MILESTONE ACCESS CONTROL MANAGER (ACM) INTERFACE

Document created with reference to Integriti Professional software version v4.3.1.10384

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Integriti Milestone ACM Interface

Table of Contents

This document details the installation and setup processes to configure Milestone ACM integration with Integriti. Please refer to Milestone documentation for help setting up Milestone.

Description

Integriti's high-level interface with Milestone's ACM is IP-based and bi-directional. ACM integration allows Milestone to be the single master "head end" security management platform, whereby Integriti functions as an access control and security sub-system. Cardholder information, alarms and events, as well as door and area statuses in Integriti are sent in real-time to Milestone. Operators are therefore empowered to effectively manage their security operation by seamlessly monitoring Integriti alarm and access points through Milestone. Operators may also unlock/lock doors and arm/disarm areas with the added ability to associate doors to cameras in Milestone, thus facilitating efficient situational awareness and immediate visual verification of alarms.

End-User Benefits in Milestone

Through the Milestone XProtect Smart Client, end-users may:

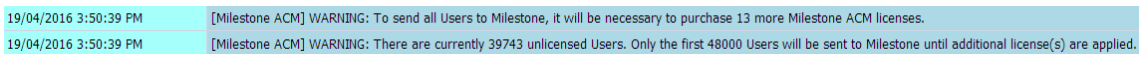
1. **View** access control operational events.
2. **Control** doors.
3. **Display** and manage video related to access control events.
4. **Display** alarms from the access control system.
5. **Full map overview** control of doors and access points.
6. **Search** for events, video or information associated to specific doors or cardholders.
7. **Immediate visual validation** of people requesting access.
8. **Manage** cardholders.
9. **Track** passages in real-time.

Milestone ACM License

Each instance of the Milestone ACM licenses allows integration of 3,000 users and 100 doors. Multiple licenses may be purchased to meet the required number of users and doors. A Review messaged is logged in Integriti stating how many additional licenses are required should there be an insufficient number of licenses. For example, the Review message might say:

"[Milestone ACM] WARNING: To send all Users to Milestone, it will be necessary to purchase 13 more Milestone ACM licenses.

Milestone ACM] WARNING: There are currently 39743 unlicensed Users. Only the first 48000 Users will be sent to Milestone until additional license(s) are applied."



Milestone also license their Access Control integration. Please ensure the appropriate number of Milestone Access Control door licenses are purchased.

ACM Integration vs Traditional CCTV Integration

ACM integration uses two plugins and allows Milestone to be the "head end" security management system. ACM integration is completely different to the traditional Milestone CCTV integration and as such, ACM integration uses separate plugins and is licensed differently.

The traditional Milestone CCTV integration uses a single plugin and allows Integriti to be the master "head end" security management system. This integration is licensed through the normal CCTV licenses and has no relationship with ACM integration.

Typically, installations would not have both the ACM integration and the traditional CCTV integration at the same time. An ACM integration license does not license the traditional CCTV integration and vice versa, the traditional CCTV integration license does not license ACM integration. Care should be taken to ensure the correct license is purchased. Should both ACM integration and traditional CCTV integration be required at the same time (i.e. to allow either system to be the "head end"), both ACM integration licenses and normal CCTV integration licenses will need to be purchased.

Technical Functions

The integration supports the following functions:

Retrieval of Information from Integriti

- Retrieve Integriti Users in Milestone
  - Name, Photo and ID fields.
  - Search Users by name.
  - Milestone automatically updates Users from Integriti every hour (or manually via the "refresh configuration" option in Milestone).
- Retrieve Integriti Doors in Milestone
  - Name, Status (locked, unlocked or error) and ID fields.
- Retrieve Integriti Areas in Milestone
  - Name, Status (armed or disarmed) and ID fields.
- Retrieve Integriti Controllers in Milestone
  - Name, Status (connected or disconnected) and ID fields.

Status Updates and Events from Integriti

- Live status updates in Milestone
  - Doors, Areas and Controllers.
  - Includes changes to status icon in Milestone as well as an event.
  - Manual update and automatic re-sync of status also supported.
- Live receiving of Integriti access events in Milestone
  - Includes access granted and denied events.
  - Displays associated door and associated user (if available), as well as time and actual Integriti Review event message.
- Live receiving of Integriti alarms/events in Milestone
  - Integriti alarms/events come into Milestone as an event and are displayed within Milestone's Alarm Manager.
  - Filtering options restrict what type of alarms/events get sent to Milestone.
  - Automatic synchronisation of buffered alarms/events.

Control Integriti Items

- Control Integriti items through Milestone
  - Doors: lock, unlock or unlock for a time. The unlock time can be customised or left as the default (5 seconds).
  - Areas: arm or disarm.

Additional Features

- Other Milestone features
  - Associate doors with Milestone cameras.
  - Display doors and areas within Milestone maps.

Programming Integriti items (such as Users, Doors etc) through Milestone is not supported with the exception that a photo may be assigned to a User through Milestone. This photo, however, will not be written back to Integriti.

General Notes

The term "users" and "cardholders" are interoperable. Integriti generally uses the term "users" and Milestone generally uses "cardholders".

Restarting the Milestone Event Server Service

Every time the Milestone Event Server service is restarted, the Event Server connects to Integriti and performs a full synchronisation of all objects. This is the same as the "refresh configuration" process. The update process can take several minutes depending on how much information needs to be synchronised, particularly if Integriti hosts a large User database. As such, the Integriti Access Control plugin/module will not appear in the Milestone Management or Smart Client until the synchronisation is complete. Do not be alarmed if the Access Control module does not appear in Milestone, please close the Milestone application(s), wait a few minutes and then re-open the Milestone application(s).

Alarm Management and Automation

The integration between Integriti and Milestone allows alarms/events in Integriti to be pushed into Milestone. Integriti alarms/events that are received into Milestone can be used to activate alarms/events or trigger a plethora of automated actions within Milestone. For example, an intruder alarm in Integriti can be used to automatically display multiple CCTV camera feeds, increase the recording framerate of these cameras and turn a PTZ to a pre-set position.

Integriti Milestone ACM Plugins

The Integriti Milestone ACM plugins were built and tested against Milestone XProtect Corporate 2016 (10.0a) and MIP SDK 10.0. Other versions of XProtect that support Access Control Manager and MIP SDK 10.0 should also work but have not been explicitly tested.

Two Milestone ACM plugins are required to be installed – one for Integriti and the other for Milestone, as detailed further below.

Integriti Professional version 4.3.1 or later and the "Milestone Access Control Manager (ACM) Integration" license (part number 996939) are required. Multiple instances of the Milestone ACM license may be purchased to increase the number of integrated users and doors.

Installation

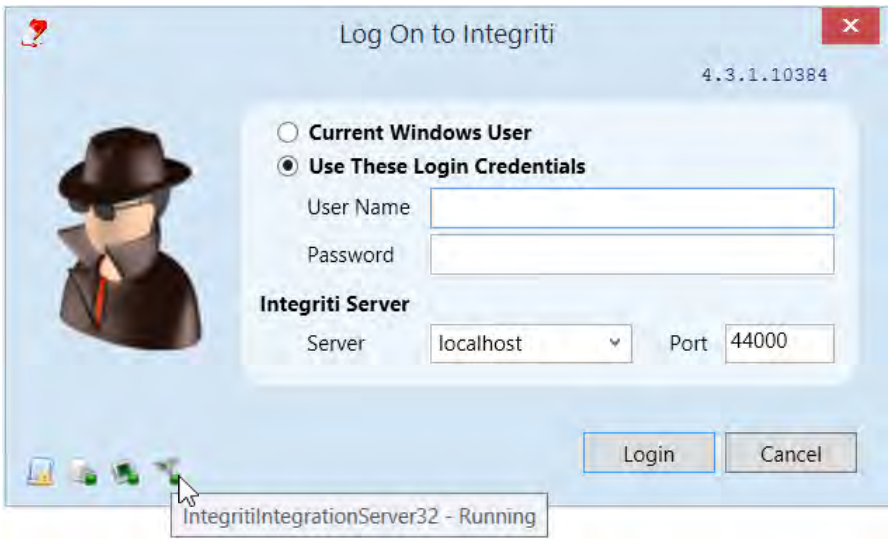
1. Installation in Integriti

Close all instances of the Integriti software suite.

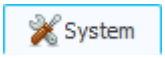
Download and run the "Integration MilestoneACMServer" plugin installer on the Integriti Integration Server.

Integration_MilestoneACMServer_Plugin_1.0_(10170).exe

After the installation has completed, restart the Integriti Integration server service. On the Integriti server, start the Integriti System Designer as an administrator. Right-click the Integration service icon on the bottom left of the login dialog to stop and start the service. Alternatively, the Integration service can be controlled through the Windows Services management window.

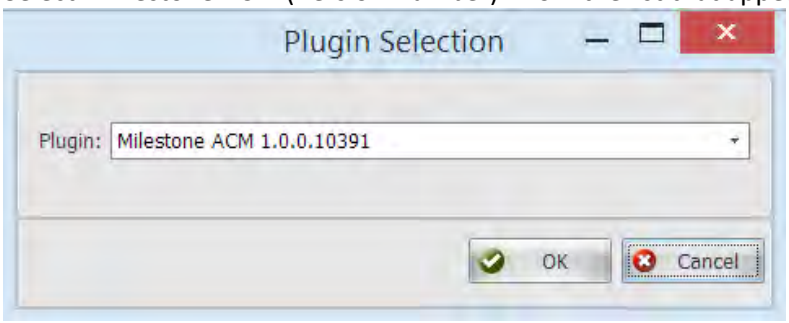


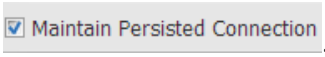
To configure the ACM integration settings in Integriti, log into System Designer and follow these steps:

1. Click on the 

tab followed by 

2. Select “Milestone ACM (Version Number)” from the list that appears and click OK.

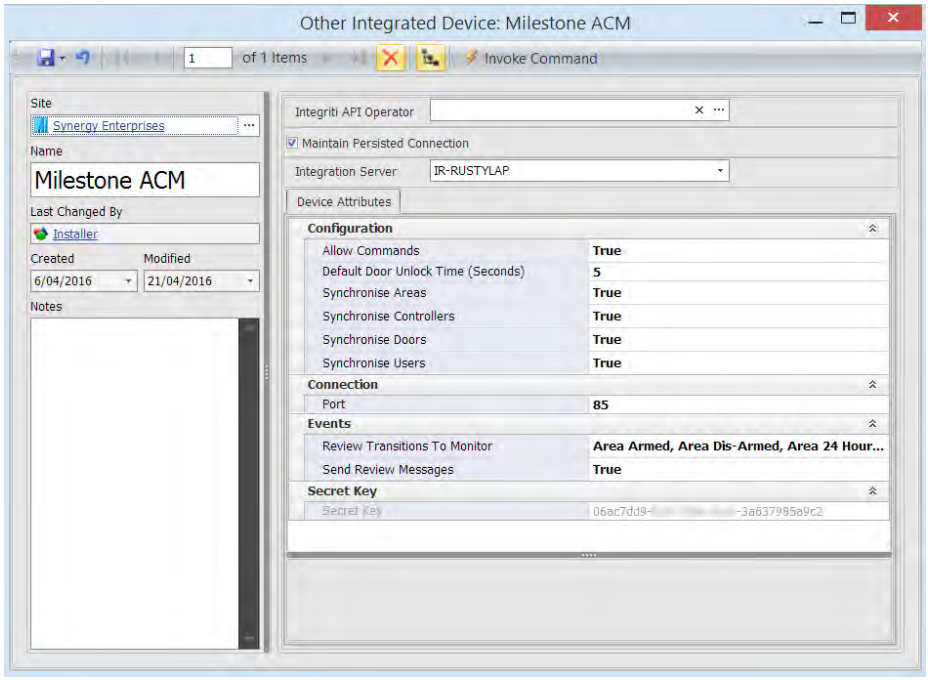


3. In the editor window that appears, name the integration module.
4. Optional: Assign an Integriti API Operator to this integration module. The assignment of an Operator allows the integration to be restricted based upon the permissions of that Operator. For example, if the assigned Operator only has permission to view Users in “Site A”, then only those Users could potentially be synchronised with the Milestone system, or if the assigned Operator only has permission to view a certain number of doors, as opposed to all doors, then only the certain number of doors will be integrated with Milestone. The Integriti API Operator field can be left blank and no Operator permission restrictions shall be applied to the interface.
5. Tick the ‘Maintain Persisted Connection’ tick box above the Device Attributes tab. 

. This must be ticked for the interface to work.
6. Allow Commands must be set to True to allow the Milestone ACM server to perform commands on the Integriti system (e.g. unlock a door).
7. Synchronise Areas must be set to True to enable the synchronisation of Areas in Integriti with the Milestone ACM server.
8. Synchronise Controllers must be set to True to enable the synchronisation of Controllers in Integriti with the Milestone ACM server.
9. Synchronise Doors must be set to True to enable the synchronisation of Doors in Integriti with the Milestone ACM server.
10. Synchronise Users must be set to True to enable the synchronisation of Users in Integriti with the Milestone ACM server.
11. Choose the port number to receive requests from the Milestone server. This is the TCP port number that the Integriti server will listen on. The default is port 85 and the port must match the port settings in Milestone. If the port number is changed at a later time, the port number must be updated to match in both Integriti and Milestone. Ensure no firewalls are blocking the specified port.
12. Select the types of Review Transitions to send to Milestone. By default all Review Transitions are selected. The list of Review Transitions directly equate to “Events” in Milestone. At a later stage, a corresponding Alarm Definition will need to be created in Milestone for the event to appear in Milestone’s Alarm Manager.

13. Send Review Messages must be set to True for Integriti to send details of new Review messages to the Milestone event server. This is necessary to receive events and state changes in Milestone, e.g. door has been unlocked.
14. The Secret Key must be copied and entered into the Milestone ACM settings when at that stage.

The following screenshot displays an example summary of the completed Milestone ACM interface settings in Integriti.

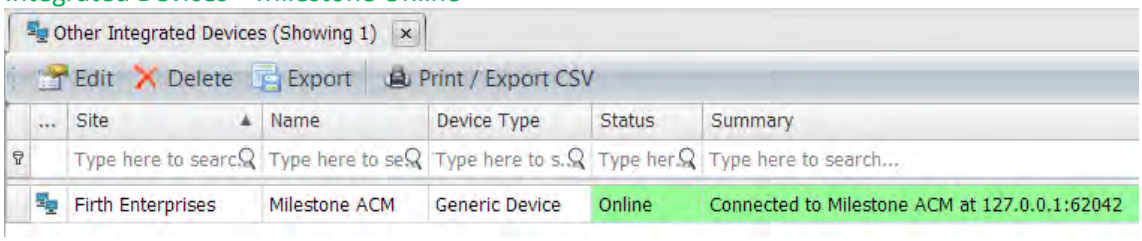


15. Save and close the Integrated Device window.

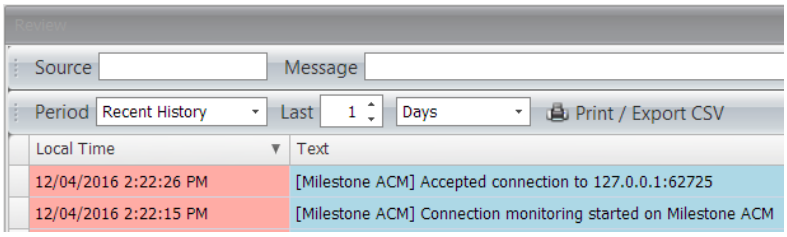
Connection Heartbeat and Monitoring

If the configuration settings are correct and there is successful communication with the Milestone Event Server, the Milestone Integrated Device status will appear Online and Review messages will be logged in Integriti. If the connection details are incorrect or if the connection between the Integriti Integration service and the Milestone Event Server service has dropped, the Milestone Integrated Device status will appear Offline and Review messages will be logged. An example of these can be seen below.

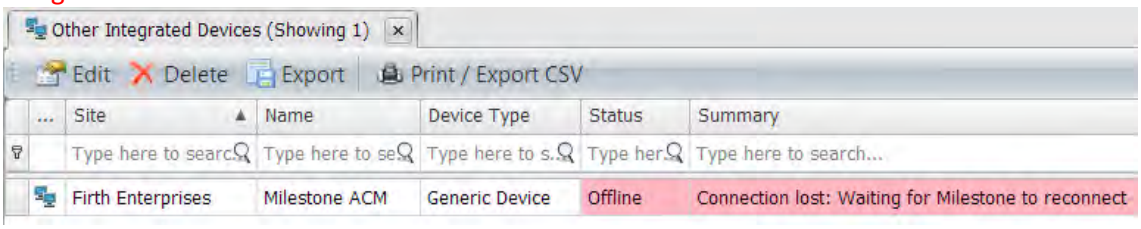
Integrated Devices – Milestone Online



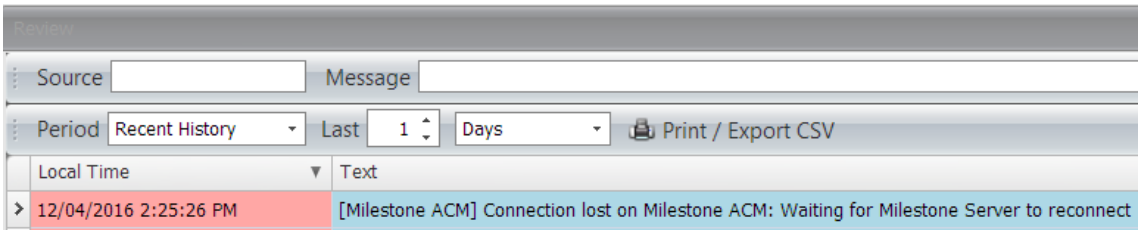
Review – Milestone Online



Integrated Devices – Milestone Offline



Review – Milestone Offline



The interface supports heartbeat connection monitoring. A heartbeat message is sent from Milestone to Integriti every 60 seconds. If Milestone does not receive a response from Integriti within 60 seconds, the TCP connection will be dropped by Milestone. Integriti too will drop the connection if Integriti has not received a heartbeat within 180 seconds. Until Integriti knows that it has lost connection with Milestone, Integriti will not be able to start receiving a new connection. After 180 seconds, Integriti will automatically attempt to re-connect to Milestone either on the next heartbeat or when the next request is sent.

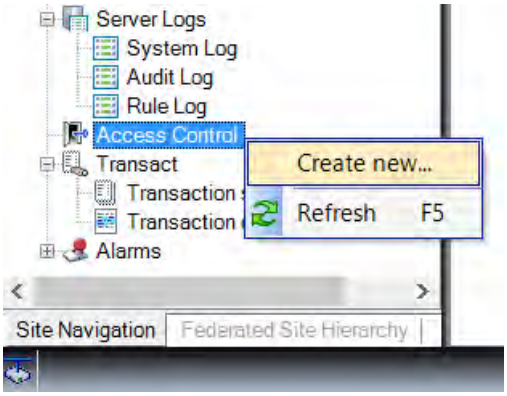
2. Installation in Milestone

Download and run the “Integration IntegritiMilestoneACM” plugin installer on the same machine as the Milestone Event Server. It may be necessary to close any open Milestone software and stop the Milestone Event Server before installing.

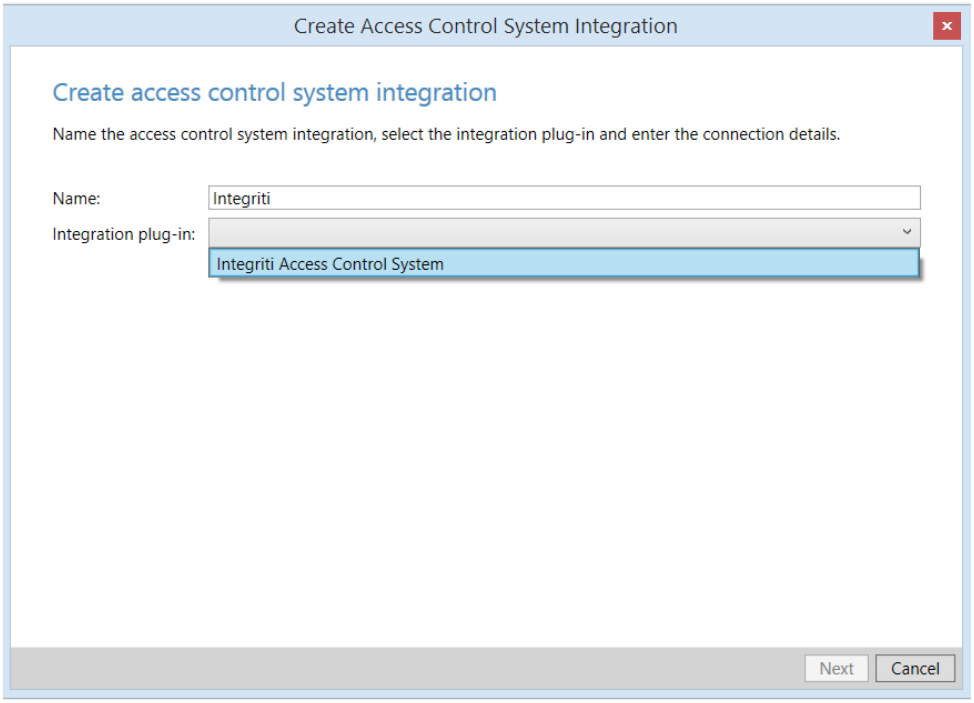
Integration_IntegritiMilestoneACM_Plugin_1.0_(10170).exe

After the installation has completed, restart the Milestone Event Server and Management Server services. These services can be controlled through the Windows Services management window.

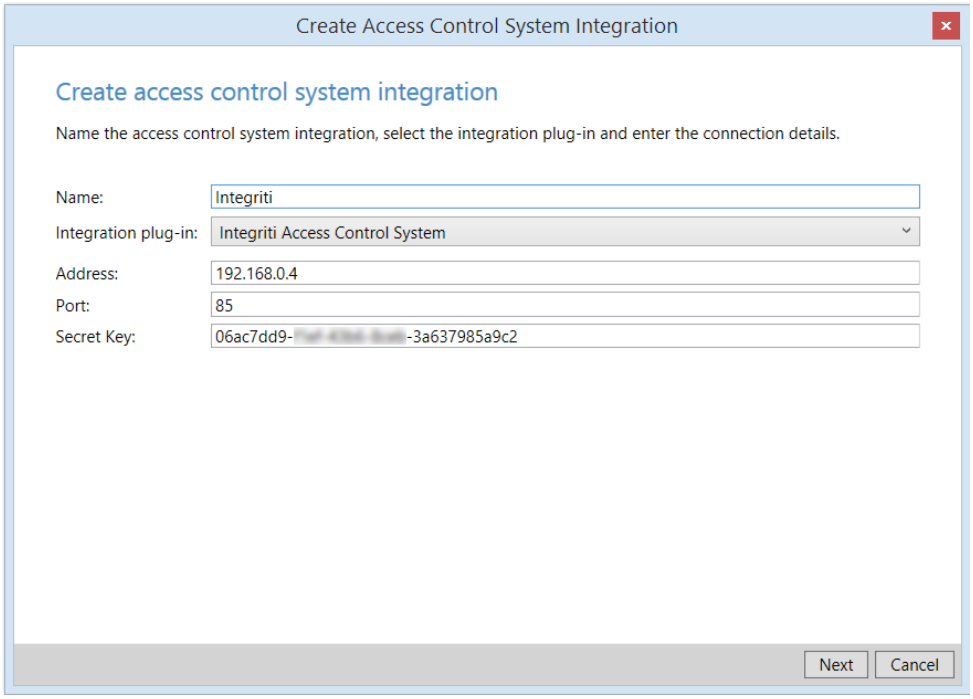
1. Open Milestone XProtect Management Client, right click on 'Access Control' and select 'Create New...'.



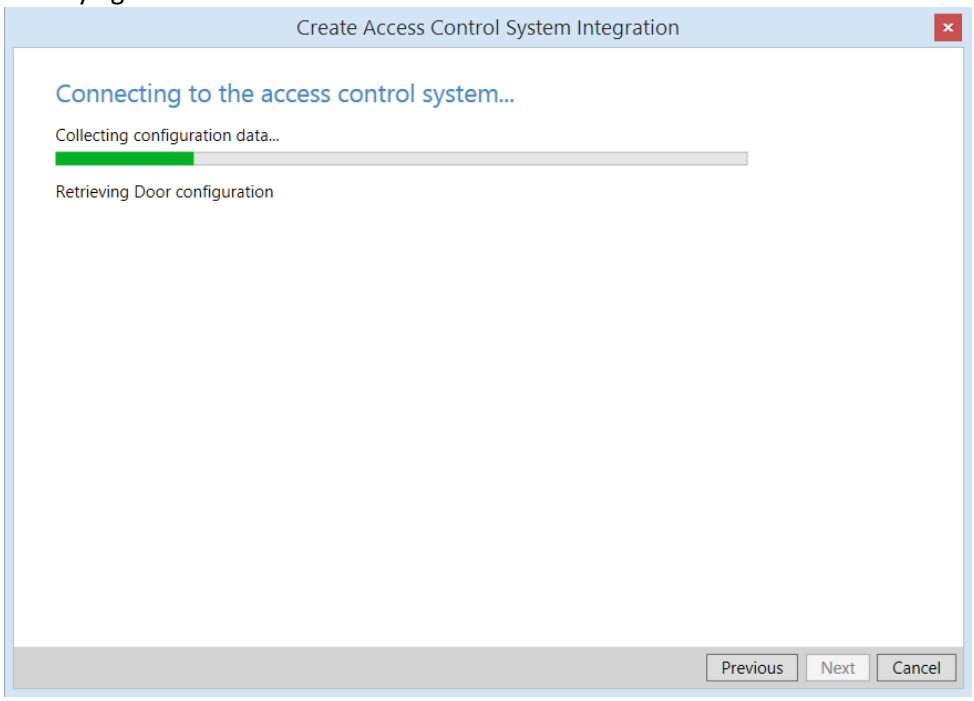
2. Name the Access Control Integration and select 'Integriti Access Control System' from the 'Integration Plug-In' dropdown box.



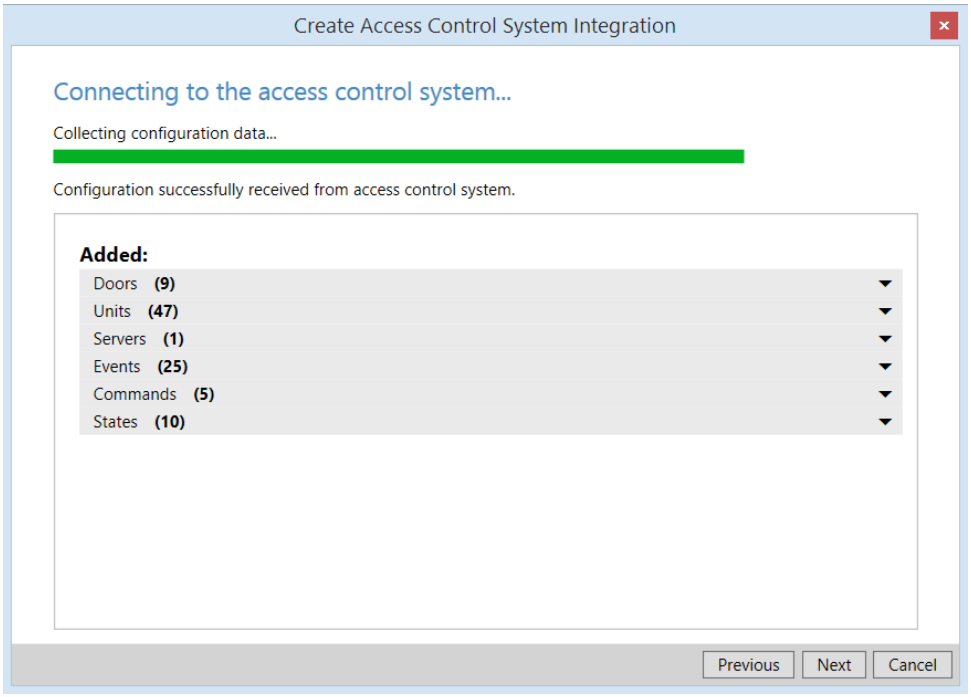
3. Enter the IP Address of the Integriti Integration Server.
4. Choose the port number to send commands to the Integriti server. This is the TCP port number that the Integriti server will listen on. The default is port 85 and the port must match the port settings in Integriti. If the port number is changed at a later time, the port number must be updated to match in both Integriti and Milestone. Ensure no firewalls are blocking the specified port.
5. Enter the Secret Key as displayed in the Milestone Integrated Device configuration settings in Integriti.



6. Press 'Next'. NOTE: The Integriti Integration Server must be running.
7. Milestone will then attempt to retrieve the configuration details from Integriti. This process should take less than 5 minutes. If the process takes longer than 5 minutes and appears to 'hang', close all Milestone applications and restart the Milestone Event and Management Server services and Integriti Integration service. Check connection details, ensure there are no firewalls blocking the connection and try again.



8. Once all configuration information has been retrieved, a summary will be displayed.



The following is an explanation of the summary configuration retrieved from Integriti as displayed above:

- **Doors** – the list of names of Doors in Integriti.
- **Units** – the list of Areas, Controllers, Access Points and Doors in Integriti. All Doors are assigned an "interior" and "exterior" access point to accommodate reader-in/reader-out Doors. The Integriti server is also displayed as a Unit.
- **Servers** – the Integriti Integration server and its IP address.
- **Events** – the list of all possible events Milestone can receive from Integriti. These Events directly correspond with Review Transitions in Integriti.
  - Area Armed
  - Area Dis-Armed
  - Area 24 Hour Armed
  - Area 24 Hour Dis-Armed
  - Area Deferred
  - Area Already Armed
  - Area Already Dis-Armed
  - Area Already 24 Hour Armed
  - Area Already 24 Hour Dis-Armed
  - Area Exit Cancelled
  - Door Lock
  - Door Unlock
  - Door Timed Lock
  - Door Timed Unlock
  - Door Lock Refreshed
  - Door Unlock Refreshed
  - Door Timed Lock Refreshed
  - Door Timed Unlock Refreshed
  - Door Timed Unlock Unnecessary
  - Door Error

- Door Override Cancelled
- Door Not Opened
- Door Opened (While Locked)
- Door Opened (Free Access)
- User Denied In
- User Denied Out
- User Granted In
- User Granted Out
- User Denied In (Passback)
- User Denied Out (Passback)
- User Granted In (Passback)
- User Granted Out (Passback)
- Global State Alarm
- Global State Tamper (Low)
- Global State Tamper (High)
- Global State Tamper
- Global State Isolate
- Global State Sealed
- Controller Connected
- Controller Disconnected

- **Commands** – the list of all possible commands Milestone can send to Integriti:
  - Lock Door
  - Unlock Door
  - Timed Unlock Door *(if no door unlock time is specified in Integriti, the default unlock time of 5 seconds will be used)*
  - Arm Area
  - Disarm Area
- **States** – the list of all possible device states Milestone can receive from Integriti:
  - Server Connected
  - Server Disconnected
  - Server State Unknown
  - Door Unlocked
  - Door Locked
  - Door State Unknown
  - Controller Connected
  - Controller Disconnected
  - Area Armed
  - Area Disarmed

9. Once the configuration has been retrieved from Integriti press 'Next'.
10. In the list of doors, optionally enable the doors that are to be used and associate Milestone cameras with them by dragging and dropping the cameras onto the appropriate Access Point within the door.

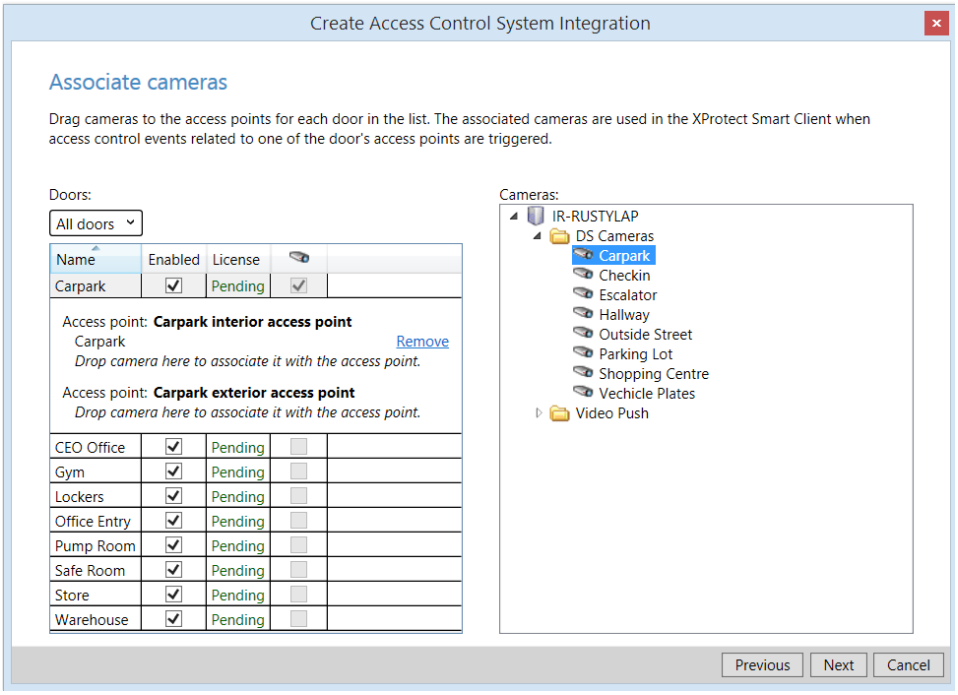
    An “Access Point” in Milestone is defined as a device that can be used to access a door. In Integriti, these map to a reader, hence there is one inside the door (interior) and one outside the door (exterior). In Integriti door programming, the reader on the inside of the door maps to the “interior access point” in Milestone,

and similarly, the reader on the outside of the door maps to the “exterior access point” in Milestone. Entry-only doors have only one reader and as such they are mapped to the outside/exterior access point.

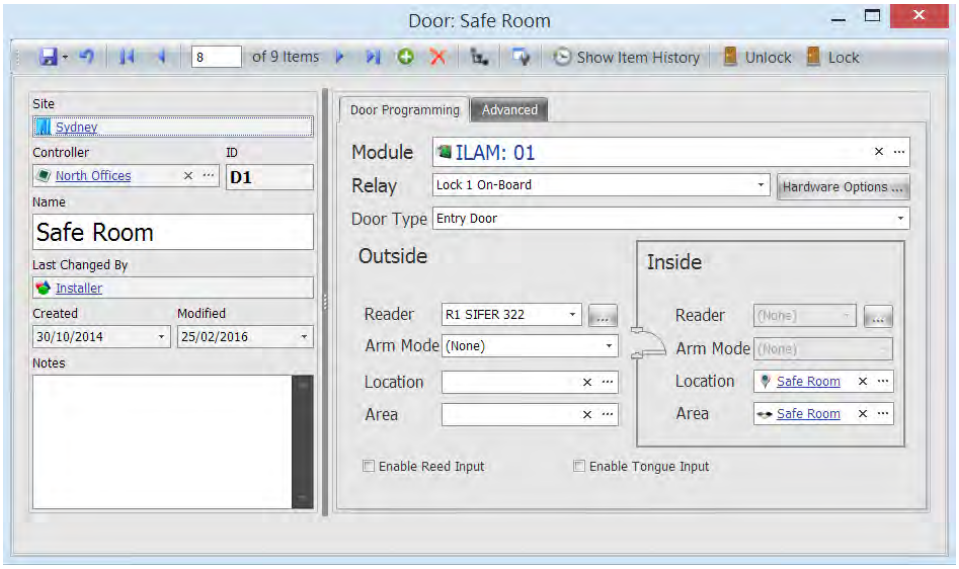
Regardless of whether the door is configured in Integriti as a “entry-only” or a “reader-in/reader-out” door, two Access Points will be displayed for each door. Simply ignore Access Points if they are not relevant.

Associating cameras with Access Points, whilst not necessary, provides additional features and helps personnel manage their security operation. Associations provide a convenient way of being able to directly view the camera at a given door. The association allows live and historic video to be displayed when an Access Point in Milestone is clicked upon, or alternatively, when an event occurs on the Access Point the operator can easily view the camera associated with that event. The same camera may be associated with multiple Access Points (e.g. in situations where the same camera views multiple doors). Conversely, multiple cameras may be associated with a single Access Point (e.g. in situations where multiple cameras view the one door).

In Milestone, Doors receive the locked and unlocked events, while an Access Point receives User events (User Denied, User Granted, etc) that occur on a card swipe.



Simply to underscore the notion of “outside” and “inside”, please refer to the screen shot below showing door programming in Integriti for an “entry-only” door. Note the Outside reader and that the Inside reader does not exist (greyed out). An Outside reader maps to an “exterior access point” in Milestone.



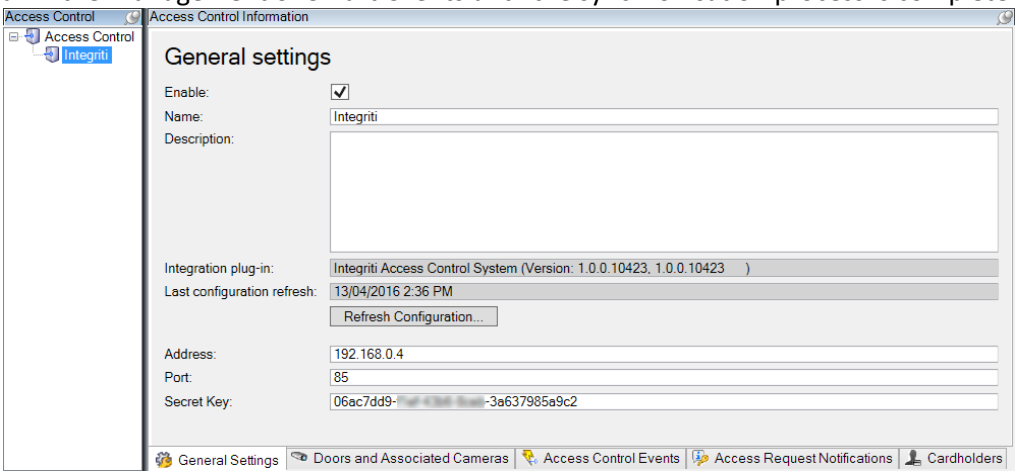
11. Press next and the Integriti ACM setup will be completed. This last process can take several minutes.

Milestone XProtect Management Client

General Settings

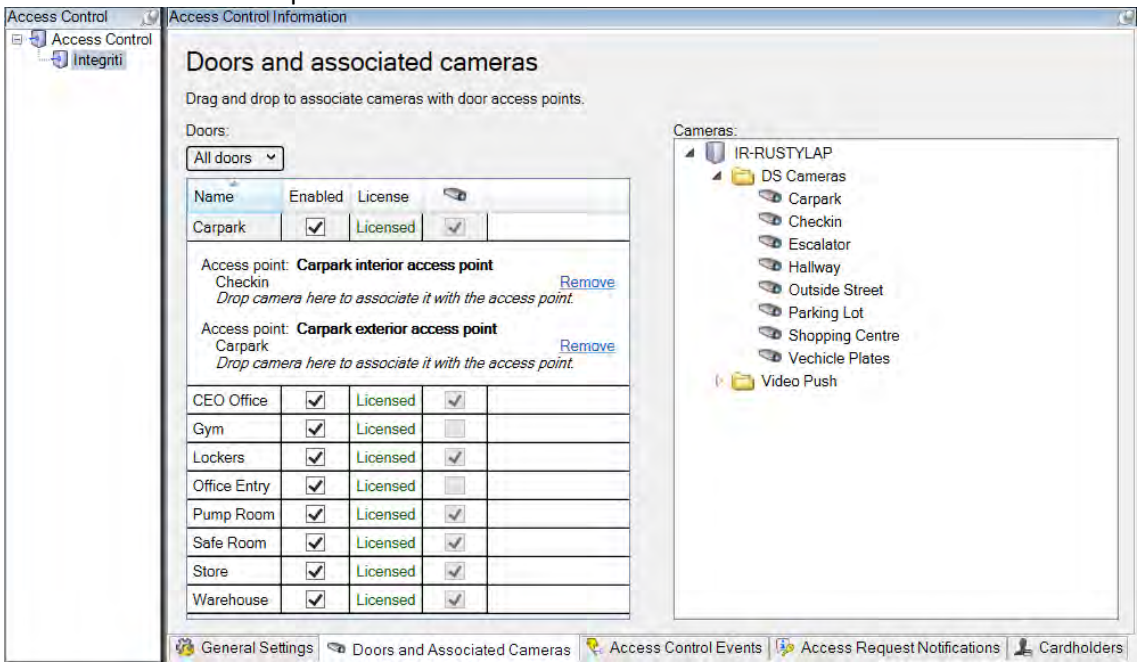
The general settings display an overview of the configuration parameters and plugin version number. The "Refresh Configuration" button updates the configuration data (Doors, Units, Servers, Events, Commands and States) from Integriti. Should changes be made to Doors, Areas or Controllers in Integriti, the "Refresh Configuration" button should be used to update those changes in Milestone. The "Refresh Configuration" should also be used whenever a new version of the Milestone ACM plugin is installed. "Refresh Configuration" will also update Users but this is not necessarily required as Users are automatically updated in the background every hour.

If the "Refresh Configuration" fails, restart the Milestone Event Server service and try again. As previously mentioned, it may take some time for the full synchronisation to complete after an Event Server restart and subsequently the Access Control module will not appear in the Management or Smart Clients until the synchronisation process is complete.



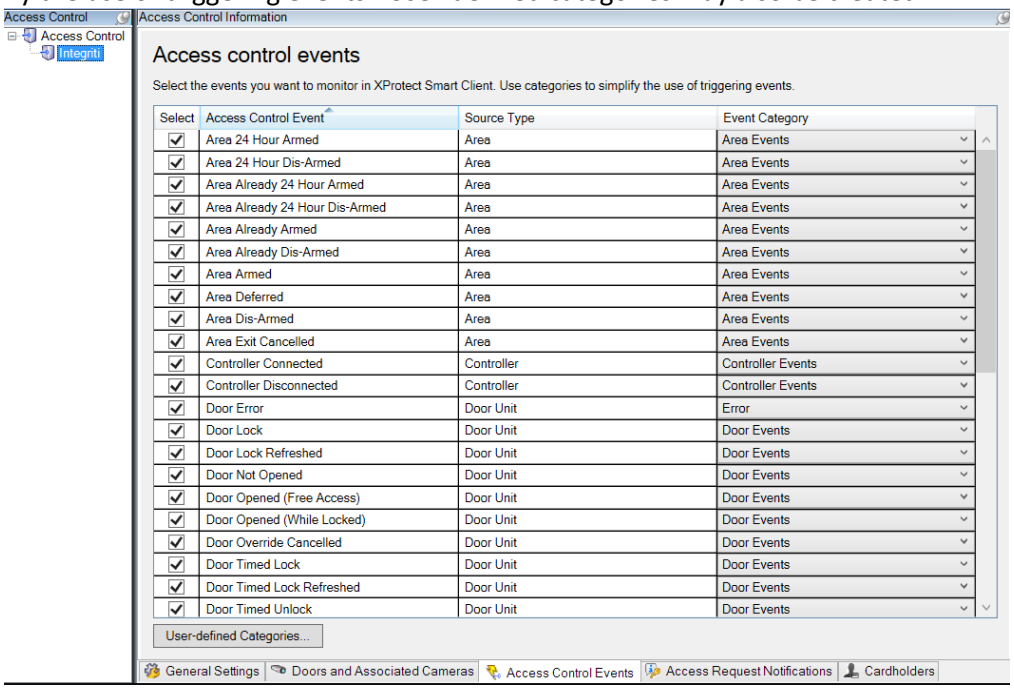
Doors and Associated Cameras

Map one or more cameras to each Access Point using drag and drop and see an overview of licensed and unlicensed doors. Please refer to step 10 under the "Installation in Milestone" section for a detailed explanation of door and camera associations.



Access Control Events

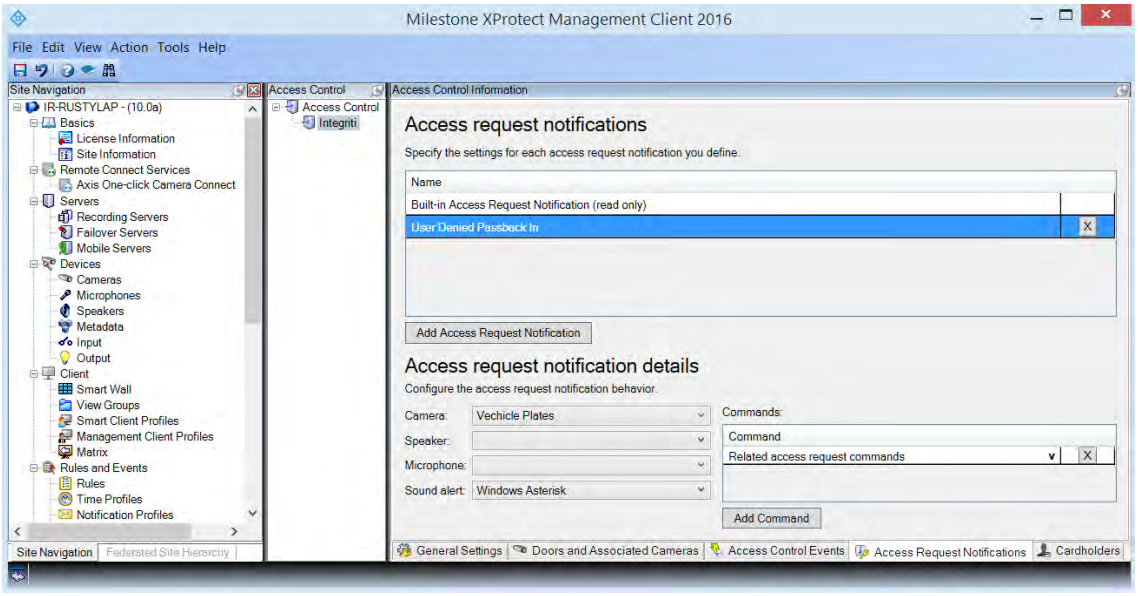
Optionally select the events to be monitored in the Milestone Smart Client. If an event has no category assigned the event will not come through to Milestone. Categories are used to simplify the use of triggering events. User-defined categories may also be created.



Access Request Notifications

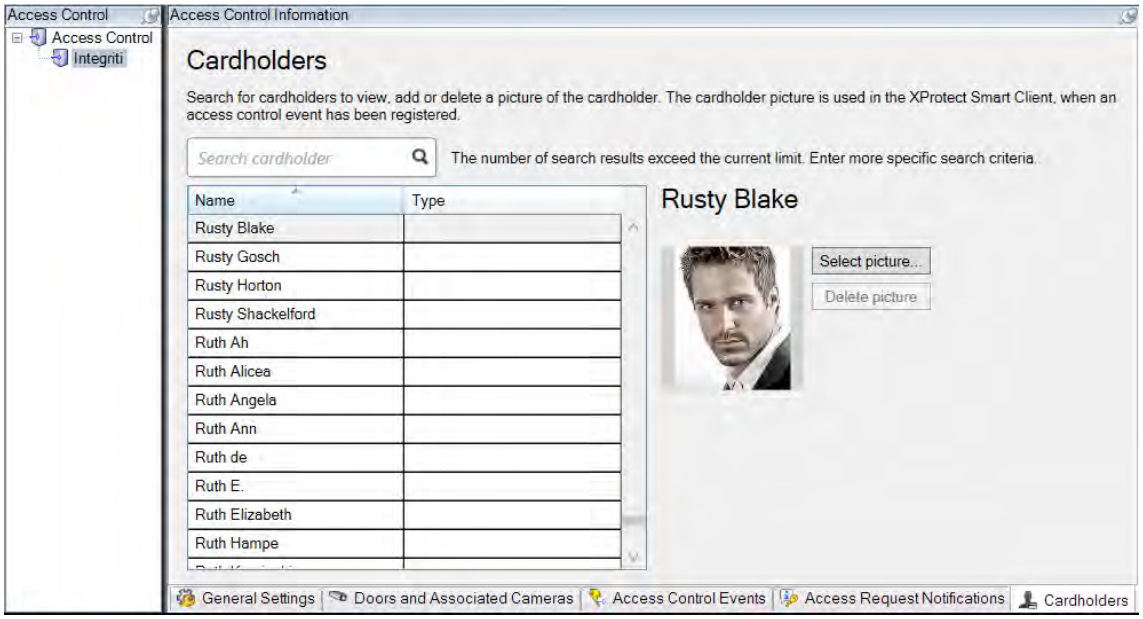
Access Request Notifications work as a “fly-in” or “pop-up” that appears over the top of the operator’s workspace. Similar to the “Challenge Response” feature in Integriti, when an event is triggered that generates this notification, for example a doorbell button is pressed or there is an access denied event, the request for access will be sent to Milestone for an operator to process instead of the door automatically opening. Whilst the Milestone Smart Client application will need to be open for the notification to appear, the Smart Client does not need to be the focus on the screen (i.e. the Smart Client can remain minimised). Access Request Notifications can be triggered by user defined events.

The Access Control Event will need to be in the “Access request” category for the event to trigger the notification. By default, “User Denied” events appear in the “Access request” category but this can be changed as necessary.



Cardholders

Search for cardholders to view, add or delete a picture of the cardholder. The cardholder picture is used in the Milestone Smart Client when an access control event has been registered. If a photo has already been assigned to a cardholder through Integriti, the photo will be displayed in Milestone. If necessary, the photo can be overwritten in Milestone but the updated photo will not be sent back to Integriti.



Alarms and Alarm Definitions

Alarms/events in Integriti are sent to Milestone based on the Integriti Review message. All alarms/events that match the selected "Review Transition" category are sent to Milestone. Refer to the configuration options within Integriti to selectively choose which types of alarms are sent by choosing the appropriate Review Transitions. Alert Definitions in Integriti are not required to be setup to send alarms to Milestone.

Only alarms/events that have an associated Area, Door or Controller will be sent to Milestone. If the alarm/event matches the selected Review Transition but does not have an associated Area, Door or Controller, the alarm/event will not be sent. This has been purposely designed to act as a filter so not all alarms/events are sent to Milestone. Whenever an alarm/event is sent to Milestone, the associated Area and/or Door ID is extracted from that alarm/event. The Area and Door units in Milestone have the same ID's as their Integriti counterparts, so when events are created in Milestone from an Integriti alarm/event, Integriti can directly provide Milestone the ID to associate the alarm/event with the correct Milestone unit. If an Integriti alarm/event has more than one associated Area, Door or Controller, there will be a new Milestone event for each entity.

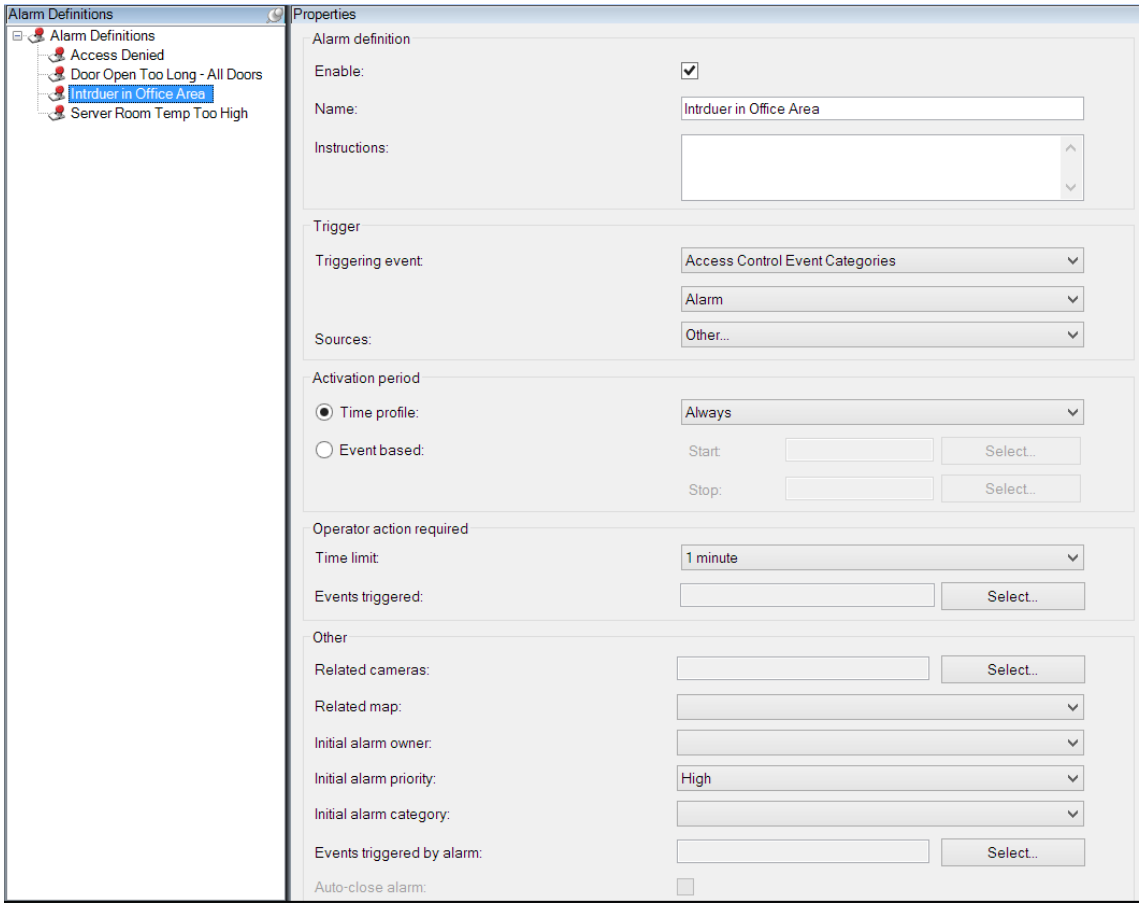
Should the Integriti and Milestone servers become disconnected, any alarms/events in Integriti will be buffered and then automatically synchronised with Milestone when the connection is re-established. This should help mitigate lost messages.

The process for displaying alarms/events in Milestone should be:

1. **In Integriti**: Generate an alarm/event and confirm this is displayed in Integriti Review. This may require configuration in Integriti, such as putting an input into an Area and ensuring the Area is armed.
2. **In Integriti**: Double-click the Review event, expand out "Other Details" and take note of its Transition.
3. **In Integriti**: Navigate to the Integrated Device settings for Milestone and ensure the relevant Review Transition category is checked. Should the Review event have

a Transition that is not displayed in this listing, the event cannot be sent to Milestone.

4. **In Milestone**: Navigate to the Milestone Management Client and create a corresponding Alarm Definition. Select "Access Control Event Categories" and then the appropriate sub-category. The source will display a list of Doors by default but this can be expanded out to include all Units (such as Areas etc).

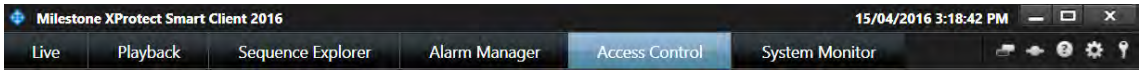


Troubleshooting

Ensure the alarm/event in Integriti has an associated Area, Door or Controller. If an Area or Door has recently been created click on "Refresh Configuration" in the Milestone Management Client so that Milestone receives the update. If Milestone does not have the ID of any newly created Areas or Doors, Milestone will not be able to receive events for that unit.

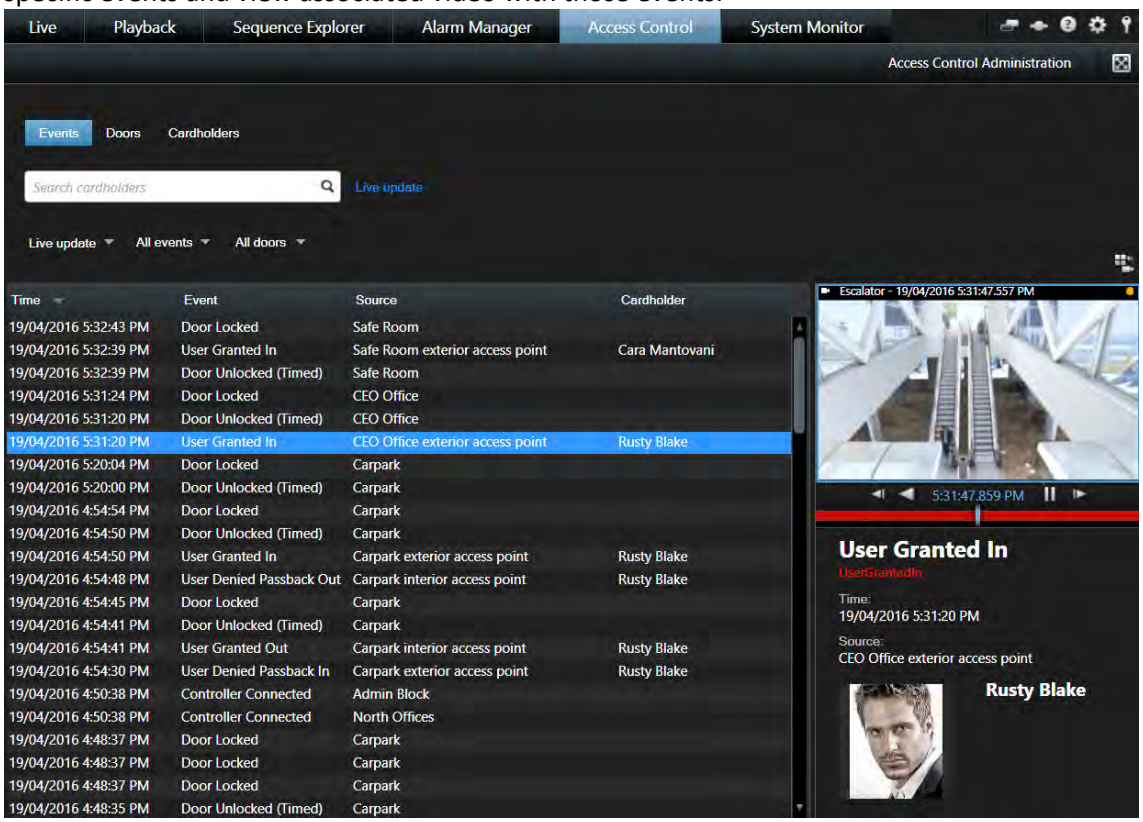
Milestone XProtect Smart Client

A dedicated "Access Control" tab is provided for optimised access control operations and investigations as well as providing a time-saving workflow and greater automation.



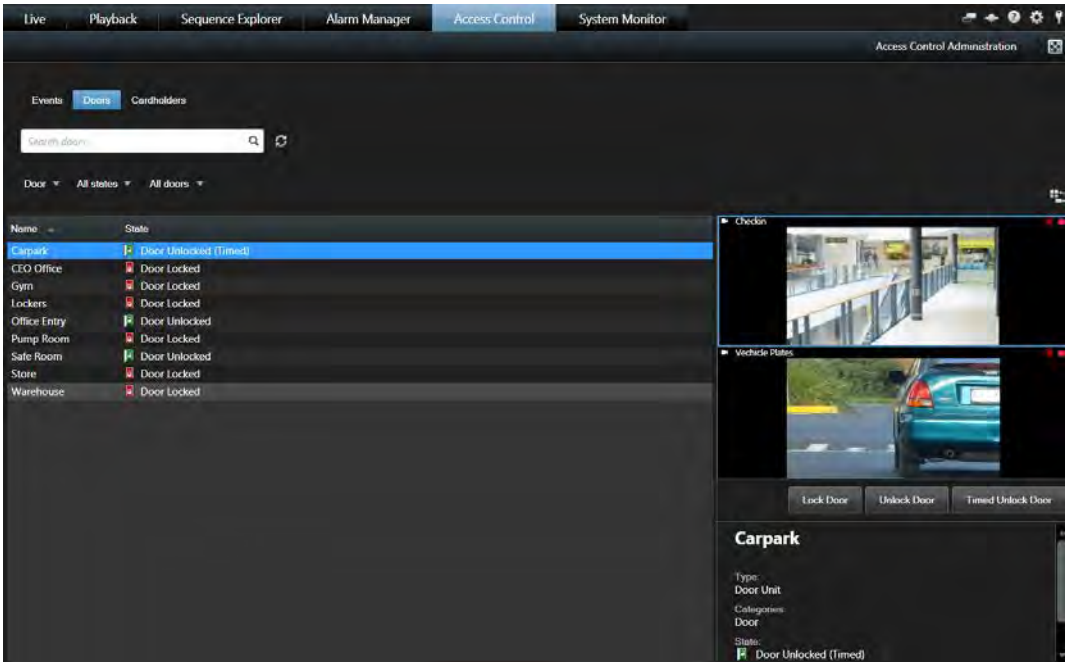
Access Control – Events

View events coming from Integriti, such as access control events, area arming/disarming, cardholder activity, server and controller connectivity and more. Easily use filters to search for specific events and view associated video with those events.



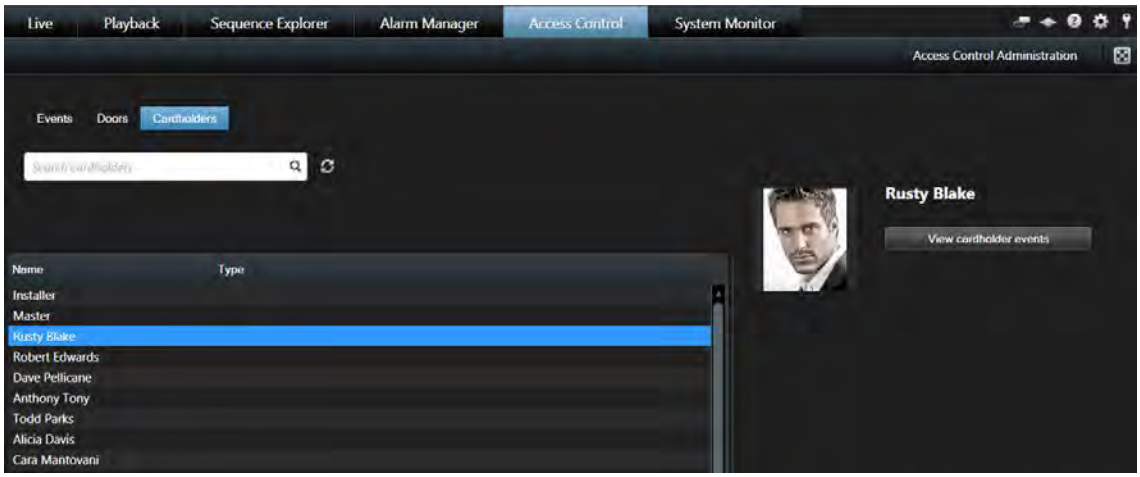
Access Control – Doors

List and search access control units, display the state of units, display associated video and control doors.

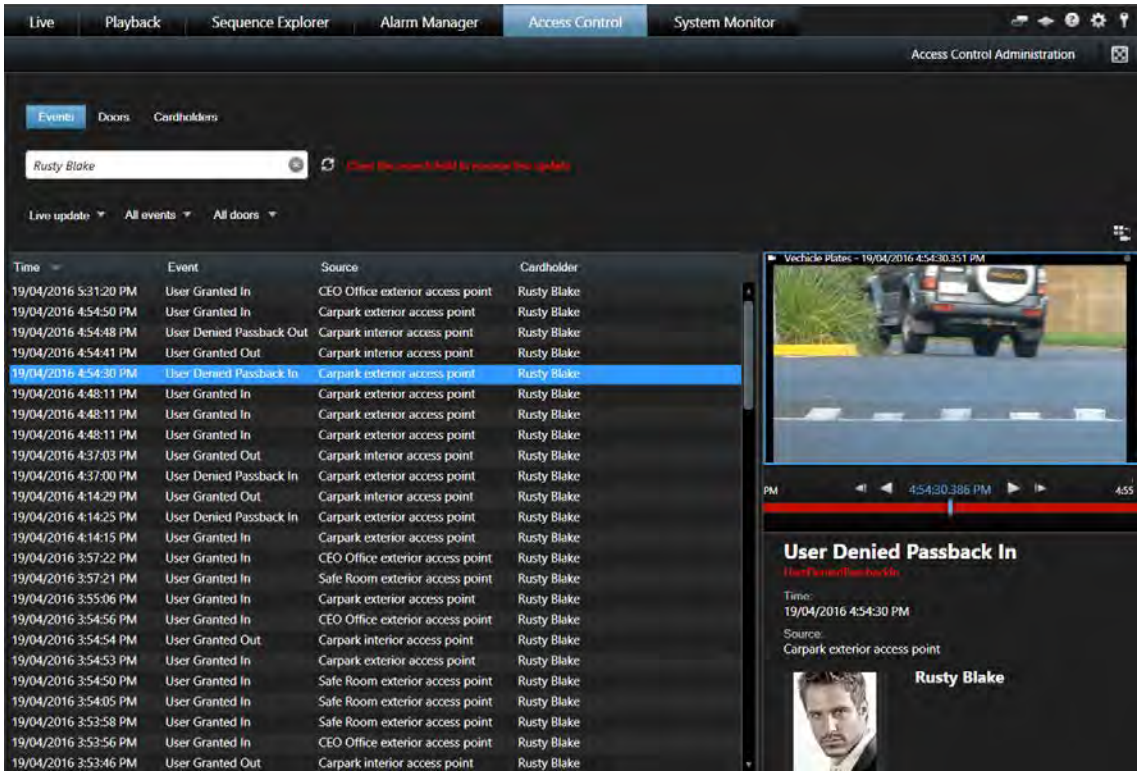


Access Control – Cardholders

View and search for cardholders. Apply or overwrite an image to a cardholder (images are not sent back to Integriti).

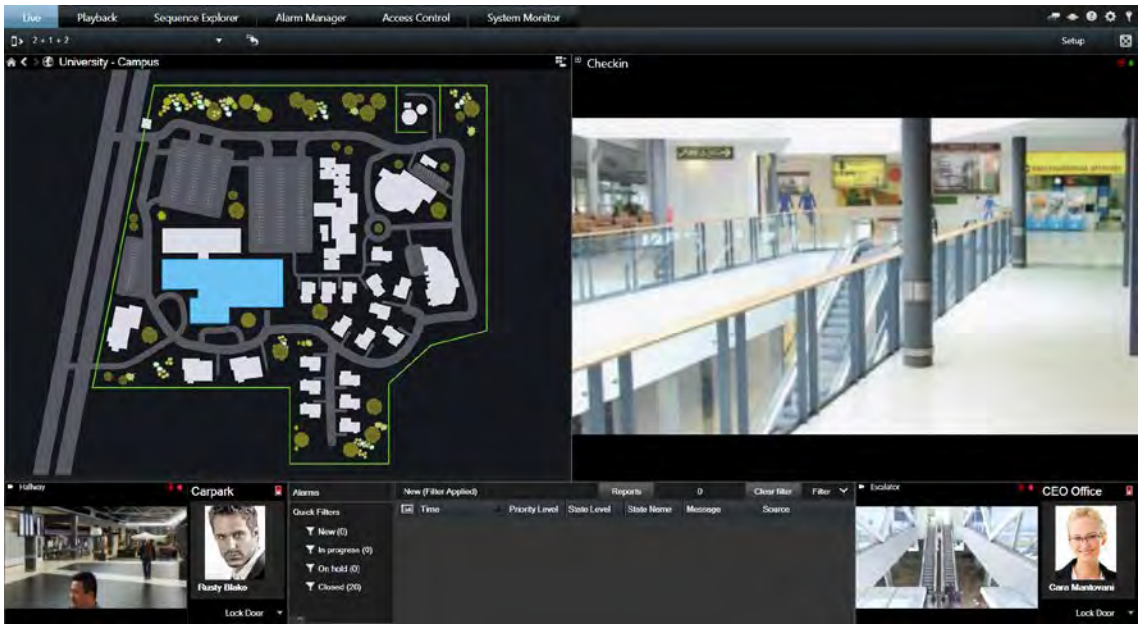


Click on the “View cardholder events” to activate an Event filter for that cardholder.



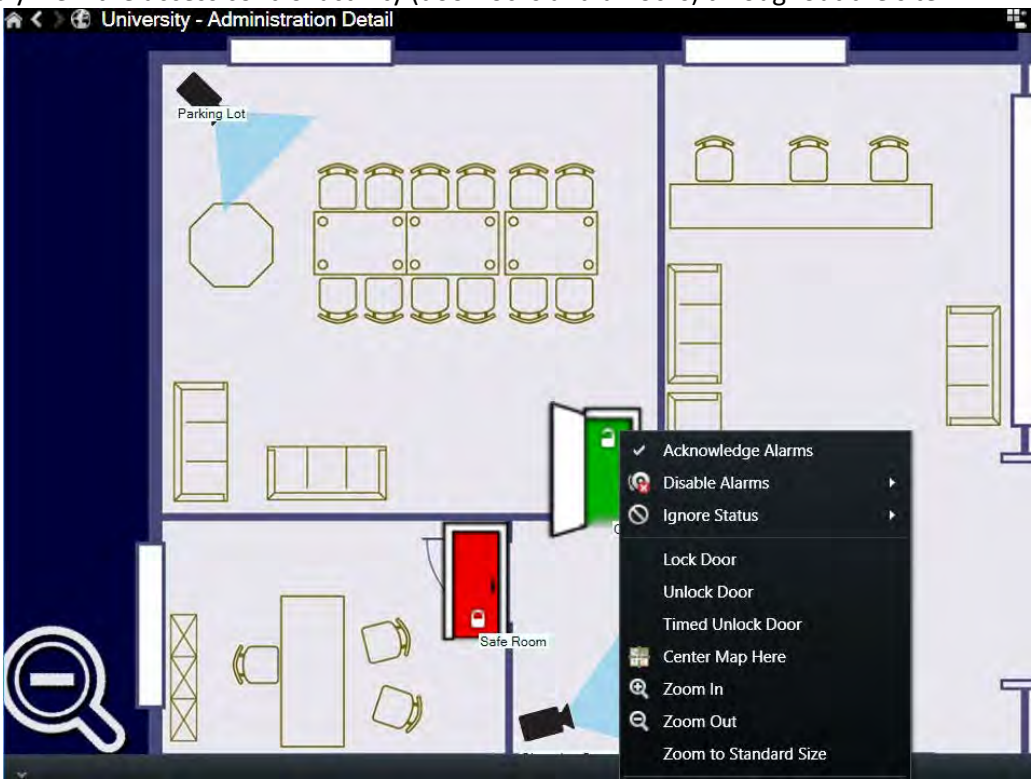
Live View

Monitor access points, view a listing of access events and cardholder information, view in-context investigation via independent playback and view overlay buttons for Access Control commands.



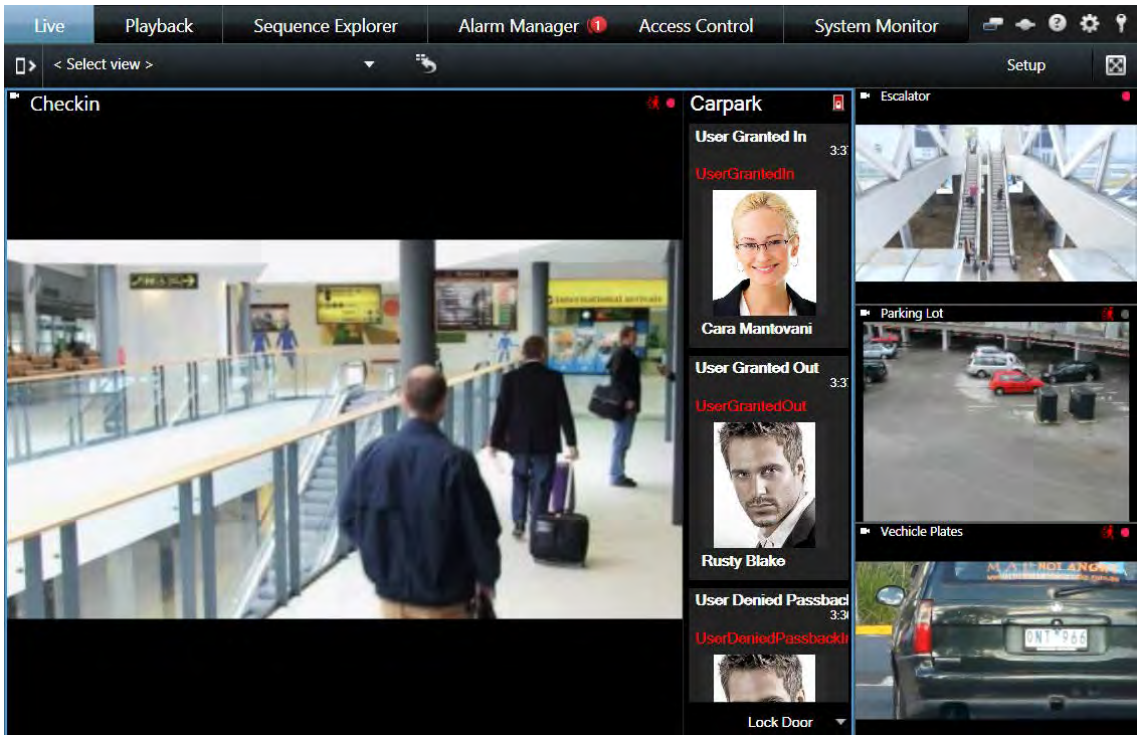
Graphical Maps

Manage access control devices via maps (lock/unlock doors) as well as view access control device status and display outstanding alarms. Maps update in real-time allowing operators to simply view the access control activity (door locks and unlocks) throughout the site.



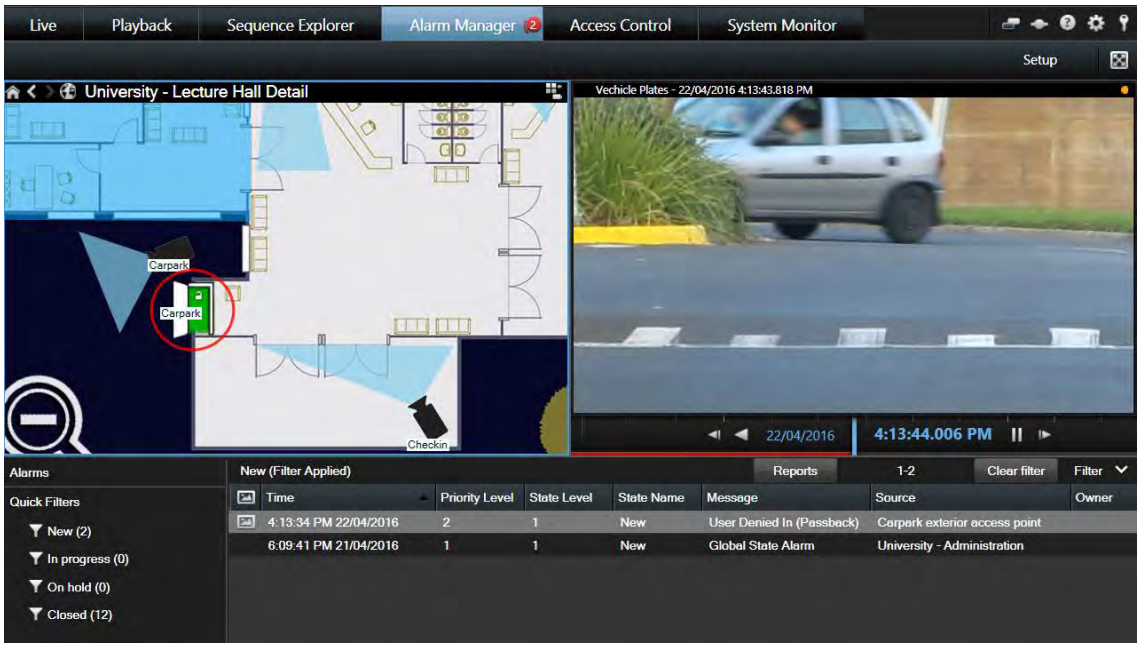
Access Monitor

Live listing of access control events with cardholder information. Door control commands are also displayed for easy access.



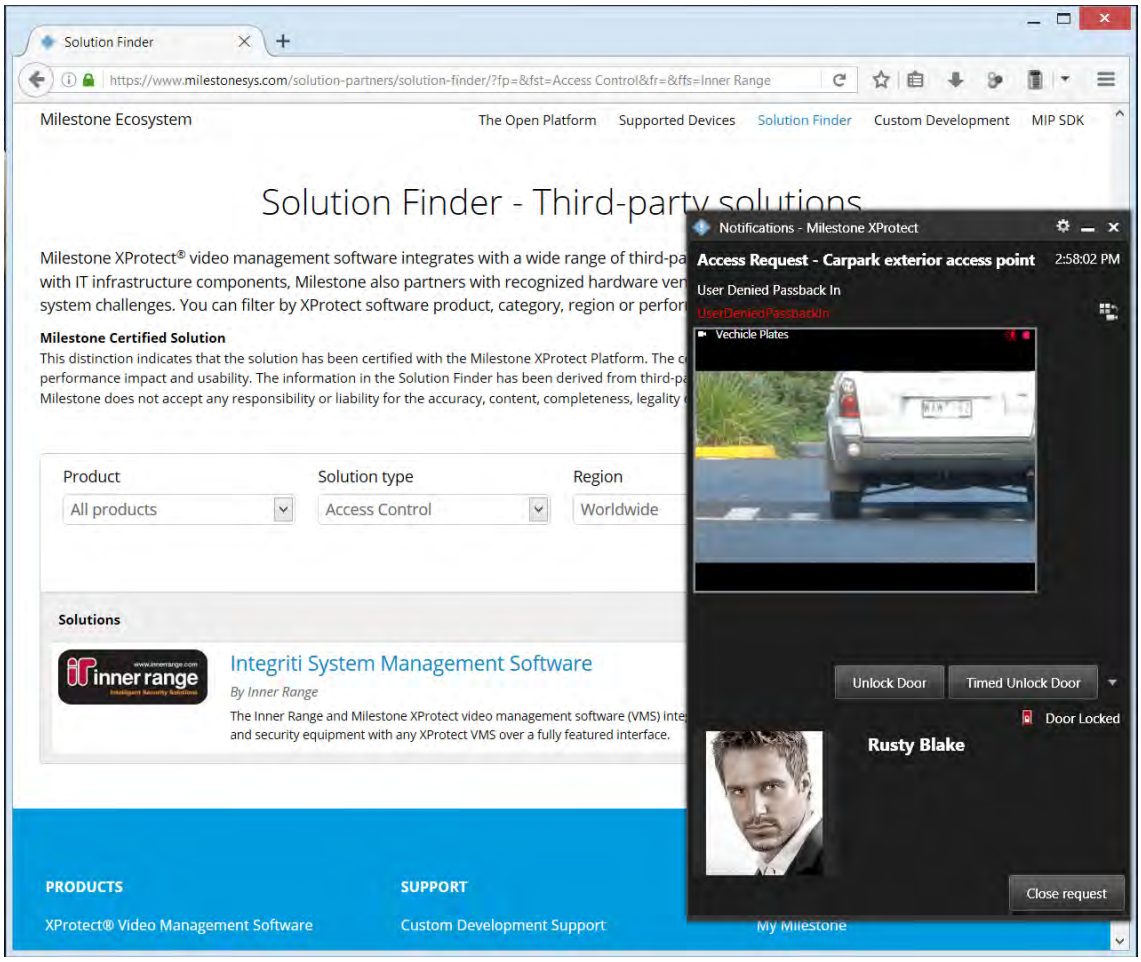
Alarm Manager

Alarms from Integriti are sent to Milestone and displayed in the Alarm Manager. View a list of events for doors and cardholder activities, search for events triggered by a specific cardholder, track personnel and preview video of events.



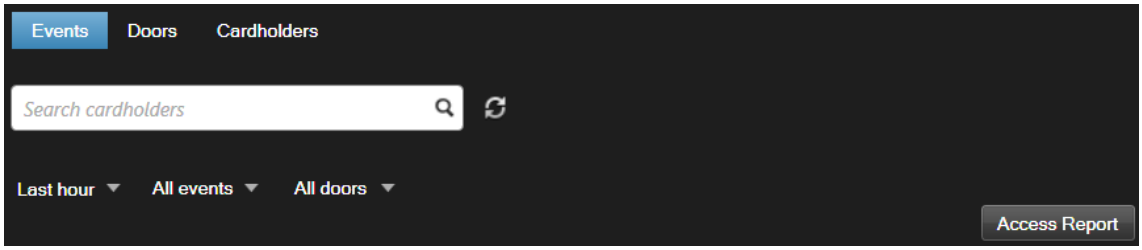
Access Request Notifications

The Access Request Notification appears as a pop-up over the operator's workspace when the requirement for an event is met, such as a door bell being pressed or an access denied event. View the event with the associated video and control the door.



Access Reports

Under Access Control → Events, whenever the time filter is set to anything other than "Live Update", the "Access Report" button is displayed. Generate an Access Report to create a PDF version of access history including the ability to filter the results of the report based on the selected event types and access doors.



Access Report

Period: 22/04/2016 2:57:24 PM -> 22/04/2016 3:57:38 PM
Event types: All events
Access units: All doors
Comment:

Time:	22/04/2016 3:57:35 PM	Vechicle Plates
Door:	Carpark	
Source:	Carpark exterior access point	
Event:	User Denied in (Passback)	
Reason:	UserDeniedPassbackIn	
Cardholder:	Rusty Blake	

Time:	22/04/2016 3:57:31 PM	Checkin / Vechicle Plates
Door:	Carpark	
Source:	Carpark	
Event:	Door Timed Unlock	
Reason:	DoorTimedUnlock	
Cardholder:		

Time:	22/04/2016 3:57:31 PM	Vechicle Plates
Door:	Carpark	
Source:	Carpark exterior access point	
Event:	User Granted in	
Reason:	UserGrantedIn	
Cardholder:	Rusty Blake	

Time:	22/04/2016 3:55:36 PM	Escalator
Door:	CEO Office	
Source:	CEO Office	
Event:	Door Lock	
Reason:	DoorLock	
Cardholder:		

Time:	22/04/2016 3:55:32 PM	Escalator
Door:	CEO Office	
Source:	CEO Office	
Event:	Door Timed Unlock	
Reason:	DoorTimedUnlock	
Cardholder:		

Time:	22/04/2016 3:55:32 PM	Escalator
Door:	CEO Office	
Source:	CEO Office exterior access point	
Event:	User Granted in	
Reason:	UserGrantedIn	
Cardholder:	Cara Mantovani	

Time:	22/04/2016 3:55:32 PM	Escalator
Door:	CEO Office	
Source:	CEO Office	
Event:	Door Lock	
Reason:	DoorLock	
Cardholder:		