



Slide Show 16:

Security and Tracking



**INSIGHT
AND
OVERVIEW**



Contents

Topic	Description
User Administration	Create users and user groups.
Safe Commands	Secure critical objects with safe commands.
IGSS Audit Trail	Record all user actions in the Audit Trail.

User Administration

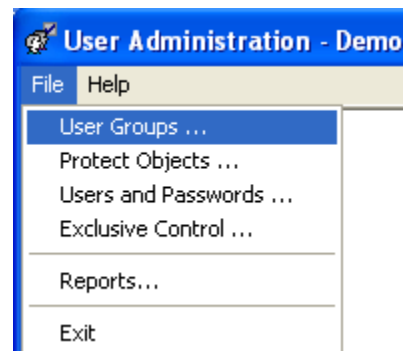


What is User Administration ?

- The User Administration program is the (optional) security module, which can be set up to prevent unauthorized access to the IGSS system
- It consists of three types of security schemes. These are:
 1. **User Groups/Users and Passwords**
 2. **Protect object** - security for individual objects
 3. **Exclusive control** - string for individual PC workstations

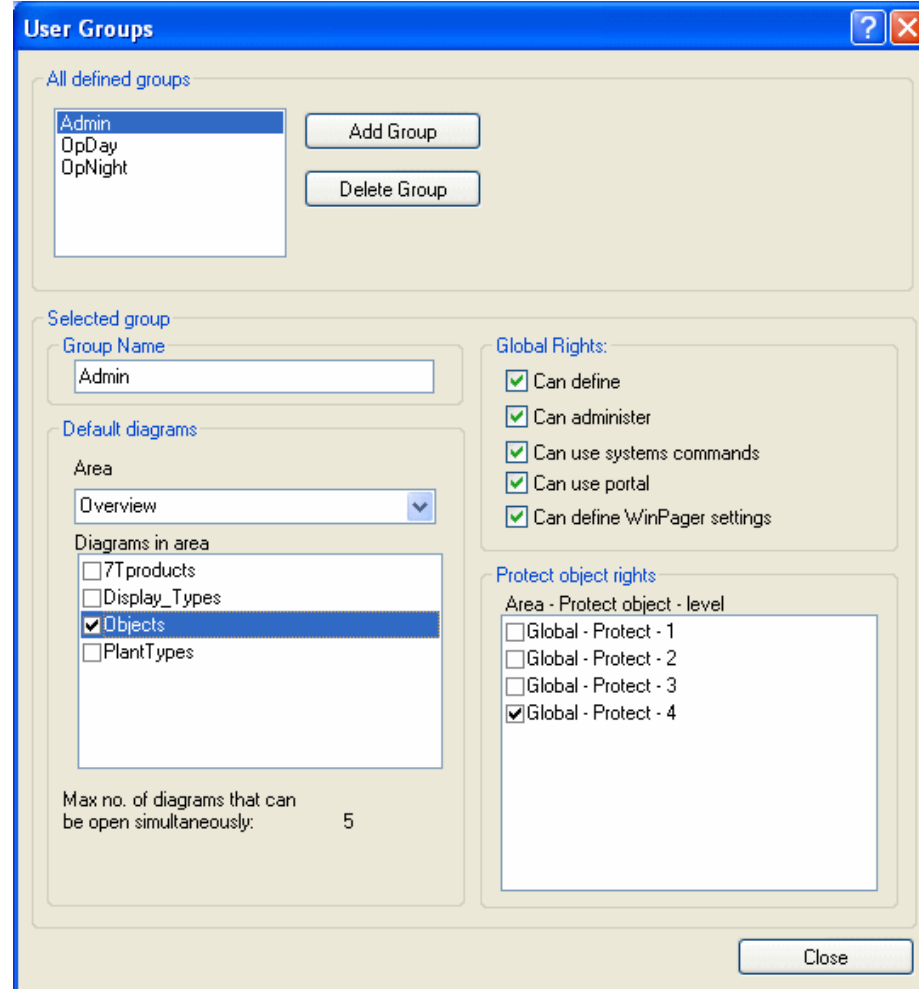
User Groups/Users and Passwords

- The User Administration program is set up for the IGSS configuration/project, which has been selected in the System Configuration program, i.e. the so-called *active configuration*.
- We'll start by looking at the first protection scheme, User Groups/Users and Passwords.



User Groups set-up

- Groups are created one at a time by using the **Add Group** button
 - ▲ A new group is displayed in the **All defined groups** box as a question mark ? followed by 4 digits.
 - ▲ This notation can be overwritten with text by highlighting it and then keying in text in the **Group Name** field.
- **Default diagrams** – select a start-up diagram for each user group.
- **Global Rights** – select one or more rights for each group (next slide).
- **Protect object rights** level can be selected for each user group (later slide).



The screenshot shows the 'User Groups' configuration window. It is divided into several sections:

- All defined groups:** A list box containing 'Admin', 'OpDay', and 'OpNight'. To the right are 'Add Group' and 'Delete Group' buttons.
- Selected group:** A text field containing 'Admin'.
- Default diagrams:** A dropdown menu set to 'Overview'. Below it is a list box 'Diagrams in area' with checkboxes for '7Tproducts', 'Display_Types', 'Objects' (checked), and 'PlantTypes'.
- Global Rights:** A list of rights with checkboxes: 'Can define', 'Can administer', 'Can use systems commands', 'Can use portal', and 'Can define WinPager settings' (all checked).
- Protect object rights:** A list of protection levels: 'Global - Protect - 1', 'Global - Protect - 2', 'Global - Protect - 3', and 'Global - Protect - 4' (checked).
- Max no. of diagrams that can be open simultaneously:** A text field containing the number '5'.
- Close** button at the bottom right.

User Groups: Global Rights

Adminin group (Bob)

OpDay group (Jim)

OpNight group (Pat)

Global Rights:

- Can define
- Can administer
- Can use systems commands
- Can use portal
- Can define WinPager settings

Global Rights:

- Can define
- Can administer
- Can use systems commands
- Can use portal
- Can define WinPager settings

Global Rights:

- Can define
- Can administer
- Can use systems commands
- Can use portal
- Can define WinPager settings

Can define

Can start the **Definition** program, change settings in System Configuration and create/edit Maintenance jobs.

Can administer

Can start the **User Administration** program.

Can use system commands

Can start and stop the configuration. Start/stop of data collection and logging.

Can use portal

Can access the IGSS Internet Portal.

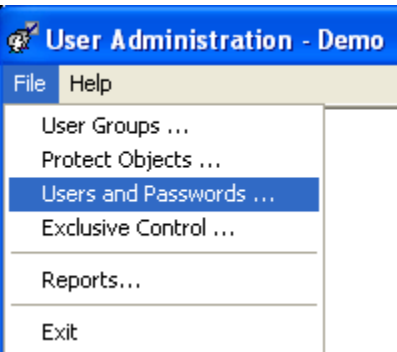
Can define WinPager settings

Can access the WinPager program to create users, change settings, etc.

Users and Passwords



STEP 1:
Click **New User**
to create a new user.



STEP 2:
Enter the user's
details. **Auto logout** will
log the user out after
xx minutes of inactivity; if
necessary, the inactive user
can also be disconnected
from the server (setting in
System Configuration).

The dialog box 'Users and Passwords' contains the following elements:

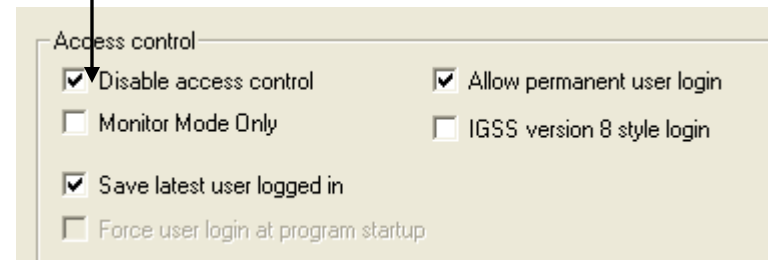
- List of defined Users:** A list box containing 'Bob', 'Jim', and 'Pat'. 'Bob' is selected.
- Buttons:** 'Delete User' and 'New User' are positioned to the right of the list.
- Selected user section:**
 - User ID:** Text box containing '?1000'
 - User name:** Text box containing 'Bob'
 - Password:** Password field with three dots
 - Full name:** Empty text box
 - Auto logout:** Text box with 'Min.' label to its right
 - User group:** Drop-down menu
- Member of groups section:**
 - Text box containing 'Admin'
 - 'Delete from Group' button
 - 'Add to Group' button
 - 'Close' button

STEP 3:
Remember to select a group for
the user in the **User group**
drop-down list
and complete by clicking **Add Group**.

Users and Passwords: set up complete



- The first security scheme has now been set up and can be enabled *without* using the two other schemes:
 - ▲ Protect object
 - ▲ Exclusive control
- To enable security, ***clear*** the check mark for **Disable access control** on the **Access Control** tab in **System Configuration**

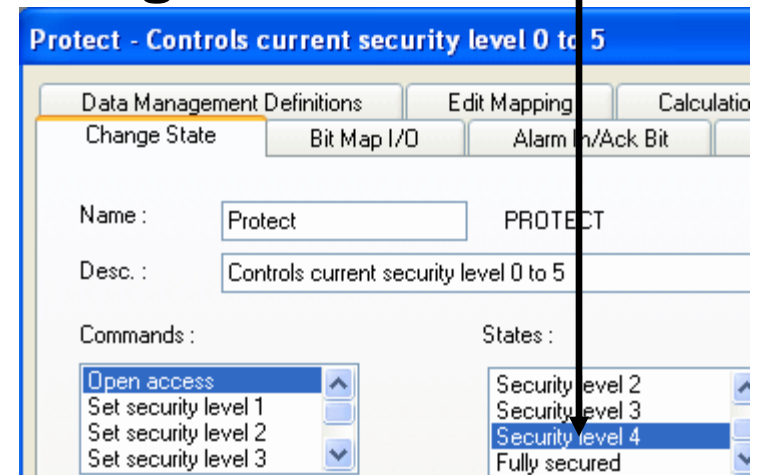
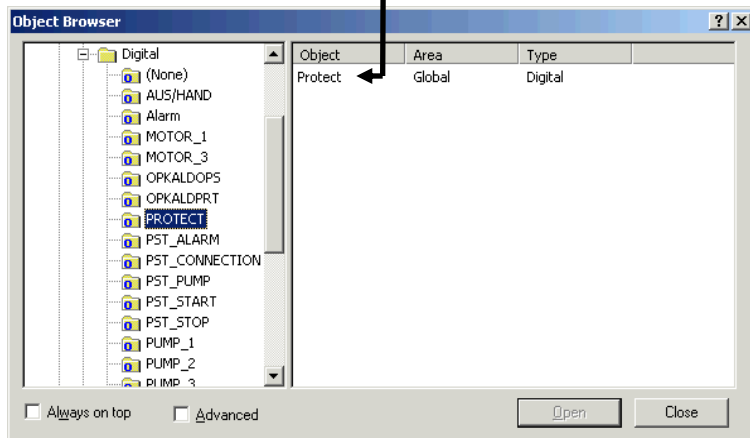


Protect object

- With the completed set up of **User Groups/Users and Passwords** it's now possible to further implement security by using the **Protect object** scheme.
- In addition to preventing unauthorized access to the IGSS system itself, we can also prevent unauthorized access to one or more objects in the IGSS configuration/application.

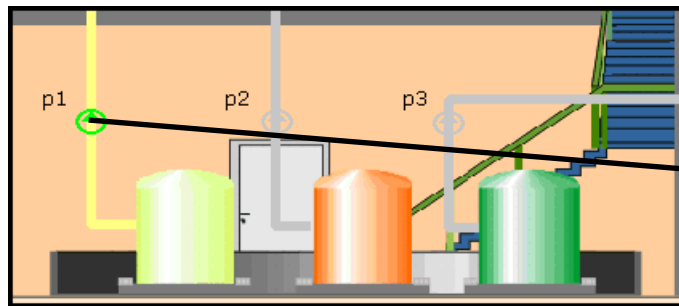
Protect object: setting up (1)

- You must make sure that the **Protect object** is properly set up in the **Definition** program.
- Use **Open by Name...** to call up the **Object Browser** and locate and open the Properties tabs for the object called **Protect**.
- Go to the **Change State** tab and under **States:** select **Security level 4** and click **OK**.
- Remember to **Save** and **Install Configuration**.



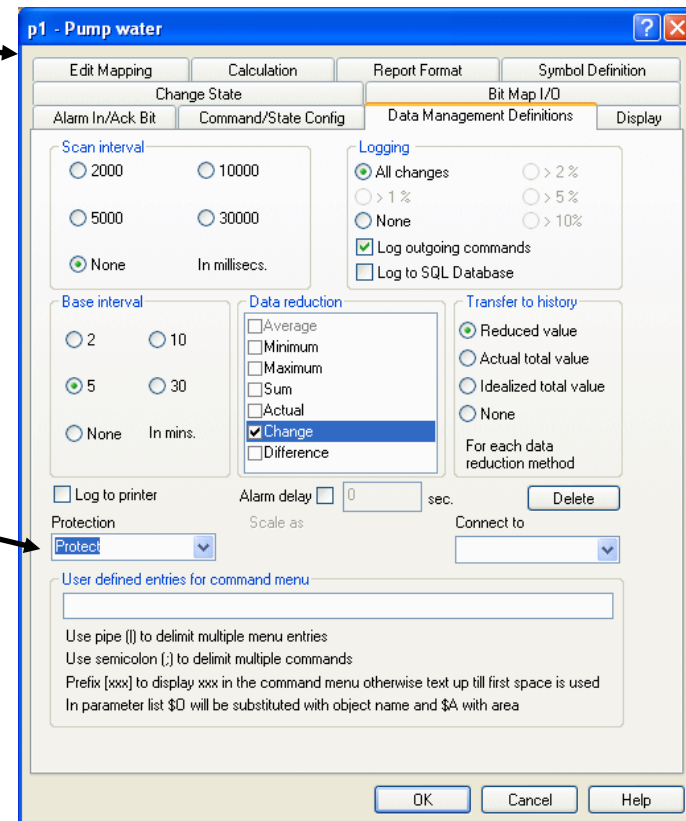
Protect object: setting up in Definition (3)

STEP 1:
Double-click the object symbol.



IMPORTANT:
Only objects that are actively protected are covered by the user administration rights. You can thus choose to leave some objects unprotected.

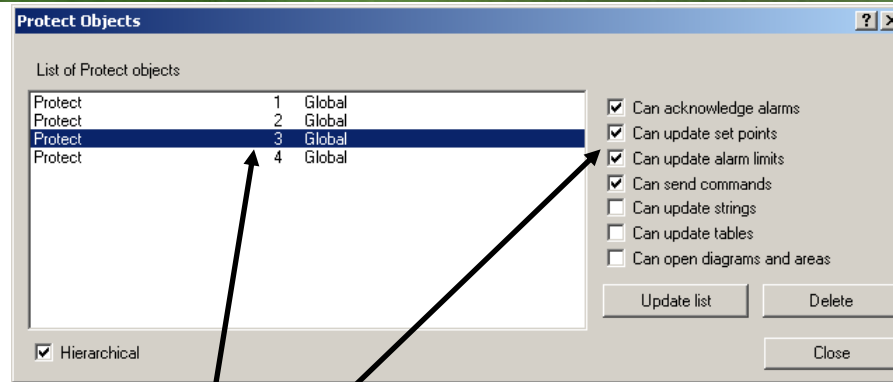
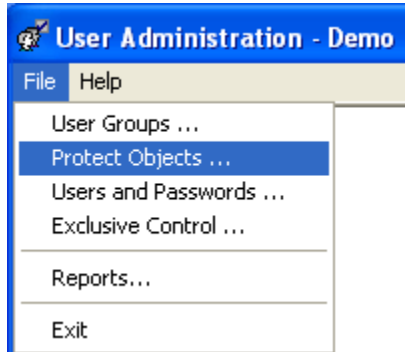
STEP 2:
On the **Data Management Definitions** tab, select the **Protect** object in the **Protection** drop-down list.



The screenshot shows the configuration window for 'p1 - Pump water'. The 'Data Management Definitions' tab is active. The 'Protection' dropdown menu is set to 'Protect'. Other settings include:

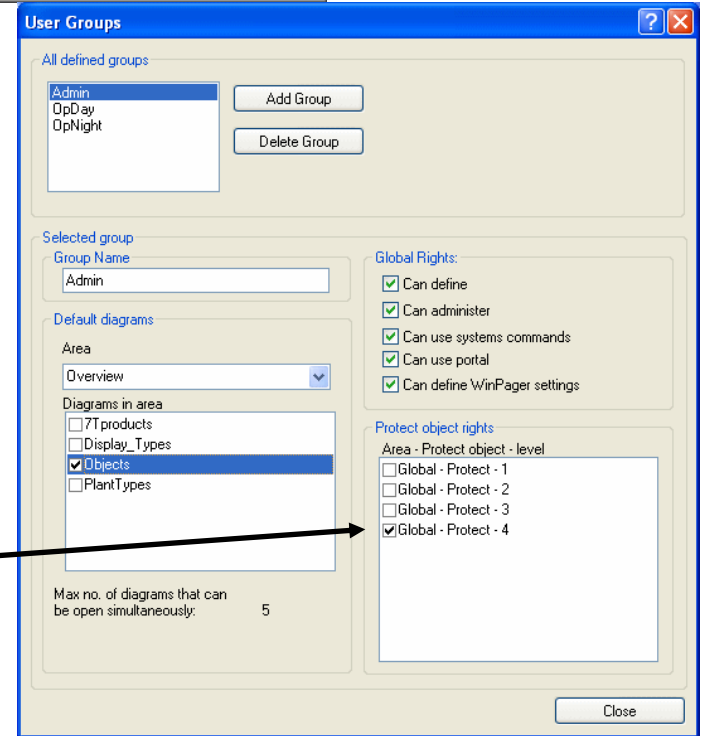
- Scan interval:** 2000 (selected), 5000, 10000, 30000, None. Unit: In milliseconds.
- Logging:** All changes (selected), > 1%, > 2%, > 5%, > 10%, None, Log outgoing commands (checked), Log to SQL Database (unchecked).
- Base interval:** 2, 5 (selected), 10, 30, None. Unit: In mins.
- Data reduction:** Average, Minimum, Maximum, Actual, Change (checked), Difference.
- Transfer to history:** Reduced value (checked), Actual total value, Idealized total value, None.
- Log to printer:** unchecked.
- Alarm delay:** 0 sec.
- Scale as:** (empty)
- Connect to:** (empty)

Protect Objects menu

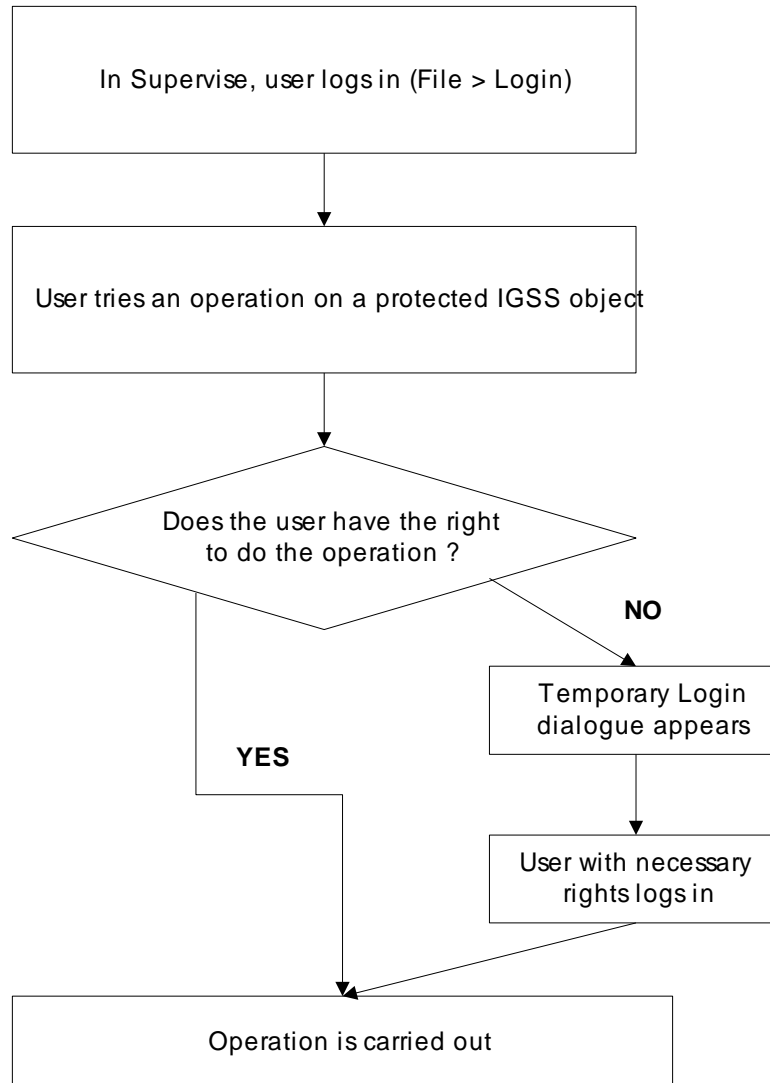


Protect Objects dialog box:
User group rights are defined here.
For each level select the rights to allocate.

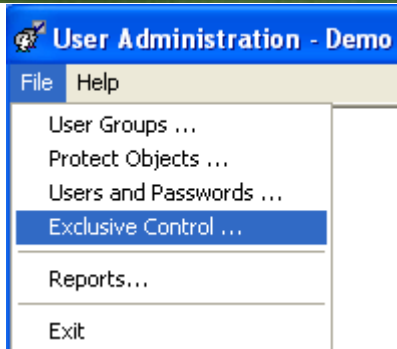
In **User Groups**, the appropriate security level is assigned to each user group by selecting the level under **Protect object rights**



User Administration enabled and Protect object used: How it works



Exclusive Control scheme



What is Exclusive Control ?

The use of **Exclusive Control** allows system designers to set up this security scheme on one or more workstations. The objects in the configuration that have the Protect object attached are then controlled only from a workstation set up with the exclusive control feature.

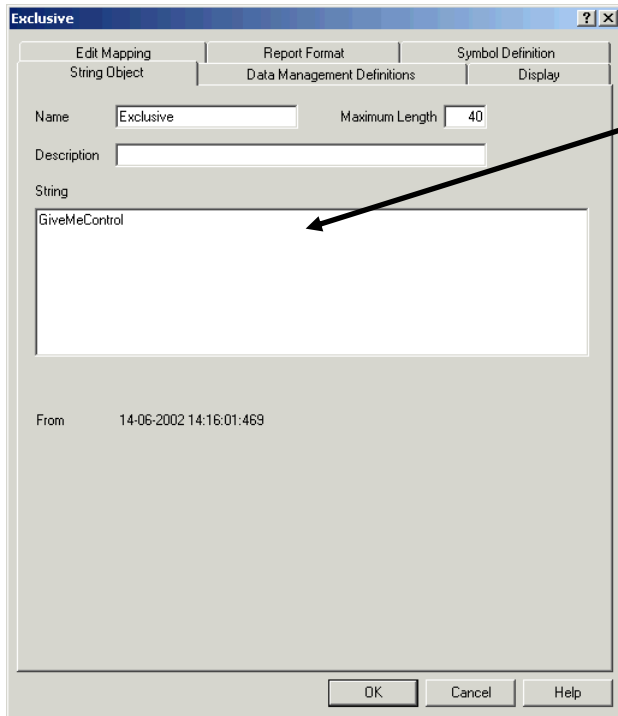
Technically, linking a string object to a Protect object accomplishes this. The feature can be used on multiple workstations, each controlling their own collection of objects. For this purpose, multiple Protect objects have to be created.

Why Exclusive Control ?

Exclusive Control adds an extra “layer” of security to the system. Controlling objects in the IGSS configuration, which have been bound to the special Protect object, is now limited to a specific workstation/PC in the network.

NOTE: The use of Exclusive Control assumes the use of the two other security schemes, i.e. **User Groups/Users and Passwords** and **Protect Objects**.

Defining exclusive control



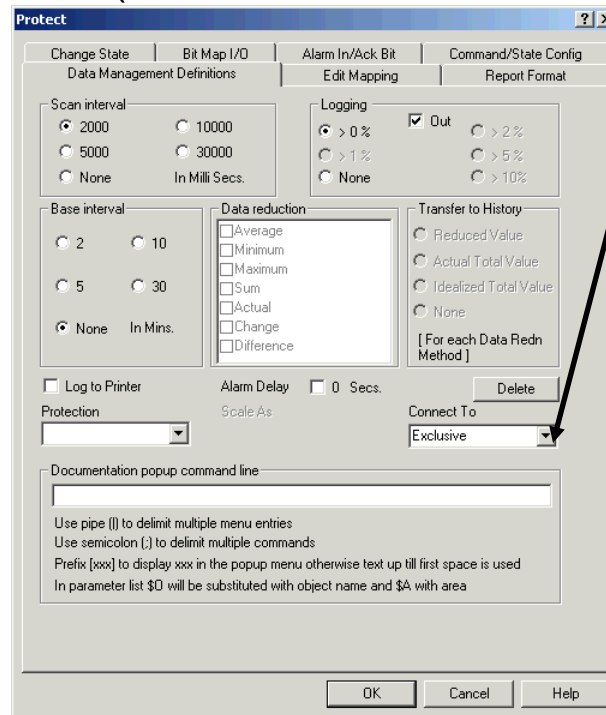
The 'Exclusive' dialog box is shown with the following fields:

- Name: Exclusive
- Maximum Length: 40
- Description: (empty)
- String: GiveMeControl
- From: 14-06-2002 14:16:01.469

Buttons: OK, Cancel, Help

STEP 1:

Define a string object and type the string that gives exclusive control (here it is "GiveMeControl")



The 'Protect' dialog box is shown with the following settings:

- Scan interval: 2000
- Logging: > 0% (checked), Out (checked)
- Base interval: None
- Data reduction: (empty)
- Transfer to History: (empty)
- Connect To: Exclusive

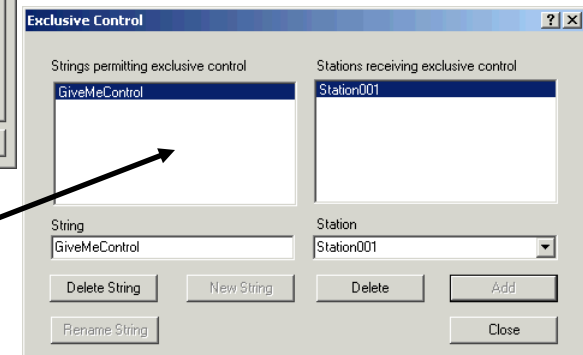
Buttons: OK, Cancel, Help

STEP 2:

Link the string object to the Protect object by choosing its name in the "Connect To" drop-down list.

STEP 3:

In User Administration, map the string to the relevant workstation(s)

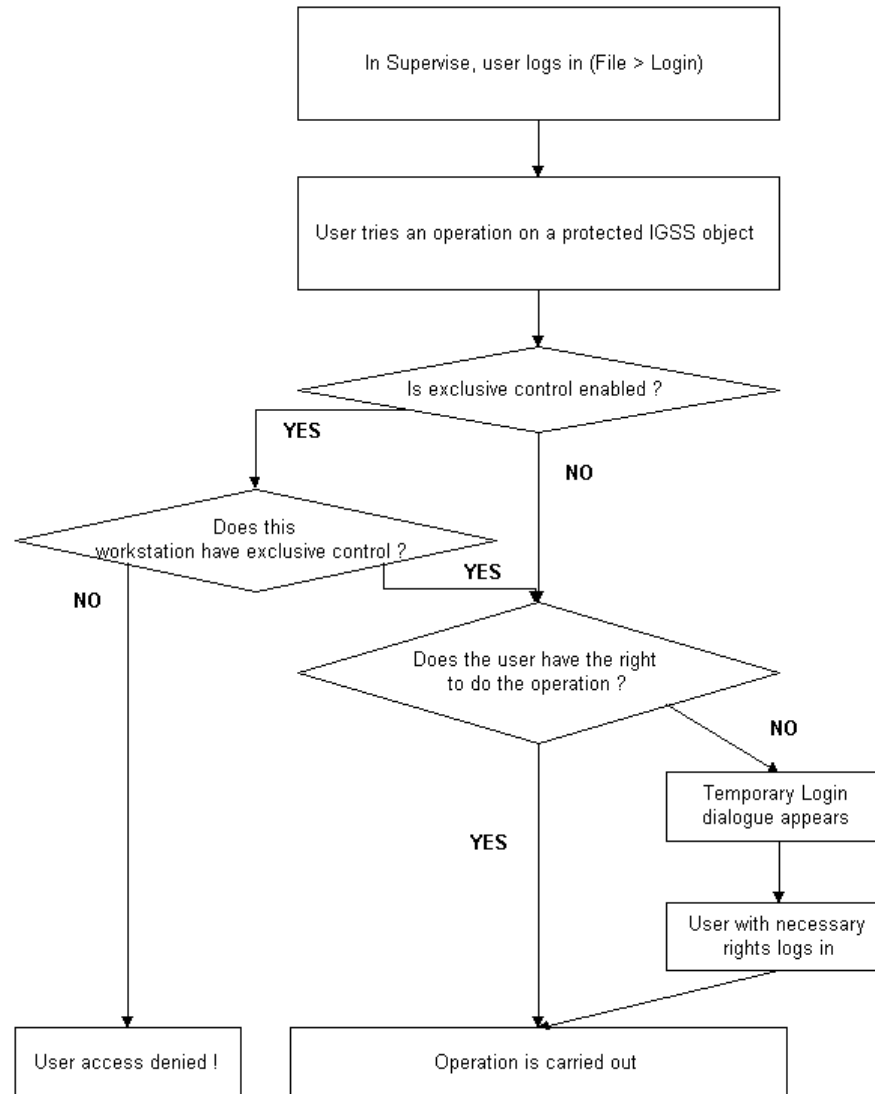


The 'Exclusive Control' dialog box is shown with the following settings:

- Strings permitting exclusive control: GiveMeControl
- Stations receiving exclusive control: Station001
- String: GiveMeControl
- Station: Station001

Buttons: Delete String, New String, Delete, Add, Rename String, Close

Exclusive control in Supervise



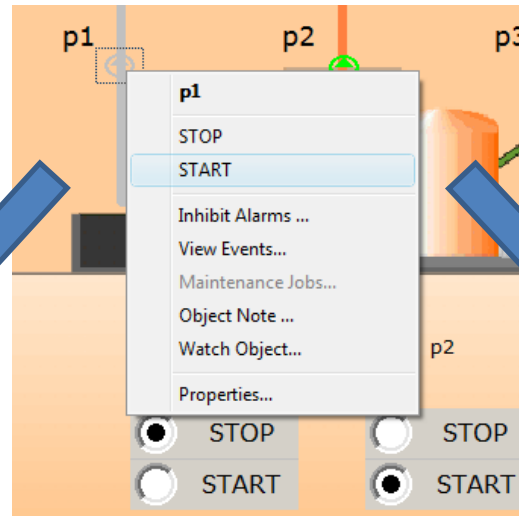
Student Exercise

Do Exercise 11 in the Exercise booklet.

When finished with the exercise, you should test your results by starting the IGSS Demo configuration and logging on and off as the different operators, you created in the exercise.

Safe Commands

Safe Commands - Supervise



Before IGSS 8

Command was
executed immediately.

After IGSS 8

Command can be
set up to be a safe
command.

Three types of safe commands

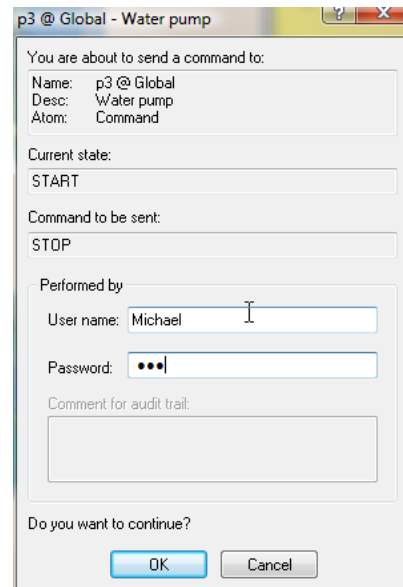
Confirm



A screenshot of a dialog box titled "p1 @ Global - Pump water". It contains the following fields: "Name: p1 @ Global", "Desc: Pump water", "Atom: Command", "Current state: START", "Command to be sent: START", and a "Comment for audit trail:" text area. At the bottom, it asks "Do you want to continue?" with "OK" and "Cancel" buttons.

User must confirm by clicking OK.

Confirm password



A screenshot of a dialog box titled "p3 @ Global - Water pump". It contains the following fields: "Name: p3 @ Global", "Desc: Water pump", "Atom: Command", "Current state: START", "Command to be sent: STOP", "Performed by" section with "User name: Michael" and "Password: ..." fields, and a "Comment for audit trail:" text area. At the bottom, it asks "Do you want to continue?" with "OK" and "Cancel" buttons.

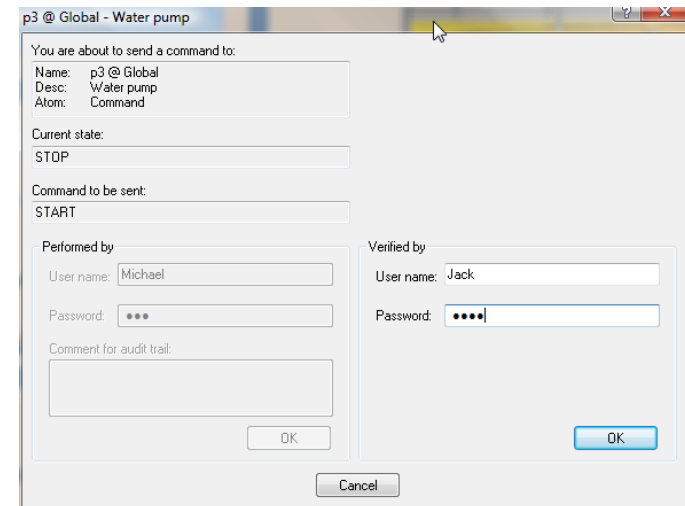
User must with user name and password.

NOTE:

Confirm password and **Confirm 2 users** only make sense, if you have user administration enabled.

Objects can be protected both with Protect and Safe Commands.

Confirm 2 Users

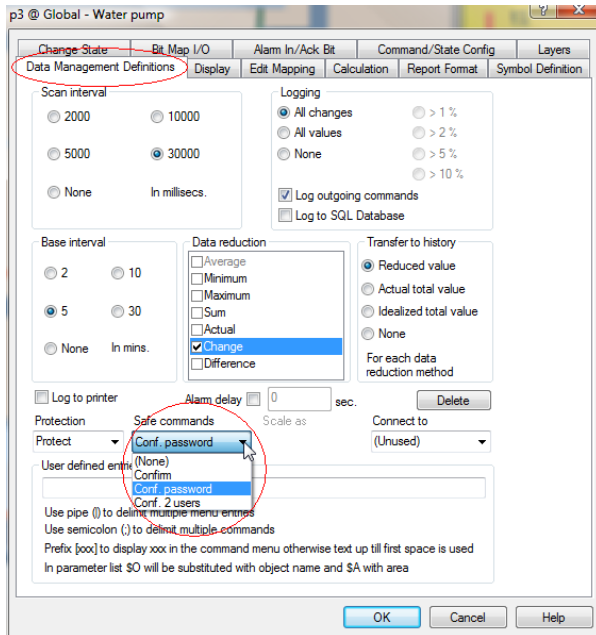


A screenshot of a dialog box titled "p3 @ Global - Water pump". It contains the following fields: "Name: p3 @ Global", "Desc: Water pump", "Atom: Command", "Current state: STOP", "Command to be sent: START", "Performed by" section with "User name: Michael" and "Password: ..." fields, and a "Verified by" section with "User name: Jack" and "Password: ..." fields. At the bottom, it asks "Do you want to continue?" with "OK" and "Cancel" buttons.

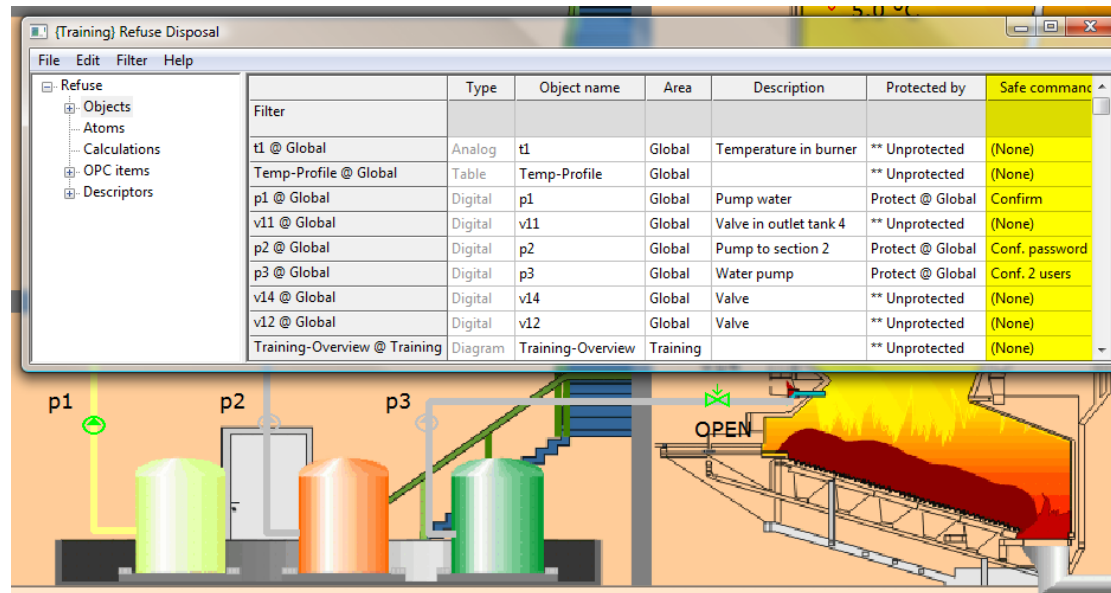
Two users must confirm with their user names and passwords.

Safe Commands in Definition

Can be set on the individual object ...



... or using Property Table View

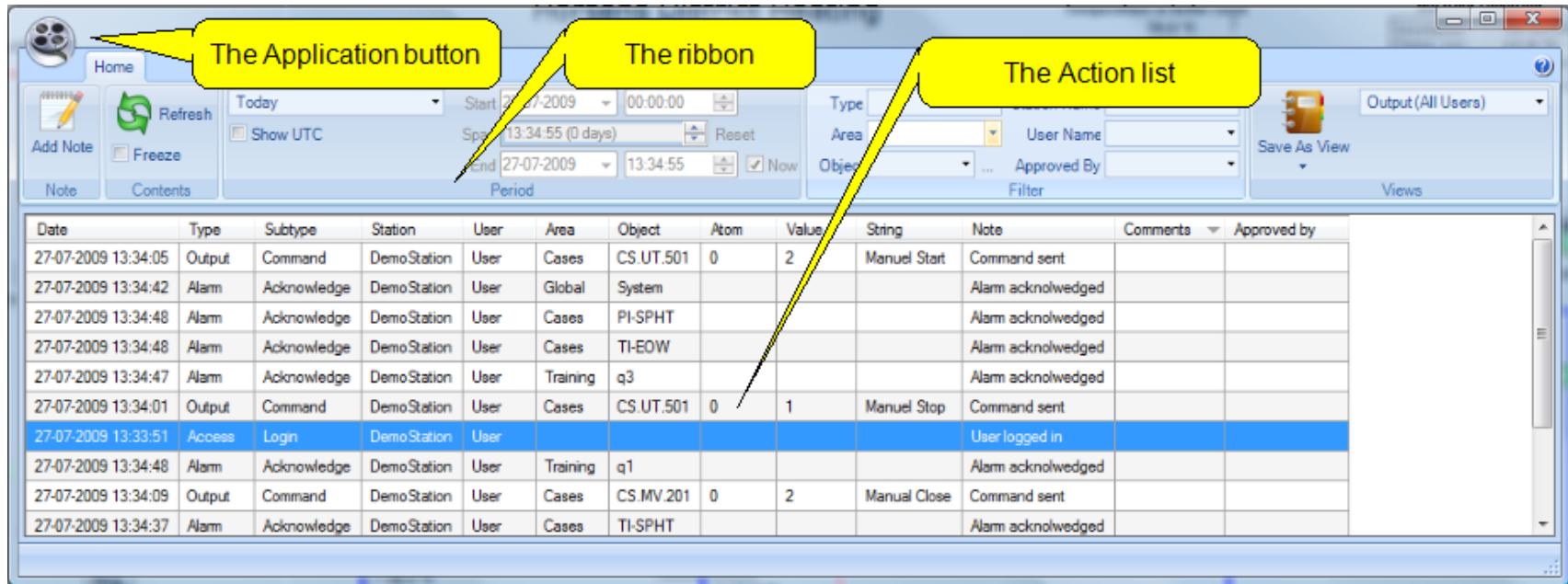


Filter	Type	Object name	Area	Description	Protected by	Safe command
t1 @ Global	Analog	t1	Global	Temperature in burner	** Unprotected	(None)
Temp-Profile @ Global	Table	Temp-Profile	Global		** Unprotected	(None)
p1 @ Global	Digital	p1	Global	Pump water	Protect @ Global	Confirm
v11 @ Global	Digital	v11	Global	Valve in outlet tank 4	** Unprotected	(None)
p2 @ Global	Digital	p2	Global	Pump to section 2	Protect @ Global	Conf. password
p3 @ Global	Digital	p3	Global	Water pump	Protect @ Global	Conf. 2 users
v14 @ Global	Digital	v14	Global	Valve	** Unprotected	(None)
v12 @ Global	Digital	v12	Global	Valve	** Unprotected	(None)
Training-Overview @ Training	Diagram	Training-Overview	Training		** Unprotected	(None)

IGSS Audit Trail



The Audit Trail window



The screenshot shows the Audit Trail window interface. Three yellow callout boxes point to specific features:

- The Application button:** Points to the application icon in the top-left corner.
- The ribbon:** Points to the ribbon menu at the top, which includes sections like 'Home', 'Note', 'Contents', and 'Views'.
- The Action list:** Points to the main data table below the ribbon.

Date	Type	Subtype	Station	User	Area	Object	Atom	Value	String	Note	Comments	Approved by
27-07-2009 13:34:05	Output	Command	DemoStation	User	Cases	CS UT.501	0	2	Manuel Start	Command sent		
27-07-2009 13:34:42	Alarm	Acknowledge	DemoStation	User	Global	System				Alarm acknowleged		
27-07-2009 13:34:48	Alarm	Acknowledge	DemoStation	User	Cases	PI-SPHT				Alarm acknowleged		
27-07-2009 13:34:48	Alarm	Acknowledge	DemoStation	User	Cases	TI-EOW				Alarm acknowleged		
27-07-2009 13:34:47	Alarm	Acknowledge	DemoStation	User	Training	q3				Alarm acknowleged		
27-07-2009 13:34:01	Output	Command	DemoStation	User	Cases	CS UT.501	0	1	Manuel Stop	Command sent		
27-07-2009 13:33:51	Access	Login	DemoStation	User						User logged in		
27-07-2009 13:34:48	Alarm	Acknowledge	DemoStation	User	Training	q1				Alarm acknowleged		
27-07-2009 13:34:09	Output	Command	DemoStation	User	Cases	CS MV.201	0	2	Manuel Close	Command sent		
27-07-2009 13:34:37	Alarm	Acknowledge	DemoStation	User	Cases	TI-SPHT				Alarm acknowleged		