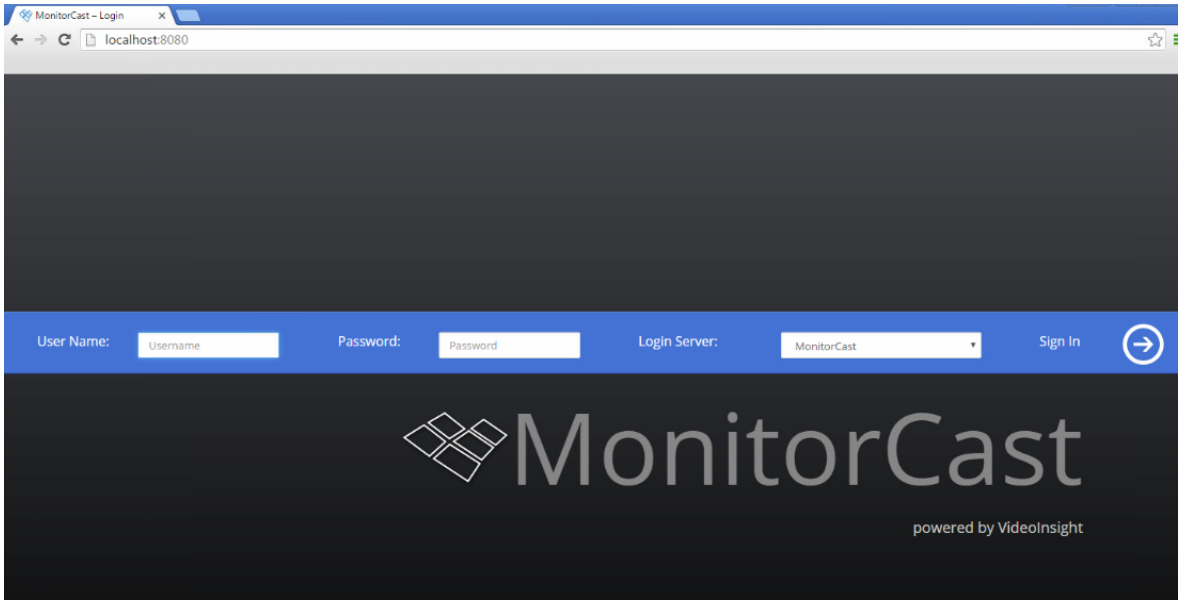
MonitorCast v3.5 Web Client Login

To launch the web client main interface into MonitorCast v3.5, open your internet browser and navigate to the following address: https:// [Server IP Address]:8080

A login screen will appear. First time users will use the default authentication provided below.



You can also click on the desktop icon for MonitorCast Web Client from the server.

Default Authentication

The default username for MonitorCast v3.5 is set to Admin. The default password is 1234.
Once logged into the application the user can navigate to one of the outlined sections:

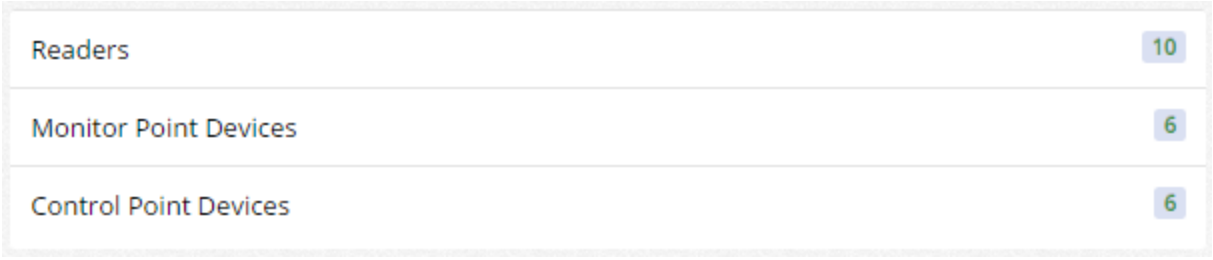
- Dashboard
- Reports
- Hardware
- Access Levels
- Personnel
- Administration
- Schedules

Dashboard

The dashboard contains 6 main components: Alarms Pending, Event Viewer, Event Filtering, Recent Personnel, Recent Activities, and Card History. *Recent activities and Card History will only show for admin users. The MonitorCast v3.5 dashboard provides at-a-glance information regarding key components in your access control system. In the sections below, you will learn about the major components that exist in the MonitorCast v3.5 dashboard.

Alarms Pending

The Alarms Pending window will display a total count of all alarms pending in the system. These alarms include transactions such as Access Denied, Door Held Open, Reader Tamper and Door Forced. Displayed to the right of alarms, the user will notice a Hardware Summary Window that displays summary of all hardware installed and detected by the database.

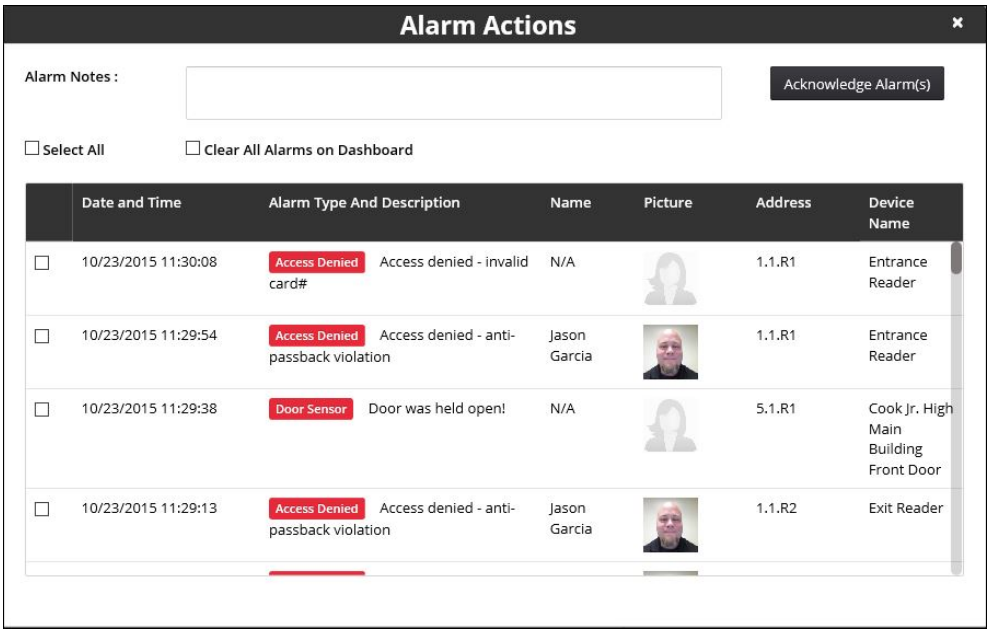


As alarms are detected, the window color will display in red, indicating there are alarms that need to be addressed.

To clear alarms, click the Clear Alarms button located in the Event Viewer Window. This action will remove all Alarms from the event window.

Alarm Acknowledgement

When an alarm is triggered and is displayed within the Alarms Pending section, each alarm can be directly acknowledged by whomever is granted access to write notes and dismiss specific alarms. In order to write a note and dismiss an alarm, click on the Alarms Pending icon and a new window will appear.



Within this window view, you are granted the ability to write alarm notes, select all alarms and dismiss alarms, clear all alarms, select specific alarms and write notes. To modify a specific event, simply check the tick box on the left side of the page, enter a note about the event and then select Acknowledge Alarms.

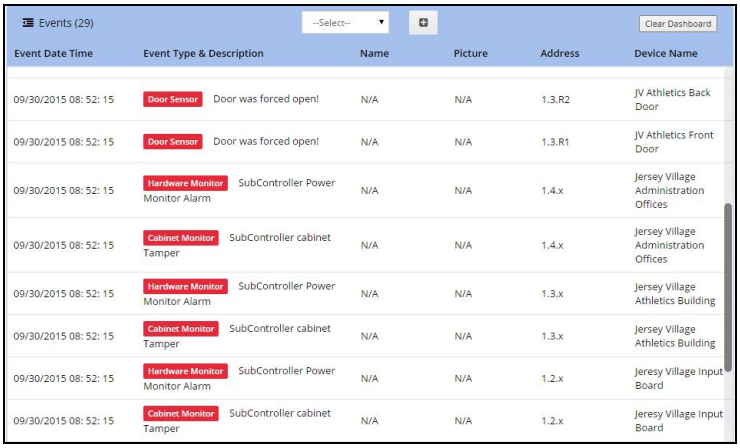
To review the message entered for a cleared item, refer to Reporting below.

Event Viewer

The event viewer will display all events by your selected readers. This allows users to monitor what transactions are taking place throughout the facility. This information will display the most recent alarms for ~4 minutes. Once the Dashboard is refreshed new data will appear and any previously shown record will only appear by conducting a search within the reporting menu. The event viewer will display the total amount of events presents, event date/time, event type and a short description, the name of the cardholder involved, and picture on file.

Alarm and Event Descriptions

Event Name	Description
Monitor Point Secure	Any door monitor point such as motion sensor inactive state; not in use
Monitor Point Active	Any monitor point in active state; in use
Control Point Active	Any control point in active state; in use
REX OK	Request to Exit activated
REX OK - Request Host	Request to Exit activated from the Door Management page
Reader Tamper	Reader is equipped with tamper proof mechanism that has been flagged
Door Secured	Represents door closed
Door Held Open	Default is 30 seconds to detect door held open; modification can be made under Hardware Config section.
Door Forced Open	Represents unauthorized door entry without a REX or valid card read
Access Denied	Represents Access Denied via card transaction
Access Granted	Represents Access Granted via card transaction
Door Open	Represents a door open
Control Point	Represents output devices
Monitor Point	Represents input devices
Trigger Procedure	Represents a trigger from a Hardware Rule

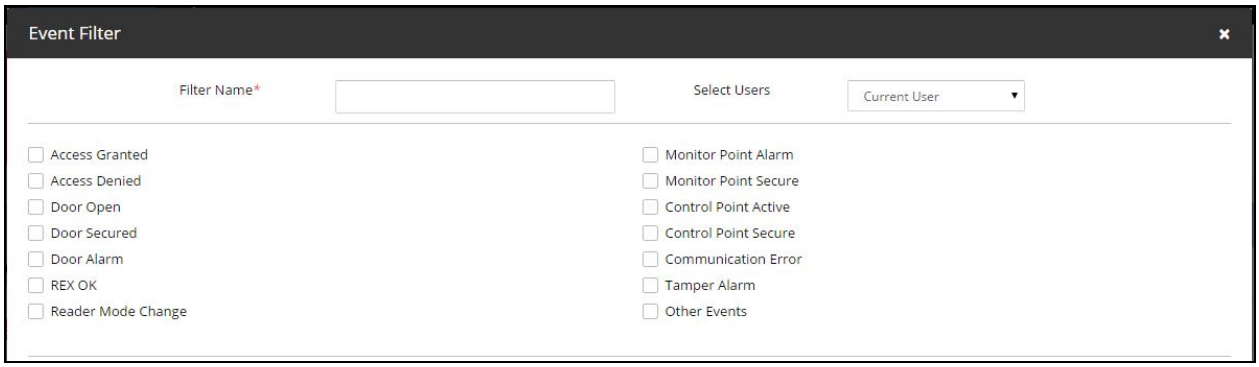


The name of the reader that holds transactions will also be listed on the Event Viewer page. Data in the event viewer is real time and automatically refreshes in the browser.

Event Filtering

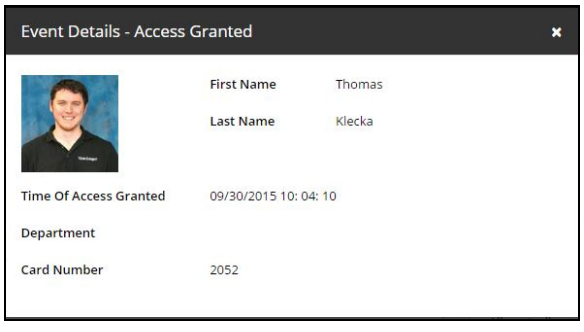
To create an event filter, click the  icon on the Event dashboard section. This feature will allow users to customize what types of events are displayed in the Dashboard. For example, if the user will like only alarms to display, the user can filter this information into an Event Filter and select this filter from the drop down list.

Next, create a Filter Name for the event filter. This name should be used to describe the contents of the filter. Select, the types of filters by selecting the checkbox next to the corresponding event.



Next, select the readers that this filter will include. You can use the Reader Groups section or manually select each reader individually from the Readers tab. If the events involve Monitor Point and/or Control Point activity, select those items from the tabs as well.

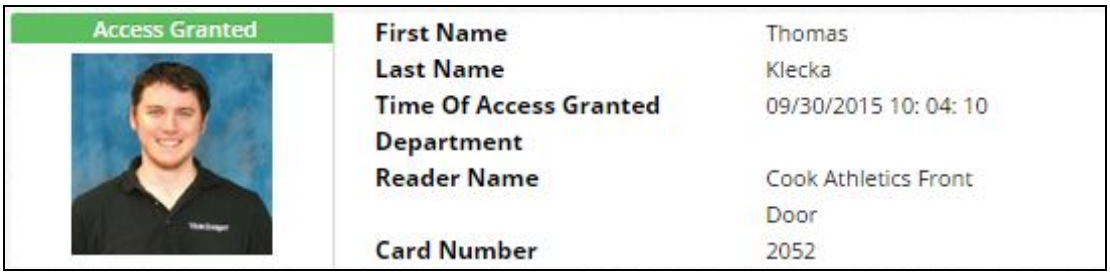
Click Save to finalize all changes. You will see your new event filter type listed in the drop down in Events. In the event, you will need to make changes, click the Edit icon , to make changes to the event filter.



Double clicking on the event name or photo will display the event details listed for the transaction.

Recent Personnel Activity

As cardholders are granted or denied access, the Recent Personnel Window will contain the last personnel who attempted access. The window will display the name, time granted, and staff details. If another personnel badges into the reader, it will reflect the most recent badge in scanned.



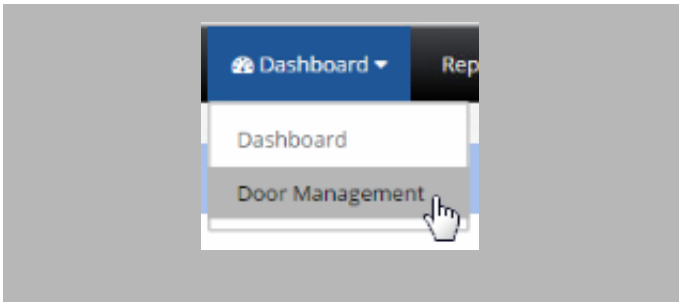
Recent Activities

On the dashboard, you will also find a window displaying all recent activities. These activities are gathered from the database and include items such as modification to controllers, user system changes, access level changes, and hardware modifications. The last 10 recent history records will be displayed in order of newest to oldest.

Card History

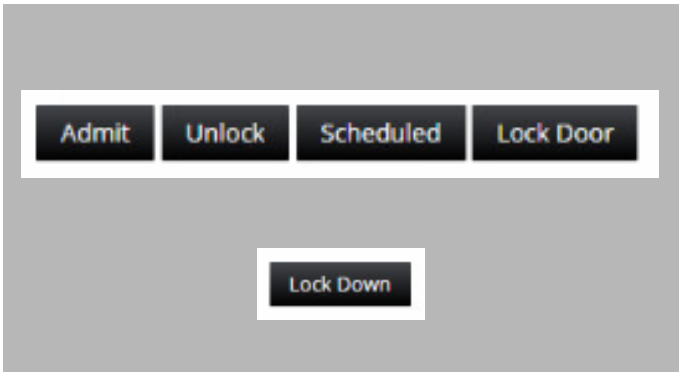
On the dashboard, you will also find a window displaying all card history. These activities are gathered from the database and include items such as cards added/removed and personnel card changes. The last 10 recent history records will be displayed in order of newest to oldest. The card history will also display which user conducted the change and at what date. If additional details are available, the event will be converted into a hyperlink, providing more information about the card history event.

Door Management



To access the Door Management tools, click on **Dashboard** then **Door Management**.

Users will be able to see the current state of each reader or reader groups in the environment.



The statuses are:

- Unlock
- Card Or Pin
- Scheduled
- Lock Door
- Lock Down

To change the status of a door reader, select the door reader or door reader groups you wish to change and click the options to make the change.

Admit: When selected this option will change the reader(s) to a temporary unlocked state. After 5 seconds, the reader will return back to its original state. This option can be used to temporarily allow access for a short period of time.

Unlock: When selected, this option will unlock the door reader until otherwise changed.

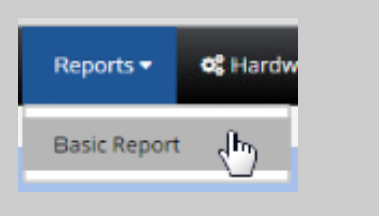
Scheduled: When selected, this option will remove any other rules and return the door state back to its original time based door schedule.

Lock Door: When selected, this option will lock the door reader until otherwise changed. While the door is locked, Card or PIN access only goes into effect.

Lock Down: This action will lock all readers simultaneously into a lockdown mode which makes the doors switch to Request to Exit only. Card or PIN access will be denied.

REPORTS

MonitorCast v3.5 offers the ability to search and extract specific details, as well as advanced log filtering. These capabilities allow the administrator to sort logs within a specific date range time, for specific events, by specific card reader, by a group of card readers, by Monitor Point Devices, by Control Point devices, specific controllers, sites, and personnel.

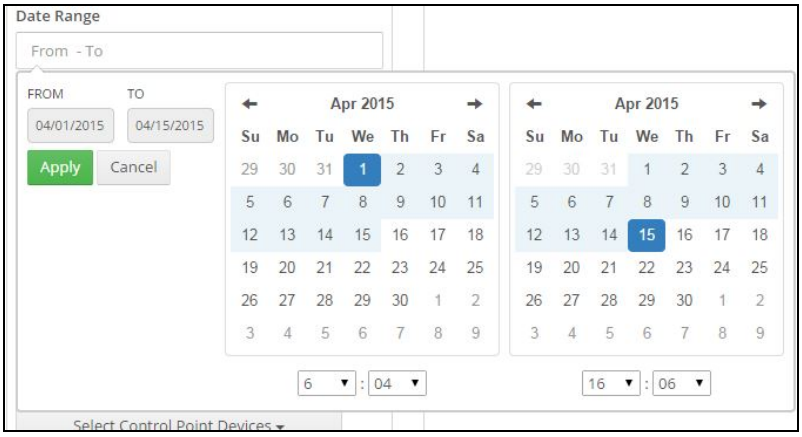


To access the reporting features, simply select the Reports tab at the top of the screen and then click Basic Report from the drop-down menu, as seen below.

On the **Event Report** page, the left hand column provides a number of Search Filters designed to help you narrow down the specific information needed for reporting output. Here, selecting any combination of the filters provided will result in the narrowing of data provided for an exported report.

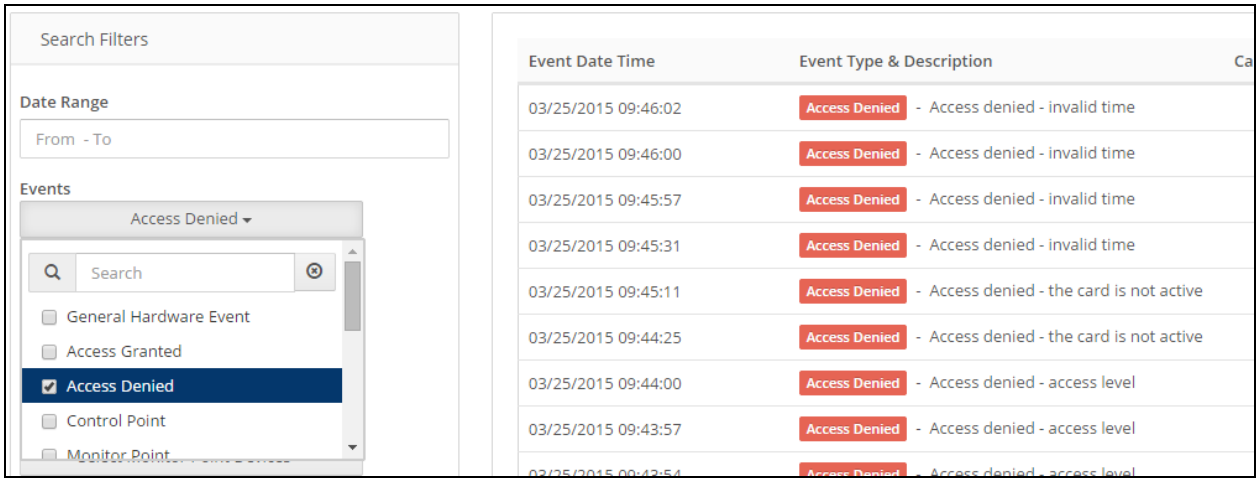
With each filter selected, the reduction of information provided narrows in the resulting search.

For example:
When a date range from 6:04am April 1, 2015 through 4:06pm April 15, 2015 (seen in the image below) is selected, the resulting information provided will be the records available within that period of time and nothing outside of that scope.

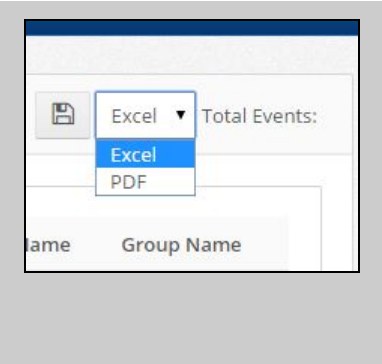


If you select the same date range, while also adding a second filter for all Access Denied Events will result in the removal of all logs not found within the specified date range that have Events other than Access Denied.

The results of your search will be displayed to the right of the Filters, as seen below.



It is our suggestion that the initial search allow for as much information possible, and then apply one filter at a time to bring your search to result to the most desired result. If too many filters are applied at one time and the search result provides no information, the option to reset all filters is available at the bottom of the Search Filter panel.



The two formats available for exporting are Excel spreadsheet or as a PDF file, for which ever you desire to use.

To export a final search result, choose one of the two format options made available in the top right-hand corner of the screen. Next, select the save icon, located to the left of the desired format drop-down menu.

After selecting save. The search results will begin to download to your computer.

Note: If no date range is specified in a search, only the last 30 days of information will be scanned for the report. If more data is needed, the data can be extracted by connecting to the database with Microsoft Excel(™) and pulling the **dbo.EventHistory** data into a spreadsheet.
For more information on how to accomplish this, please reference Microsoft's Knowledgebase article: http://support.microsoft.com/kb/306125 for more information.

Video Integration Setup – VI Monitor 6

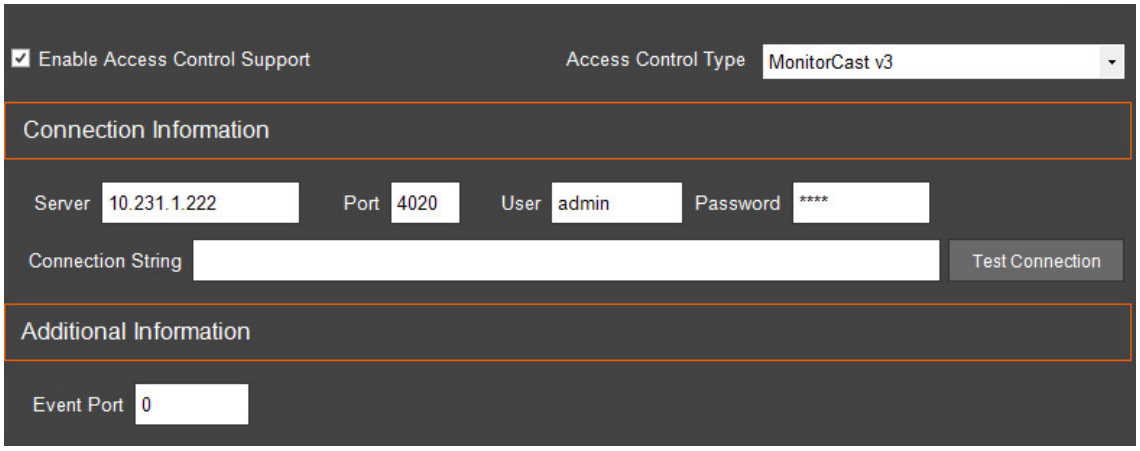
Configuring the MonitorCast v3.5 Integration with VI Monitor will allow you to have full access to the following features.

- Access View
- Door Logs and Events
- Lane Viewer
- Facility Maps with integrated Access View
- Door Management
- Mobile application integrations

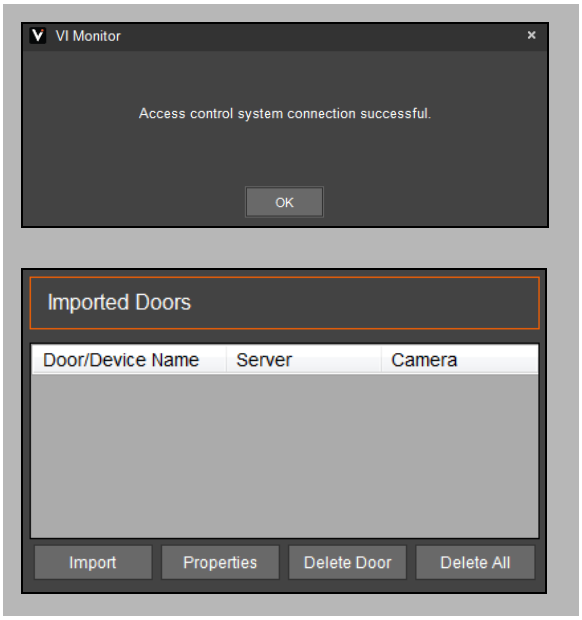
Before setting up the integration with VI Monitor 6 and MonitorCast v3.5, download the latest version of the Access Control Plugin installer at www.downloadvi.com. The installation contains all required files necessary to complete installation. The installer will need to be loaded on the IP Server for the best results. Before installation, be sure that the service is in the STOPPED state throughout the installation. During the installation, you will be prompted to select an Access Control Integration. Be sure to select the drop down VI MonitorCast v3.5 to load the complete files.

Once installed, launch VI Monitor on IP Server. Select Administration, then Server from the main ribbon menu. Select the server in which you wish to apply Access Control functionality. Next, select Access Configuration to launch the configuration settings.

First, click **Enable Access Control Support** and select the Access Control Type as MonitorCast v3.5.



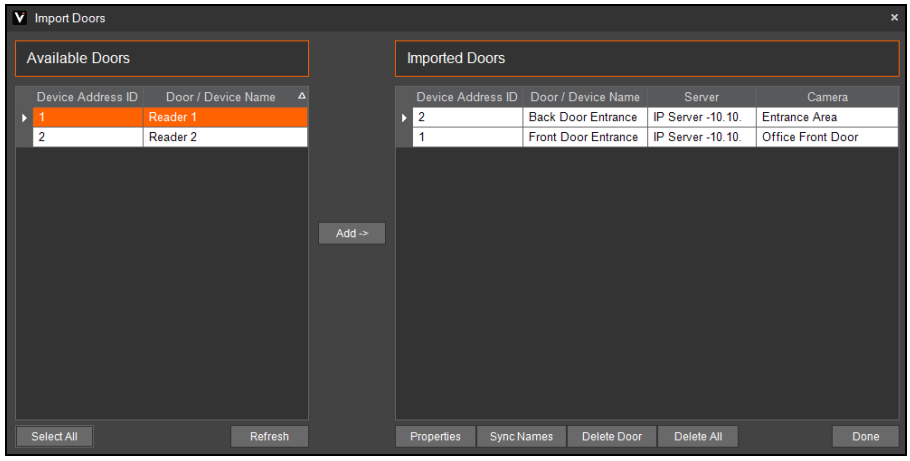
Input the server hosting MonitorCast v3.5 along with the specified username/password and specified port number (default 4020). Connection String will remain blank and Event Port should be listed as 0.



Next, click Test Connection and ensure that the connection is labeled Successful.

To set up your doors and assign camera permissions, click Import on the Imported Door section.

Next, select the Readers in which you wish to control. You can assign a number, door name and camera that will be assigned to the door by clicking Properties on the Import Doors window. By default, the doors do not associate with cameras automatically.



Once configured, click **Done**.

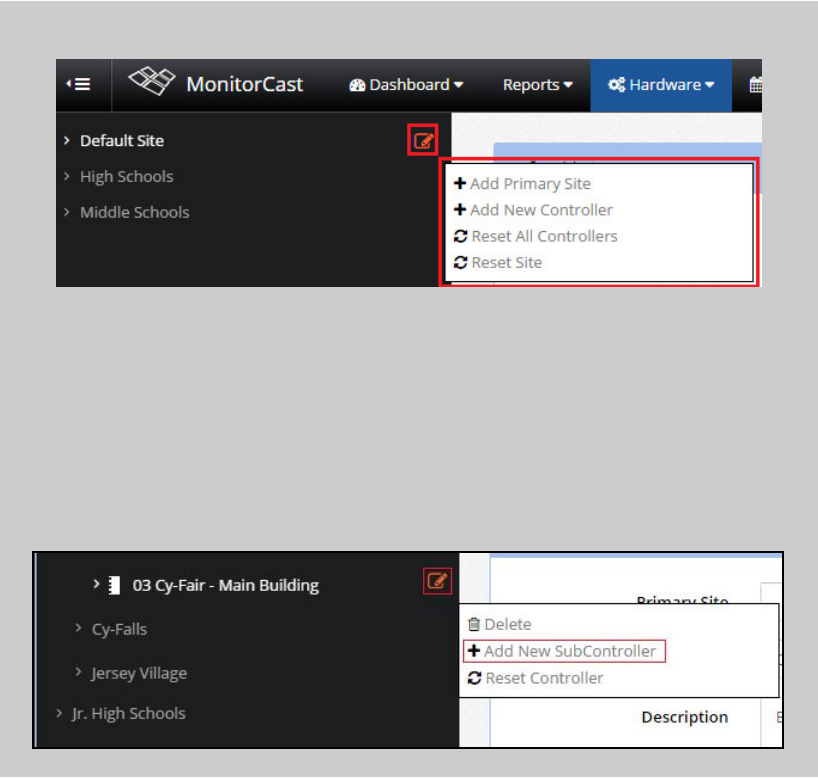
Hardware

The Hardware Section is comprised of three sections: Hardware Config, Reader Groups and Card Format.

Hardware Config

Before the hardware configuration, Video Insight recommends all controllers and sub controllers to be pre-programed with the correct network information such as IP address, default gateway and subnet mask. Ensure that no other Access Control systems are accessing the hardware during the setup process. If using MR52 sub-controllers, be sure to set up the baud rate to 38400 prior to configuration.

To begin, click Hardware Config from the main menu. Mouse over Default Site on the left side and add either a new Primary Site or add a new controller to Default Site. Sites will organize specified controllers across the network for easy organization. In this example, we will add a new controller.



After clicking Add New Controller, setup the controller name, IP address and controller type.

For the controller type, you will have a choice of:

- EP 2500 – Primary controller with 0 readers installed
- EP 1502 – Primary 2-door controller
- EP 1501 – Primary 1-door controller

After adding a controller, you can add a sub controller to it with the same icon used for adding the controller:

For the sub controller type, you will have a choice of the following controllers:

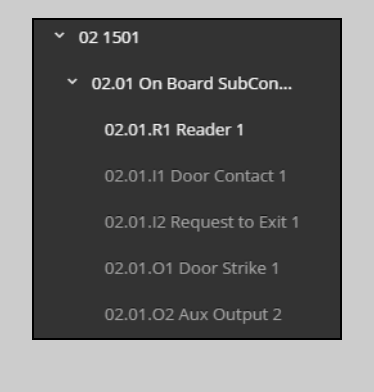
- MR50
- MR16IN
- MR16OUT

- MR52
- MR51e

Controller, and sub controller names should reflect area of installation or where the controller is physically located. For example, if the primary front door controllers are located in the IT server room, the name EP1502 – IT will appear.

Click Save and restart the AC Server service to apply changes. ***Note** - The default LED mode for Readers is set to 2. Select the Reader properties if you wish to change this setting.

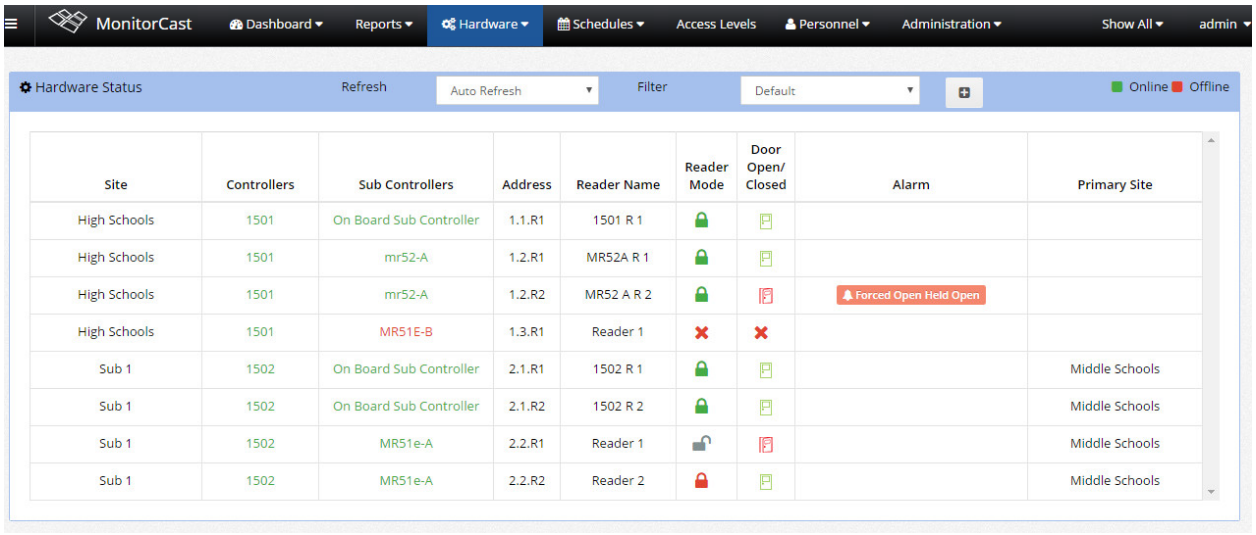
By clicking on the Edit icon located to the right of any site, the option to reset the entire site will appear as an option. The intended purpose of this feature is to allow for the temporary reset of a device, or devices, to force it to update the most recent changes made to the functionality settings by MonitorCast v3.5.



After installation of any hardware device, the input/output locations can be modified. For example, Input 1 is Door Contact and Input 2 is Request to Exit.

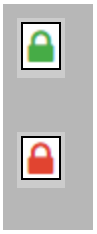
Hardware Status

This table displays the status of all controller and sub controller doors. The table is organized by controller and will display all readers within each corresponding controller or sub controller. Green represents a controller or sub controller that is online, Red if it is offline.



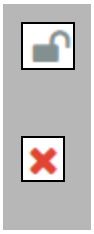
Hardware Status Icons

Reader Modes :



Locked/Card or PIN

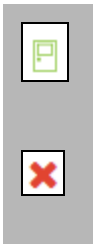
Lock Down



Unlocked

Offline

Door Open/Close :

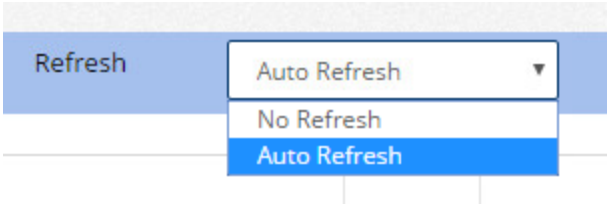


Door Closed

Door Offline

Door Open

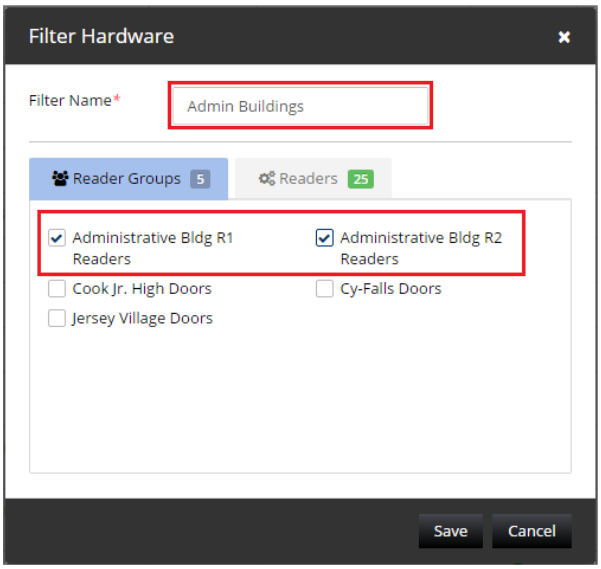
Alarms :			
Forced Open	Forced Door	Held Open	Door Held Open after a Granted or REX

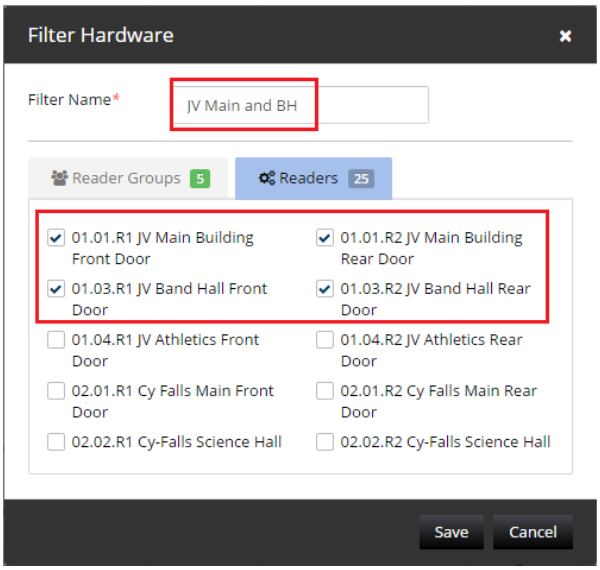


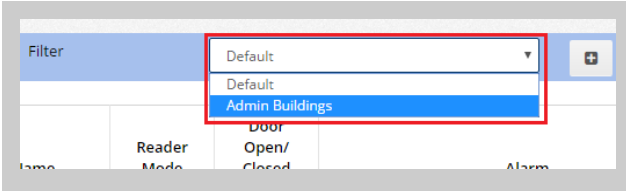
At the top of the page you will find a drop-down for Auto Refresh, seen left.

Filters can also be created to customize your view of the Hardware Status.

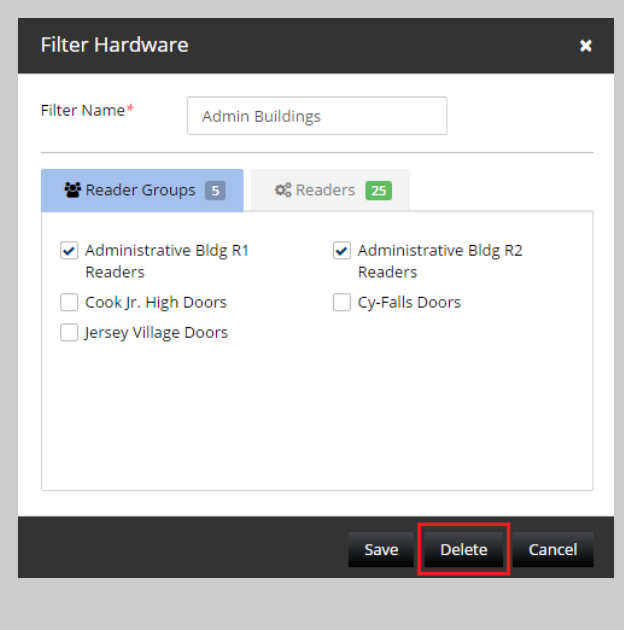
First click the Add button  to the right of the Filter drop-down. Name the Filter, and choose the Reader Groups, or individual Readers, you would like for the Hardware Status view.







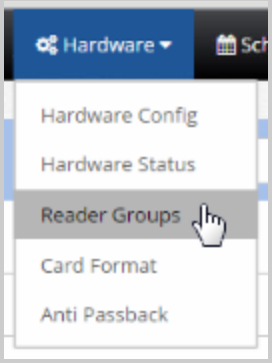
When finished, click Save and the new filter will be shown in the drop-down, as it appears on the left.



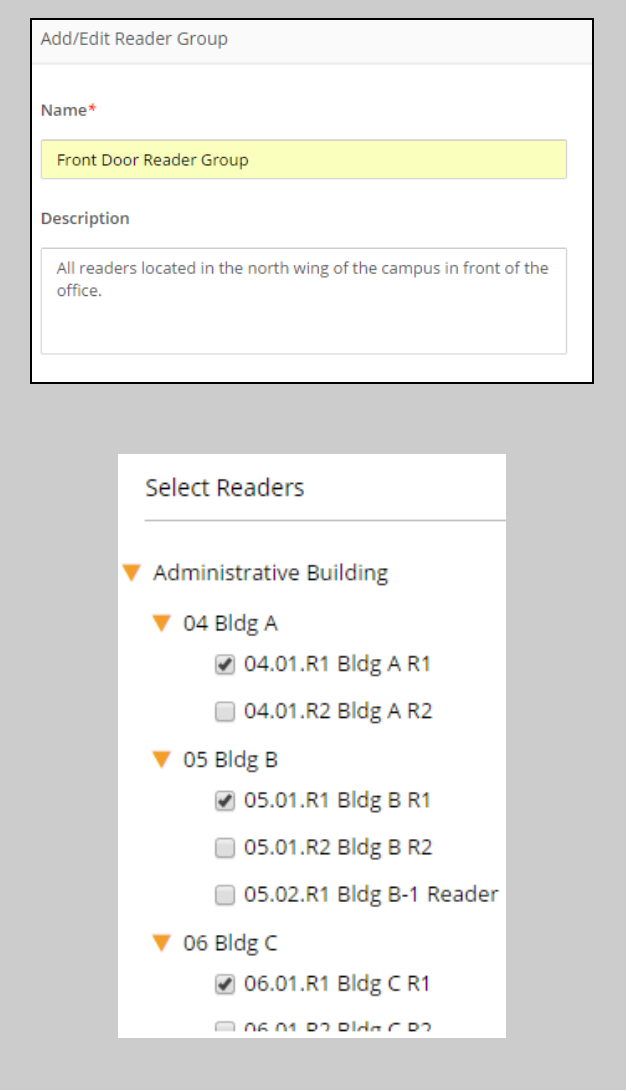
To delete a filter, select it from the drop-down, click the Edit button  and click **Delete**.

Reader Groups

Reader Groups can be setup to label sets of readers into a organized group. This allows you to use multiple readers while configuring Access Levels and Schedules.



To setup a reader group, click on Hardware, followed by Reader Groups in the main menu.



Next, create a name for the group of readers and provide a brief description of where the readers are located.

Next, assign the readers belonging to that group. The readers are organized by Site on the right area of the window.

Select readers by clicking the checkboxes next to the readers.

The reader group will be created and displayed in the Reader Groups area.

To edit an existing reader group, select the name of the Reader Group and make the changes in the right panel. Be sure to select Save after each entry. Restart the AC Server service to apply changes.

Card Format

MonitorCast v3.5 supports numerous data card formats including:

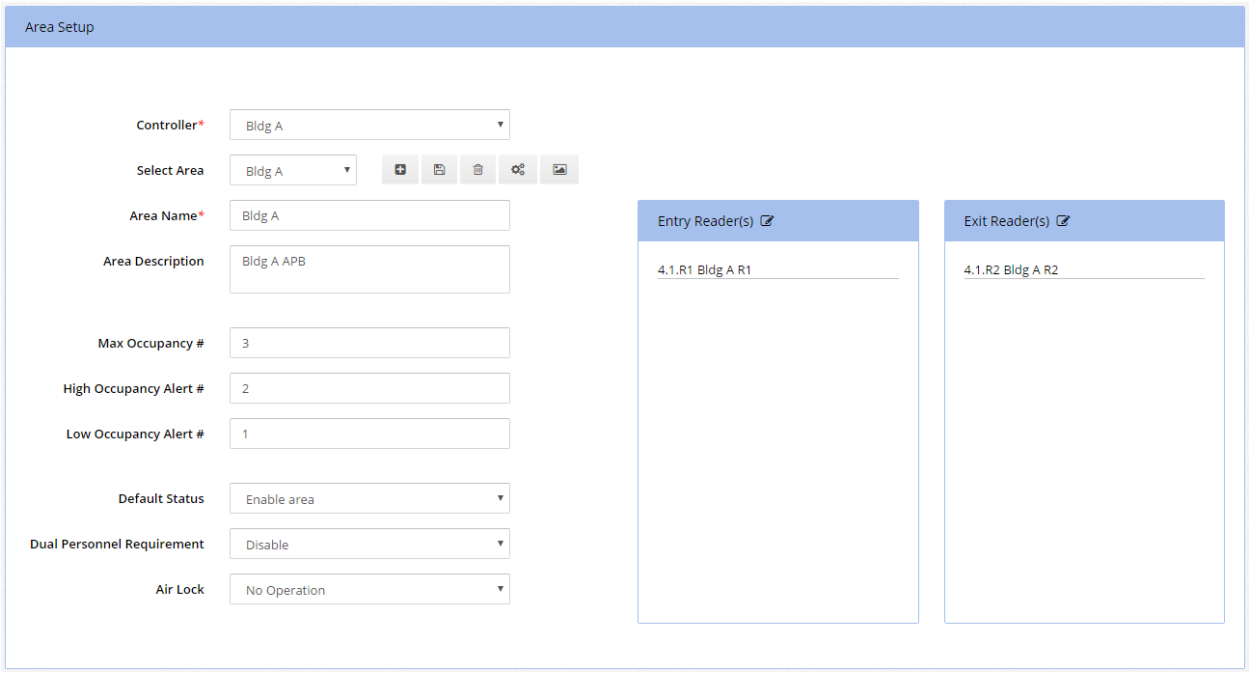
- 26 Bit Standard (HID)
- 35 Bit (HID)
- HID PIV-EP (HID)
- 36 Bit (HID Corporate)
- 26 Bit Universal Card Format
- 37 Bit Universal Card Format

- 26 Bit with 24 Bit Card number (HID)
- Magstripe (IVECO)

Additional custom formats can be added upon the request by Video Insight. Edit Card Format will allow you change different properties including Facility Code, which will allow you to configure your Facility Code that is required before use at your facility.

Anti Passback

The Anti Passback mode is used to prevent more than one person from using the same card in a controlled area.



A good example would be where MonitorCast is used to monitor a parking garage, which typically there is only one **Entry**, and one **Exit**.

For every **Entry** a cardholder would have to an area, a corresponding **Exit** would be needed for the person to use the card again at the **Entry**.

This prevents a cardholder from passing their card to another person for access. If this was attempted with the Anti Passback setting enabled, the 2nd card swipe to the **Entry** would not allow access unless the **Exit** reader was swiped first.

Occupancy Control

The Occupancy Control setting would allow the user to set the maximum amount of cardholders allowed in an area.

Using the previous parking garage example, if the garage only had 20 parking spaces, the user could deny access to the 21st person trying to enter. Once someone has exited the garage, another would be allowed in.

The user can also setup a **High Occupancy** and **Low Occupancy** alert that would be shown on the Dashboard. This would allow the user to know when the area was getting close to maximum occupancy, or the area was getting close to being empty.

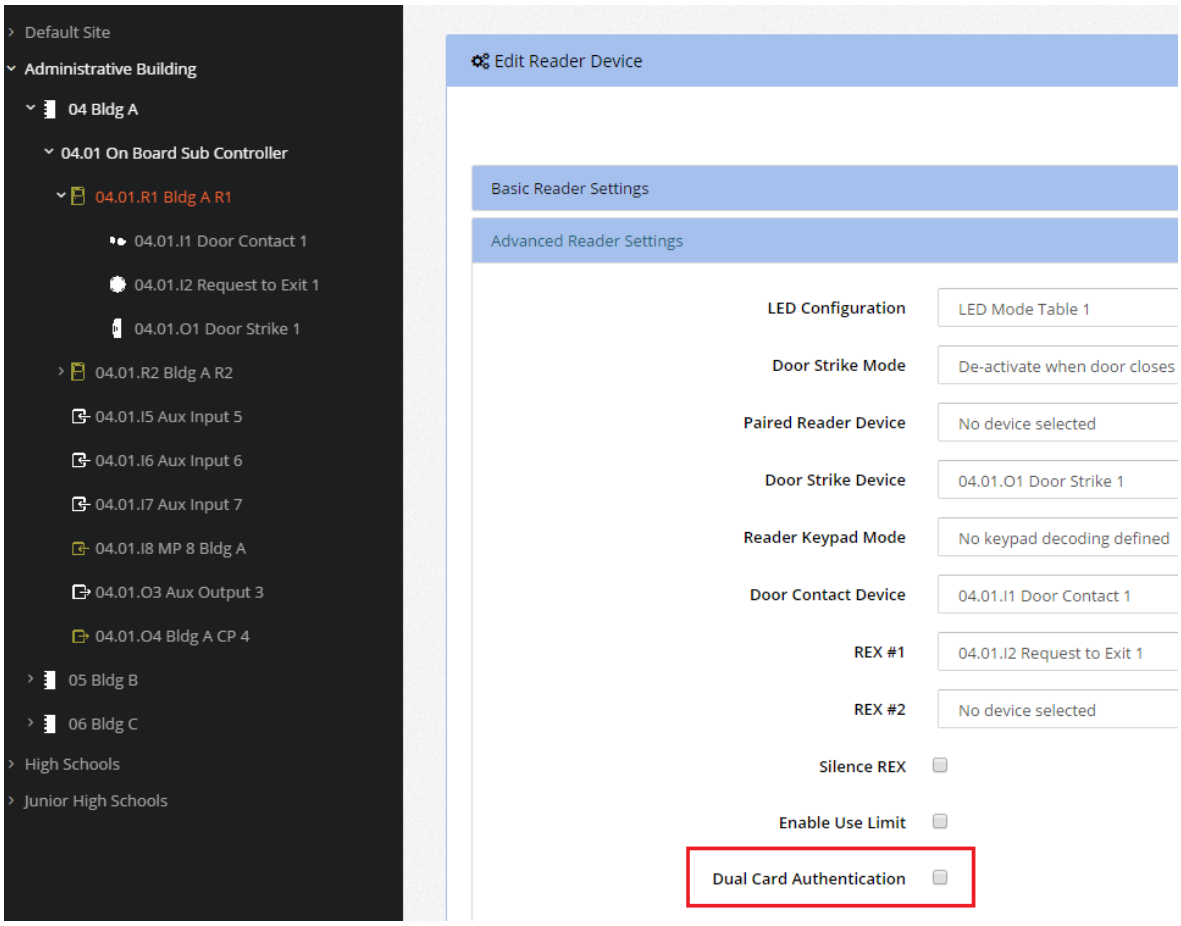
Once the last person has left the area, an **Occupancy count reached zero** event will be shown on the Dashboard.

Dual Personnel Requirement

This feature allows the administrator to create an area that is never populated by only one person. If enabled, two cardholders are required to swipe into the the area at the same time if the occupancy count is zero. If there are only two people left in the area, both would be required to swipe out at the same time as well.

***Note -** A similar feature to the Dual Personnel Requirement is also available called **Dual Card Authentication**.

Dual Card Authentication is similar to this feature. The exception being that EVERY entry and exit from the Reader requires two cardholders- instead of the first 2-in and the last 2-out. If the Dual Card Authentication setting is preferred, the settings can be altered on the Hardware Config page in the Reader settings.

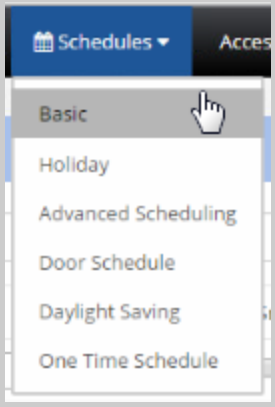


Schedules

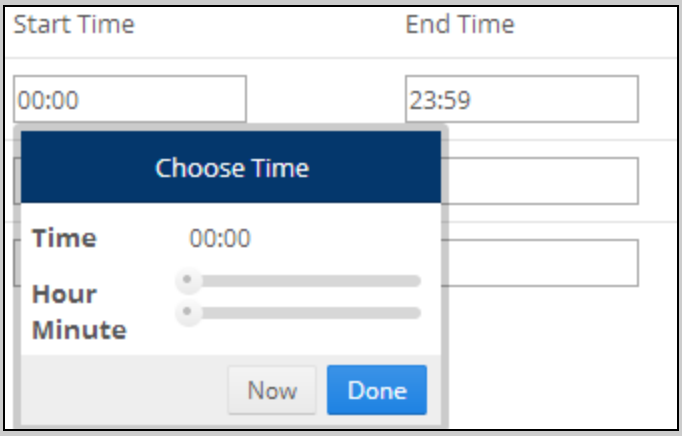
A schedule is a set period of time applied between predefined hours as a control set. For example, without an applied schedule a door will remain in a locked state and will not be accessible. There are three types of schedules that can be set up in MonitorCast v3.5: Basic, Holiday, and Door Schedule.

Basic Schedules

Basic schedules are used to define door reader activity under normal use and can also be applied to various Access Levels. The basic schedule is typically used the majority of the time and is the primary schedule for the doors during normal business hours.



To create a basic standard schedule, click **Schedules** > **Basic** from the main menu.



Click the **(+)** icon to create the Time schedule name.

Once created, set the **start time** and the **end time** intervals by using the slider tools or by typing into the fields provided.

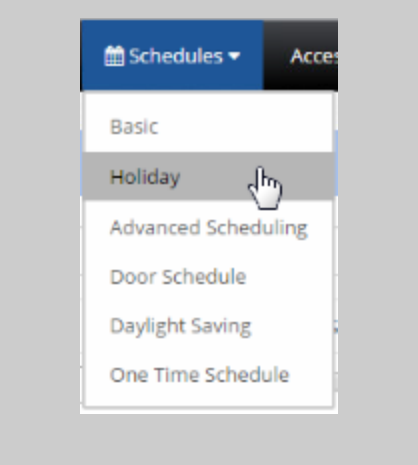
(*The time format is based on of 24 hour clock format.*)

In the example above, the sliders are being dragged in an effort to change the time interval. Optionally, on the same screen, the use of the keyboard to manually set the time is available. Next, select the days of the week in which the schedule will apply. Multiple time intervals may be added on the same day. If more time intervals are needed, click on the **(+)** sign to add another level or intervals.

Once all time intervals have been set up, click **Save**. All basic schedules will come into effect immediately. The access level and door schedule sections at the base of the page will display all Access Levels being used during the configuration of the schedule.

Holiday Schedules

Holiday schedules are used for individual full day changes from the Basic Schedule. Christmas Day, Thanksgiving Day, or Labor Day would be a good fit for a holiday schedule because it requires a full day change. Holiday schedules can be scheduled in advance and pre planned.



When active, holidays will force all readers into a Locked State and Card or Pin access will be required.

To create or plan out a desired holiday schedule, click on **Schedules** > **Holiday** from the main menu.

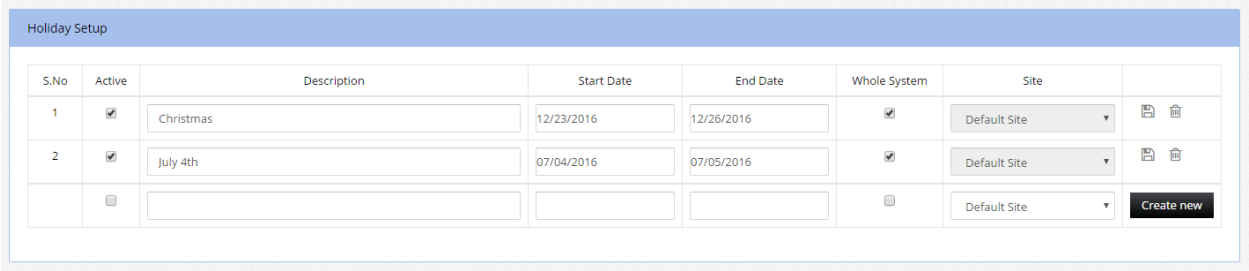
Create a holiday description, start date and end date for your holiday events.

Since time frames are not included, this function includes the full day. Any actions assigned will be in effect for a full 24 hr. period. For example, it may be desired for the doors to change to a locked status, with card or pin access only for a single, full day. The start date and end date will remain the same for that day. Select the checkbox under **Active** column to *enable* the holiday.

After adding the **Name**, **Start** and **End Dates**, choose which **Site(s)**, click **Create New**.

After editing a Holiday, make sure to click **Save** .

To remove a Holiday created, click **Delete** .

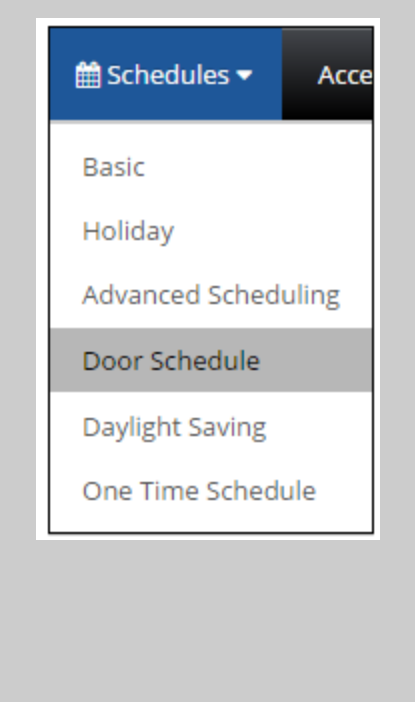


Holiday Masks

Holiday Masks will act as a temporary override of a normal schedule rule. Its intended purpose is to allow for deviations from a normal schedule cycle, and to allow for the automation of device overrides *on specific days and times*. Upon completion of a **Holiday Mask** schedule override, the default schedule created will resume as normal.

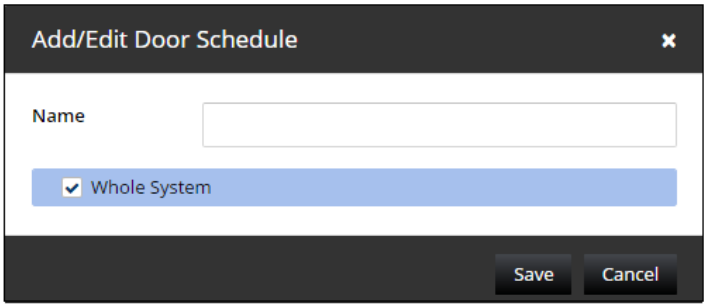
Door Schedules

Door schedules are specific time periods defined for use by MonitorCast v3.5. It is an editable, reusable time template that can be used to control when doors are accessible and at what status the door should be read. User access privileges are the result of a three way relationship that is created between users, door readers and a door schedule.



To create a door schedule, click **Schedules** > **Door Schedule** from the main menu.

Using the + icon, create a new door schedule by assigning this door schedule a unique name and selecting the designated sites desired.



Click Save to apply the name.

Next, select the desired schedule to apply to this **Door Schedule**.

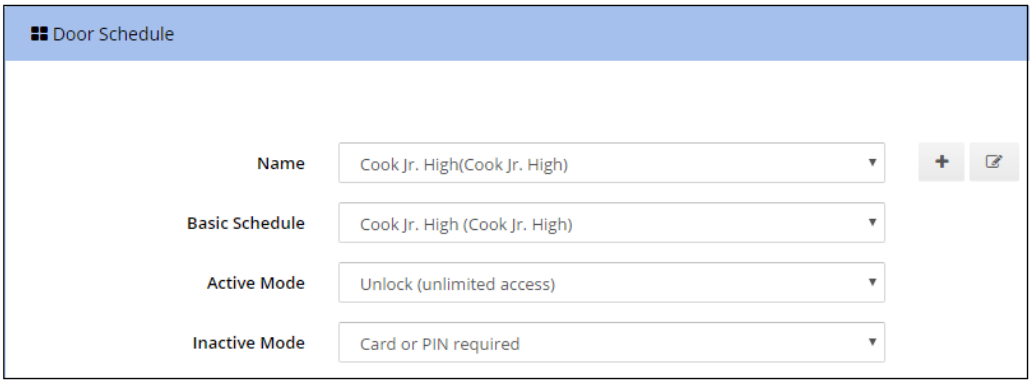
The Schedule drop-down will read all existing **Basic Schedules** in the system in order to determine the times involved for the specified door schedule. In the example below, we have selected *'Always.'*

Next, select the desired *action* for which the door schedule will take effect during the the time periods that the door schedule is **Active** and/or **Inactive**.

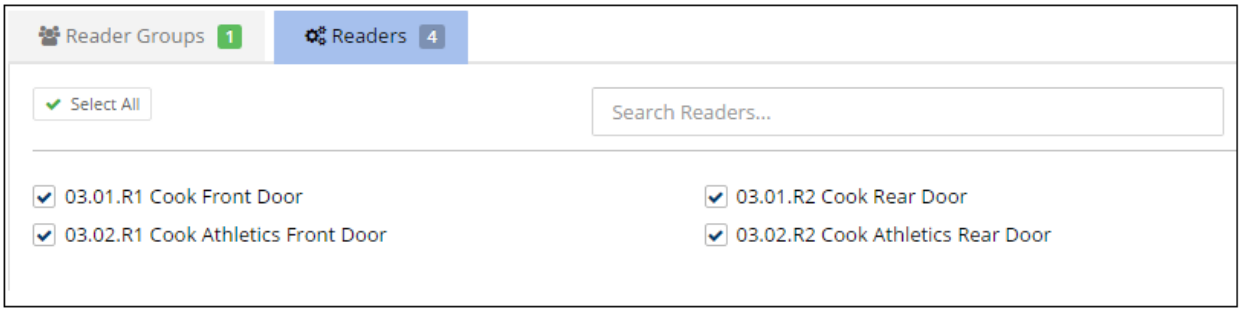
These options have been predefined as the follow:

1. Disable the ACR, No REX
2. Unlock (unlimited access)
3. Locked (No access, REX active)
4. Facility Code Only
5. Card Only
6. PIN Only
7. Card and Pin Required
8. Card or Pin Required

When the door schedule is active, the selected action will be in effect. While when the door schedule is *inactive*, the action will follow the **Inactive** action rule as defined.

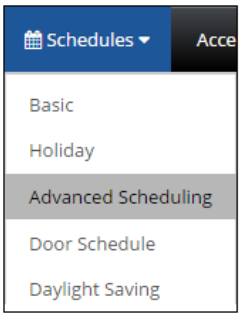


Finally, select the desired reader to include on the door schedule. The schedules available in the drop down are set up under Basic Schedule. For example, if this door schedule only appears to certain reader groups (Front and main doors), select those Reader groups from the grid , on the right.



Advanced Schedules

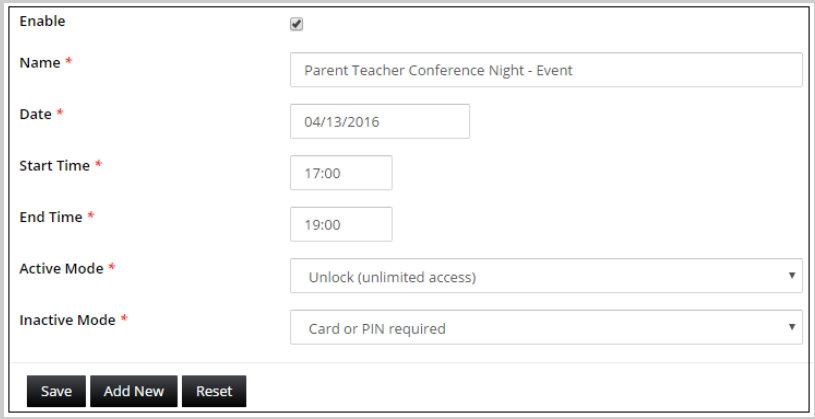
Advanced Schedules allow administrators to create custom door schedules that involve multiple time frames throughout the day. Unlike the traditional door schedules that affect a full 24-hour period, **Advanced Schedules** allow the administrator to edit specific time-frames the schedule follows. For example, Advanced Schedules can be used to schedule a special event that will place the doors of the desired locations to remain locked/unlocked. Advanced Schedules can be configured in advanced of a specific time, inclusive to a holiday schedule or a time-frame outside of a regular basic schedule to cover a special event.



To setup an Advanced Schedule, click on Schedules on the main menu, followed by Advanced Schedules.

Click **Add New**.

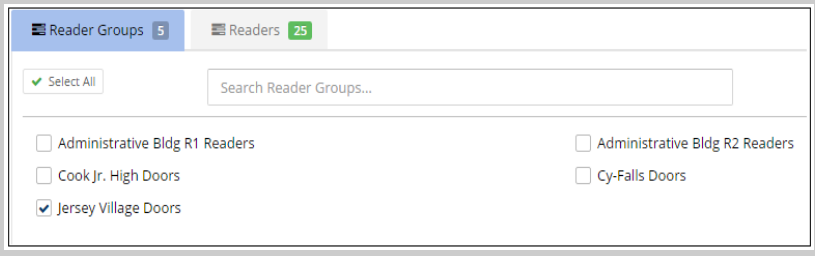
Create a new schedule by providing a Name for the schedule, dates the schedule will take effect, and start/end time. You will also need to determine what action the schedule completes when active, as well as what action the reader takes when in inactive mode.



The image above displays an example of a completed **Advanced Schedule** form.

Next, select the **Readers** to which the schedule applies.

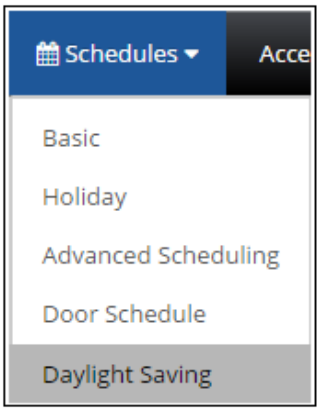
For example, if the schedule only affects a subset of main doors, select those readers from the Reader Group area or individually select the readers.



Click Save to finalize your changes and save the schedule. Once created, the schedule will appear in the table below. Edits can be made on the schedule by selecting the name of the schedule and making those changes in the form. To remove the schedule, click the icon.

Daylight Savings Settings

Daylight savings setting is preconfigured in MonitorCast v3.5 to utilize the correct time schedules. Each setting is then passed to the controllers; giving it its own independent timing settings. This allows the controller to handle daylight saving times in the event that the server is down or not available.



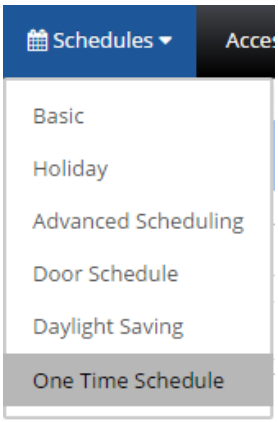
To set up your daylight savings settings, click on Schedules followed by DayLight Saving.

A general outline is setup by default as follows:

Year	Start Date	End Date
2014	3/9/2014	11/2/2014
2015	3/8/2015	11/1/2015
2016	3/13/2016	11/6/2016
2017	3/12/2017	11/5/2017
2018	3/11/2018	11/4/2018
2019	3/10/2019	11/3/2019
2020	3/8/2020	11/1/2020

If your region does not follow DST, you may remove or deactivate the settings from your controllers by removing the settings, or changing the Apply All, to deselect.

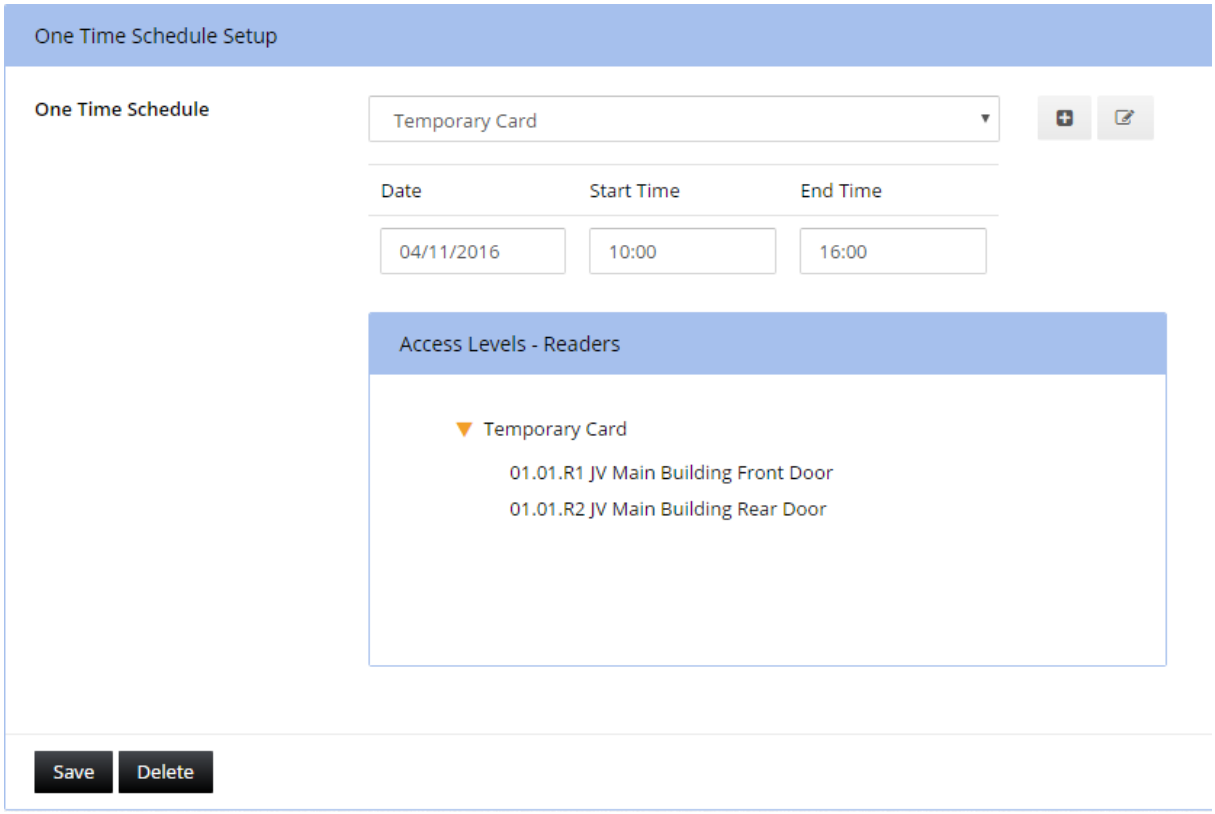
One Time Schedule



If it is necessary to create an Access Level for Personnel for just one date, instead of weekly access setup through Basic Schedule, you would create a One Time Schedule for the Access Level.

Click the **Add** button, create the name of the **One Time Schedule**, choose which **Site(s)** it will apply to. Then choose which **Date**, and the **Start** and **End Time**, and click **Save**.

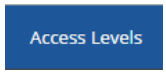
Any Access Levels assigned to the One Time Schedule will be displayed at the bottom. (Seen in the image below.



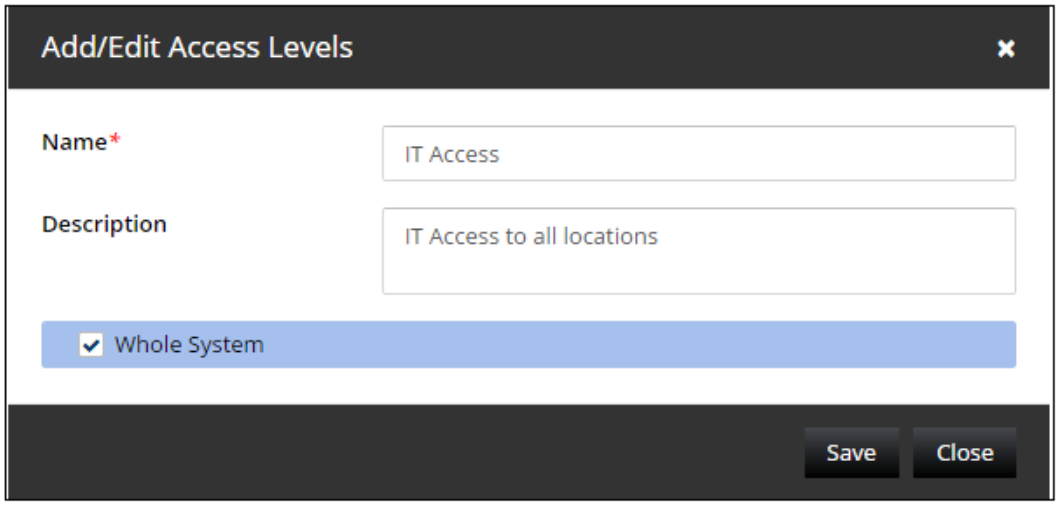
Access Levels

An Access Level is defined as a reader or group of readers with a time schedule association. Access Levels determine when a cardholder can access specified readers. Prior to creating the Access Level and Personnel in your MonitorCast v3.5 system, we advise the breakdown of your access level by sites, user groups departments, or areas of access.

Creating Access Levels

To create access levels, click 

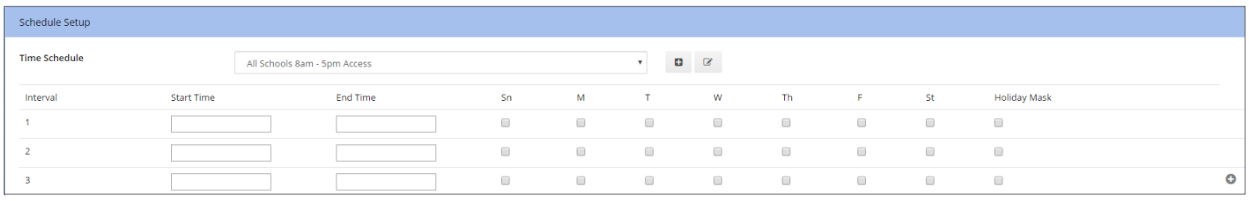
in the main menu. Click the  sign on the access level drop down, and provide a name to your access level. For this example, 'IT Access' was selected.



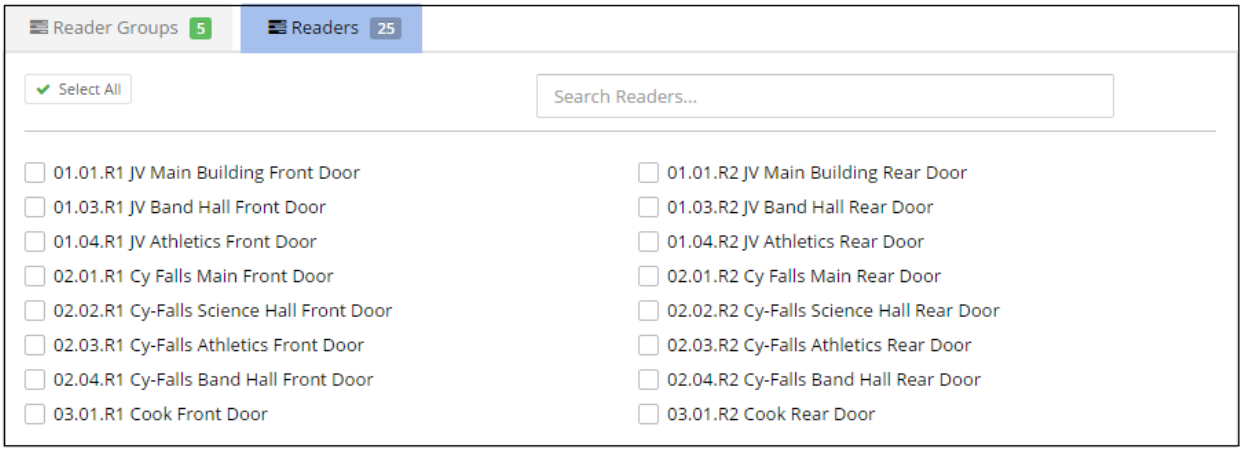
Once created, select a schedule for this access level to follow. Use the drop-down next to **Basic Schedule** to select this schedule or create a new time schedule. Creating a time schedule requires that the schedule be given a unique name and to select specific sites to be associated with that schedule, as well as selecting new time intervals.

In the example below, a predefined schedule has been created and labeled *Always*. Always is preset for all MonitorCast v3.5 setups. Other ranges of time for scheduling can be added if desired.

Click **Save** to finalize the Time schedule.



Next, select all readers that should follow this **Access Level** and time schedule.
Select the reader groups or individual readers from the **Readers** tab.



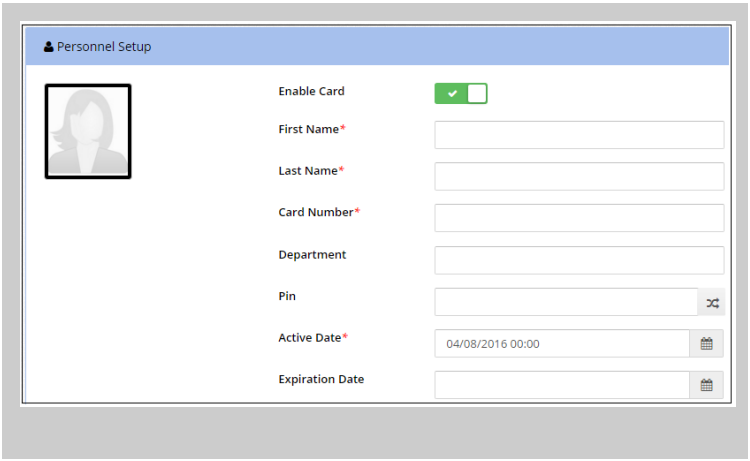
Once all desired readers are selected, click **Save** to finalize the changes.
The access levels will now be in effect. Restart the affected controllers to apply changes completely.

Personnel

To create personnel in MonitorCast v3.5, you can choose the manual method, import the card holders via Active Directory, or import via CSV.

Manual cardholder creation

To create them manually, click on **Personnel** from the main menu. Type the cardholder details you wish to create by entering the information on the form.

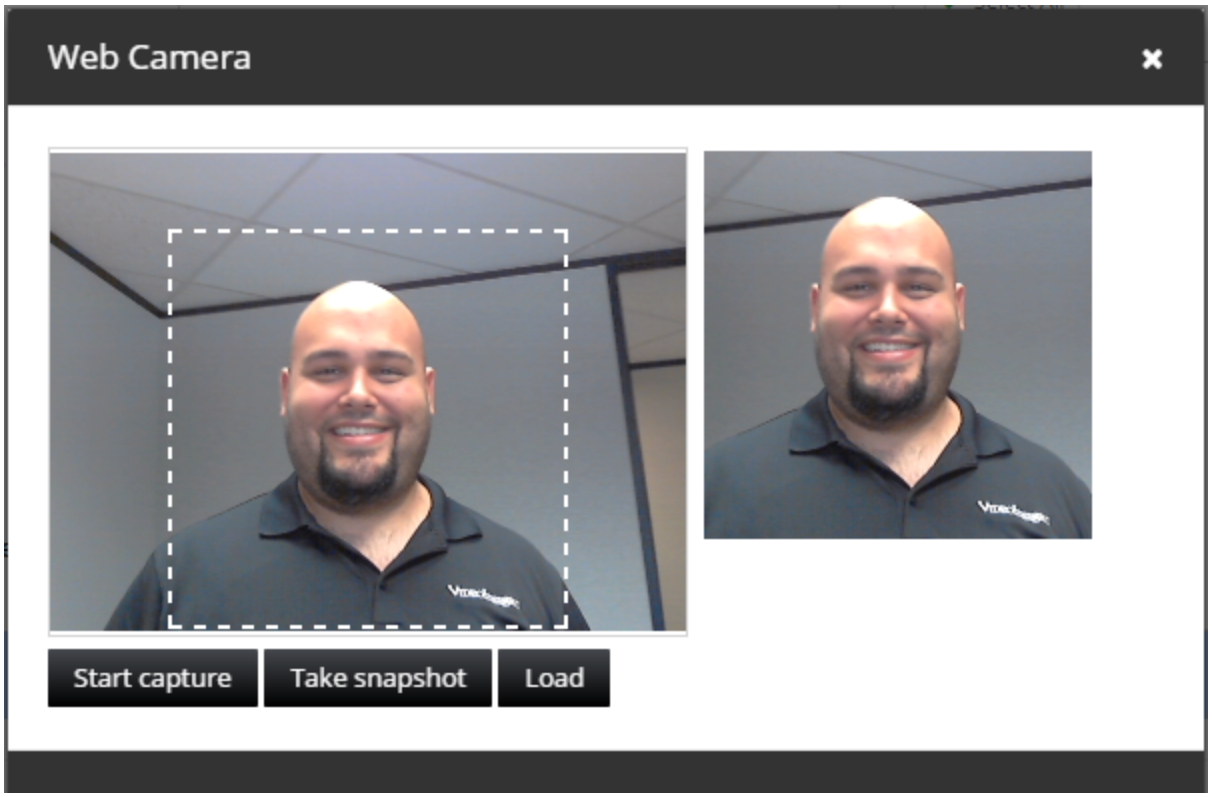


Required fields include:

- First name
- Last name
- Active date
- card number

To add a photo, click on the photo frame *or* select the (+) sign within the window. A snapshot can also be used from a camera device connected to the PC by selecting the camera icon. This action uploads the snapshot to the database for repeated use, until altered at another time.

To capture an image from a web cam, click on the photo icon. A new box appears which begins the capture process. Snapshot the image and attach it to the record. The image within the white, dotted-box is the image that will be saved to the personnel record.



A photo can also be uploaded by browsing to a known file location and then selecting Open. Browse to the photo's file location and select the desired photo. Allow the window to refresh and a photo will be attached to the record upon saving. This cardholder (user) can also be assigned to a specific personnel group and/or granted specific access levels if desired.

Additional details can be managed by expanding the **More Details** section at the base of the setup page. There it is possible to enable editing the *ENABLE ADA settings*, *Card Use limit count*, *employee_ID*, *contact details* and *address information*.

To assign a ADA setting to a cardholder, select the checkbox **Enable ADA settings**. This setting allows for extended access-granted and door-held open times, which can be configured in the Hardware Configuration settings.

Card Use Limit is used to impose a limit on the number of instances that a card can be used.
For example, if a personnel card can only be used 10 times, the number setting should be listed as '10' in the settings. After the 10 card readers are used, an *Access Denied* will be displayed on the User **Dashboard** and **Basic Report**.

Event Date Time	Event Type & Description	Name	Picture	Address	Device Name
04/08/2016 12: 49: 59	Access Denied Access denied - use limit	Jason Garcia		5.1.R1	Bldg B R1

Note: To utilize Use Limit, the setting must also be changed in the **Hardware Configuration** > **Advanced Reader settings** > **Enable Use Limit**. Each reader must be configured to enable this specific setting in order to be effective.

Editing and Searching

Locating a personnel cardholder is done by using the **Search** option above the left navigation window. Use the search box for locating first or last name of the person. The left navigation will filter the search results actively. To edit a card, click the name of the personnel and make changes to the form.

Click **Save** to apply the desired changes.

The **Save & New** option allows the current record to be saved, and subsequently clear the screen to start a new record. This option is useful when editing is utilized before creating a new record.