3xLOGIC

ACCESS CONTROL | infinias

infinias User Guide

Version 6.7

2/13/2020

This manual applies to the following products.

Product	Version
infinias ESSENTIALS	6.7
infinias PROFESSIONAL	6.7
infinias CORPORATE	6.7

Thank you for purchasing our product. If there are any questions or requests, please do not hesitate to contact the dealer.

This manual may contain technical inaccuracies or printing errors. The content is subject to change without notice. The manual will be amended if there are any hardware updates or changes

Disclaimer Statement

“Underwriters Laboratories Inc (“UL”) has not tested the performance or reliability of the security or signaling aspects of this product. UL has only tested for fire, shock, or casualty hazards as outlined in UL’s Standard(s) for Safety, UL60950-1. UL Certification does not cover the performance or reliability of the security or signaling aspects of this product. UL MAKES NO REPRESENTATIONS, WARRANTIES, OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILIYT OF ANY SECURITY OR SIGNALING RELATED FUNCTIONS OF THIS PRODUCT.”

Table of Contents

1 Software Comparison

The infinias software is consistent across all versions (CLOUD, Essentials, Pro, and Corp). Therefore, navigation, terminology and concepts are all similar. A few key differences are that CLOUD does not require you to install any software and failover and redundancy are built-in. Furthermore, CLOUD supports multi-tenant and has an additional webpage for dealers to manage all customer accounts. This guide emphasizes infinias CLOUD but does cover some local server install information near the end of the document.

infinias	CLOUD	ESSENTIALS	PROFESSIONAL	CORPORATE
Built-in Database Redundancy	✓			
Built-in Database Failover	✓			
Multi-tenant	✓			
Cloud Management	✓			
Remote Management	✓	✓	✓	✓
Multiple Security Roles	✓	✓	✓	✓
Badging	✓	✓	✓	✓
Live Muster	✓	✓	✓	✓
Built-in Standard Reports	✓	✓	✓	✓
Customizable SQL Reports	✓	✓	✓	✓
Rules Engine (For user defined configuration)	Standard	Standard	Advanced	Advanced
iPhone, iPad and Android Support	✓	✓	✓	✓
Push Notifications to Site Access Mobile App Ad Hoc and Automated (Rules-based)	✓	✓	✓	✓
Wireless Lock Support	✓	✓	✓	✓
Mobile Credential Location Sevices & Mult-Factor Authentication	✓	✓	✓	✓
Virtual Machine Support		✓	✓	✓
Video Integration	via 3xLOGIC VIGIL and Milestone XProtect®	via 3xLOGIC VIGIL Software	via 3xLOGIC VIGIL and Milestone XProtect®	via 3xLOGIC VIGIL and Milestone XProtect®
Elevator Control (Requires Elevator Control Kit & License)	✓		✓	✓
LDAP Support for AD Synchronization			✓	✓
MS Outlook/Google Calendar Integration	✓		✓	✓
Requires Certification			✓	✓
Multi-tier Management	✓			✓
Number of Events	Unlimited	Unlimited	Unlimited	Unlimited
Number of Doors	Unlimited	Unlimited	Unlimited	Unlimited
Number of Cardholders	Unlimited	Unlimited	Unlimited	Unlimited
Door Licensing	Unlimited	Unlimited	Unlimited	Unlimited

2 Terms and Concepts

infinias CLOUD approaches access control in more of a 21st Century mindset than traditional access control systems. As a result, there are several new terms and concepts that might be new to the access control environment.

2.1 Doors vs. Zones

In the old-world access control, you configured a Door and created access privileges that granted access to that Door. infinias CLOUD introduces the concept of a Zone. A Zone could be viewed as the physical space which the Door occupies in your facility, floor, or room. Simply put, a Door borders two areas of a room, floor, or building, and each of those two areas are called a Zone. When you apply privileges to a Door, you're not really granting access to a Door, you're granting access to the Zone that the door protects. Therefore, an Outside Zone can have 20 doors attached to it, allowing access into the Inside Zone. The use of Zones simplifies the configuration process. Instead of creating an access privilege rule to each door, users can create a single rule applied to the zone, for all 20 doors.

Upon installation, infinias CLOUD creates two default Zones: Inside and Outside. In general, they represent the inside of your building, and the outside of your building.

As you plan your system configuration, consider useful names for the Zones to which you will be applying access privileges. Once you have configured your Zones, it will be much easier to maintain and re-configure access privileges to the Zones than compared to the old mechanism of Per-Door privileges.

2.2 Cardholder vs. Group

Traditional access control systems define a Cardholder and allow you to configure that Cardholder's access rights within the system. infinias CLOUD borrows from the Enterprise world and extends the Cardholder as a member of a Group, similar to the way Windows contains Windows account Users and Groups. All cardholders must be a member of at least one Group and can be a member of multiple Groups.

Access Privileges are not applied to an individual Cardholder, but rather to a Group. Thus, you can modify the access privileges of a large number of Cardholders with one simple configuration change. Or you can make significant access privilege changes to a single Cardholder merely by adding them to or removing them from a Group.

2.3 Door Types

Configuring a door can be a tedious task, having to configure each input and output of every controller, often repeating the same input and output selections over and over for each door. infinias CLOUD presents the Door Type, a template that describes the input and output configuration gathered into a single entity. infinias CLOUD and IntelliM- Access has several default Door Types from which you can choose, saving you many hours of tedious configuration effort. If a Door Type is not readily available, contact tech support. They should be able to create a Door Type to fit most needs.

2.4 Rules and Privileges

The traditional access control concept of privileges is used to determine a cardholder’s level of access into a door. Intelli-M Access expands the aging concept of access control, giving you pinpoint control

over the action the software takes in the occurrence of an event. The software provides the concept of a Privilege: the combination of a Group (who has access), a Zone (where is access granted), and a Schedule (when is access granted).

Additionally, users create Access Privileges utilizing a top-down approach. Simply, grant access privileges at any Parent Zone and the privileges will automatically propagate to all associated sub zones. This approach streamlines the configuration process and saves the user time, resulting in a much cleaner database and having the potential to dramatically reduce the number of Rules.

Furthermore, infinias CLOUD extends these capabilities with its robust Rules engine. The Rules engine allows users to configure their system to perform an action or multiple actions, based off a specified condition. For example, the access control system can be programmed to send an email action upon an invalid credential event.

2.5 Schedules and Holiday Sets

An infinias CLOUD Schedule is a stand-alone set of time ranges that define a 7-day week. A Schedule is generic in that it is not defined to serve a specific purpose such as a door unlock schedule. Each day has a set of zero or more time ranges you can define. The part of the Schedule that is displayed in blue is the Active Time Range. This Schedule can be applied to a Door (via the Door Behavior) as an unlock schedule, or to a Rule to define access privileges or when the Rule will be active. For example, when a Schedule is applied to a Door, the Door will be unlocked during the Active Time Range (the blue section) and unlocked during the inactive time range (the white section).

A Holiday Set is a grouping of Holidays applied to a standard schedule. For example, a Holiday Set might consist of New Year's, Thanksgiving, the day after Thanksgiving, and Christmas Day, when the office is closed; another Holiday Set might consist of Christmas Eve and New Year's Eve because the office hours are a half day. Once a Holiday Set has been defined, as set of time ranges that define that Holiday Set can be applied. Finally, the Holiday Set can be applied to an existing schedule. This will give a single Schedule which contains the normal hours of office operation, plus all the days in which the office is to be partially or completely closed. Furthermore, that complex Schedule can be assigned to any Door Behavior, Person, Group, or Rule.

2.6 Events and Alarms

All access control systems manage Events and Alarms, and each system has their own proprietary method of determining what an Alarm is and how to manage the presence of an Alarm. Our software chooses to not tell you what is or is not an Alarm, but rather you tell the software what is or is not an Alarm. By default, our software identifies an Alarm as the usual access control denial events, but you have free reign to determine the identity of an Alarm for yourself, using the Rules Engine.

2.7 Alarm Acknowledgment

infinias CLOUD introduces the concept of Automatic Alarm Acknowledgement. Old world access control systems require you to manually acknowledge every Alarm in their system, no matter how truly important that Alarm is. infinias software dispenses with manual Alarm acknowledgement and puts you in charge of determining what events are truly important to you. You make those decisions in the Rules Engine, which is described in detail in the Advanced Setup and Configuration chapter.

2.8 Extensibility and Peripherals

All access control systems have implemented some form of extensibility with third party security markets such as video surveillance systems. infinias software introduces the Peripheral, a third-party device that can be plugged into the software's Rules Engine, giving the third-party device unprecedented integration.

A Peripheral can be a video surveillance DVR, an individual IP Camera, a hardware I/O device, or even a web service like Google Maps. Each Peripheral is supported by a Plugin, which is a software module designed to provide the bridge between the software and the third-party device or service. The Rules Engine can then be used to control the Peripheral, telling it to do things like "record video on camera X when a card with invalid credentials are swiped at Door Y."

infinias Professional, Corporate, and Cloud software packages provide a Webpage Peripheral, Generic Peripheral, and Google and Exchange Calendar Peripherals for integration by default.

2.9 Reports

Most access control systems provide a canned list of reports that provide the most commonly-requested information. infinias software utilizes Microsoft's Reporting Services engine, along with their tools allowing users to create their own reports - layout, content, graphics, or whatever they want. Custom- printed cardholder's badges also utilize the Reporting Services engine, giving the user complete control over the "look and feel" of their badges. And it's all courtesy of Microsoft Report Builder and the Reporting Services engine. For custom reports, please contact a 3xLOGIC Sales Representative.

2.10 Muster Zone

A Muster Zone is a Zone that has been tagged with the In or Out Muster attribute. When a Zone has been tagged with the In-Muster attribute, infinias software will keep track of all users that have entered that Zone. A Zone can also be tagged with the Out-Muster attribute to keep track of both sides of a door if desired. A special Muster View on the Events Page displays the location of all cardholders in these Muster Zones in real-time. Muster requires doors to have an in and out reader to track who is remaining inside or outside the zone.

2.11 Multi-Tenant

A software installation on a server that allows for management of several groups of people with shared access levels within the software. infinias CLOUD allows a single dealer to manage an unlimited number of customers from a single sign on. Those customers are assigned to a specific customer level and can only have visibility and management within their scope.

2.12 Scope

Scope inherently defines what level of visibility and management a user has based on where the user has been assigned as a Person. When giving a Person the Supervisor, Human Resources, or User Role, their ceiling of visibility can be set by assigning the user to a zone. Once the ceiling has been set for each user that is logging into the software, the users can utilize Scope to drill down to a more granular level.

The more Zones and Rules that are created within the software the more complicated it can be to navigate and configure. Therefore, infinias CLOUD introduces the ability to filter out irrelevant data points with Scope.

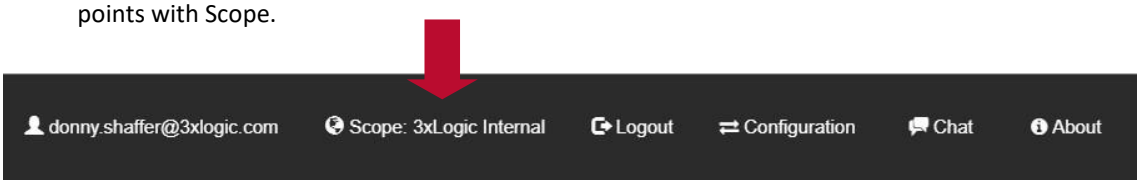


Figure 1: Scope Indicator

2.13 Zone Hierarchy

When Creating a Zone in infinias CLOUD, users will now have an option called **Parent Zone Name**. Users can create a Parent Zone which could be a region, state, or anything desired. From there, users will then create Children Zones and map out the zone hierarchy by identifying the parent and child relationship. The highest-level parent will usually be the company name but can always be identified by the red color.

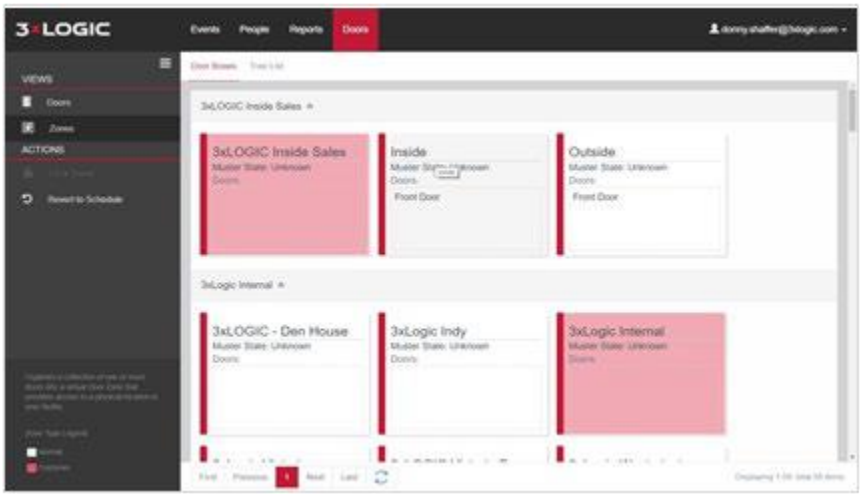


Figure 2: Door Boxes View

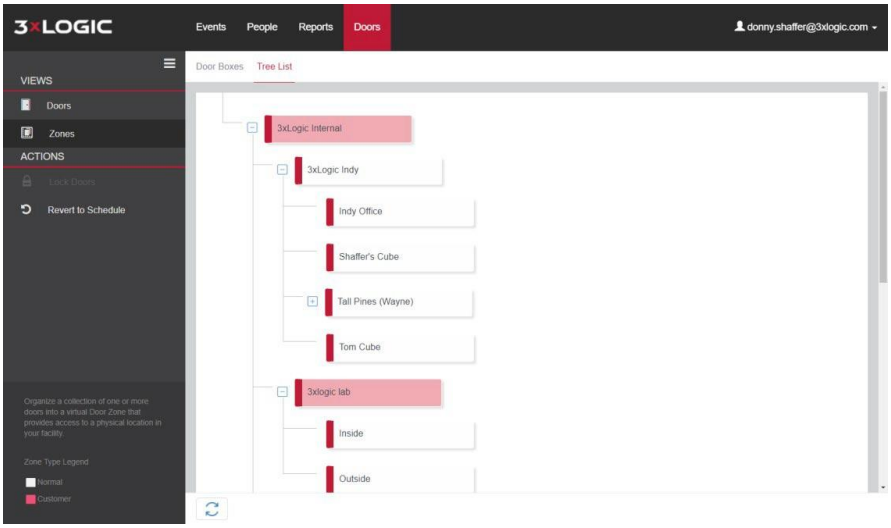


Figure 3: Tree List View

3 System Requirements

3.1 Software

3.1.1 Operating System

The following versions of Windows are currently supported:

- Windows 8.1 Professional
- Windows 10 Professional
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

NOTE: An upgraded OS that wasn't originally running a professional installation may not contain the required Internet Information Services, MS Message Queuing, or .NET software after the upgrade.

3.1.2 Supported SQL Versions:

- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

3.2 Hardware

The Intelli-M Access software requires the following hardware dedicated for optimal performance.

3.2.1 Under 50 Doors

- 2.2GHz CPU
- 4GB RAM
- 100GB of hard drive free space available AFTER installation.

3.2.2 Under 300 Doors

- 3.5 GHz
- 8 GB RAM
- 100GB of hard drive free space available AFTER installation.
- Solid State Hard Drive

3.2.3 Over 300 Doors

A server grade system should be dedicated for a large installation over 300 doors. This includes a fully licensed custom installation of SQL Server to maintain the large number of events being processed by the software. Please contact Support or Sales Engineering for recommendations.

NOTE: In some instances, a system with less than 300 doors might require a full version of SQL to prevent filling up the SQL Express 10GB limit on database size.

NOTE: Please see the infinias Installation Manual below for installation instructions

S-BASE-KIT_3x_GDE_ 2019_0610.pdf

4 Intelli-M Access Essentials

4.1 Login

Login to software using the shortcut created during the software installation.

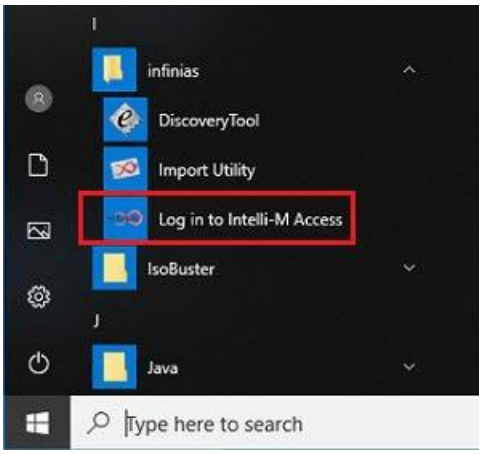


Figure 4: Login

Any client machine within the Local Area Network (LAN) that has open communication to the system where the software is installed will have the ability to remotely interface with the system UI using a current web browser such as Edge, Chrome, Firefox, or Safari and inputting the local IP address of the system followed by /intellim. **Example: 10.10.1.5/intellim**

4.2 Events Tab

The Events Tab is the first page seen upon logging in to the Intelli-M Access software. This page is updated in real time with all events streaming to the software via the door controllers and events generated on the software side. Three views are available to select from, each with their own list of actions.

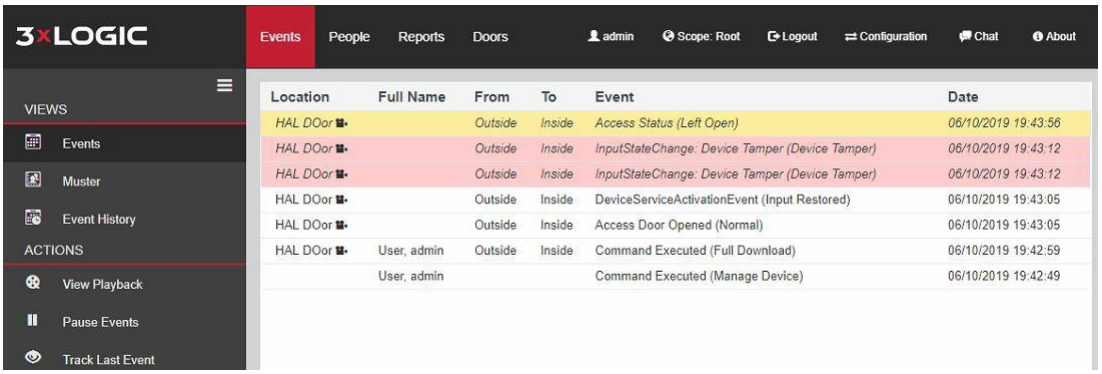


Figure 5: Events

The default **Events** view shows the live stream. If the video integration is in use, indicated by the recorder icon next to the location name, **view playback** will be highlighted for the indicated event time

under **Actions**. Events highlighted in Red indicate a tagged alarm event such as a forced open, left open, or device tamper. Please see the section pertaining to rules for further details on setting an alarm to an event.

Pause Events allows the live stream to be paused to review an event of interest. This is useful in installations where many events are streaming to the system preventing a viewer from accurately reviewing the incoming event stream.

Track Last Event will track the last highlighted event until the setting is toggled back to the default.

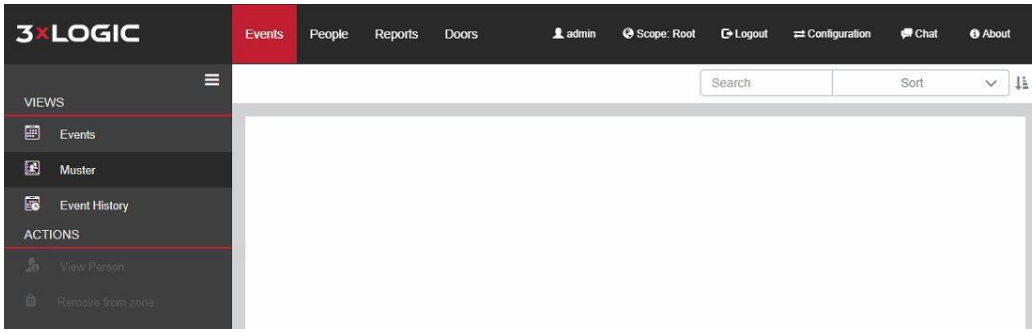


Figure 6: Muster View

The **Muster** view is for use with a site utilizing the muster feature of the software. Muster allows a site to determine who is inside or outside of particular zones or areas. This is useful for high risk areas that need monitoring. This feature is only available when a zone's entry points are utilizing dual readers that allow entry/exit of the zone. Please see the section pertaining to zones for more information on zoning.

The actions under Muster must have an existing person in the muster zone in order to be highlighted. Further details of the person can be determined by highlighting the person and using the **View Person** action under the **Actions** menu.

If a person somehow exits or enters a mustered zone without badging, they can be removed from the zone using the **Remove From Zone** action.

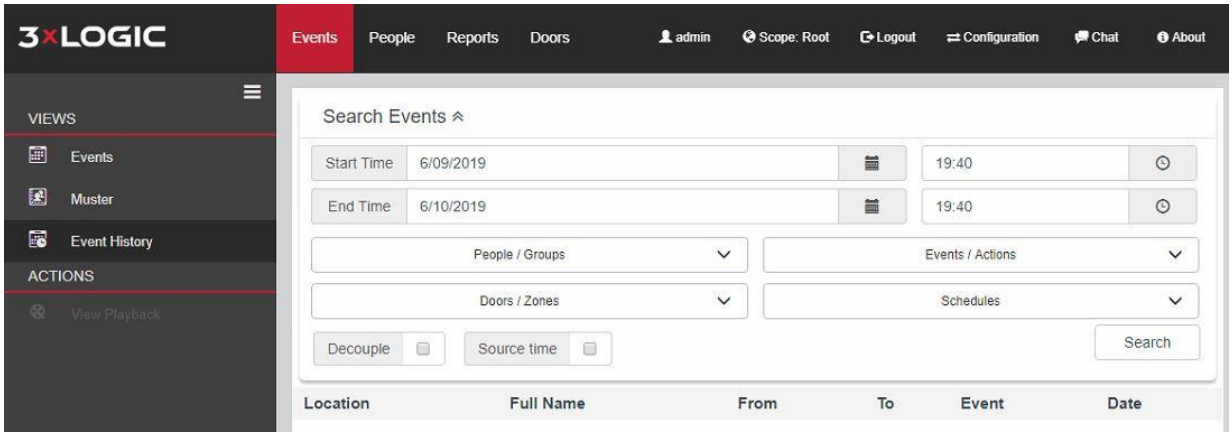


Figure 7: Event History

Event History is the final view and used to quickly filter event history to the last 100 events within a given time frame. It is important to note that this is not a report. The system will allow long periods of time to be specified in the search criteria. However, only the first 100 events gathered in that time range will be displayed. If a longer list is required, it is recommended to run a report from the **Reports Tab**.

The events will be filtered and shown below the **Search Events** filters. Any events that are integrated with video will show a recorder icon and will highlight the **View Playback** option under the **Actions** menu.

4.3 People Tab

The **People View** is where a person can be created, edited, deleted, badge printed, or events listed for a particular person. The **Groups** view under the people tab is where groups can be created, edited, or deleted that contain the people with login roles or access control credentials.

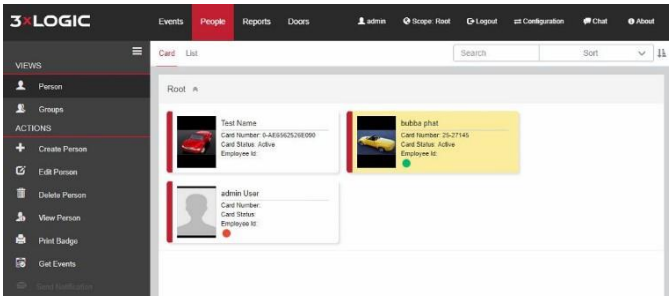


Figure 8: People Tab

4.3.1 Create Person

To create a person, simply click **Create Person** from the action menu and the page below will appear. The person's Title, First Name, Last Name, Middle Initial, Employee, and Department are available to be entered. Only First Name and Last Name are required fields.

If the person is being assigned a badge, Site Code and Card Code can be entered here. If alphanumeric credentials and readers are enabled on the system, a checkbox indicating that this is an alphanumeric card will be visible.

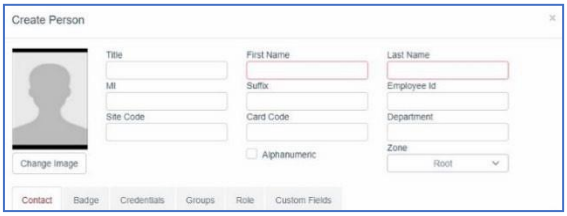


Figure 9: Create Person

The zone is automatically set to the root zone. The zone determines what scope the user will be able to view, if they have a login role to the software. See section 7.3.4 for details about scope

Upon creation, the Groups tab is selected by default. However, this document will discuss the tabs in order from left to right.

4.3.1.1 Contact Tab

A user's Company and contact information is entered on the Contact Tab. Everything under the Contact Tab is optional unless an email event rule is being utilized. Only people with email address information can be sent an email from the software

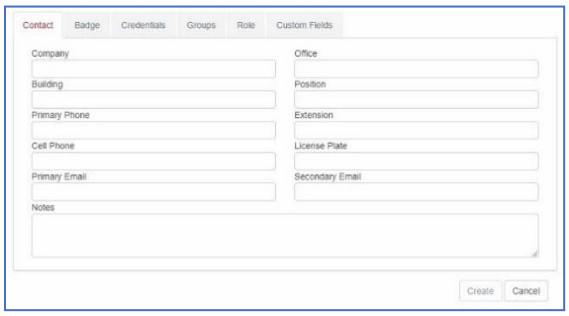


Figure 10: Create Person - Contact

4.3.1.2 Badge Tab

The badge tab is where badge information and pin code information for physical credential readers and keypads are kept. The status will show pending, active, inactive, or disabled depending on the state of the person. Pending status is determined by the activation date and time. If that time resides in the future, the status will show pending. It will change to active once the activation date and time have been reached on the system where the software resides.

NOTE: If a person is created on a PC that is remote to the system that contains the software and database, the activation time will be based on the time of the PC they are utilizing. For example, a person created in a User Interface being used in Pacific

Standard Time when the database resides in Eastern Standard Time might see a pending status for three hours on a newly created person, if they are not cognizant of the time difference.

An expiration date will lead to a person going inactive in the system on the particular date chosen. That will prevent them from gaining access with the badge credentials until such time as the expiration date is changed or deleted.

Disabling a credential prevents that credential from being used again in the system for another person. This is utilized when a physical credential is not returned or a pin code is given out. It is not suggested using pin codes at a facility that has a high turnover rate for that reason.

NOTE: The Pin Code field is ONLY used in a **Card + Pin** configuration. When using **Card OR Pin** where a person will have a physical credential and a pin code used separately, two badges will be used on the badge tab. One badge will be used for the physical credential and one for the pin code. The pin code will use a site code of 0 and the pin code itself will go in the card code field. The physical credential contains both a site code and card code embedded in the credential. If compatible with the system formats loaded in the software, the event will list the site code and card code information in place of the person's name on the events tab.

For more information on the difference between **Card + Pin** and **Card OR PIN** please see the guide on Card + Pin versus Card OR Pin.

card_pin_vs._card_or_pin.pdf

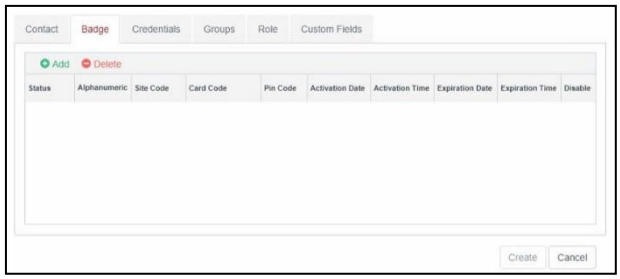


Figure 11: Create Person - Badge

4.3.1.3 Credentials Tab

The credentials tab is where Mobile Credentials are created for use with the Mobile Credential app on Apple or Android smart devices.

Please see the Mobile Credentials setup guide for further details pertaining to the configuration and setup of Mobile Credentials.

How To configure
Mobile Credentials (

Figure 12: Create Person - Credentials

4.3.1.4 Groups Tab

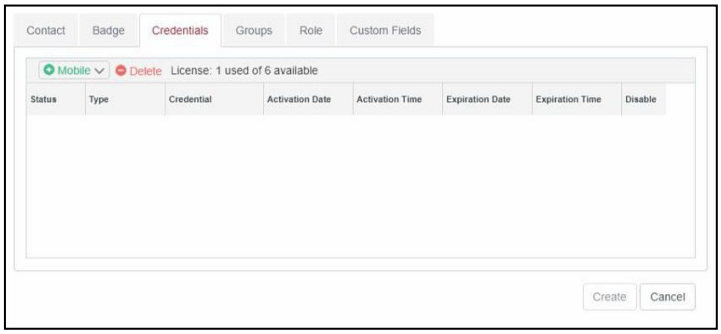


Figure 13: Groups Tab

The groups tab allows the person to be added to any number of groups that have been created in the system. Groups provide privileges to zones and other privileges for rules created in the rules tab. Please see the section on groups for further details.

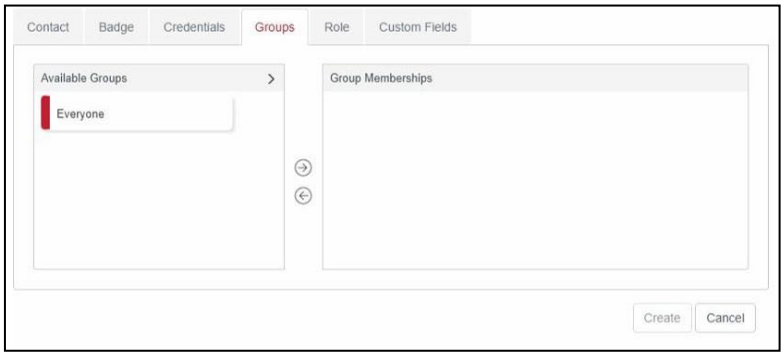


Figure 14: Create Person - Groups

4.3.1.5 Role Tab

The role tab allows the creation of an operator credential that allows a user login to the software. The role drop-down menu specifies the specific role or permission level. The zone would remain Root on Essentials and Professional software. Corporate and Cloud installations utilize a different zoning structure that those sections of the user guide go into further. User Name can be an email address or standard user name and password is case sensitive but doesn't force a specific password requirement.

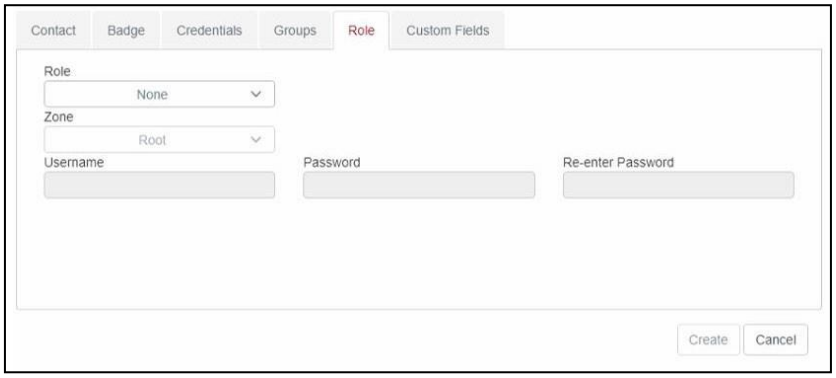


Figure 15: Create Person - Roles

4.3.1.6 Custom Fields Tab

The custom fields tab will display any custom fields created in the custom fields settings menu in configuration. Please see section 5.7.5 for more details on creating custom fields.

Figure 16: Create Person - Custom Fields

4.3.2 Edit Person

Edit person allows changes to be made to any pre-existing person in the system. Everything can be modified when editing a person.

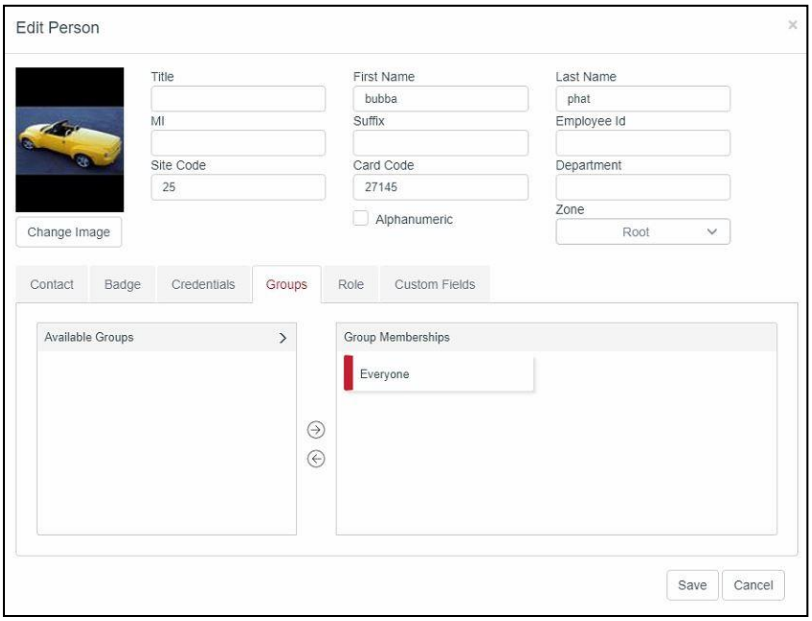


Figure 17: Edit Person

Figure 18: Edit Person

5.7.1 View Person

View person allows a quick view of some details about a particular person in the software.

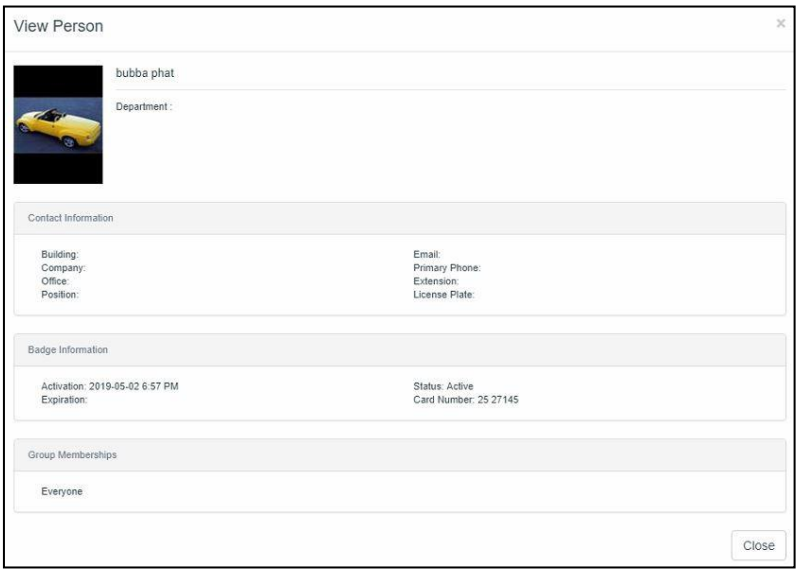


Figure 19: View Person

4.3.3 Get Events

Get events allows a user to quickly pull events for a specific person for purposes of data mining or troubleshooting.

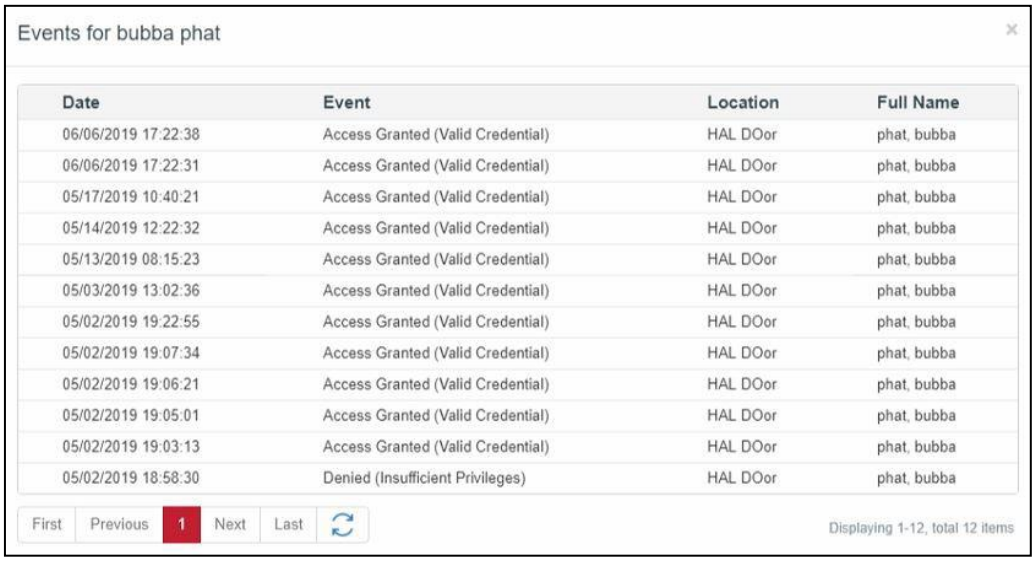


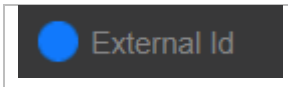
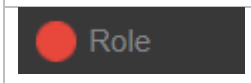
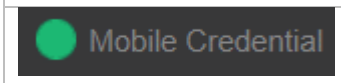
Figure 20: Get Events

4.3.4 Send Notification

This feature is used to send notifications to smart device users. More information is provided under the configuration section when implementing push notifications via the rules engine. See section 5.4.6 for more information.

4.3.5 People Tab Legend

The legend in the lower left corner provides visual details about people based on a colored circle as indicated below.

	**External ID**- Any Person created in Active Directory will display a blue dot on their user profile.
	**Role**- Any Person that has been given a login credential in infinias display a red dot on their user profile.
	**Mobile Credential**- Any Person that has been given a Mobile Credential will display a green dot on their user profile.

4.4 Reports Tab

The reports tab contains a list of all default reports, custom reports, badges, and custom badges available to be run from the system UI. Information on adding custom reports, creating custom reports,

and purchasing custom badges or reports can be found under the configuration section of this user guide.

Once a report is selected, clicking **Run Report** will pop up the interface for that particular report based on the type of report or badge it is. Additional fields might be required such as a time and date range or selection of zones prior to running the report or badge.

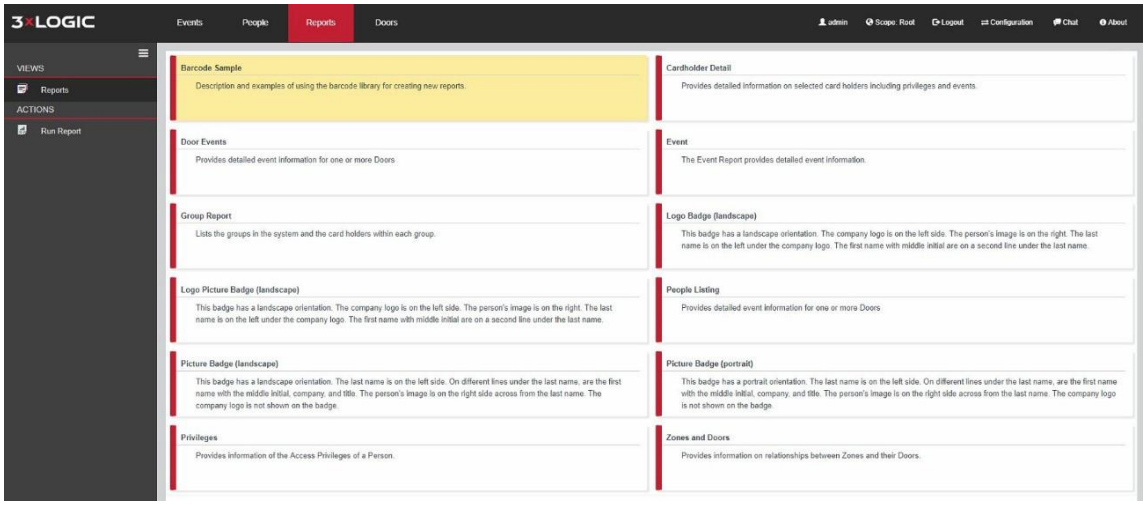


Figure 21: Reports

4.4.1 Barcode Sample

The Barcode Sample is a special report whose content explains how to add barcode fields to any report, particularly Badge reports. Run this report to view the example and instructions. No time range or other parameter input is required.

4.4.2 Cardholder Access History

The Cardholder Access History report shows access events by cardholder and door.

4.4.3 Cardholder Detail

The Cardholder Detail report displays a summary of the Persons contact information, along with their picture, and a list of all events generated by the selected Person(s) during the time range you selected.

4.4.4 Event

The Event Report displays all events generated by the selected Person(s) during the time range you selected.

4.4.5 Group Report

The Group Report displays all Groups, and a list of the members of each Group. No time range or other parameter input is required.

4.4.6 Privileges

The Privileges Report displays a matrix of all Access Privileges in the system, showing the Groups, Schedules and Zones in an access matrix. No time range or other parameter input is required.

4.4.7 Zones and Doors

The Zones and Doors Report lists all Zones, along with a summary of all Doors in each Zone. No time range or other parameter input is required.

4.4.8 Mobile Credential QR Activation

The Mobile Credential QR Activation Report will provide a scannable QR code to activate Mobile Credentials for any user that has been provided a Mobile Credential Key. This report also includes the user with instructions for activating their mobile credential.

NOTE: The Mobile Credential QR Activation is only available in cloud.

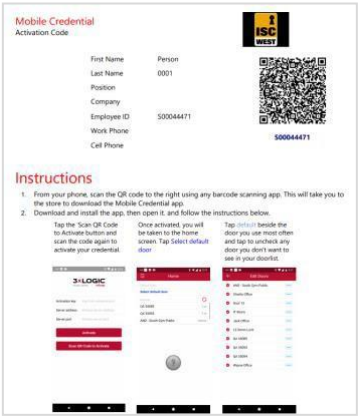


Figure 22: Mobile Credentials QR Activation

4.5 Doors Tab

There are two Doors Tabs in the software. One exists under Home, where Events, People, and Reports are located. The other is the default tab that comes up when going to configuration. This section details the Doors tab on the Home page.

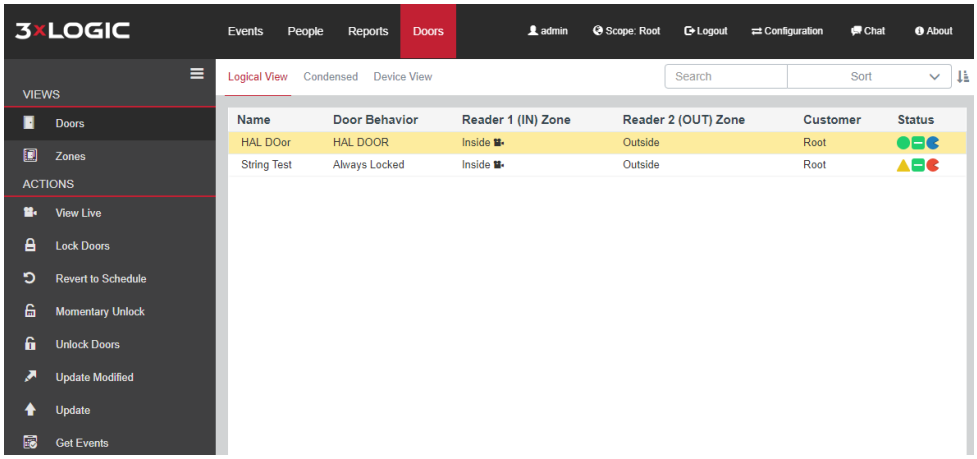


Figure 23: Doors

In the lower left-hand side of both Doors Tabs is the Doors Tab legend. Putting the mouse cursor over the icon in the legend or the icon shown on the door's status in the door list will give you the meaning of the status.

4.5.1 View Live

Figure 24: Door Status Legend

View Live only works with doors that are associated with the 3xLogic Vigil/Visix integration. If they are, the option will be highlighted for selection when a door is selected. A window similar to the one below will pop up and play live video for the selected door. Further details pertaining to the video integration will be covered under the configuration section.

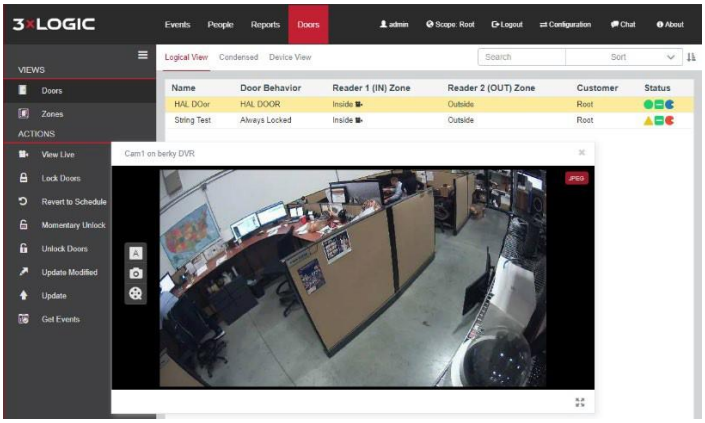


Figure 25: Doors - View Live

4.5.2 Manually Overriding Doors

Lock Doors, Revert to Schedule, Momentary Unlock, and Unlock are manual overrides for the highlighted doors. If manually Locking or Unlocking a door, it is important to remember that the door will remain permanently in that state until a revert to schedule is selected. Revert to Schedule will revert the door back to its normal scheduled behavior, be that unlocked or locked.

Manual overrides are always indicated by a yellow lock status. Momentary unlock is just as it sounds. The door will unlock for four seconds and relock.

The home doors tab is the only place these overrides can be found.

NOTE: Multiple doors can be selected from a single page by holding the **Control** key on the keyboard and selecting the specific doors to be highlighted. All the doors can be highlighted by selecting the first door in the list and holding the **Shift** key while selecting the last door in the list.

4.5.3 Update Modified

Any doors showing a yellow triangle status indicate that they require an update to be current to the programming of the software. This can be done with a single click by using the update modified option in the actions menu. All doors in the system with that status will initiate an update. All doors that were not showing that indicator will remain idle.

4.5.4 Update

The update feature is used to manually update doors that are in a state requiring an update or for troubleshooting purposes.

4.5.5 Get Events

This feature is similar to the get events feature in the person tab. The difference is this get events pulls events for the door and not a person.

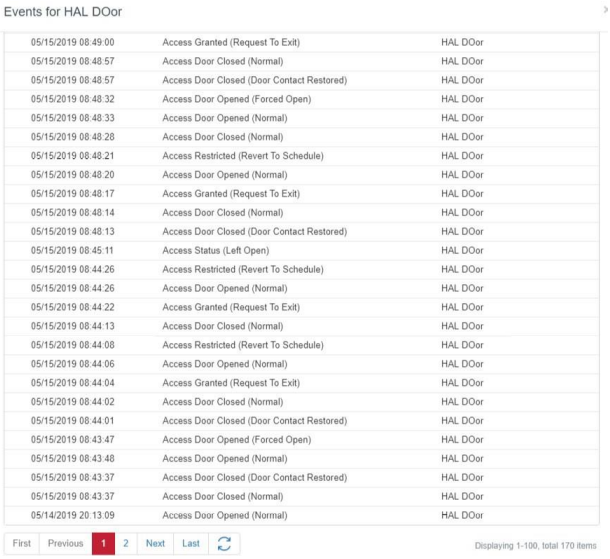


Figure 26: Doors - Get Events

4.5.6 Viewing Modes

At the top of the doors tab is a short row of viewing modes labeled Logical View, Condensed, and Device View

4.5.6.1 Logical View

Used to reference the zones, name, door behavior, customer, and door status.

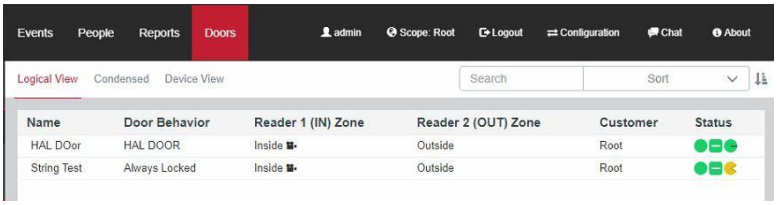


Figure 27: Doors - Logical View

4.5.6.2 Condensed View

This view will show the door status for many doors in a single screen. Useful for monitoring at a glance.

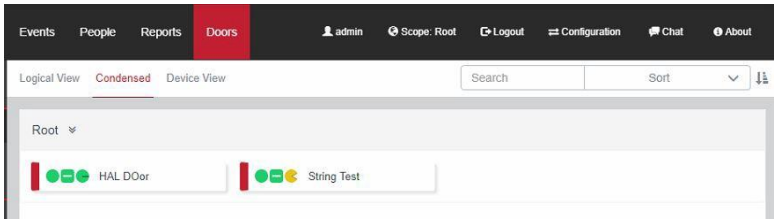


Figure 28: Doors - Condensed View

4.5.6.3 Device View

The device view is another detailed information screen used for identifying name, serial number, IP address, MAC address, data port, door type, firmware, last communication, customer, and door status.

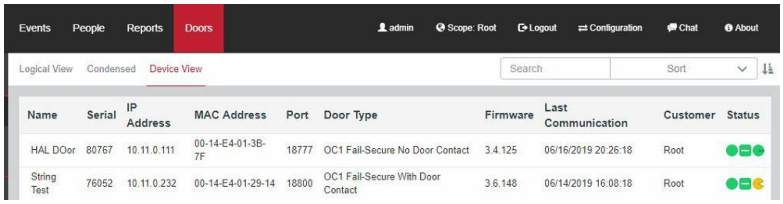


Figure 29: Doors - Device View

1.1.1 Zones View

The zones view is similar to the doors view in that it has a home page version and a configuration page version. The home page version is primarily informational.

4.5.7.1 Lock Doors

The one action you can do from this view is lock all doors associated with a particular zone.

4.5.7.2 Revert to Schedule

You can also revert all doors from a particular zone back to their schedule from here.

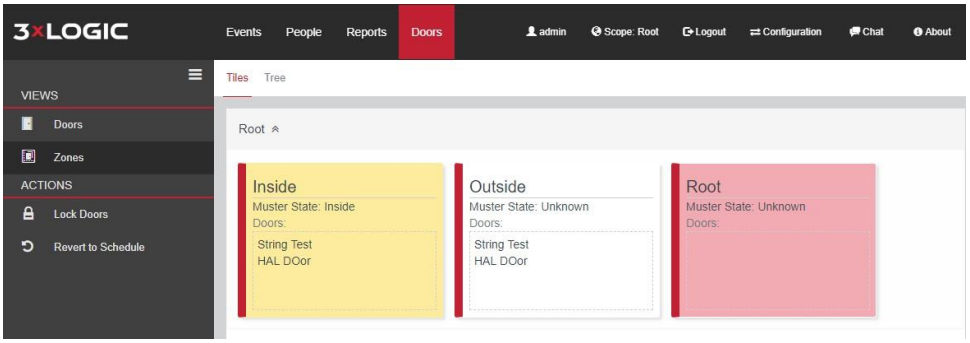


Figure 30: Zones View

4.5.7.3 Tree List

Please see the Corporate and Cloud sections of the guide for further information on the tree list in zones. This feature is not available in Essentials or Professional levels of the software.

1.1.2 Virtual Button View

4.5.7.1 Live Virtual Buttons

Virtual buttons are used to allow a virtual button to activate a rule through the rules engine to trigger a desired output. The example below shows a button being used to trigger a lockdown. Additional details are located under the doors tab configuration section of the user guide.

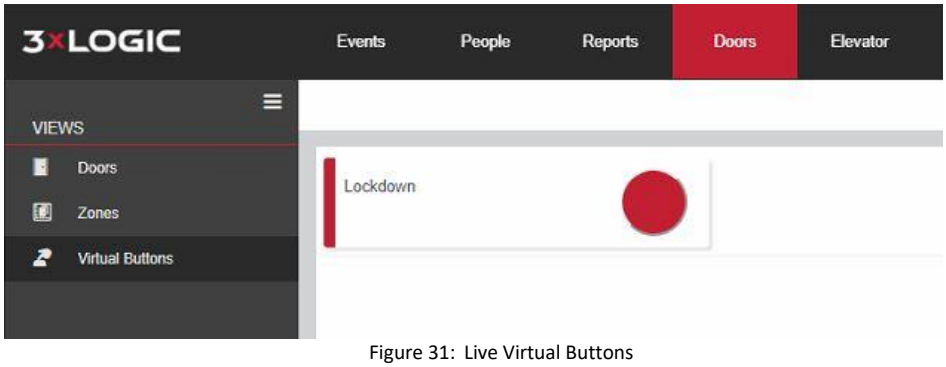


Figure 31: Live Virtual Buttons

4.5.7.2 Top Menu Bar

The menu bar at the top will help you navigate and show additional features of the software whether under the home page or configuration page.

4.5.7.3 Logged in User

The name of the user who is logged in will be visible in the upper right. This has priority and will always show be visible, regardless of the state of the menu.

Figure 32: Logged In User

Clicking user settings or clicking the user name when the system isn't collapsed into a drop-down menu will display the User Settings box. Currently the only user setting allowed is the **Show Source Time**. Checking this box will display events using the time from the controller, not the local time on the machine. This is useful when doors are located in a different time zone than the user but may be confusing on the event screen if controllers are in multiple time zones, as it may show an event occurring at 7AM and the next event may display 6AM if the readers are in different time zones.

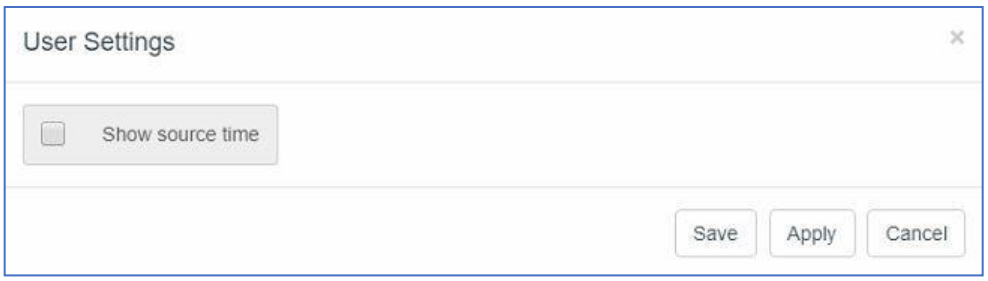


Figure 33: User Settings

4.5.7.4 Chat Assistance

The software has a chat feature built into it that allows for someone to send a chat request to the support team during business hours.

4.5.7.5 About

The about button will give the version and a link to the support web page. This will expand in functionality in upcoming releases to include additional features.

2 Intelli-M Access Essentials Configuration

The configuration section of Intelli-M Access includes a range of features that allows the programming of doors, zones, behaviors, schedules, rules, and many more. Essentials constitutes the bulk of software installations along with the bulk of the feature set for the software. The following sections will elaborate on what each section is for and how to use it to program the software.

2.1 Doors Tab

The first tab under configuration is the doors tab. The doors tab configuration page is similar to the doors tab home page but is limited to configuration and not interaction like the doors tab home page. You will not be able to lock, unlock, revert, or momentarily unlock a door from this tab. The page will show the first 100 doors in a paged view. For more than 100 doors use the paging option at the bottom of the page to move to the additional pages of doors. The search feature in the upper right can also be used to narrow down the list of doors using the filter option.

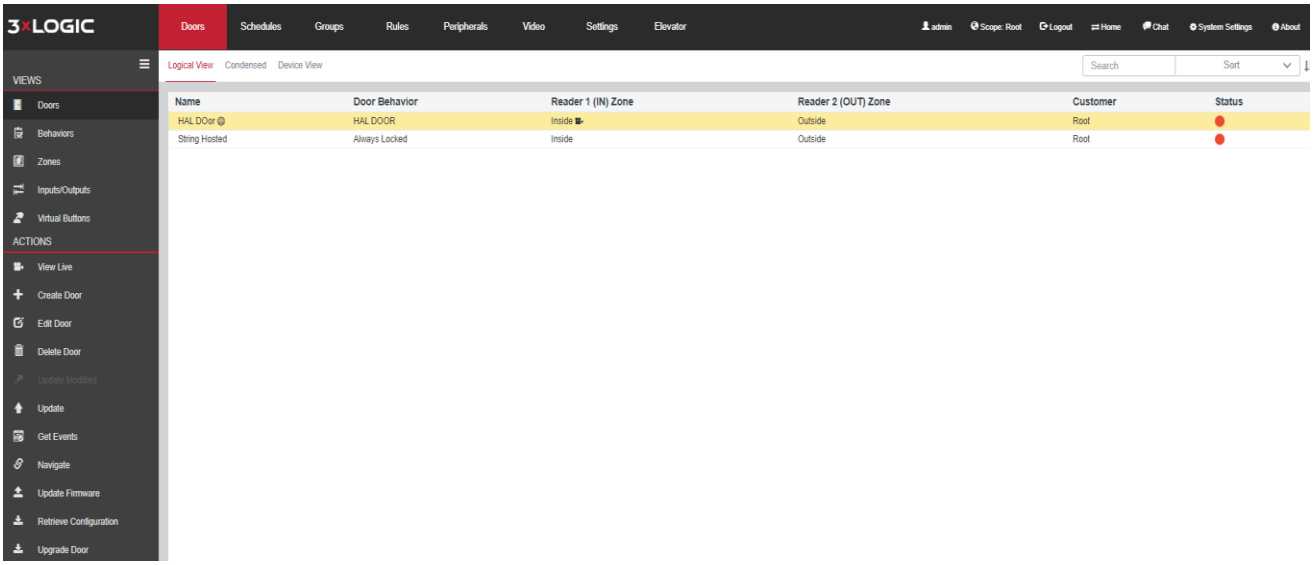


Figure 34: Doors

2.1.1 Doors View

This is the primary location for configuration of the door hardware for the software. This section will break down each action available to a supervisor or administrative role.

5.1.1.1 View Live

Identical to the one found in the doors tab home page. This will only be available if a camera is associated with the door.

5.1.1.2 Create Door

Hosted: There are two primary options when creating a door using an eIDC32 door controller in Essentials, Professional, and Corporate software. The first is eIDC32 (Hosted) and it shows up by default when creating a door under the device drop down menu as seen in the screenshot below. This option is initially more work than the older non-hosted option. However, it requires less networking access and knowledge than the non-hosted method. A separate document has been created for the purpose of configuring a site to use that newer method of programming. The hosted door option is not compatible with first generation door controllers from older systems. Using a hosted door is the preferred option when setting up a controller.

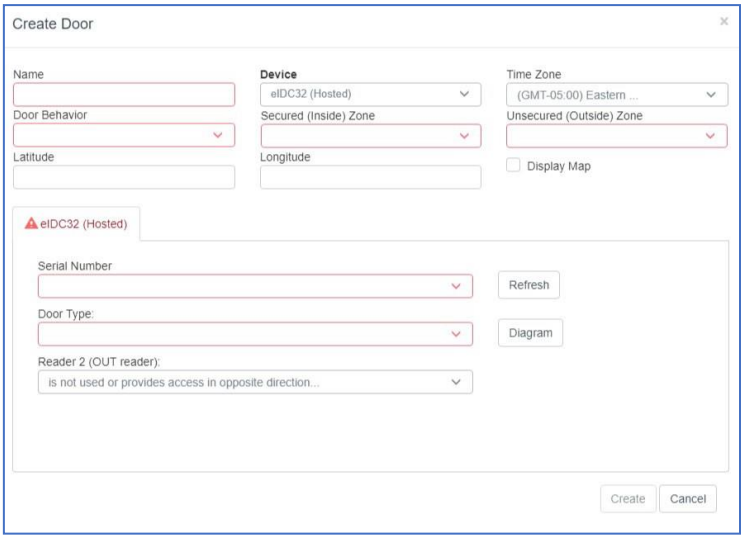


Figure 35: Create Hosted Door

Below is the embedded PDF document that will walk through the procedure for creating an eIDC32 (Hosted) door.

S-BASE-KIT_3x_HTG-Configuring a door

Non-Hosted: The non-hosted eIDC/eIDC32 option in the device drop down menu covers both first generation eIDCs and second generation eIDC32s. This is the only mode available to older generation controllers or older firmware eIDC32s.

Name – Name of the specified door.

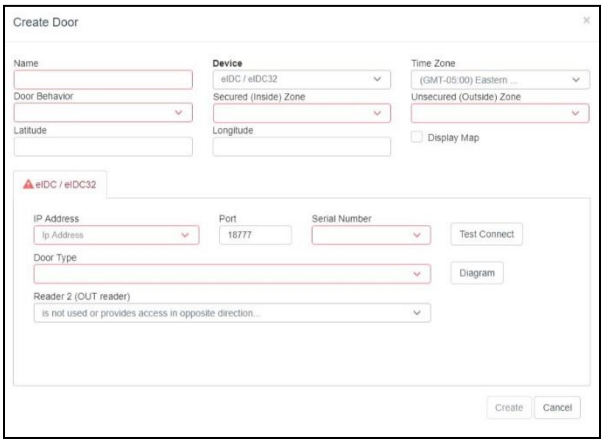


Figure 36: Create Non-Hosted Door

Time Zone – Time zone of the door, not necessarily where the software is installed.

Door Behavior – The door behavior of the door. The default is **Always Locked** but any number of others can be created under the behaviors view of the doors tab in order to make one available under the drop-down menu when creating a door. This specifies the door schedule the door will follow.

Secured (Inside) Zone – Specifies the area that is requiring a credentials to be accessed or the secured side of the door.

Unsecured (Outside) Zone – Specifies where the person is coming from and is considered unsecure or less secure than the area requiring a credential to access.

Latitude/Longitude – The GPS coordinates of the door. This is used with mobile credentials to limit the range at which someone can unlock a door from the smart device app.

Display Map – Displays the map for the coordinates when box is checked.

IP Address – IP address of the controller, either internal or public determined by the location of the door controller versus the location of the system running the software. Custom ports are supported by the controller in order to allow multiple doors at remote locations to communicate back to the system via a public IP address and proper port forwarding.

Port – Default is 18777 for all non-hosted door controllers. This can be customized for remote locations that use a single public IP address and multiple custom ports to communicate to the door controllers. Contact support for further details.

Serial Number – This links the device serial number, typically a six-digit number, to the IP address and allows the software to differentiate between it and other controllers.

Door Type – The door type is essentially the configuration that is pushed to the door controller in order for it to follow a specific wiring diagram. That diagram can be viewed via the **Diagram** button to the right of the door type drop down menu. This only applies to default door types. Custom door types will not have a diagram. See the settings tab section for further details on adding/removing door types from this drop-down menu.

Reader 2 (Out Reader) – This tells the system how to utilize the second reader. **Is not used or provides access in the opposite direction** is the default selection. This is used when two readers providing access in two directions or a single reader used for one direction is utilized. **Provides access in same direction as Reader 1 (IN reader)** is commonly used in gate access as

storage centers where two readers one at car/truck height and another at semi or tracker trailer height is required to make accessing the site easier.

Test Connection – Only available in the older eIDC (non-hosted) mode. This will ping a provided IP via the data port in order to determine if the port is being blocked by the network or antivirus software. This is useful when the door controller can be pinged (port 80) and navigated to (port 80), but no door status or events are coming through from data port (default 18777).

Allegion/Engage Door:

The Allegion door option in the device drop down is for the new wireless lockset integration that replaces the EL wireless lockset that went end-of-life. Please see the Allegion Wireless setup guide for details on programming and configuring an Allegion door lock to function with Intelli-M Access and Infinias Cloud. Once a door has been programmed, the door serial number will appear in the serial number drop down menu.

allegion_wireless_lock_quick_start_gui

EL Series:

Legacy wireless door lockset that has been discontinued by the manufacturer. Limited support is available for this on legacy sites that were originally installed when the product was being manufactured and sold. It is highly recommended to look at replacing these devices before failure as there is no supply of these available from the original manufacturer. Please contact support for additional details.

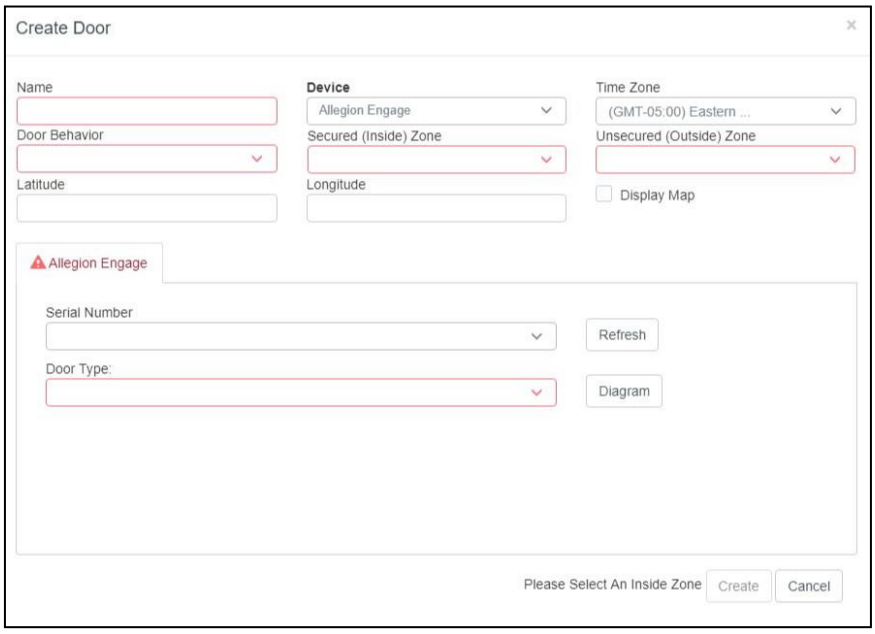


Figure 37: Allegion Engage Door

5.1.1.3 Edit Door

The edit door option will allow any created door to be edited and then saved. Most changes will require the door to be updated after saving.

5.1.1.4 Delete Door

Allows the door to be removed from the UI. The door is not deleted from the database, it is just flagged as deleted so it doesn't show up in the UI. This is for proper SQL database management and for reporting purposes.

5.1.1.5 Update Modified

This does the same as the previous doors tab. It forces all doors in the needs update state or yellow triangle status to get an update.

5.1.1.6 Update

5.1.1.7 Get Events

Pulls all events associated with the specific door as seen below.

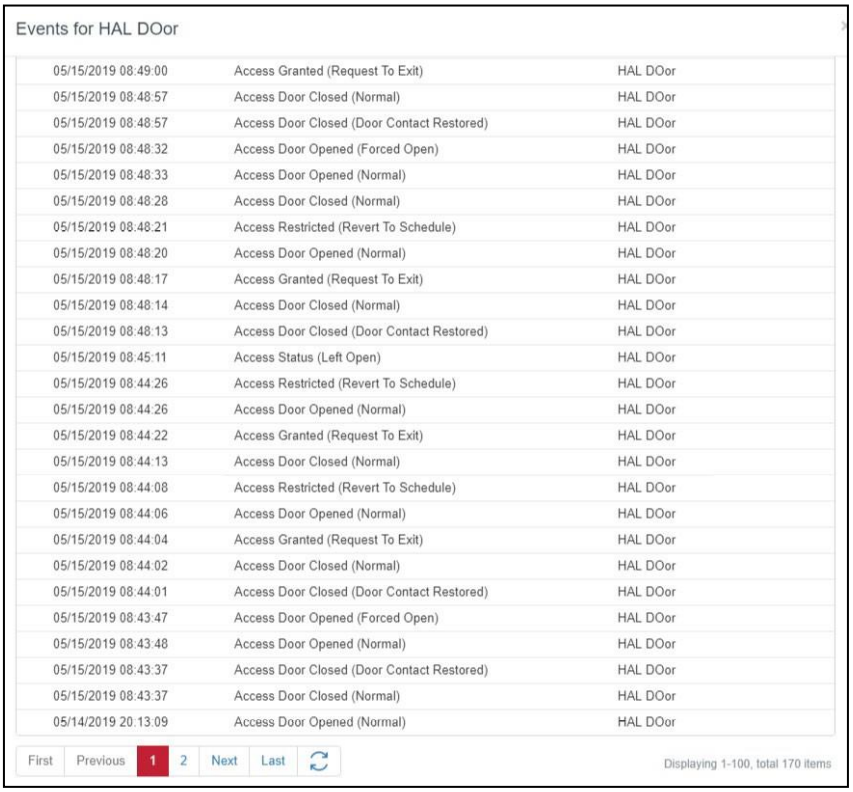


Figure 38: Get Events

5.1.1.8 Navigate

This action opens up a new tab in the web browser and attempts to pull up the login page for the door controller based on IP address. This does not work in Cloud and the software cannot connect to remotely installed controllers on another location without a network connection within the same subnet or VPN.

5.1.1.9 Update Firmware

This will attempt to update the firmware on the eIDC32 by asking for the firmware zip file location. This will not work on controllers older than version 3.x firmware. Those controllers must be updated via the Discovery Tool installed on a computer with access to the LAN on which the controller is installed.

Figure 39: Update Firmware

5.1.1.10 Retrieve Configuration

This is for troubleshooting purposes and only works with the eIDC32(Hosted) door controllers. The configuration of the device can be pulled to a file on the local system or Cloud for further investigation of potential issues or for testing purposes.

5.1.1.11 Upgrade Door

This option attempts to switch a non-hosted eIDC32 into a hosted eIDC32. The server settings need to be filled in on the **Settings Tab** in order for this to function properly. Click **Edit Server** and set the following properties:

- Address: ipaddress of server (note: if this says localhost, it needs changed to the IP address).
- Port: 18800
- Is Secure: checked

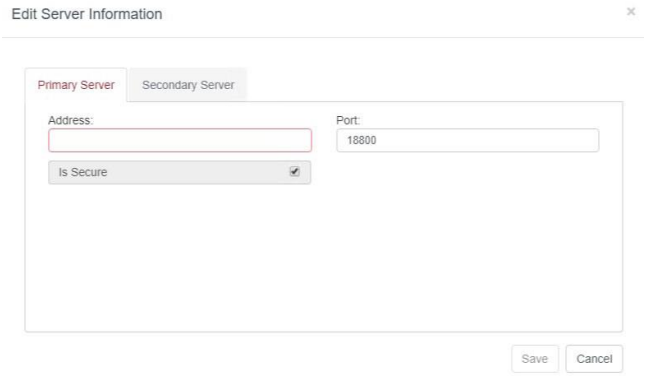


Figure 40: Server Properties

When upgrading a door from the doors tab, this section is referenced when pushing the outbound configuration to the door for the first time. For further details on creating doors, please see the “Creating a door in Intelli-M Access” guide.

S-BASE-KIT_3x_HTG-Configuring a door

2.1.2 Behaviors View

Behaviors are used to manage the lock and unlock times of each door. It also has some features to manage the type of reader tied to the controller and whether or not that reader is Card + Pin or Card OR Pin (Card Only). The default door behavior is **Always Locked**. Additional door behaviors can be created and made available in the Door Behavior drop down menu on the door edit page.

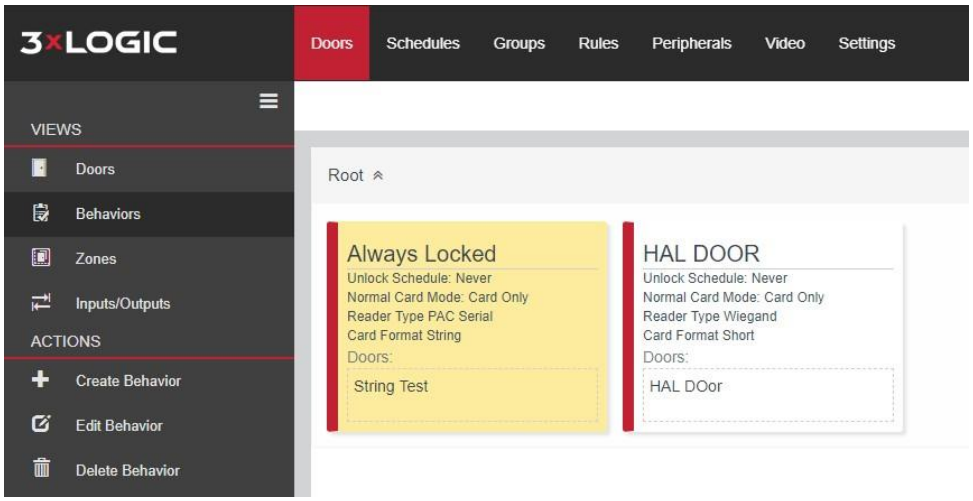


Figure 41: Door Behaviour

5.1.2.1 Create Behavior

This opens the window for behavior creation.

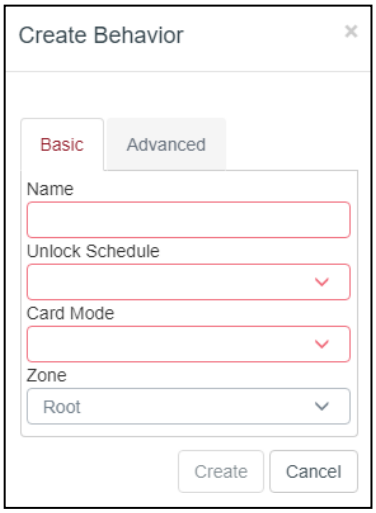


Figure 42: Create Behavior

Basic Tab

Name: Input a custom name for the behavior that will show up under the behavior drop down menu on the door edit page.

Unlock Schedule: Point the behavior to a custom weekly schedule that the door should follow. Remember that blue is unlocked and white is locked.

Card Mode: Point the behavior to a custom weekly schedule that the door should follow. Remember that blue is unlocked and white is locked.

Please See the Card + Pin versus Card OR Pin Document for explanation of each

card_pin_vs._card_or_pin.pdf

Zone: For local installations, this will be Root. If the customer name was changed from Root, it will be whatever the name was changed to. Zone refers to the visibility of the behavior. For example, users who can only view lower level zones (zones underneath root) will not be able to see this behavior.

Advanced Tab

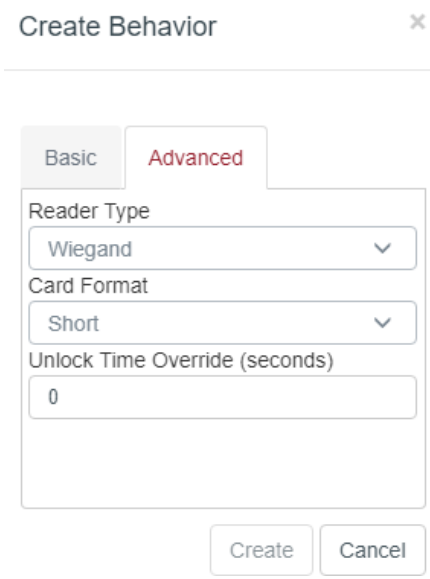


Figure 43: Behavior - Advanced

Reader Type: Wiegand, Pac Serial, Qscan

Wiegand is the standard reader type that Intelli-M Access functions with

PAC Serial is a string reader compatible setting that allows us to function with the PAC Alphanumeric reader.

Qscan – Utilized for a specific customer installation

Card Format:

Short: Short format is used for Wiegand based readers

String: String format is used for the PAC Serial alphanumeric based readers

Unlock Time Override (seconds)

This is used to override the default 4 second unlock pulse that used on all default door types.

The override can be for up to 100 seconds on eIDC32s or 30 seconds on Allegion wireless doors. Zero seconds is the default and uses the default door type time of 4 seconds.

NOTE: Times of over 100 seconds can be achieved for regular controllers. Those require a custom door type/template that needs to be uploaded to the database. Contact support for details.

5.1.2.2 Edit Behavior

Any behavior can be edited after creation.

5.1.2.3 Delete Behavior

To delete a Behavior, select a Door Behavior and click the Delete Behavior Action. A confirmation message box will appear, and the Behavior will be deleted upon confirmation.

NOTE: Door Behaviors can be deleted only when there are no Doors configured to use this Behavior. Therefore, you might get an error popup dialog indicating that one or more Doors are still utilizing this Behavior. Assign a different Behavior to those Doors, and then delete the Behavior.

2.1.3 Zones View

In the zones view the list of zones are shown in tile format for Essentials and Professional versions of the software. A tree view is available in Corporate and Cloud. Further explanation of the tree view is in the Corporate and Cloud sections of this user guide.

Any zone with doors tied to it will not be capable of deletion. All zones must be cleared of doors by going to the doors view and editing each door using that zone prior to it being able to be deleted.

Updating a zone will update all doors attached to that zone. A zone without doors is incapable of being updated.

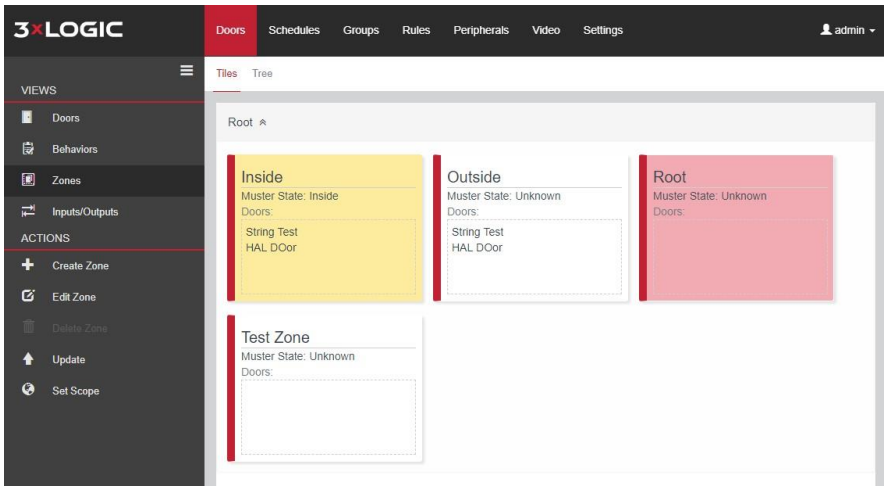


Figure 44: Zones

5.1.3.1 Create Zone

Clicking the create zone will pop up a small window with a few options. Each door has two zones. A secure side and an unsecure side are both required when creating a door. However, a zone may have more than one door. The diagram below gives a visual example of how a zone may affect multiple doors.

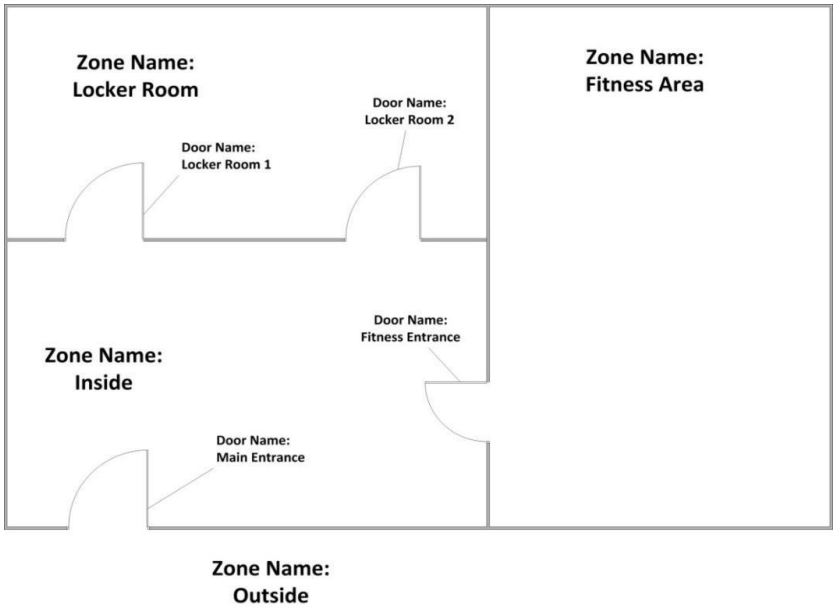


Figure 45: Zone Example

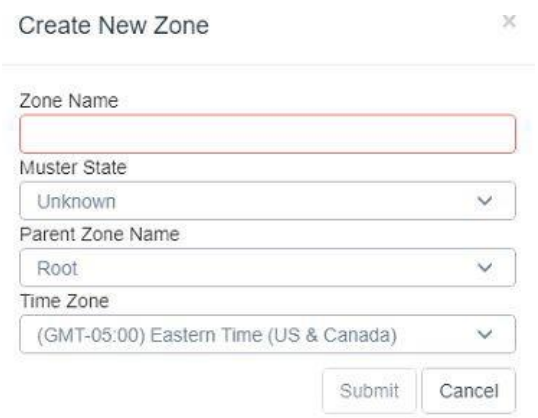


Figure 46: Create Zone

Zone Name

Name the zone however you want to identify the location requiring authorization to enter.

Muster State

Muster Zone has three states: Unknown, Outside, and Inside

Unknown is set when not using muster

Inside is used when wanting to track whomever is on the inside or secure side zone

Outside is used when wanting to track whomever is on the outside of the secure side zone

Parent Zone Name

Covered in Corporate and Cloud versions.

Time Zone

Time zone of the location. This correlates to the door time zone in most applications.

2.1.4 Inputs/Outputs View

This view is used to manage the inputs and outputs of each door controller. Below is an example of the Inputs/Outputs page. Inputs is the default page, click the Outputs link at the top of the page to switch to the outputs view.

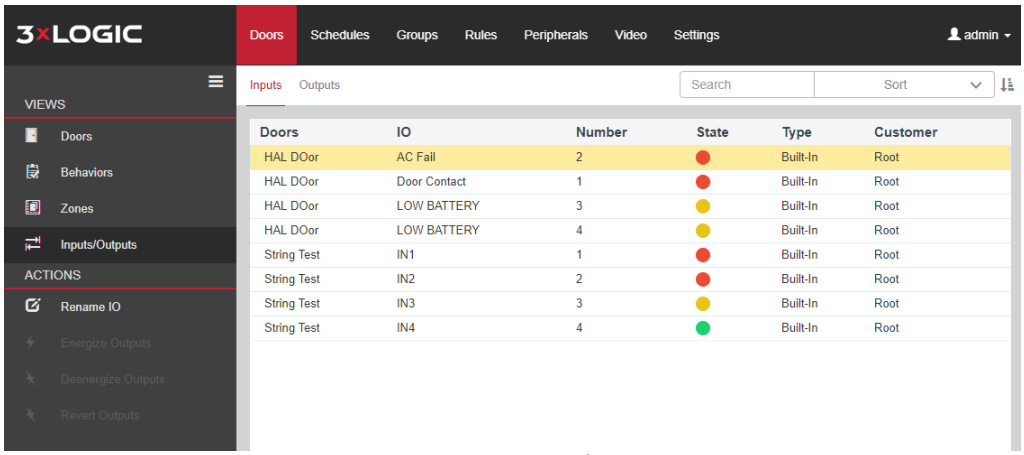


Figure 47: Inputs/Outputs

5.1.4.1 Rename IO

Highlighting an input and clicking the Rename IO action, or double-clicking on that input will allow the user to rename it. Clicking the reset button will reset the input back to the default input name.

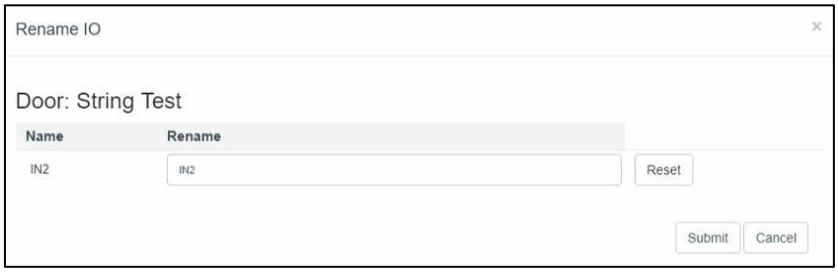


Figure 48: Rename IO

5.1.4.2 Outputs

Switching to the outputs view will show a list of all outputs on all doors. Individual outputs can be manually overridden using the energize outputs, deenergize outputs, revert outputs under actions when on the outputs view.

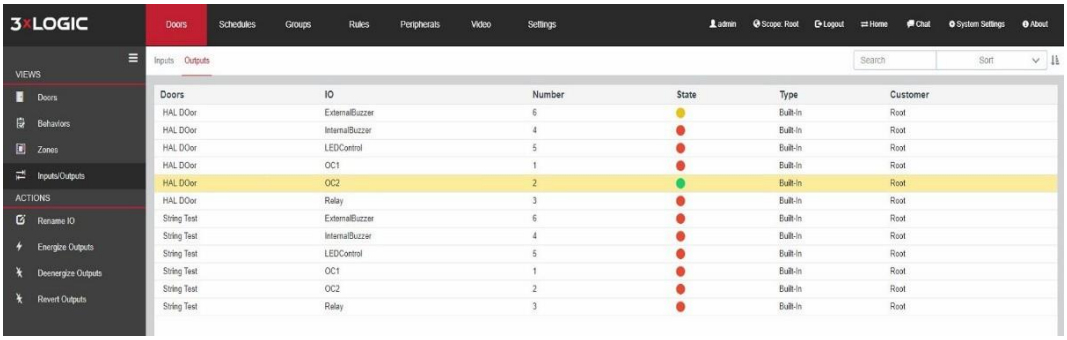


Figure 49: Outputs

Renaming outputs follows the same procedure as renaming inputs

2.1.5 Virtual Buttons

5.1.5.1 Virtual Button Configuration

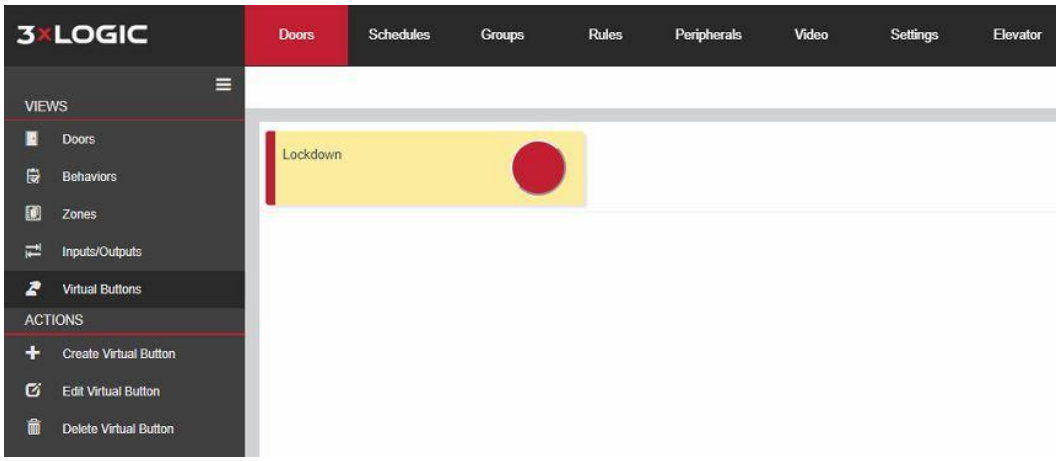


Figure 50: Virtual Button Config

Creating a virtual button can be performed by clicking the **Create Virtual Button** link and entering a name. It will obtain the zone location from whatever zone the system is currently scoped to.

Figure 51: Create Virtual Button

It is recommended to use different names for different buttons. They can be named the same name as

another button ONLY if the buttons exist in different zones.

Once the button is created, it can be used in the creation of any rule affecting an output or state of a zone in the rules tab. Example shown below.

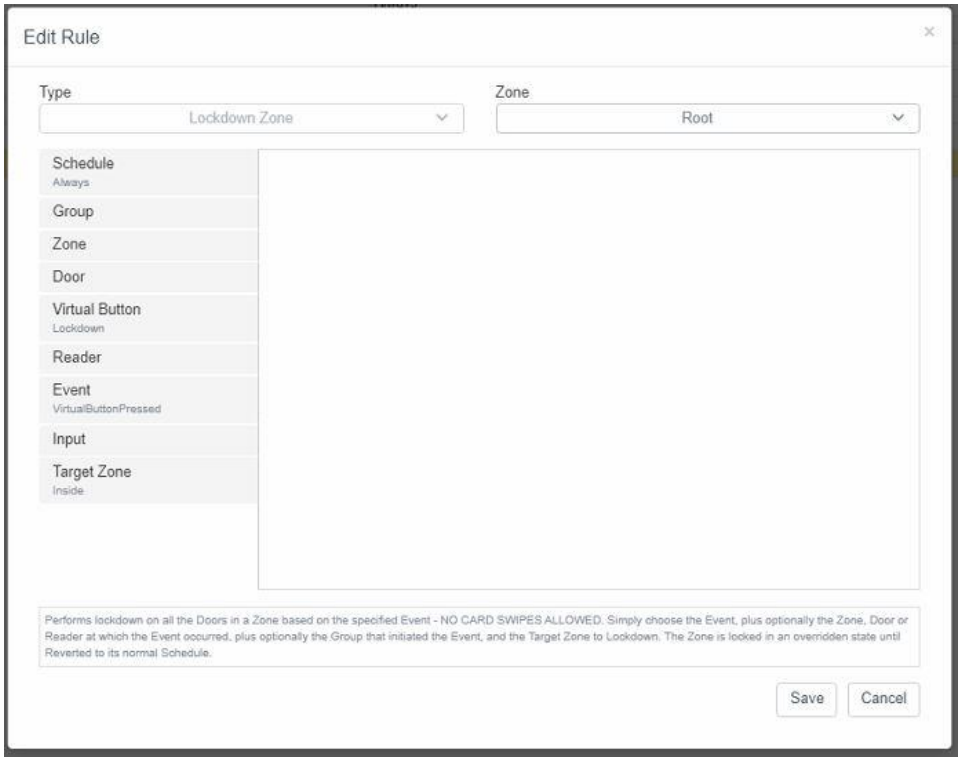


Figure 52: Edit rule

The new virtual buttons will also appear in the most recent mobile credential app on any smart device compatible with version 6.7 or later Intelli-M Access software. Infinias Cloud is also supported in this manner. See the Mobile Credential User Guide for more information.

5.2 Schedules Tab

The Schedules Page in the Configuration Section lets you create, modify or delete a Schedule, as well as create, modify or delete Holidays that can be applied to a Schedule. These schedules will be used as Door Lock schedules, Access schedules, and any other Rule.

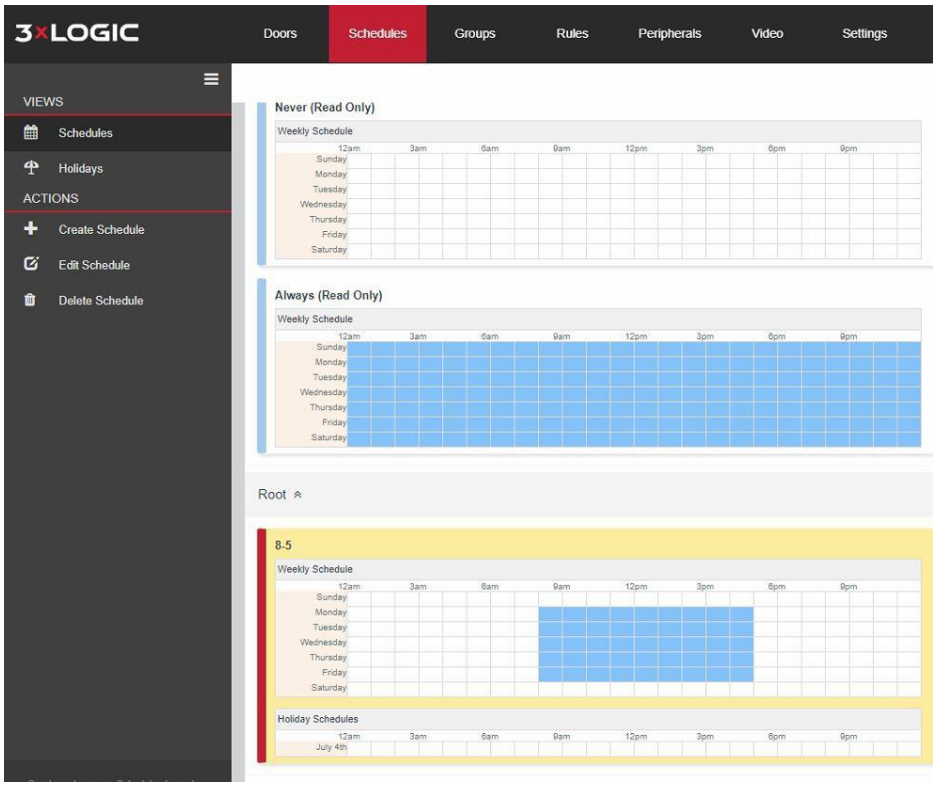


Figure 53: Schedules Tab

A blue-colored block of time represents an "Active" time block. For example, the **Always** Schedule has every minute of every day marked in blue. If this Schedule is applied to a door, the blue means the Door would be unlocked. For a Rule, blue means the Rule is allowed to execute. For a Person, blue means they will be granted access at that time block when they present their credentials.

The **Never** Schedule implies a Door that's locked 24/7, the Rule that would never run, or a Person that would never be granted access.

NOTE: The best way to memorize the behavior of schedules is to remember that blue is active and white is inactive. Thus, the Always Schedule is **ALWAYS** active, and the Never Schedule is **NEVER** active.

The Schedule page provides two Schedule views, which consists of **Schedules View** and **Holiday View**:

5.2.1 Schedules View

Schedules View displays the Schedules in a paged list, showing the first 100 Schedules. The usual paging icons are present for navigating to other pages of Schedules. Each Schedule is shown as a 7-day week, with each day as its own row. Each day row contains a 24-hour time range from midnight to 11:59:59 PM. As stated earlier, the blue areas denote the Active Time Range in the Schedule.

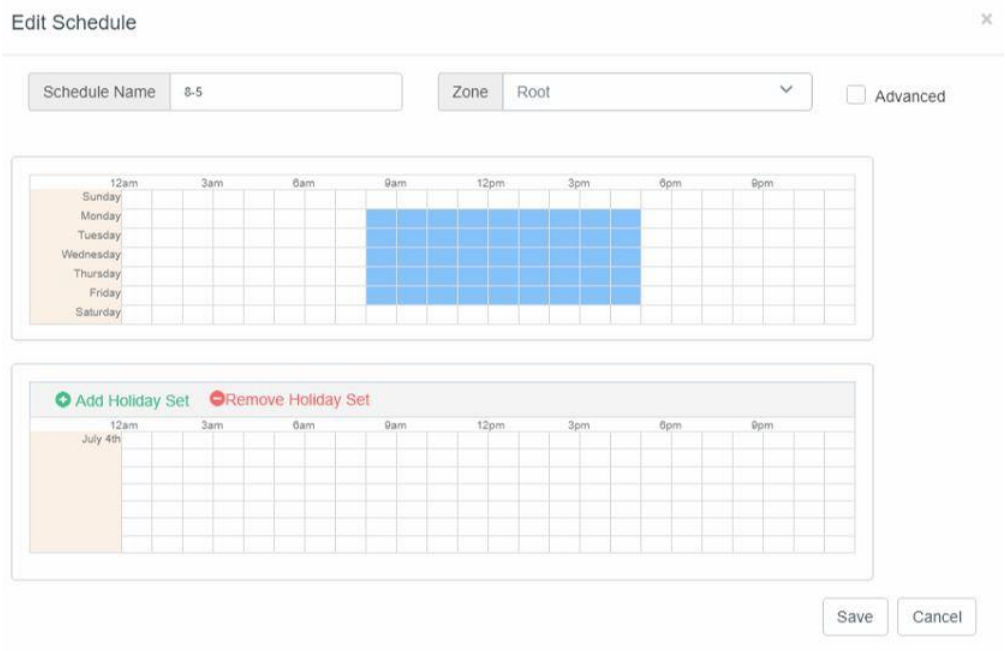


Figure 54: Schedules

5.2.2 Holidays View

Holidays View displays the Holiday Sets in a card format. Each Holiday Set shows the individual Holiday days that are contained in that Holiday Set.

5.2.3 Actions (Schedules View)

The Schedules View provides three Actions for managing Schedules, which consists of **Create Schedule**, **Edit Schedule**, and **Delete Schedule**.

5.2.3.1 Create Schedule

Steps:

1. Click the **Create Schedule** Action to create a new Schedule.
2. Choose a **Schedule Name**. Provide a name for the Schedule that is relevant to the type of Schedule you are creating. It's recommended to name the schedule the active time range, because a single schedule can be shared between Doors, Rules, and Access Privileges.
3. Create the **Active Time Range**. The Active Time Range is a contiguous block of time, shown in blue, which defines when the Schedule is Active. Users can drag the cursor up or down across rows to fill in blue color across more than one day at a time. To return a time range to white, click on the blue region you wish to modify and drag your cursor accordingly. You can also single-click on a time block to change it between blue and white. The smallest increment of a Schedule is 15 minutes. You can hover your cursor over a part of the Schedule to determine the exact time of day represented by that part of the Schedule. You can create multiple time ranges in a single day.

If you'd like more granularity with your schedule than 15-minute blocks, click the **Advanced** Box.

4. When you have finished configuring your Active Time Ranges, click the **Create** button to create your Schedule.

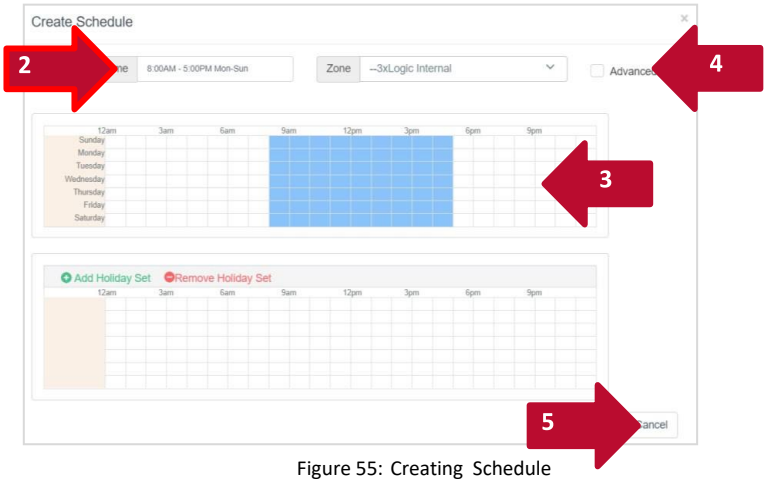


Figure 55: Creating Schedule

5.2.3.2 Edit Schedule

To modify a Schedule, click the **Edit Schedule** Action and change the Schedule Name, and/or modify the Active Time Range using the same operations described earlier. Click the **Save** button to save your changes.

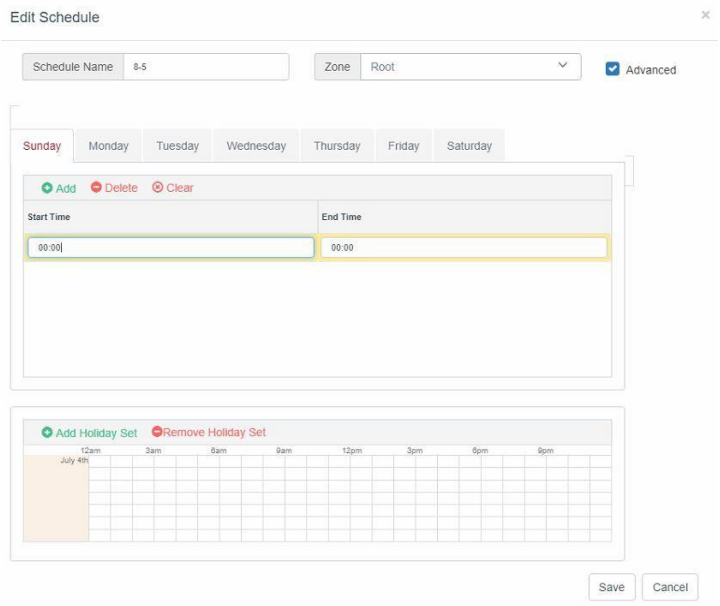


Figure 56: Editing a Schedule

5.2.3.3 Delete Schedule

If you no longer need a Schedule, you can remove it by clicking the ***Delete Schedule*** Action. A confirmation message box will appear, and the Schedule will be deleted when you confirm. You can only delete a schedule not in use by the software. If a behavior or rule is using the schedule, the delete option will not be allowed.

5.2.4 Actions (Holiday Set View)

The Holiday Set View provides three Actions for managing Holiday Sets, which consists of ***Create Holiday Set***, ***Edit Holiday Set***, and ***Delete Holiday Set***.

5.2.4.1 Create Holiday Set

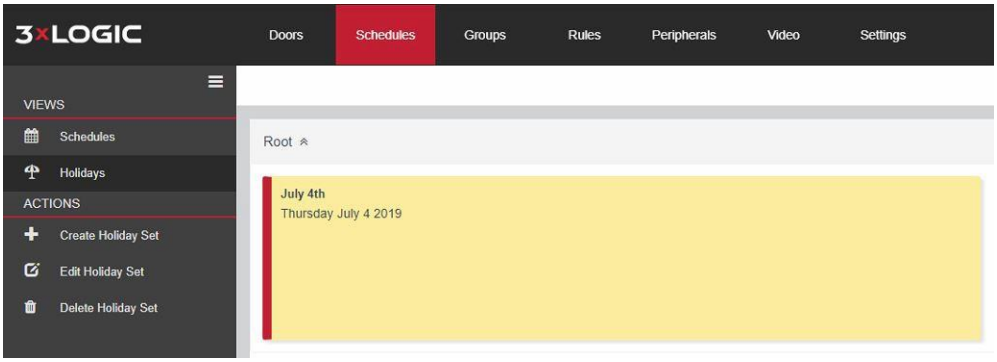


Figure 57: Holiday Set

Steps:

1. To add Holiday exceptions to your schedule, you must first create a Holiday Set to contain your list of Holidays. Click the Create Holiday Set Action, and a Create Holiday Set popup dialog will appear.
2. The dialog displays an entire year's worth of days, starting with the current year. You can press the arrows at the top of the chart to move forward and backward one year at a time. The purpose of a Holiday Set is to define a list of days whose who will share the same exception schedule behavior.
3. Apply a logical Holiday Set Name.
4. Assign the Holiday Set to a Zone within your Scope.
5. Choose your Holidays. To add a Holiday to the Set, simply click on a date shown in the year-long calendar. The date you clicked on will appear in a list of Holidays on the left pane.
6. Continue clicking on Holidays in the Create Holiday Set Dialog until you have chosen all Holidays whose Active time range for that day are identical, then press the Create button to create the Holiday Set.

NOTE: If you add one or more Holiday Sets to a Schedule, you should add that same Holiday Set to all Schedules. For example, if you apply a Holiday Set to a lock schedule for a Door, you'll also need to add that Holiday Set to the Schedule you used for cardholder access. Otherwise, when a holiday becomes the current day, the controller will not have a holiday schedule to use and, as a result, will deny access.

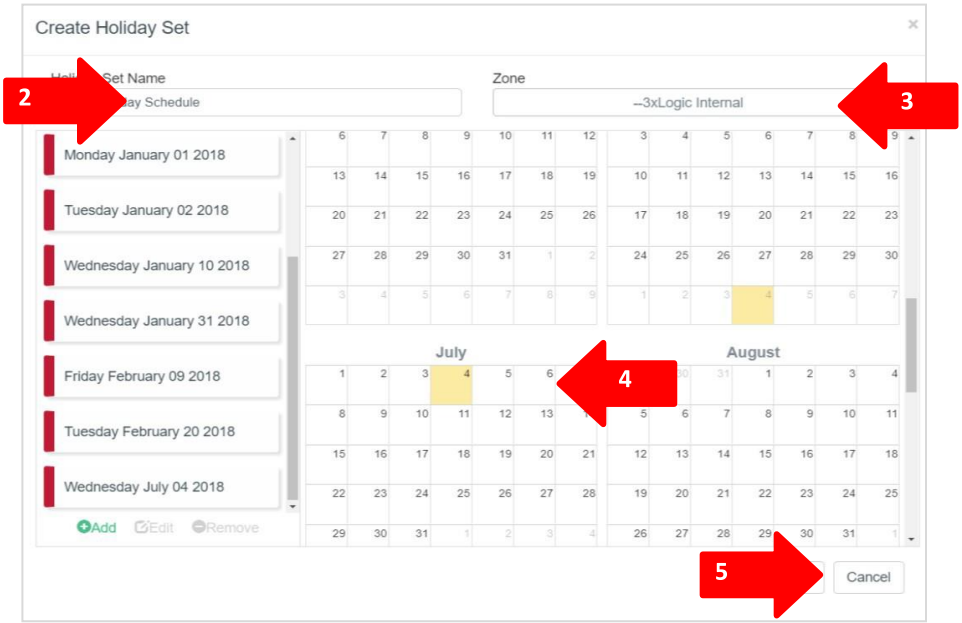


Figure 58: Add Holidays

5.2.4.2 Edit Holiday Set

To modify a Holiday Set, click the **Edit Holiday Set** Action. Click on dates in the calendar to add or remove Holidays to or from the Set, then click the **Edit** button to rename a Holiday or change its date. When finished, press the **Save** button to save your changes.

5.2.4.3 Delete Holiday Set

If you do not need a particular Holiday Set, you can remove it by pressing the **Delete Holiday Set** Action. A confirmation message box will appear, and the Holiday Set will be deleted after you confirm.

5.3 Groups Tab

The Groups Page in the configuration Section lets you create, modify or delete a Group, and add or remove People from a Group.

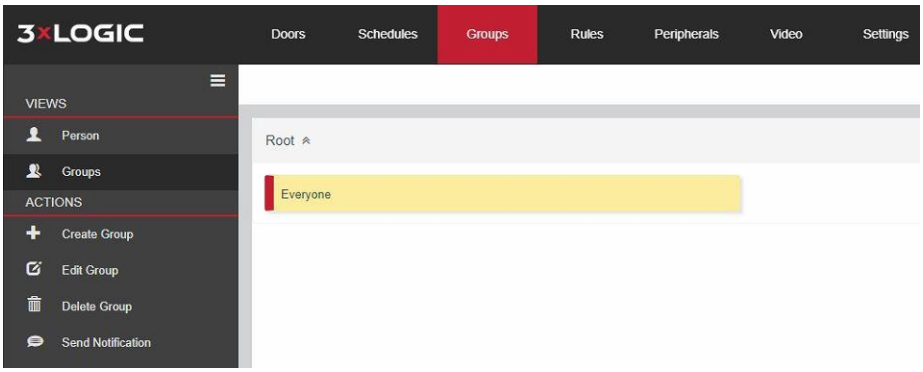


Figure 59: Groups

The person view has the same capabilities as the People Tab in the home section of the software. Please reference that section of the user guide for more information on the People tab.

5.3.1 Create Group

Creating a group is a simple operation of naming a group of people and adding those people previously added to the system via the People tab. Use the filter options on the page to find the people not in the group, find the people currently in the group, or list everyone. A built-in search option is there to filter to a specific person. Use the arrows to push people over to the group or remove from the group. Multiple people can be highlighted at once by holding the CTRL key on the keyboard and clicking any of the people in the list.

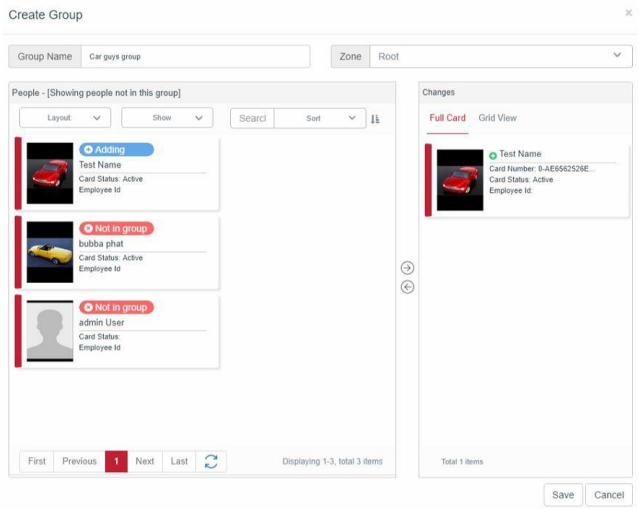


Figure 60: Create Group

5.3.2 Edit Group

Double click or highlight any group and click the edit group option to open the edit window for a group. Use the same controls from the create group to edit a group.

5.3.3 Delete Group

A group can only be deleted if it is not associated with any rules and is empty of people.

5.3.4 Send Notification

Notifications can be pushed to a group and even sent to those within a certain radius of a location by using the send notification feature. This will send a notification to those who have the site access or mobile credential app.

Figure 61: Send Notification

5.4 Rules Tab

The rules engine, the core part of the Intelli-M access software, is the biggest leap away from stereotypical access control software products. This makes it more difficult to understand to individuals in the field that have experience with other security software packages. However, once an understanding of how a rule functions and uses, the realization of how powerful the rules engine is starts to take shape.

The rules engine ties the rest of the sections this guide has been reviewing together. The access privilege rule is the most common rule that most sites will be utilizing to provide access privileges to the groups of people at a location or across multiple locations.

There are many rule types listed in the default rules list and many more that can be added or even customized by the support team to provide any number of ways to get the system to function the way a particular site requires for security purposes. The default rules range from the access privilege rule to unlock zone to lockdown zone rules. Most are self-explanatory.

For ease of explanation this guide will only review the access privilege rule creation. It is the most common and required for the system to be properly configured to let groups access specific doors on site.

There are two views on the rules page to list out the created rules. The first is the card view. As seen below it lists out the rules as easier to read cards. However, this is not able to be filter in any way other than the search filter in the upper right corner of the rules tab.

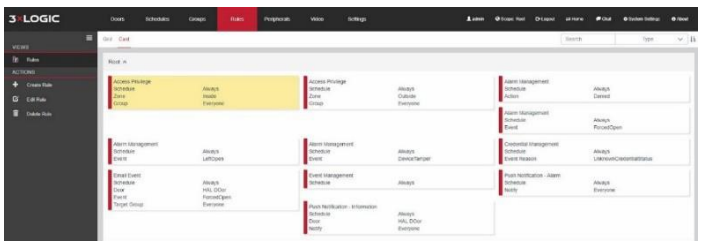


Figure 62: Rules - Cards view

The second view, grid, is a more familiar view to users and the page can be sorted by the column titles on the page.

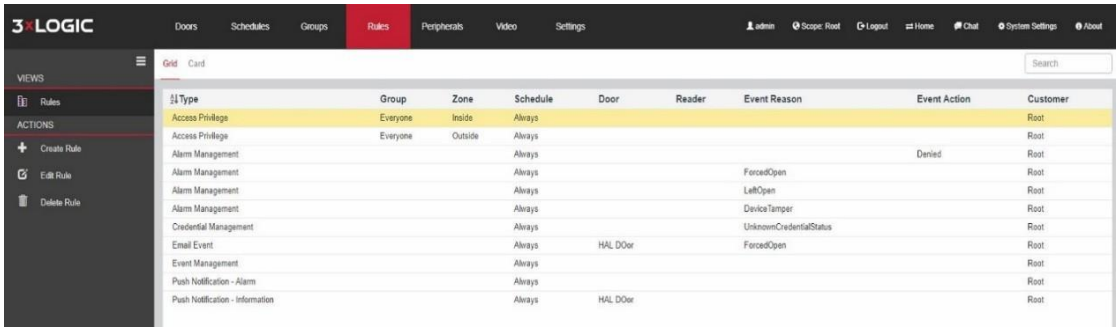


Figure 63: Rules - Grid View

5.4.1.1 Create Rule

In an Intelli-M Essentials and Professional environment, it is important to understand that the zone listed in the upper right when creating a rule should not require changing. If changed, this could lead to rules not working correctly or even disappearing from the UI if set improperly. Please contact support for questions pertaining to zoning or see the Corporate and Cloud sections for more information on advanced zoning trees.

The Access Privilege rule will always be the default rule when creating a rule. The list of rules is available in the drop-down menu at the top of the create rule. The page requirements will change based on the rule type being configured.

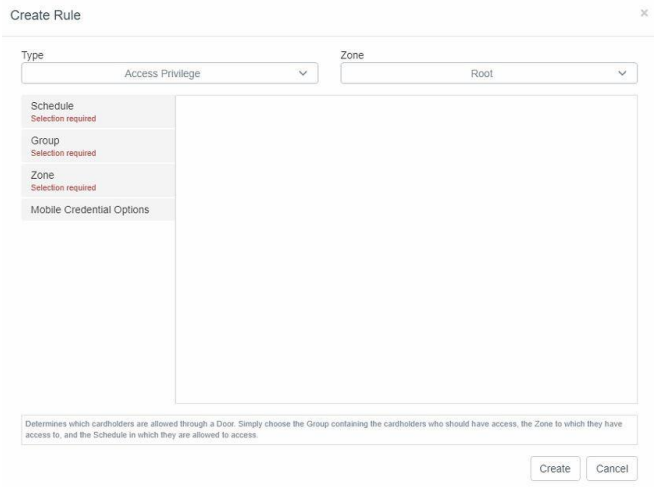


Figure 64: Create Rule

There are three primary things that make a rule work.

1. Schedule
    a. The time the rule will be active
    b. In the case of the access privilege rule, this will be when the group will be able to access the zone

2. Group
    a. The group of people being affected by the rule based on the schedule and tied to the zone
3. Zone
    a. The location the group is entering based on the schedule tied to the rule
    b. The zone is one or more doors. See the doors tab section for more information on how zones are used with doors

Once the rule is made, a group of people will be allowed to enter a zone based on the schedule they have been assigned. That could be 1 or 100 doors depending on how the doors were zoned in the previous steps.

Below is a breakdown of some of the most common rules.

5.4.2 Event Management

The Event Management Rule allows Admin users to select which Events will be visible in the Events Page. By default, all Events are made visible. You can reduce the number of Events that are visible on the Events page by using this Rule. Note that if you wish to filter out a single Event, you can alternatively use the Hide Event Rule described below.

Steps:

1. Select **Event Management** in the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which the Event will be visible on the Events Page. The Event will not be visible during the inactive time range (the "white" area) of the Schedule.
3. Select a **Group** (optional). This is an additional filter for the event trigger.
4. Select a **Zone** (optional). This is an additional filter for the event trigger.
5. Select an **Event** (optional). All Events you choose will be made visible provided the Event also meets the above criteria. If you do not specify an Event, then all Events that meet the above criteria will be made visible.
6. Select an **Action** *(optional).* An Action is another type of Event, and often covers multiple of the Events you see in the Event tab described above. All Actions you choose will be made visible provided the Action also meets the above criteria. If you do not specify an Action, then all Events that meet the above criteria will be made visible on the Events Page.

5.4.3 Hide Event

The Hide Event Rule could be considered the opposite of the Event Management Rule in that the Hide Event Rule ensures that a specific Event will *not* be made visible on the Events Page. This Rule is useful when you have only one or two Events that you wish to hide from the Events Page.

Steps:

1. Select **Hide Event** in the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which the Event will be hidden from the Events Page. The Event will not be hidden during the inactive time range (the "white" area) of the Schedule.
3. Select a **Group** (optional). This is an additional filter for the event trigger.
4. Select a **Zone** (optional). This is an additional filter for the event trigger.
5. Select an **Event** (optional). All Events chosen will be hidden, provided the Event also meets the above criteria. If you do not specify an Event, then all Events that meet the above criteria will be hidden.
6. Select an **Action** (optional). All Actions chosen will be hidden, provided the Action also meets the above criteria. If you do not specify an Action, then all Events that meet the above criteria will be hidden on the Events Page.

5.4.4 Alarm Management

The Alarm Management Rule turns any event into an Alarm. An alarm is indicated visually in the Events Page in Red. By default, Intelli-M Access creates five Alarm Management Rules to manage all the Access Denied event possibilities.

Steps:

1. To create a new Alarm Management Rule, select **Alarm Management** in the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which this Rule will be active. Events that satisfy this rule's criteria will be converted into Alarms only during the Active Time Range (blue) portion of the Schedule you select.
3. Select a **Group** (optional). This is an additional filter for the event trigger.
4. Select a **Zone** (optional). This is an additional filter for the event trigger.
5. Select an **Event** (optional). This is an additional filter for the event trigger.
6. Select an **Action** (optional). All Actions you choose will be converted to an Alarm, provided the Action also meets the criteria specified above. If you do not specify an Action, then all Events that meet the above criteria will be converted into anAlarm.

5.4.5 Credential Management

The Credential Management Rule handles any scenario where a cardholder should have access but they are denied. The most common example of this scenario is that the controller was offline during the credential download. This Rule will evaluate all 'Unknown Credential Status' errors and apply that cardholder to the controller if in fact that card number was supposed to be already present on the controller.

NOTE: This Rule will **not** download credentials that do not belong on the controller. You need only have one Credential Management Rule active on the System unless you desire different behaviors on different Schedules.

Steps:

1. Select **Credential Management** in the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which this Rule will be active. Events that satisfy this rule's criteria will be converted into Alarms only during the Active Time Range (blue) portion of the Schedule you select.
3. Select an **Event** (optional). All Events you choose will be used to evaluate the cardholder's access rights, provided the Event also meets the criteria specified above. If you do not specify an Event, then all Events that meet the above criteria will be evaluated (not recommended).

5.4.6 Events to Mobile

The Events to Mobile Rule can filter out which events that you want sent to your Site Access Mobile App.

Steps:

1. Select **Events to Mobile** in the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which the Event will be visible on the Events Page. The Event will not be visible during the inactive time range (the "white" area) of the Schedule.
3. Select a **Group** (optional). This is an additional filter for the event trigger.
4. Select a **Zone** (optional). This is an additional filter for the event trigger.
5. Select an **Event** (optional). All Events you choose will be made visible provided the Event also meets the above criteria. If you do not specify an Event, then all Events that meet the above criteria will be made visible.
6. Select an **Action** (optional). An Action is another type of Event, and often covers multiple of the Events you see in the Event tab described above. All Actions you choose will be made visible provided the Action also meets the above criteria. If you do not specify an Action, then all Events that meet the above criteria will be made visible on the Events Page.

5.4.7 Auto-Enrollment

Automatically enrolls a card upon swipe of a card not currently in the system. Simply choose the Reader designated for Enrollment, plus any desired Group membership. WARNING! Make sure this Rule runs ONLY on a Reader in a SECURED area! Delete this Rule when you no longer need automatic enrollment.

1. Select **Auto-Enrollment** the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which this Rule will be active. Events that satisfy this rule's criteria will be converted into Alarms only during the Active Time Range (blue) portion of the Schedule you select.
3. Select a **Reader** (optional). Whatever Reader that is selected will enroll cardholders when is scanned by an unknown credential.
4. **Group Membership** will allow you to enroll the cards to a specific Group of your choosing.

5.4.8 Email Event/ Email Event with Attachment

The **Email Event Rule** sends an email to one or more recipients based on the information you provide in this Rule. Additionally, the **Email Event with Attachment** Rule will include attachment of any camera associated with the event.

Note: The SMTP configuration settings are already programmed in infinias CLOUD. Your emails will come from noreply@3xlogic.com.

Steps:

1. Select **Email Event** in the Rule Type drop-down list box.
2. Select a **Schedule**. The Schedule determines the time range in which this Rule will be active. Events that satisfy this rule's criteria will generate an email to a list of selected recipients.
3. Select a **Group** (optional). This is an additional filter for the event trigger.
4. Select a **Zone** (optional). This is an additional filter for the event trigger.
5. Select a **Door** (optional). This is an additional filter for the event trigger.
6. Select an **Event** (optional). All Events you choose will be emailed to the recipient list, providing the Event also meets the criteria specified above. If you do not specify an Event, then all Events that meet the above criteria will be emailed to therecipients.
7. Select an **Action** (optional). All Actions you choose will be emailed to the recipient list, providing the Action also meets the criteria specified above. If you do not specify an Action, then all Actions that meet the above criteria will be emailed to therecipients.
8. Select a **Target Group**. Select at least one Group from the list. All members of the Group(s) you select will have emails sent to their Primary Email and Secondary Email accounts, as specified in their Person profile. Members of the Group(s) that do not have email addresses will not receive the emails.

This rule can also be used to send SMS messages for more urgency. To do this, instead of entering the user's e-mail address on the Person page, enter their SMS 'e-mail' address.

5.4.9 Lock Zone, Lockdown Zone, and Unlock Zone

The Lock Zone Rule will lock all Doors that border the Zone specified in the Rule. All Access Privileges continue to operate normally while the Zone's Doors are locked. The lock is *not* momentary - it is permanent until another action, such as Revert to Schedule or Unlock Zone, unlocks the Door. The **Lockdown Zone** Rule is similar, except that the Doors are in a lockdown mode that blocks all Access Privileges, i.e. no valid card or fob swipes or REX requests will be granted. The **Unlock Zone** Rule is likewise similar, except that it *unlocks* all Doors in the specified Zone(s), and the **Revert Zone** Rule is also similar, except that it reverts the Zone's Doors to their Scheduled lock state.

Steps:

1. To create one of these Rules, ensure that the desired Rule is selected in the drop- down list box.
2. Select a **Schedule**. The Schedule determines the time range in which this Rule will be active.
3. Select a **Group** (optional). This is an additional filter for the event trigger.
4. Select a **Zone** (optional). This is an additional filter for the event trigger.
5. Select a **Door** (optional). This is an additional filter for the event trigger.
6. Select a **Reader** (optional). This is an additional filter for the event trigger.
7. Select an **Event**. Choose one or more Events that will cause the Zone's Doors to be locked. The Doors will lock when the specified Event occurs and the above criteria is met.
8. Select a target zone. Select one or more zone whose doors will be locked when the qualifying event occurs and the above criteria met.

5.5 Peripherals Tab

The Peripherals Page in the Configuration Section lets you manage your Peripheral Devices for third-party integrations. The Peripheral will build a bridge between the infinias CLOUD software and the integrated third-party device.

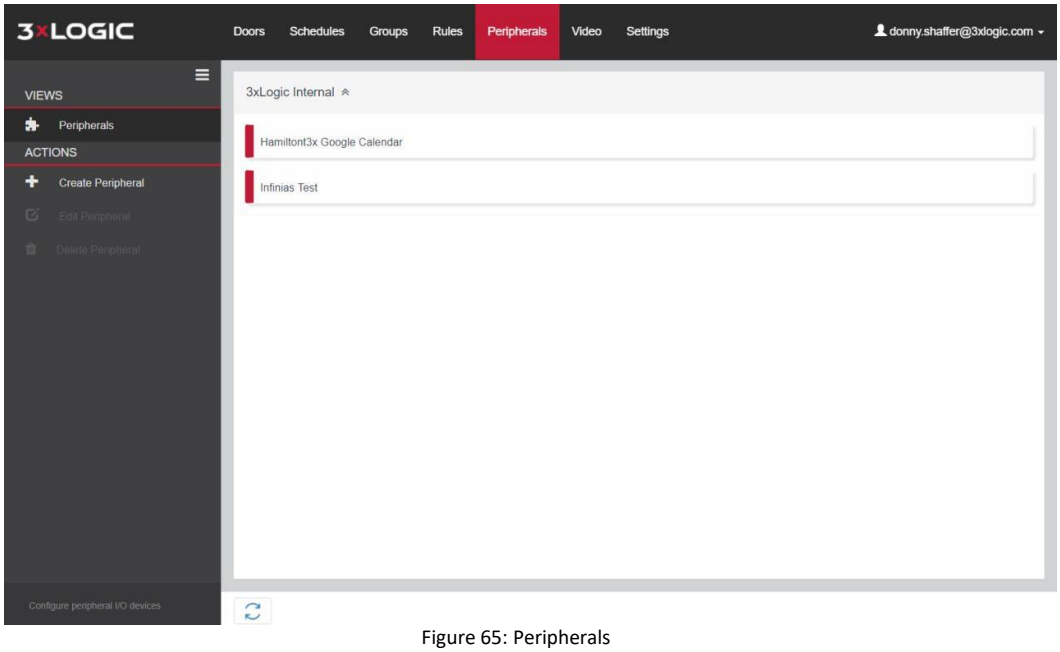


Figure 65: Peripherals

The purpose of a Peripheral is to provide Intelli-M Access with the ability to communicate with an external device, product, or service in a tightly-integrated manner. All Peripherals are third-party plugins that are managed by the infinias EAC Rule Action service.

5.5.1.1 Create Peripheral

To communicate with a third-party device or service, the user must create a Peripheral that knows how to communicate with that device or service.

Web Page:

The Web Page Peripheral allows a user to enter the URL of any web page, which can then be displayed in a web browser when a Rule is created to show that page. This Peripheral is commonly used to display live video of an IP video camera at the client browser. This feature can be used even if the IP camera is a part of a video management system. If the IP camera supports showing live video in a web browser, video can be displayed in a separate browser window when the Rule-defined Event occurs. For more information, please click here.

Generic Peripheral:

The Generic Peripheral is like the Web Page Peripheral, except that it is designed to call a *Web Service* rather than a *Web Server,* as is the case with the Web Page Peripheral. This Peripheral is intended for use by third-party integrators who wish to receive Events from infinias CLOUD into their proprietary application. The Forward Event Rule template is to create Rules that will send the Events to a specified third-party system to process however it wishes. For more information, please click here.

Google Calendar:

This allows users to create exception schedule by simply scheduling a meeting on a monitored Google account. For more information, please click here.

Exchange Calendar:

This allows users to create exception schedule by simply scheduling a meeting on a monitored Microsoft Exchange account.

5.5.1.2 Edit Peripheral

You can modify the Peripherals you have created using the **Edit Peripheral** Action. Make the necessary changes in the configuration user interface and press the **Save** button found at the bottom of the device configuration user interface.

5.5.1.3 Delete Peripheral

To remove a Peripheral, click the **Delete Peripheral** Action, and a confirmation message box will appear. The Peripheral will be deleted after you confirm

5.6 Video Tab

The Video Page in the Configuration Section allows for integration with any 3xLOGIC Video appliance. Within this section you can associate cameras from a VIGIL Server to a Door in intelli-M Access.

Configuration of the video integration requires access to the Vigil DVR/Stand-alone camera and the Intelli-M Access software. There are two options for the way the integration syncs to the DVR. One is using the Vigil Connect or Alias DNS connection and the other is a direct connection using the IP address and port information. Further information is outlined in the Video Integration guide linked below.

VIGIL+Video+and+
infinias+CLOUD+In

5.7 Settings Tab

The settings tab contains a multitude of different settings for the software. This section will review each sub menu and what it is used for in the software.

5.7.1 Registration

This section is not present in the Infinias Cloud and only exists in the local installation packages.

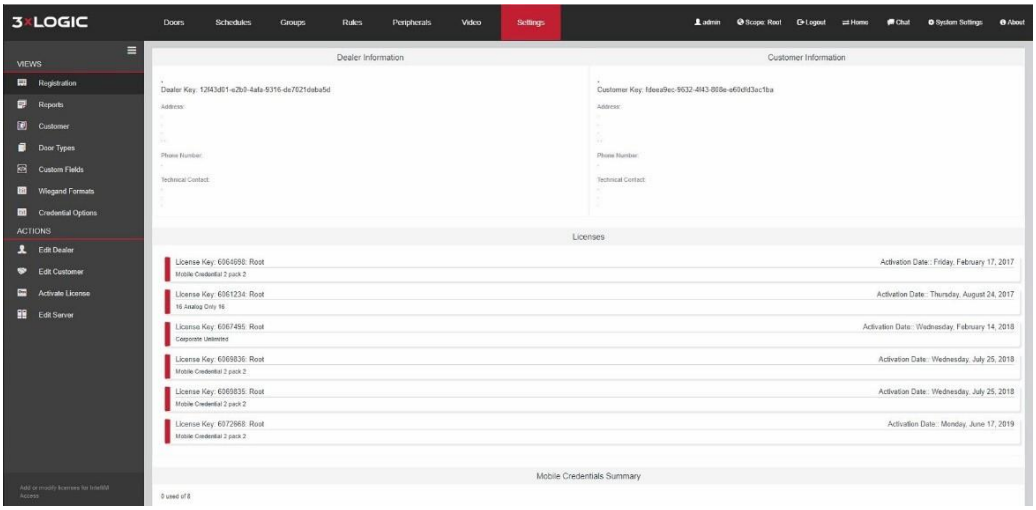


Figure 66: Registration

The section covers dealer, customer, and licensing activation of the Intelli-M Access software. The dealer and customer information must be filled out in order to license the software. The Activate license link will remain greyed out until those sections are complete.

The edit server action is used for upgrading doors to the hosted version that were previously set up as non-hosted. For further information on licensing and installation, please refer to the Intelli-M Access installation guide.

S-BASE-KIT_3x_GDE_
2019_0610.pdf

5.7.2 Reports

The reports view is one option for reviewing uploaded reports and activating the reports so they show up on the reports tab. Due to permission issues on software only installations, this option may cause an error if the system software is restricted.

Figure 67: Reports

5.7.3 Customer

This section is used for editing customer information and for additional licensing.

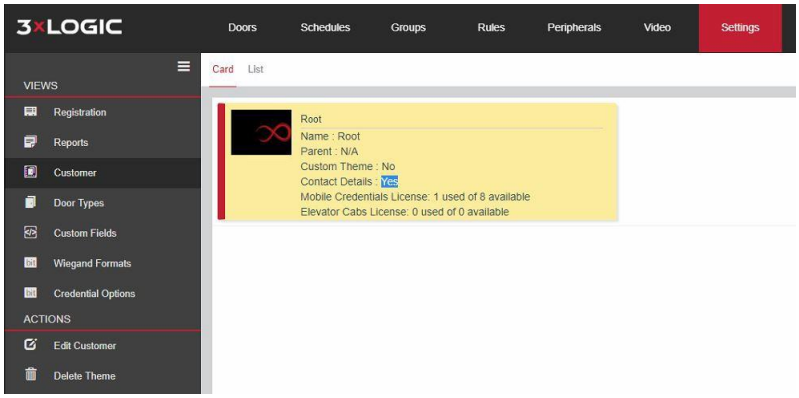


Figure 68: Customer Information

The name of the customer can be changed, which happens to be the name of the Root zone. Editing the customer will open up a new window dialog with additional options.

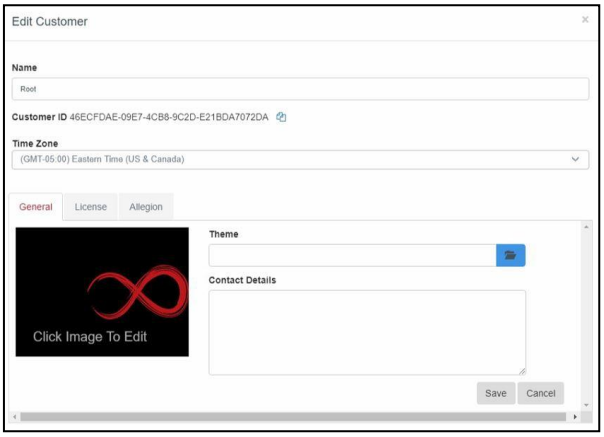


Figure 69: Edit Customer

Time zone, theme, and name can all be changed here on the general tab. Additional licenses can be added via the licensing tab.

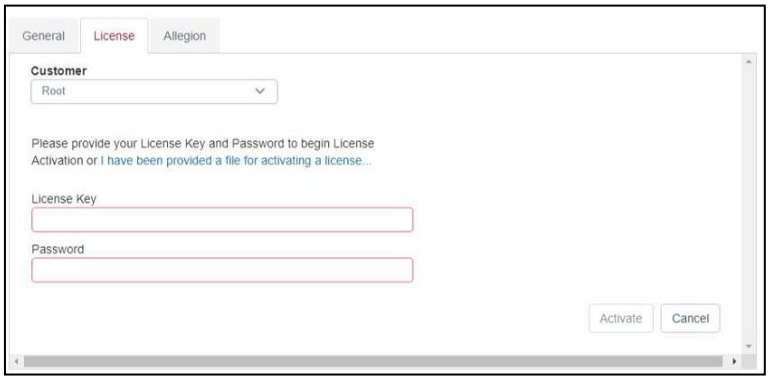


Figure 70: Edit Customer - License

Intelli-M version 6.x now integrates with Allegion wireless locks. The Allegion tab allows the addition of Allegion licensing.

Figure 71: Edit Customer - Allegion

For additional information on Allegion locksets and installation, please see the setup guide.

allegion_wireless_lock_quick_start_gui

5.7.4 Door Types

The door types page lists all active door types that will show up under the door types drop down menu when creating or editing a door. Further door types that are not active are listed under the edit door types action menu on this page. The door types are the configuration options that exist for the door controllers. Standard default and custom door types will all appear in this menu to be activated or deactivated from appearing in the selection menu.

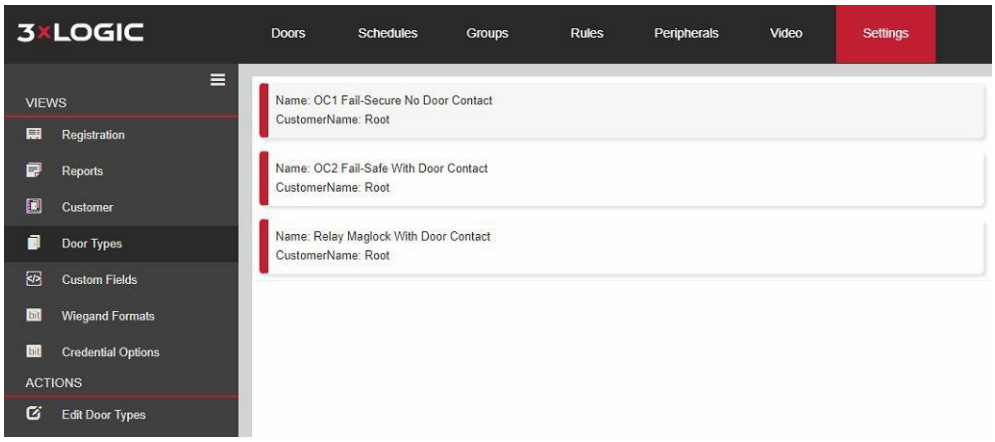


Figure 72: Door Types - Main

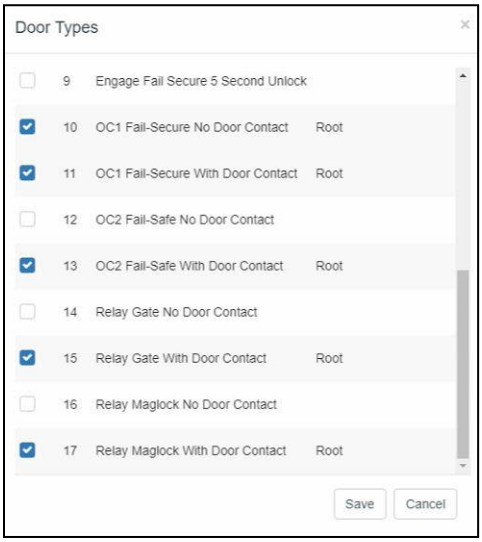


Figure 73: Door Types - Add

All standard default door types will have a configuration wiring diagram that can be viewed from the door edit page. All custom door types will not have a diagram.

5.7.5 Custom Fields

This section was initially reviewed when creating or editing a person under the people tab. Any custom fields generated on this page will appear under the custom field tab when editing or creating a person.

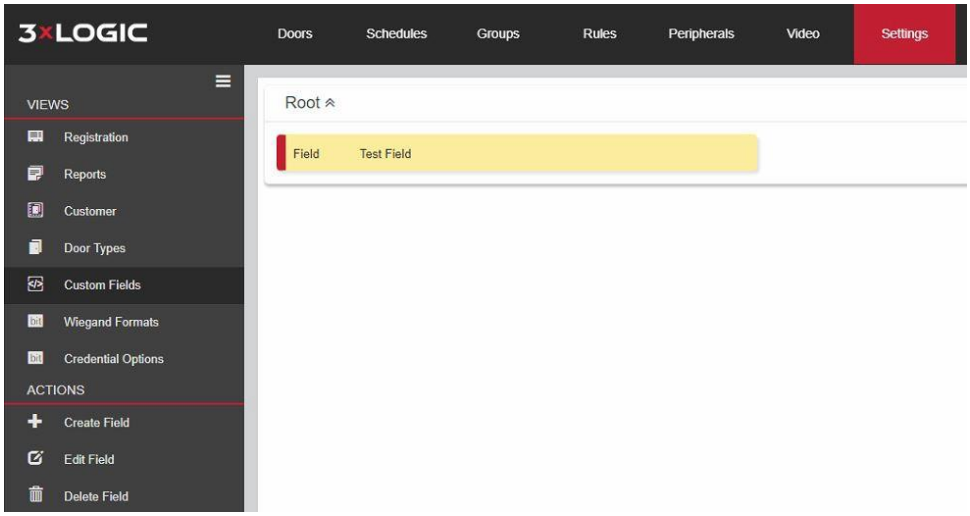


Figure 74: Custom Fields

5.7.6 Wiegand Formats

The Intelli-M Access and infinias Cloud have a multitude of addition Wiegand formats that can be supported ranging from 26 to 64 bit in length. It is important to understand that we cannot support any site code or card code bit length longer than 32 bits. Thus, a 64-bit format will be a 32-bit site code length and 32-bit card code length. That means we cannot support a 37-bit with a site code length of 0 and a 34-bit length card code.

The benefit is that the software supports many combinations of formats that many other software packages will not or do not support. We also support string formats used with PAC readers that allows an alphanumeric card code for additional security.

All active formats will be listed on the Wiegand formats page.

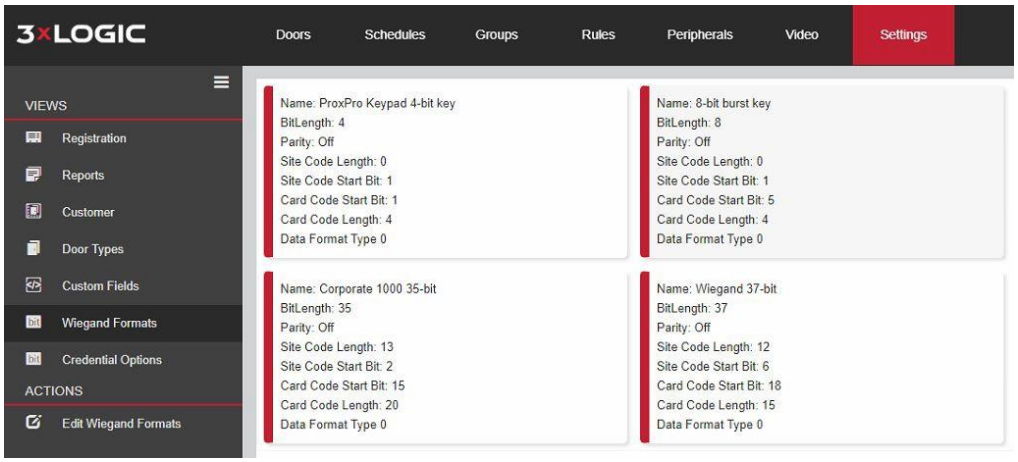


Figure 75: Wiegand Formats

No more than 8 active formats can be set at a time. This is a limitation of the door controller to store no more than 8 formats and not the software. Also, no two formats of the same bit length can be selected in the system.

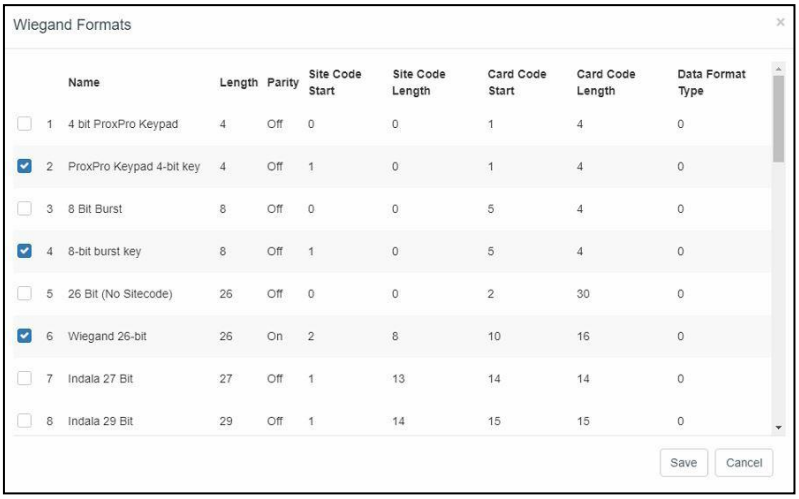


Figure 76: Enable Wiegand Formats

5.7.7 Credential Options

This section is for European compliance with String readers. Domestic customers will not likely change this setting. However, if the need arises this setting can be changed in order to make the string reader format the default instead of having to be manually set for every door behavior.

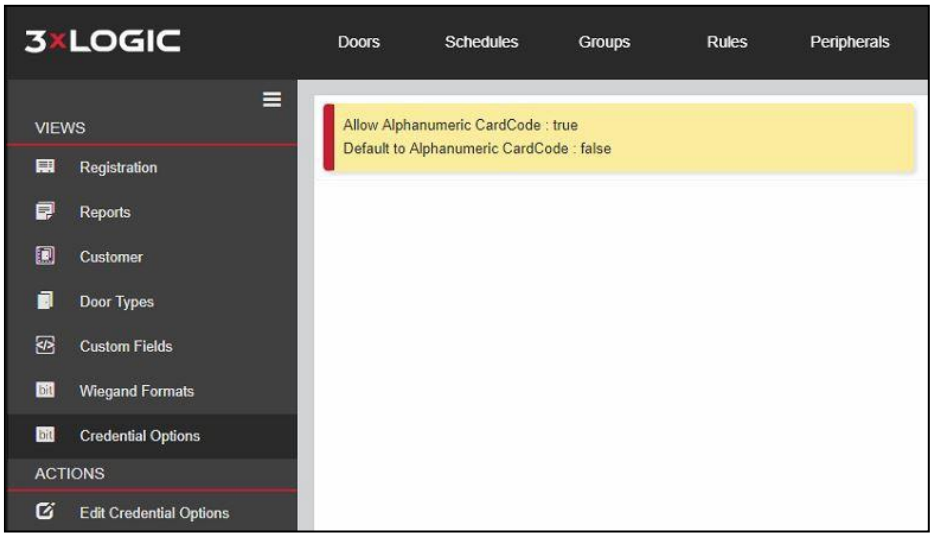


Figure 77: Credential Options

This concludes the Intelli-M Access Essentials configuration section of the user guide. The following sections will delve into the higher end software packages that require certification training in order to purchase and covering the integrations and features of what those packages provide over what the Intelli-M Access Essentials software does not.

3 Intelli-M Access Professional

The professional series software package is a license option that allows the use of advanced features. Professional series software requires the completion of a certification class prior to being able to purchase or utilize specific features or integrations that the software package supports. Intelli-M Access Professional opens the door to utilize Active Directory, Elevator Control, Outlook Exchange, and Google calendar integrations.

Active Directory integration

IA Pro can integrate with the Active Directory Server in your organization to allow the Active Directory Administrator to manage Intelli-M Access cardholders within the Active Directory User management system rather than within the Intelli-M Access User Interface. This integration provides the convenience of not having to learn and use yet another user management system on a daily basis.

Outlook Exchange integration

Intelli-M Access Professional can integrate with the Microsoft Exchange Server installed in your organization or in the cloud to allow Outlook Meetings or Appointments to automatically unlock and re-lock doors controlled by Intelli-M Access. This form of ad-hoc scheduling allows you to manage the lock status of a Door that doesn't operate on a predictable schedule like office or retail business hours. Sporting events, party reservations at public buildings or churches are typical examples of scenarios that Outlook Calendar integration can be useful. You can also apply ad-hoc Access Privileges to apply cardholders to a door based on your Outlook Meetings or Appointments.

Google Calendar integration

Intelli-MAccess Professional can integrate with Google Calendar to allow Google Calendar Appointments to automatically unlock and re-lock doors controlled by Intelli-MAccess.

Improved Elevator Control

Version 6 software introduced a new integration to the software that allows the management of elevators via the elevator tabs in the software. The tabs will appear after a license has been entered in the software. A new relay assembly was developed and released in tandem with the new software. This integration is available in Professional, Corporate, and Cloud versions.

- Pre-6.x software utilized the rules engine and a separate relay board driver that allowed a set of energize and deenergize rules to fire the relay board's outputs to the elevator control. Though this functioned well on smaller sites. The team determined that large installations required hundreds of rules all linked to the peripheral and if an issue required us to delete the peripheral, all linked rules would be deleted. This problem along with the separate driver that had to be maintained at the same version as the software along with filtering many rules caused the development team to take step back and evaluate how to best approach the problem.
- The new version 6 software eliminates the need for the separate driver installation, the peripheral requirement, and the rule requirements. Thus, simplifying the entire process.
- The older integration style is still supported so the older installations are still functional. It is highly recommended that existing sites, especially larger installations, take a look at potentially

replacing the older technology with the new to alleviate those previously mentioned configuration headaches.

- The one caveat is that every elevator car, no matter how few floors, requires a separate new generation relay board assembly. Each 1U rack mount assembly supports 16 floors with expansion 1U assemblies that will increase that by 16 up to 64 floors for one car. For large high rises, this process helps streamline the management process for the elevator cars.

3.1 Active Directory Integration

Unlike most Active Directory integrations, Intelli-M Access does not merely authenticate the provided credentials to Active Directory for a pass/fail result. Instead, it queries Active Directory for real-time changes to its user database and reflects those changes within the Intell-M Access database. The software continues to maintain the same user configuration and database that it had before the integration. However, it gets its updates from Active Directory rather than from the Intelli-M Access user interface.

The AD integration will manage all of the attributes associated with a person, including the person's group membership(s). Therefore, you can manage first name, last name, all contact information, employee ID, and even the card number associated with that person within AD's user management tools.

Although AD can modify Intelli-M Access' users and groups, that integration is one-way. At no time does Intelli-M Access modify AD with its own data, even if the UI is utilized in Intelli-M Access instead of AD, the path remains one way.

Note: It is recommended that no attempt to modify persons in Intelli-M Access once a link to AD has been established. Any changes made are likely to be overwritten by the next change made to the same user in AD. The exception to this is for multiple badges on a single person.

3.1.1 Integration Checklist

The Active Directory integration effort will require you to interface closely with the IT representative in your organization. Intelli-M Access will map AD attributes such as First Name, Last Name, Title, Department, Phone Number, Primary Email, and other important data points with the Intelli-M Access person. Many of these mappings are performed for you automatically, but some are not. The following is a complete list of all AD user attributes that are implicitly understood to map into Intelli-M Access.

Note: First Name and Last Name are not shown below because their mappings are hard-coded.

infinias Item	Active Directory Attribute
Title	personalTitle
Department	department
Company	company
Job Title	title
Phone Number	telephoneNumber
Cell Phone	mobile
Office	physicalDeliveryOfficeName
Primary Email	mail
Employee Id	employeeID
Notes	description

The Active Directory attributes are exactly what you see in the ***Active Directory Users and Computers*** administration utility on the Domain Controller. You can You can find a fairly exhaustive list of these attributes and their definitions at http://msdn.microsoft.com/en-us/library/ms675090(v=vs.85).aspx

You must enable ***Advanced Features*** in the ***Active Directory Users and Computers*** utility in order to see the attributes in the form you see in the table above. To enable Advanced Features, click the ***View*** menu and check the ***Advanced Features*** menu item. Once enabled, when viewing the Properties of any Active Directory object, an ***Attribute Editor*** tab will be visible among the numerous other tabs. The Attribute Editor tab contains all of the known attributes and their values, which you can modify directly if you wish.

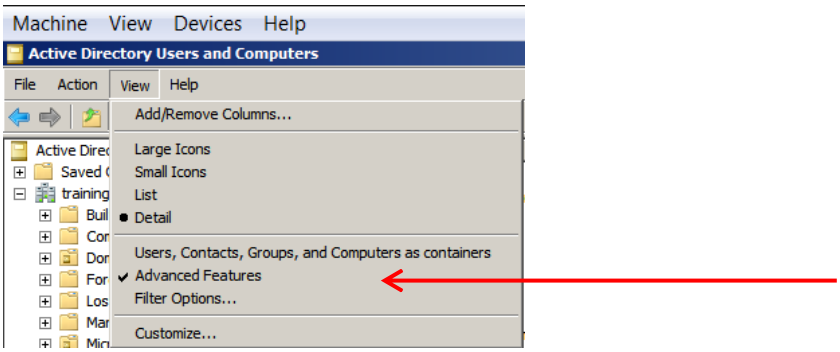


Figure 66: Active Directory - Advanced Features

In addition to the mappings above, you can map all of the remaining infinias Person items to Active Directory attributes. In all cases, coordinate these mappings with your IT representative to ensure that the proper attributes are being used for the mappings. Once you have decided which attributes to use, memorize or document the chosen attributes so you can later provide that information to Intelli-M Access.

3.1.2 Site Code and Card Code Number Attributes

Once you have the basic mappings of Active Directory attributes and infinias Person items completed, you must decide which Active Directory attributes are to be mapped to represent the Person's Site Code and Card Number. infinias requires a valid Site Code and Card Number in order to create a Person, so you cannot skip this step.

Unlike the table above, there is no obvious mapping for these items so you must work with the IT representative to decide which Active Directory attributes will be reserved to represent the Site Code and Card Number. Optionally, you can also create custom Active Directory attributes, but this is not required. By default, IA Pro maps the Site Code to the Windows User's ***Fax Number*** and maps the Card Number to the Windows User's ***Pager Number***. Windows User's typically do not have their own private FAX number, and also typically do not carry pagers in the smartphone world in which we live - therefore, these fields are usually no longer in use. If your IT representative approves of reserving these two fields in Active Directory for the Site Code and Card Number, then you need to do nothing more as the software will automatically map these attributes for you.

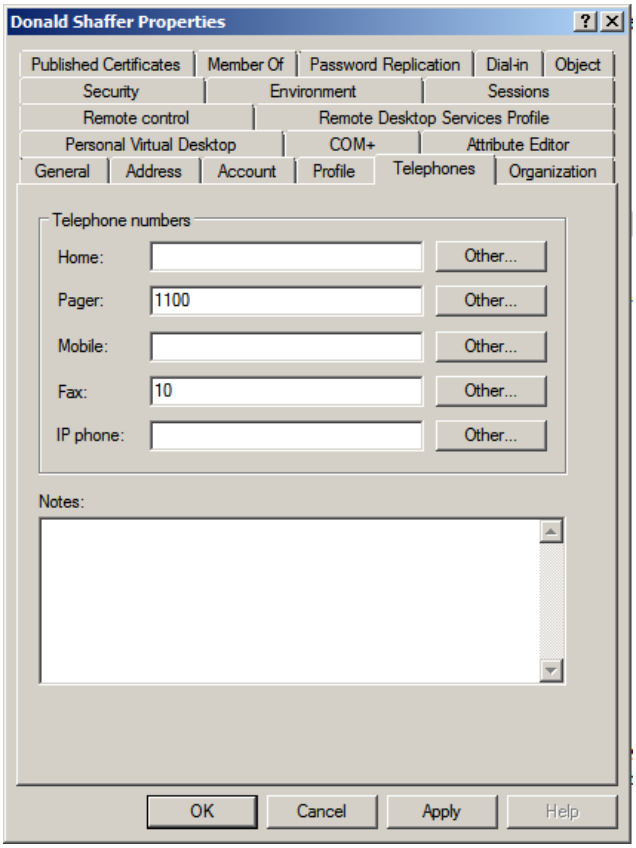


Figure 78: Active Directory - Site Code/Card Number

3.1.3 PIN Code Attribute

You can also optionally reserve an Active Directory attribute to be used as the PIN code for the user. Just repeat the steps described above for choosing the attribute and memorize or document the choice.

3.1.4 Group Filter Attribute

Active Directory contains numerous Groups that are not only of no value to Intelli-M Access, but also clutter up the infinias Groups page with numerous unnecessary Group names. Groups such as ***DHCP Administrators***, ***DnsAdmins***, ***Allowed RODC Password Replication Group***, and so on are examples of Groups that Active Directory needs but infinias does not. Therefore, infinias allows for filtering unwanted Groups from being copied from Active Directory.

infinias maintains a ***Group Filter*** that reserves an Active Directory attribute to be used to represent a Group that infinias needs. By default, infinias reserves the ***wWWHomePage*** attribute, which is an attribute for Windows Domain Groups. By setting the value at wWWHomePage to ***infinias,*** you are telling infinias that this Group belongs in Intelli-M Access. As with Site Code and Card Number, you must work with the IT representative to determine which Group attribute may be reserved for this purpose.

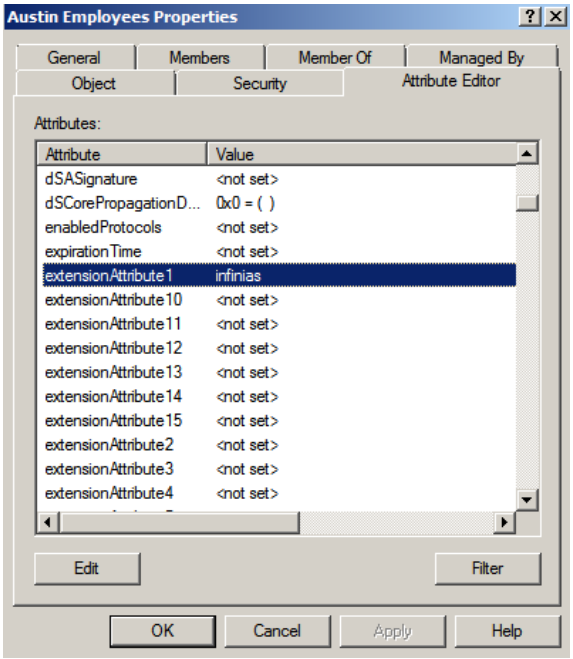


Figure 79: Active Directory - Group Properties

All Groups that do not have the infinias value set for the specified attribute, will not be copied to infinias.

NOTE: It is strongly recommended that you first complete this checklist and make the necessary changes within Active Directory before moving to the next section in this document. This includes setting the Group Filter attribute and updating all relevant Windows Users with their appropriate Site Code and Card Number.

3.1.5 Create a Peripheral

Login to infinias and proceed to the Peripherals Page under the Configuration Section. Click the **Create Peripheral** Action and a Create Peripheral Dialog will appear.

1. Select the ActiveDirectory Connection.

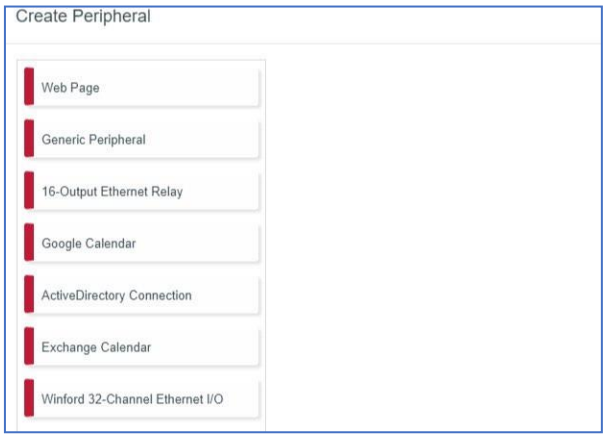


Figure 80: Active Directory - Create Peripheral

This will launch a configuration page allowing the user to apply the mapping between the fields that describe a Person in the infinias (the labels on the left side of the UI) and Active Directory Attributes (the text fields on the right side of the UI). The Active Directory Attribute names must be spelled exactly and are case-sensitive.

Most of the remaining mappings are created for you by default using the obvious choices, such as email for the Primary Email Address. Simply map the remaining fields that are important to you.

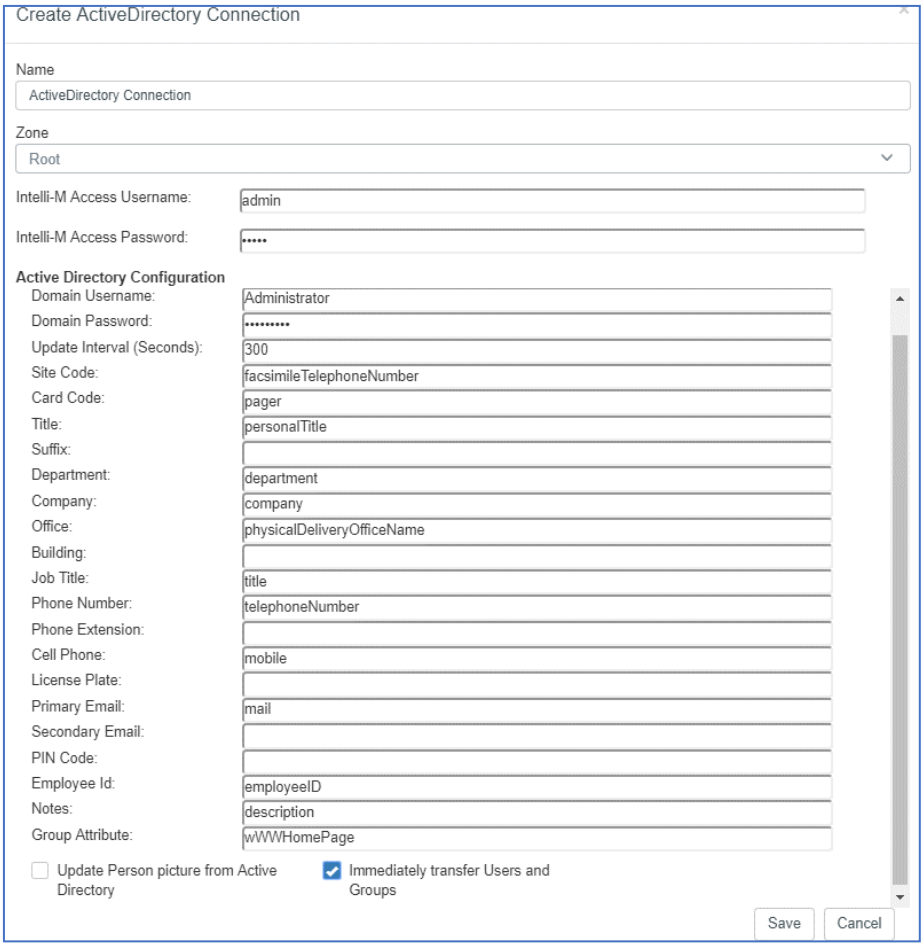


Figure 81: Active Directory - Field Mapping

2. When completed the mapping, click the **Immediately transfer Users and Groups** box and then press the **Save** button. The window will update to show a progress indicator while infinias connects to the Active Directory server using the supplied information.

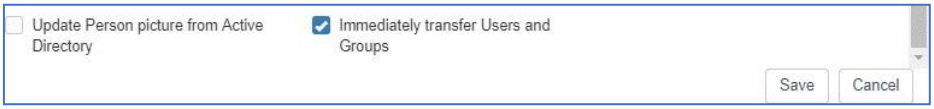


Figure 82: Active Directory - Transfer

The system will then connect to the Domain Controller and start listening for changes to the Windows Users and Groups. If you checked the **Immediately Transfer Users and Groups** checkbox, it will also start the process of downloading all appropriate Users and Groups to Intelli-M Access. This download process will run in the background as it may take several minutes or hours to complete.

Upon completion, an Information Dialog box will display with a notification that the Peripheral has been saved.

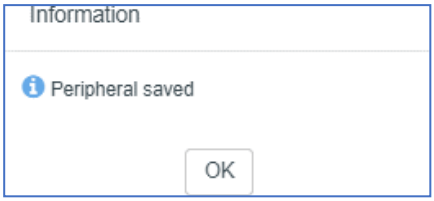


Figure 83: Active Directory - Finished

Option	Definition
Name	Provide a logical name
Zone	Assign to a specific Zone. Most people will assign to the **Root** Zone, which will apply to all locations in a Corporate configuration.
Intelli-M Access User/Pass	Use an Administrator User Account.
Domain	Enter the part of your Exchange email address that's on the right side of the '@' character.
Domain Username/ Password	Enter a valid Domain Username and Password.
Update Interval (Seconds)	Users can set the polling interval for how often infinias will download all changes from Active Directory.
Site Code	Provide an unused Active Directory Attribute that you wish to re- use and map to the Site Code (aka Facility Code) of the User's card number.
Card Code	Provide an unused Active Directory Attribute that you wish to re- use and map to the User's Card Code (Card Number).
Title	Provide the Active Directory Attribute that you wish to map to the User's name prefix (e.g. Mr., Mrs., Miss, etc). The **personalTitle** Attribute is used by default.
Suffix	Provide the Active Directory Attribute that you wish to map to the User's name suffix (e.g. Jr., Esq., etc). No default Attribute is provided.
Department	Provide the Active Directory Attribute that you wish to map to the User's company department membership. The **department** Attribute is used by default.
Company	Provide the Active Directory Attribute that you wish to map to the company at which the User is employed. The *company* Attribute is used by default.
Office	Provide the Active Directory Attribute that you wish to map to the office in which the User is employed. The **physicalDeliveryOfficeName** Attribute is used by default.

Building	Provide the Active Directory Attribute that you wish to map to the building in which the User is located. There is no default Attribute
Job Title	Provide the Active Directory Attribute that you wish to map to the User's job title. In Intelli-M Access, the Job Title is referred to as the Position. The ***title*** Attribute is used by default.
Phone Number	Provide the Active Directory Attribute that you wish to map to the User's office phone number. The **telephoneNumber** Attribute is used by default.
Phone Extension	Provide the Active Directory Attribute that you wish to User's telephone extension, if it exists. There is no default Attribute
Cell Phone	Provide the Active Directory Attribute that you wish to map to the User's cell phone number. The **mobile** Attribute is used by default.
License Plate	Provide the Active Directory Attribute that you wish to User's automobile license plate. There is no default Attribute
Primary Email	Provide the Active Directory Attribute that you wish to map to the User's work email address. The **email** Attribute is used by default.
Secondary Email	Provide the Active Directory Attribute that you wish to User's personal or secondary email address, if it exists. There is no default Attribute
PIN Code	Provide an unused Active Directory Attribute that you wish to re- use and map to the Site Code (aka Facility Code) of the User's card number.
Employee Id	Provide the Active Directory Attribute that you wish to map to the User's employee ID, if it exists. The **employeeID** Attribute is used by default.
Notes	Provide the Active Directory Attribute that you wish to map to any notes written by the Administrator about the User's account. The **description** Attribute is used by default.

Group Attribute	The Group Attribute lets you specify which Active Directory Groups should be transferred to infinias and which ones should not. Every Group in Active Directory must be given the value of **infinias** within the desired attribute.
Update Person picture from Active Directory	This will pull images associated with people, stored in Active Directory.
Immediate Transfer Users and Groups	This checkbox will connect to Active Directory and request its entire database of Groups and Users, transferring the information into Intelli-M Access.

3.2 Elevator Control

This section covers the new elevator control setup and configuration. The previous generation of elevator control, though still supported, is not covered in the new user guide. For support on the previous generation elevator control, please contact the support team.

Note: The previous generation of elevator control is discontinued and will eventually not be supported as the drivers will not be developed for the older generation relay board for the purpose of elevator control. Any new relay board purchases for elevator control will be based on the new generation relay assembly as described in this guide.

3.2.1 Elevator Setup

The first and most difficult step will be getting the relay board synced to the system. The only option for this is using the eIDC32 (Hosted) device when creating a door in the doors tab. However, if the site was pre-existing and has non-hosted eIDC32s or older configured on the site, the site will require the installer find out the system information, IP address, and network configuration to ensure the eIDC32 built in the relay assembly can sync to the system. Please see the **Configuration of a hosted door** guide in order to properly setup the device for the system linked below.

Note: Make certain the specific door type for the elevator is selected. The base unit gets the 16-channel door type. If this is not selected, the elevator control will fail to operate correctly.

Configuring a hosted door.pdf

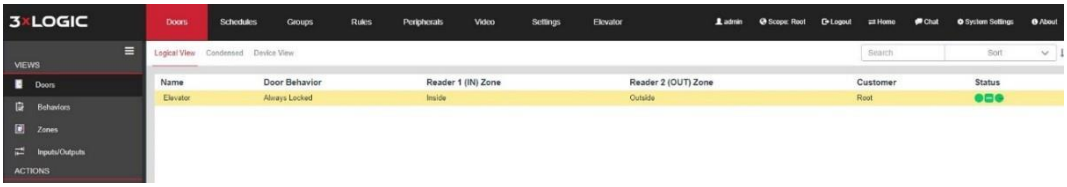


Figure 84: Elevator Setup

Now that the door is online, configuration can continue. Head over to the settings tab under configuration and register the elevator license provided when purchased the relay assembly. Once that is completed, refresh the page and the new **Elevator Tab** will appear in two places. The configuration section will have an elevator tab and the home page will have an elevator tab. They are used for different purposes and this guide will review both.

3.2.2 Elevator Tab – Elevator Banks - Configuration

Navigate to the elevator tab and the default view will be Elevator Banks.

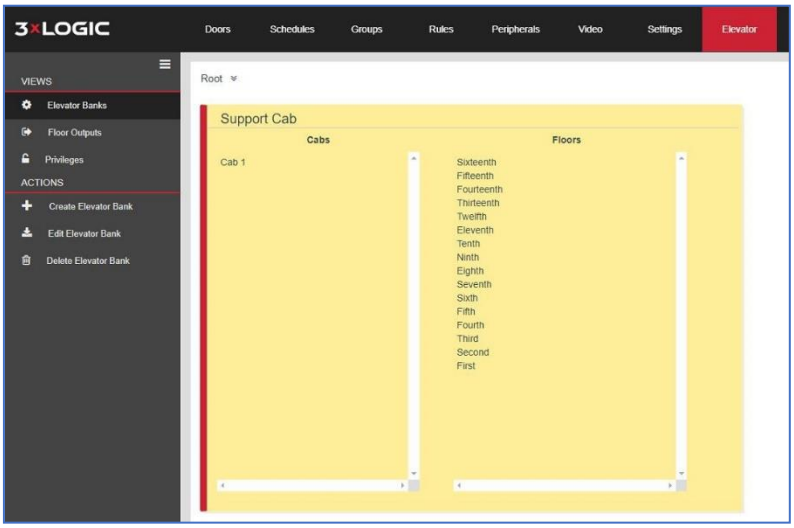


Figure 85: Elevator Banks

The page will be blank when a new cab is created. Click **Create Elevator Bank** under the action menu to the left and a new window will appear.

Enter the name of the cab. For local systems, the zone will say **Root. F**or the cloud it will be the specific customer zone. Under the **Cabs** tab within the window, click **Add** and a name and door

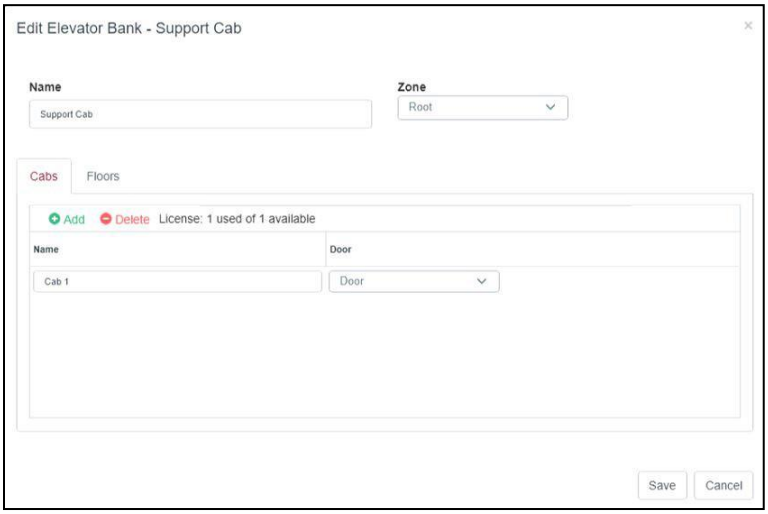


Figure 86: Create Elevator Bank

option will appear. You will also notice the licensing is listed here to allow a quick determination of how many licenses exist for this customer or installation.

Enter a name for the elevator cab. The drop-down menu will list the doors. Find the elevator door cab and select it. One of the licenses will be used for each door. Remember that each door is one elevator relay assembly wired to the elevator control.

Click on the **Floors** tab and add the floors for the site. The floors are limited to 16 unless an expansion board assembly was purchased to go beyond 16 floors.

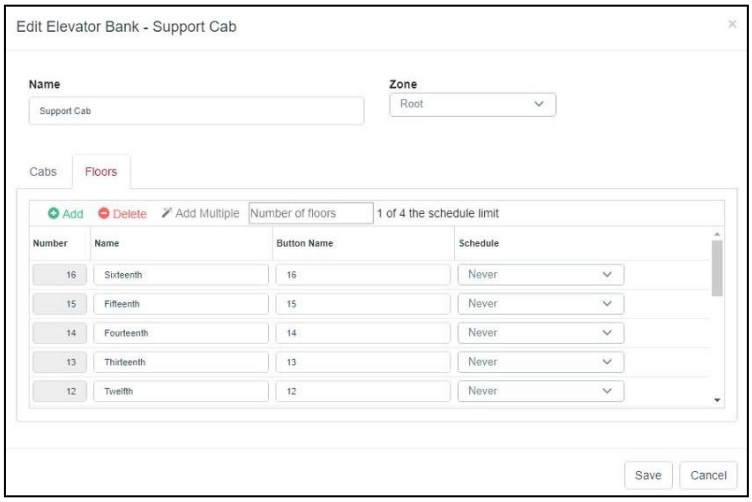


Figure 87: Elevator Bank - Floors

Multiple floors can be added at the same time by putting in the number of floors wanting to be added and clicking the **Add Multiple** button next to delete. The floor names can be entered for how they appear in the software and the button name can be modified to match the button in the elevator cab. The schedule drop-down will list every schedule programed in the system for selection. When finished, save the selections or changes.

NOTE: Only four different schedules can be utilized on a cab at a time for the different floors.

3.2.3 Elevator Tab – Floor Outputs –Configuration

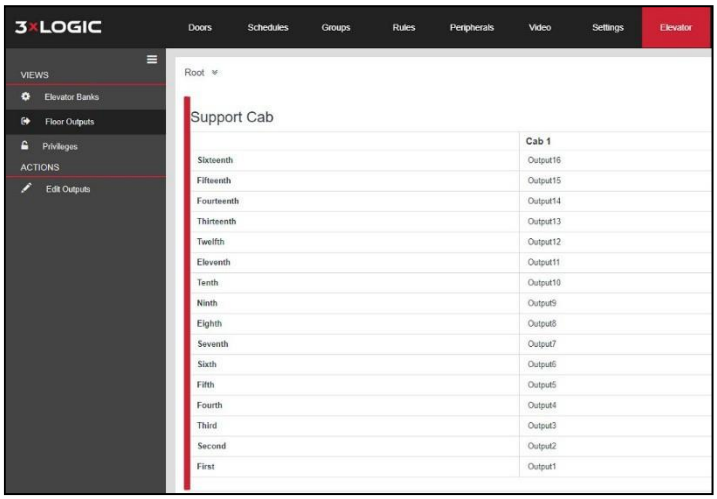


Figure 88: Elevator - Floor Outputs

The floor outputs are where the floors are tied to the relay outputs. Only one floor can be tied to an output. In the case of an elevator with dual doors, it will be up to the elevator control system to manage which door opens. The support team will be happy to assist with questions pertaining to custom setups such as those.

3.2.4 Elevator Tab – Privileges –Configuration

The privileges view is where the group is tied to the floors. By default, no group has any privileges to any floor. By clicking the group drop down menu, the group selection is being made for the checked floors.

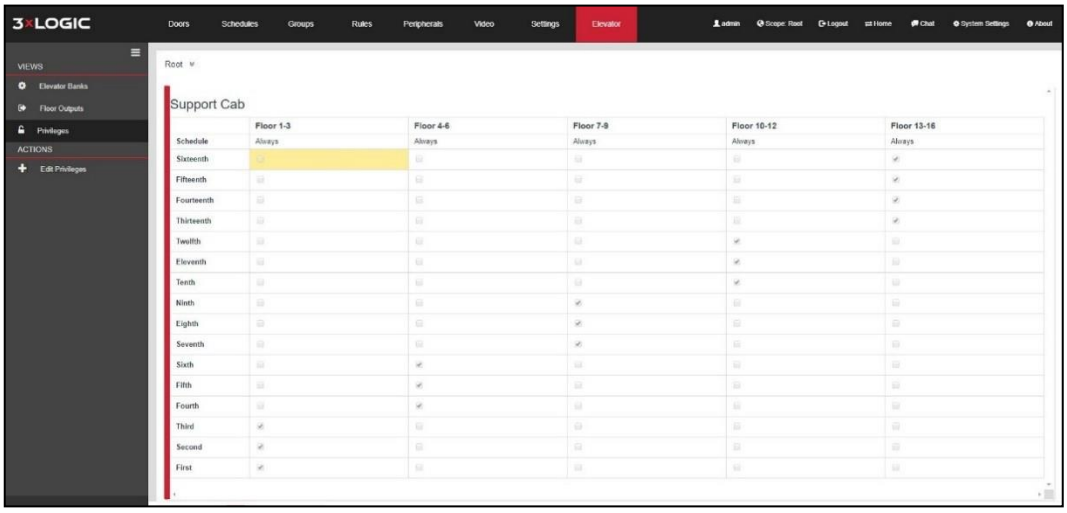


Figure 89: Elevator - Privileges

There is no create privileges action on this page. Just the cab names to edit.

Click save once all floor selections for a particular group have been added. The existing group will be edited or if selecting a new group not currently part of the list, it will be added.

Figure 90: Elevator - Edit Privileges

This finalizes the configuration steps of the elevator control. Testing should be completed for all groups and floor functionality.

3.2.5 Elevator Tab – Override –Home

The home tab contains an elevator tab that is used just for overriding an elevator's floor schedule. If an emergency comes up that requires the floor to have free access, the schedule can be overridden with a slider similar to what a smart device would have in it.

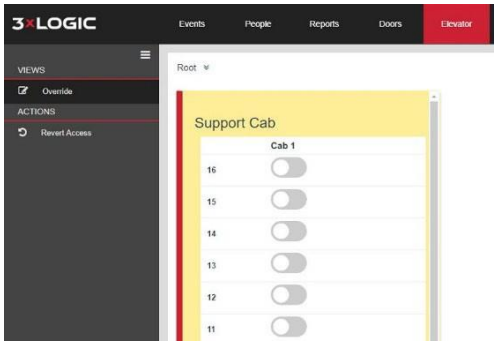


Figure 91: Elevator - Override

It is important to understand that the slider changes the state of the relay. That means if the elevator floor was locked out, access will be given. If the elevator floor was giving access, then access will be denied. Credentials for groups set to the floor will still be honored by the software. Only a lockdown zone can prevent card swipes for existing groups tied to the floor.

3.3 Google Calendar Integration

The Google calendar integration requires an active Google account. That account is linked to the Intelli-M Access software via settings in the Google calendar and a peripheral created and configured in Intelli-M Access. A separate user guide has been linked below that gives a step-by-step walk through for the calendar integration setup.

How To -
Integrating with Go

3.4 Outlook Integration

The Outlook Integration is similar to the Google Calendar integration in it lets a calendar schedule send events to the Intelli-M Access software to trigger unlock, lock, and revert zone rules for meetings and special occasions that cannot easily be met by other features of the software.

Below is a linked setup guide. The guide is dated. We are working to update it in the near future.

Outlook Exchange
Integration.pdf

4 Intelli-M Access Corporate and Cloud

Corporate and Cloud packages are very similar in performance and what features they support. As the guide progresses additional features are added as the different flavors of Intelli-M Access are reviewed. Corporate and Cloud are being combined into one section as their differences are so few that it would be redundant to go over them.

4.1 Intelli-M Access Corporate

The big difference between Corporate and Cloud versions is that Corporate is not multi-tenant capable. It has no capability to differentiate between specific customers. As the name suggests, Corporate is designed to work with a corporation where multiple facilities require a centralized location that can manage all the locations and yet still segregate the locations to prevent management groups from interacting with settings that would affect other locations. All the integrations and other features are support from the other flavors of Intelli-M Access.

4.2 infinias Cloud

infinias Cloud is a multi-tenant designed software that resides on the web. It is accessible from anywhere where internet access is and from any device that has the capability to browse the web. It allows an installer to manage and bill their customers to maintain their accounts and service the on-site hardware. It is designed for new installations where a customer is more interested in accessing the UI from anywhere without having to deal with the hardware maintenance other than the door hardware. infinias Cloud supports every feature the other software packages support other than the active directory integration.

4.3 Zoning Tree

What links Corporate and Cloud together yet separates them from Essentials and Professional packages is the zoning tree hierarchy.

In the instance of a customer that will need multi-site or multi-location management, there will be a need to identify the Parent \ Child relationship between Zones.

Note: It's recommended that customers with multi-site or multi-location management should apply a unique prefix (company name and location, or store number) for every Zone, Door, and Group.

Example:

- 3xMIA Front Door
- 3xIND Front Door
- 3xSEA Front Door

When Creating a Zone infinias CLOUD, users will now have a new option called **Parent Zone Name**. Therefore, users can create a Parent Zone which could be a region, state, company name, or anything you desire; then assign Child Zones to their respective Parent Zone.

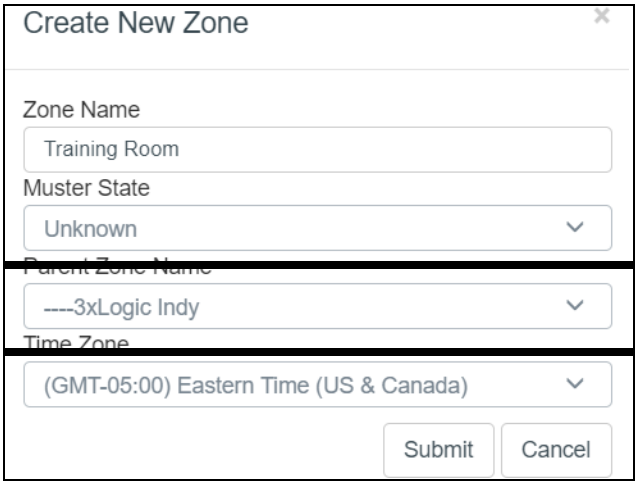


Figure 92: Create New Zone

4.3.1 Diagram Example of ZoneHierarchy

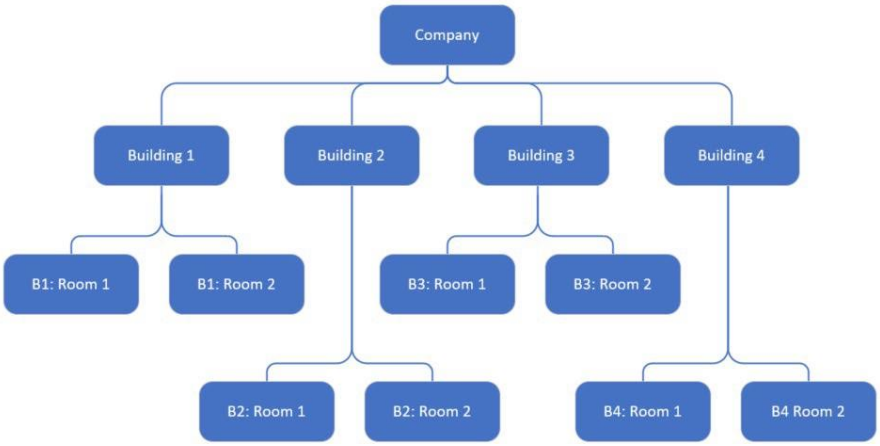


Figure 93: Zones - Diagram

4.3.2 Tree List Example of Zone Hierarchy

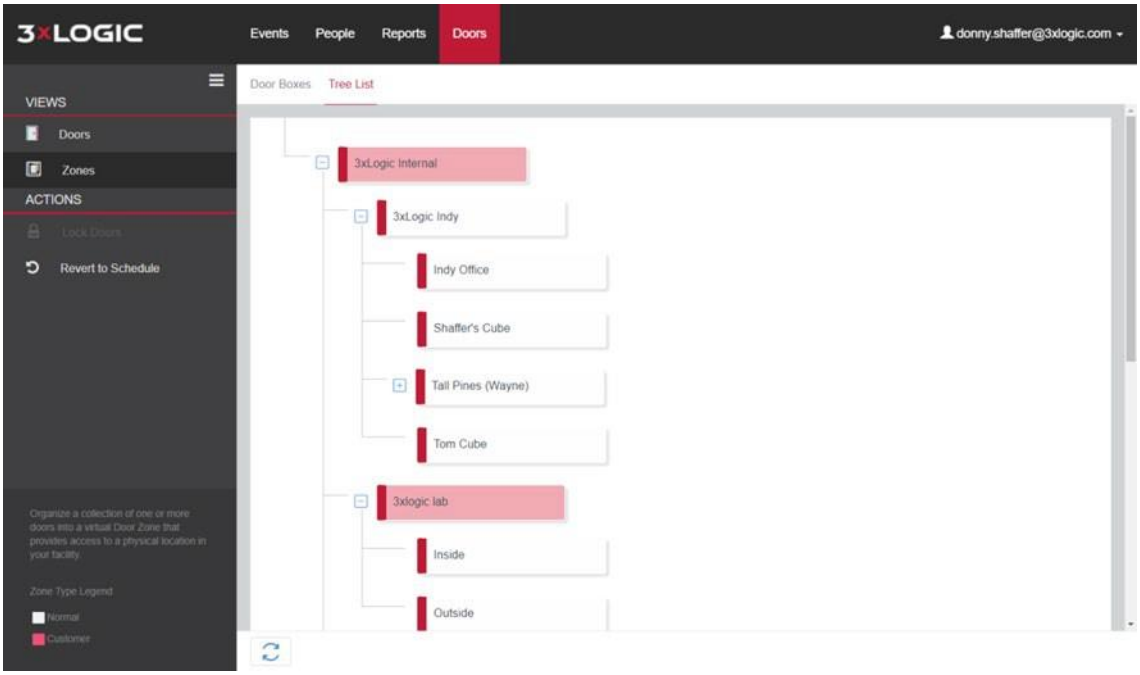


Figure 94: Zones - Tree

4.3.3 Role Zone Assignment

The Role Zone Assignment is where you assign a user with a Role to a Zone. This will set the user's Scope and will filter out anything outside of the Zone Assignment. Users assigned to a Zone will not be able to see anything above or beside them in the Zone Hierarchy.

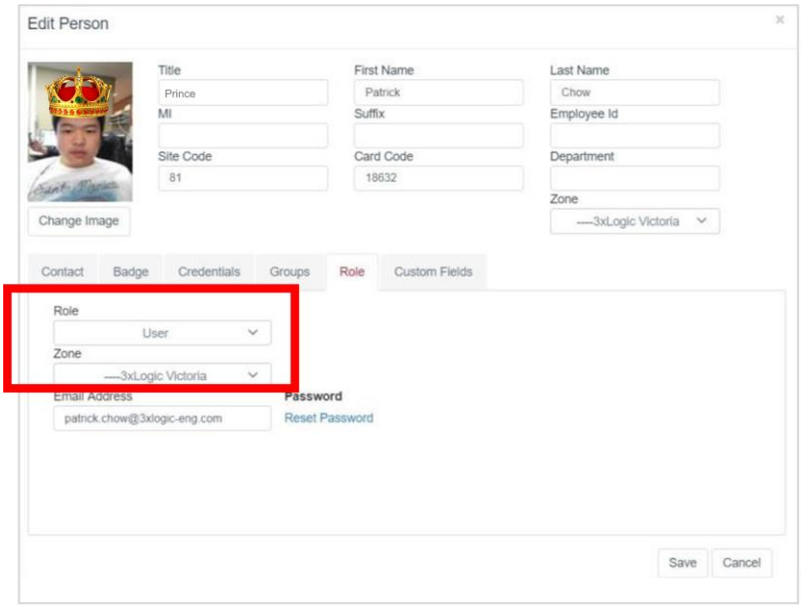


Figure 95: : Role Zone

4.3.4 Scope

The more Zones and Rules that are created within the software the more complicated it can be to navigate and configure. Therefore, infinias CLOUD allows the ability to filter out irrelevant data points with a feature called **Scope**.

Once a user has been assigned to a Zone, the software only display that zone and zones below it. Once the scope has been set for each user that is logging into the software, the users can utilize Scope button to drill down to a more granular level.

The **Scope** button can be found in the upper right-hand corner of the user interface or collapsed under the user name if in a smart device or small laptop screen.

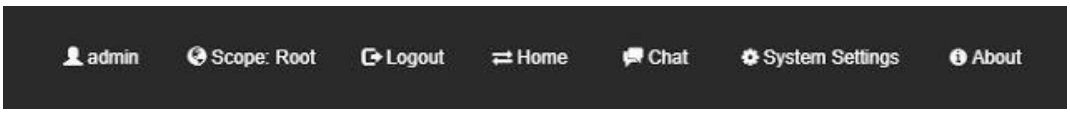


Figure 96: Scope

4.3.5 Group Zone Assignment

Assign all your groups from a specific location or office to the same Zone. This will allow members of those groups to only view that zone or below.

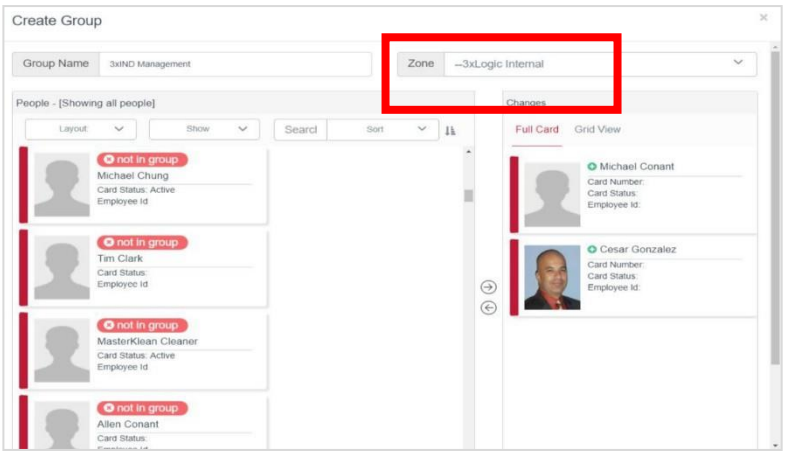


Figure 97: Zone Assignment

4.3.6 Logout of infinias CLOUD

The ***Logout*** link is accessible in the Home or Configuration Section under your User Account. There is an auto logout feature in place for security purposes to prevent a workstation from being left unattended for long periods of time that could jeopardize the security of the access software and location(s).

5 Chat and Knowledgebase Support

Customers can now access a direct line to 3xLOGIC Technical Support in either the **Home** or ***Configuration*** Sections of the software. Simply click the Chat link in the right-hand corner of infinias CLOUD, to launch chat support and a knowledgebase of useful tips, tricks, videos and documents.

You will now notice a support button that says, “Need Help?”. From there, expand the chat window by clicking the up arrow.

Figure 98: Need Help

Enter in your name, email address, and question regarding the infinias CLOUD software; then click the **Submit** button.

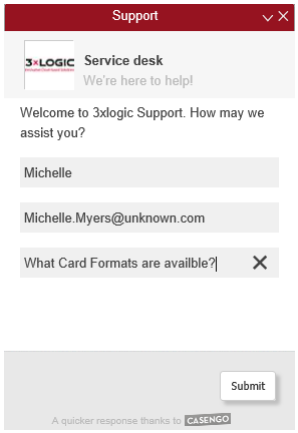


Figure 99: Ask for Help

The chat tool will perform a search against all knowledgebase articles and prioritize the top candidates for answering your question.

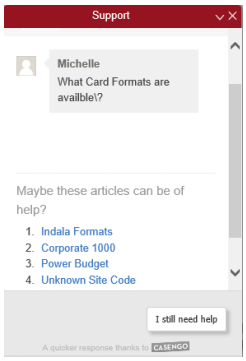


Figure 100: Chat - Articles

You can peruse through the articles before launching a live chat with technical support.

If you still need assistance beyond the knowledgebase, simply click the **I still need help** button.

The live chat session auto-creates a case in the 3xLOGIC Technical Support Environment. All chat conversation is logged in the case and you can be provided with a recap of the case upon completion, via email.

6 Best Practices

The QSG will help you get a door and cardholder added quickly to verify that the controller is functional. However, when designing and installing a system from scratch, it is important to follow the process outlined below to simplify configuration. We suggest mapping out your entire configuration (Zone Hierarchy, Zone and Door relationships, Door Unlock Schedules, Access Groups, and Access Privilege Schedules for Groups) on paper, Excel, or Visio before doing anything in infinias CLOUD.

Note: It's recommended that customers with multi-site or multi-location management should apply a unique prefix (company name and location, or store number) for every Zone, Door, and Group.

Example:

- 3xMIA Front Door
- 3xIND Front Door
- 3xSEA Front Door

6.1 Suggested Configuration Steps

1. Create Zones.
2. Create Schedules.
3. Create Behaviors for specifying Door Unlock Schedules.
4. Add Doors. Now you can apply a Behavior to the Door and specify which Zones the Door will border.
5. Create Groups.
6. Add Cardholders and give them group membership.
7. Create Access Privileges Rules for all groups.

6.2 Example of Mapped Zones and Doors

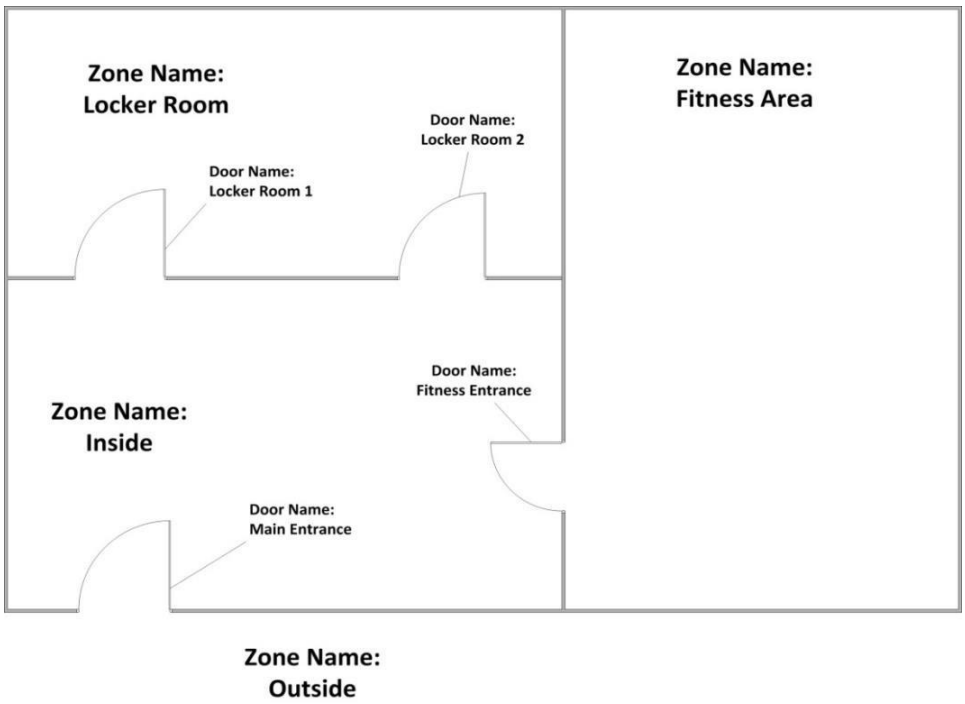


Figure 101: Mapped Zones and Doors - Example