Security White Paper

Document Information

Software Version:	4.0.1.3
Creation Date:	02 September, 2020
Author:	Danilo Rodrigues
Editor:	Fabio Carvalho
Last Edit Date:	22 December, 2020
Version:	1.1

ADISRA · 3432 Greystone Drive, Suite 125 · Austin, TX 78731
Phone: 1-833-5ADISRA (1-833-523-4772)
www.ADISRA.com

Table of Contents

1. Scope *3*

2. Summary *3*

3. Profile Permissions *4*

4. Users & Profile Settings *5*

4.1 Create Profile **6**

4.2 Edit Profile **7**

4.3 Delete Profile **8**

5. Local Users Settings *9*

5.1 Create User **10**

5.2 Edit User **11**

5.3 Delete User **12**

6. Security Options *13*

6.1 Engineering Security **13**

6.2 Runtime Security **14**

7. Security Functions *15*

8. Domain Users *22*

8.1 Using Domain Users **25**

1. Scope

The ADISRA SmartView Security White Paper document clarifies how the ADISRA SmartView security system works internally and the steps needed to configure.

The document explains how to manage profiles and users, verify the logged-in users, how to import profiles from the LDAP service, and how to customize the application adding different access permissions to different profiles.

2. Summary

The Security Settings allows the user to create profiles and users to add a layer of security to the project.
It is possible to add security to the Engineering and Runtime.

1. If the Security System is enabled for the Engineering, it is possible to prevent unauthorized users from editing the application.
2. If the Security System is enabled for the Runtime, it is possible to give different access permissions to different profiles, preventing a group of users to change tag's values, opening screens, deleting information and so on.

When editing the profiles or users, the runtime application will need to be restarted for changes to take place.

3. Profile Permissions

When creating and editing profiles, there will be permissions settings for each profile, the permissions are:

1. **Can Do Action**: Determines if the profile has permission to perform actions inside a graphic or graphic object actions, mostly scripts.

2. **Can Open Graphics**: Determines if the profile has permission to open Graphics, for example, if a button has an action that will open a graphic or open a graphic through the Viewer icon in the system tray.

3. **Can Close Graphics**: Determines if the profile has permission to close Graphics, for example, if a button has an action that will close a graphic or close a graphic through the window icons.

4. **Can Start App**: Determines if the profile has permission to start the Runtime of an application.

5. **Can Shutdown App**: Determines if the profile has permission to stop the Runtime of an application.

6. **Can Switch Tasks**: Determines if the profile has permission to switch between tasks of the system.

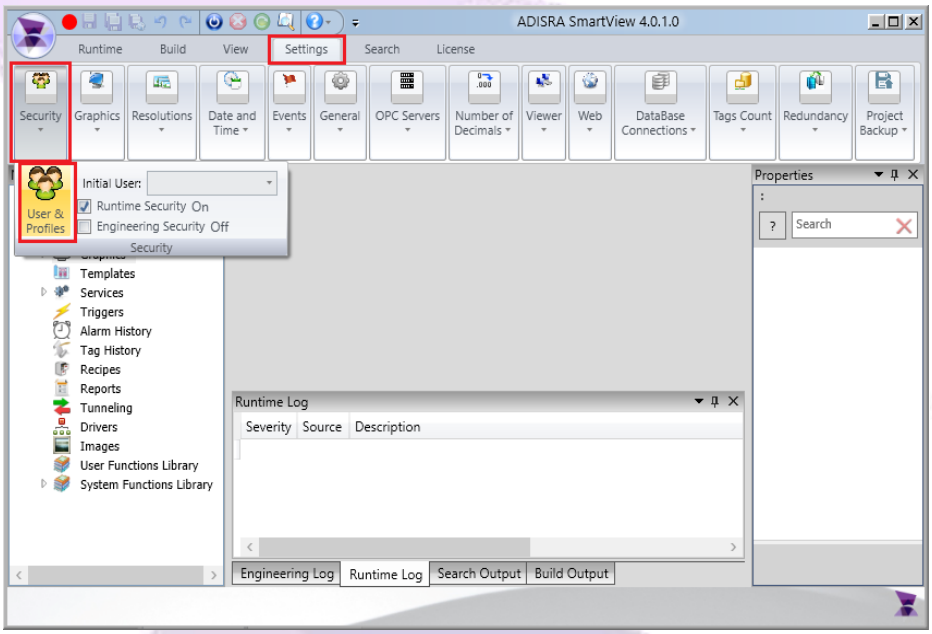
7. **Can Open Task Manager**: Determines if the profile has permission to open the task manager of the system.

8. **Is ReadOnly**: A profile with ReadOnly permission can only see the application, but cannot see or change the values of tags, and can execute buttons with simple scripts like open a graphic.

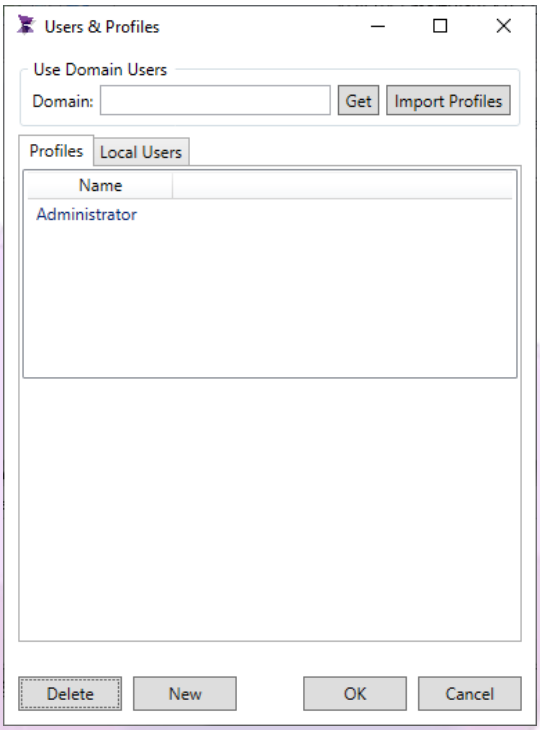
These permissions will be the default permissions for the graphics and graphics objects, but the permissions can also be set for each graphic or object and if it will or will not use the default. Overriding the default permissions can be done in the properties grid in the security area as we will see an example later in this document.

4. Users & Profile Settings

To open the "Users & Profile" window, go to the settings ribbon, then select security, and click on "Users & Profiles":

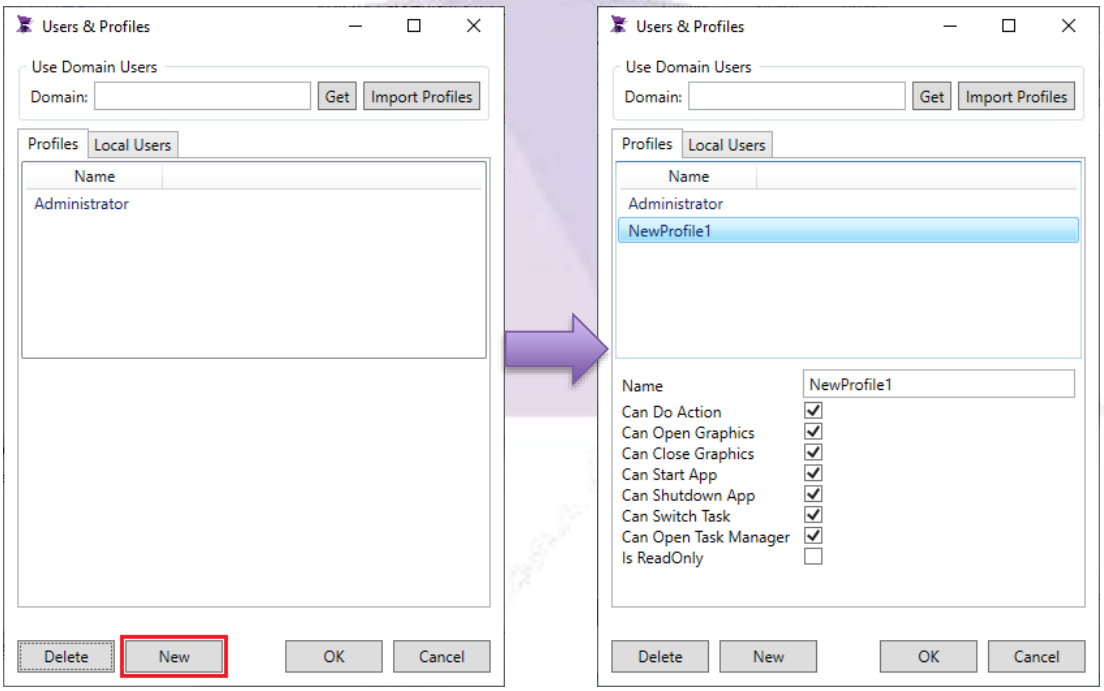


The "Users & Profile" window will open:



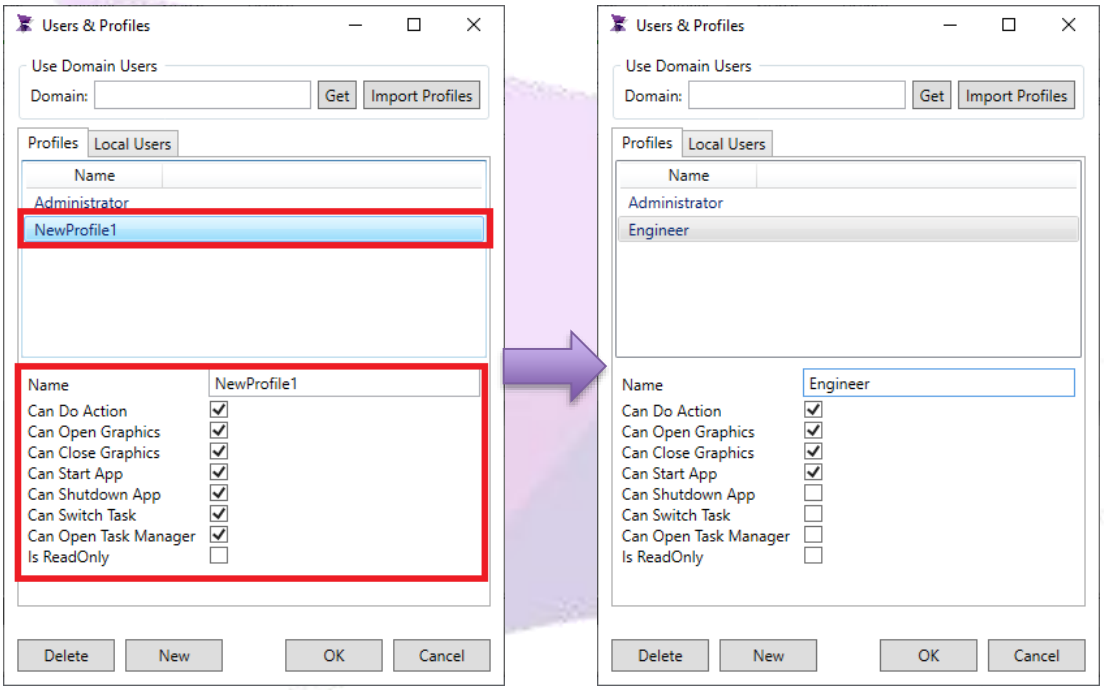
4.1 Create Profile

To create a profile, click the “new” button:



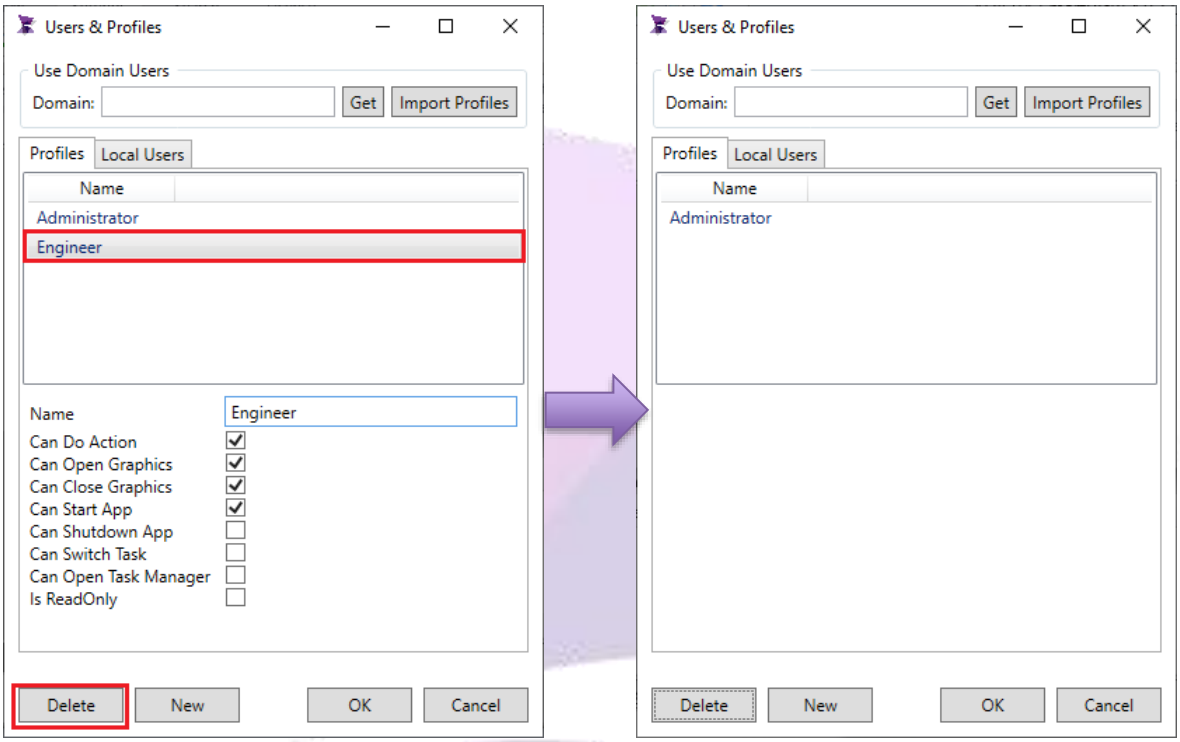
4.2 Edit Profile

To edit a profile, select the desired profile, then rename it and change the permissions:



4.3 Delete Profile

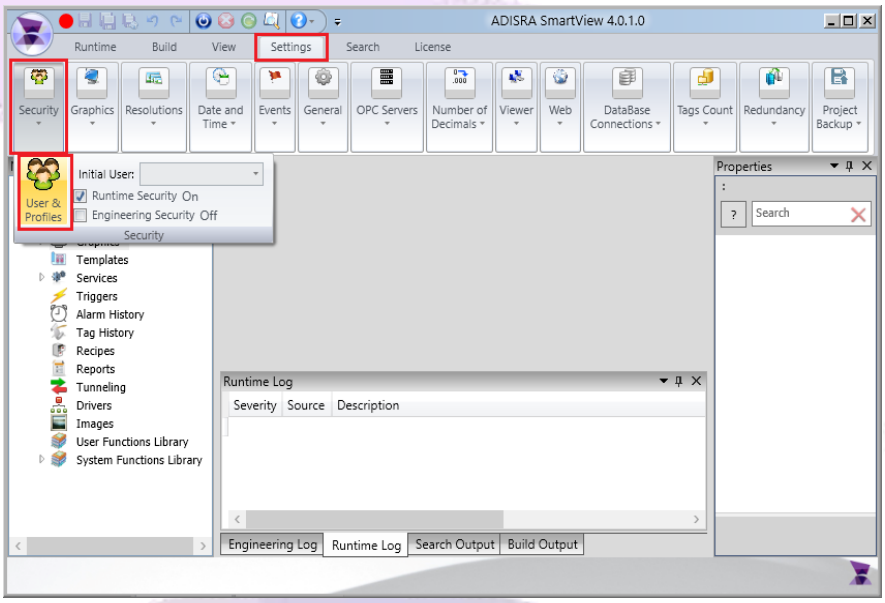
To delete a profile, select the desired profile then click the “Delete” button:



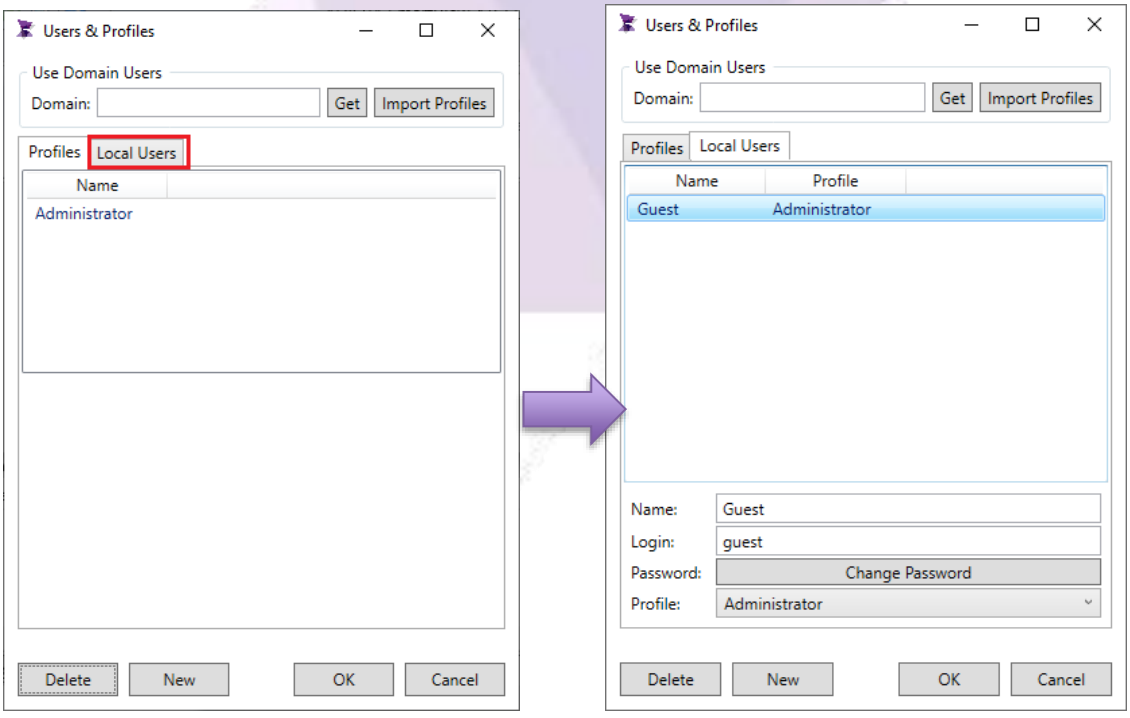
5. Local Users Settings

The Local Users are managed by ADISRA SmartView.

To open the "Users & Profile" window, open the settings ribbon, then select security, and click on "Users & Profiles":

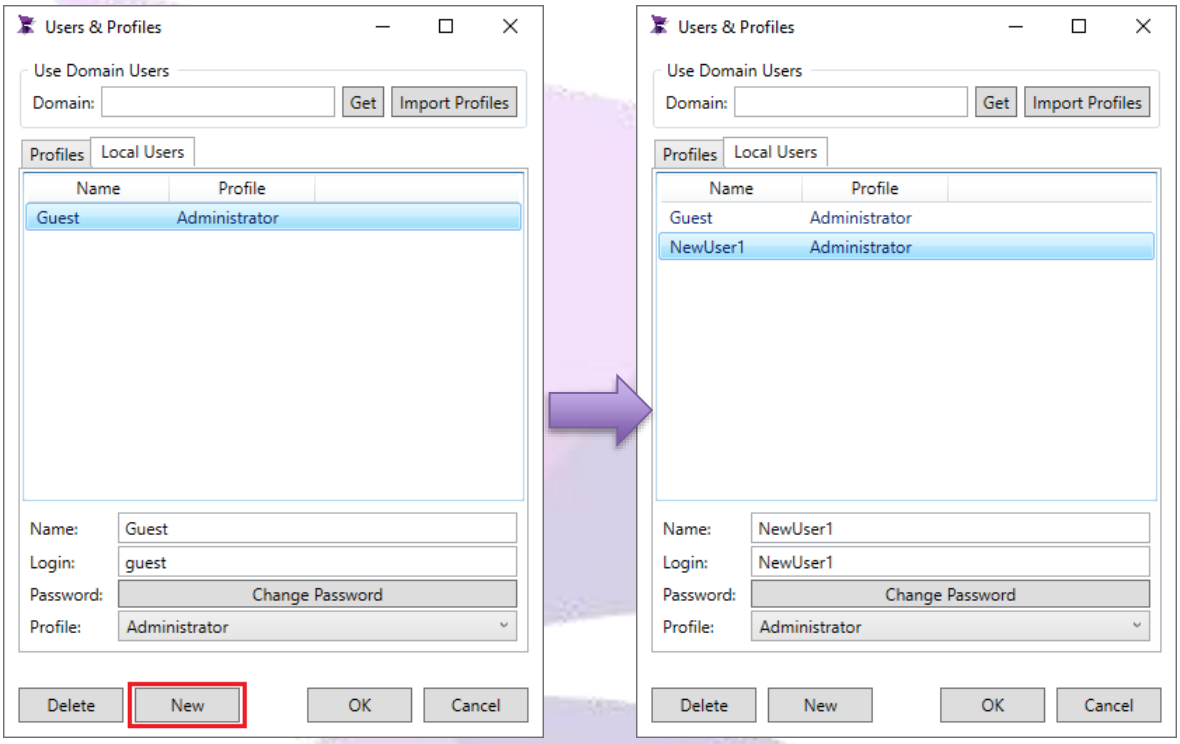


The "Users & Profile" window will open, then click the "Local Users" tab:



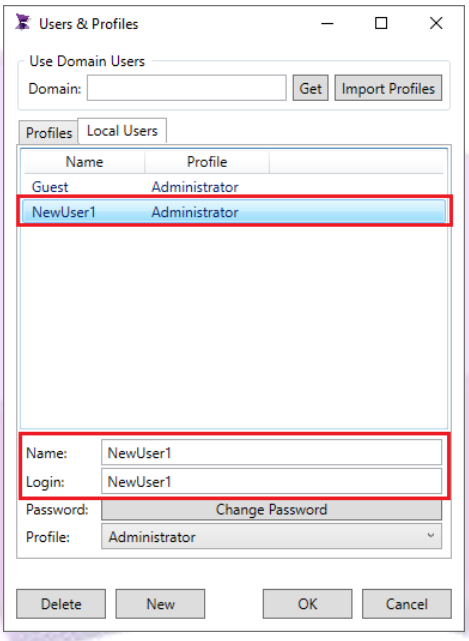
5.1 Create User

To create a Local User, click the “new” button, and then set the name, login username, password, and the profile.

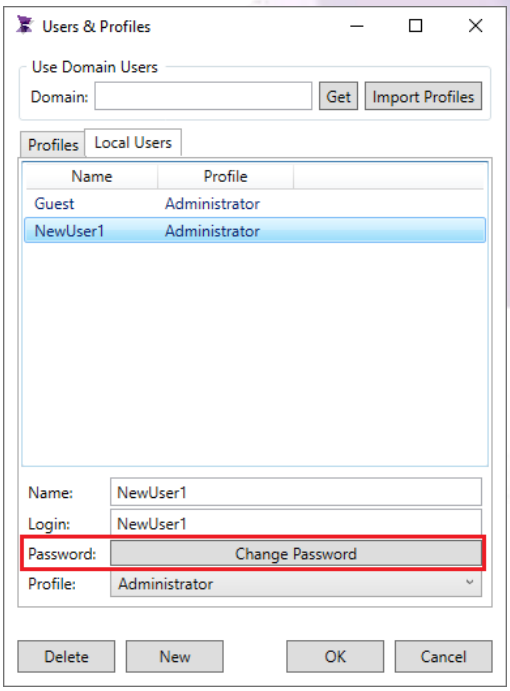


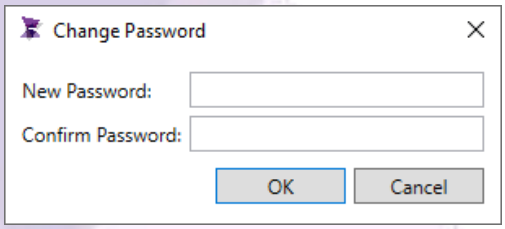
5.2 Edit User

To edit a Local User, select the desired user, then rename it and change the login:

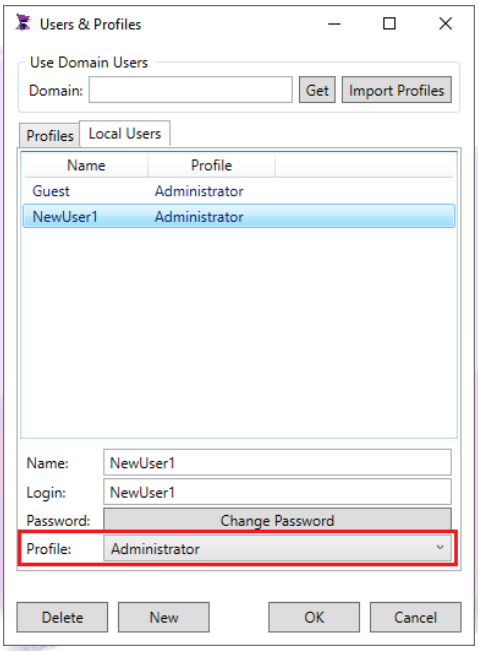


To change the password, click the “Change Password” button, it will open the “Change Password” window, type in the new password, and confirm it, then click “OK”:



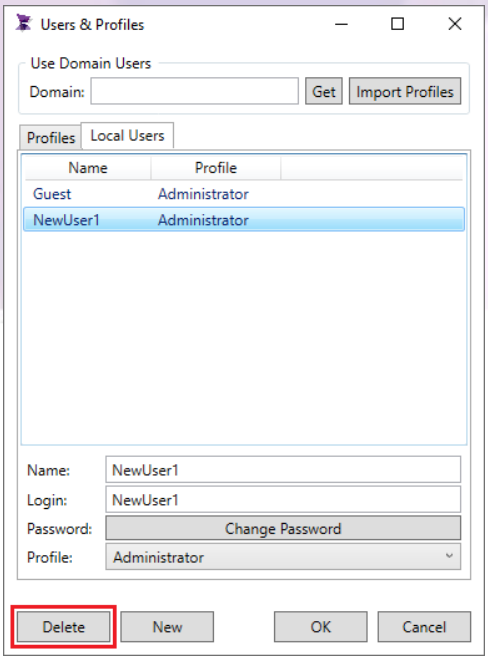


To assign the local user to a profile created in the previous chapter, use the Profile combobox to select an existing profile:



5.3 Delete User

To delete a Local User, select the desired user, then click the “Delete” button:

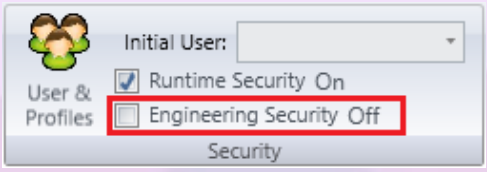


6. Security Options

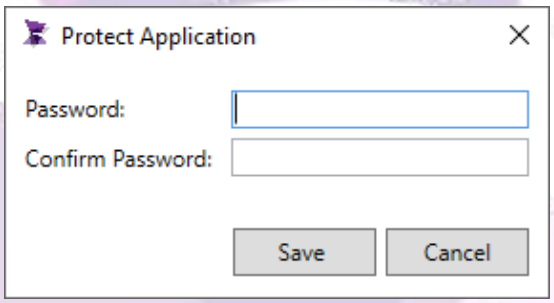
6.1 Engineering Security

Engineering Security may be turned on and off. When enabled, the user will be asked to enter their password before editing the application.

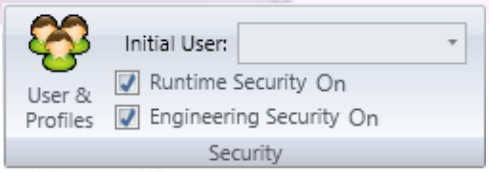
To turn Engineering Security on, go to the Ribbon Settings Security, and select the option "Engineering Security."



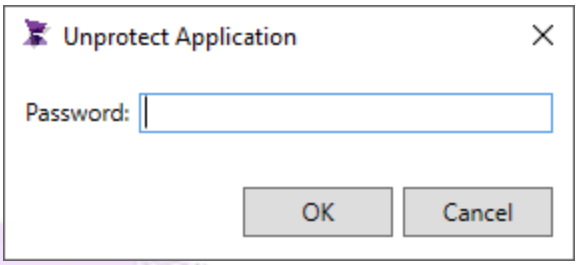
It will open the "Project Application" window, after configuring a password, click the "Save" button.



The "Engineering Security" label has changed from Off to On. Going forward, every time this project is loaded it will request the user enter the password configured.



To turn "Engineering Security" off, select the option "Engineering Security" again, and type in the configured password. This procedure will turn "Engineering Security" off.



6.2 Runtime Security

Runtime Security can be turned on and off. When enabled, the profile permissions will work as configured during Runtime. When it is off, the logged-in users will have all the permissions enabled.

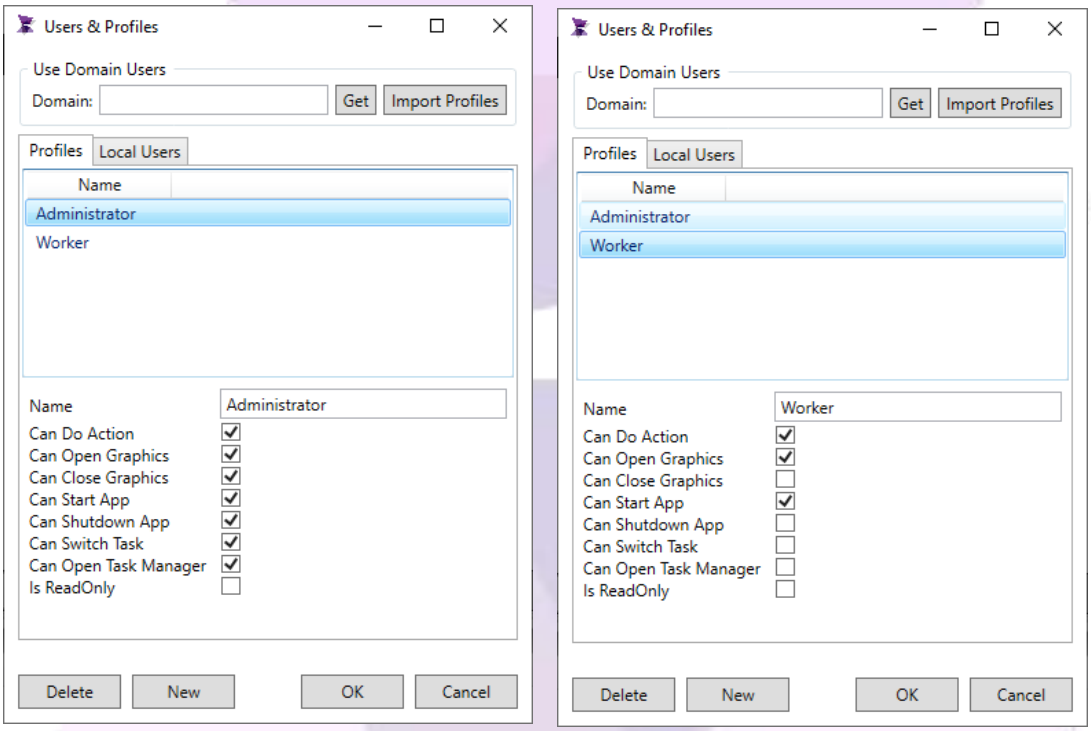
To turn "Runtime Security" off, go to the Ribbon Settings Security, and deselect the option "Runtime Security"

To turn "Runtime Security" on, just select it again.

7. Security Functions

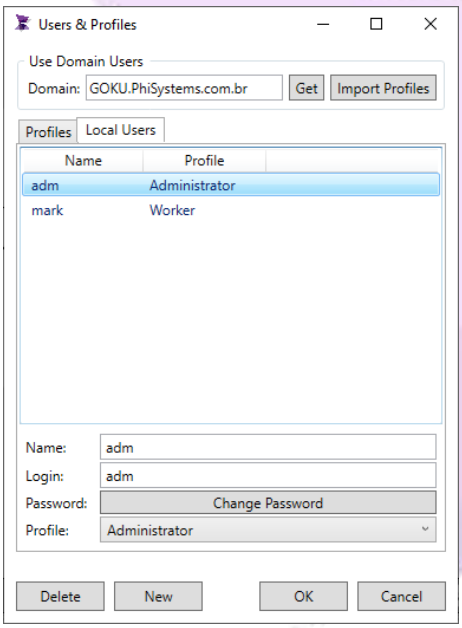
This chapter explains how to use the System Function Library SVSecurity by providing some examples.

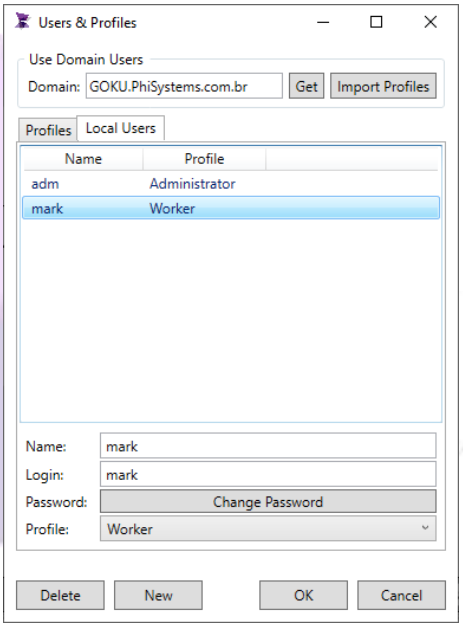
Create two (2) profiles with the permissions as shown in the images below. It is important to understand that the profile "worker" cannot close graphics and it also does not have some Operation System permissions such as, "Switch Task" (ALT+TAB):



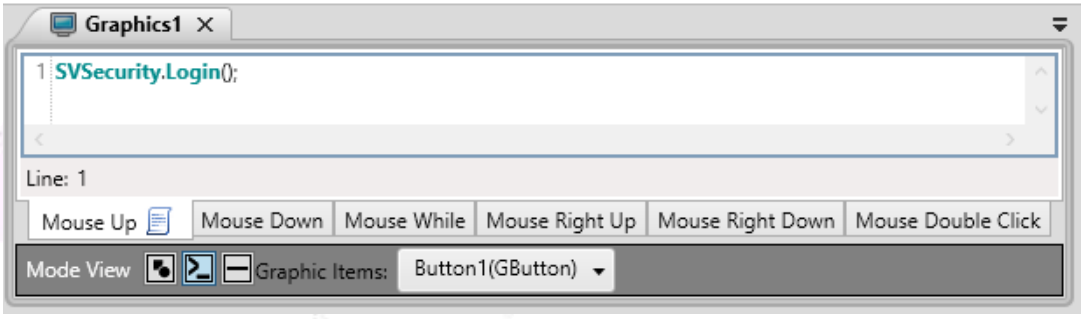
Note: *When the logged-in user does not have permission to switch tasks, they will not be able to use the machine's operating system while the Viewer is running.*

Create two (2) Local Users as shown in the images below. The passwords for each user are the same as the login (adm/adm, mark/mark):

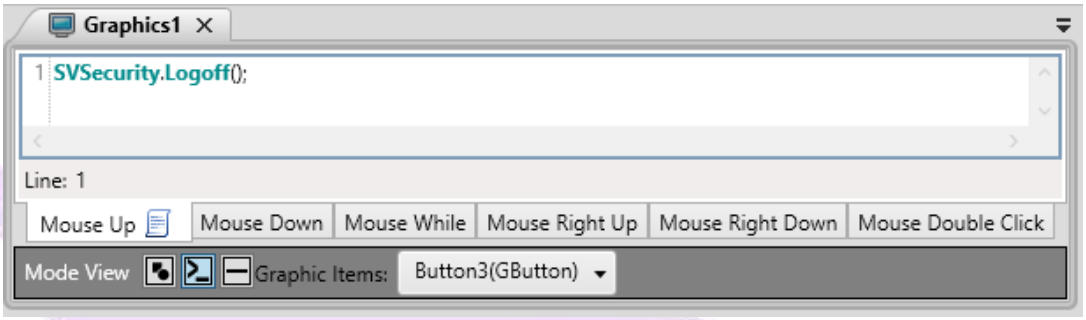




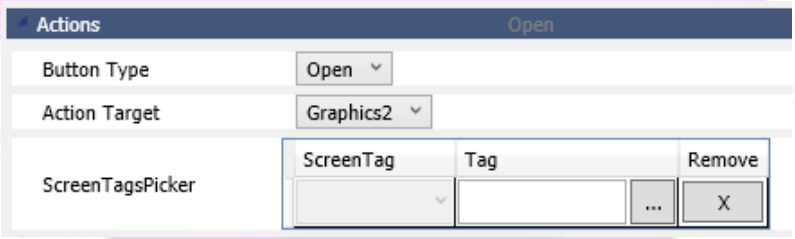
Create two (2) Graphic Documents, Graphics1 and Graphics2. Inside Graphics1, create two (2) labels, create a button with the text “login”, and the “Mouse Up” script as shown below:



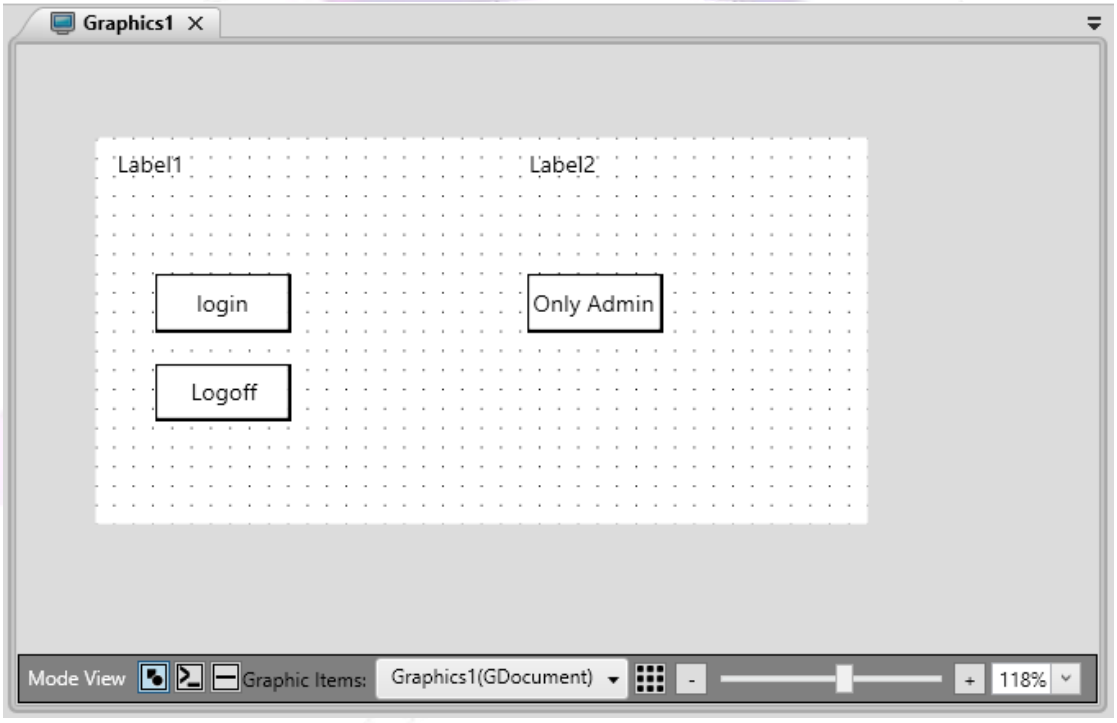
Create a button with the text “logoff” and the “Mouse Up” script as shown in the image below:



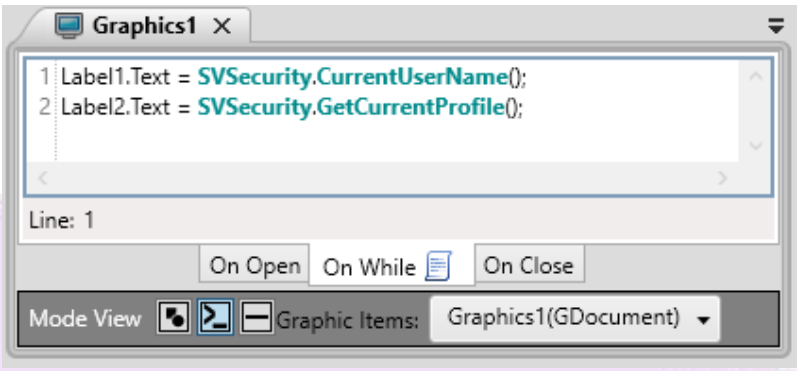
Create a button with the text "Only Admin" and in the button Properties within the "Actions" area, configure as shown in the image below:



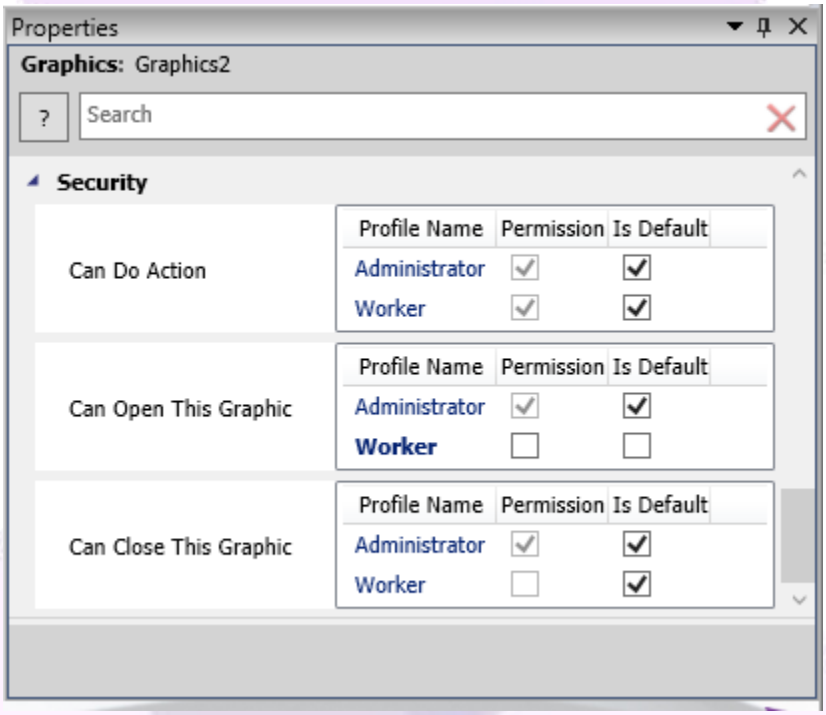
The Graphics1 should look like this:



Configure the "On While" script of Graphics1 to look like the image below. It will display which user is logged in and their profile:

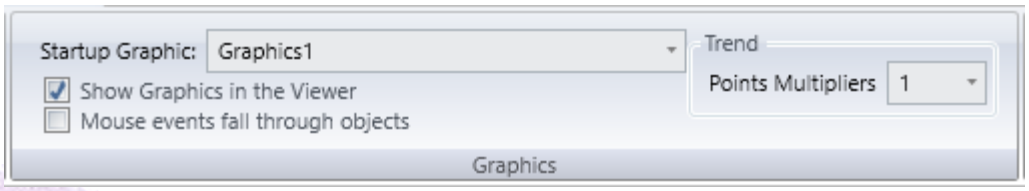


In the Graphics2 Property Grid under the "Security" area, uncheck the permission of the "Worker" profile as shown in the graphic below:

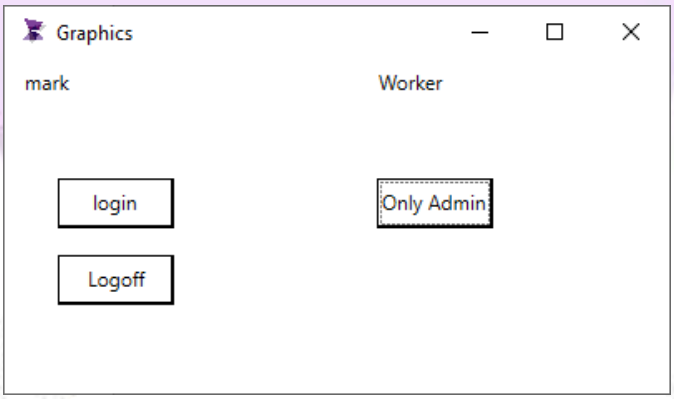


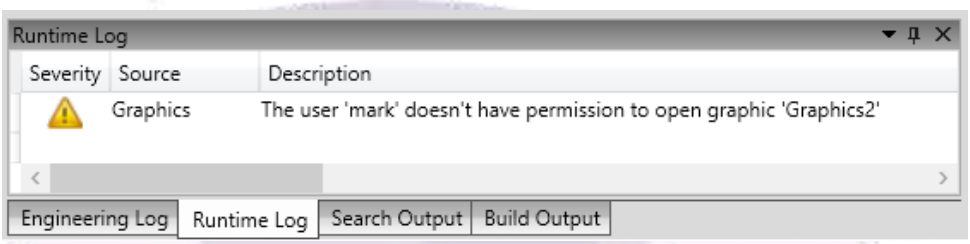
In the Ribbon Setting Security, set the initial user as "mark" so when the Runtime starts "mark" will be the default user:

In the Ribbon Setting Graphics, set the Startup Graphic as "Graphics1" so when the Runtime starts, "Graphics1" will be the graphic that will open:

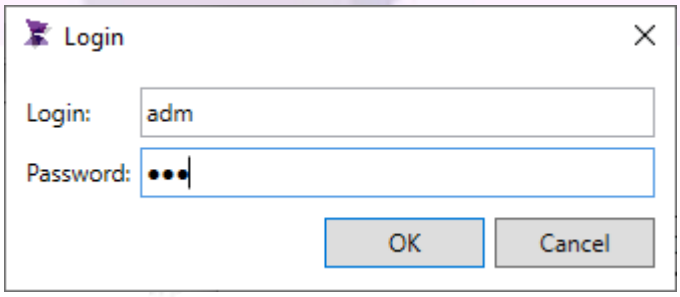


Now that it is configured, run the application by starting Runtime. The Graphics1 will open and the user "mark", with the profile "worker", will be the user logged in. Try to open the Graphics2 by pressing the "Only Admin" button; the Graphics2 will not open because the user "mark" does not have the permission and an error will be logged in the "Runtime Log":

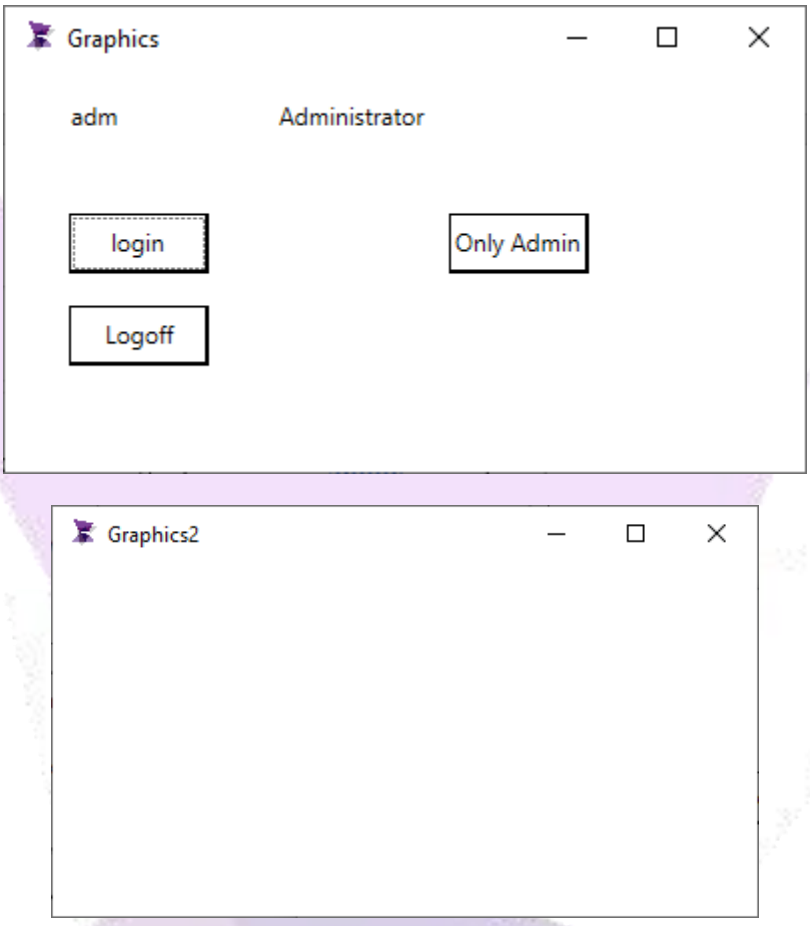




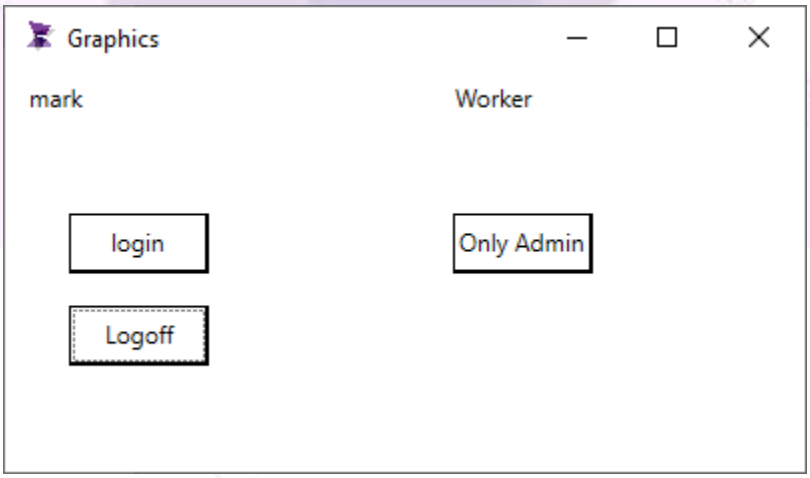
Click the "Login" button and enter the login and password "adm" and select OK.

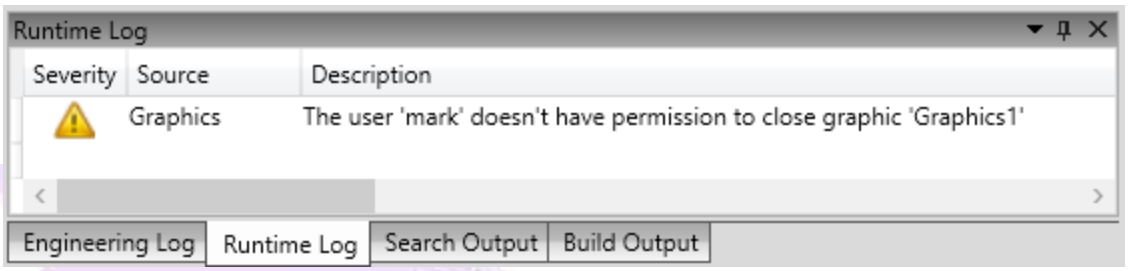


The user logged in is "adm" with the profile "Administrator" and by clicking the "Only Admin" button, the Graphics2 will open. After opening, please close Graphics2.



Click the "Logoff" button, and then, the user "mark" will be automatically logged in. Now, the graphic cannot be closed.



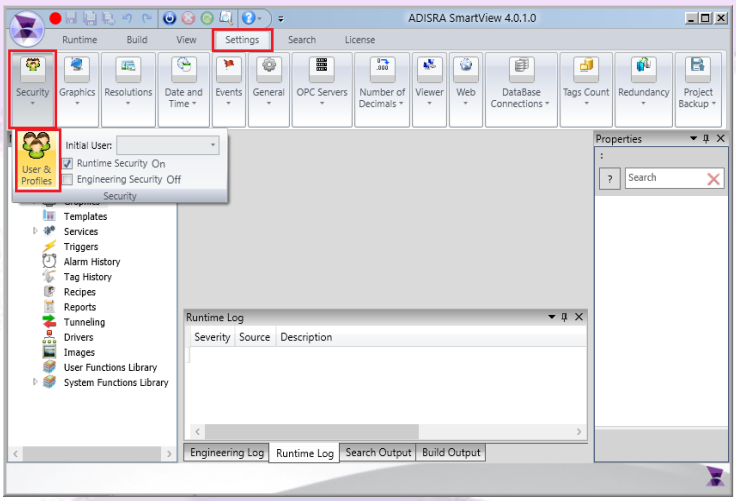


Once again, log in as the “adm” user, and now close the graphic.

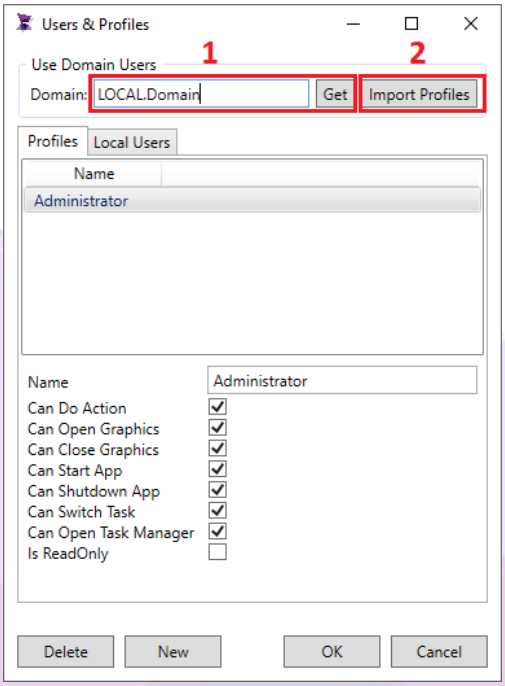
8. Domain Users

The network user's login information can be used by importing groups from a domain. Each group imported will become a profile and all the users of this group will be associated with this profile.

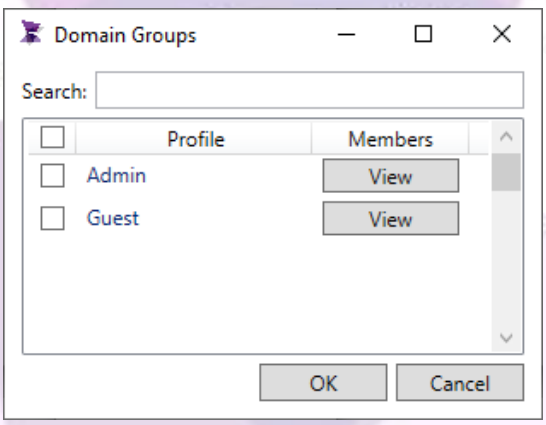
To open the "Users & Profile" window, go to settings ribbon, then security, and click on "Users & Profiles":



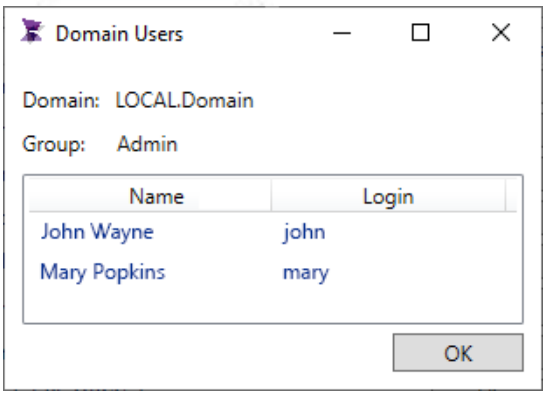
The "Users & Profile" window will open. In the "Domain" textbox, type the domain name of the profiles to be imported, or use the "Get" button to automatically load the domain name where the machine is logged in, then click the "Import Profiles" button:



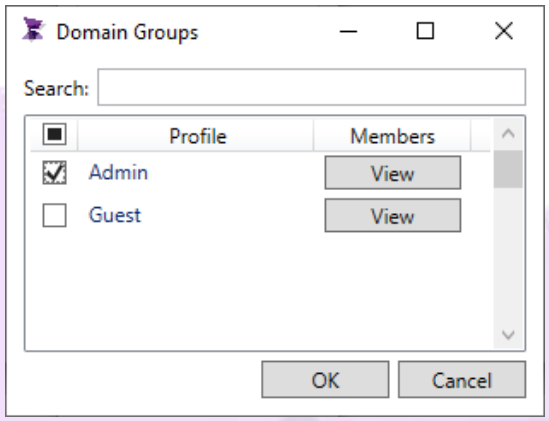
The "Domain Groups" window will open:



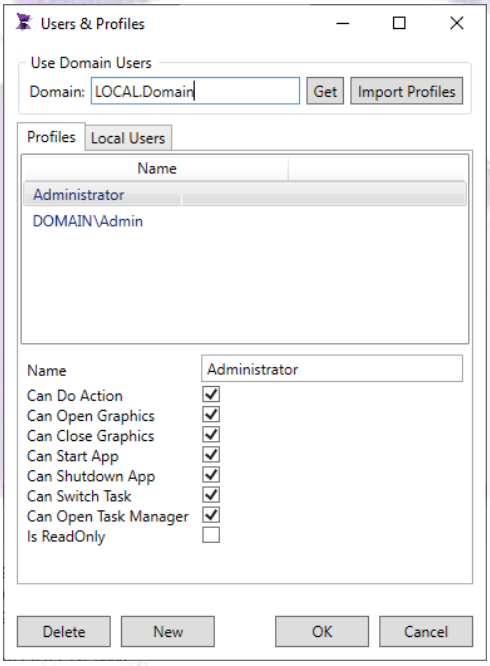
Click the "View" button to see the users associated to that profile. A new window will open. Click "OK" to close the window:



Select one or more profiles that are to be added by checking or unchecking the boxes. Click "OK" when finished.:



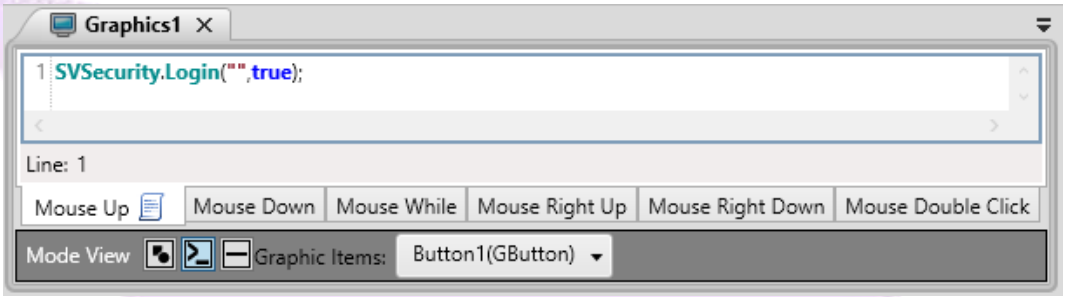
The group will be added and then can be edited like any other profile:



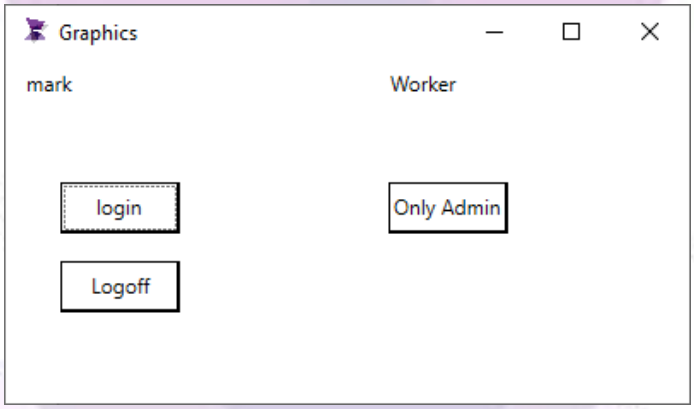
Note: *The local users cannot be associated with a domain profile.*

8.1 Using Domain Users

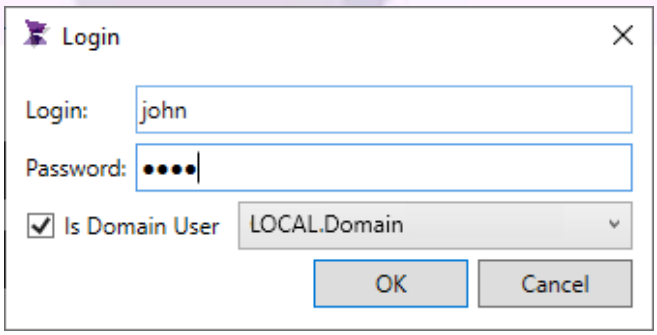
Using the same example from chapter 6, please change the script of the "Login" button to look like this:

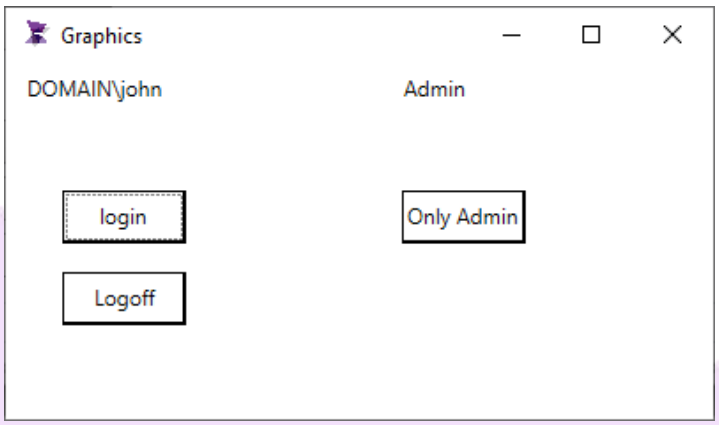


When the Runtime starts and the Graphics1 opens, click the "Login" button:



It will open the "Login" window, please understand this example is different from the last example. The "Login" window has a checkbox to indicate whether or not the user is a Domain user. It also has a combobox with which to choose the user's domain; in this case, we will log in with the "john" user:




Graphics
DOMAIN\john
Admin
login
Only Admin
Logoff