



## 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.

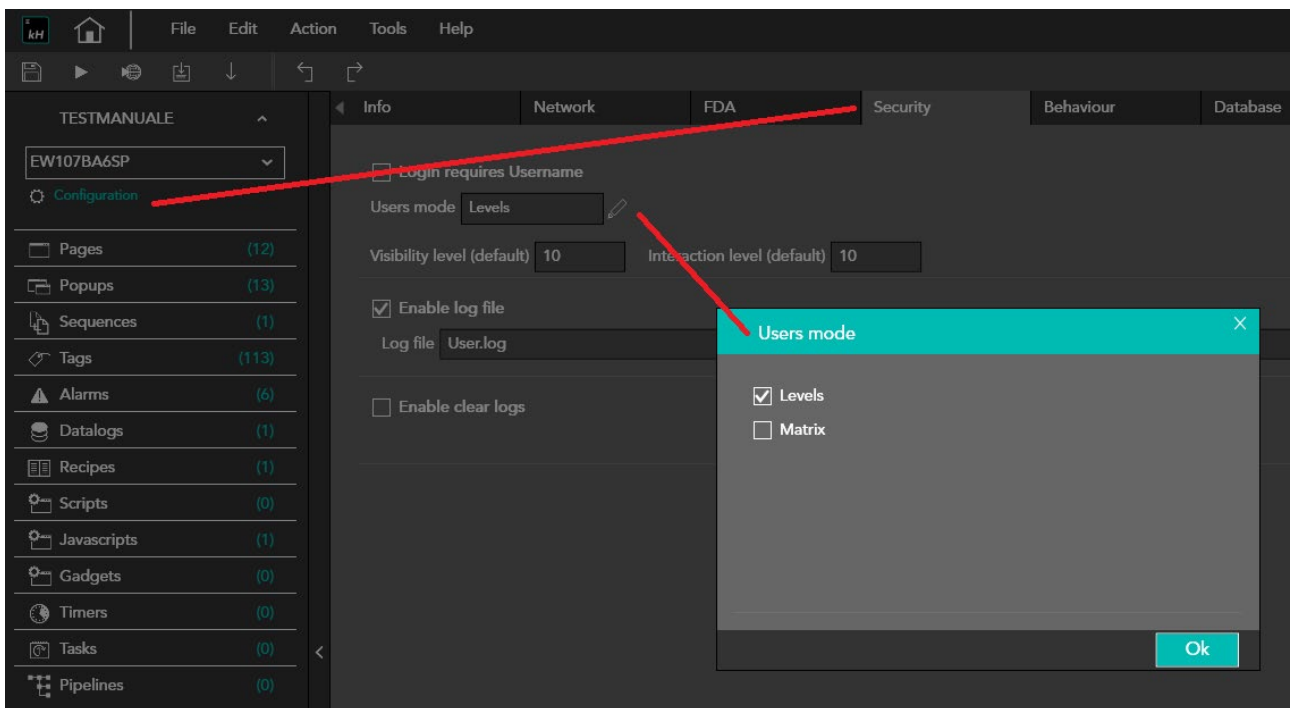


# introduction

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





## 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).

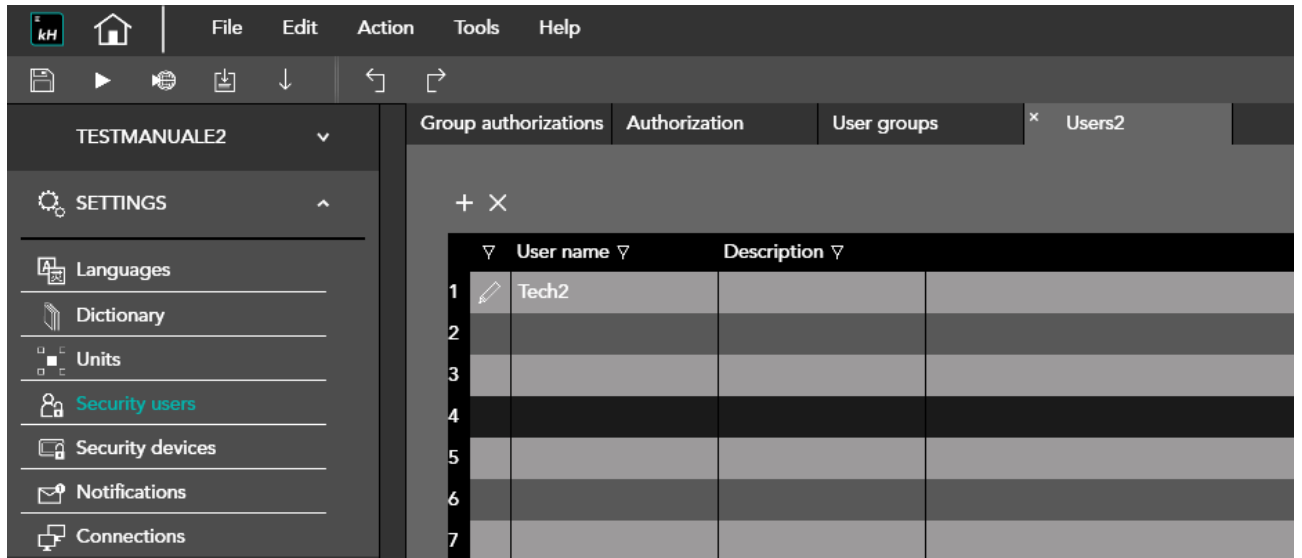
Let's see one of the many ways to use matrix user management.

#### 1) We define the project GROUPS

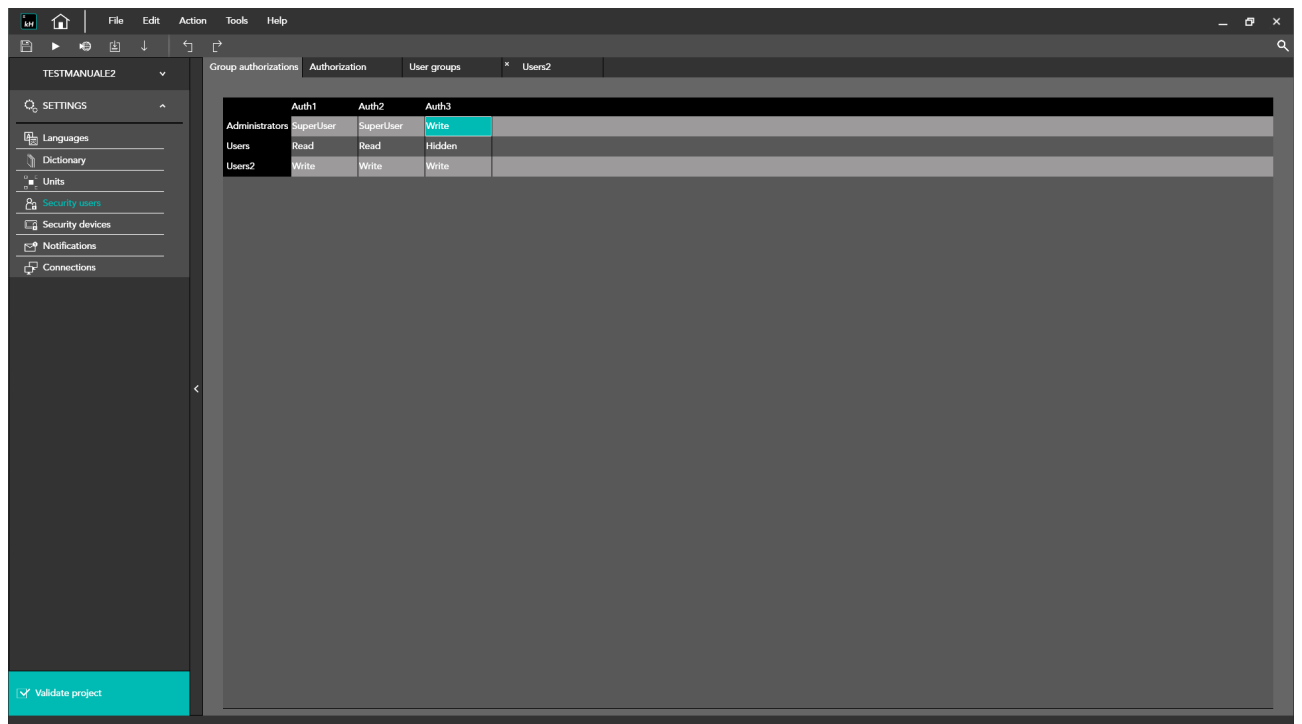
	Name	Description	VisibilityLevel	EnabledLevel	CanLockUsers	CanBeUnlocked
1	Administrators		1	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Users		10	10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Users2		5	5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4						
5						
6						
7						



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



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





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.

The screenshot shows a software interface with a dark theme. At the top, there is a menu bar with 'File', 'Edit', 'Action', 'Tools', and 'Help'. Below the menu bar is a toolbar with various icons. On the left side, there is a sidebar menu with the following items: 'TESTMANUALE2' (with a dropdown arrow), 'SETTINGS' (with an up arrow), 'Languages', 'Dictionary', 'Units', 'Security users', 'Security devices' (highlighted in blue), 'Notifications', and 'Connections'. The main area of the interface is divided into three tabs: 'Device authorizations', 'GEO Authorizations', and 'Devices'. The 'GEO Authorizations' tab is active, displaying a table with the following data:

	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.

The screenshot shows a project page editor with a grid-based layout. On the left, there are three tables: 'USER GROUPS' (red header), 'GROUP AUTHORIZATIONS' (yellow header), and 'PANELS' (green header). On the right, there is a 'GEOGRAPHIC AUTHORIZATIONS' table (orange header). Below these tables are four colored boxes with hash symbols: blue, green, yellow, and red. A blue 'Login' button is also present. A red diagonal line is drawn across the center of the page. On the right side, a 'Widgets Libraries' panel is visible, showing a search bar and a list of widgets including 'DataLog', 'TrendXY', 'Trend', 'PieChart', 'ActiveAlarms', 'AlarmsHistory', 'AlarmsStats', 'RecipeEdit', 'RecipeList', 'CustomFile', 'EventsLog', 'FrameHtml', 'FileViewer', 'Authorizations', and 'GeoAuthorizations'.

USER GROUPS		GROUP AUTHORIZATIONS			PANELS		GEOGRAPHIC AUTHORIZATIONS					
Administrators	S	S	W		Guest	R	R		Geo01			
Users	R	R	H		Tablet1	W	W		Geo02			
Users2	W	W	W		MobPh1	R	R	R	Geo03			



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

The screenshot displays a security configuration interface for a 'Login' page. It features two main authorization tables, a panels table, and a properties panel.

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

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

PANELS	Guest	R	R	R
	Tablet1	W	W	W
	MobPh1	R	R	R

The 'Properties' panel on the right shows the following security settings:

- 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

The screenshot shows a web browser window with two tables: 'GROUP AUTHORIZATIONS' and 'GEOGRAPHIC AUTHORIZATIONS'. Below the tables is a diagram showing a 'Login' button and three '0' buttons, one of which is locked.

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

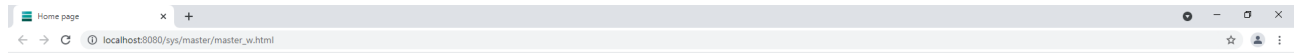
		GEOGRAPHIC AUTHORIZATIONS		
		Geo1	Geo2	Geo3
PANELS	Tablet1	W	W	W
	MobPh1	R	R	R
	MobPh2	R	R	R
	PCpanel	R	R	R
	Client5	R	R	R

Diagram elements:

- Login button (blue)
- 0 button (blue)
- 0 button (green) with a lock icon
- 0 button (yellow) with a lock icon

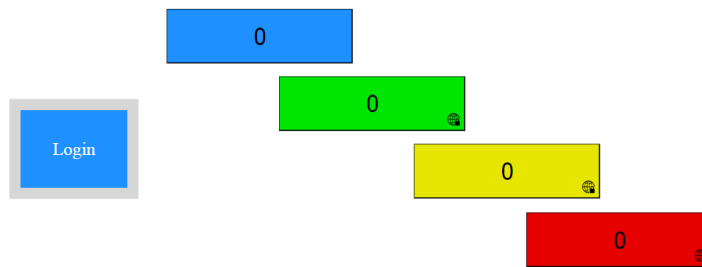


9) After a GROUP LOGIN the red box can be accessed (LOCK icon has been unlocked) but still the geographic authorization is protecting the object (see the different locked icon – GEOGRAPHIC AUTHORIZATION LOCK).



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

		GEOGRAPHIC AUTHORIZATIONS		
		Geo1	Geo2	Geo3
PANELS	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

The screenshot shows a web browser window displaying two authorization tables. The first table is titled 'GROUP AUTHORIZATIONS' and the second is 'GEOGRAPHIC AUTHORIZATIONS'. Below the tables is a flow diagram with colored boxes and numbers.

GROUP AUTHORIZATIONS			
	Amb1	Amb2	Amb3
Administrators	S	S	S
Users	R	R	R
Users2	W	W	W

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

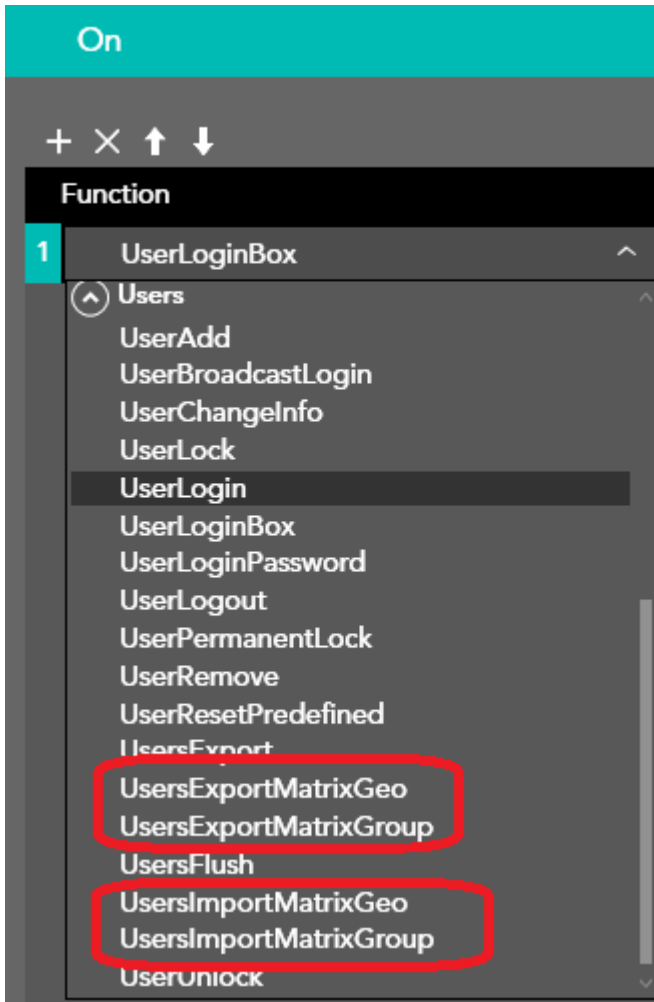
Flow diagram elements:

- Blue box: Login
- Blue box: 0
- Green box: 36
- Yellow box: 0
- Red box: 0

**Note1:** 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](http://www.esa-automation.com) |