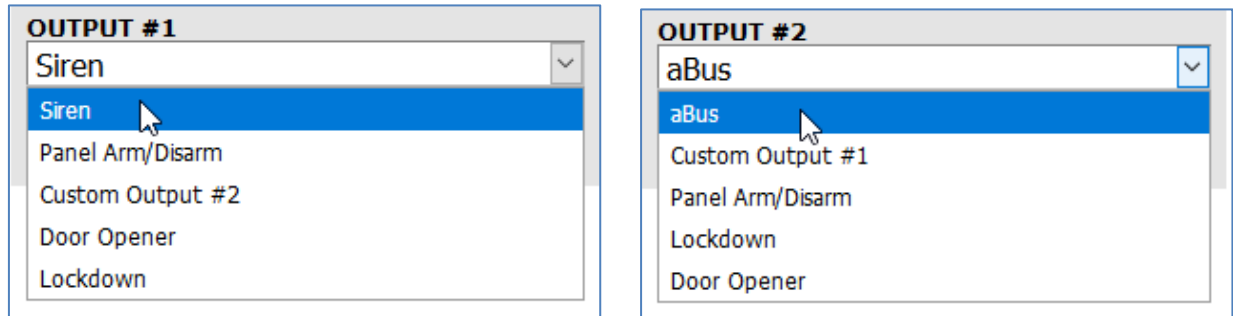
## The output points

The aPod II controller supports one 12 VDC output (**OUTPUT #1**) and one 5 VDC logic level output (**OUTPUT #2**).

Both outputs can be configured to control the arming/disarming of an alarm panel, an automatic door opener, an annunciator during a lockdown, or a custom output for a specific customer application.

In addition, **OUTPUT #1** supports a siren option which is used to drive a Piezo siren when an alarm is activated and **OUTPUT #2** supports an aBus communication option which is reserved for future development. The 'Siren' and 'aBus' are the default options.

The **OUTPUT #1** and **OUTPUT #2** drop-down lists are used to select the appropriate options.

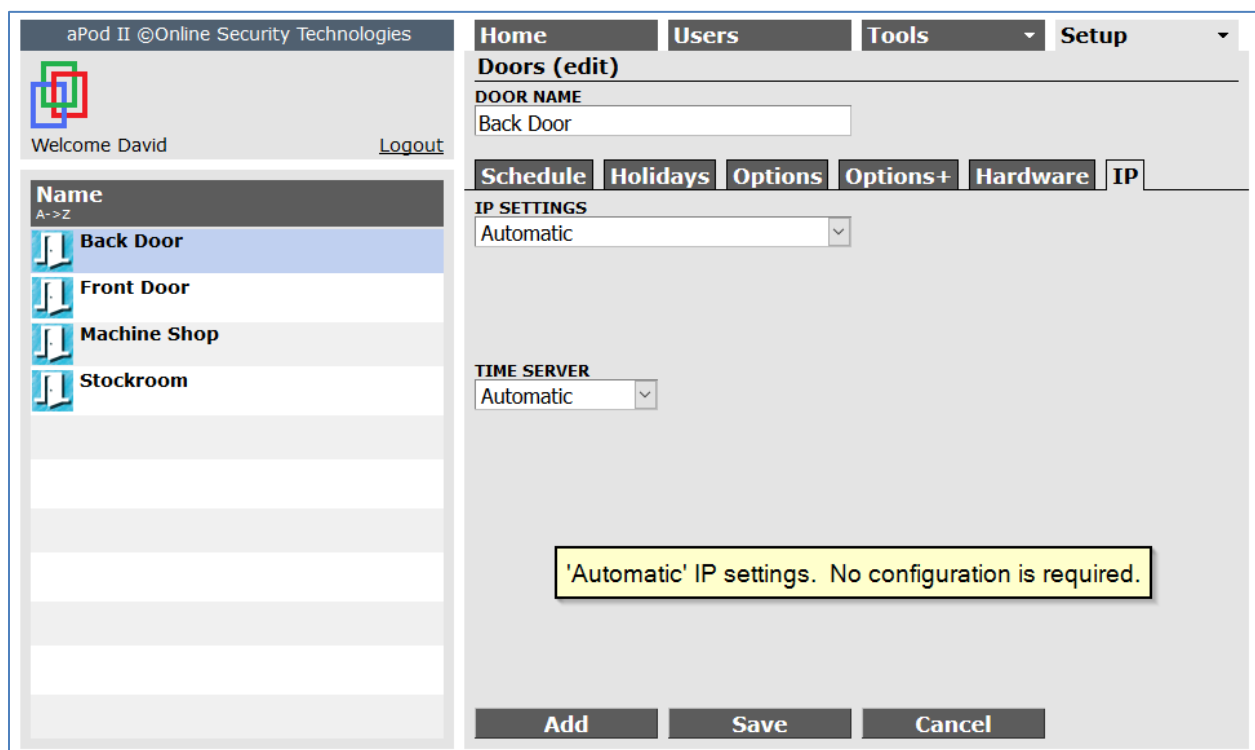


## IP

**Note:** There are no administrative tasks associated with this page.

When an aPod II controller is connected to a local area network, it will automatically self-configure its IP settings and adjust its time by locating an accurate time source. Communication between controllers and multiple browser interfaces is established and maintained automatically.

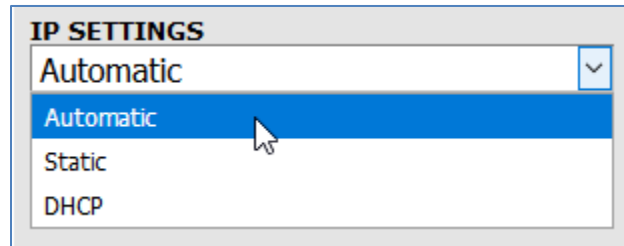
The IP tab on the Doors page provides configuration options for the **IP SETTINGS** and **TIME SERVER** for the controller of the selected door. They are defaulted to their 'automatic' settings.



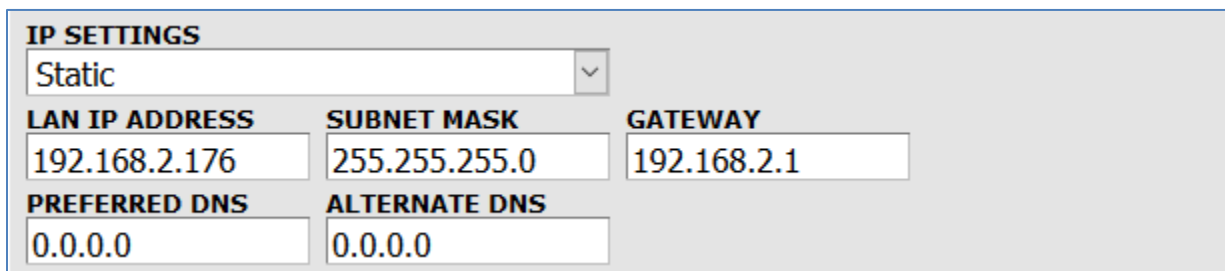
These settings do not need to be modified but you may prefer to change the configurations. For example, in large network with multiple subnets, it may be desirable to assign specific fixed IP addresses to each controller.

## IP Settings

The **IP SETTINGS** drop-down list provides three options for configuring the IP settings for the controller.



- **Automatic** – The aPod II controller will request an IP address from a DHCP server. Based on the address supplied by the DHCP server, it will select an unassigned valid IP address which should be beyond the normal range of DHCP reserved addresses and keep it as a static IP address. If a DHCP server was never detected, the aPod II controller will default to a Zeroconf address, randomly chosen in the range of 169.254.64.2 to 169.254.239.253. This is the default setting.
- **Static IP** – When this option is selected additional fields are displayed which allow the IT support person to manually configure a static IP address.

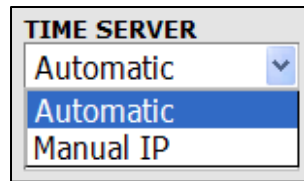
A screenshot of a web interface showing the "IP SETTINGS" form. The "IP SETTINGS" dropdown menu is set to "Static". Below the dropdown, there are five input fields arranged in two rows. The first row contains "LAN IP ADDRESS" (192.168.2.176), "SUBNET MASK" (255.255.255.0), and "GATEWAY" (192.168.2.1). The second row contains "PREFERRED DNS" (0.0.0.0) and "ALTERNATE DNS" (0.0.0.0).

- **DHCP** – The aPod II controller will request its IP configuration using DHCP. The previously assigned address will be requested. If no DHCP server is found, it will fall back to its previous address. If a DHCP server was never detected, it will default to a Zeroconf address, randomly chosen in the range of 169.254.64.2 to 169.254.239.253. If the DHCP option is selected for the Primary Controller, its address must be reserved. The IP address of the Primary Controller must not change in order to preserve the integrity of other network settings.

## Time Server

The aPod II Controller will check the accuracy of its local time approximately once every ten minutes by connecting to an NTP server (*Network Time Protocol server*) either on the Internet or the local private network. The aPod II time is adjusted automatically if necessary, to keep the time accurate to within a small fraction of a second.

The **TIME SERVER** drop-down list provides two options for configuring how the aPod II controller adjusts its local time for accuracy.



- **Automatic** – The aPod II controller requests the time from a large set of preconfigured NTP (*Network Time Protocol*) servers on the Internet or from the DHCP provided NTP server.
- **Manual IP** – When this option is selected an additional field is displayed which allows the IT support person to manually configure the **NTP SERVER IP**. This would typically only be used in a corporate network environment where a private NTP server may be used.

<b>TIME SERVER</b>	<b>NTP SERVER IP</b>
Manual IP	0.0.0.0

## Areas

With some access control functionality, the doors are linked by their association with a defined area. The operation of a door depends on the area to which it is attached. The alarm panel Interface, anti-passback and the fire alarm unlock function are area dependent and require doors to be assigned to areas.

Please refer to the following sections for more information:

- Alarm panel interface, page 159.
- Anti-passback, page 169.
- Fire alarm unlock, page 178.

Use the [Areas](#) page in the [Setup](#) menu to add and edit areas.

By default, every system has one area called 'System' which encompasses the entire facility. The System area cannot be deleted but you can modify the name.

The screenshot shows the 'Areas (add)' form in the aPod II software interface. The form is titled 'Areas (add)' and is located under the 'Setup' menu. It contains the following fields and controls:

- AREA NAME:** A text input field containing 'Machine Shop', highlighted with a red border.
- ANTI-PASSBACK RESET:** A dropdown menu set to 'None'.
- OCCUPANCY:** A dropdown menu set to 'Disabled'.
- WARNING:** An empty text input field.
- LIMIT:** An empty text input field.

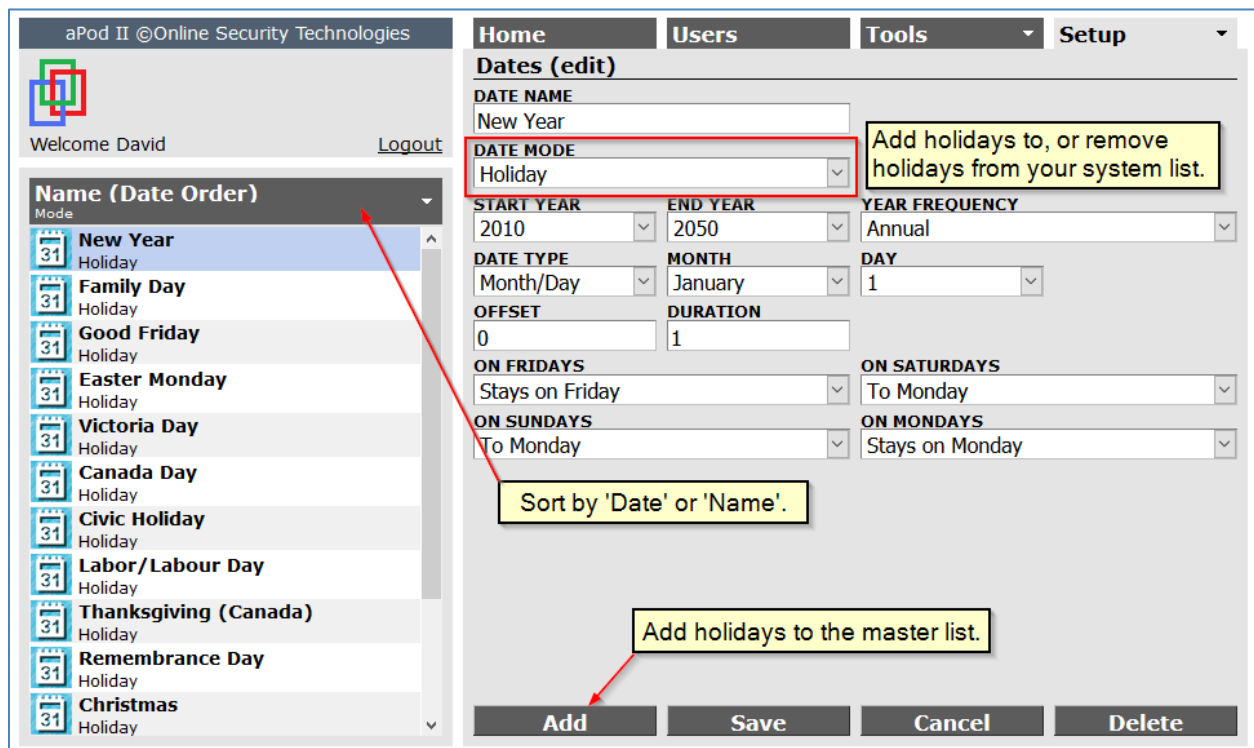
A yellow callout box contains the instruction: "Click the 'Add' button, enter an AREA NAME, and then save the record." At the bottom of the form are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'. On the left side of the interface, there is a sidebar with a 'Name' column and a table listing the 'System' area.

## Dates

### Modify your holidays list

When your locale was selected in the Quick Start Wizard during the initial system setup, the aPod II system pre-configured all the statutory holidays for your jurisdiction in a perpetual calendar. It also configured the 'spring forward' and 'fall back' dates for Daylight Savings Time. The selected holidays are listed under the Holidays tab on the Doors page. Refer to page 39.

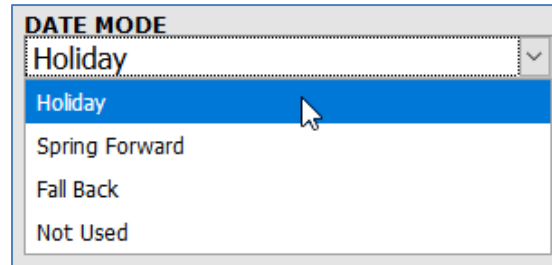
Use the date editing functions on the Dates page to add or remove holidays from your holidays list and to edit their perpetual calendars. You can also create a new holiday if you need one that is not already in the library.



The Dates list on the left can be sorted by Date or Name order. Click on a date to select its record.

You can edit the **DATE NAME** field but unless you are creating a new date, this is usually not necessary.

Use the **DATE MODE** drop-down list to add holidays to your system list or to remove holidays from your list that are not celebrated.



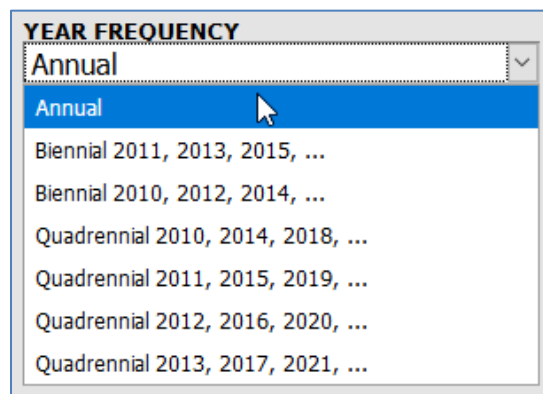
- **Holiday** – Choose this option to add the holiday to your system’s holiday list.
- **Spring Forward** – The time on the specified date is advanced by 1 hour at 2:00 a.m. Use this option to adjust the Daylight Savings Time ‘Spring Forward’ date if necessary.
- **Fall Back** – The time on the specified date is delayed by 1 hour at 2:00 a.m. Use this option to adjust the Daylight Savings Time ‘Fall Back’ date if necessary.
- **Not Used** – Choose this option to remove the holiday from your system’s holiday list.

Remember that the holidays on your system list will activate the Holidays schedule that you define for each door.

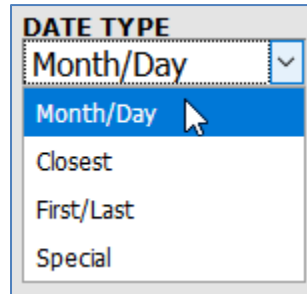
## Edit the perpetual calendar.

**START YEAR** and **END YEAR** are two fields that are normally not changed. They determine when the holiday is active. If you know that a holiday will change in a future year, you can set the **START YEAR**.

**YEAR FREQUENCY** determines the frequency of the date, from Annual (every year) to Biennial (every two years), to Quadrennial (every four years). Note that with biennial and quadrennial options you need to select the year cycle (e.g., even, or odd years).

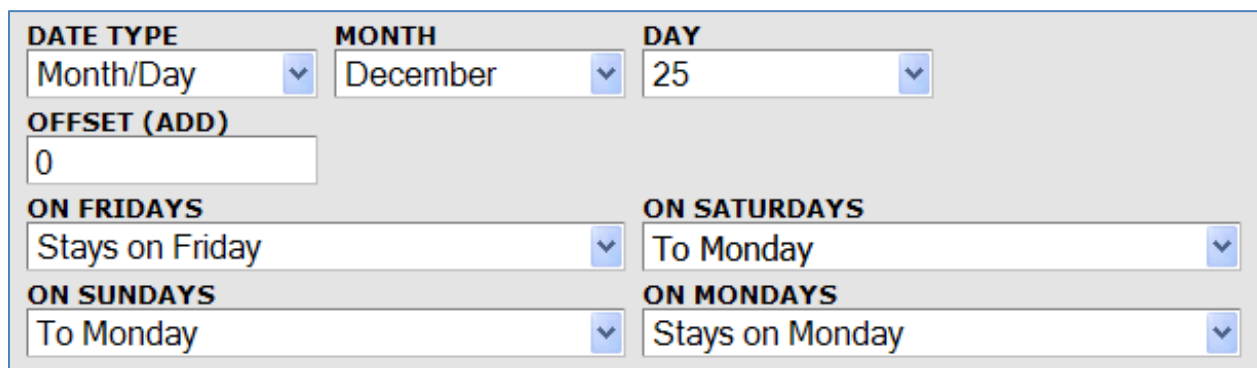


The options in the **DATE TYPE** drop-down list determine how the perpetual calendar is calculated. The drop-down list has four possible options:



DATE TYPE  
Month/Day  
Closest  
First/Last  
Special

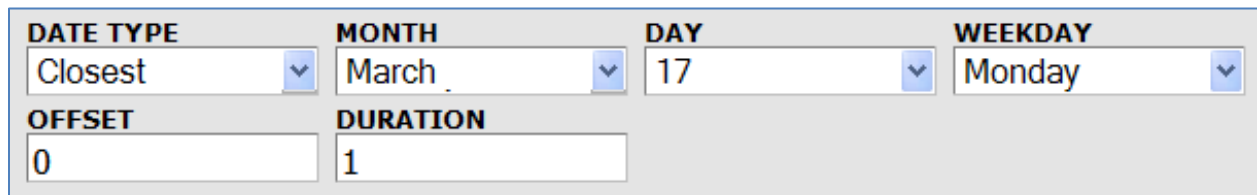
- **Month/Day** – With this option the date occurs on a specific month/day of the year. For example, the Christmas Day holiday would have the following settings.



DATE TYPE: Month/Day  
MONTH: December  
DAY: 25  
OFFSET (ADD): 0  
ON FRIDAYS: Stays on Friday  
ON SATURDAYS: To Monday  
ON SUNDAYS: To Monday  
ON MONDAYS: Stays on Monday

When the 'Month/Day' **DATE TYPE** option is selected four additional fields are displayed, that is, **ON FRIDAYS**, **ON SATURDAYS**, **ON SUNDAYS** and **ON MONDAYS**. These fields are used to move a fixed holiday that falls on a weekend to either the preceding Friday or the following Monday for the purpose of scheduling a shutdown.

- **Closest** – With this option the holiday occurs on a specific month/day of the year but is shifted to the closest specified weekday. For example, St. Patrick's Day in the province of Newfoundland is celebrated on the closest Monday to March 17<sup>th</sup>.



DATE TYPE: Closest  
MONTH: March  
DAY: 17  
WEEKDAY: Monday  
OFFSET: 0  
DURATION: 1



- **First/Last** – With this option the holiday occurs in a specific month and on a specific weekday relative to the start or end of the month. For example, Labour Day is celebrated on the first Monday of September.

<b>DATE TYPE</b> First/Last	<b>MONTH</b> September	<b>WEEKDAY</b> 1st Monday
<b>OFFSET</b> 0	<b>DURATION</b> 1	

- **Special** – This option handles the floating religious holidays. ‘Mardi Gras’ dates are pre-determined and Christian holidays are determined by an offset to the ‘Mardi Gras’ date. For example, Good Friday is determined by adding an offset of 45 days to the ‘Mardi Gras’ date. Similarly, ‘Pesach’ dates are pre-determined and Jewish holidays are determined by an offset to the ‘Pesach’ date.

<b>DATE TYPE</b> Special	<b>SPECIAL</b> Mardi Gras
<b>OFFSET</b> 0	<b>DURATION</b> 1

## Add a new holiday.

Click the **Add** button to create a new record, set **DATE MODE** to ‘Holiday’ and edit the calendar parameters. The new holiday will become part of your system’s ‘holiday list’ and will activate the holiday access schedule on the appropriate date.

### Schedule a shutdown period

It may be necessary to close your business for a short period, for example, for emergency maintenance or a planned total vacation shut down. Add a new holiday with the **DATE TYPE** set to ‘Month/Day’ and enter the start **MONTH** and **DAY**. Enter the number of calendar days from the start date up to and including the last planned day of shut down in the **DURATION** field.

Leave the default values in the other configuration fields.

Fore example, a planned two-week vacation shut down beginning on Monday, July 8<sup>th</sup> and lasting until Friday, July 19<sup>th</sup> would be configured as shown.

The screenshot shows the 'Dates (add)' form in the Online Security Technologies interface. The form is titled 'Dates (add)' and contains the following fields and options:

- DATE NAME:** Vacation Shut Down
- DATE MODE:** Holiday
- START YEAR:** 2010
- END YEAR:** 2050
- YEAR FREQUENCY:** Annual
- DATE TYPE:** Month/Day
- MONTH:** July
- DAY:** 8
- OFFSET:** 0
- DURATION:** 12
- ON FRIDAYS:** Stays on Friday
- ON SATURDAYS:** Stays on Saturday
- ON SUNDAYS:** Stays on Sunday
- ON MONDAYS:** Stays on Monday

At the bottom of the form are four buttons: Add, Save, Cancel, and Delete. On the left side of the interface, there is a list of dates with their respective modes (all are 'Holiday'):

- Civic Holiday
- Daylight Fall Back
- Daylight Spring Forward
- Easter Monday
- Family Day
- Good Friday
- Labor/Labour Day
- New Year
- Remembrance Day
- Thanksgiving (Canada)
- Victoria Day

When you save the record, the planned shutdown event will be automatically active and the holiday schedule for those dates will be applied to every door.

Although, a business shut down could occur on an annual basis, this type of holiday should be reviewed every year and re-configured, as necessary.

## Override Daylight Savings Time dates

There are two special purpose dates listed in the Dates library. They are the 'Daylight Spring Forward' and the 'Daylight Fall Back' dates.

The default settings for these dates should be correct for your jurisdiction. If Daylight Savings Time is changed, you can edit these dates to make the adjustments.

On the [Dates](#) page, select the Daylight Spring Forward record and set the **DATE MODE** to 'Spring Forward'. Change the calendar parameters to the correct settings. Save your edits.

aPod II ©Online Security Technologies

Welcome David [Logout](#)

**Name (Date Order)**  
Mode

- Easter Monday  
Holiday
- Victoria Day  
Holiday
- Canada Day  
Holiday
- Civic Holiday  
Holiday
- Labor/Labour Day  
Holiday
- Thanksgiving (Canada)  
Holiday
- Remembrance Day  
Holiday
- Christmas  
Holiday
- Boxing Day  
Holiday
- Daylight Spring Forward** 1.  
Spring Forward
- Daylight Fall Back  
Fall Back

**Dates (edit)**

DATE NAME  
Daylight Spring Forward

DATE MODE  
Spring Forward

START YEAR 2010 END YEAR 2050 YEAR FREQUENCY Annual

DATE TYPE First/Last MONTH March WEEKDAY 2nd Sunday

OFFSET 0 DURATION 1

1. Select the 'Spring Forward' date.  
2. Edit the MONTH and WEEKDAY settings.  
3. Save the record.

3.

Add Save Cancel Delete

Repeat this process for the Daylight Fall Back date.

aPod II ©Online Security Technologies

Welcome David [Logout](#)

**Name (Date Order)**  
Mode

- Easter Monday  
Holiday
- Victoria Day  
Holiday
- Canada Day  
Holiday
- Civic Holiday  
Holiday
- Labor/Labour Day  
Holiday
- Thanksgiving (Canada)  
Holiday
- Remembrance Day  
Holiday
- Christmas  
Holiday
- Boxing Day  
Holiday
- Daylight Spring Forward  
Spring Forward
- Daylight Fall Back** 1.  
Fall Back

**Dates (edit)**

DATE NAME  
Daylight Fall Back

DATE MODE  
Fall Back

START YEAR 2010 END YEAR 2050 YEAR FREQUENCY Annual

DATE TYPE First/Last MONTH November WEEKDAY 1st Sunday

OFFSET 0 DURATION 1

1. Select the 'Fall Back' date.  
2. Edit the MONTH and WEEKDAY settings.  
3. Save the record.

3.

Add Save Cancel Delete

## Non-Statutory Religious Holidays

The dates for your locale are drawn from a large library of holidays, which also includes most non-statutory religious holidays. If you wish to make the non-statutory religious holidays available for use in scheduling your access control system, you can add them by clicking the **Add dates** button on the System page.

The screenshot shows the 'System' configuration page in the aPod II interface. The 'Add dates' button is highlighted with a red box. A yellow callout box points to the button with the text: 'Click here to add non-statutory religious holidays to your Dates list.' The page includes fields for SITE NAME, SITE ADDRESS, TIME ZONE, DAYLIGHT SAVINGS, CUSTOM APP #1, CUSTOM APP #2, LANGUAGE, ACCESS AUTHORIZATION, PIN LENGTH, PIN STRENGTH, ADMINISTRATOR TEMPORARY PASSWORD, ELEVATORS, PRIMARY INTERNET IP, PORT (UDP), REMOTE LOGIN SETUP, REMOTE HTTP PORT (TCP), PC's DATE/TIME, aPod's DATE/TIME, SELECTED LOCALE, and PRIMARY IP ADDRESS. There are 'Save' and 'Cancel' buttons at the bottom.

aPod II ©Online Security Technologies		Home	Users	Tools	Setup
<b>System</b>					
SITE NAME		SITE ADDRESS			
David Martin Custom Parts		142 Oakdale Rd, Kingston ON			
TIME ZONE		DAYLIGHT SAVINGS			
Eastern Time (GMT-5:00)		Enabled			
CUSTOM APP #1		<b>Add dates</b>			
CUSTOM APP #2		Click here to add non-statutory religious holidays to your Dates list.			
LANGUAGE					
English (en)					
ACCESS AUTHORIZATION		PIN LENGTH		PIN STRENGTH	
By User Groups		4 Digits		Standard	
ADMINISTRATOR TEMPORARY PASSWORD					
None					
PRIMARY INTERNET IP		PORT (UDP)			
64.228.89.95		5268			
REMOTE LOGIN SETUP		REMOTE HTTP PORT (TCP)			
Automatic (DDNS)		25268			
PC's DATE/TIME			aPod's DATE/TIME		
Mon, May 3, 2021 2:48:37 PM			Mon, May 3, 2021 2:48:35 PM		
SELECTED LOCALE		PRIMARY IP ADDRESS			
Ontario		192.168.2.164			
Save			Cancel		

The non-statutory religious holidays are added to the list of available holiday dates with the default **DATE MODE** setting "Not Used". Activate one or more specific holidays by changing the **DATE MODE** setting to "Holiday".

## Backup

Backup the aPod system database on a regular basis. With a reasonably current backup, you can quickly recover from any system problem that you may encounter. A recent backup is required before a software update is allowed. The aPod II system will remind you to perform a backup when necessary.

The backup process saves an encrypted copy of the database in a file that is stored on the administrator's PC or in any accessible file location on the network. The data within the backup cannot be accessed except through the aPod Browser Interface using the backup restore function.

While any administrator can perform a backup, only administrators recorded in the backup file with Full Authority can restore a backup.

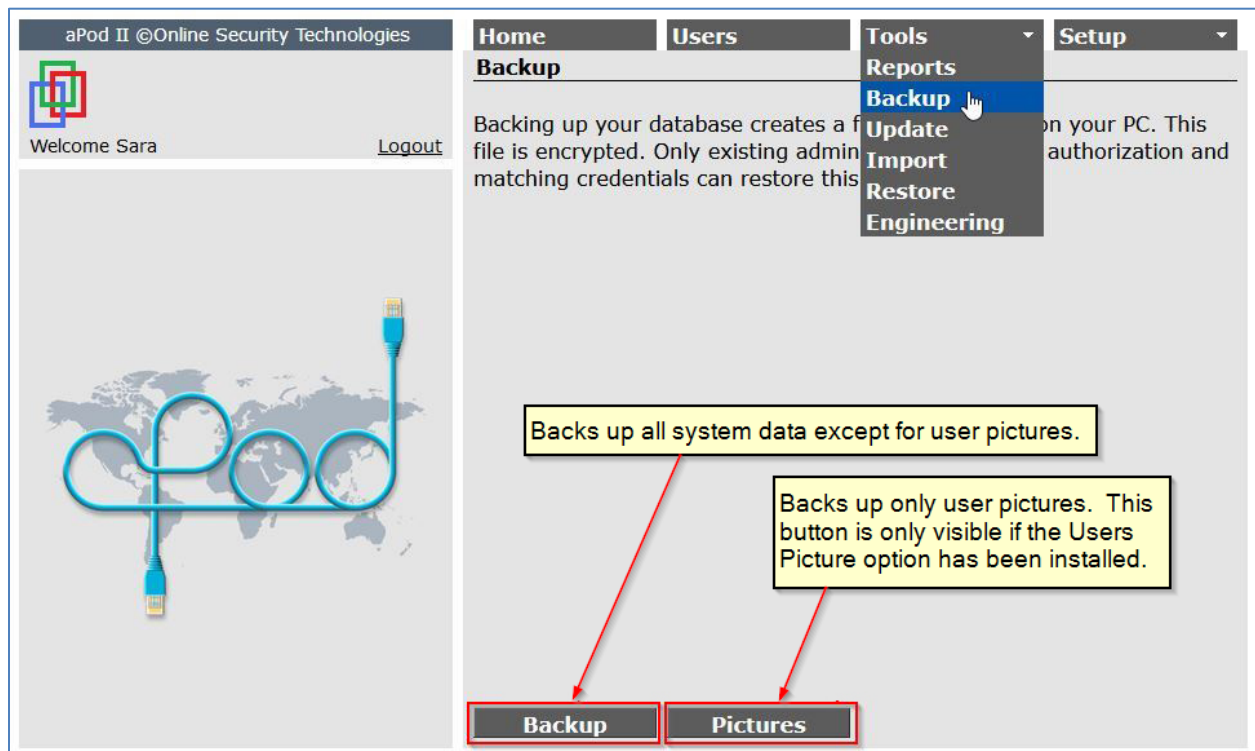
The screenshot shows the 'Administrators (edit)' page in the aPod II web interface. The page is divided into several sections:

- Header:** 'aPod II ©Online Security Technologies' and navigation tabs for 'Home', 'Users', 'Tools', and 'Setup'.
- Left Sidebar:** A 'Welcome David' message with a 'Logout' link. Below it is a user list with a dropdown menu for 'Name (First Last)'. The list includes 'David Martin' (dmartin@gmail.com) and 'Sara Friedman' (sara@securityservices.com).
- Main Form:** Fields for 'FIRST NAME' (Sara), 'LAST NAME' (Friedman), 'LOGIN EMAIL ADDRESS' (sara@securityservices.com), and 'PASSWORD' (Valid password). There is an 'Assign Temporary Password' button.
- ADMINISTRATOR PERMISSIONS:** A list of checkboxes for various permissions. The 'Full Authority' checkbox is highlighted with a red box. Other permissions include Remote Login, Manage Users, Silence Alarms, Bypass Inputs, Grant Access, Override Door Schedules, Run Reports, Arm/Disarm Alarm Panel, Manage Schedules, Manage Door Options, Manage IP Parameters, Manage Administrators, Backup the system, Restore the system, and Update Software.
- Bottom:** Buttons for 'Add', 'Save', 'Cancel', and 'Delete'.

## Backup Types

There are three types of backup.

1. Standard backup – includes all system settings and user data.
2. Picture backup – backs up only user pictures. This function is only available if the Users picture option has been installed.
3. Events backup – an archive of all system events and system edits



### Standard backup

The standard backup captures the entire system database except for user pictures and events. It contains critical system configuration detail and the login credentials of the administrators.

A standard backup file is created using the Tools→Backup→Backup function.

The standard backup file name contains a date and time stamp and has a “.bak” file extension.

A standard backup file is restored using the Tools→Restore→From Backup function.

## Pictures backup

The pictures backup captures only the user pictures. User pictures can be recovered without affecting any other live data.

A pictures backup file is created using the Tools→Backup→Pictures function.

The pictures backup file name contains a date and time stamp and has a “.upb” file extension.

A pictures backup file is restored using the Tools→Import→Import Pictures function.

## Events backup

The standard backup does not archive events. Please refer to page 75 for a description of the archiving procedure.

## Restore

Only administrators with “Full” authorization can perform Restore functions.

### Restore from Backup.

If the aPod II Primary Controller needs to be replaced, you can make your system fully operational within minutes by restoring the database from a recent backup.

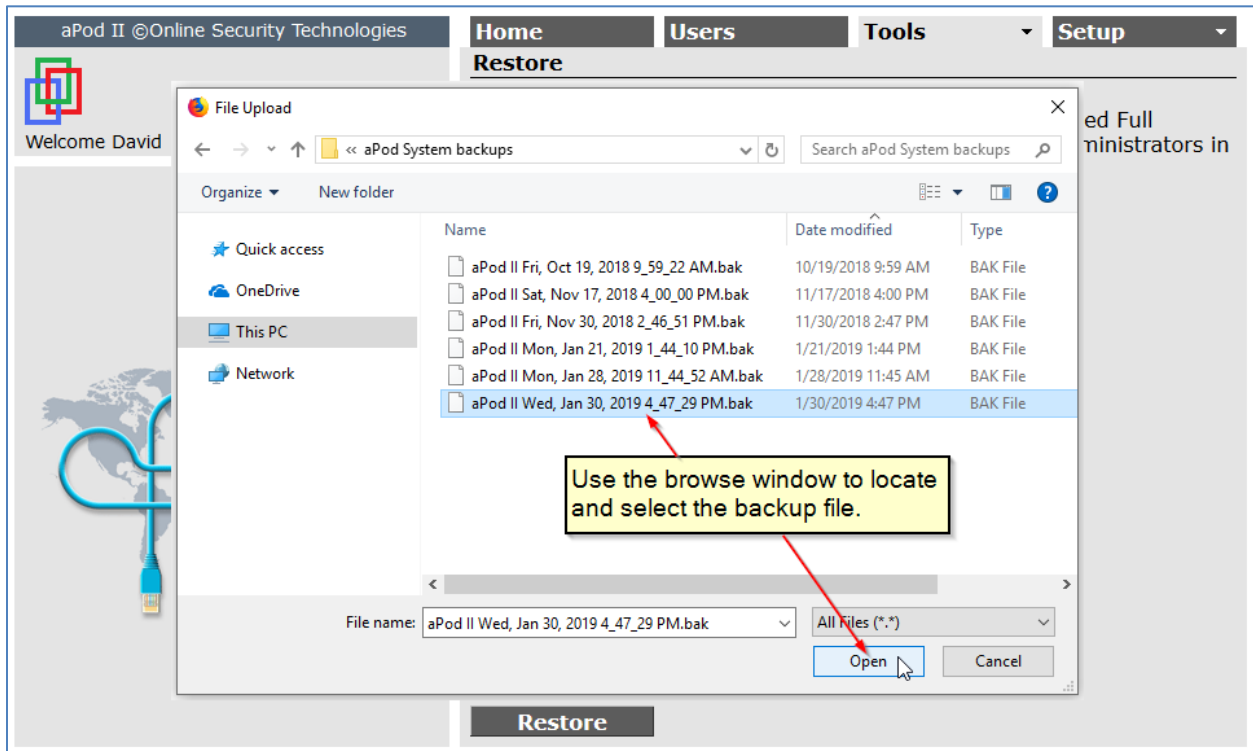
When you perform a database restore, your login credentials must match the credentials of one of the Administrators with ‘Full’ authorization recorded in the backup.

Select the “From Backup” option and then click the “Browse” button.

The screenshot displays the aPod II web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The 'Tools' dropdown menu is open, showing options like 'Reports', 'Backup', 'Update', 'Import', 'Restore', and 'Engineering'. The 'Restore' option is highlighted. The main content area is titled 'Restore' and contains the following text: 'Restore your database from a previous backup. Authority and credentials that correspond to the backed up system.' Below this text are two radio button options: 'From Backup' (selected) and 'To Defaults'. A 'Browse' button is located next to the 'From Backup' option. A yellow callout box with a black border contains the text: 'Select 'From Backup' and then click the Browse button to find the backup file.' The 'Restore' button is visible at the bottom of the page.

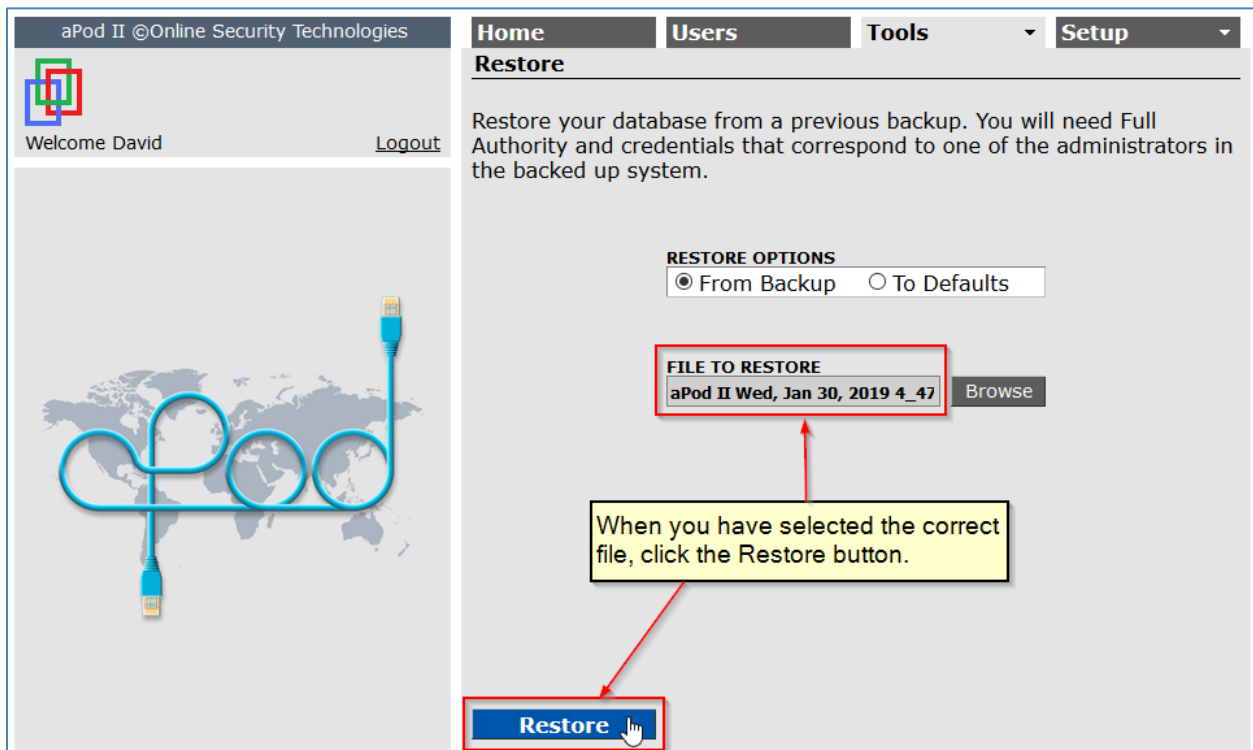


Locate and select your backup file.



Firefox 64 on Windows 10

Click the "Restore" button.



Your backup file is automatically uploaded to the Primary Controller, validated, and restored. This process can take a few minutes and progress will be indicated on the page. When the database has been restored, the Primary Controller will reboot and after thirty to forty seconds you will be re-directed to the [Login](#) page. If you have a multi-door system, all Secondary controllers will be updated automatically by the Primary Controller. Each Secondary controller will go offline for about thirty to forty seconds when it reboots but will resume normal operation automatically.

## Restore to Defaults.

Restoring a controller to factory defaults is never required under normal operation so this function would likely only be used while installing or servicing the system. When you select the “To Defaults” option, you will be required to enter an activation code in order to proceed. This ensures that this function is not performed accidentally. The activation code is a mix of alphabetical and numerical characters and is case sensitive.

aPod II ©Online Security Technologies

Welcome David [Logout](#)

Home Users Tools Setup

**Restore**

Restore to factory defaults (you need to enter an activation code to confirm).

**RESTORE OPTIONS**

From Backup  To Defaults

**ENTER THE 'xm2o' ACTIVATION CODE HERE**

xm2o

Keep IP settings  
Reset IP settings  
Keep IP settings

1. Select the 'To Defaults' option.  
2. Enter the activation code.  
3. Select the 'Reset' or 'Keep' IP settings options.  
4. Click the Restore button.

Restore

When you restore the aPod II controller to factory defaults, you have the option of keeping its IP settings. This will preserve communication with a remote controller using the Internet or a private wide area network and allow you to reconfigure it without going to the remote site. The default setting is “Keep IP settings”.

When you click the **Restore** button, the controller re-boots and re-directs you to the [Login](#) page.

**IMPORTANT WARNING**: When you restore to factory defaults, you will lose all current data. We strongly recommend that you backup your database before taking this action.

## Archive Events and the Administrators Audit Log

The aPod II System retains 100,000 events in the event log and 10,000 database changes in the audit log. For most systems this will provide enough capacity to accommodate any reasonable tracking horizon. To safeguard against a system hardware failure, the event and audit logs should be backed up periodically.

### The archiving procedure

On a regular basis run reports of the event log and the audit log and select date filters that will connect the archives in a continuous record, e.g., weekly, or monthly. Use the TSV format and save the reports to a data drive.

aPod II ©Online Security Technologies

Welcome David [Logout](#)

Home Users Tools Setup

### Reports

**REPORT TYPE**  
Events (All) 1.

**BY DOOR**  
All Doors

**FROM**  
December 1, 2018 12:00AM 2.

**UNTIL**  
January 1, 2019 12:00AM

«« 2019 »» Hour Min  
«« January »» 1 7 00 30

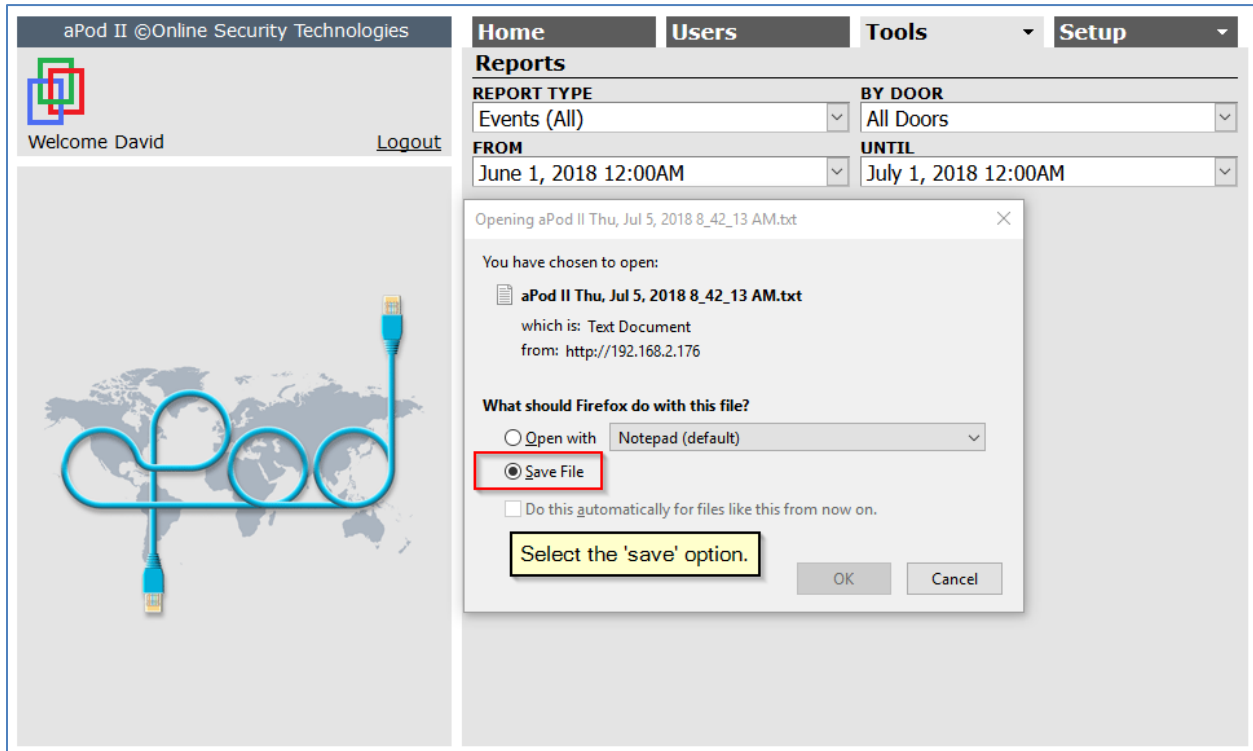
Su	Mo	Tu	We	Th	Fr	Sa	Hour	Min		
		1	2	3	4	5	2	8	05	35
30	31	1	2	3	4	5	3	9	10	40
6	7	8	9	10	11	12	4	10	15	45
13	14	15	16	17	18	19	5	11	20	50
20	21	22	23	24	25	26	6	12	25	55
27	28	29	30	31	1	2	AM	PM		
3	4						Newest			OK

**REPORT FORMAT**  
 HTML  TSV 3.

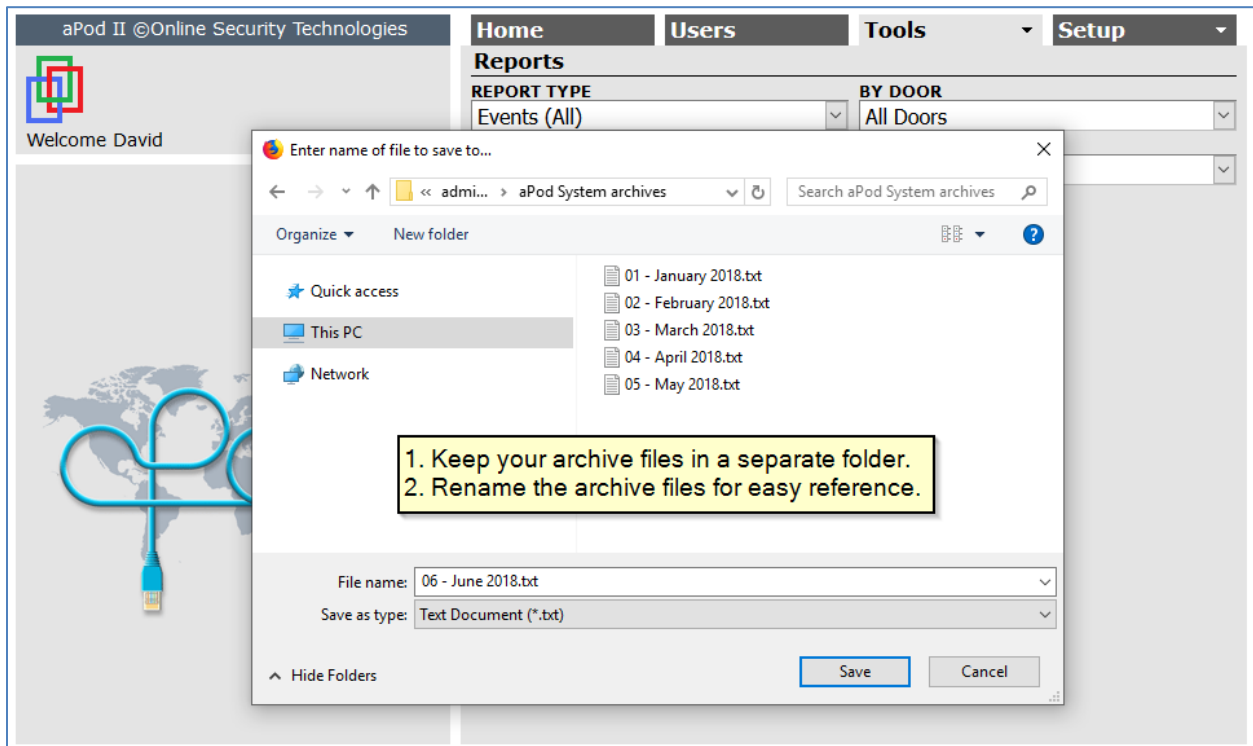
**REPORT HEADER**  
David Martin Custom Parts

**Report** 4.

1. Select all events for all doors.
2. Use the date/time applet to filter events for the archive interval.
3. Select the TSV format option.
4. Click the report button to run the report.



FireFox 64.0 on Windows 10

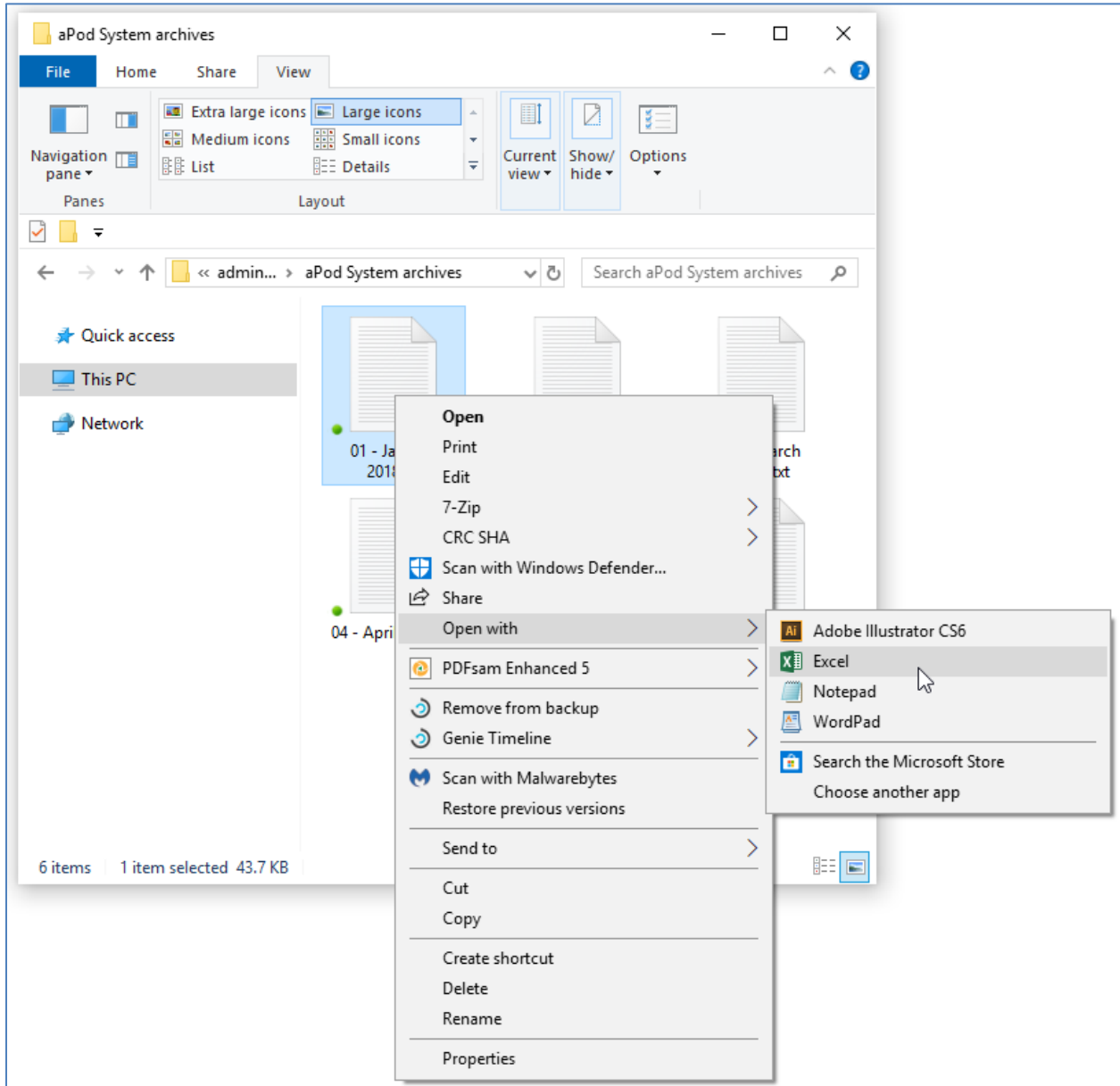


FireFox 64.0 on Windows 10

## Review the Archives

The archived reports can be imported into Excel where the records can be sorted and filtered to facilitate your investigation, or they can be opened with Notepad and reviewed in a simple two column list.

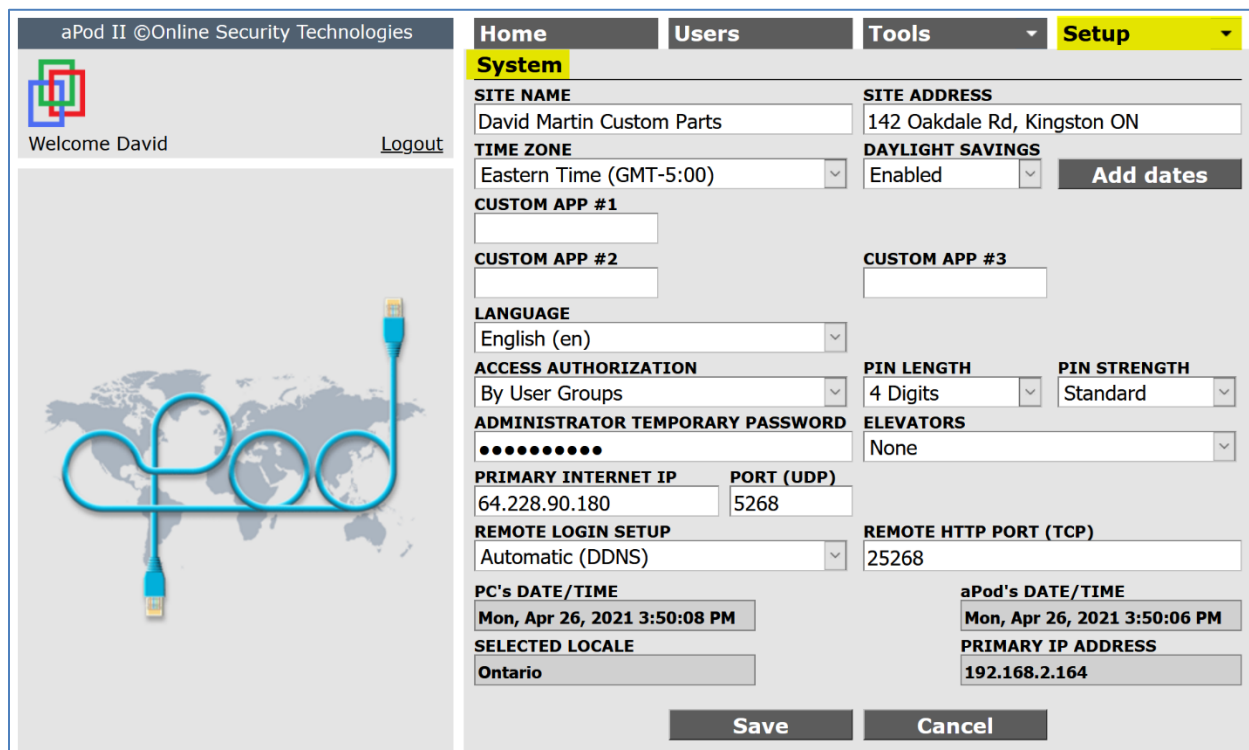
Right click on the selected file and use the “Open with” option to import the file into Excel or Notepad. The default field delimiter in Excel is the “comma”. Change this to the “tab” delimiter.



Windows Explorer on Windows 10

## System-wide Settings

The [System](#) page contains several settings which apply to the operation of the entire system. These settings are usually configured during installation but can be edited if required to support changes in functionality.



aPod II ©Online Security Technologies

Welcome David [Logout](#)

**Home** **Users** **Tools** **Setup**

**System**

**SITE NAME**  
David Martin Custom Parts

**SITE ADDRESS**  
142 Oakdale Rd, Kingston ON

**TIME ZONE**  
Eastern Time (GMT-5:00)

**DAYLIGHT SAVINGS**  
Enabled [Add dates](#)

**CUSTOM APP #1**

**CUSTOM APP #2**

**CUSTOM APP #3**

**LANGUAGE**  
English (en)

**ACCESS AUTHORIZATION**  
By User Groups

**PIN LENGTH**  
4 Digits

**PIN STRENGTH**  
Standard

**ADMINISTRATOR TEMPORARY PASSWORD**  
●●●●●●●●

**ELEVATORS**  
None

**PRIMARY INTERNET IP**  
64.228.90.180

**PORT (UDP)**  
5268

**REMOTE LOGIN SETUP**  
Automatic (DDNS)

**REMOTE HTTP PORT (TCP)**  
25268

**PC's DATE/TIME**  
Mon, Apr 26, 2021 3:50:08 PM

**aPod's DATE/TIME**  
Mon, Apr 26, 2021 3:50:06 PM

**SELECTED LOCALE**  
Ontario

**PRIMARY IP ADDRESS**  
192.168.2.164

[Save](#) [Cancel](#)

### Site Name and Site Address

The **SITE NAME** and **SITE ADDRESS** fields identify your system. The [Login](#) Page will display the site name and address in the header. They are also used to identify your system when you use Remote Login to link to the [Login](#) page. Refer to page 152 for more information.

The header in the top left panel on every page displays the system name, address, and software version number in a continuous cycle.

### Time Zone

**TIME ZONE** displays the offset of the Greenwich Mean Time (GMT; also known as Coordinated Universal Time) based upon the locale entered in the Quick Start Wizard during the initial system setup. This value should be correct but can be manually changed in this field if necessary.

## Daylight Savings

**DAYLIGHT SAVINGS**, like **TIME ZONE**, is determined automatically by your locale. However, if Daylight Savings times are not in force, this function can be disabled with this setting.

## Add Dates

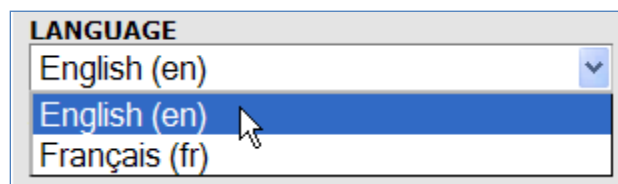
Please refer to page 67.

## Custom Applications

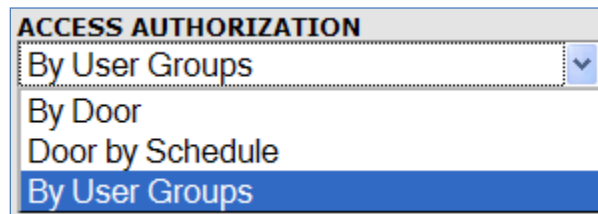
Please refer to page 198.

## Language

This is a special purpose field. Its setting determines the language of messages between the aPod II System and any other system for which an application interface (*API*) has been installed.



## Access Authorization



Use the **ACCESS AUTHORIZATION** drop-down list to select the method used to assign access permissions to Users. Normally you would make this configuration when the system is first installed but you can change the method at any time. The method you select will depend on the size and complexity of your access control system.

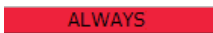
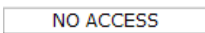
*Changing the access authorization method will change the structure of your system. To ensure that you can restore a previous configuration, the aPod will not allow you to make this change unless a backup was made within the last half hour.*




There are three **ACCESS AUTHORIZATION** options which are summarized below. For a detailed description on how to configure and use each method, please refer to the section titled “**Assign Access Permissions**” on page 128.




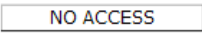
## By Door

This is the simplest implementation of access authorization and is the default method.

A list of the doors is displayed on the Users page and each door can be toggled between  and  to grant or deny access permission to that User.


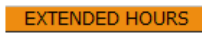

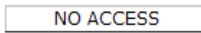
When there is only one door in the system, the list is not displayed and the single door permission defaults to . Access permission is granted or denied by issuing an access token to the User.

## Door by Schedule

Access permissions for each door vary according to the day of the week and the time of day. A list of the doors is displayed on the Users page and each door can be toggled between     to grant or deny access to that User according to a time schedule.

## User Groups

Use this access authorization method to simplify the assignment of permissions when you have many Users. Use the User Groups page in the Setup menu to create groups of Users who have the same access requirements. Next create a permission set for each group.

A list of the doors is displayed on the User Groups page and each door can be toggled between to grant     or deny access to that User Group according to a time schedule. To complete the process, use the Users page to assign each User to the appropriate User group. Each User will automatically inherit the access permissions of their group.

## Pin Length and Pin Strength

Refer to the section ‘Assigning PIN’s’ on page 120.

## Administrator Temporary Password

Please refer to page 19.

## Elevators

Elevator access control is an option within the aPod II Access Control System and is enabled with this selection box. The Administration Guide for elevator access control is available as a separate document. Please contact your service provider if you would like to add this option to your system.

## Primary Internet IP and Port

Secondary controllers may reside in a different geographical location on a separate network connected by the Internet.

In this situation, the IT Administrator must configure the network to allow UDP communication between the Primary controller and any remote Secondary controller. This is part of the configuration process when the system is installed. The **PRIMARY INTERNET IP** and **PORT (UDP)** provides the network target for every remote Secondary that is connected by the Internet.

The process of enrolling Secondary controllers is an installation task described in detail in the aPod II Installation Guide.

## Remote Login Setup

Refer to the section 'Remote Login on page 152.

## Remote HTTP Port (TCP)

This field displays the external port number for the Remote Connect application in the aPod II System. A port forward record is created in the router to map TCP communication from this port to the IP address of the aPod II Primary Controller. Use this number for both the external and internal port number entries in the port forward record if this is required. The default port number is **25268** but this can be changed to any valid port number if necessary, by editing the **REMOTE HTTP PORT (TCP)** field.

## Date and Time

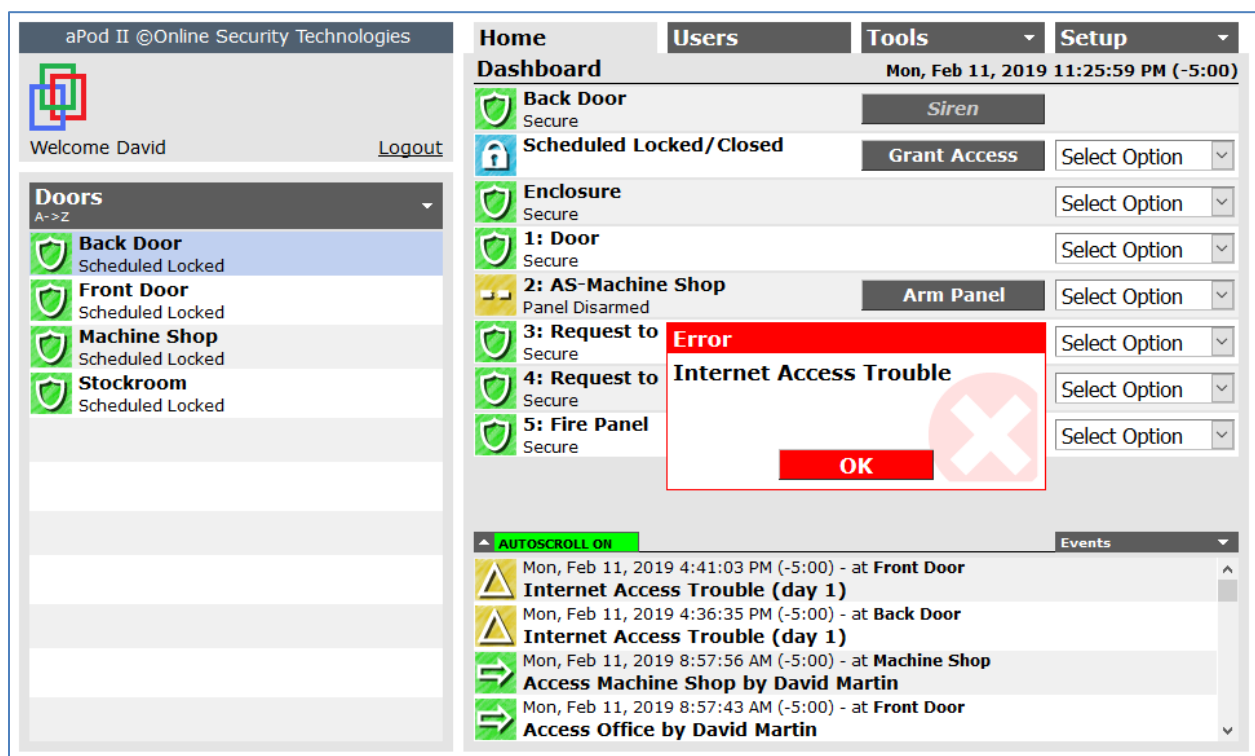
The **PC's DATE/TIME** field displays the local time of your PC. The **aPod's DATE/TIME** field displays the local time in the aPod II Primary Controller. These two times will be offset if you access an aPod II System remotely from a different time zone.

The aPod II System time shown on the aPod II Browser Interface and recorded in the event log uses **TIME ZONE** and Daylight Savings offsets to accurately reflect your local time.

The aPod II controller uses a Real-time Clock (RTC) which has a precision of  $\pm 2$  seconds/day. It also uses Internet Network Time Protocol (NTP) servers to periodically tweak its time setting for maximum accuracy. Typically, no time adjustments are required.

## Internet Access Trouble

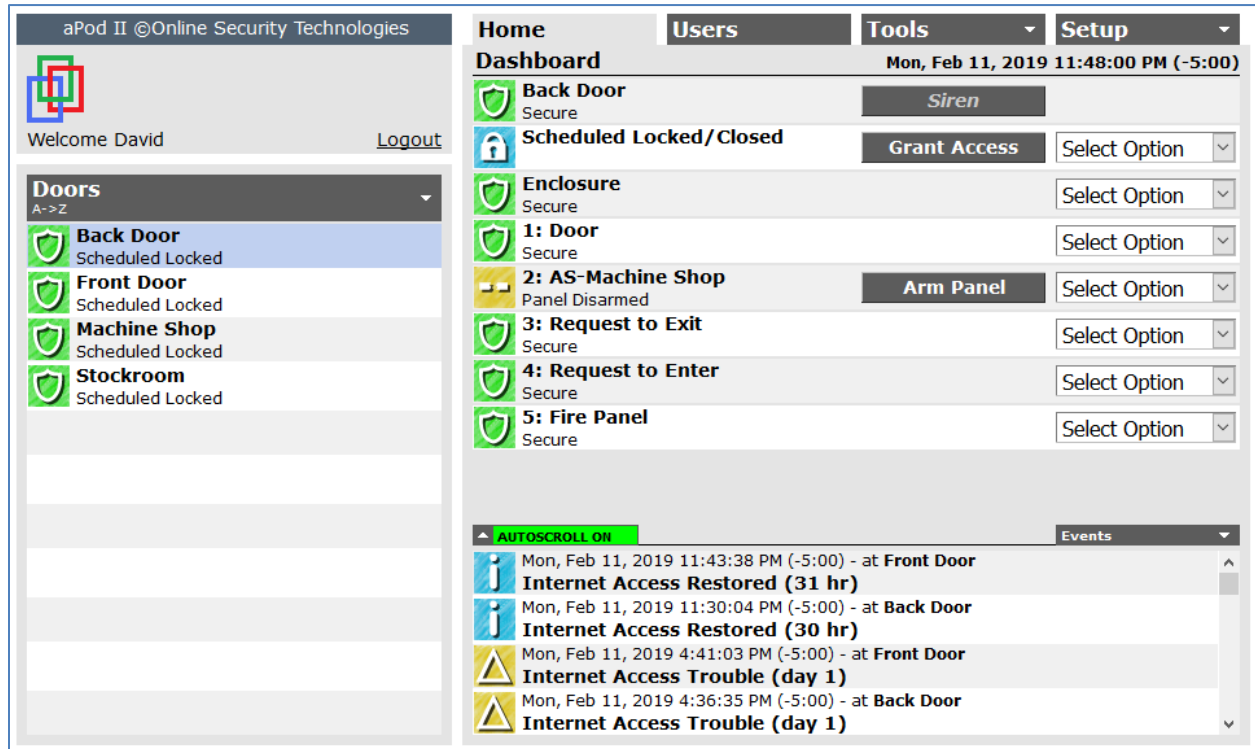
If the aPod II controller is not able to connect with an NTP server, it will report this failure in two ways. An 'Internet Access Trouble' message will be displayed when the problem first occurs and every time an Administrator logs into the system if the problem persists. Also, an 'Internet Access Trouble' event will be recorded in the event log twenty-four hours after the problem is first detected and then daily if the problem persists.



### Important Note:

An NTP failure normally occurs because the aPod II Controller is blocked from the Internet by a firewall. Your IT Administrator can remove this restriction.

The event log records when Internet access is re-established and the length of the outage.



For some very small systems, there may not be an Internet connection and an NTP server will not be available. It is still possible to reset the time of the aPod II Controller if necessary.

Whenever an Administrator logs into the aPod II Browser Interface and the 'Internet Access Trouble' message is displayed as shown above, they can manually update the aPod II time with the time on their PC. When the "NTP failure" condition exists, the System page in the Setup menu will display an 'Update' button between the **PC'S DATE/TIME** field and the **aPod's DATE/TIME** field. Click this button to update the aPod's time with the PC's time.

The screenshot shows the 'Setup' page for an aPod II device. The page is titled 'aPod II ©Online Security Technologies' and has a navigation menu with 'Home', 'Users', 'Tools', and 'Setup'. The 'System' section is active, displaying various configuration fields. A red box highlights the 'Update ->' button next to the 'PC's DATE/TIME' field, which is set to 'Mon, Apr 26, 2021 4:32:37 PM'. A yellow callout box points to this button with the text: 'Click here to set the aPod's time to the time of the connected PC.' Other visible fields include 'SITE NAME' (David Martin Custom Parts), 'SITE ADDRESS' (142 Oakdale Rd, Kingston ON), 'TIME ZONE' (Eastern Time (GMT-5:00)), 'LANGUAGE' (English (en)), 'PRIMARY INTERNET IP' (64.228.90.180), and 'PORT (UDP)' (5268).

## Selected Locale

This field displays the Locale that was selected during the initial Quick Start Wizard setup. If your Locale is not correct, your system time, scheduled holidays and Daylight Savings time changes may not be correct. **The Locale can only be changed by restoring the factory defaults in the Primary Controller. Refer to the 'Restore to Defaults' section on page 73.**

## Primary IP Address

This field displays the fixed IP address on the Local Area Network of the aPod II Primary Controller.

## The Engineering Page

**Note:** There are no administrative tasks associated with this page.

The Engineering page displays system diagnostic information to assist with troubleshooting.

The screenshot shows the 'Engineering' page of the aPod II system. The page is divided into several sections:

- Navigation:** Home, Users, Tools, Setup.
- Engineering Section:**
  - DOOR:** Back Door. IP ADDRESS:PORT: 192.168.2.164:5268. MAC ADDRESS: ee:ee:ee:86:08:89.
  - CURRENT SOFTWARE VERSION:** aPod II 2021\_04\_21 - v3.11 (0e22b3). **DB ROWS TO SYNC:** 0. (Callout 1)
  - STRIKE/OUTPUT #1/AUX12 CURRENT:** Off/Off/On. **BATTERY BACKUP:** Offline.
  - Door Status:** 1: Door (Closed), 2: AS-Machine Shop (Open), 3: Request to Exit (Open), 4: Request to Enter (Open).
  - 5: Fire Panel (Open), 6: NOT USED (Open), ENCLOSURE TAMPER (Closed).** (Callout 2)
  - CARD SCAN TIME READER #1:** Fri, Apr 23, 2021 4:32:45 PM. Configured Format: INVERSE, 50 BITS. (Callout 3)
  - 46 63 F6 7A BF A9 00 (Reader #1), B9 9C 09 85 40 56 C0 (Reader #2).**
  - fr926378; Primary aPod Serial No. #860889/en; vDB-B3829AD6 (5426 bps)** (Callout 4)
- Left Sidebar:** Doors (Back Door, Front Door, Machine Shop, Stockroom). A yellow box contains 'Diagnostics for...' with a list: 1. Software updates, 2. Hardware, 3. Card readers, 4. French language version number, database ID number, communication bandwidth.
- User Info:** Welcome David, Logout.

The **IP ADDRESS:PORT** field displays the LAN address of the selected door controller.

The reader diagnostic data is updated with every card read. The data for either reader #1 or reader #2 will be displayed for doors with two readers depending on which reader was badged.

### Diagnostics for Software Updates

When a new Secondary controller is added to the aPod II Access Control System, the Primary Controller will automatically update the Secondary's database and software to the current versions. When the software in the Primary Controller is updated or if a backup is restored, the Primary Controller will automatically update all the Secondary controllers. This is a fail-safe process. If the update of any controller is interrupted in any way, the process will be repeated until a valid software or database image has been uploaded and verified. When a valid image is available the controller goes offline, is reprogrammed and reboots with the new software and database.

The **CURRENT SOFTWARE VERSION** and the **DB ROWS TO SYNC** fields display status messages which allow you to monitor the progress of the update process for the selected controller.

# Online Security Technologies

...security evolution

The **DB ROWS TO SYNC** field displays the number of rows in the database that need to be updated. The maximum number is 12,526 which indicates that the update process has not yet begun. 0 means the database is up to date.

CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
aPod II 2019Feb07 - v3.00 (0a9a0f)	138

CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
aPod II 2019Feb07 - v3.00 (0a9a0f)	0

The **CURRENT SOFTWARE VERSION** field displays the status of the Secondary controller update process. The software version number is displayed when the process has completed, and the software is up to date.

CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
Evaluating...	0

CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
Updating 21%	0

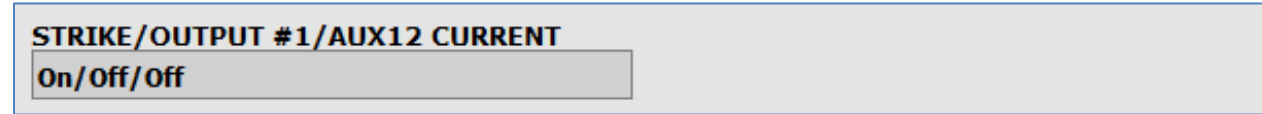
CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
Validating 52%	0

CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
Programming...	0

CURRENT SOFTWARE VERSION	DB ROWS TO SYNC
aPod II 2019Feb07 - v3.00 (0a9a0f)	0

## Diagnostics for Hardware

### Current monitoring



The **STRIKE/OUTPUT #1/AUX12 CURRENT** field indicates whether the strike, output #1 and the auxiliary 12 VDC circuits are turned on or turned off. By default, output #1 is assigned to a piezo siren.

The **STRIKE** and **OUTPUT #1** (Siren) outputs are normally **Off** unless activated by the door controller logic.

The **STRIKE** circuit can be tested by using one of the “door unlock/lock” override functions to maintain activation of the strike. The “door unlock/lock” override functions are available in the drop-down list beside the **Grant Access** button on the Home page.

The **AUX12** circuit is normally **On** if a secondary door peripheral, such as a Request to Exit PIR is connected.

### Input monitoring

<b>1: Door</b> Closed	<b>2: AS-Machine Shop</b> Open	<b>3: Request to Exit</b> Open	<b>4: Request to Enter</b> Open
<b>5: Fire Panel</b> Open	<b>6: NOT USED</b> Open	<b>SYSTEM TAMPER</b> Closed	

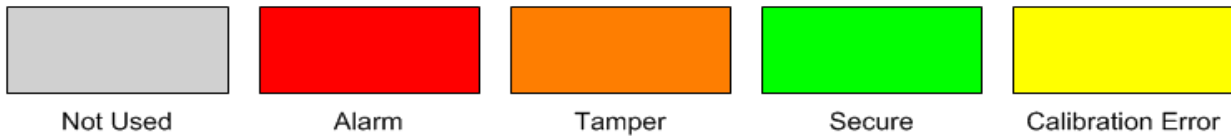
Display fields 1 to 6 correspond with the six optional input points that are assigned on the Doors→Hardware page.

The **value** in the status box indicates the physical state of the input circuit, i.e., **Open** or **Closed** for unsupervised circuits or the resistance values for supervised circuits (**1K**, **2K2** or **5K6 Ω**).





The **colour** of the status box indicates the logical state of the input circuit as determined by the input configuration. The possible states are shown below.



### Notes:

1. The colour designations for 'Alarm' (red) and 'Secure' (green) can also be described as 'Activated' (red) and 'Non-activated' (green). For example, the door contact status for a closed door would be green and the door contact status for an open door would be red, regardless of whether the open door triggers an alarm.
2. By convention, the alarm panel input status is displayed in red when the alarm panel is disarmed and in green when the alarm panel is armed.

The **SYSTEM TAMPER** field displays the status of the aPod II controller tamper switch and is not configurable. The status of its non-activated, secure state is **Closed**.

When the tamper is triggered, **Open** is displayed.

## Diagnostics for the Card Reader

<b>CARD SCAN TIME READER #1</b>	
<b>Tue, Jun 8, 2021 10:30:48 AM</b>	<b>Configured Format</b>
<b>NORMAL, 50 BITS</b>	<b>INVERSE, 50 BITS</b>
<b>46 63 F6 7A BF A8 40</b>	<b>B9 9C 09 85 40 57 80</b>

The **CARD SCAN TIME** field indicates when the last card was read at the reader whether or not the read was valid. The number of bits detected is displayed in the title of the **NORMAL** and **INVERSE** fields, which display the data in the bit stream in hexadecimal format. The **INVERSE** data is the complement of the **NORMAL** data.

By calculating both the **NORMAL** and **INVERSE** data, the aPod II controller can process the reader signals, even if the Data 0 and Data 1 inputs from the reader are reversed.

## Cards

**Note:** There are no administrative tasks associated with this page.

The aPod II controller can be connected to any commercially available access token or biometric reading device that outputs either industry standard Wiegand or MagStripe signals. The controller can be configured to accept any non-encrypted token format. A few common card formats for the Wiegand encoding technology dominate the access control market. To simplify installation, these formats are included in a format library. They are automatically configured, when the first card is badged on the reader connected to the Primary Controller. Additional formats can be added if necessary.

The screenshot shows the 'Cards (edit)' page in the aPod II web interface. The page has a top navigation bar with 'Home', 'Users', 'Tools', and 'Setup' (highlighted in yellow). The main content area is titled 'Cards (edit)' and contains the following fields:

- CARD NAME:** Auto Wiegand 50-Bit
- CARD ENCODING:** Wiegand (dropdown menu)
- BITS:** 50
- IDENTIFIER:** 18
- LENGTH:** 32
- OFFSET:** 0
- SITE CODE:** 2
- LENGTH:** 16
- SITE CODE #1:** 29496
- SITE CODE #2:** (empty)
- SITE CODE #3:** (empty)
- SITE CODE #4:** (empty)
- KEY:** 1
- LENGTH:** 8
- ODD PARITY:** Checked (dropdown menu)
- START:** 26
- LENGTH:** 24
- PLACEMENT:** 50
- EVEN PARITY:** Checked (dropdown menu)
- START:** 2
- LENGTH:** 24
- PLACEMENT:** 1

At the bottom of the page, there are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'.

Your system service provider can use the [Cards](#) page to configure one or more access token data formats. This will allow the aPod II Controller to handle any of the following situations.

- a different, less common card format
- key code formats for keypad readers
- additional site codes to a maximum of four
- additional card formats for multiple reader technologies

The OST proximity reader and cards are pre-programmed with a default site code. It is not necessary to use different site codes for different locations because the large 50-Bit card format ensures that every card sold has a unique ID number. However, you can add up to four site

codes to the aPod II database if your system uses another reader and cards which require them. This would allow you to use the same card in different systems in four locations.

The aPod II controller also supports simultaneous multiple card formats. Normally you would not use two types of card reader with different formats in your system, because this would require that Users carry two tokens and always use the correct one at every door. There are situations where a different card format may be acceptable. For example, an RF token that opens a garage door from inside your car may output a 26-Bit Wiegand format where the door access readers output a 50-Bit format. The aPod II controller can accommodate this situation.



## Monitor and Control the System

### Home - Dashboard

The system Dashboard is displayed when you click the Home tab in the navigation menu. Use the Dashboard to monitor and control the status of all the doors and alarm inputs in your system in real time. The dashboard is divided into three areas. Select the door from the list on the left and its current status and control buttons are displayed in the information panel on the right. All system events are listed in the event log in real time.

The screenshot shows the 'aPod II' security system dashboard. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The main content area is titled 'Dashboard' and shows the date and time: 'Wed, Jan 23, 2019 3:03:26 PM (-5:00)'. On the left, a 'Doors' list shows 'Back Door' (Scheduled Locked), 'Front Door' (Pending Unlock), 'Machine Shop' (Pending Unlock), and 'Stockroom' (Scheduled Locked). The main panel displays details for the selected 'Back Door', including its status (Secure), control buttons (Siren, Grant Access, Arm Panel), and a list of optional inputs (1: Door, 2: AS-Machine Shop, 3: Request to Exit, 4: Request to Enter, 5: Fire Panel). The bottom right section shows an 'Event log' with a list of recent access events, such as 'Access Office by David Martin' and 'Access Office by Jane Anderson'.

The main door information panel is divided into two areas. The top two lines are always displayed and provide status information and controls for the selected door.

The remainder of the panel provides status information and controls for the enclosure tamper and optional door inputs. The aPod II controller can receive six optional inputs. These can be used to enhance the access control operation of the door or simply monitored as separate security points. Inputs are only displayed if they are used and configured. The first and second inputs are normally used for a Request to Exit input and a door contact input, but this is not mandatory. Refer to page 51 in the about door inputs.

The screenshot shows the 'aPod II ©Online Security Technologies' dashboard. The main area displays a list of doors with their status and control options. The doors listed are: Back Door (Scheduled Locked), Front Door (Pending Unlock), Machine Shop, 1: Door, 2: AS-Machine Shop (Panel Disarmed), 3: Request to Exit, 4: Request to Enter, and 5: Fire Panel. Each door has a 'Secure' status and a 'Select Option' dropdown menu. The 'AS-Machine Shop' door has an 'Arm Panel' button. The 'Back Door' has a 'Siren' button, and the 'Scheduled Locked/Closed' door has a 'Grant Access' button. A red box highlights the door list, and a blue box highlights the control buttons. Two callout boxes provide information about the door status and controls.

Door status information and controls. Always displayed.

Inputs status information and controls. Only displayed if configured.

Click the header above the door selection list to choose one of two sort options. By default, the list is sorted alphabetically on the door name, but you can also sort "By Exception". The doors would then be listed in order of their status as shown below. The exception list will automatically re-sort as door status changes.

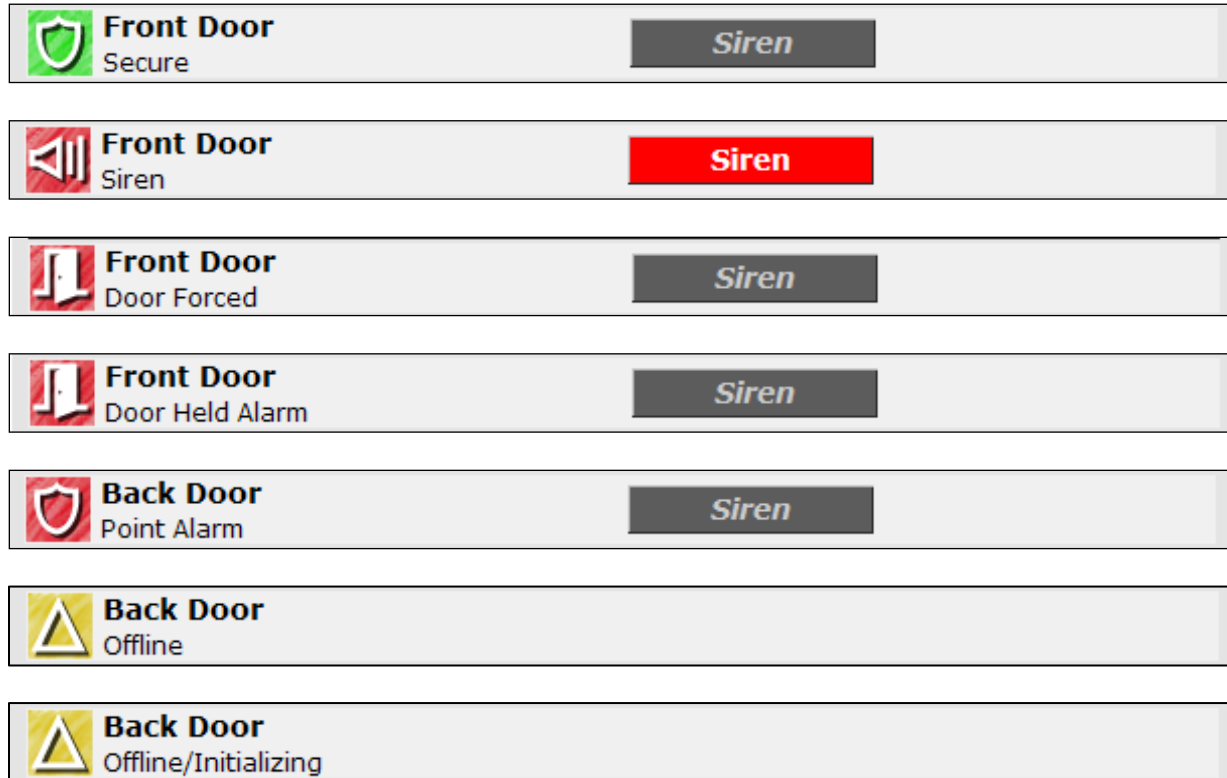
The screenshot shows the 'Doors' section of the dashboard, sorted by Exception. The 'Doors' header is highlighted in blue, and a mouse cursor is pointing at it. The status 'Exception' is displayed below the header.

## Exception Sort Order

- Siren active
- Door forced alarm
- Point alarm
- Door held open alarm
- Door offline
- Tamper alarm
- Door secure

## Door security status

The first line of the information panel displays the door name and its current security status. The seven door security status conditions are listed below.



### Cancel alarms.

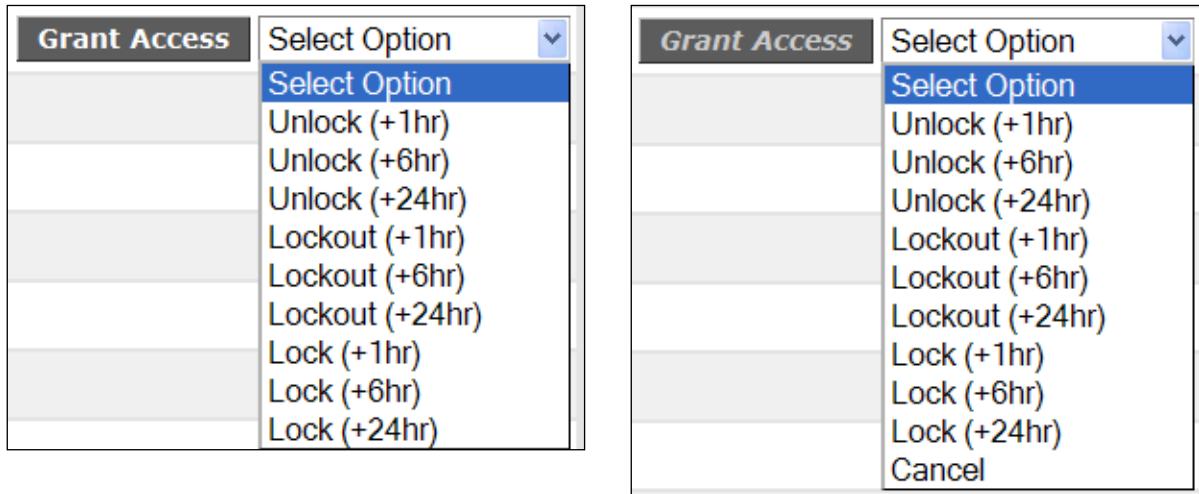
When the aPod II controller detects an alarm condition, it turns on the buzzer in the card access reader and activates the siren circuit. Installing a siren is optional but may be appropriate for a high security door. When the siren is activated, the **Siren** button will flash a bright red.

Click the **Siren** button to cancel the alarm and turn off the siren and the buzzer in the card access reader. The alarm can also be cancelled at the door by badging the access reader provided the card holder has been given the 'Silence Alarms' permission. 'Door forced' and 'Door held open' alarms can both be configured to log alarms without siren activation.

## Door locked/unlocked status and open/closed status

The second line of the information panel displays the door locked/unlocked status and the open/closed status. Of course, the open/closed status and associated alarms can only be displayed if a door contact is installed. There is a **Grant Access** button and a drop-down list with various options for overriding the door locking schedule.

### Override door schedules



When an override is selected, the 'Cancel' option is added to the list.

Use the 'Unlock' options to override a scheduled 'locked' period and the 'Lock' options to override a scheduled 'unlocked' period. During a 'Lock' override, Users with access permission can unlock the door with their access token. Choose the 'Lockout' option to lock the door and prevent all Users from gaining access.

Depending on the option selected, the override will automatically time out after 1 hour, 6 hours or 24 hours. Other override intervals can be set by selecting an interval multiple times. For example, select 24 hours twice for a 48-hour interval. The time when the override expires is displayed beneath the locked/unlocked status. The override can be cancelled at any time by selecting the 'Cancel' option.

### User controlled schedule overrides







There are times when it is appropriate to allow a User to override a schedule and unlock or lock a door temporarily without having administrative access to the system software. For example, a club member who is not a System Administrator needs to unlock the members' entrance at the beginning of a planned event and then lock it again when the event is over.

A User can toggle a door between its 'locked' and 'unlocked' states by badging their card at the reader three times in a row if they have been assigned the authority to perform this function.





Refer to page 113 in the Manage Users chapter of the guide for more information about User controlled schedules.

The various door status conditions are listed below.

### Scheduled locked intervals







 <b>Scheduled Locked/Closed</b>	<b>Grant Access</b>	Select Option 
 <b>Scheduled Locked/Open</b>	<b>Grant Access</b>	Select Option 
 <b>Scheduled Locked/Held</b>	<b>Grant Access</b>	Select Option 

### Scheduled unlocked intervals

 <b>Scheduled Unlock/Closed</b>	<i>Grant Access</i>	Select Option 
 <b>Scheduled Unlock/Open</b>	<i>Grant Access</i>	Select Option 

### Pending unlocked intervals







A scheduled unlock period has begun but the door remains locked until an authorized User opens it with a valid token. This ensures that an automatic unlock schedule will not compromise the security of your premises. This is the default option.

 <b>Pending Unlock/Closed</b>	<b>Grant Access</b>	Select Option 
 <b>Pending Unlock/Open</b>	<b>Grant Access</b>	Select Option 
 <b>Pending Unlock/Held</b>	<b>Grant Access</b>	Select Option 







## Unlock override

These conditions are displayed when you manually override a scheduled unlock period.

 <b>Locked/Closed</b> Until 19 May 10:59 AM	<b>Grant Access</b>	Select Option 
 <b>Locked/Open</b> Until 19 May 10:59 AM	<b>Grant Access</b>	Select Option 
 <b>Locked/Held</b> Until 19 May 10:59 AM	<b>Grant Access</b>	Select Option 







## Lock override

These conditions are displayed when you manually override a scheduled lock period.

 <b>Unlocked/Closed</b> Until 19 May 11:17 AM	<b>Grant Access</b>	Select Option 
 <b>Unlocked/Open</b> Until 19 May 11:17 AM	<b>Grant Access</b>	Select Option 

## Lockout override

These conditions are displayed when you manually override a scheduled lock or unlock period and deny access to all users.

 <b>Lockout/Closed</b> Until 19 May 11:23 AM	<b>Grant Access</b>	Select Option 
 <b>Lockout/Open</b> Until 19 May 11:23 AM	<b>Grant Access</b>	Select Option 
 <b>Lockout/Held</b> Until 19 May 11:23 AM	<b>Grant Access</b>	Select Option 

## Fire system unlock

An output from a fire alarm system can be connected to any one of the six inputs on any aPod II controller. If a fire alarm is triggered, the aPod II controller will automatically unlock the door and send a command to all other controllers in the same facility to unlock their doors. When this occurs one of the following door status conditions will be displayed.

 <b>Unlocked/Closed</b> Indefinitely by Fire Alarm	<b>Grant Access</b>	Select Option 
--	---------------------	---

 <b>Unlocked/Open</b> Indefinitely by Fire Alarm	<b>Grant Access</b>	Select Option 
--	---------------------	---

The doors are re-locked when the fire alarm has been cancelled and the aPod II System unlock command has been reset.

### User controlled unlock override

These conditions are displayed when an authorized User temporarily overrides a scheduled unlock period use the 3X badging lock/unlock function.

 <b>Locked/Closed</b> Temporarily	<b>Grant Access</b>	Select Option 
---	---------------------	---

 <b>Locked/Open</b> Temporarily	<b>Grant Access</b>	Select Option 
---	---------------------	---

 <b>Locked/Held</b> Temporarily	<b>Grant Access</b>	Select Option 
---	---------------------	---

### User controlled lock override

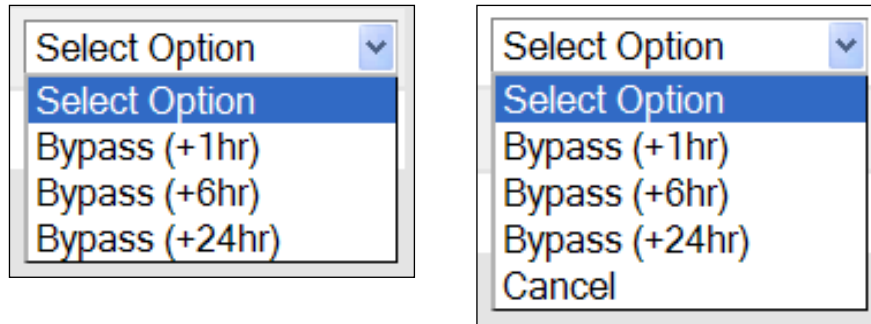
These conditions are displayed when an authorized User temporarily overrides a scheduled lock period use the 3X badging lock/unlock function.

 <b>Unlocked/Closed</b> Temporarily	<b>Grant Access</b>	Select Option 
---	---------------------	---

 <b>Unlocked/Open</b> Temporarily	<b>Grant Access</b>	Select Option 
---	---------------------	---

## Input point status

The next seven lines of the information panel display the names and the security status of the aPod II enclosure tamper plus six optional input points. There is a drop-down list with three bypass options for each point. When a point is bypassed, it is disabled and cannot trigger an alarm. Normally this is not required but could be useful for example, if the controller is being serviced.

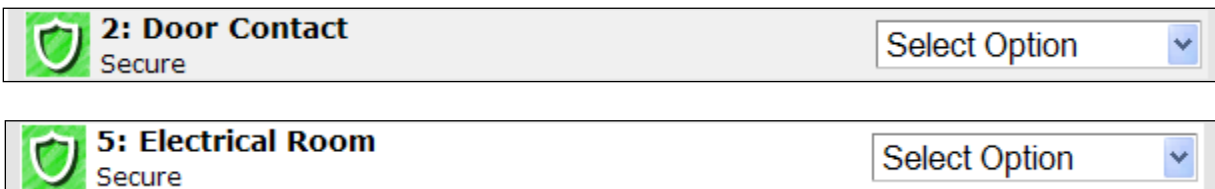


When an override is selected, the 'Cancel' option is added to the list.

There are eleven types of input points. Refer to page 51 for more information about input points.

### Secure state

When secure, all input point types except for 'Alarm Panel' display the following status condition.



### Point active state

The 'Request to Exit', 'Request to Exit (D/O)', 'Request to Enter (D/O)', 'Door', 'Door Bypass' and 'Interlock' input point types display the following status condition when triggered.



### Alarm State

The 'Enclosure', 'Reader', 'Alarm 24 Hour', 'Alarm Conditional', and 'Fire Panel' input point types display the following status condition when triggered and will activate the reader buzzer and siren.



## Alarm Conditional input

The activation of this input depends on one of two conditions.

- When used in conjunction with the aPod II alarm panel interface, it will display the “alarm” state if triggered when the area is armed and the “point active” state if triggered when the area is disarmed.
- If the conditional input is connected to an alarm point that is not part of an area managed by the alarm panel interface, it will only trigger an alarm if it occurs during an ‘After Hours’ or ‘Extended Hours’ time period in the door schedule.

## Alarm Panel input

The displayed status of the alarm panel input will follow the armed/disarmed status of the alarm panel. Refer to page 159 for more information about the alarm panel interface.



## High Security (Supervised) input points

Supervised circuits use an end of line (EOL) resistor to detect line faults in the field wiring which may occur accidentally or could be the result of sabotage. The aPod II controller will detect a known voltage drop across the input circuit with an end of line resistor installed. A cut line (open circuit) or a bypassed detector (short circuit) will produce an input alarm or a tamper alarm depending on the normal open/closed status of the circuit. Either way, if the field wiring is faulty or tampered, an alarm condition will be reported.



The tamper alarm is *schedule dependent*. If a line fault is detected during an unlock schedule, unlock pending or Regular Hours, the ‘Tamper’ status condition is displayed, and the reader buzzer is activated. At all other times, the line fault is treated like an input alarm. The ‘Alarm’ status condition is displayed, and the reader buzzer and siren are activated.

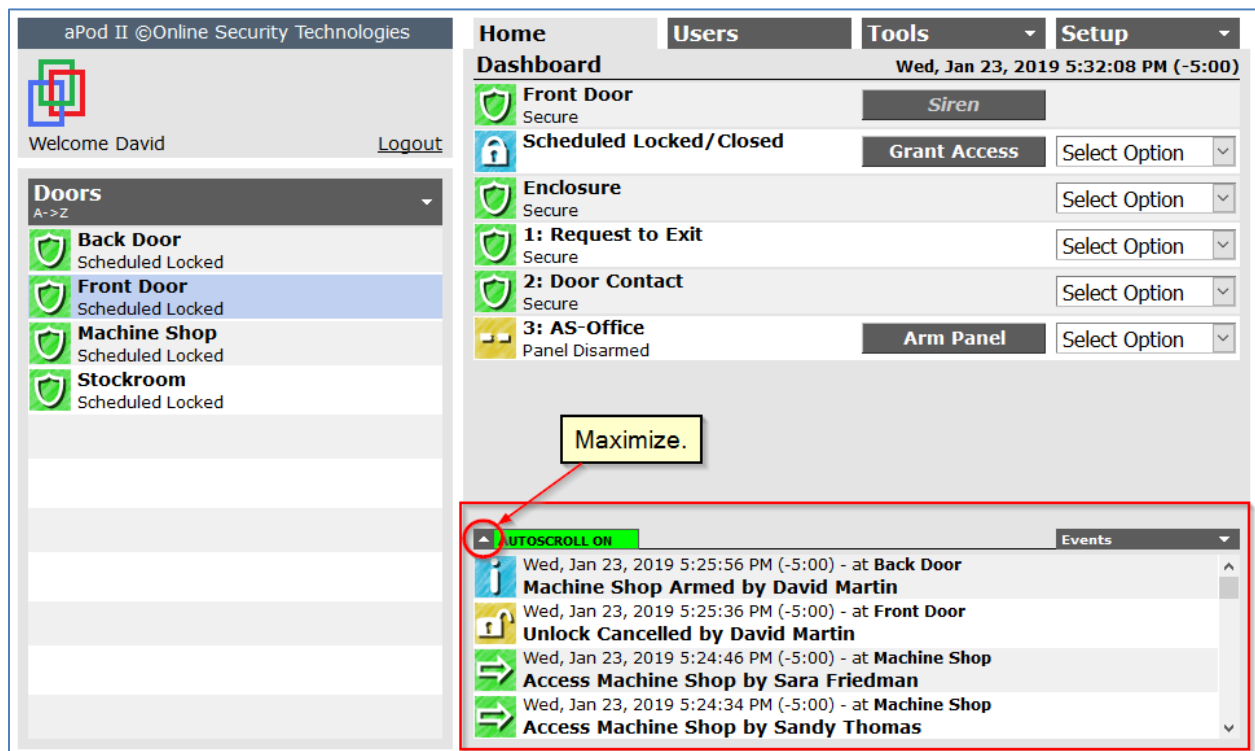
## The event log

The event log captures system events in real time and displays them on the dashboard with the most recent event at the top of the list. You can expand the list to display more events, filter events by type, and control scrolling.

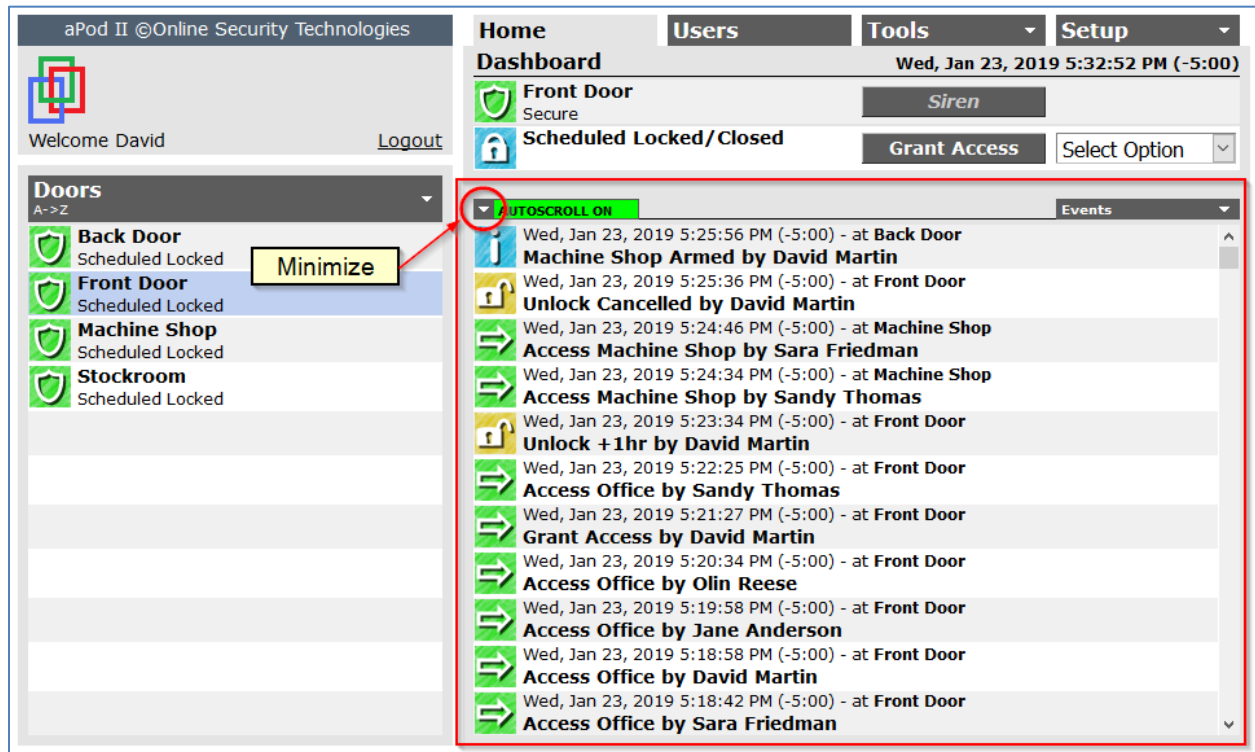
When **AUTOSCROLL ON** is displayed, events are captured and listed in real time.

When **AUTOSCROLL OFF** is displayed, events are stored in memory, but the updating of the display is suspended and scrolling stops. When the scroll bar is moved down, auto scrolling stops automatically. Clicking the auto scroll button will toggle between a real time and static display.

Click the “up” arrow icon in the top left corner of the event log to expand the event log.



Click the “down” arrow in the top left corner to minimize the event log.



Above the event log, on the right-hand side is a filter menu which by default shows all events. Choose another option to display only alarms, bad cards, or audit events.



The Home page event log is useful for monitoring the most recent events as they occur. Otherwise, it is more convenient to use the Reports function on the Tools menu to display or export events using a variety of filters.

## *The Access Denied response*

When a User presents their access token to a card reader, the door will unlock if they have permission to enter. If they do not have permission to enter the door will stay locked, the reader buzzer will sound six times and the reader LED will flash green in unison.

There are several reasons why a User may be denied access at a controlled point of entry.

- Permission is not granted for this time interval.
- The wrong PIN was entered in card plus PIN mode.
- Permission is not granted if the alarm panel is armed, and the User does not have the disarming permission.
- There may be an anti-passback lockout in force.
- The access card may not be enrolled.
- The temporary access card may have expired.
- There may be a door lockout in force.
- There may be a system-wide lockdown in force.
- The User's card may be suspended.
- The maximum occupancy count in a monitored area may have been reached.

The specific reason will be recorded in the event log of the aPod II System. When a User's token fails to unlock the door, you should check the event log to determine if this is a valid event or simply a configuration error.

The event log stores 100,000 events in a rotating buffer. Use the filtered reports to access more data.

## Reports

Use the aPod II reporting functions to review the performance of your access control system and to investigate security problems. The available reports address all common areas of interest.

The screenshot shows the 'Reports' section of the aPod II interface. It includes a navigation bar with 'Home', 'Users', 'Tools', and 'Setup'. The 'Reports' section contains several fields: 'REPORT TYPE' (set to 'Events by User Name'), 'BY DOOR' (set to 'All Doors'), 'FROM' (set to 'Oldest'), and 'UNTIL' (set to 'Newest'). There are also fields for 'FIRST NAME' and 'LAST NAME'. Below these are 'REPORT FORMAT' options for 'HTML' (selected) and 'TSV', and a 'REPORT HEADER' field. A 'Report' button is highlighted with a red box, and a yellow callout box contains the text 'Click here to run the report.' A legend box at the bottom right lists four steps: 1. Choose your report type, 2. Enter filter parameters, 3. Choose your report format, and 4. Enter a custom report header. The interface also shows a 'Welcome David' message and a 'Logout' link.

## Report Type

Use the **REPORT TYPE** drop-down list to choose a report which addresses your area of interest.

A close-up of the 'REPORT TYPE' drop-down menu. The menu is open, showing a list of report types. The 'Events (All)' option is highlighted in blue. The list includes: Events (All), Administrators, Areas, Audit, Cards, Dates, Doors, Events (All), Events by Administrator Name, Events by User Name, Events/Alarms, Events/Bad Cards, Events/Denied Access, Shifts, and Users.



## Report Filters

Filter system events by door. The default is all events at all doors.

### Reports

<b>REPORT TYPE</b> Events (All) ▼	<b>BY DOOR</b> Back Door ▼ All Doors Back Door Front Door Machine Shop Stockroom
<b>FROM</b> Oldest ▼	
<b>REPORT FORMAT</b> <input checked="" type="radio"/> HTML <input type="radio"/> TSV	
<b>REPORT HEADER</b> <input type="text"/>	
<b>Report</b>	

Filter your system events with start and stop times.

### Reports

<b>REPORT TYPE</b> Events (All) ▼	<b>BY DOOR</b> Back Door ▼
<b>FROM</b> Oldest ▼	<b>UNTIL</b> Newest ▼
<b>REPORT FORMAT</b> <input checked="" type="radio"/> HTML <input type="radio"/> TSV	<div style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">All reports based on system events allow you to query a specific time period. The default is all records.</div>
<b>REPORT HEADER</b> <input type="text"/>	
<b>Report</b>	

Click on the **FROM** field to open the date/time applet. Select the desired time and date.

The screenshot shows the 'Reports' section of the 'aPod II' interface. The 'FROM' field is highlighted in yellow and contains the text 'January 6, 2019 12:00AM'. A date/time applet is open below it, displaying a calendar for January 2019. The date '6' is selected, and the time is set to '12:00 AM'. A red arrow points from a text box to the 'FROM' field. The text box contains the following instructions:

Click the FROM field to display the date/time applet. Select the 'from' date and time for the reporting interval and click OK.

Click on the **UNTIL** field to open the date/time applet. Select the desired time and date.

The screenshot shows the 'Reports' section of the 'aPod II' interface. The 'UNTIL' field is highlighted in yellow and contains the text 'January 20, 2019 12:00AM'. A date/time applet is open below it, displaying a calendar for January 2019. The date '20' is selected, and the time is set to '12:00 AM'. A red arrow points from a text box to the 'UNTIL' field. The text box contains the following instructions:

Click the UNTIL field to display the date/time applet. Select the 'until' date and time for the reporting interval and click OK.

Track events by User or by Administrator.

### Reports

<b>REPORT TYPE</b> Events by User Name	<b>BY DOOR</b> All Doors
<b>FROM</b> Oldest	<b>UNTIL</b> Newest
<b>FIRST NAME</b> Jane	<b>LAST NAME</b> Anderson
<b>REPORT FORMAT</b> <input checked="" type="radio"/> HTML <input type="radio"/> TSV	<div style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">Enter FIRST NAME, LAST NAME or both to filter the 'Events by User Name' or the 'Events by Administrator Name' reports.</div>
<b>REPORT HEADER</b> <input type="text"/>	
<b>Report</b>	

## Database Reports

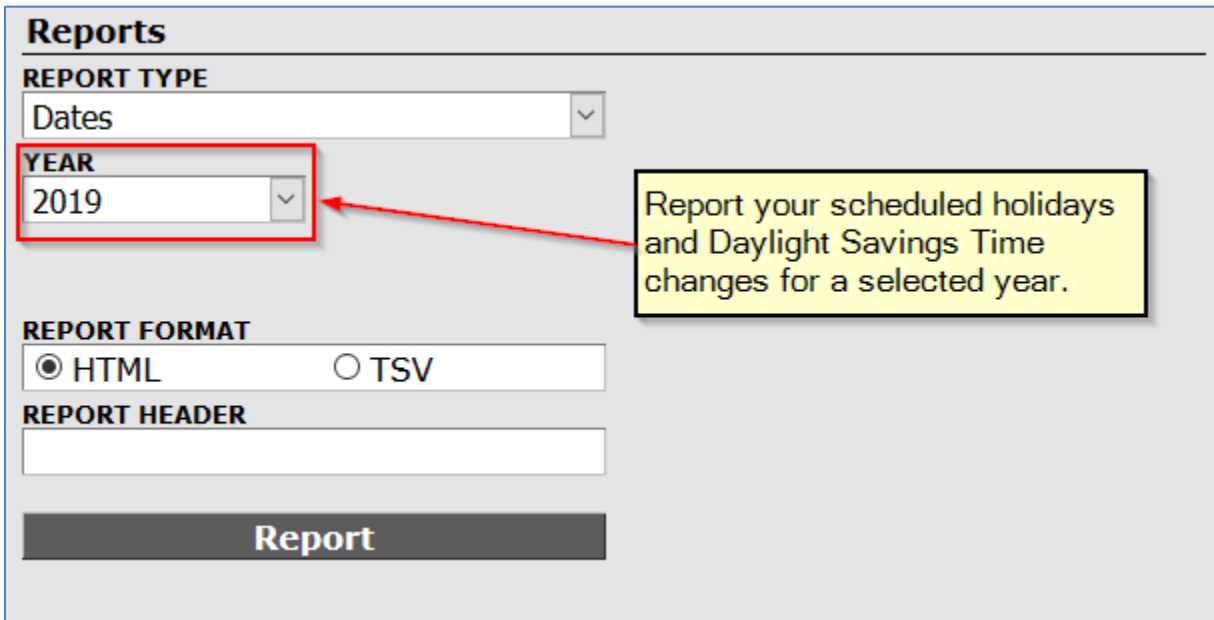
Some reports are based on database entries. Use these reports to check for entry errors and omissions.

Archive the 'Doors' report. This information will be useful to your service provider.

### Reports

<b>REPORT TYPE</b> Doors	<div style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">Database reports help you to set up and maintain your system.</div>
<b>REPORT FORMAT</b> <input checked="" type="radio"/> HTML <input type="radio"/> TSV	
<b>REPORT HEADER</b> <input type="text"/>	
<b>Report</b>	

List the scheduled holidays and Daylight Savings time changes for your locale.



**Reports**

REPORT TYPE  
Dates

YEAR  
2019

REPORT FORMAT  
 HTML  TSV

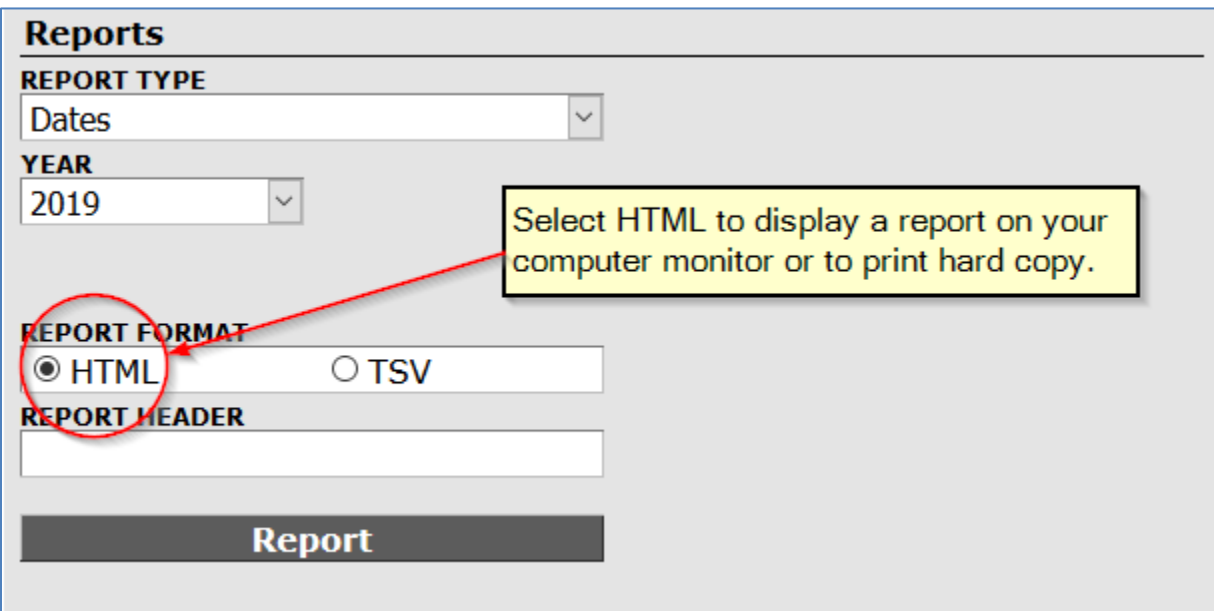
REPORT HEADER

Report

Report your scheduled holidays and Daylight Savings Time changes for a selected year.

## Report Format

Use the **HTML** report format to display reports on your computer monitor or to print hard copy.



**Reports**

REPORT TYPE  
Dates

YEAR  
2019

REPORT FORMAT  
 HTML  TSV

REPORT HEADER

Report

Select HTML to display a report on your computer monitor or to print hard copy.

Name	Date	Observed
New Year	Tue, Jan 1, 2019	Tue, Jan 1, 2019
Family Day	Varies	Mon, Feb 18, 2019
Good Friday	Varies	Fri, Apr 19, 2019
Easter Monday	Varies	Mon, Apr 22, 2019
Victoria Day	Varies	Mon, May 20, 2019
Canada Day	Mon, Jul 1, 2019	Mon, Jul 1, 2019
Civic Holiday	Varies	Mon, Aug 5, 2019
Labor/Labour Day	Varies	Mon, Sep 2, 2019
Thanksgiving (Canada)	Varies	Mon, Oct 14, 2019
Remembrance Day	Mon, Nov 11, 2019	Mon, Nov 11, 2019
Christmas	Wed, Dec 25, 2019	Wed, Dec 25, 2019
Boxing Day	Thu, Dec 26, 2019	Thu, Dec 26, 2019
Daylight Spring Forward	Varies	Sun, Mar 10, 2019
Daylight Fall Back	Varies	Sun, Nov 3, 2019

The **PRINT** and **CLOSE** buttons will not appear on the printed report.

Use the **TSV** (*tab separated values*) report format to save reports to your computer hard drive.

**Reports**

**REPORT TYPE**  
Dates

**YEAR**  
2019

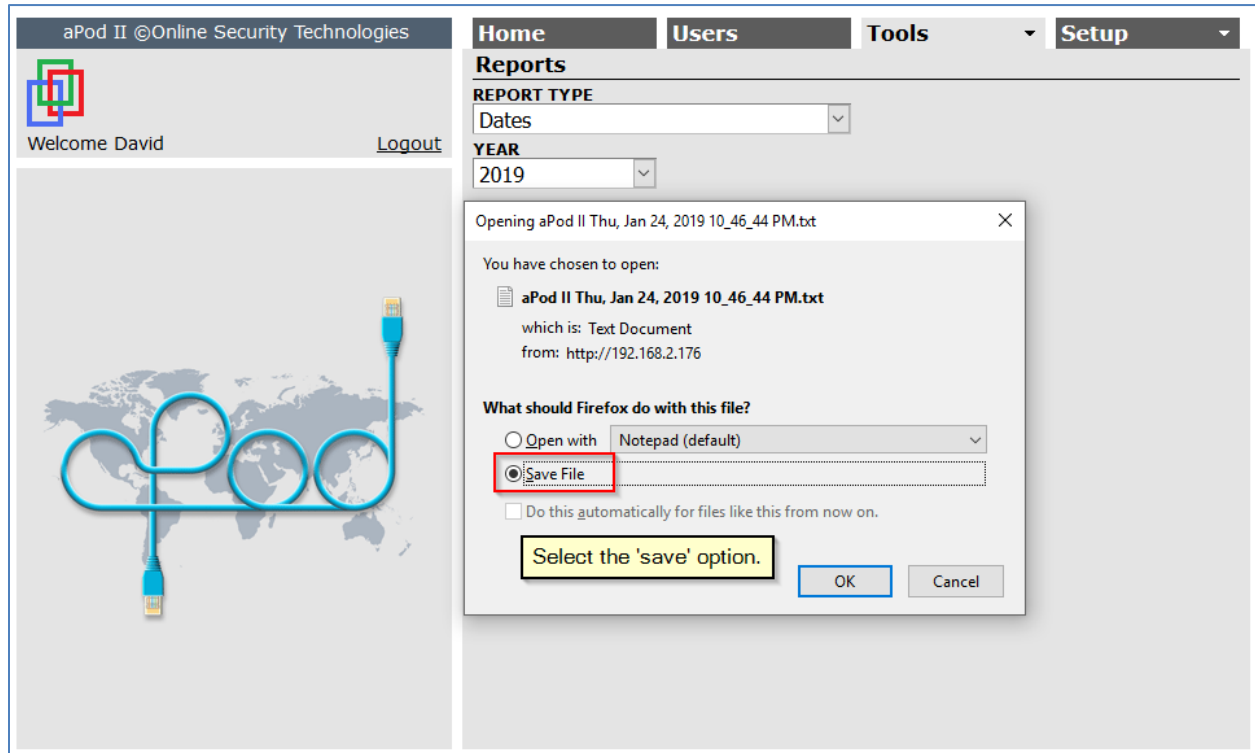
**REPORT FORMAT**  
 HTML  TSV

**REPORT HEADER**  
[Empty text field]

**Report**

Select TSV to save a report to your drive as a text file. You can email the saved report or import it into Excel.

Click the **Report** button, select the Save option if presented by your Browser and then browse to a folder location to save the report file.



FireFox 64.0 on Windows 10

## Custom Report Header

Add a custom header to your HTML report.

**Reports**

**REPORT TYPE**  
Dates

**YEAR**  
2019

**REPORT FORMAT**  
 HTML  TSV

**REPORT HEADER**  
David Martin Custom Parts

**Report**

Access Control Report - Mozilla Firefox

192.168.2.176/REPORT0AAAAABwAAABKAAW4qWoNoAbK2FxWVOAfa6IKkD

### Access Control Report

Print Close

**David Martin Custom Parts**  
**Holidays - Year 2019**

Name	Date	Observed
New Year	Tue, Jan 1, 2019	Tue, Jan 1, 2019
Family Day	Varies	Mon, Feb 18, 2019
Good Friday	Varies	Fri, Apr 19, 2019
Easter Monday	Varies	Mon, Apr 22, 2019
Victoria Day	Varies	Mon, May 20, 2019
Canada Day	Mon, Jul 1, 2019	Mon, Jul 1, 2019
Civic Holiday	Varies	Mon, Aug 5, 2019
Labor/Labour Day	Varies	Mon, Sep 2, 2019
Thanksgiving (Canada)	Varies	Mon, Oct 14, 2019
Remembrance Day	Mon, Nov 11, 2019	Mon, Nov 11, 2019
Christmas	Wed, Dec 25, 2019	Wed, Dec 25, 2019
Boxing Day	Thu, Dec 26, 2019	Thu, Dec 26, 2019
Daylight Spring Forward	Varies	Sun, Mar 10, 2019
Daylight Fall Back	Varies	Sun, Nov 3, 2019



## Manage Users

Users of your aPod II access control system are sometimes called cardholders. They are employees, residents, contractors, or visitors who have a valid reason for using your facility and have been given permission to unlock certain doors at certain times.

Managing users is your primary administrative task. The Users page makes it easy to add and delete users, enroll their access tokens, and modify their information and access permissions.

aPod II @Online Security Technologies

Welcome David Logout

Home Users Tools Setup

**Users (edit)**

FIRST NAME: Richard LAST NAME: Evans **1.**

**OPTIONS**

Assisted Access  Deny entry if Armed **2.**

Suspended

3X Lock/Unlock

3X Arming

Silence Alarms

Pending Unlock

ACCESS CARD: 319455408 **3.** READER KEYPAD OPTIONS: None

VALID FROM: Now VALID UNTIL: Forever **4.**

USER ID: 4 PIN: Unassigned **5.**

**DOOR ACCESS BY SCHEDULE**

Back Door **6.** REGULAR HOURS

Front Door ALWAYS

Machine Shop REGULAR HOURS

Stockroom NO ACCESS

Add Save Cancel Delete

**USER Management Functions.**

1. Edit the User's name.
2. Assign options.
3. Enroll the access token.
4. Make a token temporary.
5. Assign a PIN.
6. Assign access permissions.

**Note:** The **DOOR ACCESS** selection box is not displayed in a single door system when the access authorization method is 'By Door'. With this simple configuration, there are no schedules assigned to the door, so a User is given 24 X 7 access when they receive their token.

The **USER ID** and **PIN** fields, and the "3X Arming", "Pending Unlock" and "Deny Entry if Armed" options are only displayed if those features are enabled in the system.



## Add a User.

Click the **Add** button to create a new User record. Enter the first and last names in the appropriate fields. The 'first name + last name' combination must be unique.

### User Options

Additional attributes or permissions may be assigned to a User by checking the appropriate option checkbox.

#### *Assisted Access*

Some Users may need assistance when entering or exiting through a door controlled by the aPod II System. If this option is checked, the User will be granted additional unlock time. The default unlock time is 5 seconds and the default extended time is an additional 3 seconds. Both values are configurable. Refer to page 43 for more information.

The aPod II System can be interfaced to an automatic door opener. If the 'Assisted Access' option is selected the automatic door opener will be activated as follows.

- When the door is locked, a valid card swipe will enable the automatic door opener. Pressing the 'Request to Enter' button will first unlock the door and then activate the automatic door opener. Pressing the 'Request to Enter' button without a valid card swipe will not open the door but pressing the 'Request to Exit' button will trigger the unlock/activation sequence.
- When the door is unlocked, pressing either the 'Request to Enter' button or the 'Request to Exit' button will activate the automatic door opener.

If the 'Assisted Access' option is not selected, a valid card swipe will unlock the door, but the door must be opened manually.

When a Grant Access command is issued to a door with an automatic door opener, the door will be unlocked, and the automatic door opener will be enabled.

#### *Suspend*

The User remains active but the card itself is disabled locking the User out of all doors. This option also disables the use of ID+PIN.

## 3X Lock/Unlock

When this option is selected, a User is authorized to temporarily override a door's locking schedule by badging their card three times at the access reader. This is a toggle function. If the door is locked, 3X badging will unlock it. If the door is unlocked, 3X badging will lock it.

This option allows trusted Users to manage an ad hoc door locking schedule without having administrative access to the system.

This function is only available to the User during door schedules for which they have access permission.

When using the 3X Lock/Unlock function, allow 1 second between each card swipe. **The reader buzzer should beep after each swipe.** This is necessary because most access readers have a short lockout period after each card swipe to prevent accidental double reading of the same token.

If the door is locked, the first card swipe will unlock the door. This is normal operation. Two more card swipes in sequence will maintain the door in an unlocked state.

The action of the door strike and the color of the access reader LED provide immediate feedback that the door locked state has changed.

If a User does not reverse their lock/unlock action manually, the door 'locked state' will revert to its scheduled 'locked state' at the beginning of the next scheduling interval.

## 3X Arming

When this option is selected, a User is authorized to arm the alarm panel by presenting their card three times to a reader at any access point to the armed area. *This option is not displayed on the Users page if an alarm panel interface is not configured in the system.*

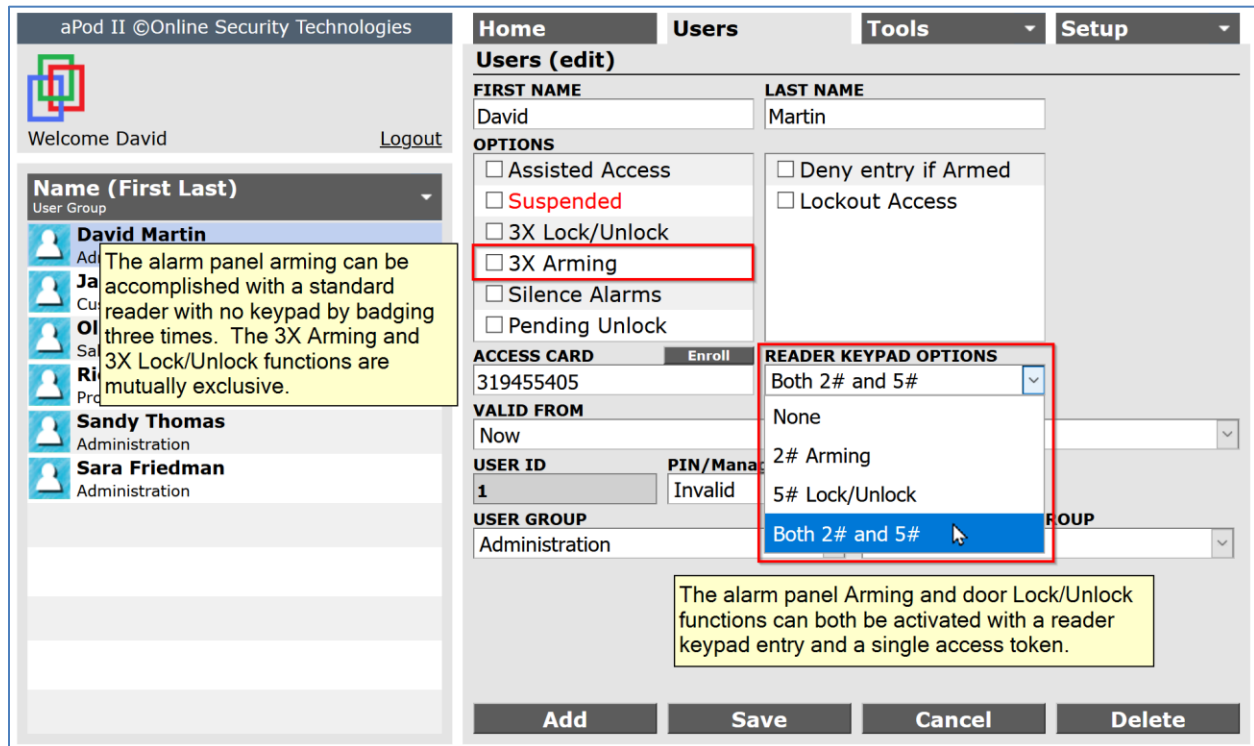
The alarm panel arming function is area centric. A secure area can be armed or disarmed from any access point. All controlled doors to the area are automatically locked when the area is armed. Refer to page 159 for more information about the alarm panel interface.

## Keypad Options

The '3X Lock/Unlock' and '3X Arming' options are mutually exclusive. Badging three times will either unlock the door if the first option is selected or arm the alarm panel if the second option is selected. If a User needs to have both functions, you can create an alternate Username for them and assign the second option to the other token.

There is another way to assign both the '3X Lock/Unlock' and '3X Arming' functions to an administrator but it can only work if there is a keypad reader installed at the access point.

Use the **READER KEYPAD OPTIONS** drop down list to assign one or both options.



If a keypad reader has been installed at a door, then a user can arm the alarm panel by entering “2” followed by “#” followed by badging the key tag. A similar sequence using “5” will toggle the lock/unlock state.

The 3X badging method is still available for doors with standard readers, but only one of the two functions is available for a single key tag with this method.

### Silence Alarms

This allows the User to silence alarms at a door by badging their card at the door’s reader.

### Pending unlock

Use this option to allow a User to unlock a door for the duration of its scheduled unlock period. Users without this option, will be granted access if they have permission but the unlock schedule will not begin until a valid User unlocks the door. Refer to page 44 for more information. *This option is not displayed on the Users page unless there is at least one door configured for ‘pending unlock by designated user’.*

## Deny Entry if Armed

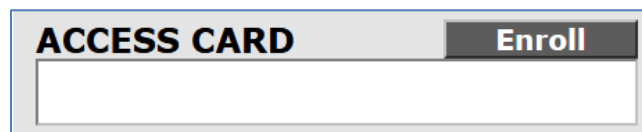
Use this option to deny entry into an area monitored by an armed alarm panel. This option supersedes the User's normal access permission. If they have permission to access the area and this option is not checked, the alarm panel will be disarmed, and the door will be unlocked. If this option is checked, the door will remain locked. *This option is not displayed on the Users page if an alarm panel interface is not configured in the system.*

## Enroll the Access Token

The most common access tokens are proximity cards and key tags. They work by simply holding the token near the access reader. The access card is the size of a credit card and typically offers better read performance than a key tag token, but many Users prefer the convenience of the key tag.

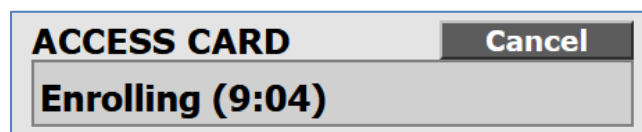
Every access token has a unique identifier that must be assigned to the User in the aPod II database. That token identifies the User to the access control system and acts like an electronic key to gain access through locked doors. Users must safeguard their access token and never loan it to anyone else.

The process of assigning the token to the User in the aPod II database is called "Enrolling the access token". With the User record selected, click the **Enroll** button to begin.



A ten-minute timer is started and during this interval the User's token can be enrolled into the system by simply badging it at any reader. The reader buzzer will beep six times and the reader LED will flash in unison to indicate a successful enrollment. Badge the token a second time and the door will unlock.

Access tokens must be enrolled one at a time.



A count-down display in the **ACCESS CARD** field shows how much time is remaining. At any time, the enrollment process can be cancelled by clicking the **Cancel** button. If the timer expires before the User enrolls the card, click **Enroll** again to repeat the process. A message is displayed when the access token has been enrolled and the enrollment is recorded in the event log.

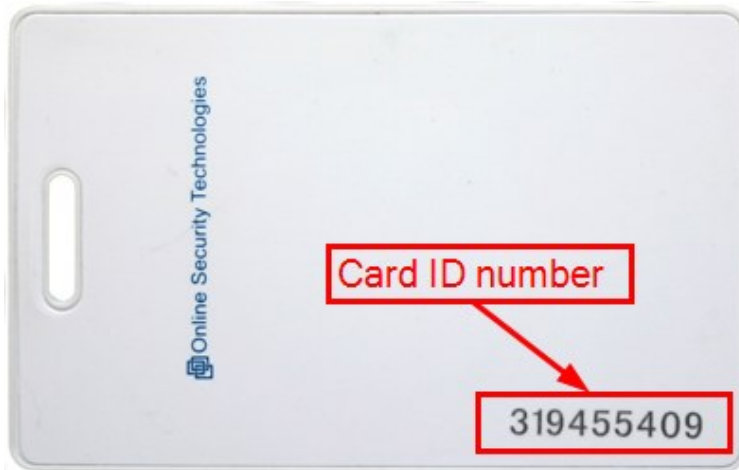
The screenshot shows the 'Users (edit)' interface. On the left, a list of users includes David Martin, Jane Anderson, Olin Reese, Richard Evans (highlighted), Sandy Thomas, and Sara Friedman. The main area shows details for Richard Evans: FIRST NAME (Richard), LAST NAME (Evans), and ACCESS CARD (319455408). An 'Info' popup window displays 'Enroll success' with an information icon. Below the details are 'Add', 'Save', 'Cancel', and 'Delete' buttons.

The screenshot shows the 'Events' log with 'AUTOSCROLL ON' status. Two events are listed: 'Enrolled Richard Evans' and 'Enrolling Started by David Martin', both dated Tue, Jan 29, 2019 2:26:03 PM (-5:00) at Machine Shop.

When the token has been enrolled the **ACCESS CARD** field will display the unique ID number.

A close-up of the 'ACCESS CARD' field with an 'Enroll' button. The field contains the unique ID number 319455408.

## Enter the Card ID Number manually

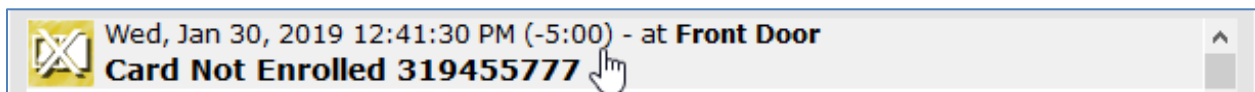


Data entry errors can be avoided with the automatic enrollment process, but you can also enter the card ID number manually. Simply enter the ID number which is printed on the card into the **ACCESS CARD** field and save the record.

<b>ACCESS CARD</b>	<b>Enroll</b>
319455409	

## Enroll an unmarked card

A third option exists for enrolling an access token. Whenever an unenrolled token is badged at a reader, the event log reports a "Card Not Enrolled" message which includes the Card ID number.



When you click the "Card Not Enrolled" message, you are directed to the [Users \(add\)](#) page with the **ACCESS CARD** pre-populated with the Card ID number.

The screenshot shows the 'Users (add)' form in the Online Security Technologies interface. The form is divided into several sections:

- Navigation:** Home, Users, Tools, Setup.
- Users (add):** A red box highlights the 'FIRST NAME' and 'LAST NAME' input fields.
- OPTIONS:** A list of checkboxes including Assisted Access, Suspended, 3X Lock/Unlock, 3X Arming, Silence Alarms, and Pending Unlock. There is also a checkbox for 'Deny entry if Armed'.
- ACCESS CARD:** A field containing '319455777' with an 'Enroll' button.
- READER KEYPAD OPTIONS:** A dropdown menu set to 'None'.
- VALID FROM:** A dropdown menu set to 'Now'.
- VALID UNTIL:** A dropdown menu set to 'Forever'.
- USER ID:** A field containing '7'.
- PIN:** A dropdown menu set to 'Unassigned'.
- DOOR ACCESS BY SCHEDULE:** A table with columns for door names and access status. All doors (Back Door, Front Door, Machine Shop, Stockroom) are set to 'ALL'.
- Buttons:** Add, Save, Cancel, Delete.

This card enrollment method is particularly useful when the Card ID number is illegible or missing.

## Give a User Temporary Access

There are many circumstances where a User should have temporary access. Contract workers, students, and gym members are examples where access should be limited to their expected use of the facility.

Use the **VALID FROM** field to define the date and time when a User's access becomes valid. The default setting is 'Now'. Use the **VALID UNTIL** field to set an expiration date and time. The default setting is 'Forever'. The temporary access applies to all modes of access.

This close-up screenshot shows the 'ACCESS CARD' and 'VALID FROM' fields. The 'ACCESS CARD' field contains the number '319455408' and has an 'Enroll' button next to it. The 'VALID FROM' field is set to 'Now'.

Click on the **VALID FROM** field to open the date/time applet. Select the desired time and date and click the **OK** button to accept the date.

The screenshot shows the 'Users (edit)' form for user Richard Evans. The 'VALID FROM' field is highlighted with a red box, and a date/time selection applet is open. The applet shows a calendar for May 2021 with the 1st selected. The time is set to 12:00 AM. The 'OK' button is highlighted with a mouse cursor.

Year	Month	Day	Hour	Min
2021	May	1	12	00

Click on the **VALID UNTIL** field to open the date/time applet. Select the desired time and date and click the **OK** button to accept the date.

The screenshot shows the 'Users (edit)' form for user Richard Evans. The 'VALID UNTIL' field is highlighted with a red box, and a date/time selection applet is open. The applet shows a calendar for May 2021 with the 31st selected. The time is set to 6:00 PM. The 'OK' button is highlighted with a mouse cursor.

Year	Month	Day	Hour	Min
2021	May	31	6	00



## Assign PIN's

You can customize the way that PINs are used in your system to obtain a balance between security and convenience that is appropriate for your circumstances.

**Note:** PIN configuration fields are not displayed unless PIN functionality has been enabled. Please refer to page 45 for more information.

### PIN length and PIN strength

You can select the **PIN LENGTH** and choose between “Standard PIN’s” and “Strong PIN’s”. You can also allow PIN’s to be managed by a System Administrator, which is often the most convenient method, or you can allow Users to manage their own PIN’s, which is the most secure method. **PIN LENGTH** and **PIN STRENGTH** are configured on the System page.

The screenshot shows the 'System' configuration page in the aPod II interface. The page is titled 'aPod II ©Online Security Technologies' and includes a navigation menu with 'Home', 'Users', 'Tools', and 'Setup'. The 'System' section is active, displaying various configuration fields. The 'PIN LENGTH' and 'PIN STRENGTH' fields are highlighted with a red box. The 'PIN LENGTH' field is set to '4 Digits' and the 'PIN STRENGTH' field is set to 'Standard'. Other fields include 'SITE NAME' (David Martin Custom Parts), 'SITE ADDRESS' (142 Oakdale Rd, Kingston ON), 'TIME ZONE' (Eastern Time (GMT-5:00)), 'LANGUAGE' (English (en)), 'ACCESS AUTHORIZATION' (By User Groups), 'ADMINISTRATOR TEMPORARY PASSWORD' (masked with dots), 'PRIMARY INTERNET IP' (64.228.90.180), 'PORT (UDP)' (5268), 'REMOTE LOGIN SETUP' (Automatic (DDNS)), 'REMOTE HTTP PORT (TCP)' (25268), 'PC's DATE/TIME' (Mon, Apr 26, 2021 4:55:45 PM), 'SELECTED LOCALE' (Ontario), 'aPod's DATE/TIME' (Mon, Apr 26, 2021 4:55:43 PM), and 'PRIMARY IP ADDRESS' (192.168.2.164). There are 'Save' and 'Cancel' buttons at the bottom.

**PIN LENGTH** is 4 digits by default and **PIN STRENGTH** is “Strong” by default.

The image shows a close-up of the 'PIN LENGTH' dropdown menu. The menu is open, showing four options: '4 Digits', '4 Digits', '5 Digits', and '6 Digits'. The first '4 Digits' option is selected and highlighted in blue.

The image shows a close-up of the 'PIN STRENGTH' dropdown menu. The menu is open, showing three options: 'Standard', 'Strong', and 'Standard'. The 'Standard' option at the bottom is selected and highlighted in blue.

With “Standard” PIN’s any number is allowed if the **PIN LENGTH** requirement is met. With “Strong” PIN’s, sequential numbers are disallowed, and the last 2 digits must not be the same. For example, “1234” and “8765” are not allowed and “4444” and “1244” are not allowed. Strong PIN’s reduce the chance that someone could guess a valid PIN.

## Assign PIN’s

Manage PIN’s on the Users page. The **USER ID** field cannot be edited. The aPod II System automatically assigns a User ID as Users are added to the system beginning at 1 and incrementing the USER ID one at a time. This ensures that the shortest User ID possible is used. For systems with less than 100 users, only a 2-digit ID is required. The **PIN** field displays the status of the User’s PIN and allows you to create or change a PIN using one of two different methods.

The screenshot shows the 'Users (edit)' form for user Richard Evans. The 'USER ID' field is set to 4 and the 'PIN' dropdown is set to 'Unassigned'. A red box highlights these two fields. The interface includes a sidebar with a user list, a top navigation bar, and a 'DOOR ACCESS BY SCHEDULE' section at the bottom.

Door	Access
Back Door	REGULAR HOURS
Front Door	ALWAYS
Machine Shop	REGULAR HOURS
Stockroom	NO ACCESS

If a PIN has not been assigned to a User, you can create a “managed PIN” or a “temporary PIN”.

The close-up shows the PIN dropdown menu with the following options: Unassigned, Unassigned, Managed PIN, and Temporary PIN.

## Managed PIN's

With this option PINs are created by a System Administrator and given to each User. It is not necessary to create unique PINs because the User ID is unique, and the User must enter his ID plus PIN.

USER ID	PIN	ENTER PIN	RE-ENTER PIN
4	Managed PIN	7943	7943

Select "Managed PIN" from the **PIN** drop-down list. Enter and confirm a PIN, save the record, and give the PIN to the user. With managed PINs, the PIN is hidden in the user record and the field title indicates that the PIN is managed.

USER ID	PIN/Managed
4	●●●●

Click on the **PIN/Managed** drop-down list to temporarily reveal the PIN.

USER ID	PIN/Managed
4	7943

When a managed PIN has been assigned, you have three options.

- change the PIN ("New Managed"),
- allow the User to manage the PIN ("Temporary PIN"),
- remove the PIN ("Unassign").

PIN/Managed
7943
7943
New Managed
Temporary PIN
Unassign

## Temporary PIN

When you select this option, the system generates a temporary PIN and tells you when the PIN will expire. A temporary PIN expires on the top of the hour following the hour during which it was created.

Save the record.

Give the temporary PIN and expiration time to the User and tell them to change their PIN at any keypad reader. Refer to page 126 for instructions on how to change a PIN at a keypad reader.

The screenshot shows the 'Users (edit)' form in the aPod II interface. The form is divided into several sections:

- Navigation:** Home, Users, Tools, Setup.
- User Information:** FIRST NAME (Richard), LAST NAME (Evans).
- OPTIONS:** Assisted Access, Suspended, 3X Lock/Unlock, 3X Arming, Silence Alarms, Pending Unlock, Deny entry if Armed.
- ACCESS CARD:** 319455408.
- VALID FROM:** Now.
- USER ID:** 4.
- TEMPORARY PIN:** Temporary PIN (dropdown), '4090' valid until 5PM.
- DOOR ACCESS BY SCHEDULE:** ALL, Back Door (REGULAR HOURS), Front Door (ALWAYS), Machine Shop (REGULAR HOURS), Stockroom (NO ACCESS).

An info pop-up box is overlaid on the form, stating: "Click 'Save' to enable the temporary PIN".

When the record has been saved, the status of the temporary PIN is displayed until it is changed by the User or expires. The temporary PIN can be exposed by clicking on the **PIN/TEMPORARY** drop-down list.

The close-up shows the following fields:

- USER ID:** 4
- PIN/Temporary:** A dropdown menu with four dots (●●●●) and a downward arrow.
- TEMPORARY PIN:** Valid until 5PM

If the temporary PIN expires before the User changes it, you will have to issue another temporary pin to re-start the process. You may cancel a temporary PIN at any time before it has expired or been changed by the User.

When the User has assigned a permanent PIN, it cannot be displayed in the Browser Interface.

USER ID	PIN
4	Assigned

A User can change their PIN at any time at a keypad reader. As a system administrator you have three options.

- force a new User assigned PIN change (“Temporary PIN”),
- switch to administrator managed PIN’s (“Managed PIN”),
- remove the PIN (“Unassign”).

## CARD+PIN MODE

- 1 Badge token
- 2 Enter PIN
- 3 Press “#” key

In card plus PIN mode, a User must first badge the card reader with their access token after which **the card reader LED will flash rapidly and continuously** indicating that the system is waiting for numeric input. The User must then enter their PIN number followed by the “#” key after which the door will unlock. If the User is not allowed access at that time or if the entered PIN is incorrect, the door will remain locked, and the reader buzzer and LED will indicate the access denied response. Refer to page 102. An access denied message will be recorded in the event log.

The User must begin entering their PIN within 10 seconds of badging their access token or the process will time out. When the process times out, the reader buzzer and LED will indicate the access denied response. and then return to its steady state. If this happens, the User can start over by simply badging their card again.

## ID+PIN MODE

- 1 Enter ID
- 2 Enter PIN
- 3 Press “#” key

In PIN only mode there is no access token to identify the User. In this situation, the PIN is preceded by a system-assigned User ID which is unique for each User. Although a PIN may not be unique, the combination of User ID plus PIN is always unique.

PIN
Assigned
Assigned
Managed PIN
Temporary PIN
Unassign

In PIN only mode, a User must first enter their User ID. After the first number key is pressed, **the card reader LED will flash rapidly and continuously** indicating that the system is waiting for numeric input. The User enters the numbers and presses the “#” key after which the door will unlock. If the User is not allowed access at that time or if the PIN entered is incorrect, the door will remain locked, and the reader buzzer and LED will indicate the access denied response. An access denied message will be recorded in the event log.

The User must continue entering their PIN within 10 seconds of pressing the first number key or the process will time out. When the process times out, the reader buzzer and LED will indicate the access denied response. and then return to its steady state. If this happens, the User can start over by simply entering their User ID again.

## Change the PIN at a Keypad Reader

Use the following sequence to change the PIN at a keypad reader. The “old PIN” refers to the temporary PIN if this is the first time the PIN has been changed.

- 1 Press “\*” key
- 2 Enter ID
- 3 Enter Old PIN
- 4 Press “#” key
- 5 Enter New PIN
- 6 Press “#” key

If tokens are used, the User may badge their token for identification in which case the following sequence can be used. Either sequence is acceptable.

- 1 Press “\*” key
- 2 Badge token
- 3 Enter Old PIN
- 4 Press “#” key
- 5 Enter New PIN
- 6 Press “#” key

A User must first press the “\*” key to initiate the PIN change process after which ***the card reader buzzer will chirp, and the LED will flash rapidly and continuously*** indicating that the system is waiting for numeric input.

The User must then enter their User ID or alternatively, badge their token to identify them self. ***The card reader LED will continue to flash rapidly and continuously.***

The User then enters the temporary or old PIN and presses the “#” key after which ***the card reader buzzer will chirp, and the LED will continue to flash rapidly and continuously*** indicating that the system is waiting for numeric input.

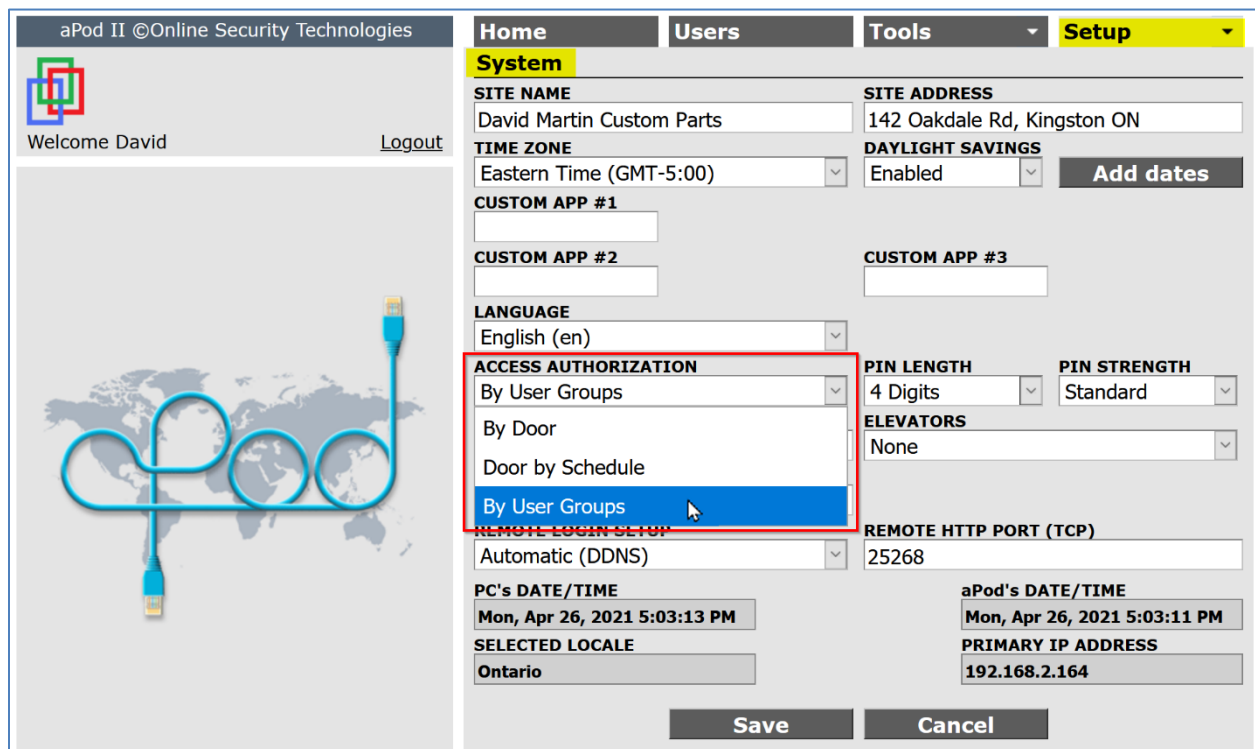
The User then enters the new PIN and presses the “#” key after which ***the reader buzzer will sound two long beeps to indicate that the new PIN has been accepted and the reader LED will resume its normal “locked/unlocked” status.***

After each step in the process, the User must continue within 10 seconds or the process will time out. When the process times out, the reader buzzer and LED will indicate the access denied response. and then return to its steady state. If this happens, the User can start over by simply pressing the “\*” key again.



## Assign Access Permissions to Users

Access permissions determine which doors a User can unlock and at what times. Assigning access permissions is a relatively simple task for small systems but can become confusing and difficult for large systems with hundreds of Users. The aPod II system addresses this issue by providing three methods for assigning access permissions, which range from simple to sophisticated. These methods are: 'By Door', 'Door by Schedule' and 'User Groups'. The selection is made in the **ACCESS AUTHORIZATION** drop-down list on the System page.



The screenshot shows the 'System' configuration page in the aPod II web interface. The 'ACCESS AUTHORIZATION' dropdown menu is open, showing three options: 'By User Groups', 'By Door', and 'Door by Schedule'. The 'By User Groups' option is highlighted in blue. The page includes various configuration fields such as SITE NAME, TIME ZONE, CUSTOM APP #1-3, LANGUAGE, PIN LENGTH, PIN STRENGTH, ELEVATORS, REMOTE LOGIN SETUP, REMOTE HTTP PORT (TCP), PC's DATE/TIME, aPod's DATE/TIME, SELECTED LOCALE, and PRIMARY IP ADDRESS. The 'Save' and 'Cancel' buttons are visible at the bottom.

You need 'Full' administrator's authority to change the method for assigning access permissions.

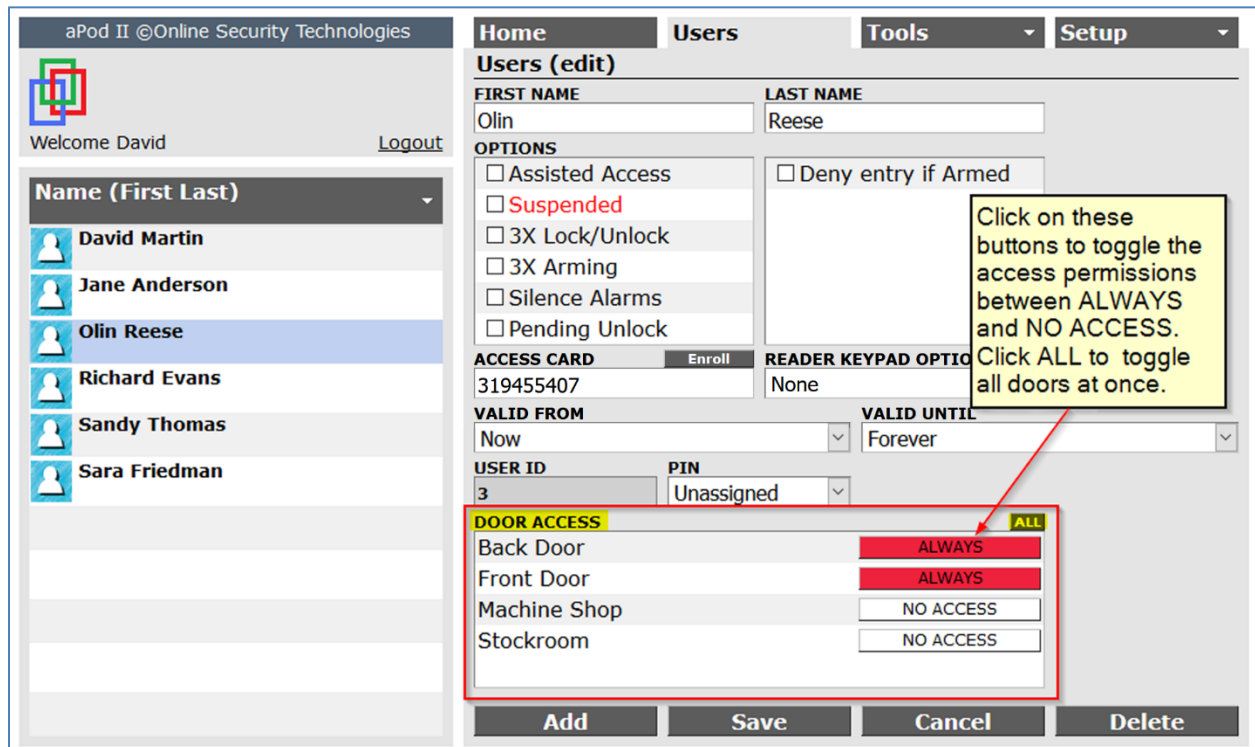
*Changing the access authorization method alters the database. For this reason, the aPod II System will not allow a change unless a backup has been made within the last thirty minutes.*

Normally you would select the access authorization method when the system is first installed but you can change it at any time. The method you select will determine what appears in the door access section on the Users page.

## By Door

This is the simplest method of assigning access permissions and it is the default method. A list of the doors is displayed on the Users page and each door can be toggled between **ALWAYS** and **NO ACCESS** to grant or deny access permission to that User.

Unlock schedules can be configured for any door but there is only one lock state. There are no time restrictions for any User who has been given permission to access the door.



When there is only one door in the system, the list is not displayed and the single door permission defaults to **ALWAYS**.

Access permission is granted or denied by giving an access token to the User.

## Door by Schedule

Access permissions for each door can vary according to the day of the week and the time of day. A list of the doors is displayed on the Users page and each door can be toggled between **ALWAYS** **EXTENDED HOURS** **REGULAR HOURS** **NO ACCESS** to grant or deny access to that user according to a time schedule. The time schedules are configured on the Schedule tab of the Doors page which is located on the Setup menu. Refer to page 29.

The screenshot displays the 'Users (edit)' interface. On the left, a user list includes David Martin, Jane Anderson, Olin Reese (selected), Richard Evans, Sandy Thomas, and Sara Friedman. The main area shows details for Olin Reese, including fields for first and last name, options for assisted access, suspended status, and 3X lock/unlock, arming, and pending unlock. It also shows access card details (319455407) and keypad options. A red box highlights the 'DOOR ACCESS BY SCHEDULE' section, which lists doors and their access permissions: Back Door (ALWAYS), Front Door (EXTENDED HOURS), Machine Shop (REGULAR HOURS), and Stockroom (NO ACCESS). A yellow callout box points to the 'ALL' button in the schedule section, stating: 'Click on these buttons to step the access permission through the four time schedules shown. Click ALL to step all doors at once.'

The three time-oriented lock states allow you to program *when* a User is allowed access through a locked door. For example, an employee may be allowed to access the workplace through a back door during normal business hours but would not be granted access on the weekend.

Create time intervals to define after hours, extended hours, and regular hours for the time that a door will remain locked. You can then restrict access by Users to the appropriate schedule by assigning the 'After Hours', 'Extended Hours' or 'Regular Hours' privilege to their card.

The time-oriented lock states have cumulative access permissions. If a User has 'After Hours' access permission, they automatically have 'Extended Hours' access permission. Similarly, if a User has 'Extended Hours' access permission, they automatically have 'Regular Hours' access permission.

## By User Groups

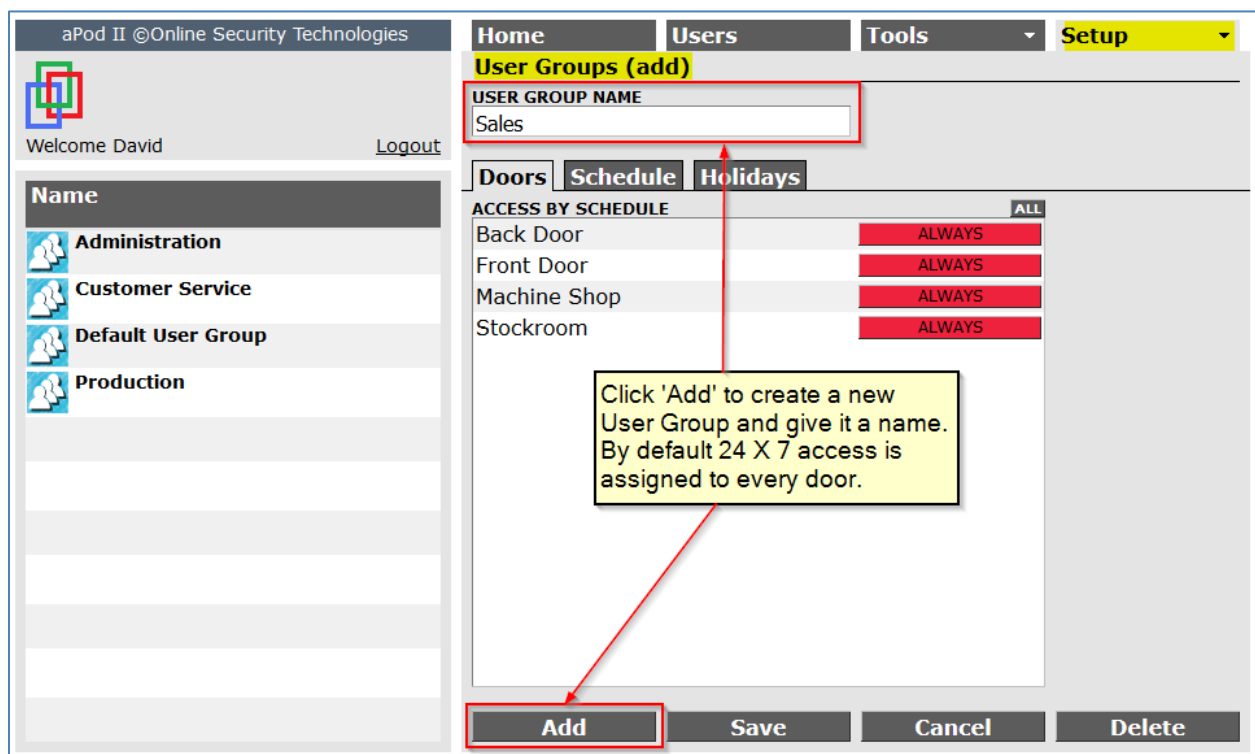
For systems with several doors and many Users, assigning access permissions can be confusing and difficult. This task can be simplified by creating groups of Users with similar access requirements and then assigning the Users to those groups.

For example, the access permissions of the entire sales force can be managed in a two-step process. In the first step, create a User Group called 'Sales' and then assign it access permissions. Use the User Groups page in the Setup menu for this step.

**Note:** The User Groups page is not available in the Setup menu unless the 'By User Groups' option is selected in the **ACCESS AUTHORIZATION** drop-down list on the System page.

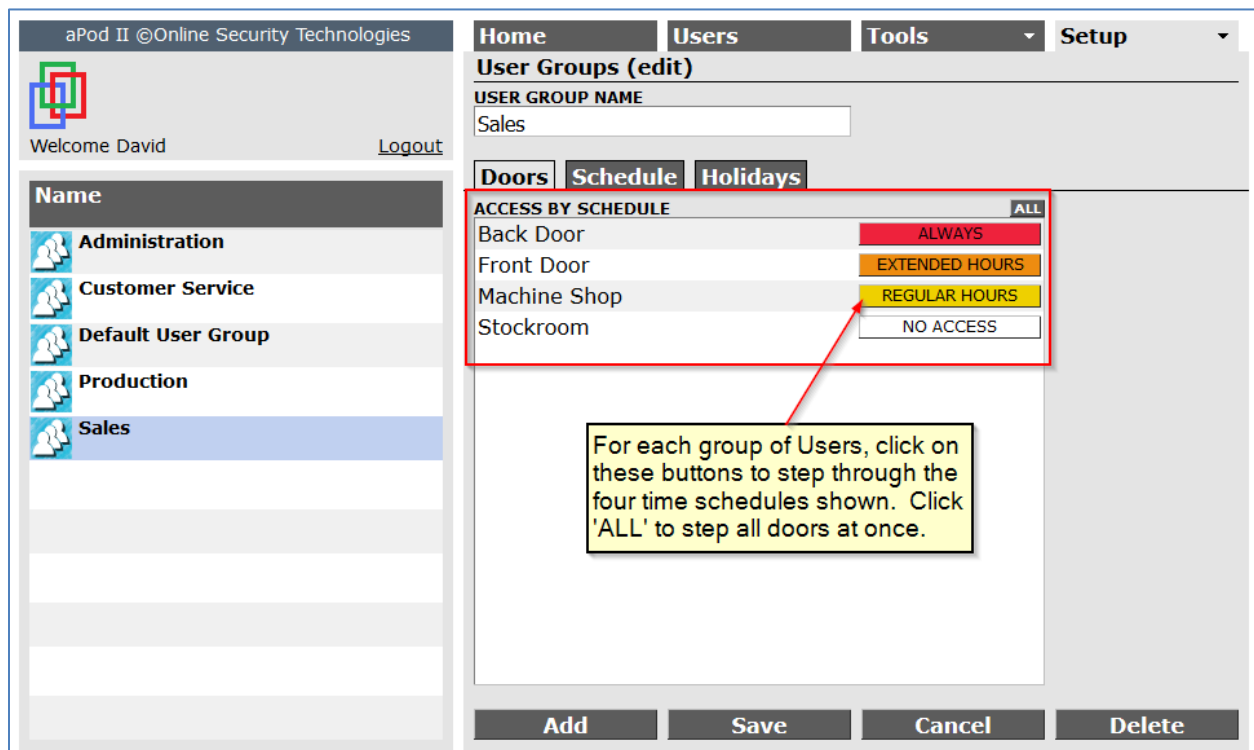
### Create the User Groups

By default, the aPod II controller's database has one User Group called 'Default User Group'. When User Groups are enabled, all Users are automatically assigned to this group which provides 24 X 7 access at all doors. This ensures that there is no impediment to normal traffic while User Groups are being configured. Once the User Groups have been created and configured, Users can be re-assigned to the appropriate group and the Default User Group can be deleted.



You assign permissions to a group in the same way that you assign permissions to a single User in the 'Door by Schedule' method. Access permissions for each door vary according to the day of the week and the time of day.

A list of the doors is displayed on the Doors tab on the User Groups page. Each door can be toggled between **ALWAYS** **EXTENDED HOURS** **REGULAR HOURS** **NO ACCESS** to grant or deny access to that User Group according to a time schedule. The time schedules are configured on the Schedule tab of the Doors page which is located on the Setup menu. Refer to page 29 for more information.



## Assign the Users to Groups

In the second step, assign members of the sales force to the 'Sales' User Group using the **USER GROUP** drop-down list on the Users page. This list is only displayed when the 'By User Groups' access authorization method is used.

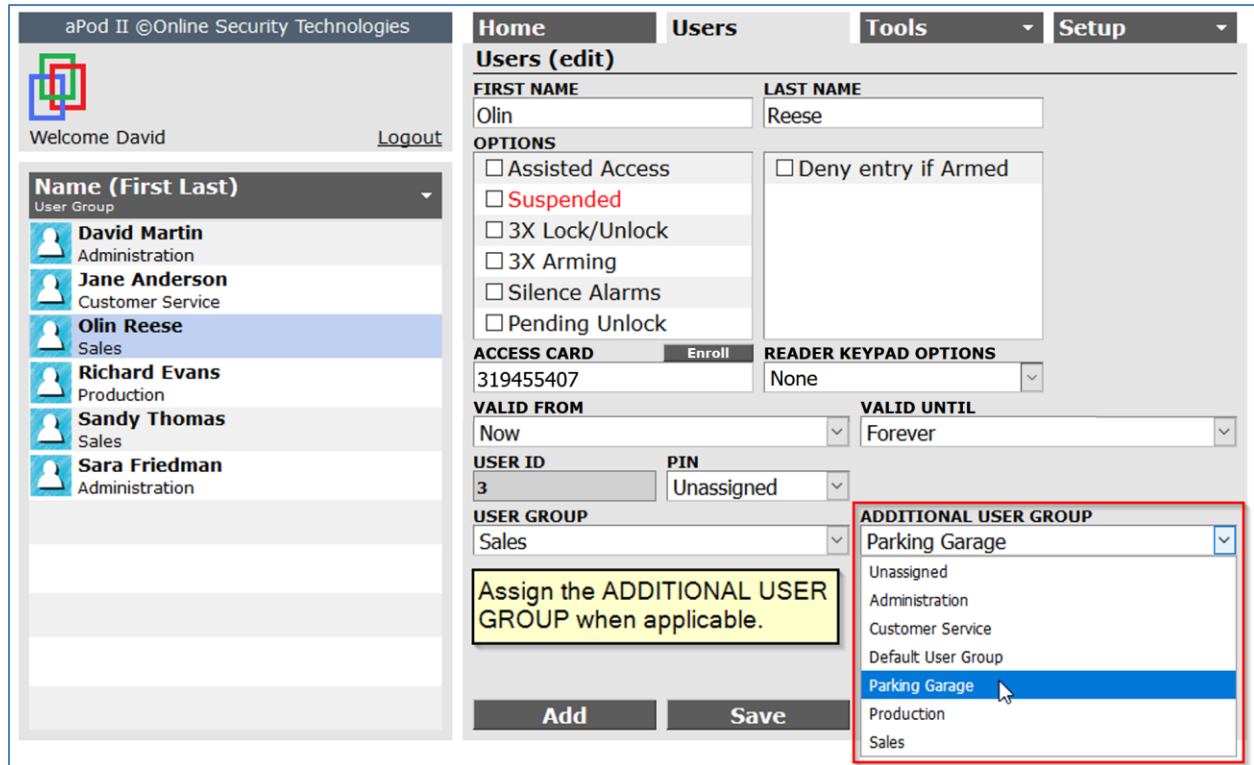
The access permissions of the group are automatically transferred to the User.

Use the USER GROUP drop down list to assign the User to a primary group.

A second optional permission set is provided by the **ADDITIONAL USER GROUP** drop-down list. Access to a parking garage is an example where a second permission set would be useful.

Doors	Schedule	Holidays
Back Door	NO ACCESS	
Front Door	NO ACCESS	
Machine Shop	NO ACCESS	
Parking Garage	ALL	
Stockroom	NO ACCESS	

Users who drive cars and use the parking garage can be assigned to this group regardless of other access permissions.



The User Groups option is available in a single door system. Only three User Groups are possible, and they would correspond to the three time-restrictions for accessing a locked door. In this case, the 'Door by Schedule' access authorization method is easier to use.

## User Group Schedules

User group schedules complement door schedules. They allow access intervals to be assigned to a user group according to the normal operation of the group regardless of the time of day. This could apply to shift workers, maintenance and house keeping, office staff or any other group with a complex work schedule. A user group schedule is created automatically when a User Group is created. By default, the entire group schedule allows access which prevents possible conflict with configured door schedules until properly implemented.

User group schedules are superimposed on door schedules. For example, in a factory operating multiple shifts a day, you may want to restrict the access of shift workers to their shift time plus 30 minutes at the beginning of the shift and 30 minutes at the end of the shift.

In this example, the user group for a shift would be assigned the 'After Hours' door schedule for doors they normally use, which would give them 24x7 access. This prevents the door schedule from interfering with the group schedule.

The screenshot shows the 'User Groups (edit)' interface for 'Shift 2'. The 'Doors' tab is active, showing a list of doors: Back Door, Front Door, Machine Shop, and Stockroom. Each door has a dropdown menu set to 'ALL'. A red box highlights the 'ALL' dropdown for the Back Door, and another red box highlights the 'ALL' dropdown for the Stockroom. A yellow callout box contains the text: 'To create a specific access schedule for a group, first set the group permission to 'ALWAYS' for any door that the group will normally access.'

In addition, the user group schedule for the shift would be configured to restrict their access to the time period of their shift plus 30 minutes before the start time and 30 minutes after the finishing time.

The screenshot shows the 'User Groups (edit)' interface for 'Shift 2' with the 'Schedule' tab active. A weekly schedule grid is displayed with columns for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday. The grid shows access permissions for various times of the day (12AM to 10PM). A blue box highlights the Thursday column, and a blue arrow points to the Thursday column. A yellow callout box contains the text: 'The night shift spans two days.'



## User Group Holidays

The holidays for your jurisdiction were determined by the selection of your locale during at the time of the system commissioning. They are renewed automatically on a perpetual calendar.

The configured holidays should be reviewed to ensure they match the operation of your facility. Please refer to page 39 for more information.

When a group schedule is in force, holiday selection should be managed on the [User Groups](#) → [Holidays](#) page and not on the [Doors](#) → [Holidays](#) page.

The screenshot displays the 'User Groups (edit)' interface. At the top, there are navigation tabs: 'Home', 'Users', 'Tools', and 'Setup'. The 'Setup' tab is active. Below the navigation, the page title is 'User Groups (edit)'. The 'USER GROUP NAME' field contains 'Shift 2'. There are three sub-tabs: 'Doors', 'Schedule', and 'Holidays', with 'Holidays' selected. The 'HOLIDAYS' section has a dropdown menu set to 'ALL'. A list of holidays is shown, each with a checked checkbox: New Year, Family Day, Good Friday, Easter Monday, Victoria Day, Canada Day, Civic Holiday, Labor/Labour Day, Thanksgiving (Canada), Remembrance Day, Christmas, and Boxing Day. At the bottom of the interface, there are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'. On the left side of the interface, there is a sidebar with a 'Name' header and a list of user groups: Administration, Customer Service, Maintenance, Sales, Shift 1, and Shift 2. 'Shift 2' is highlighted in blue. Above the sidebar, it says 'Welcome David' and 'Logout'.

## Importing User Data

### Introduction

The aPod System provides a standard function for importing user data which can greatly reduce the time needed to commission a system. The following user data fields can be imported.

#### *Required fields:*

First Name, Last Name and at least one of ... Card ID, PIN, User Group and Picture.

#### *Optional fields:*

Card ID, PIN, User Group and Picture

### The Procedure

#### *Summary*

The user import function is accomplished with the following steps.

1. Create a raw user data file in Microsoft Excel.
2. Export the raw data file as a Text file with Tab Separated Values (TSV).
3. Import the Text file into a custom PC app called UPB.exe.
4. Mark each data column with the appropriate heading.
5. Export the user data in an aPod compatible format.
6. Upload the user data file into the aPod Primary controller.
7. Review the imported data records and change the default values for non-imported fields if necessary.

**Note:** To eliminate potential problems with file paths, the Excel spreadsheet, the UPB app and all User pictures should be in the same directory.

#### *1. Create the Raw Data File in Excel.*

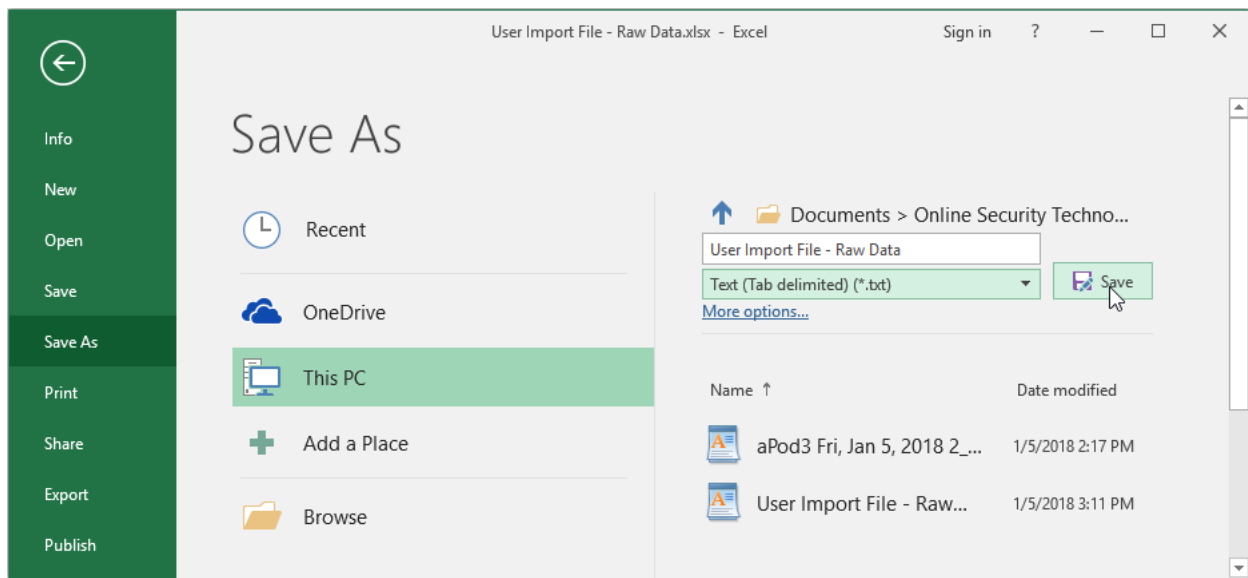
Microsoft Excel provides a good tool for organizing and editing the user data. Data from an existing system can be imported into Excel or for new systems, the Excel spreadsheet can be used to efficiently create new data. The Excel spreadsheet also provides an efficient method for finding and correcting data errors.

## Excel user data spreadsheet guidelines:

- The data can be organized in the Excel spreadsheet in any column order.
- Columns for the required fields must be included plus any optional field. Columns of additional data that may have been included in a data file import should be deleted.
- The column data does not need to be sorted.
- Every Card ID, First Name + Last Name combination, and User Picture (if included in your system) must be unique. Excel provides tools for locating duplicates.
- Set the PIN column to “text” format to prevent the truncation of leading zeros.
- Add missing data as needed to complete the file.

## **2. Export the user data as a tab delimited text file.**

The user data can be exported by saving the file as a tab delimited text file.

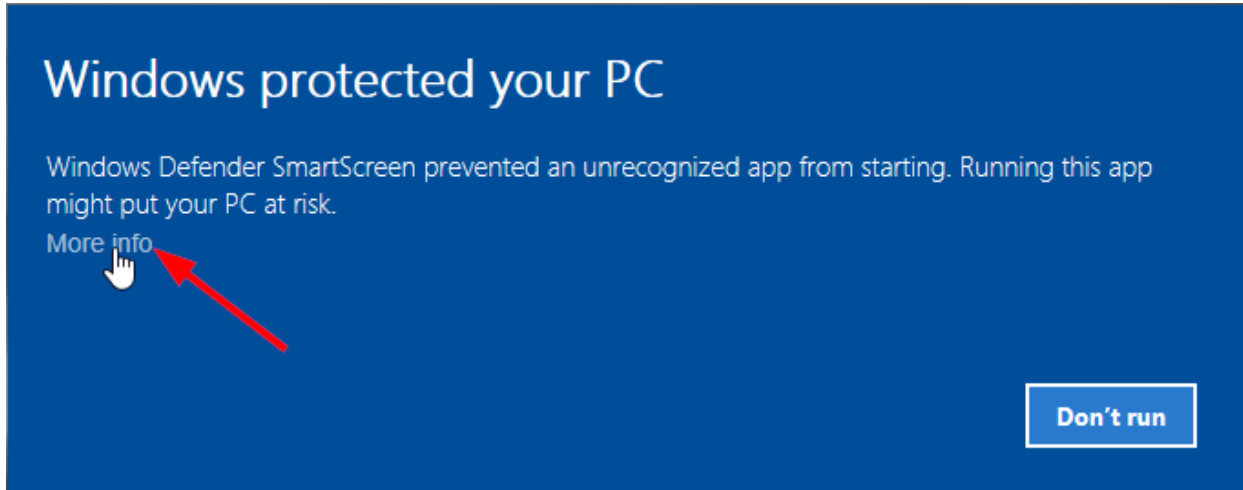


**Note:** The Excel spreadsheet of user data must also be saved as an Excel “.xlsx” file before closing the file to preserve your additions and edits in a working Excel file.

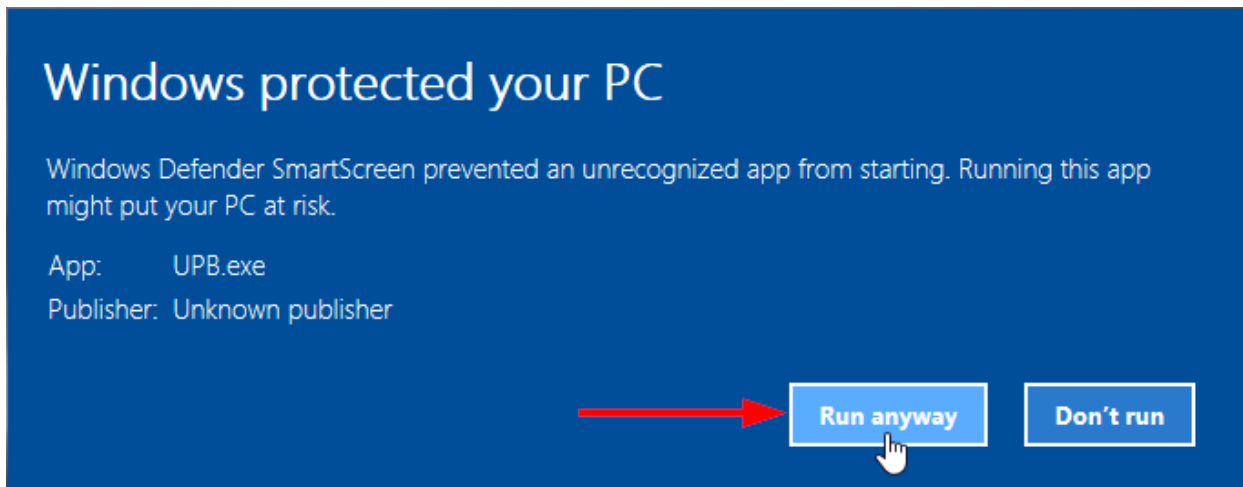
### 3. Import the Text file into a custom PC app called UPB.exe.

The UPB app validates the raw user data and creates an output file that can be uploaded directly into the aPod Primary controller. It will also identify data errors which can be corrected in the Excel spreadsheet. Currently, the UPB.exe app is not available for Mac computers.

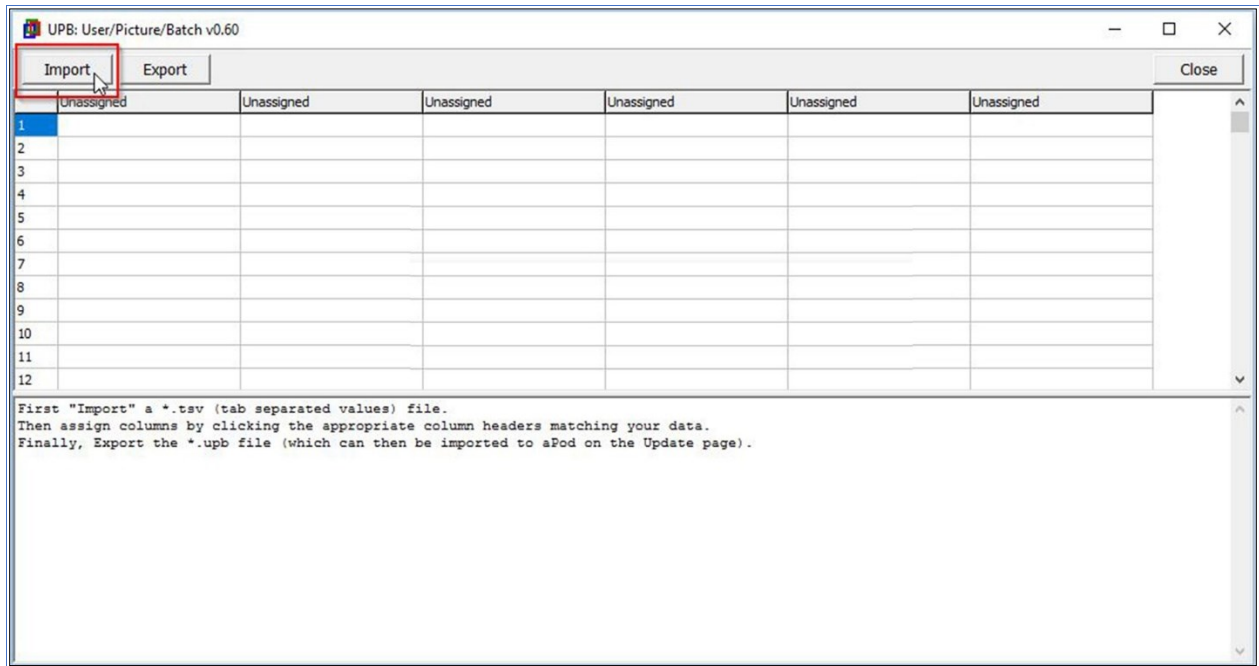
The UPB app is a single executable file and does not need to be installed on your PC. When it is executed for the first time, Windows 10 will display the following warning.



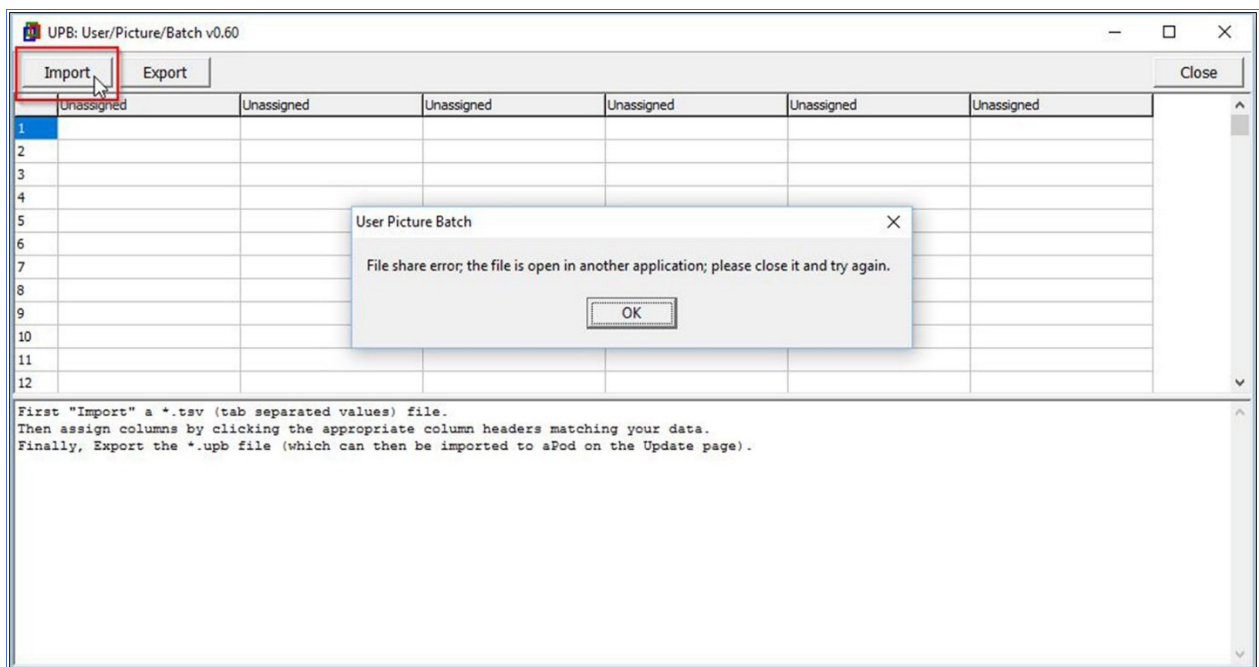
Click the More Info link and then click Run anyway to allow the program to run. This is only required on the first execution.



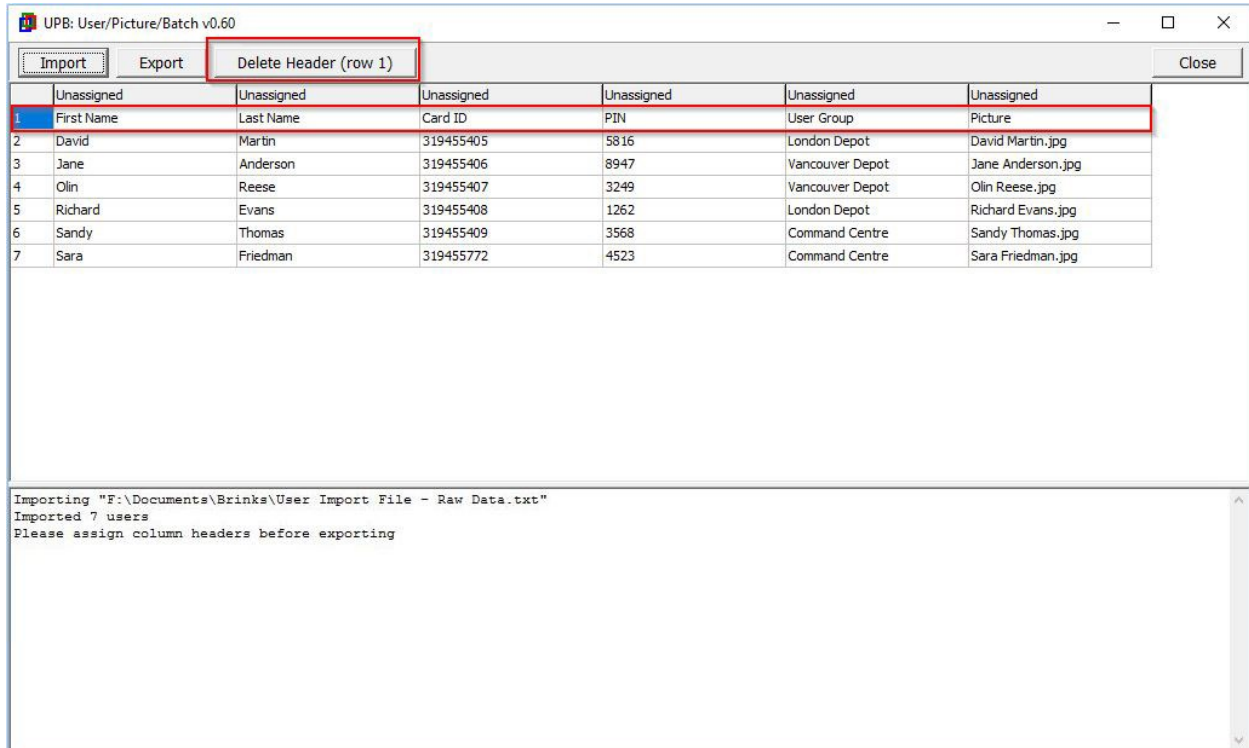
Use the Import button to import the raw user data file which was produced by the Excel spreadsheet.



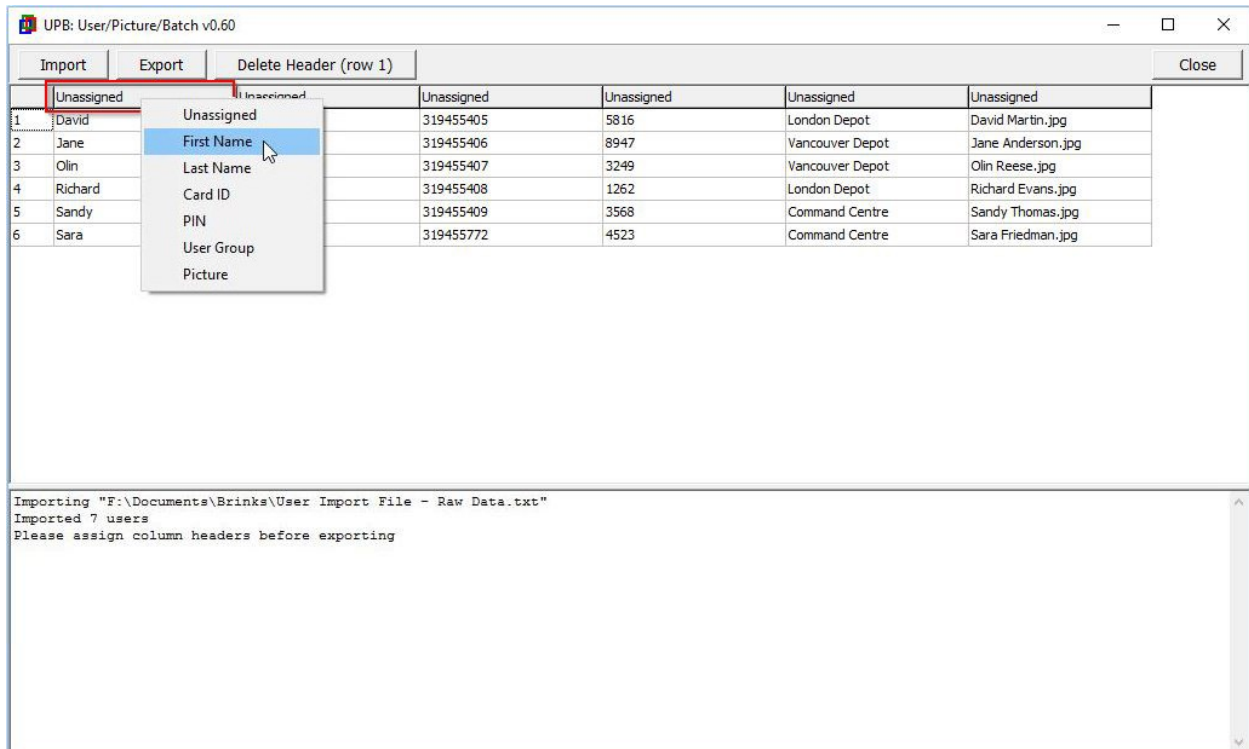
Save and close the Excel spreadsheet that contains the raw data before you import the Excel tab delimited text file. Otherwise, you may see the following error message. "File share error; the file is open in another application; please close it and try again."



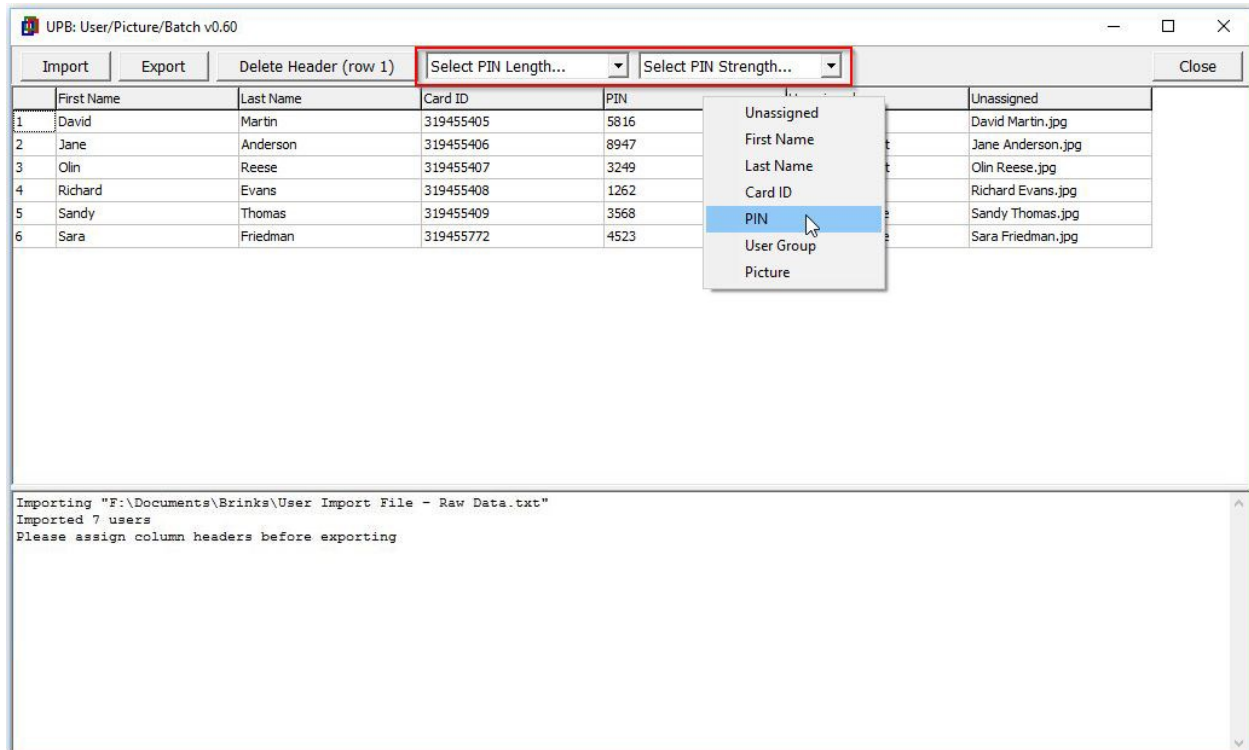
Click the Delete Header button to remove headings in row 1 if necessary.



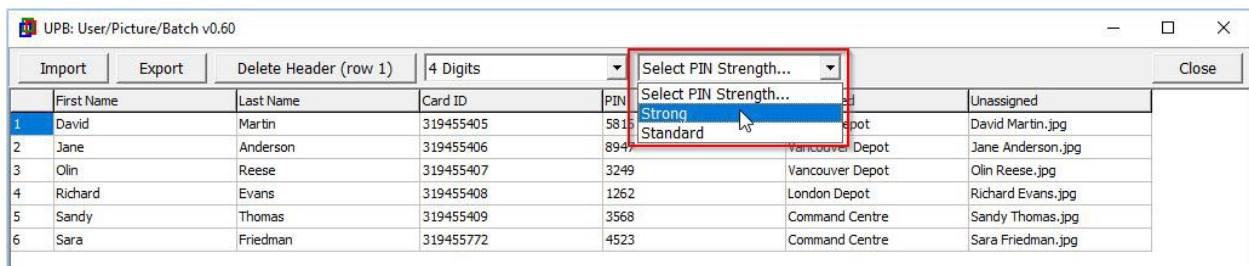
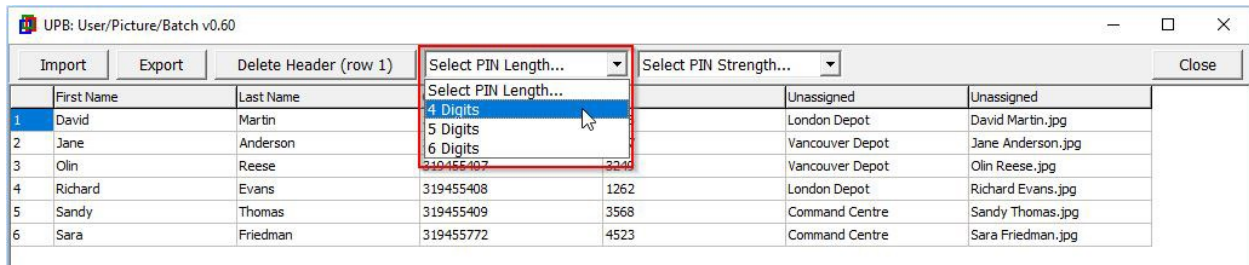
#### 4. Mark each data column with the appropriate heading.



If PINs are selected for a column heading, the PIN configuration fields are displayed.



PIN Length and PIN Strength must be set before the data can be exported. The PIN data is validated against these configurations.



Pin lengths must be exact. For example, if a 5-digit PIN is specified, leading zeros will be added to pad PIN's with fewer digits and PIN's with more digits will generate an error.

With “Standard” PINs any number is allowed if the **PIN LENGTH** requirement is met.

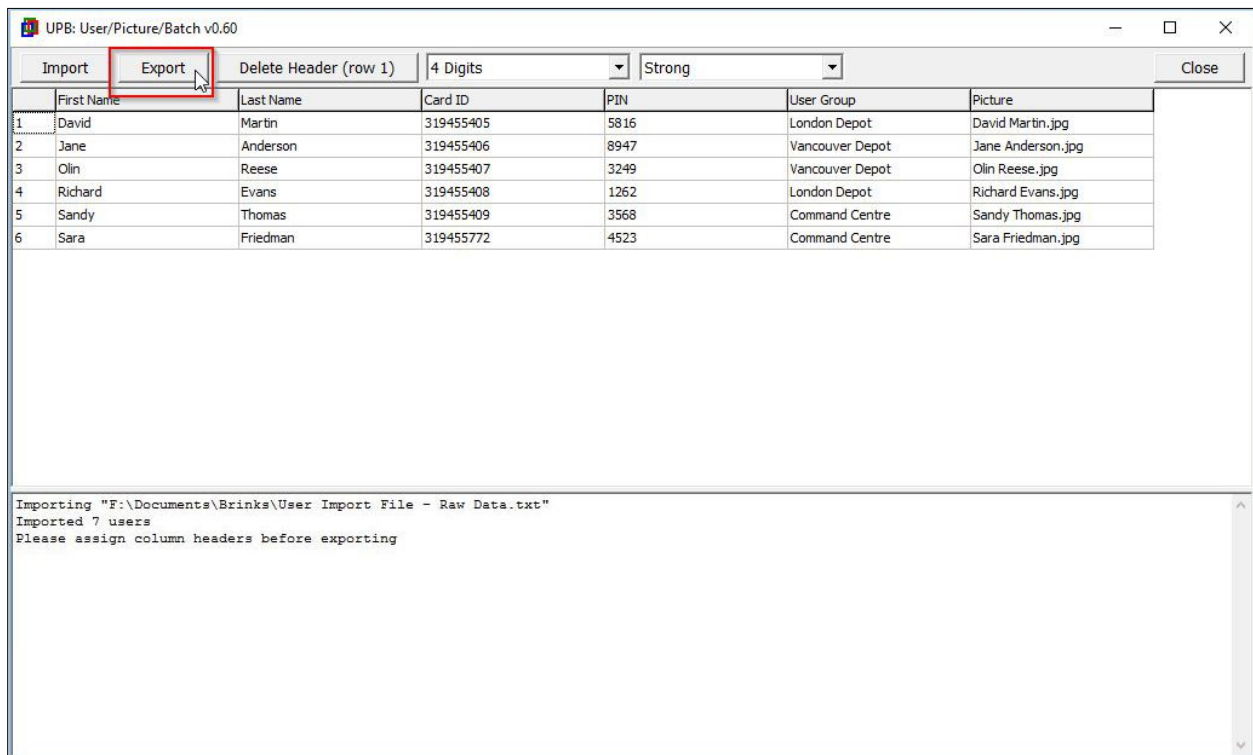
With “Strong” PINs, sequential numbers are disallowed, and the last 2 digits must not be the same. For example, “1234” and “8765” are not allowed and “4444” and “1244” are not allowed. Strong PINs reduce the chance that someone could guess a valid PIN.

A column is available for importing user pictures if the User picture option is included in your system. This column should contain the name of the image file associated with the employee and include the file extension and file path. If the image files are in the same directory as the UPB app then no file path is required.

Note: Pictures should have a width and height of 150 px and 200 px respectively and must use the “jpg” format. The maximum picture file size is 65,024 bytes. Pictures with different aspect ratios or pixel size will be scaled to fit but the picture quality may be reduced.

## 5. Export the user data in an aPod compatible format.

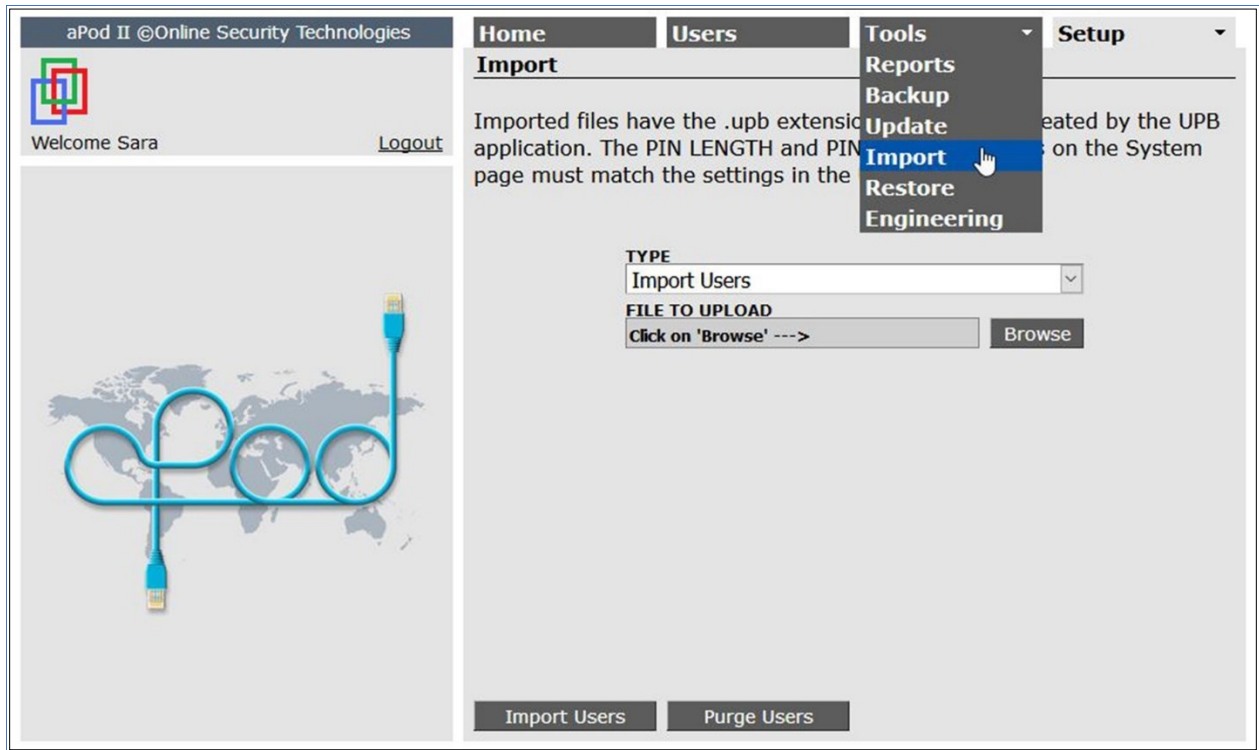
Use the Export button to generate a data file which can be uploaded to the aPod II Primary controller. It will have a “.upb” file extension.





## 6. Upload the user data file into the aPod Primary controller.

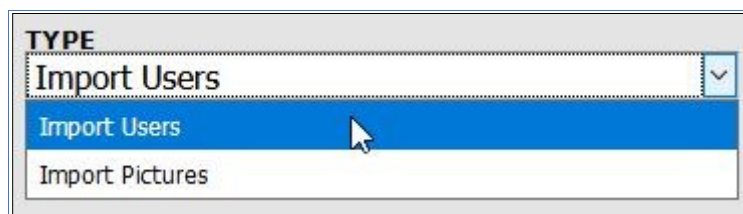
The user data import functions are located on the Tools→Import page.



There are two data import types. The “Import Users” type is primarily used when a system is first commissioned and allows the import of all required fields plus any optional fields including pictures.

The “Import Pictures” type is used to restore only the employee pictures. With this option the most up-to-date employee data that resides in the database, will not be over-written by the import.

Select the import type.



Click the Browse button, locate and select the “.upb” import file and then click the Import Users button.

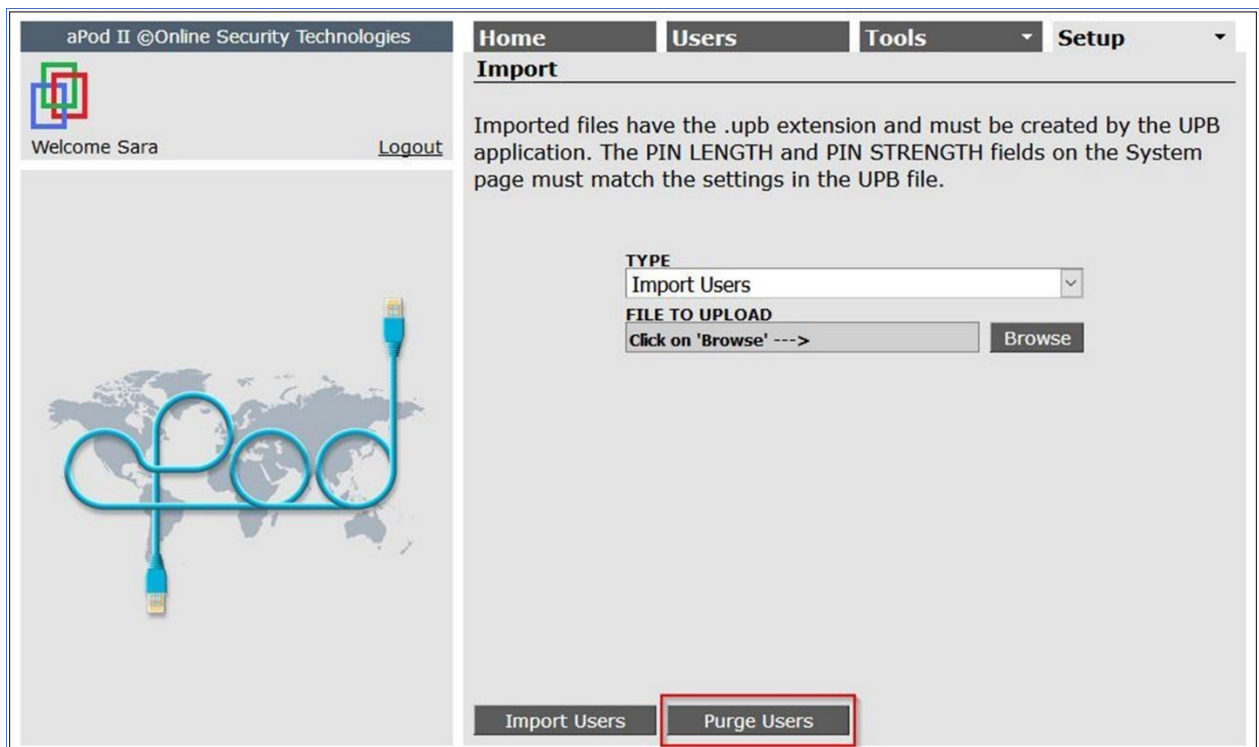
A successful import is indicated by the following message.



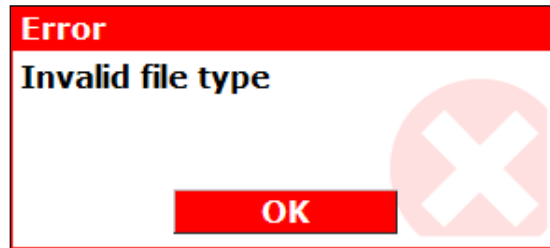
The import function does not allow duplicate records so only new records will be imported. For example, if three of the records in the previous example were already in the database the following message would be returned.



When making updates during the system commissioning stage it is advisable to purge the user database and import all records. This will ensure that previously loaded records that have been edited in Excel will be updated. Click the Purge Users button to clear the User database.



If the format of the import file is not correct, the import function will be terminated without importing any records and the following message will be displayed.



This would occur for example, if there were blank fields or records. It would also be displayed if the wrong file type were accidentally saved and imported, for example an Excel file rather than a tab delimited text file.

## 7. Review the imported data records.

Some Employee data is not imported because the system default values usually apply, and it is not practical to enter the data into the Excel spreadsheet. User options and the access token validation interval are the primary examples.

After the import, run the User report which can be found at...

[Tools](#)→[Reports](#)→[Report Type](#)→[Users](#) and check the data for possible errors.

Access Control Report														Print	Close
Users															
User Options:															
AA:	Assisted Access														
SU:	Suspended														
3L:	3X Lock/Unlock														
3A:	3X Arming														
SA:	Silence Alarms														
PU:	Pending Unlock														
DE:	Deny entry if Armed														
LA:	Lockout Access														
LD:	Lockdown Access														
Name	Card ID	User ID	AA	SU	3L	3A	SA	PU	DE	LA	LD	Validation	User Group	+ User Group	
David Martin	319455405	1				3A	SA					Always	Administration	None	
Jane Anderson	319455406	2	AA									Always	Customer Service	None	
Olin Reese	319455407	3										Always	Sales	Parking Garage	
Richard Evans	319455408	4										Always	Production	None	
Sandy Thomas	319455409	5										Always	Administration	None	
Sara Friedman	319456565	6			3L							Always	Administration	None	



## Advanced Options

### Update the Software.

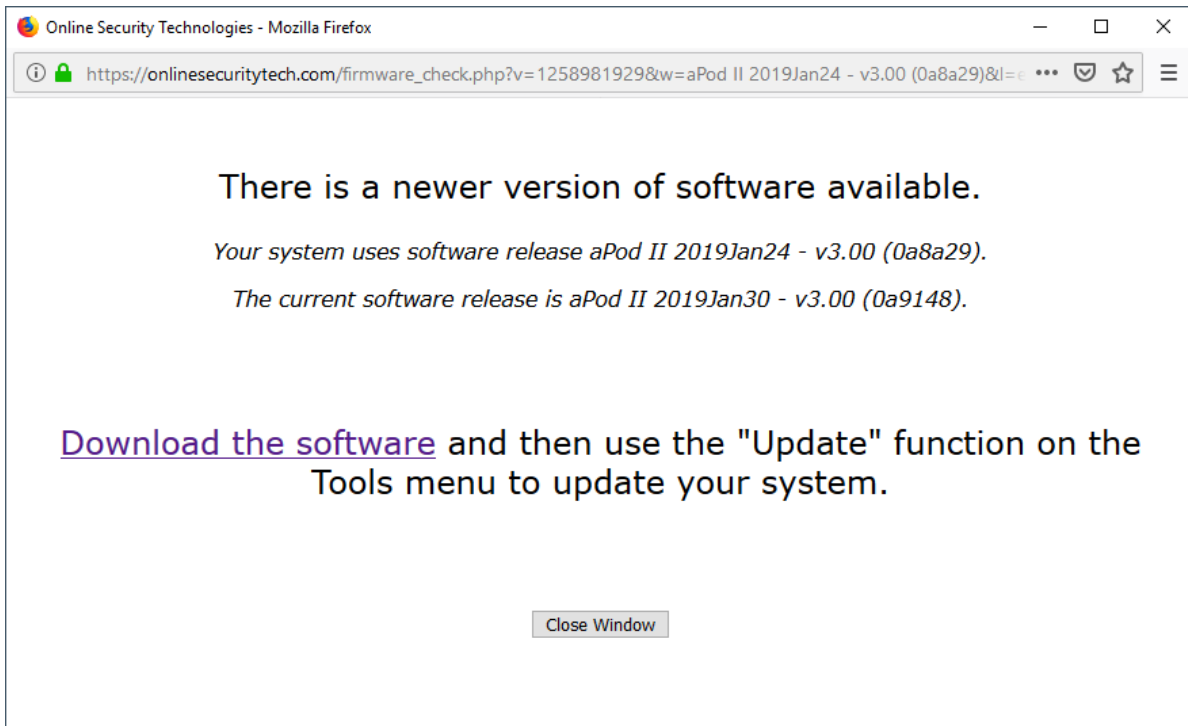
An administrator must have the “Update Software” permission to use this function. Check to see if an update is available.

The screenshot shows the 'Update' page in the aPod II admin interface. The page displays the current software version as 'aPod II 2019Jan30 - v3.00 (0a9148)'. There is a 'FILE TO UPLOAD' section with a 'Browse' button. A 'Check for latest version' button is highlighted with a red box and a red arrow pointing to a yellow callout box that says 'Click here to check if a software update is available. There must be an Internet connection.' At the bottom, there are 'Update Now' and 'Update ±4AM' buttons.

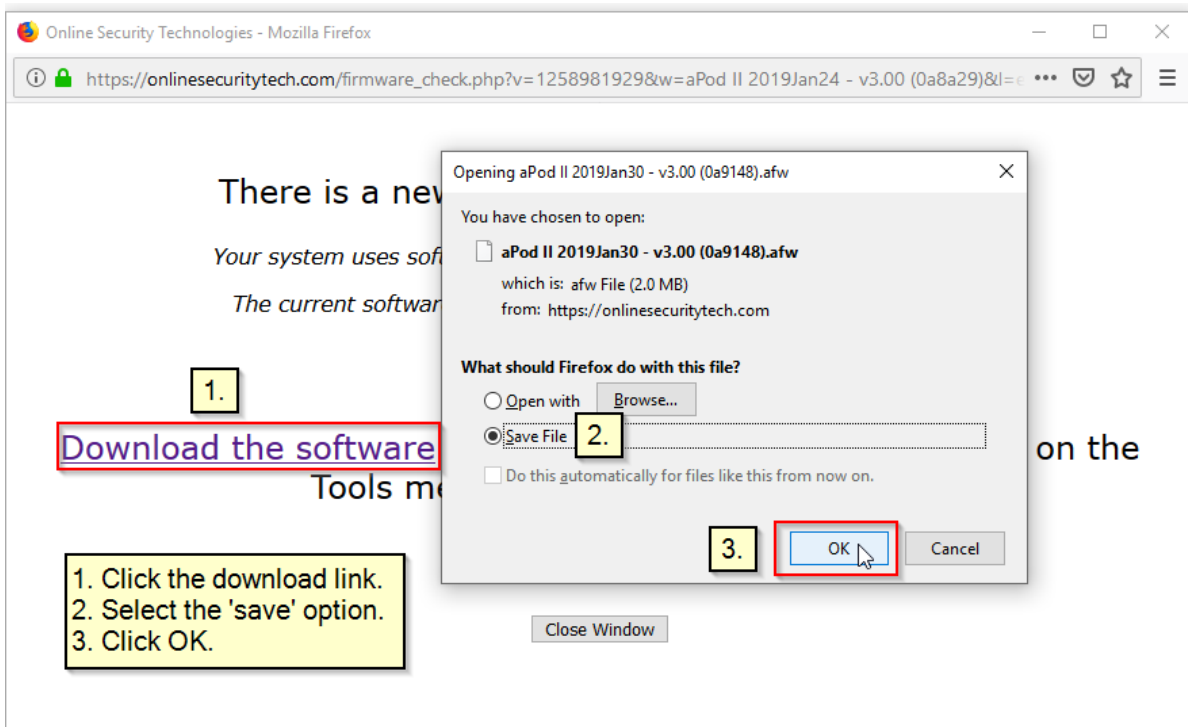
If you have the latest version of software, you will see this pop-up message.

The screenshot shows a Mozilla Firefox browser window displaying a pop-up message: 'Congratulations! Your system is up to date.' with a 'Close Window' button.

If a newer version of software is available, you will see a pop-up message like this one.



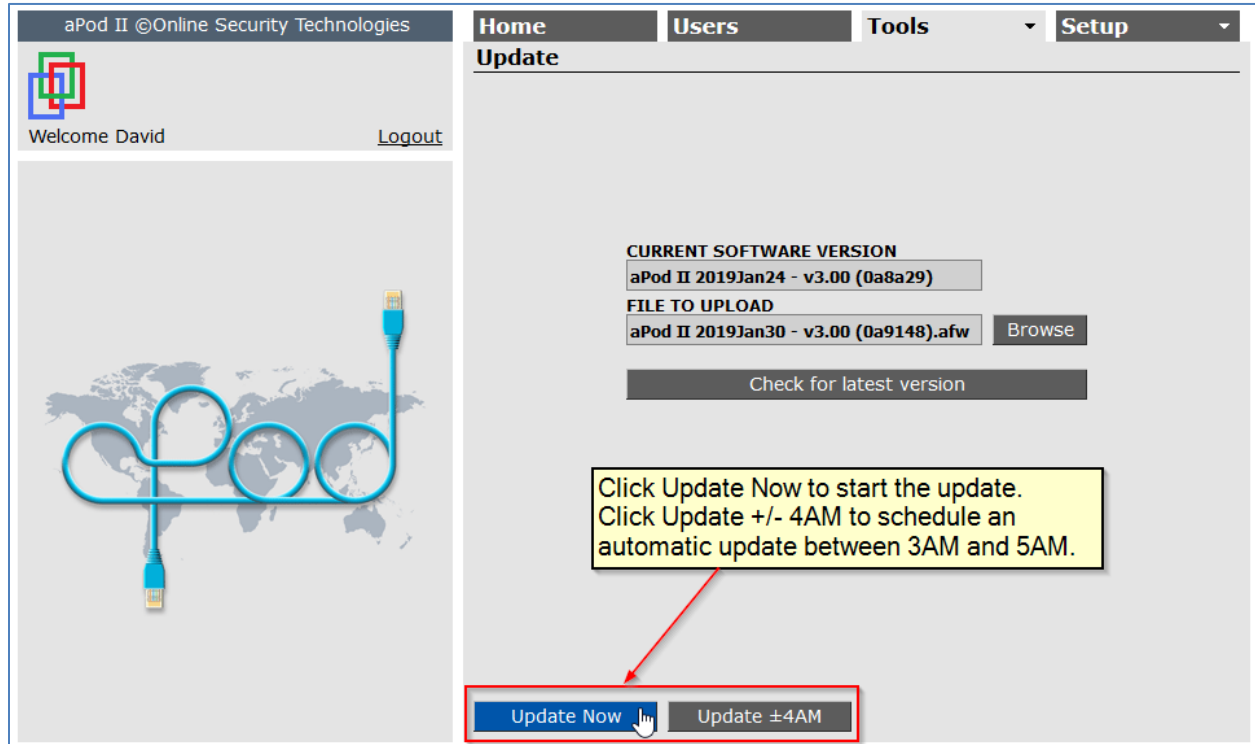
Click on the link to download the new software version through your Internet connection.



Firefox 64.0 on Windows 10

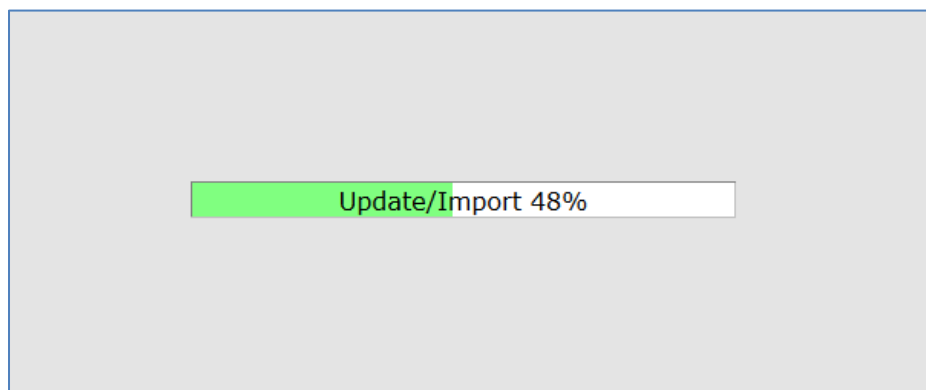
Save the new software file to your computer's hard drive, noting where it is saved. By default, most browsers on PC's save downloaded files to the 'Downloads' subdirectory in the 'My Documents' directory. You can configure your browser to ask where to save downloads which allows you to select a different save location.

Close the pop-up message. Click the **Browse** button and use the browse window to locate and select the file you just saved. Ensure that it is displayed in the **FILE TO UPLOAD** field.



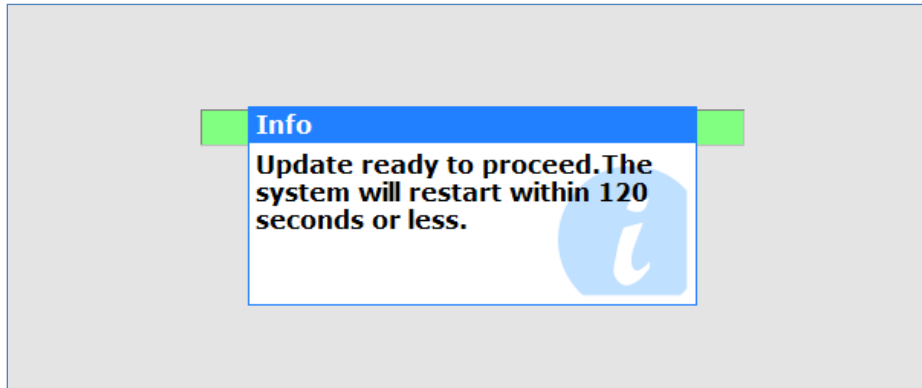
Click **Update Now** to start an automatic and complete system software update.

The new software file will be uploaded to the aPod II Primary Controller as a background task. The upload progress will be indicated by a progress bar.

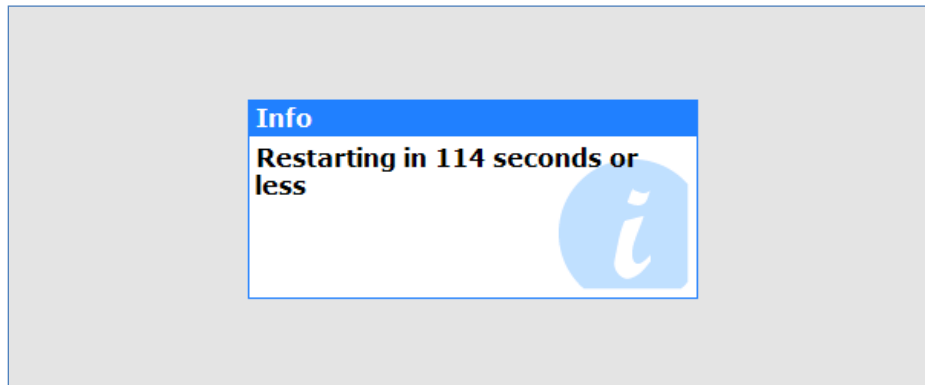


During the upload period the controller will continue to function normally. After the file has been validated to ensure its integrity, the controller will re-boot and begin using the new software. During the re-boot, the controller will be offline for approximately thirty to forty seconds.

When the software has been validated the following message is displayed.

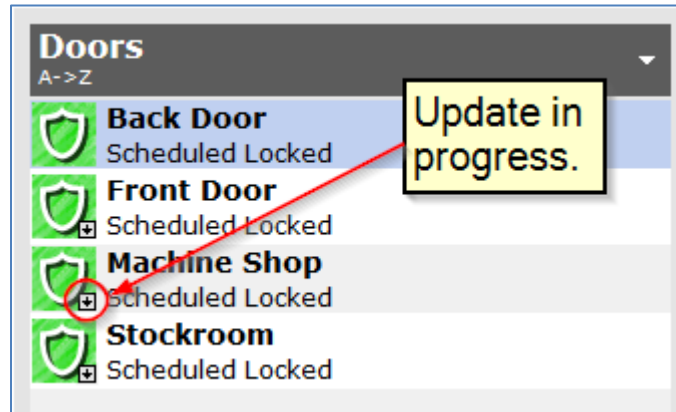


During the re-boot process the following message displays a count down from 120 seconds.



If you have a multi-door system, the updated Primary Controller will upload the new software to every Secondary controller. These controllers will validate the software; reboot using the new software and return to normal operation.

The door status icon for each Secondary controller in the doors list on the Home page will indicate that a software update is in progress. A flashing 'update' icon will appear in the lower right corner of the door status icon and will disappear when the update is complete.

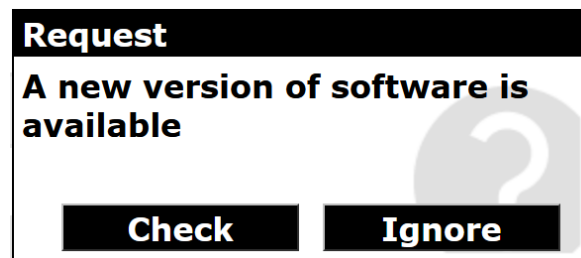


If the short period of downtime while the door controllers re-boot is too inconvenient, for example, on high traffic doors, click **Update ±4AM** . This will schedule an automatic update which will be performed automatically sometime between 3 a.m. and 5 a.m. the next morning. During the brief re-programming process the doors will remain locked.

The software update has been designed to be fail-safe. Power failures, loss of communications, removal of door controllers or any other update interruption will not cause your system to be corrupted. If the update process is interrupted, the Primary Controller will repeat the process until it is successful. The software update process does not alter your system database.

## New software notification

If a new software version is available, a notification will be displayed when you log into the Browser Interface. Only administrators with "Update Software" permission, will see this message. The **Check** button will take you to the Tools→Update page to proceed with the software update as described on page 147.





## Remote Login

The aPod II Access Control System provides the ultimate in remote connectivity. It can be managed from anywhere there is Internet access with any device that uses a browser, including PC's, MAC's, tablet computers and smart phones. Set up remote login to facilitate system management and support.

Remote Login is configured in two steps.

1. Enter a site name and address to identify your system.
2. Configure communications through the Internet and Local Area Network

Step 2 may require the assistance of your IT administrator.

### Step 1 - Identify the system

The **SITE NAME** and **SITE ADDRESS** fields on the System page identify the system. You must complete these fields to enable remote login. They can be changed at any time.

The screenshot shows the 'aPod II ©Online Security Technologies' web interface. The 'System' configuration page is active, with a red box highlighting the 'SITE NAME' and 'SITE ADDRESS' fields. The 'SITE NAME' is 'David Martin Custom Parts' and the 'SITE ADDRESS' is '142 Oakdale Rd, Kingston ON'. Other visible fields include 'TIME ZONE' (Eastern Time), 'DAYLIGHT SAVINGS' (Enabled), 'CUSTOM APP #1-3', 'LANGUAGE' (English), 'ACCESS AUTHORIZATION' (By User Groups), 'PIN LENGTH' (4 Digits), 'PIN STRENGTH' (Standard), 'ADMINISTRATOR TEMPORARY PASSWORD' (masked), 'ELEVATORS' (None), 'PRIMARY INTERNET IP' (64.228.90.180), 'PORT (UDP)' (5268), 'REMOTE LOGIN SETUP' (Automatic), 'REMOTE HTTP PORT (TCP)' (25268), 'PC's DATE/TIME' (Mon, Apr 26, 2021 5:12:28 PM), 'aPod's DATE/TIME' (Mon, Apr 26, 2021 5:12:26 PM), 'SELECTED LOCALE' (Ontario), and 'PRIMARY IP ADDRESS' (192.168.2.164). Buttons for 'Save' and 'Cancel' are at the bottom.

The **SITE NAME** and **SITE ADDRESS** are displayed in the header of the Login page.



## Step 2 - Configure communications

A remote connection is only possible if two conditions are met.

1. The browser must know the Internet address of the gateway device on the LAN that contains the aPod II Primary Controller. The Internet gateway device is typically a cable or DSL modem or a combination modem/router.

*In other words, where on the Internet is your private network?*

2. The LAN router must also be configured to direct remote connection requests from the Internet to the aPod Primary Controller's private LAN address. This process is called port forwarding.

*In other words, where on your private network is the aPod Primary Controller?*

## Configure the aPod II Controller.

Complete the first step by selecting the “Automatic (DDNS)” setting in the **REMOTE LOGIN SETUP** field on the Setup→System page.

The screenshot shows the 'Setup System' page of the aPod II controller. The 'REMOTE LOGIN SETUP' dropdown menu is open, with 'Automatic (DDNS)' selected and highlighted in blue. A red box highlights the dropdown menu. A yellow callout box with the text 'Remote login configuration options.' points to the dropdown menu. The page includes various configuration fields such as SITE NAME, TIME ZONE, LANGUAGE, ACCESS AUTHORIZATION, and PRIMARY INTERNET IP. The 'Save' and 'Cancel' buttons are visible at the bottom.

Field	Value
SITE NAME	David Martin Custom Parts
SITE ADDRESS	142 Oakdale Rd, Kingston ON
TIME ZONE	Eastern Time (GMT-5:00)
DAYLIGHT SAVINGS	Enabled
CUSTOM APP #1	
CUSTOM APP #2	
CUSTOM APP #3	
LANGUAGE	English (en)
ACCESS AUTHORIZATION	By User Groups
PIN LENGTH	4 Digits
PIN STRENGTH	Standard
ADMINISTRATOR TEMPORARY PASSWORD	••••••••
ELEVATORS	None
PRIMARY INTERNET IP	64.228.90.180
PORT (UDP)	5268
REMOTE LOGIN SETUP	Automatic (DDNS)
REMOTE HTTP PORT (TCP)	25268
aPod's DATE/TIME	Mon, Apr 26, 2021 5:16:33 PM
PRIMARY IP ADDRESS	192.168.2.164

## Configure the router.

Complete the second step by adding a port forward record in the router of the aPod II Controller's local area network. Log into the router through a browser by entering its IP address for the URL. Locate the menu page that allows the creation of port forward records.

**Note:** If necessary, you can find the default login credentials and port forward instructions on the Internet by searching for the router make and model number.

The port forward record will require the inputs that are shown in the table that follows. The terminology may vary with different routers.

<b>Application Name:</b>	A name to identify the port forward record, for example, "aPod Controller".
<b>Protocol:</b>	TCP
<b>Public (external) port range</b>	Use the default port 25268. (25268 to 25268 if a range is required).  If necessary, this port number can be changed in the port forward record with a matching entry in the <b>REMOTE HTTP PORT (TCP)</b> field on the aPod's Setup→System page. <u>Refer to the image that follows.</u>
<b>Private (internal) port range</b>	Use port 80. (80 to 80 if a range is required)
<b>Local IP address</b>	Use the address displayed in the <b>PRIMARY IP ADDRESS</b> field on the aPod's Setup→System page. <u>Refer to the image that follows.</u>
<b>Status</b>	Set to enable


Save the record.

The screenshot shows the 'System' configuration page in the aPod II interface. The 'REMOTE HTTP PORT (TCP)' field is set to 25268 and the 'PRIMARY IP ADDRESS' field is set to 192.168.2.164. A yellow callout box with a red arrow points to these two fields, stating: "These data are used to create a port forward record in the router." Other visible fields include SITE NAME (David Martin Custom Parts), SITE ADDRESS (142 Oakdale Rd, Kingston ON), TIME ZONE (Eastern Time (GMT-5:00)), LANGUAGE (English (en)), ACCESS AUTHORIZATION (By User Groups), PIN LENGTH (4 Digits), PIN STRENGTH (Standard), ADMINISTRATOR TEMPORARY PASSWORD (masked), PRIMARY INTERNET IP (64.228.90.180), PORT (UDP) (5268), PC's DATE/TIME (Mon, Apr 26, 2021 5:23:09 PM), and SELECTED LOCALE (Ontario).

## Remote Login Portal

Use the Remote Login Portal on the Online Security Technologies website to access your system's Login page through the Internet. The Remote Login Portal can be accessed by following the link on the Customer Support page.


Its direct URL is [https://onlinesecuritytech.com/remote\\_connect\\_out.php](https://onlinesecuritytech.com/remote_connect_out.php).

Bookmark this page for easy access. Enter your login email address and click the  button. A connection link is displayed for every system in which you have Remote Login permission.


### Remote Connect

**Remotely connect to your aPod Access Control System from anywhere you have Internet Access.**

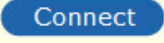
Enter your Remote Connect Email Address in the field below and click the Go button to display your link(s). Click 'Connect' to access your Login screen.

Email Address:  

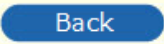
---

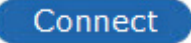
System: **Central Parts Depot - 15 Lakeside Drive, Kingston ON** 

---

System: **Dave Martin Custom Parts - 142 Oakdale Rd, Kingston ON** 

---



Click the  button to display the system Login screen for the system you wish to access. The system name and address are displayed in the header.

**aPod II - David Martin Custom Parts, 142 Oakdale Rd, Kingston ON**

**The header identifies your system.**

**ENTER LOGIN EMAIL ADDRESS**

**ENTER PASSWORD**

**Login**

**Extend Auto Logout**

## Notes:

1. If the connection link appears in the remote login portal but it does not provide a connection to the aPod II login screen, the port forward record is not properly configured in the LAN router. Re-check the port forward record following the directions on page 154.
2. The remote login feature should not be tested by accessing the OST Remote Connect web page from a device that is connected to the local area network. If the router is configured for loopback the connection will be made locally. Switch off Wi-Fi on your mobile phone and use the Internet via the phone's mobile network.

## Manage the remote login permission.

Remote Login is enabled by default. This permission can be disabled for individual administrators with restricted authority on the Administrators page under the Setup menu.

Only administrators with the 'Manage IP Parameters' permission can edit the Remote Login privilege.

The screenshot shows the 'aPod II' web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The main content area is titled 'Administrators (edit)'. On the left, there is a list of administrators: David Martin (dmartin@gmail.com), Richard Evans (richard.evans@winsome.com), and Sara Friedman (sara@onlinesecuritytech.com). The 'Sara Friedman' entry is selected. The main form displays the details for Sara Friedman: FIRST NAME (Sara), LAST NAME (Friedman), LOGIN EMAIL ADDRESS (sara@gmail.com), and PASSWORD (Valid password). Below the form, there are two columns of permissions under the heading 'ADMINISTRATOR PERMISSIONS'. The 'Manage IP Parameters' checkbox is highlighted with a red box. At the bottom, there are buttons for 'Add', 'Save', 'Cancel', and 'Delete'.

ADMINISTRATOR PERMISSIONS	ADMINISTRATOR PERMISSIONS
<input checked="" type="checkbox"/> Remote Login	<input checked="" type="checkbox"/> Full Authority
<input checked="" type="checkbox"/> Manage Users	<input checked="" type="checkbox"/> Manage Schedules
<input checked="" type="checkbox"/> Silence Alarms	<input checked="" type="checkbox"/> Manage Door Options
<input checked="" type="checkbox"/> Bypass Inputs	<input checked="" type="checkbox"/> Manage IP Parameters
<input checked="" type="checkbox"/> Grant Access	<input checked="" type="checkbox"/> Manage Administrators
<input checked="" type="checkbox"/> Override Door Schedules	<input checked="" type="checkbox"/> Backup the system
<input checked="" type="checkbox"/> Run Reports	<input checked="" type="checkbox"/> Restore the system
<input checked="" type="checkbox"/> Arm/Disarm Alarm Panel	<input checked="" type="checkbox"/> Update Software

## Proxy Servers and Firewalls

If a proxy server or firewall is used to control communication between the LAN and the Internet, then they must be configured to allow communication between the Internet and the aPod II Primary Controller. *Proxy servers and firewalls are usually encountered with larger networks that have an IT support person. Request their assistance to handle the configuration.*

## Systems with a static Internet address

The Internet address of your modem/router can be static (fixed) or dynamic (periodically changed by your Internet Service Provider). If a static IP address is used, then the Internet address of your private network is always known and can be bookmarked for easy access. In this case, there is no need to use the OST Remote Login Portal to connect with your system.

Complete the communications channel by creating a port forward record in the router for the aPod II Remote Connect application as described on page 154.

System administrators should create a bookmark on any device they use to access the aPod II System Login page through the Internet. The bookmark will contain the static IP address with the port number appended. A colon precedes an appended port number.

In the example shown on page 155, if the static IP address is 64.228.90.180 and the **REMOTE HTTP PORT (TCP)** is 25268, a bookmark labelled 'aPod II Login' would have the following URL.

**http://64.228.90.180:25268**

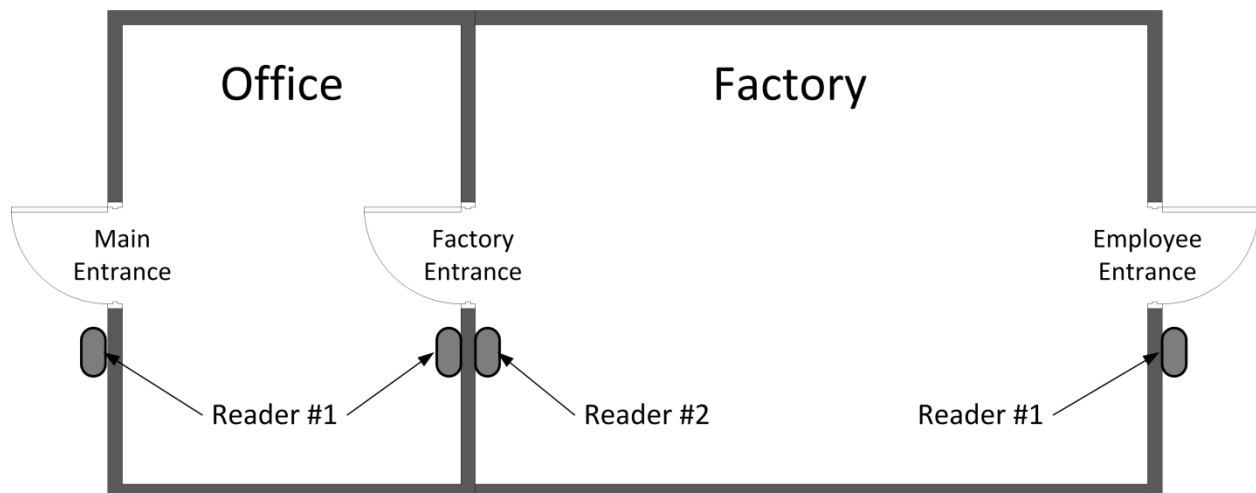
## Alarm Panel Interface

### Overview

Most alarm panels support the aPod II Alarm Panel Interface requirements. If this feature has been enabled in your system, the necessary hardware connections and configurations would have been made during the system installation. If you would like to add this function to your system or modify it, please contact your installing dealer.

Many false alarms occur when arming or disarming an intrusion detection system. Pin codes are forgotten or entered incorrectly, too much time is taken entering or leaving an armed facility, or the entry/exit route is not correct. These problems can be eliminated by interfacing the alarm panel to the aPod II Access Control system. The interface will allow an authorized User to arm or disarm the alarm panel with their access token at a reader located outside of the armed area and thus avoid tripping a false alarm.

An alarm panel provides intrusion detection for an enclosed area and uses various detectors to monitor all points of entry and any activity within the area. Many facilities use only one intrusion detection area which encompasses the entire facility. Larger facilities may be partitioned into two or more areas. This provides more flexibility for using the facility outside of normal business hours. In the example below, the office area and the factory area can be armed independently to allow work to continue in either area as required.



If your alarm panel monitors multiple areas within your facility, you will be able to arm and disarm each area independently using your aPod II Access Control System.



## Features of the aPod II Alarm Panel Interface


- Designate which Users can arm or disarm the alarm panel. If a User does not have permission to disarm the alarm panel, their token will not unlock a door into an armed area regardless of their normal access permission.
- Approved Users can arm the alarm panel from outside the armed area using their access token. There is no way to trip a false alarm.
- Approved Users will disarm the alarm panel automatically when they unlock the door with their access token. There are no false alarms caused by PIN entry errors or delays in disarming.
- Disarm the panel using Card+PIN access mode for higher security.
- There is both visual and audio feedback to indicate if the arming/disarming action was successful or not. When accessing an armed area, the unlock action is delayed until the 'disarmed' status has been verified.
- An area can be armed or disarmed at any access point to the area. There is no designated entry/exit route.
- An arming delay of 10 to 60 seconds can be configured. No delay is configured by default.
- Administrators with remote login authority can arm or disarm the alarm panel from anywhere there is Internet access.
- All arming and disarming events are recorded in the event log.
- A security alert can be transmitted by email to designated Administrators whenever the alarm panel is armed or disarmed.
- Arming an area automatically locks all doors into that area and overrides any scheduled unlock periods. Arming is prevented if a door into the area is open. The open door is indicated on the event log.
- The aPod II System can independently arm and disarm different areas within your facility if your alarm panel supports multiple partitions.

## Arm the Alarm Panel with Your Access Token

An authorized User can arm the alarm panel by presenting their access token three times to the reader of any controlled door that allows access to the armed area.

- **For a brief period while the controller waits for a response from the alarm panel the reader LED will flash the unlock colour (green) at a frequency of 2X per second.** If the arming is successful, you may not notice this because the response is almost immediate.
- **If the arming request was successful, the reader buzzer will sound six short beeps in rapid succession.** If a proximity reader that supports independent control of a tri-colour LED is used, the reader LED colour at every controlled access point to the armed area will change from blue (signifying locked and area disarmed) to red (signifying locked and area armed). Readers with bi-colour LED's will not provide this visual feedback.
- **If the arming request failed, the reader buzzer will sound one long continuous beep.** The reader LED colour will not change. If the arming request fails, the User must re-enter the building and investigate why the alarm panel failed to arm.

The arming attempt and result are recorded in the event log.

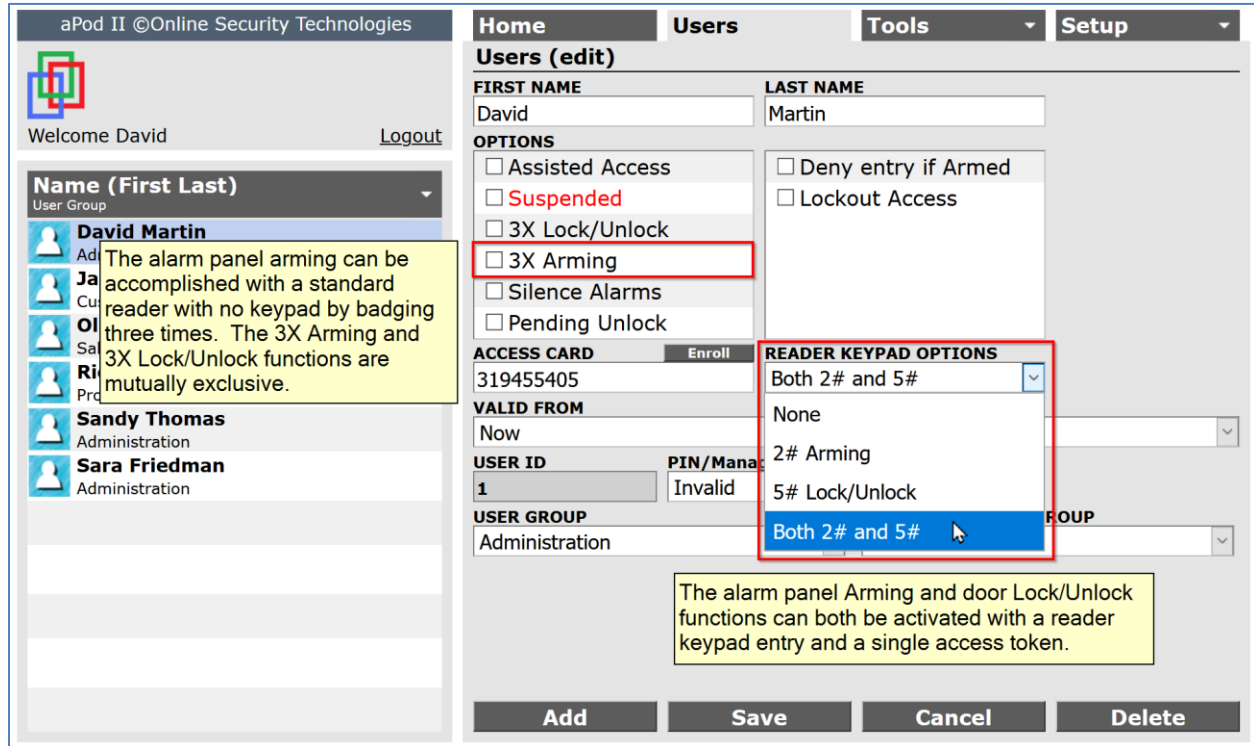
	Sat, Feb 2, 2019 12:12:17 PM (-5:00) - at <b>Front Door</b> <b>Office Armed by David Martin</b>	^
	Sat, Feb 2, 2019 12:14:27 PM (-5:00) - at <b>Back Door</b> <b>Machine Shop Armed by Richard Evans</b>	^
	Sat, Feb 2, 2019 12:17:37 PM (-5:00) - at <b>Front Door</b> <b>Office Failed to Arm (door open) by David Martin</b>	^
	Sat, Feb 2, 2019 12:21:31 PM (-5:00) - at <b>Front Door</b> <b>Office Failed to Arm (check panel) by David Martin</b>	^

**Note:** When using the 3X Arming function, allow 1 second between each card swipe. The reader buzzer should beep after each swipe. This delay is necessary because most access readers have a short lockout period after each card swipe to prevent accidental double reading of the same token.

If the door is locked, the first card swipe will unlock the door. This is normal operation. Proceed with the arming function. The door will automatically re-lock.

## Assign authority for Arming the Alarm Panel

You can give any User the authority to arm the alarm panel by selecting the '3X Arming' option on the Users page.



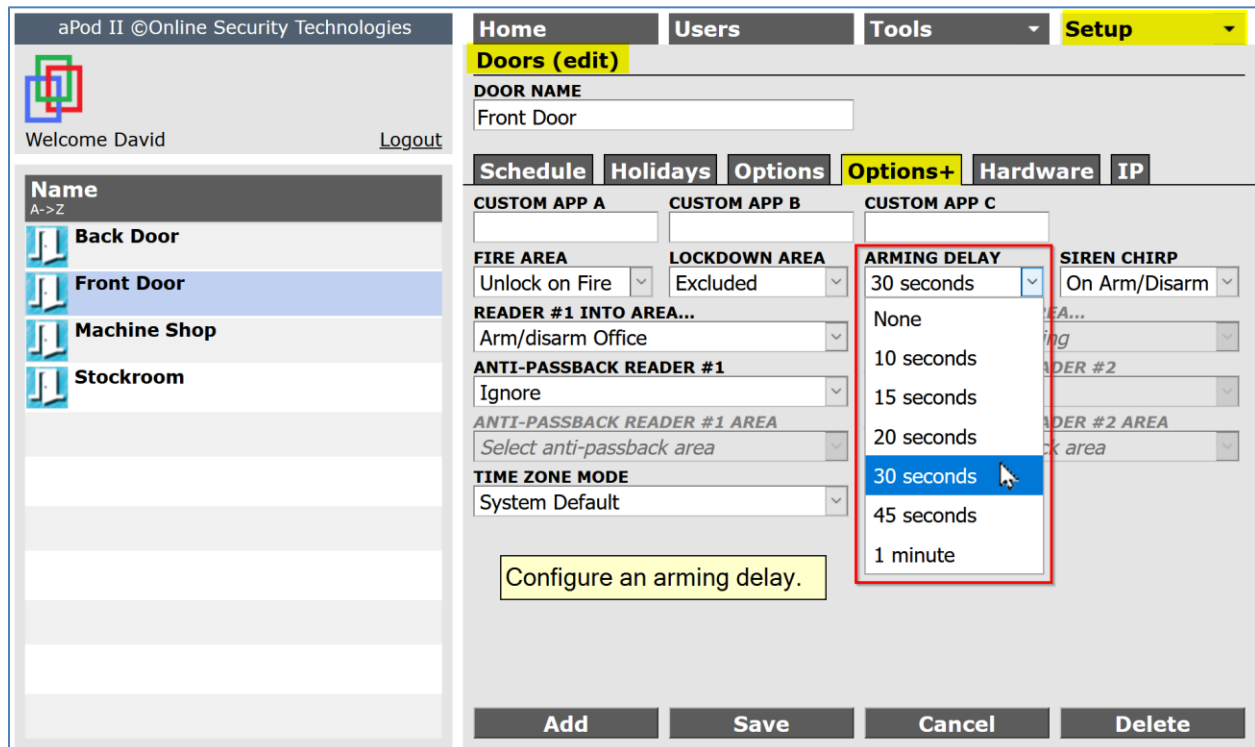
### Notes:

1. The '3X Lock/Unlock' and '3X Arming' options are mutually exclusive. Badging three times will either unlock the door if the first option is selected or arm the alarm panel if the second option is selected. If a User needs to have both functions, you can create an alternate User name for them and assign the second option to the other token. If a keypad reader is present, a user can have both permissions with a single access token. Refer to page 113.
2. The aPod II System will automatically lock all access doors to the armed area when the panel is armed regardless of the door locking schedules.
3. If a door to the armed area is open, the aPod II System will abort the arming request, provide audio feedback of the failed arming attempt using the reader buzzer and report the problem in the event log.
4. An entry point to the armed area that is not controlled by the aPod II System should be maintained in a locked state to prevent an unauthorized entry which would cause a false alarm.

## Delayed arming

The arming request from the aPod II controller to the alarm panel can be delayed by a configurable time interval. A delay may be necessary if there is an automatic door opener on one of the access doors. The delay allows the door to close and lock before the arming request is issued.

The arming delay is configured on the Setup→Doors→Options+ tab of the primary controller.



Audio feedback from the reader buzzer will indicate the status of the arming delay.

***During the arming delay the reader buzzer at every controlled access point to the armed area will sound once every two seconds.*** At the end of the arming delay, the aPod II controller will issue the arming request and then report if the attempt was successful or not.

## Disarm the Alarm Panel

Any *authorized* User will automatically disarm the alarm panel and unlock the door when they badge their token at the reader of any controlled door that allows access to the armed area.

- ***For a brief period while the controller waits for a response from the alarm panel the reader LED will flash the unlock colour (green) at a frequency of 2X per second.*** If the disarming is successful, you may not notice this because the response is almost immediate.
- ***If the disarming request was successful, the reader buzzer will sound twelve short beeps in rapid succession and then unlock the door.*** If a proximity reader that supports independent control of a tri-colour LED is used, the reader LED colour at every controlled access point to the armed area will change from red (signifying locked, and area armed) to blue (signifying locked, and area disarmed). Readers with bi-colour LED's will not provide this visual feedback.
- ***If the disarming request failed, the reader buzzer will sound one long continuous beep and then unlock the door.*** The reader LED colour will momentarily change to green when the door is locked and then return to red. If the disarming request fails, the User must proceed directly to an alarm panel keypad and enter their code to disarm the panel or delay their entry until they receive assistance.

**Note:** When the alarm panel interface is professionally installed and configured, a failure to disarm is very unlikely.

The disarming attempt and result are recorded in the event log.

	Sat, Feb 2, 2019 3:03:21 PM (-5:00) - at <b>Front Door</b> <b>Access Office by David Martin</b>
	Sat, Feb 2, 2019 3:03:18 PM (-5:00) - at <b>Front Door</b> <b>Office Disarmed by David Martin</b>

	Sat, Feb 2, 2019 3:06:45 PM (-5:00) - at <b>Back Door</b> <b>Access Machine Shop by Richard Evans</b>
	Sat, Feb 2, 2019 3:06:42 PM (-5:00) - at <b>Back Door</b> <b>Machine Shop Disarmed by Richard Evans</b>

	Sat, Feb 2, 2019 3:09:41 PM (-5:00) <b>Office Failed to Arm (check panel) by David Martin</b>
	Sat, Feb 2, 2019 3:08:42 PM (-5:00) - at <b>Front Door</b> <b>Office Disarmed through Alarm System</b>

**Note:** The alarm panel disarming process precedes the unlocking of the door. The audio and visual feedback provided by the aPod II System will confirm the panel armed/disarmed status before the User enters the area.

The door locking schedule which is in effect at the time an area is disarmed will be re-instated for each access point and the configured scheduled unlock option will be applied. Refer to page 44 for more information about the scheduled unlock options.

### Authorization to Disarm the Alarm Panel

A User is *authorized* to disarm the alarm panel if they have access permission and have not been denied entry when the area is armed.

By default, all Users have permission to disarm the alarm panel if they have access permission to the armed area. If you wish to restrict this privilege, you can use the 'Deny Entry if Armed' option on the Users page.

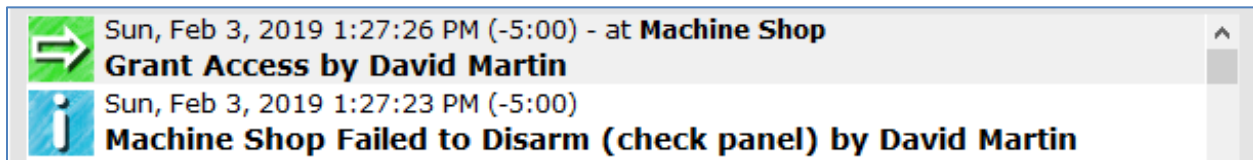
This option supersedes the User's normal access permission. If they have permission to access the area and this option is not checked, the alarm panel will be disarmed, and the door will be unlocked. If this option is checked, the alarm panel will not be disarmed, and the door will remain locked.

The screenshot shows the 'Users (edit)' form in the aPod II interface. The form is for editing the user 'David Martin'. The 'Deny entry if Armed' checkbox is highlighted with a red box. The form includes fields for First Name, Last Name, Options, Access Card, Reader Keypad Options, Valid From, Valid Until, User ID, PIN, User Group, and Additional User Group. The 'Deny entry if Armed' checkbox is currently unchecked.

Field	Value
FIRST NAME	David
LAST NAME	Martin
OPTIONS	<input type="checkbox"/> Assisted Access <input type="checkbox"/> Suspended <input type="checkbox"/> 3X Lock/Unlock <input checked="" type="checkbox"/> 3X Arming <input checked="" type="checkbox"/> Silence Alarms <input checked="" type="checkbox"/> Pending Unlock
ACCESS CARD	319455405
READER KEYPAD OPTIONS	None
VALID FROM	Now
VALID UNTIL	Forever
USER ID	1
PIN	Unassigned
USER GROUP	Administration
ADDITIONAL USER GROUP	Unassigned

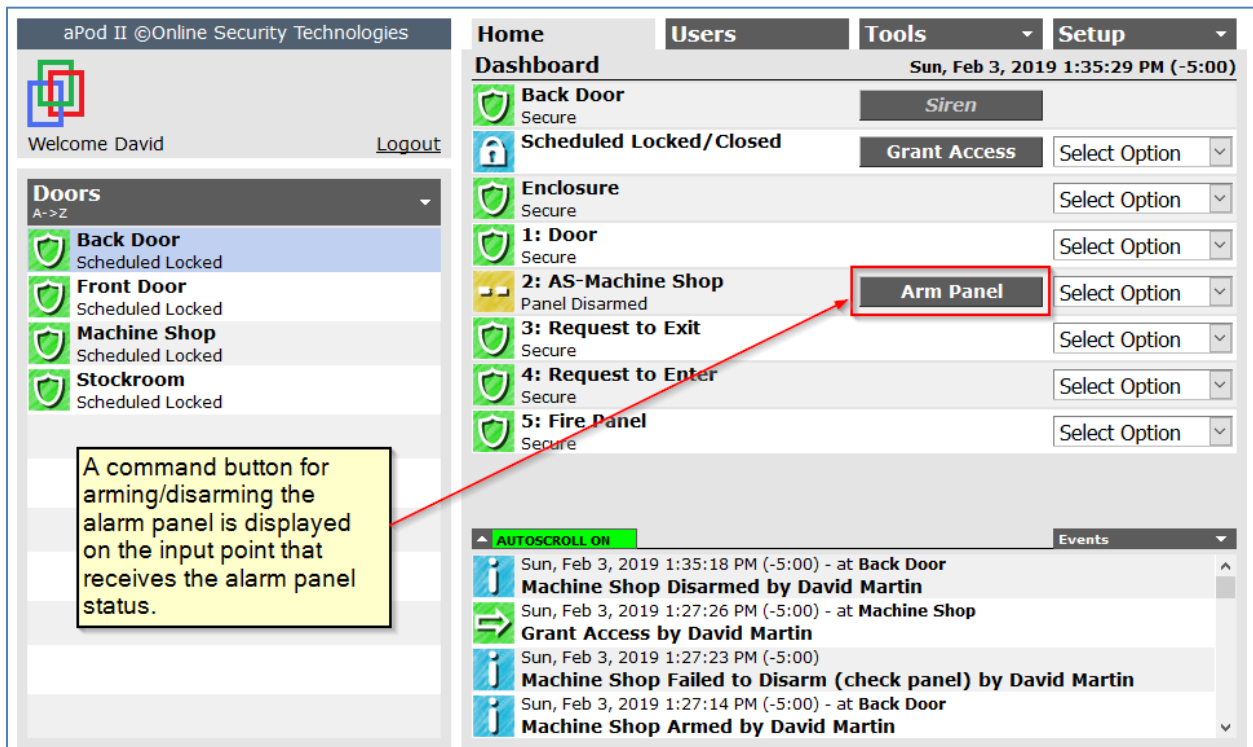
## Disarm with Grant Access

If an administrator unlocks a door to an armed area using the Grant Access command button on the Home page, the aPod II controller will issue the disarming request and then report if the attempt was successful or not.



## Remote Arming and Disarming

When a door is configured with an alarm panel interface, its record on the Home page will display a command button for arming or disarming the alarm panel.




When the alarm panel monitors two or more areas independently, the default name for the alarm panel input should be changed to indicate the area to which the door allows access. This is the area that the button will arm or disarm.


The names of input points can be changed on the [Setup](#)→[Doors](#)→[Hardware](#) page. Refer to page 51 for more information.

<b>INPUT #3</b> Alarm Panel	<b>CIRCUIT #3</b> Normally Closed	<b>NAME #3</b> AS-Machine Shop
--------------------------------	--------------------------------------	-----------------------------------

This input point will be displayed as follows.

 <b>2: AS-Machine Shop</b> Panel Disarmed	<b>Arm Panel</b>	Select Option
---	------------------	---------------

The alarm panel input point displays the arming status in real time and the command button follows the status.

 <b>2: AS-Machine Shop</b> Panel Disarmed	<b>Arm Panel</b>	Select Option
--	------------------	---------------

 <b>2: AS-Machine Shop</b> Panel Armed	<b>Disarm Panel</b>	Select Option
--	---------------------	---------------

Click the **Arm Panel** and the **Disarm Panel** buttons to remotely arm or disarm the alarm panel. The success or failure of the arm/disarm request will be indicated by the status of the alarm panel input point and the event recorded in the event log.

The arm/disarm function on the Browser Interface allows an administrator to remotely arm or disarm the alarm system through the Internet provided they have been assigned the Remote Login function and have the required authority level.

### Important Note:

The Browser Interface can be used to arm the alarm panel from a PC located within the facility. This is not advisable as it increases the potential for a false alarm. If an administrator arms the alarm panel while still in the premises, they must exit the building within the prescribed time and use the prescribed exit route. A better method is to exit the building and then arm the system using 3X badging at the aPod II access reader.



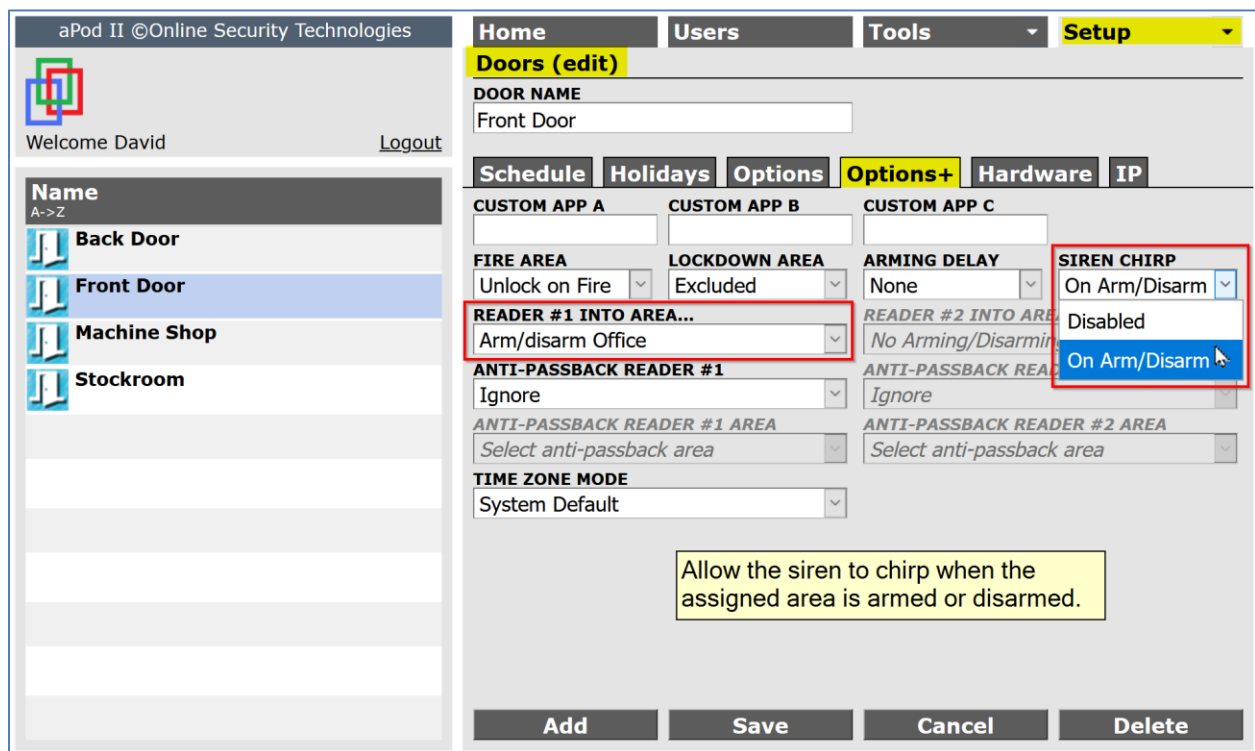
## Arming/Disarming Security Alerts

The aPod II System can transmit a security alert whenever the alarm panel is armed or disarmed. You can enable this function on the [Setup](#)→[Preferences](#) page. Refer to page 27 for more information.

## Piezo Siren Annunciation

The aPod II System can also provide a more pronounced indication of the arming and disarming status by chirping a Piezo siren connected to the primary controller. This may be useful for some external readers where the background noise makes the reader buzzer difficult to hear.

This feature is enabled on the [Options+](#) tab of the [Doors](#) page of the primary controller as shown below.



The siren will chirp once when the area is armed and twice when it is disarmed. There is no chirp if the area fails to arm or disarm.

## Anti-passback

### Introduction

A 'passback' describes an attempt to compromise an access control system in which an access token is used by more than one person. A valid User gains access and then "passes" or loans his token to someone else to enable them to enter. A parking lot with restricted access is a prime example of where a passback may be used. The anti-passback logic in the aPod II Controller prevents this manoeuvre.

Anti-passback is often used in conjunction with time and attendance reporting because it will enforce more accurate tracking of on-site time.

Logical anti-passback requires at least one access point with an exit reader as well as an entrance reader. Users must badge out to exit as well as badge in to enter. The aPod II System keeps track of the **IN/OUT** status of every User. The controller will take the appropriate action if the User is not correctly located when they badge their token at an access point. If a User fails to badge in, by tailgating for example, they may be refused an exit later because their **IN/OUT** status is incorrect.

Similarly, if a User fails to badge out, by simply turning the doorknob or pushing the crash bar to unlatch the door for example, they may be refused an entry later because their **IN/OUT** status is incorrect.

Simple timed anti-passback is possible with a single entrance reader but this mode is more inconvenient. A user cannot re-enter an access point during the pre-set anti-passback lockout period regardless of the circumstances.

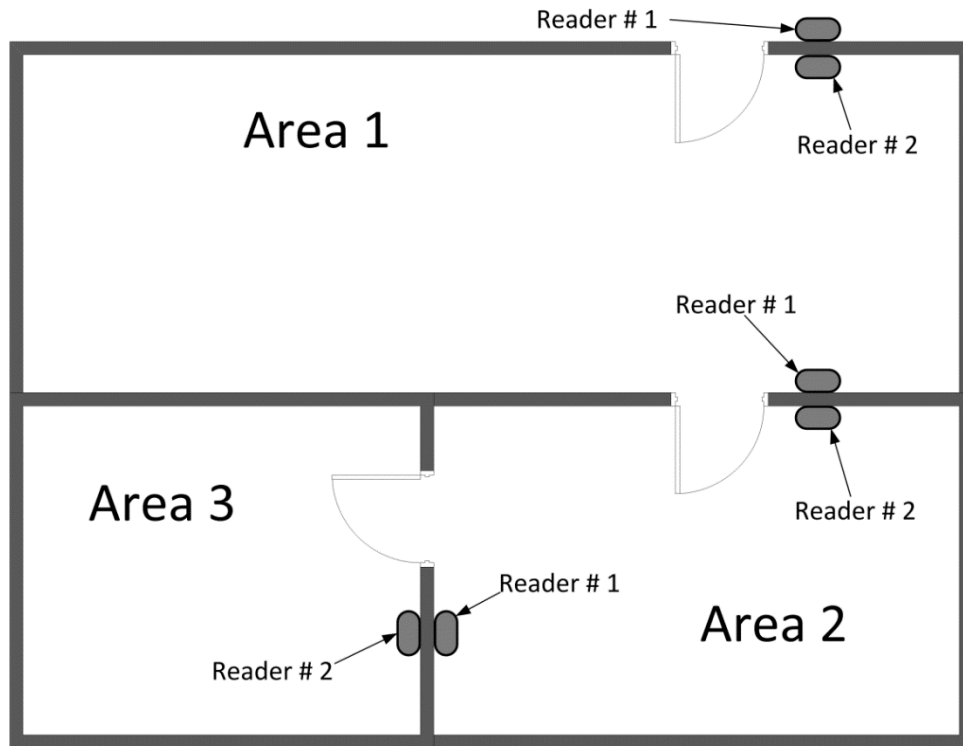
### Configure Logical Anti-Passback

The anti-passback function is configured in three steps.

#### *Step 1 – Define areas for anti-passback.*

Anti-passback logic is applied to an area. You may define up to 250 areas in the aPod II Access Control System and apply anti-passback logic to any area that has at least one entrance with bi-directional access control, i.e., an entrance reader and an exit reader. Adjoining areas and nested areas are permitted.

If there is more than one bi-directional access point to an area under anti-passback control, a User can enter at any point and exit at any point and the aPod II System will accurately track their **IN/OUT** status.



To configure anti-passback, you must first define the area that will be monitored for **IN/OUT** status. Use the [Areas](#) page under the [Setup](#) tab to add and edit areas.

The screenshot shows the 'Areas (add)' configuration page in the aPod II software. The page has a navigation bar with 'Home', 'Users', 'Tools', and 'Setup' (highlighted in yellow). The 'Areas (add)' section contains the following fields:

- AREA NAME:** Machine Shop (highlighted with a red box)
- ANTI-PASSBACK RESET:** None (dropdown menu)
- OCCUPANCY:** Disabled (dropdown menu)
- WARNING:** (empty text field)
- LIMIT:** (empty text field)

A yellow callout box contains the instruction: "Click the 'Add' button, enter an AREA NAME, and then save the record." At the bottom of the page are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'.

By default, every system has one area called 'System' which encompasses the entire facility. The System area cannot be deleted but you can modify the name and APB reset configuration.

For interior doors where there is a monitored area on either side of the door, you must define both areas before you can configure that door for anti-passback.

## Step 2 – Configure the second reader.

The aPod II door controller supports two readers. The primary reader (Reader #1) is assumed to be an **IN** reader or in other words an *access* reader. When a second reader (Reader #2) is connected to the controller at the same door, it should be configured either as an **OUT** reader or in other words an *exit* reader, or as another **IN** reader depending on the door's location.

A second reader on a perimeter door is defined as an **OUT** reader because access through the door is out of an area but not into another area. A second reader on an interior door is defined as an **IN** reader because access through the door is out of one area and into another area.

The second reader on all doors with bi-directional access control is normally configured during the installation and commission of the system. If you need to configure a second reader, use the Hardware tab on the Doors page.

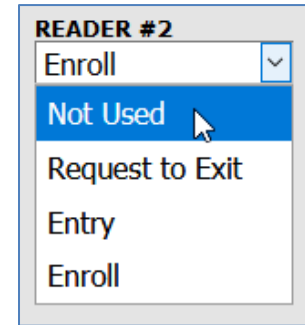
The screenshot shows the 'aPod II' configuration interface. The 'Setup' tab is active, and the 'Hardware' sub-tab is selected for the 'Machine Shop' door. The 'READER #2' dropdown menu is highlighted with a red box and set to 'Entry'. Other configuration options include SERIAL NO. (007332/2), STRIKE (Normal), READER LED (RBG OST), and various input and output settings.

FIELD	VALUE
DOOR NAME	Machine Shop
SERIAL NO.	007332/2
STRIKE	Normal
READER #2	Entry
READER LED	RBG OST
INPUT #1	Request to Exit
CIRCUIT #1	Normally Open
NAME #1	
INPUT #2	Door
CIRCUIT #2	Normally Closed
NAME #2	Door Contact
INPUT #3	Door
CIRCUIT #3	Normally Closed
NAME #3	Shipping Door
INPUT #4	Alarm Conditional
CIRCUIT #4	2K2 EOL N.O.
NAME #4	Tool Crib
OUTPUT #1	Siren
OUTPUT #2	aBus

Use the **READER #2** drop-down list to choose the correct configuration according to its use.

There are three options.

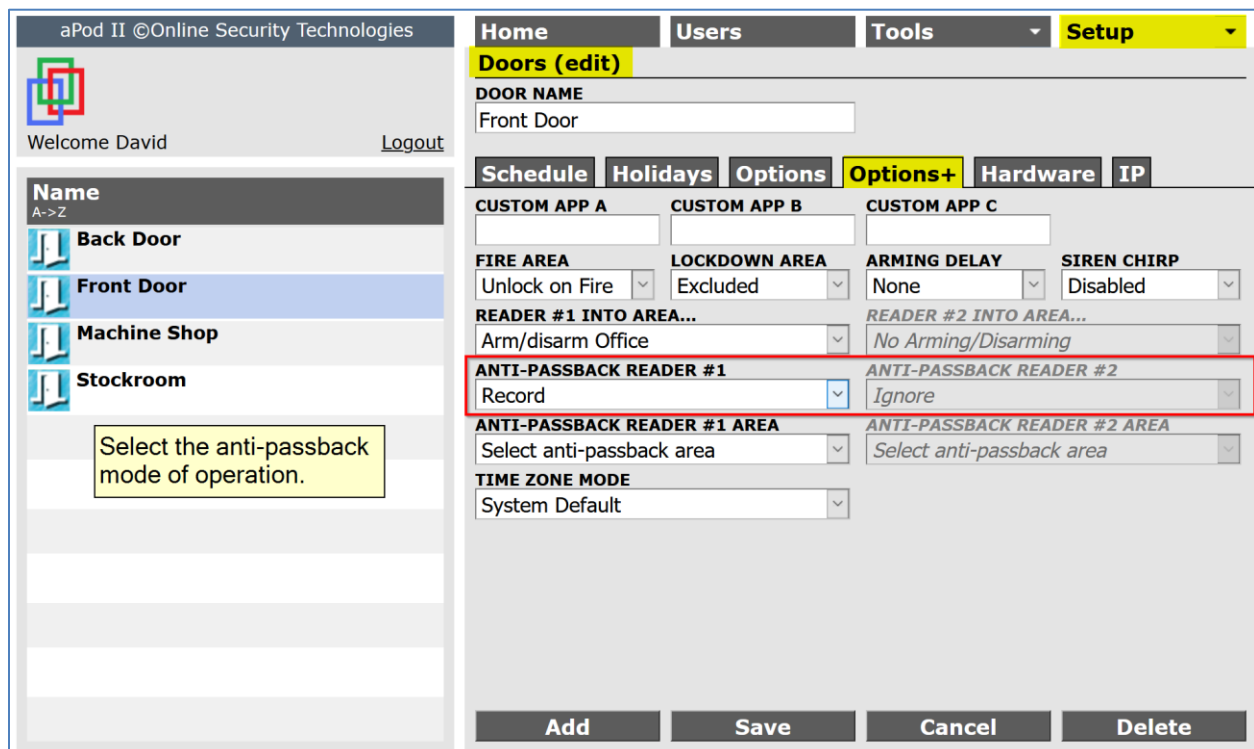
- **Not Used** – A second reader is not used. This is the default mode.
- **Request to Exit** – The door is a perimeter door and exits to the outside of the facility. The second reader is an exit reader and is used to grant an egress. It is recorded in the event log. Any valid card will be granted egress regardless of the schedule.
- **Entry** – The door is an interior door and leads from one area into another area. The second reader is an access reader. A User is granted access in both directions according to their time scheduled access permissions.
- **Enroll** – A second reader which can be desk or counter mounted and used to enroll the tokens for new Users. The door is not unlocked but an event message indicates that the enrollment was successful.



### Step 3 – Select the anti-passback mode of operation.

The anti-passback mode of operation is configured using the Options+ tab on the Doors page.

**ANTI-PASSBACK** functionality is activated if there is at least one door in the system that is configured with two readers (bi-directional access control) as described above.



Configuration options are enabled for Reader #2 if an access point has two readers and Reader #2 is configured for “Entry” mode as described in Step 2.

<b>ANTI-PASSBACK READER #1</b>	<b>ANTI-PASSBACK READER #2</b>
Record	Record
<b>ANTI-PASSBACK READER #1 AREA</b>	<b>ANTI-PASSBACK READER #2 AREA</b>
Entry into Machine Shop	Entry into Office

Use the **ANTI-PASSBACK** drop-down list to choose one of the following modes of operation.

**ANTI-PASSBACK READER #1**

Ignore

Ignore

Track

Record

Enforce

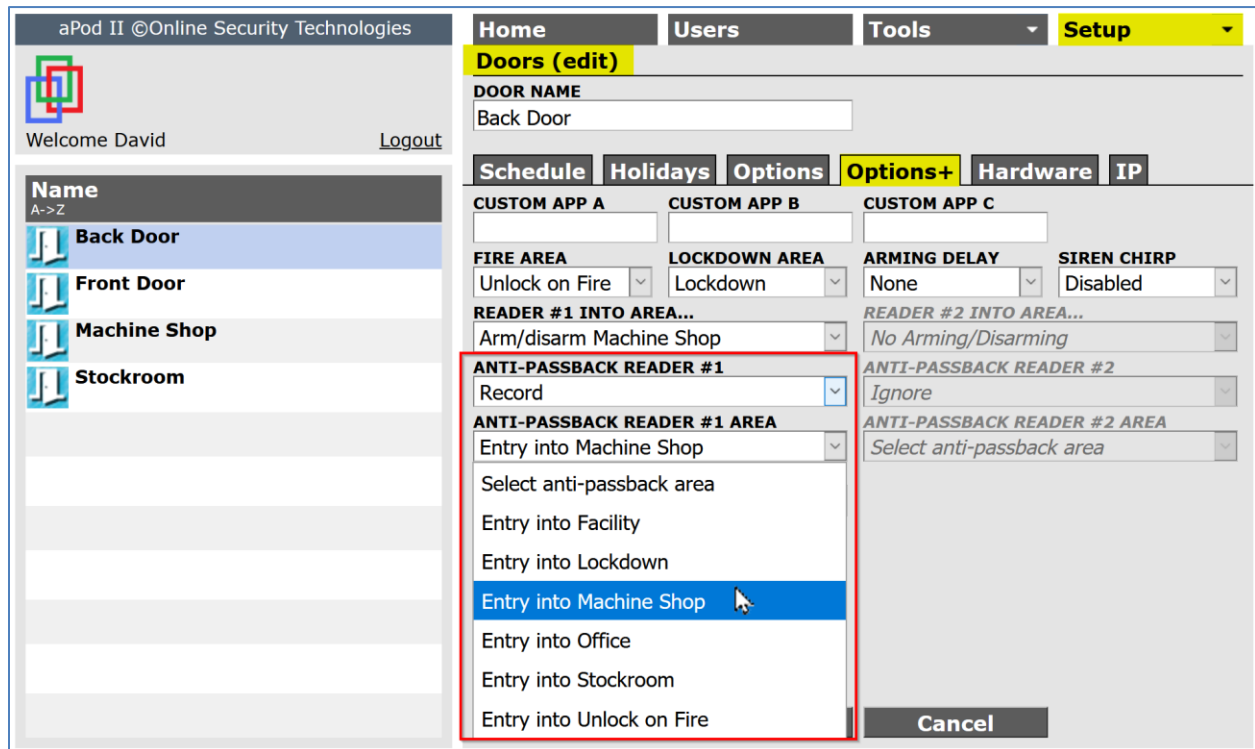
- **Ignore** – The anti-passback logic is disabled. This is the default configuration.
- **Track** – Reserved for future feature development.
- **Record** – If a passback is detected, access will be granted, and an APB warning is recorded in the event log.
- **Enforce** – If a passback is detected, access is denied. The User’s anti-passback lockout period is determined by the configuration of the anti-passback reset function. The APB event is recorded in the event log.

The anti-passback mode of operation must be selected for all access points to a monitored area and the selected mode should be the same for all doors.

#### Step 4 – Assign the access readers to an anti-passback area

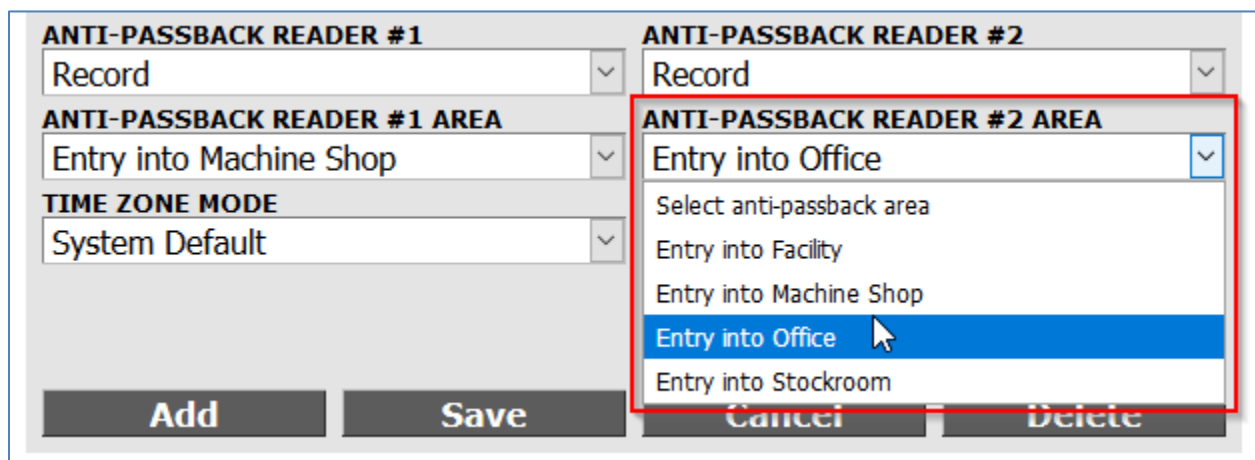
##### Access points on the perimeter of the building

If you select an anti-passback mode other than “Ignore”, the **ANTI-PASSBACK READER #1 AREA** field is enabled. Assign **READER #1** to the area to which it controls access. For a perimeter door, **READER #2** should be configured as a “Request to Exit” device and will not be assigned to an area.



## Access points in the interior of the building

If you select an anti-passback mode other than 'Ignore' and **READER #2** is configured as 'Entry' on the Doors→Hardware page, then both the **ANTI-PASSBACK READER #1 AREA** and **ANTI-PASSBACK READER #2 AREA** fields are enabled. These fields allow you to assign both readers to an access point under anti-passback control according to the area to which they grant access. This is the configuration for an interior door which connects two areas.



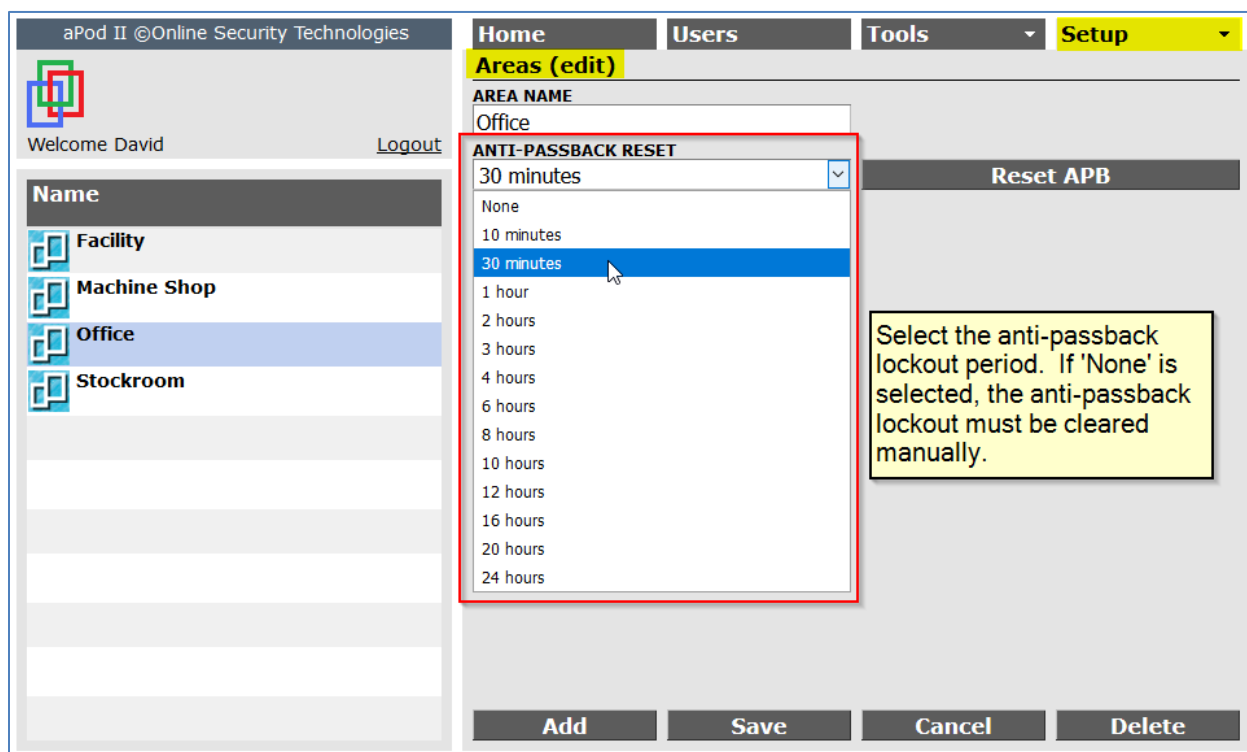
## Reset anti-passback.

Logical anti-passback requires Users to badge in and badge out every time they enter or leave the area under anti-passback control. When they fail to do this, their **IN/OUT** status is not correct. This could trigger an anti-passback lockout the next time they badge their token at the door. Users may forget to badge in or badge out when they follow someone through an already open door or exit through a door by simply turning the handle.

Whether the anti-passback lockout is caused accidentally or otherwise, it is possible to reset the lockout period and allow a User to resume normal use of the access door. Both automatic and manual reset options are available.

### Anti-passback reset by area

You can reset the anti-passback lockout period for all Users for a given area. On the [Areas](#) page, select an anti-passback lockout interval from the **ANTI-PASSBACK RESET** drop-down list. This timer is applied to all Users *individually*.



**Note:** The anti-passback lockout period is the only reset mechanism available for the simple timed anti-passback mode of operation. This mode does not require an exit reader but is generally not recommended because a user is prevented from re-entering an access point for the entire lockout period regardless of the circumstances. Logical anti-passback requires an exit reader.



You can also clear anti-passback lockouts for all users in each area at any time by clicking the button **Reset APB**.

This button is only displayed when anti-passback is enabled at any door.

## Anti-passback reset by user

When anti-passback is enabled, a reset button is displayed on the Users page.

Click the **Reset APB** button to manually reset the APB lockout for a specific User.

The screenshot displays the 'Users (edit)' interface. On the left, a user list includes David Martin, Jane Anderson, Olin Reese, Richard Evans (selected), Sandy Thomas, and Sara Friedman. The main area shows details for Richard Evans: FIRST NAME (Richard), LAST NAME (Evans), and various options like 'Assisted Access', 'Suspended', '3X Lock/Unlock', '3X Arming', 'Silence Alarms', and 'Pending Unlock'. It also shows 'ACCESS CARD' (319455408), 'READER KEYPAD OPTIONS' (None), 'VALID FROM' (Now), 'VALID UNTIL' (Forever), 'USER ID' (4), 'PIN/Managed' (Invalid), 'USER GROUP' (Production), and 'ADDITIONAL USER GROUP' (Unassigned). A 'Reset APB' button is highlighted with a red box and a red arrow. A yellow callout box contains the text: 'Click the 'Reset APB' button to reset the anti-passback lockout for this user.' At the bottom, there are 'Add', 'Save', 'Cancel', and 'Delete' buttons.

## Automatic Door Opener Interface

Some Users may need assistance when entering or exiting through a door that is controlled by the aPod II Access Control System.

Select the 'Assisted Access' option to allow a User an extended unlock time.

The screenshot shows the 'Users (edit)' interface for the aPod II system. The 'Assisted Access' checkbox is highlighted with a red box. A callout box points to this checkbox with the text: "Select this option to allow an extended unlock time and to enable an automatic door opener for this user." The interface includes fields for user name, options, access card, and validity.

Home		Users		Tools		Setup	
<b>Users (edit)</b>							
FIRST NAME Jane				LAST NAME Anderson			
<b>OPTIONS</b>							
<input checked="" type="checkbox"/> Assisted Access							
<input type="checkbox"/> Suspended							
<input type="checkbox"/> 3X Lock/Unlock							
<input type="checkbox"/> 3X Arming							
<input checked="" type="checkbox"/> Silence Alarms							
<input type="checkbox"/> Pending Unlock							
ACCESS CARD 319455406				READER KEYPAD OPTIONS None			
VALID FROM Now				VALID UNTIL Forever			
USER ID 2		PIN/Managed Invalid				Reset APB	
USER GROUP Customer Service				ADDITIONAL USER GROUP Unassigned			
Add		Save		Cancel		Delete	

The default unlock time is 5 seconds and the default extended time is an additional 3 seconds. Both values are configurable. Refer to page 43 for more information.

When the aPod II System is interfaced to an automatic door opener, the opening action will be triggered as described below.

- When the door is locked, a valid card swipe will first unlock the door and then enable the automatic door opener which can then be activated by pressing the 'Request to Enter' button. When exiting, pressing the 'Request to Exit' button will trigger the unlock/activation sequence.
- When the door is unlocked, pressing either the 'Request to Enter' button or the 'Request to Exit' button will activate the automatic door opener.

## Fire Alarm Unlock Operation

Fire and building codes can be complex, but they all have one fundamental requirement pertaining to door locking. In the event of a fire alarm, every door on an exit route from the building must allow easy and unrestricted egress even when power is lost. There are only two exceptions: penal, mental, or correctional facilities with qualifications, and unoccupied buildings.

Unrestricted free egress requires the proper installation of door hardware such as crash bars and paddle latches for easy unlatching, usually without the use of a secondary system or electrical power. Emergency lighting and fire exit signs should direct occupants to the nearest exit.

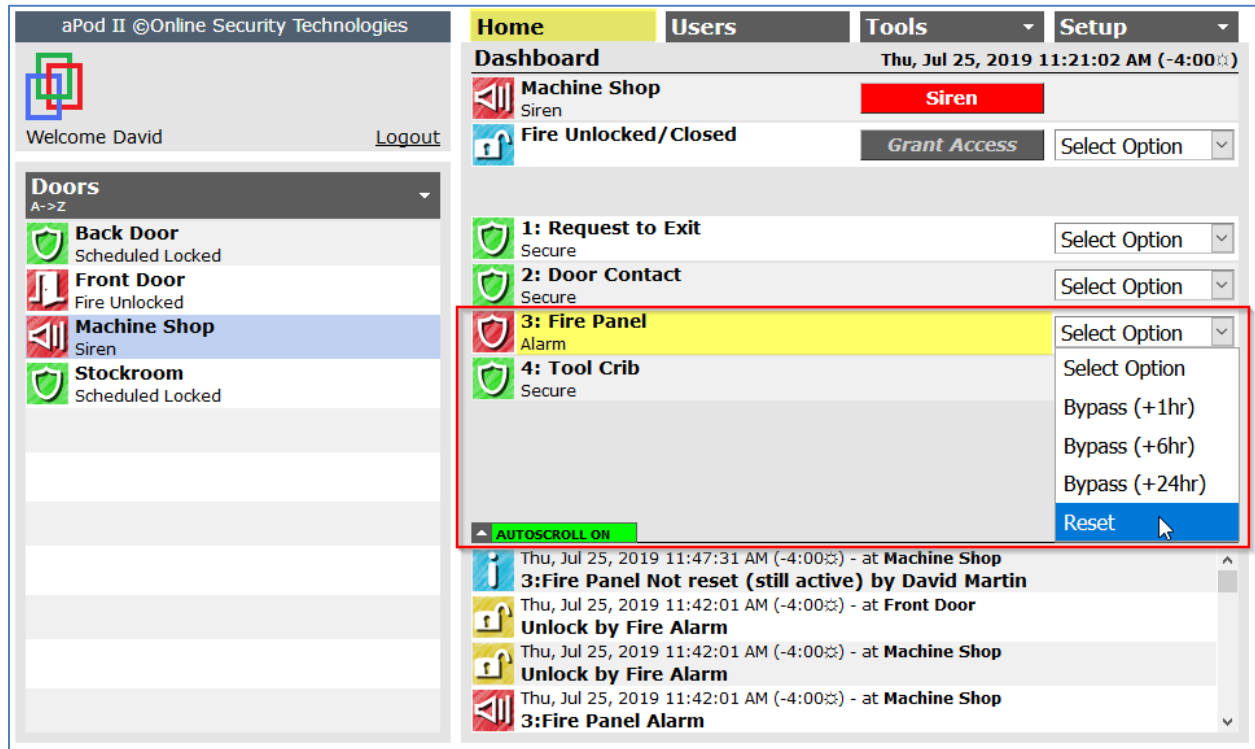
Depending on the layout of the building, some doors may require free *access* for entry, but most can remain locked. For example, in multi-floor buildings, some exits to stairwells must allow access depending on the number of floors and other factors. Bi-directional interior doors, that is, doors with controlled access in both directions, should unlock because egress could be required in either direction.

All perimeter doors can remain locked for access. For larger buildings this may require the installation of an approved Fire Department key box. Unlocking the main entrance for access in a fire emergency would avoid a destructive entry but could possibly compromise security. An intrusion detection system and video cameras would mitigate this risk.

These are guidelines. Your system installer should ensure that the installation of your access control system complies with the building and fire codes in your jurisdiction.

## Cancelled the Fire Alarm

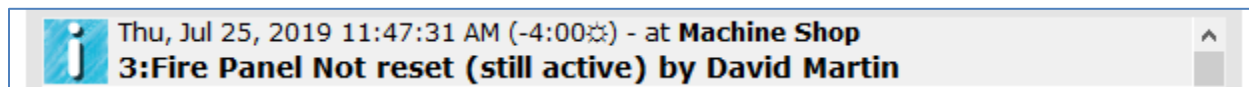
In the example below, the fire alarm input is wired to the aPod II Controller at the Machine Shop door. When the alarm input is triggered, the siren is activated, and all the designated doors are unlocked. The Back Door is a perimeter exit door. In this instance, it remains locked for access but allows free egress.



The doors are re-locked only when the fire alarm has been cancelled and the aPod II System unlock command has been reset. The reset command is located on the drop-down list for the alarm panel input point that triggered the fire alarm.

The manual reset action for the aPod II System ensures that all doors will remain unlocked even if the fire department cancels the fire alarm at the fire panel.

The aPod II System inhibits the fire unlock reset if the fire panel alarm has not been cancelled.



When the system is reset, each door resumes its normal locked/unlocked state according to its locking schedule.



The cancelling of the fire alarm unlock period is managed by the Primary Controller. If for any reason, a Secondary controller is offline, i.e., it cannot communicate with the Primary Controller; it will automatically resume its normal locking schedule in 4 hours. In the interim, any User that has the '3X Lock/Unlock' permission can re-lock the door manually by badging 3X at its reader.

## Lockdown Operation

### Introduction

Institutions like schools, government facilities, hospitals and places of worship are potentially at risk of emergency situations reaching High or even Critical threat levels. When a threat is identified a lockdown may be initiated.

The aPod System provides a lockdown function with the following features.

- Once initiated, a lockdown command will immediately lock every door in the building that is controlled by the aPod System, preventing access into the building and in certain circumstances, egress out of the building.
- During the lockdown, passage through every access point will be denied to every cardholder regardless of their normal access permissions. This restriction can be overridden for key personnel by assigning the “Lockdown Access” user option.
- A lockdown is initiated by an input device such as a panic button or a wireless switch activated by a key fob. No computer login is required. Multiple inputs are allowed which provides a better distribution of trigger points.
- A lockdown will last indefinitely and is manually cancelled by using a specific command in the aPod Browser Interface.
- One or more lockdown outputs can be configured in the aPod System. These can be used to turn-on a lockdown notification device or as an input to another system. A lockdown output remains active for the entire duration of the lockdown.
- The Grant Access command on the aPod Browser Interface [Home](#) page will momentarily unlock a specific access point during the lockout as a means of allowing emergency access.
- All access events from the start to the end of a lockdown are recorded in the event log.

### Implementation

An emergency lockdown can be an effective security measure in large buildings where many people congregate. The implementation of a lockdown operation requires planning to ensure that it provides maximum security while minimizing confusion and panic.

The triggering and lockdown notification mechanisms should be reviewed with your security system installer to ensure that all necessary hardware components are properly installed.

A lockdown protocol should be written and distributed to key personnel to define their responsibilities and actions during a lockdown. As with fire drills, a lockdown should be practised in a test scenario to ensure that the entire process works before it is actually needed.

## Triggering a lockdown

A lockdown is triggered by a physical device like a key switch, panic button or wireless button. No computer login is required. The number, type and placement of triggering devices will determine the balance between easy access and the prevention of false alarms. Every aPod controller supports six inputs and any input can be configured to support a lockdown trigger.

The lockdown input requires a momentary closure of the switch which must be held for at least two seconds. This delay will help to prevent a device like a wireless switch from triggering a false alarm because of an accidental button-push on the key fob. The first detected lockdown input initiates the lockdown and additional lockdown inputs are ignored. When a lockdown request is detected, every controlled door is immediately locked.

The start of a lockdown is recorded in the Event Log and the status of every door is changed to reflect the lockdown status.

The screenshot displays the aPod II security management interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The main dashboard area shows the status of various doors and components:

- Front Door:** Secure, Lockdown/Closed, Siren, Grant Access, Select Option
- Enclosure:** Secure, Select Option
- 1: Lockdown:** Active, Select Option
- 2: Door Contact:** Secure, Select Option
- 3: AS-Office:** Panel Disarmed, Arm Panel, Select Option

On the left, a 'Doors' sidebar lists: Back Door (Lockdown), Front Door (Lockdown), Machine Shop (Lockdown), and Stockroom (Lockdown). At the bottom, an 'EVENTS' log shows a series of 'Lockdown by System' events occurring at 10:37:13 AM on Sun, Jun 2, 2019, at the Stockroom, Back Door, Machine Shop, and Front Door.

## Lockdown notification

The announcement of a lockdown is a critical component of the lockdown protocol and can be handled with sirens, strobe lights or other mechanisms such as an automated public address message.

Trigger devices like panic buttons and wireless switches will not provide feedback that the lockdown has been initiated. The notification mechanism must provide this confirmation.

One or more lockdown outputs can be configured on the aPod System. Two output types are available. Output #1 is a 12 VDC latched output which can be used to turn on an annunciating device like a strobe light. Output #2 is a 5 VDC latched output which can be used as an input to another system, like an intrusion alarm system. The intrusion alarm system would transmit the lockdown alarm to the alarm system monitoring centre.

A lockdown output remains active for the entire duration of the lockdown.

## Lockdown override

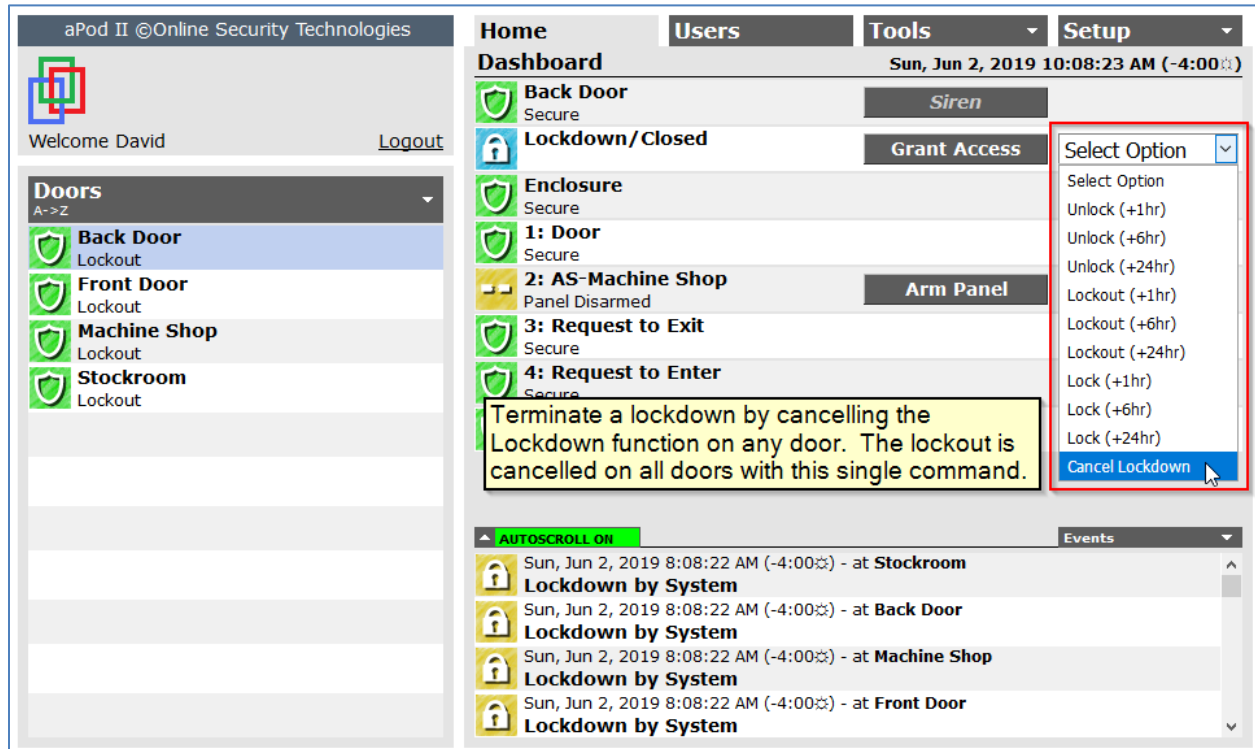
By default, a lockdown will deny passage to every user at every controlled door regardless of their normal access permissions. Key crisis management personnel should have the ability to override this function and pass through critical access points if needed. The override permission can be assigned by selecting the “Lockdown Access” User option.

The screenshot shows the 'aPod II ©Online Security Technologies' interface. On the left, a user list includes David Martin (Administration), Jane Anderson (Customer Service), Olin Reese (Sales, Parking Garage), Richard Evans (Production), Sandy Thomas (Administration), and Sara Friedman (Administration). The main area is the 'Users (edit)' form for David Martin. The form includes fields for 'FIRST NAME' (David) and 'LAST NAME' (Martin). Under 'OPTIONS', the 'Lockdown Access' checkbox is checked and highlighted with a red box. Other options include 'Assisted Access', 'Suspended', '3X Lock/Unlock', '3X Arming', 'Silence Alarms', and 'Pending Unlock'. There are also sections for 'ACCESS CARD' (319455405), 'READER KEYPAD OPTIONS' (Both 2# and 5#), 'VALID FROM' (Now), 'VALID UNTIL' (Forever), 'USER ID' (1), 'PIN/Managed' (Invalid), 'USER GROUP' (Administration), and 'ADDITIONAL USER GROUP' (Unassigned). At the bottom, there are buttons for 'Add', 'Save', 'Cancel', and 'Delete'.



## Lockdown reset

Once the emergency lockdown function has been triggered, it can only be cancelled manually in the aPod Browser Interface by cancelling the lockout function on any door. This single command will cancel the lockdown on all doors.

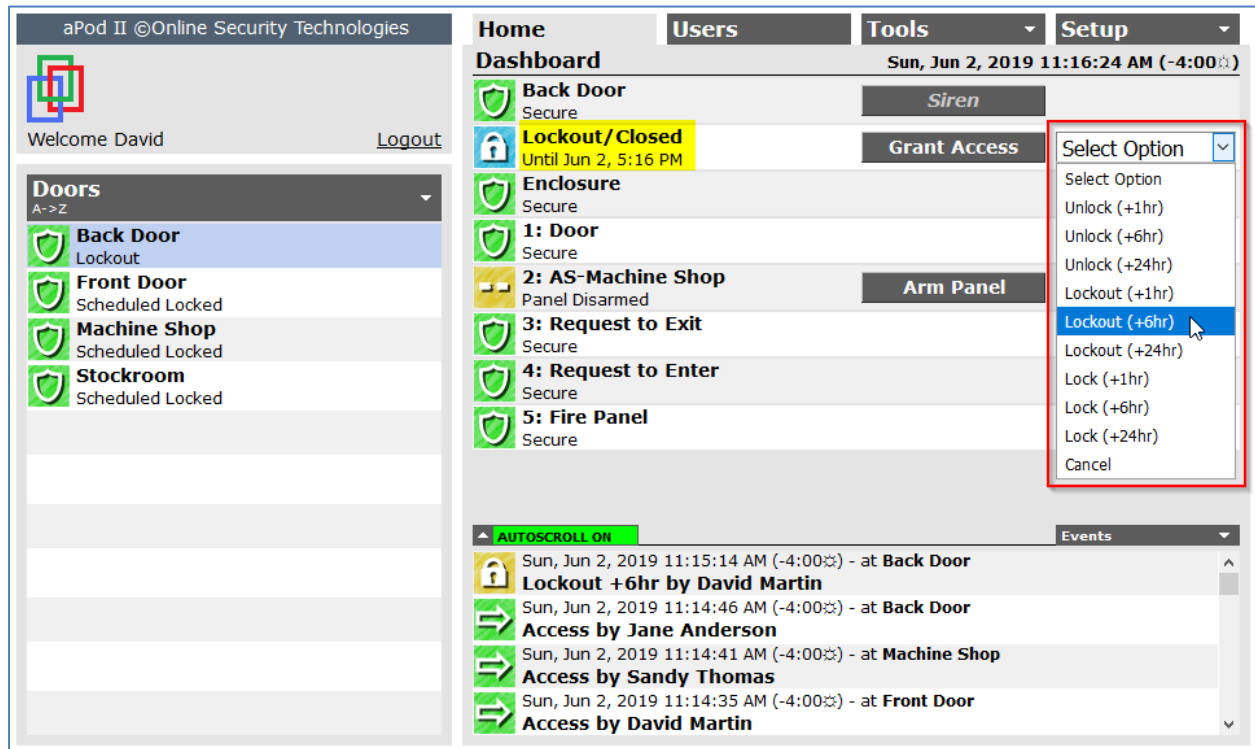


If for any reason, the aPod Browser Interface cannot be accessed, the lockdown can be terminated on a door by door basis by a user with appropriate authority performing a 3X badging function. The user must be assigned both the "Lockout Access" and the "3X Lock/Unlock" user options.

Badging the access reader three times, will put the door into an unlocked state until the end of the current door locking schedule or until the unlock state is cancelled on the Browser Interface with a reset command.

## Lockout vs. Lockdown

A lockout will prevent passage through a *specific* access point for all cardholders regardless of their normal access permissions. It is enabled for a fixed period on a door-by-door basis by selecting a lockout command on the door schedule override list on the Home page.



The lockout period can be extended by repeat selections of any lockout command. For example, Lockout (+24hr) + Lockout (+6hr) → “a lockout for 30 hours”. A lockout can be cancelled at any time by selecting the Cancel command.

*A lockout can be used to temporarily restrict passage through one or more access points but should not be used as an emergency security function.*

A *lockdown* is designed to respond to emergency situations and can immediately restrict passage through all access points, denying access into the building and in certain circumstances, egress from the building.

## Denying egress during a lockdown

Denying egress from the building can only be achieved by installing the appropriate door hardware on exit doors. Typically, electromagnetic locks would be used to prevent egress.

Preventing egress is an inherently unsafe proposition and maglocks are not allowed on exit doors except under certain circumstances. For example, they are allowed on exit doors in hospitals

where an infant abduction could be foiled with a lockdown preventing egress. A fire alarm trigger must automatically cut the power to all maglocks allowing free egress.

Maglocks can only be installed if the installation complies with several safety regulations. Your security system installer must review the building and fire codes in your jurisdiction to ensure that the installation satisfies all bylaws.

## Configure the Lockdown Doors

### Define a Lockdown Area

Areas within the aPod II System are managed on the Areas page under the Setup menu. Create a new area that will define all doors in the facility that will enter the lockout state when a lockdown is triggered. This is a virtual area so the doors can be anywhere in the building.

A lockdown trigger device must be connected to an input point on an aPod II access controller for one of the doors in this area. Select the input point type, 'Lockdown'.

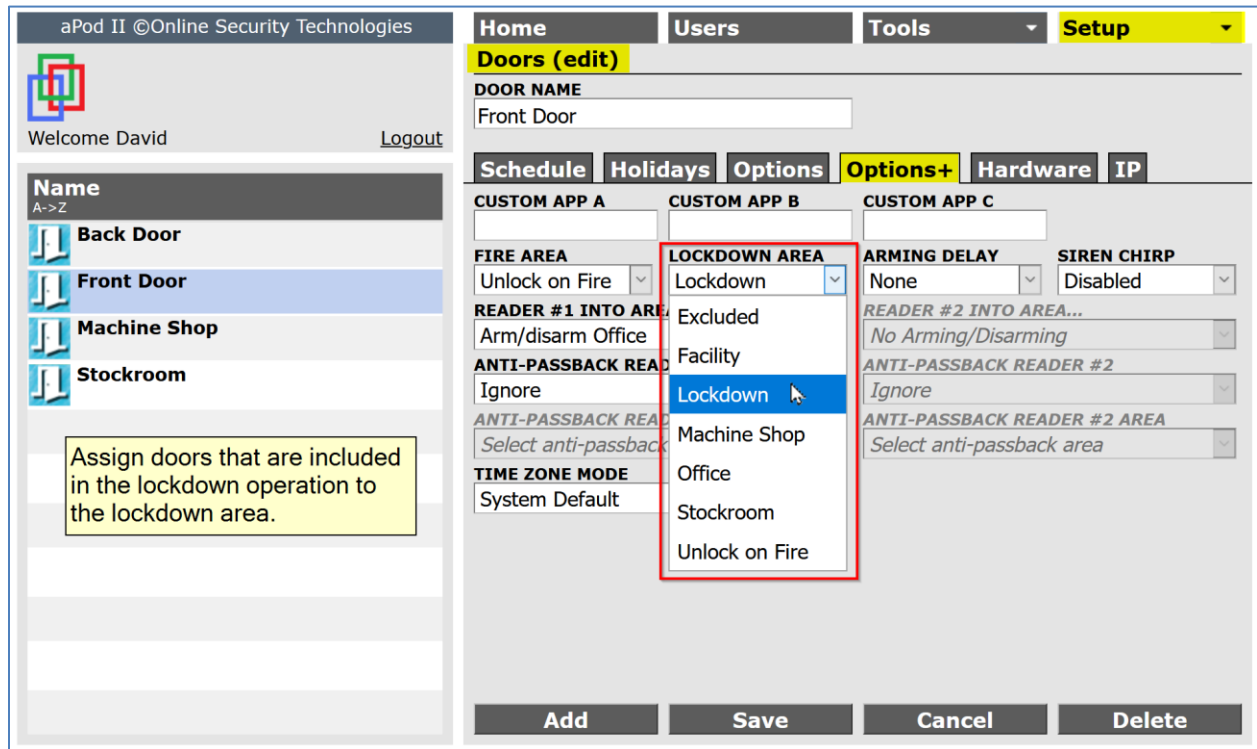
The screenshot shows the 'aPod II ©Online Security Technologies' web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup' (highlighted in yellow). The main content area is titled 'Areas (edit)'. On the left, a sidebar lists various areas: 'Facility', 'Lockdown' (selected), 'Machine Shop', 'Office', 'Stockroom', and 'Unlock on Fire'. The main form contains the following fields:

- AREA NAME:** A text input field containing 'Lockdown', highlighted with a red border.
- ANTI-PASSBACK RESET:** A dropdown menu set to 'None'.
- OCCUPANCY:** A dropdown menu set to 'Disabled'.
- WARNING:** An empty text input field.
- LIMIT:** An empty text input field.

A yellow callout box with a black border contains the text: "Create an area to define all doors in the facility that are included in the lockdown operation." At the bottom of the form are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'.

## Assign Doors to the Lockdown Area

Use the **LOCKDOWN AREA** drop-down list on the Setup→Doors→Options+ page to assign doors to the lockdown operation. The **LOCKDOWN AREA** drop-down list is inactive unless there is a least one 'Lockdown' input configured.



### Important Notes:

1. In a geographically distributed system, each location will have its own unique lockdown area. Repeat the steps described above for each location.
2. A lockdown trigger input must be connected to an aPod controller residing in the area that is segregated for lockdown.

## Occupancy Counter by Area

### Overview

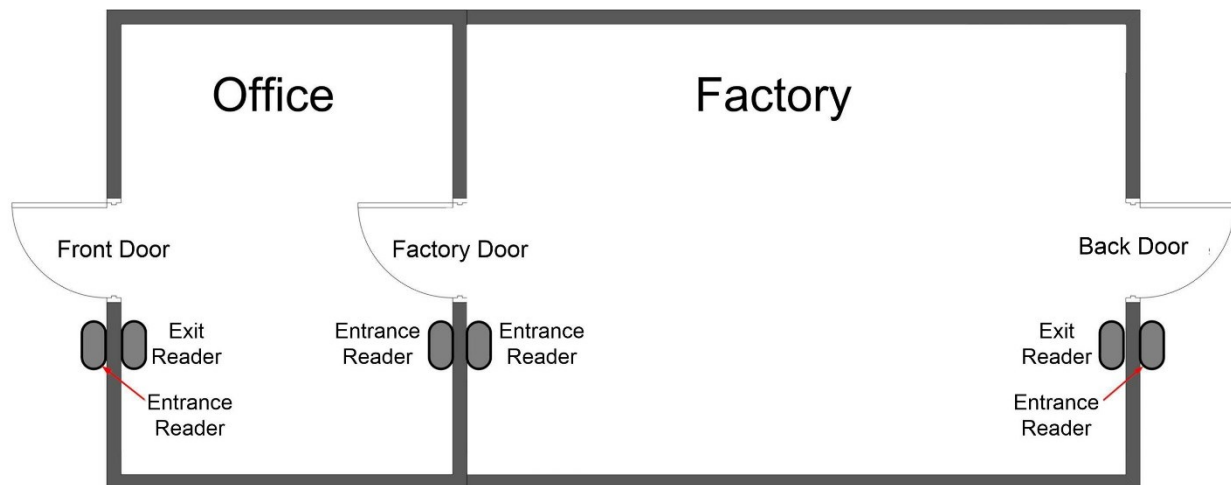
An occupancy counter can be configured for any area within a building that has at least one access point with both an entrance reader and exit reader. This feature can provide a self-governing control of the maximum number of persons allowed in the controlled area.

Users must enter the area by badging their access token which increases the occupancy count. Users must exit the area by badging their access token at the exit reader which decreases the count.

An occupancy warning count and an occupancy maximum count are configured in the aPod Access System. When the occupancy warning count is reached, an alternating output (one second on, one second off) is triggered but access is still granted. When the occupancy maximum count is reached, the output remains on and further access is denied. The output can be used to power an indicator light to provide feedback of the occupancy count status to users who wish to enter the area.

### Multiple access points

The occupancy counter function should be configured for every active access point on an area to ensure an accurate count. This requires an entrance reader and an exit reader at each active access point. The aPod Access System will maintain the in/out status of every user regardless of where they enter or exit the area. In the example shown below, an occupancy count can be maintained for both the "Office" and the "Factory" areas.



## Tailgating

Tailgating occurs when someone follows another person through the open door without badging their card. This usually occurs because employees are not aware of the reason for badging their access token even though the door is momentarily unlocked. Tailgating reduces the accuracy of the occupancy count.

Tailgating can be reduced by posting a notice to inform employees that only one person can enter or exit at a time, and everyone is required to badge in and badge out.

## Free egress

Building and fire codes require that all exits from a building allow free egress to allow for safe evacuation in the event of an emergency. It is possible for an employee to exit a controlled area by unlatching the door manually without badging the exit reader.

This problem can be reduced by activating the buzzer on both readers if the door is opened without badging the exit reader. This is accomplished with two configurations.

1. Install a door contact and configure its input point on the Setup→Doors→Hardware page as “Door”.

The screenshot shows the 'Doors (edit)' configuration page in the Online Security Technologies web interface. The page is titled 'aPod II ©Online Security Technologies' and includes a navigation menu with 'Home', 'Users', 'Tools', and 'Setup'. The 'Setup' menu is expanded, showing 'Doors (edit)'. The 'Doors (edit)' page has a sidebar with a list of doors: 'Back Door', 'Factory Door', and 'Front Door'. The 'Back Door' is selected. The main content area shows the configuration for the 'Back Door'. The 'Hardware' tab is selected, and the 'INPUT #4' dropdown is set to 'Door', which is highlighted with a red box. Other configuration options include 'SERIAL NO.', 'STRIKE', 'READER #2', 'READER LED', 'INPUT #1', 'INPUT #2', 'INPUT #3', 'INPUT #5', 'INPUT #6', 'OUTPUT #1', and 'OUTPUT #2'. The 'OUTPUT #2' is set to 'aBus'. The page includes 'Add', 'Save', and 'Cancel' buttons at the bottom.

2. Set the **DOOR FORCED PROCESSING** field on the Setup→Doors→Options page to “Alarm”.

The screenshot shows the 'Doors (edit)' configuration page. The 'Options' tab is active. The 'DOOR FORCED PROCESSING' field is highlighted with a red box and set to 'Alarm'. Other visible fields include:

- DOOR NAME: Back Door
- ALARM DURATION: 1 minute
- UNLOCK DURATION: 2 seconds
- EXTENDED UNLOCK: +3 seconds
- DOOR OPEN CHIMES: Disabled
- DOOR HELD OPEN PROCESSING: None
- SCHEDULED UNLOCK: Pending next Entry
- CARD+PIN MODE: Never Required
- ID+PIN MODE: Never Allowed
- DUAL CUSTODY MODE: Never Required

## Occupancy count display

The occupancy count for each monitored area is displayed on the Setup→Areas page and is dynamically updated with each access event.

The screenshot shows the 'Areas (edit)' configuration page. The 'Factory' area is selected. The 'COUNT' field is highlighted with a red box and set to 25. Other visible fields include:

- AREA NAME: Factory
- ANTI-PASSBACK RESET: None
- OCCUPANCY: Enabled
- WARNING: 35
- LIMIT: 40
- COUNT: 25

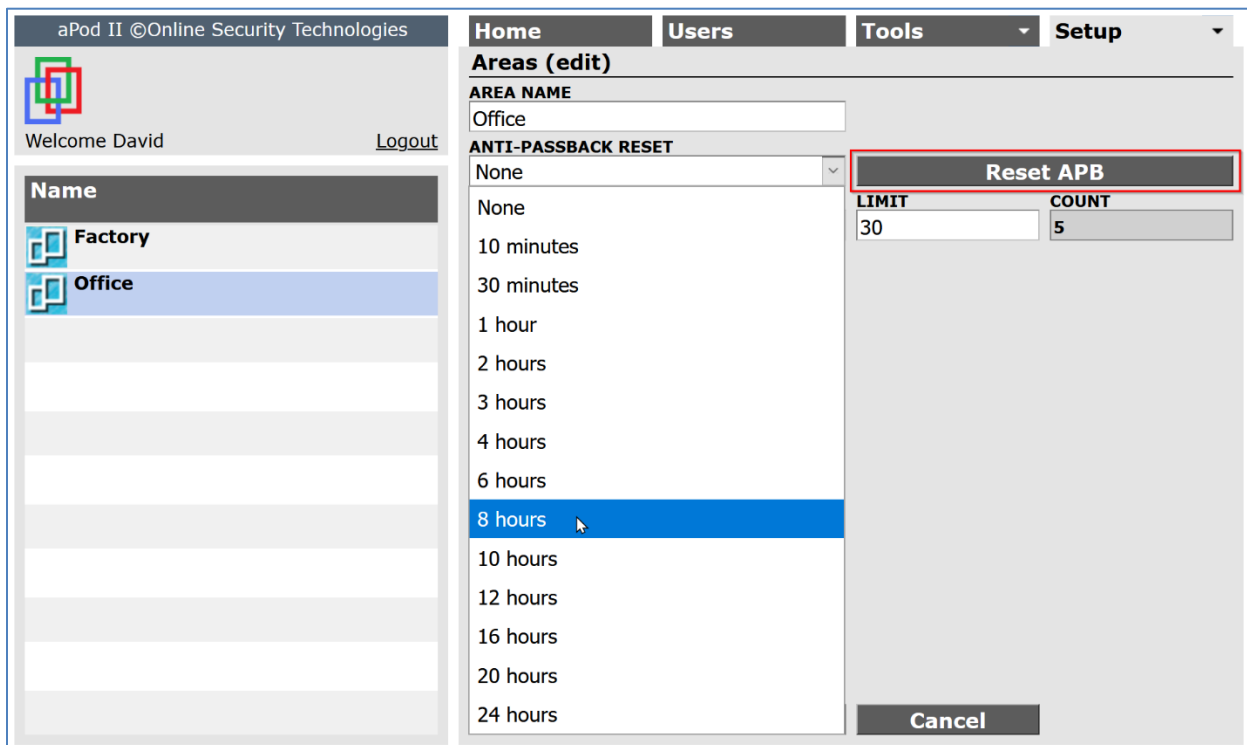
## Occupancy count reset

The anti-passback reset function is used to reset the occupancy count.

The RESET ANTI-PASSBACK drop down list is used to set the time interval after which, a user's in/out status is automatically set to "out". For example, if a user enters the monitored area but leaves without badging out, they will be automatically designated as "out" and will be subtracted from the occupancy count after the configured time interval. This is an override function only, as their status will be dynamically adjusted with a proper exit event.

Selecting the proper interval for the automatic reset of each user's in/out status, will provide a measure of auto-correction for the problem of free egress without badging.

Clicking the Reset APB button will set the occupancy count to zero.





## Software configurations

The Occupancy Counter feature is configured using the following steps.

1. On the Setup→Areas page, define the area that will be monitored and enable the occupancy counter. The aPod System has a default area called “System” which cannot be deleted. It can be renamed. Add additional areas if needed. Enter the warning and maximum values for the occupancy counter and save the record.

aPod II ©Online Security Technologies

Welcome David [Logout](#)

Home Users Tools Setup

**Areas (edit)**

AREA NAME  
System

ANTI-PASSBACK RESET  
None

OCCUPANCY **WARNING** **LIMIT**

Disabled  
Disabled  
**Enabled**

Add Save Cancel

aPod II ©Online Security Technologies

Welcome David [Logout](#)

Home Users Tools Setup

**Areas (edit)**

AREA NAME  
Factory

ANTI-PASSBACK RESET  
None

OCCUPANCY **WARNING** **LIMIT** **Reset APB** **COUNT**

Enabled 45 50 0

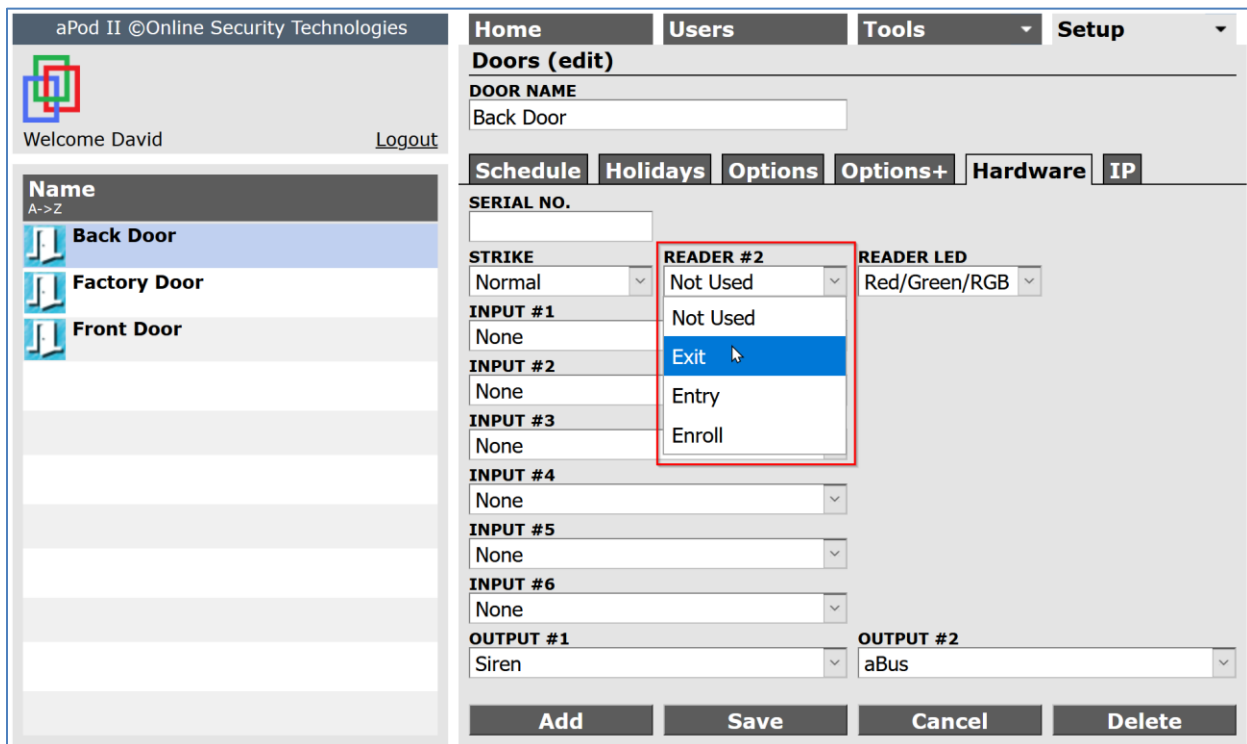
2. On the Setup→Doors→Hardware page, define the function of Reader #2

For each access point, Reader #1 and Reader #2 are determined by their connections to the aPod II controller. Please refer to the wiring diagram on page 5.

Reader #1 is always installed as an “enter” reader.

Reader #2 can be an “exit” reader, if installed on the exterior perimeter of the building or it can be an “enter” reader, if installed on an interior door and it grants access to an adjacent monitored area. When Reader #2 is installed as an “enter” reader, badging either reader at the door, will increase the count of the entered area and reduce the count of the exited area.

Define the function of Reader #2 and save the record.

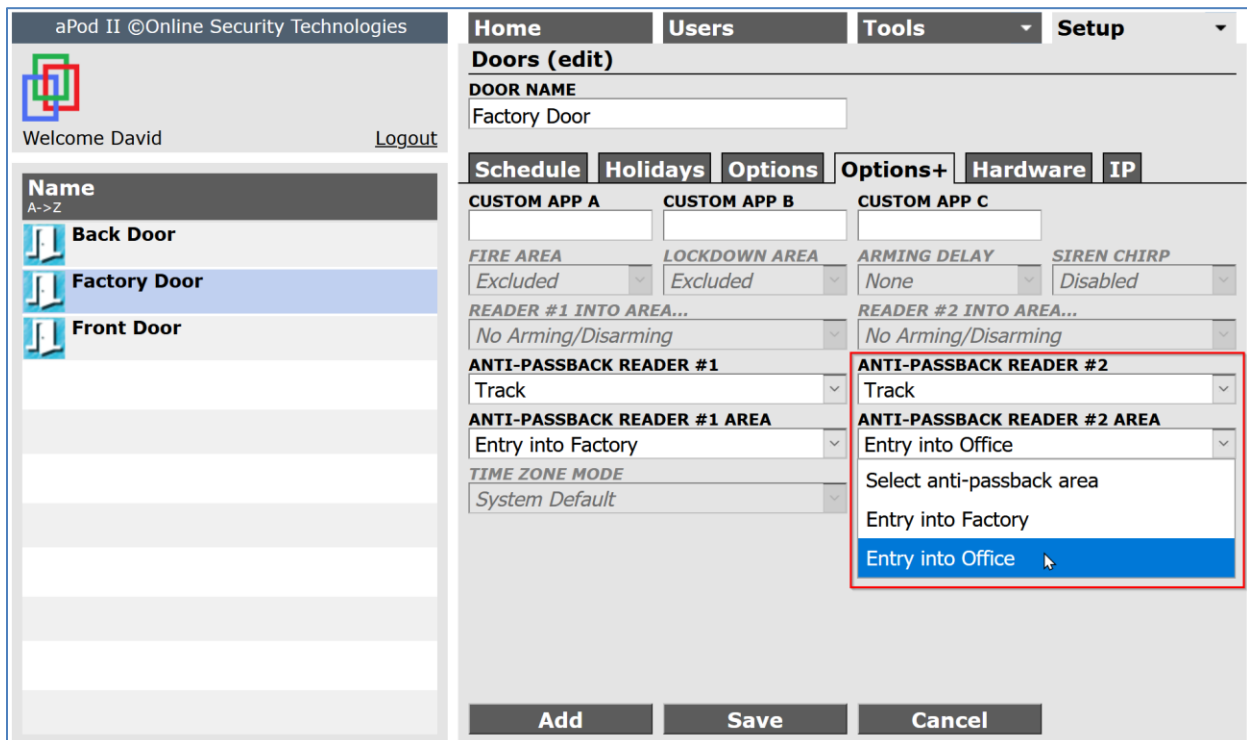


3. On the Setup→Doors→Options+ page, enable anti-passback tracking and then assign each reader to its associated area

Anti-passback logic is used to track the location of each user, which in turn, determines the occupancy count in each area. The anti-passback logic can be enabled by selecting the anti-passback mode “Track”.

Next assign each “enter” reader to the area that is accessed and save the record.

Reader #1 is always configured. Reader #2 is only configured if it is an “enter” reader.



4. On the Setup→Doors→Hardware page, assign the output function to enable the occupancy warning indicator light.

Output #1 and Output #2 can be used interchangeably provided the warning indicator light is mounted near the “enter” reader of the corresponding area.

Assign the outputs and save the record.

The screenshot displays the 'Doors (edit)' configuration page in the Online Security Technologies web interface. The page is divided into several sections:

- Header:** 'aPod II ©Online Security Technologies' with navigation tabs for 'Home', 'Users', 'Tools', and 'Setup'.
- Left Sidebar:** A list of doors: 'Back Door', 'Factory Door' (selected), and 'Front Door'.
- Main Content Area:**
  - Doors (edit):** 'DOOR NAME' is 'Factory Door'.
  - Hardware Tab:** Contains fields for 'SERIAL NO.' (728003), 'READER #2' (Entry), and 'READER LED' (Red/Green/RGB).
  - INPUT #1-4:** All set to 'None'.
  - OUTPUT #1:** A dropdown menu is open, showing options: 'Occupancy Status Factory', 'Siren', 'Panel Arm/Disarm', 'Custom Output #2', 'Door Opener', 'Lockdown', 'Occupancy Status Factory' (highlighted), and 'Occupancy Status Office'.
  - OUTPUT #2:** Set to 'Occupancy Status Office'.
  - Buttons:** A 'Cancel' button is visible at the bottom right.

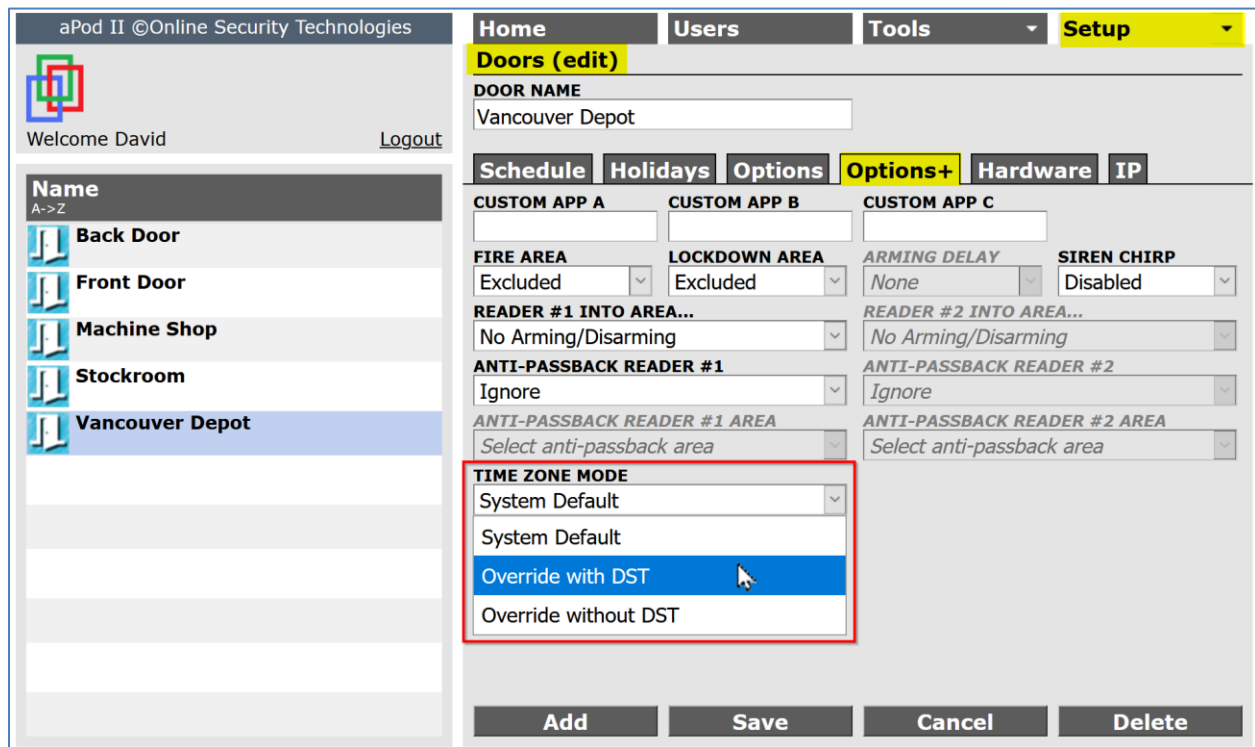
5. Repeat steps 2 to 4 for every active access point on the monitored area.

## Time Zone Mode

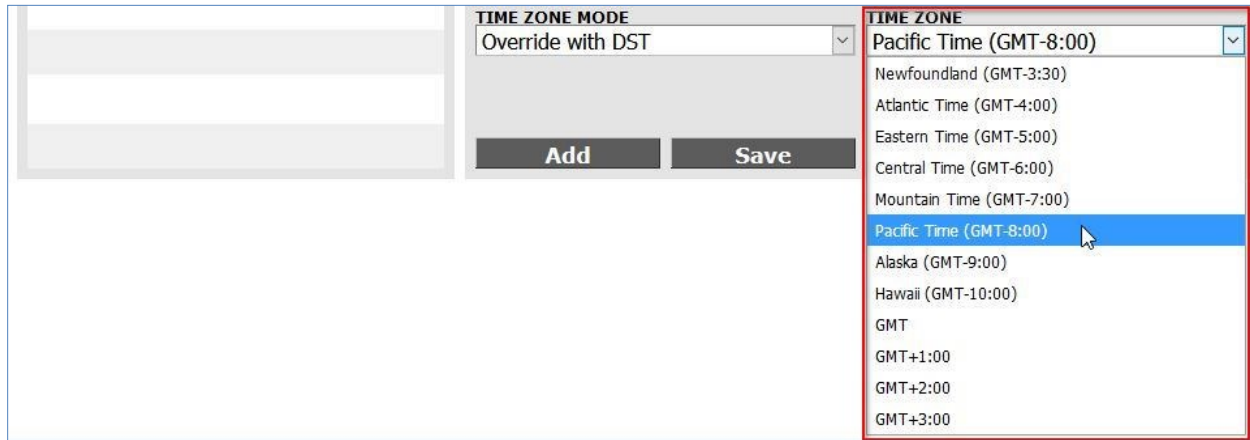
The correct time zone is automatically set for the system when the **LOCALE** is selected for the Primary Controller at the time of the system commissioning. The use of Daylight Savings Time is automatically enabled or disabled according to the jurisdiction. These default values can be overwritten, if necessary, on the System page under the Setup menu.

The time zone for Secondary controllers by default matches the time zone of the Primary Controller.

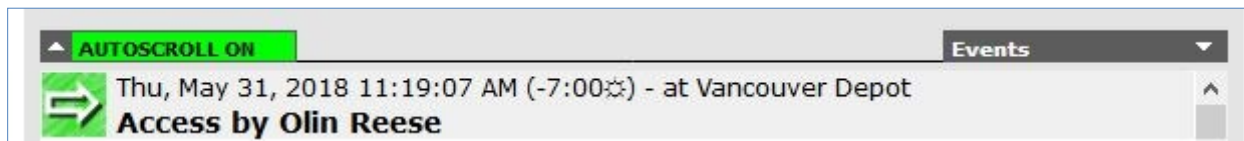
However, if the Secondary controller is remotely located and in a different time zone, its **TIME ZONE MODE** must be edited to record activity in local time. Access the Options+ page for the Secondary controller and change the **TIME ZONE MODE** from “System Default” to either “Override with DST” or “Override without DST”.



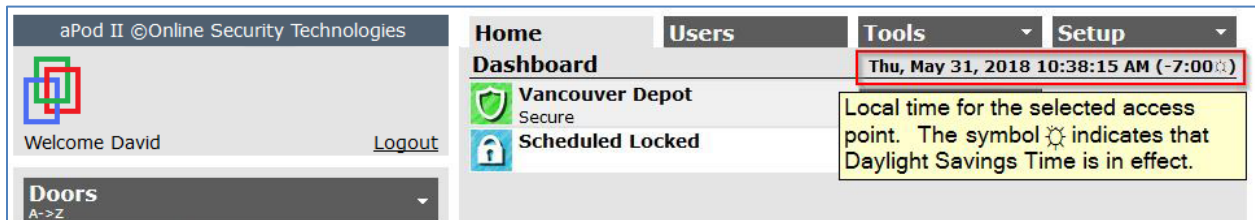
A drop-down list is displayed. Select the correct time zone for the remote Secondary.



For a widely distributed system where access points span different time zones, the access point local time is recorded in the event log. The offset to GMT corrected for DST, if applicable, is also indicated in brackets following the time stamp. The symbol “☀” indicates that Daylight Savings Time is in effect.



On the Home page, the local time is displayed in the page header according to the selected record.



## Custom Apps

**Note:** There are no administrative tasks associated with this page.

Custom applications in the aPod II system provide non-standard functionality and are only enabled by entering a specific app code in the correct location. App codes entered on the Setup→System page affect all access points in the system. App codes entered on the Setup→Doors→Options+ page for any door only affect the operation of that specific door.

A custom application can address a specific security requirement that is not available as a standard feature. For example, an email alert can be sent to specific system administrators every time a specific access point is unlocked.

If you have a special security requirement that is not addressed by your aPod II System, then you can request a quote for a custom application. Ask your security dealer to obtain the quote from Online Security Technologies.

The screenshot displays the 'aPod II ©Online Security Technologies' web interface. The top navigation bar includes 'Home', 'Users', 'Tools', and 'Setup'. The 'Setup' menu is expanded to show 'Apps (edit)'. The main content area is a form for editing an application. It has three sections: 'APP NAME' with the value 'Camera URL Info', 'APP CODE' with the value 'LVF0', and 'INFO' with the value 'axis-cgi/mjpg/video.cgi'. On the left, a sidebar shows a list of applications: 'Camera URL Info' (LVF0) and 'Pop up warning' (TXT1). At the bottom of the form, there are four buttons: 'Add', 'Save', 'Cancel', and 'Delete'.



## Appendix 1 – Specifications

Doors	Up to 100 doors with hypertext search.
Multi-site	Manage doors over multiple sites as a single connected system.
Users (Card holders)	10,000 with hypertext search.
User Groups	250
User Import Utility	Upload cardholders, ID's, and User Groups.
Administrators	250 with 5 levels of authority
Areas	250
Event log	100,000 events
Alarm log	2,000 alarms
Bad card log	2,000 bad card reads
Administrators audit log	10,000 edits
Software requirements	100% browser based. Embedded software. No external software is required.
Browser support	Edge, Firefox, Chrome, and Safari. Local or remote connection. Up to 10 simultaneous connections.
Remote Login	Manage your system from anywhere there is Internet access.
Security alerts	Scheduled alerts by email. Can be configured by administrator.



Software updates	Remote updating of software via the Internet. No fee for updates. Fail safe process.
Language support	Support for English or French, selectable by administrator or automatically matched to operating system language.
Communications	Plug and play network installation. Support for 100 MBaud communications.
Encryption	AES 128-bit encryption, SHA key management.
Reader support	1. Any reader with a Wiegand interface, 25 customizable reader formats, 200-bit capacity, ID bits - 16 to 128, 4 site codes per format. Auto configured on first card read. 2. Any ISO 7811 compliant magstripe reader with Clock and Data (TTL) output, Track 1 or Track 2.
Second reader support	Two readers per controller. Enter/exit readers for perimeter doors, Enter/enter readers for interior doors.
Access modes	Token, token plus PIN, PIN only and Dual Custody modes. Can be scheduled. Temporary card functionality.
Emergency locking	Support for lockdown and lockout operations.
Occupancy Counting	Track occupancy by area with warning and maximum notification outputs.
Access authorization methods	Three methods to match system requirements. By Door, Door by Schedule and By User Groups.
Anti-passback	Logical anti-passback by area, four modes plus timed anti-passback by area.

Unlock options	Configurable unlock time and extended unlock time for assisted access.
Unlock schedule options	Unlock pending, unlock pending by designated User, immediate unlock and unlock on schedule when cardholder is present.
Interlock	Support for Mantrap logic.
Door schedules	Single view, graphical door scheduling – 7 intervals per day with 3 levels of access permission plus unlocked.
User Group schedules	250 User Group schedules (1 per User Group). User Group schedules accommodate complex work schedules.
Holiday schedules	Perpetual, automatic holiday scheduling and Daylight Savings Time pre-configured by location. 250 holidays maximum.
Variable schedules	User-controlled unlock schedules for authorized Users. A triple swipe toggles a door between the locked and unlocked states.
Inputs	Up to 6 inputs per controller, normally open or normally closed, support for supervised high security circuits. Eleven standard input types, four custom input types.
Outputs	Strike (12 VDC up to 500 mA) and siren (12 VDC up to 250 mA). Customizable outputs for alarm system interface and door opener interface.
Fire alarm interface	One fire alarm output to any input on any system controller unlocks all controlled doors in the facility.

Alarm panel interface	Authorized Users can arm/disarm multiple partitions with their card access token. Audio and visual feedback. Arm and disarm at any access point. Remote arming and disarming with Remote Login option.
Automatic door opener interface	Activated for designated Users.
Reports	Filtered reports in HTML and TSV formats.
Backup and restore	Secure backups to any accessible storage media. Periodic backup reminders.
Power requirements	Power over Ethernet, 802.3af compliant – 13 watts
Door controller operating temperature	For indoor use (0°C to 40°C or 32°F to 105°F)

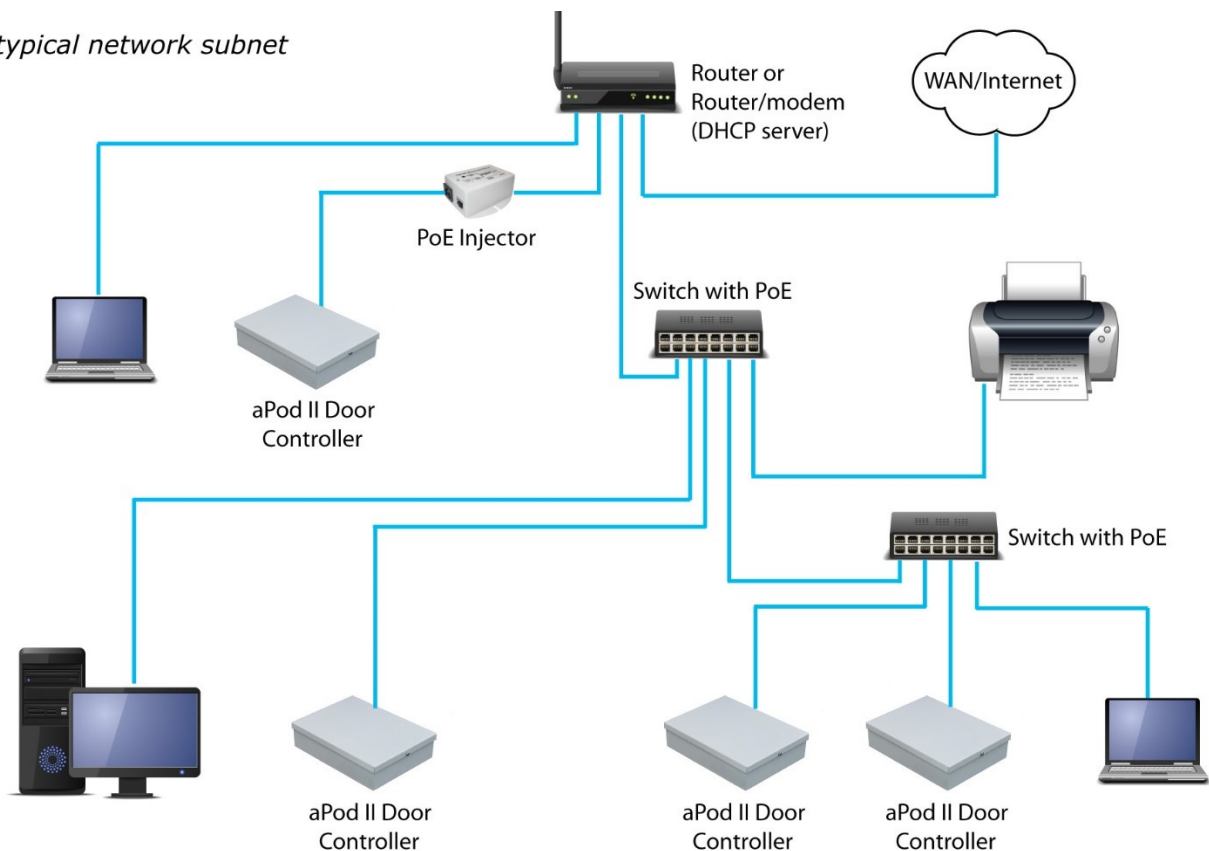


## Appendix 2 - The aPod II System Network Topology

The term network topology refers to the physical layout of the network and how network devices are connected.

### A LAN Distributed System

*A typical network subnet*



On a typical small to medium-size network, all the devices are controlled by a single router and share the same subnet. The router has a DHCP (*dynamic host configuration protocol*) server which manages the IP addresses of the subnet. It also acts as a gateway directing network traffic between its subnet devices and an Internet modem and possibly one or more routers controlling other subnets on a larger network. For most small to medium enterprises which occupy a single geographical location, the entire network consists of a single subnet and the router and internet modem may be combined in a single device.

When aPod II controllers are installed on a single subnet, they are automatically configured to communicate properly with each other, and any PC connected to the subnet. No network configuration is required.

For large facilities with extensive networks, the aPod II controllers may be connected to different subnets and DHCP servers may be disabled. In this situation, the IT or network administrator may configure a VLAN (*virtual local area network*) for the aPod II system. Network management software translates the various physical connections into a logical subnet. When aPod II controllers are installed on a single VLAN, they are automatically configured to communicate properly with each other, and any PC connected to the VLAN.

Any PC not connected to the physical or logical subnet of the aPod II Primary Controller can still communicate with the system by using the Primary Controller's fixed IP address. This can be bookmarked for easy access.

When Remote Login is configured in the aPod II Primary Controller, any device connected to the Internet can communicate with the system from virtually anywhere there is Internet access. Communications are protected with 128-bit encryption and access is restricted by a secure login process.

## **A Multi-Site Distributed System**

The aPod II System can be distributed over multiple locations. At each location, the aPod II controllers reside on the Local Area Network and all remote controllers communicate with the Primary Controller over the Internet or if available, a wide area private network.

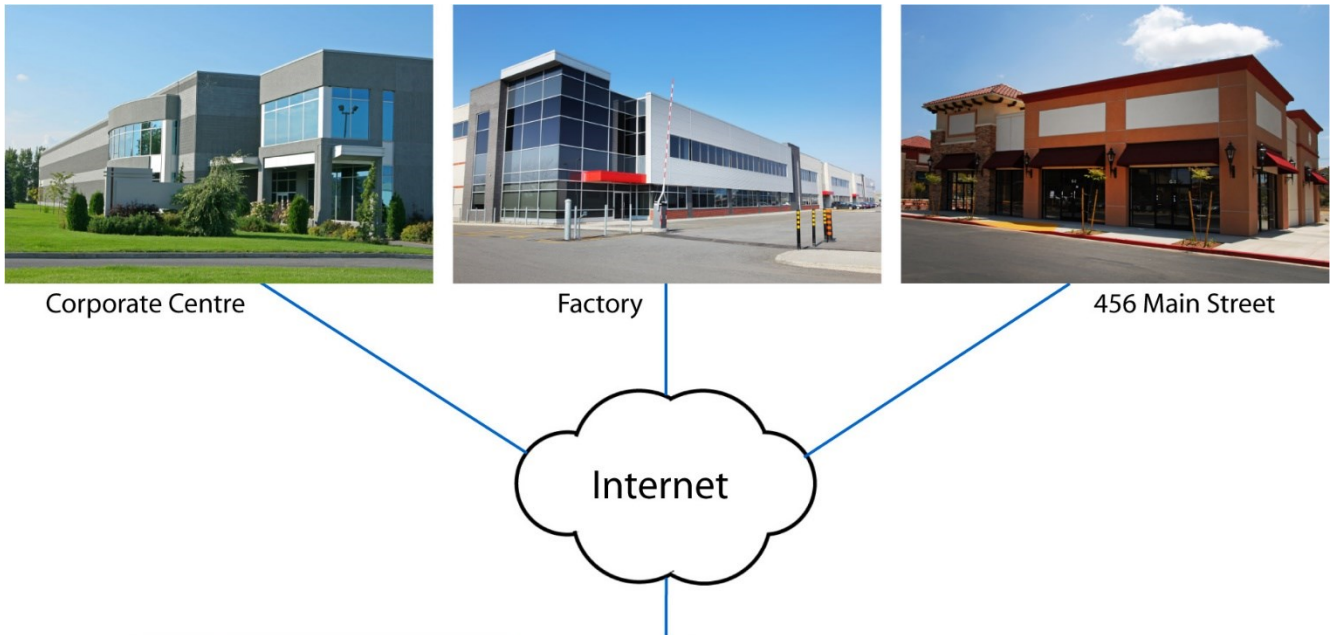
There is no restriction on the number of locations or the number of controllers at each location if the total number of controllers does not exceed the system limit of one hundred.

All communications are automatically maintained and encrypted.

All the doors in a multi-site system are managed with a single browser interface which can be accessed from anywhere there is Internet access.

The aPod II System can be expanded one door at a time at any location and each new door is automatically integrated into the system.

Communication between the Primary Controller and all Secondary controllers is necessary to distribute database changes and to report events. Otherwise, the Secondary controllers operate independently.



aPod II ©Online Security Technologies

Welcome David [Logout](#)

**Home** | **Users** | **Tools** | **Setup**

**Dashboard** Sat, Feb 9, 2019 3:41:41 PM (-5:00)

	<b>Front Door - 456 Main Street</b> Secure	<b>Siren</b>
	<b>Pending Unlock/Closed</b>	<b>Grant Access</b>   Select Option
	<b>Enclosure</b> Secure	Select Option
	<b>1: Request to Exit</b> Secure	Select Option
	<b>2: Door Contact</b> Secure	Select Option
	<b>3: Remote Unlock</b> Secure	Select Option

**Doors**  
A->Z

- Employee Entrance - Factory**  
Scheduled Locked
- Front Door - 456 Main Street**  
Pending Unlock
- Front Door - Corporate Centre**  
Scheduled Locked

**Events** (AUTOScroll ON)

- Sat, Feb 9, 2019 3:41:04 PM (-5:00) - at **Front Door - Corporate Centre**  
**Access by David Martin**
- Sat, Feb 9, 2019 3:40:56 PM (-5:00) - at **Employee Entrance - Factory**  
**Access by Olin Reese**
- Sat, Feb 9, 2019 3:40:48 PM (-5:00) - at **Front Door - 456 Main Street**  
**Access by Jane Anderson**
- Sat, Feb 9, 2019 3:40:38 PM (-5:00) - at **Front Door - Corporate Centre**  
**Access by Sandy Thomas**