KREO HMI TUTORIAL
User management (matrix and geographic mode)

Tutorial dedicated to the implementation of the user management based on matrix and geographic mode

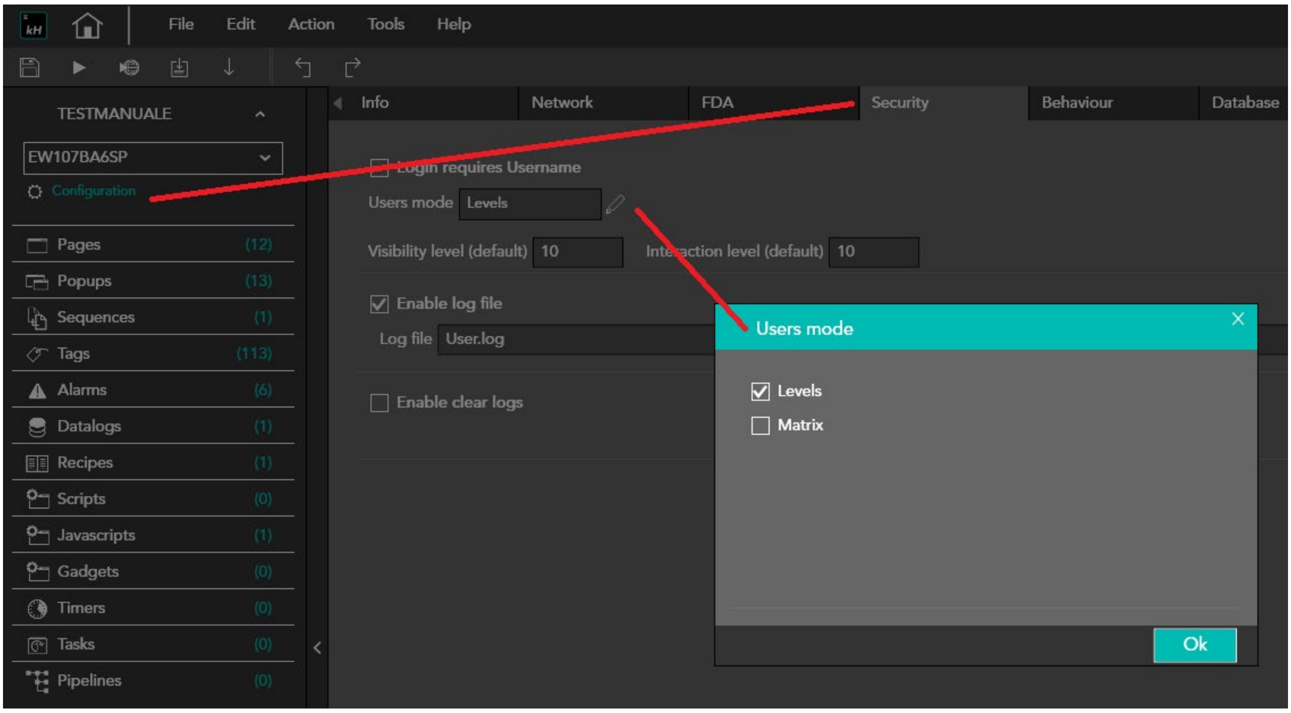
Connect
Ideas.
Shape
solutions.

introduction

In KREO HMI projects you can set different levels of security in order to filter the accessibility to the different pages and object functions.

The user management can be programmed in two different modes:

- Levels
- matrix



□ Login requires Username

Users mode: Levels

Visibility level (default): 10

Interaction level (default): 10

☑ Enable log file

Log file: User.log

□ Enable clear logs

Users mode

☑ Levels

□ Matrix

How to do:

In the MATRIX mode the traditional concept of LEVELS is replaced by GEOGRAPHIC credentials and GROUPS credentials.
The interaction between these 2 credentials filters the access to the project objects:

R: Read-Only
(the logged-in user can view the protected objects without interacting with them)

W: Write
(the logged-in user can view and interact with protected objects)

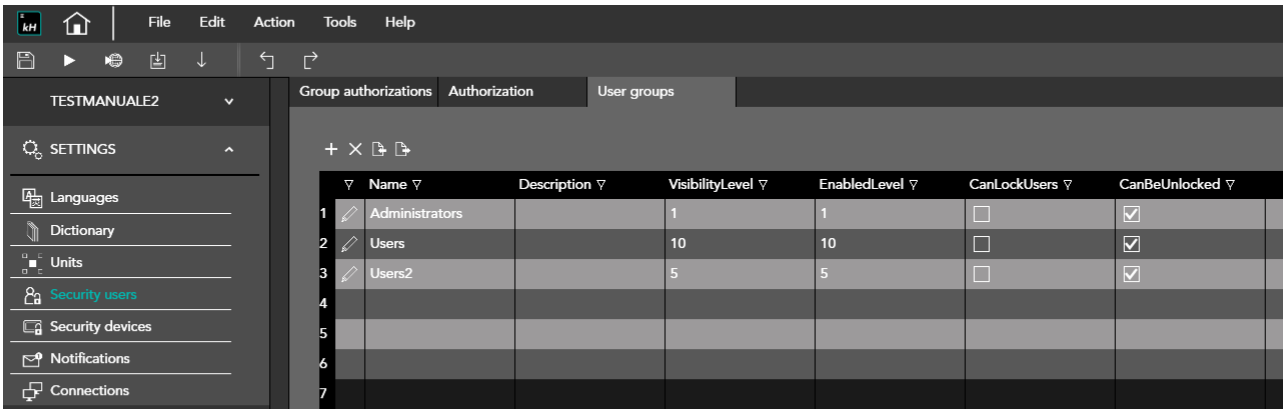
H: Hidden
(the logged-in user cannot view the protected objects)

S: Superuser
(such user can see all the project objects and interact with them)

The combination of GROUP and GEOGRAPHICAL credentials will define one of the four access modes (the most stringent is the predominant one).

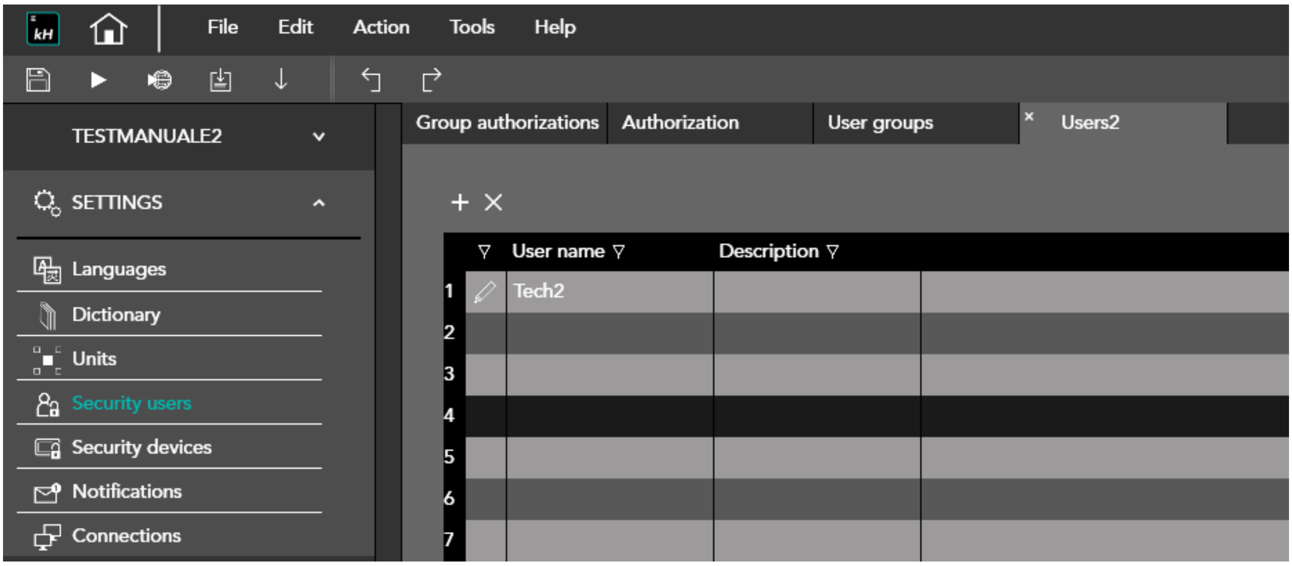
Let's see one of the many ways to use matrix user management.

1) We define the project GROUPS



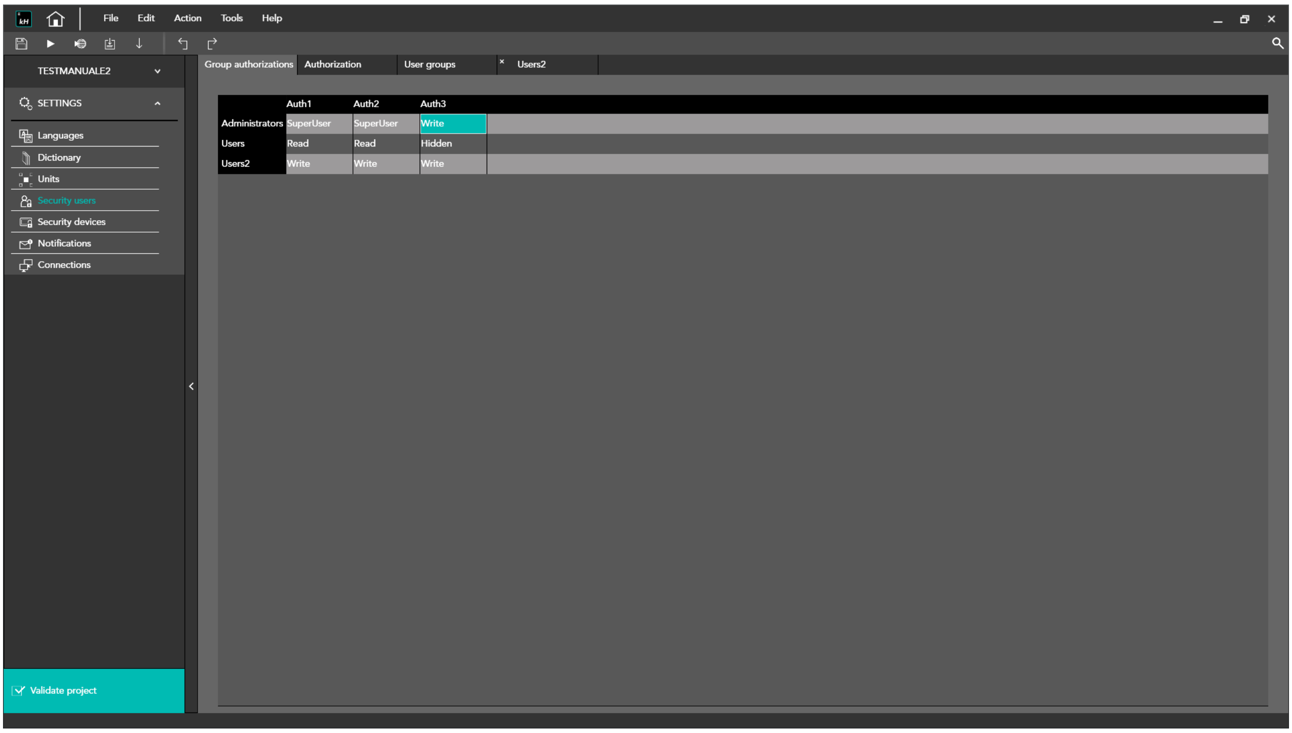
	Name	Description	VisibilityLevel	EnabledLevel	CanLockUsers	CanBeUnlocked
1	Administrators		1	1	□	☑
2	Users		10	10	□	☑
3	Users2		5	5	□	☑
4						
5						
6						
7						

2) Each group will have its own USERS with classic login + password access



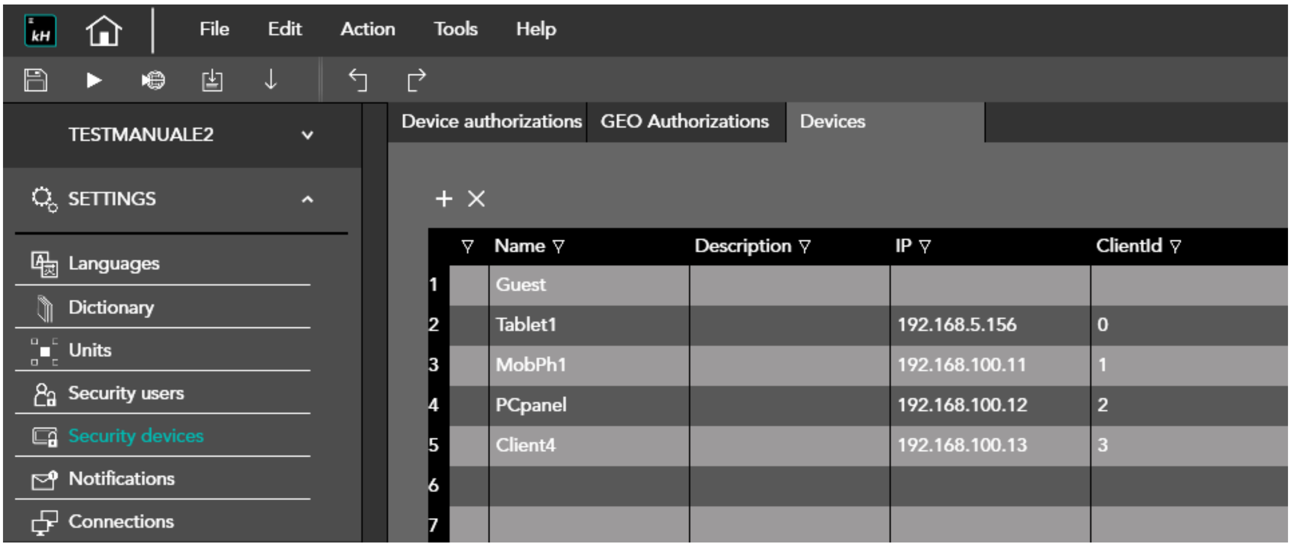
	User name	Description
1	Tech2	
2		
3		
4		
5		
6		
7		

3) The GROUP permissions are configured to EDITOR but can then be changed at RUNTIME via the specific runtime objects.



	Auth1	Auth2	Auth3
Administrators	SuperUser	SuperUser	Write
Users	Read	Read	Hidden
Users2	Write	Write	Write

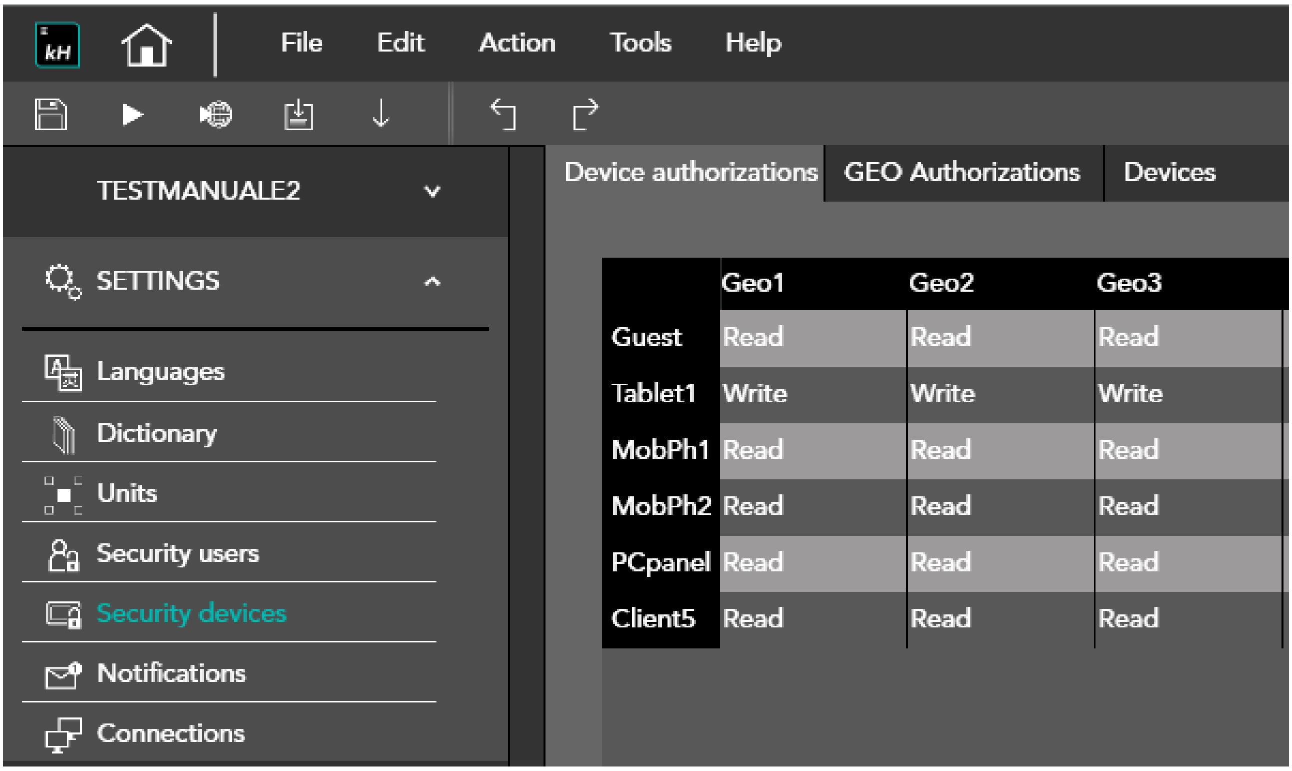
4) Now configure the GEOGRAPHIC credentials through the IP addresses provided for the client devices.
   The log-in via a specific device (having a predefined Ip address) defines the accessing credentials of type S,W,R,H.



	Name	Description	IP	ClientId
1	Guest			
2	Tablet1		192.168.5.156	0
3	MobPh1		192.168.100.11	1
4	PCpanel		192.168.100.12	2
5	Client4		192.168.100.13	3
6				
7				

NOTE: The GUEST is a CLIENT (tablet/mobile/pc) having an Ip address not predefined in the KREO HMI project.
In this case the user will always have GUEST credentials

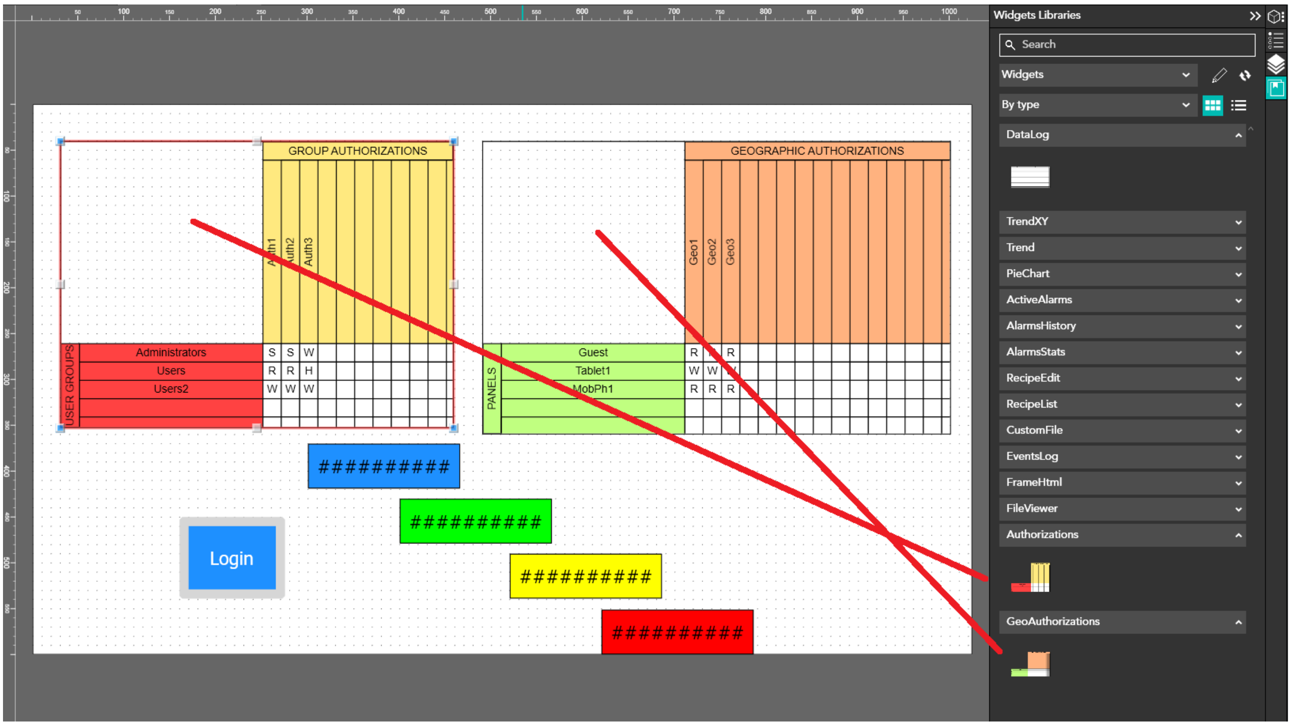
5) The same definition is necessary for the geographic credentials.



	Geo1	Geo2	Geo3
Guest	Read	Read	Read
Tablet1	Write	Write	Write
MobPh1	Read	Read	Read
MobPh2	Read	Read	Read
PCpanel	Read	Read	Read
Client5	Read	Read	Read

6) On the project pages you can now define the runtime objects necessary to manage the GROUP+GEOGRAPHIC protections.

If necessary, the GROUPS + GEOGRAPHIC grids will let the user modify the credentials at RUNTIME mode.



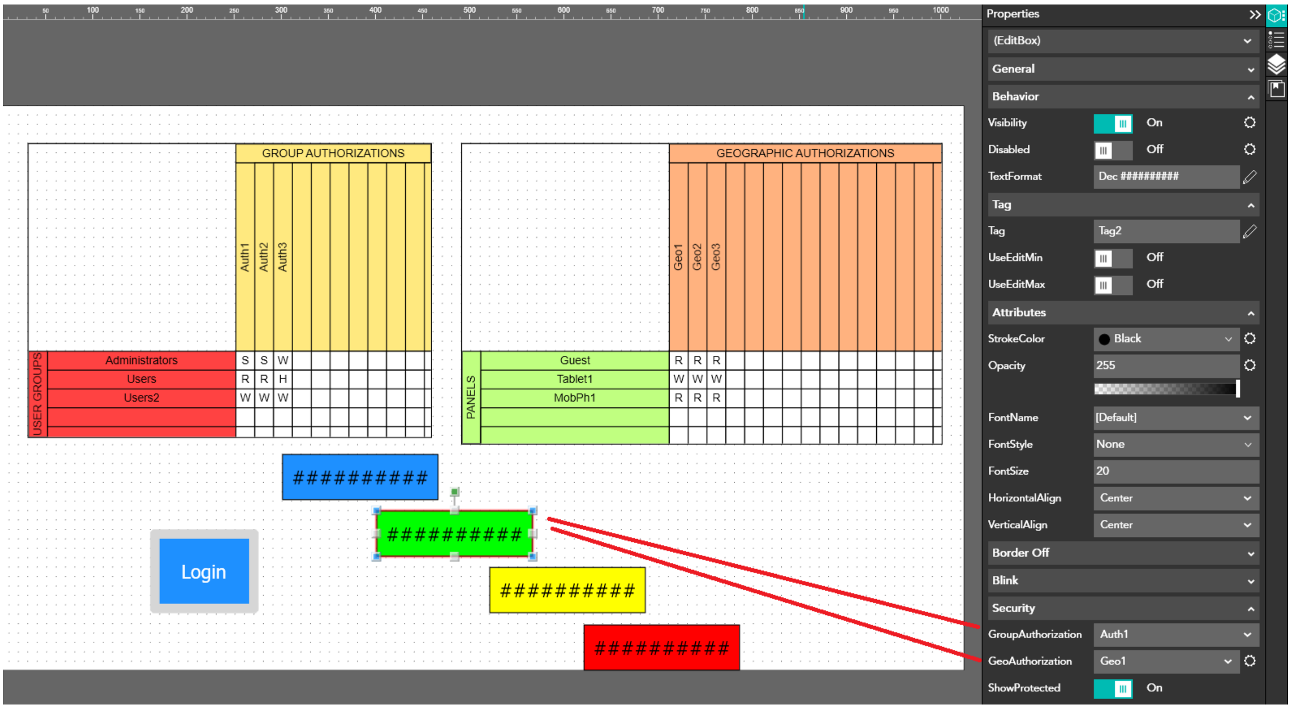
GROUP AUTHORIZATIONS

USER GROUPS	Auth1	Auth2	Auth3
Administrators	S	S	W
Users	R	R	H
Users2	W	W	W

GEOGRAPHIC AUTHORIZATIONS

PANELS	Geo1	Geo2	Geo3
Guest	R	[illegible]	R
Tablet1	W	W	W
MobPh1	R	R	R

7) Page objects security level is based on the combination of GROUPS+GEOGRAPHIC credentials

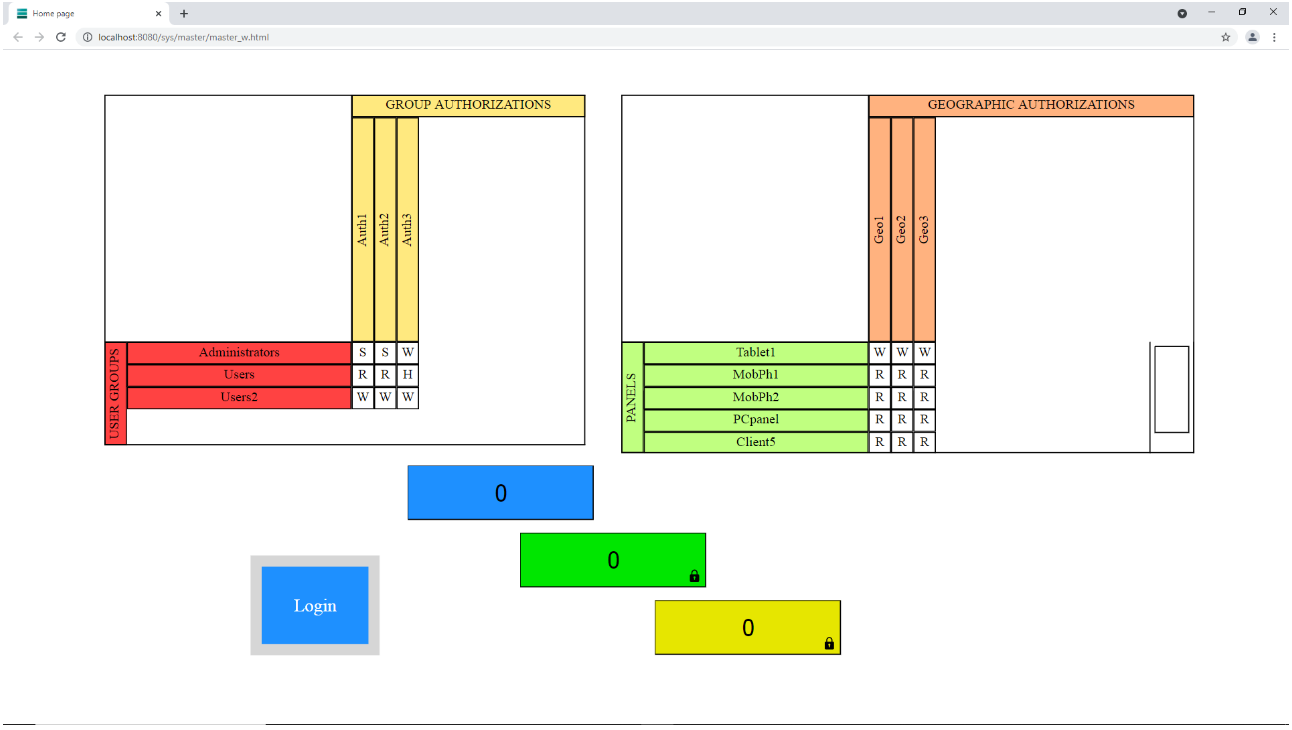


USER GROUPS	GROUP AUTHORIZATIONS		
	Auth1	Auth2	Auth3
Administrators	S	S	W
Users	R	R	H
Users2	W	W	W

PANELS	GEOGRAPHIC AUTHORIZATIONS		
	Geo1	Geo2	Geo3
Guest	R	R	R
Tablet1	W	W	W
MobPh1	R	R	R

Properties
(EditBox)
General
Behavior
Visibility: On
Disabled: Off
TextFormat: Dec ##########
Tag
Tag: Tag2
UseEditMin: Off
UseEditMax: Off
Attributes
StrokeColor: ● Black
Opacity: 255
FontName: [Default]
FontStyle: None
FontSize: 20
HorizontalAlign: Center
VerticalAlign: Center
Border Off
Blink
Security
GroupAuthorization: Auth1
GeoAuthorization: Geo1
ShowProtected: On

8) When the RUNTIME starts, before login, all objects except those with HIDDEN credentials will be displayed.
Protected objects are identified by a lock symbol



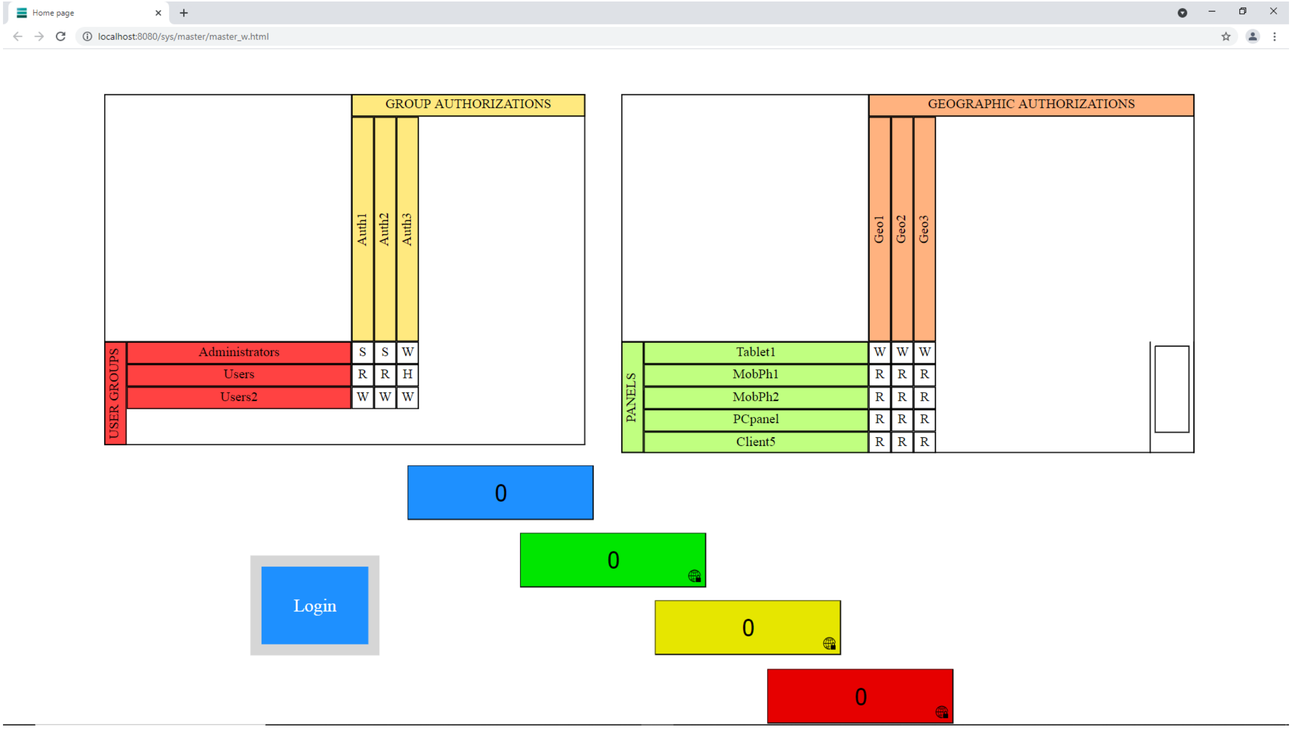
GROUP AUTHORIZATIONS

USER GROUPS		Auth1	Auth2	Auth3
	Administrators	S	S	W
	Users	R	R	H
	Users2	W	W	W

GEOGRAPHIC AUTHORIZATIONS

PANELS		Geo1	Geo2	Geo3
	Tablet1	W	W	W
	MobPh1	R	R	R
	MobPh2	R	R	R
	PCpanel	R	R	R
	Client5	R	R	R

9) After a GROUP LOGIN the red box can be accessed (LOCK icon has been unlocked) but still the georgraphic authorization is protecting the object (see the different locked icon – GEOGRAPHIC AUTHORIZATION LOCK).

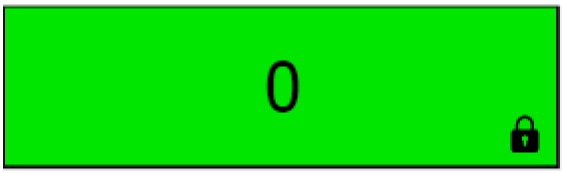


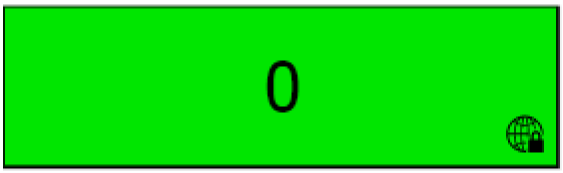
GROUP AUTHORIZATIONS

USER GROUPS		Auth1	Auth2	Auth3
	Administrators	S	S	W
	Users	R	R	H
	Users2	W	W	W

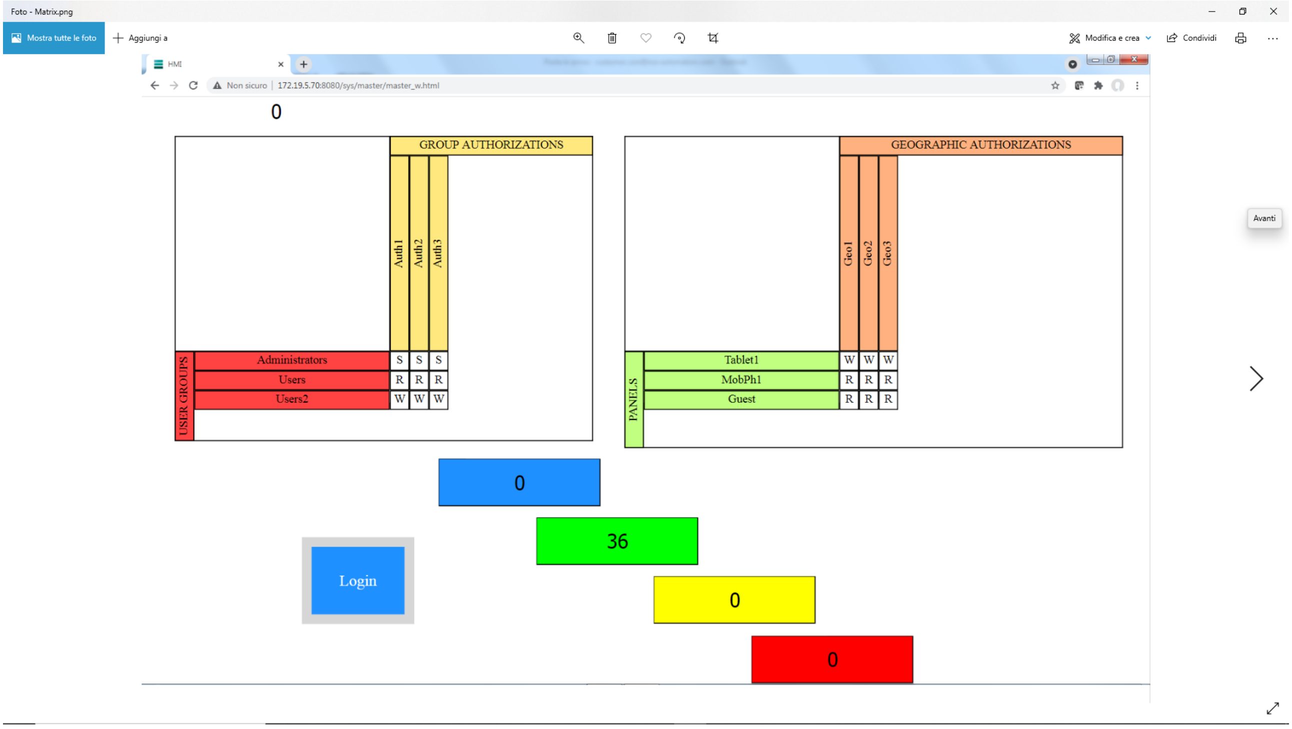
GEOGRAPHIC AUTHORIZATIONS

PANELS		Geo1	Geo2	Geo3
	Tablet1	W	W	W
	MobPh1	R	R	R
	MobPh2	R	R	R
	PCpanel	R	R	R
	Client5	R	R	R





10) The login from the expected IP address will enable the write access

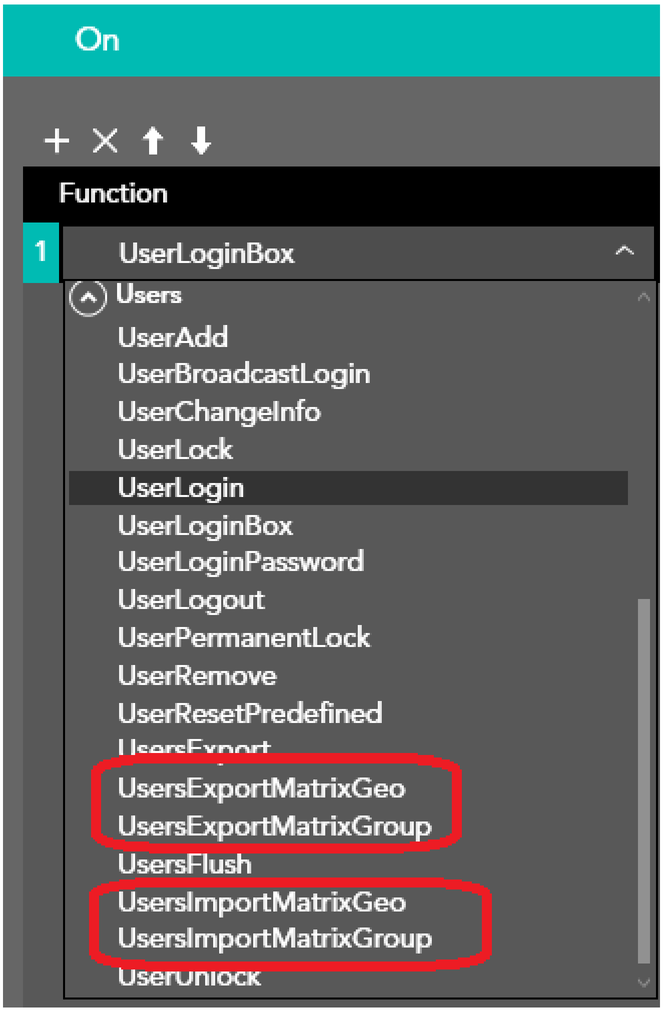


GROUP AUTHORIZATIONS	Auth1	Auth2	Auth3
USER GROUPS			
Administrators	S	S	S
Users	R	R	R
Users2	W	W	W

GEOGRAPHIC AUTHORIZATIONS	Geo1	Geo2	Geo3
PANELS			
Tablet1	W	W	W
MobPh1	R	R	R
Guest	R	R	R

<u>Note1</u>: Note that by logging in as ***http://localhost:8080*** the credentials will be limited compared to a GEOGRAPHIC login: ***http://IP-external:8080***

Note2: GROUPS+GEOGRAPHIC permissions can be exported to a different project via the built-in functions listed below:



Connect
ideas.
shape
solutions.

ESA S.p.A. | www.esa-automation.com |