User Administration User Guide
IGSS Version 9.0

Contents

Chapter 1: Welcome to User Administration

1.1 What is IGSS User Administration ?

Definition and use

The **User Administration** is used by the system administrator to administer the rights of the individual users of a specific IGSS configuration.

To provide an overview of the rights assigned in the application, a number of overview reports can be shown on-screen or printed.

The application also allows the system administrator to assign exclusive control to a specific work-station. This is practical, if all other users are to be barred from manipulating certain IGSS objects.

How it works

Basically, User Administration builds on a four-step process:

1. The system administrator and plant management plan the number of user groups, determine their appropriate rights and specify which IGSS objects in the configuration are be protected against unauthorised use.

2. The system administrator creates the users of a given configuration by assigning user names and passwords to personnel responsible for process surveillance. The system administrator also creates the user groups to be used in the configuration. Only through membership of one or more user groups are individual users allocated the rights necessary to perform their surveillance and control functions.

3. The system designer opens the configuration and attaches the IGSS system's built-in "Protect object" to the IGSS objects that must be protected and installs the configuration.

4. An operator logs into the system using his user name and password and his rights are checked against those set up for him in User Administration.

This Help file contains detailed descriptions and procedures for these basic steps.

1.2 Key features and benefits

Introduction

This topic gives you an overview of the key features and benefits of the User Administration application. These are presented on the basis of the application's five main menu items presented in the following.

User groups

The user group is the central element in User Administration. An individual user's rights are always dependent on his membership of one or more user groups. This is where you start when you set up user administration for a specific configuration. Note that the specific rights for the users of a user group are defined in the **Protect Objects** dialog box. The user group simply subscribes to a certain Protect object at one or more security levels and thus inherits the rights defined for the particular Protect object.

This feature ...	Allows you to ...
User group	Assign rights to a user group instead of the individual user. You can thus create a user profile for a number of users. Later, the users are assigned to the individual user groups.
Global rights	Assign global rights to the user group, for example, the right to use the **Definition** and **User Administration** programs. **Important:** At least one user group and one user must have administrator's rights, otherwise access to the **User Administration** program is denied.
Protect objects	Assign Protect objects to user groups to allow member users to manipulate the IGSS objects in the configuration that were protected with this object. The rights attached to a Protect object are defined in the **Protect Objects** dialog box.

Protect objects

The "Protect objects" feature can be used to prevent unauthorised use or manipulation of any object in the configuration. For this purpose, there is a predefined IGSS system object called **Protect**. For each IGSS object for which general access is to be denied, the predefined Protect object is attached. Areas, diagrams and graphs, which are also considered objects in IGSS, can get their Protect object assigned from their respective Properties dialog boxes. For other types of IGSS objects (typically process components) this is done on the **Data Management Definitions** tab.

When the protection feature is implemented in the configuration, the system administrator defines the rights that must apply to each Protect object at the four different security levels available in the system. The enabled rights are the ones that can be used by users in a user group that subscribe to this Protect object.

This feature ...	Allows you to ...
Security levels	Differentiate between different types of users. For example, you can use Level 1 for thze users with the lowest number of rights in the system, Level 2 for users with the second-lowest number of rights, etc. Security level 4 is the highest security level and level 1 is the lowest.
Hierarchical option	Overcome the difficulty in setting the Protect object to the appropriate security level. When the option is checked, the selected security level automatically inherits the rights of the next lower level (for example, level 4 inherits the rights of level 3). If you check this option for security levels 4, 3 and 2, you can set the security level of the Protect object in the configuration to **4** and all users can log into the system and get their rights checked properly. If you do not use this option, you must make sure that the security level is set to the appropriate number.
Specific rights for a user	Enable or disable the individual rights you want users of a particular user group to have. You may, for example, want to allow users on the day shift to be able to update alarm limits whereas the night shift users should not have

	this right.

Users and passwords

Defining new users in the system and assigning user names and passwords is an easy task.

This feature ...	Allows you to ...
User name and password	Easily identify and verify each user in the system and know what his rights are via his membership in one or more user groups.
Assign users to user groups	Easily include new users in appropriate user group(s) without having to define all their rights individually.
Full name	Uniquely identify each user in a large system with numerous users. When you generate the user report, you will also see the full names of all users on the system.
Auto logout	Specify a number of minutes of user inactivity before the user in question is automatically logged out. This provides a kind of "dead man's button" functionality. To re-enter after being automatically logged off, the user simply logs in again with user name and password.

Exclusive control

At times, the system administrator or another privileged user needs to have exclusive access to specific objects in the configuration. This is achieved by assigning exclusive control to one or more workstations in the system.

This feature ...	Allows you to ...
Strings	Create and name string objects in the configuration that are protected. You can then link these strings to specific workstations.
Workstations	Select the workstation(s) you want to exercise exclusive control of specific objects in the configuration.

Reports

When the system administrator has set up the desired user administration matrix, he will in many cases need an overview of his definitions. This is accomplished through the built-in report function, which can generate both on-screen and printed reports.

This feature ...	Allows you to ...
User group report	View the names of the users in the group, which Protect objects the group subscribes to and which global rights its users have.
Protect object report	View the rights defined for each security level of the Protect objects used and get a list of all IGSS objects in the configuration that are protected with this object.
User report	View details for each individual user including user name and password, membership of user group(s) and which global rights the user has.

Chapter 2: The Workflow in User Administration

2.1 Overview: The complete workflow

This topic gives you an overview of the four main phases in user administration. You can click on each phase for further details.

STEP 1: Planning administration of users

- **Who's responsible:** System administrator

- **Summary:** Schedule a meeting where the system administrator, the system designer and operator representatives are invited. The purpose of the meeting is to organise the user groups and members, assign the appropriate rights and identify the IGSS objects that must be protected in the configuration.

STEP 2: Setting up user administration

- **Who's responsible:** System administrator

- **Summary:** Open the User Administration program and use the documentation from the planning meeting to implement your decisions. During this phase, user groups are created, their rights are chosen and individual users are included in the relevant user groups.

STEP 3: Protecting objects in the configuration

- **Who's responsible:** System designer

- **Summary:** Open the **Definition** program and assign the Protect object to each of the IGSS objects agreed upon during the planning phase. The designated Protect object is attached to each ordinary object in the configuration you want to protect. The Protect object itself is then set to the desired state, and finally, you install the configuration.

STEP 4: Testing user administration

- **Who's responsible:** System administrator/system designer

- **Summary:** Open the IGSS Starter program and start the configuration in the **Supervise** program. Log in using the user names and passwords set up in User Administration and test for the desired result. Try different operations on a protected object, for instance sending commands. Try the same on an unsecured object to verify that unauthorized access, in fact, is prevented.

2.2 How user administration works during supervision

Login/logout

Before the operator starts supervising the process, he must log in by selecting **File** → **Login** and then type his user name and password. At the end of a work shift, the operator logs out by selecting **File** → **Logout**.

Access control

Once an operator is logged in, IGSS monitors all operations attempted by the operator to verify that he has the necessary rights to carry them out. In case he does not have the right to carry out a particular operation, for example send a command, the system will then call up the **Temporary Login** dialog box. When this occurs, it indicates that the current user does not have the required right for the operation in question, and therefore asks for another user with the necessary right to log in and carry out the operation.

Graphical overview

The flowchart below shows how user administration works during supervision.

> **Tip:** If you are using exclusive control, the flow is different, click here for details.
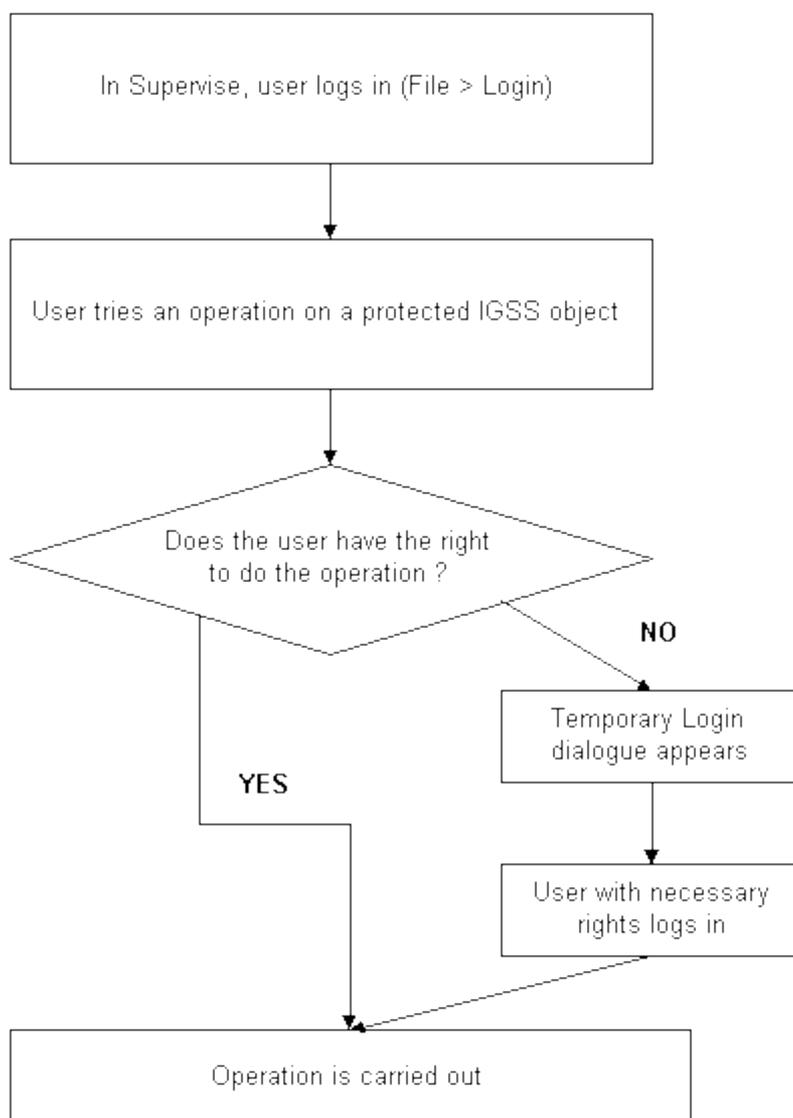
2.3 Example: Create three user groups and protect IGSS objects

What we want to do

> If you want to try out this example, use the **Demo** configuration that comes with your IGSS installation.

In this example, we want to create three user groups with different user privileges in the system.

- **Admin** group members are system administrators or superusers
- **Day** group members are operators on the day shift
- **Night** group members are operators on the night shift

In the **Demo** configuration, we will protect a few pumps and flow gauges to see how user administration actually works.

STEP 1: Define user groups and rights

Define the three user groups with the following rights:

Show Me

User group ...	Has the following rights ...
Admin	- All global rights. - Add **Protect,** state **4** - In the **Protect Objects** dialog box, enable all rights for state **4** and enable the **Hierarchical** option.
Day	- No global rights (they must not use Definition or User Administration or start and stop configurations) - Add **Protect**, state **2** - In the **Protect Objects** dialog box, enable the following rights for state **2** and enable the **Hierarchical** option: **Can acknowledge alarms**, **Can update set points**, **Can update alarm limits** and **Can send commands**.
Night	- No global rights (they must not use Definition or User Administration or start and stop configurations) - Add **Protect**, state **1** - In the **Protect Objects** dialog box, enable the **Can acknowledge alarms** right for state **1** and enable the **Hierarchical** option.

Note: Because we want to use the **Hierarchical** option, we must also enable it for level **3**.

STEP 2: Define users and passwords

Show Me

The last thing to do in User Administration is to include the relevant users in the above groups. To simplify the example, we will only include one user in each group. For each user, select the group name in the drop-down list and click **Add Group**.

- **Admin** User name: John — Password: John
- **Day** User name: Bob — Password: Bob
- **Night** User name: Kent — Password: Kent

Close the User Administration program.

STEP 3: Protect the objects in the configuration

`Show Me`

We want to protect the following objects:

- **p1**, **p2** and **p3**

- **q1**, **q2** and **q3**

Select **Edit → Open by Name** and select one of the above objects, click the **Data Management Definitions** tab in the properties dialog box and select **Protect** in the **Protection** drop-down list. Repeat for all the objects.

STEP 4: Set the state of the Protect object

`Show Me`

The last thing we need to do before installing, is to set the security level state of the **Protect** object that we used to protect the pumps and flow gauges with.

Select **Edit → Open by Name** and find the **Protect** object. Click the **Change State** tab and set its current security level state to **4**.

Tip: Because we want to use the **Hierarchical** option, we set it to **4** and this ensures that all users will be checked against their relevant rights, no matter what security level they subscribe to.

If, for some reason, we want to limit the access to protected objects to a certain user group, we can set the state of the **Protect** object to the security level that the group subscribes to and then disable the **Hierarchical** option. In our example, only the **Admin** group would have access if we set it to security level **4**.

STEP 5: Install the configuration

When we have protected the relevant objects and set the state of the **Protect** object, we only need to install the configuration to apply the changes.

STEP 6: Log into Supervise and test

Launch the **IGSS Starter** program and click the **Supervise** button. Log in as a night shift user (Kent) and try to send a command to one of the protected pumps (**P1**, **P2** or **P3**). If everything is set up correctly, the **Temporary Login** dialog box will appear, indicating that the user does not have the right to carry out this operation. Now, log in as a day shift user instead (Bob). The command is now executed.

Chapter 3: Planning and Setting Up A-Z

3.1 Planning user administration

1. Schedule a meeting where all parties involved in the user administration setup are invited. This would typically be the system administrator, the system designer, the plant manager and operator representatives.

2. Try to answer the following questions:

    - how many user groups must be defined ?

    - which users go into which user groups ?

    - which rights must be assigned to each user group ?

    > You can print screen shots from the User Administration program to see which rights you can assign to the users. Simply find the screen you want to capture, press ALT + PRINT SCREEN to copy it to the clipboard and then paste it into an application from which you can print it.

3. Document the results of the meeting on paper. This will make it much easier for the system administrator to implement the decisions.

3.2 Setting up user administration

1. Define the relevant user groups and assign the appropriate user rights by assigning Protect object security levels.

    » How?

    > **Tip:** At least one user group must have administrator's rights.

2. Select the relevant user rights for each security level used.

    » How?

3. Define the individual user and assign him to a user group.

    » How?

4. Print the three report types to get an overview and verify what you have defined.

   ⏩ How?

3.3 Protecting objects in the configuration

1. In the **Definition** program, open the configuration in which you want to protect IGSS objects.

2. Click here and follow the procedure.

3.4 Testing user administration

1. In the **Supervise** program, select **File → Login**. The **Login** dialog box appears.

2. Type your user name and password and click **OK**.

Result: The rights assigned to your user group now apply.

3. To log out and let a new operator log in, select **File → Logout** and let the new operator perform step 1 of this procedure.

> If you try to perform an operation that you are not allowed to, the **Temporary Login** dialog box appears. Another user with the necessary rights can then log in and perform the operation.

Chapter 4: User Groups

4.1 User groups

What is a user group?

A user group represents a user profile which includes a set of rights defined for a particular group of users.

Two types of rights can be defined for a user group:

- **Global rights** which apply globally and are not linked to specific IGSS objects in the configuration
- **Specific rights** which apply to IGSS objects that have been protected from unauthorised use

See details about the two types of rights below.

When appropriate rights have been attached to user groups, the individual users are simply assigned to a group which contains the rights necessary for the performance of their duties and responsibilities.

Global rights

Three global rights can be enabled or disabled for each user group, as follows:

Global right	Definition
Can define	allows the user to start the **Definition** program and modify the configuration, change options in the **System Configuration** program, define and edit maintenance jobs.
Can administer	allows the user to use the **User Administration** program.
Can use system commands	allows the user to use system commands like starting and stopping the configuration, starting and stopping data collection and logging.
Can use portal	allows the user to log into the **IGSS Internet Portal**
Can define Winpager settings	allows the user to make changes in the **Winpager** program.

Usually, only system designers should have the right to use the **Definition** program, only system administrators should have the right to use the **User Administration** program and only certain privileged users should be allowed to start and stop a configuration.

Tip: You can also disable the right to use the **Definition** program by enabling the **Disable Definition** option in the **System Configuration** program.

Specific rights on protected objects

Beside the above global rights, a set of specific rights that apply to all IGSS objects that are protected in the configuration can be defined. They are assigned to the user group by adding a Protect object at a certain security level (1 - 4). Each security level has a specific set of rights enabled. These rights are defined in the **Protect Objects** dialog box. Click here for further information.

Important: These rights only apply to IGSS objects that are protected in the configuration.

The Users Groups dialog box

To define or edit user groups, select **File → User Groups**. The following dialog box appears.
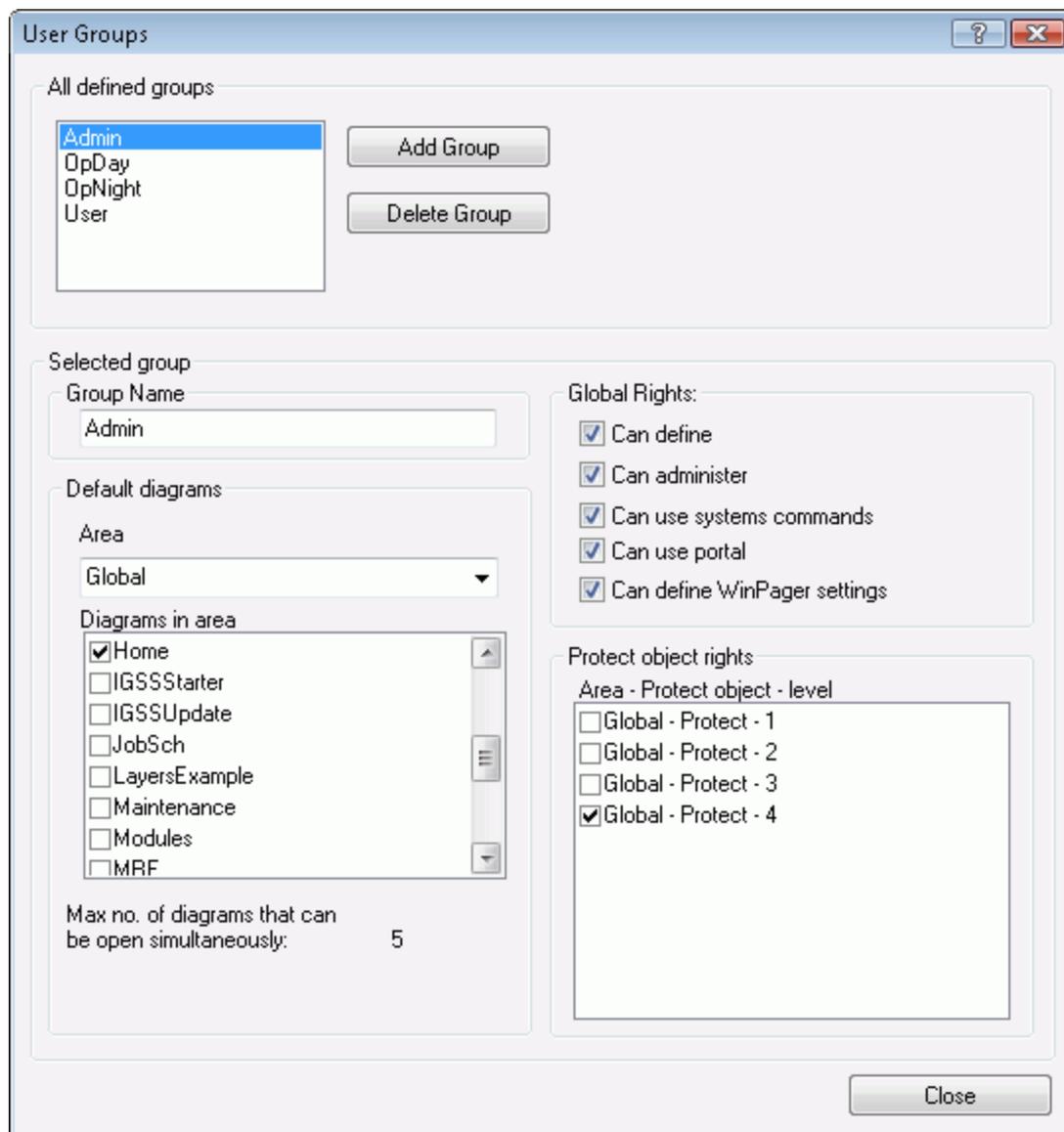
For an explanation of the individual items in the dialog box, click the ❓ in the upper right hand corner of the dialog box, and then click on top of the item you want information about.

4.2 Creating a user group

1. Select **File → User Groups**.

2. Click **Add Group**. A number appears in the group list and in the group name box.

3. Type the name of the new user group in the box.

4. Enable the global rights you want to assign to the user group by checking the corresponding boxes.

5. In the **Protect object rights** section, select the security level(s) that define the rights of the users in this group.

6. Click **Close** to save your changes and close the dialog box.

> To view the user rights associated with each security level, open the **File** menu and select **Protect Objects**.

4.3 Removing a user group

1. Select **File → User Groups**. The **User Groups** dialog box appears.

2. Select the name of the user group you need to remove.

3. Click **Delete Group**.

4. Click **Close** to save your changes and close the dialog box.

> Remember to move any users from the user groups you remove to another valid group.

Chapter 5: Protect Objects

5.1 Assigning security level(s) to a user group

1. Select the user group.

2. In the **Protect object rights** section, select the relevant security level(s). For each security level, a set of user rights are defined.

3. Repeat steps 1 and 2 for all user groups.

4. Click **Close** to save your changes and close the dialog box.

> If you do not see any Protect objects in the **All defined Protect objects** group, you need to refresh the list. Close the **User Groups** dialog box, then open the **Protect Objects** dialog box and click **Update List**. You should now see all defined Protect objects and security levels in the list. Reopen the **User Groups** dialog box and continue.

5.2 Assigning user rights to security levels

The next step is to assign the appropriate user rights for each security level. One or more security levels are assigned to each user group. The individual user will thus have the user rights enabled for the security level(s) that are assigned to his user group.

Important: 7T recommends setting the Protect object to **Security level 4** and using the **Hierarchical** option to activate all four security levels. This topic describes the recommended procedure.

> The rights you enable are **not global**, they only apply to IGSS objects which are protected in the configuration.

1. In the **File** menu, choose **Protect Objects**.

2. If all defined Protect objects are not visible in the list, click **Update List**.

3. Select security level 4 and select the appropriate rights for that level.

4. Select the **Hierarchical** check box (see below).

5. Repeat steps 3 – 4 for security level 3, 2 and 1.

> Make sure that the **Hierarchical** check box is selected for all security levels.

6. Click **Close** to save your changes and close the dialog box.

Hierarchical option

Check this box to inherit the rights defined for the next lower level. For example, if you check it for level 2, the rights from level 1 are inherited.

The option also allows a user to use a protected object, although he does not subscribe to the current protection level (1,2,3 or 4). Assuming that the protection level is set to 4 (in **Definition**) and **Hierarchical** is enabled for 4 and 3, all users subscribing to 4, 3 and 2 can manipulate protected objects.

> If you disable **Hierarchical** for a specific level (for example, 4), only users subscribing to that level can manipulate protected objects. This may be useful if you want to prevent users subscribing to other levels from manipulating protected objects.

> For an example of how you use the **Hierarchical** option, click here

5.3 Protecting objects in the configuration

1. In the **Definition** program, open the configuration in which you want to protect IGSS objects.

2. Click here and follow the procedure.

Next >

Chapter 6: Users and Passwords

6.1 Users and passwords

Adding new users

> **Note:** Before you add new users, you must create the user groups you need. User rights are defined as part of the user group definition.

To add a new user, you open the **Users and Passwords** dialog box (see below) and type the appropriate user name and password. You can also specify an **Auto logout** interval, which means that the operator will be logged out after a specified period of inactivity.

The **Full name** option allows to type the full name of the operator. This will give you a better overview when printing reports of your users on the system for documenting the user administration setup.

Assigning users to user groups

When you have created a new user, you must assign him to one or more user groups in order for him to be allocated the appropriate user rights. You simply select the user name in the list, and then select the name of the user group in the drop-down list to which he's to become a member and click **Add Group**.

> **Important:** At least one user must be a member of a user group that has the right to use the **User Administration** program. This right is typically assigned to an administrator group, for example, called **Admin**.

The Users and Passwords dialog box

When you want to define or edit the user definitions, select **File → Users and Passwords**. The following dialog box appears.

For an explanation of the individual items in the dialog box, click the [?] in the upper right hand corner of the dialog box, then click on top of the item you want information about.

To control object access rights for AMS (Alarm Management System) a user with the name 'ams' must be added in the User Administration module. The user MUST have the exact name 'ams'. The rights given to this user will then control the AMS modules access rights to the objects in IGSS. If this user has not been defined, AMS is allowed all commands options to IGSS.

6.2 Defining a new user

> Before you define any users, you must define the user groups. At least one user must have the right **Can administer**. Otherwise, no users will be able to open the **User Administration** program.

1. Select **File → Users and Passwords**.

2. Click **New User**. A user ID is assigned to the new user and is by default added as the user name.

3. In the **User name** box, type the user name of the new user.

4. In the **Password** box, type the password for the new user.

5. In the **Full name** box, type the full name of the user, if required.

6. In the **Auto logout** box, type the period of inactivity you want to allow before the user is logged out. If set to **0**, the user will not be logged out automatically.

7. In the **User group** drop-down list, select the user group you want the user to be a member of and then click **Add to Group**. A user may be a member of more than one group, if required.

8. Click **Close** to save your changes and close the dialog box.

Tips

- To view the user names and passwords of all users defined, select **File → Reports** and click **Users** to view a user report.
- Passwords are case-sensitive.

> The rights of the individual users are defined as part of the user group. Click here [»] for details.

6.3 Removing a user

1. Select **File → Users and Passwords**.

2. In the **Defined users** list, select the user you want to remove.

3. Click **Delete User**.

4. Click **Close** to save your changes and close the dialog box.

Chapter 7: Exclusive Control

7.1 Exclusive control

What is exclusive control ?

Exclusive control is a function that allows you to assign exclusive control to one or more workstations in a system with several workstations. This means that protected objects in the configuration can only be manipulated from a workstation allocated the exclusive control feature. Technically, linking a string object to a Protect object accomplishes this.

The idea behind exclusive control

The idea with exclusive control is to put an extra layer on top of the "normal" user administration. When we enable exclusive control, we do not disable user administration. Instead, we operate with two safety layers: "normal" user administration and exclusive control.

How to define exclusive control

The following description gives you an overview of how to define exclusive control. For a detailed procedure, click **How To**.

STEP 1: Protect the relevant IGSS objects in the configuration.

STEP 2: Define the string object that you want to use for applying exclusive control.

STEP 3: Open the properties dialog box of the **Protect** object and connect the string object to it.

STEP 4: Install the configuration to apply your changes.

STEP 5: Open User Administration and link the string to the relevant workstation.

How it works

The following conditions must be met before exclusive control works:

1. The relevant objects must be protected in the configuration

2. The string object that you want to use for exclusive control must be defined

3. The string object must be linked to the relevant workstation(s) in User Administration

4. The relevant user groups and rights must be defined

5. A user with the relevant rights must be logged in

6. When an operator tries to control a protected object, his rights are checked as follows:

1. Does he have the right to perform the operation (for example, send a command to a digital object) ? If yes, the next check is performed. If no, the **Temporary Login** dialog box appears allowing a user with the necessary rights to log in.

2. Is the object subjected to exclusive control ? If yes, does this workstation have exclusive control (if it has, the operation is carried out). If no, user access is denied.

The Exclusive Control dialog box

To define exclusive control for one or more workstations, select **File → Exclusive Control**. The following dialog box appears.
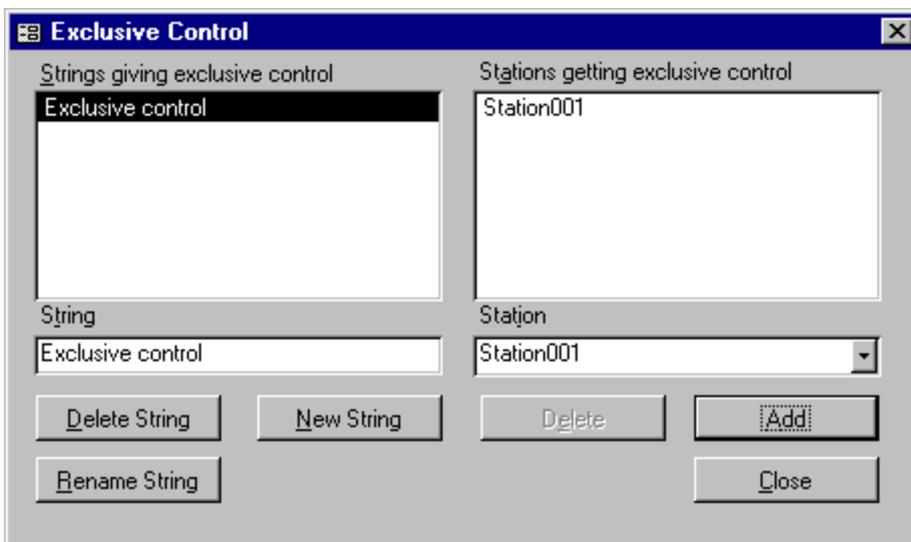
For an explanation of the individual items in the dialog box, click the ? in the upper right hand corner of the dialog box, then click on top of the item you want information about.

7.2 Assigning exclusive control to a workstation

1. In the **Definition** program, create a string object that you can use to assign exclusive control.

2. On the **String Object** tab in the **String** field, type the text string that will give exclusive control.

3. Click **OK** to save and close the string object.

4. Open the Protect object(s) that you want to use for applying exclusive control

   > That is, the Protect object you have selected for the protected objects
   > (in the **Protection** box on the **Data Management Definitions** tab).

5. Click the **Data Management Definitions** tab.

6. In the **Connect To** drop-down list, select the string object you created in step 1.

7. Click **OK** to save and close the Protect object.

8. In the **User Administration** program, select **File → Exclusive Control**.

9. In the **String** box, type the exact text string created in step 2.

10. Click **New String** to add the string.

11. Select the string in the list to the left and type the name of the workstation that will get exclusive control in the **Station** field.

12. Click **Add**. The workstation name appears in the list to the right.

13. Repeat steps 11 and 12 if you want to assign exclusive control to more than one work-station.

14. Click **Close** to save your changes and close the dialog box.

If an operator, who does not have exclusive control, tries to manipulate a protected object, the command menu will be greyed in **Supervise**.

To get an overview of how user administration works in the Supervise program, click here ⏩.

7.3 Removing exclusive control from a workstation

1. Select **File → Exclusive Control**.

2. Select the string that assigns exclusive control to the relevant workstation.

3. Select the name of the workstation in the list.

4. Click **Delete**.

5. Click **Close** to save your changes and close the dialog box.

If you want to disable a particular string from assigning exclusive con-trol, simply click the string in the list, then click **Delete String**.

Chapter 8: Reports

8.1 User administration reports

Why you should use the reports

There are several good reasons why you should use the built-in reports features:

- They provide a good overview of what you have defined in the **User Administration** program
- They provide more information than you can view directly in the dialog boxes of the program (for example, the Protect Objects report shows you the current state of the Protect objects used and which IGSS objects have been protected).

Three types of reports

The following report types are available (see details below):

- User group report
- Protect object report
- User report

The reports can either be viewed on-screen (**View**) or printed (**Print**). In both instances, user passwords may be encrypted (**Hide passwords)** in which case they are displayed as asterisks (***).

User group report

Click the **Groups** button to get a report focusing on the user groups defined. The report contains a section for each user group showing the following information.

- User names, passwords and full names
- The names and security level(s) of the Protect objects assigned to the group
- Global rights

Click here for an example.

Protect objects report

Click the **Protect Objects** button to get a report focusing on the Protect objects used. The report contains a section for each Protect object showing the following information.

- The specific rights attached to each security level of the Protect object
- The names of all IGSS objects in the configuration that are protected by this Protect object

Click here for an example.

User report

Click the **Users** button to get a report focusing on the users defined. The report contains a section for each user showing the following information.
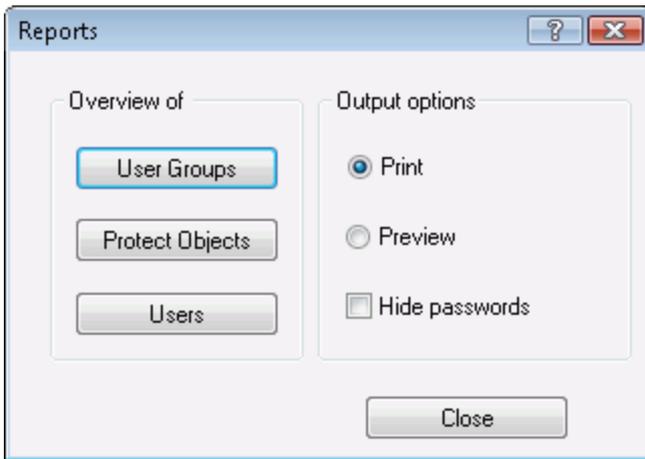
- The user name, password, full name and automatic logout interval
- The name(s) of the user group(s) that the user is a member of

- The global rights attached to the user group(s)

Click here for an example

The Reports dialog box

To generate a report, select **File → Reports**. The following dialog box appears.

For an explanation of the individual items in the dialog box, click the [?] in the upper right hand corner of the dialog box, then click on top of the item you want information about.

8.2 Creating reports

1. Select **File → Reports**.

2. In the **Output Options** group, choose whether you want to view the report on-screen (**Preview**), print it (**Print**) and encrypt passwords (**Hide passwords)** so that these will displayed as asterisks in both previewed and printed reports.

3. Click the button for the report type you want to generate. You need to print all three reports to get full documentation for all your definitions in the **User Administration** program.

Tips

- To view the current state of the Protect object(s) used, the configuration must be started. In that case, the current state will be highlighted in the Protect object report. Note that this report also contains a full list of the IGSS objects that have been protected.

- To view all user names and passwords, print the user report. You cannot view the passwords in the **Users and Passwords** dialog box.

Chapter 9: Reference and Lookup

9.1 Conventions in this Manual

The following typographical conventions are used:

Convention	Description	Example
User interface element	When referring to labels and names in the user interface.	The **Data Management** tab.
User input	When the user has to type specific data in IGSS.	Type the following description: Incoming flow in Tank 2
Module name	When referring to a module in IGSS	Open the **Definition** module.
Note	A note emphasizes or supplements important points of the main text. A note provides information that may apply only in special cases.	By default, the timestamp is in universal time format, **UTC**[1]. This can be changed in the Driver Log Filters dialog box.
Tip	A tip suggests alternative methods that may not be obvious in the user interface. A tip also helps the user in working more effectively with IGSS. A tip is not essential to the basic understanding of the text.	Alternative to this simple find function, you can also filter on text in the messages in Driver Log Filters dialog box.
Warning	A warning is an important note that is essential for the completion of a task. In some cases, disregarding a warning may result in undesirable functionality or loss of data.	If you disregard the System alarm, you may risk loss of data in the **LOG** and **BCL** files.

9.2 Getting Help in IGSS

IGSS comes with a comprehensive help system designed to help both system designers and operators to get started with IGSS as quickly as possible.

Documentation overview

The IGSS documentation includes the following items:

---

[1]Universal Time Coordinated (formerly Greenwich Mean Time), used as the basis for calculating time in most parts of the world. IGSS uses this time format internally in the database. You can switch between UTC and local time by enabling or disabling the "UTC" field in various dialog boxes in the system.

Documentation item	Description
Getting Started	An introduction to IGSS and its most fundamental terms and features. Getting Started is intended to get you up and running as fast as possible. The manual provides a system and architecture overview followed by a number of real-life use cases you can go through before building your first real IGSS project. The manual is available in Adobe Acrobat format (.pdf).
Module help	For each module there is a help file with the same name as the module itself, for example, Igss.chm for the Master module, Igss.exe. The help file is invoked by clicking the in the upper right corner of the module. The Table of Contents will then allow you to browse through the topics.
Dialog box help	For each dialog box there is a help topic with the following standard information: • Overview • Preconditions • Where do I find it? • Field help Dialog box help is invoked by clicking the help button in the upper right hand corner of the dialog box.
Thematic help	IGSS also provides thematic help. When there is a special theme that requires special attention from the user, a dedicated help file is provided. Examples include "Driver-Specific Help" and "Database Administration Help".

Where are the help files located?

The IGSS help files are located in the appropriate language folder under the [IGSS InstallPath]. The help files are available in English at release time.

The paths to the help files are:

Language	Path
English	[IGSS InstallPath]\ENG
Danish	[IGSS InstallPath]\DAN
German	[IGSS InstallPath]\DEU

Translated help files

Selected help files have been translated into Danish and German. If you require help files in your language, please contact 7T.

Help updates

The IGSS help files are continuously updated and improved. Check regularly with the **IGSS Update** module in the IGSS Start menu.

9.3 Version Information (IGSS Help System)

© 7-Technologies A/S, IGSS Version 9.0

The IGSS help files are based on software build number 10305 (initial release)

English help files

To update the help files, you must activate the **IGSS Update** module in the IGSS Start menu. There must be a connection from the PC to the Internet. Every time **IGSS Update** is run, IGSS help files as well as IGSS system files will automatically be updated on the PC from the 7-Technologies web server.

You select the languages you want to update in the **Tools** menu of the **IGSS Update** module.

If you are not able to update the IGSS system directly via the Internet, the alternative is to download the updates from the 7-Technologies website as zip files. These can then be transferred onto a CD or USB memory stick, which is then the medium used to update on site.

> After running **IGSS Update**, the build numbers in various IGSS modules may change to a higher number. This signifies that the module in question has been updated with newer files. Build numbers consist of four digits, where the first digit represents the year and the last three represent the day number in the year in question. The build number can be seen in the **About** dialog box which can be activated from the **Help** menu.

An example:

Build number = 10305
10 = the year 2010
210 = The 210th day of the year

Chapter 10: **Glossary**

A

Application menu

The Application menu is the first ribbon in the IGSS Master module. Click the icon to drop down the menu. The menu contains items that were typically found in the File menu in previous versions of IGSS. In most modules, an "Options" item allows the user to define global module settings. The Application menu was introduced in the Microsoft Office 2010 package. It replaces the Application button (nicknamed Doughnut) which was introduced in IGSS V7 and V8.

D

descriptor

A descriptor is the graphical display of an object. IGSS includes many types of descriptors including: - Built-in standard symbols - Animated symbols (Symbol Factory library) - Graphics and animation - Drawing symbols - Windows controls - ActiveX controls An IGSS object can be represented with different descriptors on different diagrams.

Q

Quick Access Bar

You can customize the Quick Access Bar to include the functions you use most frequently. Simply drag the relevant function from the ribbon to the Quick Access Bar.

R

Ribbon

The Ribbon is a new term/element in the Microsoft universe. The Ribbon replaces the well-known toolbars in applications. The Ribbon provides quick access to the most commonly used functions in the application. The Ribbon is divided into logical groups (the tabs) and each tab is divided into sections (the blocks in the tab). The Ribbon is context-sensitive which means that only relevant functions are accessible dependent on the current user action.

S

SCADA

Supervisory Control & Data Acquisition

U

UTC

Universal Time Coordinated (formerly Greenwich Mean Time), used as the basis for calculating time in most parts of the world. IGSS uses this time format internally in the database. You can switch between UTC and local time by enabling or disabling the "UTC" field in various dialog boxes in the system.