Security Center 5.6 Training Guide

Module 2 - Installation & Architecture

Default server roles

- ❑ A Genetec server role runs within:
  a) The SQL service
  b) The Genetec Server service
  c) The roles' own Windows service
  d) The DHCP service
  e) None of the above

- ❑ Match the following default server roles to their descriptions:

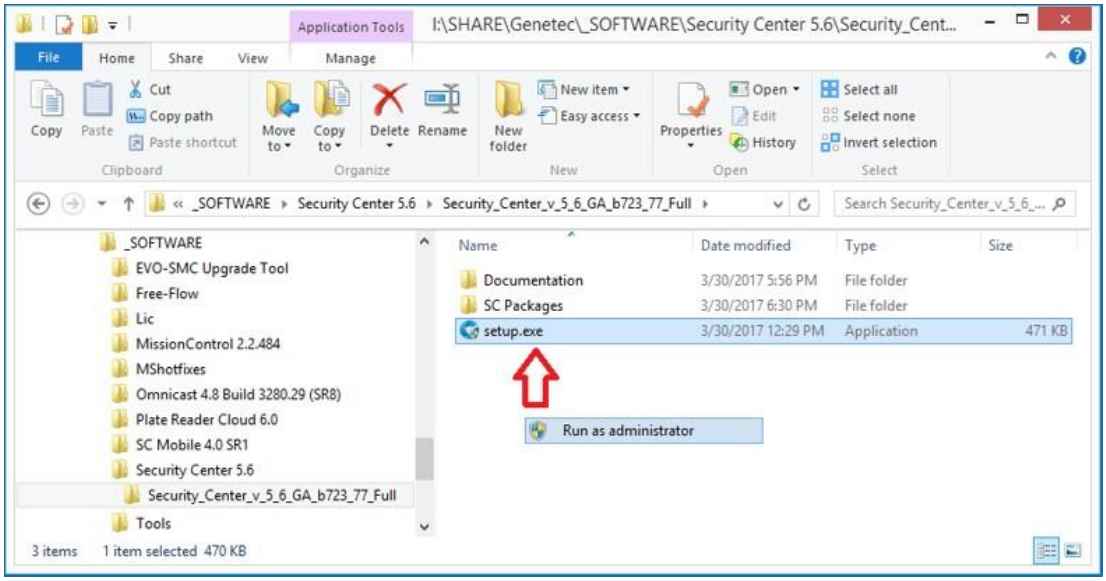
Icon	Role	?	Description
	**Report Manager**	_____	**a)** Monitors the health of system entities to populate a *Health* database
	**Access Manager**	_____	**b)** Manages video units and records video archives
	**Zone Manager**	_____	**c)** Manages *Zones* (groups of inputs)
	**Media Router**	_____	**d)** Manages door controllers and records door events in a database
	**LPR Manager**	_____	**e)** Manages the system configuration database and accepts client connections
	**Directory**	_____	**f)** Manages all map resources (images, GIS servers, KML objects)
	**Health Monitor**	_____	**g)** "Understands" the network topology to route video packets from source to destination
	**Archiver**	_____	**h)** Manages *Sharp* LPR cameras and mobile *Patrollers*
	**Map Manager**		**i)** Manages and executes the automation of reports

- ❑ What is the difference between a ***Main server*** and an ***Expansion server***?
  a) A ***Main server*** is found only in a single server system while ***Expansion servers*** are found only in multiple server systems.
  b) A ***Main server*** runs only the *Directory* role. All other roles must run on ***Expansion servers***
  c) A ***Main server*** is, by definition, the most powerful computer in your pool of servers. ***Expansion servers*** are less powerful (in terms of CPU, RAM, etc)
  d) A ***Main server*** is a Genetec server hosting the *Directory* role. An ***Expansion server*** is a Genetec server that doesn't host a *Directory* role
  e) There is no difference between a ***Main server*** and an ***Expansion server***

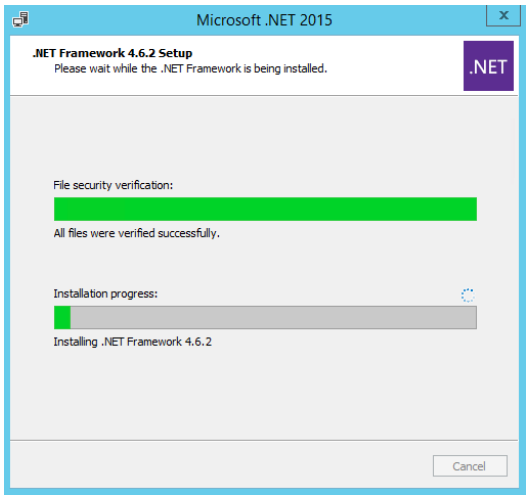
Client software installation

Security Center 5.x client installation

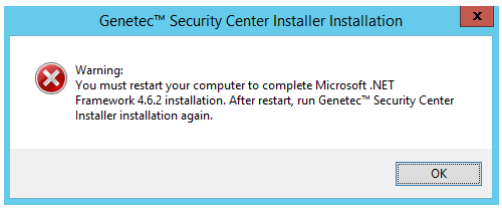
- ❑ Ensure that you have a valid IP address and that you can ping the server
- ❑ Navigate the contents of your USB flash drive to the path:
  `.\Security Center 5.x\`
- ❑ Right click the file ***setup.exe*** and select ***Run as administrator***



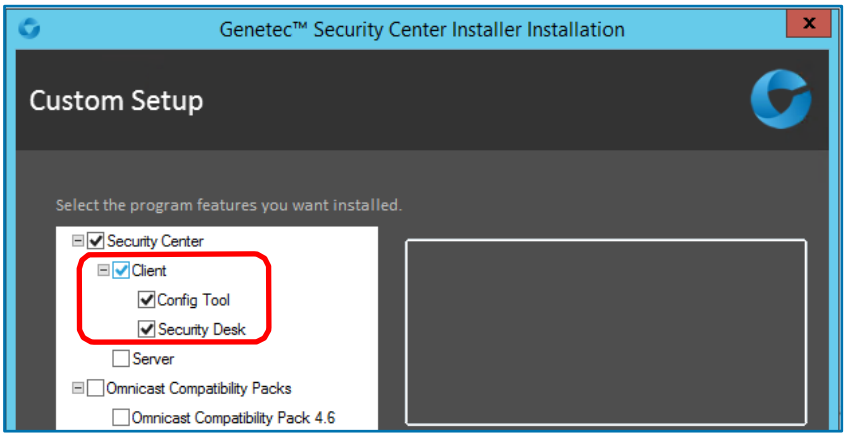
- ❑ Follow the *InstallShield* wizard to install the Security Center 5.x client software
- ❑ Allow the installer to install any prerequisite software (.NET, Visual C++, Windows hotfixes…)
  If the .NET framework must be installed, be patient, it takes some time



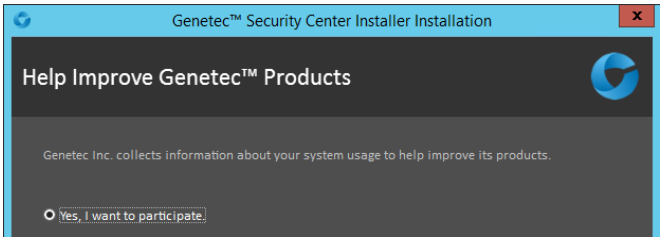
And, it requires a reboot before continuing with the Security Center installation



- ❑ Once the installer is ready to install the Security Center 5.6 components, make sure that ***Server*** is unselected and that only ***Client*** is selected



- ❑ When prompted, ***agree*** to participate in the collection of system usage information (Participate, or participate anonymously)



- ❑ Allow the configuration of the firewall rules.
- ❑ From the *Security Settings* page, select ***Custom (Advanced)***, then:
  - ❒ **Always validate the Directory certificate**
  - ☐ **Turn off basic authentication**
  - ❒ **I acknowledge…**
- ❑ Follow the prompts to complete the client installation

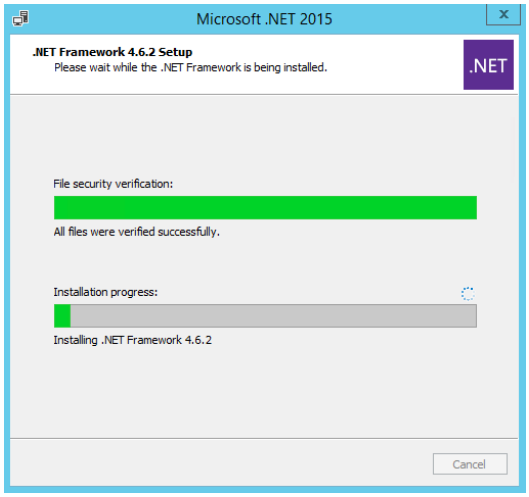
Test Client Installation

- ❑ Test your client software by launching your *Config Tool* application.
- ❑ Once the Main server installation is complete, try to connect to the server using:
  User: Admin***Password:*** (*none*)***Directory:*** *Name* or *IP* of the server

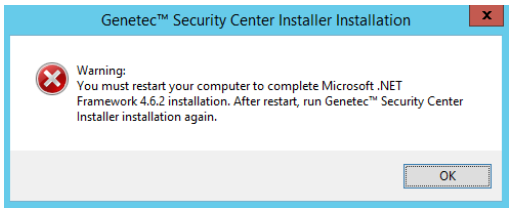
Main Server software installation (as a group)

Security Center 5.x Main Server installation

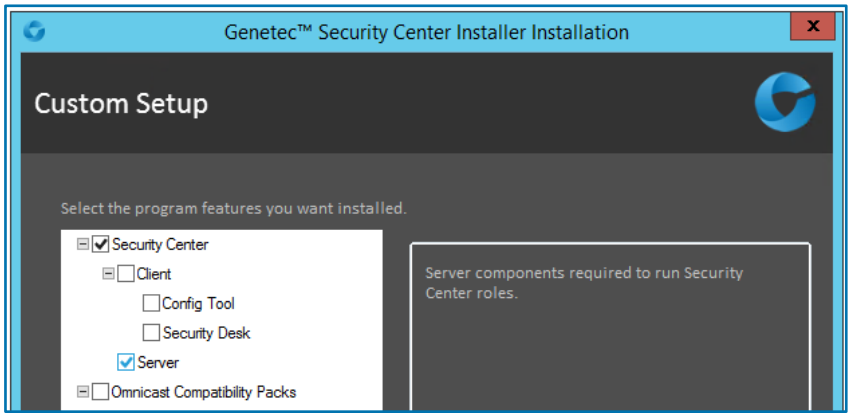
- ❑ Ensure that you have a valid IP address on the same network as the client workstations
- ❑ Navigate the contents of your USB flash drive to the path:
  `.\ Security_Center_v_5_x…\`
- ❑ Double click the file ***setup.exe***
- ❑ Follow the *InstallShield* wizard to install the Security Center 5.x server software
- ❑ Allow the installer to install any prerequisite software (.NET, Visual C++, Windows hotfixes…)
  If the .NET framework must be installed, be patient, it takes some time



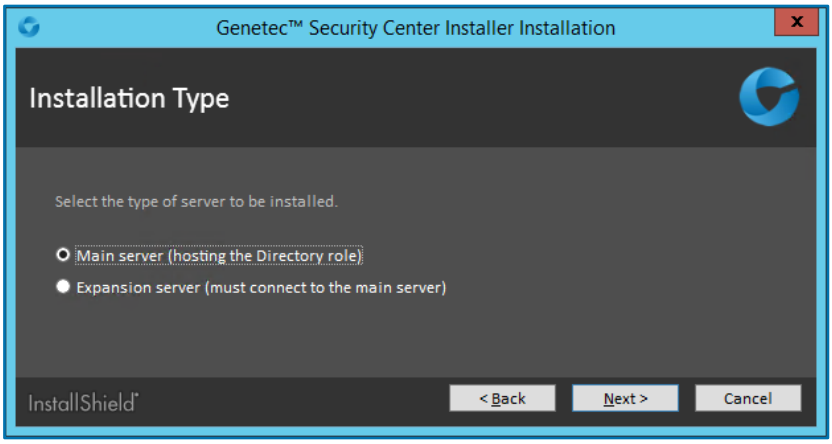
And, it requires a reboot before continuing with the Security Center installation



- ❑ Once the installer is ready to install the Security Center 5.6 components, make sure that ***Client*** is unselected and that only ***Server*** is selected (optional: select the *Config Tool* client if you want)

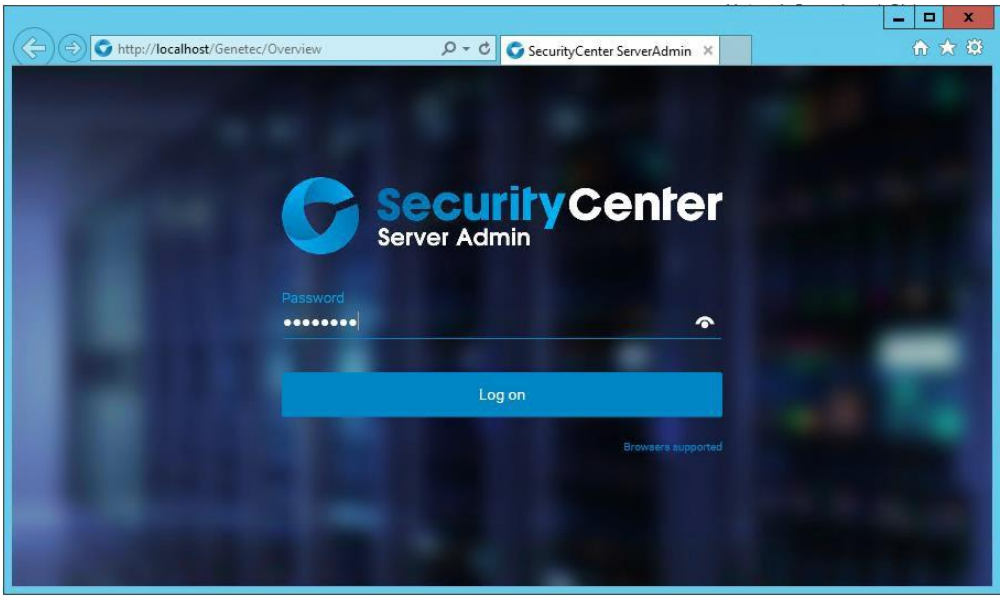


- ❑ In the *Installation Type* page, select the **Main server** option, and click **Next**.

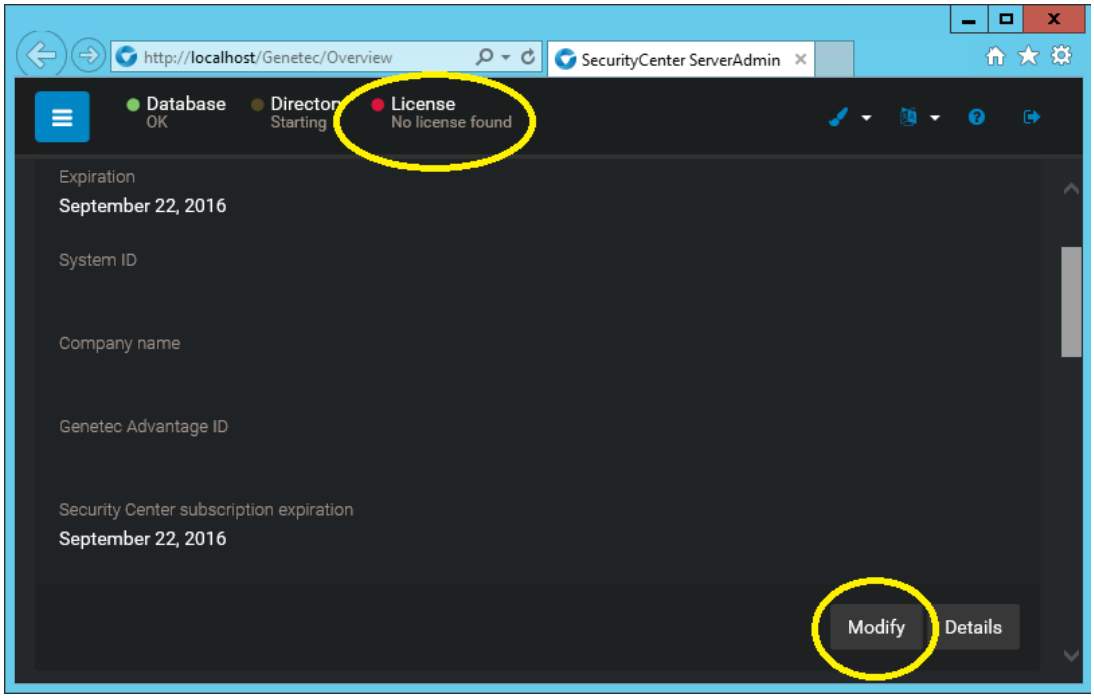


- ❑ In the *Help Improve Genetec Products* page, select ***Yes, I want to participate but anonymously***. Click ***Next.***
- ❑ In the *Database Server* page, select one of the following options:
  - **Install a new database server** (if no SQL server has already been installed)
  - **Use an existing database server** (if an SQL server has already been installed)
- ❑ In the *Services logon parameters* page:
  - Use default username and password
- ❑ In the *Server parameters* page:
  - **Server password**: `training`
- ❑ In the *Firewall rules* page:
  - **Allow Genetec Security Center to create necessary firewall rules**
- ❑ In the *WinPcap Installation* page:
  - **Install WinPcap**
- ❑ In the *Security Settings* page, select ***Custom (Advanced)***, then:
  - ❒ **Always validate the Directory certificate**
  - ☐ **Turn off basic authentication**
  - ❒ **I acknowledge…**
- ❑ Hit next, and allow Genetec Security Center 5.x server to complete installing
- ❑ You may be prompted to reboot depending on the Windows prerequisites installedYou may be prompted to reboot depending on the Windows prerequisites installed
- ❑ At the end of the installation, allow the Installation wizard to launch the *Server Admin*

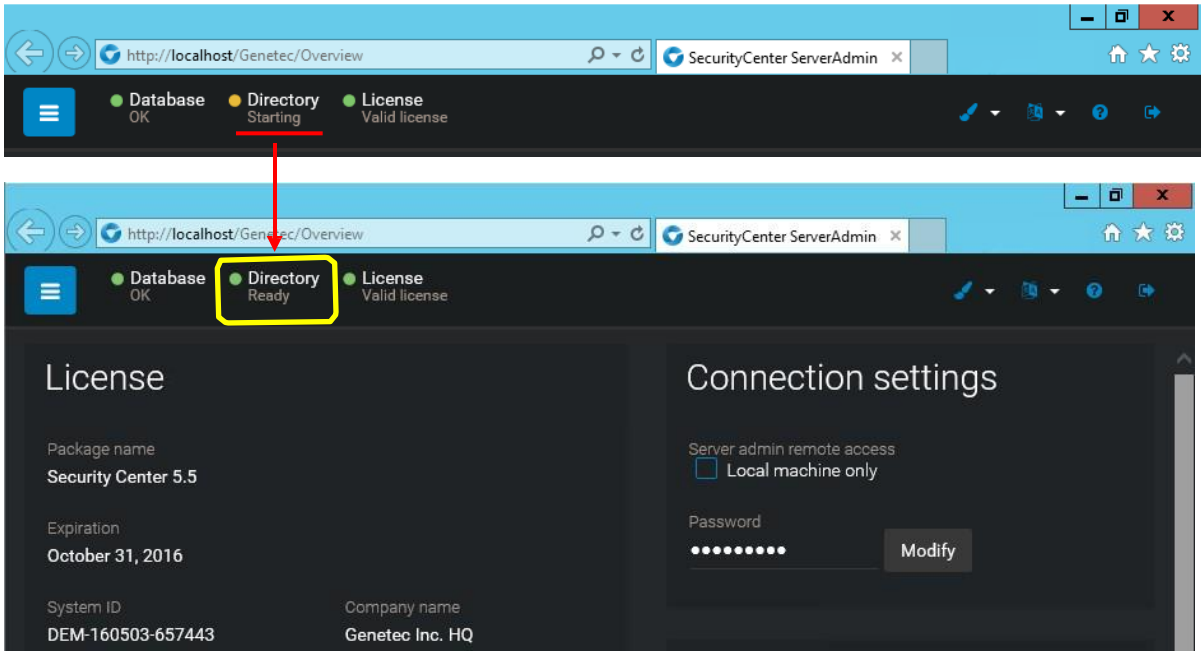
- ❑ Enter `training` as the Server Admin password and click **Log on**



- ❑ You should be alerted that no license was found, click **Modify**



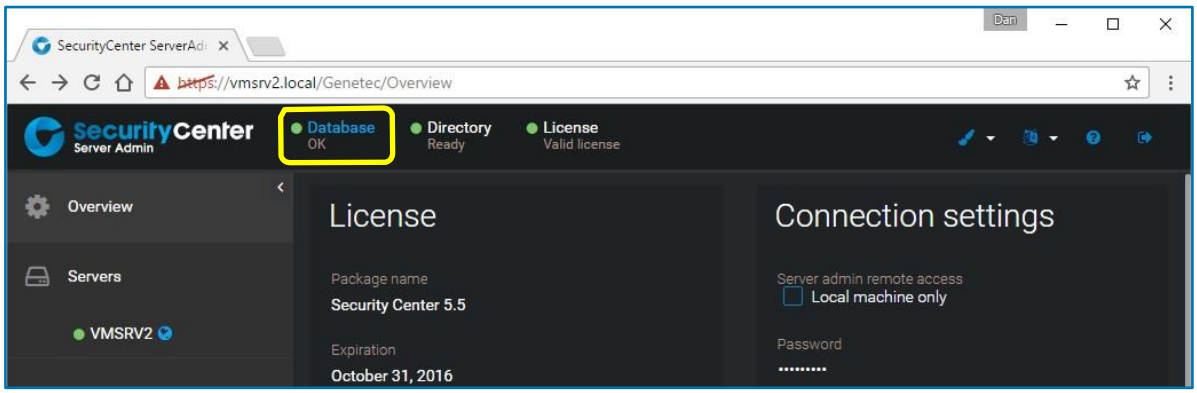
- ❑ Use either the **Manual activation** to download your license with a browser or the **Web activation** to download your license without a browser. (Ask your trainer)
- ❑ Once the license has been applied, it will take a few moments for the Directory to start.



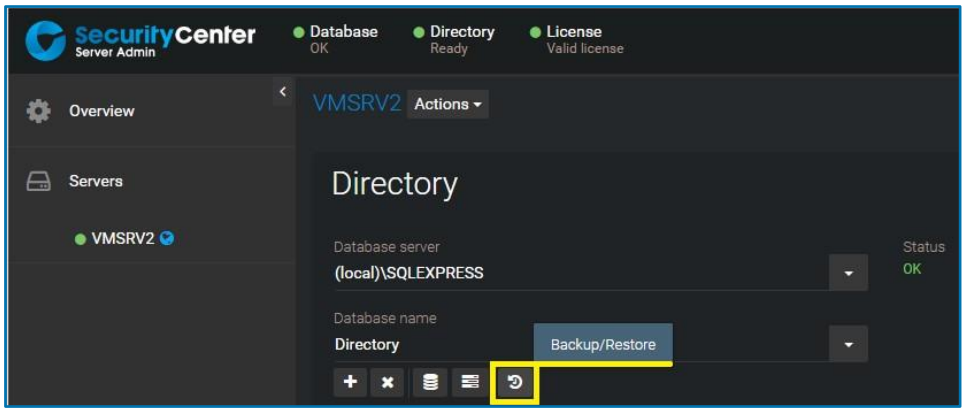
- ❑ Wait until all 3 indicators (***Database***, ***Directory*** and ***License***) are green and ready

Initial Main Server configuration (as a group)

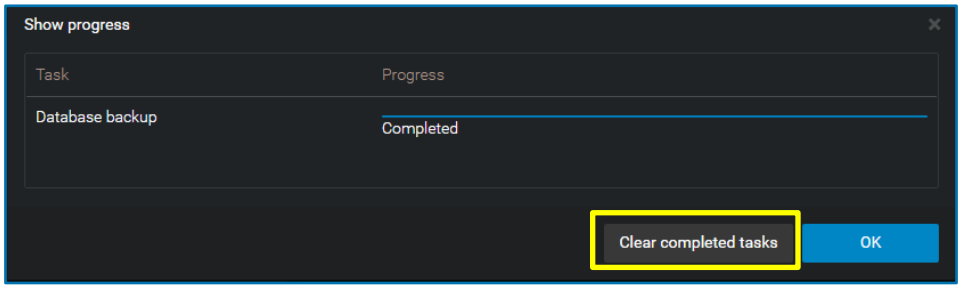
- ❑ Open a browser on one of the workstations and log in to the Main server's *Server Admin*: https://(*ServerName or IP*)/Genetec
- ❑ In the *Server Admin*, click the link at the top of the page to access the **Database** properties



- ❑ Under Directory's database connection properties, click **Backup/Restore**

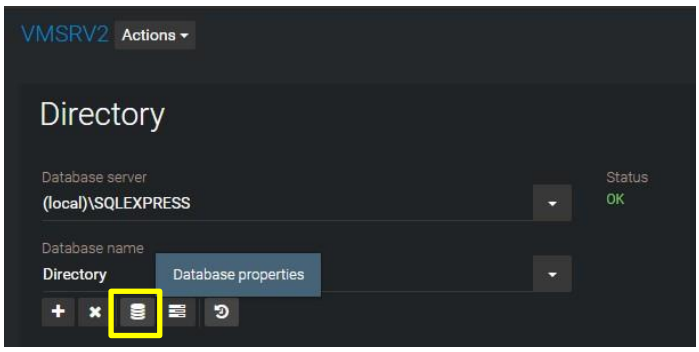


- ❑ Note the backup **Destination folder** and click ***Backup now***
- ❑ Once the database backup has completed successfully, click ***Clear completed tasks***

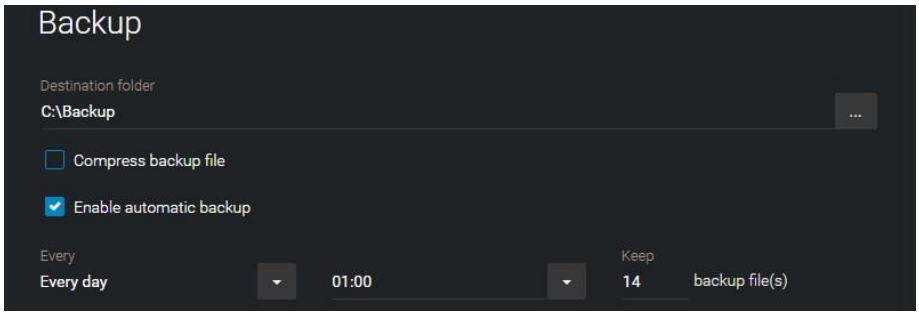


- ❑ Click ***OK***

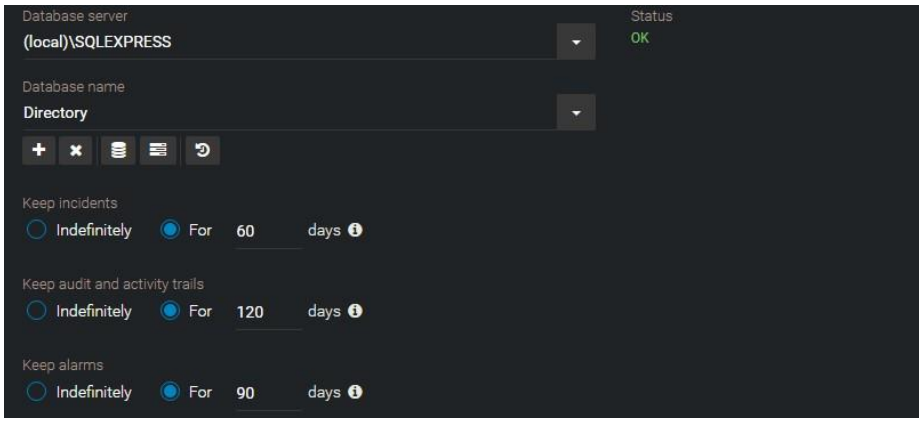
- ❑ Click the ***Database properties*** button



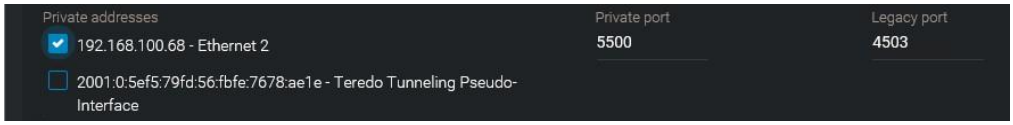
- ❑ Modify the Backup ***Destination folder*** to the path C:\Backup
- ❑ Select ***Enable automatic backup***
- ❑ Configure the automatic back schedule to run every day at 01:00 and to keep 14 backup files.



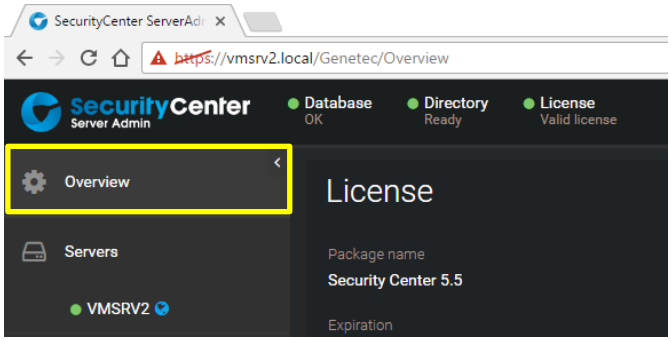
- ❑ Click **OK**. Click **Save**.
- ❑ Below the Directory's database properties, configure the following:
  - ❑ **Keep incidents** for 60 days
  - ❑ **Keep audit trails** for 120 days
  - ❑ **Keep alarms** for 90 days



- ❑ Click **Save**
- ❑ Under ***Network***, select only 1 network interface and unselect any others



- ❑ Click the ***Overview*** menu button



- ❑ If an email server is available on the network, complete the SMTP configurations in the ***SMTP*** section of the page. Click **Save**
- ❑ Click the **License** menu button at the top of the page. Validate your license for the following:

Feature	Supported	Not supported	Quantity
Remote Security Desk	☐	☐	
Number of Security Desk connections	☐	☐	
Security Center Compact	☐	☐	
Number of cameras	☐	☐	
Number of readers	☐	☐	
Number of LPR Managers	☐	☐	
Number of mobile devices	☐	☐	

- ❑ Click **Close**

Module 3 - Access Control Hardware

Understand your hardware

Before proceeding with the software configuration of your hardware door controller, you first need to understand the hardware unit itself.

Complete the following information:

Manufacturer:

- ❑ H.I.D.EVO or, legacy VertX or, Edge
- ❑ SMC / Synergis Cloud Link / Appliance
- ❑ Other: _____

Model:_____

MAC address:_____

IP address:_____._____._____._____

Webpage authentication User:_____/ PW: _____

Enrollment authentication User:_____/ PW: _____

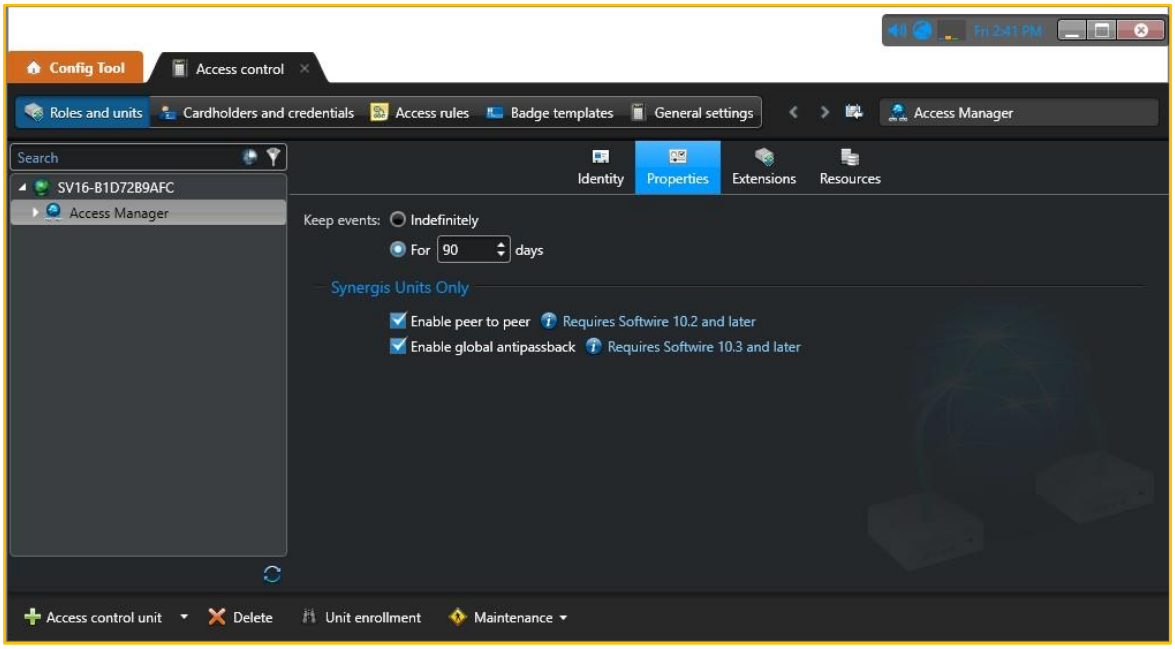
Identify the following physical connection points on your controller. If your unit does not have some of these connections, cross them off the list:

- ❑ Reader 1
- ❑ Reader 2
- ❑ Door Monitor 1
- ❑ Door Monitor 2
- ❑ REX 1
- ❑ REX 2
- ❑ Strike Relay 1
- ❑ Strike Relay 2
- ❑ Aux Relay 1
- ❑ Aux Relay 2
- ❑ Tamper Input
- ❑ AC Fail Input
- ❑ Battery Fail Input
- ❑ Power
- ❑ Ethernet
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____

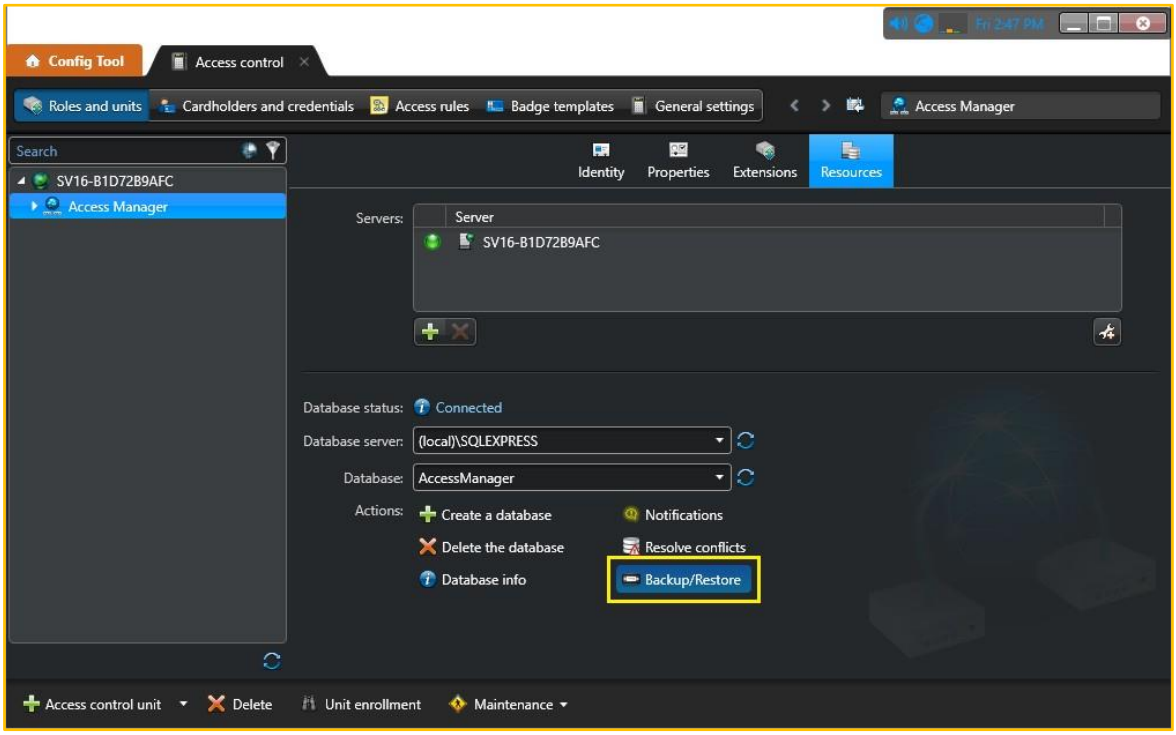
Retention period for access events

Before adding your access control hardware units, validate the retention period used in the access manager's database:

- ❑ **Config Tool** → **Access Control** task → **Access Manager** – ***Properties***



- ❑ Scheduled backups of the access manager's database can be configured from its ***Resources*** tab:

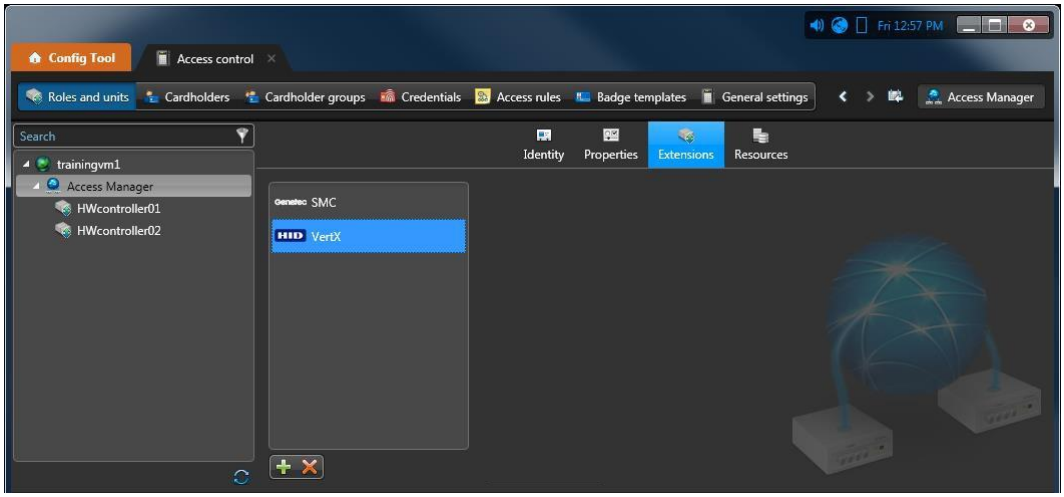


Discovering and adding access control units

Access Manager – *Extensions*

Before any doors can be created, the (hardware) door controllers must first be enrolled into the system. The Access Manager is the server role that manages the door controllers. It requires ***extensions*** for the different types of hardware that it will manage. For example, to enroll H.I.D. hardware, we must first add the H.I.D. extension to the Access Manager role. To enroll SMC/Synergis Cloud Link hardware, we must first add the Genetec Synergis extension to the Access Manager, etc.

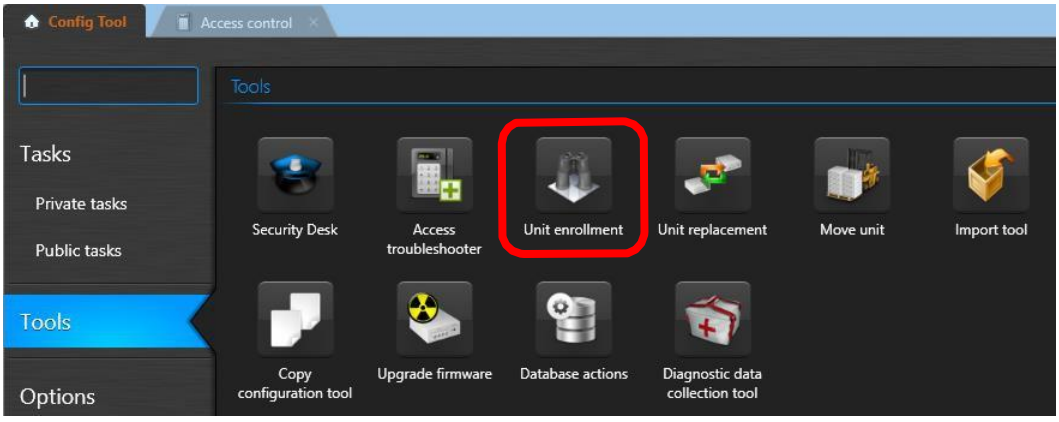
- ❑ Open the **Config Tool → Access Control → Roles and units**
- ❑ Select the **Access Manager** role
- ❑ Select the **Extensions** tab
- ❑ Click Add ( ) to add the manufacturer *extensions* for the kind of hardware you want to enroll
- ❑ Click **Apply**



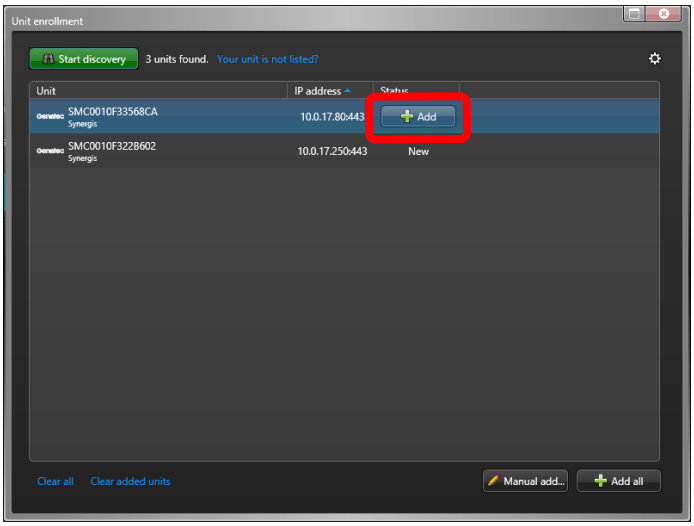
Unit Discovery and Enrollment

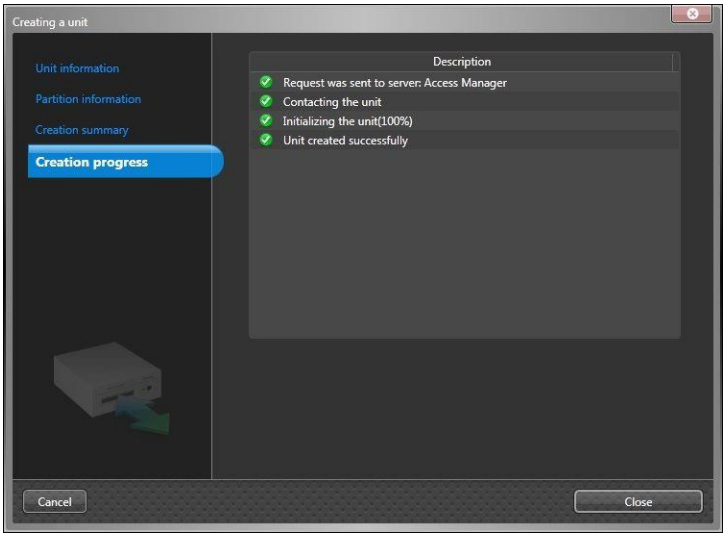
Now that the required extension(s) have been added to the Access Manager, you should be able to enroll (add) the hardware units to the system.

- ❑ Open the **Config Tool → Tools → Unit enrollment**



- ❑ Click the **Settings and manufacturers** button (☼) in the upper right corner
- ❑ Click **Add manufacturer** (✚) to add manufacturer *extensions* for the kind(s) of controller(s) that you are trying to *discover* on the network. Click **Save**
- ❑ Click **Start discovery** (Start discovery)
- ❑ Once the *Discovery tool* has finished scanning the local network, hover on the unit you want to add from the list of discovered access control units and click **Add**

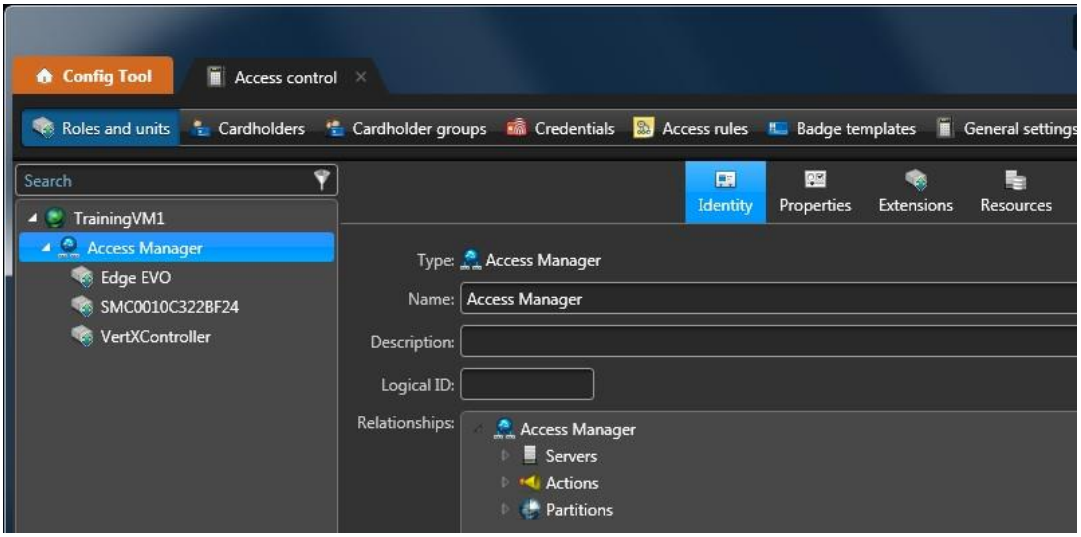




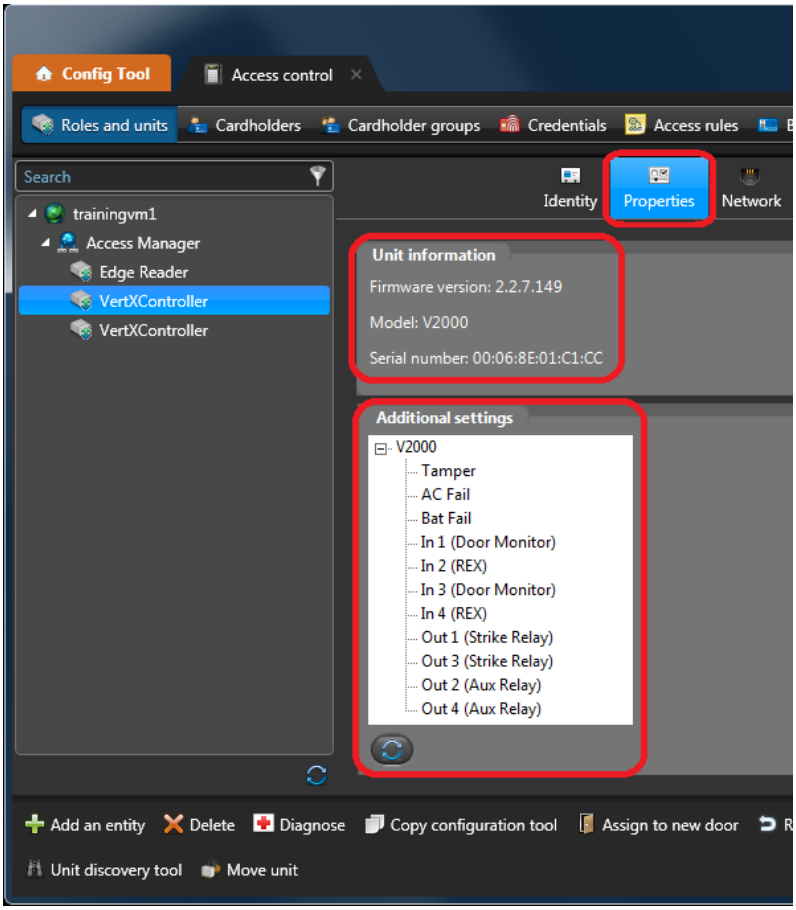
- ❑ If the unit does not successfully add, note the **Manufacturer**, **Product type** and **IP** of any access control unit that you want to add.
- ❑ Click **Manual add** (✚). In the Manual add dialog box, enter the required details and click **Add**
- ❑ Note: when adding an HID VertX unit in secure mode (FTP and Telnet protocols disabled), the admin account must be used to enroll the unit (use the root account for unsecure)
- ❑ Click **Clear completed tasks**. Click **Close**. Open the **Config Tool → Access Control** *task* to see your hardware unit.

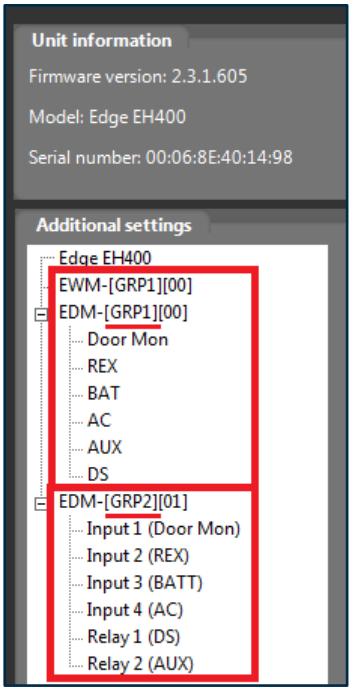
Post Enrollment Settings

Once the access control hardware unit has been enrolled into the system, it can be seen in the Config Tool's Access Control task under the Access Manager.



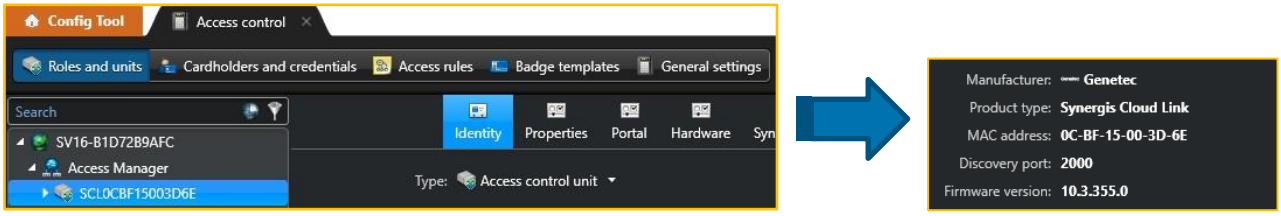
If your hardware unit is made by H.I.D., validate the hardware's enrollment by examining your unit's ***Properties*** tab in the **Config Tool → Access Control Task**.

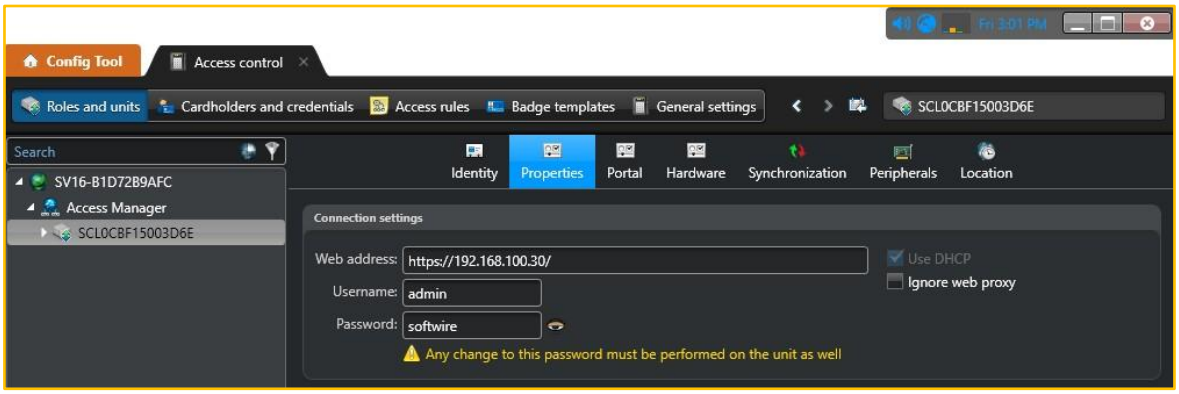




H.I.D. **V2000** properties H.I.D. **EH400** EVO properties

If your hardware is a **Synergis Cloud Link**, the ***Identity tab*** in the **Config Tool → Access Control Task** will display the MAC address, discovery port (default:2000) and firmware version. The ***Properties*** tab should display the unit's web portal properties and authentication:

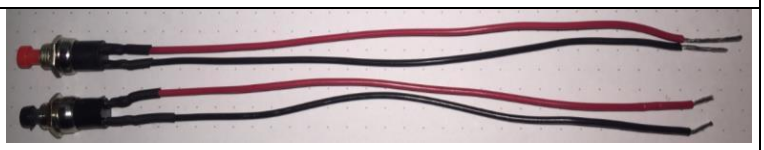
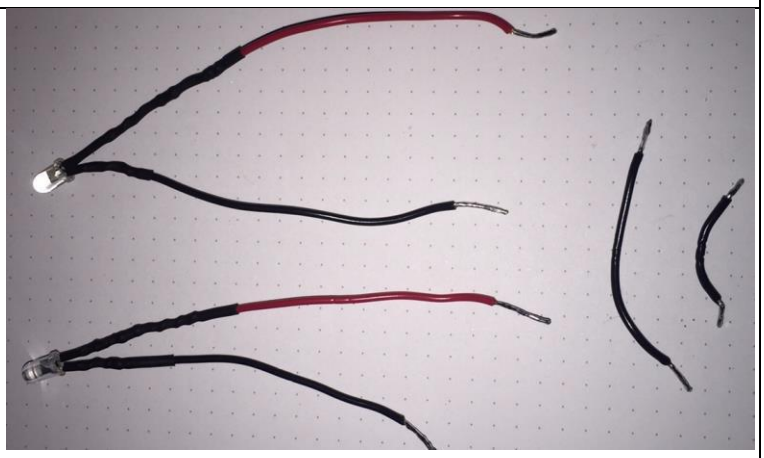
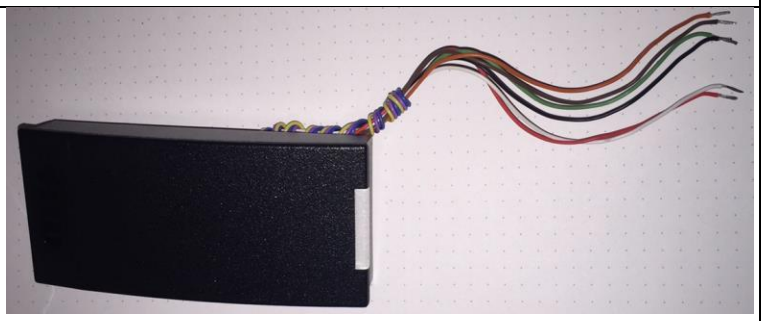




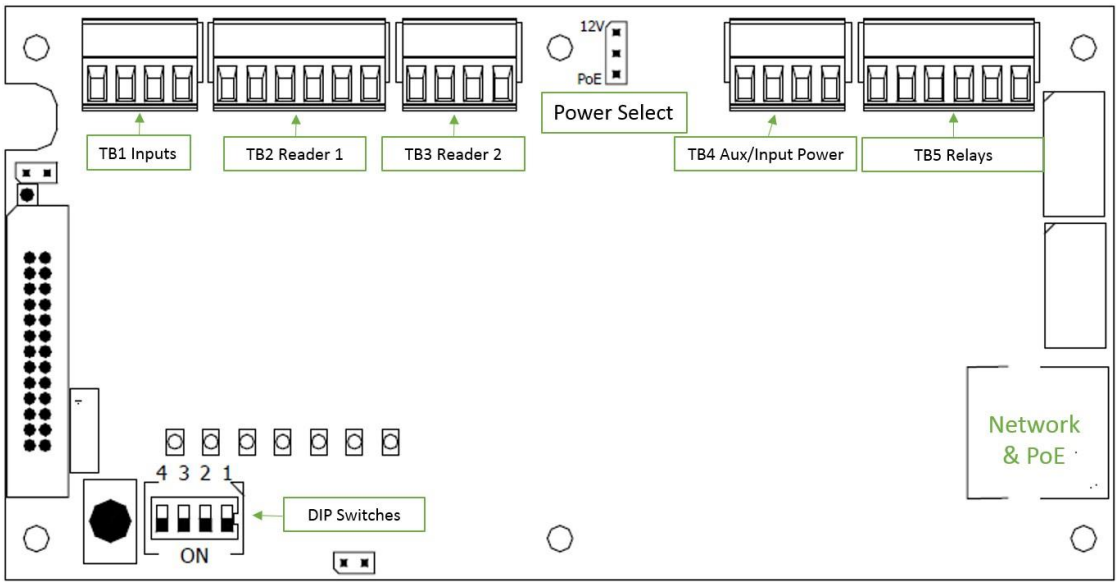
Adding Mercury EP1501's (optional)

Familiarize yourself with the components in the lab kit.

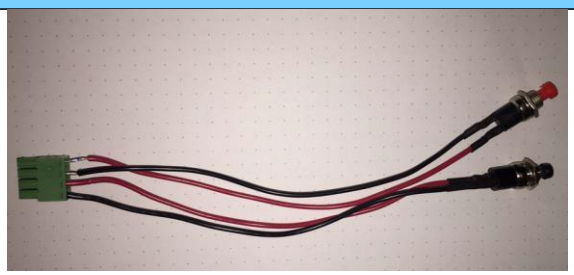
Component	Picture
Lab Component Bag Quantity: 1	

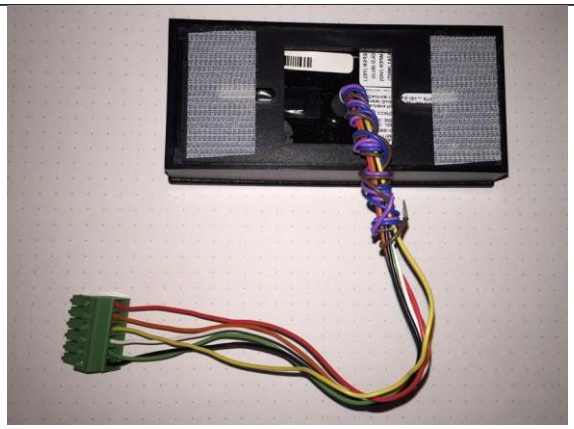
Mercury EP1501 Door Controller Quantity: 1	
Input Switches to represent Door Sensor and REX (Request to Exit) Quantity: 2	
Output LED's to represent Door Lock and Auxiliary Relays Quantity: 2 LEDs, 2 Jumper wires	
HID iClass Reader to configure a single-reader door Quantity: 1	
Small Flathead Screwdriver to connect wires to terminal blocks on Mercury EP1501. Quantity: 1	

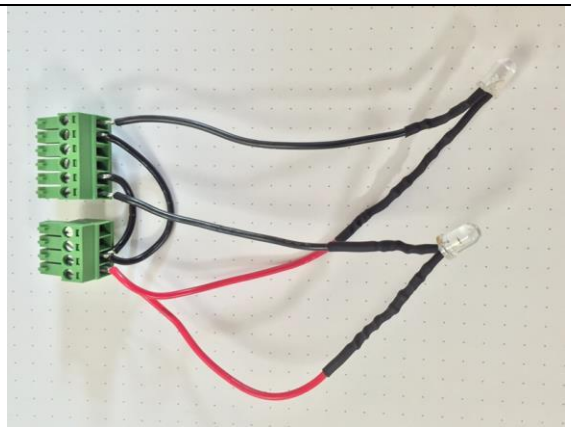
Familiarize yourself with the Mercury EP1501 Controller



Terminal Block	Symbol (L to R)	Contact Description
TB1 (Input Terminal Block)	IN1 IN2	Input 1 Input 1 Input 2 Input 2
TB2 (Reader 1 Terminal Block)	V0 LED BZR CLK DAT GND	Reader 1 Power Output – 12 VDC Reader 1 LED Output Reader 1 Buzzer Output Reader 1 CLK/Data 1/TR+ (serial) Reader 1 DAT/Data 0/TR- (serial) Reader 1 Ground
TB3 (Reader 2 Terminal Block)	LED BZR CLK DAT	Reader 2 LED Output Reader 2 Buzzer Output Reader 2 CLK/Data 1 Input Reader 2 DAT/Data 0 Input
TB4 (Power Terminal Block)	V0 GND VIN GND	Auxiliary Power Output - 12 VDC Auxiliary Power Output – Ground Input Power – 12 VDC (local power supply) Input Power Ground
TB5 (Relay Terminal Block)	NO 1-C NC NO 2-C NC	Relay 1 – Normally Open Contact Relay 1 – Common Contact Relay 1 – Normally Closed Contact Relay 2 – Normally Open Contact Relay 2 – Common Contact Relay 2 – Normally Closed Contact

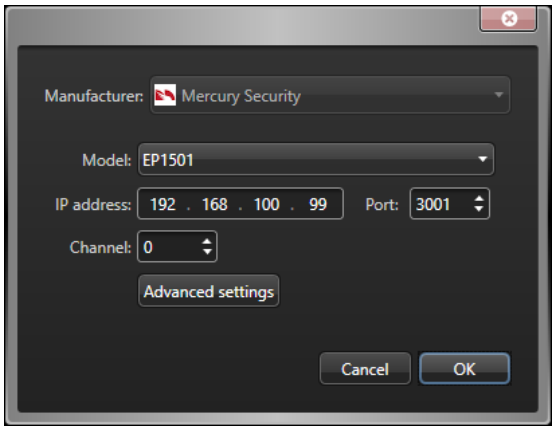
<table>
<tr><th>Terminal Block</th><th>Contact Description</th><th>Example</th></tr>
<tr><td>3.a) TB1</td><td>Connect Switches to Inputs 1 and 2. Later, in Security Center, we will assign these to the Door Sensor and REX (Request to Exit).</td><td>  </td></tr>
<tr><td>3.b) TB2 (Reader 1 Terminal Block)</td><td>Connect Reader contacts to corresponding terminal block connections. Please consult reader for wire color descriptions.

Example Reader:
<table><tr><th>iClass R10</th><th>EP1501 TB2</th></tr><tr><td>+VDC</td><td>V0</td></tr><tr><td>GRN LED</td><td>LED</td></tr><tr><td>BEEPER</td><td>BZR</td></tr><tr><td>DATA1</td><td>CLK</td></tr><tr><td>DATA0</td><td>DAT</td></tr><tr><td>GND</td><td>GND</td></tr></table></td><td>  </td></tr>
<tr><td>3.c) TB3 (Reader 2 Terminal Block)</td><td>Leave Terminal Block 3 Empty</td><td></td></tr>
<tr><td>3.d) TB4 (Power Terminal Block)</td><td>Connect both red LED wires to V0 in TB4. Connect both jumper wires to GND in TB4.</td><td></td></tr>
</table>

3.e) TB5 (Relay Terminal Block)	Connect black wire of first LED to Relay 1 - NO in TB5. Connect the black wire of the second LED to Relay 2 – NC in TB5. Finally, connect both black jumper wires to the common contacts 1-C and 2-C.	
3.f) Network / PoE	Connect Terminal blocks to EP1501. Connect the controller to PoE. One of the two relays should light up (Normally Closed). Test presenting a compatible iClass card to the reader. You should hear a beep. Door programming (access rules) be configured in a later Security Center exercise.	

Bring the Mercury EP online

Step	Description
4.a)	On the Mercury controller board, set switch 1 on the DIP switch S1 to ON. This will give you a 5 minute window to log on (see DIP switch table below)
4.b)	Log on to the Mercury controller through the Mercury Device Manager web page. Use the default IP address (192.168.0.251) and credentials (admin/password). Set your computer to an IP on the same subnet (e.g. 192.168.0.245), coordinating with the trainer to avoid IP conflicts.
4.c)	Select **Network** from the menu, configure the controller's IP address, and click ***Accept***. (Ask your instructor which IP address to use)
4.d)	Select **Host Comm** from the menu, configure the ***Port number*** used by the Synergis unit to communicate with the Mercury controller (default=3001), set ***Data Security*** to ***TLS Required*** and click ***Accept***. The field **Communication Address** found on the **Host**

	Communication page must be left at 0. It is not to be confused with the **Channel** field that needs to be unique when you enroll the Mercury controller on the Synergis unit.
4.e)	Restrict the connection to the Mercury controller to one Synergis unit. Select ***Authorized IP Address Required***, and enter the Synergis unit's IP address as **Authorized IP address**.
4.f)	Select ***Apply Settings*** and click ***Apply Settings, Reboot***.
4.g)	On the Mercury controller board, set switch 1 on the DIP switch S1 to OFF for normal operation.
4.h)	When prompted to proceed or not, select I understand, and then click Yes.
4.i)	Enroll the unit into Security Center through the SMC/SCL. Under **Config Tool** > Access Control > Roles & Units > Select the Synergis Unit > Peripherals > Hit the + sign to add an item > Select Mercury EP1501 

Mercury EP DIP Switch Reference Table

SW 1	SW2	SW3	SW4	Dip Switches Mode
OFF	OFF	either	OFF	Normal operating mode
ON	either	either	either	After initialization, enable default authentication: **user (admin), pass (password)** no need to reboot
OFF	ON	either	OFF	Factory default communication parameters Static IP: 192.168.0.251 (accessible via browser) Subnet Mask: 255.255.0.0 Default Gateway: 192.168.0.1 DNS: 192.168.0.1 Port: 3001

Connected Peripherals

An access control unit has a number of connected peripheral devices. These can include reader interfaces, inputs and outputs.

A common problem during the initial installation of an access control unit is the incorrect default state for a given input.

For example, access control units have an input used to monitor the door state (open or closed). If the input is configured in the software as "*normally closed*" but the circuit connected to the actual input is not physically closed, the door controller may start to beep as an audible warning that the door is being held open.

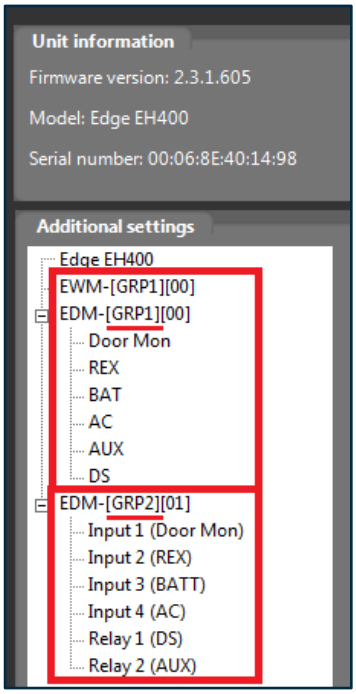
To correct the problem of the continuously beeping door controller, we could try 2 approaches:

a) Close the physical circuit connected to the input
b) Configure the input within the software as "*normally open*" instead of the default "n*ormally closed*"

Display/edit your connected peripherals

For **H.I.D** controllers go to the Config Tool → Access Control task → Roles and units

- ❑ Select your H.I.D. unit below the Access Manager in the tree on the left
- ❑ Select your unit's ***Properties*** tab

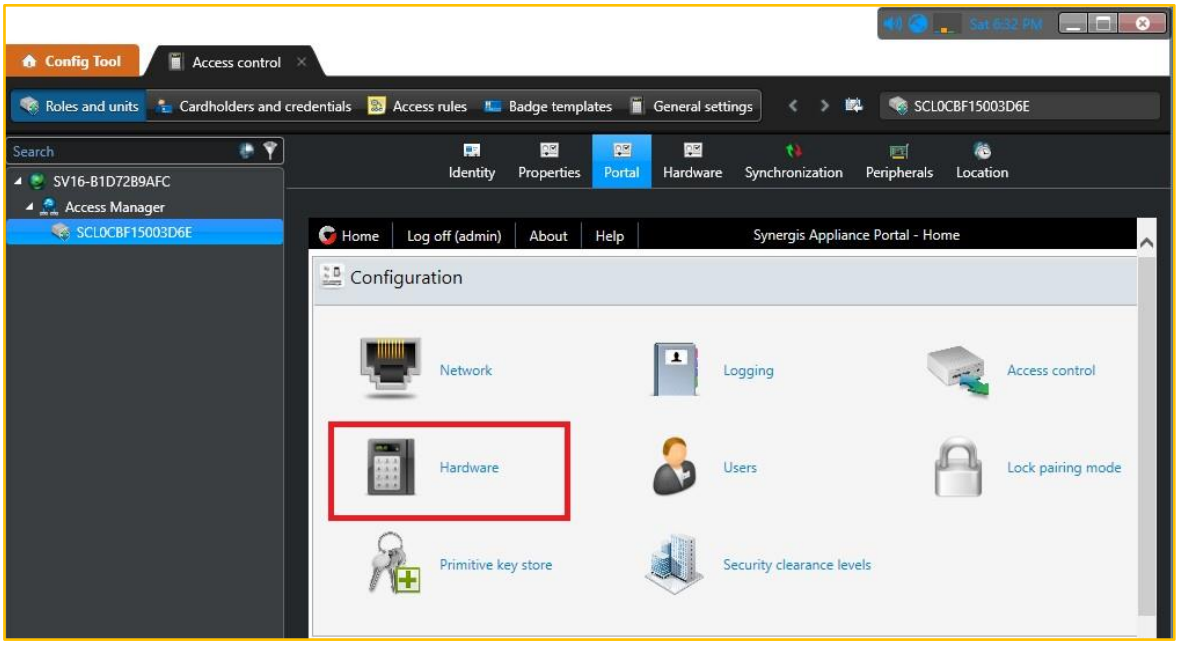


This EVO EH400 has EWM and EDM modules connected on 1 bus (00) and an EDM on the other (01)

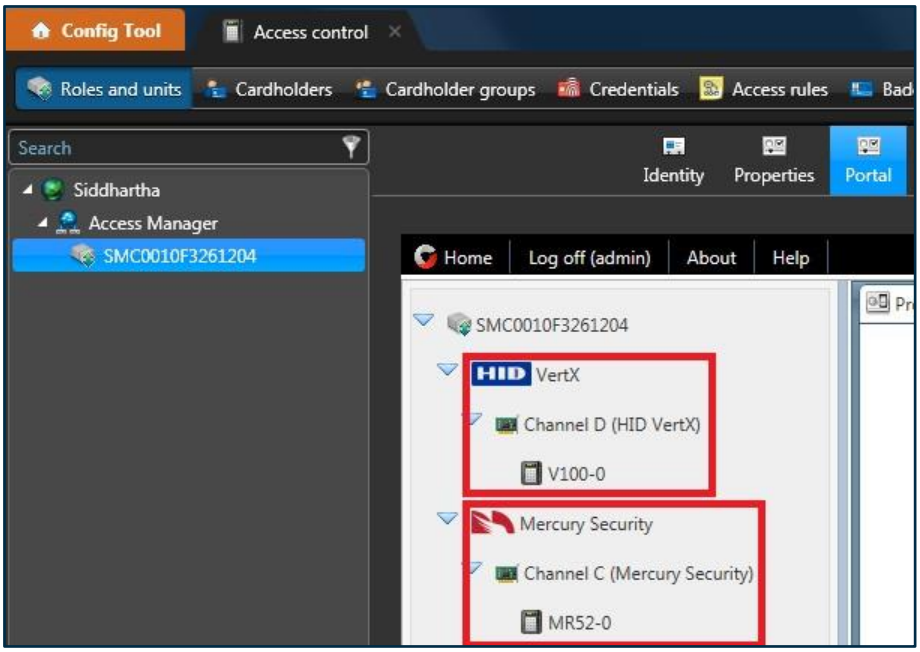
For **SMC/SCL** controllers with peripherals connected by **serial wiring** (RS-485) go to the Config Tool → Access Control task → Roles and units

Validate connectivity over the RS-485 serial bus:

- ❑ Select your SCL or SMC unit below the Access Manager in the tree on the left
- ❑ Click your unit's Portal tab
- ❑ Log in to the unit through the portal page



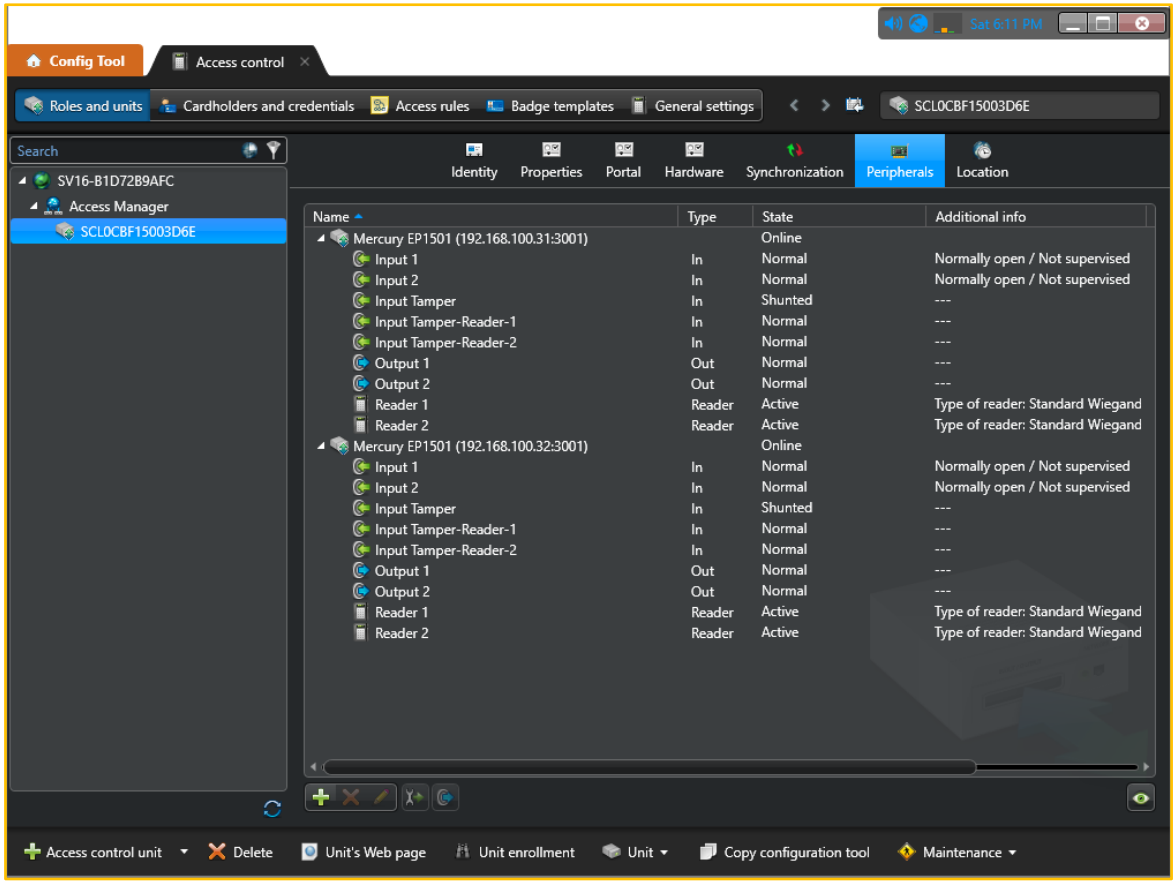
- ❑ Click the ***Hardware*** icon



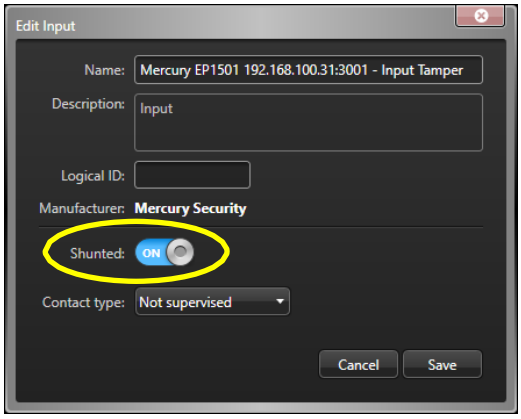
This SMC has an HID V100 on 1 serial bus (Channel D), and a Mercury MR-52 on the other (Channel C)

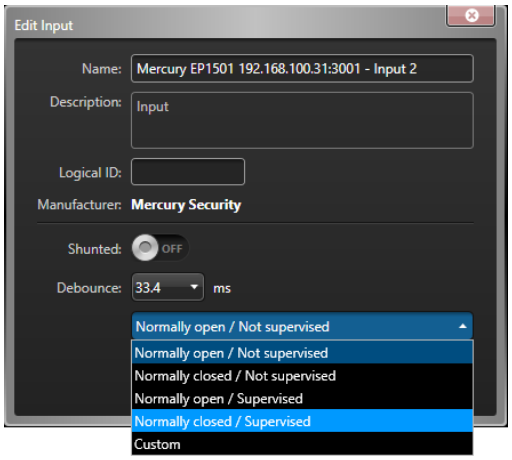
For **SMC/SCL** controllers with peripherals connected by **serial or IP** go to the Config Tool → Access Control task → Roles and units

- ❑ Select your SCL or SMC unit below the Access Manager in the tree on the left
- ❑ Select your SCL unit's ***Peripherals*** tab



- ❑ Peripherals can be shunted (disabled) and the default states of the inputs can be **edited/modified** in the unit's **Peripherals** page by double clicking a peripheral (eg an Input):

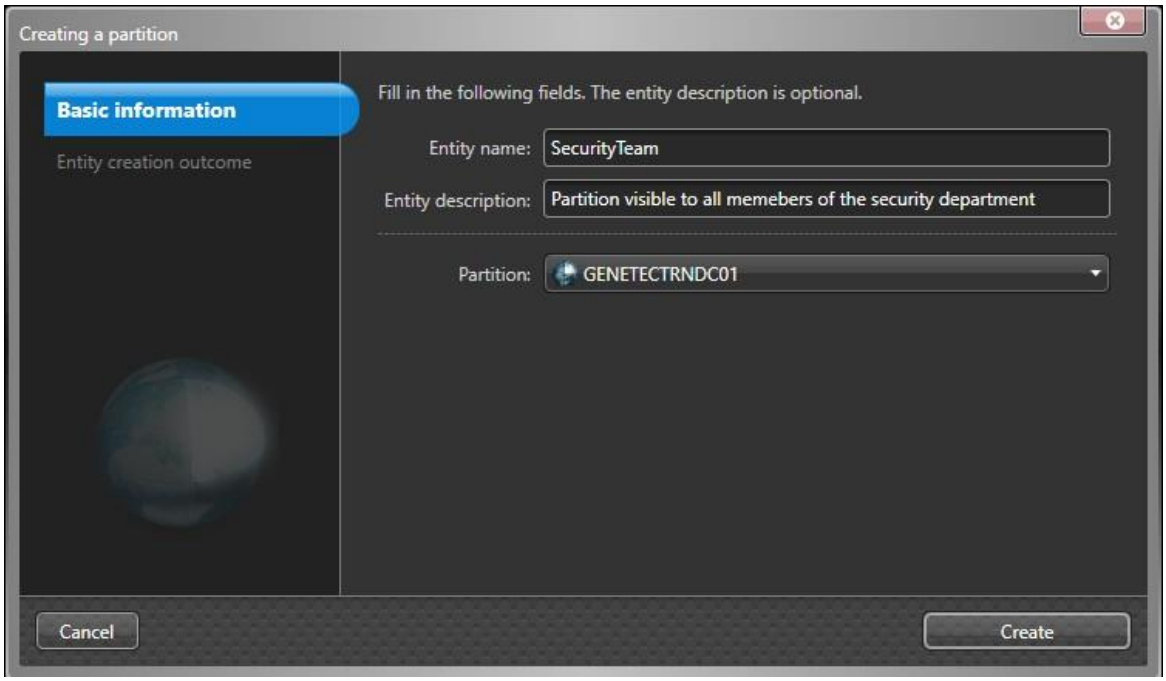




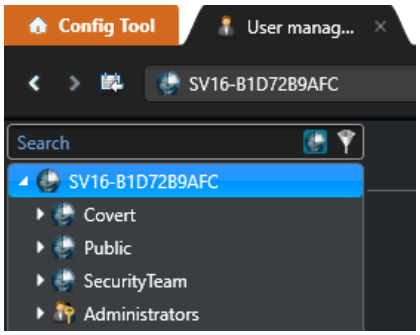
Module 4 - User Management for Access

Partitions (as a group)

- ❑ Open the *Config Tool* application on a workstation and log on with an administrative user
- ❑ Open a ***User Management*** **Task**
- ❑ Click the **Add new Partition** button ( ) at the bottom of the page
- ❑ Create a new partition called ***SecurityTeam***



- ❑ Click **Create**. Click **Close**
- ❑ Repeat the process to create a 2nd *system partition* called ***Covert***

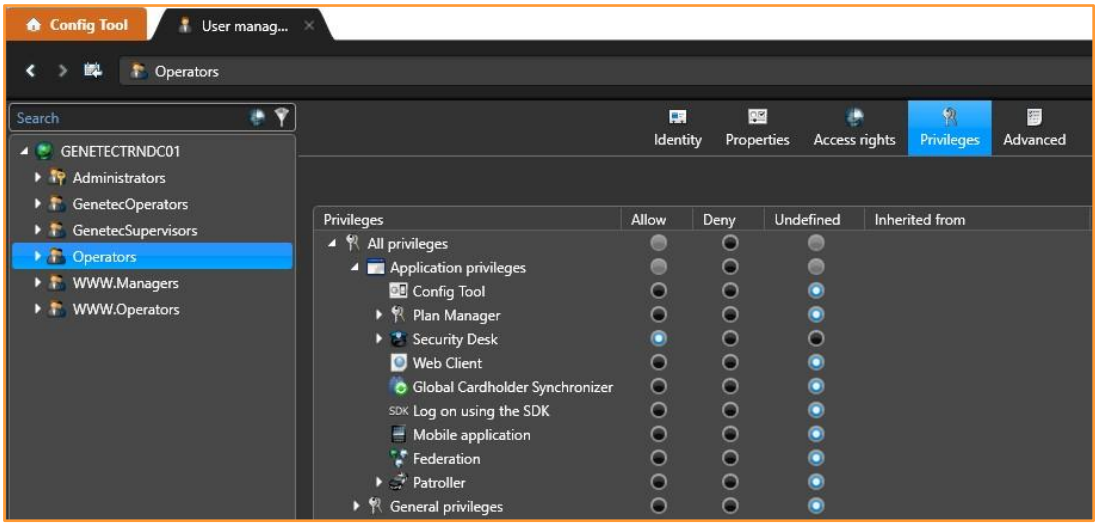


We will configure access such that any cameras, doors, alarms, etc. that are placed in the ***Covert*** partition will be visible only to administrators and supervisors but entities placed in the ***SecurityTeam*** partition will be visible to everyone.

User groups (as a group)

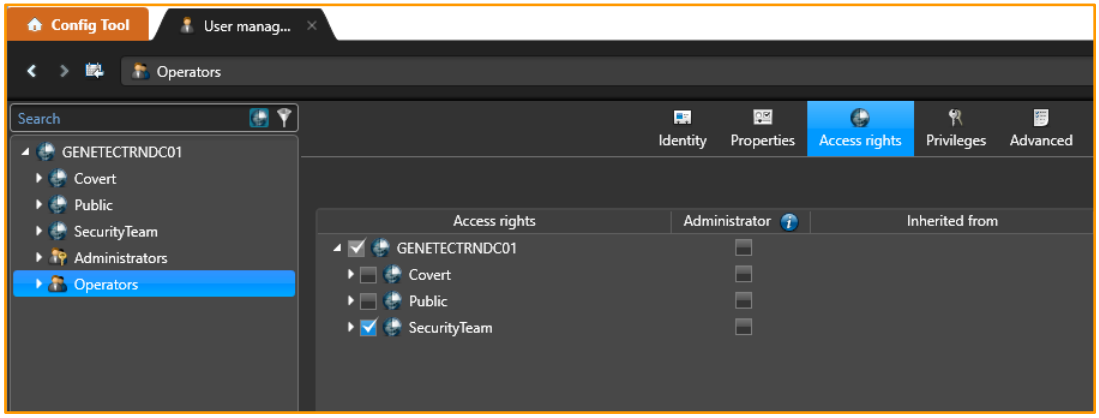
Create and configure an *Operators* user group

- ❑ Open the *Config Tool* → **User management Task** → **User groups**
- ❑ Click **Add new User group** ( ) at the bottom of the page
  - ❑ Name the new user group *Operators*. Click **Next**
  - ❑ In the **Administrative rights** page, select **Accepted users** and apply the **Operator** *Privilege template*. Click **Next.** Click **Create**
  - ❑ Click the new **Operators** user group and select its **Privileges** tab



  - ❑ Expand the branch **Application privileges**
  - ❑ Ensure that only *Security Desk* is configured with the **Allow** privilege. All the other applications should be **Undefined**
  - ❑ Expand the branch **Administrative privileges** → **Access control management**. Ensure that the following are the only privileges allowed (the rest should remain **Undefined**):
    - View badge templates
    - View cardholder groups
    - View cardholders
    - View credentials
    - View visitors
  - ❑ Expand the branch **Task privileges** and configure as follows:
    - Manage private tasks**Allow**
    - View public tasks**Allow**
    - Administration**Undefined**
    - Operation **Allow**
    - Investigation **Allow**
    - Maintenance **Undefined**
    - Alarm management**Allow**
  - ❑ Expand the branch **Action privileges** and **Allow** *Cameras*, *Access control*, *Alarms* and *Users*.
  - ❑ Click **Apply**

- ❑ Select the ***Operator*** user group's ***Access rights*** tab
- ❑ Give the Operators users group access rights to the SecurityTeam partition



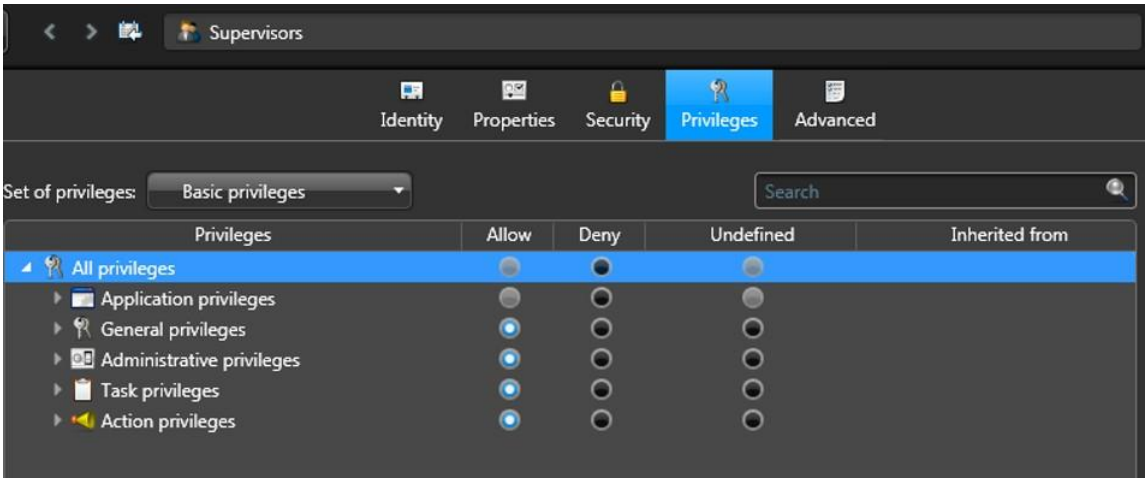
- ❑ Click ***Apply***

Members of this user group will be able to use the Security Desk application and no other applications. Within the Security Desk, members will be able to perform all *Operation*, *Investigation* and *Alarm management* tasks but no *Maintenance* nor *Administration* tasks. They will not be able to use the Config Tool to configure any system entities.

They will only be able to access entities (doors, cameras, alarms, etc.) in the ***SecurityTeam*** partition.

Create and configure a *Supervisors* user group

- ❑ Open the *Config Tool* → **Security Task** → **User groups**
- ❑ Click **Add new User group** ( ) at the bottom of the page
  - ❑ Name the new user group *Operators*. Click **Next**
  - ❑ In the **Administrative rights** page, select **Accepted users** and apply the **Provisioning** *Privilege template*. Click **Next.** Click **Create**
  - ❑ Click the new **Supervisors** user group and select its **Privileges** tab
  - ❑ Expand the branch **Application privileges**
  - ❑ Ensure that only *Security Desk, Web Client* and *Config Tool* are configured with the **Allow** privilege. All the other applications should be **Undefined**
  - ❑ Select **Allow** for all ***General privileges***
  - ❑ Select **Allow** for all ***Administrative privileges***
  - ❑ Select **Allow** for all ***Task privileges***
  - ❑ Select **Allow** for all ***Action privileges***



  - ❑ Click **Apply**

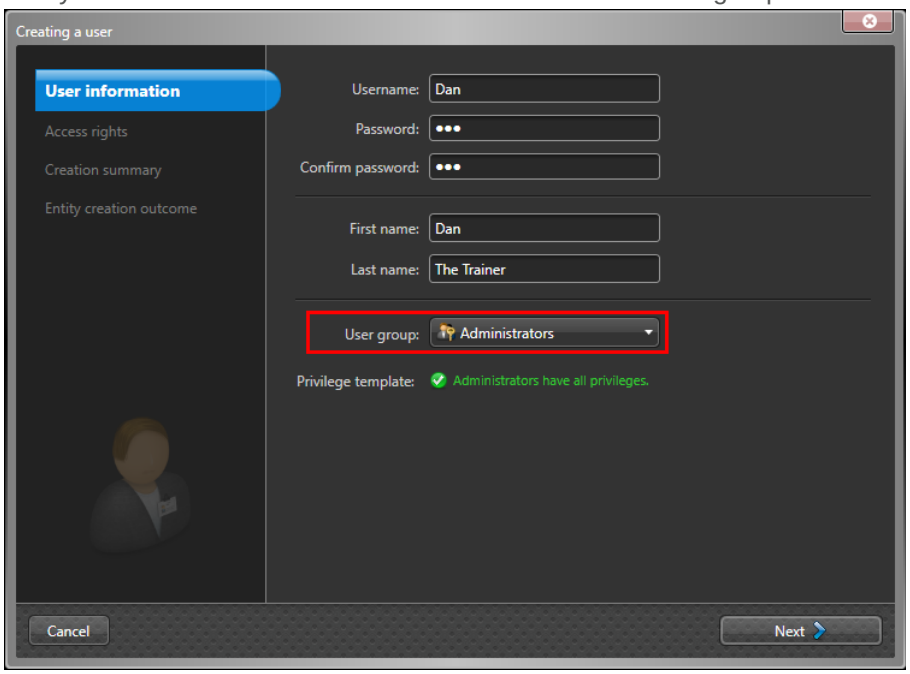
Members of this user group will be able to use the Security Desk and Config Tool applications but no other applications. They will be able to do everything within the Security Desk and Config Tool except managing other users. They are almost full system administrators.

Users

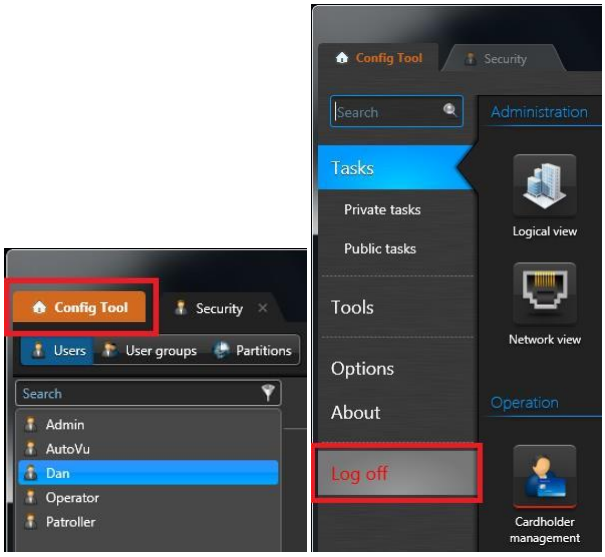
Create a 3 new user profiles

1) A new administrative user (for yourself)
2) A new operator user (basic limited user)
3) A new supervisor user (power user)

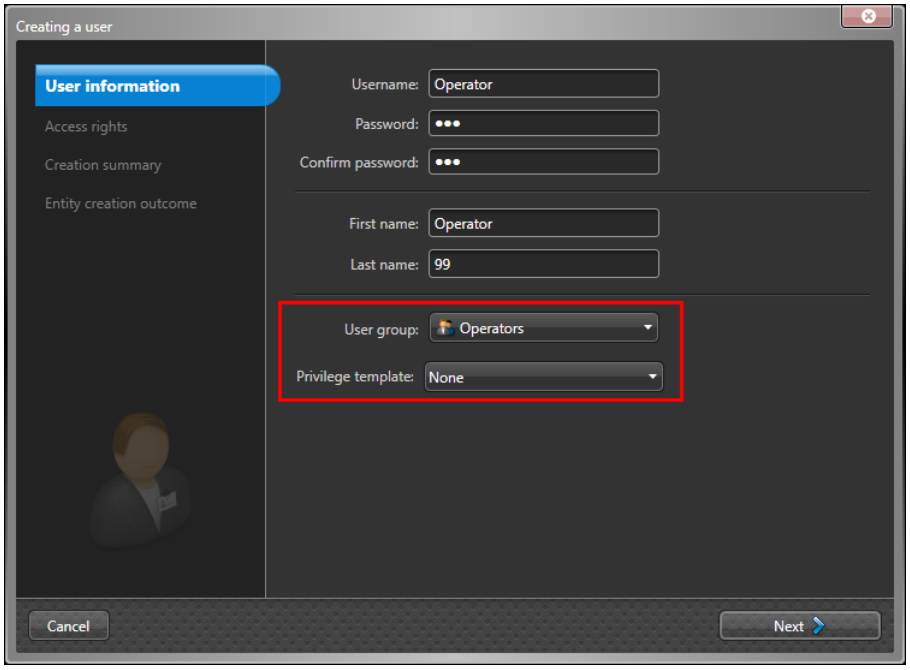
- ❑ Open the *Config Tool* → **Security Task** → **Users**
- ❑ Click **Add new User** ( ) at the bottom of the page
  - ❑ Assign a name for your new administrative user profile. Click **Next**
  - ❑ Add your new administrative user to the Administrators user group. Click Next. Click Create



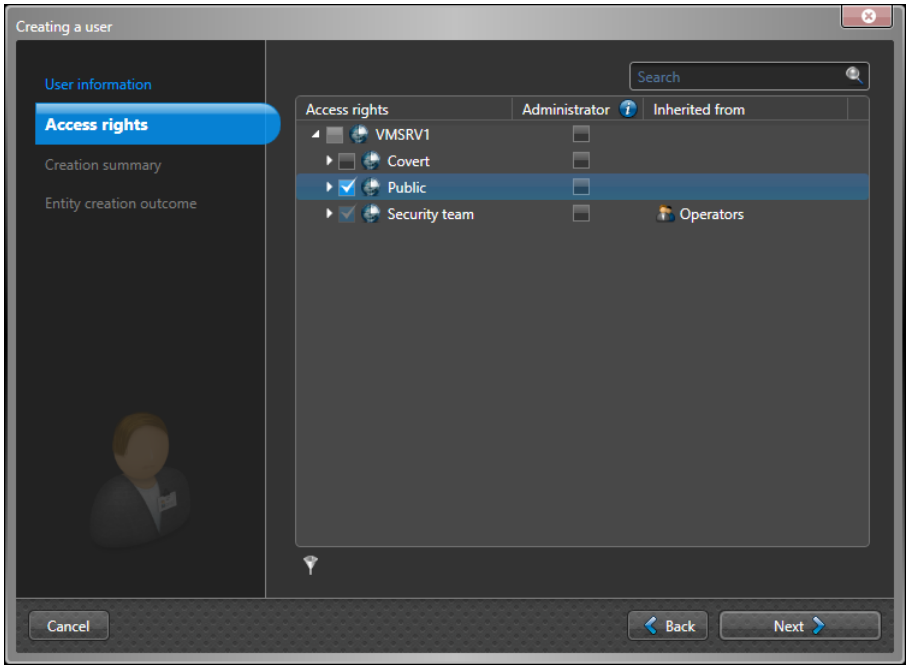
- ❑ Click the **Config Tool** *Home* tab.
- ❑ Click ***Log off***



- ❑ Log on again, this time with your new administrative user profile.
- ❑ Open the *Config Tool* → **Security Task** → **Users**
- ❑ Click **Add new User** ( ) at the bottom of the page
  - ❑ Assign a name for your new (basic) operator user profile. Click **Next**
  - ❑ Add your new user to the ***Operators*** user group. Click **Next**



  - ❑ Make your new user an **Accepted user of the public partition**. Do not apply any *Privilege template*. Click **Next**. Click **Create**.

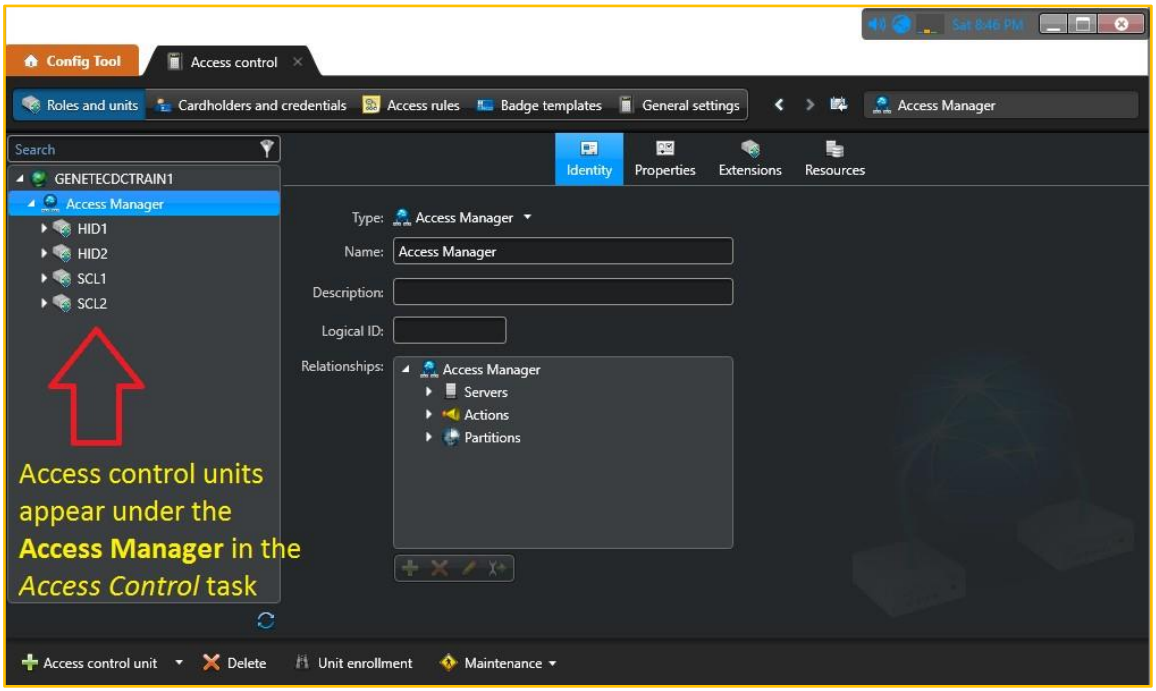


- ❑ Repeat the same steps to create a new power user except that the user group for your new power user should be the ***Supervisors***' user group.

Module 5 - Access Control Configuration

Door creation

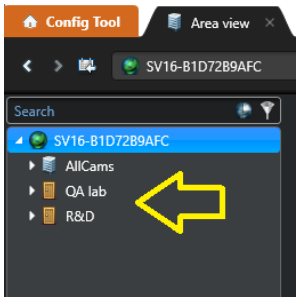
Once the physical wiring between the access control unit and the door is complete, and the access control units have been successfully enrolled into the system, the ***door*** entities can then be created.



Once the hardware units are enrolled, the doors can be created.

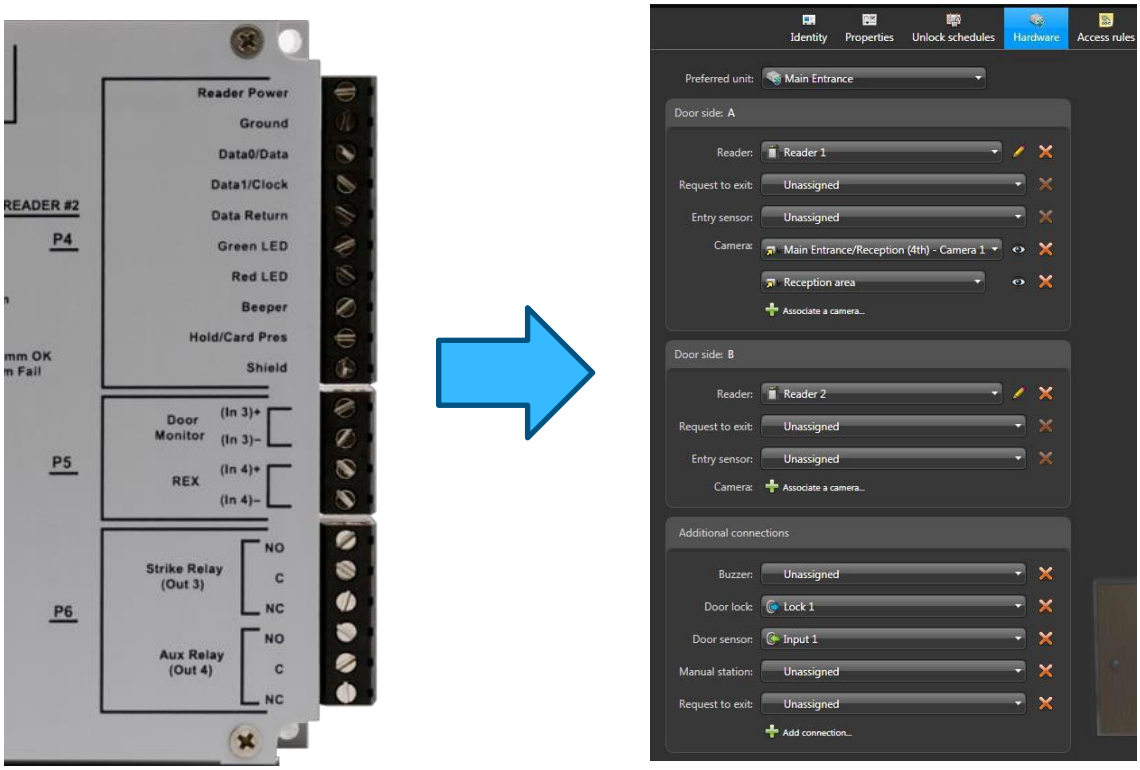
Create and configure doors

- ❑ Open the **Config Tool** → **Area View**
- ❑ Click **Add an entity** ( ) and choose **Door**
- ❑ In the **Creating a door** wizard, enter the door name and description. Click **Next**
- ❑ In the **Door information** page, assign names to the door sides (Inside/Outside, Secure/Non-secure, Entrance/Exit, East/West)
- ❑ To associate the door with the access control unit it is wired to, select a unit from the **Access control unit** drop-down list.
- ❑ Review the **Creation summary** to make sure the configuration page matches the physical wiring done at the door
- ❑ Click **Create** and **Close**. Your new door should now appear in the **Area View** tree



Validate the new door's wiring connections

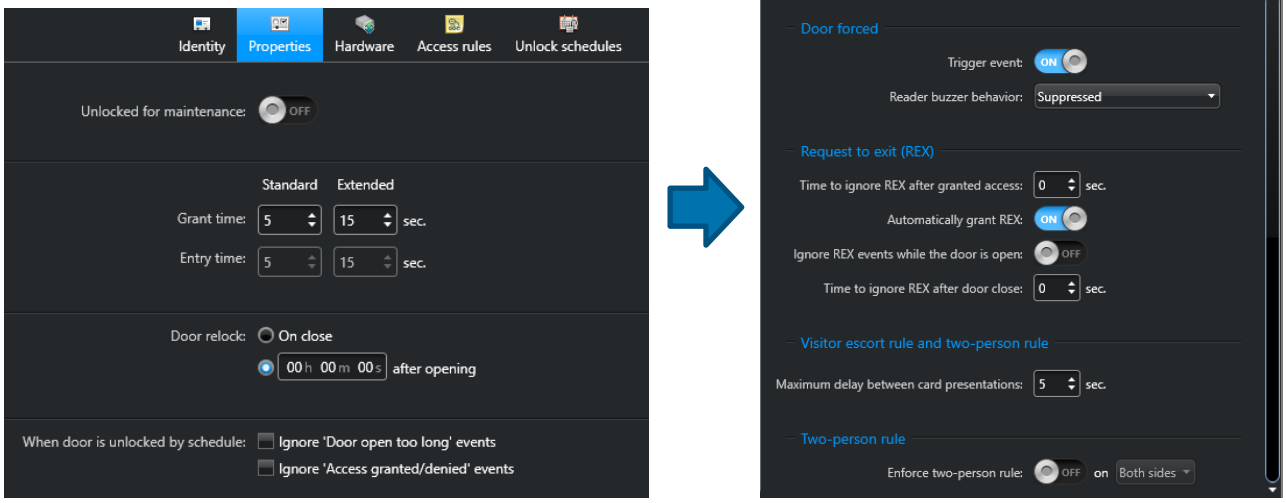
- ❑ Open the **Config Tool → Logical View** and select your new door's **Hardware** tab
- ❑ Ensure that the physical wiring connections on the access control unit itself match the wiring associations shown in the software (under your unit's **Hardware** tab)



- ❑ If you have cameras available, you can associate them to your door on this page. Note that you can link different cameras to the different sides of the door.

Validate your door's access control properties

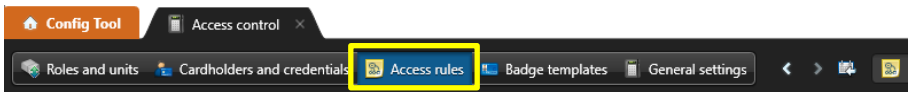
- ❑ Open the **Config Tool → Area View** and select your new door's **Properties** tab
- ❑ Ensure that the default values for ***grant time***s, ***door open too long***, ***door forced open*** and ***Request to Exit*** are all appropriate for your particular door.



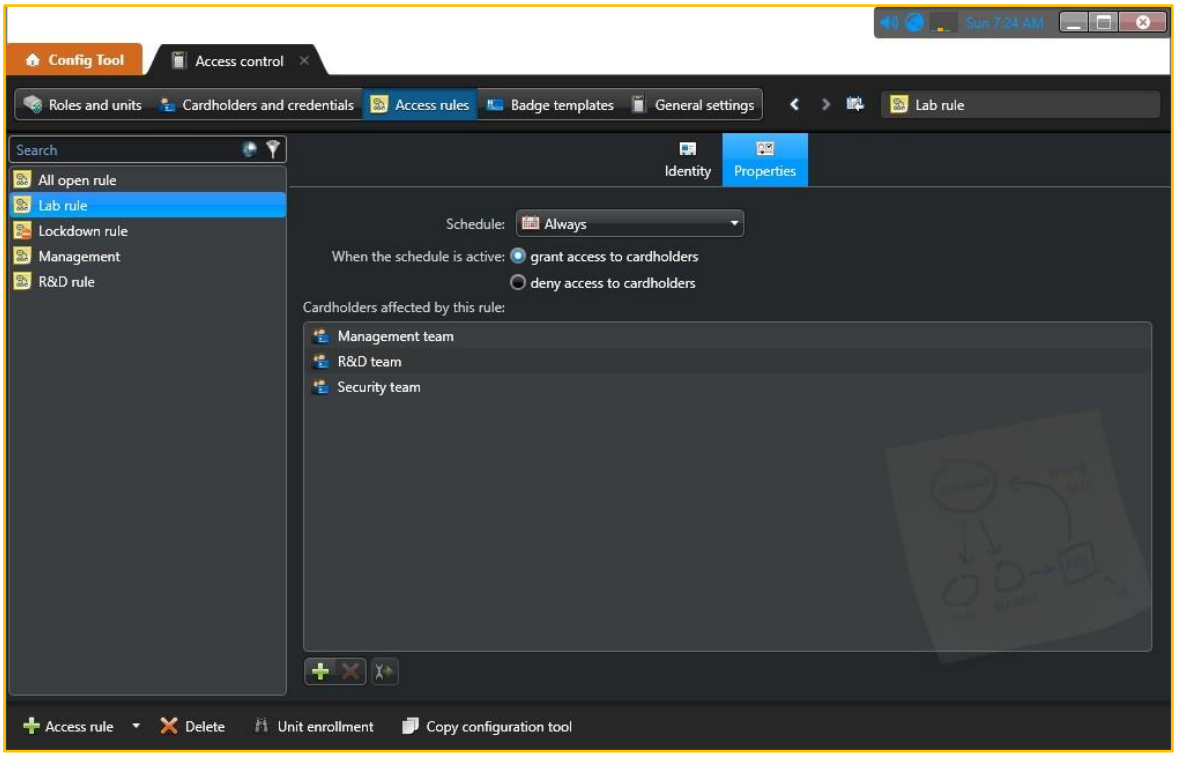
Access Rules

Create an access rule to grant your cardholders access to your doors.

- ❑ Open the **Config Tool** → **Access Control** task
- ❑ Select the **Access rules** tab

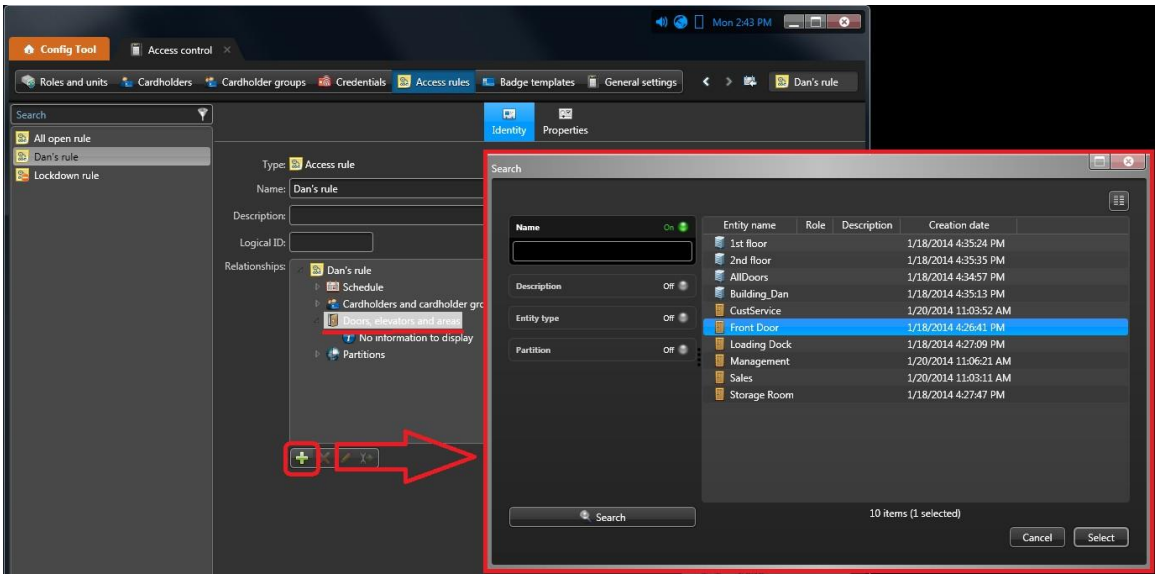


- ❑ Click Create new **Access rule** ( )
- ❑ Name the rule after yourself so it can be easily identified
- ❑ Leave you rule linked to the ***Always*** schedule. Click **Next**.
- ❑ Click **Create**. Click **Close**.
- ❑ Once your rule has been created, select the **Properties** tab of your rule
- ❑ Add a cardholder (and/or a cardholder group). Click **Apply**.

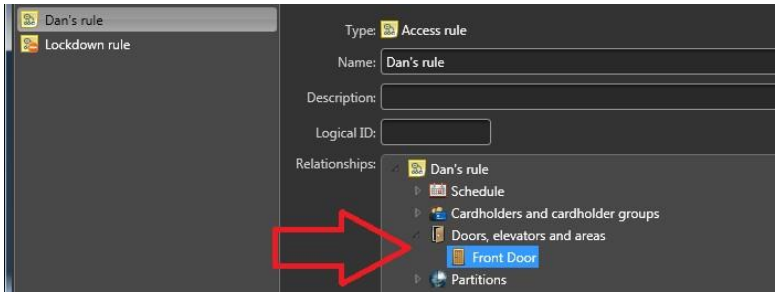


Assign your access rule to a door

- ❑ Stay in the **Config Tool → Access Control** task
- ❑ Select your access rule's **Identity tab**. Click ***Doors, elevators and areas***
- ❑ Click the green plus ( ) to link a door to your rule. Choose your door.



- ❑ Click **Select**. Click **Apply.** Your rule should now be linked to your door.



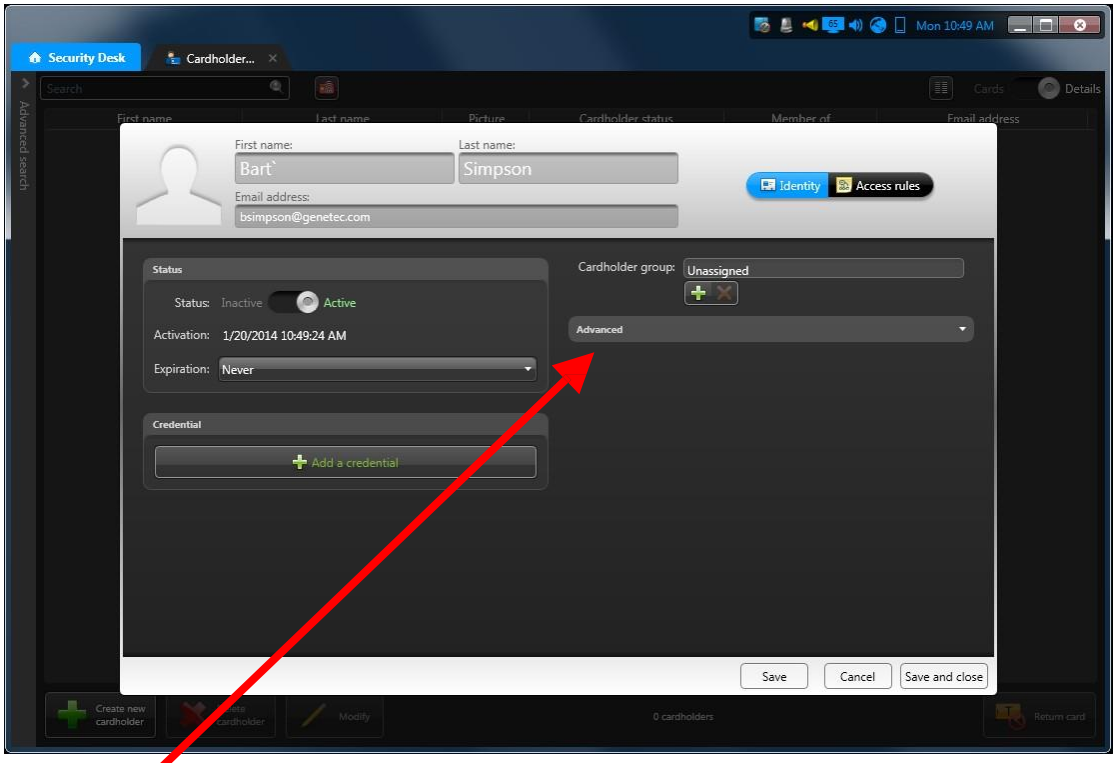
Cardholders & Credentials

The **Cardholder Management** task can be used to create cardholders, enroll credentials and assign them to the cardholders. This is an *Operation* task that can be found in both the *Config Tool* and the *Security Desk*.

- ❑ Download 3 images of people's faces from *Google Image search*. These will be used for your cardholder photos. They should be one of the following file formats: *.bmp, *.jpg, *.jpeg, *.gif, *.png.

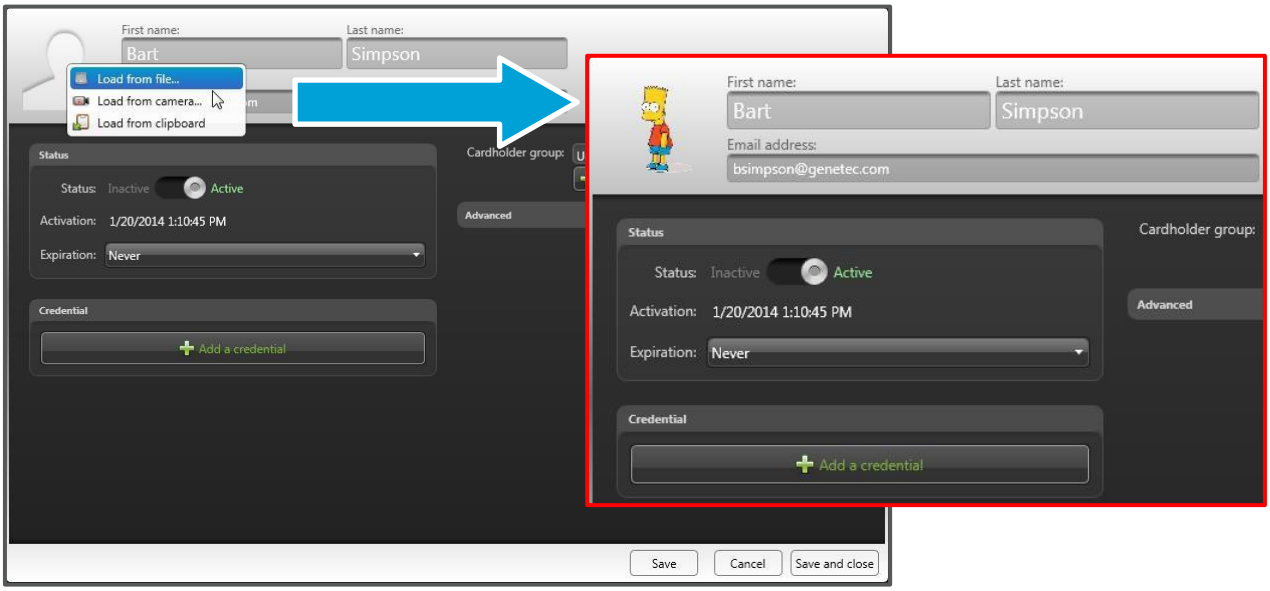
- ❑ Open the **Config Tool → Cardholder Management** task
- ❑ Click Create new cardholder ( ). 3 At the top of the dialog box, enter the cardholder's first name, last name, and e-mail address.

  NOTE If the software language (chosen at installation) is latin-based, the Name field is configured as the first name followed by the last name. This order is reversed if you are using an Asian language such as Japanese or Chinese.

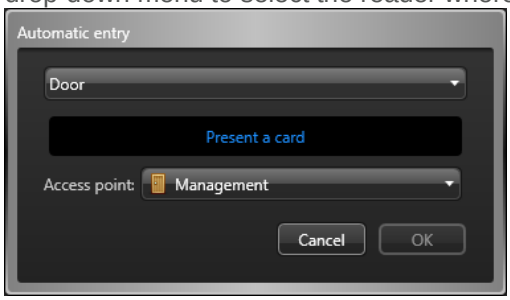


- ❑ Click ***Advanced*** and set your 3 cardholders ***Security clearance*** to different values (0 = highest priority and 99 = lowest priority)
- ❑ To assign a picture to the cardholder, click the silhouette and select one of the following options:
  - ✓ ***Load from file***. Select a picture from disk. All standard image formats are supported.
  - ✓ ***Load from webcam***. Take a snapshot with your webcam. This option appears only if you have a webcam attached to your workstation.
  - ✓ ***Load from camera***. Take a snapshot from a camera managed by Security Center.
  - ✓ ***Load from clipboard***. Load the picture copied to the clipboard. This option appears only if you used the Windows copy command to save a picture onto your clipboard.

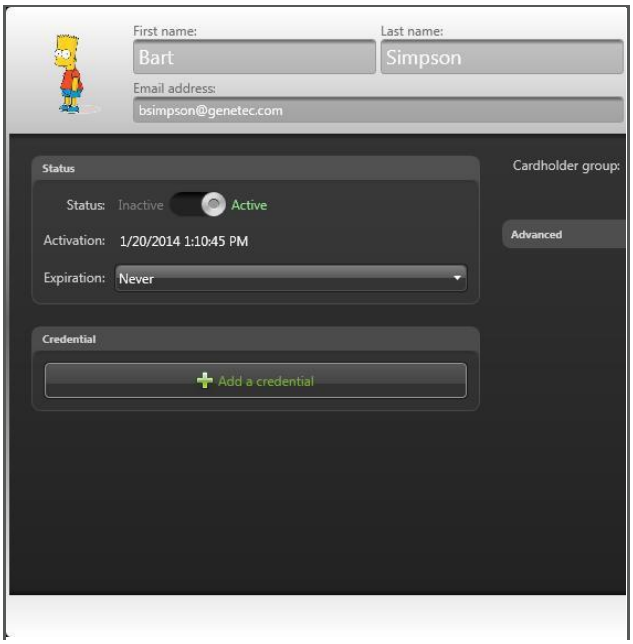
    NOTE If you select ***Load from camera***, a separate capture dialog box appears. Simply select the video source and click ***Take snapshot*** ( )



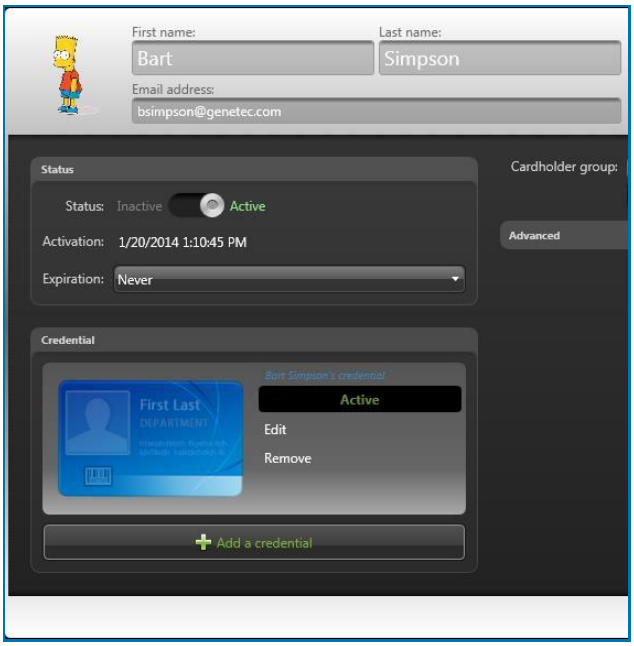
- ❑ To edit the picture, click it to open the **Image editor** and use the editing options at the top of the editor's dialog box.
- ❑ In the Status section, set the following:
  - ✓ *Status*. Set the cardholder status to **Active**.
    If the cardholder status is inactive, then the credentials assigned to the cardholder do not work, and the cardholder does not have access to any area.
  - ✓ *Activation*. Displays the current date.
  - ✓ *Expiration*. Set the cardholder to expire *Never*, on a specific date, or after a specified number of days after the first use.
- ❑ Click **Save**. Do not close the cardholder properties window.
- ❑ Click **Add a credential** (✚). Select **Automatic entry**
- ❑ In the ***Automatic entry*** dialog box, choose **Door** (instead of USB Reader) and click the Access point drop-down menu to select the reader where you will present your card



- The card read should cause the credential to be associated with your cardholder. This can be seen/validated in the ***Credential*** section of the **Cardholder Management** task

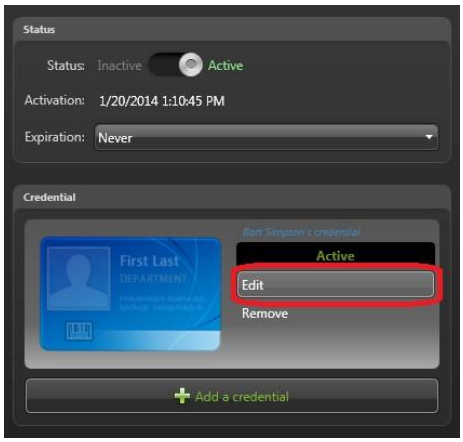


Cardholder properties **without** a credential

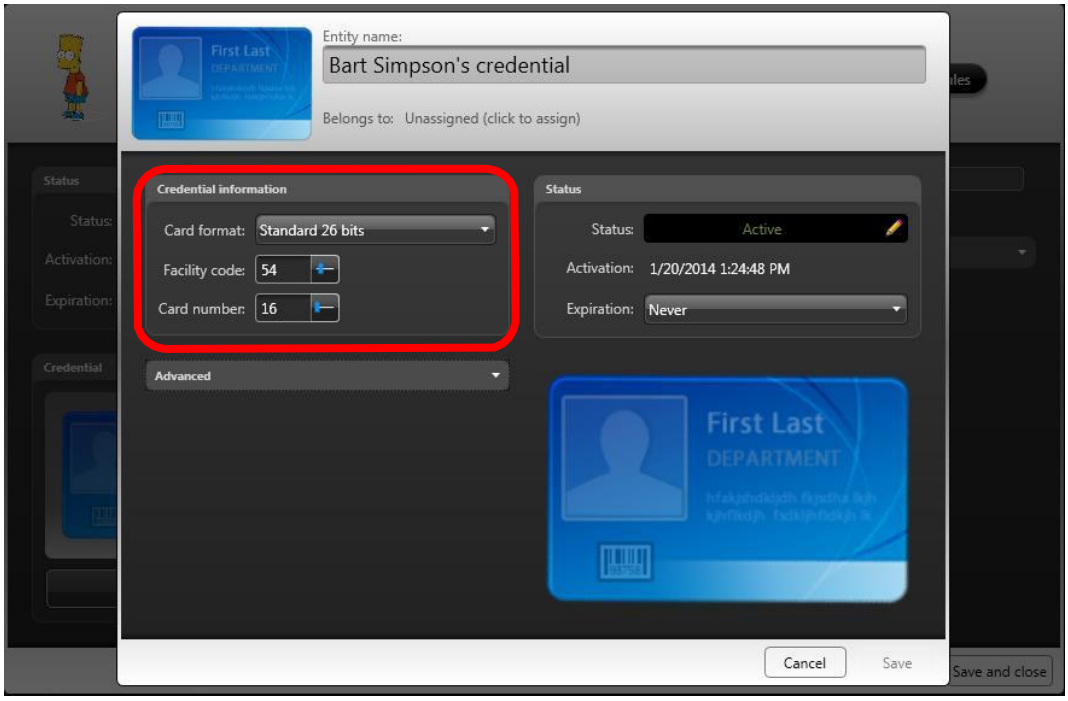


Cardholder properties **with** a credential

- To validate the card read click **Edit**



- The ***Card format***, ***Facility code*** and ***Card number*** can be validated in the credential properties window



- Click **Cancel**
- If your cardholder's credential information looks correct, click **Save and close**.

Credential Management task (Optional)

The Credential Management task allows you to add large numbers of new credentials to a system quickly. Two modes are available:

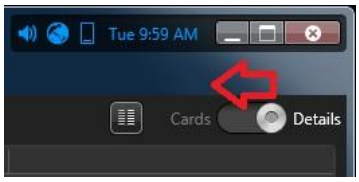
- **Automatic** mode allows reading of cards on a reader of choice (or a USB reader)
- **Manual** mode allows a user to set the parameters manually and specify the range of card numbers.

With either mode, naming convention, active status, partition membership, etc. can be set before credentials are added. Once credentials are shown in the list, the **Enroll** button at the bottom right will insert them into database. Feature useful for sites that use Visitor Management Temp Card features and wish a "pool" of credentials available in system.

The Credential Management task is an operation task that can be found in both *Config Tool* and *Security Desk* applications.

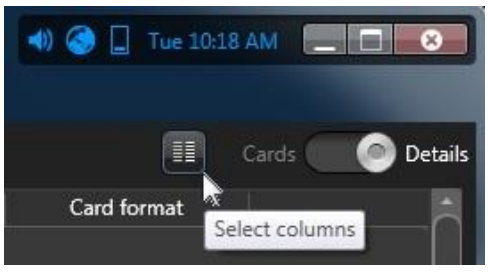
Familiarize yourself with the Credential Management task

- ❑ Open the **Config Tool** → **Credential management** task
- ❑ Toggle from ***Details*** view to ***Card*** view

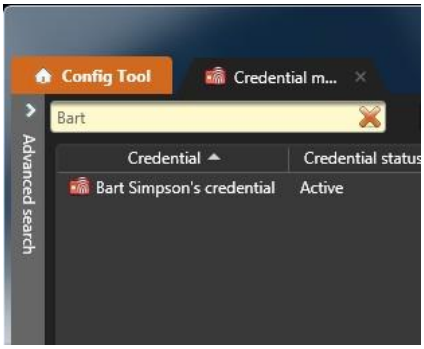


- ❑ Click the ***Zoom*** slider and try different zoom levels

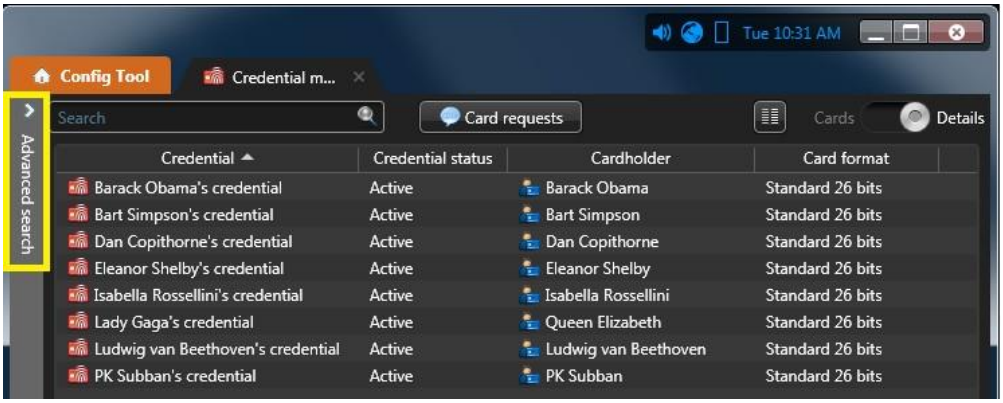
- ❑ Toggle back to ***Details*** view
- ❑ Click the ***Select columns*** button



- ❑ Remove ***Picture*** from the **Selected columns** list. Click **OK**
- ❑ Type 3 or 4 letters in the ***Search*** field. Does it filter your list of credentials accordingly?



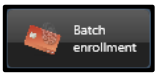
- ❑ Click the arrow to open the Advanced Search pane



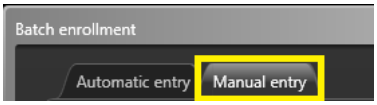
- ❑ Toggle **On/Off** the different search filters to familiarize yourself with the searching options available.
- ❑ Close the ***Advanced search*** pane

Enroll 10 new unassigned credentials as a batch

- ❑ Click the ***Batch enrollment*** button in the bottom right hand corner

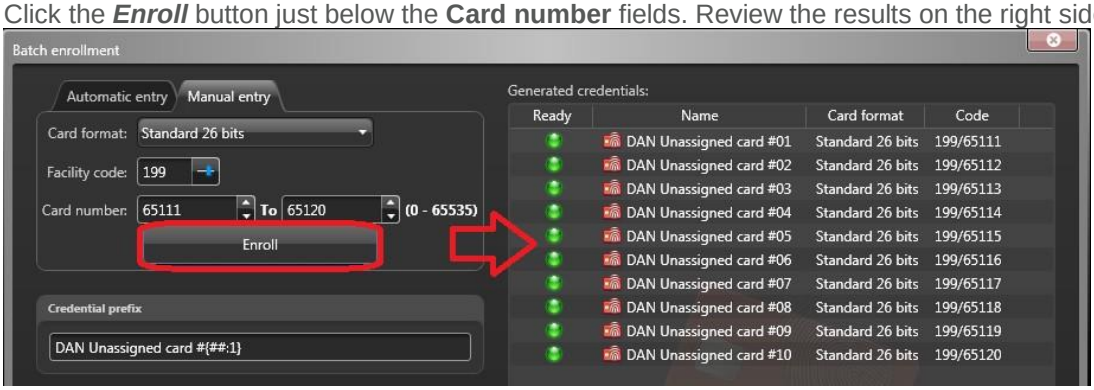


- ❑ In the **Batch enrollment** window, select the ***Manual entry*** tab

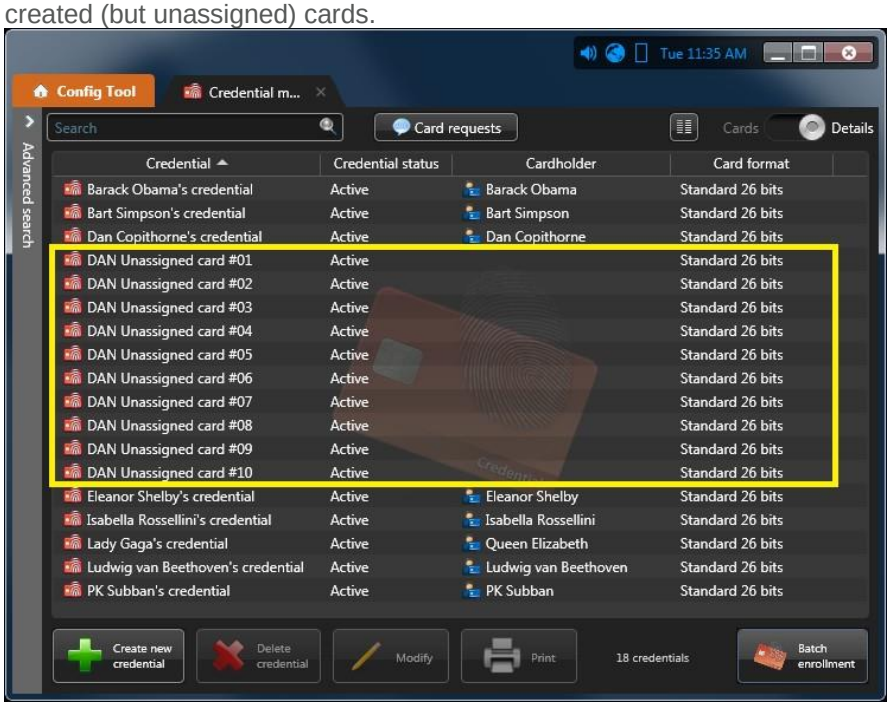


- ❑ Set the **card format** to ***Standard 26 bits***
- ❑ Choose a random number between 0-255 to apply as ***Facility code***
- ❑ Set the ***Card number*** values to a range of 10 consecutive numbers between 0-65535
- ❑ Set the ***Credential prefix*** field to:
  (YourNameHere) `Unassigned card #{##:1}`

- ❑ Click the ***Enroll*** button just below the **Card number** fields. Review the results on the right side.



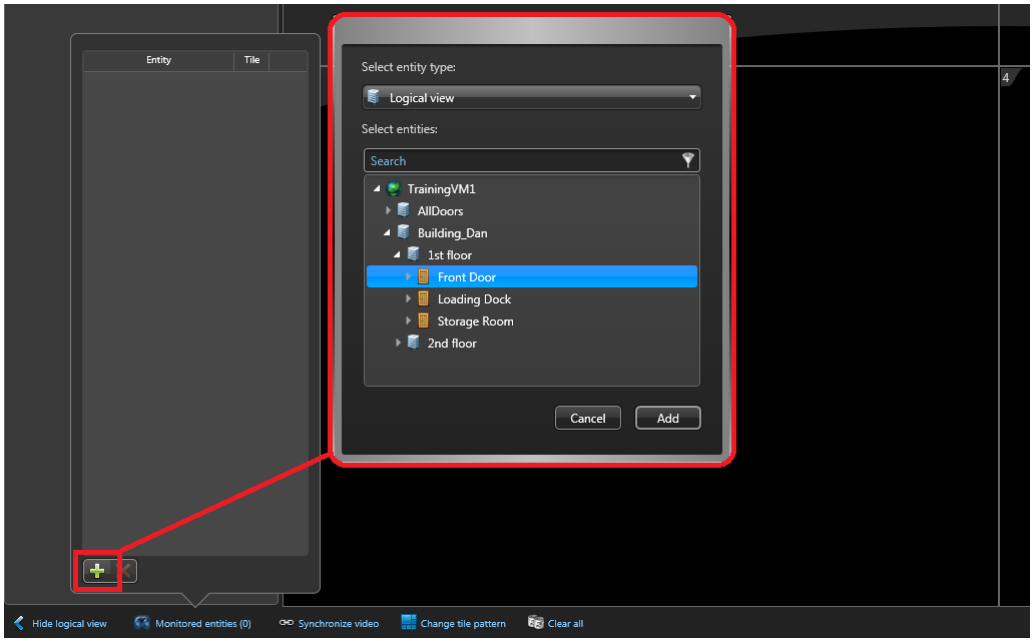
- ❑ Click the ***Enroll*** button at the bottom right hand corner of the window.
- ❑ Click ***Cancel*** to close the window. Your Credential Management task should now show all the newly created (but unassigned) cards.



Test your door, cardholder, credential and access rule configurations

To test you configurations so far, you will monitor your door(s) in the Security Desk

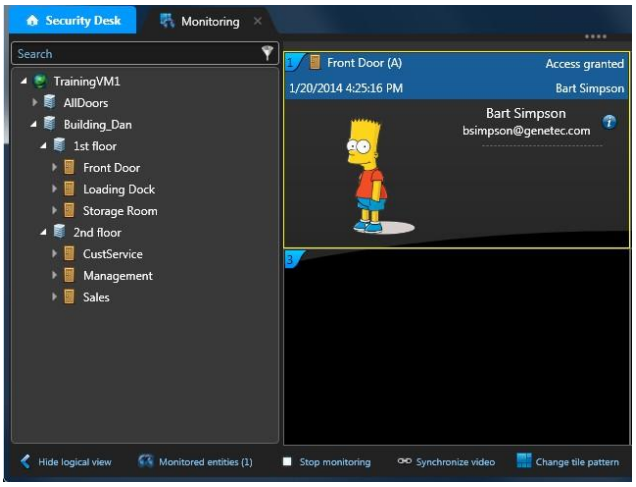
- ❑ Open the **Security Desk → Monitoring** task
- ❑ Click the button **Monitored entities** ( ) at the bottom of the page
- ❑ Click Add ( ) and navigate the logical tree to select your door(s). Click **Add**



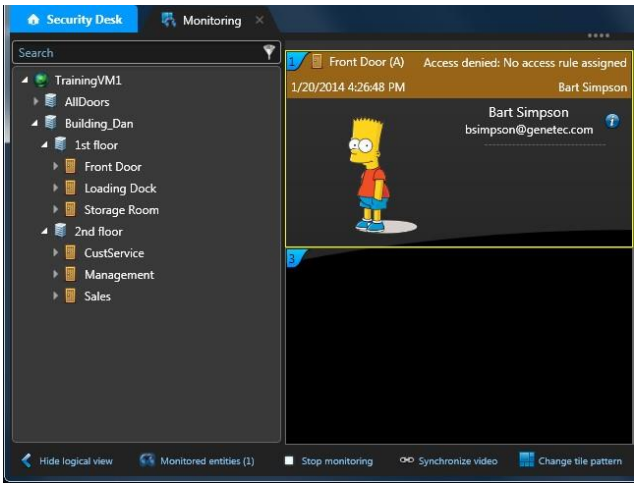
- ❑ Click any tile to make the monitored entities list disappear. Your ***Monitored entities*** icon should now display a number indicating how many entities you are actively monitoring

- ❑ Present a card to the reader of the door that you are monitoring. You should see an event appear in your Security Desk Monitoring task. We expect to see ***access granted*** for the cardholder that you added to the rule controlling your door.
- ❑ Try presenting someone else's card that is not linked to the access rule on your door. We expect to see an ***access denied*** event. Furthermore, access denied events are followed by:
    a) **Access denied: *No access rule assigned*** (The cardholder is not named in any rules assigned to the door)
    b) **Access denied*: Denied by access rule*** (The cardholder is explicitly named in a "Deny" rule)
    c) **Access denied: *Unknown credential*** (The card has not been enrolled in the system)
    d) **Access denied: *Unassigned credential*** (The card has been enrolled but not assigned to a cardholder)
    e) **Access denied: *Inactive credential*** (The credential is enrolled but is in "Inactive" state)
    f) …and many more (*Antipassback violation*, *Lost/Stolen card*, *Out of schedule*, etc)

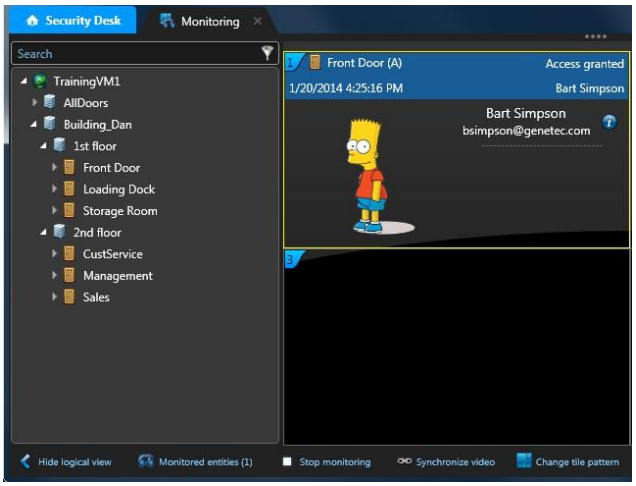
Examples of some *access granted* and *access denied* events:



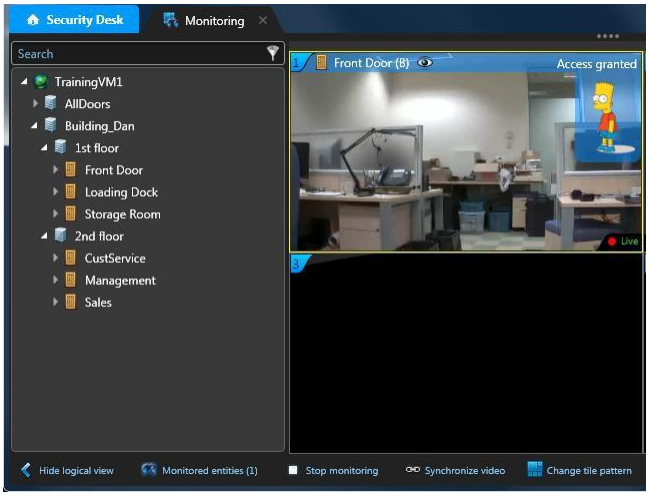
Access granted event



Access denied because cardholder is not in the rule.



Door has no camera linked to it



Door has a camera linked to it.

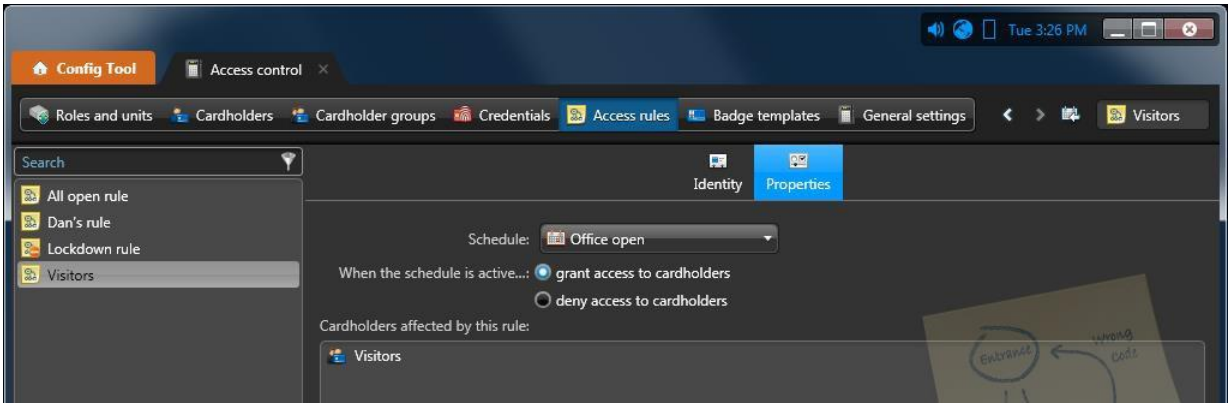
Visitor Management task (Optional)

In many respects, the **Visitor Management** task is similar to the **Cardholder Management** task. Unlike the **Cardholder Management** task, the **Visitor Management** task can only be found in the ***Security Desk***.

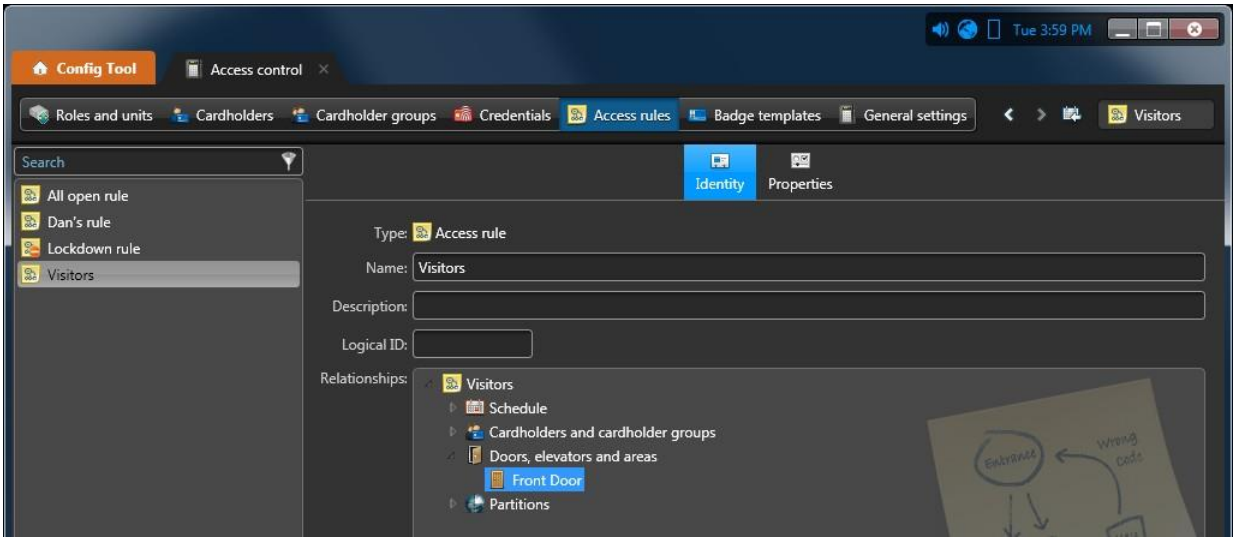
Before you begin

Make sure that you have at least 1 unassigned card available to assign to visitors. Use the built-in *cardholder group* reserved for visitors in Config Tool, and assign *access rule(s)* to the group. This is how Security Center grants access rights to visitors, access rules cannot be directly linked to a visitor.

- ❑ Open the **Config Tool** → **Access Control** task select ***Access rules***
- ❑ Create a new visitors rule granting access to the ***Visitors*** cardholder group
- ❑ If you have a "business hours" schedule is available, apply it to your ***Visitors*** rule. Click **Apply**



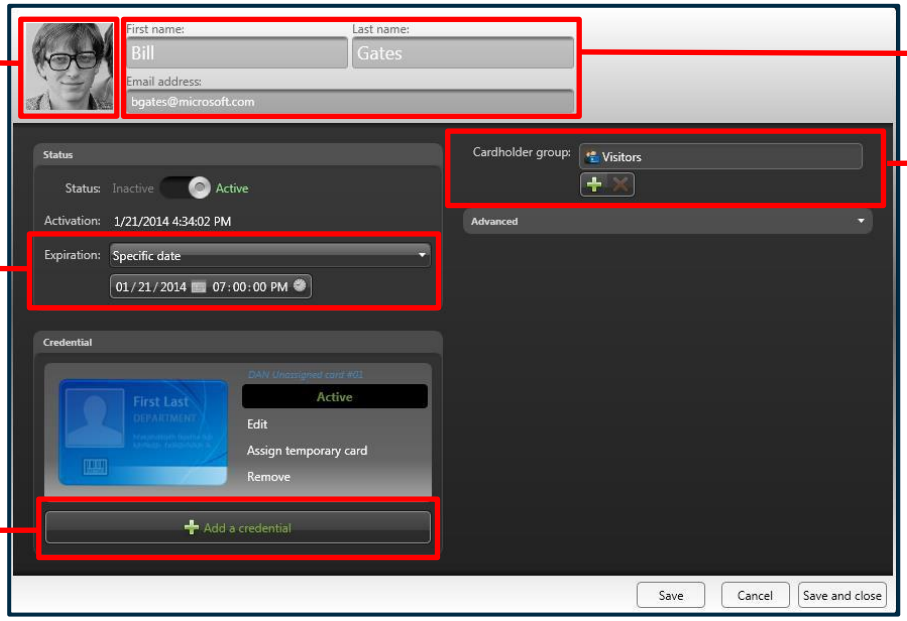
- ❑ Select your ***Visitors*** rule's **Identity** page to link it to a door.
- ❑ Expand the branch Doors, elevators and areas. Select it. Click Add ( ), select a door. Click **Apply**



Now anyone added to the ***Visitors*** cardholder group should have access granted at the front door (only during the ***Office open*** hours)

Checking in a new visitor

- ❑ Open the **Security Desk → Visitor management** task
- ❑ To check in a new visitor, click the **Check-in** button (Check-in) at the bottom of the page and complete the following:



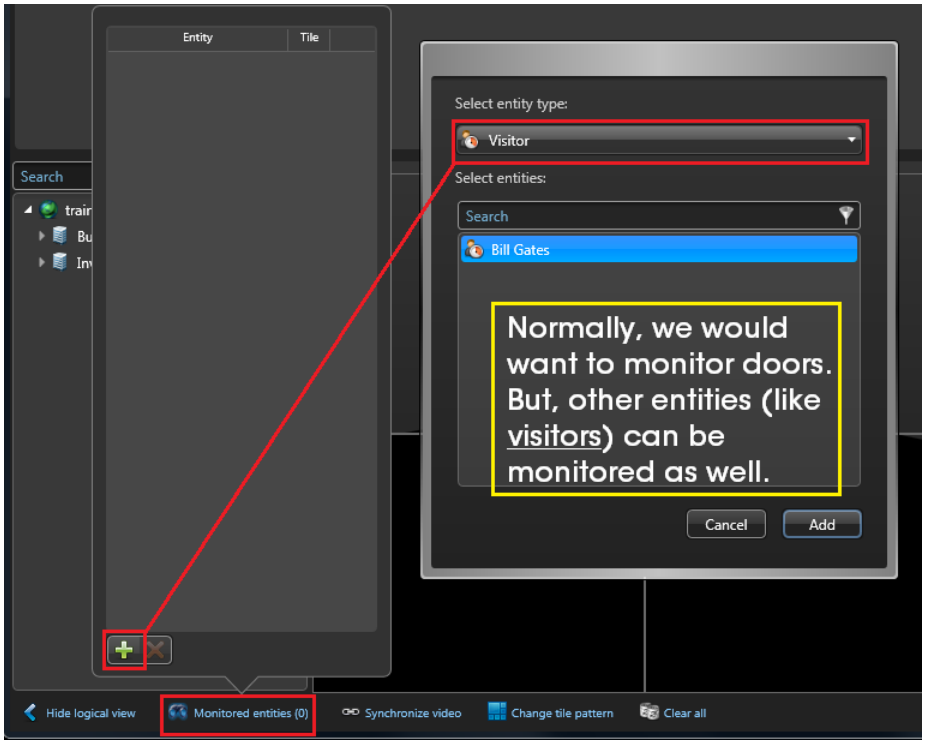
- ➢ To assign a picture to the visitor, click the silhouette and select one of the following options:
  - **Load from file**. Select a picture from disk. All standard image formats are supported.
  - **Load from webcam**. Take a snapshot with your webcam. This option appears only if you have a webcam attached to your workstation.
  - **Load from camera**. Take a snapshot from a camera managed by Security Center.
  - **Load from clipboard**. Load the picture copied to the clipboard. This option appears only if you used the Windows copy command to save a picture onto your clipboard.

  NOTE If you select ***Load from camera***, a separate capture dialog box appears. Simply select the video source and click Take snapshot ( ).

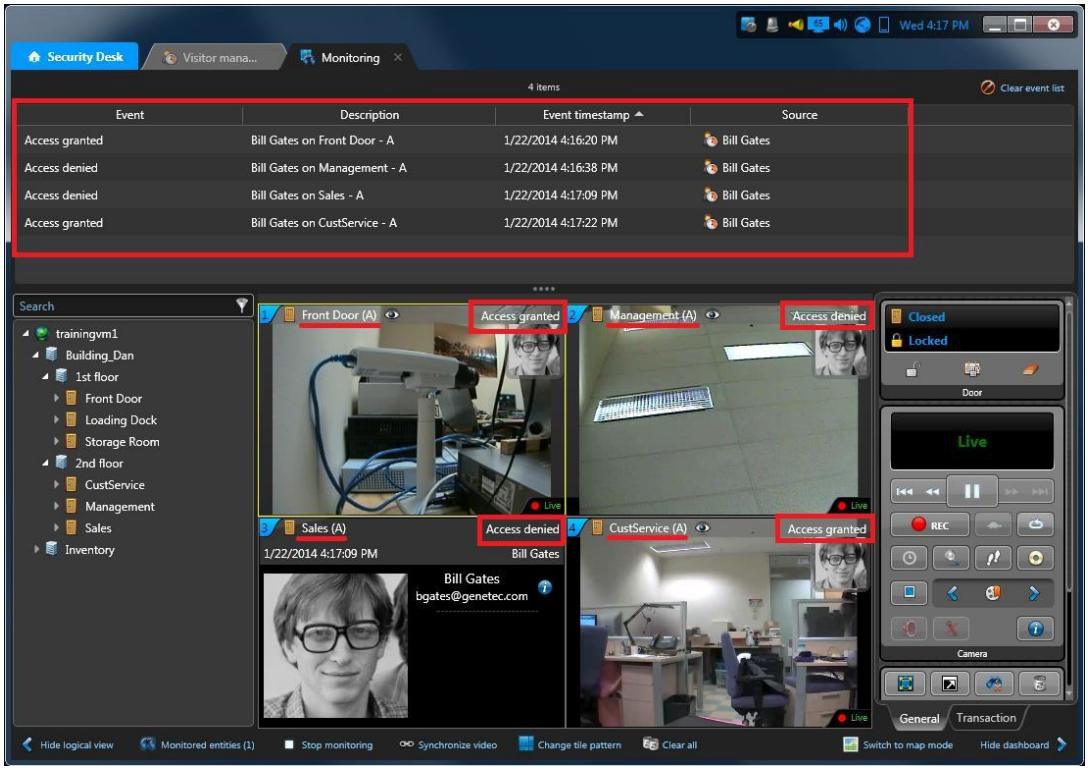
- ❑ Click **Save and close**. The new visitor should now be added to the list of visitors.

Monitoring visitors

- ❑ Open the **Security Desk → Monitoring** task
- ❑ Add the visitor(s) as monitored entities

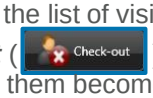


- ❑ Present the visitor's card to 2 different doors. The visitor should get an access granted event on certain doors and access denied on others.



Checking out visitors

Open the **Security Desk** → ***Visitor Management*** task

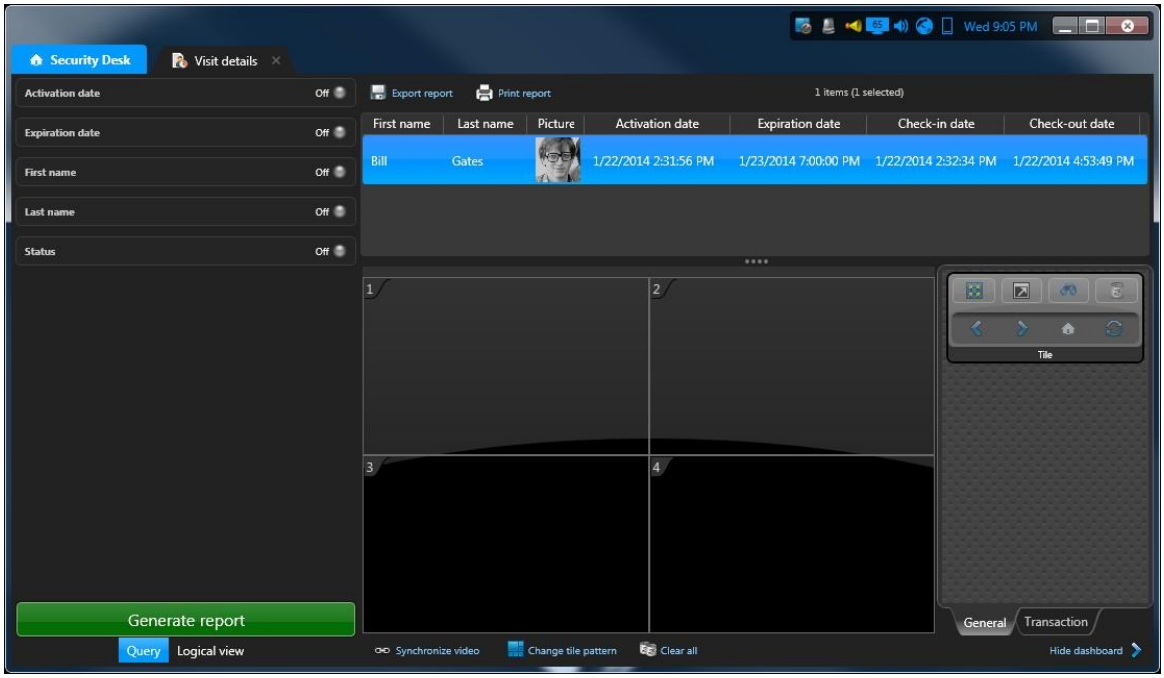
- ❑ Select a visitor from the list of visitors in the **Visitor Management** task
- ❑ Click the ***Check-out*** () button at the bottom of the page.
  The visitor's "status" them becomes de-activated (but not deleted)
  The visitor's card is put back into the pool of "unassigned credentials"

Visitor reporting

Two kinds of investigation tasks are available in the Security Desk for visitor reporting:

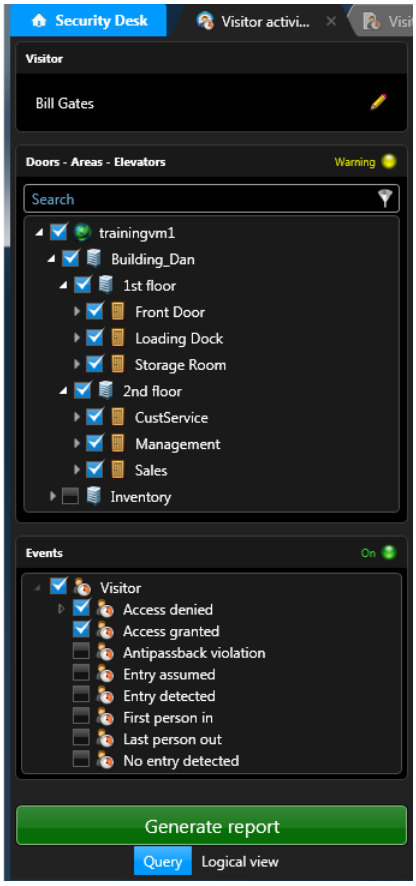
1. ***Visit details*** task
2. ***Visitor activities*** task

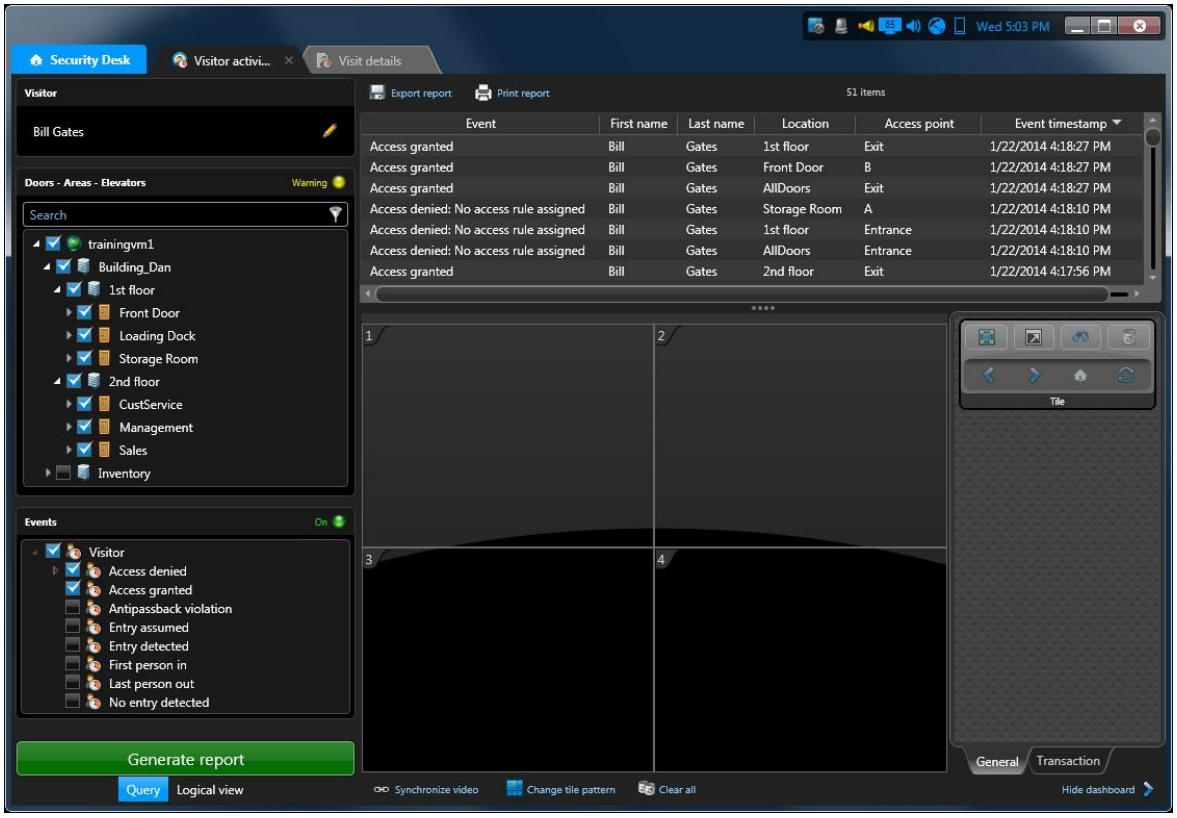
- ❑ Open the **Security Desk** → ***Visit details*** task
- ❑ Leave all search filters on the left ***OFF*** and click ***Generate report***
- ❑ The results displayed include a row for each visit.



- ❑ Right click one of the column headers and click ***Select columns***
- ❑ Select ***Picture*** and click ***Remove*** ( ). Click ***OK***
- ❑ Click ***Export report*** ( )
- ❑ Select a ***file format*** and ***destination***. Click ***Save***.
- ❑ Minimize the **Security Desk** and examine the report that was just exported.

- ❑ Open the **Security Desk** → ***Visitor activities*** task
- ❑ In the search pane on the left, click the pencil icon to select a visitor
- ❑ Select some or all areas and doors to query by placing check marks in the logical tree
- ❑ Click ***Events***. Select the ***Access granted*** and ***Access denied*** events.
- ❑ Click ***Generate report***





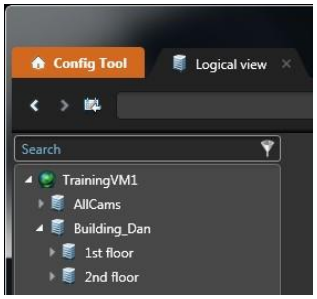
Module 6 - Additional Configurations

Organize the *Area view*

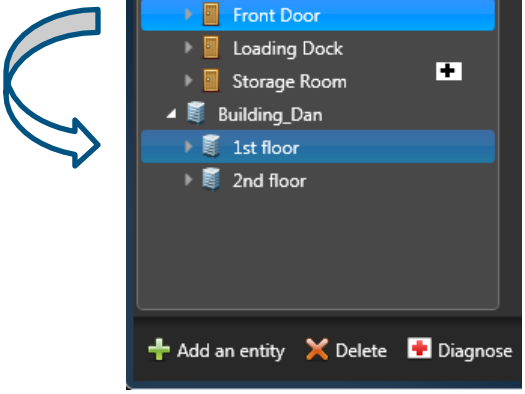
Creating and configuring the logical tree structure

The logical tree structure is what will be seen by the users when searching for an entity like a camera or door. You goal should be to create a logical structure that will be efficient and easy for the users to navigate.

- ❑ Open the **Config Tool** → **Logical view** task
- ❑ Your trainer should have already created an area called **AllDoors**
- ❑ Drag and drop your door into the **AllDoors** area
- ❑ Select the directory ( ) at the top of the logical tree
- ❑ Click **Add an entity** ( ) → **Area**
- ❑ Assign the name ***Building**_(your name)* to your new area
- ❑ Select your new building area. Click **Add and entity** and create a sub-area to your building area called ***1st floor***.
- ❑ Select your new building area. Click **Add and entity** and create a sub-area to your building area called ***2nd floor***.



- ❑ While holding the ***Ctrl*** key on your keyboard, drag and drop your door from the ***AllDoors*** area into your building's ***1st floor*** area. (This will place a copy of your door instead of moving your door to the destination area)

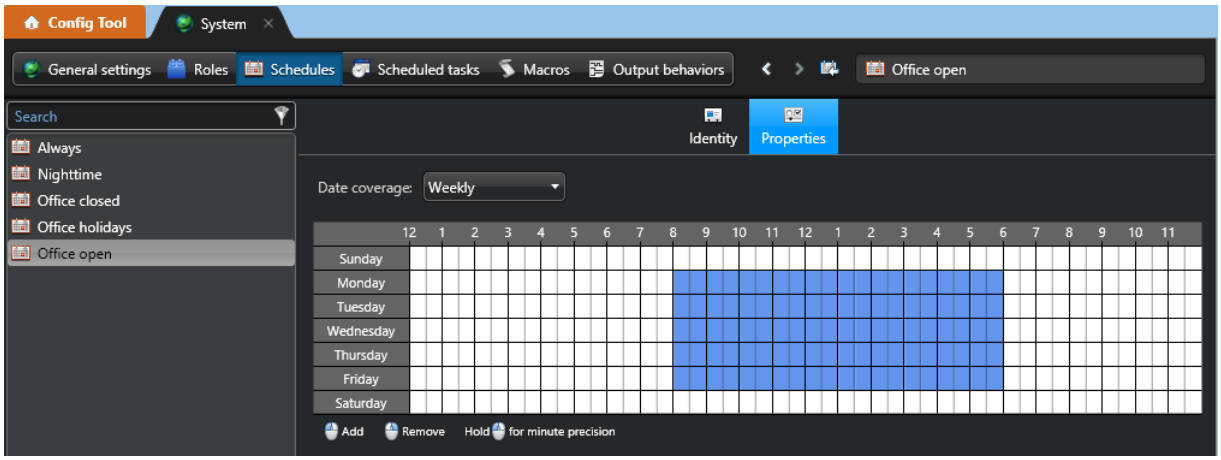


Schedules

Use the Config Tool to create and configure 3 office schedules. These can be used to control video quality, user logon hours, motion detection sensitivity, recording triggers, etc.

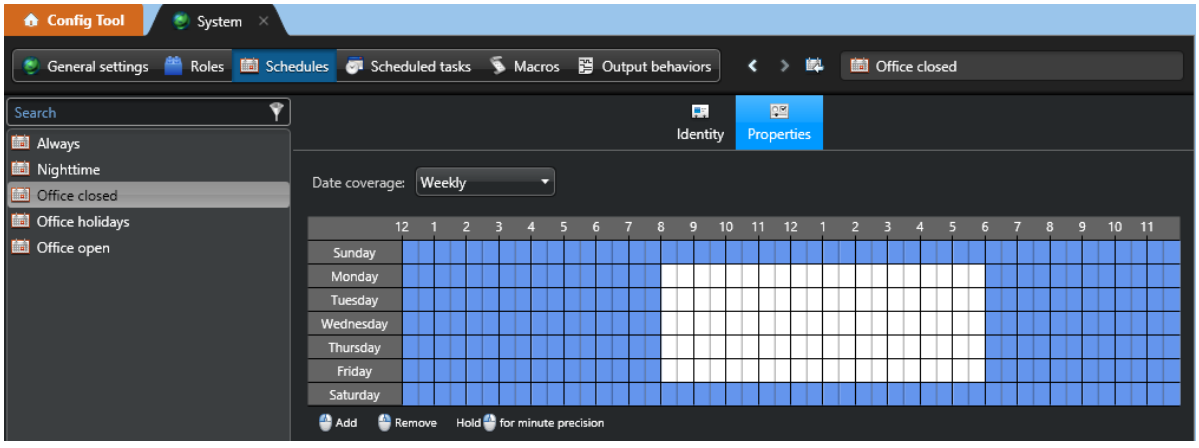
Create and configure an *office hours* schedule:

- ❑ Open the **Config Tool** → **System view** *task* → **Schedules**
- ❑ Click **Add an schedule** (**Schedule**)
- ❑ Name your schedule *(YourName)*_**OfficeOpen**
- ❑ Select your new schedule's **Properties** tab
- ❑ Set the **Date coverage** to ***Weekly***
- ❑ Using your mouse, click and select Monday 08:00 → Friday 18:00. Click **Apply**



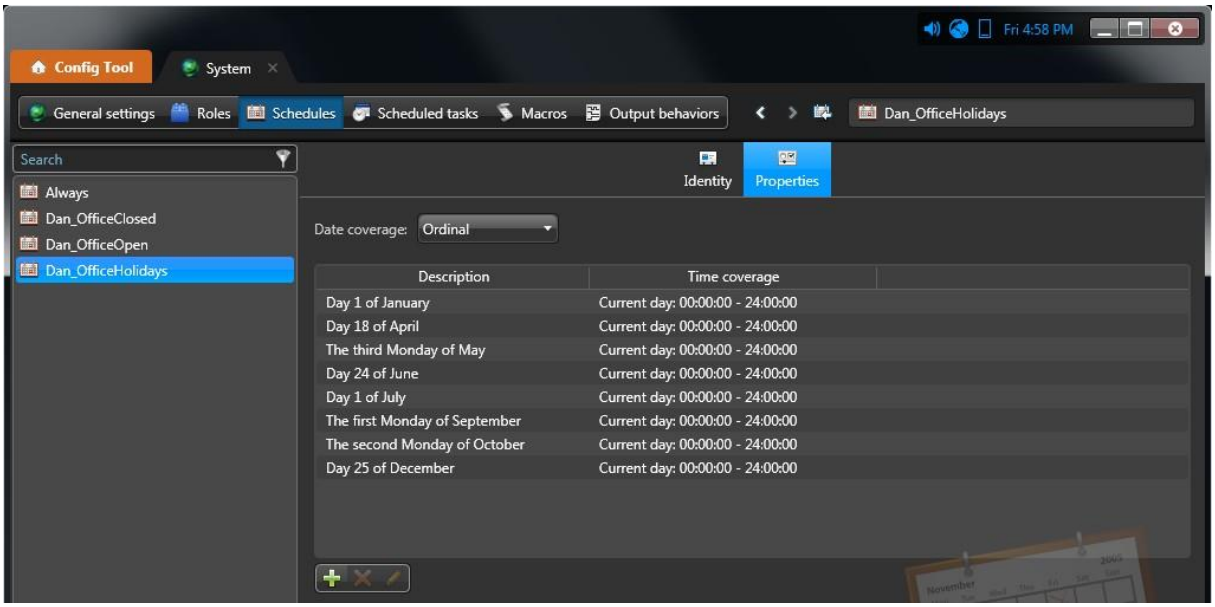
Create and configure an *office closed* schedule:

- ❑ Click **Add an schedule** (**Schedule**)
- ❑ Name your schedule *(YourName)*_**OfficeClosed**
- ❑ Select your new schedule's **Properties** tab
- ❑ Set the **Date coverage** to ***Weekly***
- ❑ Using your mouse, click and select the opposite of Monday 08:00 → Friday 18:00. Click **Apply.**
  (**Tip:** While left-clicking selects a cell, right-clicking empties a cell)



Create and configure an *office holidays* schedule:

- ❑ Click **Add an schedule** (**Schedule**)
- ❑ Name your schedule *(YourName)*_**OfficeHolidays**
- ❑ Select your new schedule's **Properties** tab
- ❑ Set the **Date coverage** to ***Ordinal***. Add ( ) the following:
  - ❑ Day 1 of January
  - ❑ Day 18 of April
  - ❑ The third Monday of May
  - ❑ Day 24 of June
  - ❑ Day 1 of July
  - ❑ The first Monday of September
  - ❑ The second Monday of October
  - ❑ Day 25 of December
- ❑ Click **Apply**

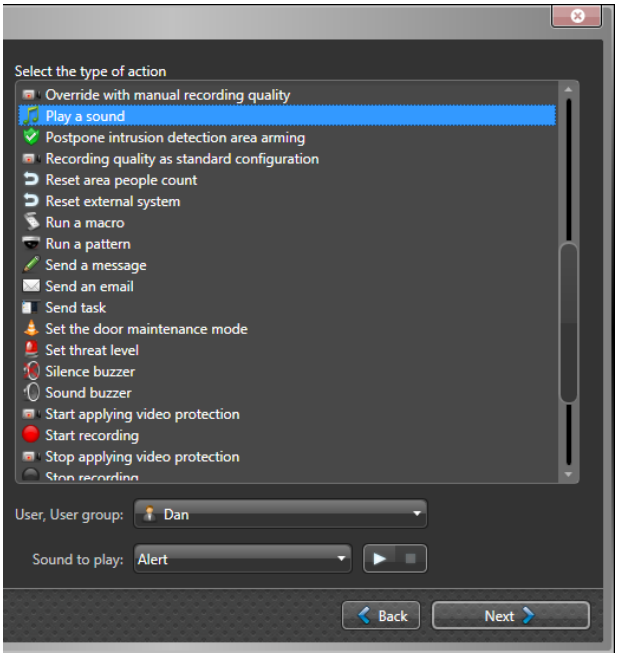


Event Handling

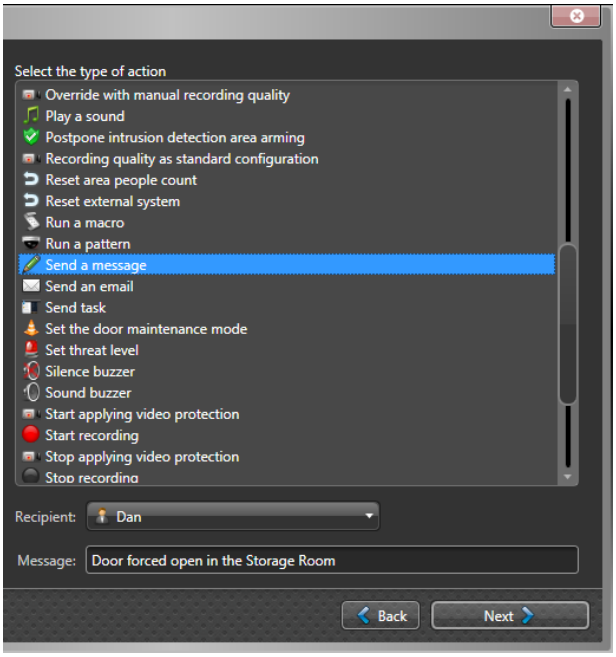
Link an automated action to an event

Create an audible alert or a pop-up message whenever the event *Door forced open* is fired

- ❑ Open **Config Tool** → **System** task → **General settings** and select the ***Actions*** tab
- ❑ Click ***Add an item*** ( ) at the bottom of the pane on the right side to add a new action
- ❑ Select the source entity that will file the event. In this case, select **Door**. Click **Next**
- ❑ Select your specific door from the logical tree. Click **Next**
- ❑ Select the event ***Door forced open***. Click **Next**
- ❑ For the "**Action**", select either **Play a sound**, or **Send a message**

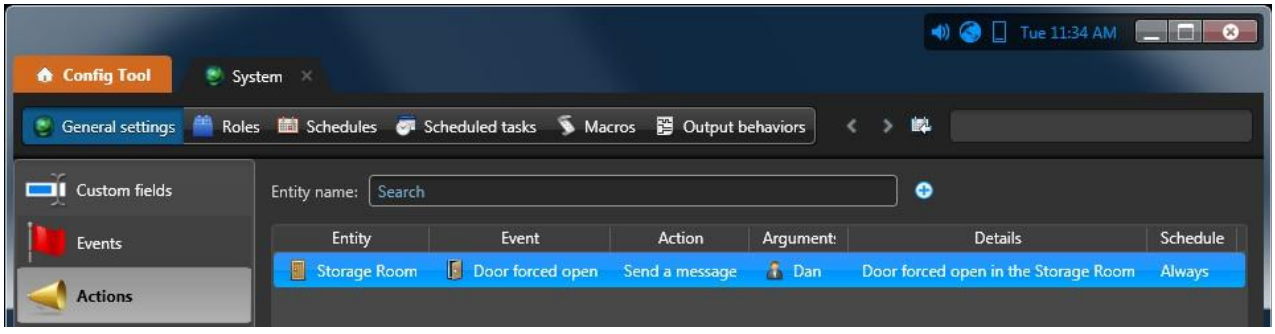


When selecting ***Play a sound*** as the desired action, a ***User*** (recipient) and sound file must be chosen.



When selecting ***Send a message*** as the desired action, a recipient must be chosen and the message text entered

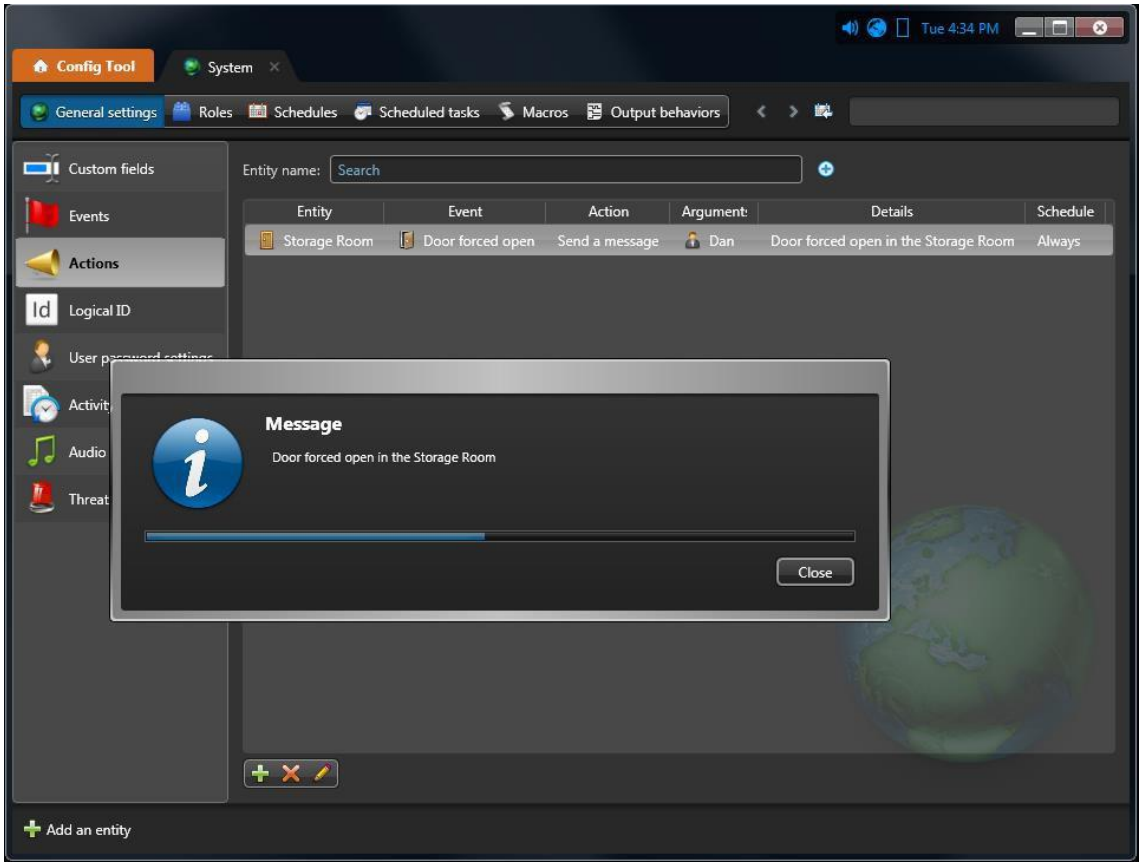
- ❑ Click **Create**. Click **Close**
- ❑ Your Event → Action relationship should now appear on the page of ***Actions*** in the **System** task



Testing the Event → Action automation

It's now time to test your event-to-action configuration.

- ❑ Toggle your door monitor input to cause a *Door forced open* event to occur.
- ❑ Do you see or hear the desired alert sound or pop-up message?



This pop-up message appeared for 10 seconds upon toggling the physical door monitor input

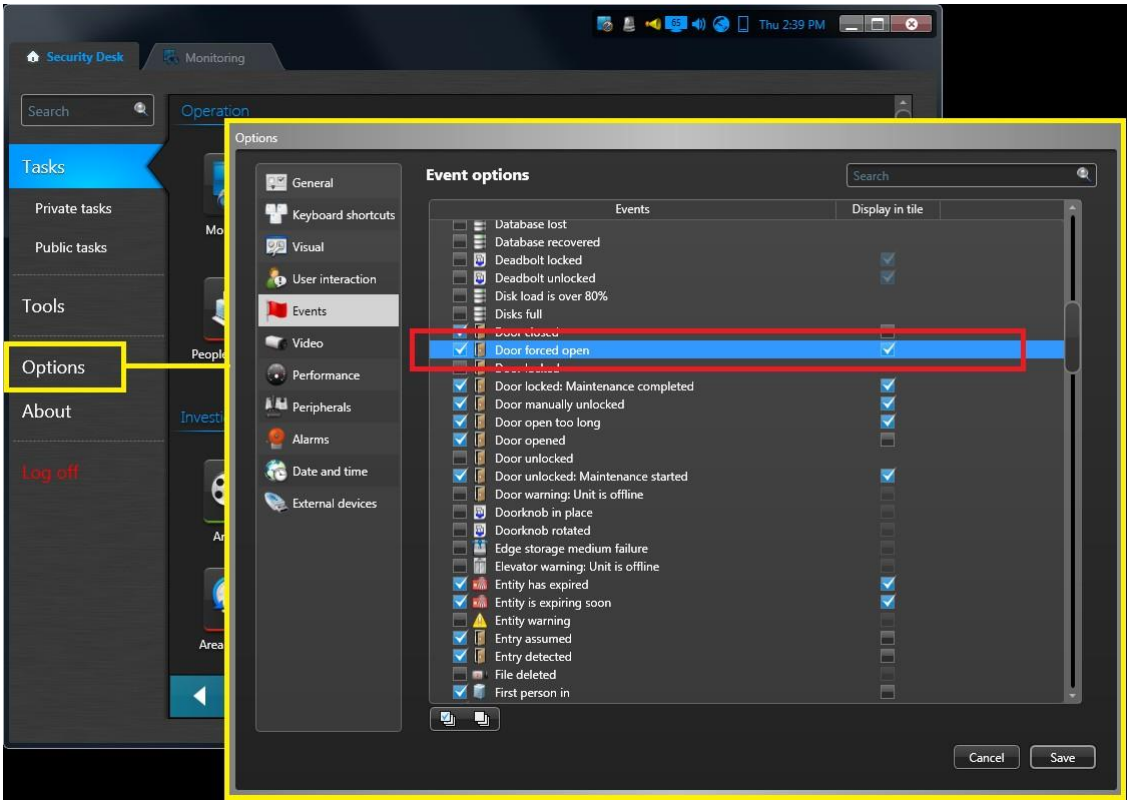
- ❑ If you do not click the ***Close*** button in the pop-up, the message will only remain on screen for 10 seconds. It will then get filed away in your *notification tray*. Double click the message icon in the tray to view or delete the messages

If your action executed automatically, you are finished with this exercise. You could try modifying your action or adding more actions.

If your action did not execute successfully, continue to the next page for some troubleshooting suggestions.

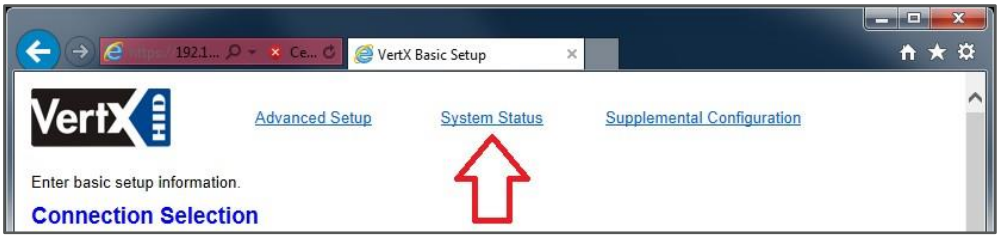
Troubleshooting the Event → Action automation

- ❑ If you chose the actions **Play a sound** or, **Send a message**, you had to select a recipient when configuring your action. Are you logged into the client application as the user who should see/hear the action? (Or, are you perhaps logged in as user Admin?)
- ❑ If you selected the action **Play a sound**, make sure that your PC speakers are not muted. Check the volume control on your laptop.
- ❑ Are you toggling the correct input on the door controllers? Access control units offer anywhere from 4 – 16 inputs each. Perhaps the wrong input was toggled.
- ❑ Is the source event (in this case, *Door forced open*), firing at all?
    - Open a new monitoring task and monitor your door. Ignore the desired action, do you see the event ***Door forced open*** at all?
    - If you don't see the Door forced open event, check the event filters in your Security Desk ***Options*** menu:

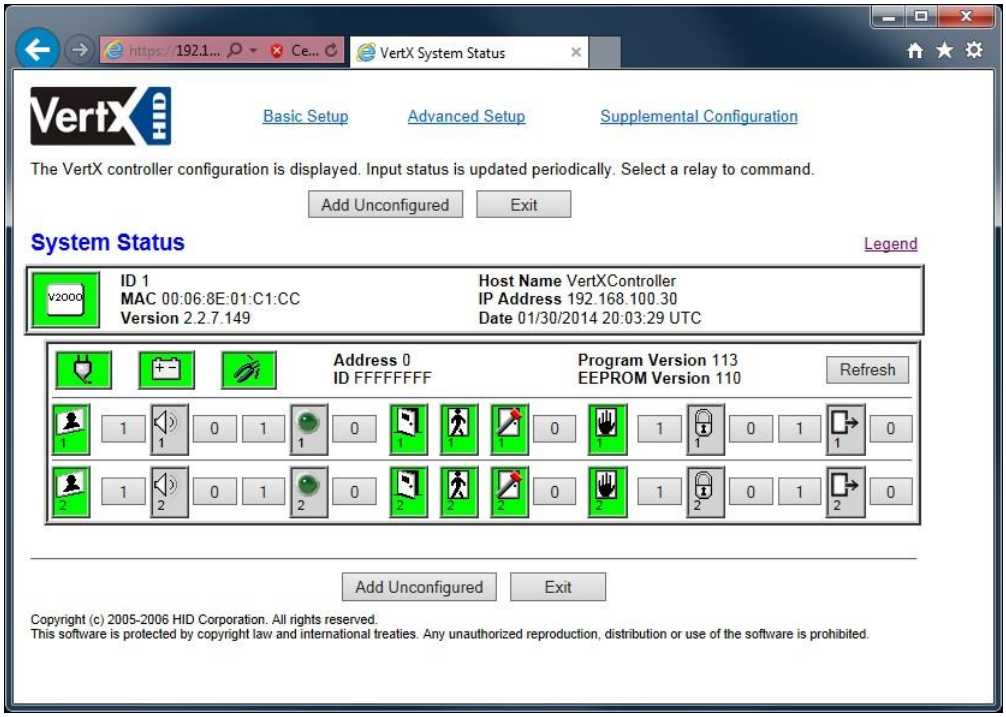


- ❑ Check the state of the inputs in the controllers own web interface. Both HID hardware and SMC/ Synergis Cloud Link hardware offer a web page where we can see the state of its inputs and outputs. Open a web browser and login to your controller's IP address

- ❑ If you have an HID controller (for SMC/ Synergis Cloud Link, skip to the SMC/Synergis Cloud Link section):
  - Click the link ***System Status*** at the top of the page

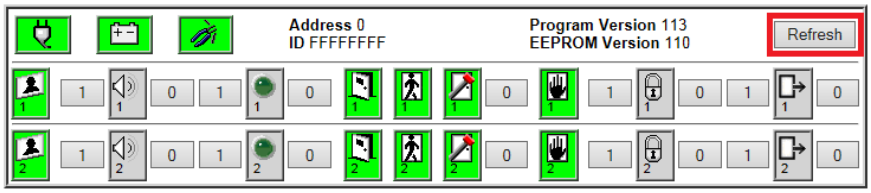


  - The ***System Status*** page should show all of your inputs in "Normal" state (green)

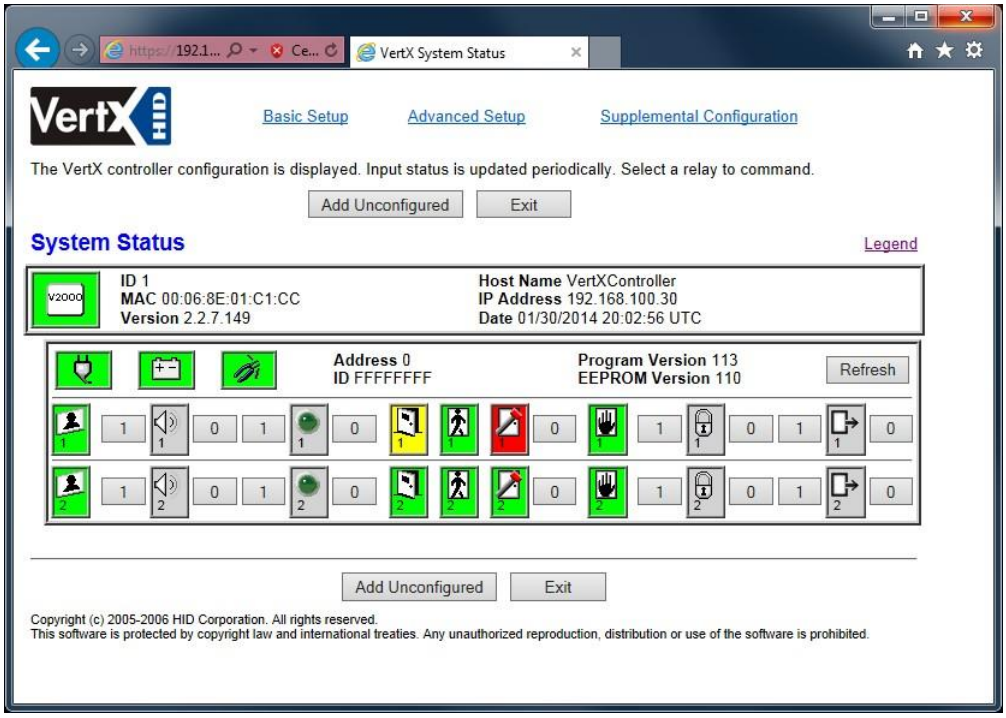


All inputs are shown in "Normal" state (green)

  - Toggle your door monitor input and click ***Refresh*** in the ***System Status*** page

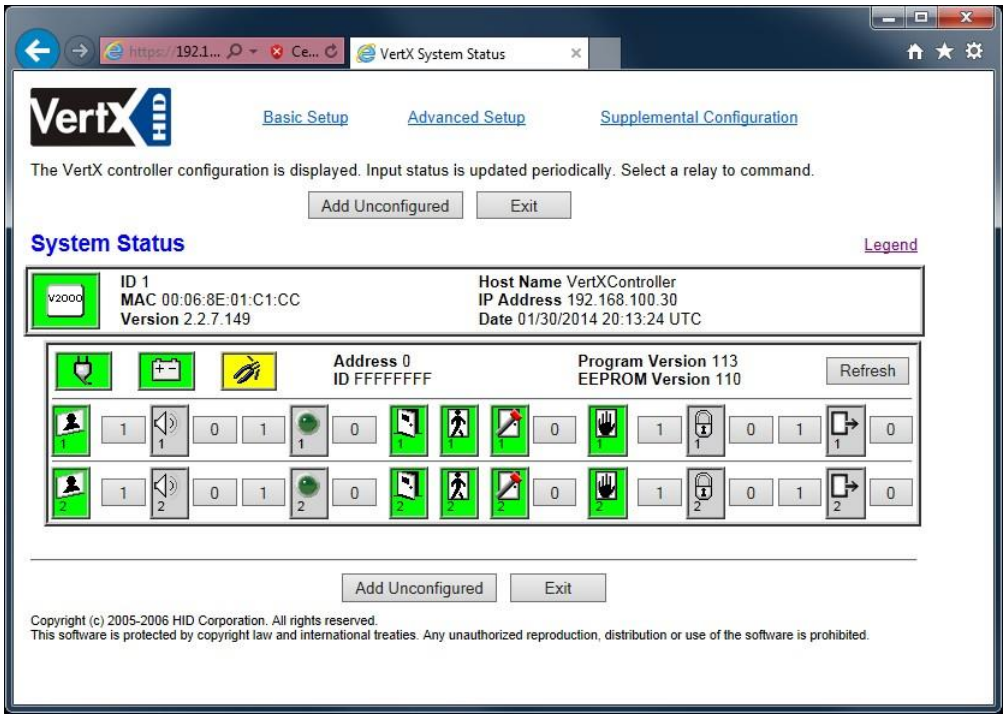


- If the controller sees the door monitor input in active state, it should show the Door monitor input ( ) “Active” (yellow) and the Door forced icon ( ) in “Alarm” state (red)



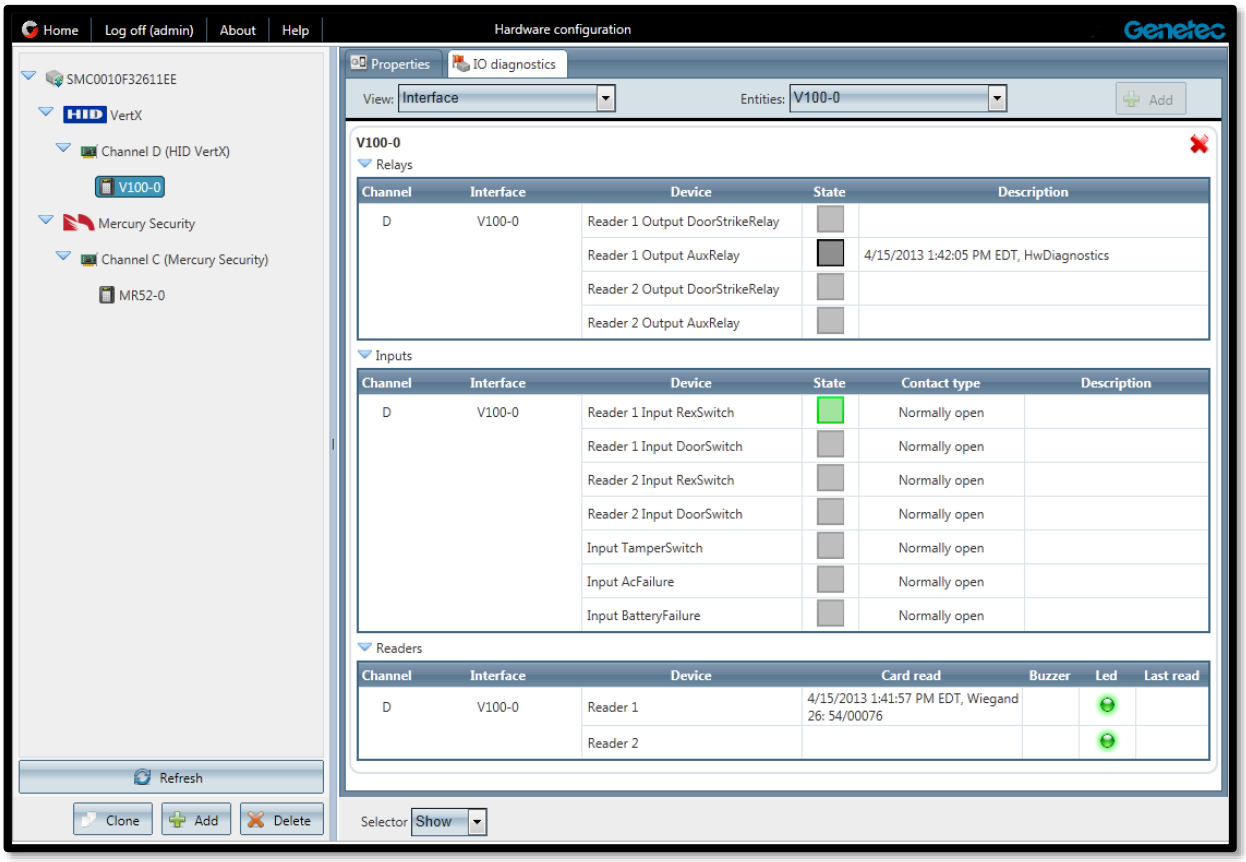
Door monitor “active”, door forced “alarm”

- However if anther input has been toggled, it would show “Active” in the System Status page



Tamper input has been toggled as is “active” (instead of door monitor)

- ❑ If you have an SMC/Synergis Cloud Link controller:
  - From the **Controller Portal – Home** page, click **IO diagnostics**
  - Select what you want to monitor in real time.
    a) From the **View** drop-down list, select ***Interface***.
    b) From the **Entities** drop-down list, select the panel you wish to monitor.



The ***Reader 1 Input RexSwitch*** on the V100 is in "active" state (green)

  - Toggle your door monitor input and observe the state on the ***IO diagnostics*** page

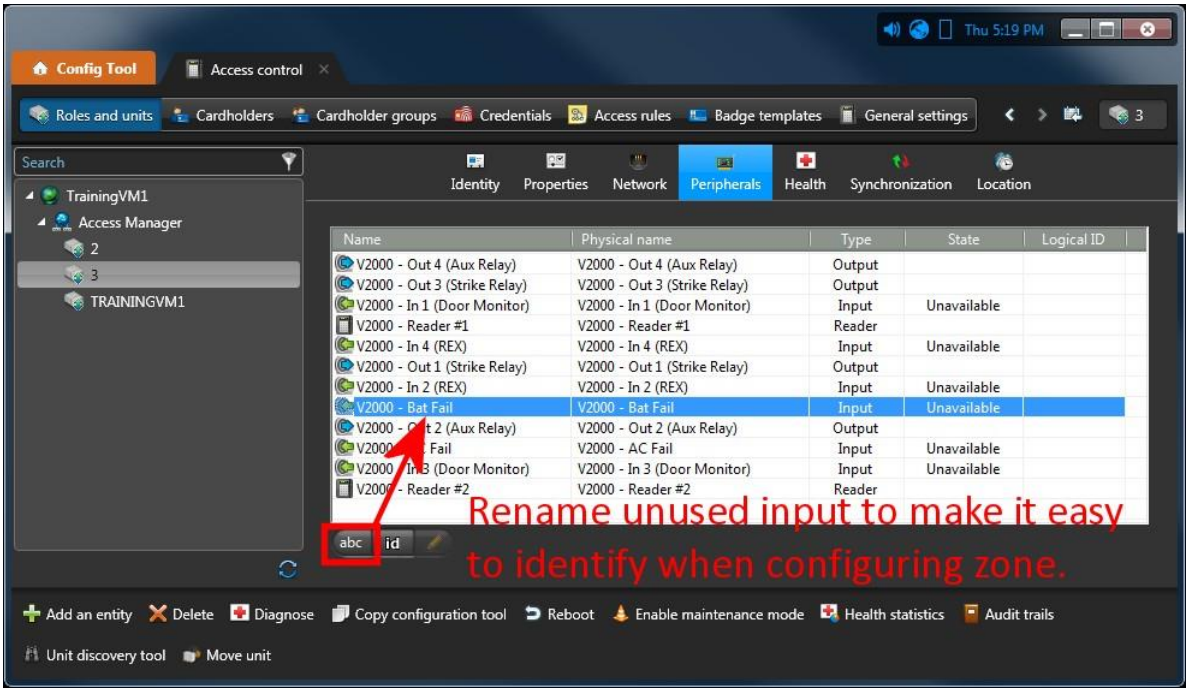
- ❑ Does your door switch input appear active (green) in the IO diagnostics page when you toggle the physical input?

Zones

Create a hardware zone to monitor inputs on an access control unit.

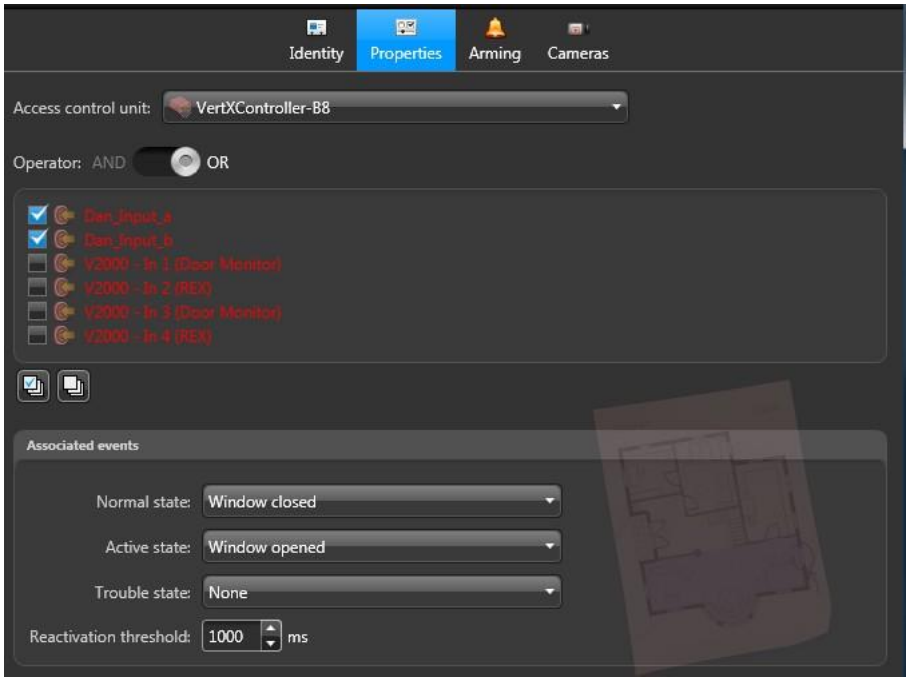
Identify your inputs

- ❑ Open **Config Tool** → **Access control** task → **Roles and units**
- ❑ Select your access control unit. Click its Peripherals tab
- ❑ Select an unused input and click **Rename** (abc) to rename it. This is done to make it easy to identify when configuring your zone



- ❑ Rename the input(s) to something like (*YourName*)_Input_a, (*YourName*)_Input_b, (*YourName*)_Input_c, etc.
- ❑ Once you have renamed one or more inputs, open Config Tool → Logical view
- ❑ Click ***Add an entity*** (✚) and select **Zone**
- ❑ When asked ***What kind of zone do you want to create?*** Select "***Zone***" not "***Virtual zone***"
- ❑ Select your access control unit. Click ***Create***. Click ***Close***
- ❑ In the Logical view task, select your zone's Properties tab
- ❑ Select the input(s) you renamed earlier

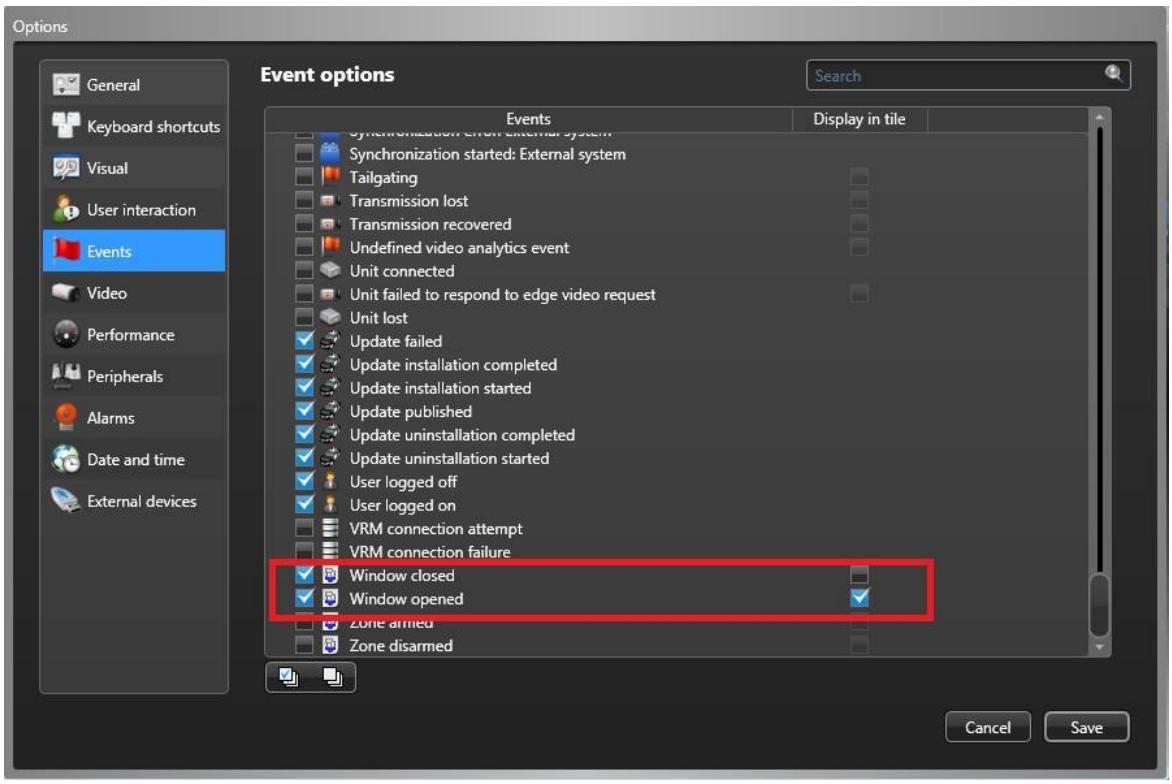
- ❑ *Operator*: ***OR***
- ❑ ***Normal state: Window closed***
- ❑ ***Active state: Window opened***
- ❑ ***Trouble state: None***
- ❑ ***Reactivation threshold: 1000 ms***



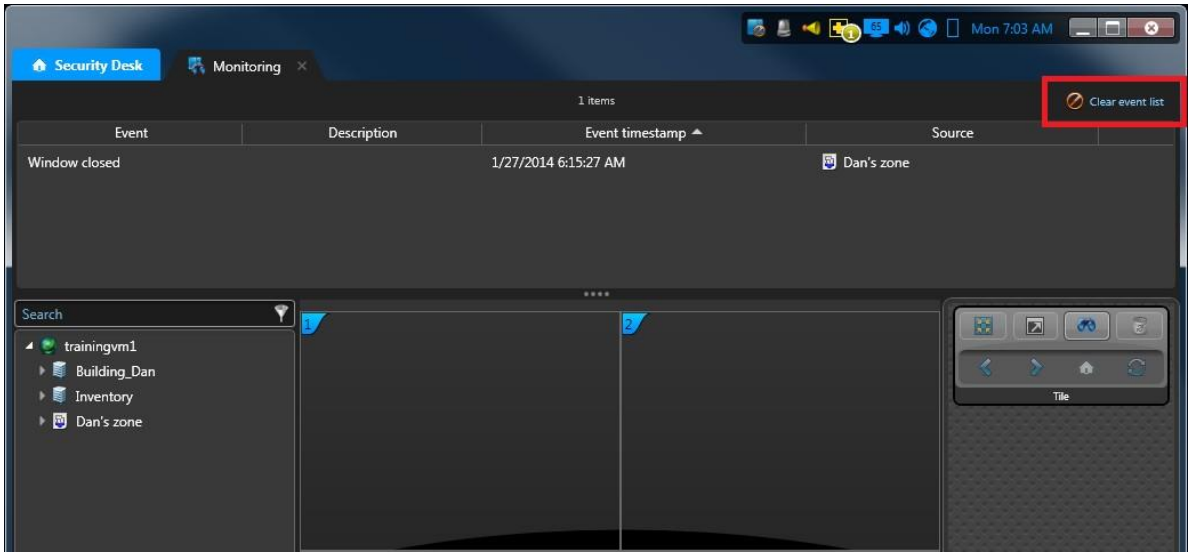
- ❑ Click ***Apply***. Your zone should then come online and change from red to white

Testing/Monitoring your zone

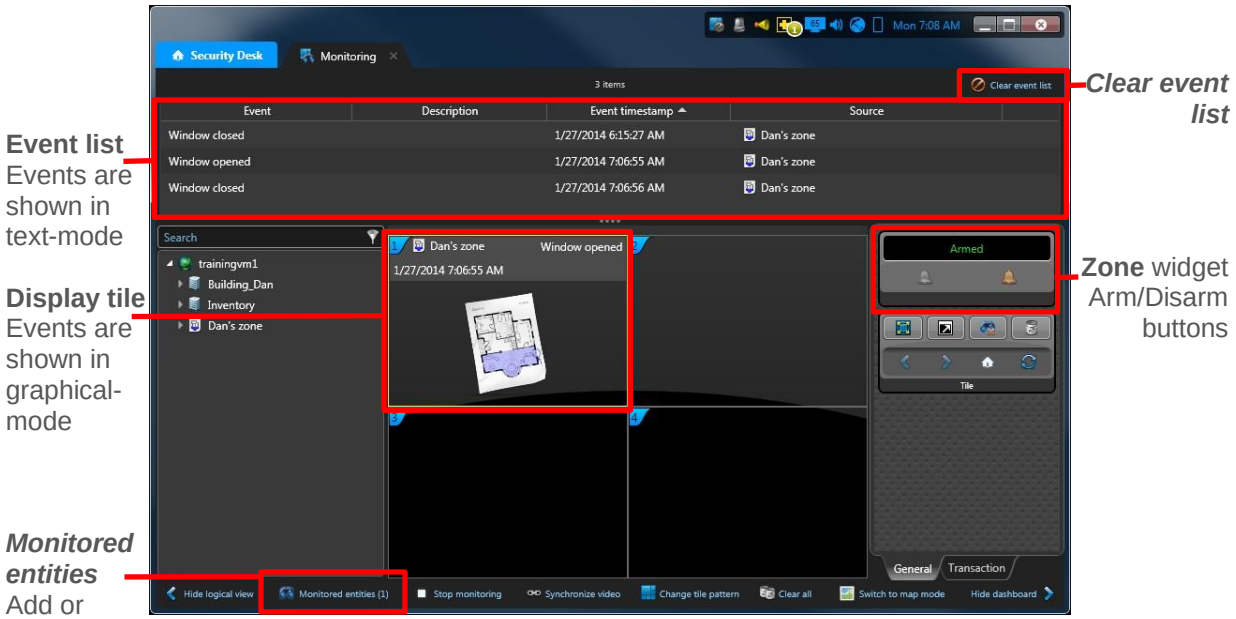
- ❑ Open the **Security Desk → Monitoring task**
- ❑ Click the Home button (Security Desk) and select ***Options***. Click ***Events***
- ❑ Scroll down the event list to ensure that the event ***Window closed*** has a checkmark in the column to the left and ***Window opened*** has checkmarks in both left and right columns.



- ❑ Click the button **Monitored entities** ( ) at the bottom of the page
- ❑ Click **Add** ( ) and navigate the logical tree to select your zone. Click **Add.** Click any tile to close the **Add monitored entity** window
- ❑ Tap the F9 key twice so that your Security Desk Monitoring task displays both tiles and the event list.
- ❑ If any events appear in the list, click the ***Clear event list*** button



- ❑ Force an input in your zone to change its state (from open to closed or closed to open)
- ❑ Does your monitoring task display the Zone event? Click the ***Disarm zone*** widget and try again.



Event list Events are shown in text-mode

Display tile Events are shown in graphical-mode

Monitored entities Add or Remove entities to monitor

Clear event list

Zone widget Arm/Disarm buttons

Module 7 - Advanced access control

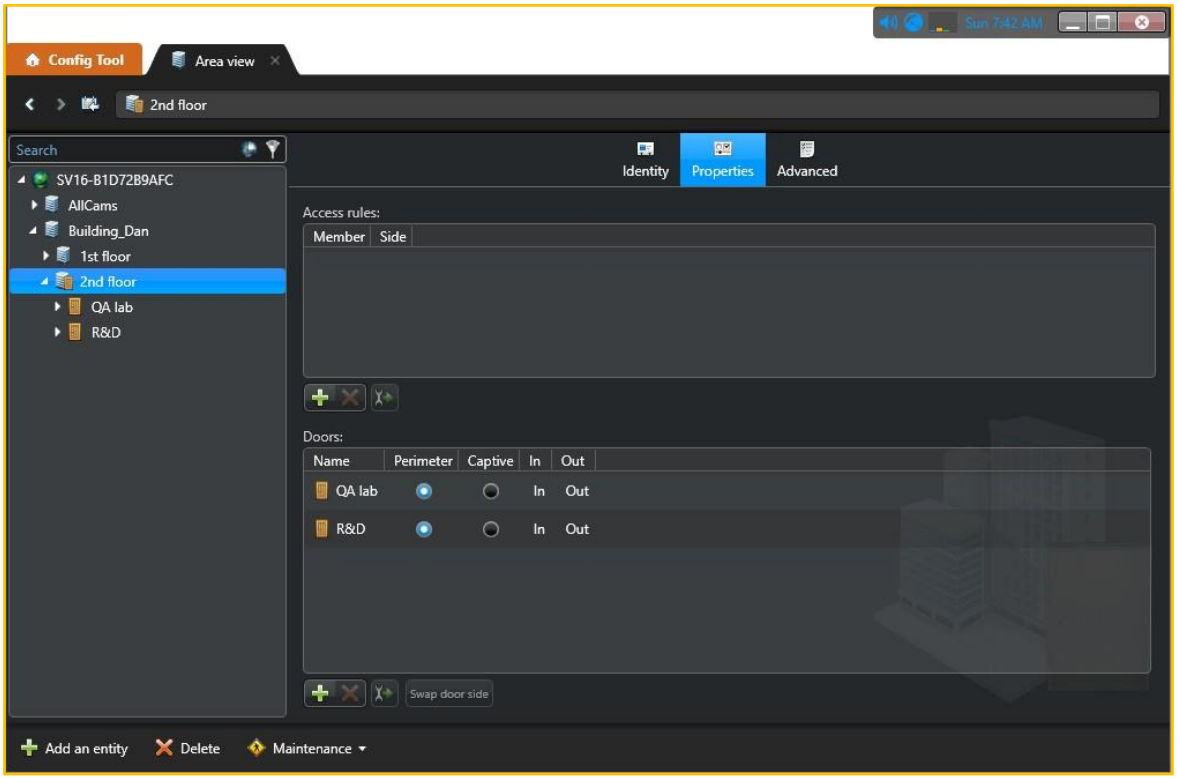
Areas: Antipassback

3 important points must be noted before beginning:

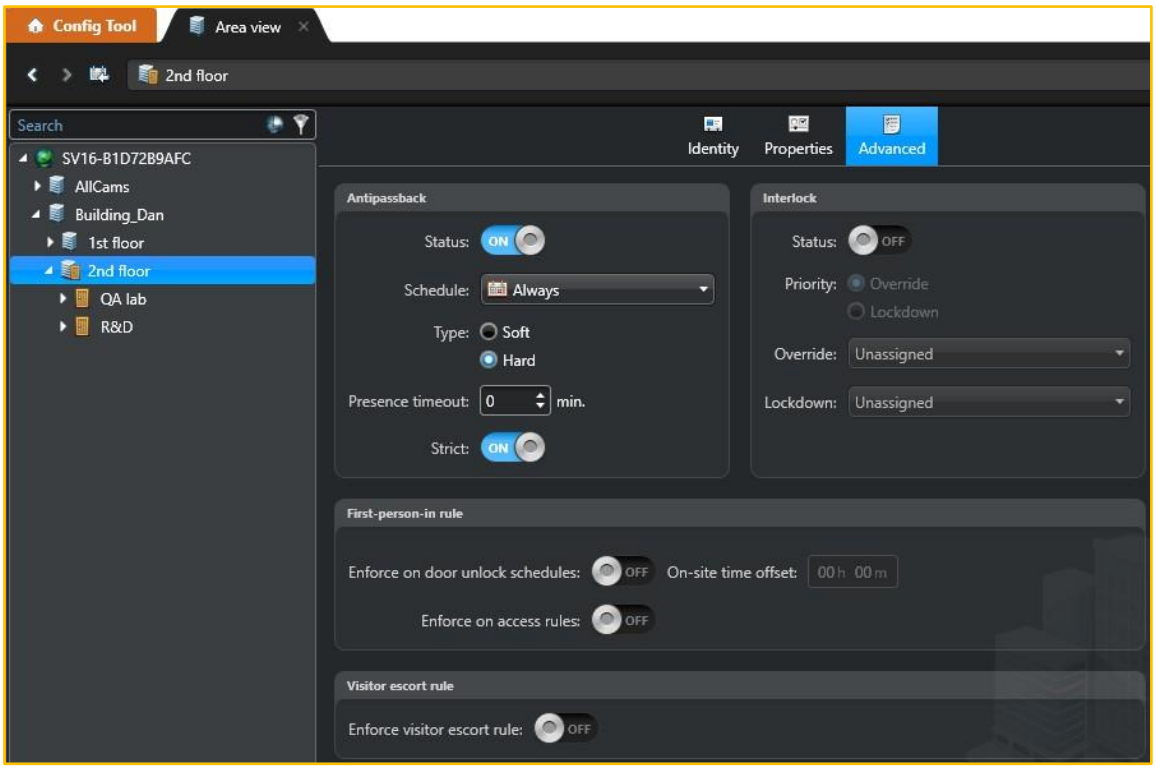
a) Antipassback and interlocking are configured on an area, not a door.
b) Antipassback and interlocking is not supported for doors with a single reader + a REX.
c) Antipassback and interlocking are mutually exclusive. It's one or the other, not both.

Configure an area for a anitpassback

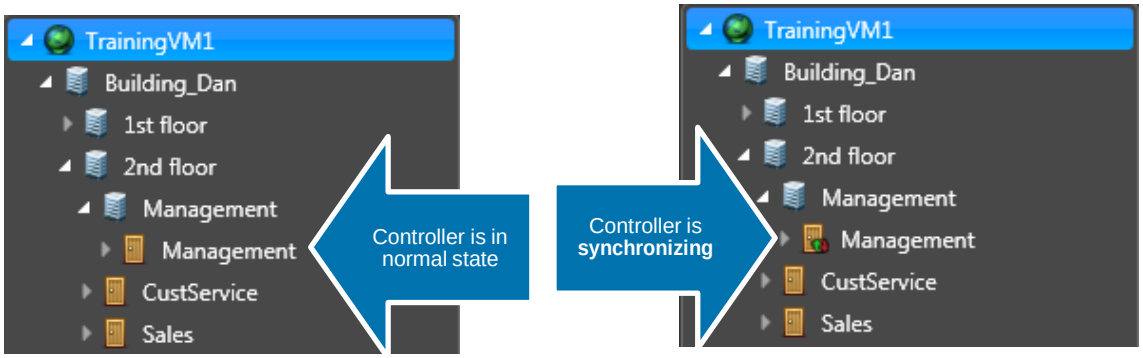
- ❑ Open Config Tool → Area view
- ❑ Configure an area with a single controller (can be 1 or more doors running on a single controller)
- ❑ Configure the door(s) as perimeter door(s) of the area under the ***Members*** tab



- Configure the area's antipassback properties as:
  - **Status**: ON
  - **Type**: Hard
  - **Timeout**: 0 min.
  - **Strict**: ON

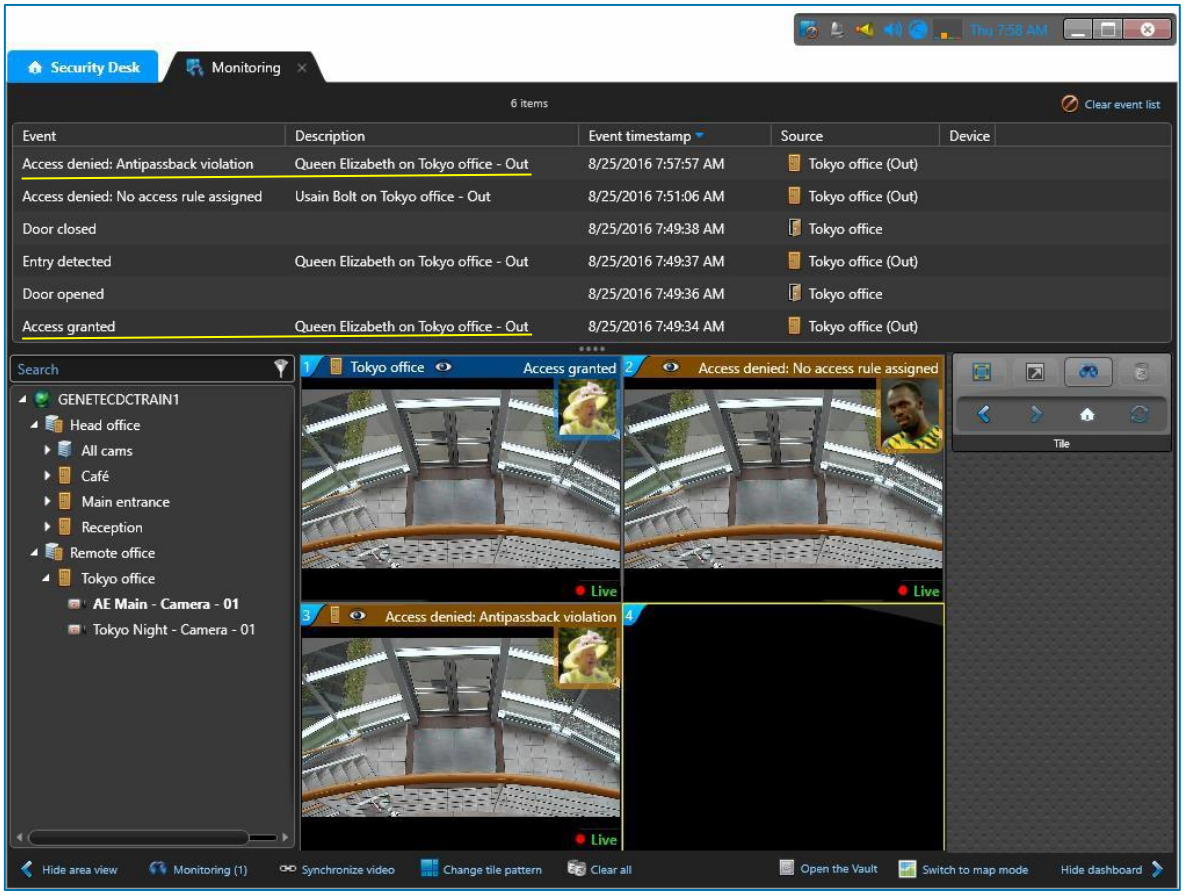


- Click **Apply.** The access manager role should then synchronize the new configuration down to the door controller. Antipassback will not work until the unit has synchronized. Watch the door icon for the synchronization process ( ).



Test the antipassback area

- ❑ Open a **Security Desk → Monitoring** task
- ❑ Make sure that you can see both the display tiles and the event list (on top)
- ❑ Click the Security Desk Home tab (Security Desk)
- ❑ Click **Options → Events**
    - Check the box beside **Antipassback violation** Click **Save**
- ❑ Add the antipassback area to the Monitored entities list
- ❑ Chose a cardholder who should get access granted to the antipassback area/door(s)
- ❑ Present the card to exit the area. Be sure to toggle the door monitor input to force the ***Door open*** and ***Door closed*** events. We expect to see ***access granted*** events when entering the area. You may see some other area events (like ***First person in***)
- ❑ Examine the results in your monitoring **event list**.
- ❑ Present your card on the other reader to exit the area. Toggle the door monitor again. (Exit the area)
- ❑ Try again but this time, present the card to enter the area, toggle the door monitor, pause 10 seconds, and present the card again on the same reader. This time, we expect to see an ***access granted*** event upon the first reading, but an ***Access denied: Antipassback violation*** for the second reading of the same card.

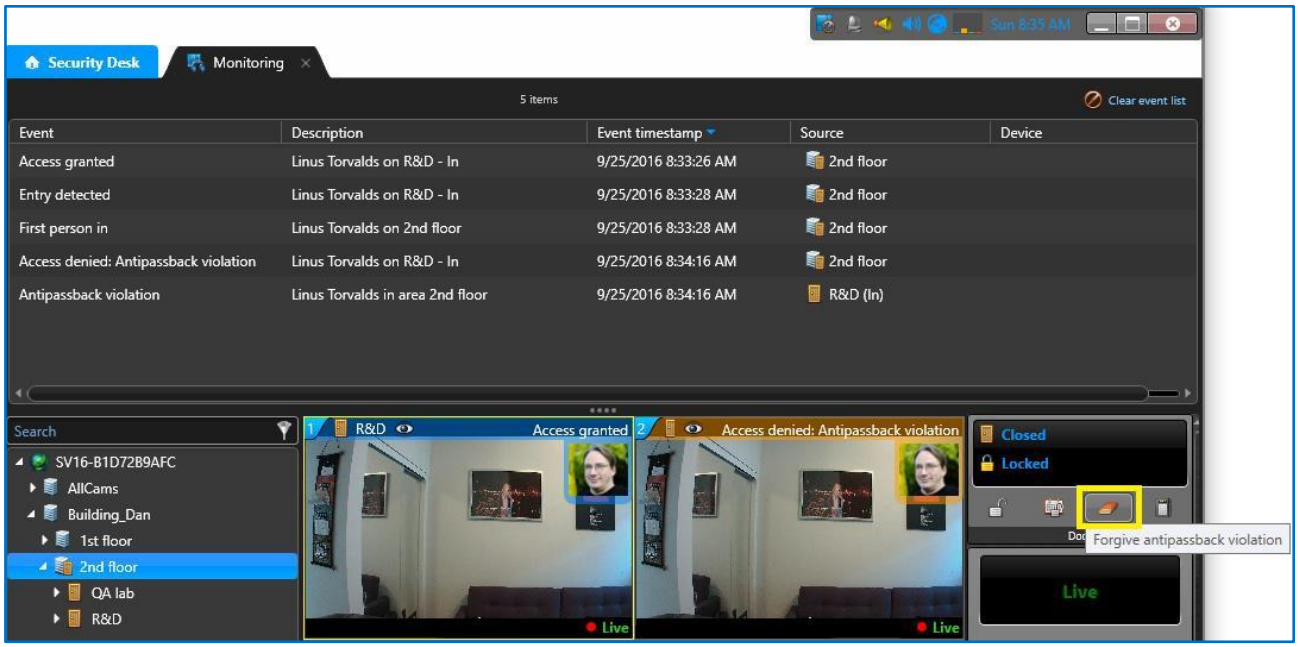


In the illustration above, Queen Elizabeth has been locked out of the *Remote office* area due to an antipassback violation. Because antipassback is configured in “strict” mode, someone will have to explicitly “forgive” the violation so that the cardholder can gain access to the area.

Forgive the antipassback violation

To forgive an antipassback violation and make the card usable again:

- ❑ Select the display tile showing the antipassback violation and click the ***Forgive*** widget



- ❑ Once the antipassback violation has been forgiven, try presenting the card again. Do you now see an access granted event?

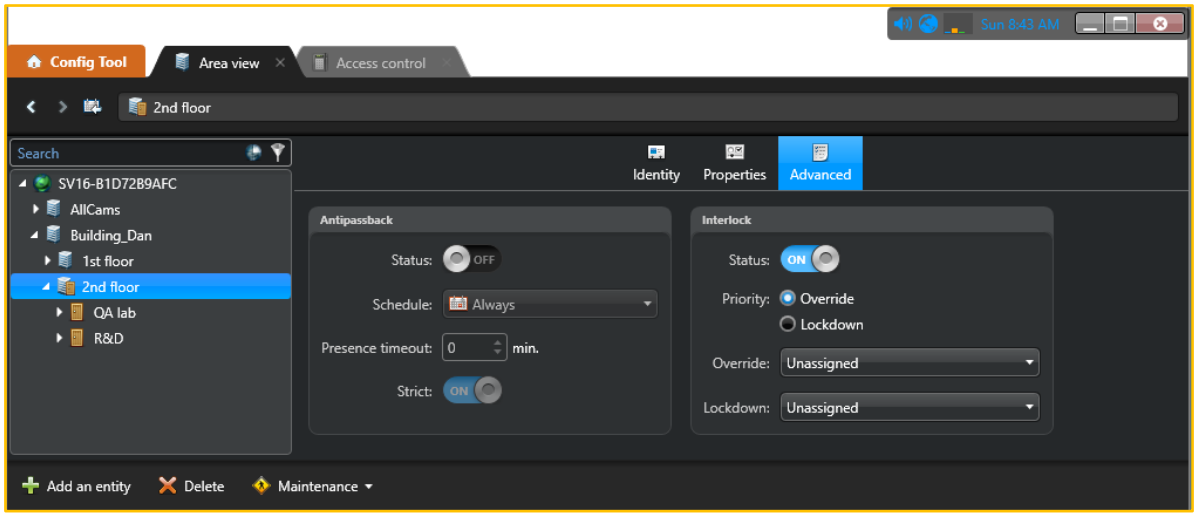
Areas: Interlock (Mantrap, SAS, Airlock, etc…)

3 important points must be noted before beginning:

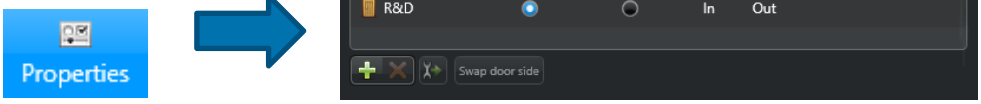
a) Antipassback and interlocking are configured on an area, not a door.
b) Antipassback and interlocking is not supported for doors with a single reader + a REX.
c) Antipassback and interlocking are mutually exclusive. It's one or the other, not both.

Configure an area for an interlock

- ❑ Open **Config Tool → Logical view**
- ❑ Create an **area** that contains 2 **doors** (on a single access control unit)
- ❑ Configure the area's ***Advanced*** properties with ***Antipassback OFF*** and ***Interlock ON***



- ❑ Select the area's **Properties** tab to confirm that both doors are perimeter doors

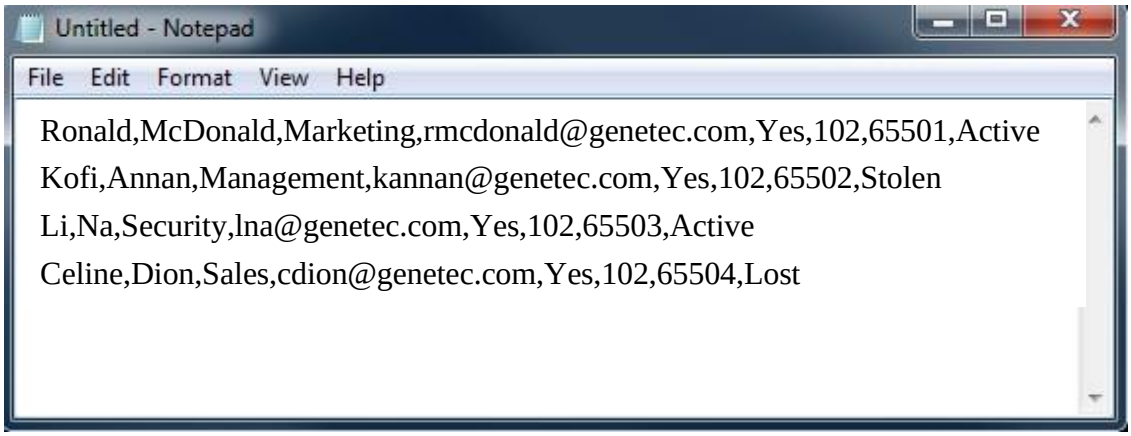


- ❑ Select the area's **Properties** tab to assign an access rule to the interlock
- ❑ Test the interlock with the Monitoring task in the Security Desk application (see next page)
- ❑ If your interlock grants/denies access correctly, try configuring an ***Override*** button (input) or a ***Lockdown*** button (input) in the **Logical view** → Interlock area → **Properties** page
- ❑ Test the interlock's **Override** or **Lockdown** input in the **Security Desk *Monitoring*** task

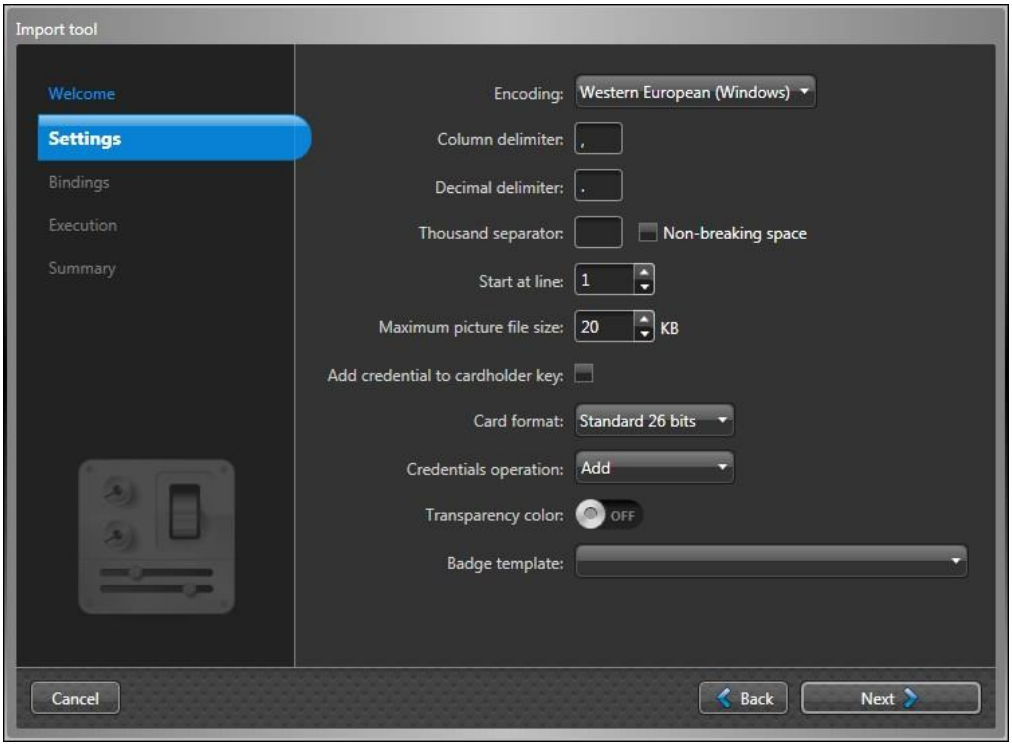
Import Tool

Create a plain text, CSV file using notepad. Once it has been saved, use the **Import Tool** to import the file into Security Center.

- ❑ Open Windows notepad and create a new text file
- ❑ Use the following in your text file (modify to personalize with your own cardholders/credentials):

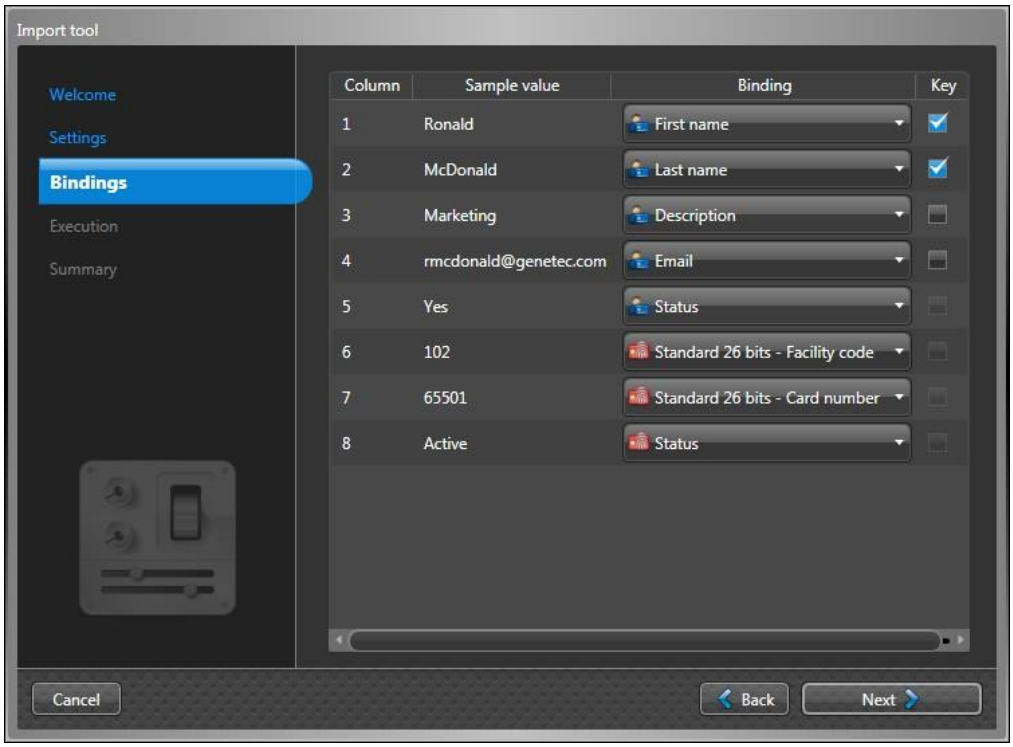


- ❑ Save the file on your desktop as Import.TXT. Close Notepad
- ❑ Browse your Windows desktop and rename the file Import.TXT file to Import.CSV
- ❑ Open **Config Tool → Tools → Import Tool** ( )
- ❑ Click the Browse button (**…**) and point to the text file you prepared earlier (*Import.CSV*). Click **Next**
- ❑ Leave the defaults in the ***Settings*** page (unless you modified the structure of your import file)

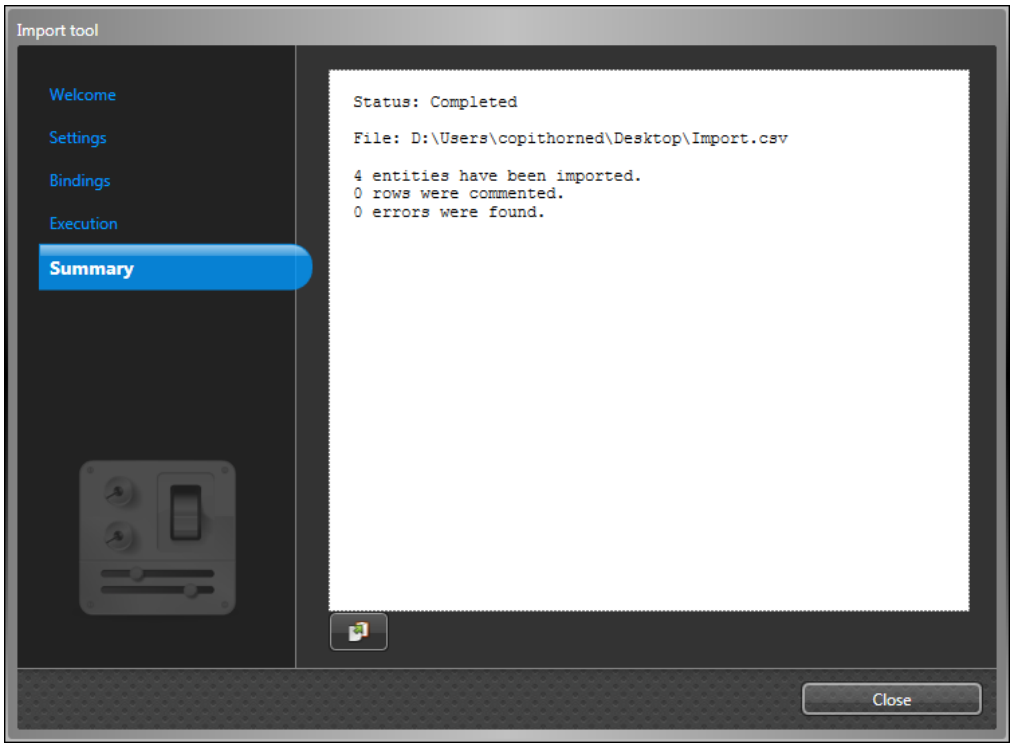


- ❑ Click ***Next***

- ❑ Map the contents of your import file to Cardholder and Credential fields in the database:



- ❑ Click ***Next***. The Import Tool will then try to import the contents of your file into the database
- ❑ Note the results of the import process. Are there any errors?

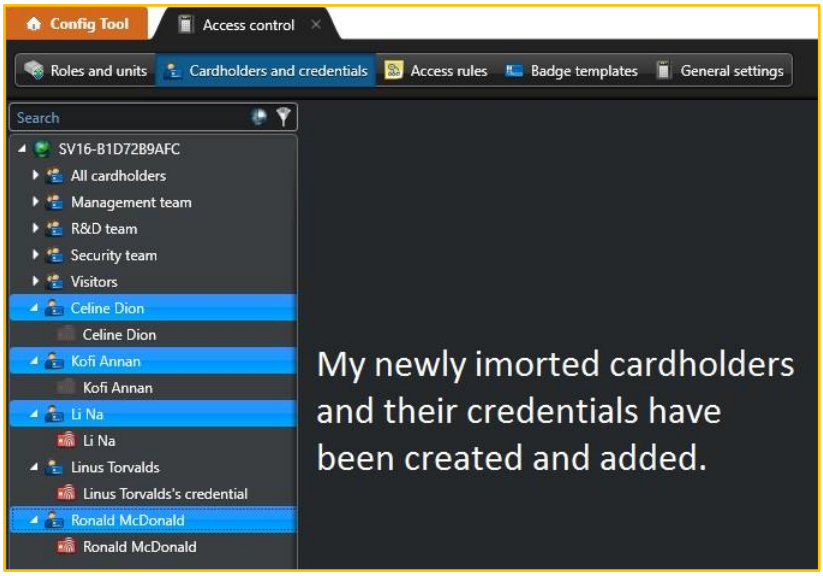


- ❑ Click ***Close***

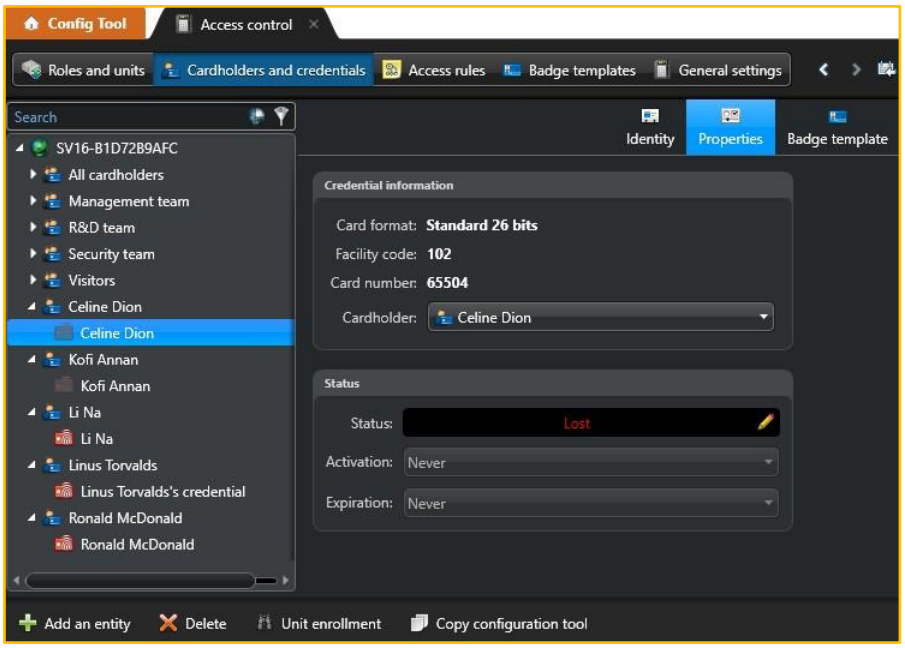
Validating the results of the import process

If the import tool successfully imported the contents of your Import.CSV file, we should find some new cardholders and credentials in the database:

- ❑ Open **Config Tool → Access Control** task → **Cardholders**
- ❑ Do you see you newly imported cardholders? (You may need to refresh the list with F5)



- ❑ Select one of the newly imported cardholders. Select the ***Identity*** tab and the ***Properties*** tab Do you see the values you had imported from your CSV file (eg Description, email address)?
- ❑ Select a ***Credential***



- ❑ Do you see the *credential status* value imported from your CSV file? Some may be ***Active, Lost or Stolen***

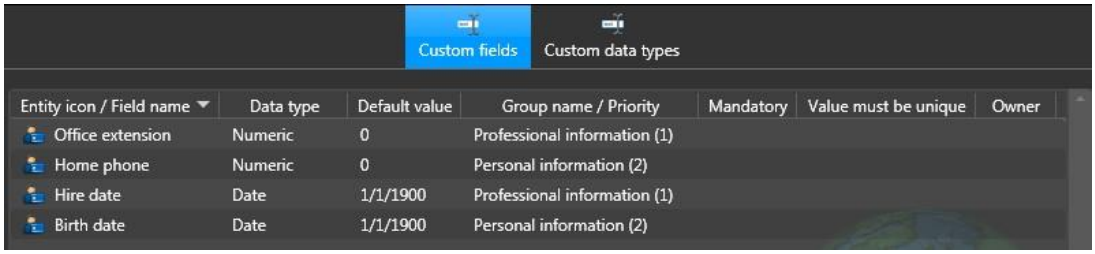
Custom Fields (as a group)

Create custom fields to be added to a cardholder's properties like *Office extension, Home phone, Hire date* and *Birth date*. Then group them into to ***Layout*** groups. 1 for personal information and the other for professional information.

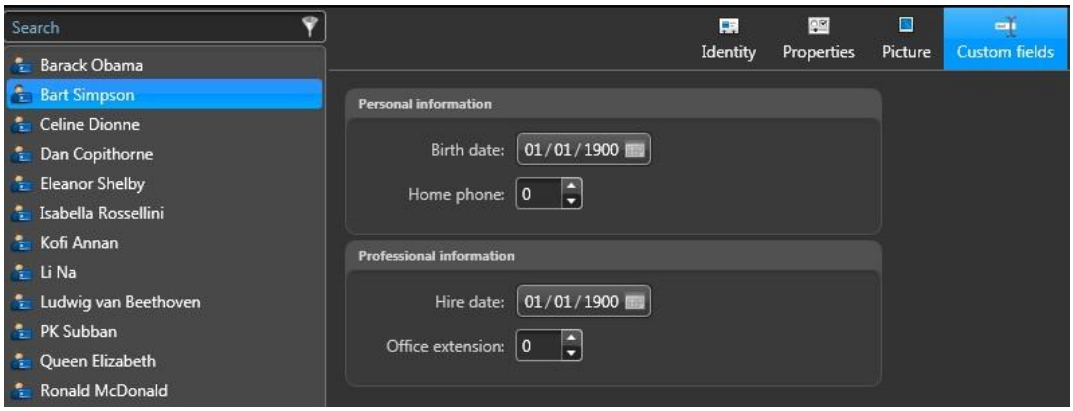
- ❑ **Open Config Tool → System task → General Settings**
- ❑ Select ***Custom fields*** from the column on the left
- ❑ Click *Add* ( ) ***Custom Field*** at the bottom of the page
- ❑ Create the following new custom fields:

	Office extension	Home phone	Hire date	Birth date
Entity type	Cardholder	Cardholder	Cardholder	Cardholder
Data type	Numeric	Numeric	Date	Date
Name	Office extension	Home phone	Hire date	Birth date
Default value	0	0	01/01/1900	01/01/1900
Group name	Professional information	Personal information	Professional information	Personal information
Priority	1	2	1	2

- ❑ Click **Save and close**



- ❑ Open the **Config Tool → Access control** task → **Cardholders**
- ❑ Select a cardholder. Click the cardholder's ***Custom fields*** tab. Do the custom fields appear?



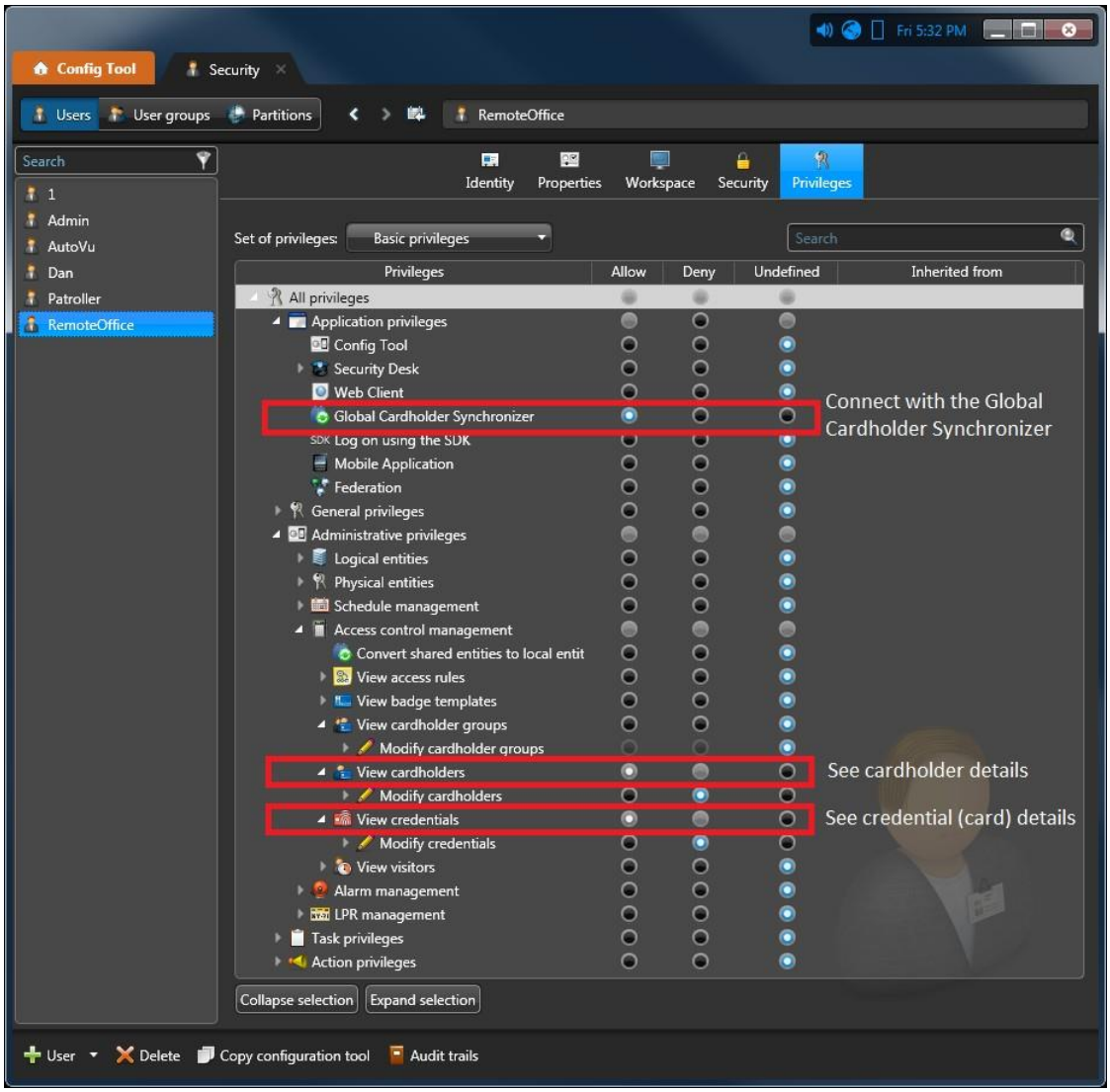
Global Cardholder Synchronization (as a group)

Global cardholders are local cardholders who can be shared with other (independent) Security Center systems. You will need 2 independent Security Center systems to try this exercise. We will consider the existing training server as the “Sharing host”, and the newly added secondary system as the “Sharing guest”.

Create a user profile for the Global cardholder synchronizer on the Sharing host

For a remote system to be able to connect and download cardholder and credential information from a central system, authentication will be required to establish the connection. It is recommended to create a new user profile on the host system to be used by remote systems who need to connect.

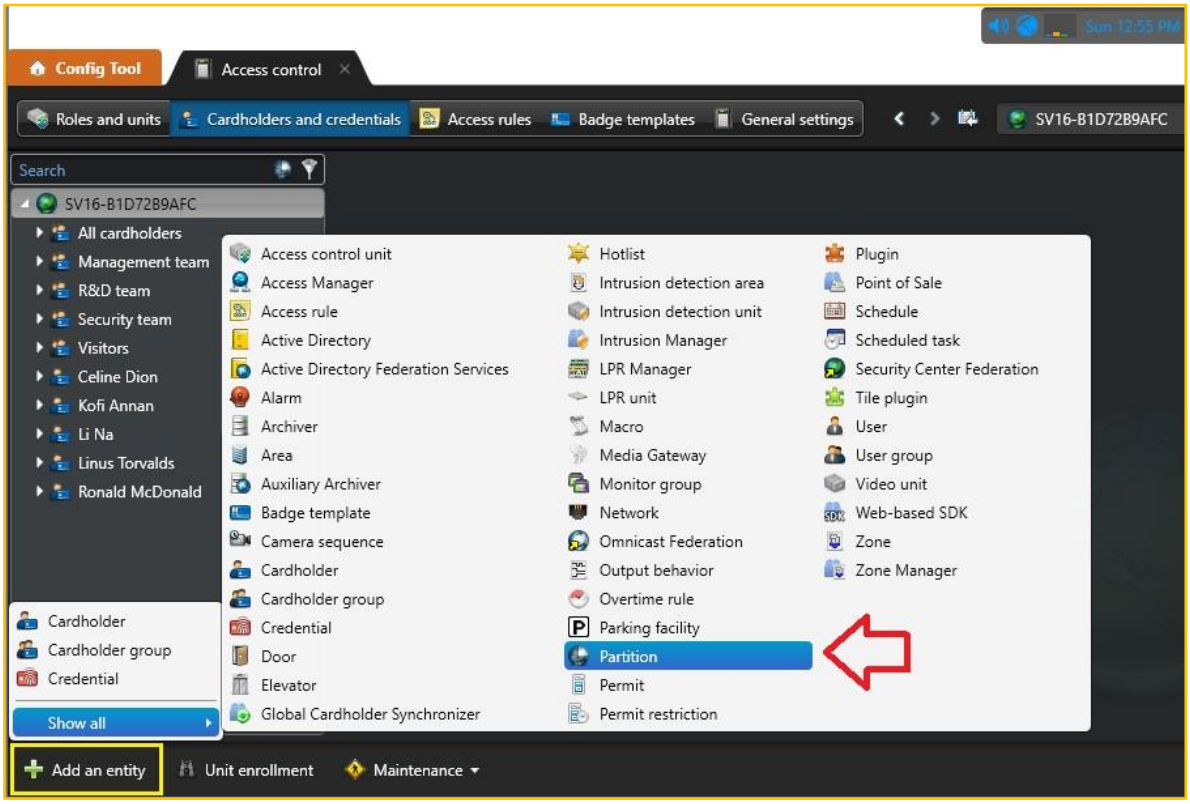
- ❑ Open **Config Tool → Security → Users**
- ❑ Create a new user with the following (minimum) privileges:
  - **Application privileges → Global Cardholder Synchronizer**: ALLOW
  - **Administrative privileges → Access control management → *View cardholders***: ALLOW
  - **Administrative privileges → Access control management → *View credentials***: ALLOW



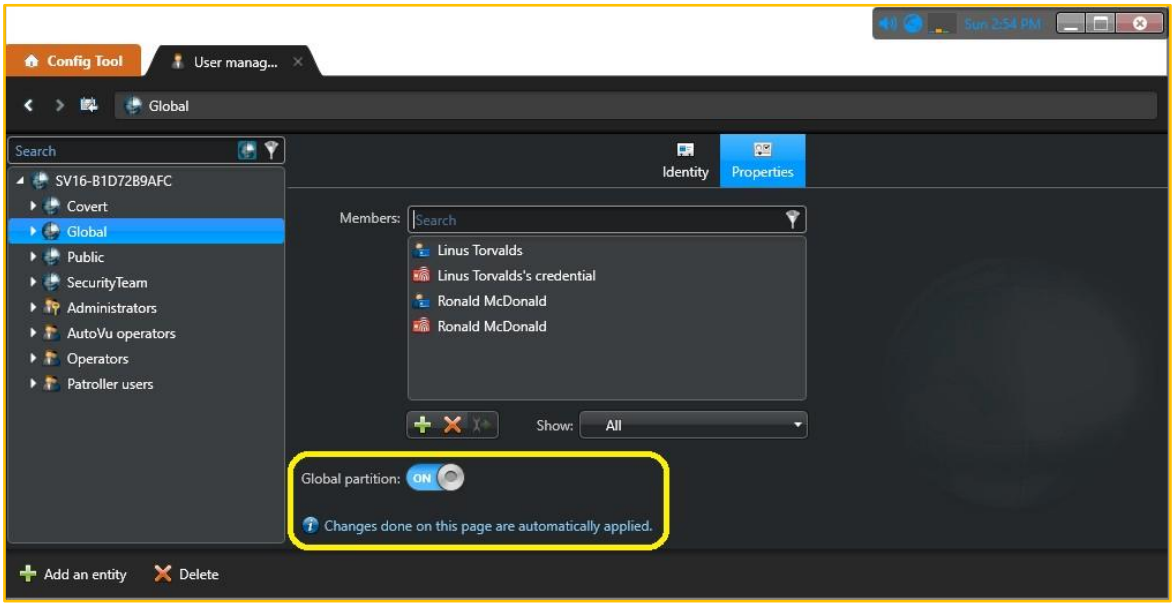
The minimum privileges required for a remote system to connect and download cardholder/credential info.

Create and configure a *Global partition* on the *Sharing host*

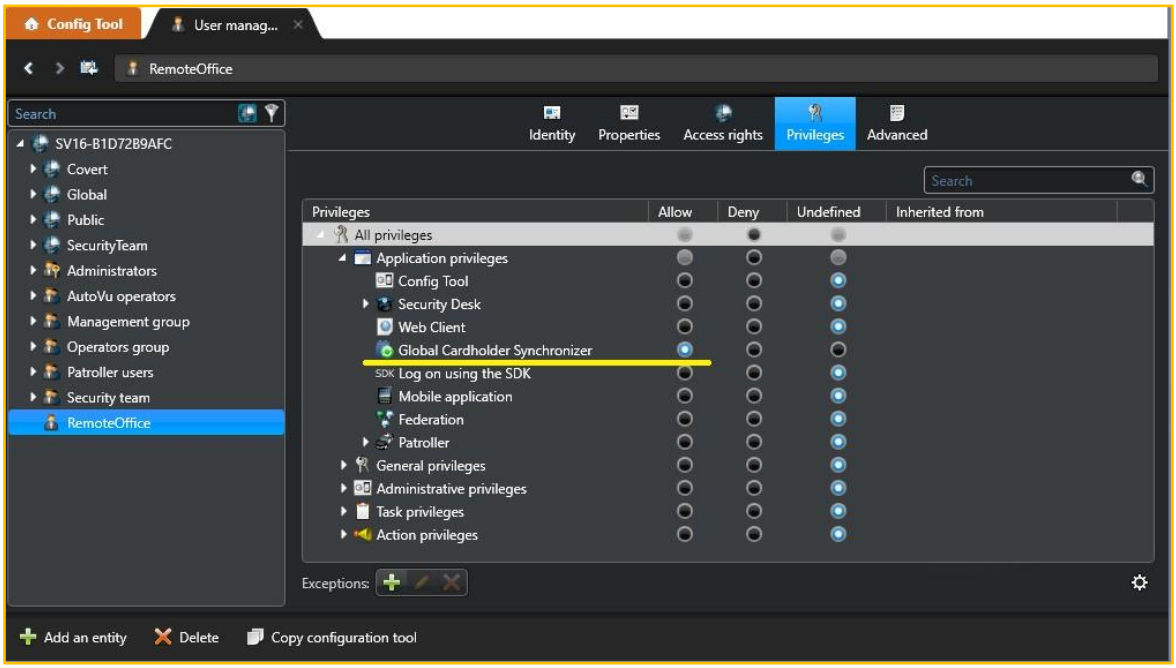
- ❑ With your Config Tool logged into the "master system" or the **Sharing host**, click **Add an item** (➕) to create a new *Partition*



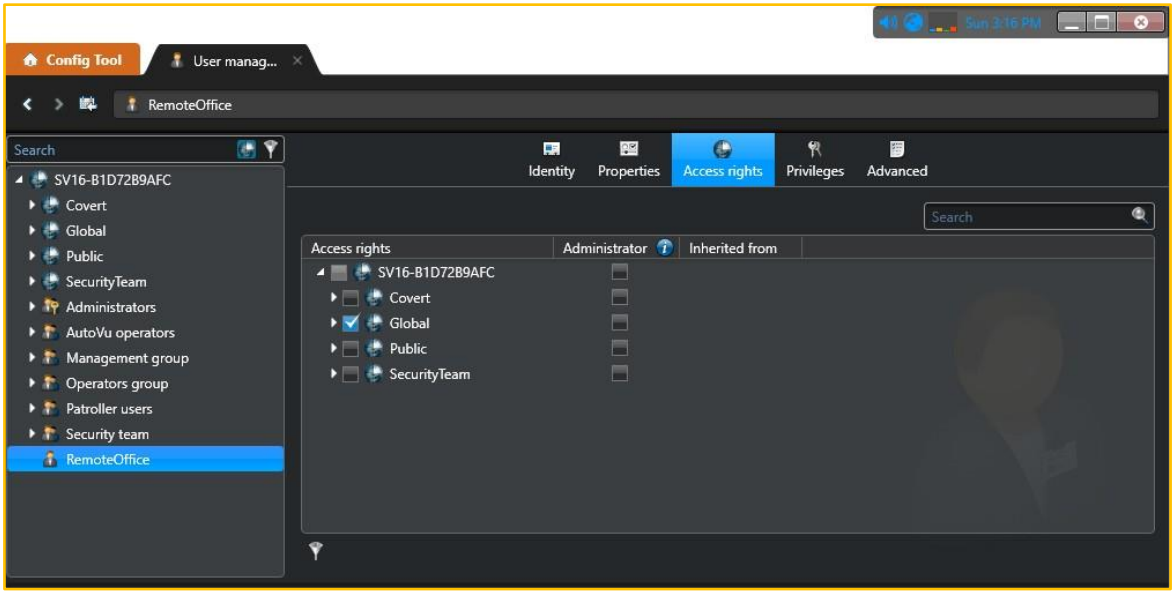
- ❑ Assign a name to the new partition and click ***Create***
- ❑ Select the new partition's ***Properties page*** and click **Add** (➕) to add 2 cardholders and their credentials as members of this new partition
- ❑ Toggle **Global partition** to ***ON***.



- Create a new user account that will be used by the guest system to connect to the host system and download cardholder information from the shared **Global partition**. make sure that the user profile has the privilege to use the ***Global cardholder synchronizer***



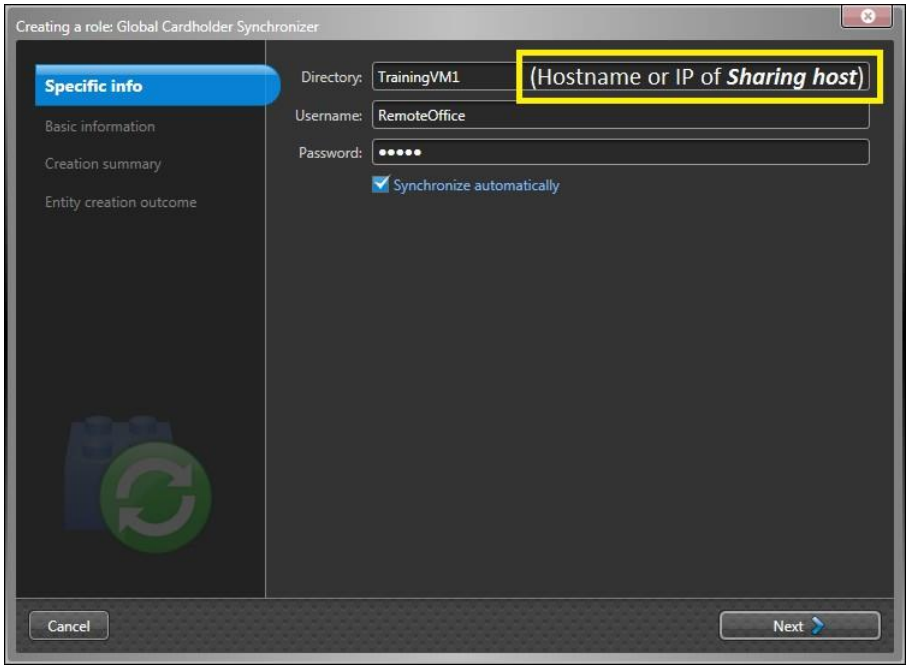
- Select the user's ***Access rights*** tab. Grant the user account access to the Global partition.



Configure the remote system to connect to the main system as a *Sharing guest*

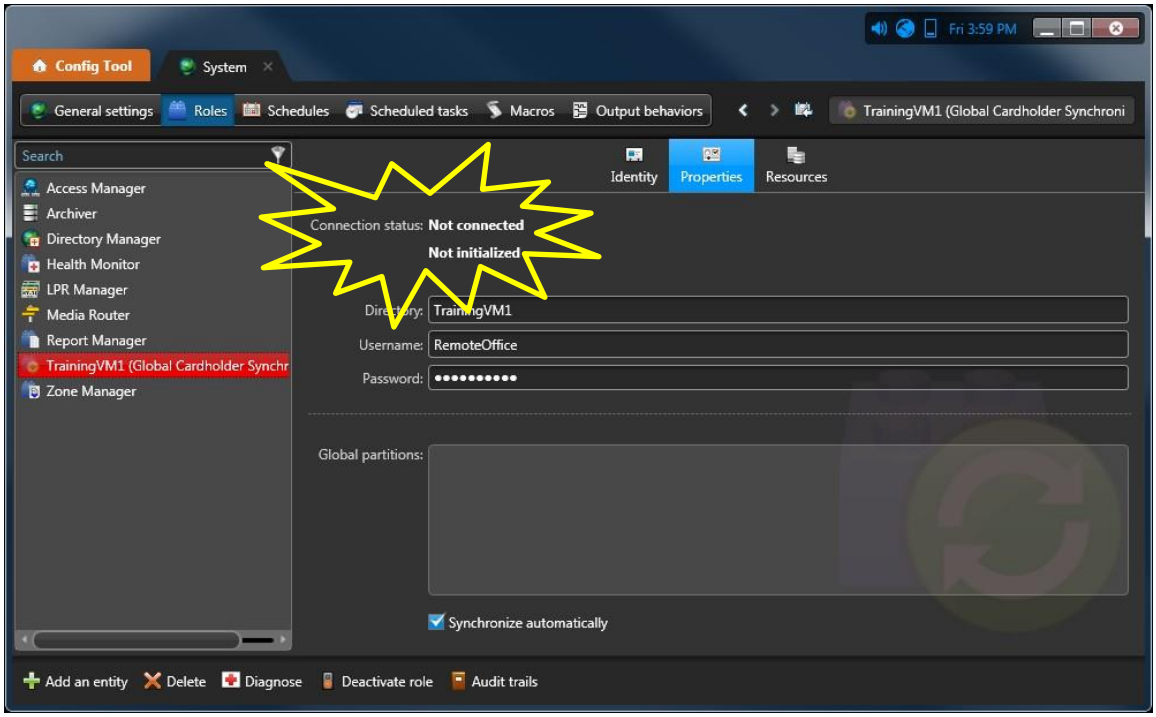
This part of the configuration exercise is for the remote system who will connect to the main system to download some cardholder and credential information.

- ❑ With your Config Tool logged into the "remote system" or the **Sharing guest**, open **Config Tool** → **System** task → **Roles**
- ❑ Click **Add an entity** ( ) → ***Global Cardholder Synchronizer***
- ❑ In the **Specific info** page, enter the following parameters, and click **Next**.
  - ❑ *Server*. Server where this role will be hosted.
  - ❑ *Directory*. Sharing host's main server name or IP.
  - ❑ *Username and Password*. Credentials used to connect to the sharing host. The extent of what the sharing guest can do on the global partition will be limited by what this user can see and do on the sharing host. The user must have the *Global Cardholder Synchronizer* privilege on the sharing host in order to connect as well as the privilege to see *cardholders* and *credentials*
  - ❑ *Synchronize automatically*. Select this option to have the GCS to update the guest system immediately, every time a change is made on the host.

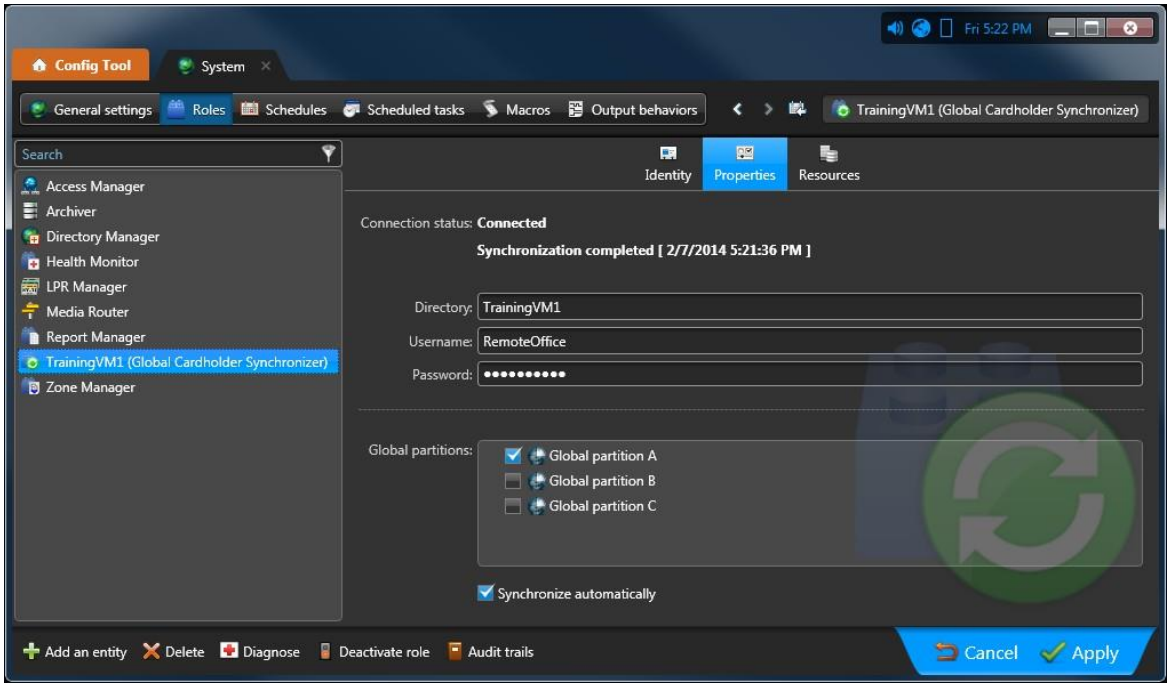


- ❑ In the **Basic information** page, enter the name, description, and partition where the GCS role should be created.
- ❑ Click **Next**, **Create**, and **Close**.

- ❑ Click the **Properties** tab.
- ❑ Ensure that the remote *Global Cardholder Synchronizer* role can successfully connect to the host system for cardholder and credential information. What does the ***Connection status*** indicate? Be patient, sometimes it takes a minute or so to connect, authenticate and download the information.



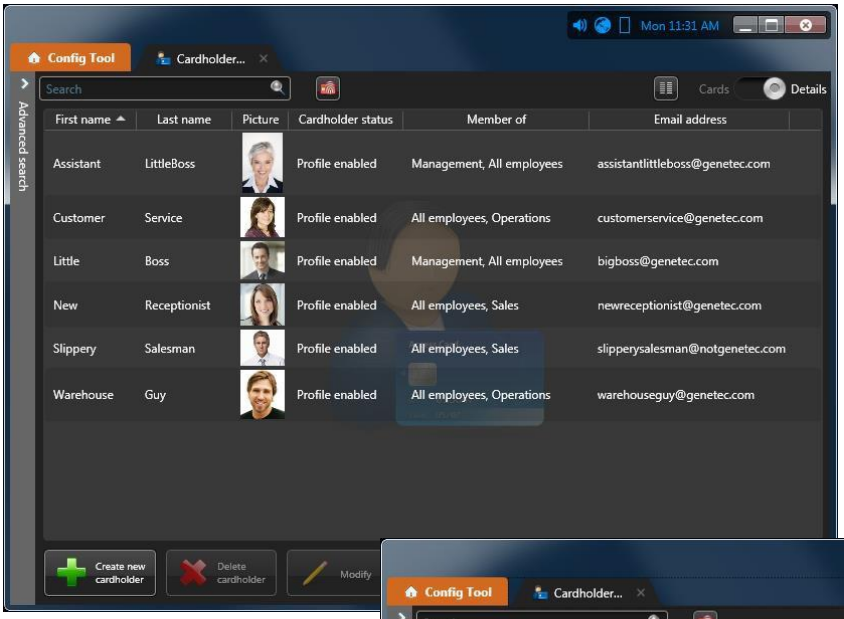
- ❑ Select the partition(s) you want your local system to synchronize and click **Apply**.



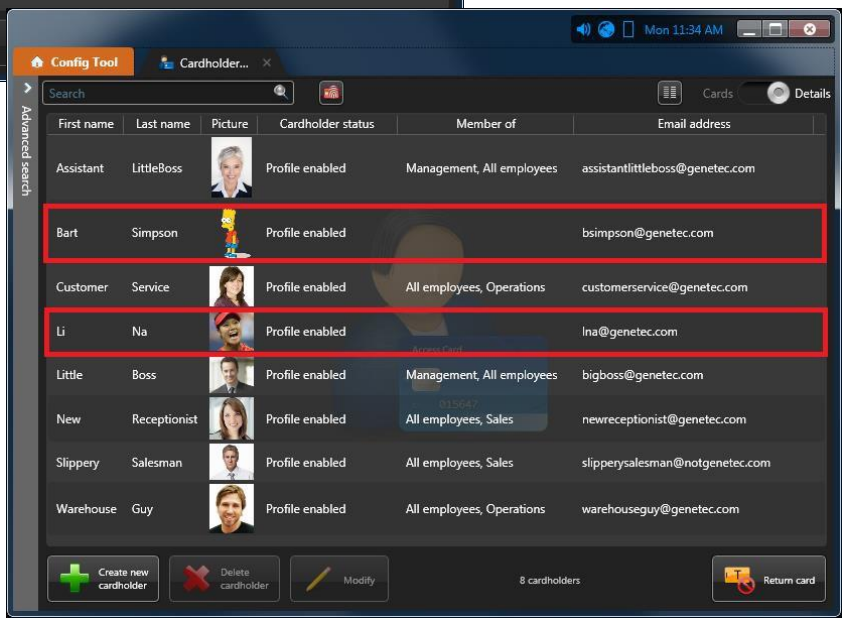
- ❑ If the ***Global Cardholder Synchronizer*** is not configured to synchronize automatically, then click **Synchronize now** ( ). Click ***Apply***.

Once the **Global Cardholder Synchronizer** has successfully connected and synchronized with the **Sharing Host**, we find can both local cardholders and global cardholders in our own system.

- ❑ Open **Config Tool → Cardholder management** task
- ❑ Do you see the new, global cardholders?



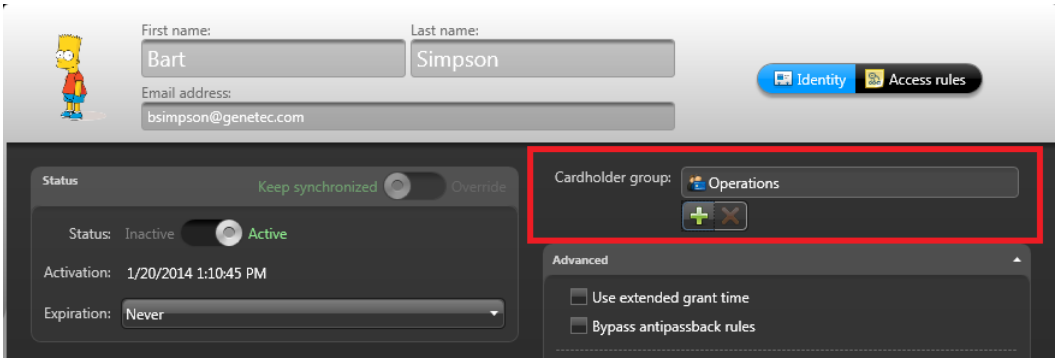
List of cardholders before the ***Global Cardholder-Synchronizer*** was configured.



List of cardholders after the ***Global Cardholder-Synchronizer*** was configured.

Notice that the global cardholders and their credentials have been imported but not automatically added to any cardholder groups nor access rules.

- ❑ Double click one of the newly imported cardholders and add them to a cardholder group

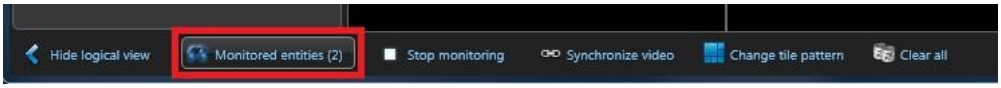


- ❑ Click Save and close

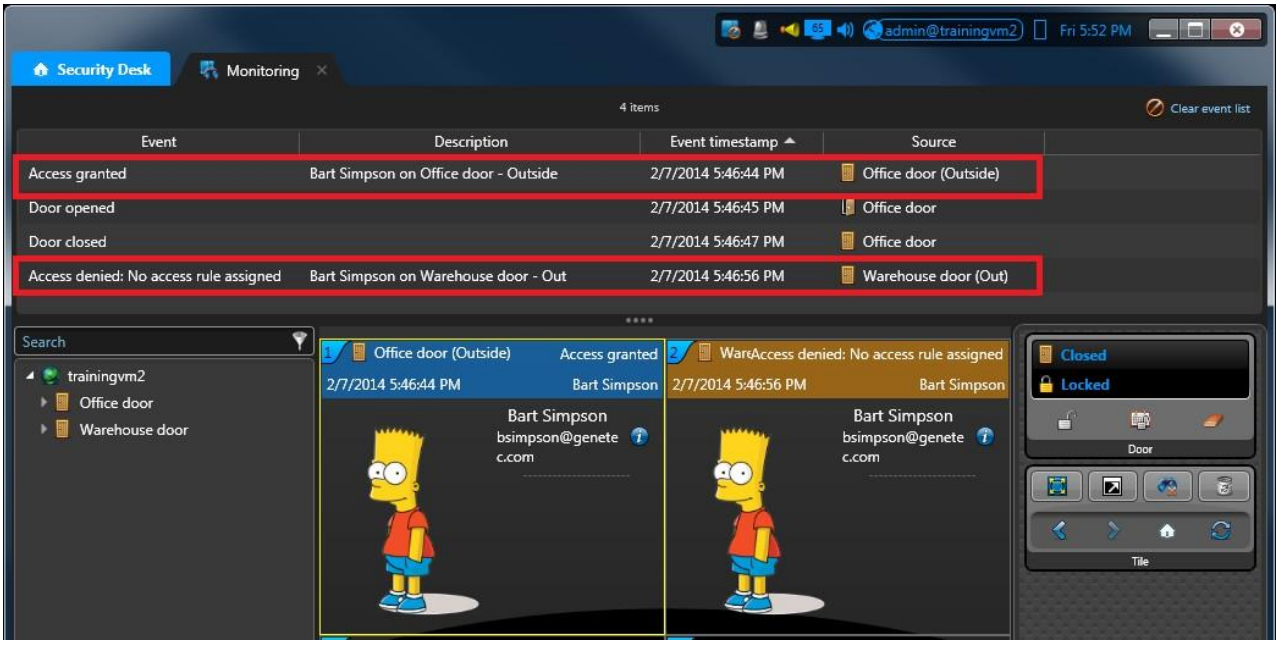
The imported cardholder should now inherit access through any access rules that name the cardholder group to which he/she was added

Test the global cardholders' access rights

- ❑ Identify 1 door where the global cardholder should have access granted (due to his/her cardholder group membership) and 1 door where he/she should have access denied
- ❑ Open **Security Desk → Monitoring** task
- ❑ Add the 2 test doors to the *Monitoring task*'s list of ***Monitored entities***



- ❑ Test access at each of the doors. Do you see the appropriate access granted and access denied events?



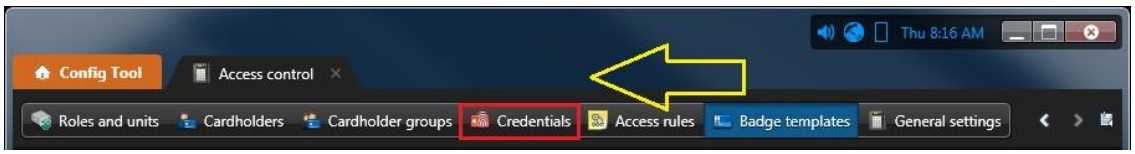
Badge Designer

The **Badge designer** is a tool that allows you to design and modify badge templates.

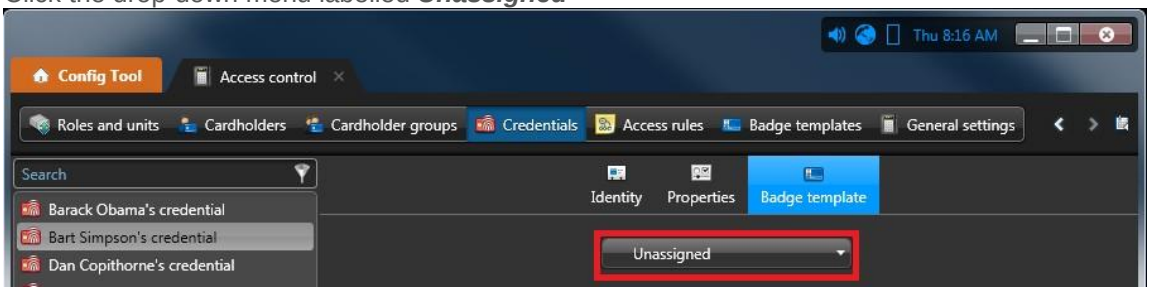
- ***Badge templates*** can be created, using:
  - Cardholder information
  - Credential information
  - Pictures
  - Custom fields
  - Other text & images, such as logos
- ***Badges templates*** can printed for batches of credentials
- Templates can be imported & exported using an XML file

- ❑ Open the Config Tool → Access control task → Badge templates
- ❑ Click the *Add* ( ) ***Badge template*** button at the bottom left corner
- ❑ Immediately rename the new template so you can identify it
- ❑ Complete the following:

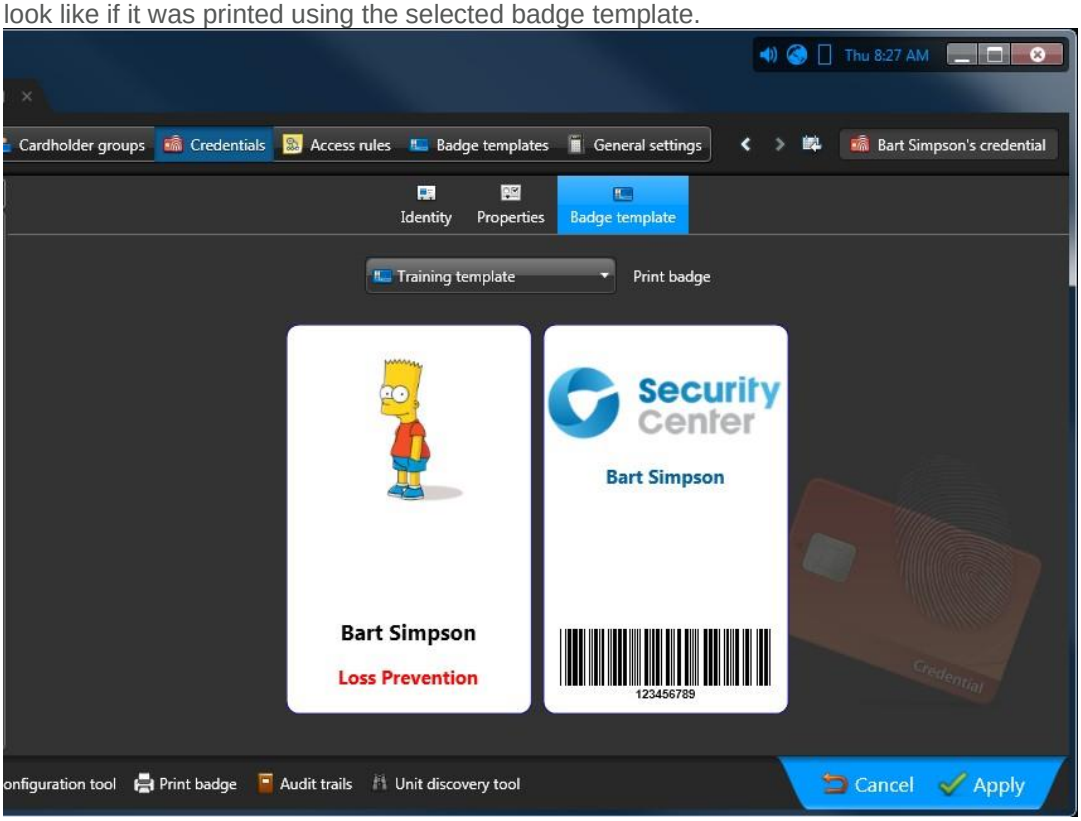
- ❑ Once you have saved your new badge template, you can preview cards with your template by selecting the ***Credentials*** tab of the **Access control** task



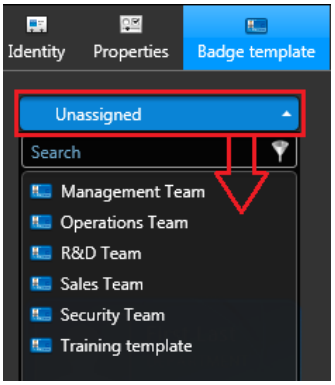
- ❑ Select a credential and click its ***Badge template*** tab.
- ❑ Click the drop-down menu labelled ***Unassigned***



- ❑ Choose your badge template from the list. A preview should appear showing what the card would look like if it was printed using the selected badge template.



- ❑ Preview several other badge templates



- ❑ Click ***Apply***.

Module 8 - Alarms & Threat Levels

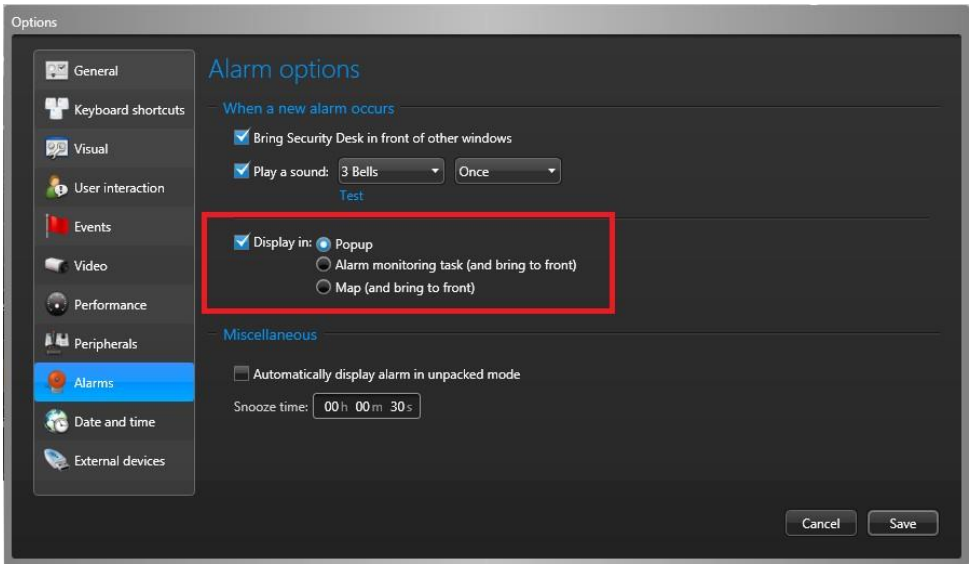
Alarms

Create and configure an alarm

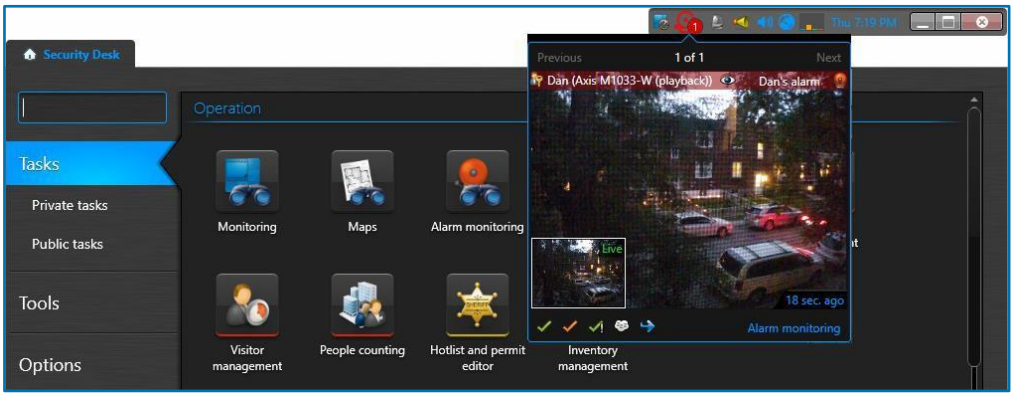
- ❑ Open the **Config Tool** → **Alarm** *task*
- ❑ Click **Add an alarm** ( ) and assign your name to the new alarm immediately
- ❑ Select your new alarm's **Properties** tab ( )
  - ❑ Set the alarm **Priority** to *100*
  - ❑ Click **Add recipient** ( ) and add your own user profile as the alarm recipient
  - ❑ Click **Attach an entity** ( ) and add 2 cameras to your alarm
  - ❑ Click **Video display option** and select **Live and playback** from the drop-down menu
  - ❑ Click the properties button ( ) and choose the picture-in-picture options
  - ❑ Ensure that **Content cycling** is set to ***ON*** with a dwell time of **5 seconds**
  - ❑ Click **Apply** ( )
- ❑ Select your new alarm's **Advanced** tab ( )
  - ❑ Set the **Reactivation threshold** to 5 seconds
  - ❑ Set the **Alarm procedure (URL)** to ***ON*** and set the path to http://www.google.com
  - ❑ Set the **Schedule** to ***Always***
  - ❑ Set **Automatic acknowledgement** to ***OFF***
  - ❑ Set **Create an incident on acknowledgement** to ***OFF***
  - ❑ Set the **Color** to anything you would like
  - ❑ Click **Apply** ( )

Test your alarm by triggering it manually

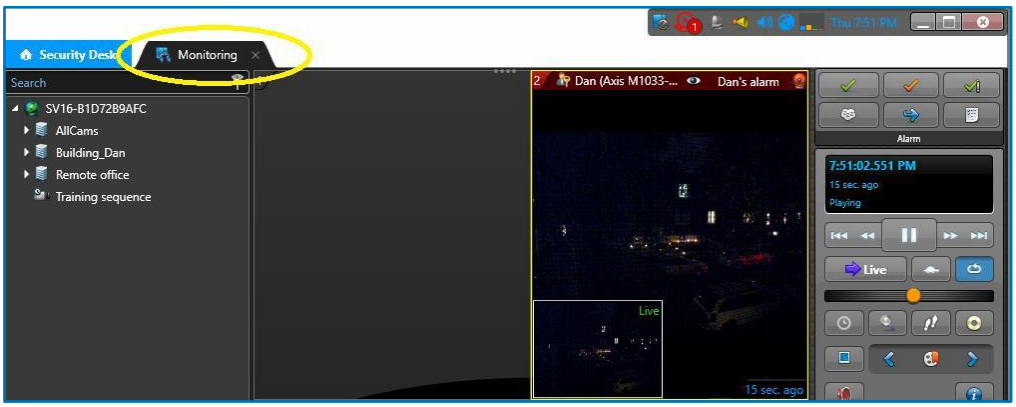
- ❑ Open the **Config Tool** → **Alarm** *task*
- ❑ Open the **Security Desk** → **Options** *menu.* Select ***Alarms*** and make the sure ***Alarm options*** are configured to display the alarm in a popup window. Click ***Save***



- ❑ In the Config Tool's **Alarm** task, select your alarm and click the ***Trigger alarm*** ( ) button at the bottom of the page. You should receive the alarm in your Security Desk regardless of which task, if any, is open. The alarm highlight color will be the one configured in the alarm's **Advanced** tab.



- ❑ Inspect the alarm video. Do you see the rotation of 2 cameras and a web page?
- ❑ Is the picture in picture image the way you had configured it in your alarm properties?
- ❑ Click the **Default acknowledge** widget ( ) to dismiss the alarm
- ❑ Click the Security Desk **Home** tab (Security Desk)
- ❑ Click **Options → Alarms**
  - ❑ Check the box beside **Bring Security Desk in front of other windows**
  - ❑ Check the box beside **Play a sound** and select a sound file
  - ❑ Change the **Display in** option from **Popup** to **Alarm monitoring task (and bring to front)**
  - ❑ Under **Miscellaneous** alarm options, set the **Snooze time** to 20 seconds. Click **Save**.
- ❑ In your **Config Tool → Alarm** *task*, select your alarm
- ❑ Select your alarm's **Advanced** properties page and toggle the setting ***Create an incident on acknowledgement*** to **ON**. Click **Apply**
- ❑ Ensure your Security Desk is connected and that no tasks are open. From your Config Tool's **Alarm** task manually trigger your alarm again. This time, it should display differently in your Security Desk.
- ❑ Did your Security Desk open a new **Alarm Monitoring** task and display the alarm in a tile instead of showing the alarm as a popup from the notification tray?
- ❑ Try the different alarm widgets like **Show procedure** ( ), **Snooze** ( ), and **Forward** ( )
- ❑ Click the *composite entity* icon ( ) at the top of the alarm tile
- ❑ Click **Unpack** What happens? Click **Pack tile** ( )
- ❑ Click **Default Acknowledge** ( )
- ❑ Enter some text in the *incident report*. Click **Create**
- ❑ In the Security Desk, close all tasks except a **Monitoring** task, Remove any cameras from tiles
- ❑ Click the Security Desk **Home** tab (Security Desk)
- ❑ Click **Options → Alarms**
  - ❑ Change the **Display in** option from **Alarm monitoring task (and bring to front)** to **Popup**.
  - ❑ Click **Save**
- ❑ Select (click) tile #2 in the **Monitoring** task and press alt+A to arm the tile for alarms
- ❑ Trigger an alarm again. Did it show up in the armed tile (red number tab) instead of the notification tray or the **Alarm Monitoring** task?



Test your alarm by triggering it automatically

- ❑ Use the Config Tool > System task > Actions to configure an automatic event/action link:
  - ***Event*** = Door forced open → ***Action*** = Trigger alarm (use your door & alarm)
- ❑ Test your automatic alarm trigger by manually toggling your door monitor input

Threat levels

Create and configure a threat level

- ❑ Open the **Config Tool** → **Logical view** task. If you don't have your own *area*, create one now. Drag and drop your door into your area
- ❑ Open the **Config Tool** → **System** *task* → **Threat levels**
- ❑ Click **Add an item** (➕) to create a new *threat level*
  - ❑ Name your threat level after your own user name
  - ❑ Select a colour for your new threat level
  - ❑ Under **Activation actions**, Click **Add an item** (➕)
  - ❑ Select the action **Start recording**, and select a **Camera**
  - ❑ Under **Activation actions**, Click **Add an item** (➕) again
  - ❑ Select **Add a bookmark**, select your own **Camera** and type the message: ***Threat level activated_(YourThreatLevelName).***
  - ❑ Under **Activation actions**, Click **Add an item** (➕) again
  - ❑ Select **Send a message**, select your own user as the recipient and type the **Message:** ***(YourThreatLevelName) has been activated***
  - ❑ (Will only work with SMC's): **Add an item** → **Set minimum security clearance**: 50
  - ❑ Under **Dectivation actions**, Click **Add an item** (➕)
  - ❑ Select the action **Stop recording**, and select your own **Camera,** select **Stop in:** ***Now***
  - ❑ Under **Deactivation actions**, Click **Add an item** (➕) again
  - ❑ Select **Add a bookmark**, select your own **Camera** and type the message: ***Threat level deactivated_(YourThreatLevelName).***
  - ❑ Under **Deactivation actions**, Click **Add an item** (➕) again
  - ❑ Select **Send a message**, select your own user as the recipient and type the **Message:** ***(YourThreatLevelName) has been deactivated***
  - ❑ (Will only work with SMC's): **Add an item** → **Set minimum security clearance**: 99

- ❑ Click **OK.** Click **Apply**

Test your threat level

- ❑ In the Security Desk, double click the threat level icon in the notification tray

- ❑ Select your **Area**, select your **Threat level** and click **Apply**
- ❑ You should receive your treat level activation message
- ❑ Display your door in the *Monitoring task*
- ❑ Try presenting credentials to your door reader. If the door is controlled by an SMC, any cardholders whose clearance level is a value higher than 50 should get access denied.
- ❑ Double click the threat level icon in the notification tray again
- ❑ Remove your threat level from the area

One at a time, please:

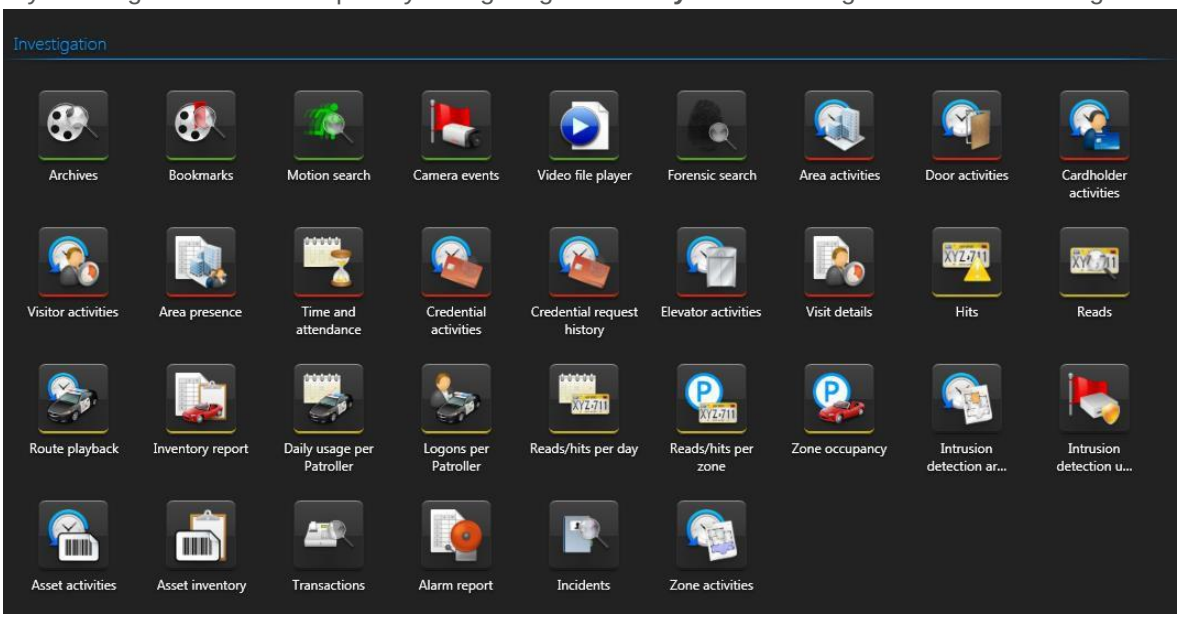
- ❑ In the Security Desk, double click the threat level icon in the notification tray
- ❑ Apply your threat level to the entire system instead of your area.
  All users connected with the Security Desk should see a colour change to the Security Desk skin

Automated emails & reports

Create a custom report and configure a **Scheduled task** to run the report and send it to a user by email on a weekly basis.

Creating a customized report template

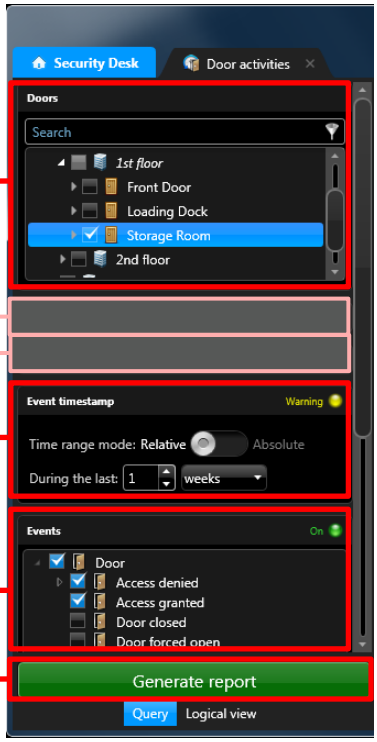
Start by creating a customized report by configuring a **Security Desk** investigation task and saving it.



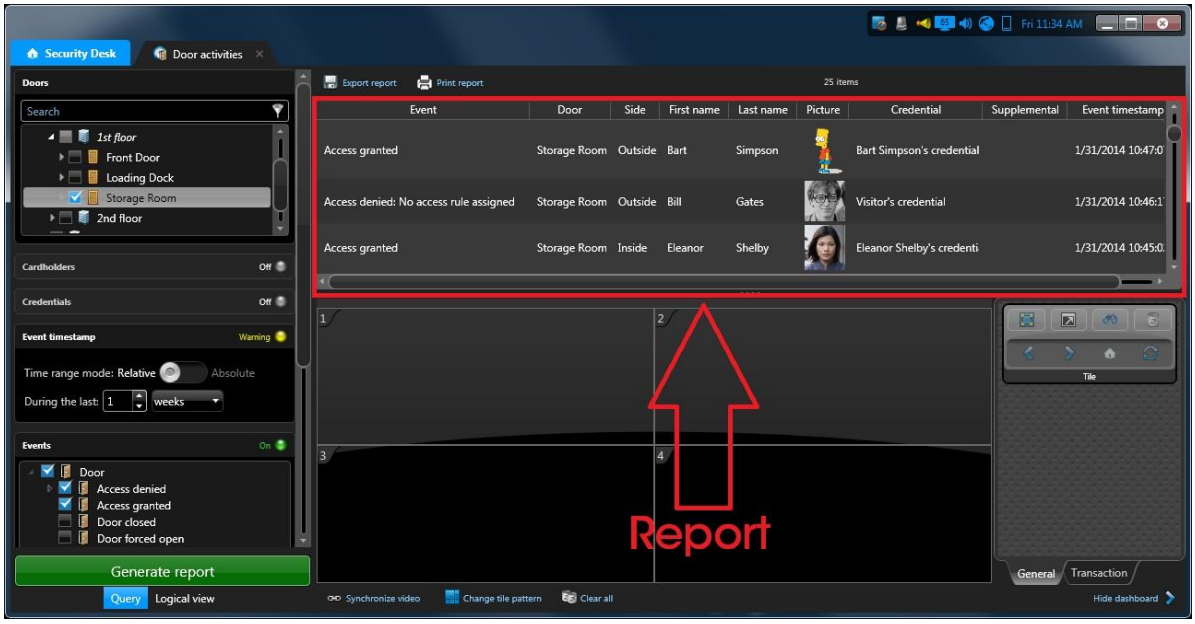
33 different *Investigation tasks* (reports) can be run by the ***Task scheduler***

The following is an example *investigation task* only. Feel free to configure any other *investigation task*:

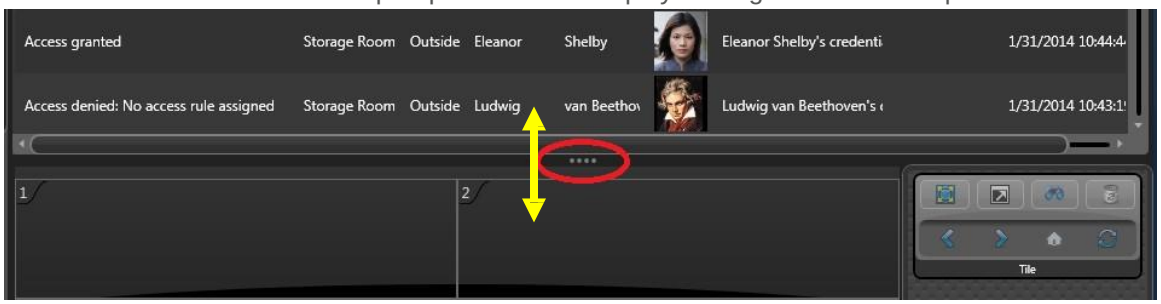
- ❑ Open **Security Desk** → *Investigation task* → **Door activities** task. Configure the search filters as:
- ❑ **Doors**: Select your door
- ❑ (Optional: select cardholders)
- ❑ (Optional: select credentials)
- ❑ **Event timestamp**: (Relative) *During the last 1 week*
- ❑ **Events**: *Access denied* and *Access granted*
- ❑ Click ***Generate report***



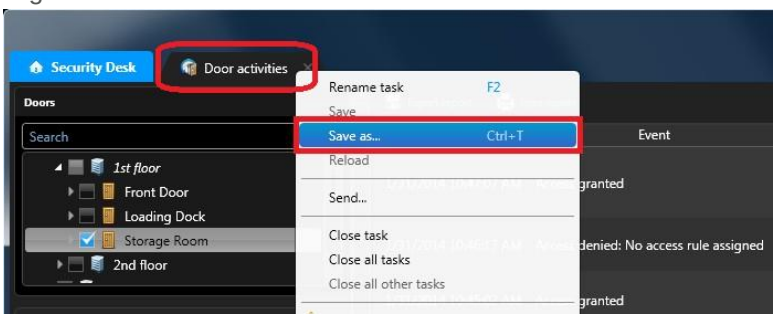
- ❑ Does your report display the expected results? The report results will be found in the report pane of the Security Desk *Door activities* task:



- ❑ Click the handle between the report pane and the display to drag and resize the pane borders



- ❑ Try the F9 keyboard shortcut to show tiles only, report only, or both.
- ❑ Right click one of the column headers and click **Select columns** (or, CTRL+Shft+C)
- ❑ Remove the column ***Supplemental credential*** from the fields displayed (Click)
- ❑ Select the ***Event timestamp*** field and push it up ( ) to the top of the list. Click **OK**
- ❑ Did the report's displayed columns and order of the columns change?
- ❑ Click the ***Export report*** button and export to PDF format on your desktop. Examine the exported file.
- ❑ Right click the Door activities task tab and select ***Save as***



- ❑ Save the report as a public task and give it a name you will recognize

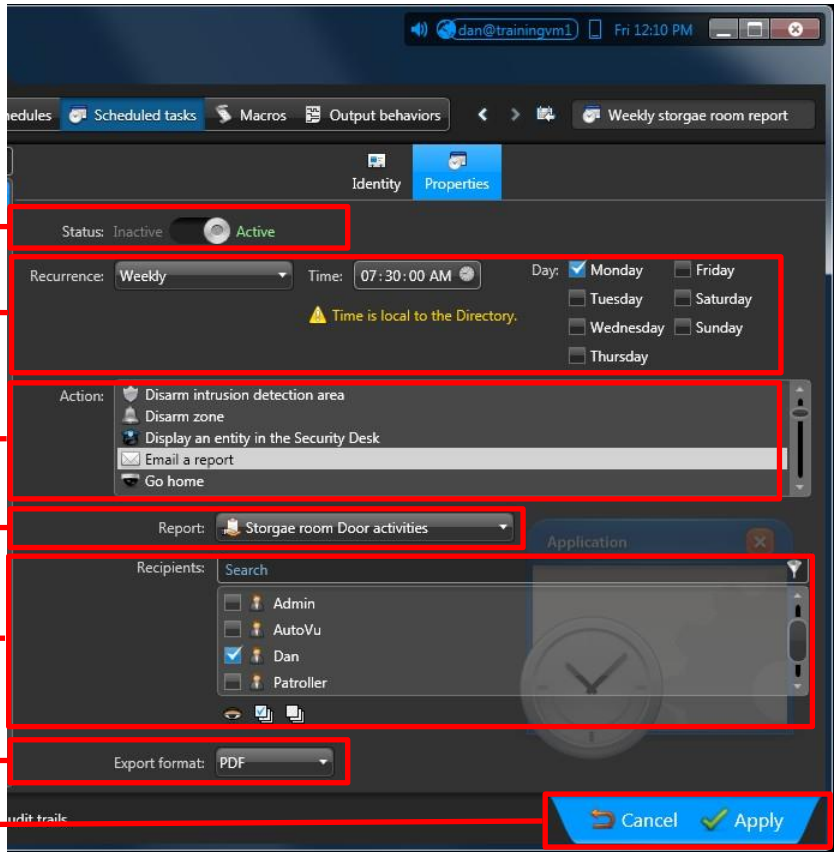
Creating a scheduled task

Now that you have a customized report saved as a public task, we can use the task scheduler to run the report and send it to the Security Manager every Monday morning.

- ❑ Open **Config Tool** → **System** task → ***Scheduled tasks***
- ❑ Click Add ( ) **Scheduled task**. Name your scheduled task immediately
- ❑ Select your scheduled task's **Properties** tab

  Configure the following properties

- ❑ **Status**: Active
- ❑ **Recurrence**: Weekly / Mon. 07:30
- ❑ **Action**: Email a report
- ❑ **Report**: (your report)
- ❑ **Recipients**: (who will receive report)
- ❑ **Export format**: PDF
- ❑ Click **Apply**



Done. According to the configurations above, the Security Manager, Dan will receive a PDF report by email every Monday morning. The report will show all access granted and access denied events at the Storage Room door over the last week.

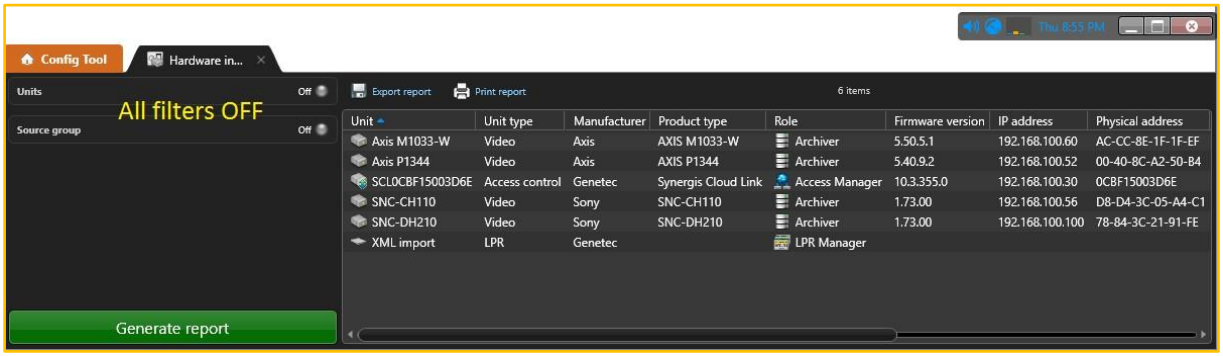
If there is no email server accessible for the Genetec server to send emails, you may not be able to test any further.

Module 9 - Maintenance & Troubleshooting

Hardware inventory task

Generate a Hardware inventory report

- ❑ Using either the Security Desk or the Config Tool, open a new **Hardware inventory** *task* (Maintenance)
- ❑ In the query filters pane on the left hand side, turn off the **Units** filter and turn off the **Source group** filter
- ❑ Click **Generate Report**

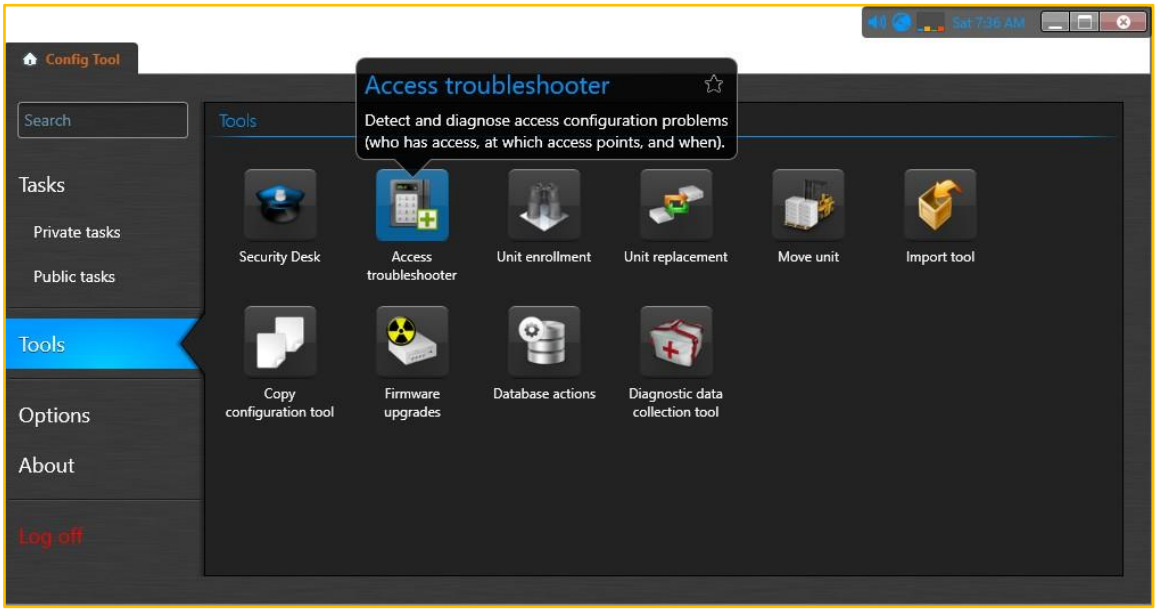


- ❑ Click **Export report**. Save your inventory report as a Microsoft Excel file.
- ❑ In the query filters pane on the left hand side, turn on the **Units** filter and turn on the **Source group** filter. Try different combinations of query filters

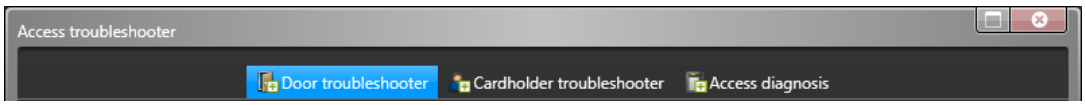
Access troubleshooter tool

Run the Access troubleshooter tool

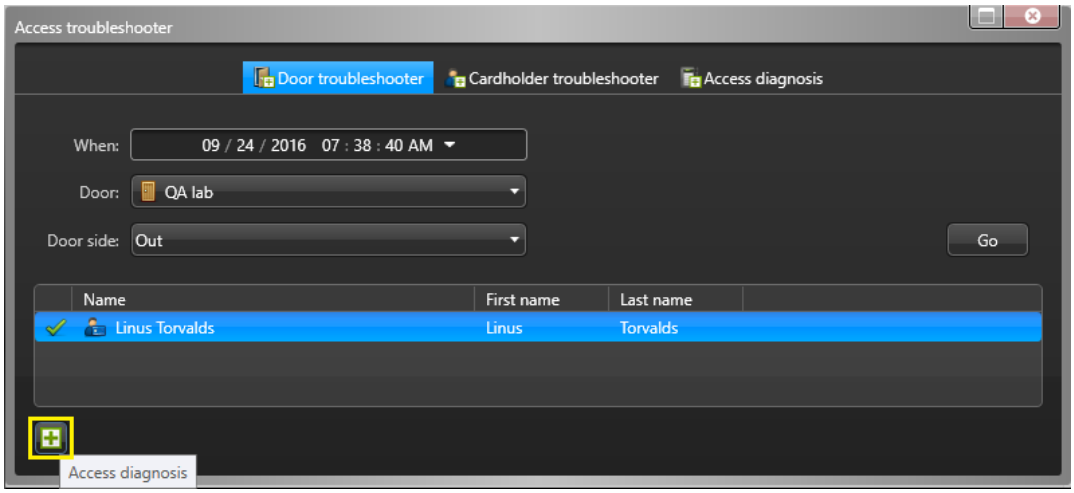
- ❑ Open the **Config Too**l → ***Tools*** → ***Access troubleshooter***.



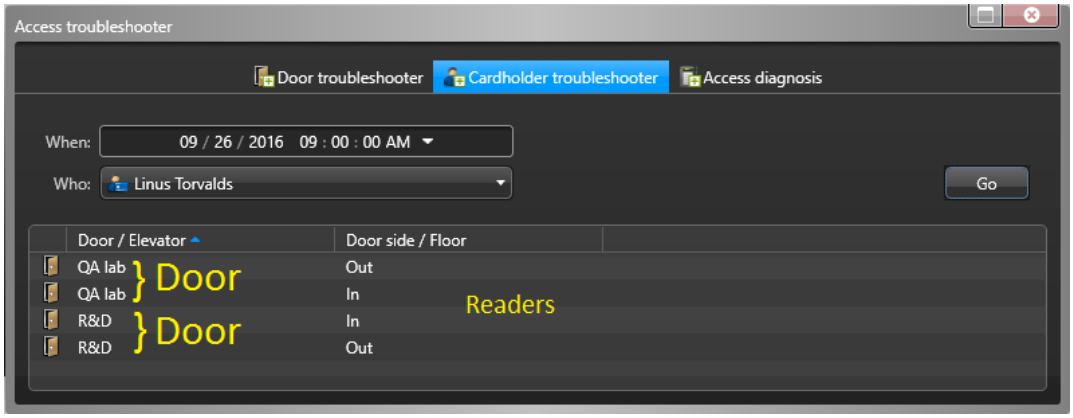
- ❑ Notice the 3 tabs across the top of the **Access troubleshooter tool**



- ❑ Under the ***Door troubleshooter*** tab try querying who will have access to a given door by setting the filters: ***When:*** / ***Door:*** / ***Door side:*** and click ***Go***
- ❑ How many cardholders will have access? _____ Modify the query filter and try again.
- ❑ Select a cardholder and click the ***Access diagnosis*** button at the bottom of the page



- ❑ What happens?
- ❑ This feature is helpful when you need to verify why someone doesn't have access to a door
- ❑ Click the cardholder troubleshooter tab
- ❑ Under the ***Cardholder troubleshooter*** tab try querying which doors will be accessible to a given cardholder by setting the filters: ***When:*** / ***Who:*** and click ***Go***

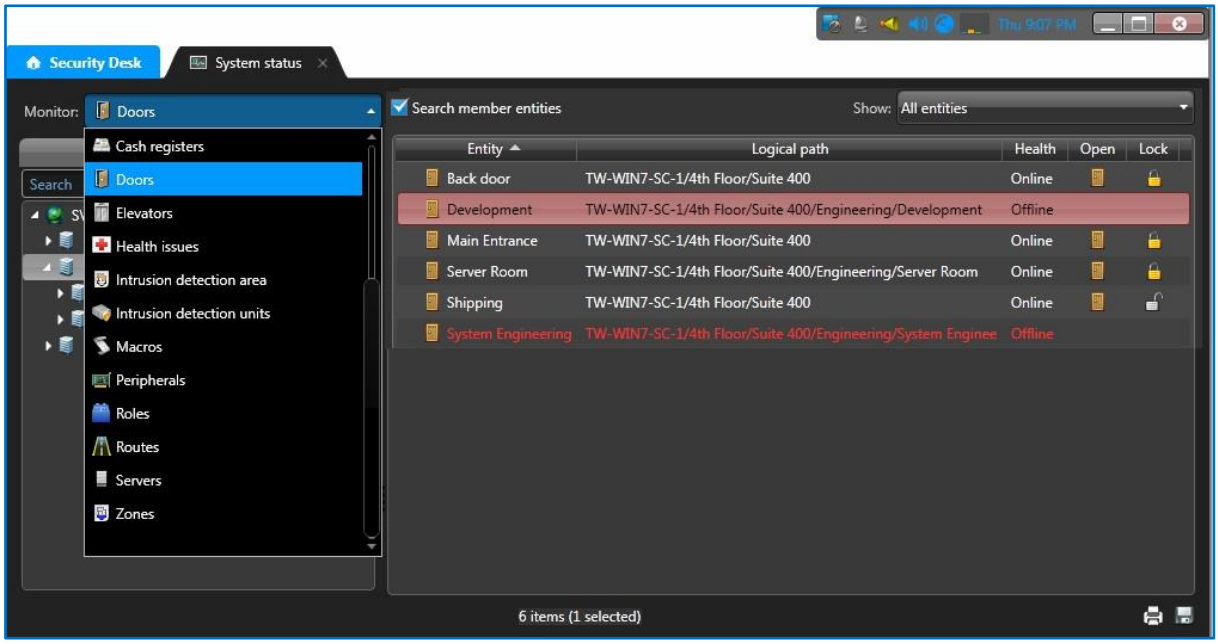


- ❑ To how many door readers will the cardholder have access? _____

System status task

Monitor the status of system components

- ❑ Using either the Security Desk or the Config Tool, open a new **System status** *task* (Maintenance)
- ❑ Select **Monitor: *Applications***. Click **Refresh now**
- ❑ Select **Monitor: *Doors***. Click **Refresh now**
- ❑ Select **Monitor: *Roles***. Click **Refresh now**
- ❑ Try monitoring the status of other components



Health monitoring task

Run a Health statistics report to monitor the overall health of your system.

- ❑ Using either the Security Desk or the Config Tool, open a new **Health statistics** *task* (Maintenance)
- ❑ In the query filters in the left hand pane, select a **Time range**
- ❑ In the query filters in the left hand pane, select some or, all **Source entities**
- ❑ Click **Generate report**
- ❑ Click **Export report** and save it on your *Windows desktop*