

VisiWinNET 2005

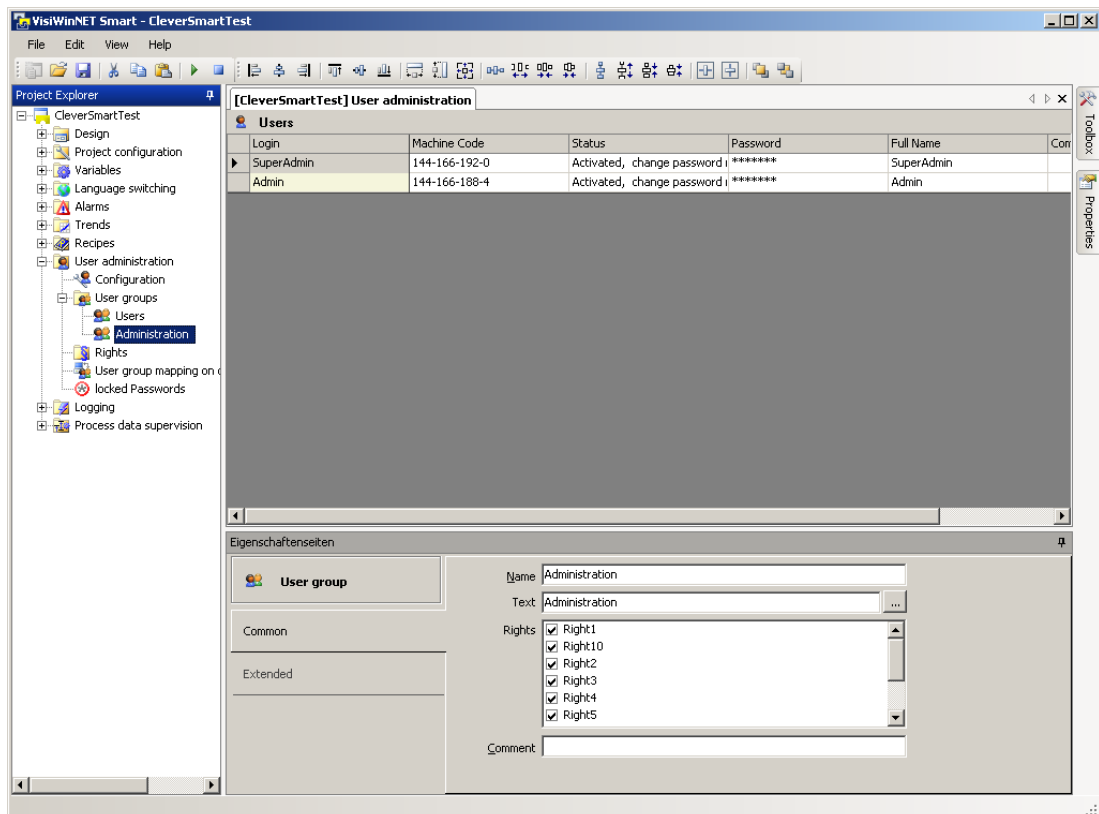
User administration



- VisiWin
- VisiWinNET 2005
 - Common
 - Class Library
 - Systems
 - Tools
 - Technical Informations
- Inosoft OPCServer
 - Basics and helping tools
 - Protocols

VisiWinNET 2005

User administration









The contents of this manual must not otherwise be used without explicit written consent from INOSOFT GmbH.

We have checked the contents of this manual for compliance with the described software. Discrepancies can, however, not be ruled out. For this reason we cannot guarantee full compliance. The contents of the manual are subject to regular checking for necessary updates/amendments. Such amendments will be made in the subsequent edition.

Suggestions for improvement are welcome.

Legend

In order to point out particular paragraphs the following symbols are used in the INOSOFT documentations:

	Attention	Passages with this sign should be read – and observed – with particular attention.
	Hint	Important paragraph “additional information”
	Tip	Many roads lead to Rome; here a shortcut is to be found.
	In work	Functions that are in preparation or already implemented but not yet prepared for documentation.
	Example execute	Instructions to be carried out in an example
	Observe result	Results to be observed with carrying out the exemplary instructions

© / ™ / ®

Windows®, Windows NT®, Windows 2000®, Windows XP® are registered trademarks of the Microsoft company.

Further product names marked ® are trademarks of the appropriate manufacturers.

INOSOFT GmbH created on

VisiWinNET Version: from 6.04.000

created on 07.06.2010

Contents

1 Preamble	1
2 User administration introduction	2
2.1 Right- or level-oriented.....	4
3 User administration editor	7
4 User administration definitions	8
4.1 User Group.....	8
4.1.1 Edit User groups	9
4.2 User.....	10
4.2.1 Edit Users	10
4.3 Right.....	11
4.3.1 Edit Rights	12
4.4 Forbidden passwords.....	12
4.4.1 Edit forbidden passwords.....	13
5 Parameter sets of the user administration definitions	14
5.1 Parameter sets in alphabetic order.....	15
5.1.1 Authorization level.....	15
5.1.2 Comment.....	15
5.1.3 Disable unused account after...[days].....	15
5.1.4 Forbidden Password	15
5.1.5 Full Name	16
5.1.6 Lock account due to failed logins for...[minutes]	16
5.1.7 Login	16
5.1.8 Machine code.....	16
5.1.9 Maximum permitted login failures.....	16
5.1.10 Name.....	17
5.1.11 Password	17
5.1.12 Password change.....	17
5.1.13 Password change interval.....	18
5.1.14 Propose last user name for... [hours].....	18
5.1.15 Rights	18
5.1.16 Text.....	18
5.1.17 Status	19
5.1.18 Time until automatic logoff.....	19
5.1.19 User Groups	19
5.1.20 Users of this group may be deleted.....	20
6 User administration configuration	21
6.1 Domain user administration in VisiWinNET	24
6.2 cross project user administration	26

1 Preamble

About this manual

This manual contains specific information on the VisiWinNET user administration such as (amongst others) the explanation of the involved components, the operating reference of the editor, and the description of the system definitions.

Questions and Problems

For technical questions and problems please contact your responsible INOSOFT agent or the INOSOFT GmbH Support under +49 (5221) 16 66 02 or email: Support@INOSOFT.com

Frequent questions and problems are dealt with on our homepage under www.inosoft.com

There you will also find a support area for direct contact with our Main Office.

2 User administration introduction

The VisiWinNET user administration serves for assignment of personal rights within the visualization application. Input controls can be locked; Information access through output controls can be denied.

VisiWinNET supports two different user administration systems:

Level-oriented user administration User and controls can be assigned to one of 999 levels. If during runtime the level of a control is higher than the one of the logged-in user, operation of the control will be refused.

Rights-oriented user administration A right is allocated to the Controls in the application that the user must possess in order to operate the control element (e.g. "edit recipe". Subsequently, the users are allocated the rights that they can exercise.

This makes particular sense in a Client-Server system when multiple staff member hierarchies (groups of staff members who are split up into rights levels independently from each other) work in the network. The clearing procedure determines the comparison between the rights of users and Controls.

User administration is processed through three different definitions in the project database:

User group Pools the users into a group, and contains the characteristic parameters for all those users. Via the user group all references to the rights required for the operation of the application are administrated.

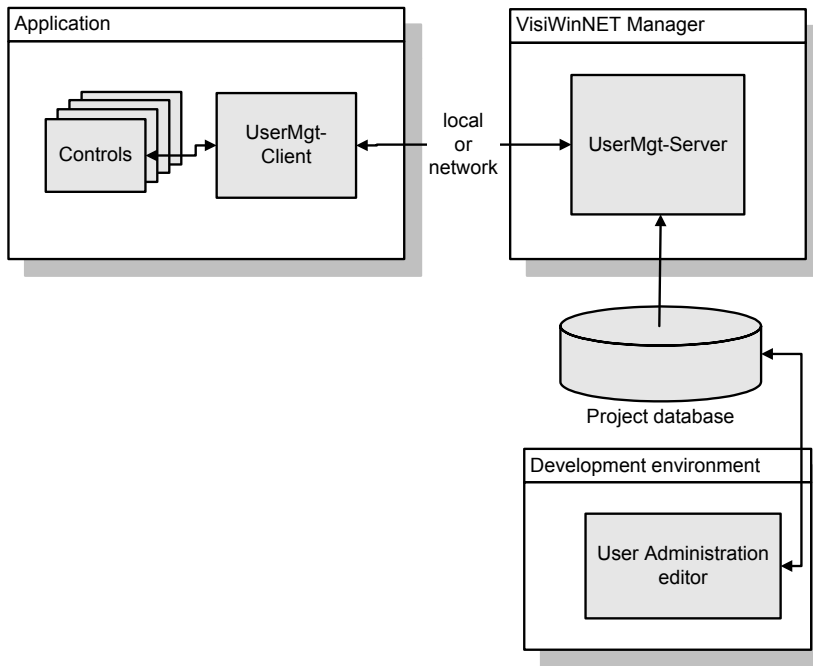
User Contains access information (Login and password) and the activity state of a user.

Right Rights define the information that is allocated to the Controls of the application. Via the "Authorization" property a right is allocated to a control element. A logged-on user must possess a reference to that right in his user group definition to be allowed to operate that control element.

Rights are only used in the rights-oriented user administration.

In the following block circuit diagram the VisiWinNET user administration components are introduced. Further component information is provided as cross-reference.

Components of VisiWinNET User administration



Component	Description
UserMgtServer	The UserMgtServer is initiated through the VisiWinNET Manager. Its task is to realize user login and administration for a project centrally. The user login process is routed to the UserMgtServer. The Server verifies the login information by comparison with project database data. Administrative process, as i.e. adding a new user during runtime, is passed on to the UserMgtServer through the client applications. Thus, the UserMgtServer provides the new administration information as permanent data in the project database for all connected clients.
UserMgtClient	The UserMgtClient manages the control enabling of a visualization application. Additionally it provides the connection between the administration dialogs of the VWSDialog-component and the UserMgtServer.
Controls	The Controls design the visualization application surface. Each control contains release information through the property "Authorization" (either a authorization level or else the name of a right). With new user login the UserMgtClient is notifying the controls. In dependence on the user releases the controls switch to either active or inactive.

Continued information is provided in the handbook "VisiWinNET Class library".

User administration editor	The user administration editor serves for designing of definitions during development time. It is integrated in the development environment. The processed definitions here are saved in the project database. An operating reference is provided in the chapter "User administration editor" in this handbook.
Project database	The project database contains the user administration definitions that are designed in the development environment through the user administration editor. During runtime the UserMgtServer manages the data. Continued information about user administration definitions and their parameter sets are provided in the chapters of the same name in this handbook.

2.1 Right- or level-oriented

As introductory described VisiWinNET supports two different user administration systems. Only one at a time, of both the systems can be activated for a VisiWinNET-Project, which means, that the decision for one of the systems is to be made already with designing. To understand, where the differences between the two systems are, the functions of the two systems are to be explained.

Explanation of system functions

Level-oriented user administration	<p>An authorization between 0 and 999 is assigned to each user. Additionally, each control with which input can be processed a respective release level is assigned to. After login the user authorization is notified to all controls. On the basis of their release level, they decide about active (Release of control \leq User authorization) or inactive presentation (Release of control $>$ User authorization).</p> <p>The user authorization distribution enables the structure of a user hierarchy: According to the user authorization level, more releases can theoretically be reached in the application. Usually, the staff hierarchy of a company is duplicated by this system: A manager has all access rights assigned to his staff, and additionally to all access rights assigned to him. His manager has more even rights, etc.</p>
Rights-oriented user administration	<p>The Controls of the application are linked with rights from the project database. A right can e.g. be named "may edit recipes".</p> <p>User groups are also linked with rights. While a control element can always have a link with one right only a user group can contain any number of rights.</p> <p>The distribution of individual rights allows the creation of multiple rights hierarchies that are independent from each other. This can be appropriate in a Client-Server system if it is operated by multiple departments that have no connection with each other in the hierarchy.</p>



Selection of the system is processed in the "user administration configuration" (also see chap. 6).

Difference between the systems

The level-oriented system represents a simple way of user administration structuring. The class-oriented system requires a great planning effort but enables apportionment of the users into several hierarchies. The following example presents a simple case that excludes level-oriented user administration. The project can only be realized through class-oriented user administration.

Example:

- Operating of the visualization is to be processed by two different departments, independent of each other.
- Each department has a private area in the application, meant for them exclusively.
- In addition there are controls that can be operated of both departments.

Management through level-oriented user administration is excluded as:

- A user always has more rights than all users that own lower authorization.
- A user owns all user rights of those who are authorized in a lower level.

Management through class-oriented user administration runs as follows:

Projecting of rights

In this case three rights can be created:

Name	Description
A	Input only by Dept. A
B	Input only by Dept. B
Common	Input by all

Projecting of user groups

A user group is projected for every department.

Within the user groups the references to the rights can be defined:

Users of Dept. A are allocated access to the rights "A" and "Common".

Users of Dept. B are allocated access to the rights "B" and "Common".

Allocation of rights to the NET Controls

Controls that are only to allow access by one department are allocated the appropriate right ("A" or "B"). Controls that are to be operated by both departments are allocated the "Common" right.


At runtime a control element is advised which rights are allocated to the logged-on user. The control element compares these rights with the clearance. If the control element's right is not included in the rights of the logged-on user the control element is blocked. The example below shows several constellations:

Right in the control element	Rights of the currently logged-on user	Control element activated
A	A/Common	Yes
A	B/Common	No
B	A/Common	No
B	B/Common	Yes
Common	A/Common	Yes
Common	B/Common	Yes

This shows that Controls with the rights A and B are really only restrictedly usable by the appropriate department. Controls with the individual Common right can be operated by both departments.

3 User administration editor

VisiWin provides an editor for designing the user administration system. VisiWin integrates the editor in Visual Studio during the installation. The user administration definitions are stored within the project database.

The user administration editor is represented by the symbol  in the VisiWin-Project Explorer.

After first selection of the node "user administration" the editor is being initialized. In dependence on the selected administration system following minor groups will be inserted into the project explorer:

Level-oriented user administration

Configuration user administration	Contains as a VisiWinNET properties page global settings that control the performance of the user administration. Here for example the switching between level and rights-oriented performance is effected.
User groups	All designed user groups are listed under this node. After selecting a User group the included user definitions will be presented in the table editor. Designing of a User group is enabled through the object menu of the respective node.
Forbidden passwords	Here a collection of passwords can be projected that are not recognized as valid passwords at runtime.

Right-oriented user administration

in addition is displayed:

Rights	Rights are only displayed in the rights-oriented user administration. They are shown – as are the users – in the index editor.
---------------	--



After adding the server component "user administration", the system is set to "level-oriented", that means, the node "rights" is hidden. System change over is processed through the node "Configuration user administration".

Project-spanning user administration Server

In the configuration of the user administration the "Project-spanning user administration Server" setting expands the Project Explorer by the following nodes:

User group allocation with other computers	This allows in table format the allocation of users to other groups for every projected computer name.
---	--

4 User administration definitions

Below a collection of definitions in the VisiWinNET user administration. In addition the information is provided as to which product version contains the definition.

Definition	VisiWinNET Standard	VisiWinNET Embedded	VisiWinNET Compact
User group	✓	✓	✓
User	✓	✓	✓
Right	✓	✓	✓
Forbidden password	✓	✓	✓

4.1 User Group

User groups are represented in the project explorer under the access node of the same name. All users, contained in a User group show the same behaviour, defined through the User group parameter sets.

User groups contain following functionality:

- Definition of single rights for class-oriented user administration
- Definition of authorization level for level-oriented user administration
- Automatic logoff with time stamp
- Definition of interval for creation of a new password
- Automatic user deselecting with exceeding a defined number of failed login attempts

User group parameter sets

Name	Description
Authorization level	Defines the level, assigned to the group users.
Users of this group can be deleted	Locks during runtime the possibility of user deletion of this User group.
Comment	Optional text for definition
Disable unused account after...[days]	Determines for how long a user account cannot be used before it is barred by the system
Lock account due to failed logins for...[minutes]	Time span of deactivation with reaching the "maximum number of failed logon attempts"
Maximum allowed logon attempts	Number of logon attempts as of which a user will be deselected.
Name	Definition name.
Password change	Settings that cyclically force the user to select a new password

Password change interval	Number of days after which a user has to change the password.
Propose last user name for... [hours]	Determines for how long the user last logged on to the system is pre-selected in the login dialog
Rights	Determines the rights to which the user group refers.
Text	Language-switchable User group name during runtime.
Time until automatic logoff	Defines the time after which a user will automatically be logged off with not operating the visualization application.

4.1.1 Edit User groups

User groups are displayed in the Project Explorer under the equally named node. Every user group definition contains:

- an editable set of parameters: Here the name or for example the link with the projected rights can be set.
- users where applicable: User definitions are displayed in the table editor. They contain the real logon information of the persons that log on to the project at runtime.

The editor provides the following functions for projecting user groups:

Create new user group	Through "New" entry in the context menu of the "User Groups" node.
Edit parameters	A click on a user group node loads the appropriate parameters to the VisiWinNET properties page. Here the parameter values of the user group definition can be edited.
Delete user group	Through the "Delete" entry in the context menu of a user group the definition is deleted. In the process all secondary definitions (users) are also deleted from the project.

4.2 User

Users are edited in the table editor. They represent users, who can log on to the system with login and password. User definitions contain following functionality:

- Representation through name and login
- Individual lock possibility through the parameter set "active", etc.

User definition parameter sets

Name	Description
Comment	Freely choosable comment on definition
full name	Description of person
Login	Name, that serves for user identification.
Computer code	Alternative information for automate user logon.
Name	User name
Password	Authenticity check for login.
Status	Determines, whether and how a user can logon during runtime.

4.2.1 Edit Users

Users are projected in groups, and displayed in the table editor. Every user definition contains an editable set of parameters: Here the name, the password and further functions are set.

The table editor of the user administration is opened through a click on an appropriate node in the Project Explorer.

The editor provides the following functions for the projection of users:

Create new user	Through the "New" entry in the context menu of the table editor a new user is added to the project.
Edit parameters	The VisiWinNET properties page displays the parameters of the users highlighted in the table editor. Editing a user is, however, also allowed directly in the fields of the table editor.
Delete user	One or multiple user definitions can be deleted by: <ul style="list-style-type: none"> • first highlighting the trend definitions that are to be deleted (click on the selector column at the l.h. margin of the table, where applicable with the Ctrl or Shift key held down for multiple selection) • then selecting the "Delete" entry in the context menu of the table editor.

4.3 Right

Rights are used in two places of a VisiWinNET application:

- User groups can be allocated multiple rights.
- One right can be allocated to a control element through the "Authorization" property.

If a logged on user has in his user group tied in the right of a control element then that control element is activated.

Rights contain amongst others the following additional function:

- Localizable designator that can at runtime be displayed as a rights description in the administration dialogs of the user administration,

Parameter sets of rights

Name	Description
Comment	Freely choosable comment on definition
Name	Definition name.
Text	Localizable text of the definition
User groups	Determines user groups that can activate the right.

4.3.1 Edit Rights

Rights are displayed in the table editor if the equally named node in the Project Explorer has been clicked on. Every right contains an editable set of parameters: Here the name and further functions are set.

The table editor of the user administration is opened through clicking on the appropriate node in the Project Explorer.

The editor provides the following functions for the projection of rights:

Create new right Through the "New" entry in the context menu of the table editor a new right is added to the project.

Edit the parameters of a right The VisiWinNET properties page displays the parameters of the right highlighted in the table editor. Editing a right is, however, also allowed directly in the fields of the table editor.

Delete rights One or multiple rights can be deleted by:

- first highlighting the rights that are to be deleted (click on the selector column at the l.h. margin of the table, where applicable with the Ctrl or Shift key held down for multiple selection)
- then selecting the "Delete" entry in the context menu of the table editor.



Rights can only be edited if the user administration has been set to "rights-oriented".

4.4 Forbidden passwords

The definition allows explicit blocking of individual passwords. Passwords projected here cannot be assigned at runtime. The administration dialogs of the class library deny the user entry of a password locked here with a password change.

Parameters of the forbidden passwords

Name	Description
Forbidden password	Direct input of password that is not to be used at runtime.

4.4.1 Edit forbidden passwords

Forbidden passwords are displayed in the table editor if the equally named node in the Project Explorer has been clicked on. Forbidden passwords are directly edited in the table editor.

The table editor of the user administration is opened through clicking on the appropriate node in the Project Explorer.

The editor provides the following functions for the projection of Forbidden passwords:

- | | |
|--------------------------------------|--|
| Create new forbidden password | Through the "New" entry in the context menu of the table editor a new forbidden password is added to the project. |
| Edit | Editing a forbidden password is allowed directly in the fields of the table editor. |
| Delete forbidden passwords | One or multiple forbidden passwords can be deleted by: <ul style="list-style-type: none">• first highlighting the forbidden passwords that are to be deleted (click on the selector column at the l.h. margin of the table, where applicable with the Ctrl or Shift key held down for multiple selection)• then selecting the "Delete" entry in the context menu of the table editor. |

5 Parameter sets of the user administration definitions

The parameter description contains following information:

Block	Description
Parameter for	List of definitions that contain this parameter set.
Description	Provides a parameter functionality specification.
Database field	Name of the table column in the VisiWinNET-Project database
Data type	Parameter data type.
Default value	Value that is standardized assigned after insertion of a new definition.
Max. Length	Maximum length of possible input.

A parameter list of definitions in alphabetic order is provided in the following.

Parameter name	VisiWinNET Standard	VisiWinNET Compact	VisiWinNET Embedded
Authorization level	✓	✓	✓
Comment	✓	✓	✓
Disable unused account after...[days]		✓	✓
Forbidden password	✓	✓	✓
Full name	✓	✓	✓
Lock account due to failed logins for...[minutes]		✓	✓
Login	✓	✓	✓
Maximum permitted login attempts	✓	✓	✓
Name	✓	✓	✓
Password	✓	✓	✓
Password change		✓	✓
Password change interval	✓	✓	✓
Propose last user name for... [hours]		✓	✓
Status	✓	✓	✓
Text	✓	✓	✓
Time until automatic logoff	✓	✓	✓
UserGroups	✓	✓	✓
Users of this group can be deleted	✓	✓	✓

5.1 Parameter sets in alphabetic order

5.1.1 Authorization level

Parameter for	User group (level-oriented user administration)
Description	<p>In the level-oriented user administration it is determined through the authorization level, which authorization level users of this User group will take. Through the property "Authorization" a release level can be assigned to the controls. If the property value is less or equal with the authorization level value of the currently logged on user, the control is released for input.</p> <p>The level-oriented user administration is based on following principle: by means of the authorization level and the property "Authorization", a staff hierarchy can be created. The higher the authorization level of a user, the more releases can be received with the respective "Authorization" -value allocation of the input values within the application.</p>

5.1.2 Comment

Parameter for	User group, User, Right
Description	Through the comment, the designer is able to write comments on the definitions. The comment has no function during project runtime.

5.1.3 Disable unused account after...[days]

Parameter for	User group
Description	<p>Determines for how long a user account cannot be used before it is barred by the system</p> <p>This parameter eases the user administration. If a user leaves the company he will automatically be barred after the time span set here. Unauthorized logon under this account is, therefore, prevented.</p> <p>If the parameter is set to 0 there is no automatic barring. The user remains active indefinitely.</p>

5.1.4 Forbidden Password

Parameter for	Forbidden passwords
Description	Specifies a password whose assignation at runtime is to be blocked. When changing a user password at runtime the new password is compared with the collection of all forbidden passwords. If the system finds a match the assignation of this password is denied. The user is requested to choose a different password.

5.1.5 Full Name

Parameter for	User
Description	The "full name" serves the unequivocal identification of the user. Typically, the combination of first and surname is chosen. With homonymous names input is denied by the system.

5.1.6 Lock account due to failed logins for...[minutes]

Parameter for	User group
Description	Determines for how long a user account remains barred once a user has reached the "maximum permitted login failures". After the time span set here has passed the user is re-activated by the system. He can now again attempt to log on. Specification of the value "0" means that the user remains barred permanently. Where applicable he can ask an authorized person to re-activate him through the user administration dialogs.

5.1.7 Login

Parameter for	User
Description	The login serves the system for user identification. A user can logon to the system with login and password. While several users can have the same password, the login for every user must be unique within the complete system.

5.1.8 Machine code

Parameter for	User
Description	The parameter set "machine code" provides for alternative login information assignment. Here, i.e. labels of personalized chip- and bar code cards can be specified. If an inquiry of a device respective is implemented, user login through the code is possible. Via the classes in the "VisiWinNET.UserManagement" namespace an appropriate registration can be effected.

5.1.9 Maximum permitted login failures

Parameter for	User group
Description	Number of failed login attempts that will lock a user. If an unauthorized person tries to logon with an existing login name, the user will automatically be locked if the number of login attempts with wrong password exceeds the value specified here. If the value 0 for "maximum permitted unsuccessful login attempts" is specified here, any number of login attempts is permitted. The user will not be locked automatically.

5.1.10 Name

Parameter for	User group, Right
Description	User groups/Rights
	Definition name

5.1.11 Password

Parameter for	User
Description	<p>Through the assignment of a password for each user the personalized access to the system is guaranteed: A user has to identify with the personal login name and verify the identity through the password.</p> <p>The password is filed as numerical code in the project database. Not even the administrator can reproduce the password, which means, if the user does forget about his password, it cannot longer be inquired from the administrator. But, the administrator can provide the possibility of creating a new password through the runtime dialogs.</p>



Through the user administration configuration the minimum length for validity of a password can be defined. The attempt to input a shorter password will be denied.

General: Longer passwords increase the system protection.

5.1.12 Password change

Parameter for	User group
Description	Administrates settings that force the user to renew his password in pre-set intervals
Settings	

Invalid after ... [days] Number of days after which a user must select another password. To enhance system security there is the option to force all users to cyclically choose new passwords. Before the time limit set here runs out the user is requested to change his password. If he fails to do so he is deactivated by the user administration.

If "0" is set as a value this function is deactivated.

Minimum age ...[days] Number of days after password change within which the user cannot choose a new password.

In connection with the setting "Password can be used again after ... password changes" in the user administration configuration a user must avoid to change his password repeatedly in order to use his original password again.

Hint ... [days before] When a user logs on the system generates a message saying that he is due to select a new password. The value set here determines for how many days before the time limit runs out the message is to be shown.

5.1.13 Password change interval



Dieser Parameter ist ab der Version 6.2 Bestandteil von der Einstellung "Password change".

Parameter for

User group

Description

Number of days, after which a user has to change the password. For increase of system protection, there is the possibility of forcing the users cyclical to change their passwords. Before the exceeding of the time period, defined through the "Password change interval" the user is asked to change his password. If he does not, he will be deselected in the user administration.

If the value 0 is given as password change interval, the function is deselected.

5.1.14 Propose last user name for... [hours]

Parameter for

User group

Description

Determines for how long the user last logged on to the system is to be preselected in the logon dialog.

This option makes it easier for the user to log on again if for example he has been logged out automatically by the system, not used the visualization for some time or logged out because of short-term absence.

5.1.15 Rights

Parameter for

User group

Description

Determines the rights to which the user group refers. In the user group dialog all projected rights definitions are listed. Setting the control box to a right creates a link with that right. Controls whose "Authorization" properties contain that right can, therefore, be operated by the users of the group.

5.1.16 Text

Parameter for

User group, Right

Description

Localizable text that is displayed in the user administration dialogs at runtime instead of the definition name.

5.1.17 Status

Parameter for

User

Description

Determines the way of user login during runtime. A user can be deselected during development time already. This is especially necessary if i.e. training on the program is to be processed before starting, where the user is supposed to assign a password himself for the first time.

During runtime a user can be deselected through the administrator (if he is absent for a longer time).

The automatic deselecting is processed through the parameter set "maximum permitted login attempts": If a user forgets his password or else an unauthorized person tries to logon with an existing login name, the user will automatically be locked after several unsuccessful attempt.

Settings	Value	Description
Deactivated	0	The user cannot logon to the system. He is deselected in the administration dialogs during runtime.
Active	1	The user can logon with login name and password.
Active, next time change password	3	The user can logon with login name and a prescribed password. After login he will be asked to change his password.

5.1.18 Time until automatic logoff

Parameter for

User group

Description

Defines the period of time (in minutes) after that a user will automatically be logged off, because of not operating in the visualization. If a user forgets to log off after operating the visualization, this will be processed automatically after the specified period of time, defined in the parameter set "Time until automatic logoff". This will prevent that by mistake operating remains released after a user left his working place.

If the parameter is set to 0, automatic logoff will not be processed.

5.1.19 User Groups

Parameter for

Rights

Description

Determines the links with the user groups. In the rights dialog all projected user group definitions are listed. Setting the control box of a user group creates a link with the right. Controls whose "Authorization" properties contain that right can, therefore, be operated by the users of the group.

5.1.20 Users of this group may be deleted

Parameter for	User group
Description	<p>Locks the right to deletion of users of this User group during runtime.</p> <p>In certain system areas it is a duty to prove which users have ever been working on the system during the entire runtime of visualization. In this case the possibility of user deletion is undesirable.</p>
Settings	Description
False	Deleting users of this group is not permitted. This alternative is not shown in the dialogs of the user administration at runtime.
True	User deletion of this group is permitted.

6 User administration configuration

The configuration of the user administration allows system-wide settings.

The user administration configuration enables system-wide settings.

The configuration dialog of the user administration is opened through the equally named node in the Project Explorer. The settings are displayed on the VisiWinNET properties page.

Here the following settings are possible:

Index card	Setting	Description
Common	System	Determines which user administration is to be used. Further information about the different user administration systems can be found in chapter "Rights or level-oriented" (chap. 2.1).
	Minimum length user name	Determines the minimum number of characters required for a user name
	Maximum length user name	Determines the maximum number of characters required for a user name
Password policies 1	Minimum password length	Determines the minimum number of characters a password must contain to be accepted as valid.
	Maximum password length	Determines the maximum number of characters a password can contain to be accepted as valid
	Allow password reuse after ... [Password changes]	The UserMgtServer allows a user to establish a password that he has used before only after the number of password changes set here.
	Allow password reuse after ... [days]	The UserMgtServer allows a user to establish a password that he has used before only after the number of days set here.
	Minimum difference	Determines how many different characters a password must contain to be accepted by the system.
	Maximum subsequent equal characters	Determines how many identical consecutive characters are accepted in a password. As an example the password "AAAA" can be barred if the parameter is set to a value <4.
	Minimum difference to prior password ... [characters]	Determines by how many characters the new password must differ from the old one to be accepted by the system. As an example a change from the password "MyPassword1" to "MyPassword2" can be prevented.

Password policies 2

Password must contain letters

If a user changes his password the new password must contain letters. Otherwise the password change is not accepted.

Password must contain digits

If a user changes his password the new password must contain digits. Otherwise the password change is not accepted.

Password must contain special characters

If a user changes his password the new password must contain special characters. Otherwise the password change is not accepted.

Password must contain lowercase and uppercase letters

A password is only accepted if it contains lower as well as upper case letters.

Password must not be equal to user name

A password is only accepted if it not identical with the user name.

Special (not implemented in Compact)

local

Activates the user administration of the project. Only the data specified in the project are used.

Domain user administration

Activates the domain user administration (See chap. 6.1)

A domain user can belong to multiple user groups. One of these is the "primary" user group. Verification of user authorization can be set to two options.

- If only the primary user group of the logged-on user is to be checked for authorization the "primary user group" setting is to be selected.
- If all user groups of the loggon-on user are to be checked for authorization the "all user groups" setting is to be selected.

Windows local

Similar to the domain user administration here the user information of operating system and VisiWin application are linked. Here, however, there is no possibility for common administration of multiple projects distributed in the network.

cross project user

Determines that the project is to be used as a

**administration
(Server)**

central user administration project in the network.

The cross project user administration is used when multiple workstations are connected via a network, there is no Client-Server project, and still a common user administration is requested.

Further information is to be found in chapter "cross project user administration" (Chap.: 6.2)

The cross project user administration requires an extra runtime licence (see current price list).

**cross project user
administration
(Client)**

Determines that the project is to search the network for a central user administration project, and obtains the user data from there.

Further information can be found in chapter "cross project user administration" (Chap.: 6.2)

**Save full name in
runtime data**

When this option is activated the full user name is saved in the files created at runtime instead of the logon name. The following files are affected:

- Recipe files (change history/notes)
- Protocol files
- Historical message records (Notes)

6.1 Domain user administration in VisiWinNET

The VisiWinNET domain user administration allows to use Windows user data in VisiWinNET applications. In addition to the user locally administrated in VisiWinNET users of a Windows domain with an appropriate account can log on to a VisiWinNET application.

For this the user groups in the domain account that have been installed in a domain controller by the administrator are used.

Equivalent to the groups in the domain controller a homonymous user group must exist in the VisiWinNET user administration. An appropriate user need not be created.

Precondition

Domain controller	Windows NT 4.0 Server or Windows 2000/2003 Server
VWN-Workstation (Application computer)	Windows NT 4.0, Windows 2000 prof. or Windows XP prof. The workstation must be logged on to the domain. Membership of a Windows workgroup is not sufficient.

Activating the domain user administration

This option is found under "Special" in the configuration of the VisiWinNET user administration. The appropriate Windows domain and a matching domain controller for verification of the domain users are automatically identified from the settings of the workstation, and displayed in the diagnosis file when the application is started.

In addition the users locally created in the VisiWinNET user administration are accepted.

For every primary user group of a domain user an appropriate user group (homonymous) must be created in VisiWinNET in which the VisiWinNET-specific properties are set since these cannot be fully allocated in the domain administration. If the system does not find a matching local user group the fault value "vwNoCorrespondingLocalUserClass" is returned in the "LogOn" function.

Scope of functions

With the following functions of the user administrations it is first attempted to find the specified user in the local user administration. If he is registered there they system performs as usual. If the user is not found in the local list an attempt is subsequently made to register the user with the domain controller, identify – dependent on the setting of the "User authorization" option – either only the primary or all user groups, and establish a match with a local user group. If this is successful the system also performs as usual.

All information about this user can also be found out. The system recognizes automatically which users are to be obtained from the local user group, and which from the domain controller. Even the password can be changed in the domain controller.

The following functions obtain their information from the domain controller:

- UserManager.LogOn
- UserManager.LogOff
- UserManager..CurrentUser
- UserManager.VerifyUser
- User.Name
- User.FullName
- User.ChangePassword

All other functions perform as previously, and relate only to the users created locally. If the user is not found in the local user group the functions return "unknown user".

Remarks

If the VWN workstation runs under Windows 2000 prof. the VisiWinNET Manager must be registered as a service (access of "...\VWNManager.EXE /Service as otherwise it cannot check the users in the domain controller (not necessary under Windows XP prof.). After that the VisiWinNET Manager is to be found under the (System control -> Administration -> Services) system services. It is automatically started with the application start. A small particularity is to be observed. After the application is ended the VisiWinNET Manager is no longer ended automatically, i.e. the icon with the yellow bridge remains in the task bar next to the time indication. This has no negative effects and the VisiWinNET Manager is automatically re-connected with the next application start. The VisiWinNET Manager can be manually ended via the system services administration (stop service).

6.2 cross project user administration



The cross project user administration requires an extra runtime licence (see current price list).

The cross project user administration is used when multiple workstations are connected via a network, there is no Client-Server project but still a common user administration is desired.

This kind of user administration has the advantage of a common administration being possible. New users for example need only be added with one computer. Subsequently, all computers in the network have this new user information.

The cross project user administration is set in the VisiWinNET project via the user administration configuration on the "Special" index card. This determines the computer connection.

Server

The VisiWin project for the computer that is to administrate the user data at runtime must possess the setting "cross project user administration (Server)". In the user administration editor and at runtime user groups, rights and users are registered as in the local user administration.

In addition to the settings of the local user administration it can be determined for every user which user group he is to belong on which computer via the project explorer node "User group mapping on other computers". This makes it possible for example that a user has full access to the Controls of the visualization on one computer but only restricted access on another.

The computer names of the linked client projects are determined in the project configuration. Computer names defined here appear as columns in the table editor.

Client

The projects that at runtime are to obtain the user data from the common administration computer must in the configuration be set to "cross project user administration (Client)". The "Computer name" parameter specifies from which computer the user data are to be obtained.

In the client project the user groups projected in the server must be created homonymously. The rights and the links with the user groups must not be different. Users need not be projected here as the user data are obtained from the server at runtime.