

Visor Tablette

TECHNICAL MANUAL

FOREWORD

This document explains how to configure Visor as well as the Visor Tablette V1.2.0.0 application.
This document describes all of the features of the Visor Tablette application.



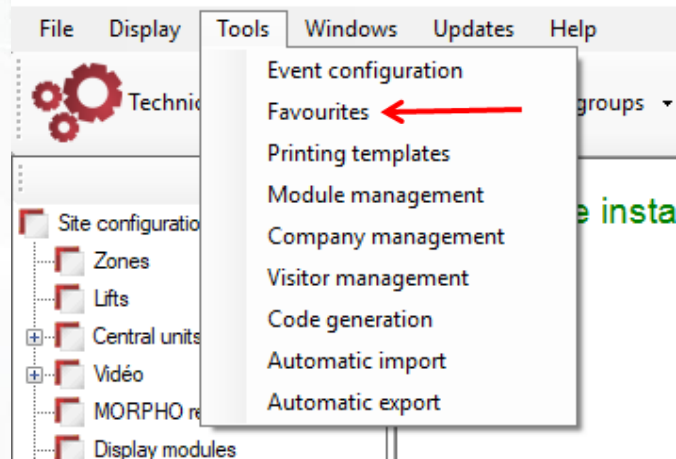
CONTENTS

- FOREWORD 2**
- TO CONFIGURE VISOR..... 4**
- TO CONFIGURE WINDOWS 9**
 - WINDOWS 7:..... 9
 - WINDOWS 10:..... 13
- TO USE THE APPLICATION 17**
 - HOME SCREEN 17
 - ABOUT US..... 18
 - SETTINGS 19
 - MAIN MENU..... 20
 - EVENTS..... 21
 - OVERVIEW 23
 - USERS 24
 - USER RECORD 25
 - GROUPS 26
 - GROUP RECORD..... 27
 - PLANNING 28
 - SECURITY LEVEL 34
 - CAMERAS..... 35

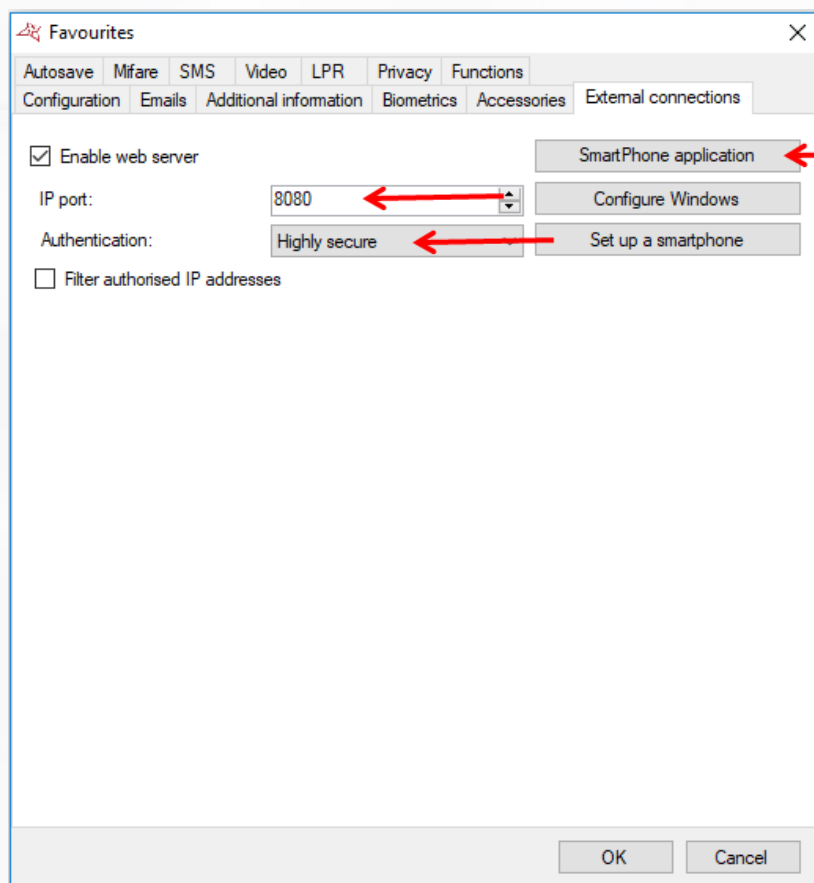


TO CONFIGURE VISOR

Enable external connections. To do so, click on the Tools menu and then Favourites.



From the External connections tab, click on Smartphone application. Specify an IP port and select the Highly secure authentication mode.



If you have WINDOWS 7, click on the Configure Windows button and click on Yes when prompted.

If you are using Visor 2.0.0.16 or a higher version, ignore step 2, 'To Configure Windows'. VISOR will automatically configure Windows Firewall when you click the Configure Windows button.

You can restrict connections by entering IP addresses authorised to log in. To do so, check the Filter authorised IP addresses box and add the various addresses.



From the Administration-> Managers menu, create a manager who will be authorised to use the smartphone application as follows:

Manager 2

Information Rights Companies

Last name: admin

First name:

E-mail address:

Telephone:

Password: ●●●●

Confirm password: ●●●●

Validity dates

Enable

The password may be changed

The password must be changed

Manager prohibited

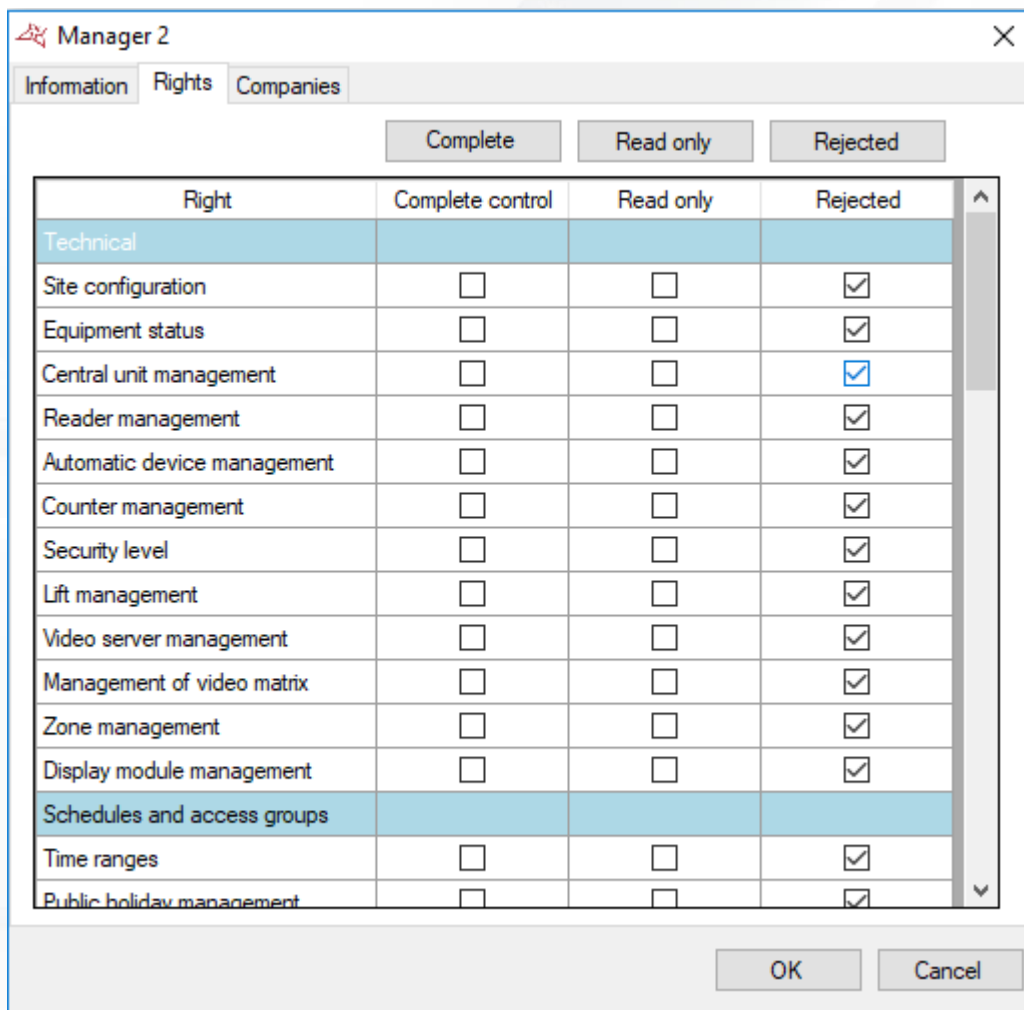
Manager using the SmartPhone application

Receive e-mail alerts

Operator able to acknowledge

OK Cancel

For the smartphone application, enter this manager's name ('admin' here) and password. In the Rights tab, check the boxes corresponding to the permissions you want to assign to the manager.



For the tablet application connected to VISOR version 2.0.0.16 or higher, the following permissions will be used:

- Users:

Users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
-------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to view and edit users. Check Read only so the manager may view but not edit users. Lastly, check Rejected to hide user management.

- Overview:

Overview display	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
------------------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to control a reader for a floor plan. Check Read only so the manager may view but not control readers in floor plans. Lastly, check Rejected to hide overview management.

- Security level:

Security level	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
----------------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to edit the installation's security level. Check Read only so the manager may view but not edit the installation's security level. Lastly, check Rejected to hide security level management.

- Access groups:

Access groups	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
---------------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to view and edit access groups. Check Read only so the manager may view but not edit access groups. Lastly, check Rejected to hide access group management.

- Time ranges:

Time ranges	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
-------------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to view and edit time periods. Check Read only so the manager may view but not edit time periods. Lastly, check Denied to hide time period management.

- Public holiday management:

Public holiday management	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
---------------------------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to view and edit holidays. Check Read only so the manager may view but not edit holidays. Lastly, check Rejected to hide holiday management.

- List of special days:

List of special days	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
----------------------	--------------------------	--------------------------	-------------------------------------

Check Complete to enable the manager to view and edit lists of special days. Check Read only so the manager may view but not edit lists of special days. Lastly, check Rejected to hide the management of lists of special days.

Visor configuration has now been completed.

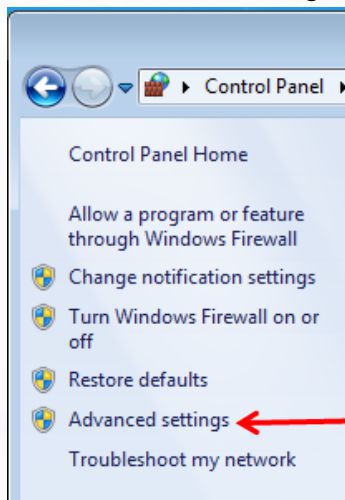


TO CONFIGURE WINDOWS

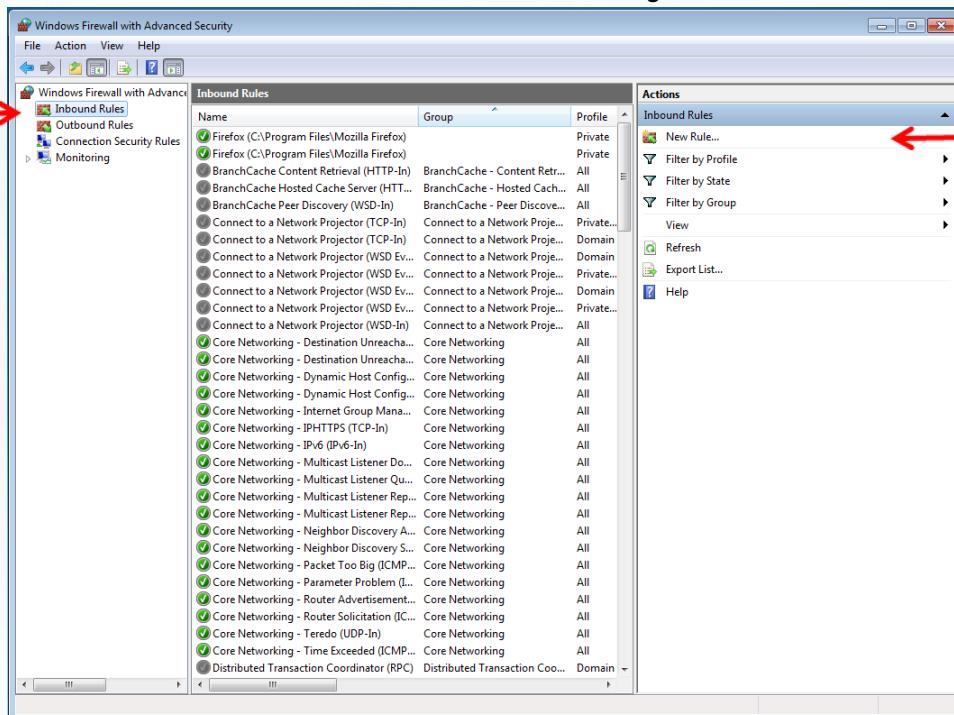
WINDOWS 7:



Go into the Control Panel and open 'Windows firewall'
Click on Advanced settings in the left-hand column

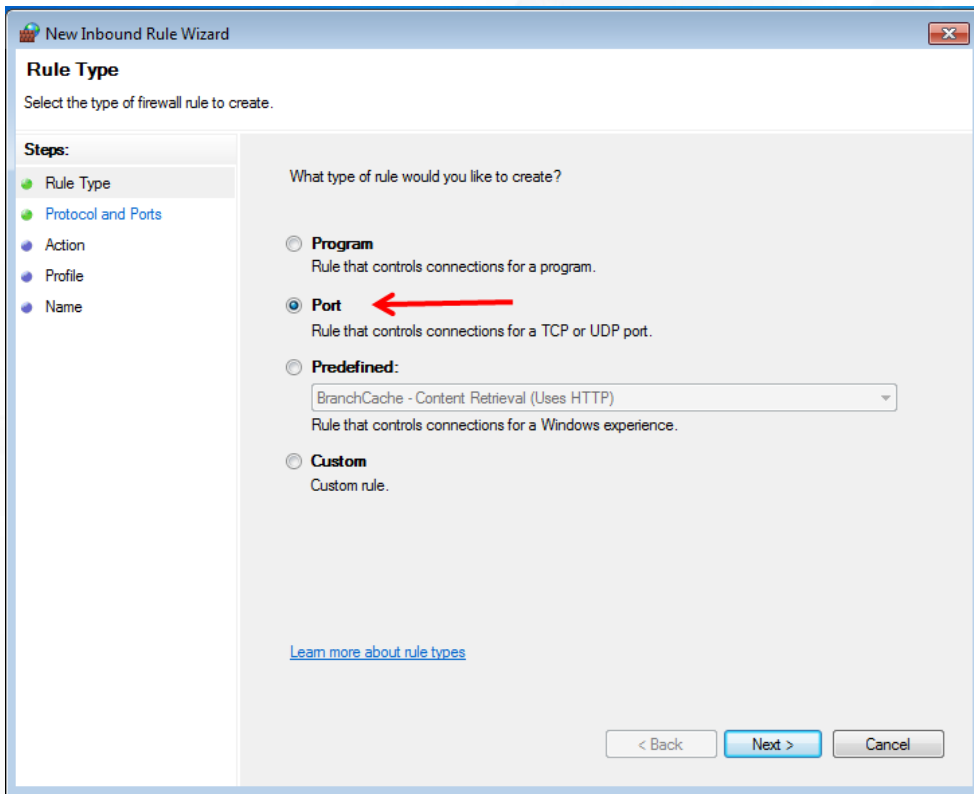


In the left-hand column, select Inbound rules. In the right-hand column, click on New rule

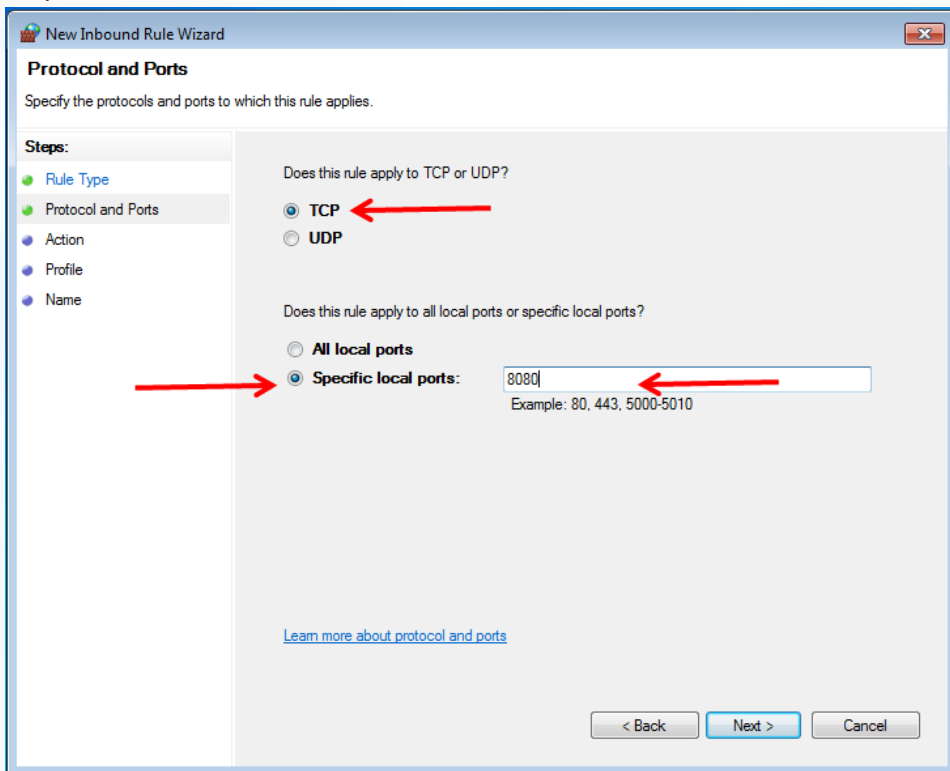


Select 'Port', then click on Next





Select TCP and Specific local ports. Specify the port (8080 or the port you used in the previous steps), then click on Next



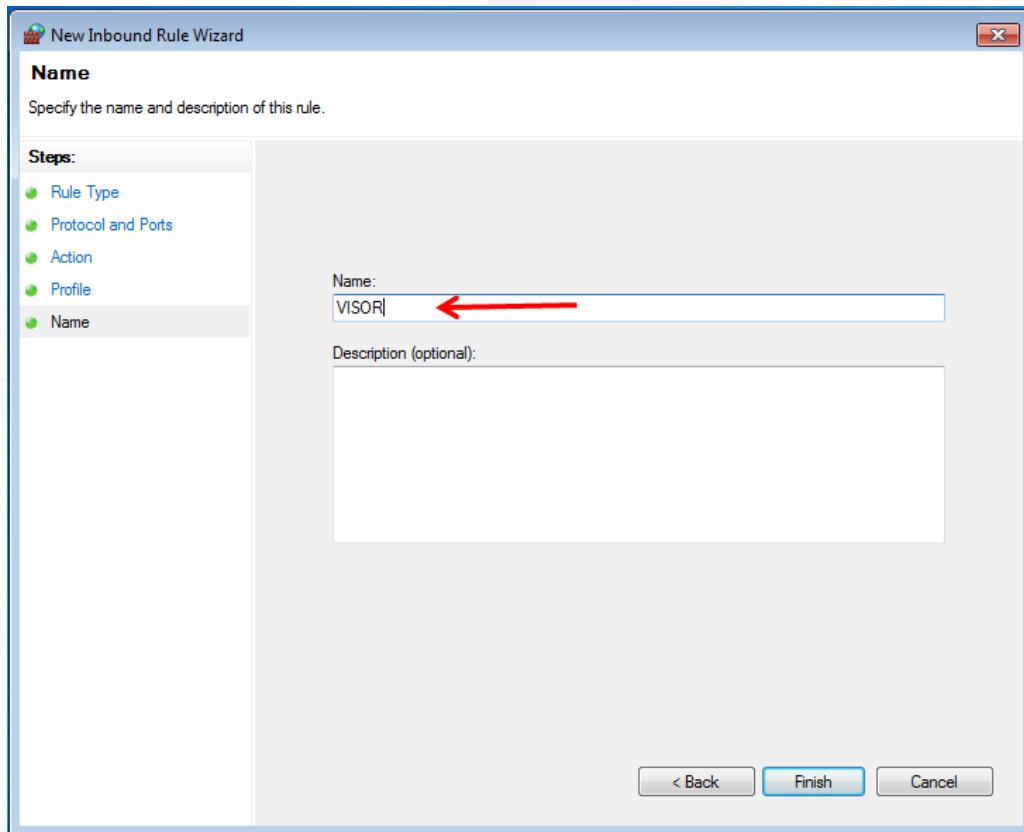
Select Allow the connection, then click on Next

The screenshot shows the 'New Inbound Rule Wizard' dialog box at the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. A red arrow points to the 'Action' step. The main area asks 'What action should be taken when a connection matches the specified conditions?' and offers three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. A 'Customize...' button is next to the 'Allow the connection if it is secure' option. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

Check all the boxes, then click on Next

The screenshot shows the 'New Inbound Rule Wizard' dialog box at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Profile' step is highlighted. The main area asks 'When does this rule apply?' and offers three checked checkbox options: 'Domain', 'Private', and 'Public'. Each option has a brief description: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location.), and 'Public' (Applies when a computer is connected to a public network location.). A 'Learn more about profiles' link is at the bottom. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

Enter the name of the rule, then click on Finish



New Inbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
VISOR

Description (optional):

< Back Finish Cancel

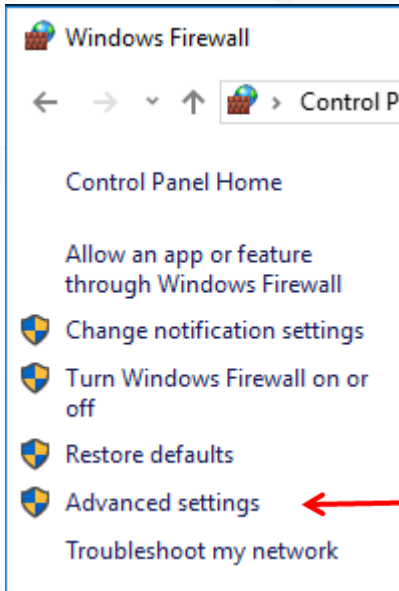
Firewall configuration has now been completed.

WINDOWS 10:

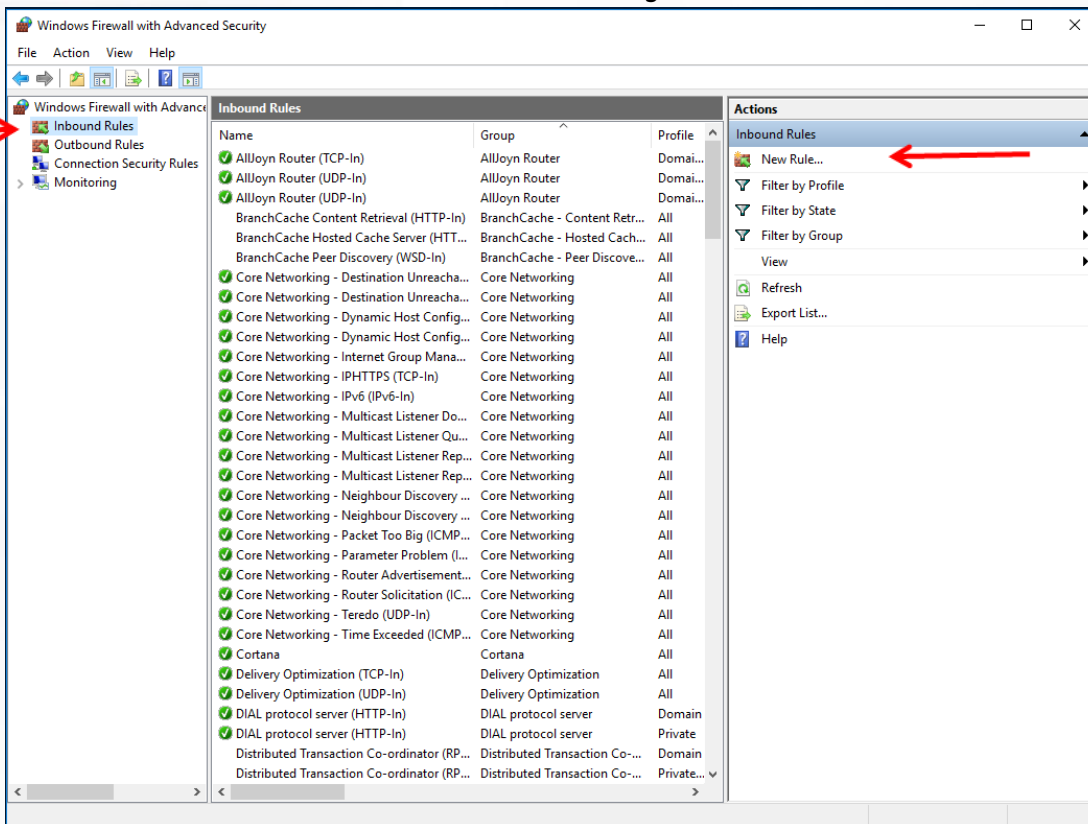


Windows Firewall

Go into the Control Panel and open 'Windows firewall'
Click on Advanced settings in the left-hand column

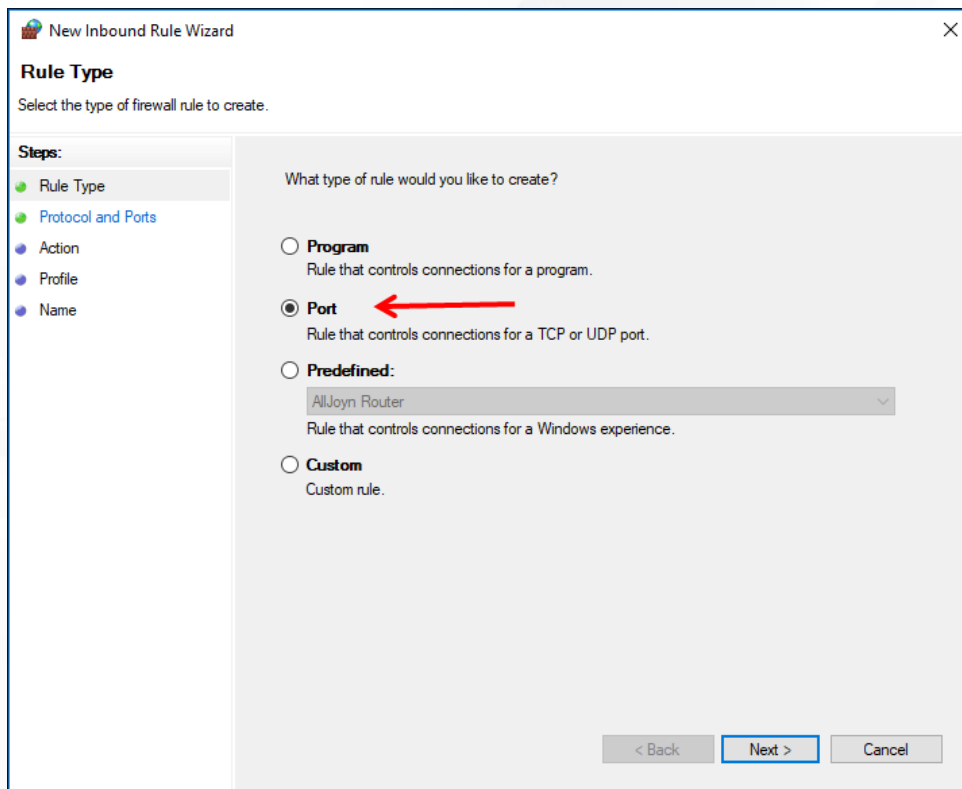


In the left-hand column, select Inbound rules. In the right-hand column, click on New rule

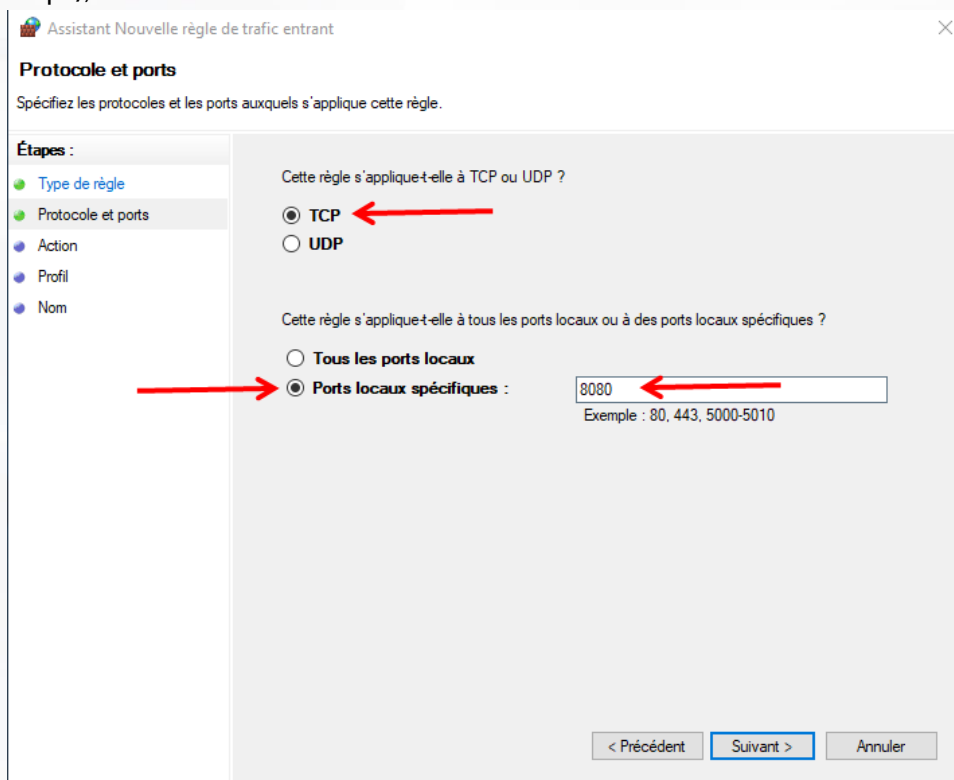


Select 'Port', then click on Next





Select TCP and Specific local ports. Specify the port (8080 or the port you used in the previous steps), then click on Next



Select Allow the connection, then click on Next

New Inbound Rule Wizard

Action
Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- **Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

Allow the connection
This includes connections that are protected with IPsec as well as those are not.

Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Block the connection

< Back Next > Cancel

Check all the boxes, then click on Next

New Inbound Rule Wizard

Profile
Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- **Profile**
- Name

When does this rule apply?

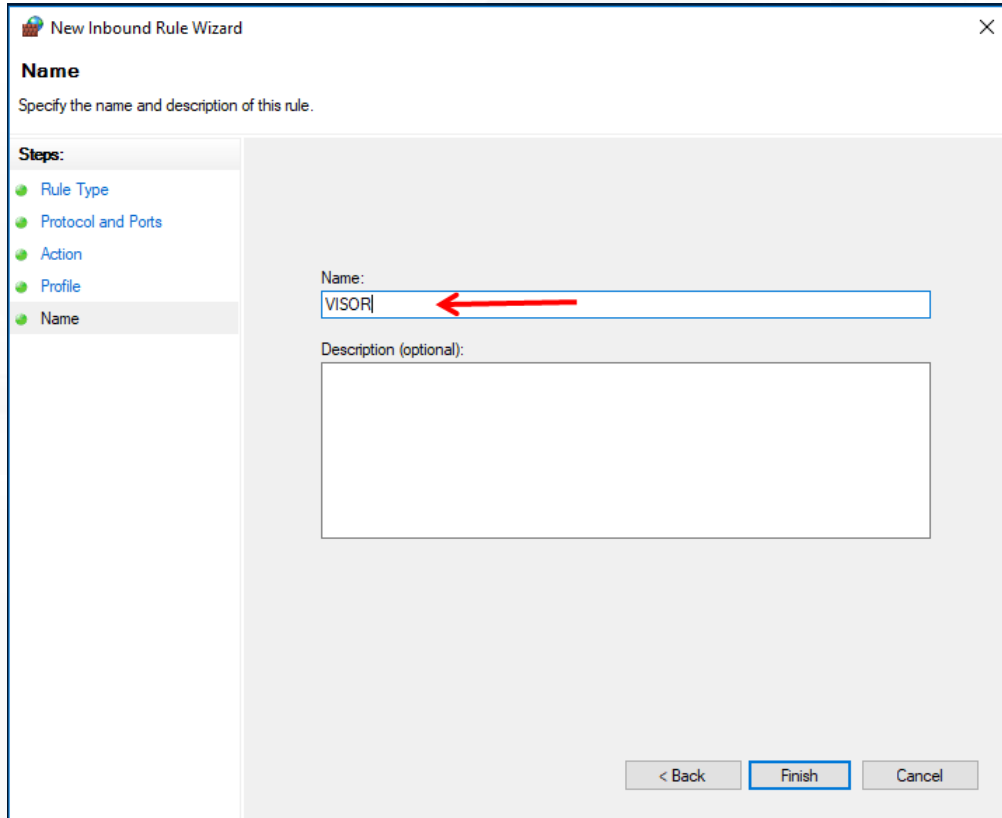
Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

< Back Next > Cancel

Enter the name of the rule, then click on Finish



New Inbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:

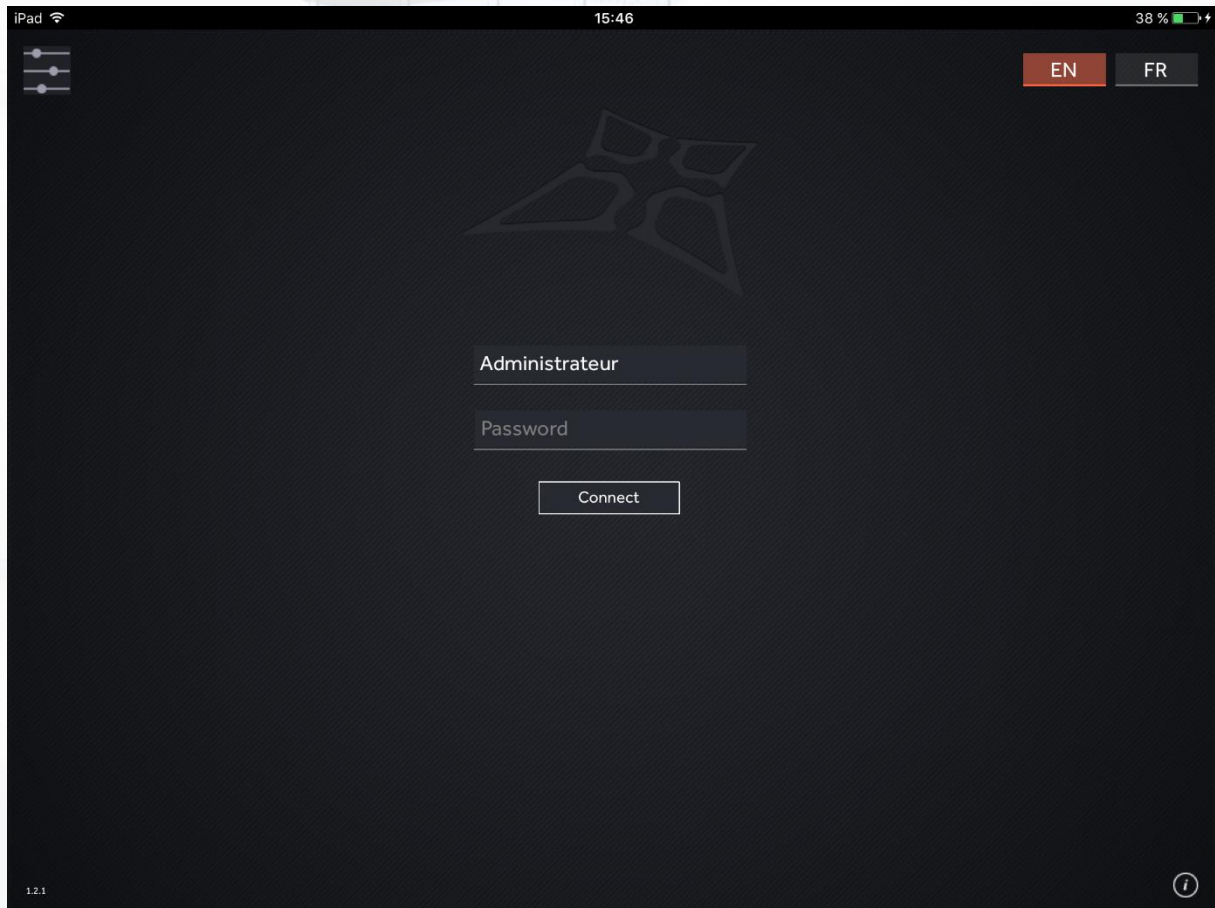
Description (optional):

< Back Finish Cancel






Firewall configuration has now been completed.

TO USE THE APPLICATION

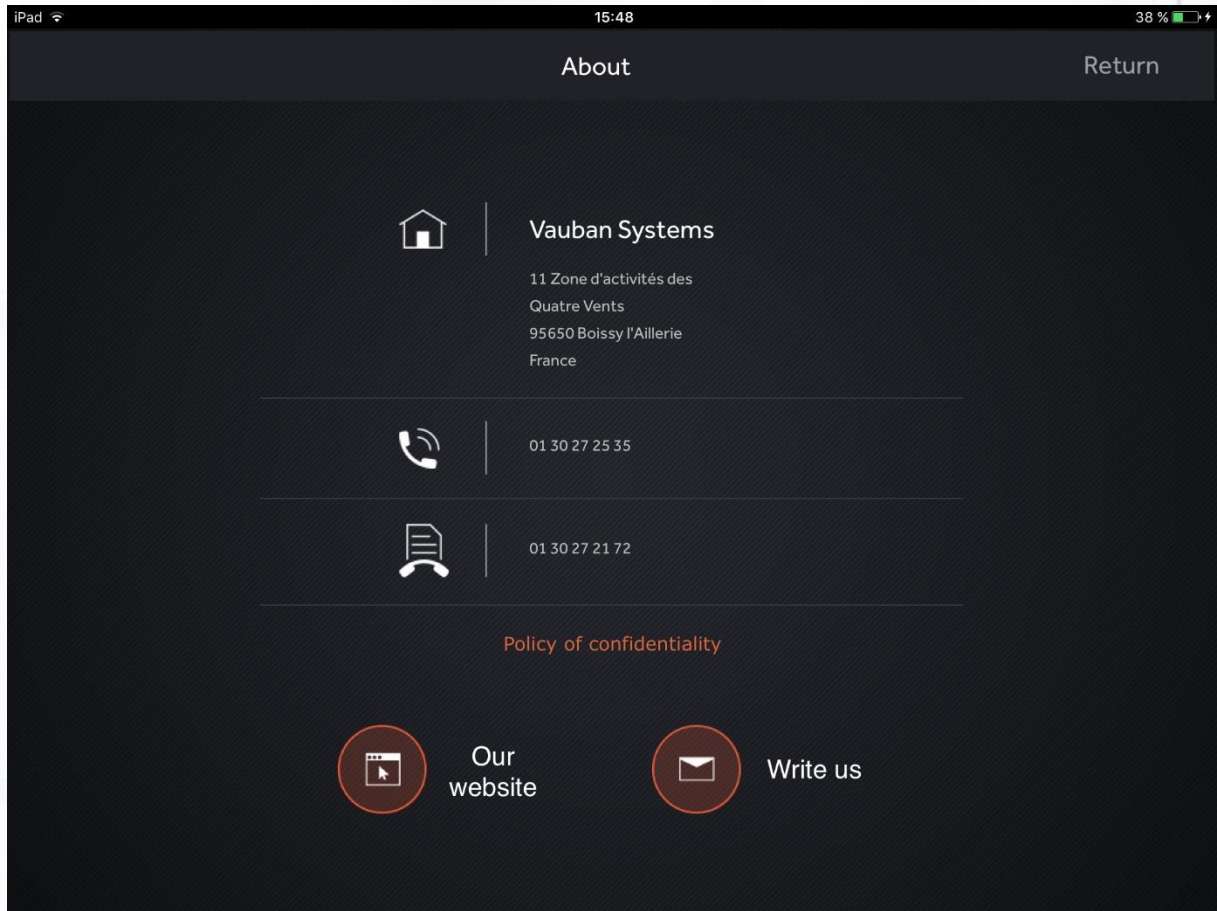
HOME SCREEN



From this window, you can:

- Access the settings window by clicking on the  icon.
- Access Vauban Systems information by clicking on the  icon.
- Log in by clicking on the  button.
- Change the application's language (French or English) thanks to the   buttons.

ABOUT US



Screen showing the company's information with the ability to go to Vauban's website and send an email to info@vauban-systems.fr.



SETTINGS

The screenshot shows the 'Setting' screen on an iPad. At the top, there is a 'Return' button. Below it is a faint logo. The main section is titled 'Setting' and contains five input fields: 'Internal IP address', 'Internal port', 'External IP address', 'External port', and 'Key'. Below these fields is a toggle for 'Enable Touch ID' with 'Oui' and 'Non' options. At the bottom, there are three buttons: 'Launch scan', 'Verify', and 'Validate'.

If your tablet is connected via WIFI to your company's network, simply enter the IP address of the PC on which VISOR is running in the Internal IP address field.

From the Settings menu, enter the PC's IP address starting with **http://** (for example: **http://192.168.1.1** where 192.168.1.1 is your PC's IP address). Then specify the IP port (8080 or the port you used in the previous steps) in the Internal port field.

Tip: Use a static IP address on your PC. Ask your network administrator for advice.

Note: VISOR will need to keep running in order for you to be able to use the application.

If your tablet is connected from outside your company's network, enter the public IP address of your Internet connection. To do so, create a NAT rule to translate to the IP address of the PC running VISOR on your router. We advise you to contact your network administrator.

Tip: Make sure that your PC uses a static IP address and that your Internet connection also has a static IP address.

From the Settings menu, enter the public IP address of your Internet connection in the External IP address field starting with **http://** (for example: **http://80.80.80.80** where 80.80.80.80 is the public IP address of your Internet connection). Then specify the IP port (8080 or the port you used in the previous steps) in the External port field.

Or, if you have VISOR nearby, you can begin scanning to be able to scan a QR Code generated from VISOR. It will automatically fill in all the connection settings.

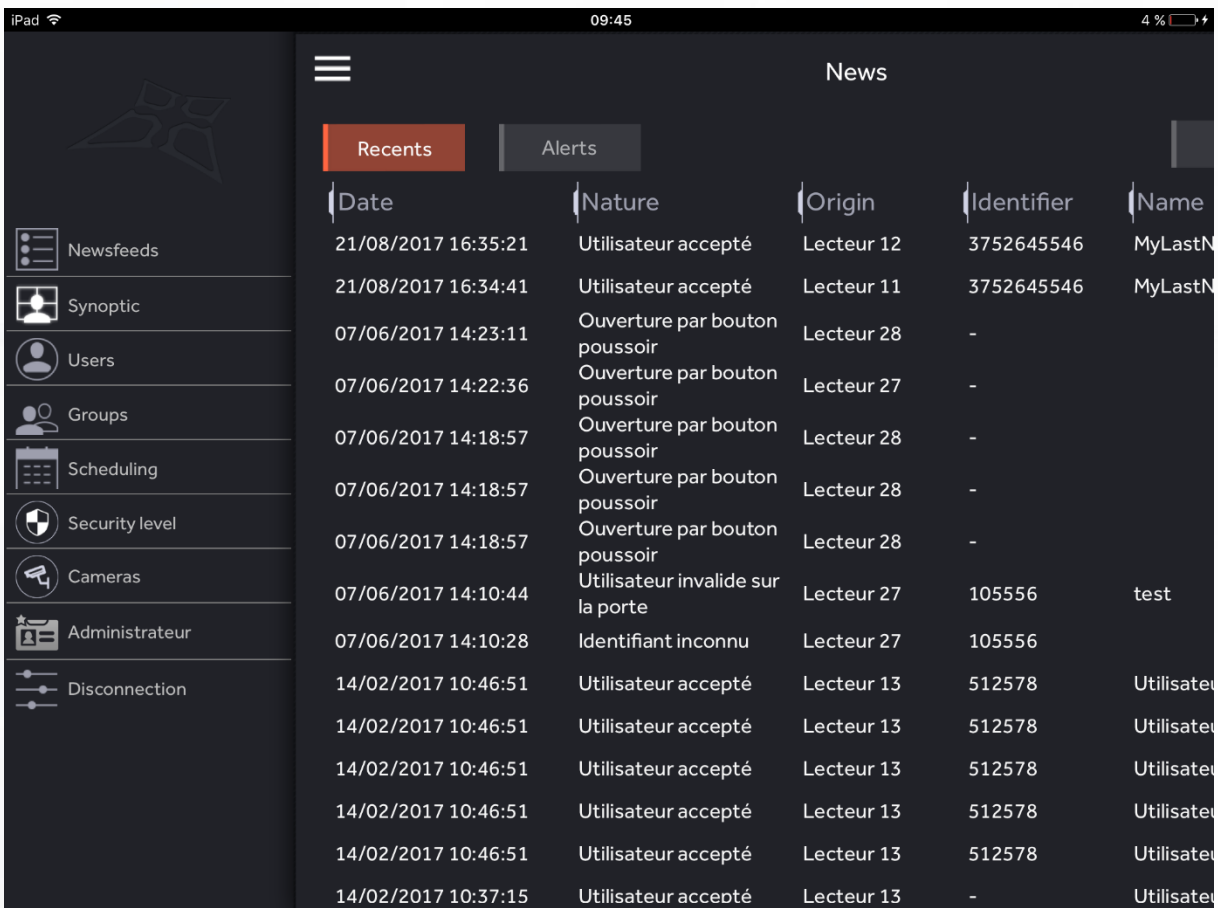
If you want to use the highest security mode, you will need a key.

You can obtain this key from VISOR. Enter it manually or scan the QR Code generated by VISOR.

If you are using an iPad with Touch ID, you can enable it. Enabling Touch ID will allow you to connect via your iPad's fingerprint sensor. When prompted, enter the VISOR login and password. To log in, from the login window, click on 'Se connecter' (Log in) and put your finger on the sensor.

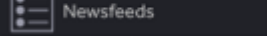
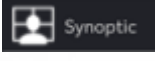
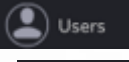
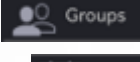
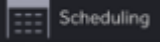
MAIN MENU

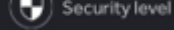
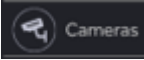

To access the main menu, click on the  icon located at the top left of the application. The following menu appears:



	Date	Nature	Origin	Identifier	Name
Newsfeeds	21/08/2017 16:35:21	Utilisateur accepté	Lecteur 12	3752645546	MyLastN
Synoptic	21/08/2017 16:34:41	Utilisateur accepté	Lecteur 11	3752645546	MyLastN
Users	07/06/2017 14:23:11	Ouverture par bouton poussoir	Lecteur 28	-	
Groups	07/06/2017 14:22:36	Ouverture par bouton poussoir	Lecteur 27	-	
Scheduling	07/06/2017 14:18:57	Ouverture par bouton poussoir	Lecteur 28	-	
Security level	07/06/2017 14:18:57	Ouverture par bouton poussoir	Lecteur 28	-	
Cameras	07/06/2017 14:10:44	Utilisateur invalide sur la porte	Lecteur 27	105556	test
Administrateur	07/06/2017 14:10:28	Identifiant inconnu	Lecteur 27	105556	
Disconnection	14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateu
	14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateu
	14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateu
	14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateu
	14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateu
	14/02/2017 10:37:15	Utilisateur accepté	Lecteur 13	-	Utilisateu

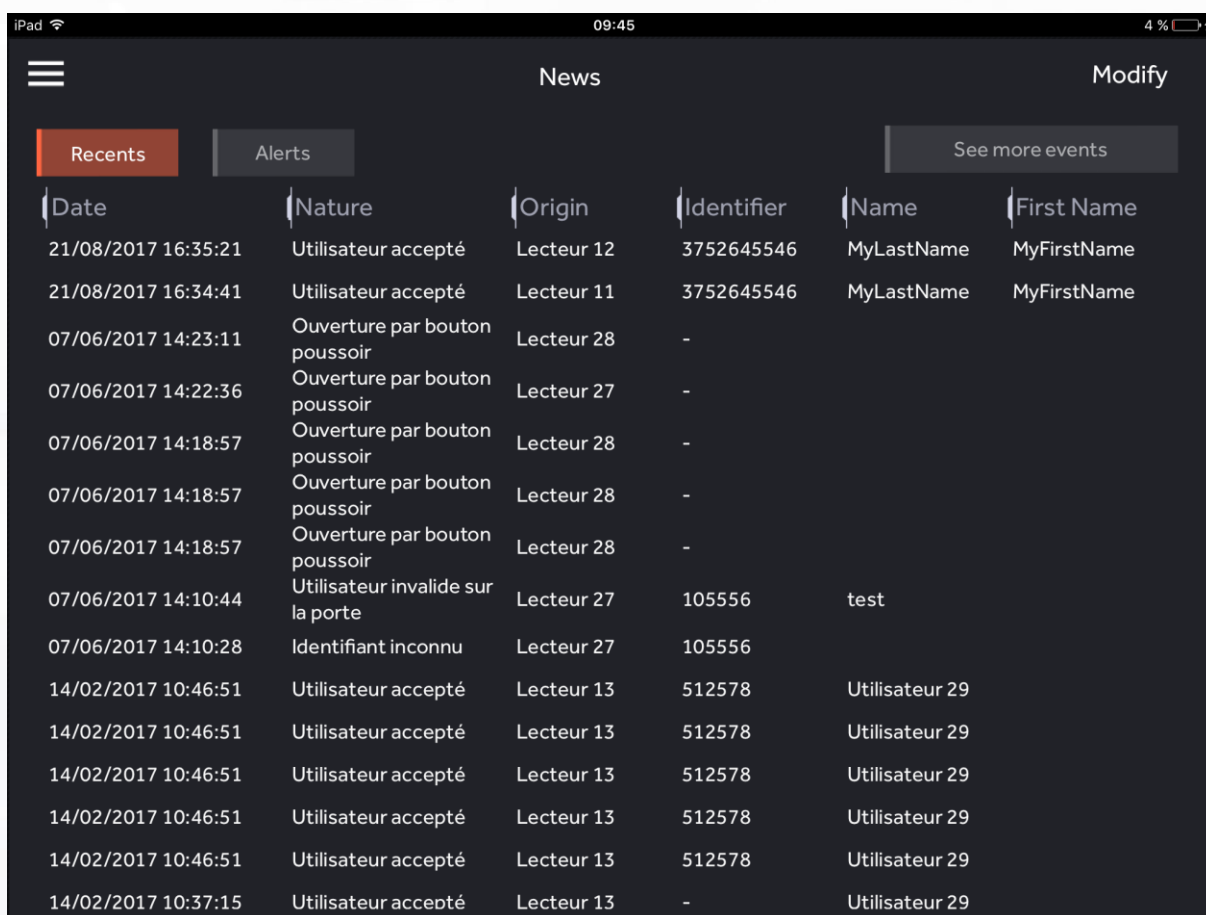
From this menu, you can:

- Access the event window by clicking on the  button
- Access the overview window by clicking on the  button
- Access the user window by clicking on the  button
- Access the group window by clicking on the  button
- Access the planning window by clicking on the  button

- Access the security level window by clicking on the button 
- Access the camera window by clicking on the button 
- Log out by clicking on the  button



Note: if you are using a higher version of VISOR than 2.0.0.16, some buttons may be hidden depending on the manager's permissions.


EVENTS

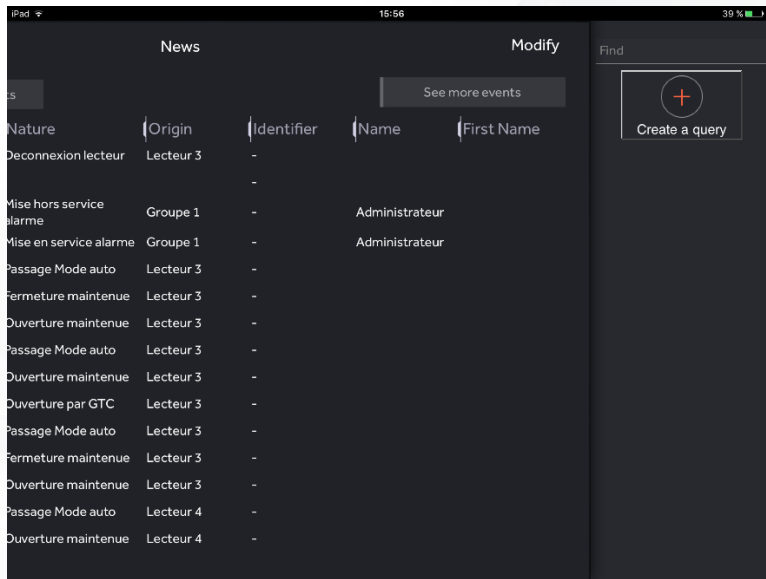


Date	Nature	Origin	Identifiant	Name	First Name
21/08/2017 16:35:21	Utilisateur accepté	Lecteur 12	3752645546	MyLastName	MyFirstName
21/08/2017 16:34:41	Utilisateur accepté	Lecteur 11	3752645546	MyLastName	MyFirstName
07/06/2017 14:23:11	Ouverture par bouton poussoir	Lecteur 28	-		
07/06/2017 14:22:36	Ouverture par bouton poussoir	Lecteur 27	-		
07/06/2017 14:18:57	Ouverture par bouton poussoir	Lecteur 28	-		
07/06/2017 14:18:57	Ouverture par bouton poussoir	Lecteur 28	-		
07/06/2017 14:18:57	Ouverture par bouton poussoir	Lecteur 28	-		
07/06/2017 14:10:44	Utilisateur invalide sur la porte	Lecteur 27	105556	test	
07/06/2017 14:10:28	Identifiant inconnu	Lecteur 27	105556		
14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateur 29	
14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateur 29	
14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateur 29	
14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateur 29	
14/02/2017 10:46:51	Utilisateur accepté	Lecteur 13	512578	Utilisateur 29	
14/02/2017 10:37:15	Utilisateur accepté	Lecteur 13	-	Utilisateur 29	

In this window, you can:

- Display alerts
- Display more events
- Access the main menu by clicking on the  button
- Edit the displayed information by clicking on the  button


Click on  to open the customised query menu:

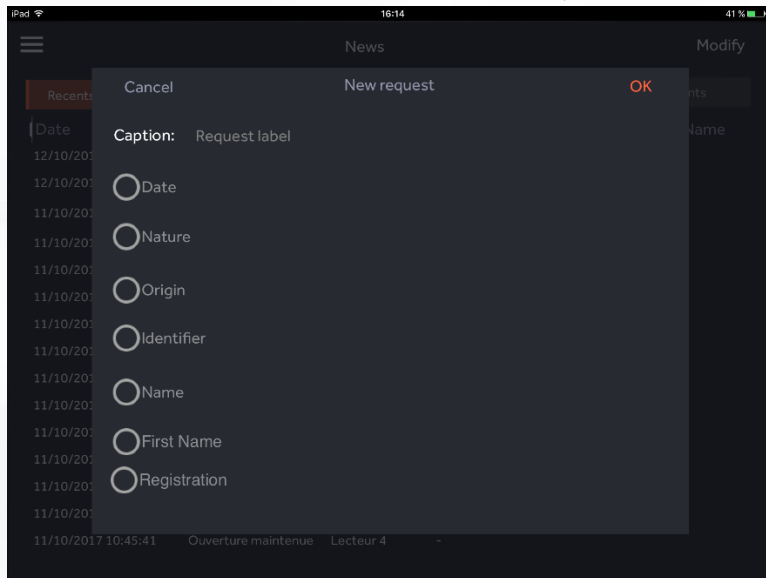


From this window, you can:

- View the list of queries
- Run a query
- Create a query



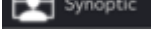
Click on the  button to create a query:

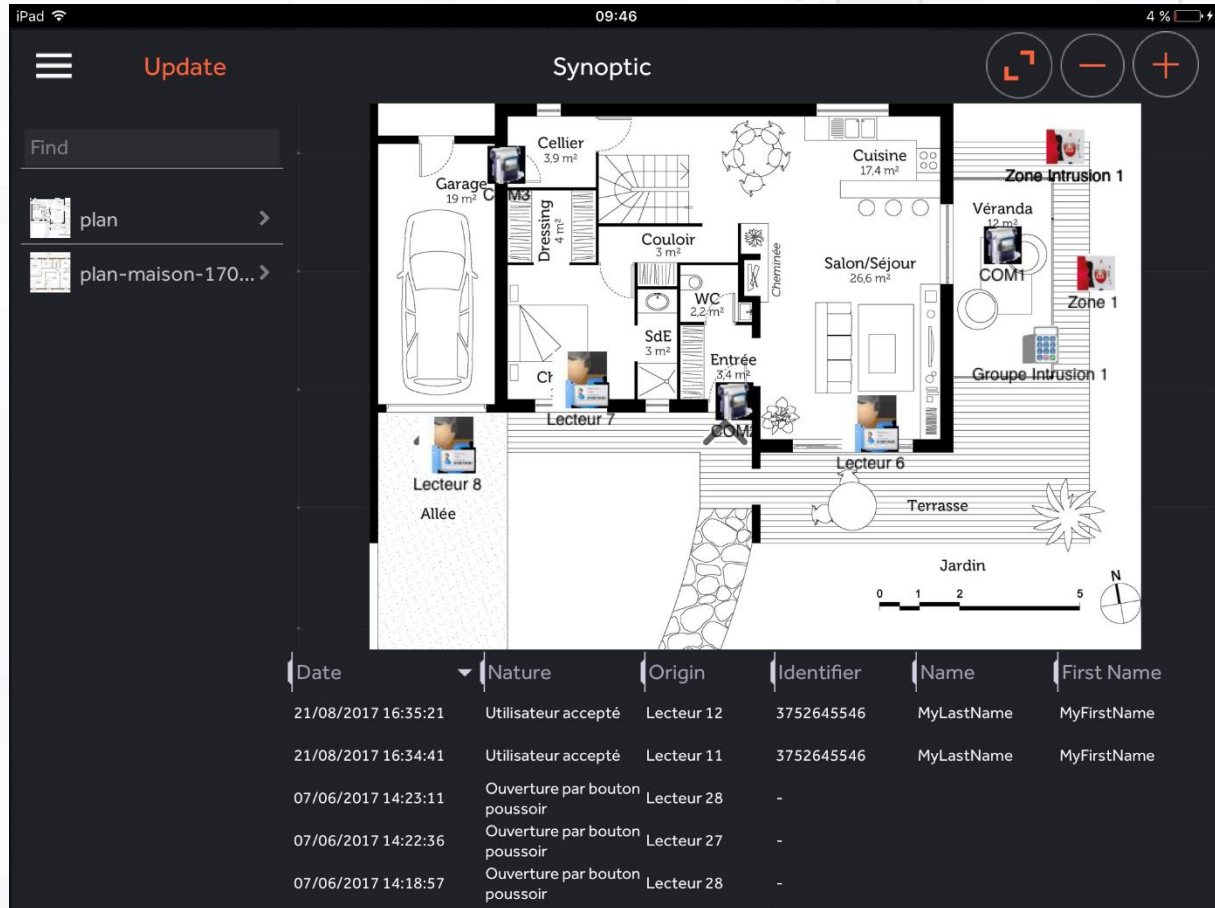


From this window, you can:

- Set the name of the query
- Define all of the query's settings

OVERVIEW

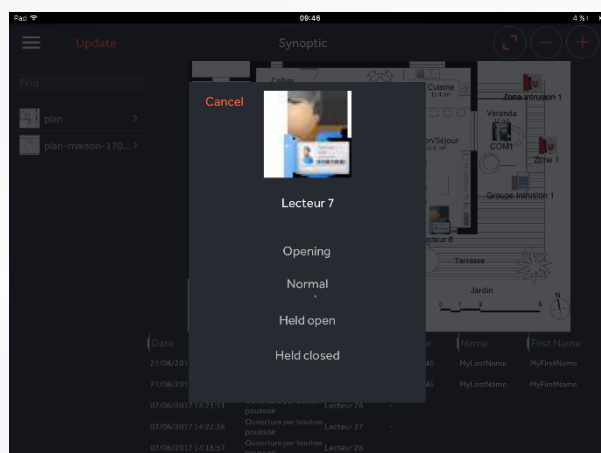
The overview window appears once you have clicked on the  button from the main menu.



Date	Nature	Origin	Identifiant	Name	First Name
21/08/2017 16:35:21	Utilisateur accepté	Lecteur 12	3752645546	MyLastName	MyFirstName
21/08/2017 16:34:41	Utilisateur accepté	Lecteur 11	3752645546	MyLastName	MyFirstName
07/06/2017 14:23:11	Ouverture par bouton poussoir	Lecteur 28	-		
07/06/2017 14:22:36	Ouverture par bouton poussoir	Lecteur 27	-		
07/06/2017 14:18:57	Ouverture par bouton poussoir	Lecteur 28	-		

From this window, you can:

- Display a floor plan from the list of floor plans
- Search for a floor plan in the list of floor plans
- Zoom in to the floor plan
- Zoom out of the floor plan
- Display the floor plan in full-screen mode
- View recent events

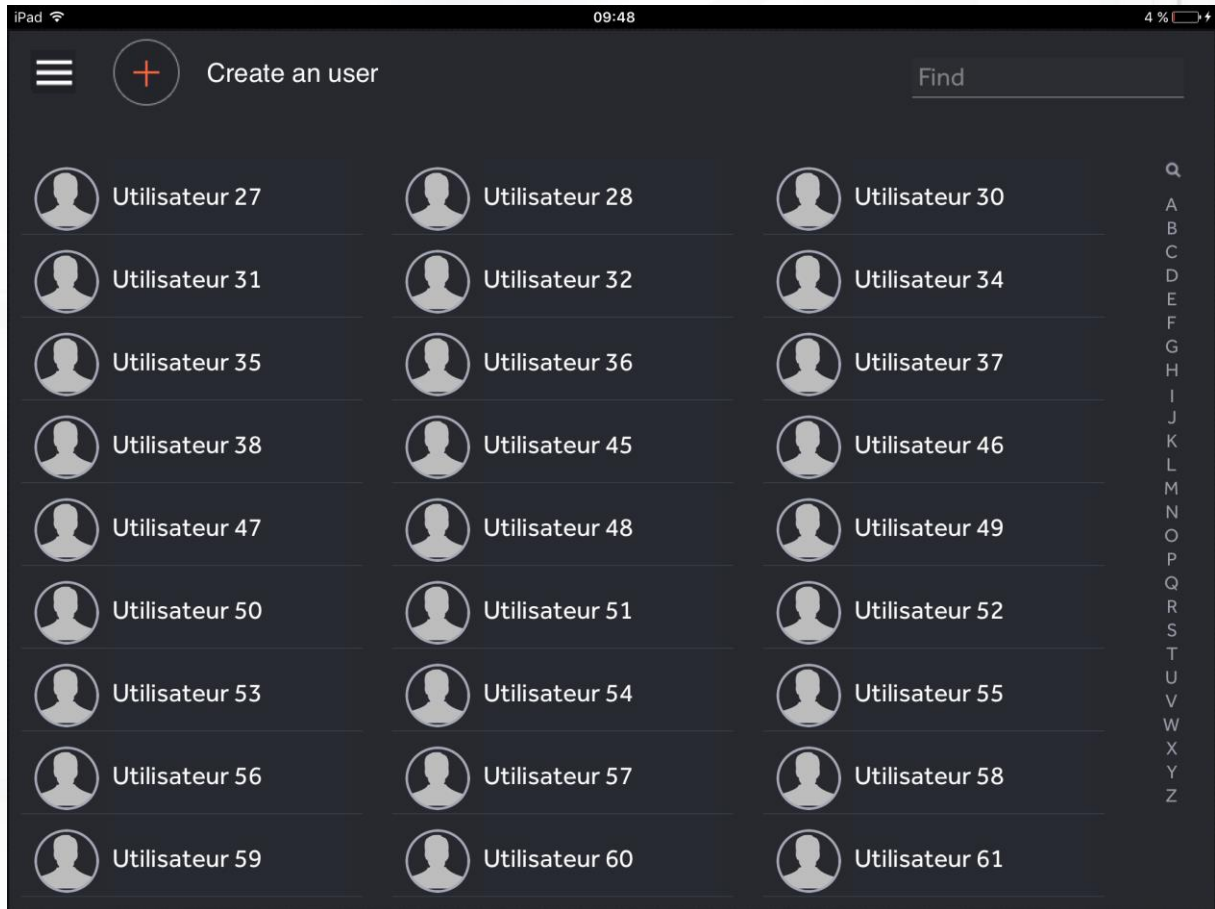


Click on a reader on the floor plan to control it. The following window appears:

From this window, you can:

- Control the selected reader

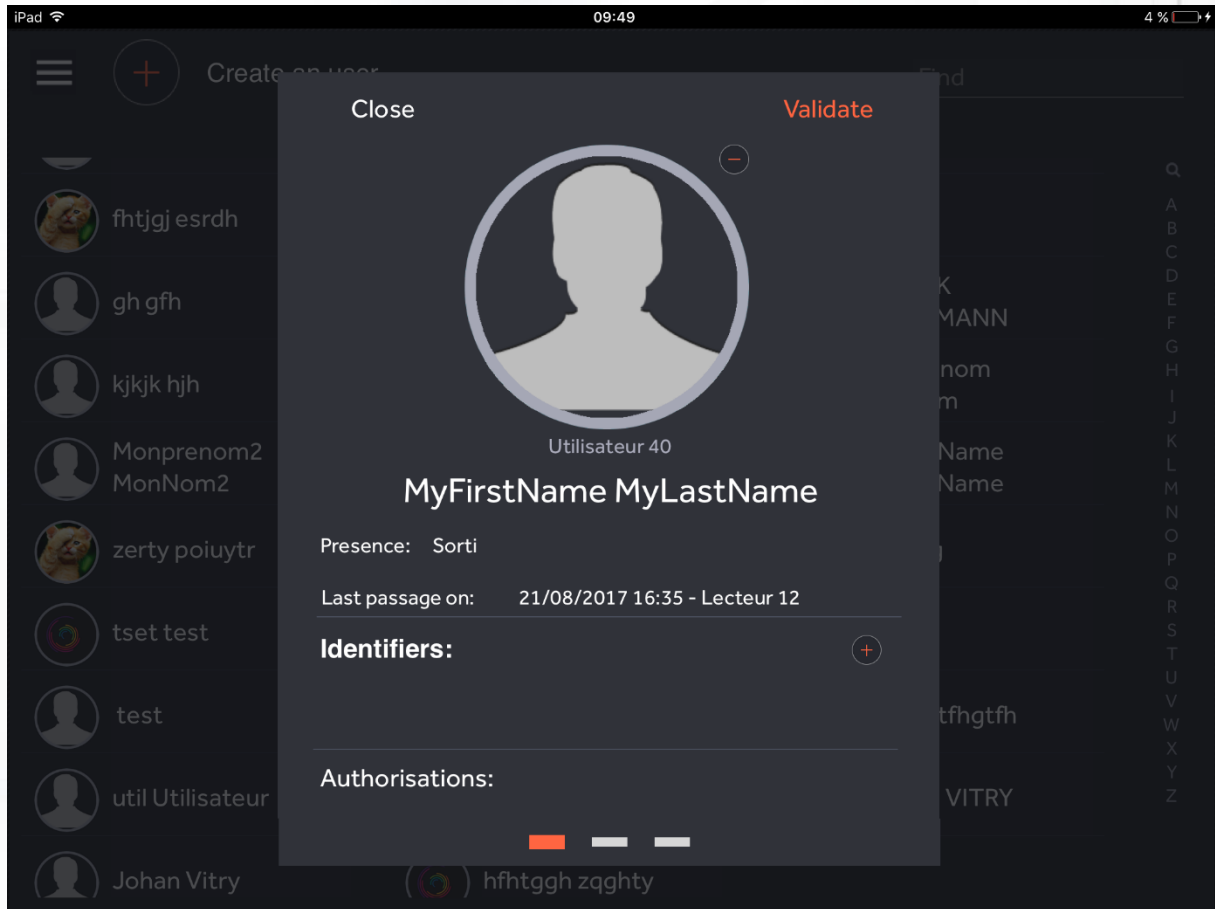
USERS



From this window, you can:

- Search for a user
- Display a user's record
- Add a new user
- Display the main menu
- Edit a user
- Delete a user

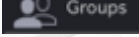
USER RECORD

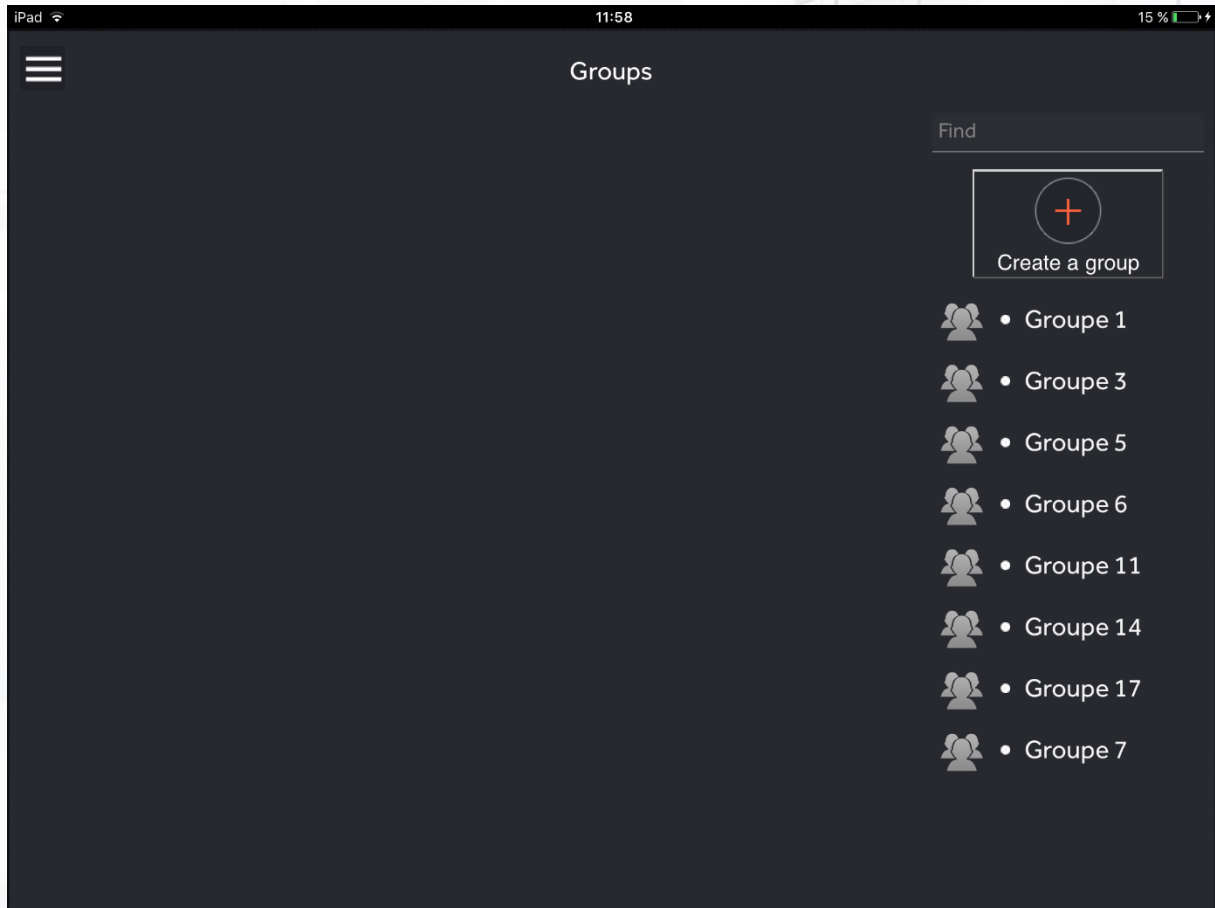


From this window, you can:

- Change the user's photo
- Edit the user's last name
- Edit the user's first name
- Allow or prohibit the user
- Assign a time period to the user
- Assign up to 3 groups to the user
- Enable validity dates
- Assign user names
- Assign registration numbers (if the LPR module is active)

GROUPS

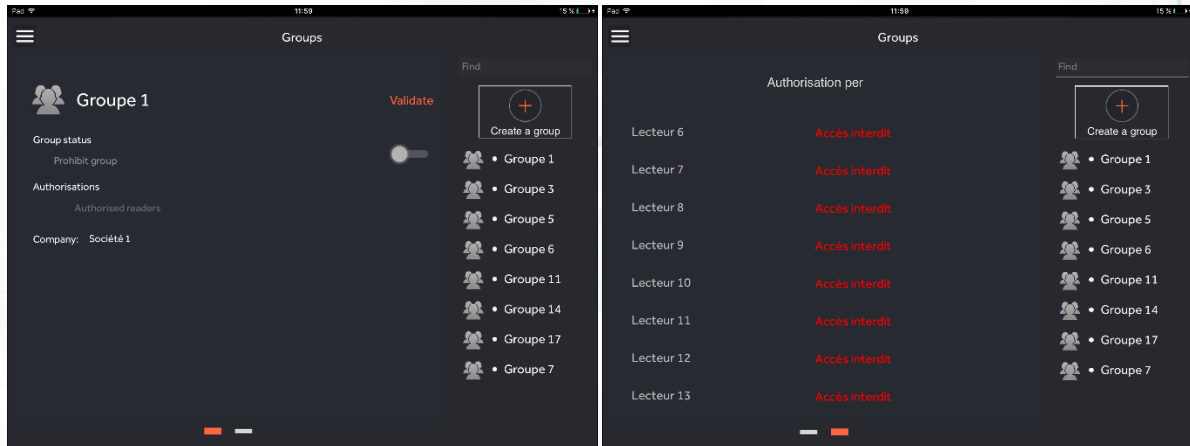
The group management window appears once you have clicked on the  button from the main menu.



From this window, you can:

- Search for a group
- Create a group
- Delete a group
- Edit a group
- Display a group


GROUP RECORD

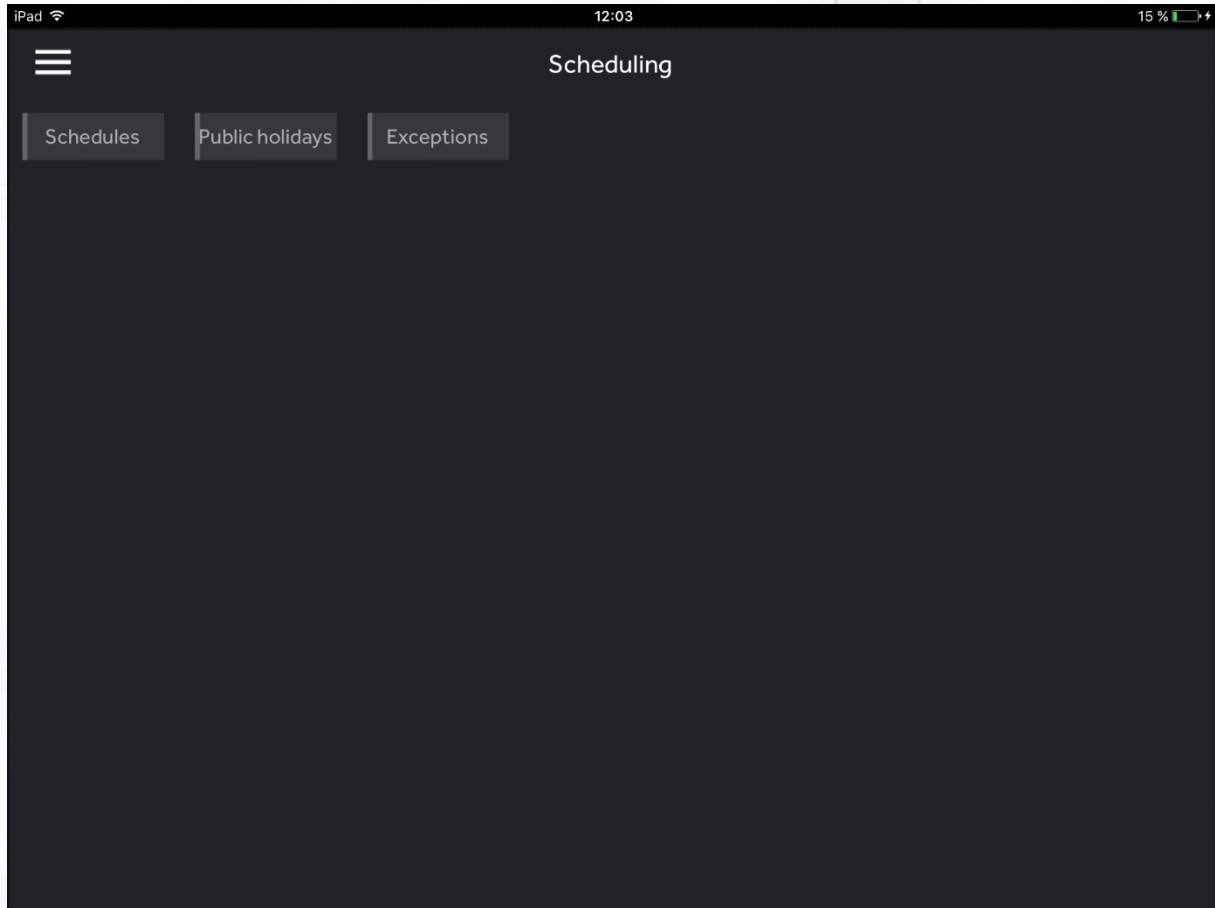


From this record, you can:

- Edit the group's name
- Prohibit the group
- Allow readers
- Assign a company

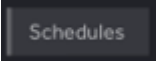
PLANNING

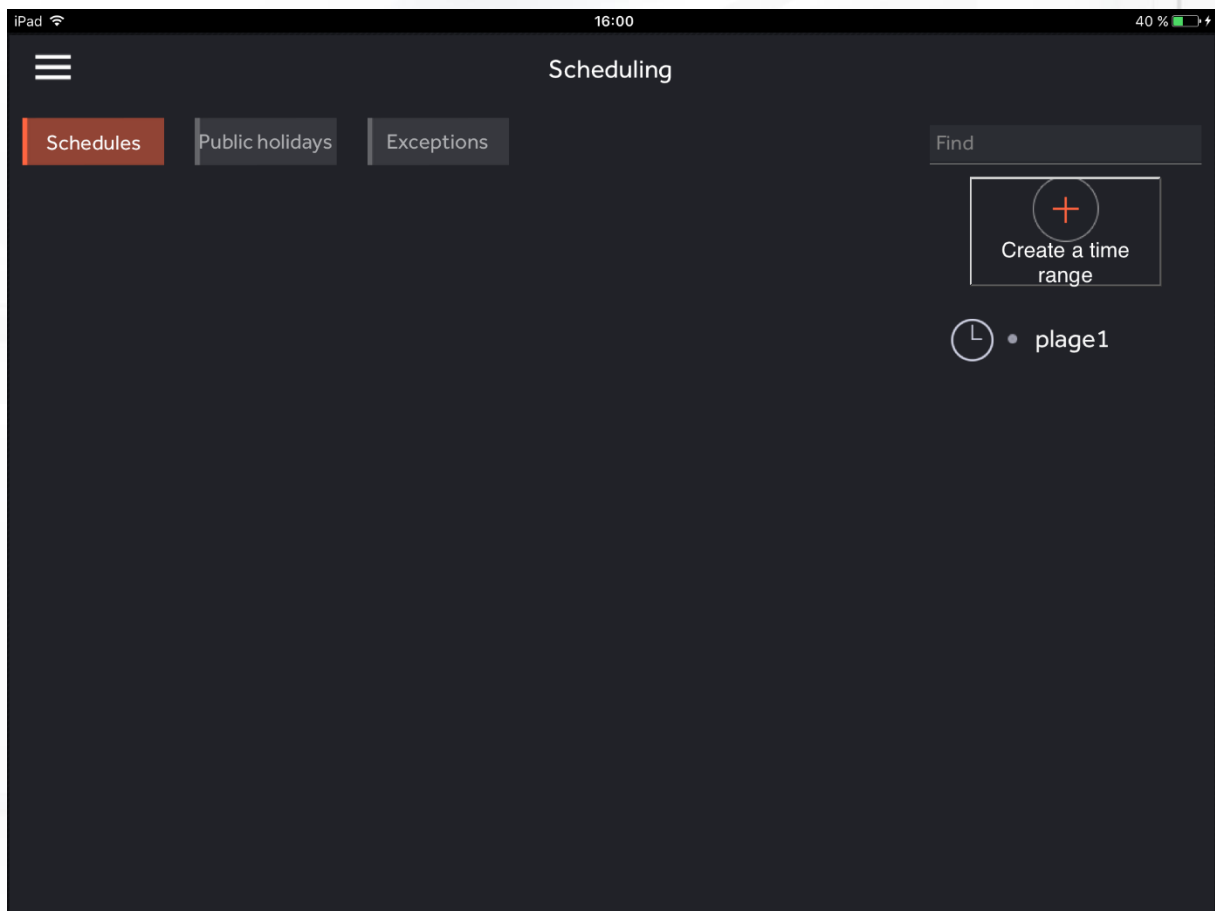
The planning window appears once you have clicked on the  Scheduling button from the main menu.



From this window, you can:

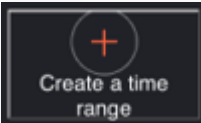
- Display time periods
- Display holidays
- Display exceptions

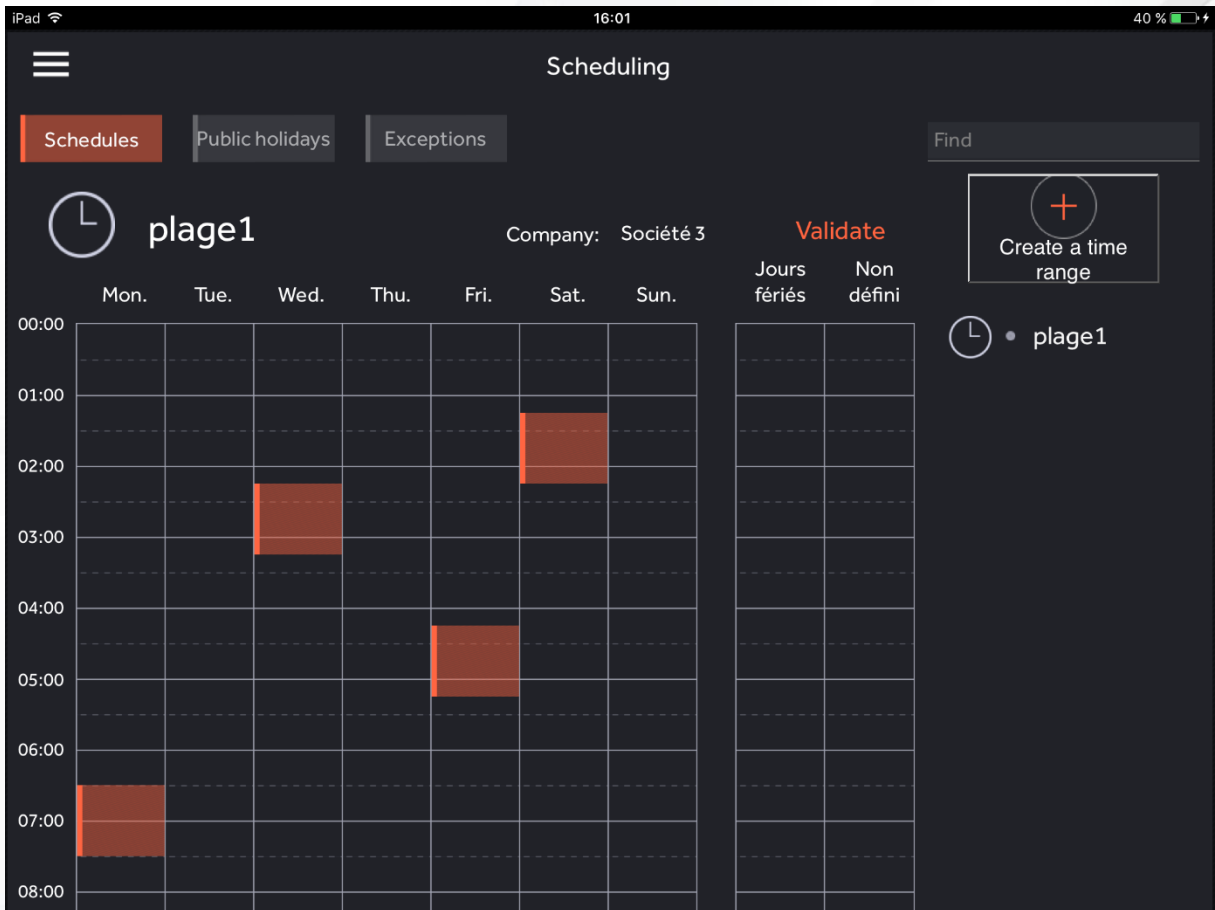
Click on  to display time period management. The following window appears:



From this window, you can:

- Create a time period
- Search for a time period in the list of time periods
- Display holiday management
- Display exception management

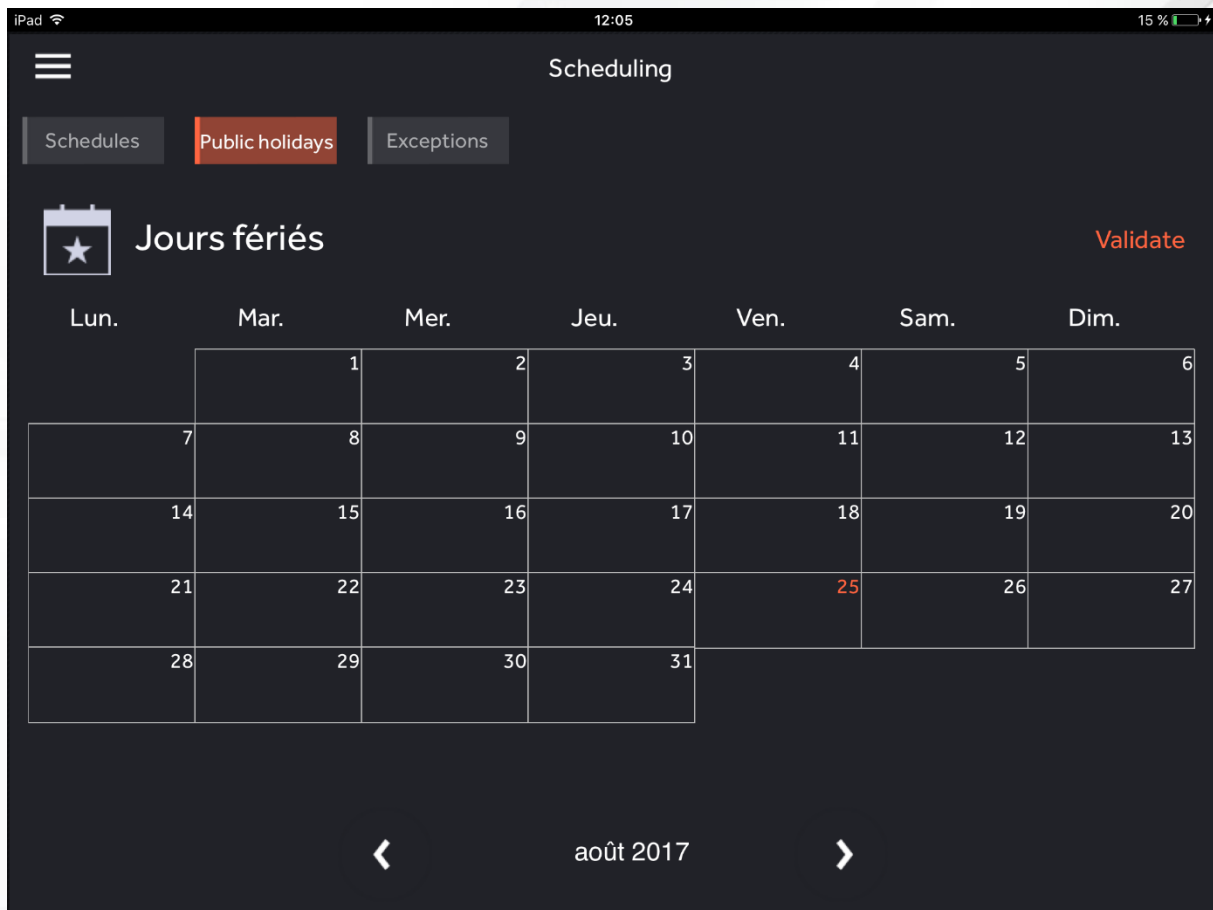
Click on  to create a time period. The following window appears:



From this window, you can:

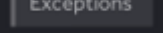
- Set a name for the time period
- Add various slots for each day
- Assign a company to the time period
- Delete a time period

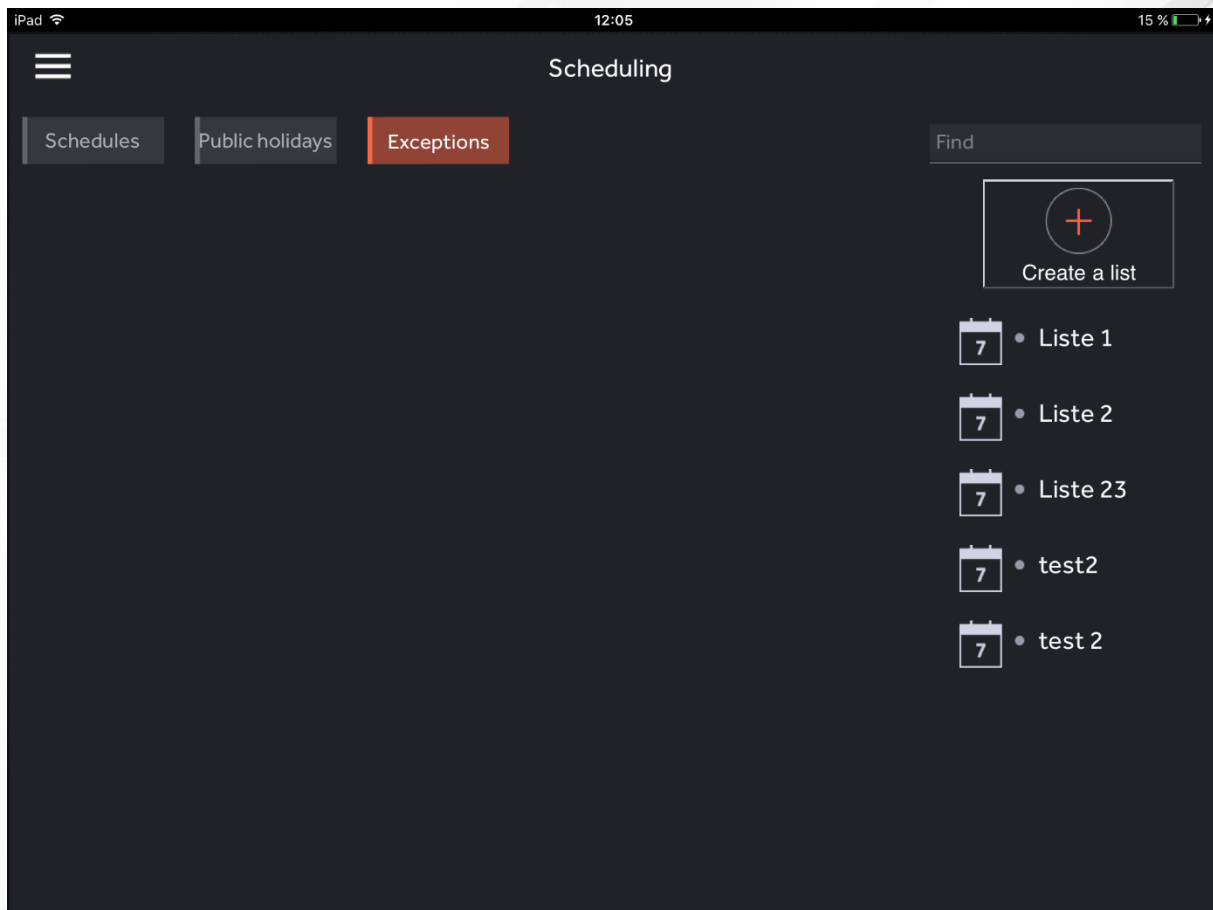
Click on **Public holidays** to display holiday management. The following window appears:



From this window, you can:

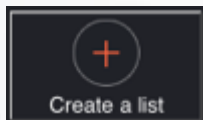
- Define holidays by selecting a day

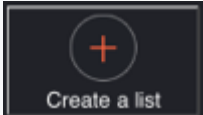
Click on  to display exception management. The following window appears:



From this window, you can:

- Create an exception list
- Search for a list in the list of exception lists
- Display time period management
- Display holiday management



Click on  to create an exception list. The following window appears:

iPad 12:05 15%

Scheduling

Schedules Public holidays Exceptions

Find

Liste 1 Company: Société 2 Validate

+ Create a list

Lun.	Mar.	Mer.	Jeu.	Ven.	Sam.	Dim.
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

7 • Liste 1

7 • Liste 2

7 • Liste 23

7 • test2

7 • test 2

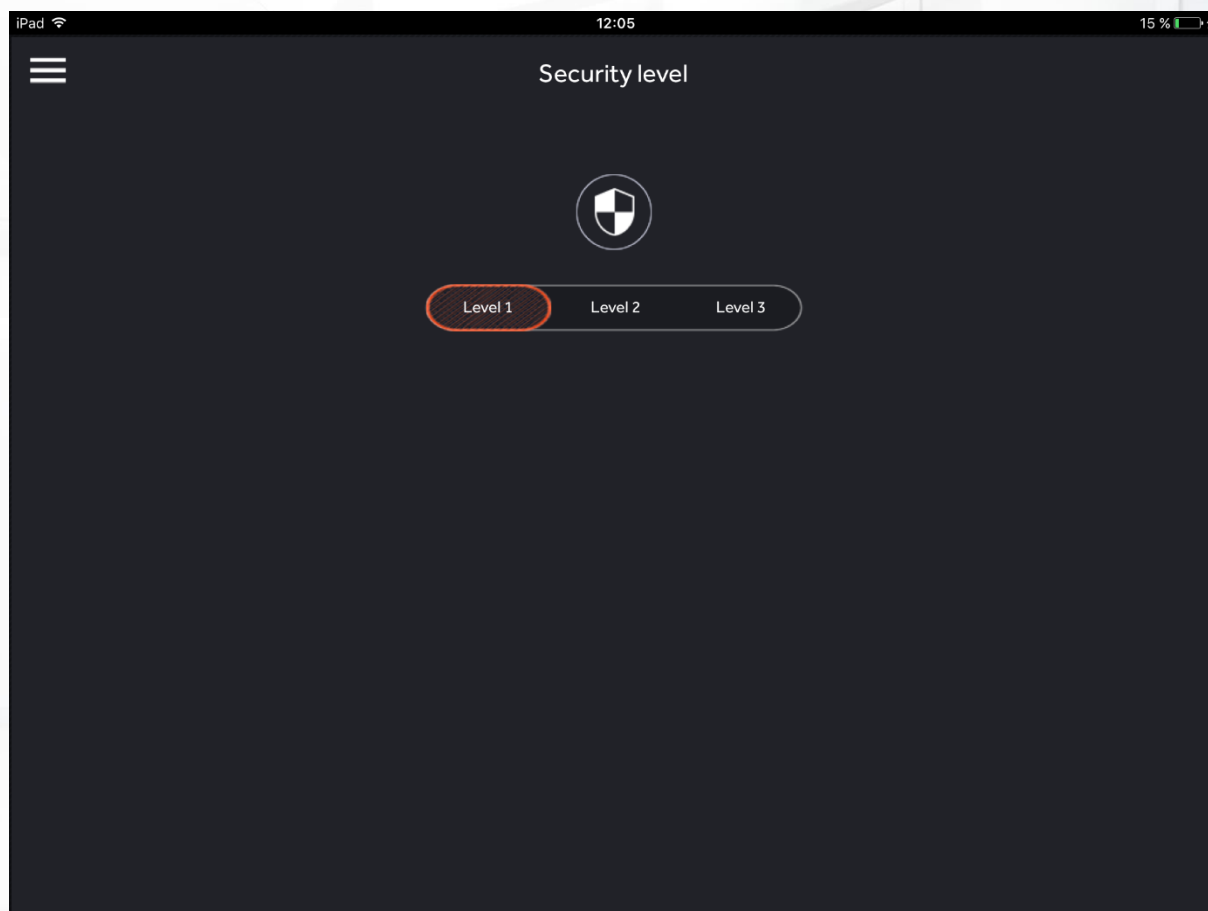
< août 2017 >

From this window, you can:

- Set a name for the exception list
- Add exceptions by selecting a day
- Assign a company to the exception list
- Delete an exception list



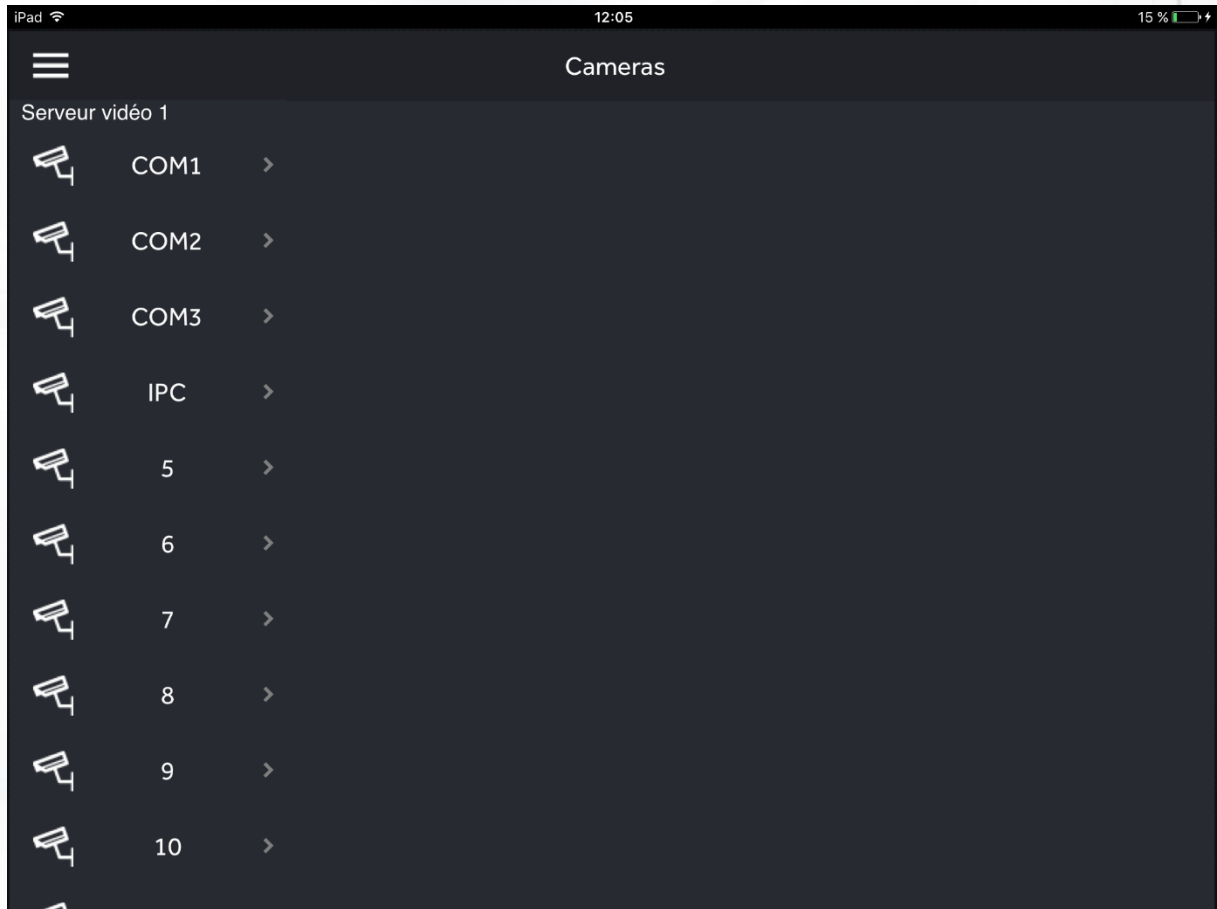
SECURITY LEVEL



From this window, you can:

- Change the installation's security level
- Display the main menu

CAMERAS



From this window, you can:

- Display a camera
- Display the main menu