



TUTORIAL KREO HMI Gestione utenti a matrice

Tutorial dedicato alla implementazione della gestione utenti con approccio a matrice

Connect
Ideas.
Shape
solutions.

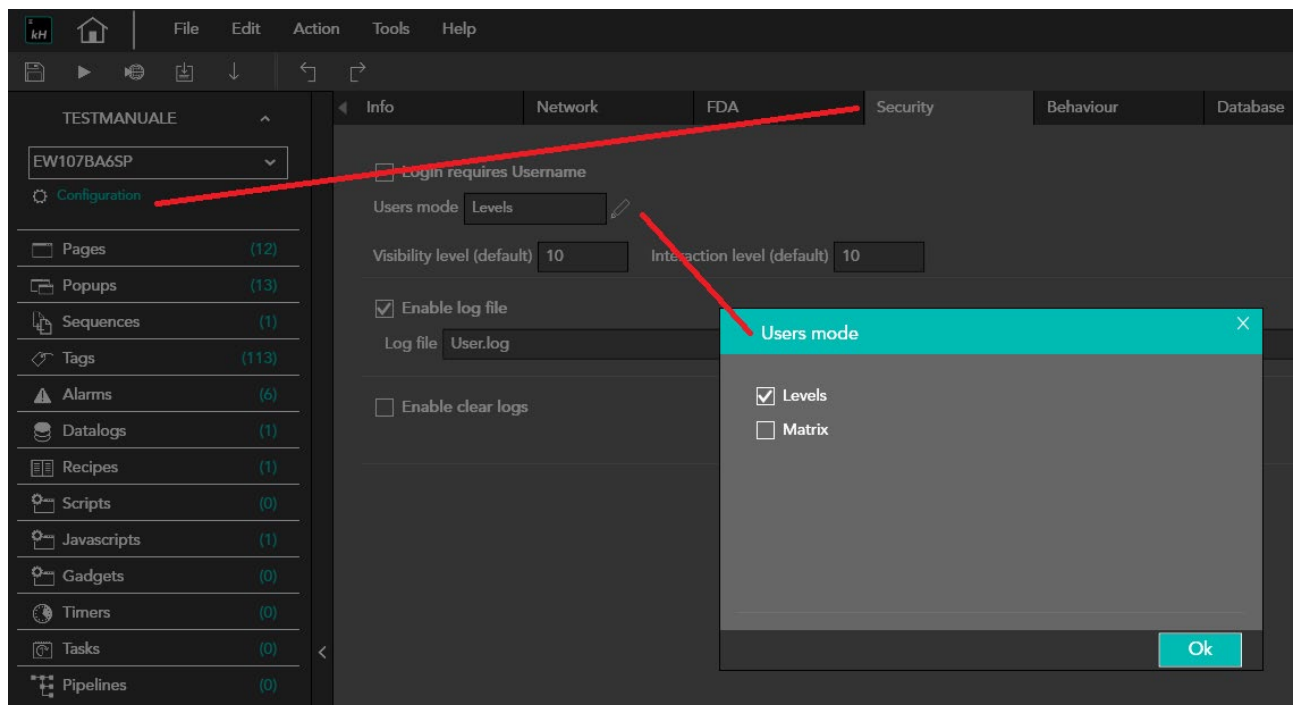


Introduzione

Nei progetti KREO HMI si possono impostare differenti gradi di sicurezza x filtrare l'accessibilità alle varie pagine e funzioni oggetti.

Tali configurazioni si suddividono in 2 diverse modalità dove una esclude l'utilizzo dell'altra:

- LIVELLI
- MATRICE





Come fare:

Nella modalità A MATRICE cade il concetto tradizionale di LIVELLI e vengono introdotte, insieme alle credenziali di GRUPPI, anche le credenziali GEOGRAFICHE.

L'interazione fra tali 2 credenziali filtra le varie modalità di accesso agli oggetti:

R: Read-Only

(l'utente loggato può visualizzare gli oggetti protetti senza interagire con essi)

W: Write

(l'utente loggato può visualizzare e interagire con gli oggetti protetti)

H: Hidden

(l'utente loggato non può visualizzare gli oggetti protetti)

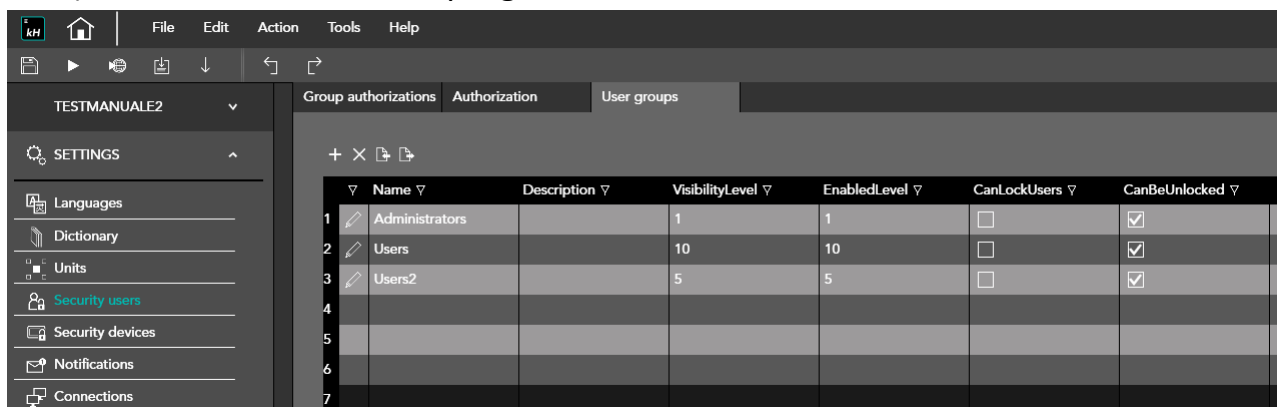
S: Superuser

(tale utente può tutto)

La combinazione di credenziali di GRUPPO+GEOGRAFICHE determinerà uno dei 4 modi di accesso (il più stringente è quello predominante).

Vediamo uno fra i tanti modi di poter usare la gestione utenti A MATRICE.

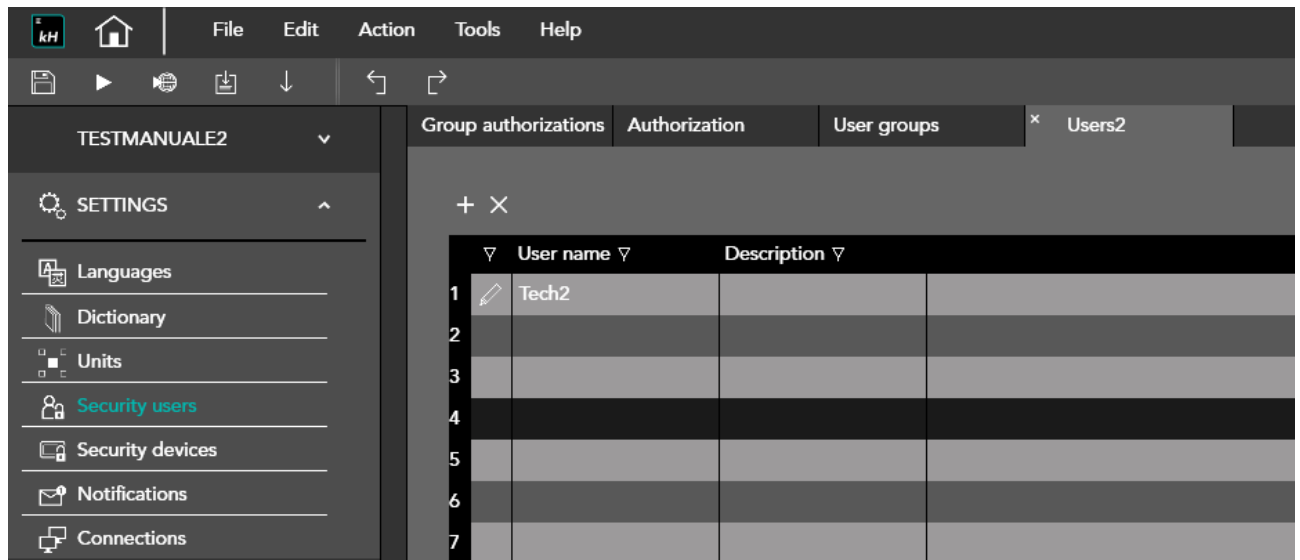
1) Definiamo i GRUPPI di progetto



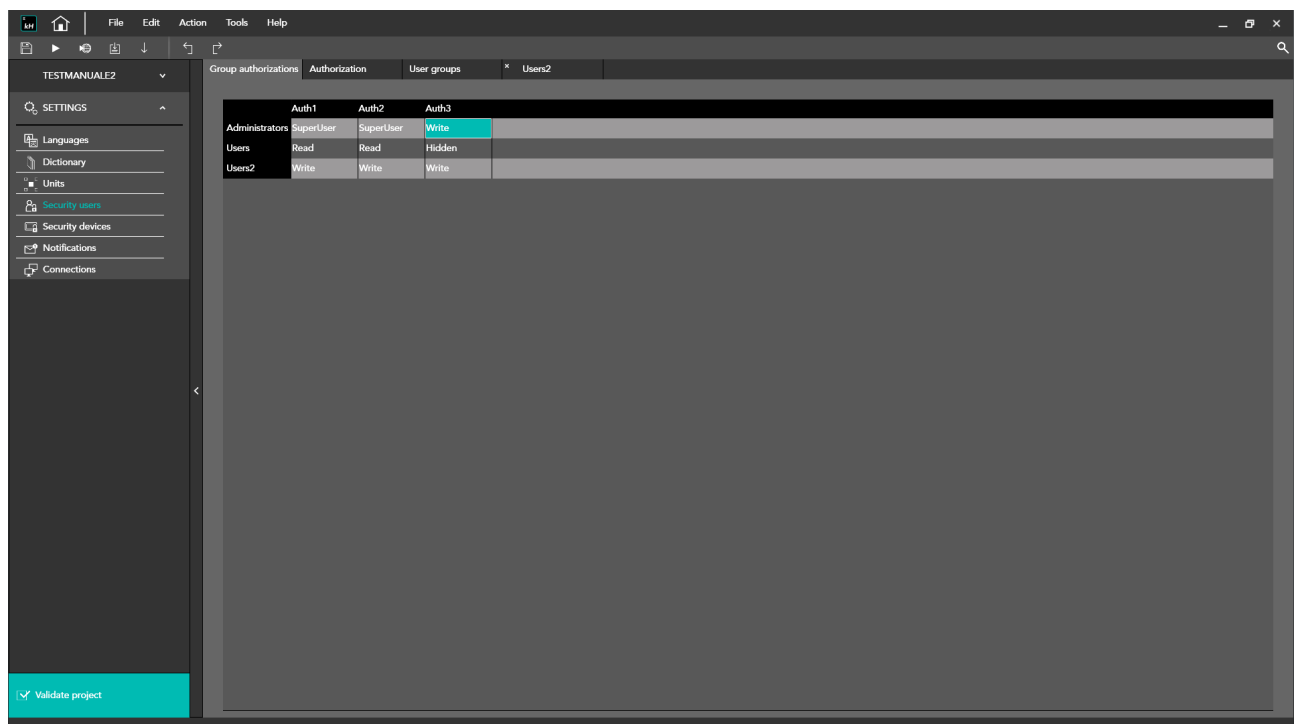
	Name ▾	Description ▾	VisibilityLevel ▾	EnabledLevel ▾	CanLockUsers ▾	CanBeUnlocked ▾
1	Administrators		1	1	☐	☒
2	Users		10	10	☐	☒
3	Users2		5	5	☐	☒
4						
5						
6						
7						



2) Ogni gruppo avrà i propri UTENTI con accesso classico di login+password



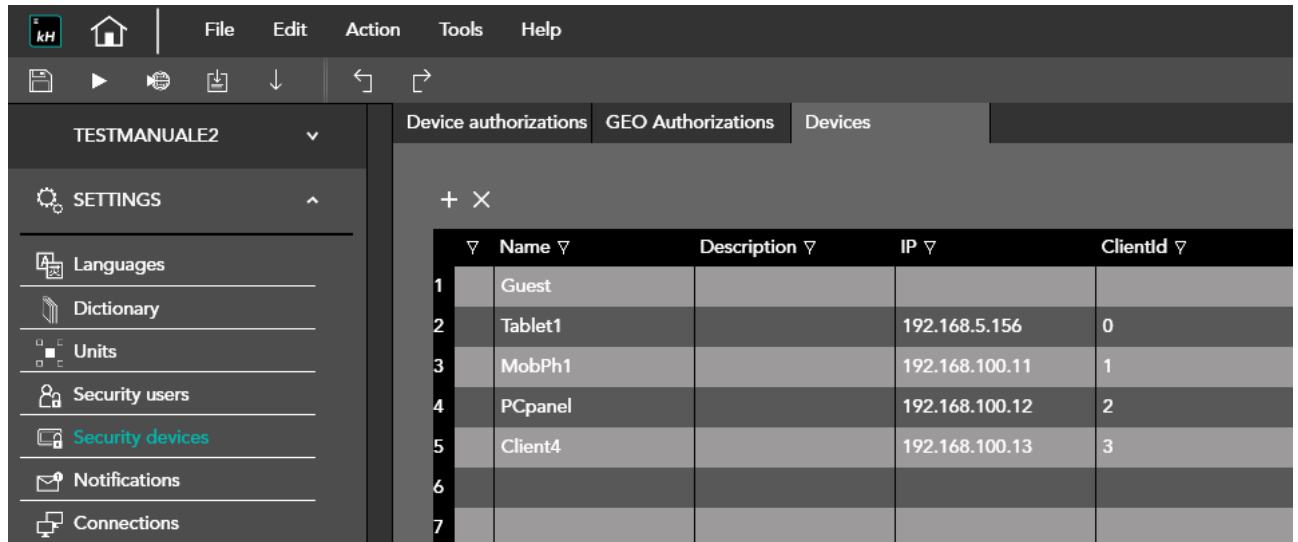
3) Le autorizzazioni di GRUPPO si configurano a EDITOR ma potranno poi essere cambiate a RUNTIME da LOGIN autorizzati





4) Configuriamo ora le credenziali GEOGRAFICHE attraverso gli indirizzi IP previsti per i dispositivi client.

Collegarsi da un certo indirizzo IP prevede di accedere a credenziali di tipo 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				

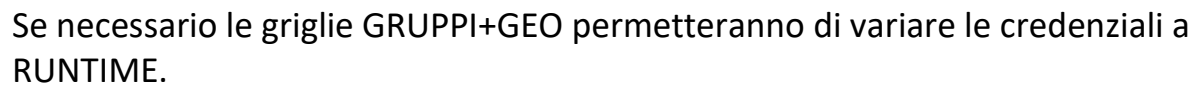
Nota: l'indirizzo GUEST identifica una connessione GEOGRAFICA da parte di CLIENT (tablet/mobile/pc) non previsto a livello di progetto KREO HMI.
In questo caso l'utenza avrà sempre credenziali GUEST



- 5) Anche per le credenziali GEO configuro a EDITOR la modalità corrispondente (S,W,R,H) comunque modificabile a RUNTIME.

	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) Sulle pagine di progetto si possono configurare ora gli oggetti con protezioni GRUPPI+GEO.





7) Gli oggetti della pagina vengono protetti con credenziali GRUPPI+GEO secondo necessità

The screenshot displays the ESA software interface with a grid-based workspace and a Properties panel on the right.

GROUP AUTHORIZATIONS Table:

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

GEOGRAPHIC AUTHORIZATIONS Table:

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

PANELS Table:

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

Workspace Elements:

- A blue "Login" button.
- A green rectangular object with a red outline and a red arrow pointing to the "GroupAuthorization" property in the Properties panel.
- A yellow rectangular object with a red outline and a red arrow pointing to the "GeoAuthorization" property in the Properties panel.
- A red rectangular object with a red outline.

Properties Panel (EditBox):

- General: (EditBox)
- Behavior: Visibility (On), Disabled (Off), TextFormat (Dec: #####), 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) All'avvio del RUNTIME, prima del LOGIN, verranno visualizzati tutti gli oggetti tranne quelli con credenziali HIDDEN.

Gli oggetti protetti sono identificati da un lucchetto

Home page x +

localhost:8080/sys/master/master_v.html

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

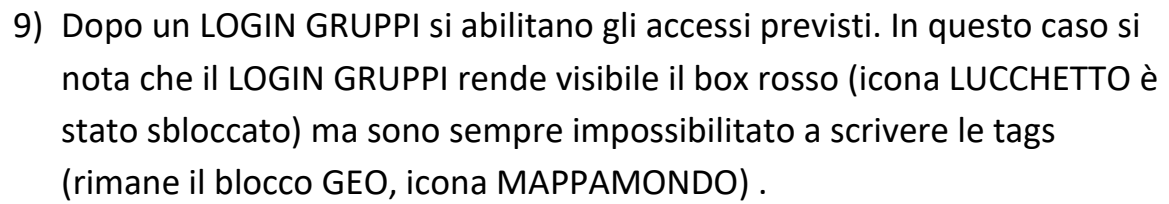
		GEOGRAPHIC AUTHORIZATIONS		
		Geo1	Geo2	Geo3
PANELS	Tablet1	W	W	W
	MobPh1	R	R	R
	MobPh2	R	R	R
	PCpanel	R	R	R
	Client5	R	R	R

0

Login

0

0

Page 10 of 13



- 10) Sarà solo una connessione GEO dall'indirizzo IP previsto che mi abiliterà alla scrittura tags protette (il box verde è ora scrivibile)

The screenshot displays a web application interface with two main tables: "GROUP AUTHORIZATIONS" and "GEOGRAPHIC AUTHORIZATIONS". Below these tables is a diagram illustrating a login flow with colored boxes and numbers.

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

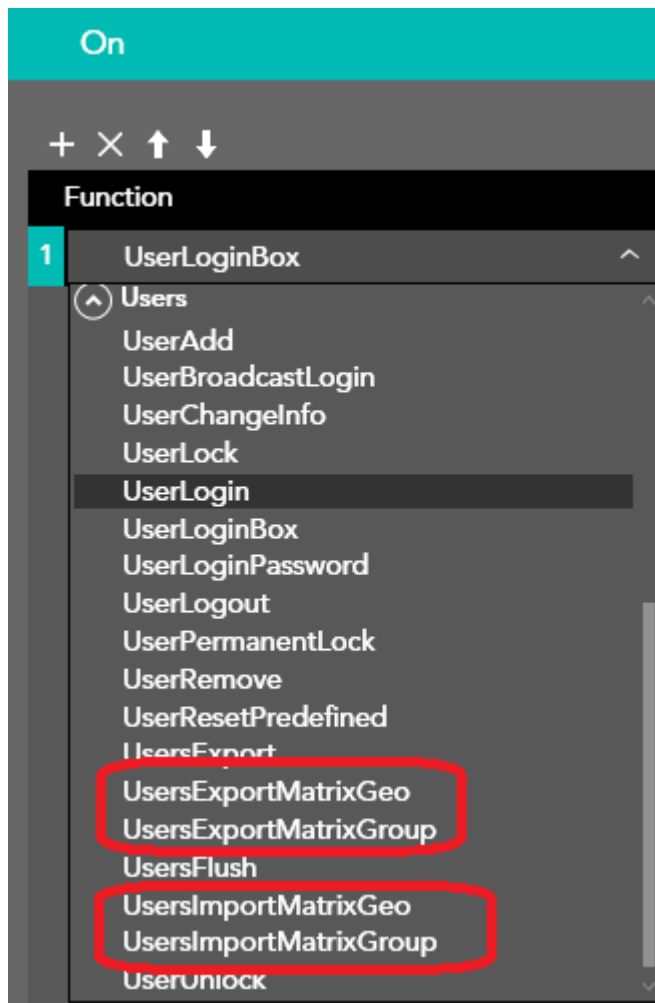
GEOGRAPHIC AUTHORIZATIONS				
		Geo1	Geo2	Geo3
PANELS	Tablet1	W	W	W
	MobPh1	R	R	R
	Guest	R	R	R

Below the tables, a diagram shows a login flow:

- A blue box labeled "Login" leads to a blue box with "0".
- The blue box with "0" leads to a green box with "36".
- The green box with "36" leads to a yellow box with "0".
- The yellow box with "0" leads to a red box with "0".

Nota1: Si nota che loggandosi come ***http://localhost:8080*** avrò credenziali limitate rispetto ad un login GEO abilitato: ***http://IP-esterno:8080***

Nota2: Autorizzazioni GROUPS+GEO sono esportabili da progetto all'altro attraverso funzioni predefinite





Connect
ideas.
shape
solutions.

[ESA S.p.A. | www.esa-automation.com](http://www.esa-automation.com) |