User Administration User Guide
IGSS Version 12.0

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained therein. The documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application of use thereof.

Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein, If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Contents

Chapter 1: Welcome to User Administration

1.1 What is IGSS User Administration?

Definition and use

The User Administration module 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

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 unauthorized 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.

1.2 Key features and benefits

The key features of the User Administration module are:

- User Groups: Create users and define global and specific permissions.
- Object-level Protection: Define and set up user access rights for specific object
- Users and Passwords: Create and maintain users and passwords.
- Exclusive Control: Define which operator stations a user may issue commands to protected objects.
- Safe Commands: Help reduce the risk of sending unintended commands to objects as well as create a procedure for the signing of sent commands.
- Microsoft Active Directory: Integrate your IGSS users with your Windows users to create a single-sign on procedure to IGSS
- User Administration Reports: Get an overview of your User Administration setup in your installation report.

User groups

The user group is the central element in IGSS User Administration. An individual user's rights are always dependent on his membership of one or more user groups. Start by creating user groups and defining rights when you set up user administration for a specific configuration.

Note that the specific Protect Object rights for the users of a user group are also defined in the **Permissions** group box. The user group 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** modules. **Important:** At least one user group and one user must have administrator's rights, otherwise access to the **User Administration** form 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.

Object-level protection

Object level protection can be used to prevent unauthorized use or manipulation of any object in the configuration. For this purpose, an IGSS system object called **Protect** is used. 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** tab.

When object -level protection 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.

Protect objects are set up in the Definition module.

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

Sometimes, you will need to further restrict access to a specific object, limiting access to only permit changes made to a protected object from a specific operator station. 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.

Safe Commands

If an object with Safe Commands enabled is manipulated by an operator, a prompt box will be displayed, requiring the operator to either confirm the submitted change, enter the user's password or get a second IGSS user to sign the changes with their password.

Safe Commands that require passwords for submission cannot be used without enabling User Administration in IGSS

This feature ...	Allows you to ...
Confirm	A prompt box is displayed, requiring the operator to acknowledge a change to the object value(s) by clicking the OK button. This is the only type of Safe Command that does not require the User Administration is enabled.
Password	A prompt box is displayed, requiring the operator to acknowledge a change to the object value(s) by entering the user's password. This Safe Command requires the User Administration is enabled.
Confirm, 2 Users	A prompt box is displayed, requiring two different users to acknowledge a change to the object value(s) by entering their user names and passwords. This Safe Command requires the User Administration is enabled.

Microsoft Active Directory

You can integrate your IGSS User Administration with your company's Microsoft Active Directory / Windows Users to simplify and streamline your plant or company-wide user access rights policies. Once you integrate your IGSS User Administration with the Microsoft Active Directory, all set up of users and passwords will be conducted in the Microsoft Active Directory.

This feature ...	Allows you to ...
Domain Groups	Connect an IGSS User Group to an existing User Group in the Microsoft Active Directory. You can combine this with Local groups.
Local Groups	Connect an IGSS User Group to an existing User Group on the local machine. Set up of users and passwords is now conducted in the local machine's user groups. You can combine this with Domain Groups.
Auto login	Automatically login to IGSS with the current windows user when IGSS is started. If another user needs to permanently login to IGSS, the user must log on to the windows machine and start IGSS.

Reports

When you have finished your user administration setup, you can get an overview of the User

Administration by installing the configuration and selecting the **Show User Administration setup** option in the Installation options dialog.

The User Administration setup will be added to the installation report and you can

This feature ...	Allows you to ...
User group section	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 section	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 section	View details for each individual user including user name and membership of user group(s) and which global rights the user has.

See Also

"User groups" on page 21

"Users and passwords" on page 26

"Exclusive control" on page 31

"Integration with Microsoft User Administration" on page 36

"The User Administration Setup Report" on page 40

1.3 About Global and Specific Rights

In IGSS you can assign two types of rights (Global and Specific) to a user group. Each user that is a member of that user group will gain the rights defined for that user group.

The 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 unauthorized use

> At least one user group and one user must have administrator's rights, otherwise access to the **User Administration** form is denied.

Global rights

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

Global right	Definition
Can administer	allows the user to use the User Administration module to manage users and user groups in IGSS.
Can define	allows the user to start the **Definition** module and modify the configuration as well as open and edit options in the **System Configuration** form. The **Can Define** Global right also determines access to the **Operator Report Formats**, **Events** and **Alarms** options in the **Tools** menu in the **Supervise** module.
Can define Winpager settings (Legacy)	allows the user to make changes in the **Winpager** module. This settings is only used for the legacy Winpager feature. Legacy features are included in the IGSS program package for backwards compatibility reasons and are not maintained or updated.
Can edit Maintenance jobs	allows the user to create, edit and delete maintenance jobs in the **Maintenance** module.
Can use IGSS Mobile	allows the user to access the IGSS Mobile Server to retrieve and acknowledge alarms from an Apple (IOS-based) smartphone. The IGSS Mobile app must be installed and configured on the smartphone prior to connecting to the IGSS configuration.
Can use system commands	allows the user to use IGSS system commands: • Start/stop the configuration • Start/stop data collection • Start/stop IGSS event logging. • Start/stop and close the Notifier module This right also enables the user to edit Dashboards.

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

> You can remove access to the **Definition** module for operator stations if necessary by selecting the **Application is not available** option for the **Definition** row in the **System Configuration** form > **Applications** tab.
>
> Remember to select the correct IGSS station. It is not recommended removing access to the **Definition** module for the IGSS server.

Specific rights

Specific rights can be defined to all IGSS objects that are protected in the configuration and are a part of IGSS object-level protection scheme.

Specific rights 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 on the protect

object that manages the object-level protection of a specific object. The protect object in question is accessed in the **Definition** module.

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

Chapter 1: IGSSMaster Tab Help

1.4 Groups form

Overview

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

Where do I find it?

In **IGSS Master** click the User Administration button under the **Design and Setup** tab in the **Configure** ribbon. Then choose the **Groups** tab.

Field Help

Field name	Description
User Group	Select the user group you want tot edit.
Add New	Click to create a new user group.
Group Name	Type the name you want to give to the group.
Delete	Deletes the user group
Auto log out	Automatically logs out the user after the specified period of inactivity (neither keyboard nor mouse has been touched). If set to **0**, the user will not be logged out automatically.
Permissions	Check the Global permissions you want to give the selected group. The Permissions group box also displays a list of all Protect objects from the active configuration. Each object has four protection levels (1 to 4), where 4 is the highest protection level. You can assign an active (valid) protection level by selecting the relevant check box .
Area	Select the area which is to be opened as the default area when a user from the active user group log on to IGSS. The defined area enables you to select which diagrams are to be opened as the default diagrams for all members of the user group.
Diagrams	Select the diagrams which are to be opened as the default diagrams when a user from the active user group log on to IGSS. If a user is a member of multiple user groups, all defined diagrams will be opened, subject to the value in the **max open diagrams** field on the **Supervise & Language** tab in the **System Configuration** form. The Areas and Diagrams selected in the **Group** tab will override any diagrams (and graphs) defined as the Initial Display in the **Definition** module. If there are no diagrams selected in this field, the diagrams and graphs set as Initial Display diagrams in the **Definition** module will be used.

Field name	Description
	Note: You have to install the configuration, before you can see the areas and diagrams.
Restore open diagrams on login	Select this check box to restore any diagrams and graphs which were open in the Supervise module when the previous user logged off IGSS. If this check box is selected, the Areas and Diagrams selected as default diagrams in the **Diagrams** field will be ignored. If a user is a member of multiple user groups, this check box need only be selected for one of the user groups in order to ignore all defined diagrams in the **Diagrams** field of the user groups. If a user logs on to IGSS and then starts the **Supervise** module, there will not be any open diagrams or graphs to restore. In this case, the system will default back the selected diagrams in the **Diagrams** field If there are no diagrams defined as default diagrams, the diagrams and graphs defined by the **Set Initial Display** command in the **Definition** module (if any) will be opened.
Connect to Windows user group	Note: You have to activate this function by checking Windows authentication, in System Configuration under the Access Control tab. Instead of using IGSS user groups, you can with this function, select the users you have on your computer or your domain.
Commit	Confirms the changes you made.
Revert	Cancels the changes you made

See Also

"About Global and Specific Rights" on page 5

"Opening default diagrams in Supervise" on page 23

1.5 Users

Overview

Here you can define the users you want to have, define passwords and then assign them to a group defined in **Groups**. The groups appear under Group membership, you can then check the ones to assign to.

Where do I find it?

In **IGSS Master** click the User Administration button under the **Design and Setup** tab in the **Configure** ribbon, **Users**.

Field Help

Field name	Description
User	Choose the user you want to edit.
Add New	Adds a new user.
User ID	Type the name of the user.
Password	Type your password as defined in the **User Administration** program. You must be a member of a user group with the **Can use User Administration** right in order to log in.
Full Name	Type the full name of the person. This is a useful function if you have many users. **Tip:** You can view all user information by selecting **File** , then **Reports** and then selecting the user report.
Auto log out	Automatically logs out the user after the specified period of inactivity (neither keyboard nor mouse has been touched). If set to **0**, the user will not be logged out automatically.
Delete	Deletes the selected user.
Commit	Confirms the changes you made.
Revert	Cancels the changes you made

1.6 Exclusive Control

Overview

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.

Where do I find it?

In **IGSS Master**, click the User Administration button under the **Design and Setup** tab in the **Configure** ribbon, then click the tab **Exclusive Control**.

Field Help

Field name	Description
Control String	Strings which will give exclusive control. Click **Add** to add it to the list. **Note:** Type the text string exactly as you did in Definition. Do not type the string object name.
Controlled Station	After have chosen a string, check the workstation which will get exclusive control. Use the workstation names as defined on the **Type** tab in the **Setup** program. Click **Add** to include it in the list.
Add	Adds a new control string. **Tip:** You can link a string object to more than one workstation, if required. Only the listed workstations will have access to protected objects.
Delete	Deletes the selected workstation or string from the list.
Edit	Changes the string or the station, according to what is typed in the box. Type the desired name.
New	Adds a new station to the list.
Control String	Shows the list of strings which give exclusive control of protected objects. For each object, add the names of the workstation(s) you want to give exclusive control. Type the text string exactly as you did in the **Definition** program. Do not type the string object name.
Controlled Stations	Shows the workstation(s) which get exclusive control with the selected string. Use the station names as defined on the **Station** tab in the **System Configuration** program. Once the string is linked to a workstation, only this workstation will be allowed to manipulate protected objects. All other workstations cannot access the protected objects, the command menu will simply be grayed in Supervise.

1.7 Protect Object settings

The Protect Object settings allow you to select a protection level and define its associated rights. The members of a user group subscribing to the protection level will own the enabled rights, for example, **Can acknowledge alarms**.

These rights only apply to IGSS objects which are protected. You protect an object by selecting the name of the Protect object in the **Protection** list on the **Data Management** tab in the **Definition** module.

Where do I find it?

In **Definition** module, open the click **File** > **Object Browser** to open the Object Browser. Find the Protect object and select **Show Properties** check box. Click the **Open / Select** button to open the

object properties form.

In the object properties form, click the **Command / State config** tab.

Additional Information

All protect objects are digital objects based on the PROTECT digital object template. You can create multiple protect objects to get a finer detail in your object level protection and to better differentiate between the objects to be protected and the protect objects themselves.

The **Default Command** field and **Commands** group box are disabled for protect objects. If you need to change a default command or command settings for a protect object, do not edit the original PROTECT digital object template.

Instead, create a new copy of the PROTECT digital object template, create a new protect object based on the new PROTECT digital object template and edit that template.

Field Help

Field name	Description
Hierarchical	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) in the active configuration. 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. Check **Hierarchical** for levels 4,3 and 2 and set the protection level of the Protect object to **4** in the configuration. This will ensure that all users are checked correctly against their rights, irrespective of whether they subscribe to protection level 4, 3, 2 or 1.
Can acknowledge alarms	Allows the user to acknowledge and hide alarms originating from the protected objects from the **Supervise** or **Alarm** programs. The ability to hide alarms must be enabled in the **System Configuration** form > **Alarms** tab for all operators in order to hide alarms .
Can update set points	Allows the user to change the set point for protected analog objects.
Can update high/low scale	Allows the user to change the values of the high scale and low scale (maximum and minimum) atoms for analog objects.
Can update free value	Allows the user to change values on the free value atoms for analog and digital objects.

Field name	Description
Can update alarm limits	Allows the user to change alarm limits for protected analog objects.
Can send commands	Allows the user to send commands to protected digital objects, for example, start or stop pump.
Can update strings	Allows the user to change the text in protected string objects.
Can update tables	Allows the user to change values in protected tables.
Can open diagrams and areas	Allows the user to open protected areas and diagrams.

See Also

"Create a new Protect Object" on page 29

"Assigning user rights to security levels" on page 29

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 organize 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 module. 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 clicking **File > Logout**

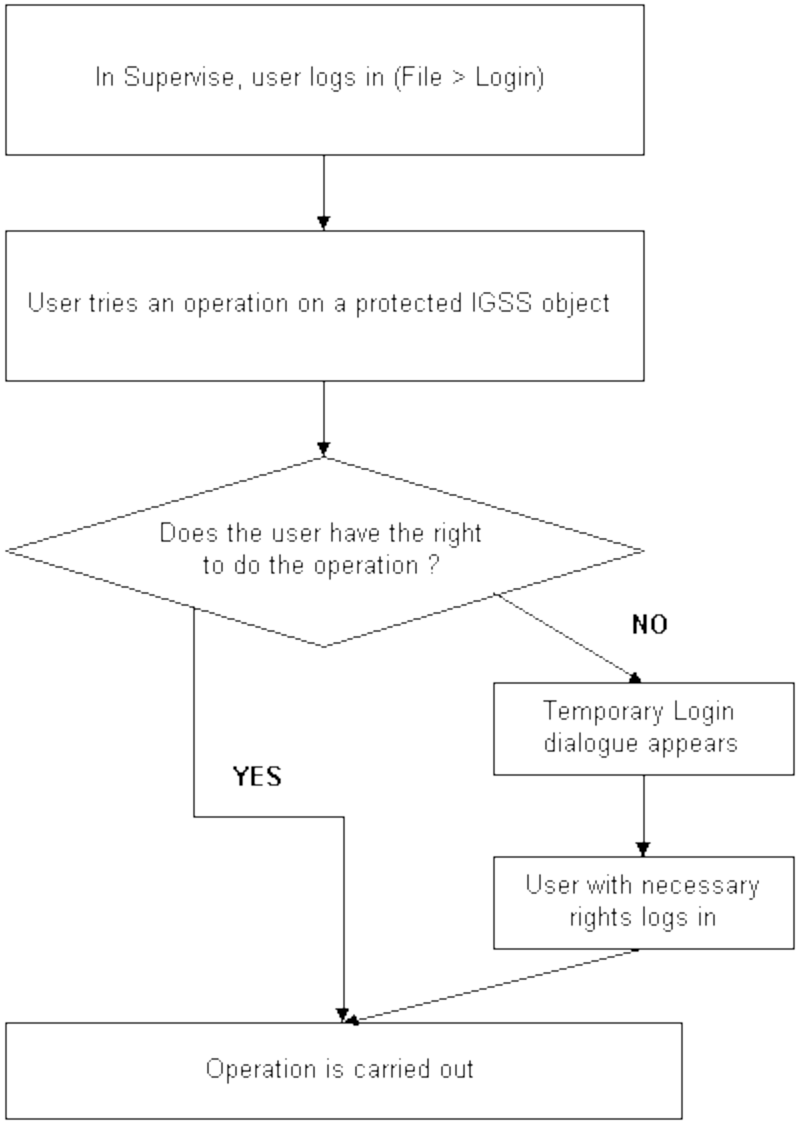
Access control

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

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.

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

STEP 1: Define user groups and rights

Define the three user groups with the following rights:

User group ...	Has the following rights ...
Admin	• All global rights. • Select the **Protect@Global : Level 4** check box
Day	• No global rights (they must not use Definition or User Administration or start and stop configurations) • Select the **Protect@Global : Level 2** check box
Night	• No global rights (they must not use Definition or User Administration or start and stop configurations) • Select the **Protect@Global : Level 1** check box

STEP 2: Define users and passwords

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: Define the security level permissions for the Protect object

In the **Definition** module, open the **Object Properties** form for the **Protect** object.

Set the following security level permissions:

Security Level	Protect Object Rights
1	Select the following permissions • Can Acknowledge
2	Select the **Hierarchical** check box Select the following permissions • Can Acknowledge

Security Level	Protect Object Rights
	• Can update set points • Can update alarm limits • Can send commands
3	Select the **Hierarchical** check box Select the following permissions • Can Acknowledge • Can update set points • Can update alarm limits • Can send commands • Can update strings
4	Select the **Hierarchical** check box Select the following permissions • Can Acknowledge • Can update set points • Can update alarm limits • Can send commands • Can update strings • Can update tables • Can open diagrams and areas

Save and close the **Object Properties** form and check and install the **Definition** Module.

STEP 4: Protect the objects in the configuration

We want to protect the following objects:

- p1
- p2
- p3
- q1
- q2
- q3

In the **Definition** Module, Click **Edit** > **Open by Name** and select one of the above objects, click the **Data Management** tab in the properties dialog box and select **Protect** in the **Protection** drop-down list. Repeat for all the objects.

STEP 5: Set the state of the Protect Object

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.

In the **Definition** module, click **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 6: 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 7: Log into Supervise and test

Click the **Supervise** button on the **Home** tab of the **IGSS Master** module.

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 will appear, indicating that the user does not have the right to carry out this operation.

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 ?

> Print screen shots from User Administration to see which rights you can assign to the users.
>
> 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.

Next >

3.2 Setting up user administration

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

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

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

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

4. Print the Installation report and select the display user administration setup check box to get an overview of your user administration setup.

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.

Next >

3.4 Testing user administration

1. In the **IGSS Master**, click **Home** tab > **Log in** button to open the **Login** form.
2. In the **Login** form, enter your user name and password
3. Click the **OK** button.

To login and logout from the Supervise module, in Supervise click **File** > **Login** or **File** > **Logout**.

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

< Previous

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.

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

User groups must be set up and defined for the IGSS configuration, regardless of whether you are using IGSS User Administration or integrating to Microsoft Windows user administration because IGSS utilizes the IGSS user groups to distribute rights and privileges within the IGSS configuration to the specific IGSS users.

Automatic logout

You can define automatic logout policies for the entire User Group or the specific user. Automatic logout policies defined for the User Group will affect all members of that User Group, while Automatic logout policies defined for the user will affect only the specific user.

The most restrictive (i.e. first occurring) logout policy will always be enforced, regardless of whether it is a User group logout policy or a specific user automatic logout setting.

See Also

"About Global and Specific Rights" on page 5

4.2 Creating a user group

1. In the **IGSS**, click **Design and Setup** tab > **User Administration** button.
2. In the **User Administration** tab, click **Groups** tab > **Add New** button.
3. In the **Group Name** field, enter the group name.
4. Select the **Auto logout** check box and set the period of inactivity you want to allow before any members of the user group is logged out in the **Minutes** field. If you set the value to **0** minutes, users will never be logged out automatically.
5. In the **Permissions** group box, select Global permissions of the group.
6. In the **Permissions** group box, select the security level(s) that define the rights of the users in this group.
7. In the **Default diagrams** group, select the Area and default diagram for the User Group.
8. Click **Commit** to save your changes.

4.3 Removing a user group

1. In the **IGSS**, click **Design and Setup** tab > **User Administration** button.
2. In the User Administration tab, User Group field, select the group you want to delete
3. Click the **Delete** button.
4. Click **Commit** to save your changes

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

4.4 Connect User groups

Once you have enabled IGSS Windows Authentication in the **System Configuration** form, you must connect the IGSS user groups with Windows user groups.

You can only connect an IGSS user group to one Windows user group.

1. In the **IGSS Master** module, click **Design and Setup** tab > click the **User Administration** button to open the **User Administration** tab in the **IGSS Master** workspace.
2. In the User Administration tab, click the **Groups** tab.
3. In the **User Group** field, select the IGSS User group you want to connect to a Windows user group.
4. Select the **View groups in Joined domain** check box to list the domain Windows user groups in the drop-down list.
5. Select the **View groups in local computer** check box to list the local machine Windows user groups in the drop-down list.
6. In the drop-down list, select the Windows user group you want to connect to the IGSS user group
7. Click the **Commit** button to save the user group setup.

If you do not connect an IGSS user group to an Windows, users of that user group will not be able to log in to IGSSsince user authentication is conducted through the user groups.

See Also

"Enable Windows Authentication" on page 37

4.5 Define default diagrams

You can select which diagrams are to be opened as the default diagrams when a members of the user group logs onto IGSS. Any diagrams defined as default will override diagrams and graphs defined as **Initial Display** diagrams in the **Definition** module.

If a user logs onto IGSS while the Supervise module is running with open diagrams and/or graphs, all diagrams and graphs will be closed and the defined default diagram will be opened instead.

1. In the **IGSS**, click **Design and Setup** tab > **User Administration** button.
2. In the **Groups** tab > **User group** group, select the user group you want to define default diagrams for.
3. In the **Default** diagrams group:
4. In the **Area** field, select the area which contains the diagrams to be defined as default from the drop-down list which
5. In the **Diagram** field, select one or more diagrams as default diagrams
6. Click the **Commit** button to update the User Group settings.

> If you want to keep any open diagrams and graphs in the **Supervise** module when logging in as a user, you can select the **Restore open diagrams at login** check box. Any diagrams defined as default diagrams in the **Diagrams** field will be ignored when the user logs onto IGSS.

See Also

"Groups form" on page 8

"Opening default diagrams in Supervise" on page 23

4.6 Opening default diagrams in Supervise

You can define which diagrams should automatically open by default when a user logs onto IGSS on the **Groups** tab of the **User Administration** workspace tab in the IGSS Master.

Diagrams defined as default diagrams on the **Groups** tab will override any diagrams or graphs set as default diagrams in the **Definition** module using the **Set Initial Display** command. Additionally, you can select the **Restore open diagrams at login** check box in the **Groups** tab as well as select the **Go to Initial Display** check box on the **Supervise & Language** tab in the **System Configuration** form.

The combination of check boxes will result in the following:

Go to initial display check box selected

When the **Go to initial display** check box is selected, all open diagrams are closed when a user logs off IGSS and the set of diagrams and graphs defined as the Initial Display in the **Definition** module is displayed in the **Supervise** module.

Restore open diagram at login check box selected

When the **Restore open diagram at login** check box is selected, all default diagrams in the **Group** tab are removed and the diagrams that were open in Supervise when the user logged off will be remain open or will opened when a user logs onto IGSS again.

- Supervise Running:
    - User restarts Supervise, does not log on: Initial Display is opened.
    - User logs off: Initial Display is opened.
    - User logs on: Initial Display is opened.
- Supervise Stopped:
    - User starts Supervise, does not log on: Initial Display is opened.
    - User logs on: Initial Display is opened.

Restore open diagram at login check box cleared

When the **Restore open diagrams at login** check box is cleared, all selected default diagrams in the **Group** tab will be opened when the user logs on to IGSS.

- Supervise Running:
    - User restarts Supervise, does not log on: Initial Display is opened.
    - User logs off: Initial Display is opened.
    - User logs on: User Group default diagrams are opened. If no default diagrams then Initial Display.
- Supervise Stopped:
    - User starts Supervise, does not log on: default diagrams are opened. If no default diagrams then Initial Display.
    - User logs on: User Group default diagrams are opened. If no default diagrams then Initial Display.

Go to initial display check box cleared

When the **Go to initial display** check box is cleared, any open diagrams will remain open when the user logs off IGSS.

Restore open diagram at login check box selected:

When the **Restore open diagram at login** check box is selected, all default diagrams in the **Group** tab are removed and the diagrams that were open in Supervise when the user logged off will be remain open or will opened when a user logs onto IGSS again.

- Supervise Running:
    - User restarts Supervise, does not log on: Initial Display is opened.
    - User logs off: Open diagrams are kept.
    - User logs on: Open diagrams are kept.
- Supervise Stopped:
    - User starts Supervise: Initial Display is opened.
    - User logs on: Initial Display is opened.

Restore open diagram at login check box cleared

When the **Restore open diagrams at login** check box is cleared, all selected default diagrams in the **Group** tab will be opened when the user logs on to IGSS.

- Supervise Running:
    - User restarts Supervise, does not log on: Initial Display is opened.
    - User logs off: Open diagrams are kept.
- User logs on: User Group default diagrams are opened.
    - Supervise Stopped:
    - User starts supervise, does not log on: Initial Display is opened.
    - User logs on: User Group default diagrams are opened.

See Also

"Groups form" on page 8

For more information about the **Go to Initial Display** check box, see the **System Configuration** online help file.

For more information about the **Set Initial Display** command, see the **Definition** online help file.

Chapter 5: Users and Passwords

5.1 Users and passwords

If you are using IGSS User Administration, you can manage users and passwords from the **IGSS Master** > **Design and Setup** tab > **User Administration** button.

If you have integrated IGSS User Administration with the Microsoft Windows User Administration, all user and password management is conducted in Microsoft Windows instead of in IGSS. The **Users** tab will not be displayed in the User Administration tab in the IGSS Master.

Adding new users

To add a new user, open the **Users** tab (see below) and enter 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 set-up.

> Before adding new users, you must create the user groups. User rights are defined as part of the user group definition.

Assigning users to user groups

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

> At lleast 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**.

Automatic logout

You can define automatic logout policies for the entire User Group or the specific user. Automatic logout policies defined for the User Group will affect all members of that User Group, while Automatic logout policies defined for the user will affect only the specific user.

The most restrictive (i.e. first occurring) logout policy will always be enforced, regardless of whether it is a User group logout policy or a specific user automatic logout setting.

5.2 The Notifier (AMS) User

The Notifier module can be set up to permit the sending of commands to IGSS digital objects by SMS from Notifier operators, or more precisely, from specific Notifier operator cell phone numbers assigned to Notifier operators.

By default, all Notifier operators are granted access to all objects in IGSS (included protected objects) when sending commands by SMS. Sending SMS commands to objects ignores the ordinary IGSS User Administration setup.

If you want to set up IGSS to include Notifier operators in the enforcement of object-level protection, you must do the following:

1. Create a User group to manage object-level protection for incoming SMS commands to those objects.
2. In the new User group, create and define object-level protection for all objects that are to be protected from SMS commands.
3. Create a user with the exact name "ams" (the user name does not contain quotation marks and is in lower case.)
4. Assign the "ams" user to the new user group which contains the object-level protection setup.
5. Restart the IGSS configuration for the changes to take effect.

When set up IGSS User Administration to extend object-level protection to encompass SMS commands sent from Notifier operators, all commands sent from any Notifier operator will be affected. It is not possible to differentiate between Notifier operators. If the "ams" user has been created, all commands from Notifier operators will adhere to the defined user group policies.

See Also

"Creating a user group" on page 21

"Defining a new user" on page 27

"Assigning security level(s) to a user group" on page 29

"Assigning user rights to security levels" on page 29

5.3 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. In the **IGSS**, click **Design and Setup** tab > **User Administration** button.
2. In the **User Administration** tab, click **Users** tab > **Add New** button.
3. In the **User identification** field, type the user name of the new user.
4. In the **Password** field, type the password for the new user.
5. In the **Full name** field, type the full name of the user, if required.
6. Select the **Auto logout** check box and set the period of inactivity you want to allow before the user is logged out in the **Minutes** field. If you set the value to **0** minutes, the user will never be logged out automatically.
7. In the **Group Membership**group box, select the user group you want the user to be a

member of. A user may be a member of more than one group, if required.

8. Click **Commit** to accept the changes you made.

> Passwords and users are case-sensitive.

See Also

"Creating a user group" on page 21

5.4 Removing a user

1. In the **IGSS**, click **Design and Setup** tab > **User Administration** button.
2. In the **User Administration** tab, click **Users** tab
3. In the User field, select the user you want to delete.
4. Click the **Delete** button to delete the selected user.
5. Click **Commit** to save your changes.

Chapter 6: Protect Objects

6.1 Create a new Protect Object

You can create new digital Protect objects based on the PROTECT digital object template in the Definition module. Additional Protect digital objects can be used to get a finer detail in your object level protection and to better differentiate between the objects to be protected and the protect objects themselves.

To create a new Protect digital object

1. In the **Definition** module, click **File** > **Object Browser** (or press **CTRL + E**) to open the **Object Browser** form
2. In left pane of the **Object Browser** form, click the area you want to create the new Protect digital object in and click the **Digital** folder.
3. In the **Digital** folder, select the PROTECT digital object template
4. In the **Name** field, enter the name of the new Protect digital object
5. Click the **Create** button and select **New Unreferenced object** to open the **Object Properties** form.
6. In the **Command/State Config** tab > **States** group box, customize the new Protect digital object by selecting the desired Security levels and setting permissions for each selected Security level.
7. Click the **OK** button to create the new Protect digital object.

6.2 Assigning security level(s) to a user group

1. In the **IGSS**, click **Design and Setup** tab > **User Administration** button.
2. In the **User Administration** tab > User group field group, select the user group you want to assign security level to
3. In the **Permissions** group box, select the relevant security level(s). For each security level, a set of user rights have been defined in the **Definition** module.
4. Repeat steps 1 and 2 for all user groups.
5. Click **Commit** to save your changes.

6.3 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.

We recommend setting the Permissions to **Protect Global: level 4**. This topic describes the recommended procedure.

The rights you enable are not global and only apply to IGSS objects which are protected in the configuration.

1. In the **Definition** module, press **CTRL+E** to open the **Object Browser** and find the Protect object
2. In the right pane of the **Object Browser** form, select the Protect object, select the **Show Properties** check box and click the **Open / Select** button to open the object properties form.
3. In the Object properties form, click the **Command/State config** tab and in the **States** group box, select **Security level 4**
4. In the **Permissions** field group, select the appropriate rights for Security level 4.
5. Select the **Hierarchical** check box (see below).
6. Repeat steps 4 and 5 for Security levels 3, 2 and 1.

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

6. In the Object Properties form, click the **OK** button to save your changes and close the form.

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

6.4 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 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 form 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:

   - 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** form appears allowing a user with the necessary rights to log in.

- 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 form

To define exclusive control for one or more workstations, select the tab **Exclusive Control**.

For an explanation of the individual items in the dialog box, see the form help for **exclusive control**.

7.2 Assigning exclusive control to a workstation

In the Definition module

1. In the **Definition** module, 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** tab).

5. Click the **Data Management** 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.

In the IGSSMaster:

1. Click **Design and Setup** tab > **User Administration** button.
2. In the **User Administration** tab, click the **Exclusive Control** tab.
3. In the **Control String** box, add a new string, click edit and type the exact text string created in step 2.
4. Select the string in the list to the left, click new to create a new station, and then click edit to type the name of the workstation that will get exclusive control in the **Controlled Station** field. Check then the checkbox of the station to be controlled.
5. Repeat steps 11 and 12 if you want to assign exclusive control to more than one work-

station.

6. Click **Commit** to save your changes.

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

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

7.3 Removing exclusive control from a workstation

1. Click **Design and Setup** tab > **User Administration** button.
2. In the **User Administration** tab, click the **Exclusive Control** tab.
3. In the **Control String** group box, select the string that assigns exclusive control to the relevant workstation.
4. In the **Controlled Station** group box, select the name of the workstation in the list.
5. Click the **Delete** button to remove the selected operator station from the Exclusive control list.
6. Click **Commit** to save your changes.

> If you want to disable a particular string from assigning exclusive control, select the string in the list and click the **Delete String**. button

Chapter 7: Safe Commands

7.4 About Safe Commands

Safe Commands are applied to specific objects which may require special consideration or checks before submitting changes. Using Safe Commands can help reduce the risk of unintentionally submitting commands as well as reduce the risk of commands being sent by unauthorized personnel.

If an object with Safe Commands enabled is manipulated by an operator, a prompt box will be displayed, requiring the operator to either confirm the submitted change, enter his password or get a second IGSS user to sign the changes with their password.

Additionally, Safe Command acknowledgments are entering in the Audit Trail database if the Audit Trail functionality is set up and enabled.

Safe Commands that require passwords for submission cannot be used without enabling User Administration in IGSS.

An object can only have one Safe Command assigned to it. Safe Commands for the object are defined in the **Data Management** tab of the **Object Properties** form.

> To assign Safe Commands to multiple objects in the **Definition** module, you can use the **Property Table Viewer** for the Diagram or the Area.
> Click the **Objects** folder in the left pane of the Property Table Viewer to assign Safe Commands to multiple objects.

Safe Command Types

There are three types of Safe Commands

Safe Command Type	Description
Confirm	When enabled, a prompt box is displayed requiring the operator to acknowledge a change to the object value(s) by clicking the **OK** button. This is the only type of Safe Command that does not require the User Administration is enabled.
Password	When enabled, a prompt box is displayed requiring the operator to acknowledge a change to the object value(s) by entering the user's password. This Safe Command requires the User Administration is enabled.
Confirm, 2 Users	When enabled, a prompt box is displayed requiring two different users to acknowledge a change to the object value(s) by entering their user names and passwords. This Safe Command requires the User Administration is enabled.

See Also

For more information about Safe Commands, please see the **Adding Access Control and Security** chapter in the **Definition** help file found in the IGSS Master > **Help** Navigation pane.

Chapter 7: Microsoft User Administration

7.5 Integration with Microsoft User Administration

You can integrate your IGSS User Administration with the Microsoft Windows user management, enabling single sign-on to your IGSS system.

You can also have a single and centralized administration of IGSS users and their access rights for Windows machines that are included in a Windows domain or Active Directory.

Additionally, you can use Windows machines that utilize alternate logon methods such as fingerprint scanning or the use of smart cards to sign Safe Commands in IGSS as well.

The main features of the Windows User Management integration are:

1. Single sign-on to Windows and IGSS
2. Centralized user administration when used with a Windows Domain Controller or Active Directory
3. IGSS user access rights tied to Windows User Groups
4. Biometric sensors may be used to sign Safe Commands

Users and User Groups

IGSS integration with Windows Authentication is through the users groups of both applications. A user group in IGSS is connected to a user group in Windows and management of users is afterwards conducted in the Windows user administration environment.

Users that are members of IGSS user groups not connected to Windows user groups cannot log into IGSS.

> While it is possible to set up and combine IGSS stations and servers utilizing IGSS User Administration and Windows user administration in an IGSS configuration, it is highly recommended to chose one type of user administration and use it exclusively for the configuration.

Temporary and Permanent login

When Microsoft Windows user authentication is enabled, you can still temporarily log in to IGSS to complete restricted tasks for users that do not have sufficient rights or privileges to perform the task in question.

It is not possible to log in permanently in the same procedure though. The previous user must first log off IGSS before a new user can log on.

7.6 Windows Authentication and IGSS workflow

If you want set up your IGSS configuration to utilize Windows Authentication, you should:

- Create or edit the users you want to use for IGSS operations in your Windows user administration.
- Create and set up the User groups, Object-level protection and exclusive control settings you want to use in IGSS.

- Enable your IGSS station to use Windows Authentication in IGSS.
- Connect an IGSS user group to a Windows user group in IGSS.
- Enable User Administration access control on your IGSS station or server.

See Also

"Creating a user group" on page 21

"Enable Windows Authentication" on page 37

"Connect User groups" on page 38

"Enable Access Control in IGSS" on page 38

"Enable Windows user auto login to IGSS" on page 39

7.7 Enable Windows Authentication

Before you can utilize windows authentication in IGSS User Administration. you must enable windows authentication for each operator station and/or IGSS server.

An operator station or IGSS server that is not enabled to utilize windows authentication can only use IGSS User Administration.

1. In the **IGSS Master**, click **Design and Setup** tab > **System Configuration** button to open the **System Configuration** form.
2. In the left pane of the **System Configuration** form, right-click the IGSS station or IGSS server you want to enable windows authentication for and select **This PC**.

   The selected station or server icon will be displayed with a green screen.
3. In the right pane of the **System Configuration** form, click the **Access Control** tab.
4. On the **Access Control** tab, select the **Windows Authentication** check box

When Windows Authentication is enabled, the **Users** tab in the User Administration tab in the IGSS Master will not be displayed. All future administration of users and passwords is done in Windows instead of IGSS.

> While it is possible to set up and combine IGSS stations and servers utilizing IGSS User Administration and Windows user administration in an IGSS configuration, it is highly recommended to chose one type of user administration and use it exclusively for the entire configuration.

See Also

"Enable Windows user auto login to IGSS" on page 39

7.8 Enable Access Control in IGSS

Before you can use the User Administration setup in IGSS, you must enable access control for each operator station and/or IGSS server.

If access control is not enabled for an operator station or IGSS server, all users will have access to the IGSS configuration on that operator station.

1. In the **IGSS Master**, click **Design and Setup** tab > **System Configuration** button to open the **System Configuration** form.
2. In the left pane of the **System Configuration** form, right-click the IGSS station or IGSS server you want to enable windows authentication for and select **This PC**.

   The selected station or server icon will be displayed with a green screen.
3. In the right pane of the **System Configuration** form, click the **Access Control** tab.
4. On the **Access Control** tab, select the **Disable access control** check box

7.9 Connect User groups

Once you have enabled IGSS Windows Authentication in the **System Configuration** form, you must connect the IGSS user groups with Windows user groups.

You can only connect an IGSS user group to one Windows user group.

1. In the **IGSS Master** module, click **Design and Setup** tab > click the **User Administration** button to open the **User Administration** tab in the **IGSS Master** workspace.
2. In the User Administration tab, click the **Groups** tab.
3. In the **User Group** field, select the IGSS User group you want to connect to a Windows user group.
4. Select the **View groups in Joined domain** check box to list the domain Windows user groups in the drop-down list.
5. Select the **View groups in local computer** check box to list the local machine Windows user groups in the drop-down list.
6. In the drop-down list, select the Windows user group you want to connect to the IGSS user group
7. Click the **Commit** button to save the user group setup.

> If you do not connect an IGSS user group to an Windows, users of that user group will not be able to log in to IGSSsince user authentication is conducted through the user groups.

See Also

"Enable Windows Authentication" on page 37

7.10 Enable Windows user auto login to IGSS

If you have enabled Windows authentication in your IGSS configuration, you can also set up your IGSS system configuration to automatically log the current windows user into IGSS when IGSS is started.

When a windows user starts IGSS, the user name and credentials are automatically used to log into the IGSS User group associated with the user's Windows user group..

1. In the **IGSS Master**, click **Design and Setup** tab > **System Configuration** button to open the **System Configuration** form.
2. In the left pane of the **System Configuration** form, right-click the IGSS station or IGSS server you want to enable windows authentication for and select **This PC**.

   The selected station or server icon will be displayed with a green screen.
3. In the right pane of the **System Configuration** form, click the **Access Control** tab.
4. On the **Access Control** tab, select the **Auto login current Windows user** check box

Access Control must be enabled in order to utilize windows authentication.

Chapter 8: Reports

8.1 The User Administration Setup Report

The Installation report for your configuration contains a User Administration area where you can get an overview of your present User Administration setup for your configuration. The User Administration area provides additional User Administration information that is quicker to process than can be viewed directly in the User Administration tabs in the IGSS Master.

The installation report is be produced when you check and install your IGSS configuration and can be run from the IGSS Master as needed.

Generate an installation report from the IGSS Master

Click the **IGSS Master** > **Design and Setup** tab > **Check and Install** button to open the **Installation Options** form and install your configuration and create an installation report.

Remember to select the **Show user administration setup** check box to display the User Administration area in the installation report.

> In the **Installation Options** form, you can select the **Do NOT install - show only report** check box to only generate the installation report and thereby avoid stopping your configuration.

> Passwords are not displayed in the Installation report and cannot be displayed in any report generated from IGSS.

The User Administration area of the Installation report contains a section for:

- User Groups
- Protect objects
- User
- Exclusive Control

The User Group section

A user group represents a user profile which includes a set of rights relevant for a particular group of users. When the appropriate rights have been defined, the individual users are simply assigned to the group.

The user group section displays the following information for each User Group:

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

The Protect object section

The Protect object section displays the following information for each Protect object:

- 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

The User section

The User section displays the following information for each user:

- The user name, 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)

The Exclusive Control section

The Exclusive control section displays the following information for each station with exclusive control:

- The control string and all stations that are connected to that control string
- The control string status of the controlled stations (active/deactivated)

Chapter 8: Registry Key Settings

8.2 Block Stop commands sent from operator stations

You can block all Stop commands sent to objects from operator machines by enabling the **DisableOPcontrolCMD** registry key for the local machine.

The registry key is created the first time a Stop command is sent from the local operator station but you can create the registry key manually if you need to.

The **DisableOPcontrolCMD** registry key is disabled by default and must subsequently be enabled after it is created.

When the **DisableOPcontrolCMD** registry key is enabled, all Stop and related commands originating from the local operator station are ignored by the IGSS server. Related commands are commands originating from the Status and Control form in the **Supervise** module

To manually create the DisableOPcontrolCMD registry key

1. On the local machine, click **Start** and type "Regedit.exe" in the search field of the Windows Start menu to open the **Registry Editor** form.
2. In the **Registry Editor** form, In the **DC_HIKLM** folder found in HKEY_CURRENT_USER\Software\Schneider Electric\IGSS32\V12.00.00 right-click in the right pane and select **New** > **DWORD (32-bit) value**.
3. In the **Name** column, type "DisableOPcontrolCMD" and press **Enter** to create the new key.
4. Click **File** > **Exit** to exit the **Registry Editor** form and save the registry values.

To enable the DisableOPcontrolCMD registry key

1. On the local machine, click **Start** and type "Regedit.exe" in the search field of the Windows Start menu to open the **Registry Editor** form.
2. In the **DC_HKLM** folder in HKEY_CURRENT_USER\Software\Schneider Electric\IGSS32\V12.00.00, right-click the **DisableOPcontrolCMD** key and select **Modify**.
3. In the **Value Data** field of the **Edit String** form, enter "1" to enable the registry key and click **OK** to save.
4. Click **File** > **Exit** to exit the **Registry Editor** form and save the registry values.

To disable the DisableOPcontrolCMD registry key

1. On the local machine, click **Start** and type "Regedit.exe" in the search field of the Windows Start menu to open the **Registry Editor** form.
2. In the **DC_HKLM** folder in HKEY_CURRENT_USER\Software\Schneider Electric\IGSS32\V12.00.00, right-click the **DisableOPcontrolCMD** key and select **Modify**.

3. In the **Value Data** field of the **Edit String** form, enter "0" to enable the registry key and click **OK** to save.
4. Click **File** > **Exit** to exit the **Registry Editor** form and save the registry values.

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, Def.chm for the Definition module. 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.
Form and Dialog help	For each Form or dialog there is a help topic with the following standard information: • Overview • Preconditions • Where do I find it? • Field help Form help is invoked by clicking the help button  in the upper right hand corner of the dialog box or located in the Table of Contents of the individual help file.
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 in the installation path of IGSS, by default C:\Program Files\Schneider Electric\IGSS32\V12.0. 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. If you require help files in your language, please contact Schneider Electric.

Help updates

The help files are continuously updated and improved. Check regularly with the IGSS Update in the IGSS Master.

9.3 Version Information (IGSS Help System)

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

English help files

To update the help files, click the **Update IGSS Software** button on the **Information and Support** tab in the **IGSS Master**. 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 web server at Schneider Electric.

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

If you are not able to update the IGSS system directly via the Internet, the alternative is to download the updates from the Schneider Electric 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 updating your IGSS installation , 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
16 = the year 2016
305 = The 305th 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.

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.