3xLOGIC

INFINIAS™

INFINIAS 6.8

Software User Guide

v1.0

3xLOGIC Inc.
11899 Exit 5 Parkway, Suite 100
Fishers, IN 46037
United States. (303) 430-1969

Disclaimer
Information in this document is subject to change without notice and does not represent a commitment on the part of 3xLOGIC Inc. The software and / or databases described in this document are furnished under a license agreement or nondisclosure agreement. They may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement. The purchaser may make one copy of the software for backup purposes. No part of this manual and / or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including (but not limited to) photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of 3xLOGIC Inc.

3xLOGIC & INFINIAS are trademarks of 3xLOGIC, Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. 3xLOGIC Inc. disclaim any proprietary interest in trademarks and trade names other than their own.

Table of Contents

1 Software Details

This manual applies to the following products.

PRODUCT	VERSION
INFINIAS ESSENTIALS	6.8
INFINIAS PROFESSIONAL	6.8
INFINIAS CORPORATE	6.8
INFINIAS CLOUD	6.8

The INFINIAS software is consistent across all versions (CLOUD, Essentials, Professional, and Corporate). 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 portal for dealers to manage all customer accounts.

This guide emphasizes INFINIAS CLOUD but also covers local server information. Please reference the table below.

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	✓	✓	✓	✓
IPHONE, IPAD, ANDROID	✓	✓	✓	✓
PUSH NOTIFICATIONS TO SITE ACCESS MOBILE APP	✓	✓	✓	✓
WIRELESS LOCK SUPPORT	✓	✓	✓	✓
MOBILE CREDENTIAL LOCATION SERVICE	✓	✓	✓	✓
VIRTUAL MACHINE SUPPORT		✓	✓	✓
VIDEO INTEGRATION	✓	✓	✓	✓
ELEVATOR CONTROL (REQUIRES ELEVATOR CONTROL KIT & LICENSE)	✓		✓	✓
LDAP SUPPORT FOR AD SYNCHRONIZATION			✓	✓
MS OUTLOOK CALENDAR + GOOGLE CALENDAR INTEGRATION	✓		✓	✓
REQUIRES CERTIFICATION			✓	✓
MULTI-TIER MANAGEMENT	✓			✓
NUMBER OF EVENTS, DOORS, CARDHOLDERS, AND LICENSING	Unlimited	Unlimited	Unlimited	Unlimited

2 Terms and Concepts

INFINIAS 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.

Note: Any references to Intelli-M or intellim are artifacts of previous nomenclature, they refer to an antiquated naming convention but are still important for current functionality.

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 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 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 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 presents the Door Type, a template that describes the input and output configuration gathered into a single entity. INFINIAS has several default Door Types to choose from, saving 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. INFINIAS 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 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 **Schedule** is a 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 locked 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 the freedom to determine the identity of an Alarm for yourself, using the Rules Engine.

2.7 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 is swiped at Door Y."

2.8 Reports

INFINIAS software utilizes Microsoft's Reporting Services engine, along with their tools allowing users to create their own reports.

Custom cardholder badges also utilize the Reporting Services engine, giving the user complete control over the "look and feel" of their badges, courtesy of Microsoft Report Builder and the Reporting Services engine. For custom reports, please contact a 3xLOGIC Sales Representative.

2.9 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.

2.10 Multi-Tenant

This 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.

2.11 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, Schedule Manager, 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.

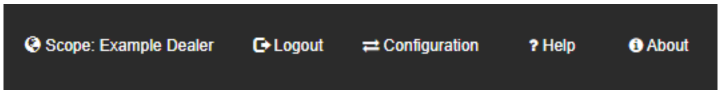
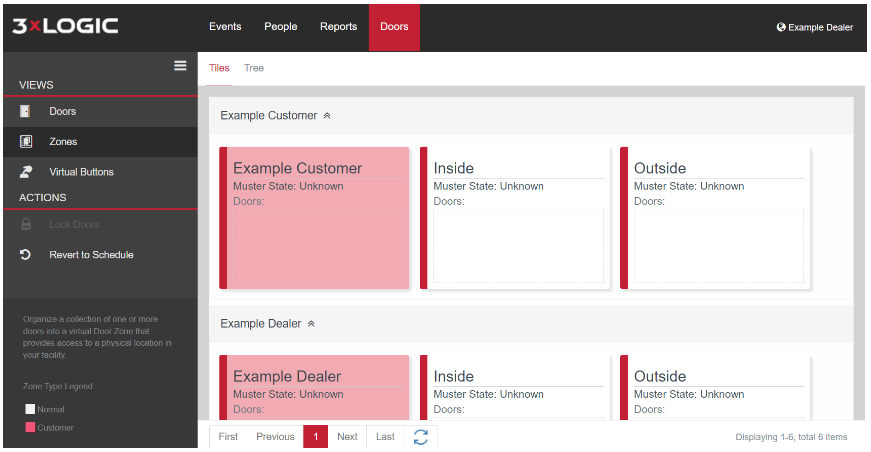


Figure 1-1: Scope Indicator

2.12 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.

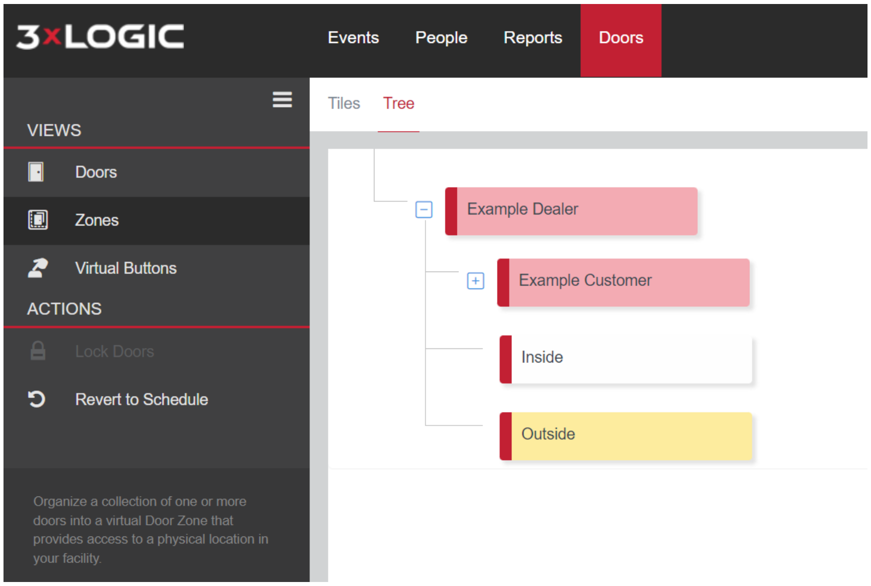


Organize a collection of one or more doors into a virtual Door Zone that provides access to a physical location in your facility

Example Customer Muster State: Unknown Doors:	Inside Muster State: Unknown Doors:	Outside Muster State: Unknown Doors:
Example Dealer Muster State: Unknown Doors:	Inside Muster State: Unknown Doors:	Outside Muster State: Unknown Doors:

Displaying 1-6, total 6 items

Figure 1-2: Tiles View



Organize a collection of one or more doors into a virtual Door Zone that provides access to a physical location in your facility.

Figure 1-3: Tree List View

3 System Requirements

3.1 Software

3.1.1 Operating System

The following versions of Windows are currently supported:

- Windows 10 Professional
- Windows 11 Professional
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Supported SQL Versions:

- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

3.2 Hardware

The INFINIAS software requires the following hardware dedicated for optimal performance.

3.2.1 Under 50 Doors

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

3.2.2 Under 300 Doors

- 3.5GHz CPU
- 16 GB RAM
- 250GB 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 of 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 10 GB limit on database size.

4 INFINIAS Essentials Overview

The content below highlights features and functions within INFINIAS.

4.1 Login

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

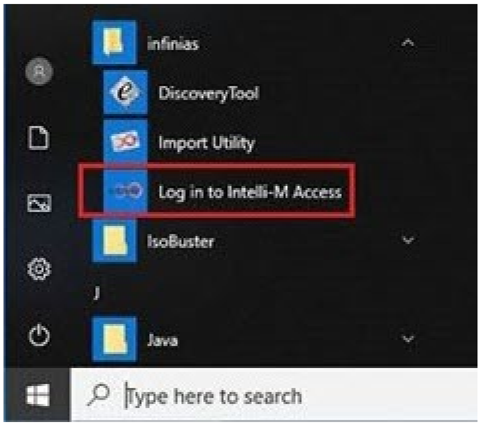


Figure 1-4: Windows Login

The following password requirements apply to INFINIAS on premises local installations.

- At least 8 characters with 3 of the following:
  - Upper Case
  - Lower Case
  - Number
  - Special Character

There is a limit of **10 characters** on the eIDC32 controller password.

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**

Note: On Premises (on-prem) installations enable users to adjust requirements for passwords, such as setting how long they are valid before expiring.

4.2 Events Tab

The Events Tab is the first page displayed after INFINIAS software login. This page updates 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.

4.2.1 Views

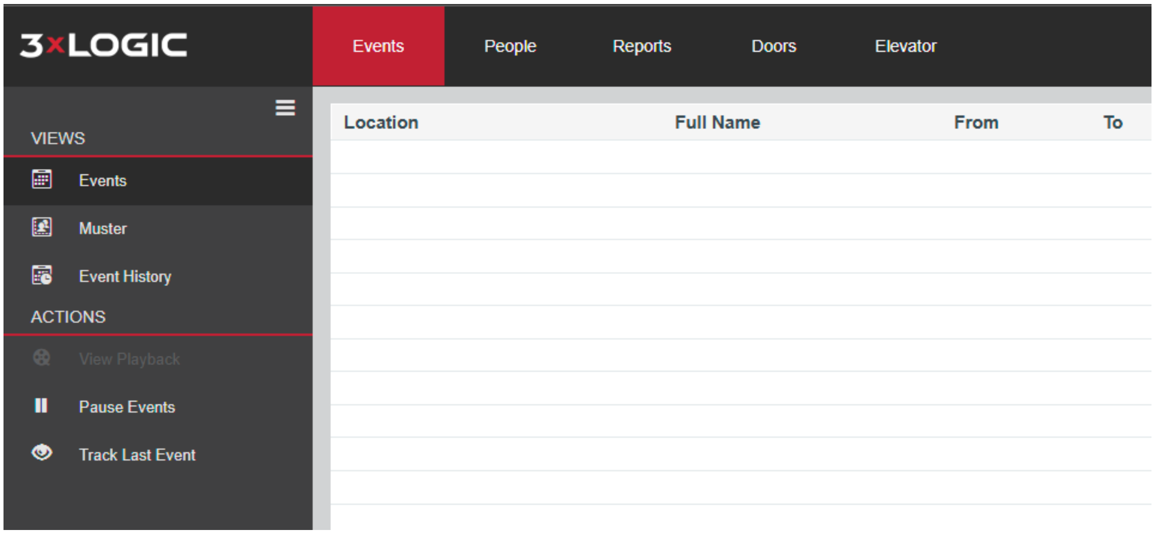


Figure 1-5: Events Tab

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.

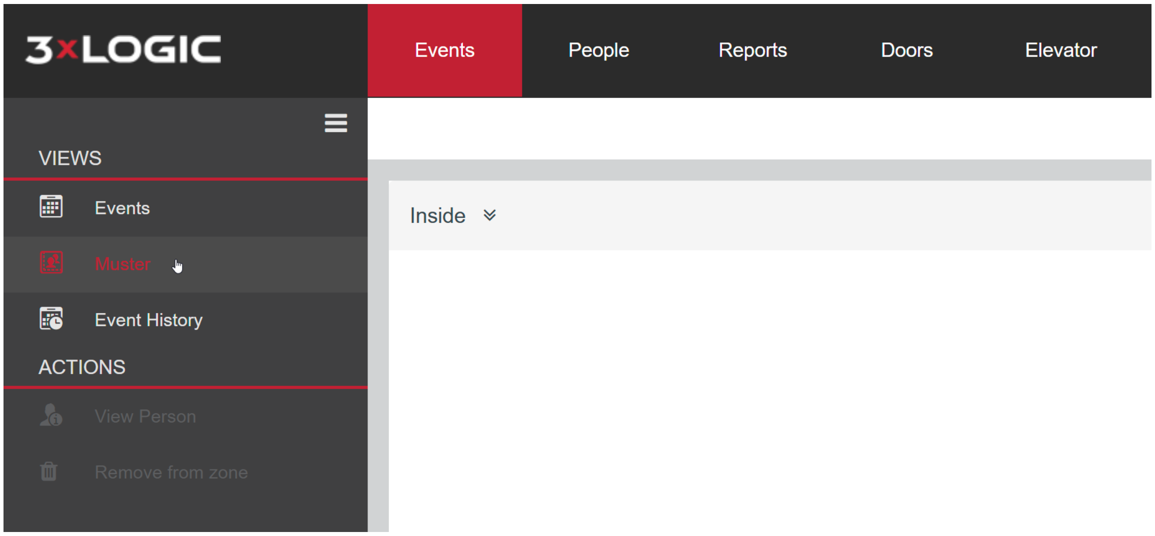
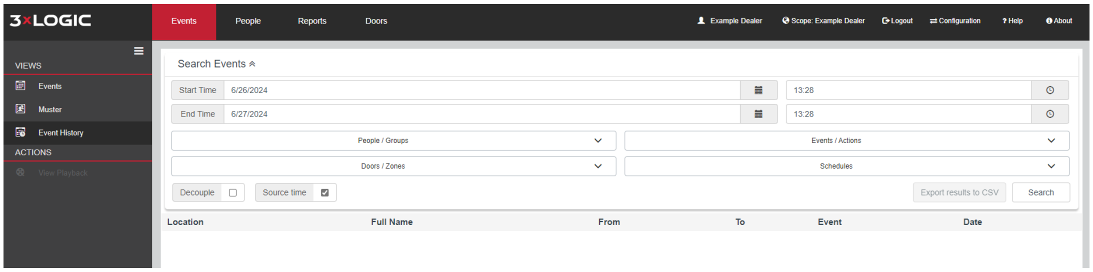


Figure 1-6: Muster View

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.



Start Time 6/26/2024 13:28

End Time 6/27/2024 13:28

Decouple ☐ Source time ☑

Location	Full Name	From	To	Event	Date

Figure 1-7: 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.

Note: INFINIAS offers the ability to export the Event History search results to a CSV file.

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.

4.2.2 Actions

Below the Views section, the Actions section offers three options as well.

View Playback allows access to the integrated video functionality (when available).

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.

4.3 People Tab

The **People** tab 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.

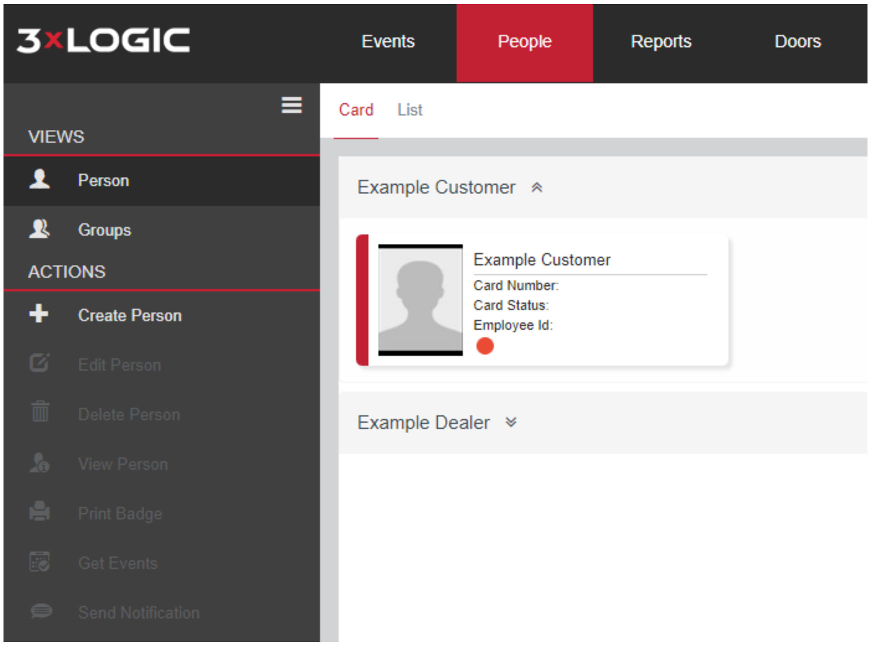


Figure 1-8: People Tab

4.3.1 Views

There are two primary *View* options available from the side navigation, **Person** and **Group**.

Person

This is the default view that has two *Sorting* options, **Card** and **List**, detailed under Person Sorting. **Create Person** is available by default. Selecting an entry enables related Actions:

- Edit Person
- Delete Person
- View Person
- Print Badge
- Get Events
- Send Notification (if available)

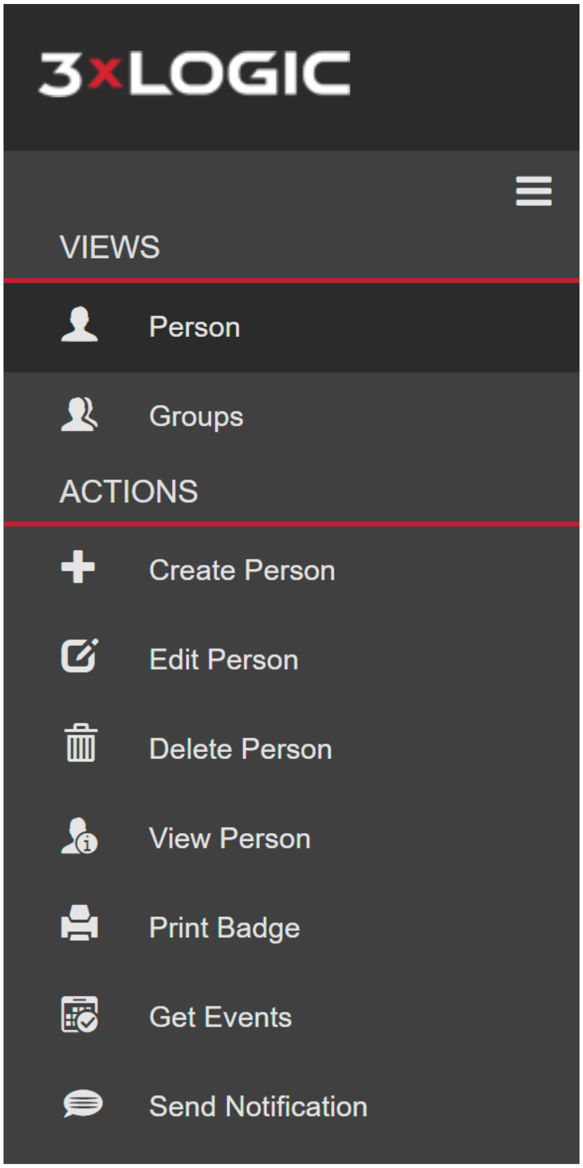


Figure 1-9: Person - Actions

Groups

This view displays groups and subgroups. The **Create Group** *Action* is available by default. Selecting a specific entry enables related Actions:

- Edit Group
- Delete Group
- Send Notification (if available)

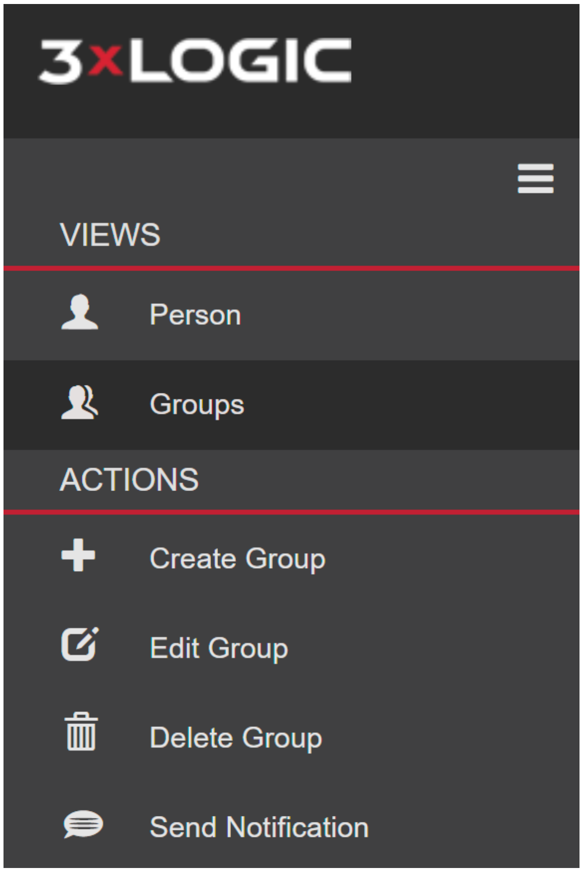


Figure 1-10: Group - Actions

4.3.2 Person Sorting

There are also two *Sorting* options when selecting Person, **Card** and **List**, with Card being the default Sorting option for the *People Tab*.

Card

Displays entries as summaries with details such as:

- Card Number
- Card status
- Employee Id
- Pictures of staff (if available)

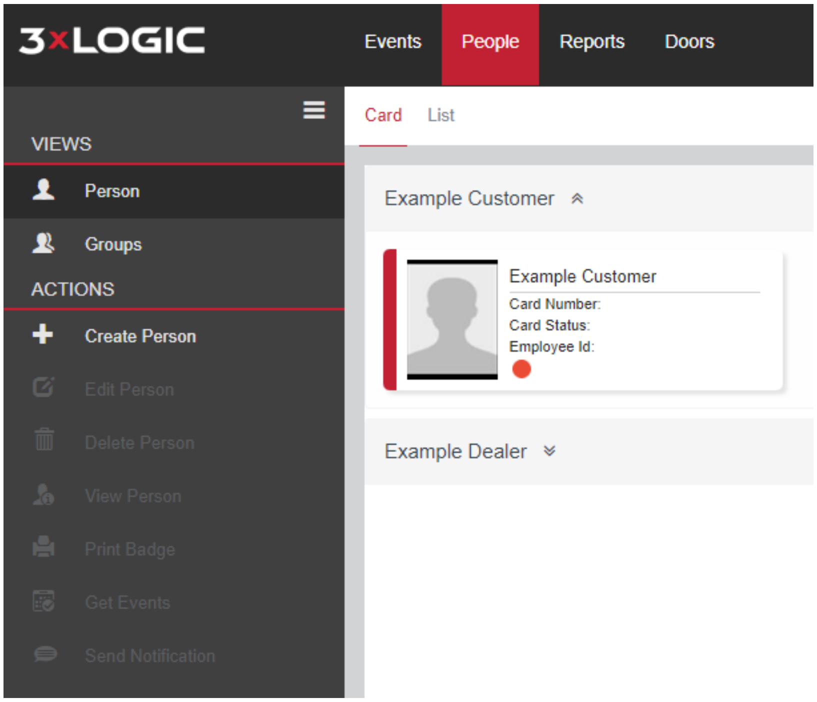
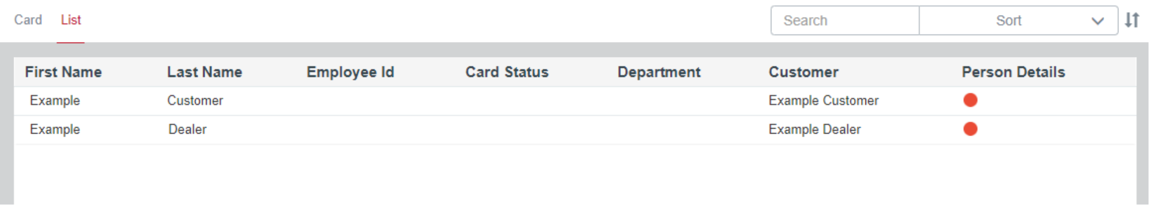


Figure 1-11: People Tab - Card

List

Displays entries as columns and rows with details such as:

- First Name
- Last Name
- Employee Id
- Card Status
- Department
- Customer
- Person Details
    - See **People Tab Legend** for icon specifics.



First Name	Last Name	Employee Id	Card Status	Department	Customer	Person Details
Example	Customer				Example Customer	●
Example	Dealer				Example Dealer	●

Figure 1-12: People Tab - List

4.3.3 People Tab Legend

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

ICON	EXPLANATION
🔵 External Id	**External ID** - Any Person created in Active Directory will display a blue dot on their user profile.
🔴 Role	**Role** - Any Person that has been given a login credential in INFINIAS display a red dot on their user profile.
🟢 Mobile Credential	**Mobile Credential** - Any Person that has been given a Mobile Credential will display a green dot on their user profile.

4.3.4 Create Person

To create a person, simply click Create Person from the action menu.

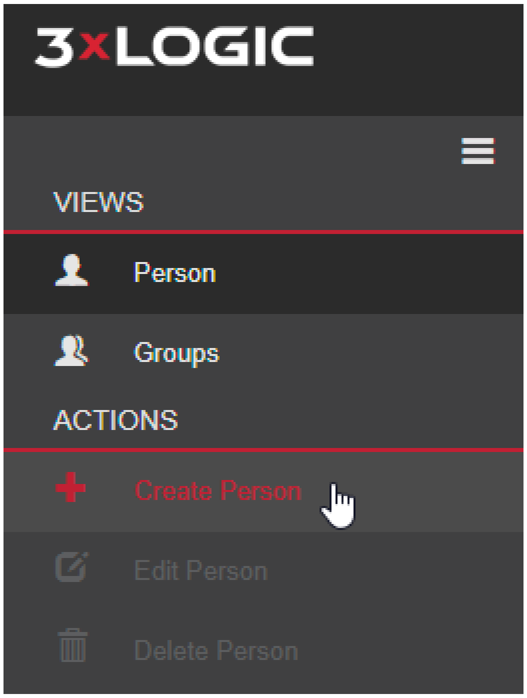


Figure 1-13: Create Person (Action)

The person's Title, First Name, Last Name, Middle Initial, Employee ID, and Department are available to be entered. The **required fields** are first name, last name, and either a login role for the software *or* a site code plus card code.

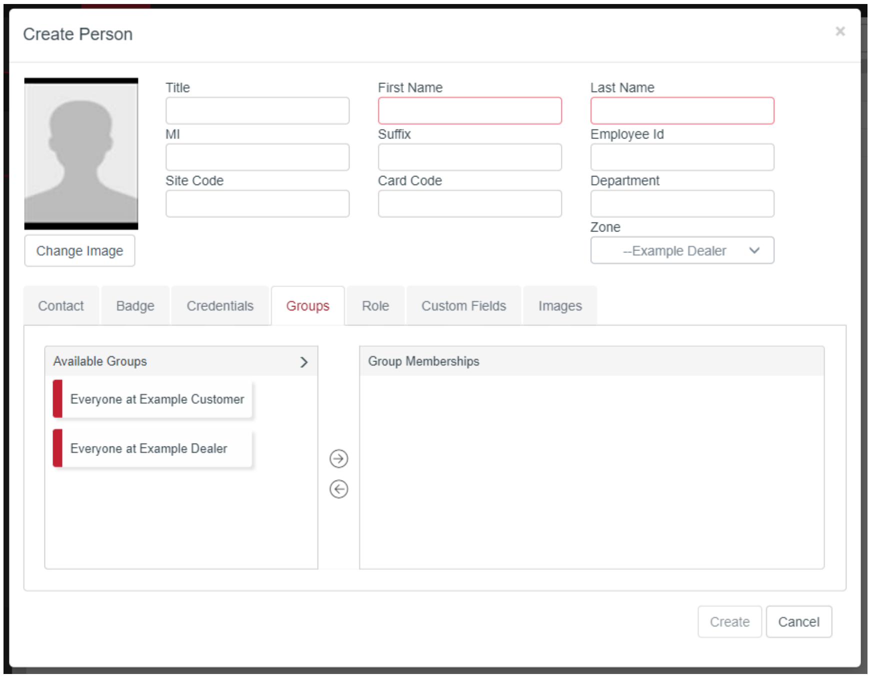


Figure 1-14: Create Person (Fields)

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 check box indicating that this is an alphanumeric card will be visible.

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 "Scope" on page 89.

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

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.

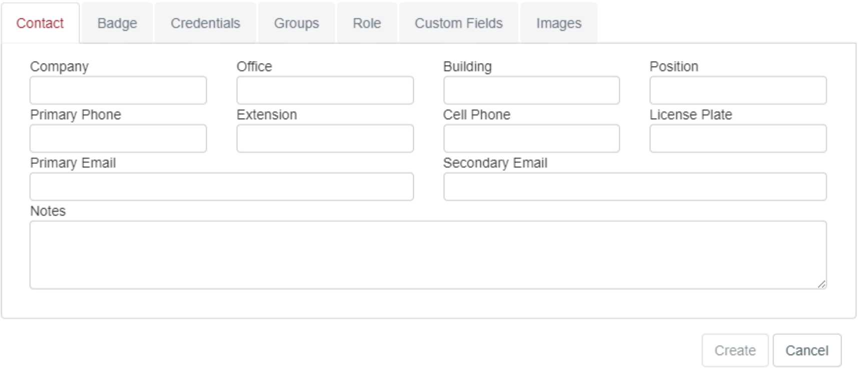


Figure 1-15: Create Person - Contact

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.

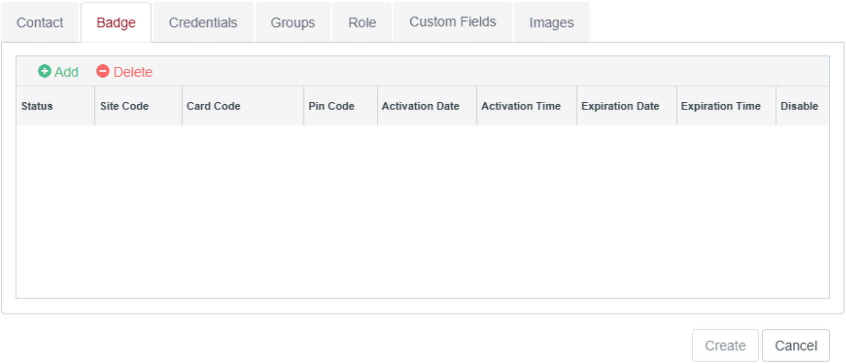
Note: If a person is created on a PC that is remote to the system that contains the software and database, the activation time will be based on the time of the PC they are utilizing. For example, a person created in a User Interface being used in Pacific Standard Time when the database resides in Eastern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

Please also note that 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 external guide on *Card + Pin versus Card OR Pin*.

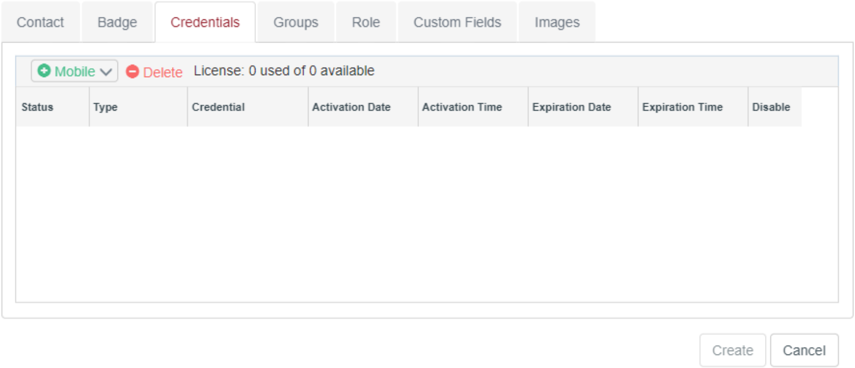


Status	Site Code	Card Code	Pin Code	Activation Date	Activation Time	Expiration Date	Expiration Time	Disable

Figure 1-16: Create Person - Badge

Credentials Tab

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



License: 0 used of 0 available

Status	Type	Credential	Activation Date	Activation Time	Expiration Date	Expiration Time	Disable

Figure 1-17: Create Person - Credentials

Please see the *Mobile Credentials* setup guide (**How to Configure Mobile Credentials**) for further details pertaining to the configuration and setup of Mobile Credentials.

Groups Tab

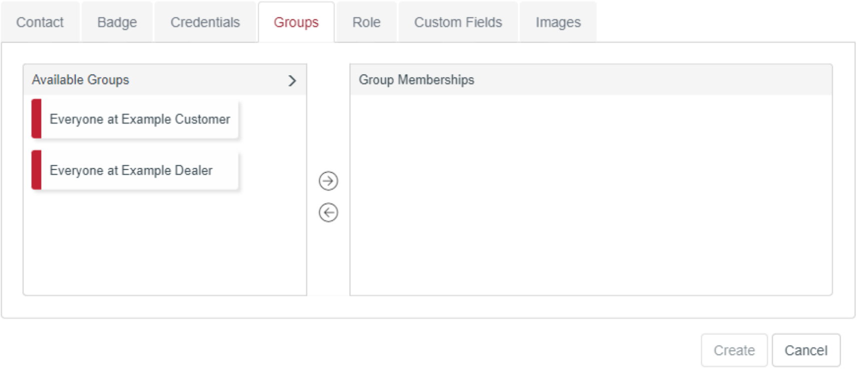
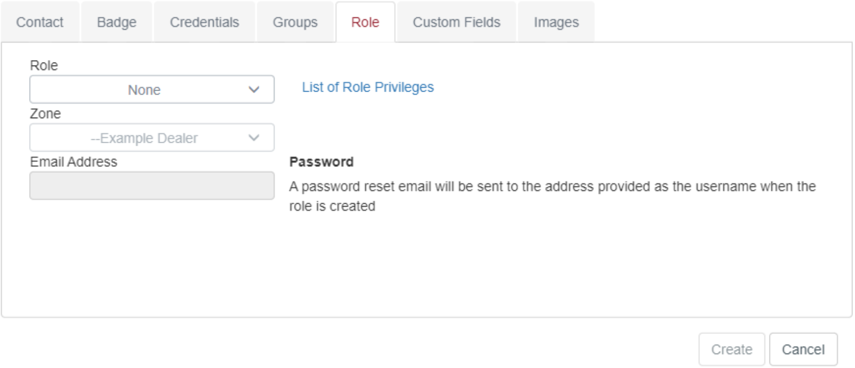


Figure 1-18: Create Person - Groups

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.

Role Tab



Password

A password reset email will be sent to the address provided as the username when the role is created

Figure 1-19: Create Person - Role

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, outlined in further details under the corresponding sections.

Note: To view the differences in permissions for roles click on "List of Role Privileges" to view the permissions matrix.

For on-premises installations, a temporary password can be generated for a new user to log in for the first time and then set their own password.

Custom Fields Tab

The Custom Fields Tab displays any custom fields created in the custom fields settings menu in configuration. Please see "Custom Fields" on page 66 for more details on creating custom fields.

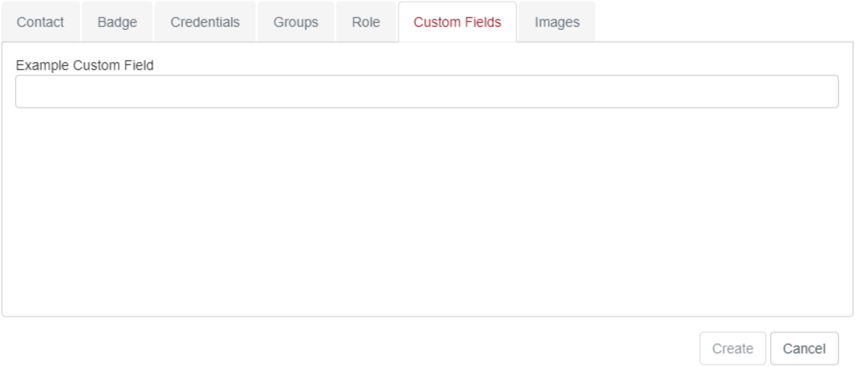


Figure 1-20: Create Person - Custom Fields

Images Tab

The Images Tab enables file uploads for the front and back of the user's badge.

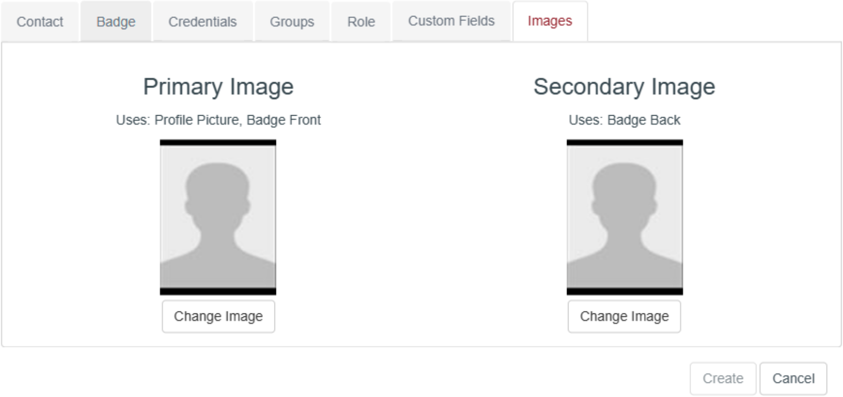


Figure 1-21: Create Person - Images

4.3.5 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.

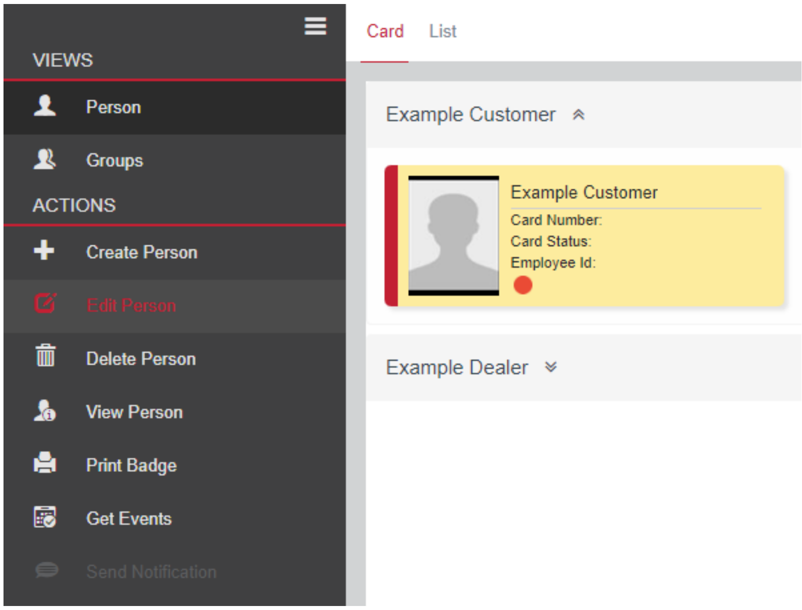
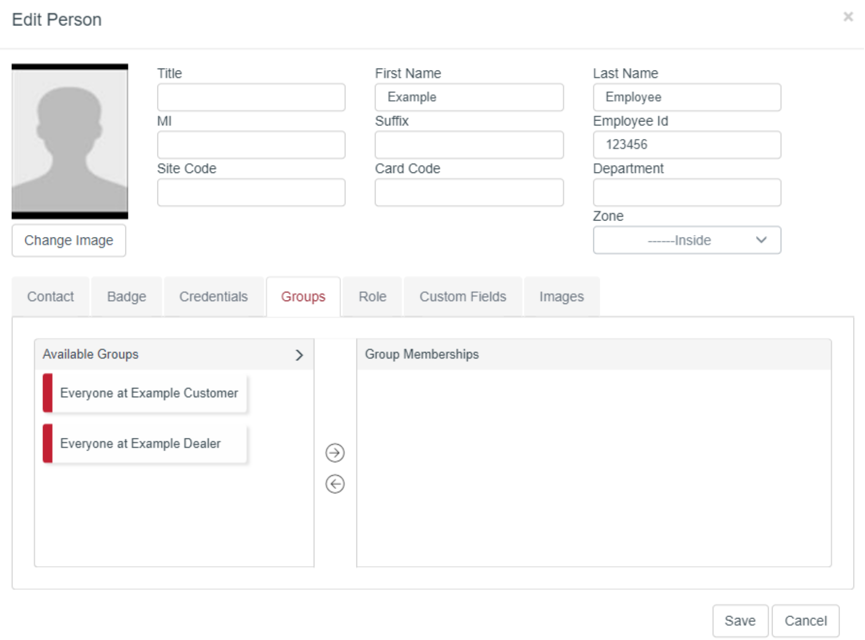


Figure 1-22: Edit Person (Action)

Fields

The fields include:

- Title (optional)
- First Name
- Last Name
- MI (optional)
- Suffix (optional)
- Employee ID (if applicable)
- Site Code
- Card Code
  - Option for Alphanumeric (checkbox)
- Department (if applicable)
- Zone



Edit Person

Title:

First Name: Example

Last Name: Employee

MI:

Suffix:

Employee Id: 123456

Site Code:

Card Code:

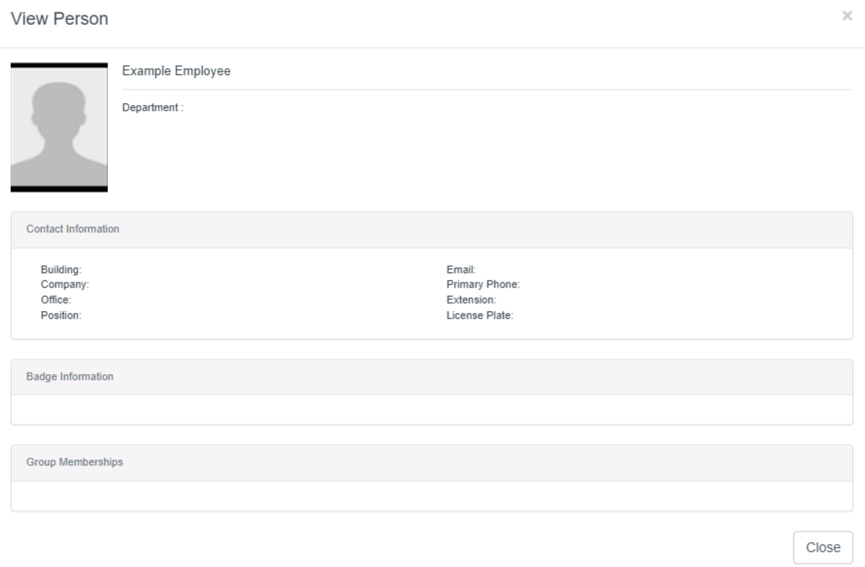
Department:

Zone: ------Inside

Figure 1-23: Edit Person (Fields)

4.3.6 View Person

View Person allows a quick view of some details about the selected individual in the software.



View Person

Example Employee

Department :

Contact Information

Building:

Company:

Office:

Position:

Email:

Primary Phone:

Extension:

License Plate:

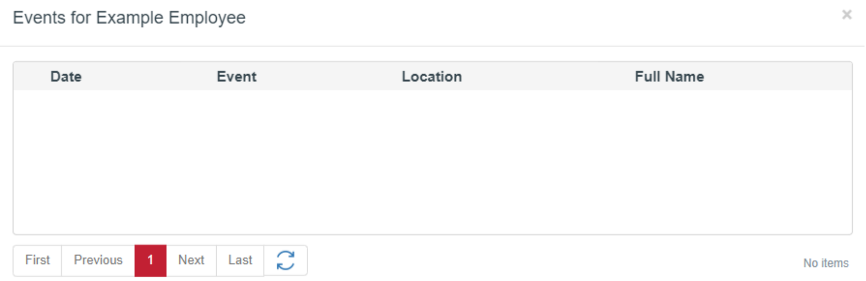
Badge Information

Group Memberships

Figure 1-24: View Person

4.3.7 Get Events

Get Events pull events for a specific person for purposes of data mining or troubleshooting.

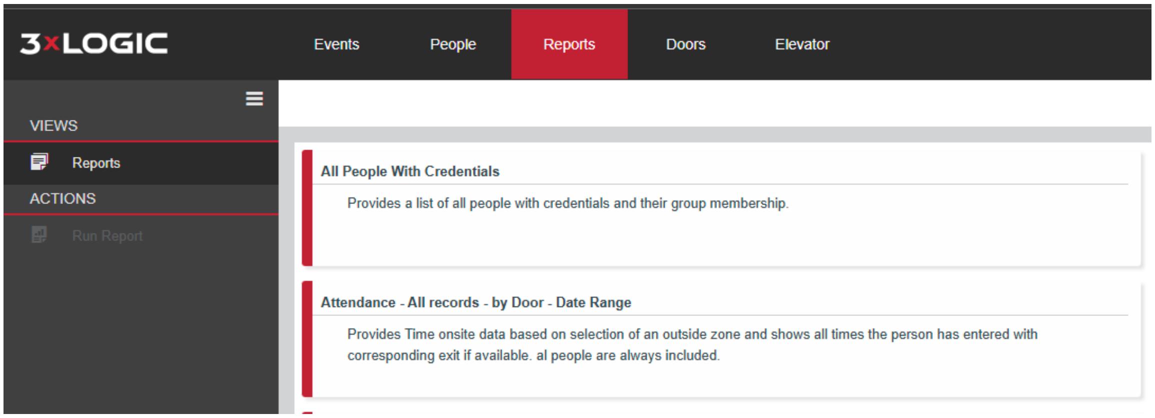

Events for Example Employee

Date	Event	Location	Full Name

Figure 1-25: Get Events

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.



All People With Credentials

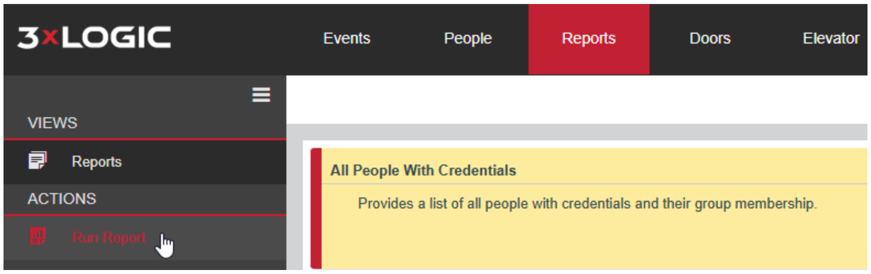
Provides a list of all people with credentials and their group membership.

Attendance - All records - by Door - Date Range

Provides Time onsite data based on selection of an outside zone and shows all times the person has entered with corresponding exit if available. al people are always included.

Figure 1-26: Reports

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. INFINIAS CLOUD offers the ability to get reports in CSV format.



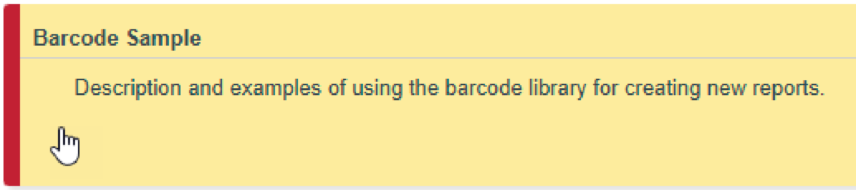
All People With Credentials

Provides a list of all people with credentials and their group membership.

Figure 1-27: Run Report

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.



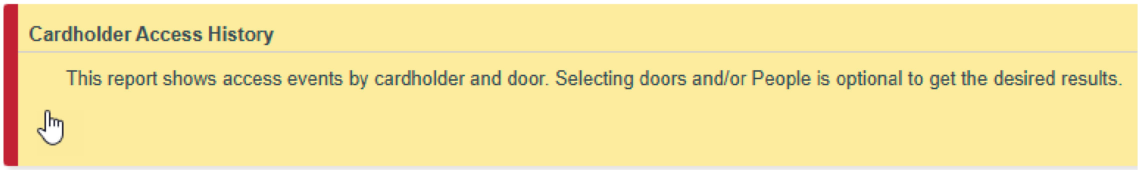
Barcode Sample

Description and examples of using the barcode library for creating new reports.

Figure 1-28: Barcode Sample

4.4.2 Cardholder Access History

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



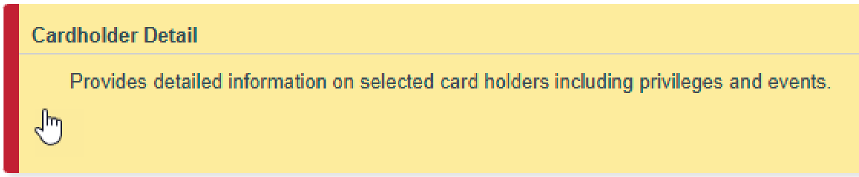
Cardholder Access History

This report shows access events by cardholder and door. Selecting doors and/or People is optional to get the desired results.

Figure 1-29: Cardholder Access History

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.



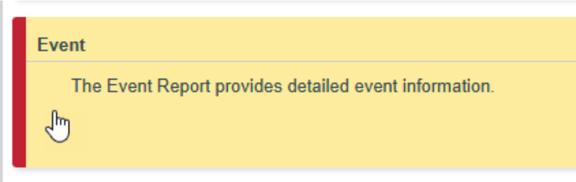
Cardholder Detail

Provides detailed information on selected card holders including privileges and events.

Figure 1-30: Cardholder Detail

4.4.4 Event Report

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



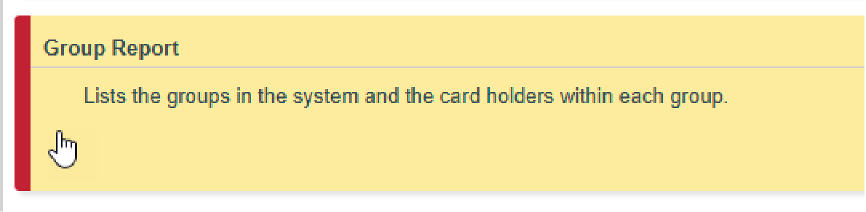
Event

The Event Report provides detailed event information.

Figure 1-31: Event

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.



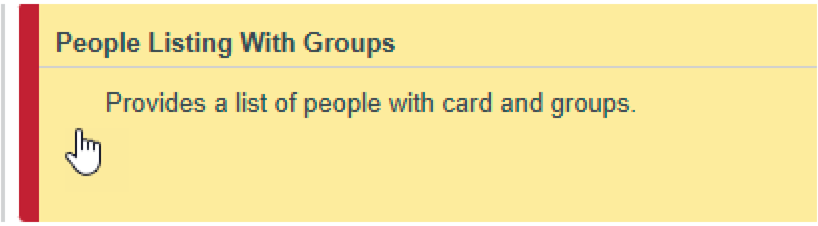
Group Report

Lists the groups in the system and the card holders within each group.

Figure 1-32: Group

4.4.6 People Listing with Groups

The People Listing with Groups report is a list of all people with their card number and group assignment.



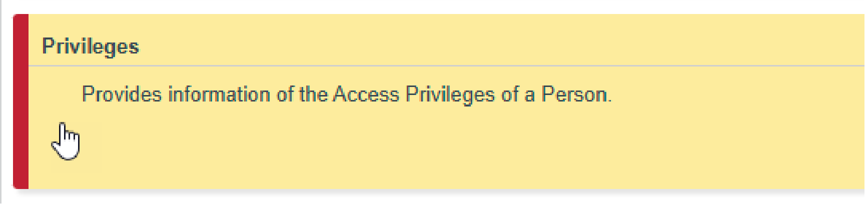
People Listing With Groups

Provides a list of people with card and groups.

Figure 1-33: People Listing with Groups

4.4.7 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.



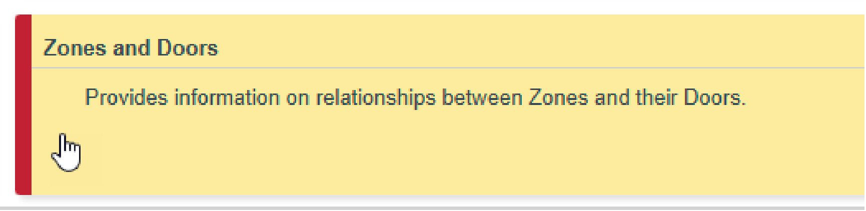
Privileges

Provides information of the Access Privileges of a Person.

Figure 1-34: Privileges

4.4.8 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.



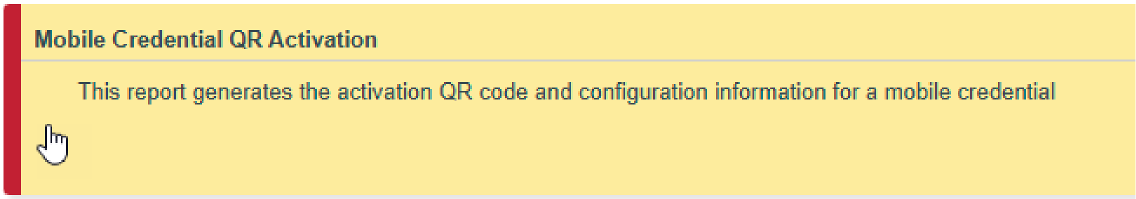
Zones and Doors

Provides information on relationships between Zones and their Doors.

Figure 1-35: Zones and Doors

4.4.9 Mobile Credential QR Activation

The Mobile Credential QR Activation Report will provide a QR code for scanning 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.

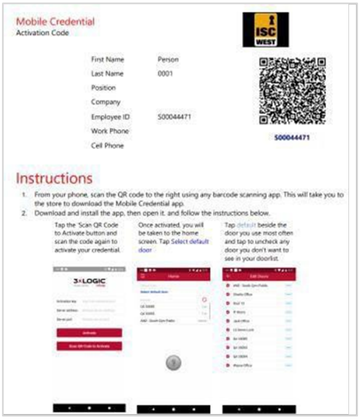


Mobile Credential QR Activation

This report generates the activation QR code and configuration information for a mobile credential

Figure 1-36: Mobile Credential QR Activation

Note: The Mobile Credential QR Activation is only available in CLOUD.



Mobile Credential
Activation Code

First Name	Person
Last Name	0001
Position	
Company	
Employee ID	S00044471
Work Phone	
Cell Phone	

S00044471

Instructions

1. From your phone, scan the QR code to the right using any barcode scanning app. This will take you to the store to download the Mobile Credential app.
2. Download and install the app, then open it, and follow the instructions below.

Tap the 'Scan QR Code to Activate button and scan the code again to activate your credential.

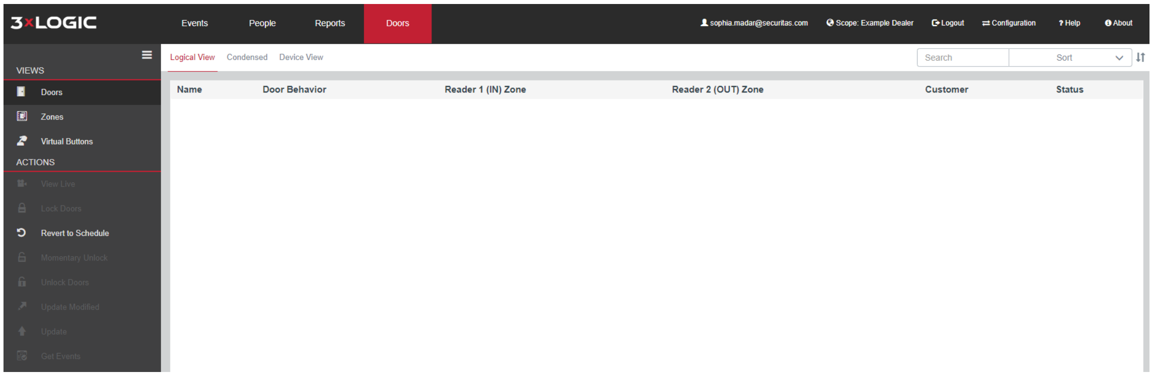
Once activated, you will be taken to the home screen. Tap Select default door

Tap default beside the door you use most often and tap to uncheck any door you don't want to see in your doorlist.

Figure 1-37: QR Activation Example

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 Homepage.



Name	Door Behavior	Reader 1 (IN) Zone	Reader 2 (OUT) Zone	Customer	Status

Figure 1-38: 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.

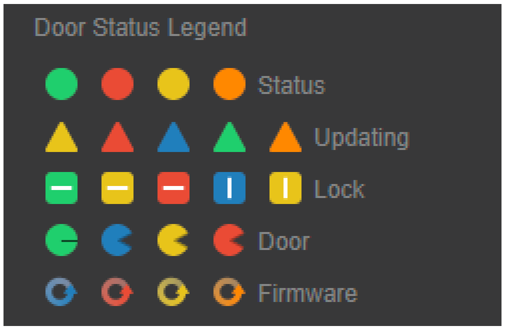


Figure 1-39: Door Status Legend

4.5.1 View Live

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.

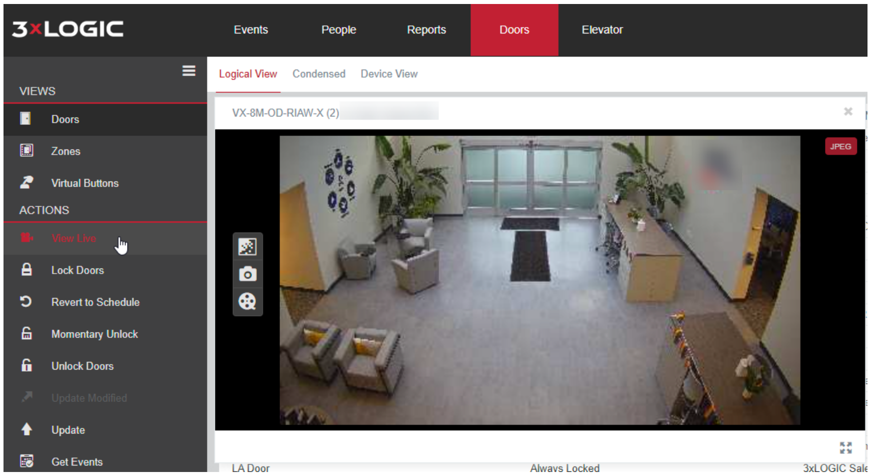


Figure 1-40: View Live

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 (if set to the default value in the door behavior) and then 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

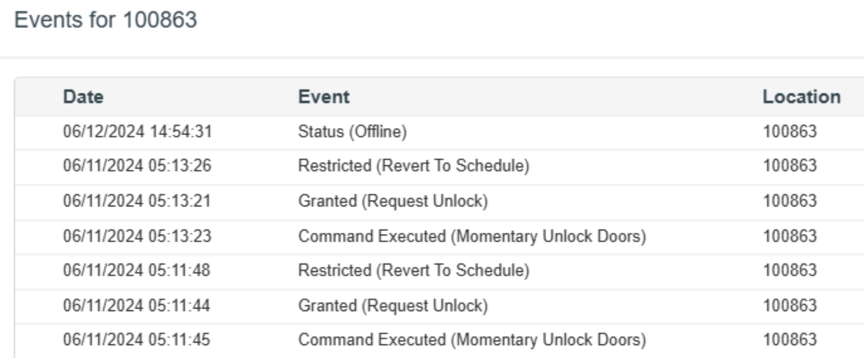
Any doors showing a yellow triangle status indicate that they require an update to be current to the programming of the software. This can be done with a single click by using the update modified option in the actions menu. All doors in the system with that status will initiate an update. All doors that 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.



Events for 100863

Date	Event	Location
06/12/2024 14:54:31	Status (Offline)	100863
06/11/2024 05:13:26	Restricted (Revert To Schedule)	100863
06/11/2024 05:13:21	Granted (Request Unlock)	100863
06/11/2024 05:13:23	Command Executed (Momentary Unlock Doors)	100863
06/11/2024 05:11:48	Restricted (Revert To Schedule)	100863
06/11/2024 05:11:44	Granted (Request Unlock)	100863
06/11/2024 05:11:45	Command Executed (Momentary Unlock Doors)	100863

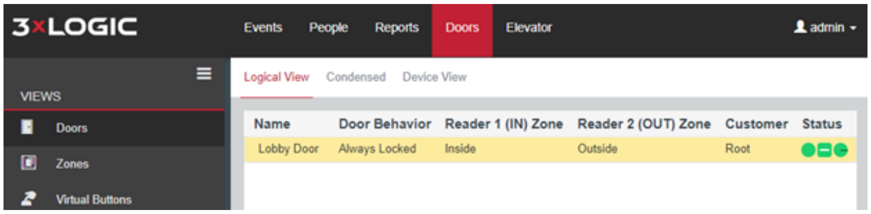
Figure 1-41: Get Events

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.

Logical View

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



Name	Door Behavior	Reader 1 (IN) Zone	Reader 2 (OUT) Zone	Customer	Status
Lobby Door	Always Locked	Inside	Outside	Root	●▬●

Figure 1-42: Logical View

Condensed View

This view shows the status for multiple doors on a single screen. Useful for monitoring at a glance.

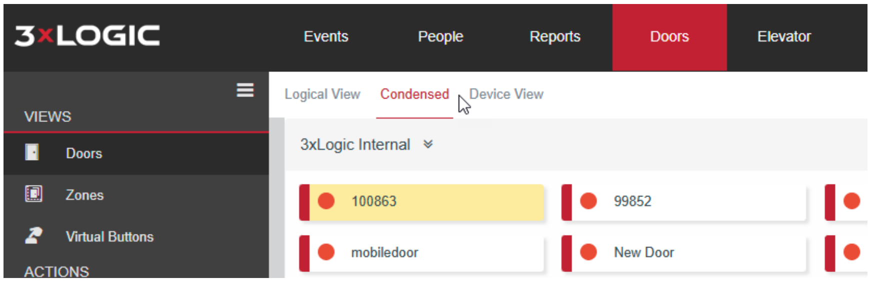
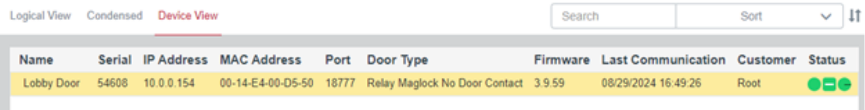


Figure 1-43: Condensed View

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.



Name	Serial	IP Address	MAC Address	Port	Door Type	Firmware	Last Communication	Customer	Status
Lobby Door	54608	10.0.0.154	00-14-E4-00-D5-50	18777	Relay Maglock No Door Contact	3.9.59	08/29/2024 16:49:26	Root	●▬●

Figure 1-44: Device View

4.5.7 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.

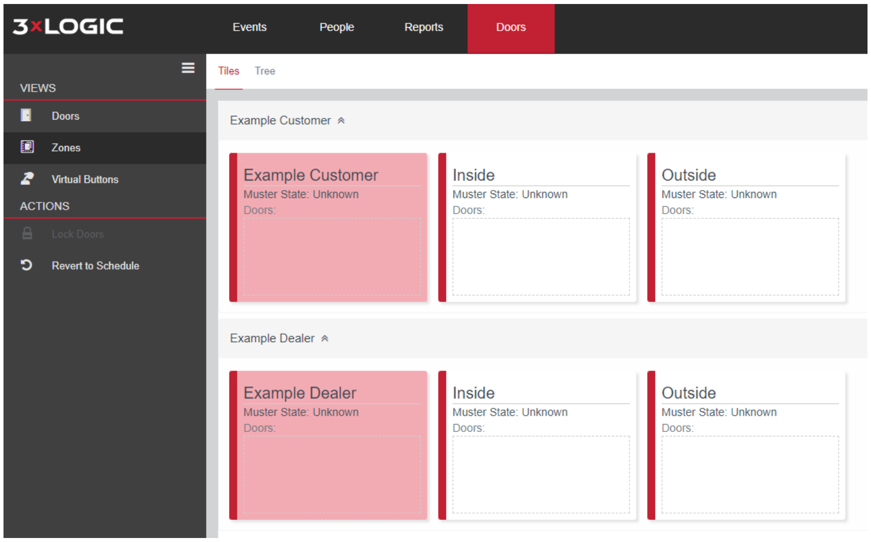


Figure 1-45: Zones View (Tiles)

Lock Doors

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

Revert to Schedule

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

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.

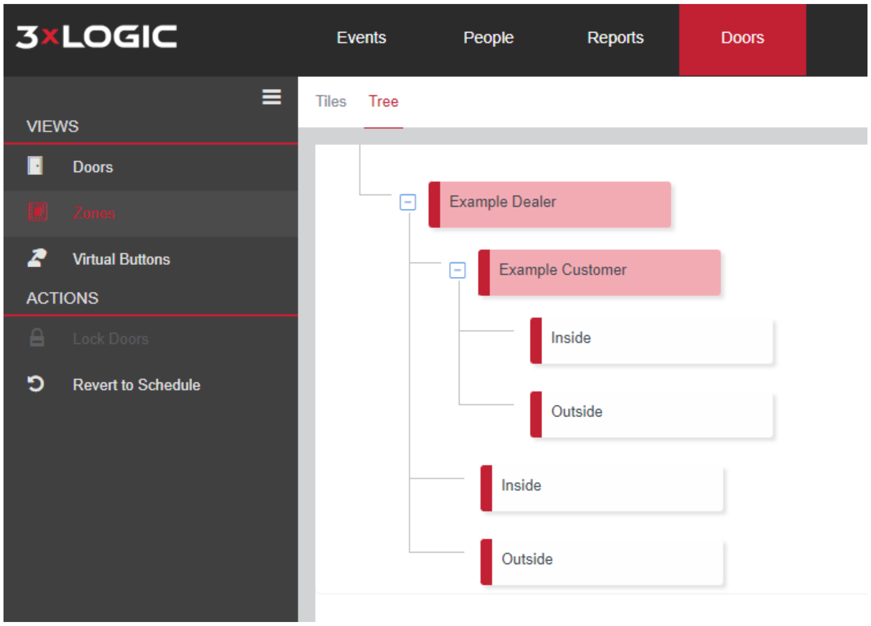


Figure 1-46: Zones View (Tree)

4.5.8 Virtual Buttons

Virtual buttons are used to allow a virtual button to activate a rule through the rules engine to trigger a desired output.

Live Virtual Buttons

The example below shows a button being used to trigger a lockdown. See "Doors Tab" on page 32 for details.

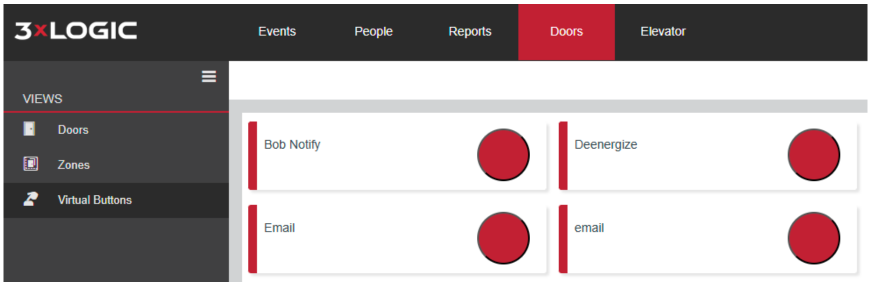


Figure 1-47: Virtual Buttons

4.6 Top Menu

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.

4.6.1 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 be visible, regardless of the state of the menu.

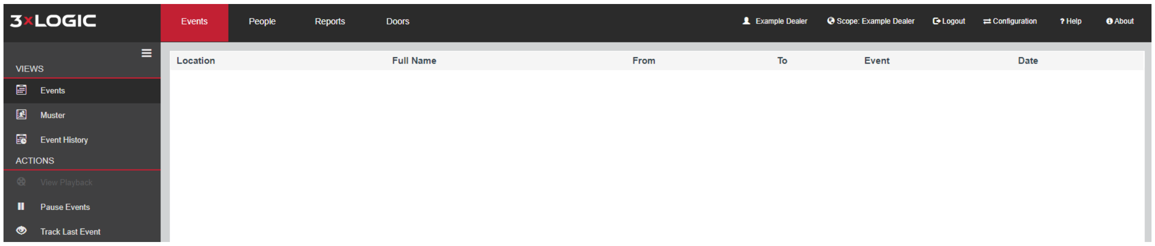
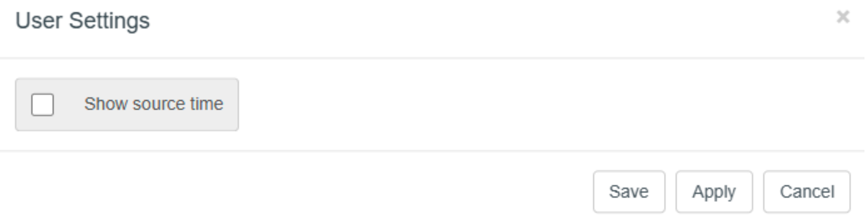


Figure 1-48: Logged-in User

Clicking user settings or clicking the username when the system isn't collapsed into a drop- down menu will display the User Settings box. The primary user setting featured is **Show Source Time**.


User Settings

☐ Show source time

Figure 1-49: User Settings

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.

Note: For On Premises installations, there is also an option to **Reset Password** under *User Settings*.

4.6.2 Scope

See "Scope" on page 5

4.6.3 Logout

Click this to log out of the system.

4.6.4 Configuration

Click to access advanced settings for INFINIAS.

4.6.5 Help

Click to display a list of contact information specific to the local configuration.

4.6.6 About

The about button will give the version and a link to the support web page.

5 INFINIAS Essentials Configuration

The **Configuration** section of INFINIAS includes a range of features that allows the programming of doors, zones, behaviors, schedules, rules, and many more. The following sections will elaborate on what each section is for and how to use it to program the software.

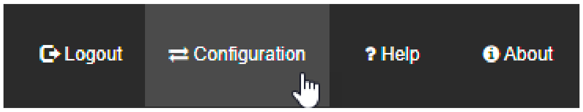
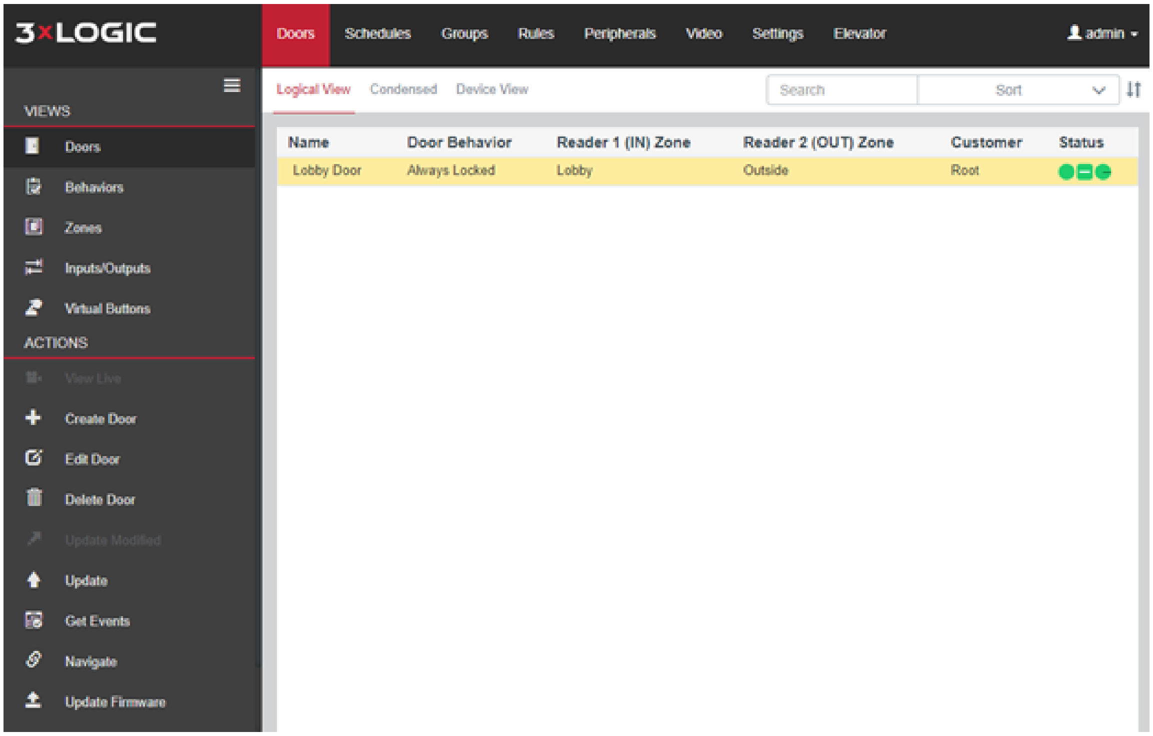


Figure 1-50: Configuration

5.1 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.



Name	Door Behavior	Reader 1 (IN) Zone	Reader 2 (OUT) Zone	Customer	Status
Lobby Door	Always Locked	Lobby	Outside	Root	●■●

Figure 1-51: Configuration - Doors

5.1.1 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.

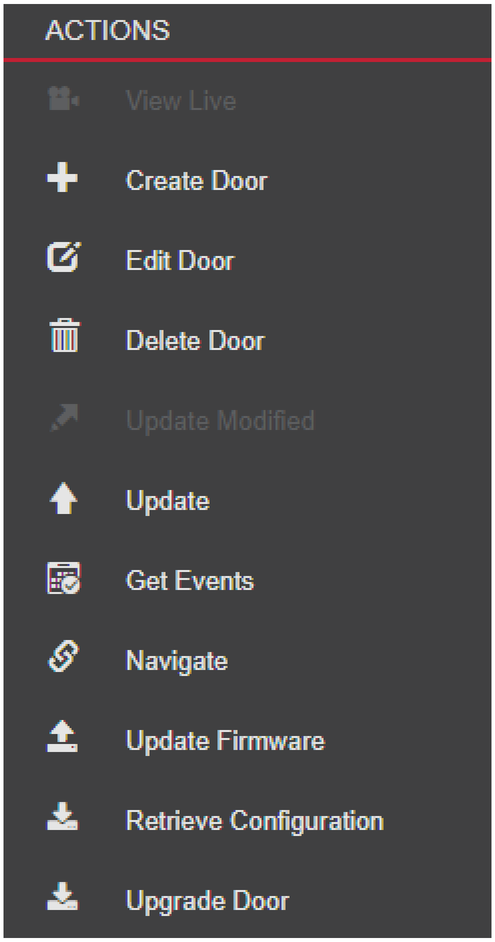


Figure 1-52: Configuration - Doors (Actions)

View Live

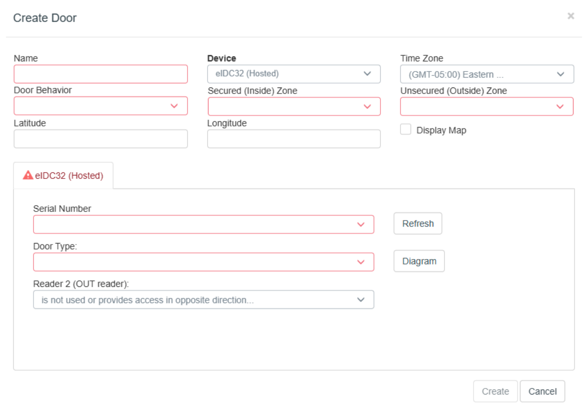
Identical to the one found in the doors tab home page. This will only be available if a camera is associated with the door.

Create Door

There are three different sets of procedures when creating a door using an eIDC32 door controller in Essentials, Professional, and Corporate software: Hosted, Non-Hosted, and Allegion/Engage.

Hosted

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 Figure 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. Using a hosted door is the preferred option when setting up a controller.



Create Door

Name

Device: eIDC32 (Hosted)

Time Zone: (GMT-05:00) Eastern ...

Door Behavior

Secured (Inside) Zone

Unsecured (Outside) Zone

Latitude

Longitude

□ Display Map

eIDC32 (Hosted)

Serial Number

Door Type:

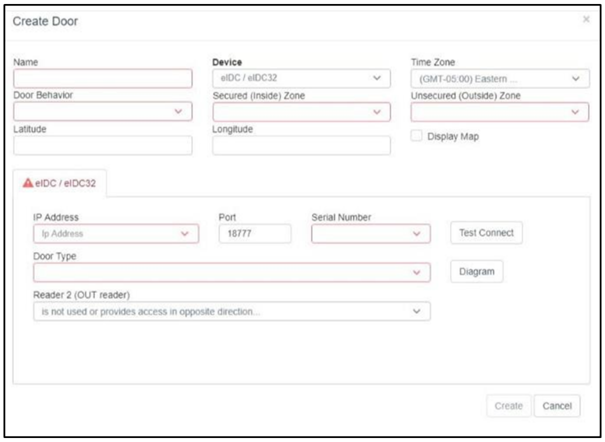
Reader 2 (OUT reader): is not used or provides access in opposite direction...

Figure 1-53: Create Hosted Door

A separate document has been created for the purpose of configuring a site to use that newer method of programming. The document previously entitled **S-BASE-KIT_3x_HTG-Configuring_a_door** provides a guide for the procedure of creating an eIDC32 (Hosted) door. See "Configuring and Creating a Hosted Door" on page 107

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.



Create Door

Name

Device: eIDC / eIDC32

Time Zone: (GMT-05:00) Eastern ...

Door Behavior

Secured (Inside) Zone

Unsecured (Outside) Zone

Latitude

Longitude

□ Display Map

eIDC / eIDC32

IP Address: Ip Address

Port: 18777

Serial Number

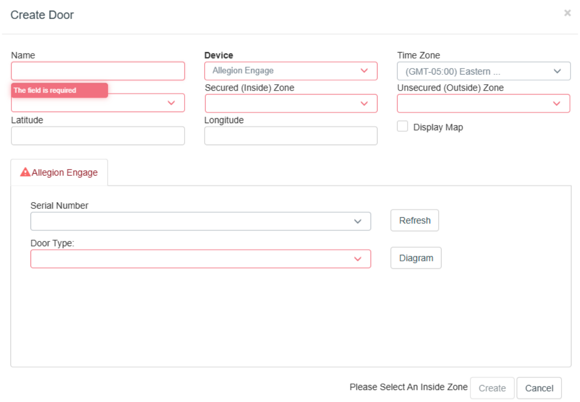
Door Type

Reader 2 (OUT reader): is not used or provides access in opposite direction...

Figure 1-54: Create Non-Hosted Door (Legacy)

Allegion/Engage Doors

The Allegion/Engage door option in the device drop down is for wireless lockset integration. Please see the separate document entitled **Allegion Wireless Quick Start Guide** for details on programming and configuring an Allegion door lock to function with INFINIAS Access and INFINIAS CLOUD.



Create Door

Name

The field is required

Device: Allegion Engage

Time Zone: (GMT-05:00) Eastern ...

Secured (Inside) Zone

Unsecured (Outside) Zone

Latitude

Longitude

□ Display Map

Allegion Engage

Serial Number

Door Type:

Please Select An Inside Zone

Figure 1-55: Allegion/Engage Door

Once a door has been programmed, the door serial number will appear in the serial number drop down menu.

Fields

For any door, the following fields are available within INFINIAS.

LABEL	DESCRIPTION
Name	Name of the specified 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	GPS coordinates of the door; 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. Customizable for remote locations that use one public IP address and multiple custom ports to communicate to door controllers. Contact support for details.
Serial Number	This links the device serial number, typically a six-digit number, to the IP address and allows the software to distinguish it from 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)	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 provide access in two directions, or a single reader 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 pings a provided IP via the data port 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).

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.

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.

Update Modified

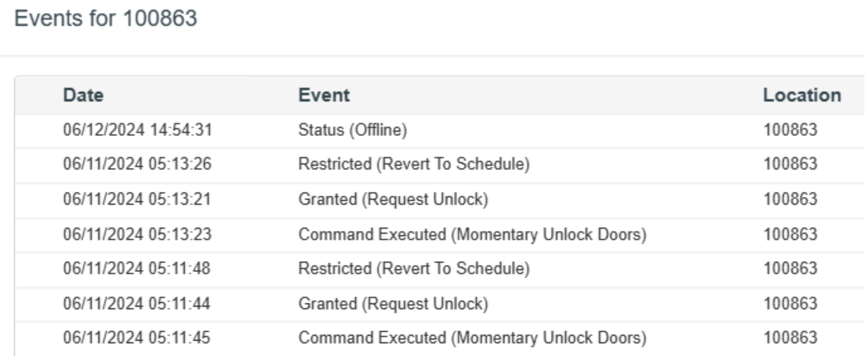
This does the same as the previous doors tab. It forces all doors in the needs update state or yellow triangle status to get an update.

Update

The update feature is used to manually update doors that are in a state requiring an update or for troubleshooting purposes. This pushes the software configuration for the door down to the door controller.

Get Events

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



Events for 100863

Date	Event	Location
06/12/2024 14:54:31	Status (Offline)	100863
06/11/2024 05:13:26	Restricted (Revert To Schedule)	100863
06/11/2024 05:13:21	Granted (Request Unlock)	100863
06/11/2024 05:13:23	Command Executed (Momentary Unlock Doors)	100863
06/11/2024 05:11:48	Restricted (Revert To Schedule)	100863
06/11/2024 05:11:44	Granted (Request Unlock)	100863
06/11/2024 05:11:45	Command Executed (Momentary Unlock Doors)	100863

Figure 1-56: Get Events

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.

Update Firmware

This will attempt to update the firmware on the eIDC32 by asking for the firmware zip file location.

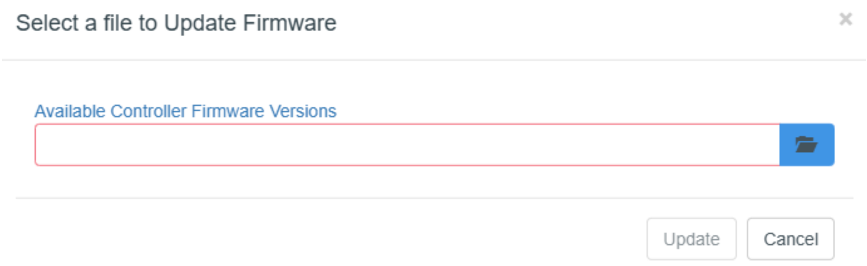

Select a file to Update Firmware
×
Available Controller Firmware Versions
Update
Cancel

Figure 1-57: Update Firmware

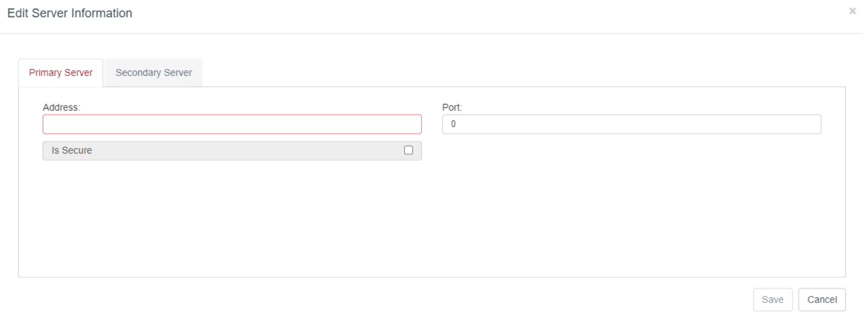
Note: This will only work on Hosted doors above 3.4.20 firmware and the selected controller must be on firmware version 3.4.20 or above. Other controllers must be updated via the Discovery Tool installed on a computer with access to the LAN on which the controller is installed.

Upgrade Door

This option attempts to switch a non-hosted eIDC32 (legacy) 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
  - If this says *localhost*, it needs changed to the IP address
- Port: 18800
- Is Secure: checked



Port: 0

Is Secure ☐

Figure 1-58: 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 separate guide entitled **Creating a Door in INFINIAS Access**.

5.1.2 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.

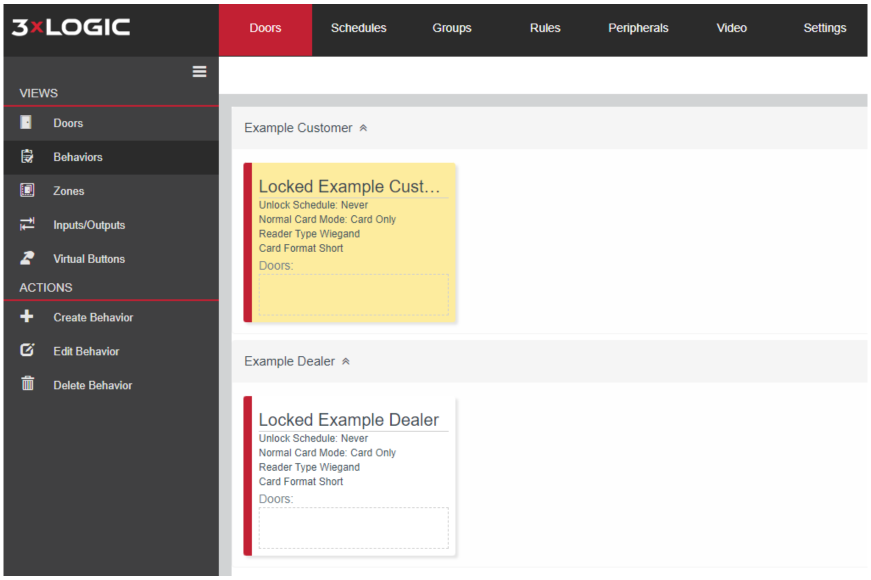
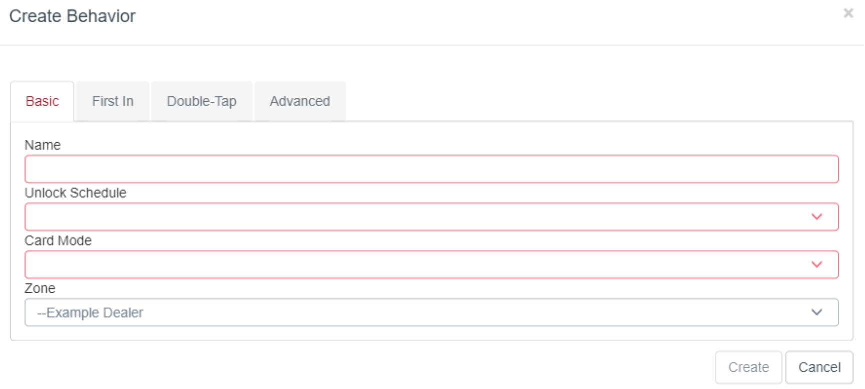


Figure 1-59: Door Behavior

Create Behavior

This opens the window for behavior creation. The double tap lock option in the behavior allows a person to lock a door with a double tap of their badge on a reader.


Create Behavior

Name

Unlock Schedule

Card Mode

Zone
--Example Dealer

Figure 1-60: Create Behavior

Please see the separate guide **First In Door Behavior Setup Guide**, included as "First In Door Behavior" on page 123 in this document.

Basic Tab

LABEL	DESCRIPTION
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 separate documentation on **Card + Pin versus Card OR Pin**.
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

LABEL	DESCRIPTION
Reader Type	■ Wiegand is the standard reader type that INFINIAS Access functions with. ■ PAC Serial is a string reader compatible setting that allows us to function with the PAC Alphanumeric reader. ■ Qscan is 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	■ Measured in 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.

Edit Behavior

Any behavior can be edited after creation.

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.

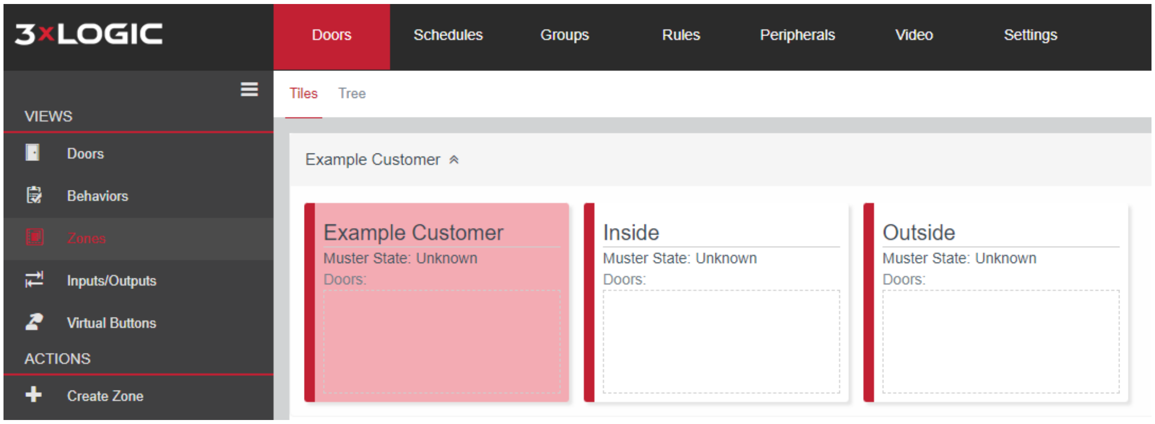
Note: Door Behaviors can be deleted only when there are no Doors configured to use this Behavior. Therefore, you might get an error popup dialog indicating that one or more Doors are still utilizing this Behavior. Assign a different Behavior to those Doors, and then delete the Behavior.

5.1.3 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.



Example Customer
Muster State: Unknown
Doors:

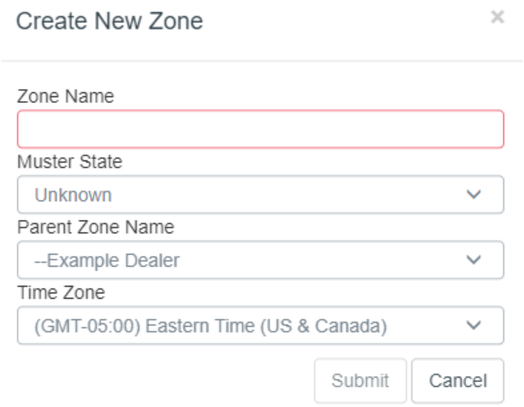
Inside
Muster State: Unknown
Doors:

Outside
Muster State: Unknown
Doors:

Figure 1-61: Zones

Create Zone

Clicking Create Zone will pop up a small window with a few options.



Zone Name

Muster State: Unknown

Parent Zone Name: --Example Dealer

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Figure 1-62: Create Zone

LABEL	DESCRIPTION
Zone Name	Name the zone however you want to identify the location requiring authorization to enter.
Muster State	■ Muster has three states: ▶ **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.

Multiple Doors

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 gives a visual example of how a zone may affect multiple doors.

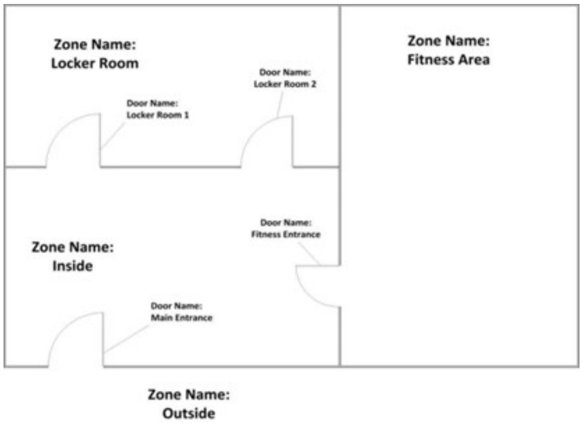
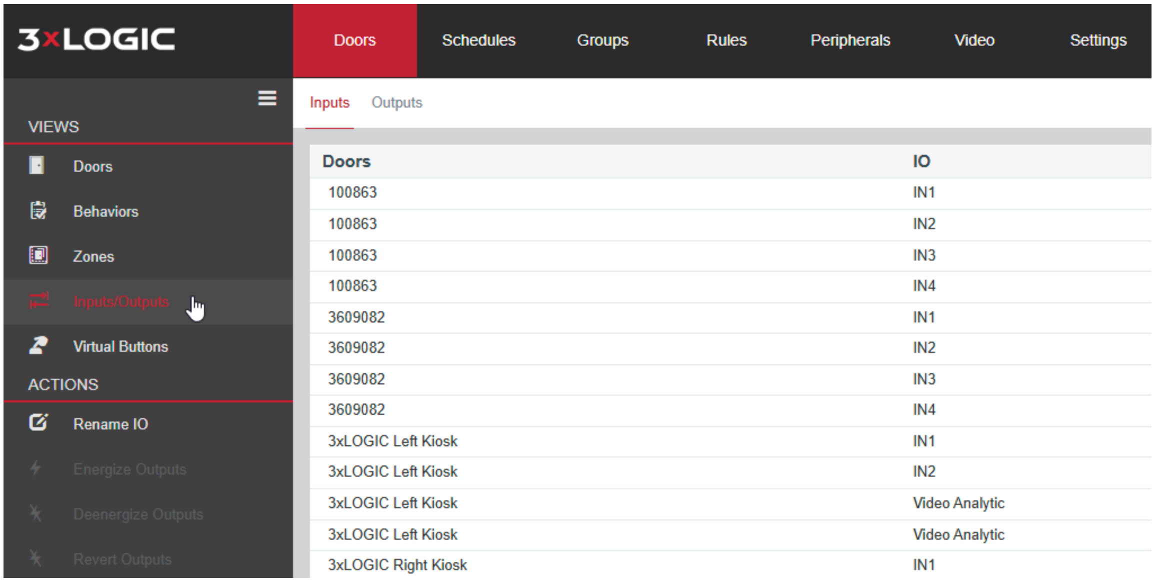


Figure 1-63: Zone Diagram

5.1.4 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.

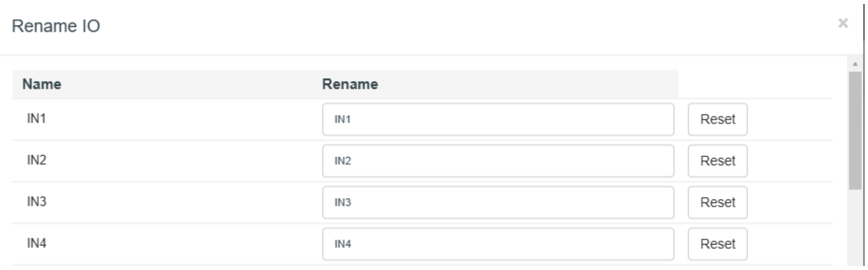


Doors	IO
100863	IN1
100863	IN2
100863	IN3
100863	IN4
3609082	IN1
3609082	IN2
3609082	IN3
3609082	IN4
3xLOGIC Left Kiosk	IN1
3xLOGIC Left Kiosk	IN2
3xLOGIC Left Kiosk	Video Analytic
3xLOGIC Left Kiosk	Video Analytic
3xLOGIC Right Kiosk	IN1

Figure 1-64: Inputs/Outputs

Rename I/O

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.

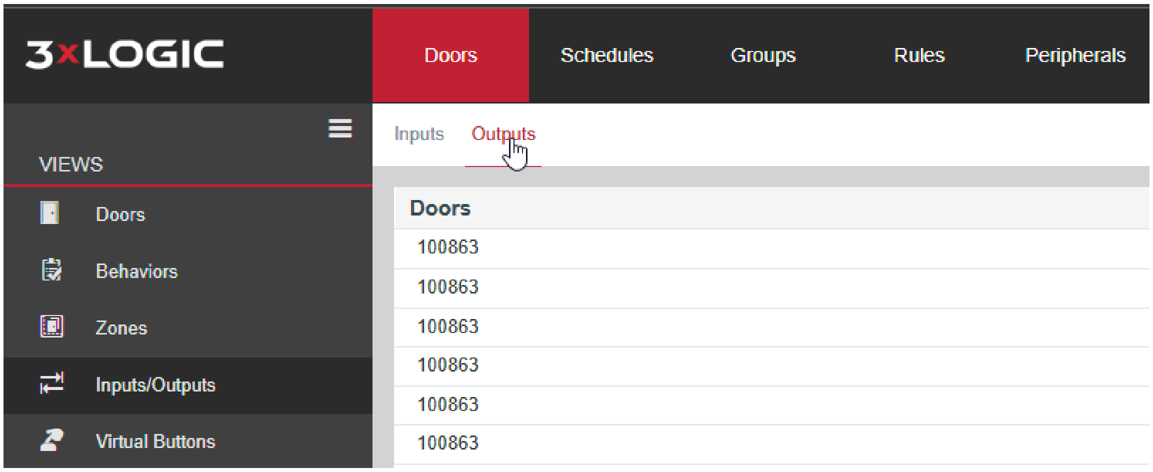


Name	Rename	
IN1	IN1	Reset
IN2	IN2	Reset
IN3	IN3	Reset
IN4	IN4	Reset

Figure 1-65: Rename IO

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.



Doors
100863
100863
100863
100863
100863
100863

Figure 1-66: Outputs

Renaming outputs follows the same procedure as renaming inputs.

5.1.5 Virtual Buttons

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.

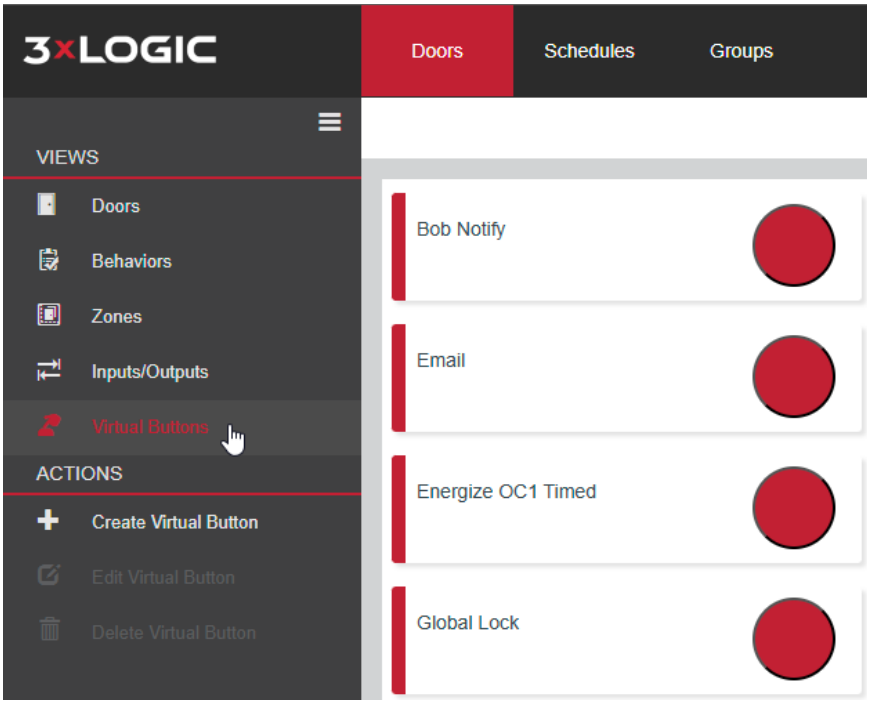
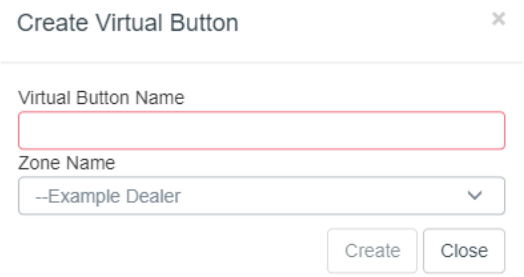


Figure 1-67: Virtual Button Configuration

Configuration

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.



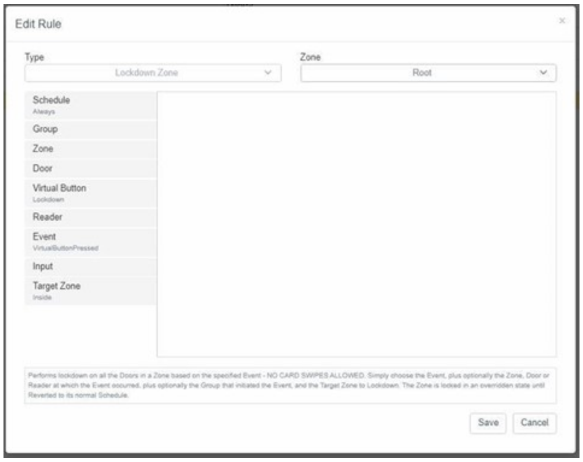
Create Virtual Button

Virtual Button Name

Zone Name: --Example Dealer

Figure 1-68: Create Button

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.



Edit Rule

Type: Lockdown Zone

Zone: Root

Schedule: Always

Group

Zone

Door

Virtual Button: Lockdown

Reader

Event: VirtualButtonPressed

Input

Target Zone: Inside

Performs lockdown on all the Doors in a Zone based on the specified Event - NO CARD SWIPES ALLOWED. Simply choose the Event, plus optionally the Zone, Door or Reader at which the Event occurred, plus optionally the Group that initiated the Event, and the Target Zone to Lockdown. The Zone is locked in an overridden state until Reverted to its normal Schedule.

Figure 1-69: 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 INFINIAS Access software; INFINIAS CLOUD is also supported in this manner. The user must also have an access privilege rule assigned to the zone the button is in to see it in the Mobile Credential app. See the separate*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.

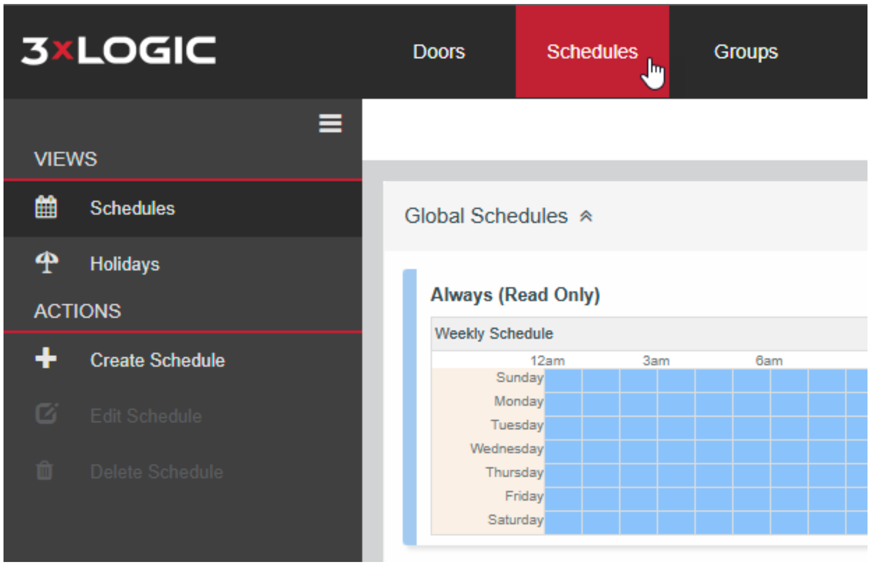


Figure 1-70: Schedules Tab

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.

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:

- Schedules View
- 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.

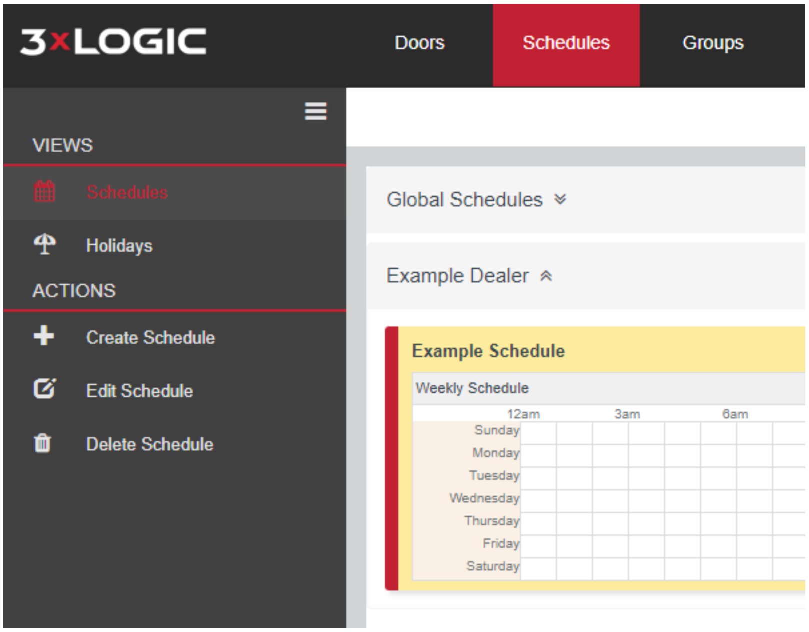


Figure 1-71: Schedules View

The Schedules View provides three Actions for managing Schedules, which consist of:

- Create Schedule
- Edit Schedule
- Delete Schedule

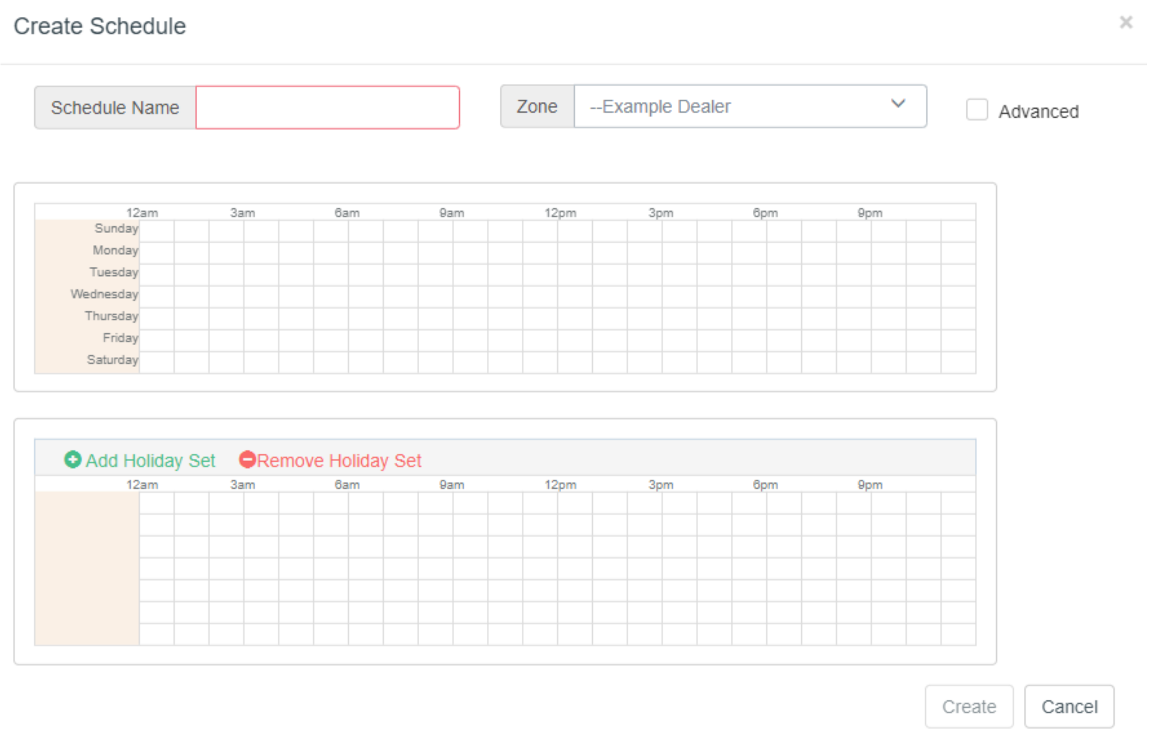
Create Schedule

To create a Schedule, perform the following 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 singleday.

   Note: If you'd like more granularity with your schedule than 15-minute blocks, click the Advanced Box; schedule segments created in Advanced mode are purple.

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



Create Schedule

Schedule Name:

Zone: --Example Dealer

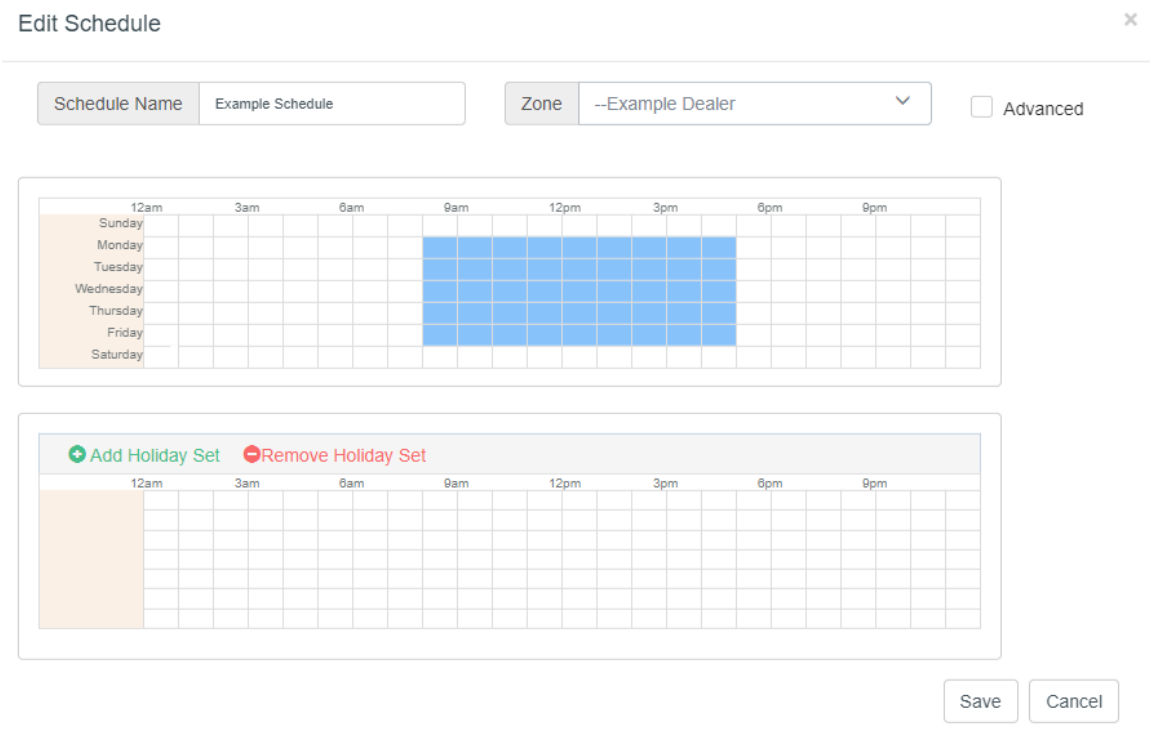
□ Advanced

Figure 1-72: Create Schedule

Edit Schedule

To modify a Schedule, perform the following steps:

1. Click the Edit Schedule Action.
2. Change the Schedule Name, and/or modify the Active Time Range using the same operations described earlier.
3. Click the Save button to save your changes.



Edit Schedule

Schedule Name: Example Schedule

Zone: --Example Dealer

☐ Advanced

Figure 1-73: Edit Schedule

Delete Schedule

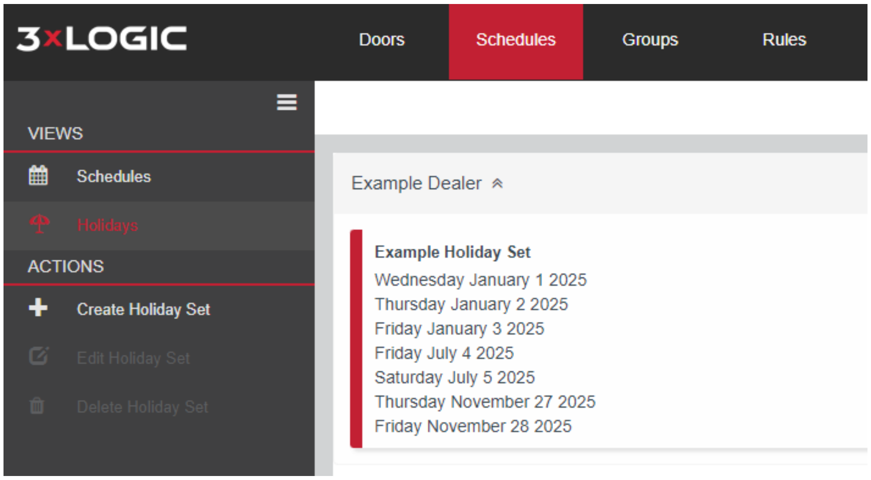
If you no longer need a Schedule, you can remove it:

1. Click the Delete Schedule Action.
2. A confirmation message box will appear, and the Schedule will be deleted when you confirm.

Note: 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.

5.2.2 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.



Example Holiday Set
Wednesday January 1 2025
Thursday January 2 2025
Friday January 3 2025
Friday July 4 2025
Saturday July 5 2025
Thursday November 27 2025
Friday November 28 2025

Figure 1-74: Holiday Set

Holidays View provides three Actions for managing Holiday Sets, which consist of:

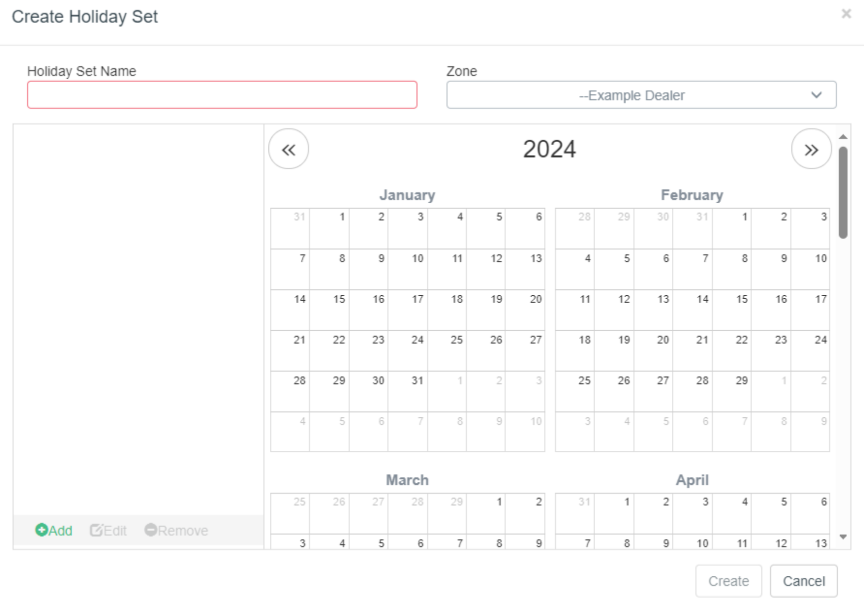
- Create Holiday Set
- Edit Holiday Set
- Delete Holiday Set

Note: There is a limit of 7 holiday sets per schedule

Create Holiday Set

To add Holiday exceptions to your schedule, you must first create a Holiday Set to contain your list of Holidays:

1. 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.



Create Holiday Set

Holiday Set Name:

Zone: --Example Dealer

Figure 1-75: Add Holiday Set

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 allow access.

Edit Holiday Set

To modify a Holiday Set:

1. Click the Edit Holiday Set Action.
2. Click on dates in the calendar to add or remove Holidays to or from the Set
3. Click the Edit button to rename a Holiday or change its date.
4. When finished, press the Save button to save your changes.

Delete Holiday Set

If you do not need a particular Holiday Set, you can remove it:

1. Press the Delete Holiday Set Action.
2. A confirmation message box appears and the Holiday Set will be deleted after confirmation.

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.

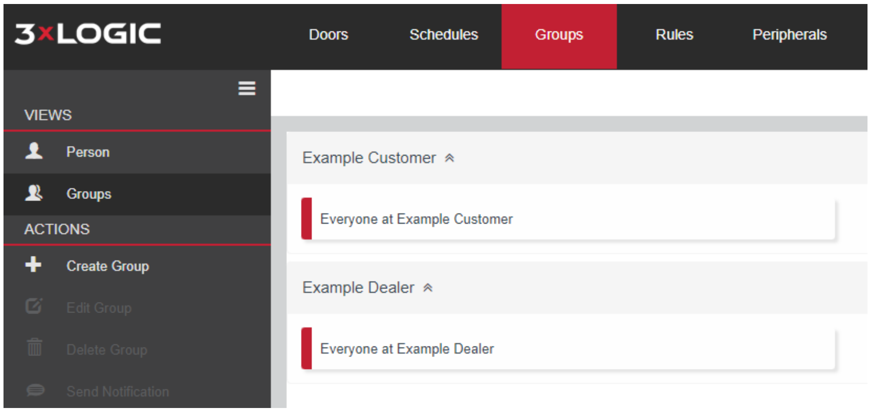


Figure 1-76: Groups Tab

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.

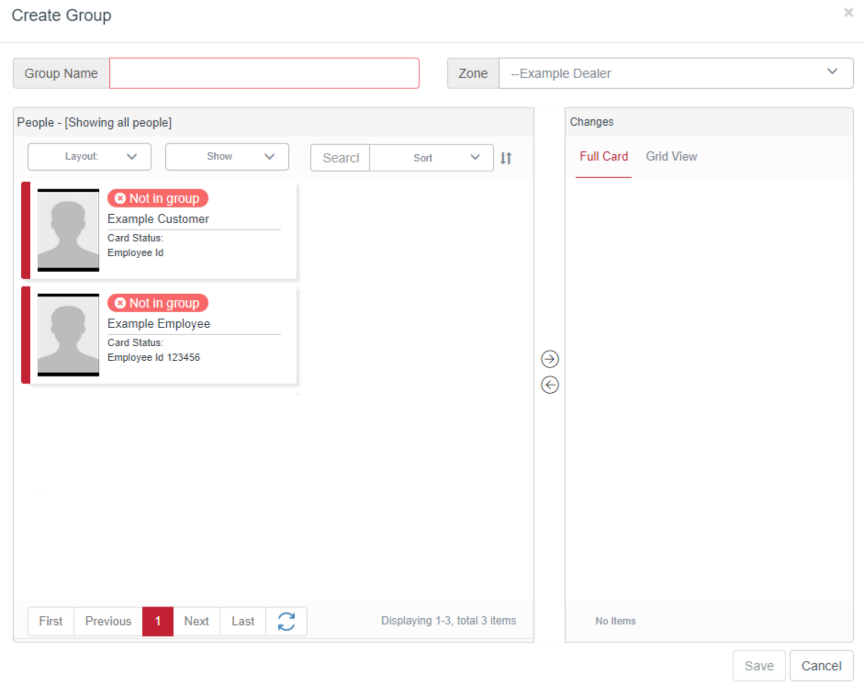


Figure 1-77: Create Group

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

Removes the selected Group.

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.

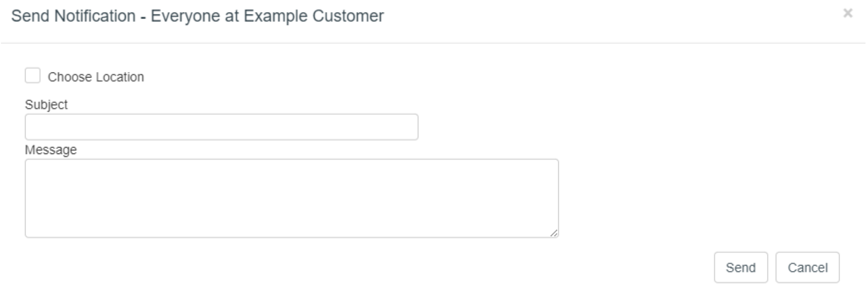


Figure 1-78: Send Notification

5.4 Rules Tab

The rules engine, the core part of the INFINIAS 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.

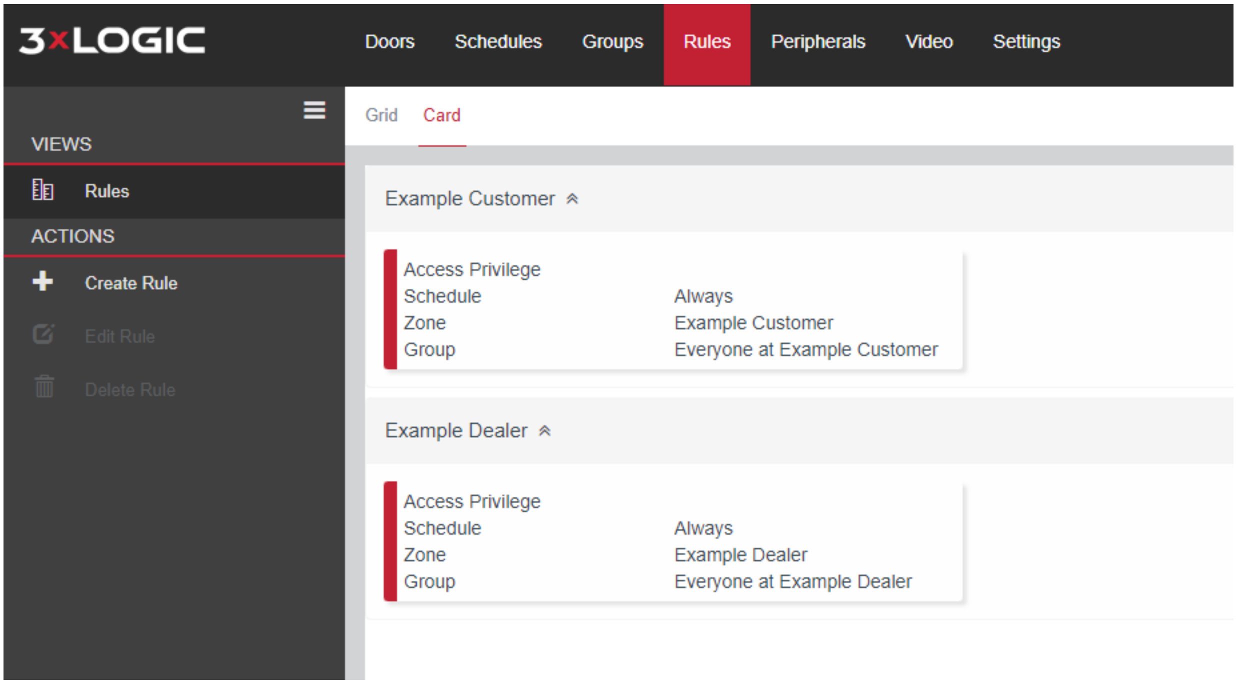
There are many rule types listed in the default rules list and many more that can be added or even customized by the support team to provide any number of ways to get the system to function the way a particular site requires for security purposes. The default rules range from the access privilege rule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

5.4.1 Views

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.



Example Customer

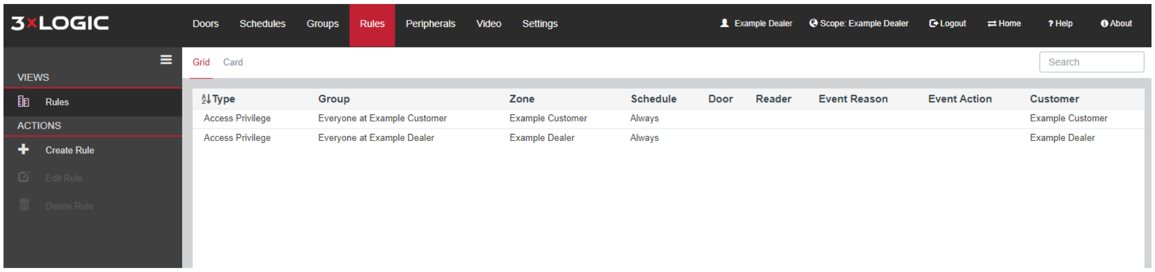
Access Privilege
Schedule Always
Zone Example Customer
Group Everyone at Example Customer

Example Dealer

Access Privilege
Schedule Always
Zone Example Dealer
Group Everyone at Example Dealer

Figure 1-79: 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.



Type	Group	Zone	Schedule	Door	Reader	Event Reason	Event Action	Customer
Access Privilege	Everyone at Example Customer	Example Customer	Always					Example Customer
Access Privilege	Everyone at Example Dealer	Example Dealer	Always					Example Dealer

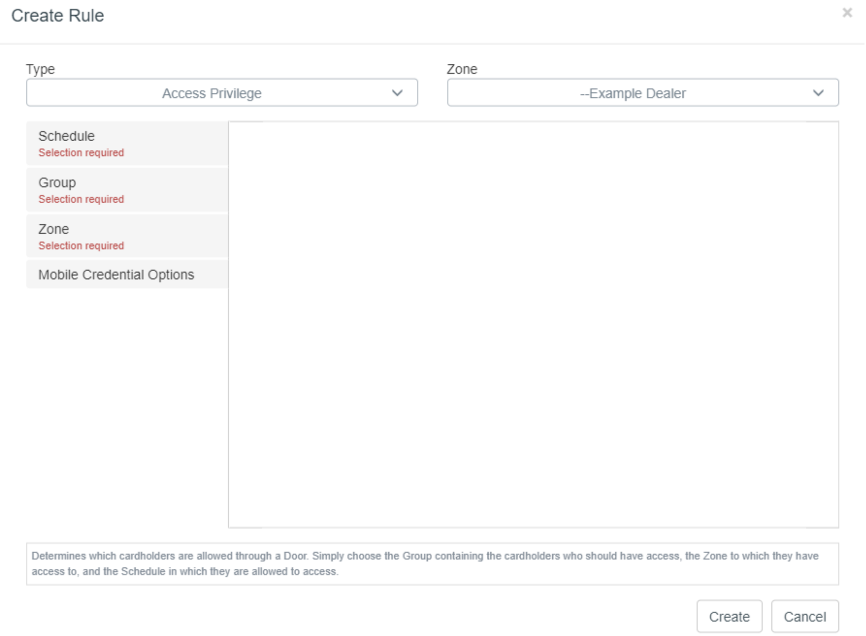
Figure 1-80: Grid View

5.4.2 Create Rule

In an INFINIAS 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.

Note: 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.



Type: Access Privilege

Zone: --Example Dealer

Schedule
Selection required

Group
Selection required

Zone
Selection required

Mobile Credential Options

Determines which cardholders are allowed through a Door. Simply choose the Group containing the cardholders who should have access, the Zone to which they have access to, and the Schedule in which they are allowed to access.

Figure 1-81: Create View

There are three primary things that make a rule work: Schedule, Group, and Zone.

- **Schedule**
  - The time the rule will be active.
  - In the case of the access privilege rule, this will be when the group will be able to access the zone.
- **Group**
  - The people being affected by the rule based on the schedule and tied to the zone.
- **Zone**
  - The location the group is entering based on the schedule tied to the rule.
  - The *Zone* is one or more doors. See "Doors Tab" on page 32 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.

The following sections list some common rule types and their workflows.

5.4.3 Event Management

The Event Management Rule allows events to be shown on the Events page.

5.4.4 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.

Workflow Steps:

1. Select **Hide Event** in the Rule Type drop-down list box.
2. Select a **Schedule**, which 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.

5.4.5 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, INFINIAS Access creates five Alarm Management Rules to manage all the Access Denied event possibilities.

Workflow Steps:

1. To create a new Alarm Management Rule, select **Alarm Management** in the Rule Type drop-down list box.
2. Select a **Schedule**, which 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 an Alarm.

5.4.6 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' events 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.

5.4.7 Email Events

- 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. The emails will come from noreply@3xlogic.com.

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.

Workflow Steps:

1. Select **Email Event** in the Rule Type drop-down list box.
2. Select a **Schedule**, which 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 the recipients.
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 the recipients.
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.

5.4.8 Locking Rules

This section includes details for Lock Zone, Lockdown Zone, and UnlockZone.

- 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).
  - Furthermore, the **Revert Zone** Rule is also similar, except that it reverts the Zone's Doors to their Scheduled lock state.

Workflow 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**, which 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 eventtrigger.
5. Select a **Door** (optional). This is an additional filter for the eventtrigger.
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.

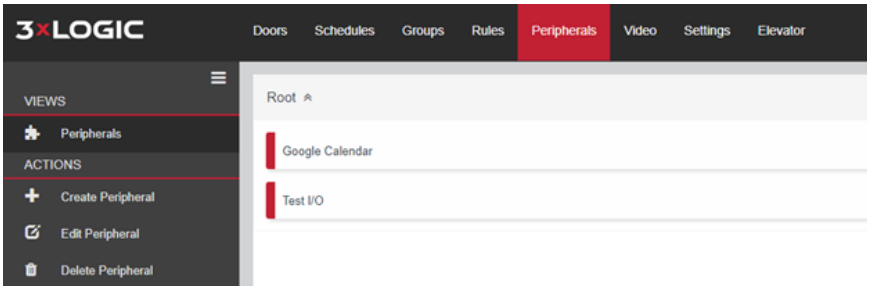


Figure 1-82: Peripherals

The purpose of a Peripheral is to provide INFINIAS 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 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.

Generic

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 Access 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.

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.

Google Calendar

This allows users to create exception schedule by simply scheduling a meeting on a monitored Google account. For more information, please reference the Google Calendar Integration section of this user guide.

Microsoft Outlook Exchange Calendar

This allows users to create exception schedule by simply scheduling a meeting on a monitored Microsoft Exchange account. For more information, please reference the Outlook Exchange Calendar Integration section of this user guide.

5.5.2 Edit Peripheral

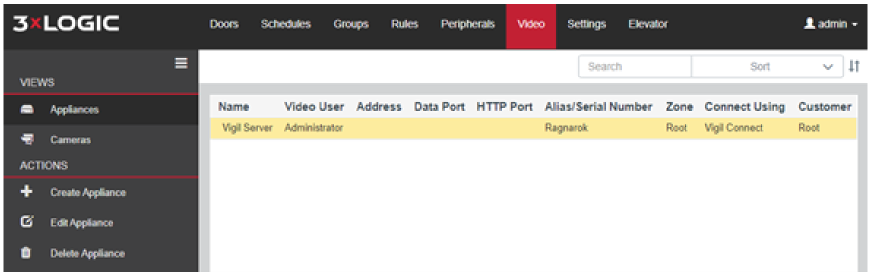
You can modify the Peripherals you have created using the **Edit Peripheral** Action. Make the necessary changes in the configuration user interface and press the Save button found at the bottom of the device configuration user interface.

5.5.3 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 the action.

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 INFINIAS Access.



Name	Video User	Address	Data Port	HTTP Port	Alias/Serial Number	Zone	Connect Using	Customer
Vigil Server	Administrator				Ragnarok	Root	Vigil Connect	Root

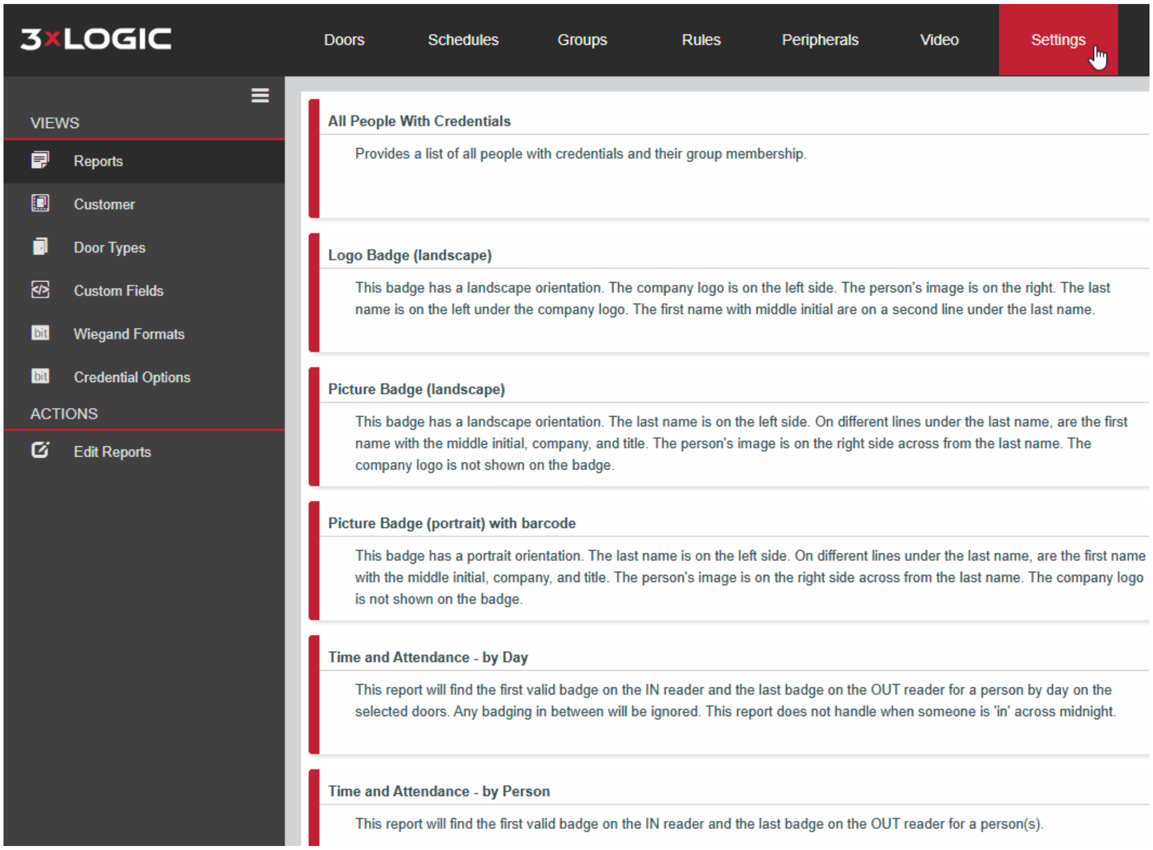
Figure 1-83: Video Tab

Configuration of the video integration requires access to the Vigil DVR/Stand-alone camera and the INFINIAS 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.

Note: Please reference "VIGIL Video Integration" on page 138.

5.7 Settings Tab

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



All People With Credentials

Provides a list of all people with credentials and their group membership.

Logo Badge (landscape)

This badge has a landscape orientation. The company logo is on the left side. The person's image is on the right. The last name is on the left under the company logo. The first name with middle initial are on a second line under the last name.

Picture Badge (landscape)

This badge has a landscape orientation. The last name is on the left side. On different lines under the last name, are the first name with the middle initial, company, and title. The person's image is on the right side across from the last name. The company logo is not shown on the badge.

Picture Badge (portrait) with barcode

This badge has a portrait orientation. The last name is on the left side. On different lines under the last name, are the first name with the middle initial, company, and title. The person's image is on the right side across from the last name. The company logo is not shown on the badge.

Time and Attendance - by Day

This report will find the first valid badge on the IN reader and the last badge on the OUT reader for a person by day on the selected doors. Any badging in between will be ignored. This report does not handle when someone is 'in' across midnight.

Time and Attendance - by Person

This report will find the first valid badge on the IN reader and the last badge on the OUT reader for a person(s).

Figure 1-84: Settings

5.7.1 Registration

This section is not present within INFINIAS CLOUD and only exists in the local installation packages.

This section covers Dealer, Customer, and licensing activation of the INFINIAS software. The Dealer and Customer information must be filled out in order to license the software. The **Activate** license link is unavailable (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.

Note: For further information on licensing and installation, please refer to the separate INFINIAS Access *Installation Guide*.

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.

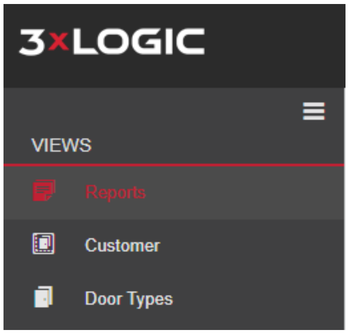
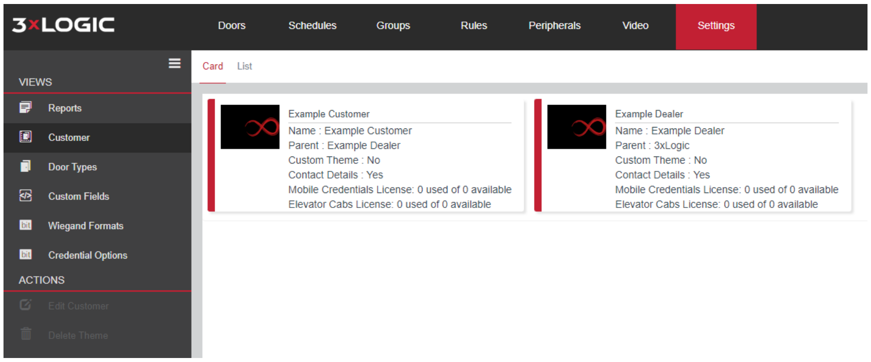


Figure 1-85: Reports

Note: Due to permission issues on software only installations, this option may cause an error if the system software is restricted.

5.7.3 Customer

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

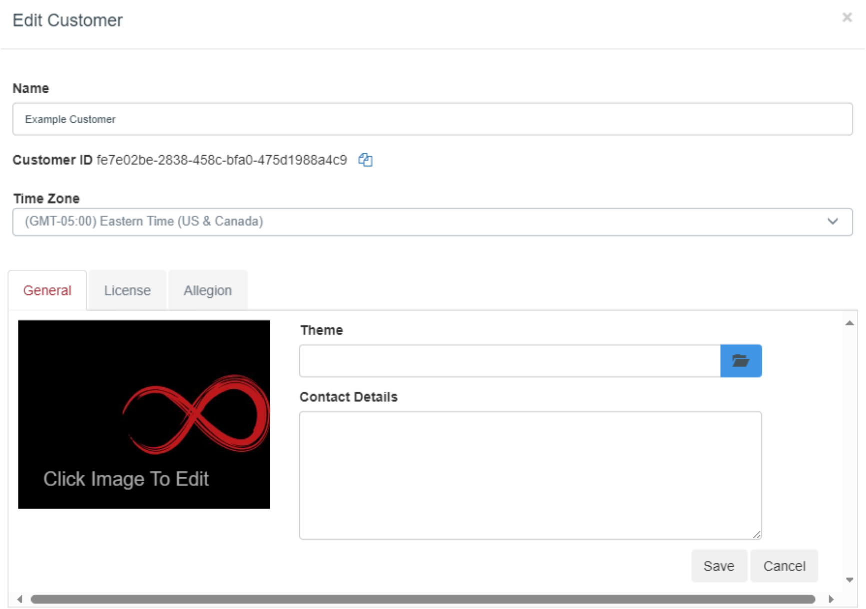


Example Customer
Name : Example Customer
Parent : Example Dealer
Custom Theme : No
Contact Details : Yes
Mobile Credentials License: 0 used of 0 available
Elevator Cabs License: 0 used of 0 available

Example Dealer
Name : Example Dealer
Parent : 3xLogic
Custom Theme : No
Contact Details : Yes
Mobile Credentials License: 0 used of 0 available
Elevator Cabs License: 0 used of 0 available

Figure 1-86: 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.



Edit Customer

Name: Example Customer

Customer ID fe7e02be-2838-458c-bfa0-475d1988a4c9

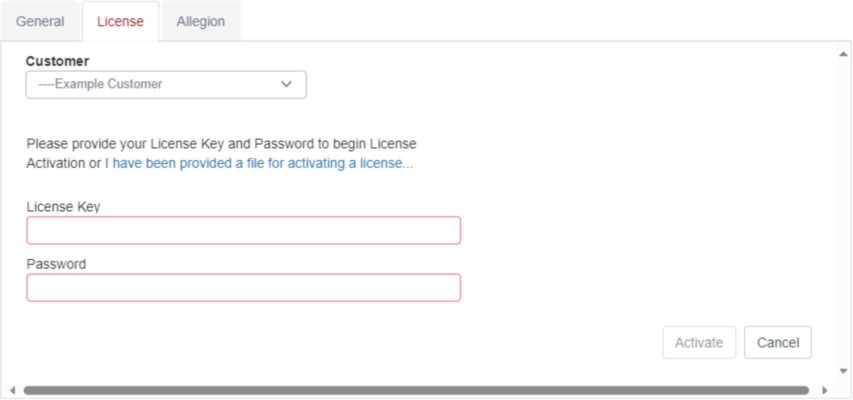
Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Theme

Contact Details

Figure 1-87: 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.



Customer: ----Example Customer

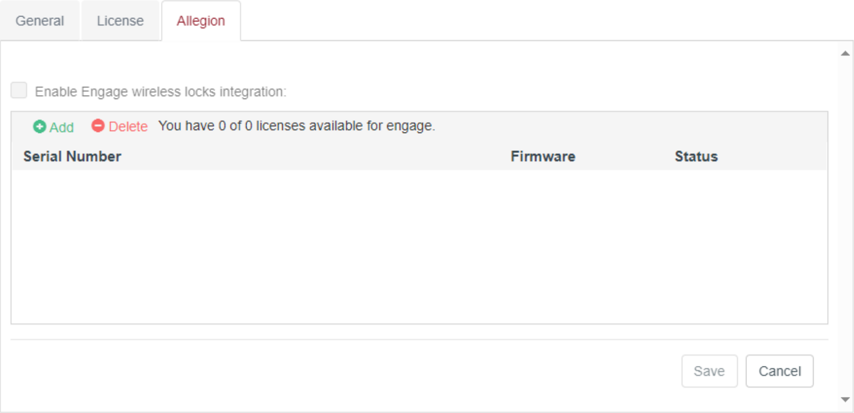
Please provide your License Key and Password to begin License Activation or I have been provided a file for activating a license...

License Key

Password

Figure 1-88: License

INFINIAS integrates with Allegion wireless locks. The Allegion tab allows the addition of Allegion licensing.



□ Enable Engage wireless locks integration:

You have 0 of 0 licenses available for engage.

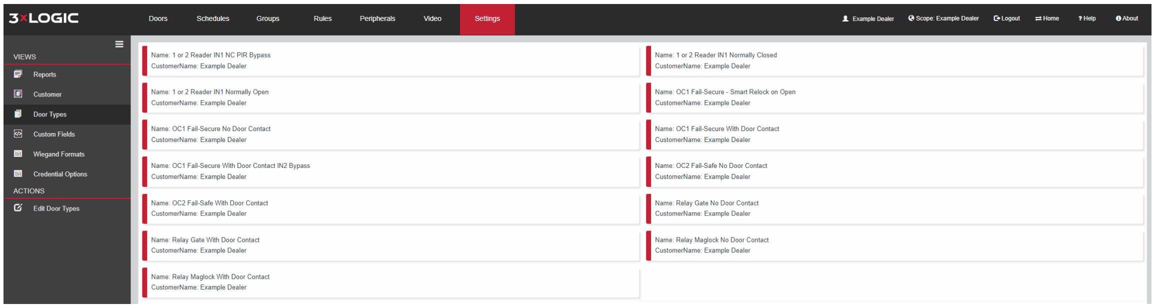
Serial Number	Firmware	Status

Figure 1-89: Allegion

For additional information on Allegion/Engage locksets and installation, please see the separate *S-Engage-Gateway Quick Start Guide*.

5.7.4 Door Types

The Door Types tab 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.



Name: 1 or 2 Reader IN1 NC PIR Bypass
CustomerName: Example Dealer

Name: 1 or 2 Reader IN1 Normally Closed
CustomerName: Example Dealer

Name: 1 or 2 Reader IN1 Normally Open
CustomerName: Example Dealer

Name: OC1 Fail-Secure - Smart Relock on Open
CustomerName: Example Dealer

Name: OC1 Fail-Secure No Door Contact
CustomerName: Example Dealer

Name: OC1 Fail-Secure With Door Contact
CustomerName: Example Dealer

Name: OC1 Fail-Secure With Door Contact IN2 Bypass
CustomerName: Example Dealer

Name: OC2 Fail-Safe No Door Contact
CustomerName: Example Dealer

Name: OC2 Fail-Safe With Door Contact
CustomerName: Example Dealer

Name: Relay Gate No Door Contact
CustomerName: Example Dealer

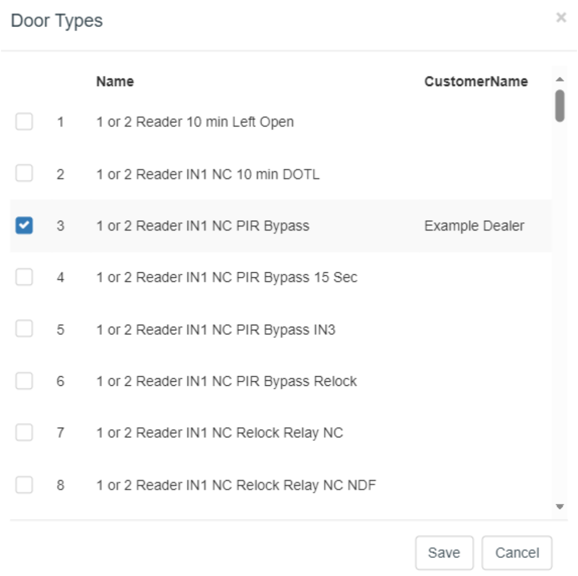
Name: Relay Gate With Door Contact
CustomerName: Example Dealer

Name: Relay Maglock No Door Contact
CustomerName: Example Dealer

Name: Relay Maglock With Door Contact
CustomerName: Example Dealer

Figure 1-90: Door Types Tab

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.



Door Types

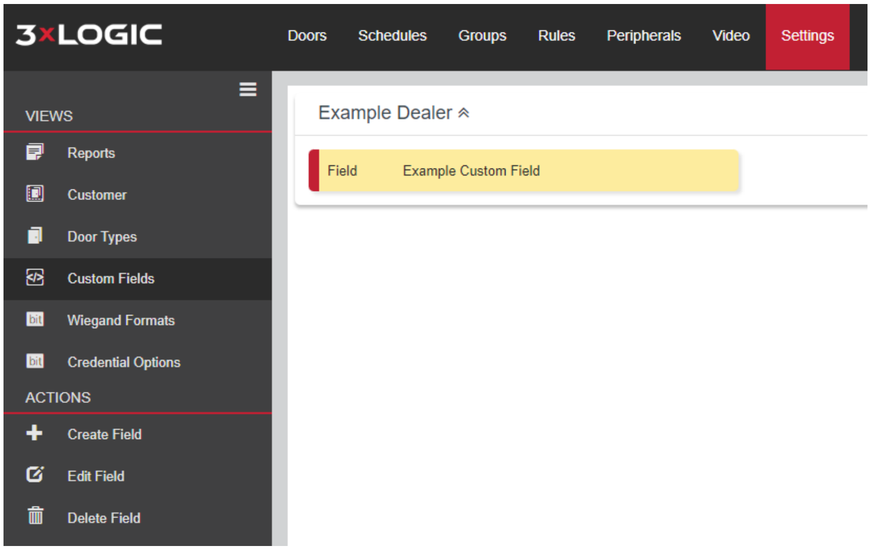
		Name	CustomerName
□	1	1 or 2 Reader 10 min Left Open	
□	2	1 or 2 Reader IN1 NC 10 min DOTL	
☑	3	1 or 2 Reader IN1 NC PIR Bypass	Example Dealer
□	4	1 or 2 Reader IN1 NC PIR Bypass 15 Sec	
□	5	1 or 2 Reader IN1 NC PIR Bypass IN3	
□	6	1 or 2 Reader IN1 NC PIR Bypass Relock	
□	7	1 or 2 Reader IN1 NC Relock Relay NC	
□	8	1 or 2 Reader IN1 NC Relock Relay NC NDF	

Figure 1-91: Add Door

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.



Example Dealer

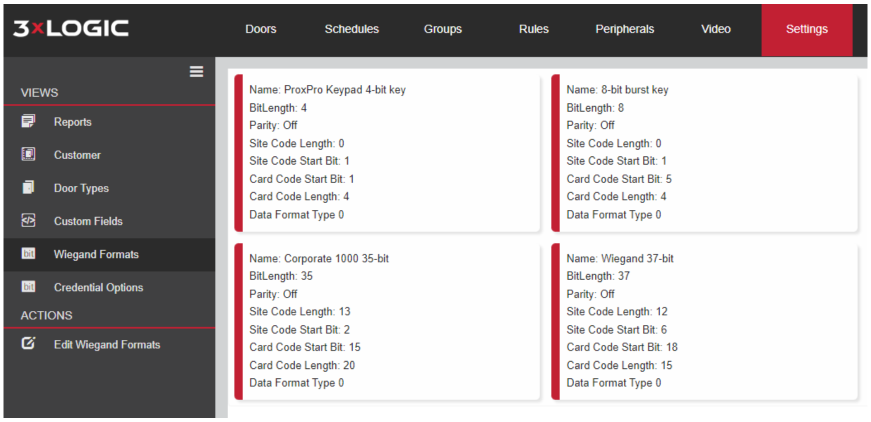
Field	Example Custom Field

Figure 1-92: Custom Fields

5.7.6 Wiegand Formats

INFINIAS Access and INFINIAS CLOUD have a multitude of supported Wiegand formats ranging from 26 to 64 bit in length. However, INFINIAS does not 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. INFINIAS supports 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.



Name: ProxPro Keypad 4-bit key
BitLength: 4
Parity: Off
Site Code Length: 0
Site Code Start Bit: 1
Card Code Start Bit: 1
Card Code Length: 4
Data Format Type 0

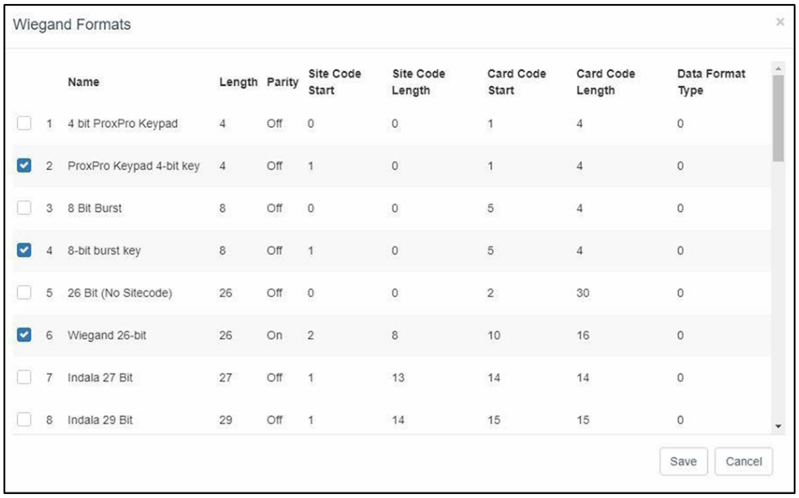
Name: 8-bit burst key
BitLength: 8
Parity: Off
Site Code Length: 0
Site Code Start Bit: 1
Card Code Start Bit: 5
Card Code Length: 4
Data Format Type 0

Name: Corporate 1000 35-bit
BitLength: 35
Parity: Off
Site Code Length: 13
Site Code Start Bit: 2
Card Code Start Bit: 15
Card Code Length: 20
Data Format Type 0

Name: Wiegand 37-bit
BitLength: 37
Parity: Off
Site Code Length: 12
Site Code Start Bit: 6
Card Code Start Bit: 18
Card Code Length: 15
Data Format Type 0

Figure 1-93: Wiegand Formats

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


Wiegand Formats

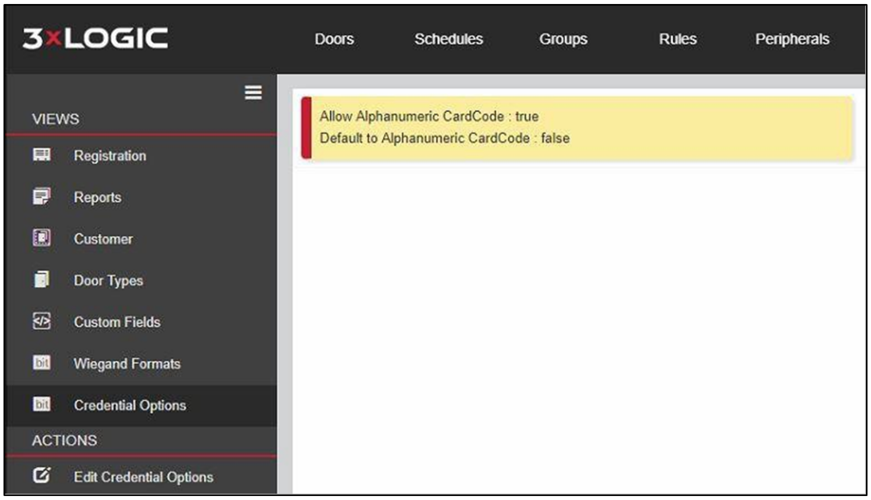
		Name	Length	Parity	Site Code Start	Site Code Length	Card Code Start	Card Code Length	Data Format Type
☐	1	4 bit ProxPro Keypad	4	Off	0	0	1	4	0
☑	2	ProxPro Keypad 4-bit key	4	Off	1	0	1	4	0
☐	3	8 Bit Burst	8	Off	0	0	5	4	0
☑	4	8-bit burst key	8	Off	1	0	5	4	0
☐	5	26 Bit (No Sitecode)	26	Off	0	0	2	30	0
☑	6	Wiegand 26-bit	26	On	2	8	10	16	0
☐	7	Indala 27 Bit	27	Off	1	13	14	14	0
☐	8	Indala 29 Bit	29	Off	1	14	15	15	0

Figure 1-94: Enable 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.

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.



Allow Alphanumeric CardCode : true
Default to Alphanumeric CardCode : false

Figure 1-95: Credential Options

5.8 System Settings

For On-Premises physical installations (On-Prem), users with administrative access have an additional tab for system variables using the System Settings section. This is distinct from the general *Settings Tab*.

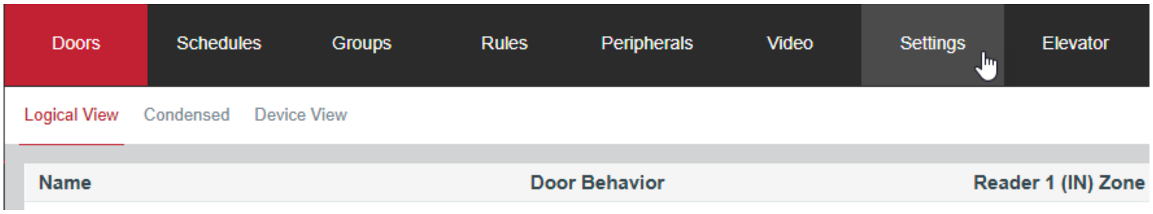


Figure 1-96: Settings Tab

After selecting *Configuration*, the top menus change.

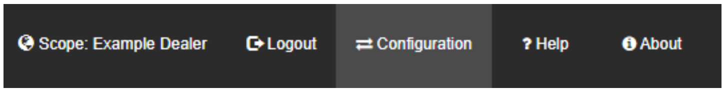


Figure 1-97: Configuration

The **System Settings** appears in the top menu between *Help* and *About*.

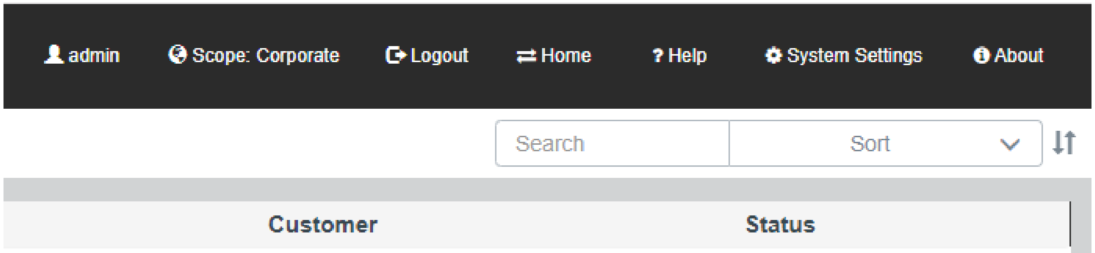
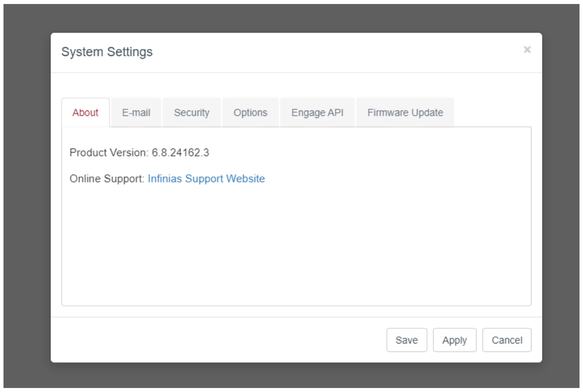


Figure 1-98: System Settings (top right)

5.8.1 About

The *About* tab under System Settings mirrors the other "About" option in the top menu, but, notably, does not contain a direct link to the Privacy Policy.



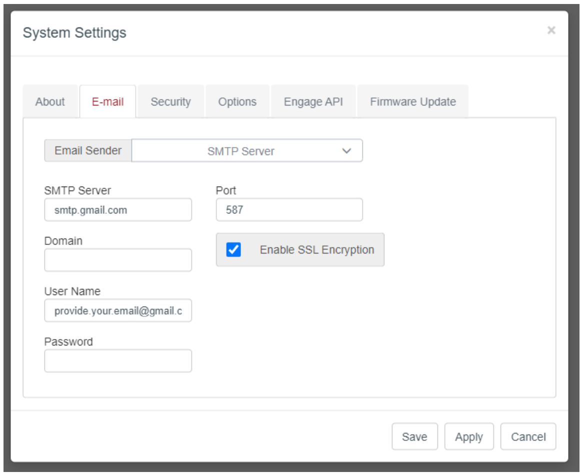
Product Version: 6.8.24162.3

Online Support: Infinias Support Website

Figure 1-99: System Settings > About

5.8.2 E-mail

The *E-mail* tab under System Settings is for administrative users to set up an SMTP Server and customize email alerts.



Email Sender: SMTP Server

SMTP Server: smtp.gmail.com

Port: 587

Domain:

☑ Enable SSL Encryption

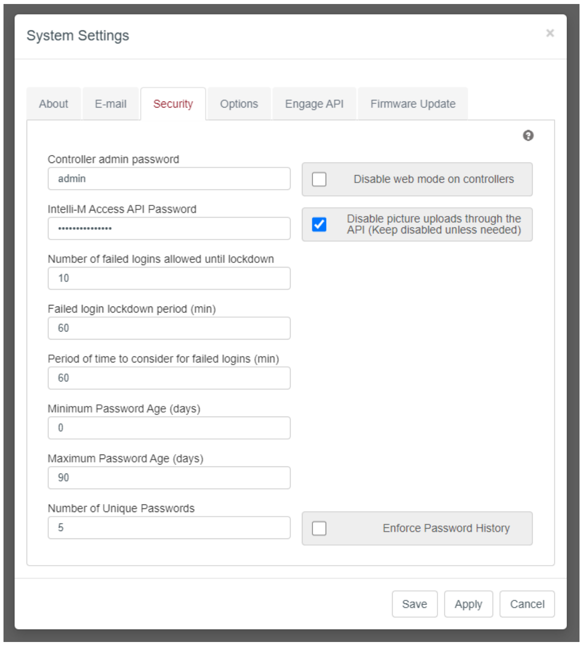
User Name: provide.your.email@gmail.c

Password:

Figure 1-100: System Settings > Email

5.8.3 Security

The *Security* tab under System Settings enables changes to software variables.



Controller admin password: admin

☐ Disable web mode on controllers

Intelli-M Access API Password: •••••••••••••••

☑ Disable picture uploads through the API (Keep disabled unless needed)

Number of failed logins allowed until lockdown: 10

Failed login lockdown period (min): 60

Period of time to consider for failed logins (min): 60

Minimum Password Age (days): 0

Maximum Password Age (days): 90

Number of Unique Passwords: 5

☐ Enforce Password History

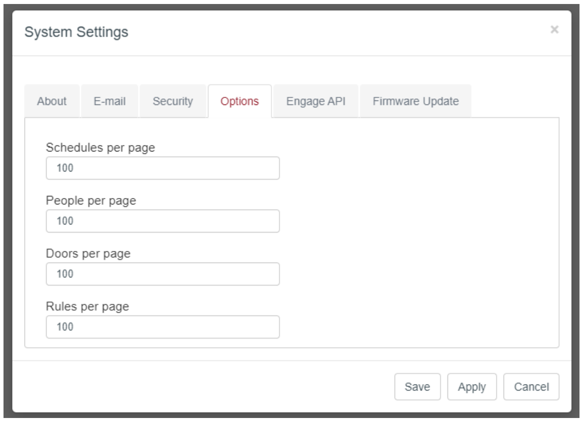
Figure 1-101: System Settings > Security

- **API Password**
  - This password is for the INFINIAS Rule Action service.
  - Changing it requires custom configuration in other areas of the application.
- **Number of failed logins allowed until lockdown**
  - This is the number of attempts a user is allowed to make with an incorrect password before their account is put into lockdown status.
- **Failed login lockdown period**
  - This is the amount of time in minutes that a user account will stay in lockdown status after failing to provide a correct password in the number of attempts specified above.
- **Period of time to consider for failed logins**
  - This is the amount of time that must pass before a user's failed attempts count will reset.
- **Minimum password age**
  - This is the minimum number of days that must pass before a user is allowed to change their password.
- **Maximum password age**
  - This is the maximum number of days a user can use the same password until they are required to change it.
  - 1 - 999 is the allowed range.
- **Number of unique Passwords**

  - Set the number of unique passwords a user must create before reusing a prior password.
- **Enforce password history**
  - Enforces the unique password policy if checked.
- **eIDC32 Password**
  - This password must be 10 characters or less and may not include any of the following special characters: # & = + \ ' " < > / ?
- **Disable web mode on controllers**
  - Checking this box will disable web UI access on infinias door controllers which prevents access of the device using its IP address.
- **Disable picture uploads through the API**
  - Checking this box disables picture uploads through the API/Active Directory integration.

5.8.4 Options

The *Options* tab under System Settings allows administrative users to set pagination for Schedules, People, Doors, and Rules per page.



Schedules per page: 100

People per page: 100

Doors per page: 100

Rules per page: 100

Figure 1-102: System Settings > Options

5.8.5 Engage API and Firmware Update

See "Allegion ENGAGE Integration" on page 187 regarding the *Engage API* tab and do not use the *Firmware Update* tab unless specifically instructed.

5.9 Transition

This concludes the content specific to the INFINIAS Essentials configuration. The following sections 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 INFINIAS Essentials software does not.

6 INFINIAS Professional

The INFINIAS 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. INFINIAS Professional opens the door to utilize Active Directory, Elevator Control, Outlook Exchange, and Google calendar integrations.

6.1 Primary Integrations Overview

- **Elevator Control**

This integration 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.

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

- **VIGIL Video**

Connect a VIGIL Server or V-Series Camera to Doors within INFINIAS CLOUD for the purposes of viewing video on the **INFINIAS Mobile App**. See "VIGIL Video Integration" on page 138.

- **Active Directory**

INFINIAS Access Professional integrates with the Active Directory Server in your organization to allow the Active Directory Administrator to manage INFINIAS Access cardholders within the Active Directory User management system rather than within the INFINIAS Access User Interface. This integration provides the convenience of not having to learn and use yet another user management system on a daily basis. See "Active Directory Integration" on page 154

- **Outlook Exchange**

INFINIAS integrates with Microsoft Office (O365) to allow Outlook Meetings to create exception schedules for doors controlled by INFINIAS. This form of ad-hoc scheduling allows you to schedule a door to unlock at meeting start and re-lock at meeting end, helping an organization to control door access for events that do not occur on a predictable schedule. INFINIAS is designed to act as a way for Microsoft Exchange to send Meeting Reminder, Meeting Started, and Meeting Ended Events to INFINIAS for specified Exchange Room Mailboxes, and for all relevant Meeting Attendees. The integration plugin accomplishes this task by monitoring the Calendar of each specified Exchange Room Mailbox. See "Microsoft Calendar Integration" on page 162.

- **Google Calendar**

INFINIAS Professional integrates with Google Calendar to allow Appointments to automatically unlock and re-lock doors controlled by INFINIAS. See "Google Calendar Integration" on page 180.

- **Allegion Engage**

The S-ENGAGE Gateway device enables communication with Allegion wireless door locks. See "Allegion ENGAGE Integration" on page 187.

6.2 Active Directory

Unlike most Active Directory (AD) integrations, INFINIAS Access does not merely authenticate the provided credentials to AD for a pass/fail result. Instead, it queries AD for real-time changes to its user database and reflects those changes within the INFINIAS 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 INFINIAS 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 INFINIAS Access' users and groups, that integration is one-way. At no time does INFINIAS Access modify AD with its own data, even if the UI is utilized in INFINIAS Access instead of AD, the path remains one way.

Note: It is recommended that no attempt to modify persons within INFINIAS Access once a link to Active Directory becomes 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.

6.2.1 Active Directory Checklist

The Active Directory (AD) integration requires direct involvement with and assistance from an IT representative within your organization. INFINIAS maps AD attributes such as First Name, Last Name, Title, Department, Phone Number, Primary Email, and other important data points with the INFINIAS Access *person* entry. 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 INFINIAS Access.

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

INFINIAS LABEL	AD 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 hosted by Microsoft online.

- The Domain Controller that is used must have the PDC (primary domain controller) role.
- You must then 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.

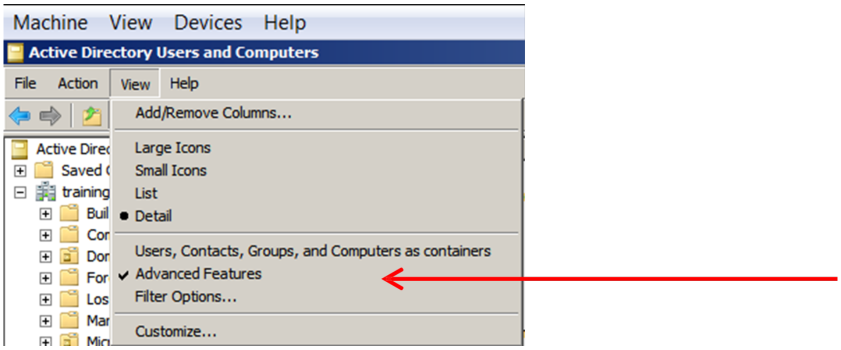


Figure 1-103: Advanced Features

- In addition to the mappings listed here, 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 INFINIAS Access.

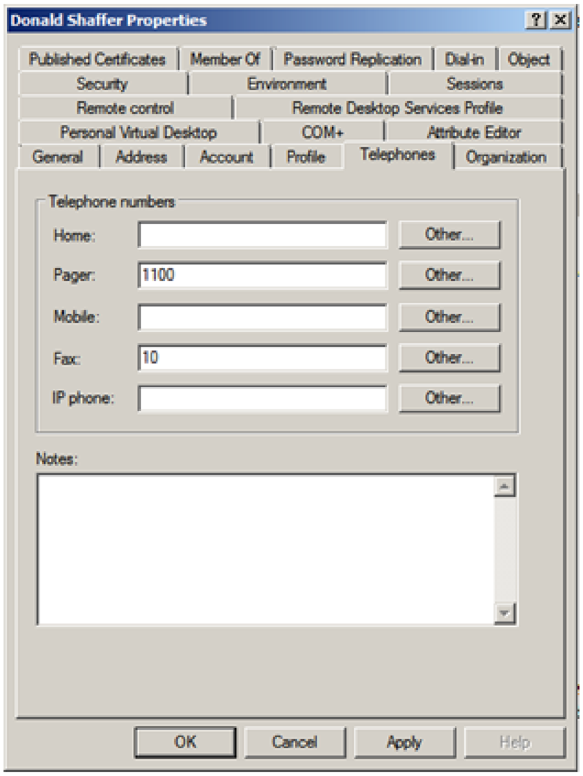
6.2.2 Site Codes and Card Codes

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 "Active Directory Checklist" on the previous page, 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.



Home:

Pager: 1100

Mobile:

Fax: 10

IP phone:

Figure 1-104: AD - Site Code & Card Number

6.2.3 PIN Code Attribute

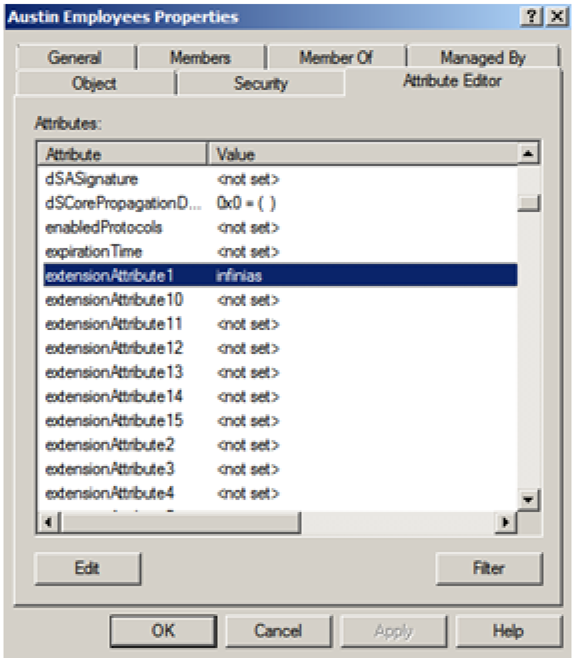
INFINIAS offers the option to reserve an Active Directory attribute to be used as the PIN code for the user. Just repeat the steps for "Site Codes and Card Codes" on the previous page to select the desired attribute and document the selection.

6.2.4 Group Filter Attribute

Active Directory contains numerous Groups that are not only of no value to INFINIAS 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*, etc. 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 INFINIAS 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.



Attribute	Value
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
enabledProtocols	<not set>
expirationTime	<not set>
extensionAttribute1	infinias
extensionAttribute10	<not set>
extensionAttribute11	<not set>
extensionAttribute12	<not set>
extensionAttribute13	<not set>
extensionAttribute14	<not set>
extensionAttribute15	<not set>
extensionAttribute2	<not set>
extensionAttribute3	<not set>
extensionAttribute4	<not set>

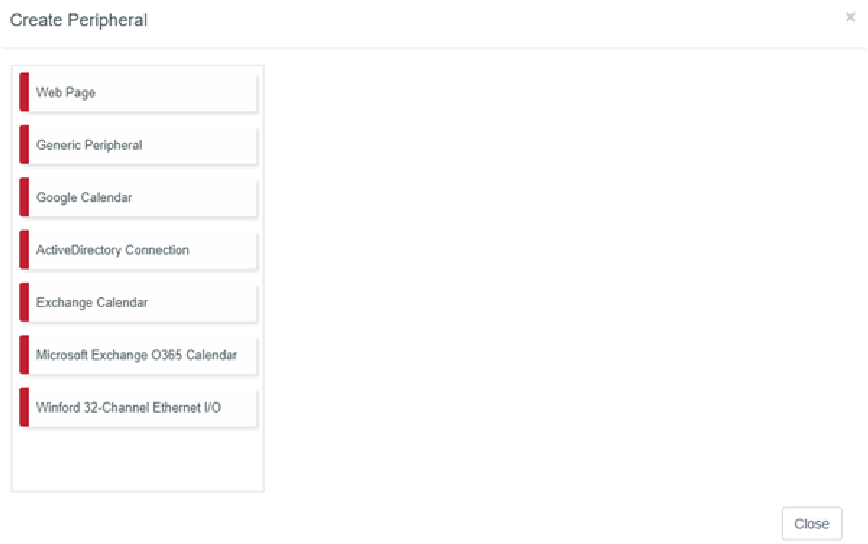
Figure 1-105: AD - Group Properties

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.

6.2.5 Create Peripheral

1. To create a **Peripheral**, login to INFINIAS and proceed to the Peripherals Page under the Configuration Section.
2. Click the Create Peripheral Action and a Create Peripheral Dialog will appear.

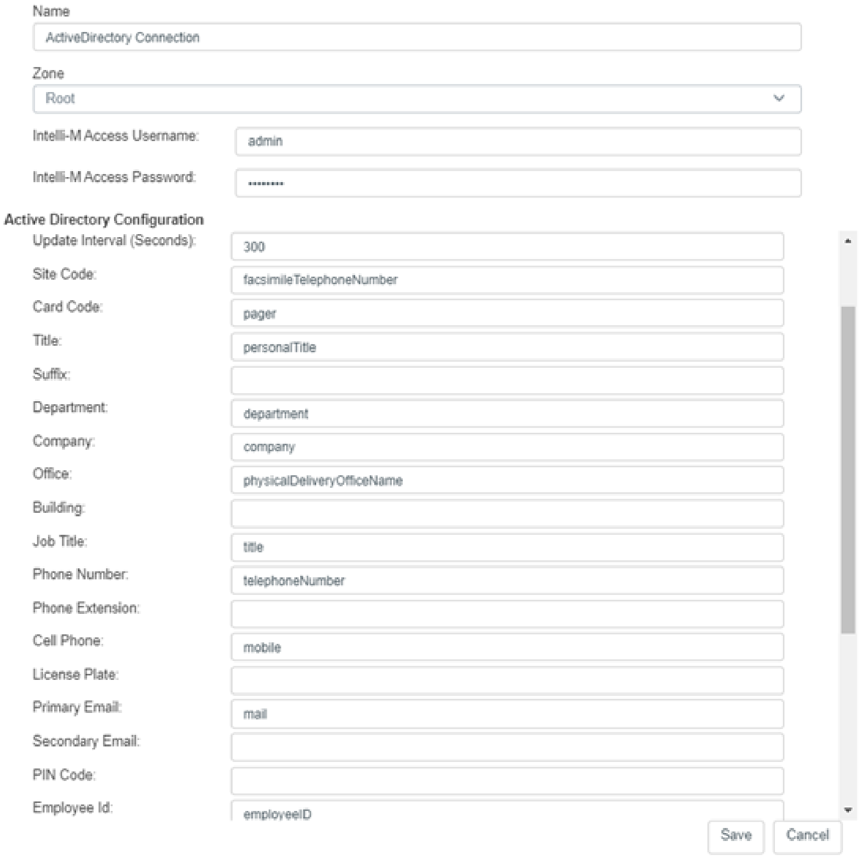


Create Peripheral

×
Web Page
Generic Peripheral
Google Calendar
ActiveDirectory Connection
Exchange Calendar
Microsoft Exchange O365 Calendar
Winford 32-Channel Ethernet I/O
Close

Figure 1-106: AD - Create Peripheral

3. Select the ActiveDirectory Connection.
    a. 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.
    b. 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.



Name

ActiveDirectory Connection

Zone

Root

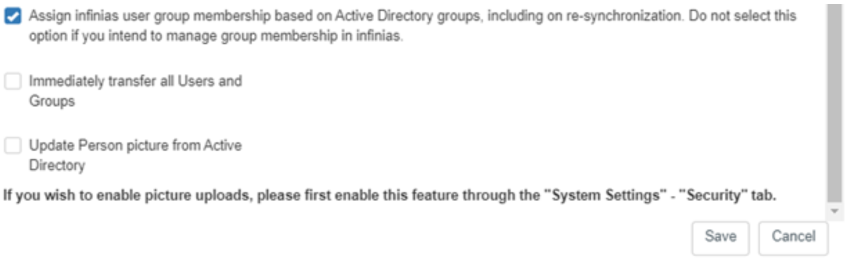
Intelli-M Access Username:	admin
Intelli-M Access Password:	••••••••

Active Directory Configuration

Update Interval (Seconds):	300
Site Code:	facsimileTelephoneNumber
Card Code:	pager
Title:	personalTitle
Suffix:	
Department:	department
Company:	company
Office:	physicalDeliveryOfficeName
Building:	
Job Title:	title
Phone Number:	telephoneNumber
Phone Extension:	
Cell Phone:	mobile
License Plate:	
Primary Email:	mail
Secondary Email:	
PIN Code:	
Employee Id:	employeeID

Figure 1-107: AD - Create Connection

4. 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.



☑ Assign infinias user group membership based on Active Directory groups, including on re-synchronization. Do not select this option if you intend to manage group membership in infinias.

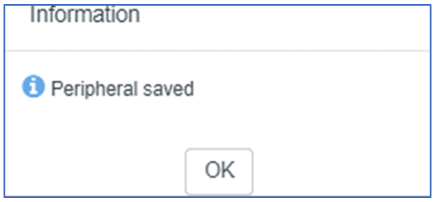
□ Immediately transfer all Users and Groups

□ Update Person picture from Active Directory

If you wish to enable picture uploads, please first enable this feature through the "System Settings" - "Security" tab.

Figure 1-108: AD - Checkboxes

5. The system will then connect to the Domain Controller and start listening for changes to the Windows Users and Groups.
    a. 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.
6. Upon completion, an Information Dialog box will display with a notification that the Peripheral has been saved.



Information

Peripheral saved

Figure 1-109: AD - Save Confirmation

Peripheral Attribute Table

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.
INFINIAS 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.
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 reuse 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 INFINIAS 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 INFINIAS Access.

6.3 Elevator Control

This section covers the control setup and configuration.

Support for older generations 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 generation of relay assembly as described in this guide.

6.3.1 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.

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.

Note: Please reference "Configuring and Creating a Hosted Door" on page 107 in order to properly setup the device for the system using that guide.

Now that the door is online, configuration can continue.

- Navigate to the settings tab under configuration and register the elevator license provided when purchased the relay assembly.
- Once completed, refresh the page and the new Elevator Tab will appear in two places.
  - Both the configuration section and the home page have an Elevator tab now.

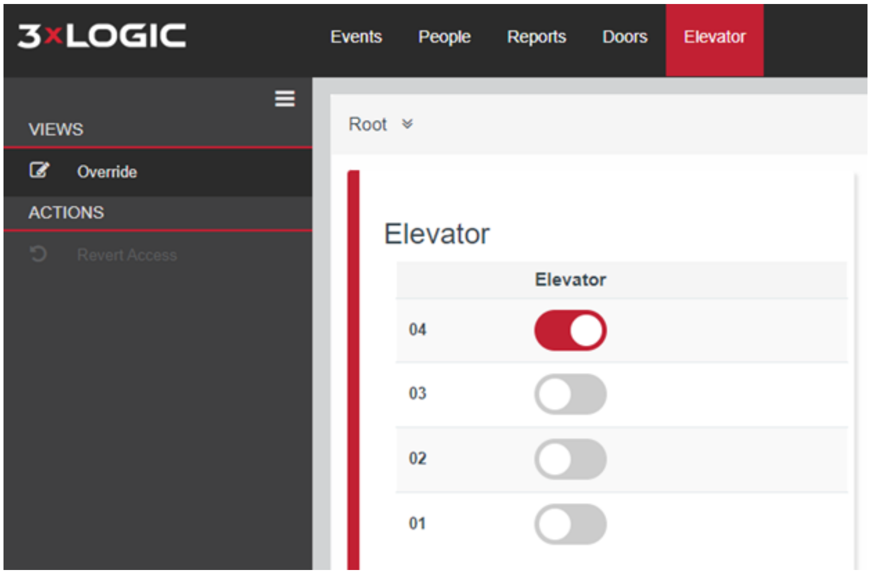
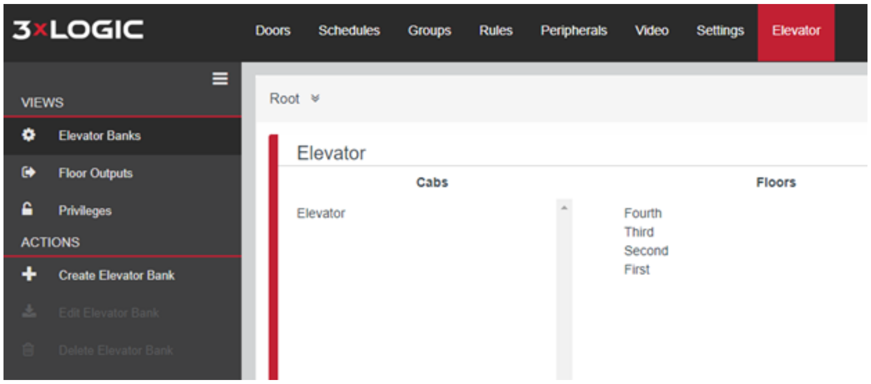


Figure 1-110: Elevator (Home Page)



Elevator

Cabs	Floors
Elevator	Fourth Third Second First

Figure 1-111: Elevator (Configuration)

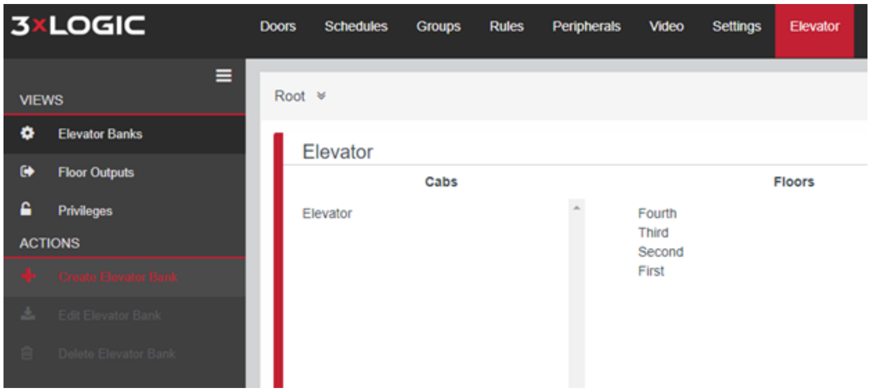
- They are used for different purposes and this guide will review both.

6.3.2 Elevator Tab

Navigate to the elevator tab and add important information. The default view is Elevator Banks.

Elevator Banks

The page will be blank when a new cab is created.



Elevator

Cabs	Floors
Elevator	Fourth Third Second First

Figure 1-112: Elevator Banks

Click **Create Elevator Bank** under the action menu to the left and a new window will appear.

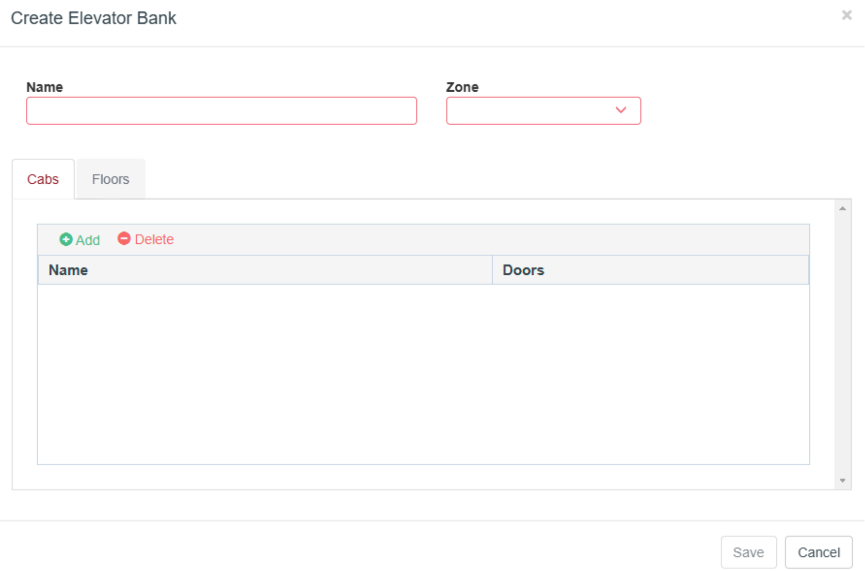
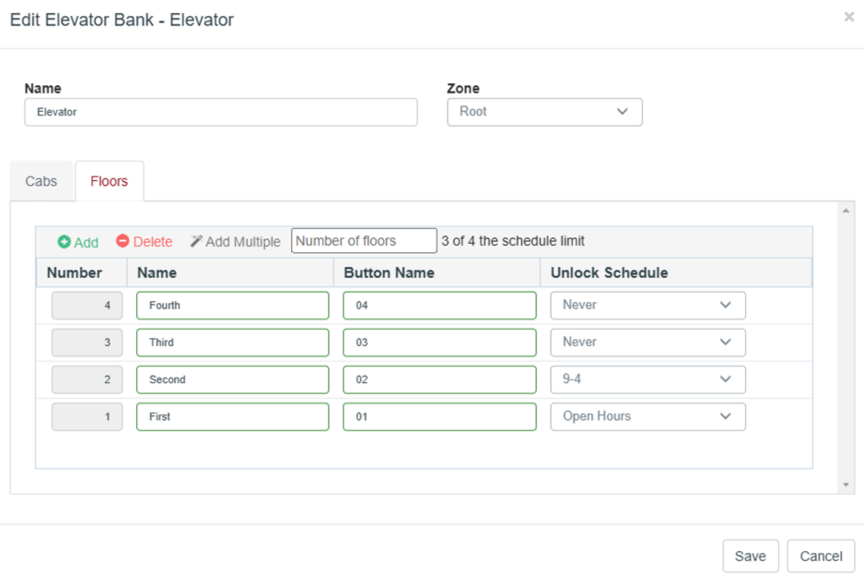


Figure 1-113: Create Elevator Bank

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



Edit Elevator Bank - Elevator

Name: Elevator

Zone: Root

3 of 4 the schedule limit

Number	Name	Button Name	Unlock Schedule
4	Fourth	04	Never
3	Third	03	Never
2	Second	02	9-4
1	First	01	Open Hours

Figure 1-114: 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.

Floor Outputs

The floor outputs are where the floors are tied to the relay outputs.

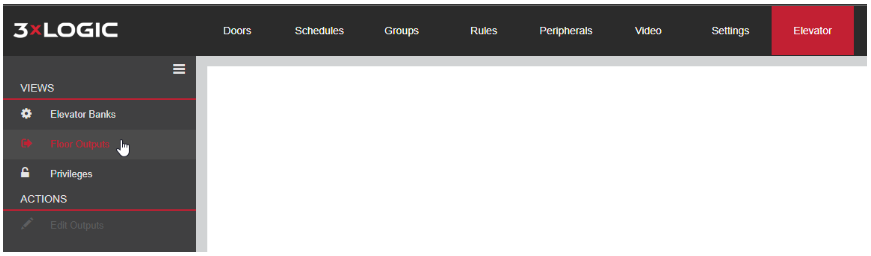
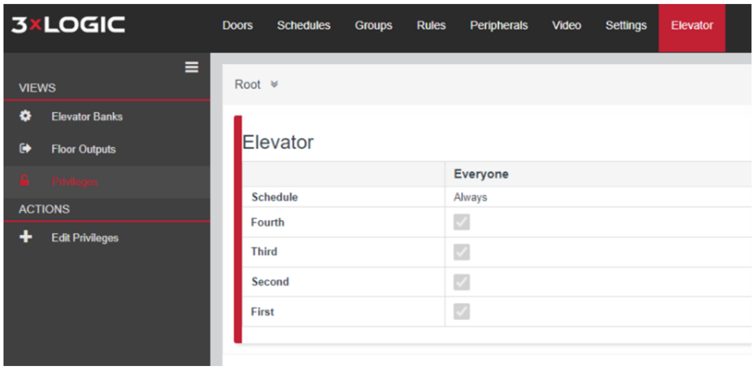


Figure 1-115: Elevator Floor Outputs

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.

Privileges

The **Privileges view** is where the group is tied to the floors.

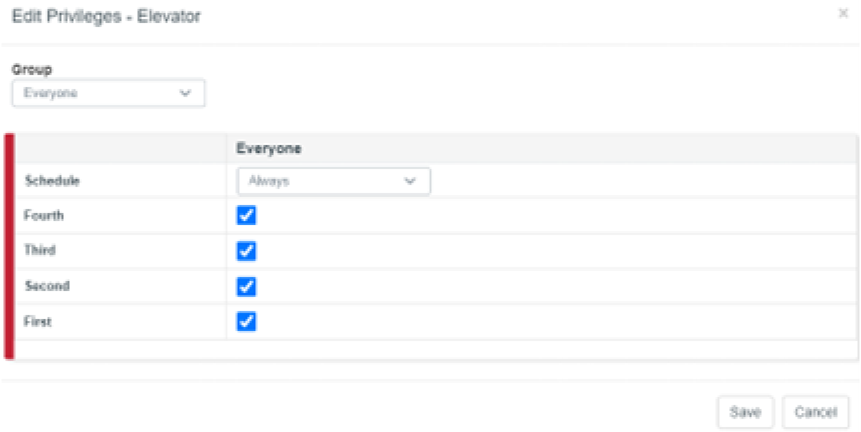


Elevator

	Everyone
Schedule	Always
Fourth	☑
Third	☑
Second	☑
First	☑

Figure 1-116: Elevator Privileges

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. There is no create privileges action on this page.



Edit Privileges - Elevator

Group: Everyone

	Everyone
Schedule	Always
Fourth	☑
Third	☑
Second	☑
First	☑

Figure 1-117: Edit Privileges

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.

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

Override

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.

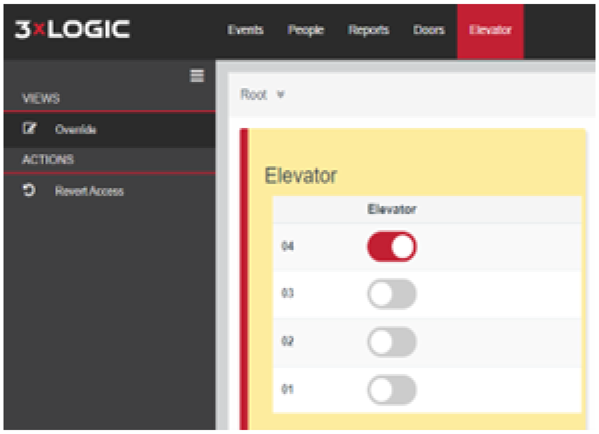


Figure 1-118: Elevator Override

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.

6.4 Microsoft Exchange

A separate document, the Exchange Server Integration User Guide, covers detailed setup steps for this integration. See "Microsoft Calendar Integration" on page 162.

6.5 Google Calendar

A separate document, the Google Calendar Integration User Guide, covers detailed setup steps for this integration. See "Google Calendar Integration" on page 180.

7 INFINIAS Corporate and CLOUD

Corporate and CLOUD packages are very similar in performance and what features they support. Corporate and CLOUD are being combined into one section as their differences are so few that it would be redundant to go over them.

7.1 Similarities

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

7.1.1 Zoning Trees

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

7.2 Differences

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.

7.2.1 Corporate

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 versions of INFINIAS.

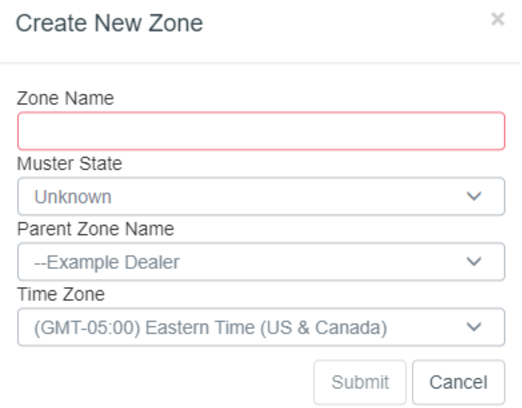
7.2.2 CLOUD

INFINIAS CLOUD is a multi-tenant designed software that resides on the web. It is accessible from anywhere and from any device that has the capability to browse the web. It allows a **Dealer** to manage their customers to maintain their accounts and service the on-site hardware. It is designed for **Customers** who are more interested in accessing the UI from anywhere without having to deal with server maintenance or software updates. INFINIAS CLOUD supports all features other than active directory integration.

7.3 Zoning Tree Configuration

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.


Create New Zone

Zone Name:

Muster State: Unknown

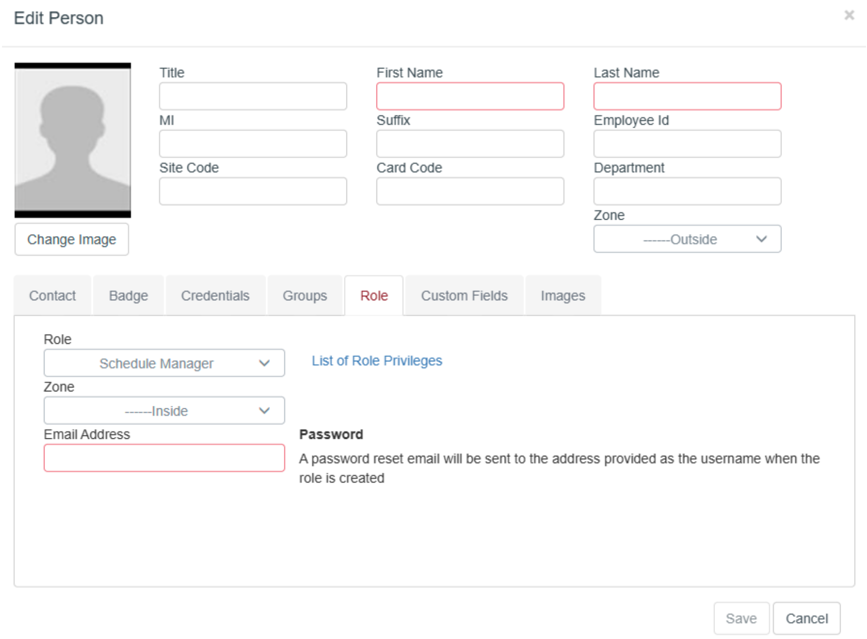
Parent Zone Name: --Example Dealer

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Figure 1-119: Create New Zone

7.3.1 Role Zone Assignment

The Role Zone Assignment is where you assign a user with a Role to a Zone by *Editing* a Person. 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.


Edit Person

Title: | First Name: | Last Name:
MI: | Suffix: | Employee Id:
Site Code: | Card Code: | Department:

Zone: ------Outside

Role: Schedule Manager

Zone: ------Inside

Email Address:

Password

A password reset email will be sent to the address provided as the username when the role is created

Figure 1-120: Role Zone

7.3.2 Scope

The more Zones and Rules that are created within the software the more complicated it can be to navigate and configure. Therefore, INFINIAS Access 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 displays 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 is in the upper right-hand corner of the user interface or collapsed under the username if in a smart device or small laptop screen.

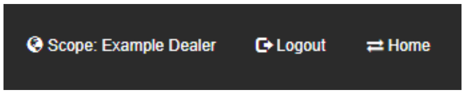


Figure 1-121: Scope

INFINIAS Access has the ability to go up one scope level from the currently viewed scope.

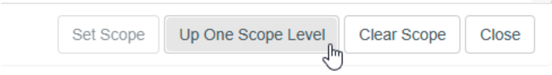


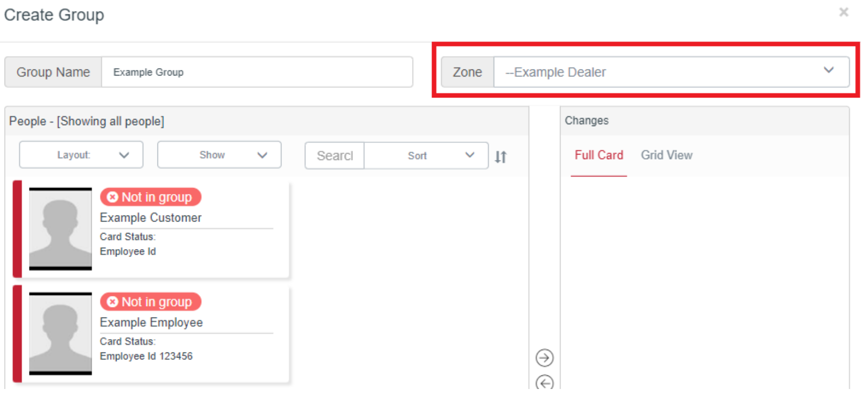
Figure 1-122: Scope Level

Click the currently selected Scope to display a list with available options, which include:

- Set Scope
- Up One Scope Level
- Clear Scope
- Close

7.3.3 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.


Create Group

Group Name: Example Group

Zone: --Example Dealer

Figure 1-123: Zone Assignment

7.3.4 CLOUD Logout

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).

7.3.5 Help Button

Points **Customers** to their **Dealer's** contact information.

7.3.6 Zone Hierarchy

The following visuals illustrate Zone Hierarchy:

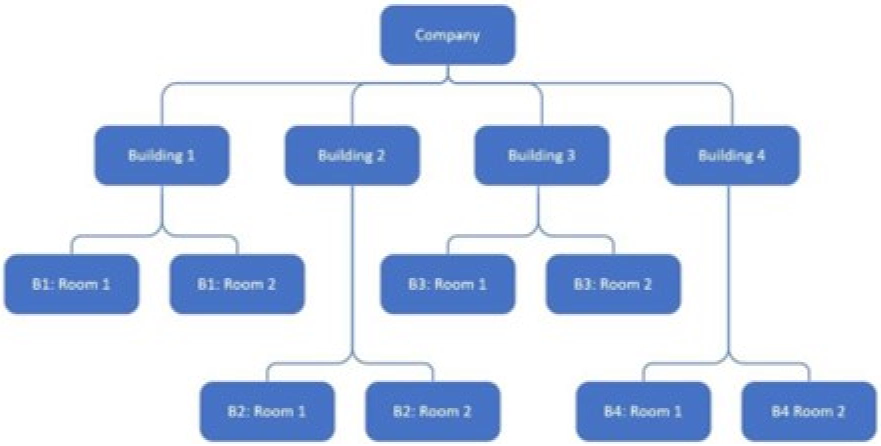


Figure 1-124: Zone Hierarchy Diagram

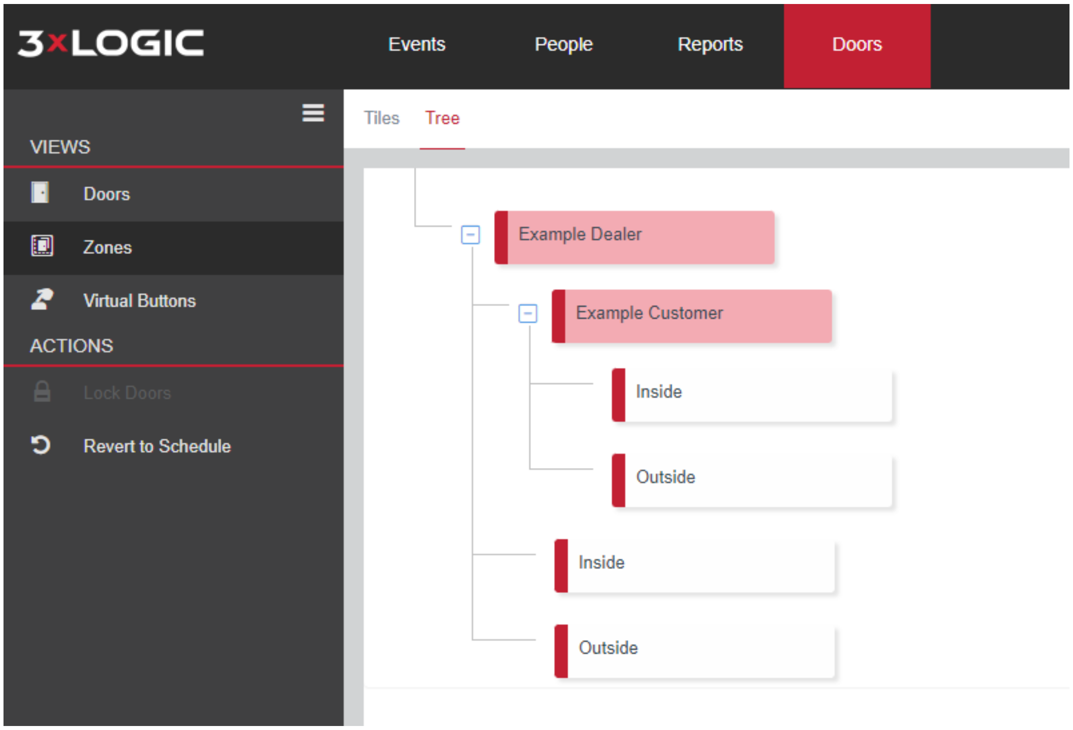


Figure 1-125: Zone Hierarchy Tree

8 Best Practices

The Quick Start Guide (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 (also shown under "Zoning Trees" on page 87):

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

8.1 Recommended Configuration

Follow these steps, in sequence:

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

8.2 Diagram

Example showing mapped Zones and Doors (also featured under "Multiple Doors" on page 42):

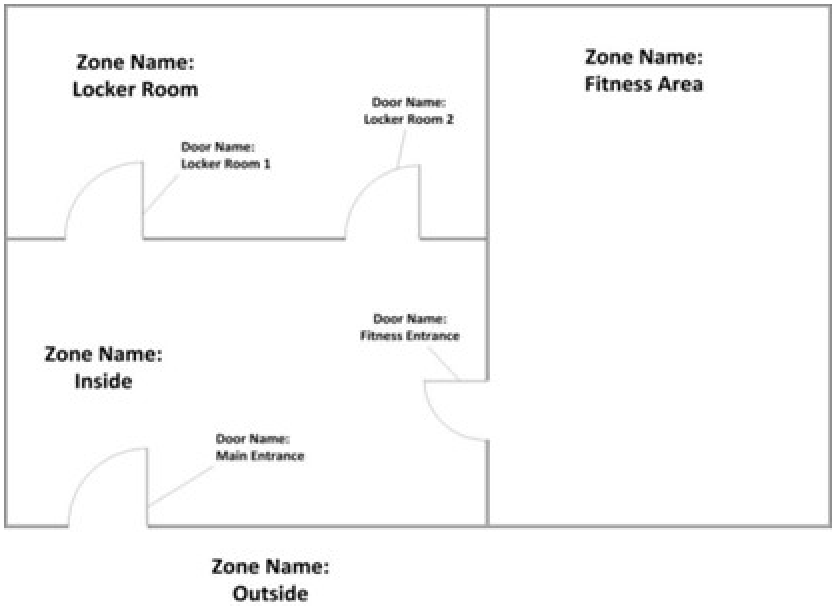


Figure 1-126: Zone Diagram

9 Single and Dual Authentication

This section features the contents of the Cards and PIN Bulletin, which focuses on differences between Card **+** Pin vs. Card **or** Pin and how they are used in the security industry.

9.1 Card + PIN

Card + PIN configurations require a card holder to input a keypad PIN code followed by a physical credential swipe in order to validate card holder's access at the particular entry point.

Also known as Dual Authentication, the Card + PIN method is utilized in locations where Card or Pin is not considered secure enough of an entry method.

Note: The HID 5355AGK00 and R-MPKW-CHAR-AH are examples of common dual authentication readers used with INFINIAS.

This is a Card + PIN device:

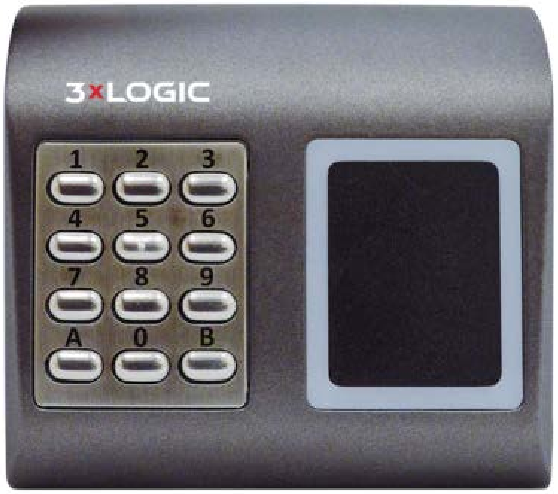


Figure 1-127: Card + PIN device (R-MPKW-CHAR-AH)

9.2 Card or PIN

Card or Pin configurations require a card holder to present a single credential from a keypad, card/fob reader, biometric reader, or similar device to gain access to a secured location. This method of verification is the most common method used in the industry.

There are many available technologies used for this single authentication method versus dual authentication. These are examples of Card or Pin output devices:

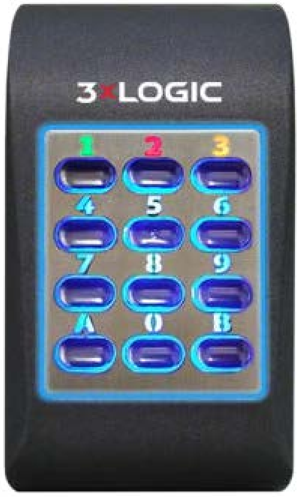


Figure 1-128: PIN device (R-MPADW-CHAR)

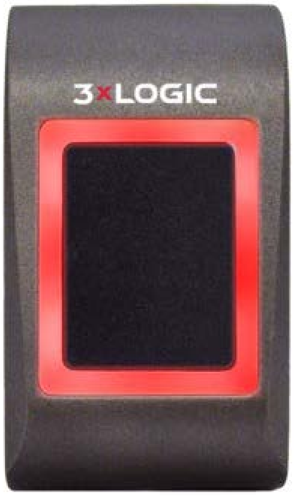
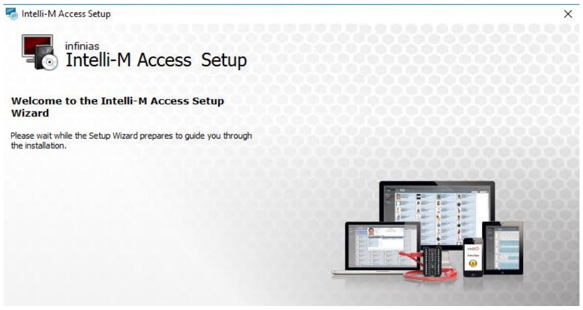


Figure 1-129: Card Reader (R-MPW-CHAR-AH)

10 INFINIAS Installation Guide

This section features the contents of the INFINIAS Installation Guide, which covers the setup instructions for the software.

10.1 Installation Procedures



Welcome to the Intelli-M Access Setup Wizard

Please wait while the Setup Wizard prepares to guide you through the installation.

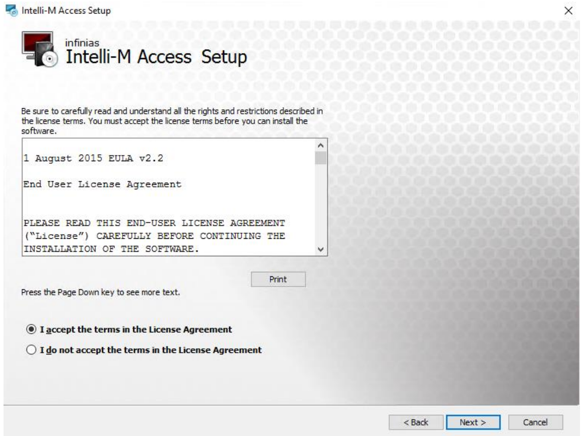
Figure 1-130: Setup

10.1.1 Initial Setup

1. Download the latest **Full** installation package from http://www.3xlogic.com/software-center to ensure that the latest release is being installed.
    a. An Administrative level local *user account* is necessary to perform the installation.
    b. On domains, make certain the user has both domain administrative rights and local administrative rights to prevent permission issues from rolling back the installation.

Note: The S-Base-Kit purchased from distributors could be dated and would require a further upgrade after the initial installation.

2. Right Click and “Run as administrator” to initialize the installation.
3. Click **Next** to proceed to the following screen.
4. Depending on the speed of the system, it could take several minutes to progress. SQL installations can take many minutes to complete. A 40-minute installation time is very common.
5. An End User Level Agreement (EULA) displays.



Be sure to carefully read and understand all the rights and restrictions described in the license terms. You must accept the license terms before you can install the software.

```
1 August 2015 EULA v2.2

End User License Agreement


PLEASE READ THIS END-USER LICENSE AGREEMENT
(“License”) CAREFULLY BEFORE CONTINUING THE
INSTALLATION OF THE SOFTWARE.
```

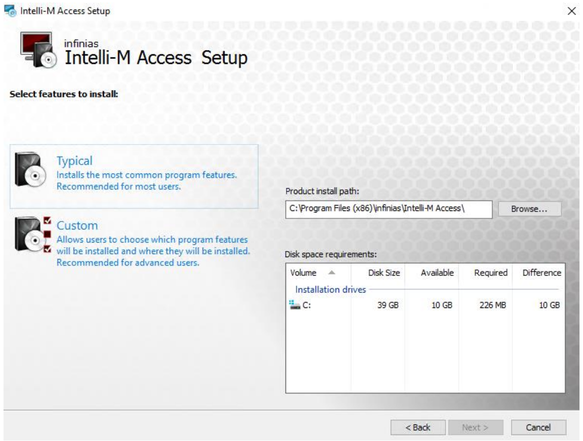
Press the Page Down key to see more text.

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Figure 1-131: EULA

6. After selecting the radio button for agreement to the terms, click **Next**.
7. A features page will appear with an option to change primary directories and select a **Typical** or **Custom** installation.



Intelli-M Access Setup

infinias
Intelli-M Access Setup

Select features to install:

Typical
Installs the most common program features.
Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed.
Recommended for advanced users.

Product install path:
C:\Program Files (x86)\infinias\Intelli-M Access\

Disk space requirements:

Volume	Disk Size	Available	Required	Difference
Installation drives				
C:	39 GB	10 GB	226 MB	10 GB

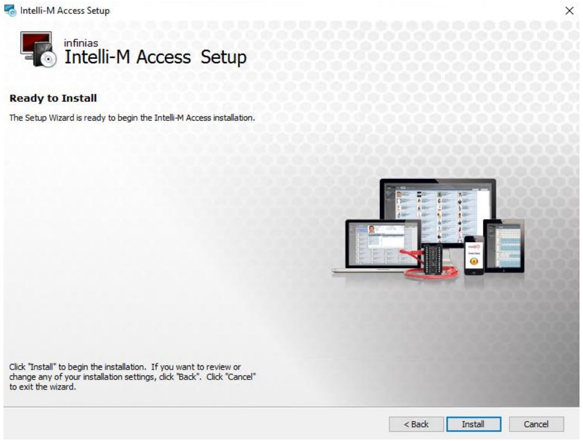
Figure 1-132: Installation Types

8. The next step depends on the desired configuration.

10.1.2 Typical Installation

These procedures cover **Typical** installation, after performing *Initial Setup*.

1. Select Typical Installation and click **Install**.



Intelli-M Access Setup

infinias
Intelli-M Access Setup

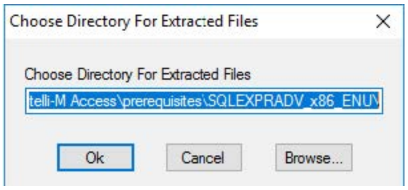
Ready to Install

The Setup Wizard is ready to begin the Intelli-M Access installation.

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Figure 1-133: Ready to Install

2. The installer prompts for confirmation of a *temporary* directory for SQL to use.
   a. Proceed with the default download location by clicking **OK**.



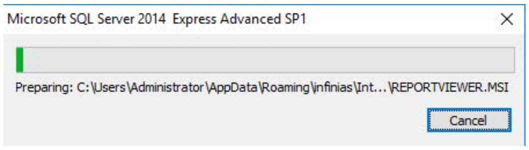
Choose Directory For Extracted Files

Choose Directory For Extracted Files

telli-M Access\prerequisites\SQLEXPRADV_x86_ENU\

Figure 1-134: Choose Location

3. A dialog window displays to indicate the files are extracting to the confirmed location to proceed with installation of SQL.

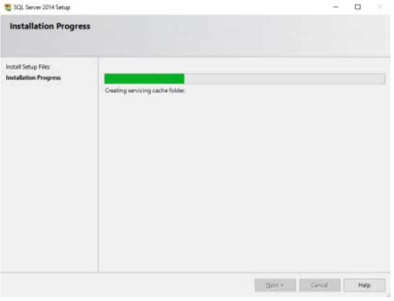


Microsoft SQL Server 2014 Express Advanced SP1

Preparing: C:\Users\Administrator\AppData\Roaming\infinias\Int...\REPORTVIEWER.MSI

Figure 1-135: SQL Installation

   a. A progress bar displays for the SQL setup.



SQL Server 2014 Setup

Installation Progress

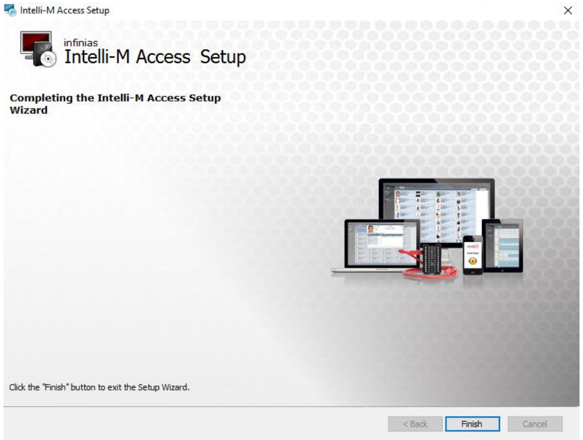
Install Setup Files

Installation Progress

Creating servicing cache folder.

Figure 1-136: Installation Progress

4. For the final steps of installation, it is highly recommended in not attempting to install the software on a partition other than the main system installation drive, or "root" (e.g. "C:\").
   a. SQL installations on secondary drives have known conflicts.
   b. Unless otherwise instructed, choose the root drive as the default location.
5. After successful installation, the last step is to click the **Finish** button to close the window.



Intelli-M Access Setup

infinias Intelli-M Access Setup

Completing the Intelli-M Access Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

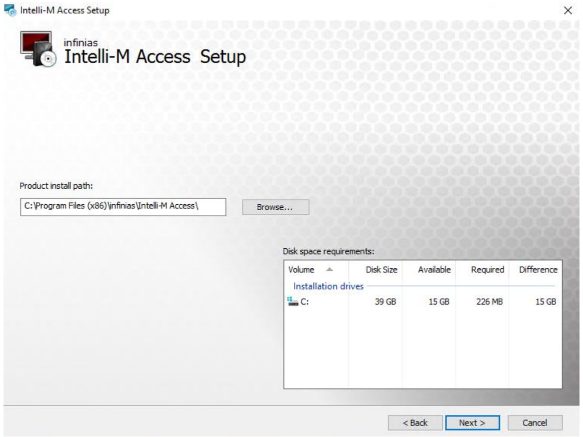
Figure 1-137: Setup Finished

Note: If the software *rolls back* and displays an installation log check box, leave the window up and contact the Support team for assistance.

10.1.3 Custom Installation

These procedures cover **Custom** installation, after performing *Initial Setup*.

1. Select Custom Installation and click **Install**.
2. The installer prompts for confirmation of a *temporary* directory for SQL to use.
    a. Proceed with the default download location by clicking **OK**.
    b. Please allocate an additional 100GB of free space on the root drive for future use.



Product install path:

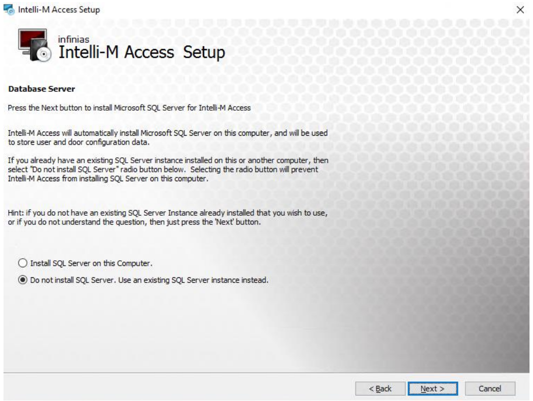
C:\Program Files (x86)\infinias\Intelli-M Access\

Disk space requirements:

Volume	Disk Size	Available	Required	Difference
Installation drives				
C:	39 GB	15 GB	226 MB	15 GB

Figure 1-138: Setup and Allocation

3. Choose the type of SQL configuration.
    a. To use SQL Express, select the “Install SQL server on this Computer” option.
    b. To use an established SQL server, select the “Do not install SQL Server. Use an existing SQL Server instead” option.



Database Server

Press the Next button to install Microsoft SQL Server for Intelli-M Access

Intelli-M Access will automatically install Microsoft SQL Server on this computer, and will be used to store user and door configuration data.

If you already have an existing SQL Server instance installed on this or another computer, then select "Do not install SQL Server" radio button below. Selecting the radio button will prevent Intelli-M Access from installing SQL Server on this computer.

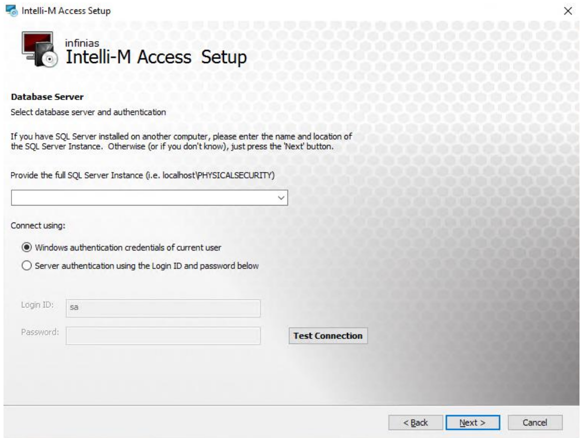
Hint: if you do not have an existing SQL Server Instance already installed that you wish to use, or if you do not understand the question, then just press the 'Next' button.

○ Install SQL Server on this Computer.

● Do not install SQL Server. Use an existing SQL Server instance instead.

Figure 1-139: SQL Choices

4. After clicking **Next**, use the drop down and select the SQL instance.



Intelli-M Access Setup

infinias
Intelli-M Access Setup

Database Server

Select database server and authentication

If you have SQL Server installed on another computer, please enter the name and location of the SQL Server Instance. Otherwise (or if you don't know), just press the 'Next' button.

Provide the full SQL Server Instance (i.e. localhost\PHYSICALSECURITY)

Connect using:

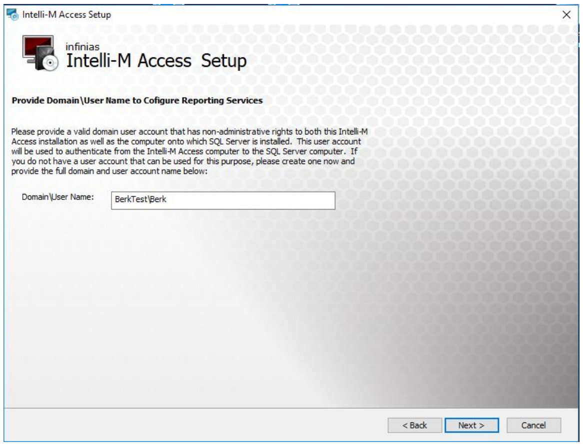
● Windows authentication credentials of current user
○ Server authentication using the Login ID and password below

Login ID: sa

Password:

Figure 1-140: SQL Selection

5. Proceed with the logged in Windows account or a specific SQL Server authenticated user.
6. Perform a Test Connection to confirm there is communication between the software installer and the SQL server.
    a. If it passes successfully, click **Next**.
7. Input the *domain user* if the installation location is managed by a domain. Otherwise, select the *default user* when not running a domain or if the user has proper domain privileges.



Intelli-M Access Setup

infinias
Intelli-M Access Setup

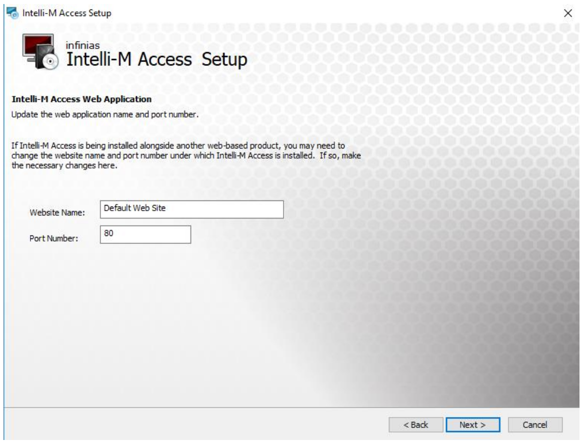
Provide Domain\User Name to Cofigure Reporting Services

Please provide a valid domain user account that has non-administrative rights to both this Intelli-M Access installation as well as the computer onto which SQL Server is installed. This user account will be used to authenticate from the Intelli-M Access computer to the SQL Server computer. If you do not have a user account that can be used for this purpose, please create one now and provide the full domain and user account name below:

Domain\User Name: BerkTest\Berk

Figure 1-141: User Selection

8. After clicking **Next**, an option to create a custom website name and/or port number binding becomes available on systems that have the default ports in use or the default web site in use by another program.



Intelli-M Access Web Application

Update the web application name and port number.

If Intelli-M Access is being installed alongside another web-based product, you may need to change the website name and port number under which Intelli-M Access is installed. If so, make the necessary changes here.

Website Name: Default Web Site

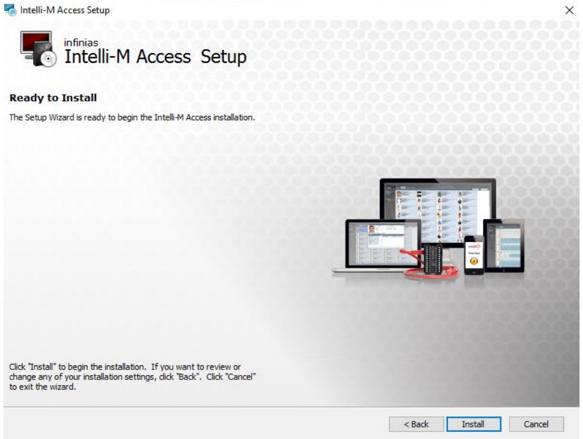
Port Number: 80

Figure 1-142: Website and/or Port Input

a. Leave the default selection(s) if no other programs or variables require changes.

b. Click **Next** to proceed.

9. Select **Install** to complete the setup process.



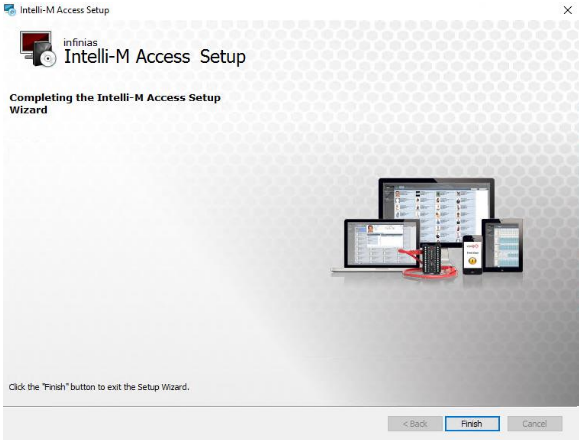
Ready to Install

The Setup Wizard is ready to begin the Intelli-M Access installation.

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Figure 1-143: Initiate Installation

10. After successful installation, the last step is to click the **Finish** button to close the window.



Completing the Intelli-M Access Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

Figure 1-144: Finish Installation

Note: If the software *rolls back* or displays an error and shows an installation log check box, leave the window up and contact the Support team for assistance.

10.2 Upgrading from Older Versions

When upgrade from previous versions of the software to the latest version, the same process will be followed but using the upgrade installer package from:

http://www.3xlogic.com/software-center

Please complete a backup of the SQL database prior to upgrading the software.

10.3 Licensing INFINIAS

Once the INFINIAS software is successfully installed, there is a shortcut in the start menu under the INFINIAS app for linking to the User Interface.

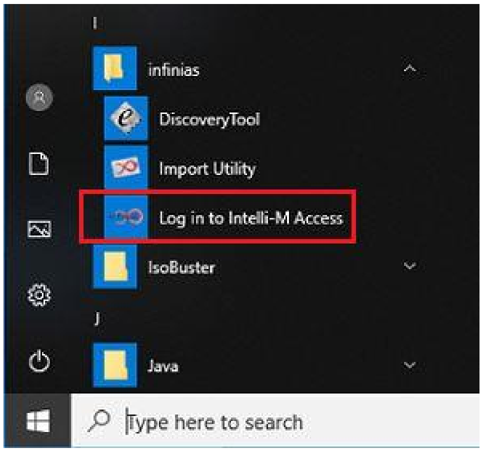


Figure 1-145: Start Menu Example

10.3.1 Initial Login

Clicking the shortcut opens the default browser for the system and brings up the login screen for INFINIAS. Alternatively, access the software by using //localhost/intellim in the address bar of any current web browser.

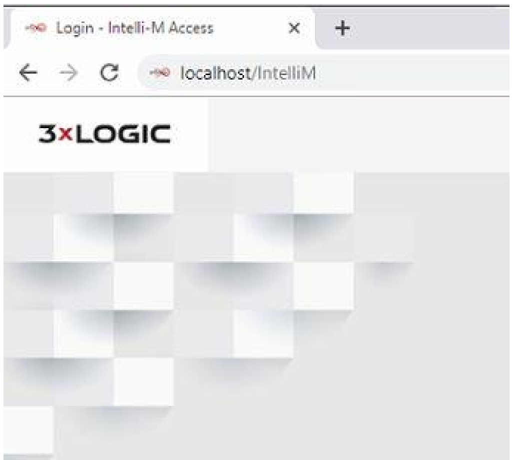
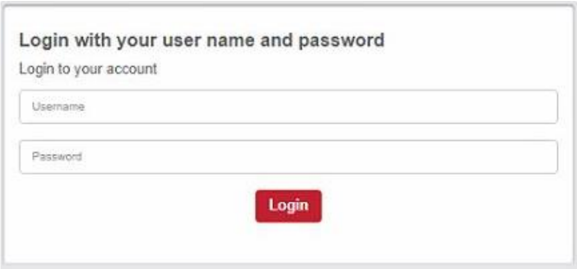


Figure 1-146: Login Access

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

Use the following login information to log in for the first time.

- User: admin
- Password: admin



Login with your user name and password

Login to your account

Username

Password

Figure 1-147: Login Credentials

10.3.2 Administration

The *Admin User* person is a default person in the system and contains no credential information. This person is not intended to be given credentials or turned into an actual person used to access the site.

The role of the Admin User is used to give **administrator level privileges to the software**. The role tab can be used to give rights to any other person for the purpose of logging in and managing the software.

Within INFINIAS, the password is not manually generated and cannot be seen by anyone, not even the development engineering team at 3xLOGIC. A link is generated by email and sent to the email address used for the user name. In a local system, the user name is not required to be an email address and the password can be set by the administrator level role.

10.3.3 Activation

Once logged in, the first step will be to activate the purchased license(s). The settings tab is located under the configuration section in the software.

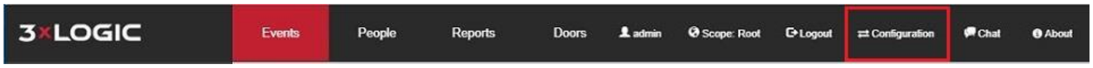
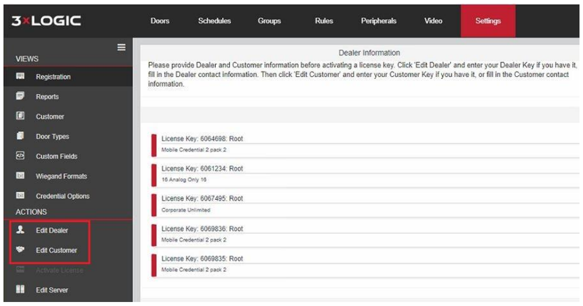


Figure 1-148: Configuration

This tab requires the Dealer and Customer information to be entered prior to being allowed to enter any licensing information.



Please provide Dealer and Customer information before activating a license key. Click 'Edit Dealer' and enter your Dealer Key if you have it, fill in the Dealer contact information. Then click 'Edit Customer' and enter your Customer Key if you have it, or fill in the Customer contact information.

License Key: 6064698: Root
Mobile Credential 2 pack 2

License Key: 6061234: Root
16 Analog Only 16

License Key: 6067495: Root
Corporate Unlimited

License Key: 6069836: Root
Mobile Credential 2 pack 2

License Key: 6069835: Root
Mobile Credential 2 pack 2

Figure 1-149: Editing Options

This information is not used for anything other than internal use within 3xLOGIC. The information provided is not required to match anything on the original purchase order. It is only for reference.

- Dealer

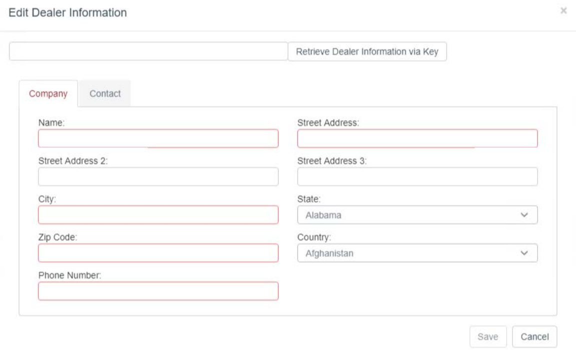


Figure 1-150: Dealer Information - Company

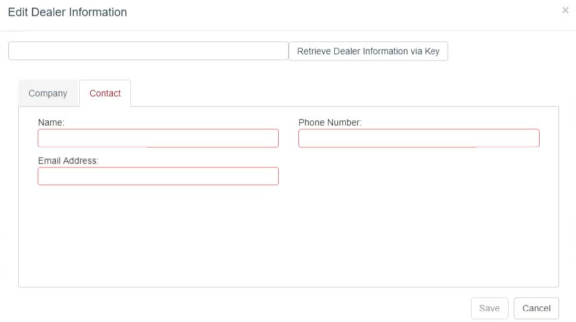
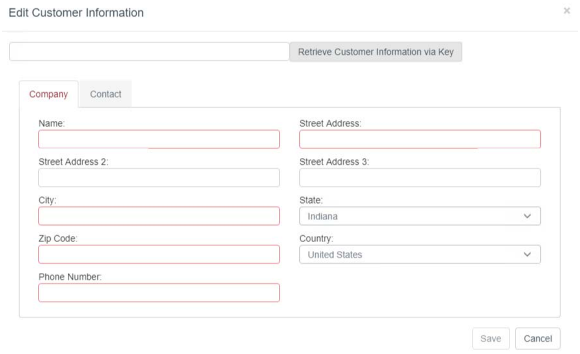


Figure 1-151: Dealer Information - Contact

- Customer

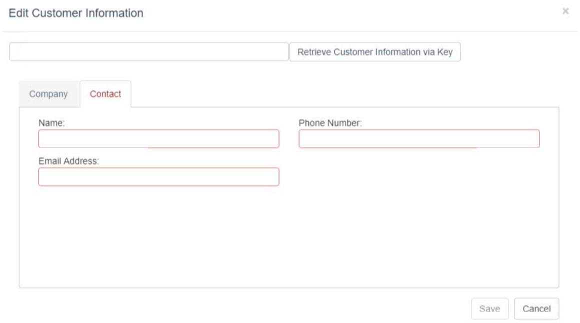


Edit Customer Information

State: Indiana

Country: United States

Figure 1-152: Customer Information - Company



Edit Customer Information

Figure 1-153: Customer Information - Contact

After inputting Dealer and Customer information, the **Activate License** link under the Actions menu becomes available.

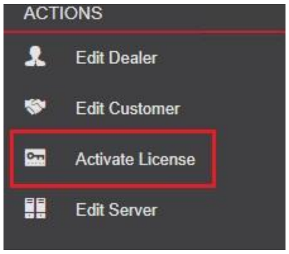
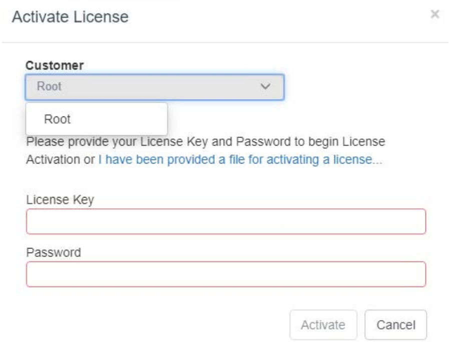


Figure 1-154: License Activation

Selecting the link opens a window prompting for a License Key and Password.



Activate License

Customer

Root

Root

Please provide your License Key and Password to begin License Activation or I have been provided a file for activating a license...

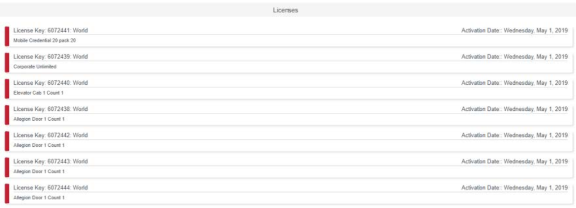
License Key

Password

Figure 1-155: License Activation Credentials

These credentials are provided via email or on physical placards. The placards are located in the physical package purchased from distribution or that came with the access server accessory pack.

Verify the licenses display on the registration page to confirm.



Licenses

License Key: 6072441: World — Activation Date:: Wednesday, May 1, 2019
Mobile Credential 20 pack 20

License Key: 6072439: World — Activation Date:: Wednesday, May 1, 2019
Corporate Unlimited

License Key: 6072440: World — Activation Date:: Wednesday, May 1, 2019
Elevator Cab 1 Count 1

License Key: 6072438: World — Activation Date:: Wednesday, May 1, 2019
Allegion Door 1 Count 1

License Key: 6072442: World — Activation Date:: Wednesday, May 1, 2019
Allegion Door 1 Count 1

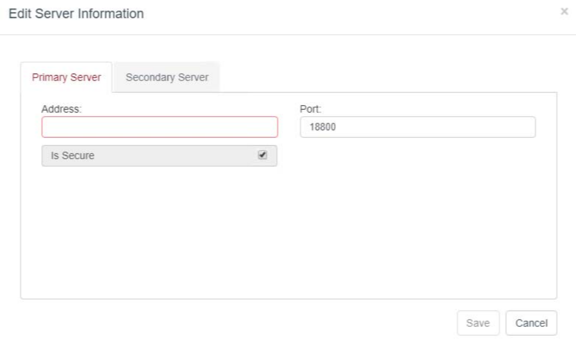
License Key: 6072443: World — Activation Date:: Wednesday, May 1, 2019
Allegion Door 1 Count 1

License Key: 6072444: World — Activation Date:: Wednesday, May 1, 2019
Allegion Door 1 Count 1

Figure 1-156: Verification

10.3.4 Upgrading

The Edit Server link is optional and used for upgrading Non-SSL (Standard HTTP) doors in a pre-existing system or in the future to upgrade doors that require SSL (Hosted) communication. The information input here will be the IP address of the system where the software is installed. The SSL check boxes are checked and the port 18800 is entered in the port field.



Edit Server Information

Address:

Port: 18800

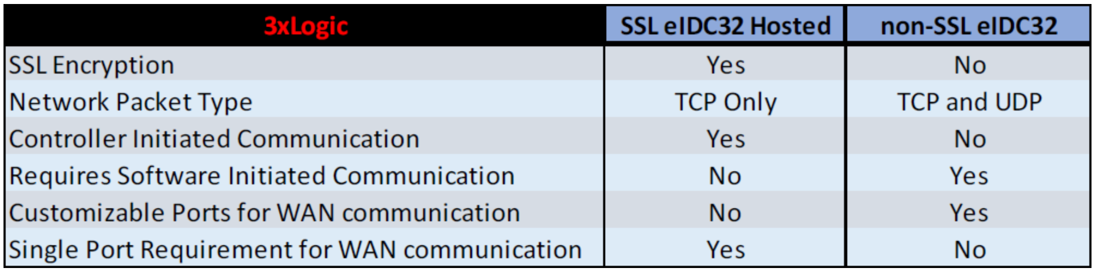
Is Secure ☑

Figure 1-157: Server Information

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, see "Configuring and Creating a Hosted Door" on the next page.

11 Configuring and Creating a Hosted Door

This guide will walk through the creation and configuration of Hosted Door Controllers on locally installed OS environments, INFINIAS CLOUD, and both using the *Discovery Tool* as well as the Controller's User Interface (UI). A hosted door controller differs from the standard non-hosted door controllers in the following ways (see figure below).

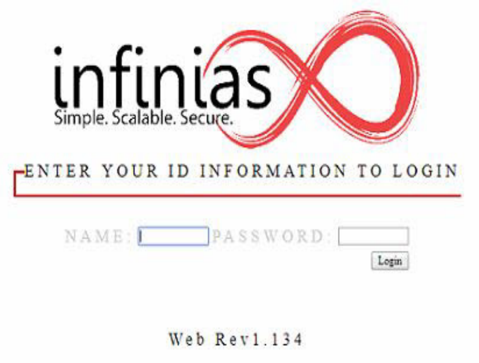


3xLogic	SSL eIDC32 Hosted	non-SSL eIDC32
SSL Encryption	Yes	No
Network Packet Type	TCP Only	TCP and UDP
Controller Initiated Communication	Yes	No
Requires Software Initiated Communication	No	Yes
Customizable Ports for WAN communication	No	Yes
Single Port Requirement for WAN communication	Yes	No

Figure 1-158: Door Differences

Hosted door controllers also require special configuration. As noted earlier, the two methods are:

- On the Controller side using the Controller's UI.



infinias
Simple. Scalable. Secure.

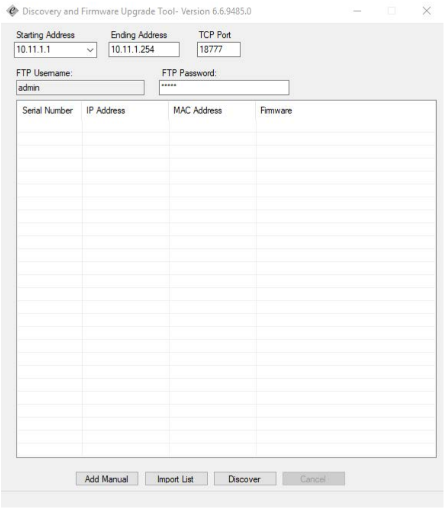
ENTER YOUR ID INFORMATION TO LOGIN

NAME: PASSWORD:

Web Rev1.134

Figure 1-159: Controller UI

- The Discovery Tool.



Discovery and Firmware Upgrade Tool- Version 6.6.9485.0

Starting Address: 10.11.1.1
Ending Address: 10.11.1.254
TCP Port: 18777
FTP Username: admin
FTP Password: *****

Serial Number	IP Address	MAC Address	Firmware

Figure 1-160: Discovery Tool

11.1 Configuring a Door Controller

11.1.1 Downloading the Discovery Tool

The Discovery Tool can be downloaded from: http://www.3xlogic.com/software-center

The purpose of this program is to detect and configure eIDC32 door controllers for use in local or CLOUD configurations.

11.1.2 Extracting the Discovery Tool

Once downloaded, perform the following steps:

1. Extract the tool from the zip file by *right clicking* it and selecting **Extract All**.

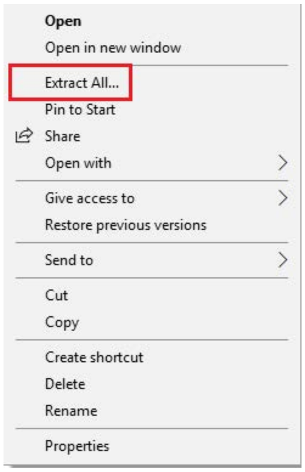
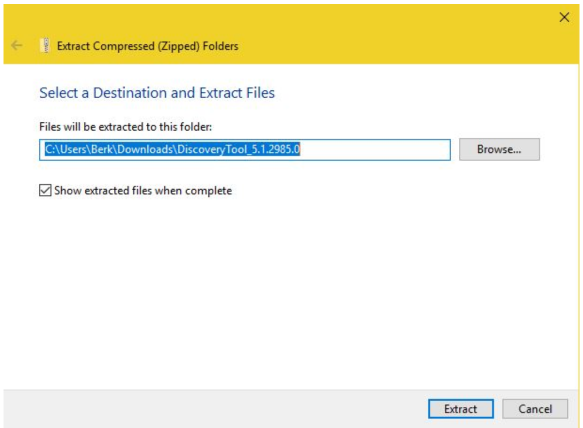


Figure 1-161: Extract All

2. Leave the destination location as the *default selection* and choose **Extract**.


Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

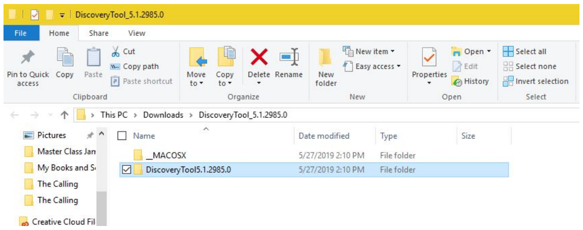
Files will be extracted to this folder:

C:\Users\Berk\Downloads\DiscoveryTool_5.1.2985.0

☑ Show extracted files when complete

Figure 1-162: Default Destination

3. The files will extract it in the location of the zip file.



Name	Date modified	Type	Size
__MACOSX	5/27/2019 2:10 PM	File folder	
☑ DiscoveryTool5.1.2985.0	5/27/2019 2:10 PM	File folder	

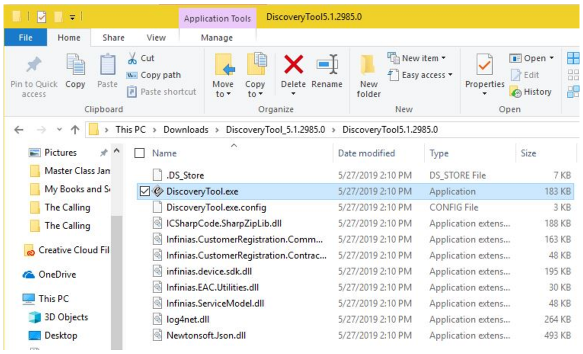
Figure 1-163: Extracted Files

Note: The Discovery Tool is pre-loaded in 3xLOGIC based INFINIAS Access servers.

11.1.3 Configuration Using the Discovery Tool

Perform the following steps to complete configuration:

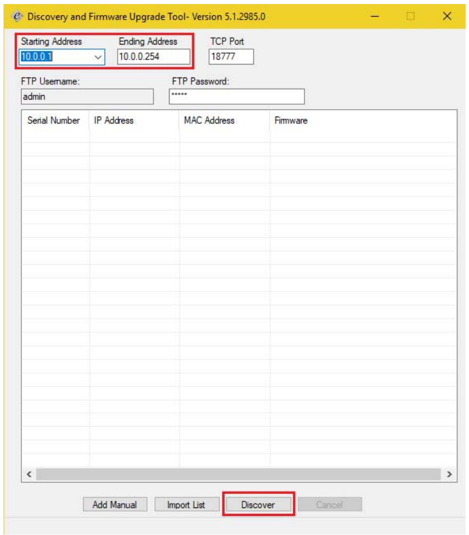
1. Navigate to the *Discovery Tool folder* and look for the application file (.exe) as shown in the figure below and **double click it**.



Name	Date modified	Type	Size
.DS_Store	5/27/2019 2:10 PM	DS_STORE File	7 KB
☑ DiscoveryTool.exe	5/27/2019 2:10 PM	Application	183 KB
DiscoveryTool.exe.config	5/27/2019 2:10 PM	CONFIG File	3 KB
ICSharpCode.SharpZipLib.dll	5/27/2019 2:10 PM	Application extens...	188 KB
Infinias.CustomerRegistration.Comm...	5/27/2019 2:10 PM	Application extens...	163 KB
Infinias.CustomerRegistration.Contrac...	5/27/2019 2:10 PM	Application extens...	48 KB
infinias.device.sdk.dll	5/27/2019 2:10 PM	Application extens...	195 KB
Infinias.EAC.Utilities.dll	5/27/2019 2:10 PM	Application extens...	30 KB
Infinias.ServiceModel.dll	5/27/2019 2:10 PM	Application extens...	48 KB
log4net.dll	5/27/2019 2:10 PM	Application extens...	264 KB
Newtonsoft.Json.dll	5/27/2019 2:10 PM	Application extens...	493 KB

Figure 1-164: Discovery Tool Folder

2. Once the application is open, enter the **IP address range** to *scan*.
   a. It is important that the discovery tool scans the same IP range that the system it is running on is assigned to, as the chances of successfully discovering the door controllers on a different subnet are very limited.



Discovery and Firmware Upgrade Tool- Version 5.1.2985.0

Starting Address: 10.0.0.1

Ending Address: 10.0.0.254

TCP Port: 18777

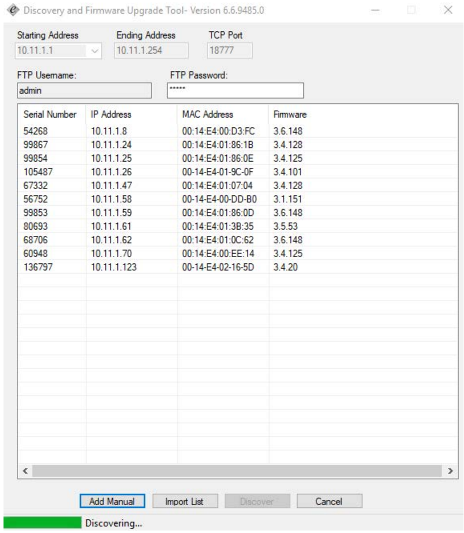
FTP Username: admin

FTP Password: *****

Serial Number	IP Address	MAC Address	Firmware

Figure 1-165: IP Ranges

b. Leave the TCP port and FTP *username and password* as <u>default</u>.



Discovery and Firmware Upgrade Tool- Version 6.6.9485.0

Starting Address: 10.11.1.1

Ending Address: 10.11.1.254

TCP Port: 18777

FTP Username: admin

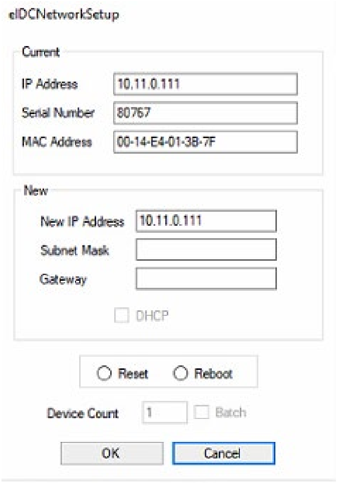
FTP Password: *****

Serial Number	IP Address	MAC Address	Firmware
54268	10.11.1.8	00:14:E4:00:D3:FC	3.6.148
99867	10.11.1.24	00:14:E4:01:86:1B	3.4.128
99854	10.11.1.25	00:14:E4:01:86:0E	3.4.125
105487	10.11.1.26	00-14-E4-01-9C-0F	3.4.101
67332	10.11.1.47	00:14:E4:01:07:04	3.4.128
56752	10.11.1.58	00-14-E4-00-DD-B0	3.1.151
99853	10.11.1.59	00:14:E4:01:86:0D	3.6.148
80693	10.11.1.61	00:14:E4:01:3B:35	3.5.53
68706	10.11.1.62	00:14:E4:01:0C:62	3.6.148
60948	10.11.1.70	00:14:E4:00:EE:14	3.4.125
136797	10.11.1.123	00-14-E4-02-16-5D	3.4.20

Figure 1-166: Default Credentials

Note: If unable to discover the door controllers, yet can successfully navigate to them via a web browser, please jump to "Configuration Using the Controller User Interface" on page 112.

3. If the IP address settings need to be altered, that can be done by right clicking the door controller requiring change and selecting **Modify**.



eIDCNetworkSetup

Current

IP Address: 10.11.0.111

Serial Number: 80767

MAC Address: 00-14-E4-01-3B-7F

New

New IP Address: 10.11.0.111

Subnet Mask:

Gateway:

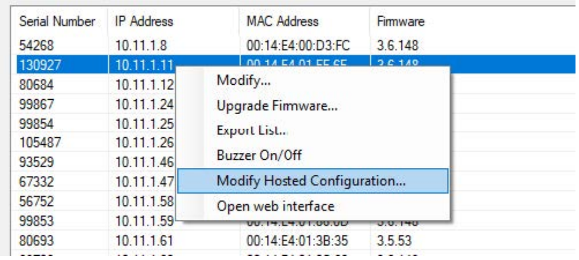
□ DHCP

○ Reset ○ Reboot

Device Count: 1 □ Batch

Figure 1-167: Settings

4. The next step is to *verify* the latest firmware is updated on the controller(s).
    a. Always check to see what the latest firmware is by navigating to: http://www.3x-logic.com/software-center
    b. It is not required to extract the firmware zip file.
        i. Simply click on the **Upgrade Firmware** option on the menu and point that to the downloaded file.
    c. If unsuccessful, try defaulting the configuration on the controller or perform a factory reset.
5. Upon Success, right click and select Modify Host Configuration.

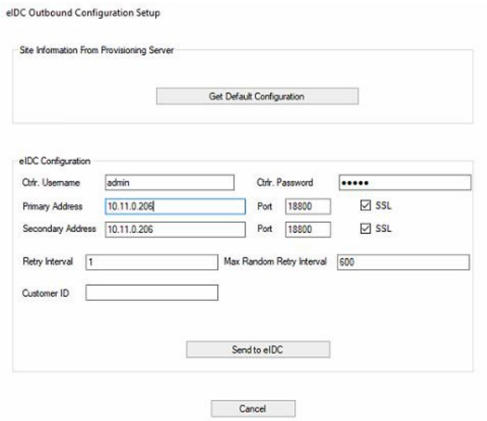


Serial Number	IP Address	MAC Address	Firmware
54268	10.11.1.8	00:14:E4:00:D3:FC	3.6.148
130927	10.11.1.11	[illegible]	[illegible]
80684	10.11.1.12		
99867	10.11.1.24		
99854	10.11.1.25		
105487	10.11.1.26		
93529	10.11.1.46		
67332	10.11.1.47		
56752	10.11.1.58		
99853	10.11.1.59	[illegible]	[illegible]
80693	10.11.1.61	00:14:E4:01:3B:35	3.5.53

Figure 1-168: Modify Host Configuration

Note: New door controllers are programmed out of the box to sync with INFINIAS CLOUD. Please see the "INFINIAS CLOUD Quick Start Guide" on page 1 for further details on the initial steps of the CLOUD configuration.

6. Click Get Default Configuration if programming an eIDC32 for use with INFINIAS CLOUD. The fields automatically populate with the relevant information.
7. If using a locally installed (hosted) setup, change the Primary and Secondary address fields to match the IP address of the system where the software is installed.
8. Leave the other fields as the default selections.



eIDC Outbound Configuration Setup

Site Information From Provisioning Server

Get Default Configuration

eIDC Configuration

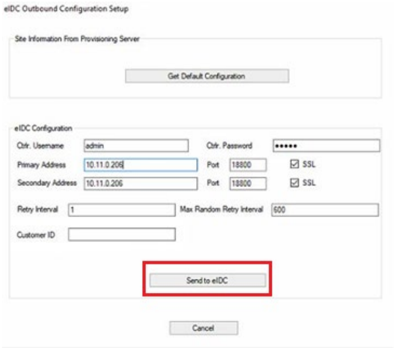
Ctlr. Username: admin
Ctlr. Password: •••••
Primary Address: 10.11.0.206 Port: 18800 ☑ SSL
Secondary Address: 10.11.0.206 Port: 18800 ☑ SSL
Retry Interval: 1
Max Random Retry Interval: 600
Customer ID:

Send to eIDC

Cancel

Figure 1-169: Default Field Entries

9. Click Send to eIDC when finished.
   a. The outbound configuration section of the eIDC32 will be reprogrammed to match the settings listed shown in the figure below.



eIDC Outbound Configuration Setup

Site Information From Provisioning Server

Get Default Configuration

eIDC Configuration

Ctlr. Username: admin
Ctlr. Password: •••••
Primary Address: 10.11.0.206 Port: 18800 ☑ SSL
Secondary Address: 10.11.0.206 Port: 18800 ☑ SSL
Retry Interval: 1
Max Random Retry Interval: 600
Customer ID:

Send to eIDC

Cancel

Figure 1-170: Programmed Settings

Note: The Customer ID is not required on local system installation using hosted controllers. It is only required in special circumstances within INFINIAS CLOUD.

11.1.4 Configuration Using the Controller User Interface

Configuring the eIDC32 Door Controller is similar to programming using the Discovery Tool. This method is an alternative to the Discovery Tool when the tool has difficulty locating the Controller (s) on the network. In such cases, it is necessary to determine the IP address of the Controller(s) via other means such as:

- A network device scanning utility
- The UI of the switch the devices are plugged into
- Rebooting the Controller(s) and reading off the IP address that pulses on the LEDs located on the face of the eIDC32.

After determining the IP address of the eIDC32:

1. Open a web browser.
2. Input the IP address in the URL address bar and then press **Enter** on the keyboard.
3. The Login Page displays, as shown in the figure below.

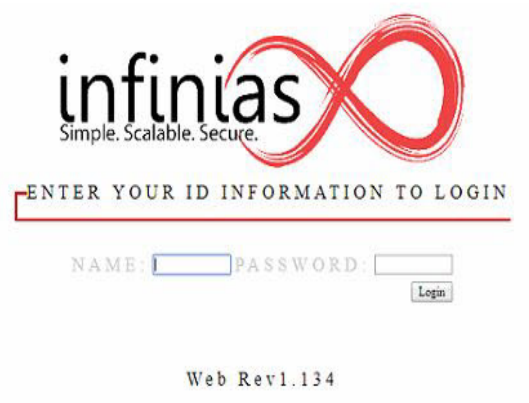
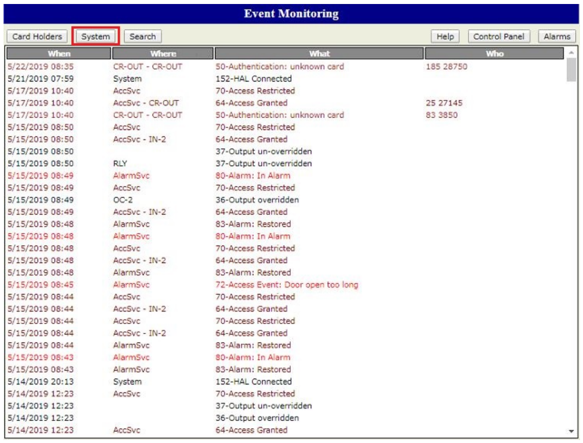


Figure 1-171: Login Page

4. Login with the default user: admin and password: admin.
5. The **Event Monitor system** displays upon success.
   a. Click **System** in the upper left to navigate to the System Management Screen.



When	Where	What	Who
5/22/2019 08:35	CR-OUT - CR-OUT	50-Authentication: unknown card	185 28750
5/21/2019 07:59	System	152-HAL Connected	
5/17/2019 10:40	AccSvc	70-Access Restricted	
5/17/2019 10:40	AccSvc - CR-OUT	64-Access Granted	25 27145
5/17/2019 10:40	CR-OUT - CR-OUT	50-Authentication: unknown card	83 3850
5/15/2019 08:50	AccSvc	70-Access Restricted	
5/15/2019 08:50	AccSvc - IN-2	64-Access Granted	
5/15/2019 08:50		37-Output un-overridden	
5/15/2019 08:50	RLY	37-Output un-overridden	
5/15/2019 08:49	AlarmSvc	80-Alarm: In Alarm	
5/15/2019 08:49	AccSvc	70-Access Restricted	
5/15/2019 08:49	OC-2	36-Output overridden	
5/15/2019 08:49	AccSvc - IN-2	64-Access Granted	
5/15/2019 08:48	AlarmSvc	83-Alarm: Restored	
5/15/2019 08:48	AlarmSvc	80-Alarm: In Alarm	
5/15/2019 08:48	AccSvc	70-Access Restricted	
5/15/2019 08:48	AccSvc - IN-2	64-Access Granted	
5/15/2019 08:48	AlarmSvc	83-Alarm: Restored	
5/15/2019 08:45	AlarmSvc	72-Access Event: Door open too long	
5/15/2019 08:44	AccSvc	70-Access Restricted	
5/15/2019 08:44	AccSvc - IN-2	64-Access Granted	
5/15/2019 08:44	AccSvc	70-Access Restricted	
5/15/2019 08:44	AccSvc - IN-2	64-Access Granted	
5/15/2019 08:44	AlarmSvc	83-Alarm: Restored	
5/15/2019 08:43	AlarmSvc	80-Alarm: In Alarm	
5/15/2019 08:43	AlarmSvc	83-Alarm: Restored	
5/14/2019 20:13	System	152-HAL Connected	
5/14/2019 12:23	AccSvc	70-Access Restricted	
5/14/2019 12:23		37-Output un-overridden	
5/14/2019 12:23		36-Output overridden	
5/14/2019 12:23	AccSvc	64-Access Granted	

Figure 1-172: Event Monitoring - System

6. Click on **Controllers** in the upper right.

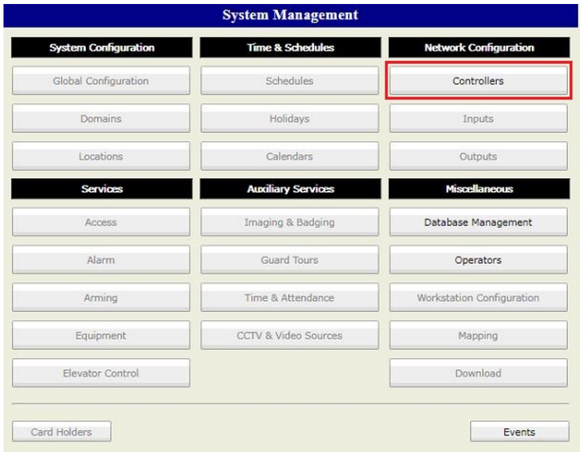
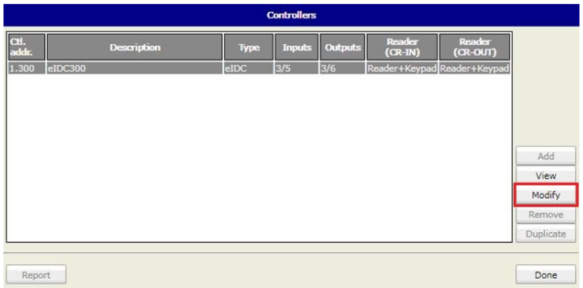


Figure 1-173: System Management - Controllers

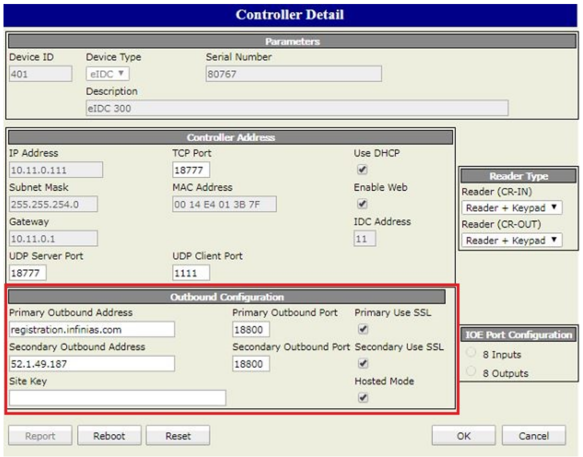
7. Highlight the controller and click **Modify** in the lower left.



Ctl. addr.	Description	Type	Inputs	Outputs	Reader (CR-IN)	Reader (CR-OUT)
1.300	eIDC300	eIDC	3/5	3/6	Reader+Keypad	Reader+Keypad

Figure 1-174: Controllers - Modify

8. For INFINIAS CLOUD Controllers, fill out the Outbound Configuration field with the information highlighted in the figure included below.
    a. If using salesdemo.infinias.com, the sales demo kit should be pre-configured.
        i. If it is not configured, please contact support.
    b. If it is connecting to a locally installed INFINIAS software package, please fill out all the fields under Outbound Configuration, as shown in the figure below.
        i. Change the Primary and Secondary Host address fields to the **IP Address** of the system where the software is installed.



Controller Detail

Parameters

Device ID: 401
Device Type: eIDC
Serial Number: 80767
Description: eIDC 300

Controller Address

IP Address: 10.11.0.111
TCP Port: 18777
Use DHCP: ☑
Subnet Mask: 255.255.254.0
MAC Address: 00 14 E4 01 3B 7F
Enable Web: ☑
Gateway: 10.11.0.1
IDC Address: 11
UDP Server Port: 18777
UDP Client Port: 1111

Reader Type

Reader (CR-IN): Reader + Keypad
Reader (CR-OUT): Reader + Keypad

Outbound Configuration

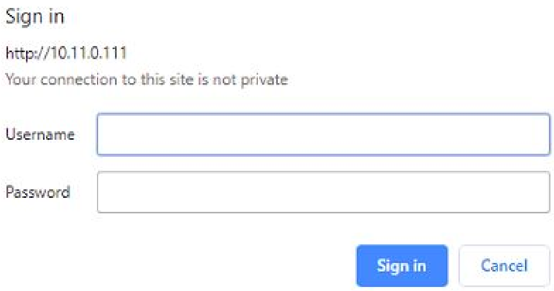
Primary Outbound Address: registration.infinias.com
Primary Outbound Port: 18800
Primary Use SSL: ☑
Secondary Outbound Address: 52.1.49.187
Secondary Outbound Port: 18800
Secondary Use SSL: ☑
Site Key:
Hosted Mode: ☑

IOE Port Configuration

○ 8 Inputs
○ 8 Outputs

Figure 1-175: Controller Detail - Outbound Configuration

9. Once configured, click **OK** in the lower right-hand corner.
10. The Controller may prompt for credentials after this is complete.
    a. Use the same credentials as the login.
    b. Username: admin Password: admin



Sign in

http://10.11.0.111

Your connection to this site is not private

Username

Password

Figure 1-176: Credentials

The controller is now configured. The next step is to program the door in the INFINIAS software.

11.2 Creating Doors

11.2.1 Creating a Hosted Door using INFINIAS

1. After logging into INFINIAS within a browser, navigate to the **Configuration** section.

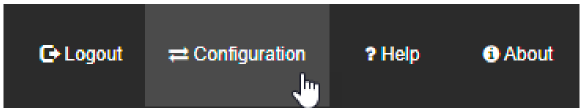
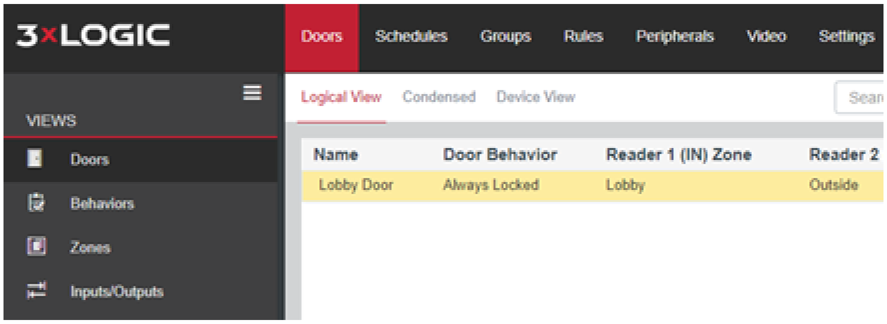


Figure 1-177: Top Menu - Configuration

2. The Doors Tab displays by default.



Name	Door Behavior	Reader 1 (IN) Zone	Reader 2
Lobby Door	Always Locked	Lobby	Outside

Figure 1-178: Views > Door Types

3. Choose **Create Door** under *Actions*.

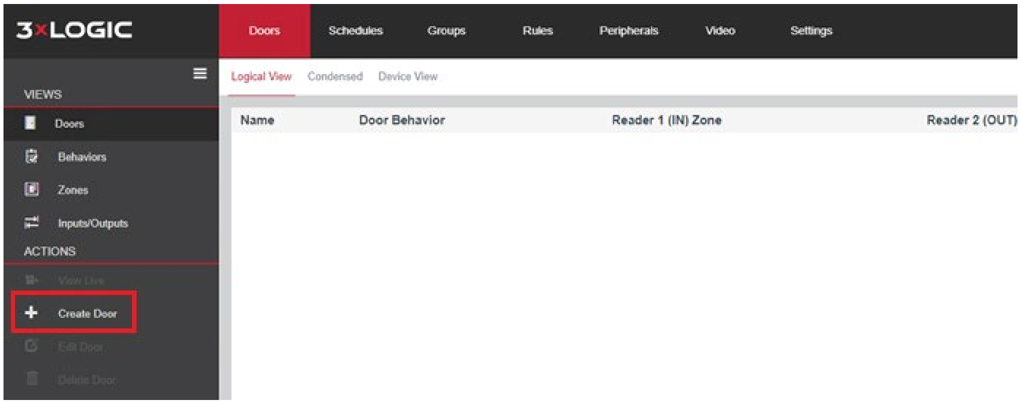
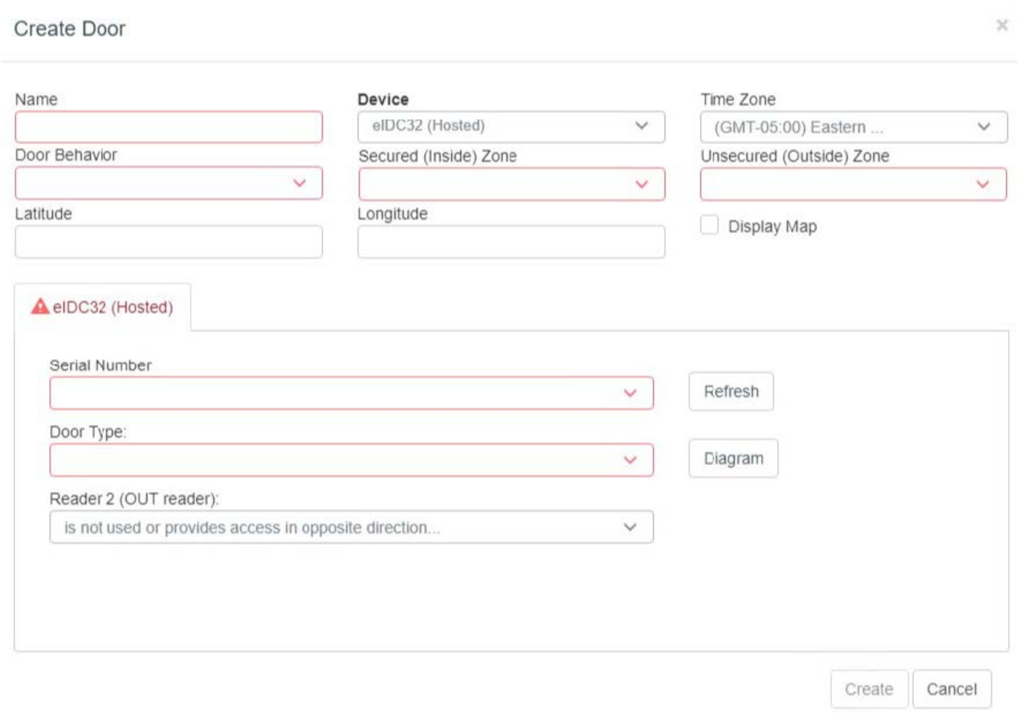


Figure 1-179: Doors > Create Door

4. The door creation screen displays and eIDC32 (Hosted) loads under the device drop down menu by default.



Create Door

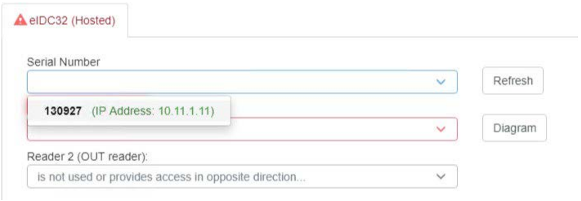
Device: eIDC32 (Hosted)

Time Zone: (GMT-05:00) Eastern ...

Reader 2 (OUT reader): is not used or provides access in opposite direction...

Figure 1-180: Default Device

5. Check to see if the hosted doors are synced in the system.
    a. Click the **serial number drop down menu** and see if the door controller's serial numbers populate.



130927 (IP Address: 10.11.1.11)

Reader 2 (OUT reader): is not used or provides access in opposite direction...

Figure 1-181: Serial Number Selection

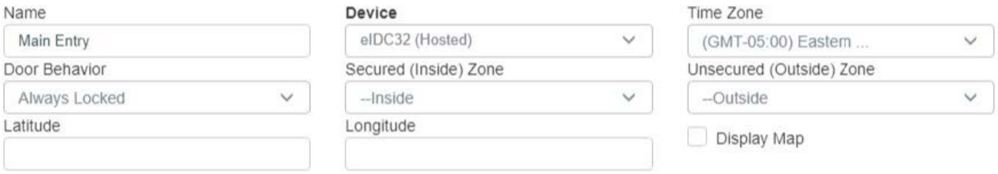
6. Select the **Serial Number** of the controller to configure and proceed back to the top to fill out the *required fields*.
    a. Name the door
    b. Select the Door Behavior
        i. The door behavior follows the lock/unlock schedule.
        ii. Always locked is the default.
    c. Set Time Zone
    d. Secured (Inside) Zone
        i. This is the area or location that requires the credential for entry/access.
    e. Unsecured (Outside) Zone

   i. This is the area or location that the person with the credential is coming from.

   ii. Unless an out-reader is being used in conjunction with an in-reader, this field is just informational.

f. GPS coordinates (Longitude and Latitude)

   i. These are only required if you plan on putting restrictions on how far away a person can use their Mobile Credential phone app.



Name	**Device**	Time Zone
Main Entry	eIDC32 (Hosted)	(GMT-05:00) Eastern ...
Door Behavior	Secured (Inside) Zone	Unsecured (Outside) Zone
Always Locked	--Inside	--Outside
Latitude	Longitude	□ Display Map

Figure 1-182: Serial Number Fields

7. Select the **Door Type** that will be used for this Door.

   a. The Diagram Button shows the configuration for the default door type.

      i. If the *Door Type* is Custom, no diagram will be available.

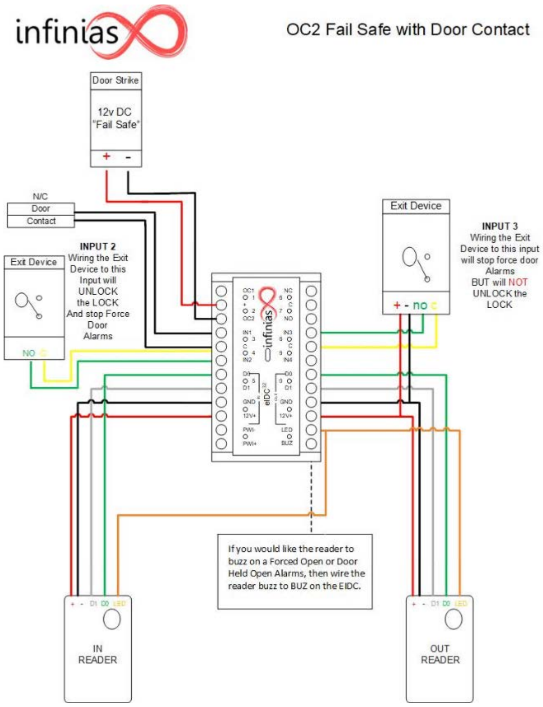
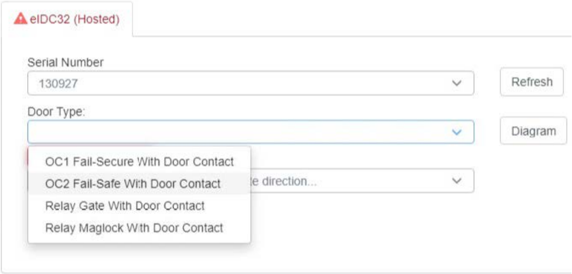

infinias
OC2 Fail Safe with Door Contact
Door Strike
12v DC
"Fail Safe"
+ -
N/C
Door
Contact
Exit Device
INPUT 2
Wiring the Exit Device to this Input will UNLOCK the LOCK And stop Force Door Alarms
NO C
Exit Device
INPUT 3
Wiring the Exit Device to this input will stop force door Alarms BUT will NOT UNLOCK the LOCK
+ - no c
OC1
OC2
IN1
IN2
IN3
IN4
NC
C
NO
D0
D1
GND
12V+
PWI-
PWI+
LED
BUZ
infinias
eIDC32
If you would like the reader to buzz on a Forced Open or Door Held Open Alarms, then wire the reader buzz to BUZ on the EIDC.
+ - D1 D0 LED
IN
READER
+ - D1 D0 LED
OUT
READER

Figure 1-183: Configuration Diagram

   b. Additional *Door Types* are available.

      i. Enable these under the Settings Tab > Door Types > Edit Door Types.

      ii. Process details covered in the next section, see "A new window displays additional door types that can be enabled or disabled." on page 121 for details.

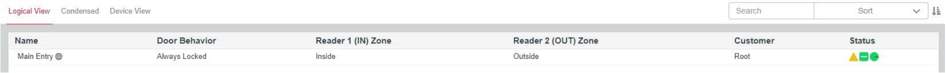

eIDC32 (Hosted)
Refresh
Diagram
OC1 Fail-Secure With Door Contact
OC2 Fail-Safe With Door Contact
Relay Gate With Door Contact
Relay Maglock With Door Contact
e direction...

Serial Number: 130927

Door Type:

Figure 1-184: Door Types

8. Click **Create** when finished.
   a. If successful, the Door will come online and show an online status, lock status, door open/closed status, all within a few minutes.



Name	Door Behavior	Reader 1 (IN) Zone	Reader 2 (OUT) Zone	Customer	Status
Main Entry	Always Locked	Inside	Outside	Root	▲■●

Figure 1-185: Door Status

Note: The Logical View, Condensed, and Device View links will provide different information and layouts to the doors tab.

   b. **Right clicking** the configured *Door* displays a submenu.
      i. These functions match the Actions Menu on the left-hand side of the screen.

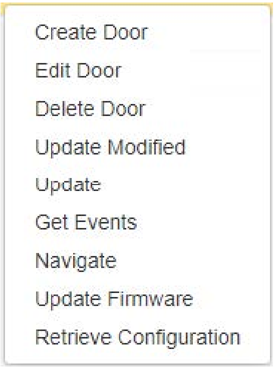


Figure 1-186: Door Submenu

11.2.2 Enabling Additional Door Types

In the door creation screen, only some door types are visible by default.

To enable the additional door types, follow these steps:

1. Navigate to the **Configuration** section.

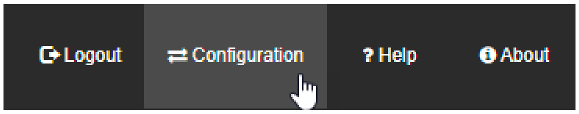


Figure 1-187: Top Menu - Configuration

2. Select the **Settings Tab**.

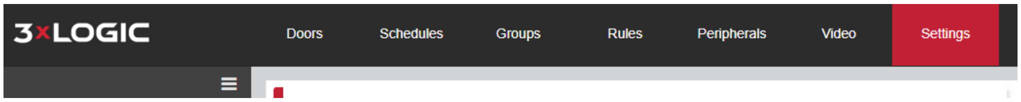
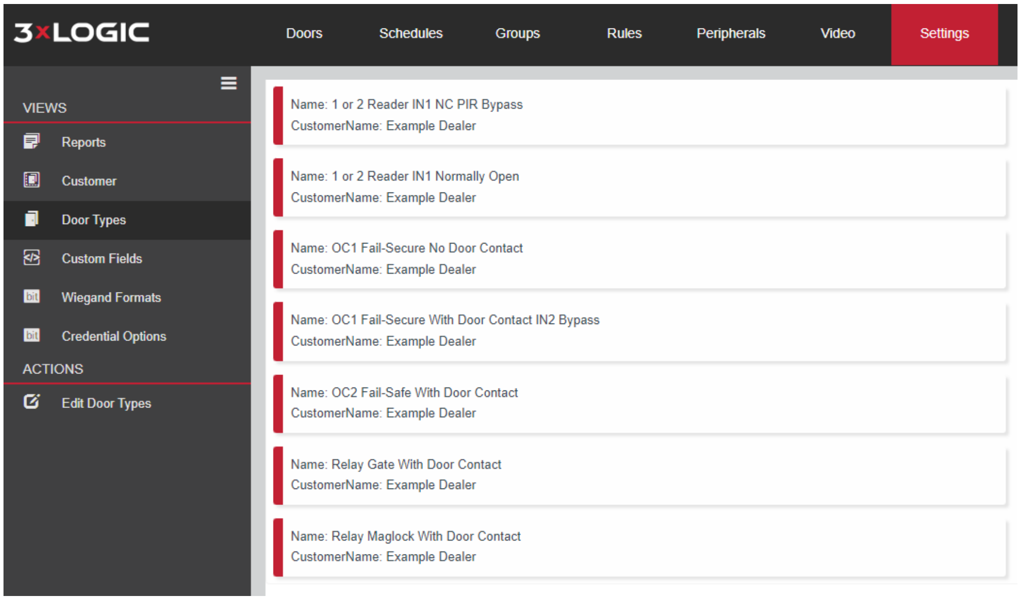


Figure 1-188: Top Menu - Configuration > Settings

3. Under the Views section, click Door Types.



Name: 1 or 2 Reader IN1 NC PIR Bypass
CustomerName: Example Dealer

Name: 1 or 2 Reader IN1 Normally Open
CustomerName: Example Dealer

Name: OC1 Fail-Secure No Door Contact
CustomerName: Example Dealer

Name: OC1 Fail-Secure With Door Contact IN2 Bypass
CustomerName: Example Dealer

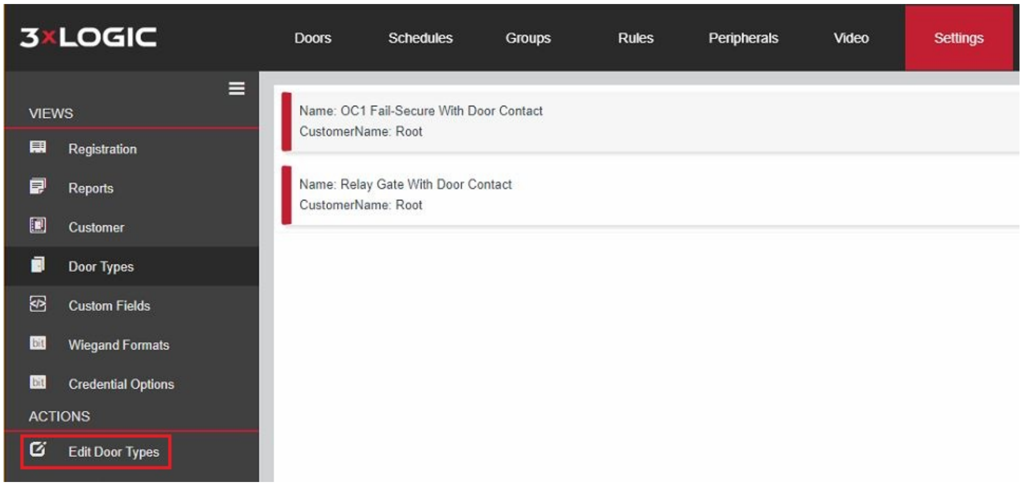
Name: OC2 Fail-Safe With Door Contact
CustomerName: Example Dealer

Name: Relay Gate With Door Contact
CustomerName: Example Dealer

Name: Relay Maglock With Door Contact
CustomerName: Example Dealer

Figure 1-189: Views > Door Types

4. Click on the **Edit Door Types** under the Actions menu section.

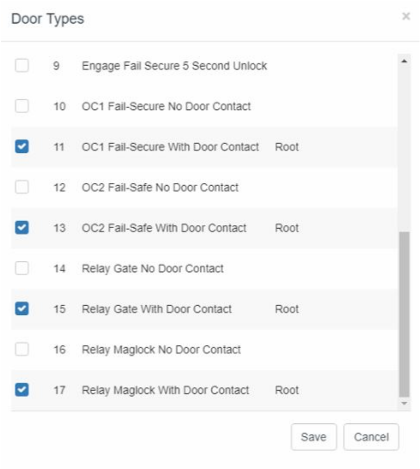


Name: OC1 Fail-Secure With Door Contact
CustomerName: Root

Name: Relay Gate With Door Contact
CustomerName: Root

Figure 1-190: Settings > Door Types > Edit Door Types

5. A new window displays additional door types that can be enabled or disabled.
    a. Select a *Door Type* and click **Save** and the new door type(s) will be added to the door types list on the Door Edit page (see Step 7b, "Additional Door Types are available. " on page 118).



☐	9	Engage Fail Secure 5 Second Unlock	
☐	10	OC1 Fail-Secure No Door Contact	
☑	11	OC1 Fail-Secure With Door Contact	Root
☐	12	OC2 Fail-Safe No Door Contact	
☑	13	OC2 Fail-Safe With Door Contact	Root
☐	14	Relay Gate No Door Contact	
☑	15	Relay Gate With Door Contact	Root
☐	16	Relay Maglock No Door Contact	
☑	17	Relay Maglock With Door Contact	Root

Figure 1-191: Available Door Types

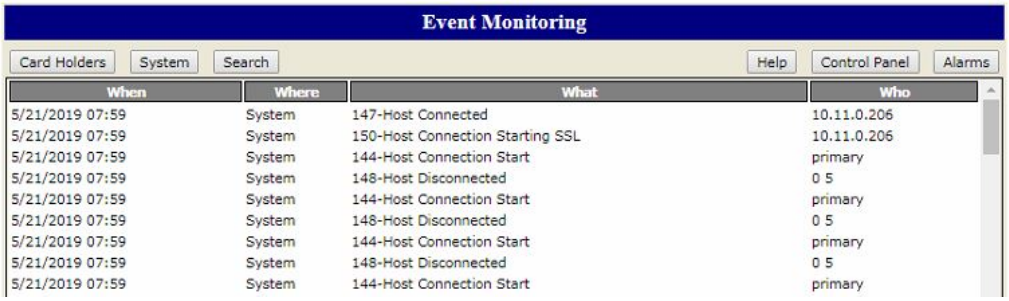
Note: Please remember, there are two Doors tabs in the software. This Doors Tab exists under the **Configuration menu** and is the only menu where a door can be created. The other Doors tab exists under the *Home Screen*. That Doors tab is the only menu with the option for manually overriding the door with a Unlock, Lock, Momentary Unlock, and Revert to Schedule.

6. Proceed to add *People* and *Credentials*.
    a. If custom zones, groups, or access privileges are required, please see the appropriate sections of the main user guide for further details.

11.3 Hosted Door Troubleshooting

When encountering problems having a hosted door sync to the server or to CLOUD, there are some simple steps to determine what might be causing the lack of communication.

1. Use a command from the address bar of the web browser to get an outbound status from any eIDC32.
    a. In the address bar, type the IP address of the eIDC32 Door Controller followed by: */eidc/getoutboundstatus*
        i. Example: 10.11.0.111/eidc/getoutboundstatus
    b. The result should resemble the following:
        i. *{"result":true, "cmd":"GETOUTBOUNDSTATUS", "body":{disabled 0, _bUsingPrimary 1, _obTimer 160648822, currentTick 294707083, _obState 10, _obSocket 0, hostIp 10.11.0.206:18800, dnsServer 10.11.0.10, retryInterval 900, HAL connection 0}}*
    c. The three primary things to look for are:
        i. *Obstate = 10*, if it is any other number the device is timing out.
        ii. *Host IP* must be populated with an address.
        iii. *DNS Server* address should have something listed if the eIDC32 is communicating outside the LAN.
2. When troubleshooting a CLOUD-synced Controller, the updated configuration should **prevent** logging into the eIDC32 using the default username (admin) and password (admin).
    a. The first step a CLOUD sync accomplishes is changing the password for the admin user to a **customer specific password** that is found on Portal.3xLogic.com under the *Settings* in the lower left.
3. The Controller's **Event Monitoring** page will show its attempts to connect to the host.
    a. If it succeeds it should look similar to the figure included below.



When	Where	What	Who
5/21/2019 07:59	System	147-Host Connected	10.11.0.206
5/21/2019 07:59	System	150-Host Connection Starting SSL	10.11.0.206
5/21/2019 07:59	System	144-Host Connection Start	primary
5/21/2019 07:59	System	148-Host Disconnected	0 5
5/21/2019 07:59	System	144-Host Connection Start	primary
5/21/2019 07:59	System	148-Host Disconnected	0 5
5/21/2019 07:59	System	144-Host Connection Start	primary
5/21/2019 07:59	System	148-Host Disconnected	0 5
5/21/2019 07:59	System	144-Host Connection Start	primary

Figure 1-192: Events - Event Monitoring

4. If the site running a Hosted Controller is tightly managed by network administration, it could be that the controller is being prevented from communicating out of the LAN or over different subnets.
    a. Please contact the local network admin and verify nothing is being blocked by firewall, domain, or antivirus.

For any additional issues or further assistance, please contact INFINIAS Support.

12 First In Door Behavior

This section features the contents of the First in Behavior Guide, which covers the "in software" **First In** setup that modifies Door behavior.

By modifying the door behavior itself, the First In scheduled door behavior is programmed into the Door Controller directly and still works even if the software crashes or CLOUD controller loses it's network connection. A First In schedule prevents the specified Doors from opening with their normal unlock schedule unless a valid credential is swiped at the reader.

In Example: A small business may be closed due to inclement weather during the winter and the door is normally unlocked from 8am-5pm; with a First In schedule, the door remains locked if no employee show up to work that morning to present a card.

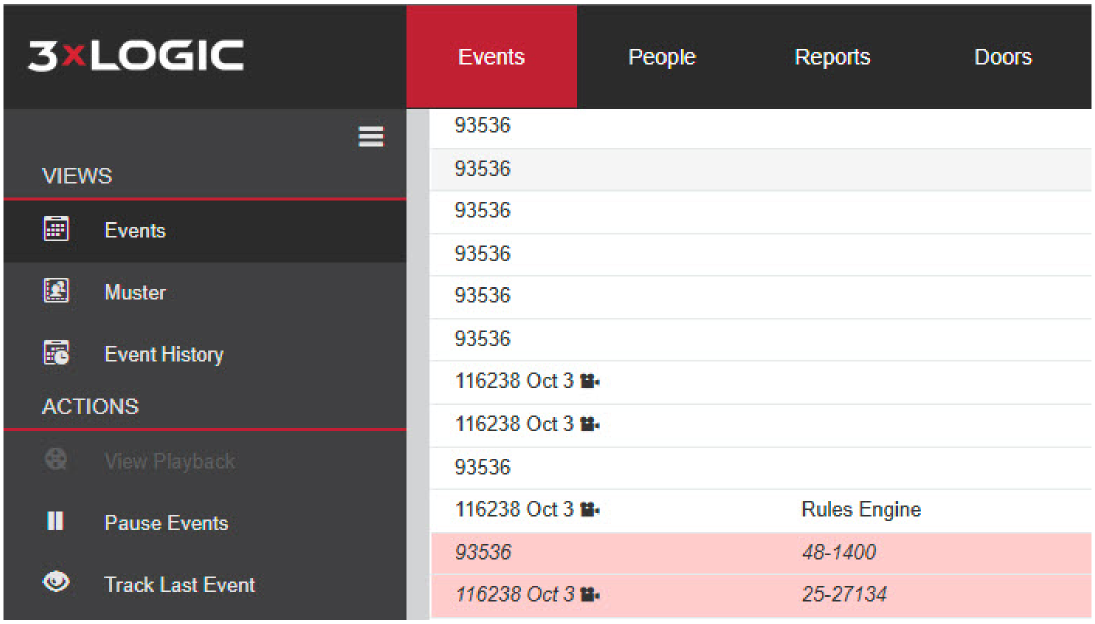
12.1 Requirements

- Software version 6.7.10485 or higher
- Controller firmware 3.9.59 or higher
- Door/Controller must be created as "Hosted"

12.2 Configuration

Access the Portal via the following URL: https://portal.3xlogic.com

Once logged in the software, the Events tab loads by default.



93536	
93536	
93536	
93536	
93536	
93536	
116238 Oct 3	
116238 Oct 3	
93536	
116238 Oct 3	Rules Engine
93536	48-1400
116238 Oct 3	25-27134

Figure 1-193: Portal > Events

Navigate to the **Configuration** section to use the **Doors Tab** there (separate from the Doors Tab in the same menu as Events, which does not have the Behavior configuration section). The *correct* Doors Tab loads by default when navigating to Configuration.

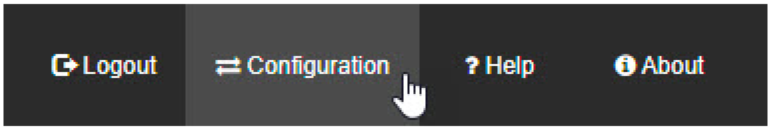
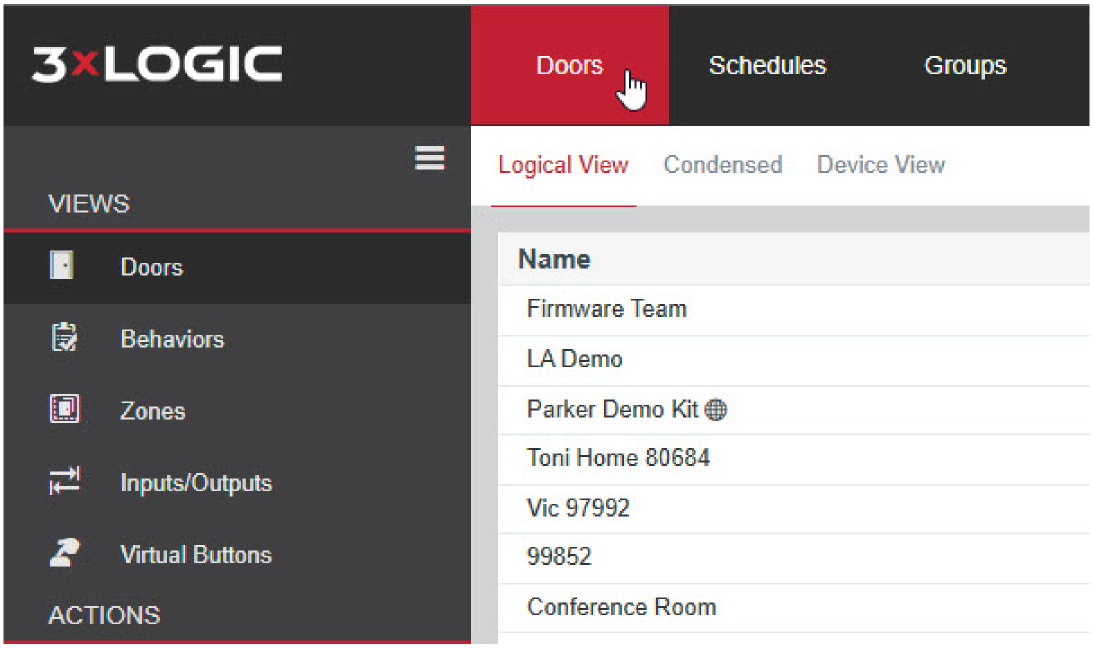


Figure 1-194: Configuration



Name
Firmware Team
LA Demo
Parker Demo Kit 🌐
Toni Home 80684
Vic 97992
99852
Conference Room

Figure 1-195: Configuration > Doors

Select **Behaviors** under *Views* on the left side of the screen.

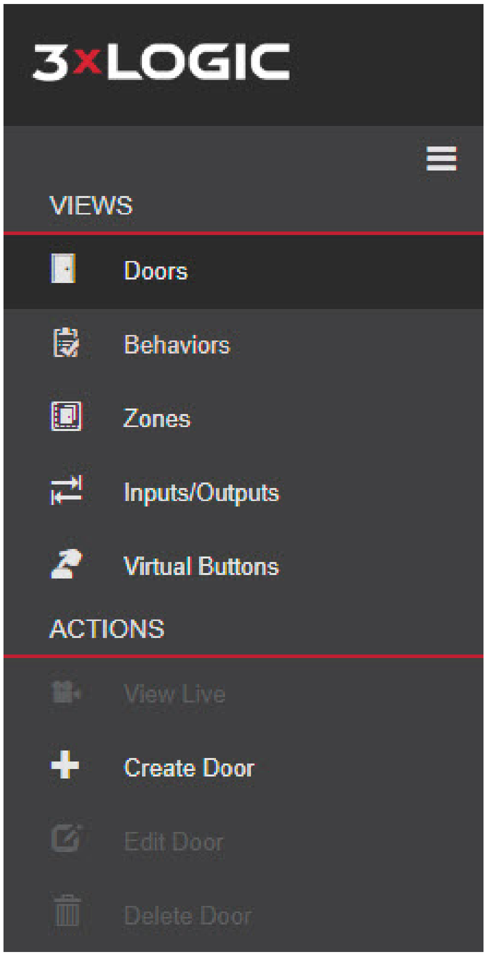


Figure 1-196: Left side Menu (default)

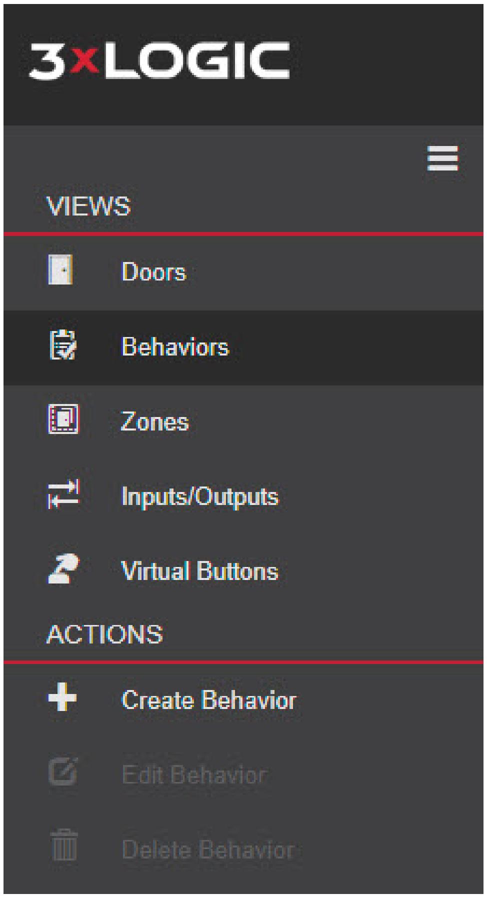
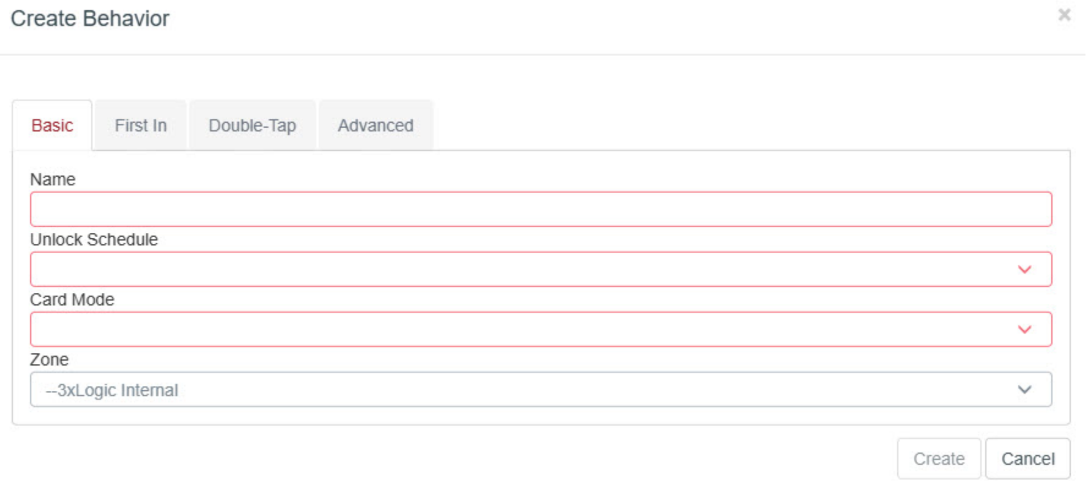


Figure 1-197: Behaviors left side Menu (on click)

Either *Edit* or *Create* a door Behavior. Select a existing Door or Create, Edit, or Delete Behavior associated with that Door.



Name

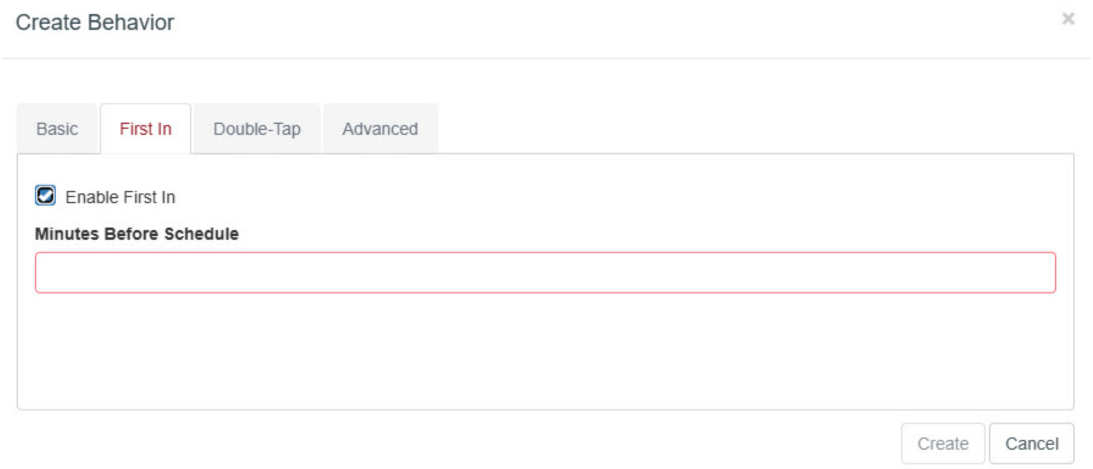
Unlock Schedule

Card Mode

Zone: --3xLogic Internal

Figure 1-198: Create Behavior dialog

Choose the **First In tab** to enable the feature using the checkbox, then choose the minutes prior for the card swipe to work to revert the door back to its normal schedule/behavior.



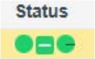
☑ Enable First In

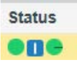
Minutes Before Schedule

Figure 1-199: Enable First In Behavior

12.3 Verification

To confirm correct setup, verify the following:

1. When the unlock schedule beginning time is reached the door simply will not unlock.
2. The lock status will remain locked.
    a. 

    Green Icon
3. Swipe a valid credential and the door should then start it's normal unlock schedule.
    a. 

    Blue Icon

12.4 FAQ

These are some common questions and answers:

- Q: Can a certain group be tied to the first in schedule?
    - A: No not for this behavioral first in schedule; only a first in set up via rules engine can accomplish this.
- Q: Can an alternative event be used to trigger the first in other than "Valid Credential" card swipes like a toggle button?
    - A: No, this can only be accomplished using the rules based First In set up.

13 Configuring Mobile Credentials

This section features the contents of the Configuring Mobile Credentials Guide, which allows users to unlock Doors using a smartphone app.

13.1 Overview

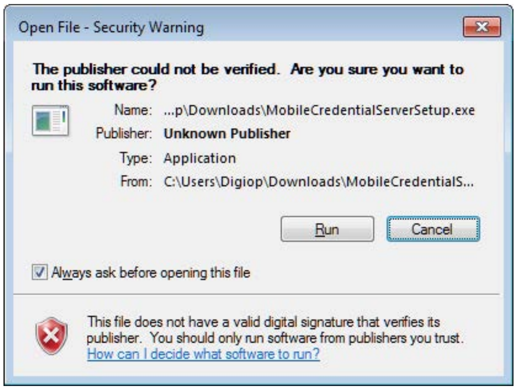
Mobile Setup involves the following requirements:

1. The installation of Mobile Credential Server software.
    a. The version should match the version of INFINIAS.
    b. Upgrading INFINIAS to latest release is recommended.
2. Licensing INFINIAS with a Mobile Credential license.
    a. Purchase required beyond the 2-pack license that comes with software.
3. Installation of the Mobile Credential Application.
    a. The app is a free download, available for Android and Apple devices.
4. Both Wi-Fi connectivity for internal smart device usage and Port Forwarding setup for external usage.
    a. IT Administrator to configure setup (workflow details not covered here).

13.2 Mobile Credential Server

The INFINIAS Mobile Credential Server installation package installs the necessary components for a smart device application to communicate with INFINIAS.

1. **Download** Mobile Credential Server Setup from www.3xlogic.com
    a. Found under Support > Software Downloads
2. **Move** the file to the desired installation directory (PC folder).
    a. The installer will choose the current location by default, but also offers the option to choose an alternate location (see Step 7) during the setup.
3. **Run** (e.g. double click) the downloaded file to initialize the installation.
    a. A window similar to the following may appear. If so, click **Run**.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

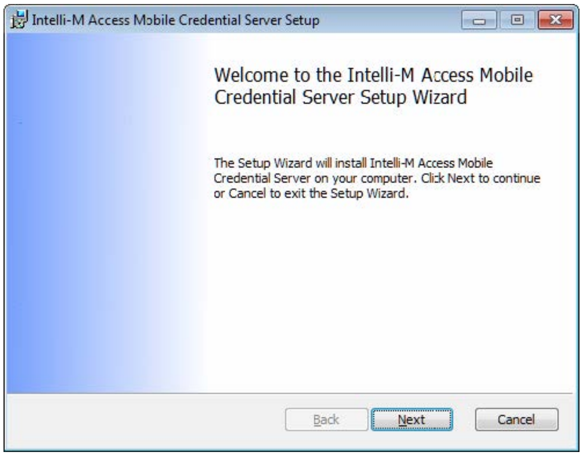
Name: ...p\Downloads\MobileCredentialServerSetup.exe
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\Digiop\Downloads\MobileCredentialS...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Figure 1-200: Run confirmation

4. Follow the Welcome window (installation dialog) prompts to continue.

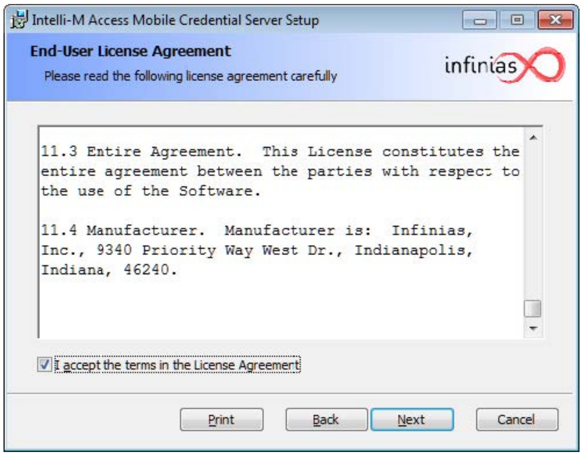

Intelli-M Access Mobile Credential Server Setup

Welcome to the Intelli-M Access Mobile Credential Server Setup Wizard

The Setup Wizard will install Intelli-M Access Mobile Credential Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 1-201: Welcome window

5. When the *License Agreement* window appears, read the contents thoroughly.
6. After reviewing the terms and conditions, **click the checkbox** next to 'I accept the terms in the License Agreement,' then click **Next** to continue.
    a. Otherwise, click *Cancel* and discontinue installation of this product.


Intelli-M Access Mobile Credential Server Setup

End-User License Agreement

Please read the following license agreement carefully

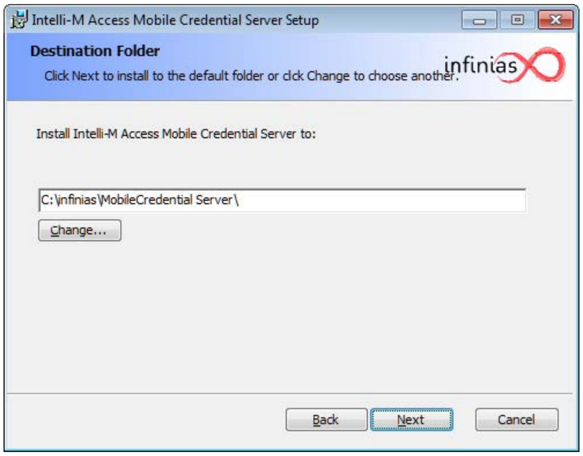
```
11.3 Entire Agreement.  This License constitutes the
entire agreement between the parties with respect to
the use of the Software.

11.4 Manufacturer.  Manufacturer is:  Infinias,
Inc., 9340 Priority Way West Dr., Indianapolis,
Indiana, 46240.
```

☑ I accept the terms in the License Agreement

Figure 1-202: License Agreement

7. In the Destination Folder screen, specify an installation location, if desired.



Intelli-M Access Mobile Credential Server Setup

Destination Folder

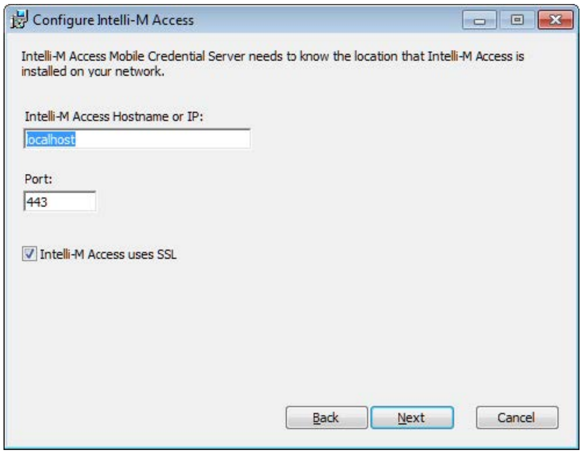
Click Next to install to the default folder or click Change to choose another.

Install Intelli-M Access Mobile Credential Server to:

C:\infinias\MobileCredential Server\

Figure 1-203: Destination Folder

8.



Configure Intelli-M Access

Intelli-M Access Mobile Credential Server needs to know the location that Intelli-M Access is installed on your network.

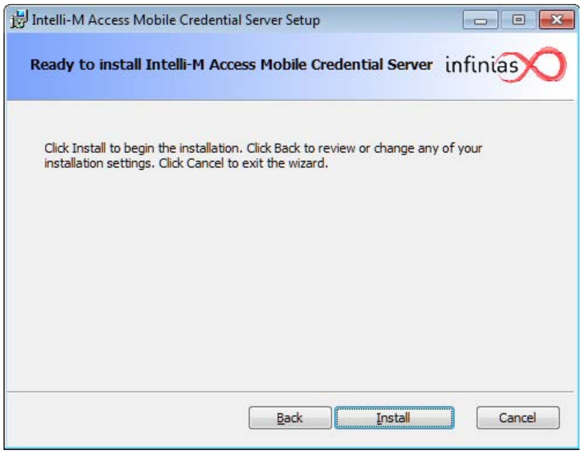
Intelli-M Access Hostname or IP: localhost

Port: 443

☑ Intelli-M Access uses SSL

Figure 1-204: Hostname or IP, and Port

9. *Verify* that the options shown on the screen are correct, then click **Next** to continue.
10. On the following screen, click **Install** to execute the installation.



Intelli-M Access Mobile Credential Server Setup

Ready to install Intelli-M Access Mobile Credential Server

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 1-205: Confirm Installation

11. After the installation completes, click **Finish** to close the Setup Wizard.
    a. Contact Support for assistance concerning any errors.

13.3 Mobile Credentials Licensing

This section covers the steps to add a license pack to the INFINIAS software and configure users for Mobile Credentials. The following restrictions apply:

- Licensing is tied to the **Device** being used, not the *Person*.
  - If a Person has three smart Devices using Mobile Credentials and the software is licensed for a 10 pack, three Licenses of the 10 pack will cover the three Devices for the one Person.
- The Licenses are permanently *encrypted* to the Device.
  - If the Device is replaced or the application is uninstalled from it, that assigned license is permanently used from the pack.
- A license *cannot* be transferred to another Device nor can it be transferred to another person.
- Every purchase of INFINIAS comes with an included 2-pack license of Mobile Credentials
  - This permits testing the feature without investing additional funds to obtain licensing.
- Additional license packs are available for purchase in the following quantities:
  - Single Pack
  - 20 Pack
  - 50 Pack
  - 100 Pack
  - 500 Pack

Note: Please contact 3xLOGIC Sales for additional licenses and pricing.

To begin, access the Infinias application and log in.

1. Once logged in the software, the Events tab loads by default.
2. Navigate to the Settings Tab of the INFINIAS software in the *Configuration* section.

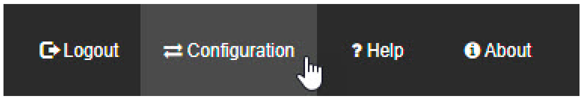


Figure 1-206: Configuration

   a. This is the same location where the INFINIAS software license was activated.

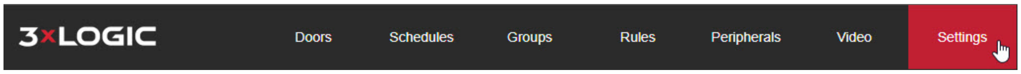
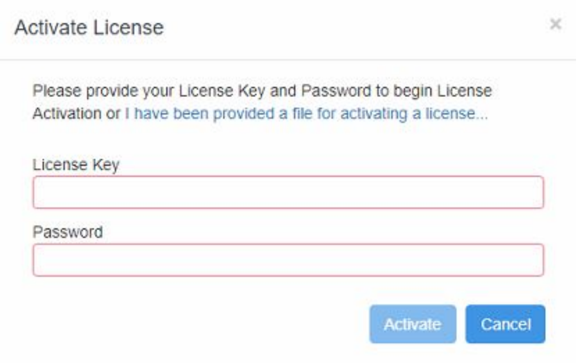


Figure 1-207: Settings Tab

3. **Enter the license details** as they appear on the *Settings Tab*.


Activate License

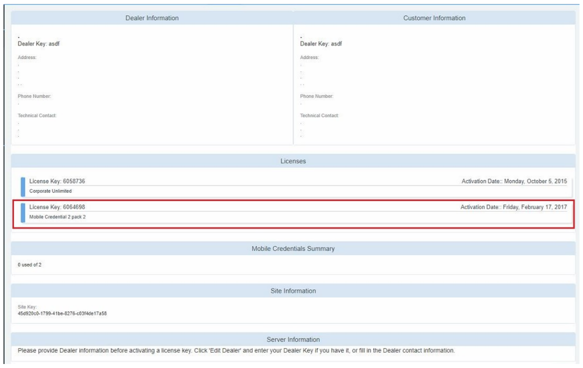
Please provide your License Key and Password to begin License Activation or I have been provided a file for activating a license...

License Key

Password

Figure 1-208: Settings Tab > Activate License

a. Ensure the entry properly designates the number of licenses in the license pack.


Dealer Information

Dealer Key: asdf
Address:
Phone Number:
Technical Contact:

Customer Information

Dealer Key: asdf
Address:
Phone Number:
Technical Contact:

Licenses

License Key: 6058736 Activation Date:: Monday, October 5, 2015
Corporate Unlimited

License Key: 6064698 Activation Date:: Friday, February 17, 2017
Mobile Credential 2 pack 2

Mobile Credentials Summary

0 used of 2

Site Information

Site Key:
45d920c0-1799-41be-8276-c03f4de17a58

Server Information

Please provide Dealer information before activating a license key. Click 'Edit Dealer' and enter your Dealer Key if you have it, or fill in the Dealer contact information.

Figure 1-209: Settings Tab > License information

4. After successful licensing, navigate over to the Person Tab using the **Home** shortcut.

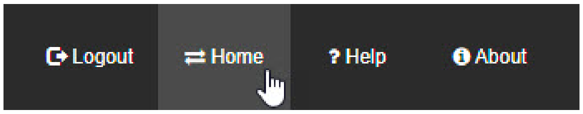


Figure 1-210: Home shortcut (top right)

a. Click the **3xLOGIC logo** at the top left of the page *also* navigates Home.

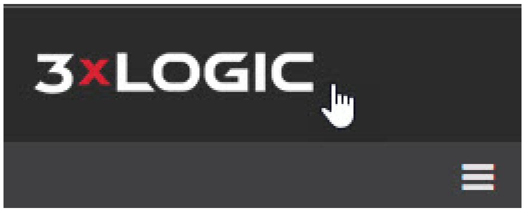


Figure 1-211: 3xLOGIC logo (Home shortcut)

b. Again, the *Events Tab* loads by default when using the Home shortcut.

5. Select the **People Tab** from the top menu.

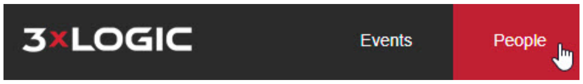


Figure 1-212: People Tab

6. From the People Tab, highlight the person (single left click) and then:
   a. Click **Edit** under the Actions options on the left side menu or…
   b. *Right-click the person* and select **Edit** on the on-screen menu that appears.

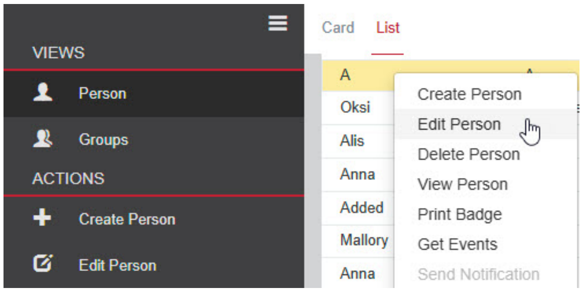
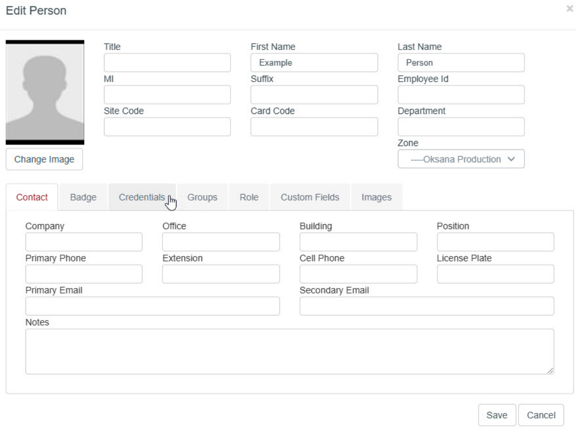


Figure 1-213: People > Actions > Edit Person (options)

7. On the *Edit Person* page, click on the **Credentials Tab**.

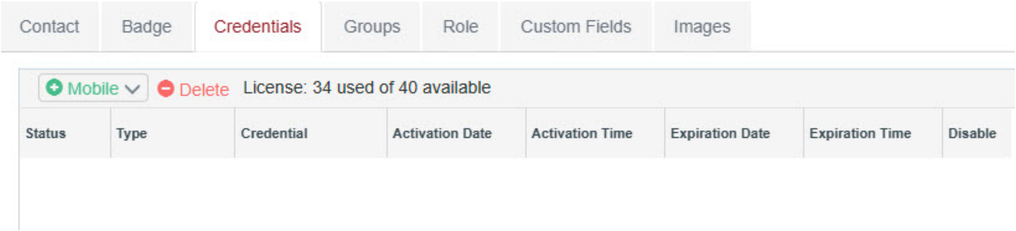

Edit Person

First Name: Example

Last Name: Person

Zone: —Oksana Production

Figure 1-214: Edit Person page

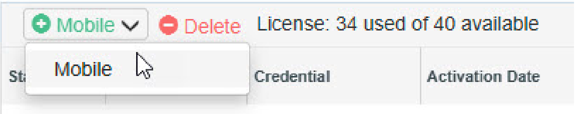


License: 34 used of 40 available

Status	Type	Credential	Activation Date	Activation Time	Expiration Date	Expiration Time	Disable

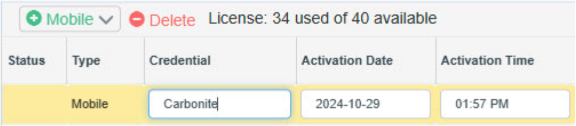
Figure 1-215: Credentials Tab

a. Add a **Mobile Credential** and enter a credential into the Credential Field.
   i. A complex credential is not required as the credential will be encrypted once the smart device app syncs with the software and then it will not be visible or required again.



License: 34 used of 40 available

Figure 1-216: Credentials Tab > Add Mobile



License: 34 used of 40 available

Status	Type	Credential	Activation Date	Activation Time
	Mobile	Carbonite	2024-10-29	01:57 PM

Figure 1-217: Credentials Tab > Mobile Added

8. Once the configuration is **Saved**, the software-side setup is complete.

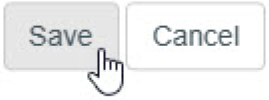


Figure 1-218: Save changes

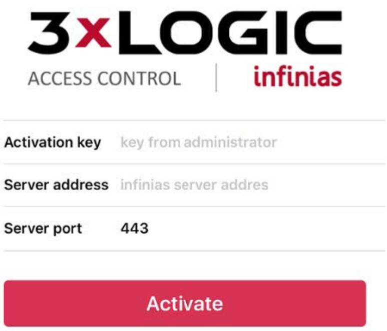
9. Proceed to install and configure the smart device application (see the next section).

13.4 Mobile Credential Application

Navigate to the corresponding app store on the device and search for INFINIAS and look for the INFINIAS Mobile Credential by 3xLOGIC Systems Inc. Install the app on the smart device.

Note: While the free Mobile Credential app can be installed on Android and Apple devices, the examples shown here are captured from an iPhone.

1. To begin, open the app and enter the following information:
    a. Activation Key
        i. This is the credential set to the person on Intelli-M Access
    b. Server Address
        i. The internal address is for smart devices that are Wi-Fi only.
        ii. The public or external address along with port forwarding is for external use (from outside of the local network).
    c. Server Port
        i. Leave as the default value unless a custom port option was set in the initial installation process of the Mobile Credential setup wizard.
2. Once the setup details are verified, click **Activate**.



3xLOGIC
ACCESS CONTROL | infinias

Activation key key from administrator
Server address infinias server addres
Server port 443

Figure 1-219: Setup details

3. After successful activation, a list of doors that the Person has permission to use populates in a list.
    a. A single Door can be selected as the default door and it can be changed by editing the door list.
    b. The app can also be re-activated in case of issues from the Menu:

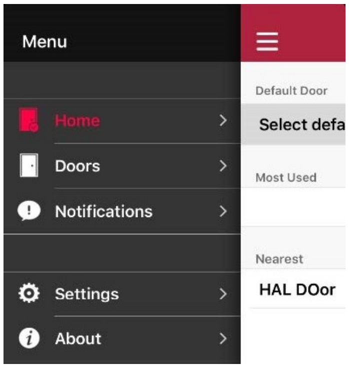
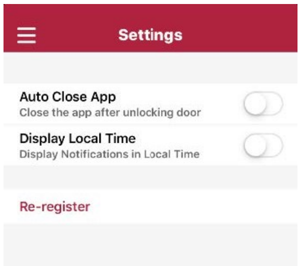


Figure 1-220: Main Menu

i. Select Re-register on the Settings page:


Settings

Auto Close App
Close the app after unlocking door

Display Local Time
Display Notifications in Local Time

Re-register

Figure 1-221: Settings page

4. Initial setup is now complete.
5. Please contact support if there are any problems that prevent completing the installation process or if there are any errors.
    a. Be prepared to provide remote access using either TeamViewer or by using our Remote Support utility downloaded from 3xLOGIC.com.

14 VIGIL Video Integration

This section features the contents of the VIGIL Video and INFINIAS CLOUD Integration Guide, which covers associating Video from a VIGIL Server or V-Series Camera to Doors within INFINIAS CLOUD for the purposes of viewing video on the **INFINIAS Mobile App**.

14.1 Prerequisites

This guide assumes that VIGIL and/or V-Series cameras are already setup, and an INFINIAS CLOUD account with devices is already created.

14.2 Video Setup

VIGIL Connect is used to quickly and easily access video remotely without requiring an advanced configuration. Using VIGIL Connect removes the requirements of configuring a router for port forwarding and having a static IP. Without VIGIL Connect, proper port forwarding rules must be in place. Please consult the separate VIGIL Server User Guide for further instructions.

Note: V-Series cameras with appropriate licensing can also be integrated without a VIGIL Server and associated with INFINIAS CLOUD doors.

14.2.1 Configure VIGIL Connect Alias on VIGIL Server

1. After logging into the VIGIL Server appliance, click the Settings button.

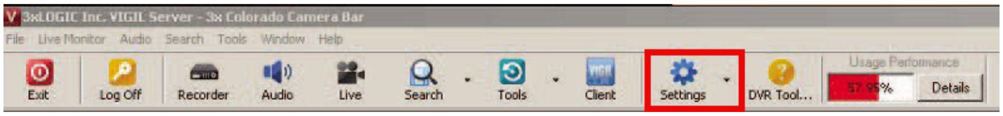
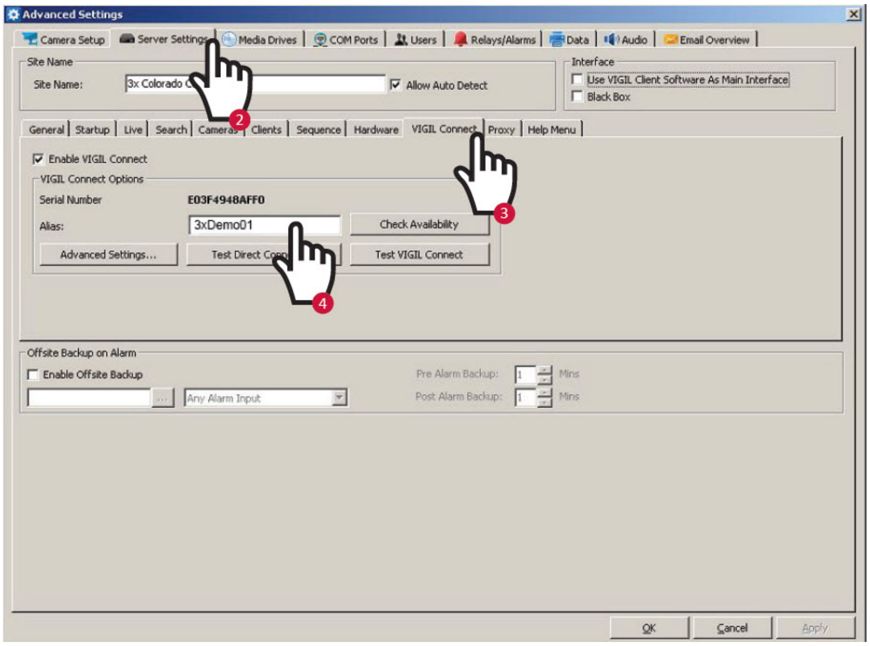


Figure 1-222: Settings button

2. Select the **Server Settings** tab.
3. Select the **VIGIL Connect** sub tab.
4. Take note of the *existing Alias* if one has already been setup; otherwise *create an Alias* and check to see if it's available.



Site Name

Site Name: 3x Colorado C

☑ Allow Auto Detect

Interface

□ Use VIGIL Client Software As Main Interface

□ Black Box

☑ Enable VIGIL Connect

VIGIL Connect Options

Serial Number E03F4948AFF0

Alias: 3xDemo01

Offsite Backup on Alarm

□ Enable Offsite Backup

Any Alarm Input

Pre Alarm Backup: 1 Mins

Post Alarm Backup: 1 Mins

Figure 1-223: Steps 2-4, in order

14.2.2 Associate Video with a Door

1. Using a web browser, navigate to the **INFINIAS CLOUD portal** URL: https://ia.3xlogic.com
   a. Login using established credentials.
   b. The *Events* page loads by default.

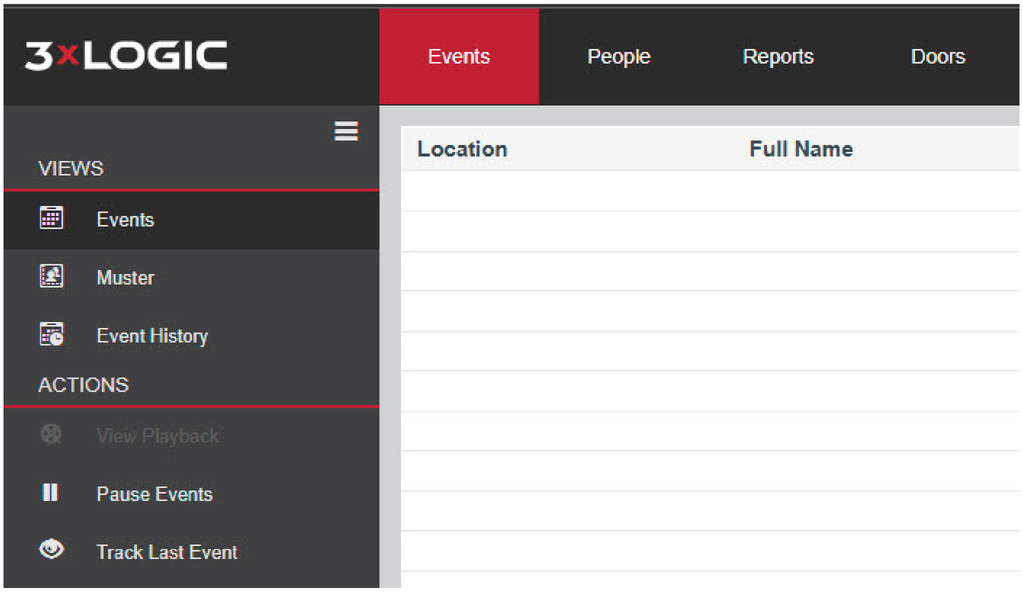


Figure 1-224: INFINIAS CLOUD portal

2. From the top right-hand corner, click **Configuration**.

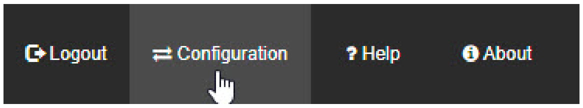


Figure 1-225: Configuration

3. Select the **Video Tab** within the *Configuration* Section (the Doors Tab loads by default).
    a. If the Configuration link isn't shown, ensure the logged user has administrative rights.

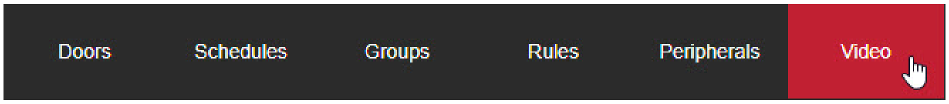


Figure 1-226: Video Tab

4. From the left side menu click **Create Appliance** (under *Actions*).

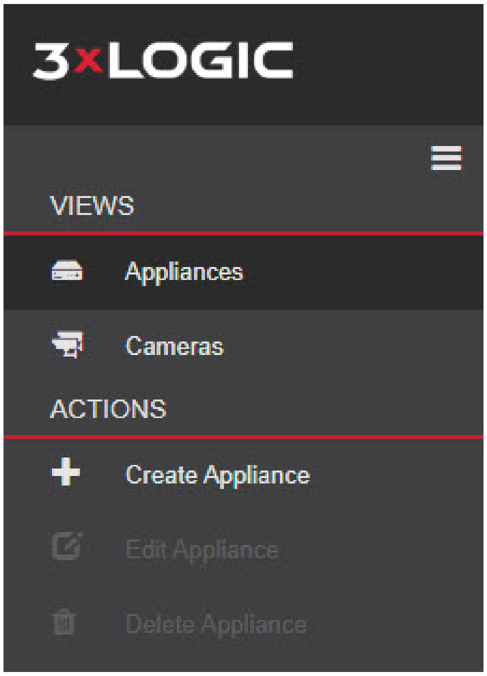
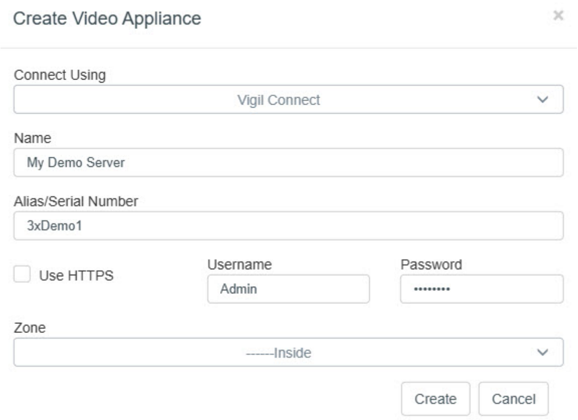


Figure 1-227: Left side menu

5. Fill in the relevant information in the resulting dialog box.
    a. **Type**: From the dropdown menu select the device type.
        i. In this example, VIGIL Connect is configured as part of the *Alias*.
    b. **Name**: Enter the name of the VIGIL Server; this is for description purposes only.
    c. **Alias/Serial Number**: Enter information for the respective VIGIL device (Server or V-Series Camera).
        i. If entering an *Alias*, ensure that the Alias matches the Alias originally created on the VIGIL Server Appliance or V-Series Camera.
    d. **Username and Password**: This is the username and password of an individual with admin credentials on the VIGIL Server.

e. **Zone**: This field will determine which INFINIAS CLOUD administrators are able to configure camera associations.



Create Video Appliance ×

Connect Using: Vigil Connect

Name: My Demo Server

Alias/Serial Number: 3xDemo1

□ Use HTTPS

Username: Admin

Password: ••••••••

Zone: ------Inside

Create | Cancel

Figure 1-228: Dialog box fields

6. To associate cameras to doors click **Cameras** from the left side menu.

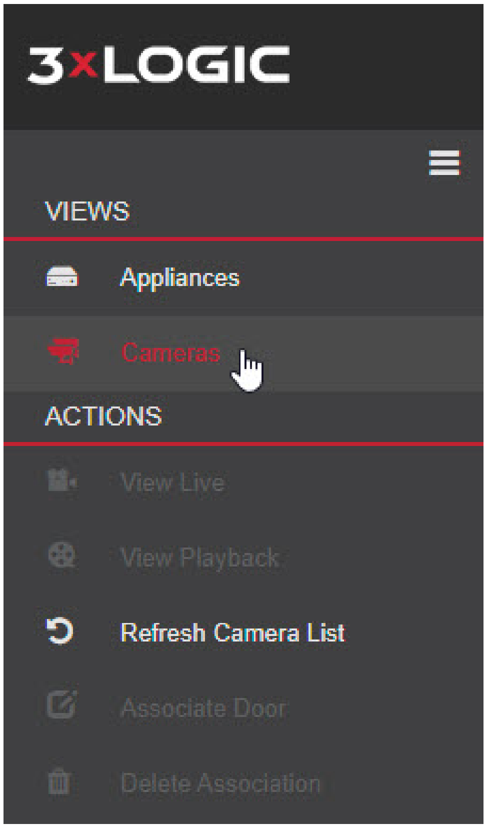


Figure 1-229: Cameras option

7. Click **Associate Door** (under Actions).

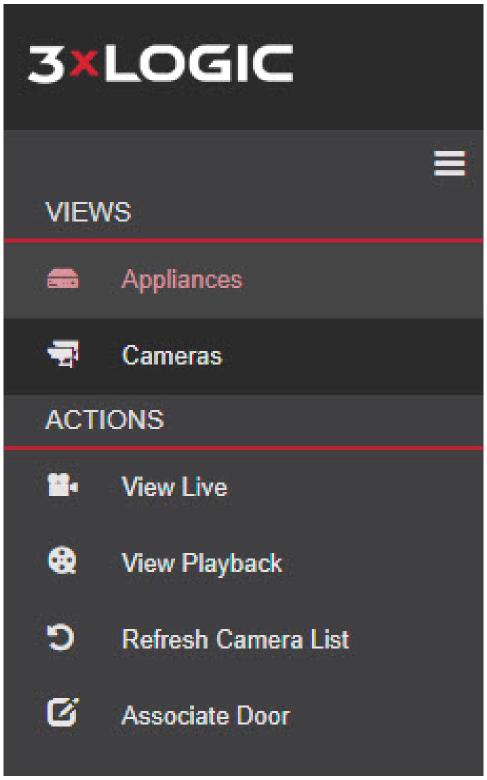
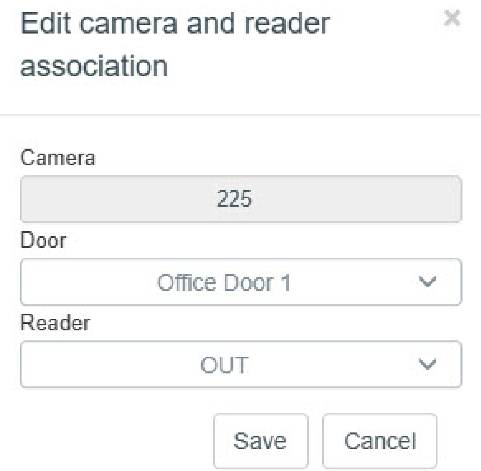


Figure 1-230: Actions > Associate Door

8. Select the appropriate *Camera*, *Door*, and *Reader*.
   a. In some cases a Door may have a Camera on both sides of the Door.
   b. The Reader field determines which **side** of the Door the Camera is viewing.


Edit camera and reader association

Camera: 225

Door: Office Door 1

Reader: OUT

Figure 1-231: Camera and Reader Association

9. If specific Doors are unavailable, ensure the appropriate Zone is selected in the previous step.

14.3 Mobile App Navigation

The INFINIAS Mobile App is intended for reviewing events, associated video (when configured), and suspending cardholders.

Note: This is not a replacement for the Mobile Credential app.

14.3.1 Download and Login

Access from the Google Play or iTunes store.

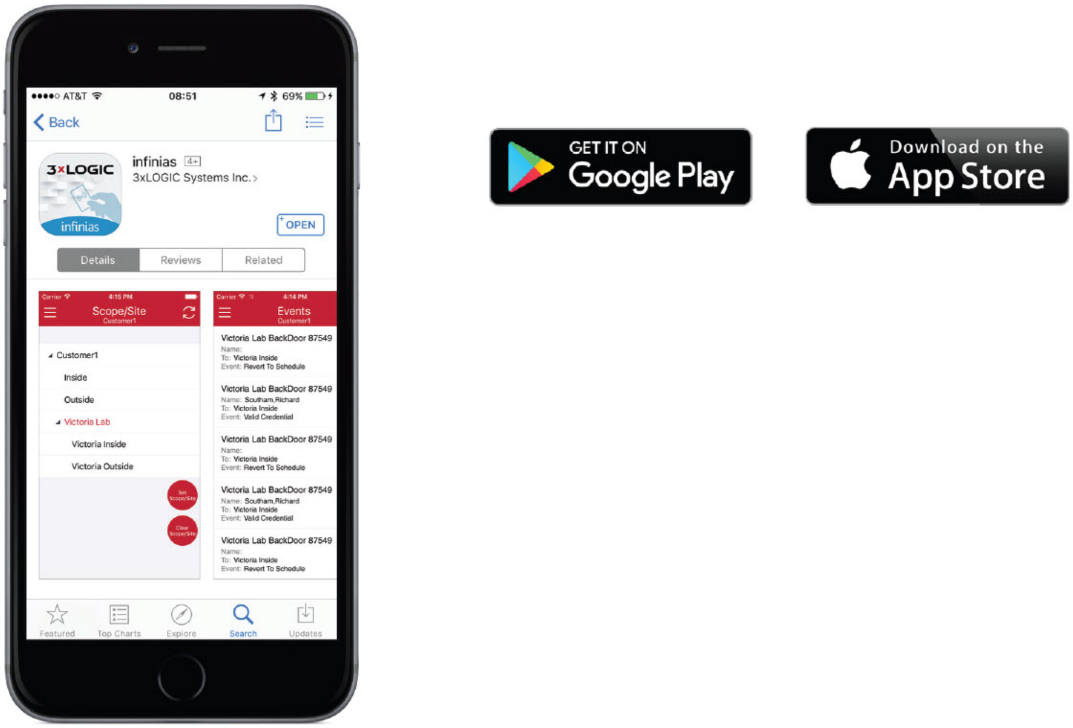


Figure 1-232: Mobile App options

Select the **Cloud Host** option and then enter INFINIAS CLOUD username and password.

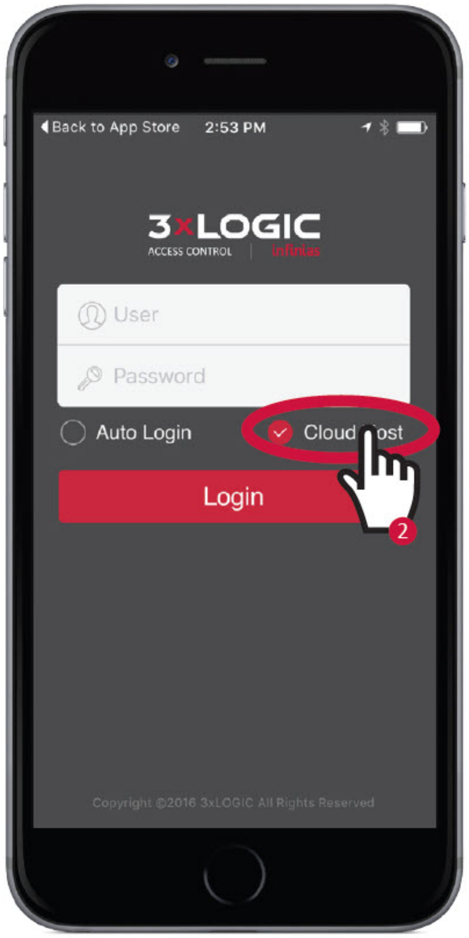
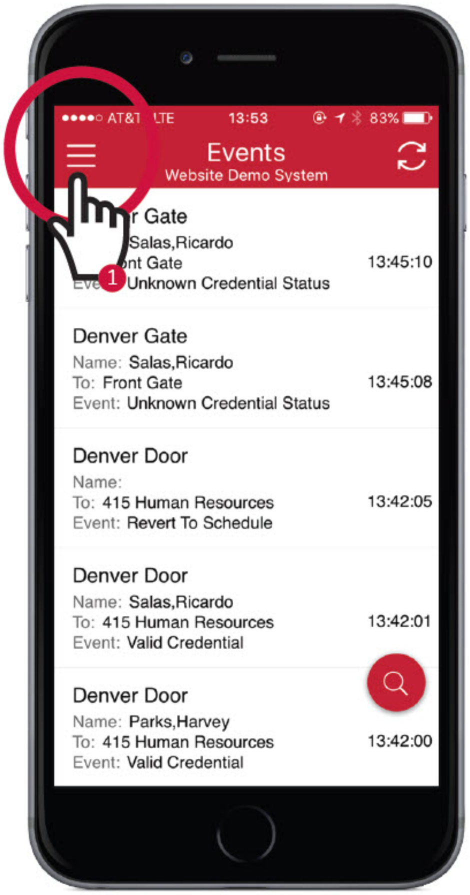


Figure 1-233: Cloud Host (2)

14.3.2 Menu Options

Moving to different areas of the app is simple. Select the Overflow Menu **Icon** (three stacked, horizontal lines) in the top left of the screen to view the Navigation Menu.



Events
Website Demo System

r Gate
Salas,Ricardo
nt Gate
Eve Unknown Credential Status
13:45:10

Denver Gate
Name: Salas,Ricardo
To: Front Gate
Event: Unknown Credential Status
13:45:08

Denver Door
Name:
To: 415 Human Resources
Event: Revert To Schedule
13:42:05

Denver Door
Name: Salas,Ricardo
To: 415 Human Resources
Event: Valid Credential
13:42:01

Denver Door
Name: Parks,Harvey
To: 415 Human Resources
Event: Valid Credential
13:42:00

Figure 1-234: Overflow Menu Icon

The Navigation Menu features access to:

- Scope/Site
- Events
- People
- Doors
- Settings
- Exit

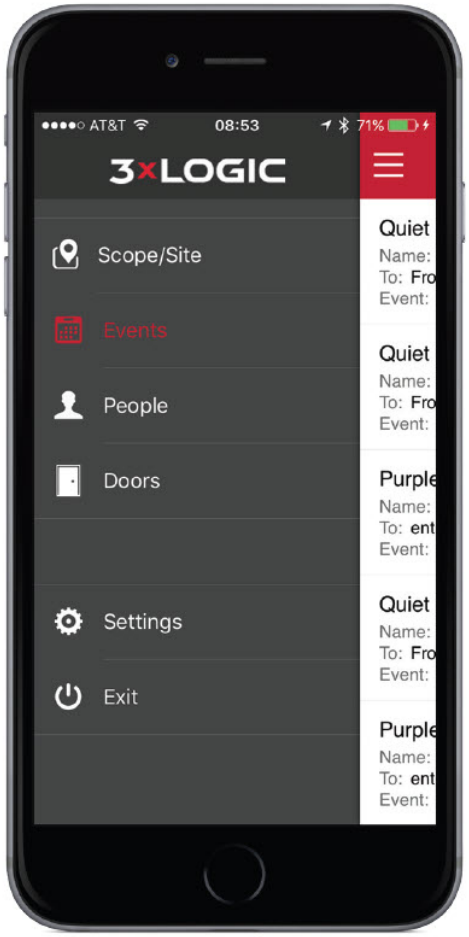


Figure 1-235: Navigation Menu

14.3.3 Live Video

Go to the Doors screen from the Navigation Menu.

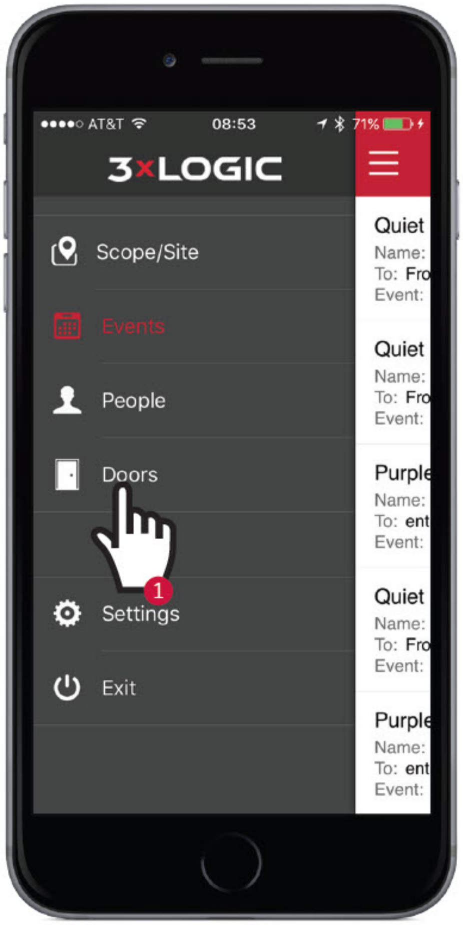
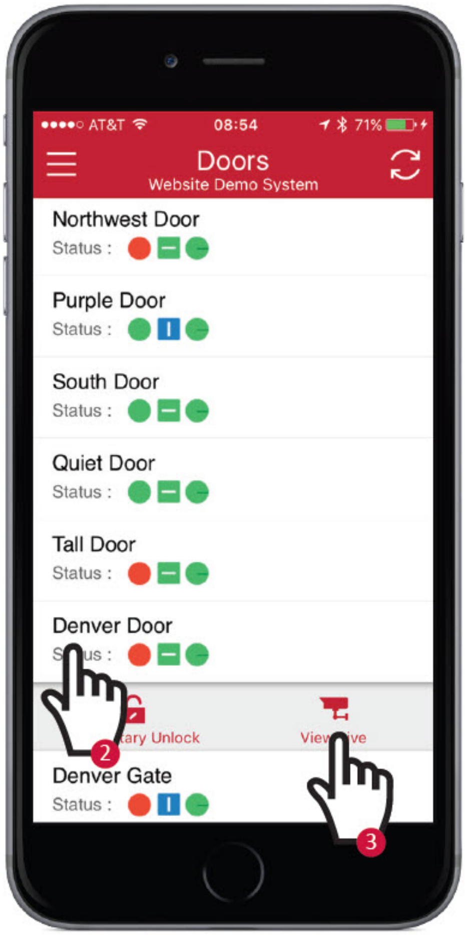


Figure 1-236: Navigation Menu > Doors (1)

Select the target Door and then the View Live icon.



●●●●○ AT&T 08:54 71%

Doors

Website Demo System

Northwest Door

Status :

Purple Door

Status :

South Door

Status :

Quiet Door

Status :

Tall Door

Status :

Denver Door

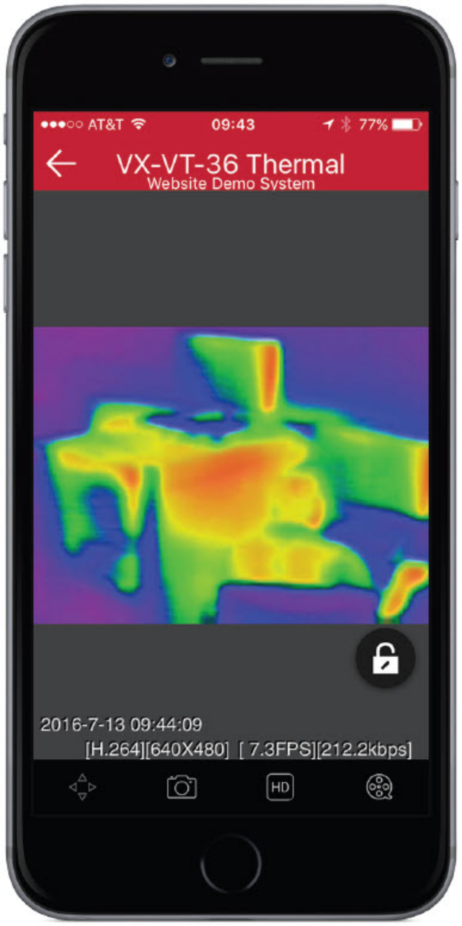
Status :

Denver Gate

Status :

Figure 1-237: Door (2) and View Live (3)

The Camera feed displays.



●●●○○ AT&T 09:43 77%

VX-VT-36 Thermal
Website Demo System

2016-7-13 09:44:09
[H.264][640X480] [7.3FPS][212.2kbps]

Figure 1-238: Camera Feed (thermal)

14.3.4 Unlock a Door

From the *Navigation Menu*, access the **Doors** screen and select the target Door.

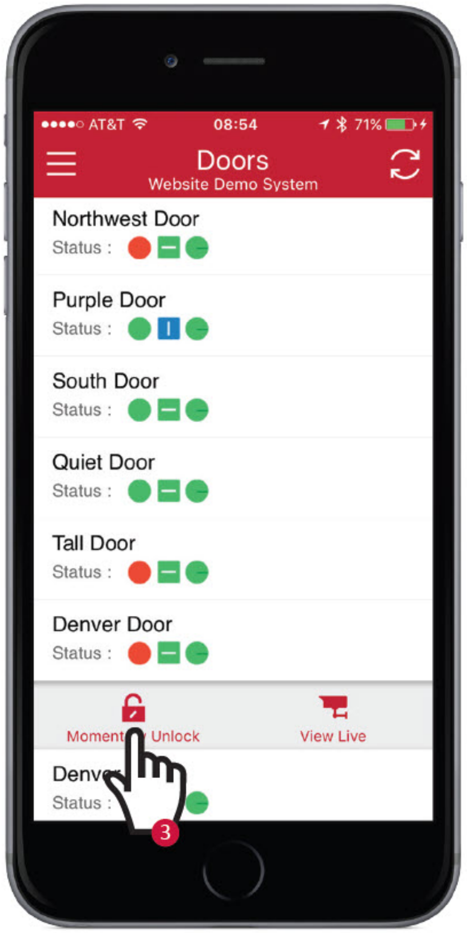


Figure 1-239: Target Door > Momentary Unlock (3)

Choose the **Momentary Unlock** option using the icon, which unlocks the *Door* for 5 seconds. An **Unlocked icon** displays to indicate the status.

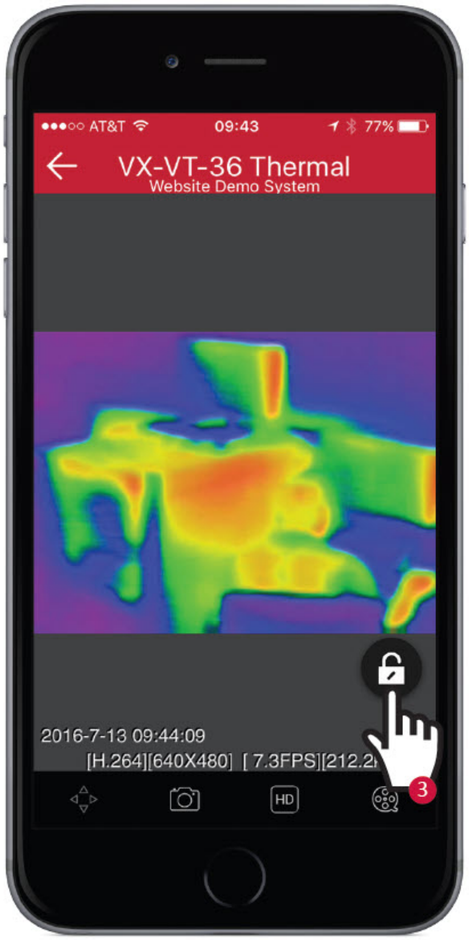
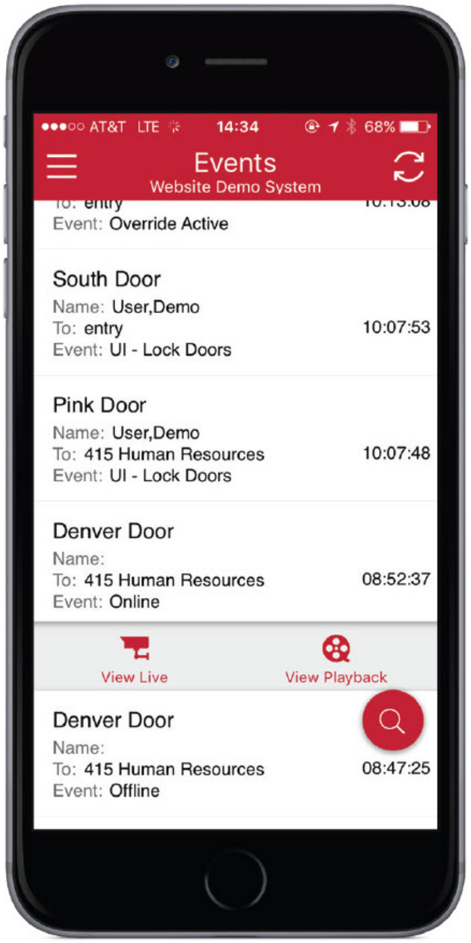


Figure 1-240: Camera feed > Unlocked icon (3)

14.3.5 Review Events

From the *Navigation Menu*, access the **Events** screen and select the target Event.



To: entry 10:13:08
Event: Override Active

South Door
Name: User,Demo
To: entry 10:07:53
Event: UI - Lock Doors

Pink Door
Name: User,Demo
To: 415 Human Resources 10:07:48
Event: UI - Lock Doors

Denver Door
Name:
To: 415 Human Resources 08:52:37
Event: Online

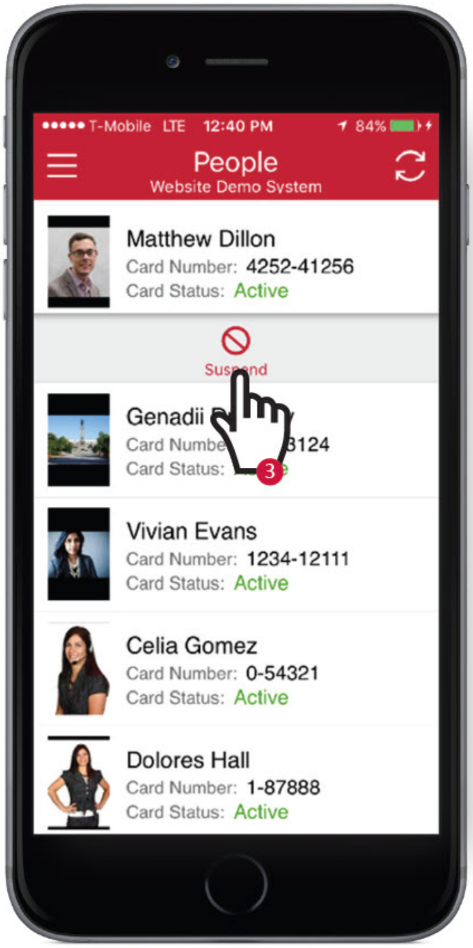
Denver Door
Name:
To: 415 Human Resources 08:47:25
Event: Offline

Figure 1-241: Target Event > Icon options

Select either the **View Live** icon for the *current feed* or the **View Playback** icon for *recordings*.

14.3.6 Suspend a Cardholder

From the *Navigation Menu*, access the **People** screen and select the target Person.



Matthew Dillon
Card Number: 4252-41256
Card Status: Active

Genadii R y
Card Numbe 3124
Card Status: e

Vivian Evans
Card Number: 1234-12111
Card Status: Active

Celia Gomez
Card Number: 0-54321
Card Status: Active

Dolores Hall
Card Number: 1-87888
Card Status: Active

Figure 1-242: Target Person > Suspend icon

Select the **Suspend** icon to revoke all card access rights, making the card status *inactive*.

15 Active Directory Integration

This section features the contents of the Active Directory Integration Guide.

INFINIAS integrates with Active Directory (AD) entries and rules to easily import existing infrastructure from your location's network. It not only conveniently replicates the work already done by your IT team, but also utilizes unused data entry fields in those records for better security. This documentation explains how to configure INFINIAS 2.3 or newer to allow a Microsoft Active Directory environment to manage the INFINIAS cardholders.

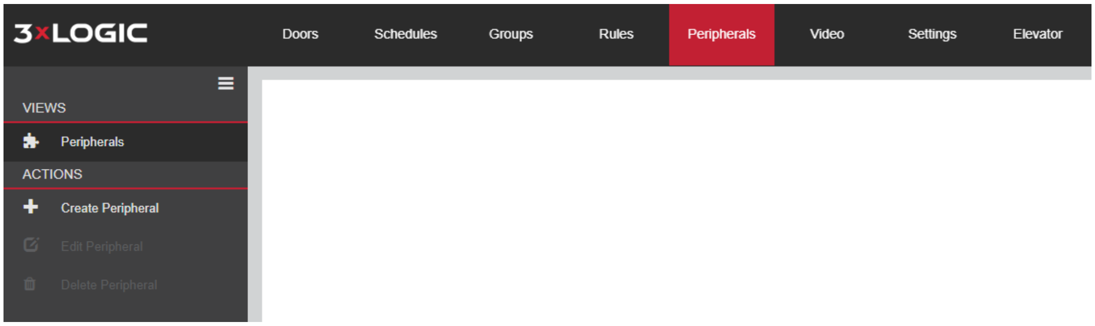
Note: Active Directory integration is only available for On Premises installations with INFINIAS Professional or Corporate licenses.

15.1 Access Control Configuration

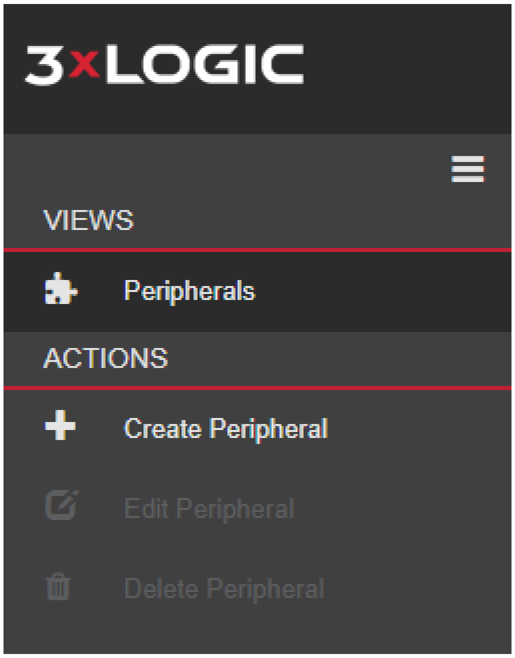
INFINIAS needs to be made aware of your Active Directory server information. This task is accomplished by creating an INFINIAS Peripheral, then referencing that Peripheral when you create one or more Rules designed to utilize that Peripheral.

15.1.1 Create a Peripheral

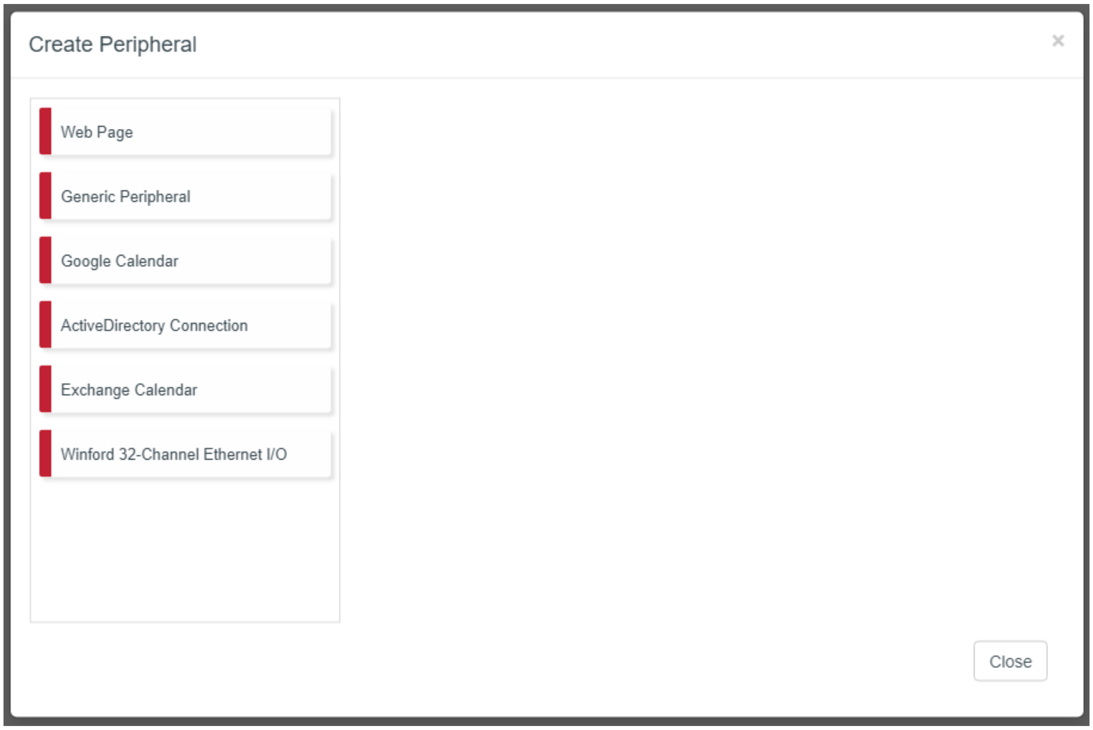
Login to INFINIAS and proceed to the **Peripherals** page.



Select **Create Peripheral** in the left side menu under *Actions*.

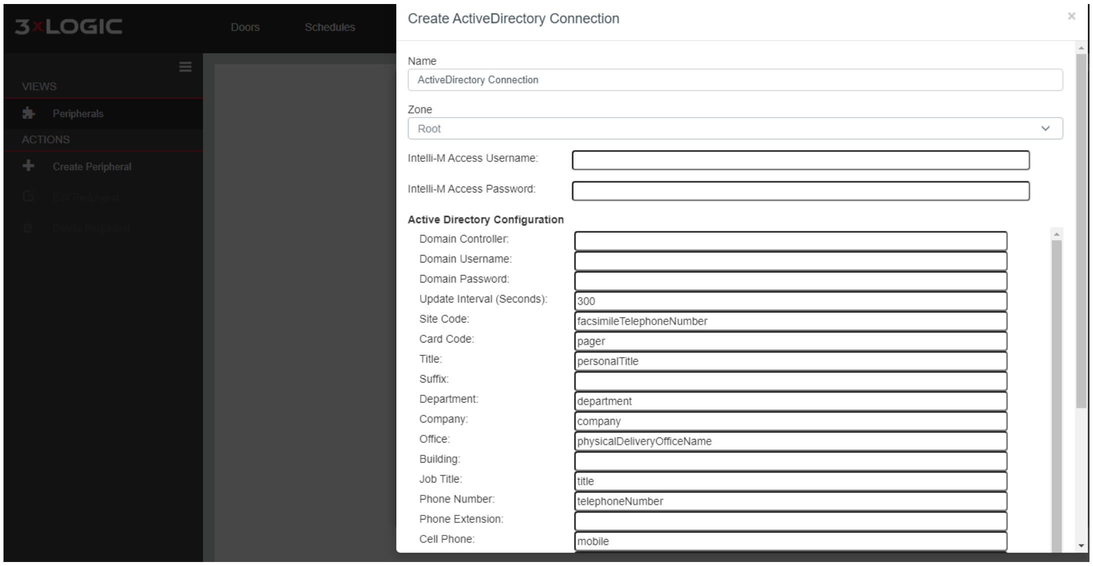


This generates the **Create Peripheral** options menu.



Choose the **ActiveDirectory Connection** option in the menu for the configuration dialog to appear.

Choose a *Name*, a *Zone*, and provide the INFINIAS login credentials, then proceed to the configuration elements.



Create ActiveDirectory Connection

Name: ActiveDirectory Connection

Zone: Root

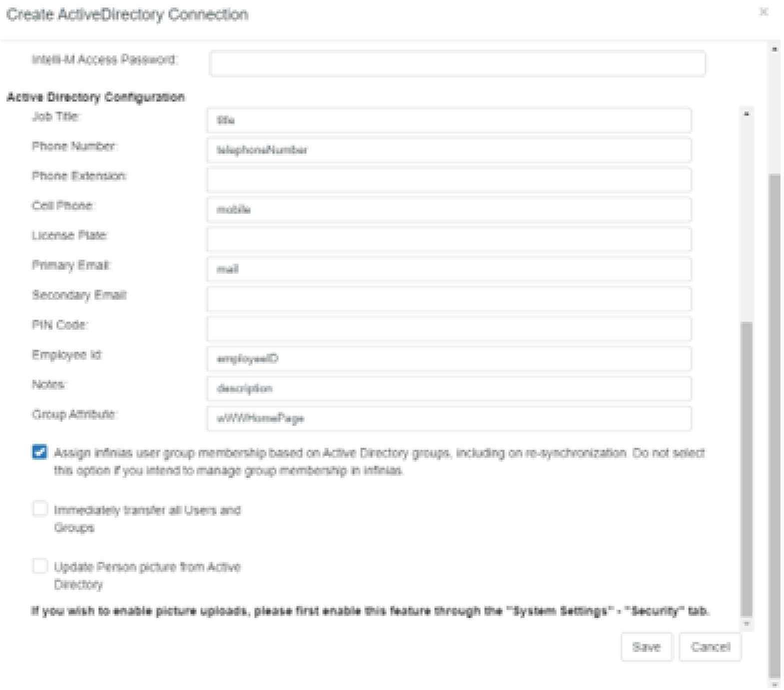
Intelli-M Access Username:

Intelli-M Access Password:

Active Directory Configuration

Domain Controller:	
Domain Username:	
Domain Password:	
Update Interval (Seconds):	300
Site Code:	facsimileTelephoneNumber
Card Code:	pager
Title:	personalTitle
Suffix:	
Department:	department
Company:	company
Office:	physicalDeliveryOfficeName
Building:	
Job Title:	title
Phone Number:	telephoneNumber
Phone Extension:	
Cell Phone:	mobile

The purpose of these elements is to create a mapping between the fields that describe a *Person* in INFINIAS (the labels on the left side of the UI), and the Active Directory Attributes (the text fields on the right side of the UI).



Create ActiveDirectory Connection

Intelli-M Access Password:

Active Directory Configuration

Job Title: title

Phone Number: telephoneNumber

Phone Extension:

Cell Phone: mobile

License Plate:

Primary Email: mail

Secondary Email:

PIN Code:

Employee Id: employeeID

Notes: description

Group Attribute: wWWHomePage

☑ Assign infinias user group membership based on Active Directory groups, including on re-synchronization. Do not select this option if you intend to manage group membership in infinias.

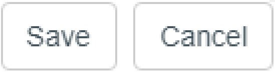
☐ Immediately transfer all Users and Groups

☐ Update Person picture from Active Directory

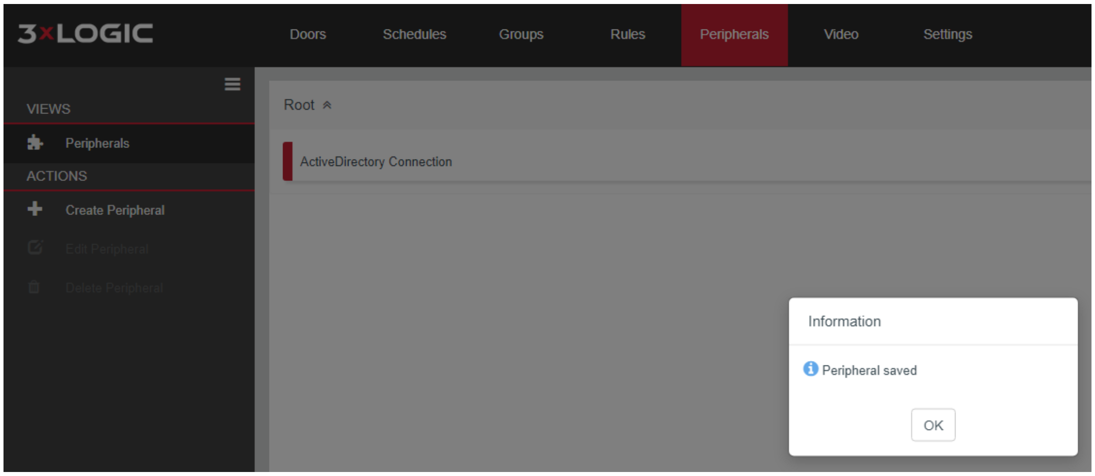
If you wish to enable picture uploads, please first enable this feature through the "System Settings" - "Security" tab.

By mapping an Active Directory Attribute, anything typed into that text field in Active Directory will show up in the corresponding INFINIAS field for that *Person*.

Select **Save** to submit the new Active Directory Connection (or Cancel to discard all entries).



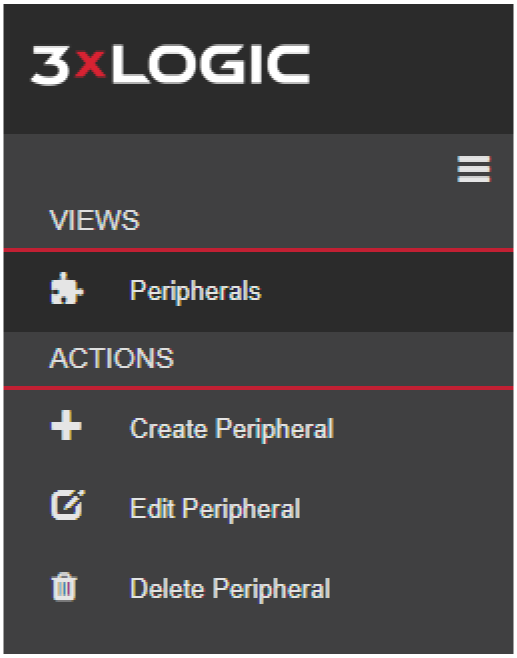
An *Information* dialog window confirms the successful creation. Click **OK** to dismiss the message.



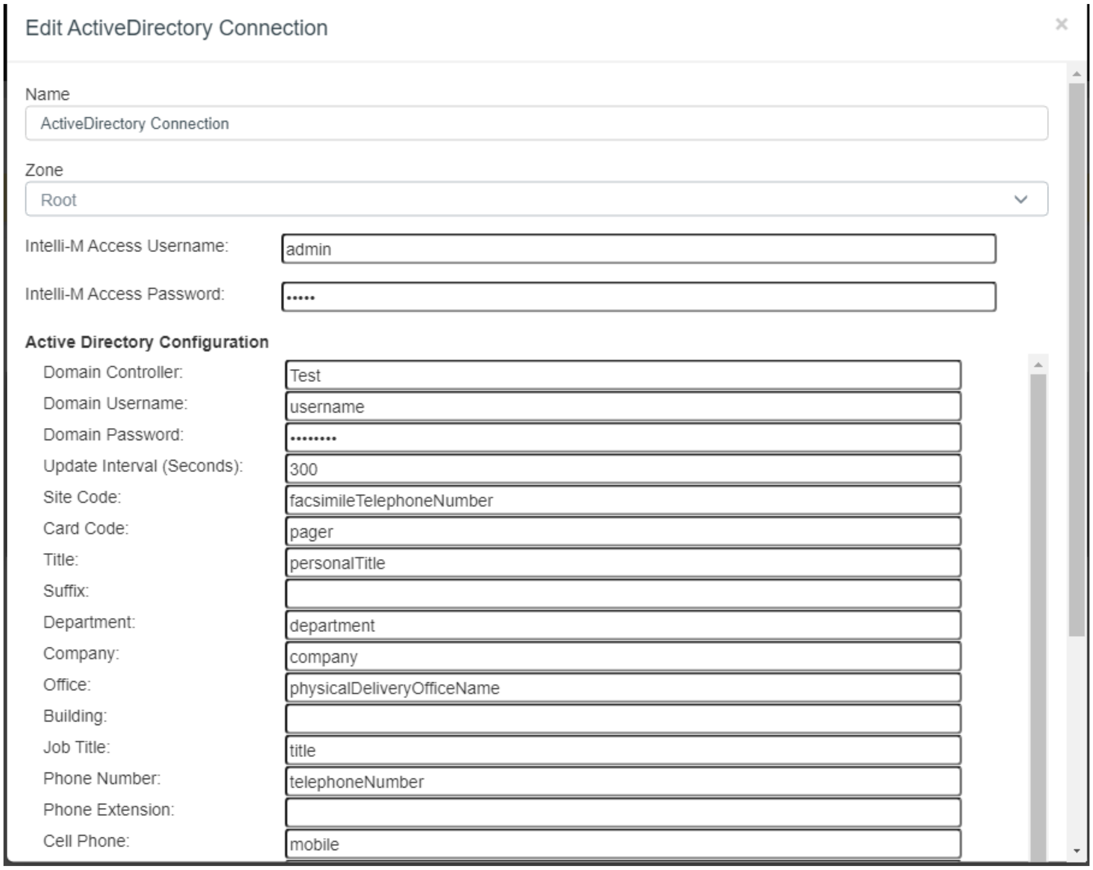
Information

Peripheral saved

The **Edit Peripheral** option becomes available under the Actions side menu.



The *Edit* menu brings up the same entry fields for any revision(s).



Name: ActiveDirectory Connection

Zone: Root

Intelli-M Access Username: admin

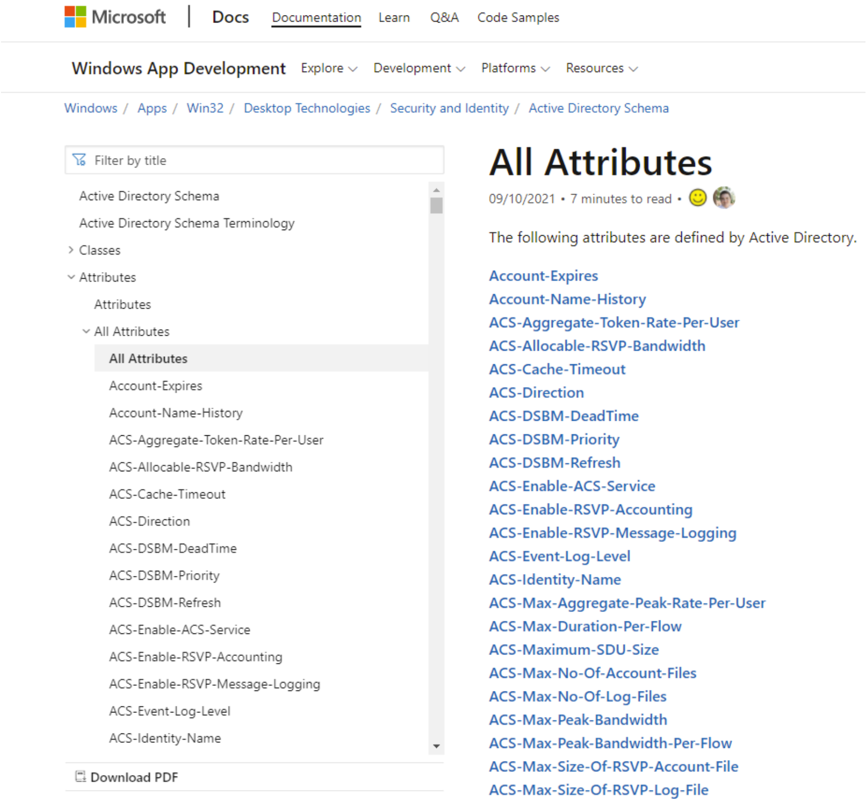
Intelli-M Access Password: •••••

Active Directory Configuration

Domain Controller:	Test
Domain Username:	username
Domain Password:	••••••••
Update Interval (Seconds):	300
Site Code:	facsimileTelephoneNumber
Card Code:	pager
Title:	personalTitle
Suffix:	
Department:	department
Company:	company
Office:	physicalDeliveryOfficeName
Building:	
Job Title:	title
Phone Number:	telephoneNumber
Phone Extension:	
Cell Phone:	mobile

15.1.2 Attributes

The Active Directory Attribute names must be spelled exactly and are case-sensitive. The names you must enter into the text fields are rarely visible in Active Directory itself. You can find the actual names you need to enter by going to websites such as: http://msdn.microsoft.com/en-us/library/ms675090(v=vs.85).aspx.



All Attributes

09/10/2021 • 7 minutes to read •

The following attributes are defined by Active Directory.

Account-Expires
Account-Name-History
ACS-Aggregate-Token-Rate-Per-User
ACS-Allocable-RSVP-Bandwidth
ACS-Cache-Timeout
ACS-Direction
ACS-DSBM-DeadTime
ACS-DSBM-Priority
ACS-DSBM-Refresh
ACS-Enable-ACS-Service
ACS-Enable-RSVP-Accounting
ACS-Enable-RSVP-Message-Logging
ACS-Event-Log-Level
ACS-Identity-Name
ACS-Max-Aggregate-Peak-Rate-Per-User
ACS-Max-Duration-Per-Flow
ACS-Maximum-SDU-Size
ACS-Max-No-Of-Account-Files
ACS-Max-No-Of-Log-Files
ACS-Max-Peak-Bandwidth
ACS-Max-Peak-Bandwidth-Per-Flow
ACS-Max-Size-Of-RSVP-Account-File
ACS-Max-Size-Of-RSVP-Log-File

The only Active Directory Users that will be transferred to INFINIAS are Users who have a Site Code and Card Code field mapping. Because Active Directory has no concept of Site, Card Code, or PIN Code, you must map a currently unused object in Active Directory to these fields.

The default value for Site Code, facsimilteTelephoneNumber, was chosen because it is rare in today's world for an individual to have his own fax machine telephone number. The default value for Card Code, pager, was chosen for the same reasons. There is no default mapping supplied for the PIN Code.

Note:If any of these values are being used in your Active Directory environment, then please provide a different unused Attribute.

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.

Group Attribute Specifics

The Group Attribute tells the system to pull all users in that defined group. For example, if an administrator put a group of personnel under “INFINIAS” and put that same text in the form field for the Group Attribute, then all of those users would receive those attribute updates.

Beneath the final Parameter Mapping form field, Group Attribute, there are checkboxes for global actions based on the Active Directory infrastructure already in place for the network.

1. The top option not only pulls in the personnel from an Active Directory defined group, but also recreates that group within INFINIAS for management of the details on the software side.
2. The middle option prioritizes a sync between the systems for the very next time that the Active Directory detects the change.
3. The bottom option simply imports the personnel photos (if applicable) into INFINIAS.
    a. If photos will be syncing this option will need to be checked in System Settings.

Unlike other plugins, the behavior of the Active Directory Peripheral is fixed; it updates INFINIAS whenever a corresponding change is made in Active Directory.

15.1.3 Field Entries

- *Domain*: Enter the Exchange email address portion that's on the right of the '@' symbol.
- *Update Interval*: Specifies the number of seconds to wait between checking for updates.
- *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 desired Active Directory Attribute to map to the User's job title. In INFINIAS Access, the Job Title is referred to as the Position, the default Attribute is title.
- *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.
- *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 INFINIAS Access. This is highly recommended when starting for the very first time. In a large system, this may take several hours.

15.1.4 No Rules

Unlike other plugins, the behavior of the Active Directory Peripheral is fixed; it updates INFINIAS whenever a corresponding change is made in Active Directory.

16 Microsoft Calendar Integration

The next two sections feature the contents of the Exchange Server Integration Guide.

INFINIAS integrates with Microsoft Exchange to allow Outlook Meetings to create exception schedules for doors controlled by INFINIAS. This form of ad-hoc scheduling allows you to schedule a door to unlock at meeting start and re-lock at meeting end, helping an organization to control door access for events that do not occur on a predictable schedule.

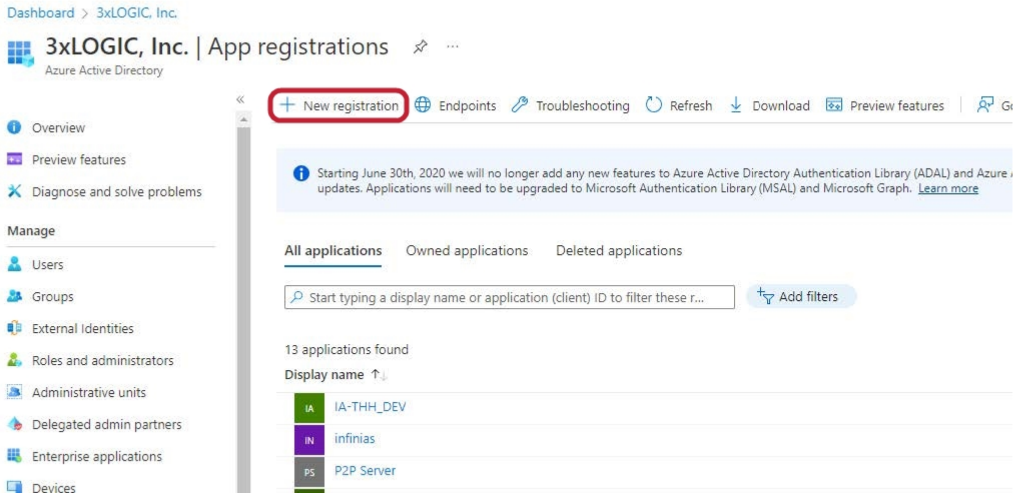
17 MS Exchange O365 Calendar Setup

As of October 1, 2022, Microsoft (MS) discontinued Basic authentication as planned for Outlook, Exchange Web Services (EWS) and several other products. The MS Outlook peripheral that INFINIAS uses to communicate with EWS was disabled as a result. To restore functionality, we implemented OAuth authentication in our software. However, for this to work, each user of this peripheral needs to create an Azure Active Directory application and grant it certain rights.

Note: Admin rights are required to successfully create the application.

17.1 Azure Active Directory Instructions

1. Select the **App Registrations** option on the tab to begin the process.
2. Select **New Registration** from the top menu.

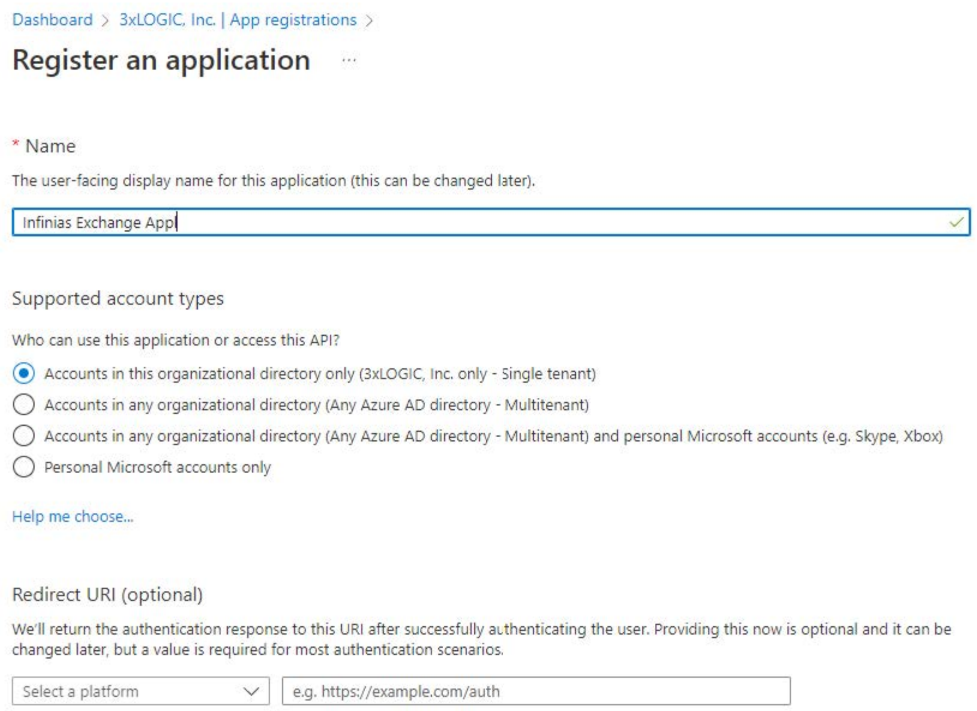


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

13 applications found

Figure 1-243: New registration

3. Name and select the supported account types. It does not appear to matter if it is a single or multi tenant app. Leave the *Redirect URI* option blank and save.



Dashboard > 3xLOGIC, Inc. | App registrations >

Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

Infinias Exchange Appl

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (3xLOGIC, Inc. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

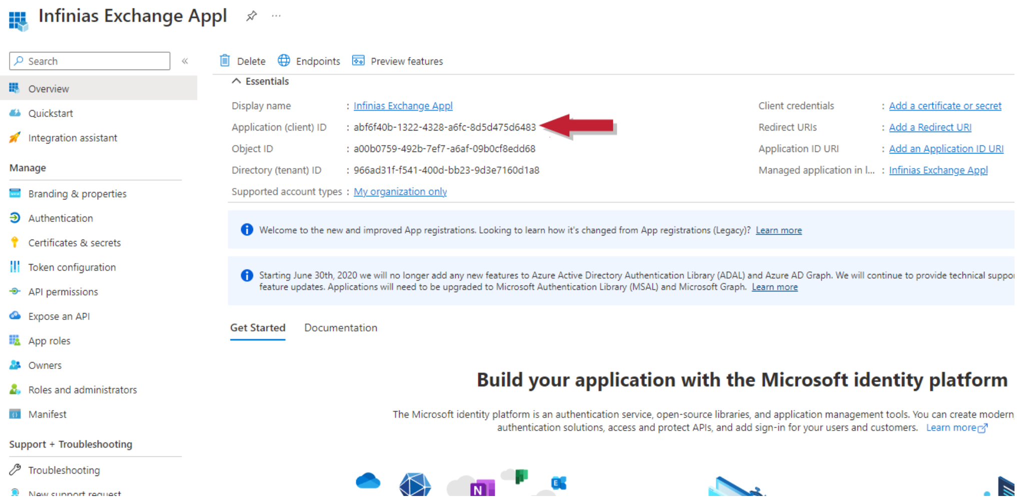
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Figure 1-244: Register an Application Page

4. On the **Overview** page, select the Application (client) ID value. This will be needed later to be entered in INFINIAS along with your tenant ID.



Essentials

Display name	: Infinias Exchange Appl	Client credentials	: Add a certificate or secret
Application (client) ID	: abf6f40b-1322-4328-a6fc-8d5d475d6483	Redirect URIs	: Add a Redirect URI
Object ID	: a00b0759-492b-7ef7-a6af-09b0cf8edd68	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 966ad31f-f541-400d-bb23-9d3e7160d1a8	Managed application in l...	: Infinias Exchange Appl
Supported account types	: My organization only		

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

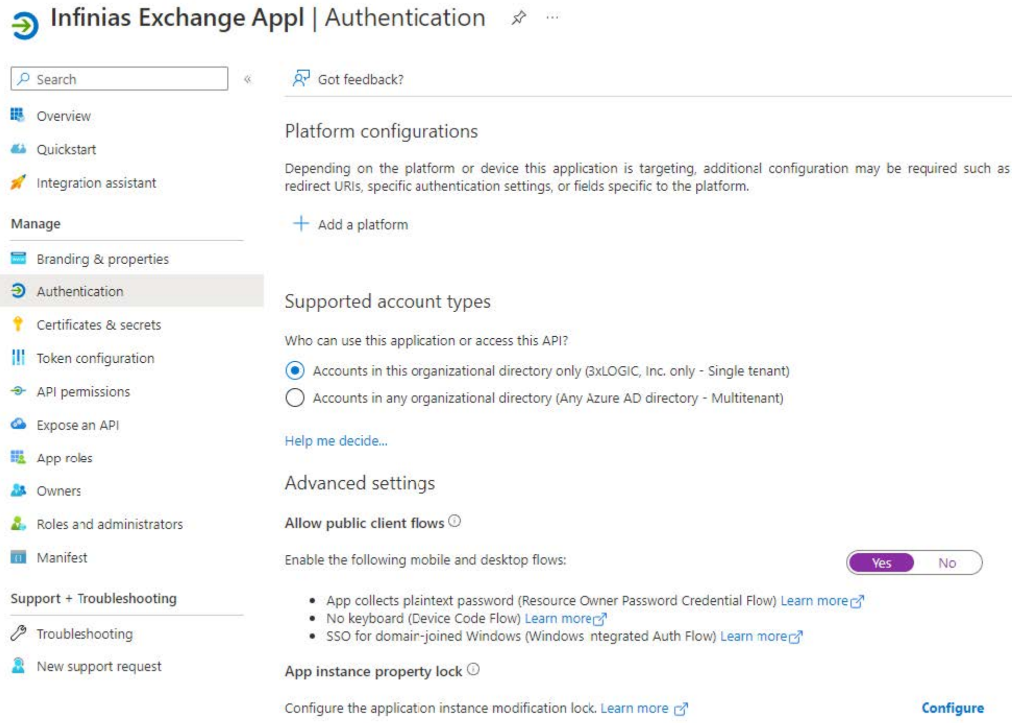
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical suppo feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Figure 1-245: Application (client) ID value

5. Navigate to the **Authentication** page (it does not matter if it is single or multi tenant).



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (3xLOGIC, Inc. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

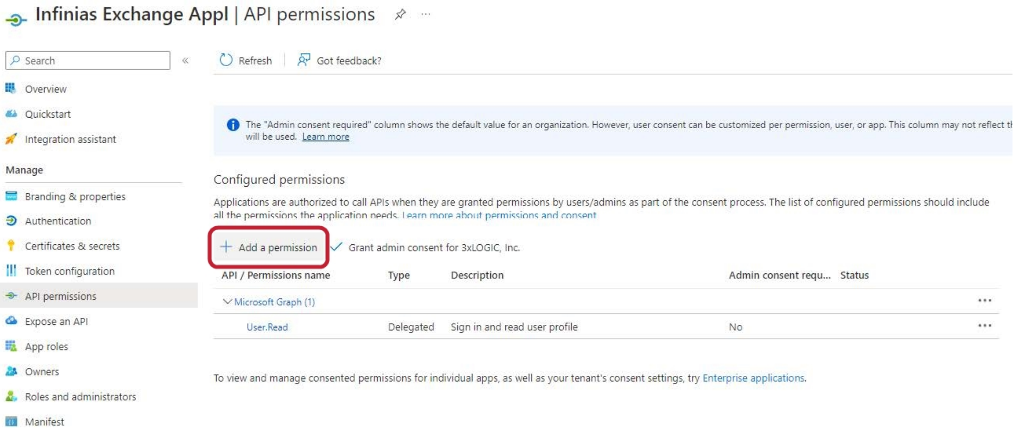
- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

App instance property lock

Configure the application instance modification lock. Learn more

Figure 1-246: Authentication Page

6. Under **Advanced Settings** turn the value for *Allow public client flows* to Yes. This is very important and will prevent the Microsoft Exchange peripheral from being able to connect if it is not turned on. Save your changes before proceeding.
7. Navigate to the **API Permissions** page and click *Add a permission*. We are looking to add the Microsoft Graph *EWS.AccessAsUser.All* permission as a delegate.



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect th will be used. Learn more

Configured permissions

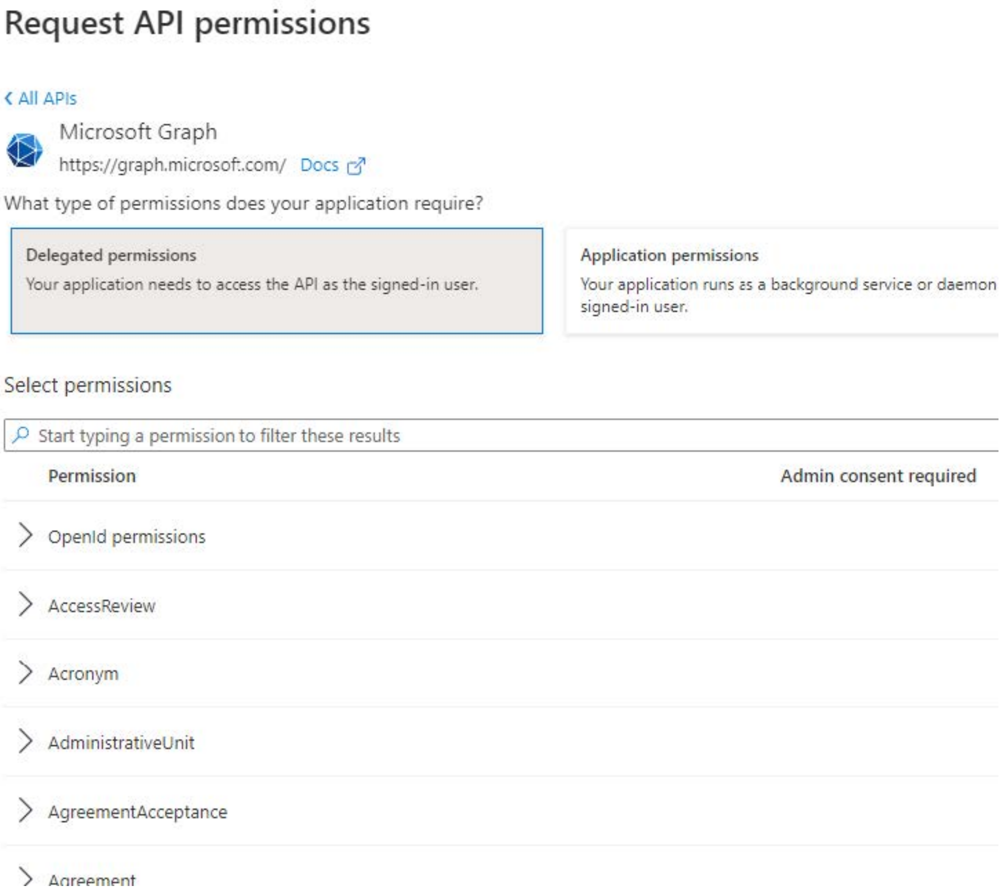
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Figure 1-247: API Permissions Page

8. Select **Microsoft Graph** (should be near the top of the page) and click on *Delegated Permissions*.



Request API permissions

‹ All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon
signed-in user.

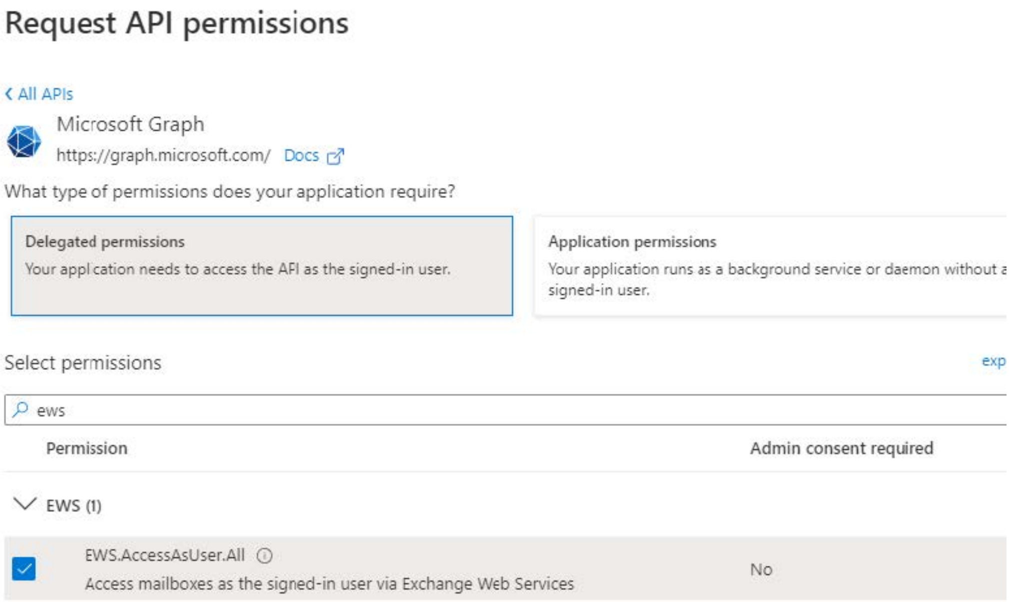
Select permissions

Start typing a permission to filter these results

Permission	Admin consent required
OpenId permissions	
AccessReview	
Acronym	
AdministrativeUnit	
AgreementAcceptance	
Agreement	

Figure 1-248: Microsoft Graph - Delegated Permissions

9. Enter "EWS" in the search bar and check the **EWS.AccessAsUser.All** option. *Save* your changes before proceeding.



Request API permissions

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

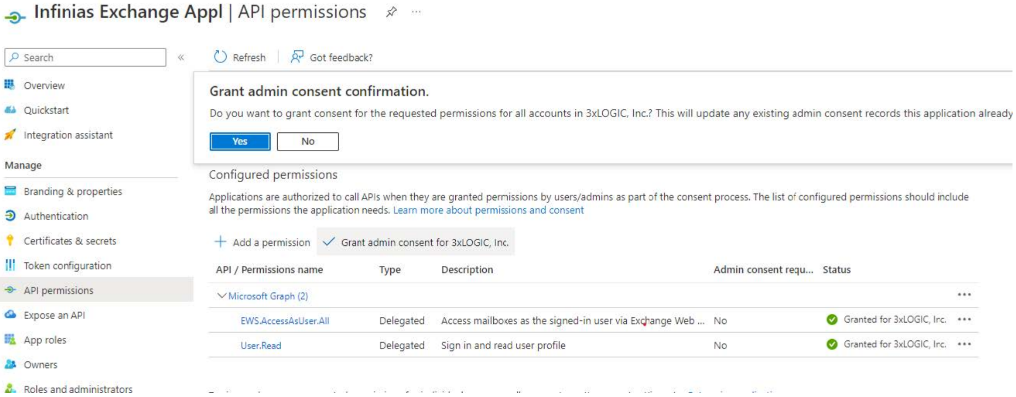
Select permissions

ews

Permission	Admin consent required
EWS (1)	
☑ EWS.AccessAsUser.All Access mailboxes as the signed-in user via Exchange Web Services	No

Figure 1-249: EWS Keyword Search

10. Back on the **API Permissions** page, click on *Yes* for Grant admin consent confirmation for (your organization), then confirm.



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in 3xLOGIC, Inc.? This will update any existing admin consent records this application already

Yes No

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange Web ...	No	✓ Granted for 3xLOGIC, Inc.
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for 3xLOGIC, Inc.

Figure 1-250: Grant Admin Consent Confirmation

   a. Without this step, the Microsoft Exchange peripheral will receive a 401 access denied error when it attempts to pull calendar data

11. After completing the previous steps, the application should now be ready. Please wait a few minutes for all the back end processing to complete for Azure Active Directory.

12. Take note of the application ID and tenant ID which will be needed when creating the peripheral in INFINIAS.

   a. If you are unfamiliar, the tenant ID should look something like "name.onmicrosoft.com" in general.

17.2 Create a Meeting for O365

This step assumes that you have completed the Azure Active Directory steps outlined above.

Create a meeting in your O365 Outlook calendar and set the location as the name of the door you want to control with this integration.

Note: The meeting will need to be set for at least 15 minutes in the future or less if your polling time is set lower in the peripheral configuration.

17.3 INFINIAS O365 Configuration

The final configuration for Microsoft Exchange O365 integration takes place within INFINIAS. Please note that these steps mirror the legacy instructions but with noteworthy differences.

17.3.1 Create a Peripheral for O365

With Calendar Permissions set, you may proceed to create an INFINIAS Peripheral.

1. 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.

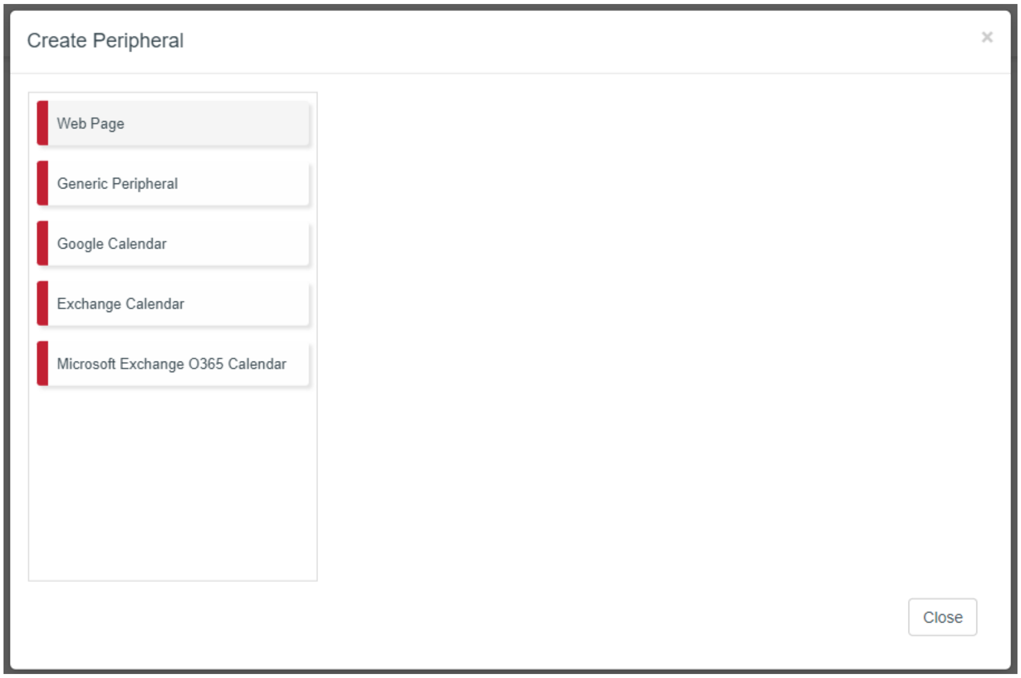
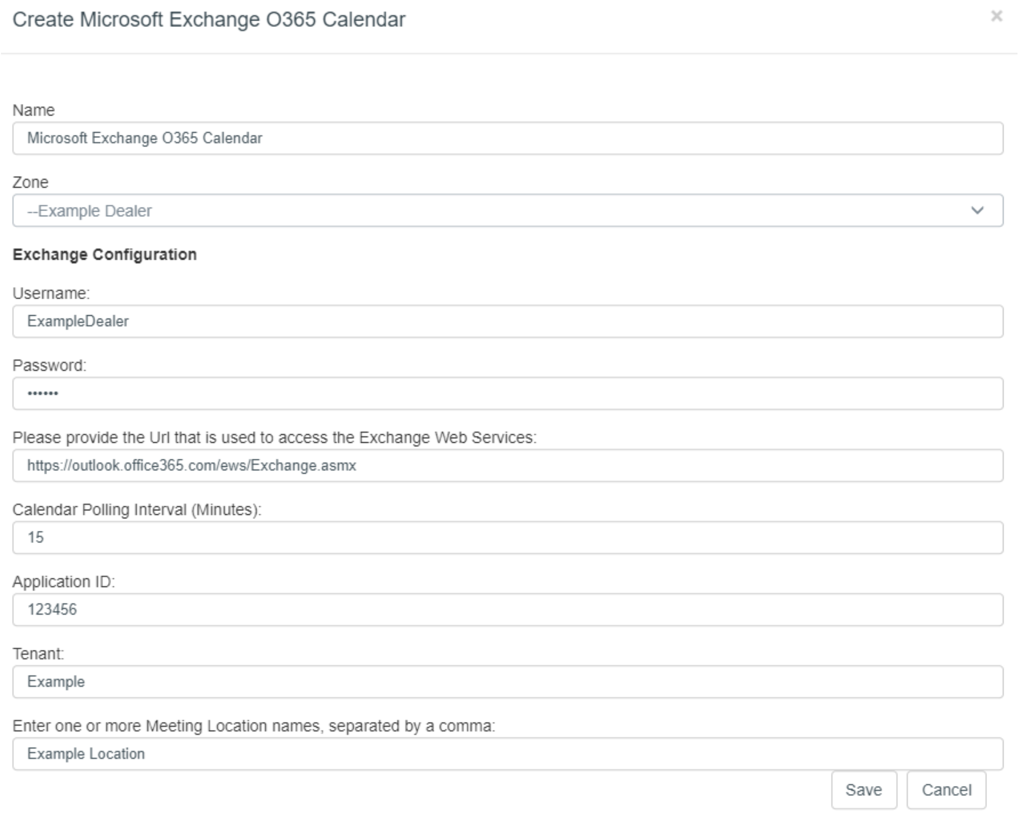


Figure 1-251: New Peripheral Window

2. Select the *Microsoft Exchange O365 Calendar* option to start creating the Peripheral based on this plugin. A Create Microsoft Exchange O365 Calendar popup dialog appears.



Create Microsoft Exchange O365 Calendar

Name: Microsoft Exchange O365 Calendar

Zone: --Example Dealer

Exchange Configuration

Username: ExampleDealer

Password: ••••••

Please provide the Url that is used to access the Exchange Web Services: https://outlook.office365.com/ews/Exchange.asmx

Calendar Polling Interval (Minutes): 15

Application ID: 123456

Tenant: Example

Enter one or more Meeting Location names, separated by a comma: Example Location

Figure 1-252: New O365 Calendar Configuration

a. Configure the Zone - Select "Root" for Professional and Corporate license users or the *customer name* for INFINIAS CLOUD users.

b. Configure the Username - Provide the username of the O365 Exchange calendar account you will be using to create the meetings INFINIAS will monitor.

c. Configure the Password - Provide the password for the user account associated with the *Username*.

d. Configure the WebMail URL - Replace the mail.mycompany.com portion of the sample *WebMail URL* with your corporate webmail name.

e. Set the Calendar Polling Interval (Minutes) - This field is user-definable and will poll the Exchange Server for all calendar updates. If you book a meeting, make sure that the meeting reminder (the first event that hits our database) is beyond the polling interval.

f. Configure the Application ID - Enter the ID as shown in step 4 of the Azure Active Directory instructions above.

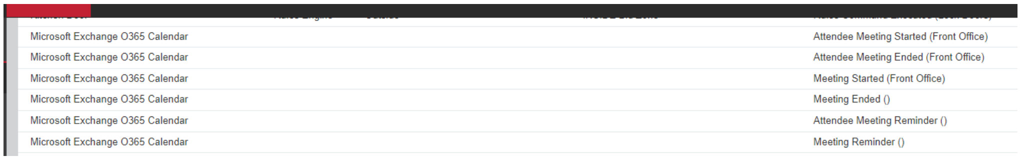
g. Configure the Tenant - Enter the Tenant ID specified for your organization via Azure AD in the format of the example shown in Figure directly above.

h. Configure the Meeting Location Names - Enter the name of the door(s) you want to control with Meeting invites.

3. Click *Save* to proceed.

Note: You need to create a calendar meeting before the peripheral will Save.

4. The Exchange plugin will send INFINIAS six test Events: one for Meeting Reminder, one for Attendee Meeting Reminder, one for Meeting Started, one for Attendee Meeting Started, one for Meeting Ended, and one for Attendee Meeting Ended. This allows INFINIAS to be able to display this information on the Rules page for creating Rules.



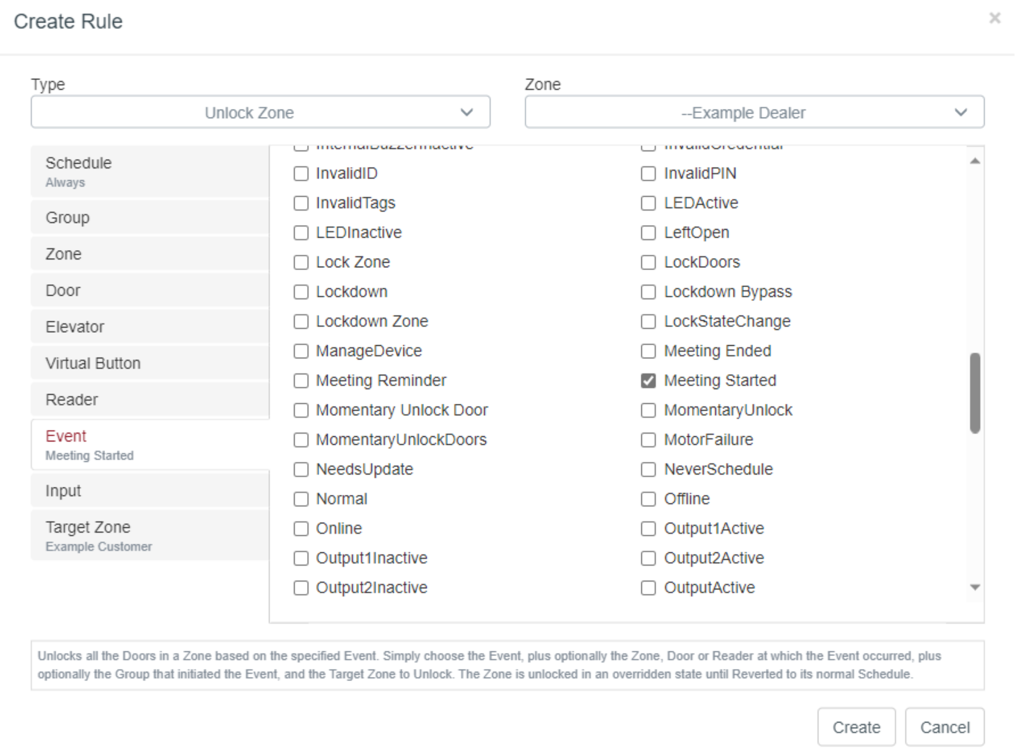
Microsoft Exchange O365 Calendar	Attendee Meeting Started (Front Office)
Microsoft Exchange O365 Calendar	Attendee Meeting Ended (Front Office)
Microsoft Exchange O365 Calendar	Meeting Started (Front Office)
Microsoft Exchange O365 Calendar	Meeting Ended ()
Microsoft Exchange O365 Calendar	Attendee Meeting Reminder ()
Microsoft Exchange O365 Calendar	Meeting Reminder ()

Figure 1-253: O365 Test Events

17.3.2 Unlock Zone Rule for O365

Unlock the zone of the door where the meeting location is set by creating an Unlock Zone Rule.

1. From the INFINIAS interface, click the *Configuration* link and click on the *Rules* tab.
2. When the Rules page appears, click the *Create Rule* Action from the Actions menu. A popup dialog will appear and will show the Access Privilege Rule by default. Select *Unlock Zone* from the *Rules Type* drop down box. The popup dialog will populate with fields for supplying information to configure the unlock zone rule.



Create Rule

Type: Unlock Zone

Zone: --Example Dealer

Schedule: Always

Event: Meeting Started

Target Zone: Example Customer

□ InvalidID
□ InvalidPIN
□ InvalidTags
□ LEDActive
□ LEDInactive
□ LeftOpen
□ Lock Zone
□ LockDoors
□ Lockdown
□ Lockdown Bypass
□ Lockdown Zone
□ LockStateChange
□ ManageDevice
□ Meeting Ended
□ Meeting Reminder
☑ Meeting Started
□ Momentary Unlock Door
□ MomentaryUnlock
□ MomentaryUnlockDoors
□ MotorFailure
□ NeedsUpdate
□ NeverSchedule
□ Normal
□ Offline
□ Online
□ Output1Active
□ Output1Inactive
□ Output2Active
□ Output2Inactive
□ OutputActive

Unlocks all the Doors in a Zone based on the specified Event. Simply choose the Event, plus optionally the Zone, Door or Reader at which the Event occurred, plus optionally the Group that initiated the Event, and the Target Zone to Unlock. The Zone is unlocked in an overridden state until Reverted to its normal Schedule.

Figure 1-254: Unlock Zone

a. Configure the *Schedule* - Choose a Schedule that defines the time range you want to allow this Rule to run (usually the Always Schedule).

b. Configure the *Event* - Select Meeting Reminder or Meeting Started Event from the displayed list.

c. Configure the Input (Optional) - Select the input Microsoft Exchange O365 Calendar "Door Name" option.

d. Configure the *Target Zone* - Choose a Zone to unlock, which contains the Door that will be controlled with this integration.

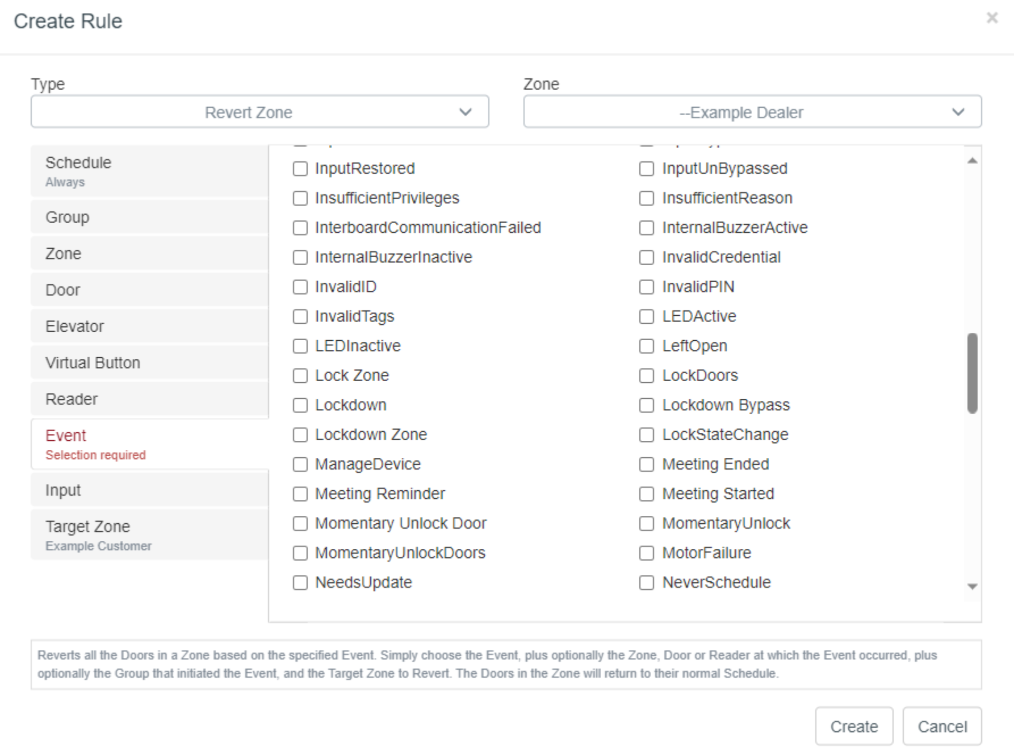
Note: The rule executes for all doors in the specified Target Zone. To only effect one door, place that single door in its own zone.

3. Click the **Create** button to create the Rule

17.3.3 Revert Zone Rule for O365

You can re-lock the zone of a door by creating a Revert Zone Rule. This reverts the door to its normal lock schedule (which is assumed to be locked).

1. From the INFINIAS interface, click the *Configuration* link and click on the *Rules* tab.
2. When the Rules page appears, click the *Create Rule* Action from the Actions menu. A popup dialog will appear and will show the Access Privilege Rule by default. Select *Revert Zone* from the *Rules Type* drop down box. The popup dialog will populate with fields for supplying information to configure the Revert Zone rule.



Create Rule

Type: Revert Zone

Zone: --Example Dealer

Schedule: Always

Group

Zone

Door

Elevator

Virtual Button

Reader

Event: Selection required

Input

Target Zone: Example Customer

□ InputRestored
□ InsufficientPrivileges
□ InterboardCommunicationFailed
□ InternalBuzzerInactive
□ InvalidID
□ InvalidTags
□ LEDInactive
□ Lock Zone
□ Lockdown
□ Lockdown Zone
□ ManageDevice
□ Meeting Reminder
□ Momentary Unlock Door
□ MomentaryUnlockDoors
□ NeedsUpdate

□ InputUnBypassed
□ InsufficientReason
□ InternalBuzzerActive
□ InvalidCredential
□ InvalidPIN
□ LEDActive
□ LeftOpen
□ LockDoors
□ Lockdown Bypass
□ LockStateChange
□ Meeting Ended
□ Meeting Started
□ MomentaryUnlock
□ MotorFailure
□ NeverSchedule

Reverts all the Doors in a Zone based on the specified Event. Simply choose the Event, plus optionally the Zone, Door or Reader at which the Event occurred, plus optionally the Group that initiated the Event, and the Target Zone to Revert. The Doors in the Zone will return to their normal Schedule.

Figure 1-255: Revert Zone

a. Configure the *Schedule* - Choose a Schedule that defines the time range you want to allow this Rule to run (usually the Always Schedule).

b. Configure the *Event* - Select Meeting Ended from the list.

c. Configure the Input (Optional) - Select the input Microsoft Exchange O365 Calendar "Door Name" option.

d. Configure the *Target Zone* - Choose the same Zone that you specified in the Unlock Zone Rule.

3. Click the **Create** button to create the Rule

18 MS Outlook Legacy Instructions

INFINIAS is designed to act as a way for Microsoft Exchange to send Meeting Reminder, Meeting Started, and Meeting Ended Events to INFINIAS for specified Exchange Room Mailboxes, and for all relevant Meeting Attendees. The integration plugin accomplishes this task by monitoring the Calendar of each specified Exchange Room Mailbox.

Whenever a Meeting is scheduled in the Calendar of a Room Mailbox being monitored, the INFINIAS Exchange integration will send Events to INFINIAS informing it of these Calendar Events. A **Meeting Started** or **Attendee Meeting Started** Event will be sent to INFINIAS the moment that a meeting is scheduled to begin, and **Meeting Ended** or **Attendee Meeting Ended** Events will be sent to INFINIAS the moment that a meeting is scheduled to end. In addition, the plugin will also send **Meeting Reminder** or **Attendee Meeting Reminder** Events to INFINIAS at this time as well. These Events appear within INFINIAS no differently than any other Event and can therefore be configured for use on the Rules page like any other Event.

18.1 Ad-Hoc Door Lock Schedule

The most common usage for these Events is to unlock and re-lock meeting room or public-access doors. For example, INFINIAS can be programmed to unlock a door when Exchange sends the Meeting Reminder or Meeting Start Events and programmed to re-lock the door (or revert the door schedule) when the Meeting Ended Event occurs. This is useful for doors requiring public access, such as gymnasiums, public conference rooms, and so on. Once you have configured the unlock/revert Rules in INFINIAS, all you have to do is create Meetings or Appointments in Outlook to control the meeting room door.

18.2 Integration Checklist

You must provide the following information in Microsoft Exchange to the INFINIAS Exchange plugin when you configure it. Please be prepared to have the following information available:

- **Internet Domain** - You must know the internet domain name that Exchange uses for creating its email addresses, i.e. the part of your Exchange email address that's on the right side of the '@' character. If your Exchange Server allows using the full email address as the username, you can leave this field blank.
- **Exchange User Account** - You must know the chosen Exchange User account (and its password) that you specified for Calendar permissions in the Exchange Management Console. If you specified the Domain name in the Domain field, then provide the user account name. If you leave the Domain field blank, provide the entire email address.
- **WebMail URL** - INFINIAS logs into Exchange via Exchange Web Services (formerly known as WebDAV) to monitor the requested Calendars, using the ordinary Mailbox account you specified. If you don't know your Exchange Web Services URL, consult the IT Administrator.
- **Room Mailbox Email Addresses** - You must know the email address of each Room Mailbox you gave Full Access Permissions to the ordinary Mailbox account in the Exchange Management Console. These email addresses will be used by the INFINIAS plugin to know which Room Mailbox accounts to monitor.

Once you have this information, you are ready to install and configure the Exchange integration.

18.3 Calendar Permissions

Configuration of the Exchange Calendar is performed by creating an INFINIAS Peripheral, then referencing that Peripheral when you create one or more Rules designed to utilize that Peripheral. Integrating Microsoft Exchange with INFINIAS means you must configure Exchange to allow an ordinary Exchange Mailbox account to have Full Access Permission rights to each Room Mailbox account who's Calendars you wish to monitor. While you can use any Exchange Mailbox account for this purpose, we recommend that you create a Mailbox account specifically for monitoring Calendars.

Note: Administrator Mailbox accounts do not automatically have Full Access Permission rights to anyone's Calendar. You must specifically assign these rights.

To provide Full Access Permission rights which will allow the Mailbox to monitor the Room Mailbox Calendars, open the Microsoft Exchange Management Console and complete the following:

1. In the tree view on the left side of the console window, click the plus sign to open the **Microsoft Exchange On-Premises (...)** item.
2. Click the plus sign to open the **Recipient Configuration** item.
3. Select the **Mailbox** item to view all Exchange Mailboxes in the right-side view.
4. Right- click each Room Mailbox you wish to manage and select the **Manage Full Access Permission...** menu item.
5. Follow the wizard's instructions to add the chosen ordinary Mailbox account to the list of accounts that have full access permissions to this Room Mailbox.
6. Perform this same task for all Room Mailboxes that represent areas with doors being managed by INFINIAS.

18.4 Create a Peripheral

With Calendar Permissions set, you may proceed to create an INFINIAS Peripheral.

1. 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.

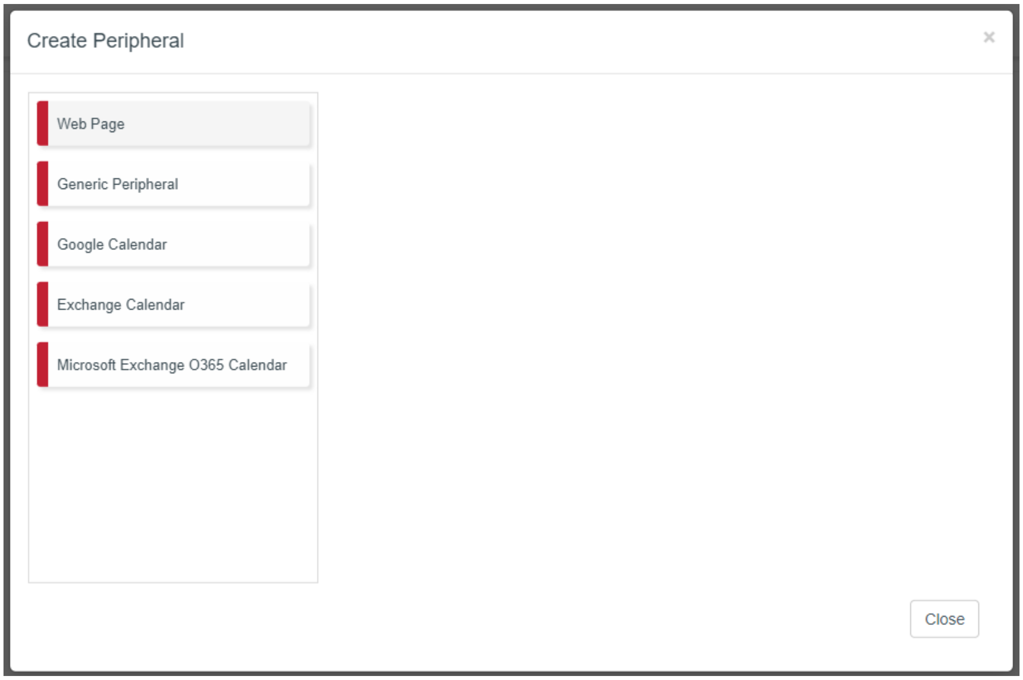
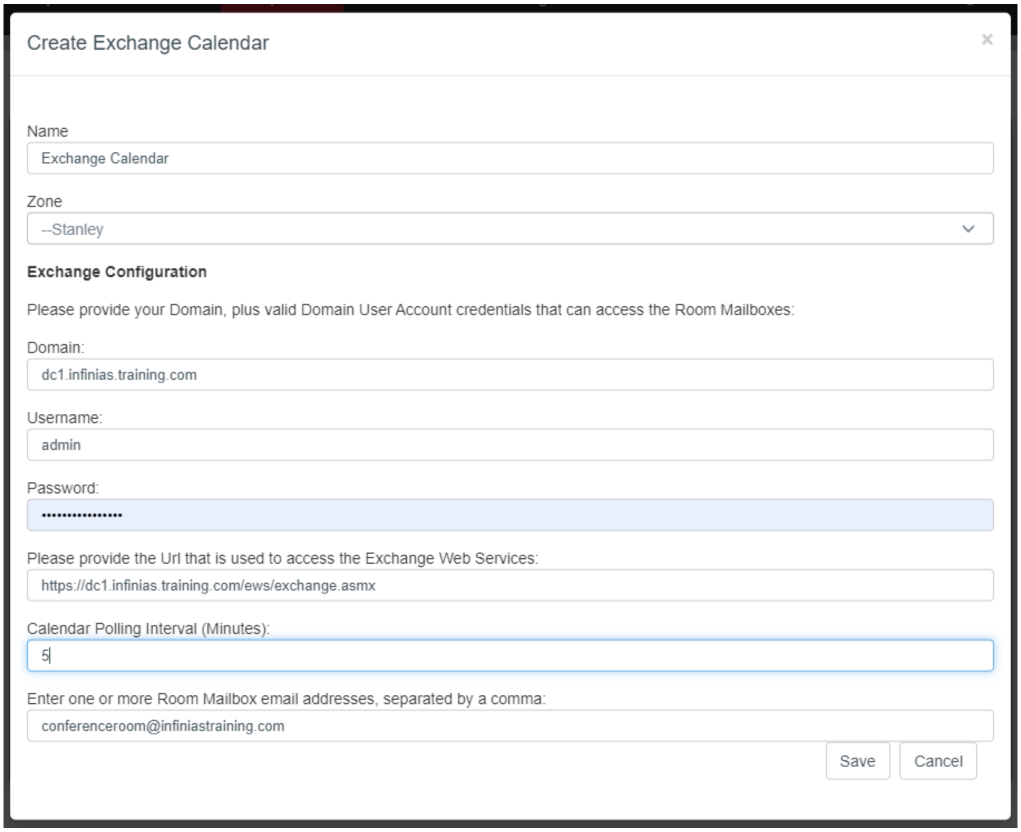


Figure 1-256: New Peripheral Window

2. Select the *Exchange Calendar* menu item to start creating the Peripheral based on this plugin, and a Create New Exchange Calendar popup dialog will appear.



Create Exchange Calendar

Name: Exchange Calendar

Zone: --Stanley

Exchange Configuration

Please provide your Domain, plus valid Domain User Account credentials that can access the Room Mailboxes:

Domain: dc1.infinias.training.com

Username: admin

Password: ••••••••••••••••

Please provide the Url that is used to access the Exchange Web Services: https://dc1.infinias.training.com/ews/exchange.asmx

Calendar Polling Interval (Minutes): 5

Enter one or more Room Mailbox email addresses, separated by a comma: conferenceroom@infiniastraining.com

Figure 1-257: New Calendar Configuration

a. Configure the Domain - Enter the part of your Exchange email address that's on the right side of the '@' character, or leave this field blank and enter the entire email address below.

b. Configure the Username - Provide the username of the ordinary Mailbox account you previously gave Full Access Permissions to the Room Mailboxes in Exchange Management Console. Enter just the username portion of the account, not its email address. If you left the Domain field blank, enter the entire email address.

c. Configure the Password - Provide the password for the user account associated with the *Username*.

d. Configure the WebMail URL - Replace the mail.mycompany.com portion of the sample *WebMail URL* with your corporate webmail name.

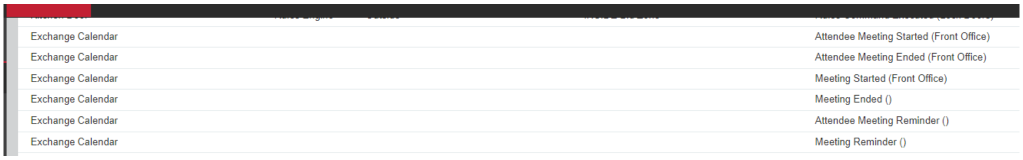
e. Set the Calendar Polling Interval (Minutes) - This field is user-definable and will poll the Exchange Server for all calendar updates. If you book a meeting, make sure that the meeting reminder (the first event that hits our database) is beyond the polling interval.

f. Configure the Room Mailboxes. For each Room Mailbox you have previously configured, enter the email address of each conference room, separating each email address with the comma (,) character.

3. Click *Save* to proceed.

Note: If one or more pieces of information were entered incorrectly on the Create Peripheral popup, or if there is some other connectivity issues like a firewall blocking the port, the previous configuration page will appear, giving you the ability to adjust the values you entered and try again.

4. For each Room Mailbox you specified, the Exchange plugin will send INFINIAS six test Events: one for Meeting Reminder, one for Attendee Meeting Reminder, one for Meeting Started, one for Attendee Meeting Started, one for Meeting Ended, and one for Attendee Meeting Ended. The purpose for these test Events is so INFINIAS will be informed of the Room Mailbox names and the Events they will generate. This in turn allows INFINIAS to be able to display this information on the Rules page for creating Rules.



Exchange Calendar	Attendee Meeting Started (Front Office)
Exchange Calendar	Attendee Meeting Ended (Front Office)
Exchange Calendar	Meeting Started (Front Office)
Exchange Calendar	Meeting Ended ()
Exchange Calendar	Attendee Meeting Reminder ()
Exchange Calendar	Meeting Reminder ()

Figure 1-258: Test Events

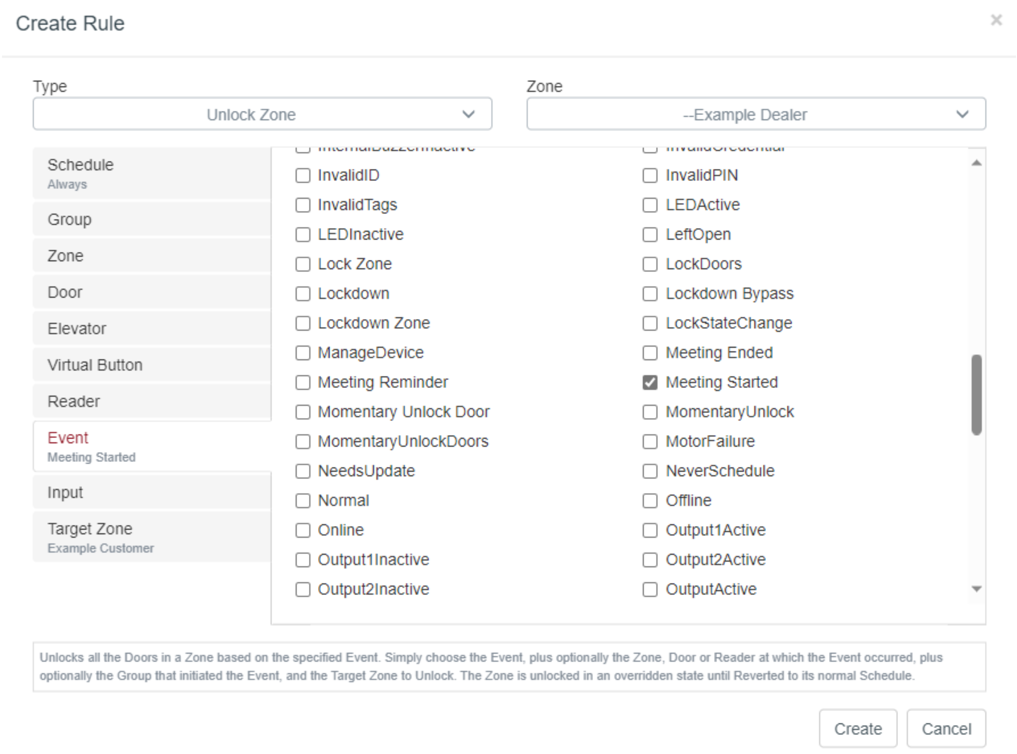
18.5 Create Rules

Now that you have created the Peripheral you can create Rules that act on Events that will be generated by the Exchange for meeting notifications.

18.5.1 Unlock Zone Rule

You can unlock the zone of a door associated with an Exchange Room Mailbox by creating an Unlock Zone Rule.

1. From the INFINIAS interface, click the *Configuration* link and click on the *Rules* tab.
2. When the Rules page appears, click the *Create Rule* Action from the Actions menu. A popup dialog will appear and will show the Access Privilege Rule by default. Select *Unlock Zone* from the *Rules Type* drop down box. The popup dialog will populate with fields for supplying information to configure the unlock zone rule.



Create Rule ×

Type: Unlock Zone

Zone: --Example Dealer

□ InvalidID	□ InvalidPIN
□ InvalidTags	□ LEDActive
□ LEDInactive	□ LeftOpen
□ Lock Zone	□ LockDoors
□ Lockdown	□ Lockdown Bypass
□ Lockdown Zone	□ LockStateChange
□ ManageDevice	□ Meeting Ended
□ Meeting Reminder	☑ Meeting Started
□ Momentary Unlock Door	□ MomentaryUnlock
□ MomentaryUnlockDoors	□ MotorFailure
□ NeedsUpdate	□ NeverSchedule
□ Normal	□ Offline
□ Online	□ Output1Active
□ Output1Inactive	□ Output2Active
□ Output2Inactive	□ OutputActive

Unlocks all the Doors in a Zone based on the specified Event. Simply choose the Event, plus optionally the Zone, Door or Reader at which the Event occurred, plus optionally the Group that initiated the Event, and the Target Zone to Unlock. The Zone is unlocked in an overridden state until Reverted to its normal Schedule.

Figure 1-259: Unlock Zone

a. Configure the *Schedule* - Choose a Schedule that defines the time range you want to allow this Rule to run (usually the Always Schedule).

b. Configure the *Event* - Select Meeting Reminder or Meeting Started Event from the displayed list.

c. Configure the *Target Zone* - Choose a Zone to unlock, which contains the Door that is physically securing the area represented by the Room Mailbox.

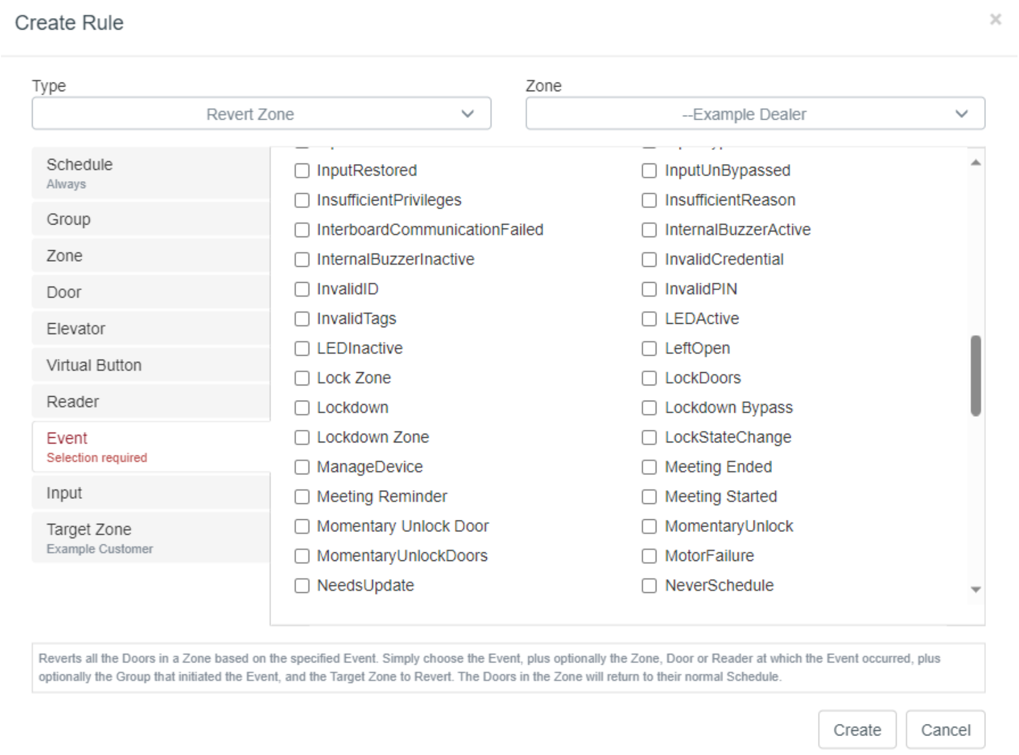
Note: The rule will execute for all doors in the specified Target Zone. If the intent is to only effect one door then the door will need to be put into its own zone.

3. Click the **Create** button to create the Rule

18.5.2 Revert Zone Rule

You can re-lock the zone of a door associated with an Exchange Room Mailbox by creating a Revert Zone Rule. This reverts the door to its normal lock schedule (which is assumed to be locked).

1. From the INFINIAS interface, click the *Configuration* link and click on the *Rules* tab.
2. When the Rules page appears, click the *Create Rule* Action from the Actions menu. A popup dialog will appear and will show the Access Privilege Rule by default. Select *Revert Zone* from the *Rules Type* drop down box. The popup dialog will populate with fields for supplying information to configure the Revert Zone rule.



Type: Revert Zone

Zone: --Example Dealer

□ InputRestored
□ InputUnBypassed
□ InsufficientPrivileges
□ InsufficientReason
□ InterboardCommunicationFailed
□ InternalBuzzerActive
□ InternalBuzzerInactive
□ InvalidCredential
□ InvalidID
□ InvalidPIN
□ InvalidTags
□ LEDActive
□ LEDInactive
□ LeftOpen
□ Lock Zone
□ LockDoors
□ Lockdown
□ Lockdown Bypass
□ Lockdown Zone
□ LockStateChange
□ ManageDevice
□ Meeting Ended
□ Meeting Reminder
□ Meeting Started
□ Momentary Unlock Door
□ MomentaryUnlock
□ MomentaryUnlockDoors
□ MotorFailure
□ NeedsUpdate
□ NeverSchedule

Reverts all the Doors in a Zone based on the specified Event. Simply choose the Event, plus optionally the Zone, Door or Reader at which the Event occurred, plus optionally the Group that initiated the Event, and the Target Zone to Revert. The Doors in the Zone will return to their normal Schedule.

Figure 1-260: Revert Zone

a. Configure the *Schedule* - Choose a Schedule that defines the time range you want to allow this Rule to run (usually the Always Schedule).

b. Configure the *Event* - Select Meeting Ended from the list.

c. Configure the *Target Zone* - Choose the same Zone that you specified in the Unlock Zone Rule.

3. Click the **Create** button to create the Rule

18.6 Create a Meeting

This step assumes that you have completed the installation and configuration of the INFINIAS Exchange integration, and setup your system to manage the Door locks via Microsoft Exchange. To set a locking schedule, create a meeting in the Microsoft Exchange calendar starting when you want your door to unlock and ending when you want your door to re-lock.

Make sure you set the *Meeting Reminder* if that is what will provoke the *Unlock Zone*

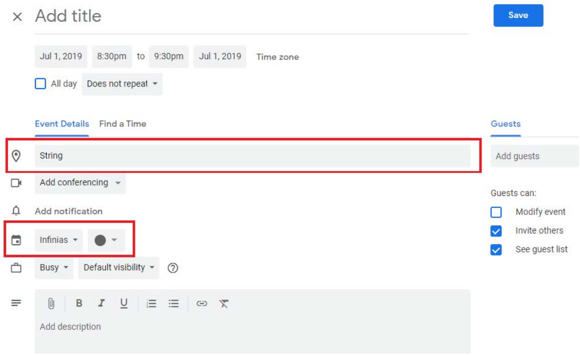
19 Google Calendar Integration

This section features the contents of the Google Calendar Integration Guide, which allows users to create exception schedules for their Doors by simply booking a calendar invite using Google.

19.1 Introduction

Once the Google Calendar *Peripheral* is configured, using it is easy:

- The peripheral monitors the Google Calendar for each scheduled meeting or appointment.
  - INFINIAS CLOUD receives *Meeting Started* (start time of meeting), *Meeting Ended* (end time of meeting), and *Meeting Reminder* (Reminder notification programmed for meeting) events for each scheduled meeting or appointment in that calendar.
- Create Meeting Location Names that match **Zone** or **Door** Names in the INFINIAS system configuration.
  - When booking a meeting in Google Calendar, these meeting location names must match the **Where** field.
- Once the Peripheral has been created, create *Rules* in INFINIAS and begin scheduling meetings in Google Calendar.



Jul 1, 2019 8:30pm to 9:30pm Jul 1, 2019

□ All day Does not repeat

String

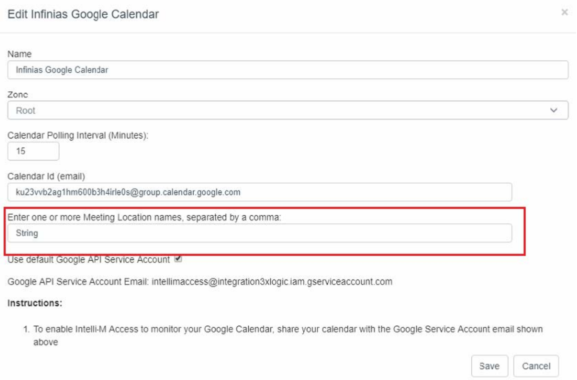
Infinias ●

Busy Default visibility

□ Modify event
☑ Invite others
☑ See guest list

Figure 1-261: Google Calendar - New entry

The Meeting Location Name acts as a link to a Rule and should match the Google Calendar “Where” field as shown.



Edit Infinias Google Calendar

Name: Infinias Google Calendar

Zonc: Root

Calendar Polling Interval (Minutes): 15

Calendar Id (email): ku23vvb2ag1hm600b3h4irle0s@group.calendar.google.com

Enter one or more Meeting Location names, separated by a comma: String

Use default Google API Service Account ☑

Google API Service Account Email: intellimaccess@integration3xlogic.iam.gserviceaccount.com

Instructions:

1. To enable Intelli-M Access to monitor your Google Calendar, share your calendar with the Google Service Account email shown above

Figure 1-262: Google Calendar > Meeting Location

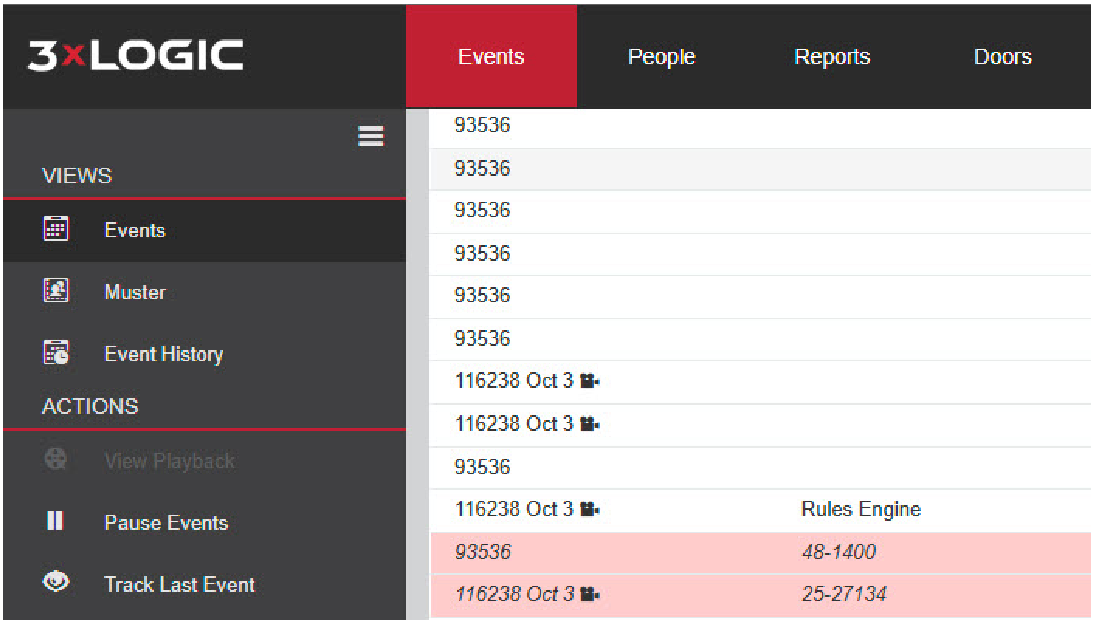
19.1.1 Requirements

For INFINIAS to monitor a Google Calendar, the calendar must exist and have a future scheduled event for each meeting location. The Google Service Account used by the INFINIAS software needs access to the Google Calendar. 3xLOGIC features a default service account in the software specifically for calendar integration, so the simplest configuration is to share the Google Calendar with this service account.

19.2 Google Calendar Peripheral Setup

Access the Portal via the following URL: https://portal.3xlogic.com

Once logged in the software, the Events tab loads by default.



93536	
93536	
93536	
93536	
93536	
93536	
116238 Oct 3	
116238 Oct 3	
93536	
116238 Oct 3	Rules Engine
93536	*48-1400*
116238 Oct 3	*25-27134*

Figure 1-263: Portal > Events

Navigate to the **Configuration** section from the right of the top menu.

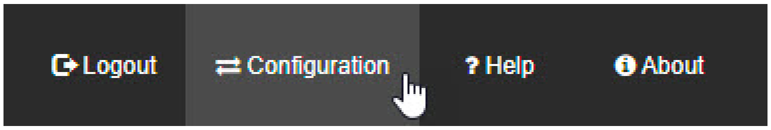


Figure 1-264: Configuration

Select the **Peripherals Tab** from the middle of the new options in the top menu.

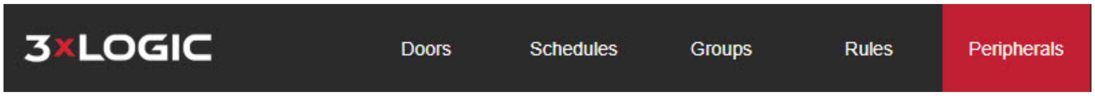


Figure 1-265: Peripherals Tab

Select **Create Peripheral** under *Actions* on the left side of the screen.

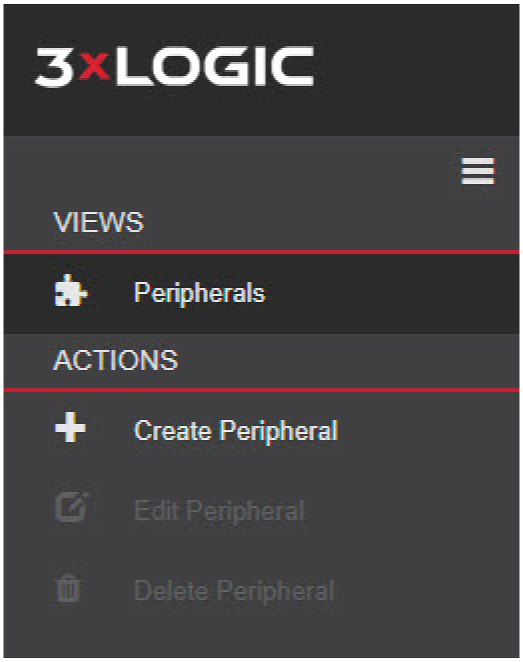


Figure 1-266: Peripherals > Actions > Create Peripheral

The *Create Peripheral* dialog populates with multiple options; select **Google Calendar**.

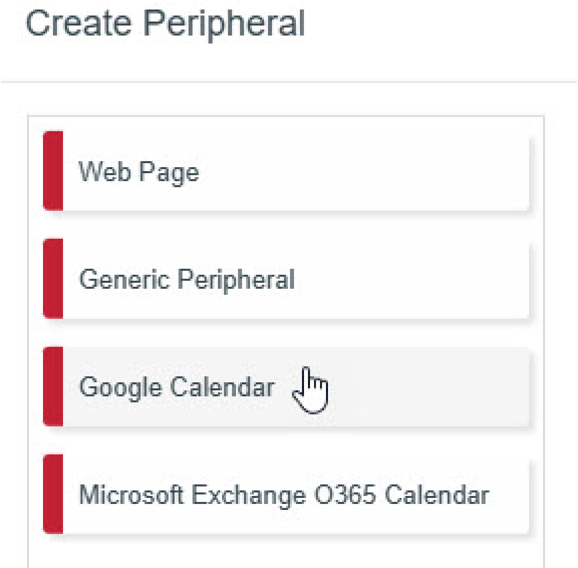
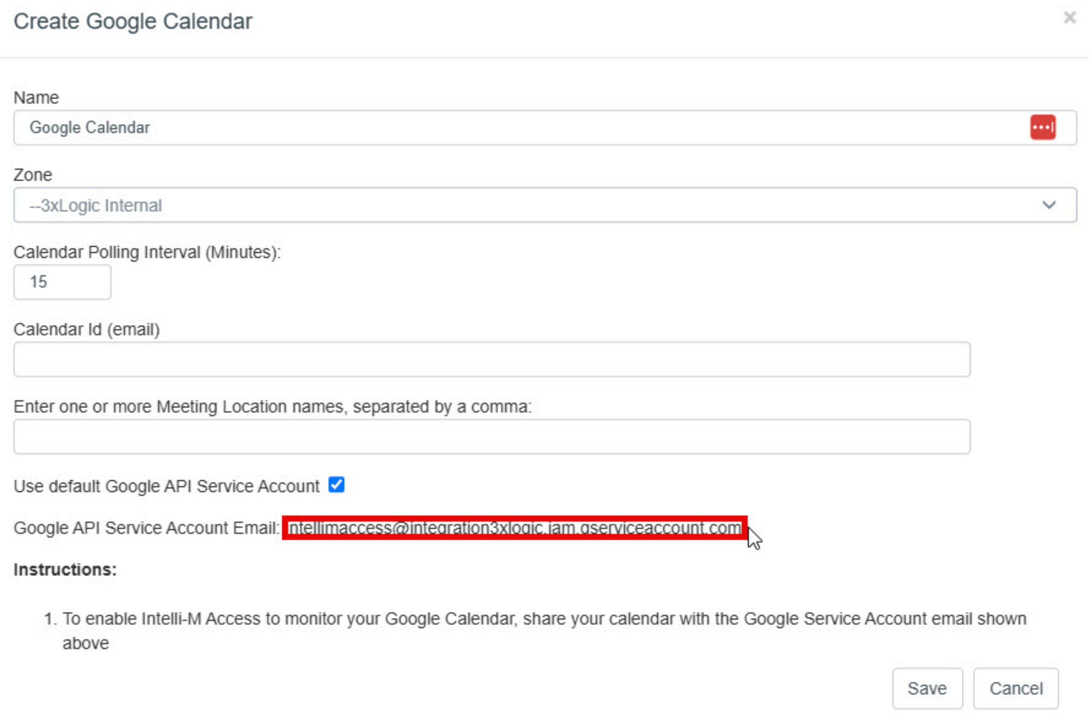


Figure 1-267: Create Peripheral dialog window

Highlight and copy the **Google API Service Account Email** (necessary for future steps).



Create Google Calendar ×

Name

Google Calendar

Zone

--3xLogic Internal

Calendar Polling Interval (Minutes):

15

Calendar Id (email)

Enter one or more Meeting Location names, separated by a comma:

Use default Google API Service Account ☑

Google API Service Account Email: intellimaccess@integration3xlogic.iam.gserviceaccount.com

Instructions:

1. To enable Intelli-M Access to monitor your Google Calendar, share your calendar with the Google Service Account email shown above

Figure 1-268: Example Google API Service Account Email

19.3 Google Account Setup

Login to the Google account and access Google Calendars.

- Go to Google Calendar.
- Find the desired Calendar.
- Click the Dropdown Menu.
- Choose Settings and sharing for the specific calendar.

It is possible to link multiple calendars in this way. All of them need their own INFINIAS *Peripheral*.

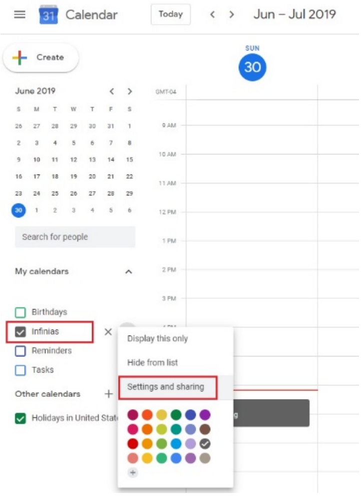
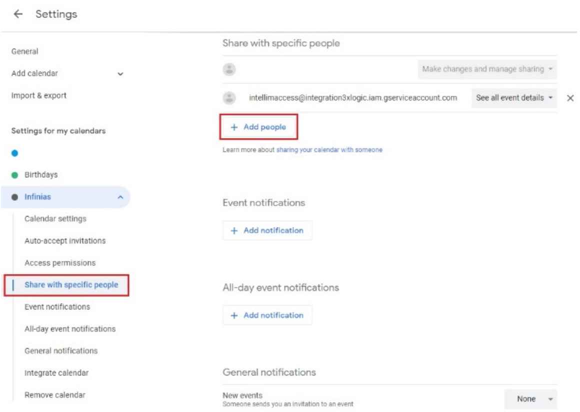


Figure 1-269: Calendar Settings

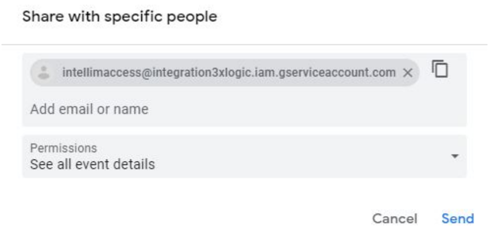
Navigate to *Share with Specific People* and click the **Add People** button to add the specific address pulled from the Google Calendar INFINIAS Peripheral.



intellimaccess@integration3xlogic.iam.gserviceaccount.com — See all event details

Figure 1-270: Sharing Settings

A new window appears; **paste the address** and set the *See All Event Details* and <u>send</u>.


Share with specific people

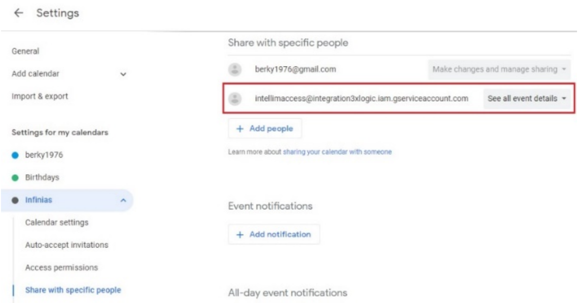
intellimaccess@integration3xlogic.iam.gserviceaccount.com

Add email or name

Permissions
See all event details

Figure 1-271: Sharing with specific people

The new address displays under the *People* being allowed to get details for the calendar.

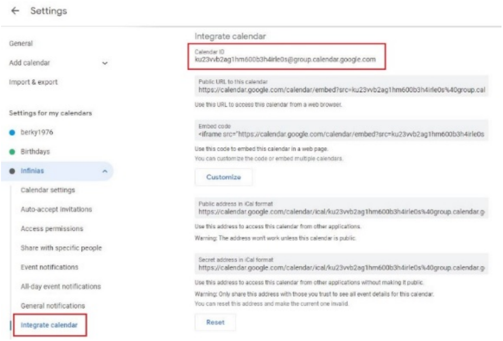


berky1976@gmail.com — Make changes and manage sharing

intellimaccess@integration3xlogic.iam.gserviceaccount.com — See all event details

Figure 1-272: People with access

Have the **Calendar ID** available, which is typically the associated email address. However, if an *additional calendar* was created under the primary Google account, a string style <u>autogenerated email address</u> will be created by Google.



Integrate calendar

Calendar ID
ku23vvb2ag1hm600b3h4irle0s@group.calendar.google.com

Public URL to this calendar
https://calendar.google.com/calendar/embed?src=ku23vvb2ag1hm600b3h4irle0s%40group.cal

Use this URL to access this calendar from a web browser.

Embed code
<iframe src="https://calendar.google.com/calendar/embed?src=ku23vvb2ag1hm600b3h4irle0s

Use this code to embed this calendar in a web page.
You can customize the code or embed multiple calendars.

Public address in iCal format
https://calendar.google.com/calendar/ical/ku23vvb2ag1hm600b3h4irle0s%40group.calendar.g

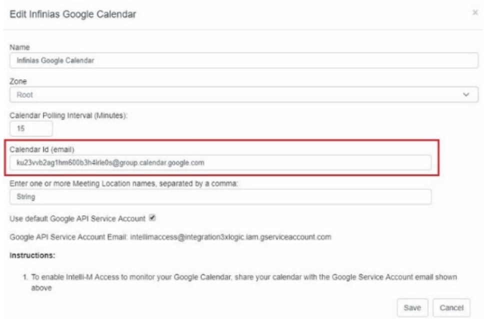
Use this address to access this calendar from other applications.
Warning: The address won't work unless this calendar is public.

Secret address in iCal format
https://calendar.google.com/calendar/ical/ku23vvb2ag1hm600b3h4irle0s%40group.calendar.g

Use this address to access this calendar from other applications without making it public.
Warning: Only share this address with those you trust to see all event details for this calendar.
You can reset this address and make the current one invalid.

Figure 1-273: Integrate Calendar > Calendar ID

In the same Settings Menu, navigate further down the list to **Integrate Calendar** as shown below and copy the information from Google to the *Peripheral*.



Edit Infinias Google Calendar

Name
Infinias Google Calendar

Zone
Root

Calendar Polling Interval (Minutes):
15

Calendar Id (email)
ku23vvb2ag1hm600b3h4irle0s@group.calendar.google.com

Enter one or more Meeting Location names, separated by a comma:
String

Use default Google API Service Account ☑

Google API Service Account Email: intellimaccess@integration3xlogic.iam.gserviceaccount.com

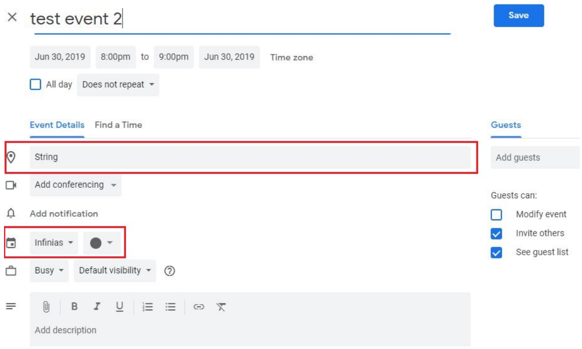
Instructions:

1. To enable Intelli-M Access to monitor your Google Calendar, share your calendar with the Google Service Account email shown above

Figure 1-274: Edit Calendar > Calendar ID

Note: In order to schedule a meeting for a future time within the Google Calendar, complete "Google Calendar Peripheral Setup" on page 181.

Click any **Calendar Day** that occurs in the future (e.g. any day greater than the current time). Fill in the *Title* of the event, and the *Location Field*. Make sure the Calendar Selection matches the Calendar that you just enabled permissions on. Click **Save**.



test event 2

Jun 30, 2019 8:00pm to 9:00pm Jun 30, 2019

□ All day Does not repeat

String

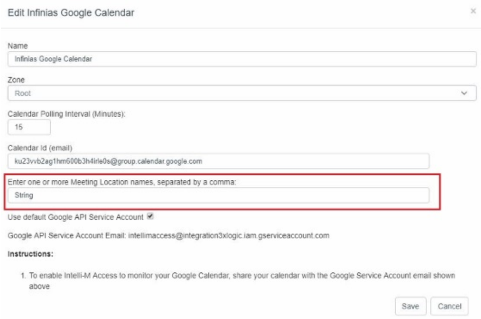
Infinias ●

Busy Default visibility

Guests can:
□ Modify event
☑ Invite others
☑ See guest list

Figure 1-275: New Calendar Event

It's important to remember *exactly* how content was entered into the Location Field, as this information will be used in INFINIAS. If the name does not match, an error will occur.



Edit Infinias Google Calendar

Name: Infinias Google Calendar

Zone: Root

Calendar Polling Interval (Minutes): 15

Calendar Id (email): ku23vvb2ag1hm600b3h4irle0s@group.calendar.google.com

Enter one or more Meeting Location names, separated by a comma: String

Use default Google API Service Account ☑

Google API Service Account Email: intellimaccess@integration3xlogic.iam.gserviceaccount.com

Instructions:

1. To enable Intelli-M Access to monitor your Google Calendar, share your calendar with the Google Service Account email shown above

Figure 1-276: Location Field input

Repeat this step, creating a future event for each Location to link to the Calendar. Keep note of the details in the Location field to reference each time. If even one location is not entered in the Peripheral the same as indicated in the Calendar, an error will occur. Locations are separated in the peripheral by a comma, as indicated.

If all information is correct, a success message will be displayed when saving the peripheral. It is now possible to add Calendar Events within Google Calendar and associate them with INFINIAS Access Rules.

20 Allegion ENGAGE Integration

This section features the S-ENGAGE Gateway Setup steps (for Allegion wireless locks).

The setup assumes that the secured location already completed initial setup with INFINIAS and has the needed hardware installed, including the Gateway. If you have any questions or need assistance with preliminary steps, installation, etc., please reach out to your point of contact with INFINIAS. There are links to instructional videos provided in the form of QR codes (included here).

20.1 Before You Begin

This guide is abridged for users already familiar with the ENGAGE install. For more detailed instructions, please reference the linked video (QR Code) at the end of this guide..

The following items are required prior to configuring the integration:

1. An Apple or Android mobile device with Bluetooth.
2. The ENGAGE Mobile App installed.
3. An ENGAGE Gateway, model S-ENGAGE-GATEWAY.
4. License per wireless lock S-WL-1.
5. INFINIAS CLOUD or Server version 6.4 or above (ESSENTIALS, CORPORATE, or PROFESSIONAL).
6. Install the physical lock (LE or NDE models); use a QR code scanner to view installation videos for the associated for the applicable model.

20.2 Pre-configuration Requirements

1. Install the activation license from 3xLOGIC in the INFINIAS server software.
2. Visit https://portal.allegionengage.com/signup to create a user account.
3. Program API settings ***for local server install only in INFINIAS.*** The Allegion site must be created by INFINIAS.

20.3 INFINIAS Setup

1. Edit a **Customer** to enable Allegion integration, and specify the **Weigand format** and the **Serial Number** of your ENGAGE Gateway.
2. Navigate to the **Door Types view** under the **Settings** tab within **Configuration** to enable the *ENGAGE Fail Safe 5 Second Unlock*, and the *ENGAGE Fail Secure 5 Second Unlock*.

20.4 ENGAGE Gateway and Lock Setup

1. Connect the gateway to a Power Over Ethernet switch.
    - If using a standard switch, use the supplied AC cable to power the gateway.

2. Download and install the ENGAGE Mobile App.
3. Login to the ENGAGE Mobile App with the previously created account.
4. Select the desired **Customer Name** (customer name will auto populate from INFINIAS), click the **+ sign** to add a “Gateway” to the list.
5. Select the **IP** Tab; choose **IP Behind Firewall**; then select **Next**.
6. Enter the following information:
   - *Local Server Access Control*
     a. **Server URL:** *https://[SERVER IP ADDRESS]:19800*
     b. **Certificate Authority (CA) Server URL:** *http://[SERVER IP ADDRESS]/webhal/engage*
   - *CLOUD-Based Access Control*
     a. **Server URL:** https://devices.ia.3xlogic.com:19800
     b. **CA Server URL:** http://devices.ia.3xlogic.com/webhal/engage

20.5 Link Lock Gateway

1. In the ENGAGE App, Select the **Customer Name** to which you want to associate the lock.
2. Click the **+ sign** to select the applicable model of the lock.
3. Return to the **Device Selection Screen** and select **Managed Linked Devices**.
4. Link your wireless lock to the gateway.

20.6 Add Lock to INFINIAS

1. In the INFINIAS software, Select **Create Door** action under **Configuration**, select **Allegion ENGAGE** and fill out the door details.
2. Select the lock that was previously configured under Serial Number.

20.7 Installation Video

Scan the QR code for step by step video for comprehensive ENGAGE Gateway Installation.

21 Contact Information

3xLOGIC has offices in Victoria BC, Canada and in Fishers, Indiana, USA. Please visit our 3xLOGIC website at www.3xlogic.com. Please contact us by e-mail at helpdesk@3xlogic.com (technical support), or using the following contact information:

3xLOGIC Technical Support

Toll Free:(877) 3XLOGIC
(877) 395-6442
Email: helpdesk@3xlogic.com
Website: www.3xlogic.com

3xLOGIC USA Main Office

11899 Exit 5 Parkway, Suite 100
Fishers, IN 46037
United States. (303) 430-1969

3xLOGIC INFINIAS™

Simple. Scalable. Secure.