

Security Manager

User Guide



Invensys

EUROTHERM

About

Title	Security Manager User Guide
Part Number	HA 028 131
Issue (Date)	3 (10/06)
Initially Supplied With	EurothermSuite Version 4.3

Contents

Security Manager User Guide

Security Manager	1
Welcome!	1
This is the Security Manager Help File	1
Related Documents	1
Project Organiser Online Help File	1
LINtools Online Help file	1
Overview of Security Manager	2
Why Security Manager	2
The 'Database'	2
Security Manager Utility	3
Standalone Utility	3
Project Utility	3
Open Security Manager	4
Configure a Database	5
Examples for Configuring a Database	5
Security Manager Window	7
Menu Regions	8
Menu Bar	8
Toolbar	8
Status bar	8
User global	11
What is the User Global tab?	11
Display Fields	11
Buttons	11
The Login dialog timeout field	11
The keep retired User Ids	11
The Maximum User Id length	11
The Maximum login attempts	12
The Maximum password length	12
The Minimum User Id length	12
The Minimum password length	12
The Password reuse period	12
User	13
What is a User?	13
What is the User tab?	13
Display Fields	13
Buttons	13
All Users	14
Active Users	14
A Current User	14
Current Logged in User	14
A Disabled User	14
A Retired User	14
A Recovery User Account	14
User group	15
What is a User Group?	15
What is the User groups tab?	15

Display Fields.....	15
Buttons.....	15
Deciding on User Groups	15
allocate a User to a group	16
Security items	17
What is a Security item?	17
What is the Security items tab?	17
Display Fields.....	17
Buttons.....	17
5000/6000 Series instruments.....	17
QuickChart Software	17
Review Software.....	18
T800 Visual Supervisor specifics.....	18
Windows Domain.....	18
Windows Domain specifics	19
Deploy Security	19
configure a Deployment computer	19
Now at the Deployment Computer	19
Deployable	22
Security zones	23
What is a Security zone?.....	23
What is the Security zones tab?	23
Deciding on Security Zones	23
What is Management Data?.....	24
configure Management Data.....	24
What is Access Rights?	25
configure Access Rights.....	25
How to.....	26
Open.....	26
Close	27
Exit	28
Login.....	29
Logout	30
Print.....	31
Master UNC path.....	33
Switch to MasterDB (database)	34
output to a printer	34
output to a .CSV file.....	35
select Print categories.....	35
Enable Security on EurothermSuite PC's	36
Save Changes	37
Discard Changes.....	38
Defining the Regulation	39
edit the User global tab parameters.....	40
How to configure the User global?	40
change the maximum login attempts	40
change the minimum password length.....	41
change the minimum User Id length	41
change the maximum password length.....	41

edit the User tab parameters	43
How to add a User	43
How to configure the User?	44
How to show Active or All Users	45
Display Active or All users by.....	45
re-enable a User	45
edit the User group tab parameters.....	45
add a User group	46
How to configure the User group?	47
delete a User group	47
edit the Security items tab parameters	49
add a Security item	49
How to configure the Security items?	50
modify a Security item	50
deploy to selected Security items	51
What is Deployment?	53
Example 4 - Deployment Computer configuration	53
edit the Security zones tab parameters	54
add a Security zone	54
How to configure the Security zone?	55
allocate Security items	56
allocate User groups	57
Example 1 - Allocating Security items / User groups	59
Example 2 - Management Data	59
Example 3 - Access Rights	59
edit the Security Manager permissions.....	59
edit the 5000 Series permissions.....	60
edit the 6000 Series permissions.....	62
edit the EurothermSuite PC permissions	63
edit the QuickChart software permissions	65
edit the Review software permissions.....	66
edit the T800 Visual Supervisor permissions	67
edit the Windows Domain permissions	68
Configure Security item parameters.....	69
configure the Access level access rights	69
configure the Acknowledge Alarms access rights.....	69
configure the Action Demand Writes access rights.....	69
configure the Adjust Inputs access rights	69
configure the Admin only access rights	70
configure the Administration access rights	70
configure the Administrator Password field.....	70
configure the Administrator UserId field.....	70
configure the Alarm authorisation field.....	71
configure the Alarm signing field.....	72
configure the AlarmHistMaxItems access rights	73
configure the Archiving Control access rights	73
configure the Audit Ports	74
configure the Audit Trail field	75
configure the Authorisation field.....	75
configure the Authorise access rights	76
configure the Auto Logon UserId field.....	76
configure the Batch Control access rights	76
configure the Change Alarm Setpoints access rights	77
configure the Change Language access rights.....	77
configure the Change Password on Expiry access rights	77
configure the Change own expired password access rights	78

configure the Change own password access rights	78
configure the Chart Annotate access rights	78
configure the Chart Approve access rights	79
configure the Chart Open/Close access rights	79
configure the Chart Release access rights.....	79
configure the Chart Review access rights	80
configure the Chart Setup access rights	80
configure the Confirmation field	80
configure the Connect from remote access rights.....	81
configure the Create Chart access rights	81
configure the Custom1 to Custom5 access rights.....	81
configure the Custom6 to Custom10 access rights.....	81
configure the Debug access rights	81
configure the Delete retired users field	82
configure the Deploy Security access rights	82
configure the Deploy existing users field.....	83
configure the Disable Service Account field.....	83
configure the Display access level field	83
configure the Edit Deployable Flag access rights	84
configure the Edit Maths Constants access rights	84
configure the Edit Output Channel Default access rights.....	84
configure the Edit Security Manager setup access rights	85
configure the Edit security item data access rights	85
configure the Edit user data access rights	85
configure the Edit user global data access rights.....	86
configure the Edit user group data access rights	86
configure the Edit zone access rights data access rights.....	86
configure the Edit zone configuration data access rights	87
configure the Edit zone management data access rights.....	87
configure the Event Permission access rights.....	87
configure the Export Data access rights	87
configure the Export Historical Trend access rights	88
configure the Export Setup access rights.....	88
configure the FTP access rights.....	89
configure the Faceplate Configurator access rights	89
configure the Faceplate Modify access rights	89
configure the File Services access rights.....	90
configure the Full Configuration access rights	90
configure the Full Security access rights.....	90
configure the Global Alarm Acknowledge access rights	91
configure the Groups access rights.....	91
configure the IO data writes access rights	91
configure the Inactivity timeout field	92
configure the Lockout Level field.....	92
configure the Log Invalid Times field.....	93
configure the Login by User List field	93
configure the Login timeout field	94
configure the Modify Chart View access rights	95
configure the Notes field	95
configure the Offline data writes access rights.....	95
configure the Operator Point Display access rights	95
configure the Operator group global access rights.....	96
configure the Operator groups access rights	96
configure the Override Server Redundancy access rights	97
configure the Password Expiry field	97
configure the Paste/Delete Files access rights	97
configure the Perform Upgrade access rights.....	98
configure the Preset Counters access rights.....	98

configure the Preset Totalisers access rights	98
configure the Print Setup access rights	98
configure the Print access rights.....	99
configure the Recipe Download access rights	99
configure the Record Logins field	100
configure the Recovery account field.....	100
configure the Recovery user field	101
configure the Reference Number access rights	101
configure the Remote access rights.....	102
configure the Reset Maths access rights	102
configure the Save Chart access rights	102
configure the Save/Restore access rights	103
configure the Set Clock access rights	103
configure the Sign access rights.....	103
configure the Signing field	103
configure the Start/Reset Timers access rights	104
configure the Synchronise Files access rights	105
configure the System User writes access rights	105
configure the Tag Security Area access level fields.....	105
configure the TagEdit access rights.....	105
configure the Task Switch access rights.....	106
configure the Transfer Files access rights	106
configure the Trend Global access rights	106
configure the Trends access rights.....	107
configure the User1 to User4 access rights	107
configure the View Only access rights.....	108
configure the View Security Data access rights.....	108
configure the With unapplied changes field	108
configure the downloaded Recipes field	109
Editing parameters	110
change the User Id	110
change the Password field.....	110
change the Change Password field	111
change the Password expiry time period	111
change the Remote User Id.....	111
change the Remote password field.....	112
change the Enabled.....	113
change the Fullname	113
change the System field	113
change the Retired field	114
change the Reason field	115
change the Login dialog timeout.....	115
change the keep retired User Id.....	115
change the Password reuse period	116
change the maximum User Id length	117
Default accounts	118
Default Account 1	118
Default Account 2	118
Incorrect User Id or Password	118
Access Level enumeration's	118
User group Access Level.....	118
Tag	118
Location	118
Tag Security Area	118
Tag Access Level	118
Change Password	118
delete a Security item	120

recover a Security Database.....	121
Recover T800 Visual Supervisor Security Database	121
Customise Security Manager	125
How to show Active or All Users	125
How to hide/show toolbar.....	125
How to hide/show status bar	126
Regulatory Defaults.....	127
Regulatory Defaults	127
Other Information	134
What is a Master Database?	134
What is a Client Database?	134
What is the PC Name/Code?.....	134
LIN Information	135
Default LIN User Names.....	135
Default LIN Access	135
LINOPC Client Security	136
LINOPC Security specifics	137
Tag and LINBlock specifics	138
Tag Profile Configurator specifics.....	138
Tag Security Areas specifics	139
create a Tag Security Area (Project Organiser)	139
Command Line Parameters.....	140
Path to SecManDb.ujx Command line parameter.....	140
Command line prompt example	140
Command Line parameters.....	140
/RegServer Command line parameter	141
Command line prompt example	141
/Help Command line parameter.....	141
Command line prompt example	141
/Login Command line parameter	142
Command line prompt example	142
/Secure Command line parameter.....	142
Command line prompt example	142
/HideTaskBar Command line parameter	143
Command line prompt example	143
/Autodeploy Command line parameter	143
Command line prompt examples	144
Shortcut example	144
/UnRegServer Command line parameter	145
Command line prompt example	145
Audit Trail Information.....	146

Examples **147**

 Example 1 - Each User in their own User group solution 147

 Example 2 - All Users in a single User group solution 147

 Example 3 - Simple Management Data and Access Rights solution 148

 Example 4 - Complex Management Data and Access Rights solution 148

 Example 4a - Modified Complex Management Data and Access Rights solution 149

 Example 4b - Modified Complex Single Access Rights solution 150

 Example 4c - Modified Complex Multiple Access Rights solution 151

 Example 5 - Tag Security Areas configuration solution 152

 Example 6 - Typical System configuration solution 153

Security Manager help **160**

 To get help on using Security Manager, click the shortcuts: 160

 Getting specific help: 160

Index **I**

Security Manager

Welcome!

This is the Security Manager Help File

The purpose of the Security Manager is to define security features and User actions (Management Data and Access Rights) for systems containing a combination of instruments including,

- Computer's, running a Project based system and/or configured in a Windows Domain
- 5000 Series instruments
- 6000 Series instruments
- QuickChart Software
- Review Software
- T800 Visual Supervisor

It has a wide range of configuration options allowing a user to configure a system needing only basic security through to a system that needs to comply with the 21 CFR Part 11 (Electronic Records and Electronic Signatures) for FDA Regulations.

Related Documents

Project Organiser Online Help File

Project Organiser provides a central managed environment for configuring and maintaining a Project. A large part of the system configuration, particularly those involving assignment of Tags to functions, can be configured directly from within Project Organiser. Where further configuration is required, the relevant application will be launched from the context-sensitive Application Toolbar.

LINtools Online Help file

This Online Help file document describes the use of LINtools Engineering Studio, giving enough detailed information needed to configure the function blocks in a control strategy, both offline and online.

Note

Contact your distributor if these documents are unavailable.

Overview of Security Manager

Why Security Manager

Security Manager simplifies the ability to manage and control all security features across a security configuration by providing a central environment to set-up user accounts and carry out regular account management. It provides update functionality to user accounts, logins, password changes, etc., and has the ability to distribute the security database to any Security item nodes, including itself, in the security configuration. This Utility includes security features such as secure electronic signatures, and '[Audit Trail](#)' trace-ability.

Note

The [Security Manager Utility](#) separates the system security configuration in to various security parameter categories. Each security parameter category is defined on a tab.

It defines security in the following terms,

- [Users](#)
- [User groups](#)
- [Security items](#)
- [Security zones](#)
 - [Management Data](#)
 - [Access Rights](#)
 - [Tag Security Areas](#)

Note

For a full description of these features refer to [Tag and LINBlock specifics](#).

There are other areas of security outside the Utility which are covered by

- [5000 Series instruments](#)
- [6000 Series instruments](#)
- [QuickChart Software](#)
- [Review Software](#)
- [T800 Visual Supervisor](#)
- [Windows Domain](#)
- [Tag Profile Configurator](#)
- [LINOPC Security](#)

The 'Database'

The Security Manager database is automatically configured with the [2 default accounts](#). An [ESDataSrv](#) system account can also be automatically created to perform system functions.



User Id	Administrato	Engineers	Operators
ADMIN	X		
ADMIN2	X		

With the enabling and disabling of Management Data (features) and activating Access Rights (including levels of confirmation), the database provides a secure system. The Management Data and Access Rights are controlled and stored by the [master database](#). A [client database](#) exists on other Security items in the security system.

Security Manager Utility

Security Manager Utility can be used either as a standalone Utility or as part of a Project depending on the installation. The Utility is installed in a directory at

C:\Programs Files\eurotherm\SecurityManager

There are no differences in the operation of the 2 methods.

Standalone Utility

If installed as a standalone Utility it is NOT automatically incorporated as part of any Project. This enables instruments without in-built security to be configured as part of a security environment.

Once installed, Security Manager can be opened and the database accessed using a correct User Id and Password by simply selecting

Start > Programs > Eurotherm > Security Manager

Project Utility

If installed as part of a Project it is automatically incorporated in a Project folder. The Utility is accessible through a Project folder of a Product Type.

New projects are created by,

Start > Programs >... > New Eurotherm Project

After creating a Project the Security Manager can be opened and the database accessed using a correct User Id and Password.

Note

Security Manager can also be accessed via the Operations Server, when attempting to edit a password.

Open Security Manager

The User may configure the database after completing a successful login to the selected database. A User may open a Security Manager [master database](#) or a [client database](#) database on any Security item node. The SecManDb.ujx icon represents the Security Manager Utility.



SecManDb.ujx

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown 'File > [Switch to MasterDB](#)' to open the master database.

To open Security Manager,

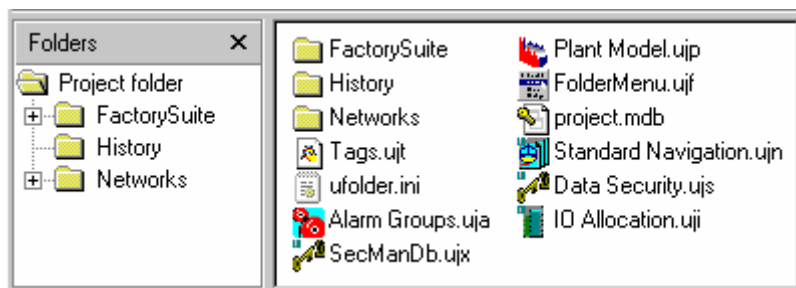
1 At the computer,


An Standalone Utility

- Open an explorer window and use standard Windows navigation commands to locate the Project Folder.
- Open the Project Folder.

A Project Utility

- Select 'Start > Programs > Eurotherm > Project Folder > <Project Name>'.
This opens a window displaying the following Development Tools.



- In the Project Folder, open the Utility (SecManDb.ujx icon) using the  (or 'File > Open...').
 - Alternatively, double-click the SecManDb.ujx icon.
 - Before database opens, a Login dialog window appears. To edit a Security database, enter a valid User Id and associated Password.
 - [Default User Ids and Passwords](#) have been configured and can be used.
- 2 A correct login will open the database and display the [Security Manager Window](#).

IMPORTANT NOTE

An incorrect login results in a [Login attempt failure](#). Exceeding the maximum consecutive login attempts value results in a 'Lockout'.

There are 2 prompts prior to opening a database for the first time, a

- Reminder to enter a '[Master UNC Path](#)',
 - And a request to set a [level of Regulation](#).
- 3 Now, [configure the database](#).

Configure a Database

To simplify the configuration of the database it has been divided into security elements, each represented by a tab.

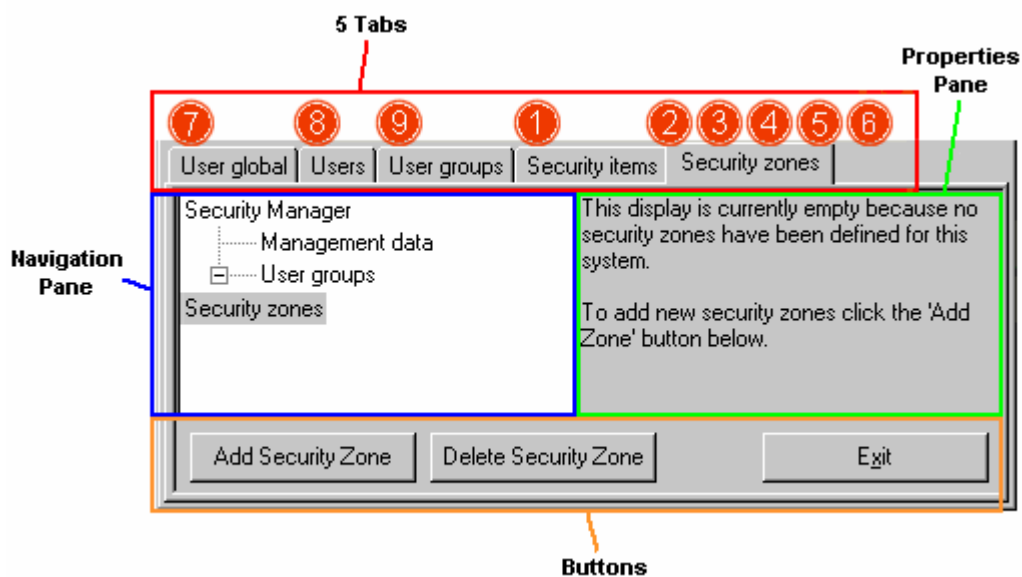
There are no definitive rules about how to structure security, but it is important remember there is usually more than 1 possible configuration. Users and Security items are easy to create as they relate to individual Users and computer's, instruments and programs.

Where complications start to arise is when considering what Security zones and User groups to assign. This is due to the Users, the type of functions they will need access to, and the levels of security needed to successfully complete the tasks required.

- [Deciding on Security zones](#)
- [Deciding on User groups](#)

Note

Click any field in the illustration below to display the relevant details. For brief instructions select each numeric indicator in order.



Examples for Configuring a Database

The following examples are not complete but they attempt to show how Security zones, User groups and Tag Security Areas can be configured.

Example: One User to one User Group solution

- explains a 1 User, per User group, per Security zone solution.

Example: All Users in one User group solution

- explains an All Users, per User group, per Security zone solution.

Example: Simple Management Data and Access Rights solution

- explains a User group by name, per Security zone solution.

Example: Complex Management Data and Access Rights solution

- explains a multiple Security zone and multiple Access Rights solution.

Example: Tag Security Areas Configuration solution

- explains a User group by name, per Security zone and additional Tag Security Area solution.

Example: Typical System Configuration solution

- explains a Tag Security Area solution that restricts access dependant on where the request originated.

Configuring database Step 1

Identify the Security items in the system.

Security items are added at the Security items tab. These items are generally instruments, computers and/or programs that require a User Id and Password before use. The Security items in the security configuration are controlled by the deployment of the master database.

Configuring database Step 2

Decide what Security zones are needed.

Security zones are added using a button at the Security Zone tab.

Configuring database Step 3

Allocate Security items to Security zones.

Security items are allocated at the Security Zone tab.

Configuring database Step 4

Decide the Management Data required within each Security zone.

Configure the Management Data at the Security Zone tab.

Configuring database Step 5

Decide what User Groups are needed.

Are any of the roles (Access Rights) common across a number of the Security zones. If so a single User group for these roles will suffice. Otherwise consider a User group per role, per Security zone.

Configuring database Step 6

Allocate User groups to Security zones.

User groups are allocated at the Security Zone tab.

Configuring database Step 7

Edit the overall User security Project parameters. This entails editing login and password constraints in the User Global tab parameters.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown 'File > Switch to MasterDB' to open the master database.*

Configuring database Step 8

The User accounts need to be added. The User tab has all the features to do this. It also has the option to view current or all users.

Note

Accounts can **ONLY** be deleted from the database if using the **Default Regulation** constraints and the **Keep Retired User Id** field on the User global tab reads False. Any other configuration will store account details allowing the database to automatically check that accounts are unique when added. This is in accordance with 21 CFR Part 11.

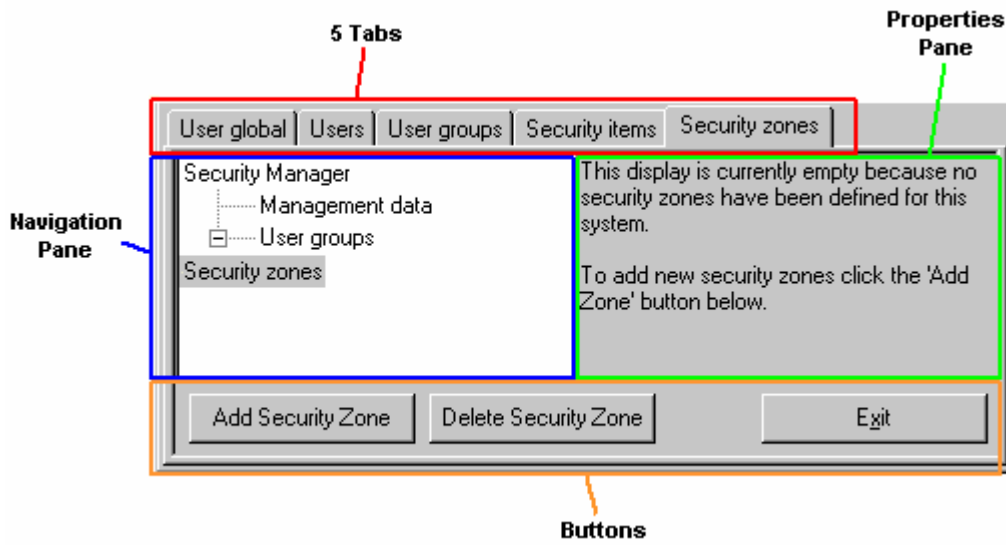
Configuring database Step 9

Allocate Users to User Groups.

This step allocates Users to a User group that has or will have sufficient Management Data and Access Rights to enable the User to successfully complete the tasks required.

Security Manager Window

The Security Manager database is split into the security categories. The categories are displayed as a tab across the top of the Security Manager window. Each tab displays tabulated security configuration parameters.



 Click to display the relevant configuration details.

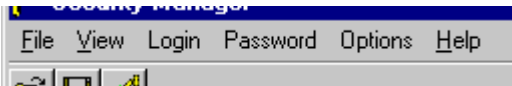
Menu Regions

The Menu Regions can be divided into command and information areas.

Menu Bar

The Menu Bar is a special toolbar at the top of the *Editor* screen that contains the pulldown commands. Each pulldown displays a further list of commands.

The Menu bar contains the following items,



Toolbar

The Toolbar has 3 icons that enable quick access to the Open, Save and Deploy Security options. It is displayed by default and is located at the top of the Security Manager window.

The Toolbar contains the following items,



Note

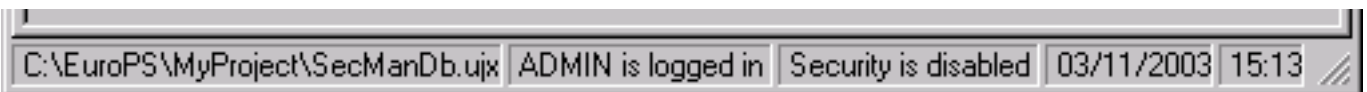
The Toolbar can be displayed or hidden using the **View > Toolbar** command.

Status bar

The Status Bar displays Security Manager database status information, including location, current user, security status, date and time. It is displayed by default and is located along the foot of the Security Manager window. A check mark indicates it is currently displayed.

The Status Bar displays specific *Editor* information. It is displayed by default and is located along the foot of the *Editor* screen.

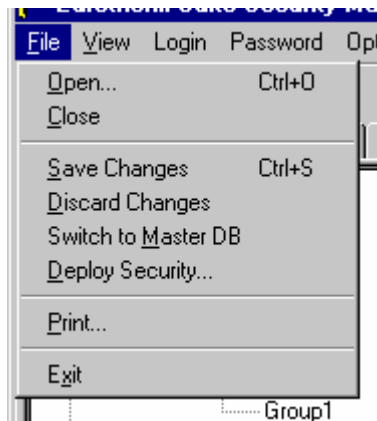
The Status bar contains the following items,



Click an option to find out more!

File pulldown

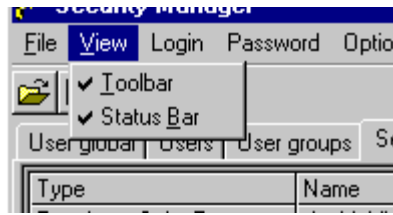
The File pulldown menu enables the manipulation of an individual database offering the following options.



Click to display the relevant configuration details.

View pulldown

The View pulldown menu enables the Toolbar and/or Status Bar to be temporarily hidden.



 **Click to display the relevant configuration details.**

Login pulldown

The Login pulldown allows the User to get 'into' and 'out of' a security database using a valid User Id and password.

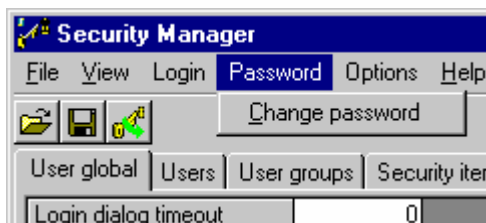


The Login pulldown menu offers the following functions,

- [Login](#)
- [Logout](#)

Password pulldown

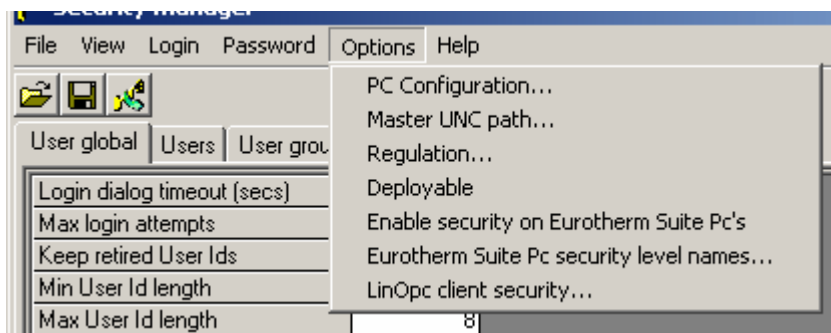
The Password pulldown menu offers the opportunity to change the current Users password. This is achieved via the [Change Password](#) option.



 **Click to display the relevant configuration details.**

Options pulldown

The Options pulldown menu allows the User to manipulate the security of the Security Manager master database itself. This is achieved using the,



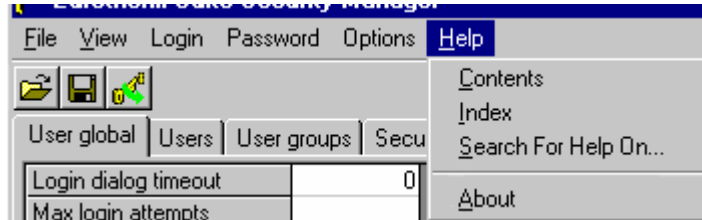
 **Click to display the relevant configuration details.**

Help pulldown

The Help pulldown menu is divided into 2 sections.

- Documentation (including Contents, Index, and Search for Help on)
- Utility (About)

Any of the first 3 options opens the on-line help documentation with the selected as the priority command.



Click to display the relevant details.

The About option displays the program details including the name, version number, and description.

User global

What is the User Global tab?

The User global tab is used to display and edit security configuration parameters applicable to all User accounts. The parameters are defined below.

Display Fields

[The Login dialog timeout field.](#)

[The Maximum login attempts field.](#)

[The keep retired User Ids field.](#)

[The Maximum User Id length.](#)

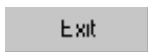
[The Minimum User Id length.](#)

[The Maximum password length.](#)

[The Minimum password length.](#)

[The Password reuse period.](#)

Buttons



 [How to configure the User global tab](#)

The Login dialog timeout field

This field is edited to increase or decrease the amount of time a Login prompt window will remain displayed on the T800 Visual Supervisors throughout the system before disappearing from view (see [change the login timeout field](#)).

This field can only be configured within the selected [Regulatory value constraints](#).

By default this function will NOT automatically timeout (disabled), indicated by the '0' (zero) displayed.

This is a 21 CFR part 11 compliant feature.

The keep retired User Ids

This field is edited to allow User Ids and Passwords to be stored in the Project database or to be erased when the User is configured as retired.

■ True

Retired User Id's and Passwords remain in the Project database.

■ False

Retired User Id's and Passwords are erased when retired.

It is recommended that...

User Ids and Passwords remain stored in the Project database to ensure unique identities for all Users through the Security Project.

This is a 21 CFR part 11 compliant feature.

The Maximum User Id length

The field is edited to increase or decrease the maximum number of characters used for ALL User Id's in the Project database (see [change the maximum User Id length](#)).

This field can only be configured within the selected [Regulatory value constraints](#).

The Maximum login attempts

This field is edited to increase or decrease the amount of consecutive failed logins attempted before the being automatically disqualified (locked out) (see [change the maximum login attempts](#)).

Note

An account, disqualified due to exceeding the maximum login attempts can be re-enabled by setting this field to '0'.

This field can only be configured within the selected [Regulatory value constraints](#).

This is a 21 CFR part 11 compliant feature.

The Maximum password length

This value in this field is edited to increase or decrease the maximum number of characters used by the Administrator for ALL password's in the database (see [change the maximum password length](#)).

This field can only be configured within the selected [Regulatory value constraints](#).

The Minimum User Id length

The value is edited to increase or decrease the minimum number of characters used for ALL User Id's in the database (see [change the minimum User Id length](#)).

This field can only be configured within the selected [Regulatory value constraints](#).

The Minimum password length

This value in this field is edited to increase or decrease the minimum number of characters used by the Administrator for ALL password's in the database (see [change the minimum password length](#)).

This field can only be configured within the selected [Regulatory value constraints](#).

The Password reuse period

This field is edited to increase or decrease the minimum number of days before an expired password may be used again (see [change the Password reuse period](#)).

A password cannot be used again before this time period has elapsed.

This field can only be configured within the selected [Regulatory value constraints](#).

User

What is a User?

A User is the owner of an account that accesses the security database of assigned to a Security item. There are three kinds of User accounts,

- [Current User](#)
 - There are various grades of current Users, including Administrator, Supervisor, Engineer, and Operator, each having specific requirements for the system.
- [Disabled \(Disqualified\) User](#)
- [Retired User](#)

The account may be part of one or more user groups and contains all the details needed for a User to login to Security items types within the system. These details include a User Id and password. The data in these accounts is controlled by the User global element that is used to determine things such as maximum and minimum password lengths. By default a User without [Access Rights](#) (read only) can only change their password.

It is recommended that...

default account parameters are NOT changed, except when first attempting to login to the database to ensure strict security for the User throughout the security configuration. This is a 21 CFR part 11 regulation and can be automatically configured using the [Change Password](#).

What is the User tab?

This tab defines, and enables the User to edit parameters specific to each User account.

Display Fields

[User Id](#)

[Password](#)

[Change Password](#)

[Password Expiry](#)

[Remote User Id](#)

[Remote Password](#)

[Fullname](#)

[System](#)

[Retired](#)

[Enabled](#)

[Login Attempts](#)

[Locked Out](#)

[Reason](#)

Buttons

Add user

Active users

All users

Re-enable User

Exit

 [How to configure the User tab](#)

All Users

Users configured for Security Manager. Disqualified Users are greyed out.

Active Users

These Users comply with ALL the requirements of the Security database.

A Current User

This User is able to access the database depending upon the Access Rights configured.

A T800 Visual Supervisor highlights the User account green until saved.

A Current User can be disabled (Disabled User) or terminated (Retired User).

Current Logged in User

This part of the Status Bar shows the current User of the database.

A Disabled User

A Disabled User is denied access to the Security database. This User account is refused access if

- the Administrator has disabled the account,
- consecutive attempts with an incorrect password exceed the value entered in the Max Login Attempts field (User Global),
- or the password has expired.

Note

Only automatically disabled accounts can be re-enabled.

A T800 Visual Supervisor highlights a disabled account red, and if the password has expired the account is highlighted orange.

There is no colour reference for computer User accounts.

This user account can be re-instated as a current user or be Retired (terminated).

A Retired User

A Retired User is an account that has been terminated.

These User details can either remain in the Project database to prevent duplication or reuse of User Ids (21 CFR part 11 compliant) or can be erased depending on the configured Regulations.

Note

The account will only be erased if the Keep Retired Users field is set to False and the Default Regulations are configured.

Beware

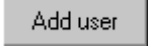
A Retired User cannot be re-instated.

A Recovery User Account

A Recovery User Account is an emergency User account with full access rights.

The Recovery User can access the database using a blank User Id and a password that is valid for 1 hour ONLY (as supplied).

Add User button

Press the  button to start the new User wizard.

Re-enable User Button

Press this button to re-instate a locked out User if the,

- User account has been disabled ('Enabled' field reads 'False', Reason field reads 'Account disabled').
- login attempts have been exceeded,
- password has expired.

User group

What is a User Group?

A User group is a collection of 1 or more User accounts. However, Users may belong to more than one User group. Access Rights assigned to a User group control ALL allocated User accounts. An unlimited number of User groups can be supported.

[Deciding on User groups](#)

What is the User groups tab?

This tab consists of a grid listing all Users and User groups (when added) and 3 automatically created User groups, Administrators, Supervisors, Engineers, and Operators.

Display Fields

UserId column

Other columns

Buttons

Add user group

Delete user group

Exit

[How to configure the User groups tab](#)

Deciding on User Groups

The extreme cases that can be set-up for User groups are,

- each User in their own User group or
- all Users in a single User group.

Either of these cases could be sensible, but only in a very small system. The guiding principle is that a User group corresponds to a role within a Security zone. The role of the User group is defined by the Access Rights configured for each User group has within a Security zone. Roles could be System Administrator, Supervisor, Engineer, and Operator. A User may perform multiple roles within a Plant. This can be implemented by allocating the User to multiple User groups.

If a particular role, for example Engineers, is common across some or all Security zones a single User group for Engineers would suffice. However if there are distinct groups of Engineers working in different zones then each Security zone will require an Engineer's User group.

In general fewer User groups make it the easier to change the security set-up, although not enough User groups may make the system inflexible in the future.

It is recommended that...

due to the quickness of creating User groups and allocating Users to/from User groups, start with a minimal set of User groups and add User groups as required.

Add User group button

Operated to display the Add User Group dialog box. When completed the User Group appears on the User Group tab.

An Administrator

An Administrator has control of ALL User accounts via the database, by default.

The Administrator should be able to add, disable/enable, and retire User accounts. The Administrator can also modify accounts, but this should require approval by a second Administrator.

An Operator

This User has the most restricted level of access, generally, similar to read only.

Delete User group button

Operated to display the Delete User Group dialog box. When completed the User Group is removed from the User Group tab.

allocate a User to a group

When Users are added to a database, they have yet to be allocated to a User Group. Users may be allocated to any number of User Groups in order to enable different access within a single Security zone.

Allocate a User to a group by

- 1 Choosing the appropriate User Id and clicking in any number of User group boxes in the row. The User group name will then only be able to perform those tasks configured at the Security zone tab.

Note

To remove the User from a User group, uncheck the applicable group.

User Id	Administrators	Engineers	Office Operator	Operators
ADMIN	X			
ADMIN2	X			
Beth	X		X	
Dick			X	X
Harry		X	X	
Thomas	X			X

- 2 Finally [save changes](#).
 - Now proceed with adding [Security items](#).

Security items

What is a Security item?

The definition of a Security item is any object within the system that contains a security database and controlled by Security Manager. These objects, typically instruments, PC's and/or programs require a **User Id** and **Password** before use. Security Manager Utility is an example of a Security item, and is special because it is always present.

All Security items are configured by type and require a unique name. They are displayed in type order when the Security items tab is selected.

A Security item can only be integrated to a single Security zone.

What is the Security items tab?

This tab defines and enables the User to edit the unique name and address of each Security item.

Display Fields

Type

Name

Enabled

Address

Buttons

Add security item

Delete security item

Modify security item

Deploy Security...

Exit

[How to configure the Security items tab](#)

5000/6000 Series instruments

This Utility operates by providing a Centralised Security Control environment for a system consisting of any combination of Series 5000 and 6000, T800 instruments and/or computers running Review.

In order for it to operate as required, the Enable Security and Centralised Security Control check box's may need to be configured. The default Security Database path is added automatically, but may need to be verified.

When checked, the Enable Security check box states that security is needed, and the Centralised Security Control check box states the Security Manager Utility will control the security of computer's and instruments. If the Centralised Security Control check box remains unchecked it is automatically configured for use with Review software on a single computer.

QuickChart Software

Security Manager Utility operates in one of two modes, providing security features with the QuickChart Software on a single computer, or providing a Centralised Security Control environment for a system consisting of any combination of Series 5000 and 6000, T800 instruments and/or computers running Review or QuickChart.

When providing security restrictions (Access Rights only) to QuickChart Software on a single computer the permissions apply to QuickChart Software only.

In order for the Security Manager Utility to operate as required, the Enable Security and Centralised Security Control check box's may need to be configured. The default Security Database path is added automatically, but may need to be verified.

When enabled, the Enable Security check box states that security is needed, and the Centralised Security Control check box indicates the Security Manager Utility will control the security of computer's and instruments. If the Centralised Security Control check box remains empty it is automatically configured for use with QuickChart software on a single computer.

Review Software

Security Manager Utility operates in one of two modes, providing security features with the Review Software on a single computer, or providing a Centralised Security Control environment for a system consisting of any combination of Series 5000 and 6000, T800 instruments and/or computers running Review or QuickChart.

When providing security restrictions (Access Rights only) to Review Software on a single computer the permissions apply to Review Software only.

In order for the Security Manager Utility to operate as required, the Enable Security and Centralised Security Control check box's may need to be configured. The default Security Database path is added automatically, but may need to be verified.

When enabled, the Enable Security check box states that security is needed, and the Centralised Security Control check box indicates the Security Manager Utility will control the security of computer's and instruments. If the Centralised Security Control check box remains empty it is automatically configured for use with Review software on a single computer.

T800 Visual Supervisor specifics

After a security database has been downloaded to a T800 Visual Supervisor, it will reject any other databases unless they have been generated from the same source. To enable the T800 Visual Supervisor to accept databases generated from a different source it is necessary to reconfigure as master mode and then back into client mode.

Windows Domain

The Windows Domain security item type allows Security Manager to configure users either locally on a PC or globally in a domain. When adding this security item type the user must specify the item name and whether the item is a Domain or a PC. The security item name is how it is referenced within Security Manager, it may be convenient to make this the same as the PC/Domain name but it is not necessary.

IMPORTANT NOTE

Due to Windows preventing external processes from reading passwords or setting the creation dates, the Windows Domain Security Item causes Password Reconciliation and Password Expiry limitations.

The Windows Domain Security item type updates the Windows security for the User groups assigned to the same Security zone when the database is deployed.

For each User allocated to the domain it update the following properties.

- UserIds
- Passwords
- User descriptions
- Enable flag
- Failed Login attempts
- Group membership

It updates the following password polices.

- Password minimum length
- Password expiry time

It updates the following User account lockout polices

- Maximum login attempts

During deployment, Security Manager detects changes made to the Windows security and reconciles those changes back into the Security Manager database. However, certain limitations exist when attempting to deploy the Security Database to a Windows Domain Security item.

IMPORTANT NOTE

Security Manager deploys all User account properties, but [Windows software restricts the deployment](#) of the Password Reconciliation and Password Expiry parameters.

Windows Domain specifics

Windows restricts deployment of the Password Reconciliation and Password Expiry fields of the Windows Domain Security Item. This prevents external processes from reading passwords, or setting the creation dates respectively.

The prevention of external processes from reading passwords restricts any Windows User password from being reconciled in to Security Manager. This means that deployment of the Security Manager database will override any Windows User passwords generated in Security Manager.

As part of the Windows Domain Security Item, Password Expiry dates can be configured, however individual User password creation dates are prevented. This means the Password Expiry will only remain correct if deployed on the same day the Password Expiry date was changed.

Note

These are also displayed on the Add Windows Domain Security Item dialog.

Add security item button

Starts the Security item creation wizard. This enables the creation of computer items with unique 'Security item name' and 'Project path' and T800 items with unique 'Security item name', 'Lin port name' and 'Lin db name'.

Modify security item button

Operated after selecting the item opens the Modification dialogue window. This enables the selected item parameters to be changed.

Delete security item button

Operated after selecting the unwanted item starts the Security item deletion procedure. When completed the item and all its configured parameters are removed from the database.

Deploy Security**configure a Deployment computer**

Configuring a Deployment computer is necessary for systems requiring autodeployment of the security database.

Autodeployment ensures the latest changes to any Security database in the system will be deployed to the remaining Security databases. This is achieved by each Deployment computer comparing the Master Security database revision to the Security database revision of all the Security items in its assigned Security zone. The Master Security database is updated with the changes from the Security database of the Security items in the Security zone. Then each Deployment computer deploys the Master Security database to the remaining security databases in the Security zones.

Example: Deployment Computer configuration**IMPORTANT NOTE**

Each Deployment Computer MUST start the Security Manager Utility using the [/Autodeploy Command line parameter](#)

Configure a Deployment zone by

- 1 Ensuring that the master SecManDb.ujx has the appropriate PC listed in the PC Configuration table.

Options > PC Configuration

and it is checked as Deployable.

Options > Deployable

- 2 Next, click the Security zone tab, and then the in the navigation pane click the Security zone name that will need a Deployment computer configured.

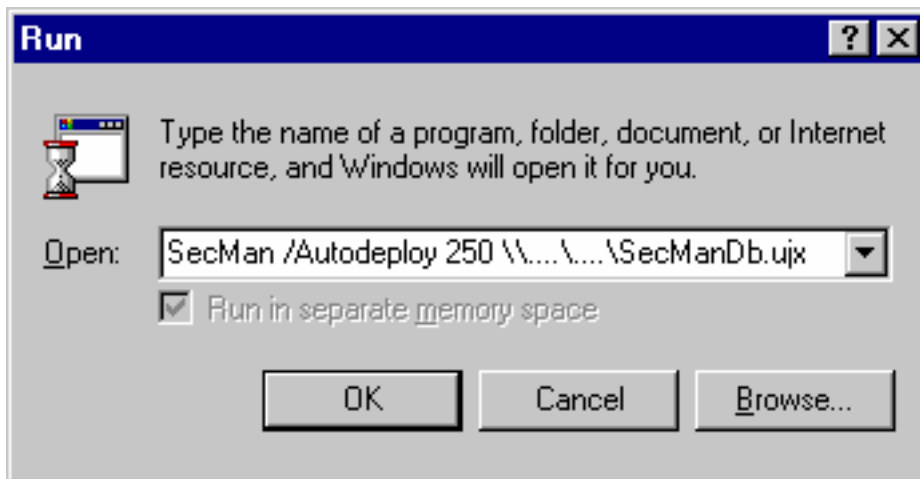
This displays the Deployment Computer configuration window.

- 3 From the drop down list select the PC for that Security zone.
- 4 Finally [save changes](#).

Now at the Deployment Computer

- 5 Start up the SecManDb.ujx using the /AutoDeploy Command Line parameter.

Command line prompt example



"SecMan" /AutoDeploy 60 "\\EuroPS\MyProject\SecManDb.ujx"

"SecMan" /AutoDeploy 300 "SecManDb.ujx"


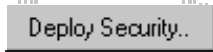
Note

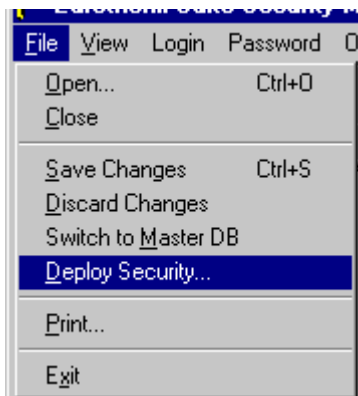
The full path can be omitted if the Security Manager Utility and the Security Manager database operate from the same directory.

Deploy Security

This function allows the master database to be 'Deployed' to selected Security items.

The deployment of the master database can be initiated by either

- Clicking the  on the Toolbar,
- Clicking the  button available via the Security items tab, or





- Selecting 'File > Deploy Security'.

Any of the previous operations will open the [Deploy Security window](#) allowing the User to replicate the master database to selected destination nodes.

- [How to Deploy a Security Database](#)

Deploy Security Window

The Deploy Security window is displayed to allow the 'deployment' of the master security database to selected Security item nodes. It is displayed after selecting  from the Toolbar,  from the Security items tab, or from the 'File > Deploy Security'.

Display fields

Security items

Log

Buttons

Deploy

Deploy all

Note

This button can be used in conjunction with the Zones drop down list if available.



Exit

Summary display field

This lists the current deployment status of the Security items.

Deploy All/Zone button

Operating this button replicates the master security database to all security items in the security configuration. Deployment will NOT occur if operated before selecting the destination.

This button is used in conjunction with the Zones drop down list. Used to start the deployment to either ALL Security items (button reads Deploy All) or the Security items in the zone selected from drop down (button reads Deploy Zone) after successfully confirming the operation if requested.

Deploy Security... button

Opens the Deploy Security window. This enables the Deployment of a Security database to selected items.

Deploy button

Operating this button replicates the master security database to an individual destination or groups of items by selecting the first and last item in a group while continuously pressing the 'shift' key on the keyboard. Deployment will NOT occur if operated before selecting the destination.

Log display field

Displays an ordered list of operations when deploying the master database including 'reconcile' (retrieving and collating databases and ensuring all relevant changes are saved to the master security database) 'download' (replicating the master security database) and any errors that have been found.

Exit (Deploy) button

Operating this button closes the 'Deploy Security' window, cancelling the operation.

Deployable

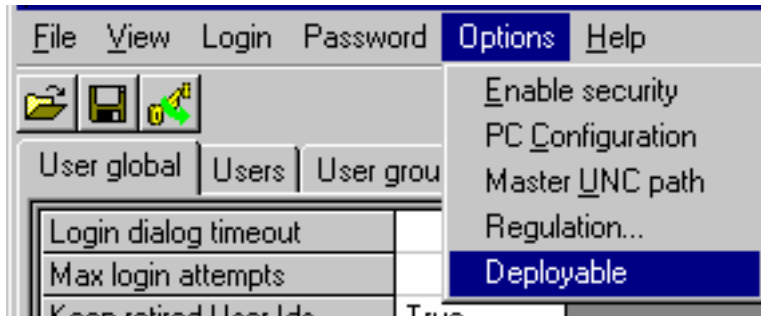
This function allows non-privileged Users to replicate the database to an individual destination or groups of Security items without requesting a signature.

Primarily this option can be used to deploy the database after changing a password.

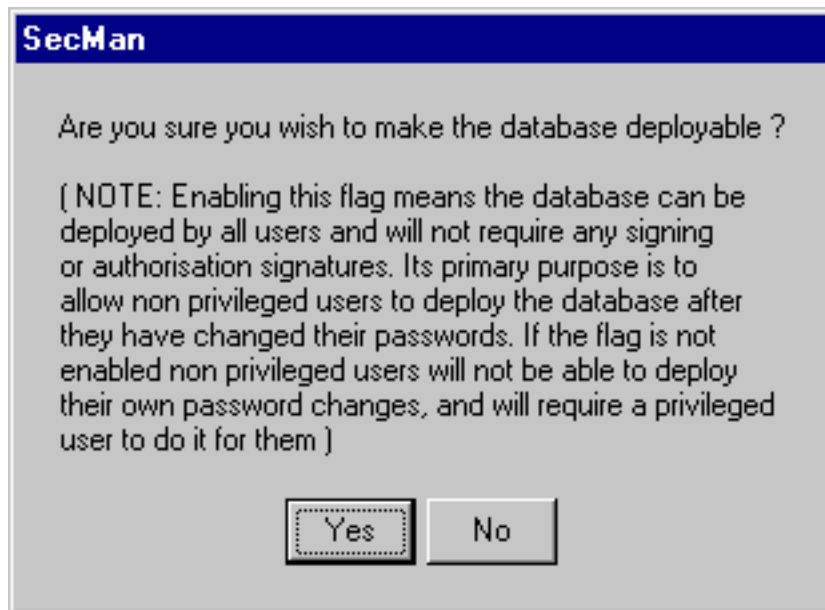
A check mark beside the option indicates it is a currently deployable database.

To define the Deployable database

- 1 Select '**Options > Deployable**' from the Menu Bar. A dialog window appears.



- 2 Read the information displayed and then click **Yes** to define the database as deployable or not depending on its current status, or **No** to cancel the command.



Security zones

What is a Security zone?

A Security zone is a grouping of Security item(s) and/or User group(s) and may not necessarily be a physical boundary. Security items within a zone display the [Management Data](#) configured for each Security item type, whereas Security items within a User group display the [Access Rights](#). A Security item cannot be allocated to multiple Security zones. User Groups are assigned Access Rights to the Security Zone.

Note

A Security zone is NOT the same as a Tag Security Area (formerly Security Area).

Each allocated Security item type and User group inherit the Management Data and Access Rights configured for the Security zone they are allocated to.

See Also [Deciding on Security zones](#)

What is the Security zones tab?

This tab defines the allocation (set-up) of Security items and User groups and the configuration of [Management Data](#) specific to each item type and Access Rights specific to each User group available within the selected zone.

Display Fields

Navigation pane (left hand)

Properties pane (right hand)

Example 1: Allocating Security items and User groups

- This example shows how to allocate Security items and User groups to a Security zone.

Example 2: Displaying management data

- This example shows how to display the required Security zone management data.

Example 3: Displaying access rights

- This example shows how to display the required User group access rights.

Example 4: Deployment computer configuration

- This example shows how to configure and set up of the Security Manager database for AutoDeployment on the specified Deployment Computer.

Buttons

Add Security Zone

Delete Security Zone

Exit

 [How to configure the Security zone tab](#)

Deciding on Security Zones

Probably the most important decision when setting up the security is to make sure that appropriate Security zones are created. Security zones allow the configuration of the [Management Data](#) (security features). Generally, less Security zones mean that security is easier to manage.

IMPORTANT NOTE

ALL security items in a security zone share the same security features.

More explicitly Security items of the same type (computer, Instrument, program (excluding Review Software which does not have Management Data)) will share the same Management Data (security features).

Earlier Security systems could only support a single Security zone apart from Security Manager, i.e. all computers in the system share the same security access.

A single Security Zone configuration will suffice for many systems. However if decided that Security item nodes require different security features then multiple Security zones can be used.

Add Security zone button

Operated after entering a Security zone name in the field beside creates and displays a new Security zone in the main display.

Delete Security zone button

Operated after entering a Security zone name in the field beside enables the deletion of Security zones.

Security Zone selection field

When selected this drop down list displays all the Security zones in the system.

The selection of All zones from the list indicates that the Security database will be deployed to all Security items in all Security zones.

The selection of a specific Security zone from the list causes the Deploy all button to change to a Deploy zone button. At which point only Security items in the selected Security zone will be deployed to.

What is Management Data?

Defines security features that can be enabled within the constraints of the selected Regulation on any Security item excluding Review Software that does not have Management Data.

Example

Audit Trail and Electronic Signatures are enabled or disabled on Security Manager or computer Security items when using the Default Regulation constraints.

Management Data are Security features that may be 'ON' (enabled) or 'OFF' (disabled) or a value that initiates a feature. If the Management Data is 'OFF' (disabled) the feature is NOT be available to the User group.

configure Management Data

Management Data are features available within a Security item that can be enabled or disabled. If a Management Data option has been enabled any User with the appropriate Access Rights option activated can perform the Management Data option.

Example

If 'Sign' Management Data is enabled () any User allowed to authenticate changes ('Sign' Access Rights) may do so. If the 'Sign' Access Rights are disabled ('Sign' Access Rights) the User will NOT be allowed to authenticate changes.

Each item has specific editable management data available to the User.

Select the appropriate point below for relevant details.

- [Security Manager Management Data](#)
- [EurothermSuite PC Management Data](#)
- [Review Software Management Data](#)
- [QuickChart Software](#)
- [5000 Series Management Data](#)
- [T800 Visual Supervisor Management Data](#)
- [Windows Domain Management Data](#)

What is Access Rights?

Defines what actions are available to each Security item type and the User group has before changes can be implemented.

Access rights are either a 'level of Confirmation' or an 'action'. A 'level of Confirmation' requires the User in the User group to accept changes by complying with the requested level of response before any changes can be implemented. An 'action' can only be used if the User group has the access rights to use it.

configure Access Rights

Access Rights allow or prohibit a User to use the configured Management Data.

Example

If 'Sign' Management Data is enabled () the 'Sign' Access Rights MUST be enabled () to allow the User to authenticate changes. If the 'Sign' Access Rights are disabled () the User will NOT be allowed to authenticate changes.

Each item has specific editable Access Rights available to the User.

Select the appropriate point below for relevant details.

- [Security Manager Access Rights](#)
- [EurothermSuite PC Access Rights](#)
- [Review Software Access Rights](#)
- [QuickChart Software](#)
- [5000 Series Access Rights](#)
- [T800 Visual Supervisor Access Rights](#)
- [Windows Domain Access Rights](#)

How to...

Open

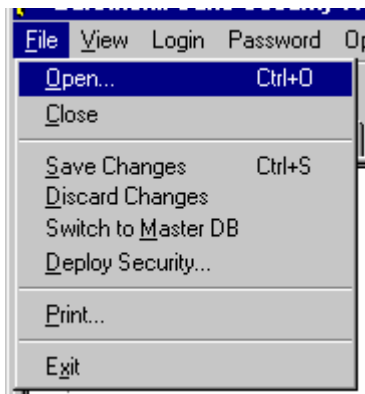
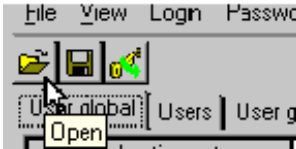
This function allows the User to find and open a database from the security configuration.

It is recommended that...

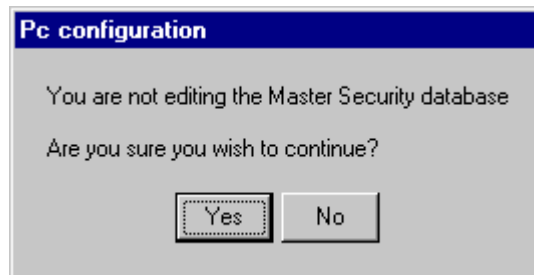
if a database is already open, save the changes before opening another.

Open a database by,

- 1 Selecting '**File > Open**' from the Menu Bar to display a browse dialog box.
 - Alternatively, click the Open toolbutton.



- Using standard windows navigation browse for the SecManDb.ujx file and open.
- If attempting to open a client database the following window is shown. Press '**Yes**' to open the client database and '**No**' to return to a blank Security Manager window.



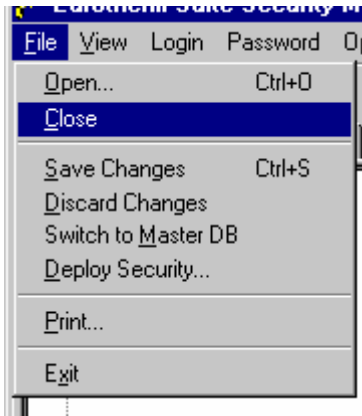
- 2 The user is prompted to [Login](#). After a successful login the selected Security Manager database will appear.

Close

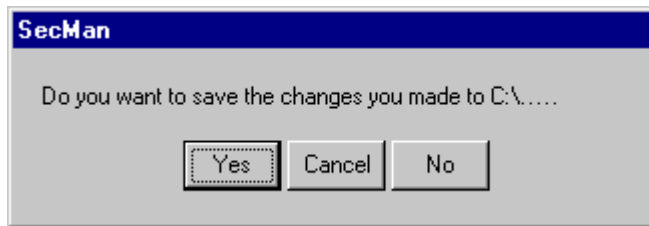
This function closes the database, returning to a blank Security Manager Window, after prompting to save any changes.

Close the current database by,

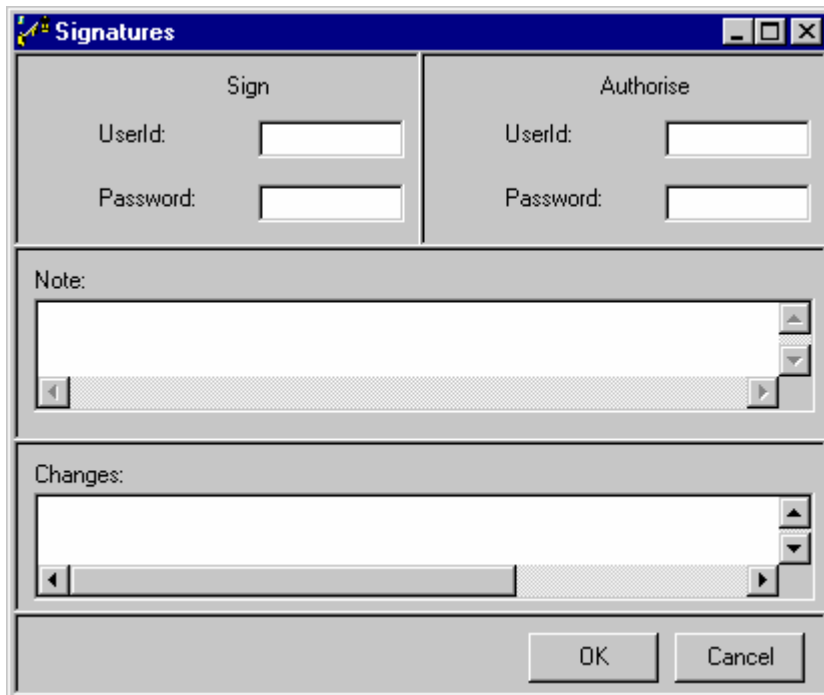
- 1 Selecting '**File > Close**' from the Menu Bar.



- 2 The save changes dialog window appears, press '**Yes**' to save any changes, and '**Cancel**' to return to the current Security Manager window. Select '**No**' to discard any changes made since the last save and revert to a blank Security Manager window.



If the 'Sign', 'Authorise' and/or 'Note' Management Data and Access Rights are configured a window is displayed with the appropriate fields available. Press '**OK**' to save any changes, and '**Cancel**' to return to the current Security Manager window

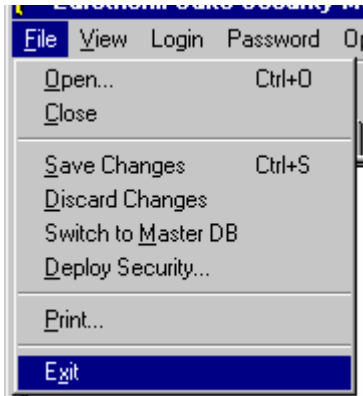


Exit

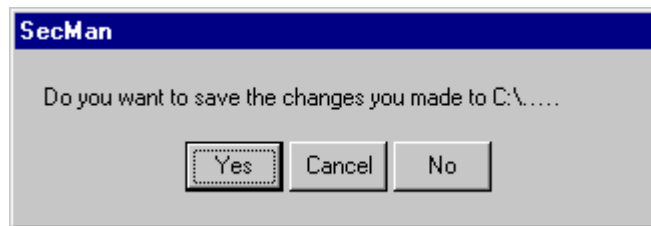
This function is similar to the 'Close' option. It terminates this Utility and returns to the Project Folder.

Exit the Utility by,

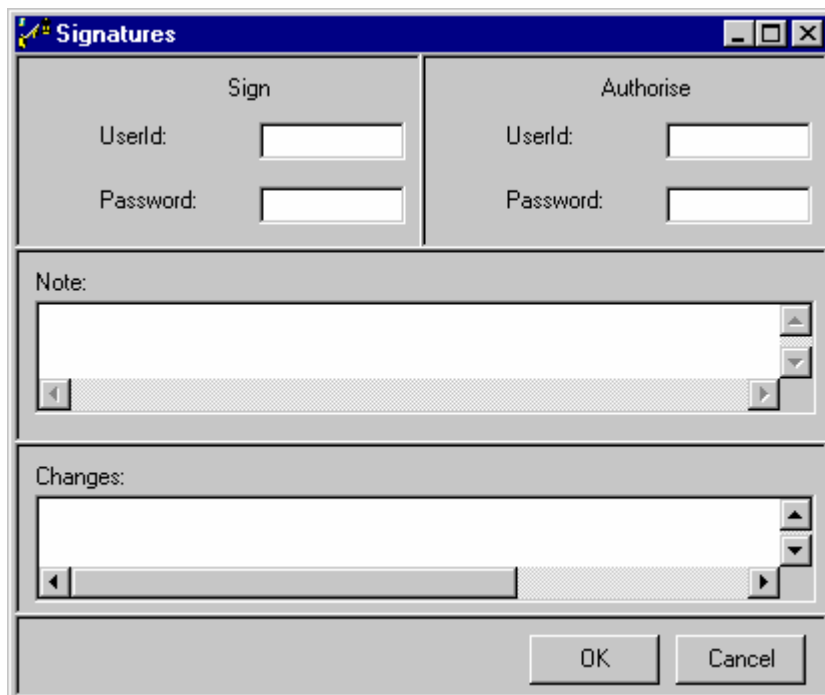
- 1 Selecting the  or 'File > Exit' from the Menu Bar.



- If changes have not yet been saved a dialog window appears.
- 2 At the prompt, click the appropriate button. 'Yes' to save any changes and close, 'Cancel' to return to the current Security Manager window or 'No' to discard any changes made since the last save.



- If the database is configured to requested 'Signatures', 'Authorisation' and 'Note', and additional dialog window appears. Complete the required fields and observe the database amendments listed in the 'Changes' field.



- Click 'OK' if satisfied with the information or 'Cancel' to discard **ALL** changes made. The dialog window and the Utility closes. The Project Folder is now active.

Login

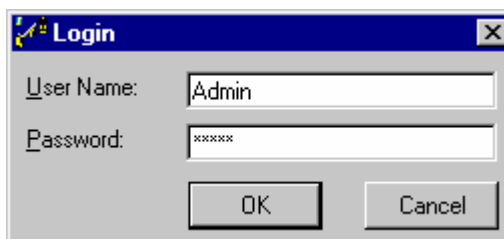
The function enables the User to access a database using a valid User Id and password.

To login,

- 1 Select '**Login > Login**' from the Menu Bar to display a dialog window.



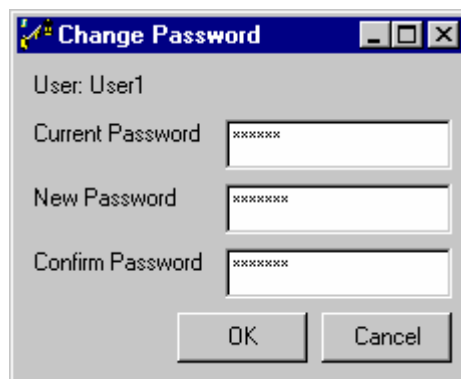
- 2 Enter a correct '**User name**' and '**Password**' in the appropriate fields. Click the '**OK**' button to attempt a login and '**Cancel**' to return to the logged out state. The login is successful if a correct User Id and password were input and there was NOT a prompt to change the password.



If the '[Change password](#)' field in the '**User**' tab is set to '**True**' the following prompt appears.

Note

If attempting to login using an unauthorised User account, a prompt appears, press '**OK**' to return to a logged out database.



- 3 At this dialog window, complete the fields, entering a new unique password and repeat the new password in the confirmation field. Accept the changes by clicking the '**OK**' button.

Note

For security purposes passwords are '**always**' displayed as '**xxxxxxx**' irrespective of the constraints specified in the [User global tab](#).

- 4 The database returns to a logged out state. Repeat steps 1, 2 and 3 to login.

Logout

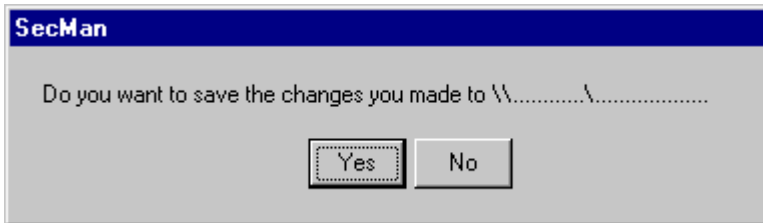
This function enables the User to close of the database, returning to the blank Security Manager Window, after saving or discarding changes if requested.

To logout,

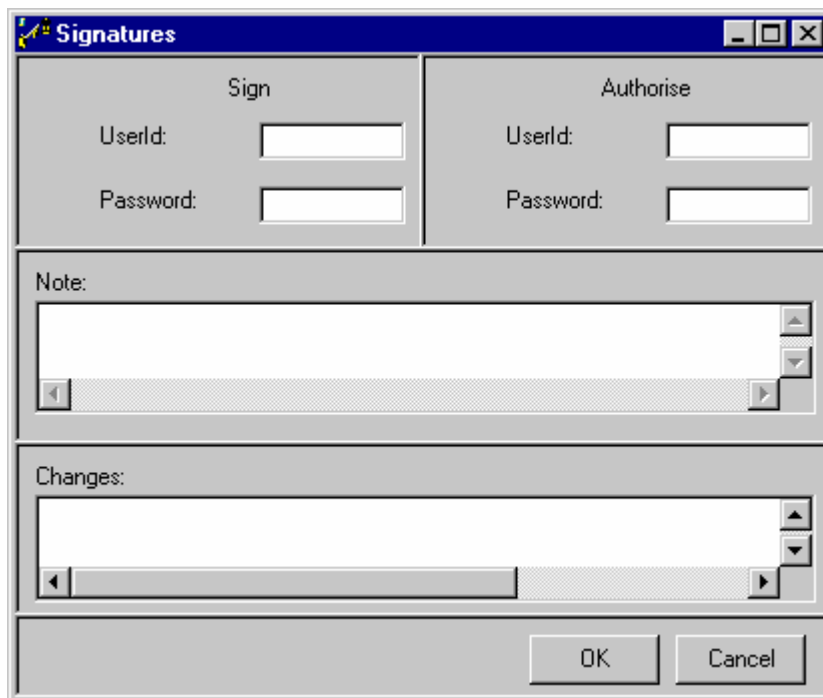
- 1 Select '**Login > Logout**' from the Menu Bar.



- A blank Security Manager window appears if no changes exist.
 - If changes have not yet been saved a dialog window appears.
- 2 At the prompt, click the appropriate button. '**Yes**' to save any changes and close, or '**No**' to discard any changes made since the last save.



- If the database is configured to requested '**Signatures**', '**Authorisation**' and '**Note**', and additional dialog window appears. Complete the required fields and observe the database amendments listed in the '**Changes**' field.



- 3 Click '**OK**' if satisfied with the information or '**Cancel**' to discard **ALL** changes made. The dialog window and the Utility closes. The Project Folder is now active.

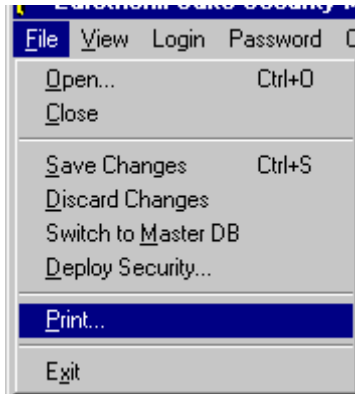
Print

This function allows the User select an output format for selected elements of the 'Security Manager'. The selected elements may be output to a printer or file. The printer produces a paper copy using the parameters defined in the Printer area. The file option converts the selected elements to an electronic .csv file. The Print dialog window has 3 configuration areas

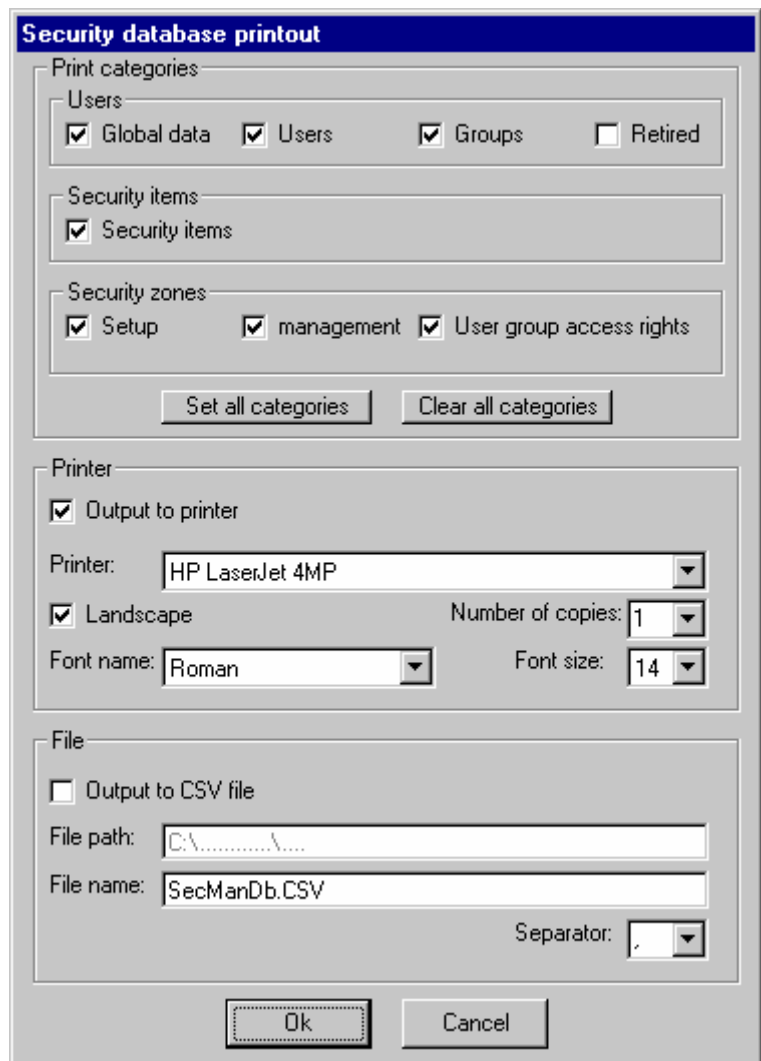
- [Print categories](#)
- [Printer](#)
- [File](#)

An output of the selected categories is produced by,

- 1 Selecting '**File > Print**' from the Menu Bar.



- 2 The Print dialog window is displayed allowing the User to select elements and set up the printer or file options.
- 3 After the Print dialog window is setup, press '**Ok**' to print or '**Cancel**' to abandon the print instructions and return to the current Security Manager window.



Printer selection

When the printer is the selected output format, the User can select from a list of printer.

This field allows the User to select any printer from the drop-down list. The list is derived from the Printers directory on the computer.

Element selection

If the element check box is

an output will be produced

but, if

an output will NOT be.

Output to CSV file check box

When the .CSV file is the selected output format, this check box defines an electronic output format of the selected elements. It converts selected elements to .CSV file type that can be opened using Microsoft Excel.

If the Output to CSV file check box is

the selected elements will be converted to an .CSV file

but, if

the selected elements will NOT be converted.

Output to printer check box

This field indicates if the printer is the selected output format.

If the Output to printer check box is

the selected elements will be output in a printed format

but, if

the selected elements will NOT be printed.

Clear all categories button

When this button is operated all elements are deselected.

An output can NOT be produced if there are no elements selected.

Set all categories button

When operated, this button selects all elements in the print categories section.

After selecting an output format and pressing 'OK', an output will be produced for all elements.

Font name field

When the printer is the selected output format, the character font of the print can be changed.

The User can select any font installed from the drop-down list. The list is derived from the Fonts directory on the computer.

Font size field

When the printer is the selected output format, the size of printed text can be changed.

The User can select any font size between 1 and 12 point (point is the recognised character measurement) from the list.

It is recommended that...
to ensure the printed text is readable, the font size is set to 6 or above.



Number of copies field

When the printer is the selected output format, the number of printed copies can be altered.

The User can select between 1 and 99 copies from the drop-down list.

Landscape check box

When the printer is the selected output format, the orientation of the print can be changed.

If the Landscape check box is Landscape the elements print  but, if Landscape the elements print .

Separator field

When the .CSV file is the selected output format, this field designates how the .CSV file divides the information received from the selected elements.

Microsoft Excel displays values in a tabular form.

If the **Separator:** is selected, Microsoft Excel separates the information into multiple columns. If the

Separator: is selected, Microsoft Excel does NOT separate the information. Instead all data is shown in 1 column, and the separated using spaces.

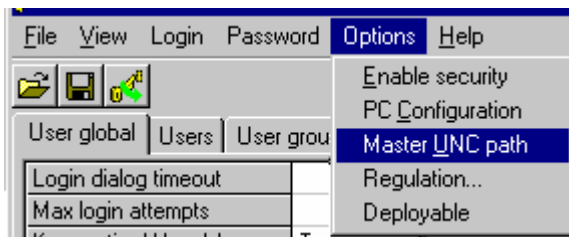
Rows are separated with paragraph marks.

Master UNC path

This function allows the User to identify the Universal Naming Convention (UNC) path to the Security Manager master database. Securities Manager needs this location path in order to successfully deploy the master database.

The location will ONLY be updated after entering a valid location path and pressing the update button.

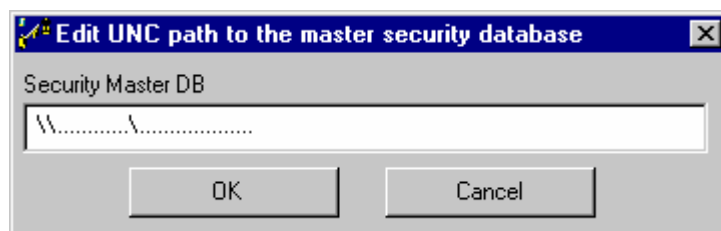
- 1 Select 'Options > Master UNC Path' from the Menu Bar.



If all changes are saved the 'Edit UNC path to the master security database' dialog window appears. If there are unsaved changes, the User is instructed to save or discard them before continuing. Press 'OK' and save changes. Repeat the instructions.

- 2 Enter the correct path and press the 'Update UNC path' button.

Example
 \\<shared PC name>\<directory>\<project folder>



- 3 If the correct path is entered, the confirmation dialog window is displayed. Press 'OK' to return to the 'Edit UNC path to the master security database' dialog window.



- 4 After the path has been successfully, updated press 'Close' to return to the current security database window.

Switch to MasterDB (database)

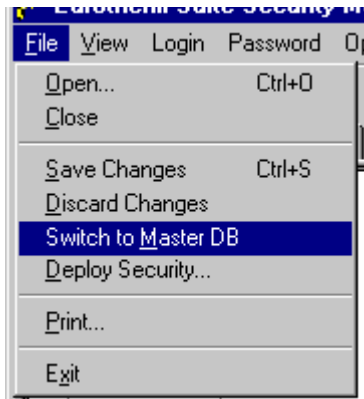
This function allows the User to switch from editing a Security Manager client database to the master database. This feature will automatically,

- logout the current User
- prompt to save any changes in a client database
- prompt for a User to Login

A successful switch to the master database is dependant on the correct '[Master UNC Path](#)', set up at the '**Options**' pulldown. The Master UNC path defines the location of the master database.

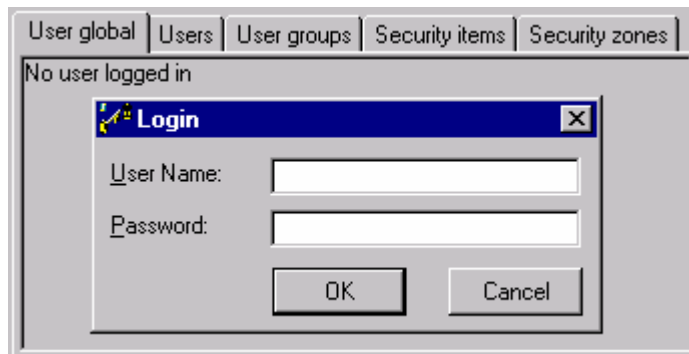
Switch to the master database by,

- 1 Selecting '**File > Switch to MasterDB**' from the Menu Bar.



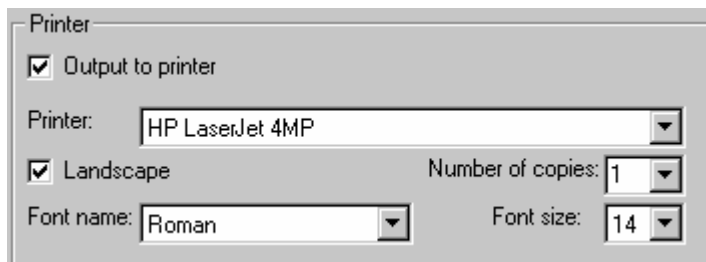
- 2 If the database detects unsaved changes, the save prompt appears. Press '**Yes**' to save changes and continue, '**No**' to discard changes and continue, or '**Cancel**' to revert to the current client security configuration.

If '**Yes**' or '**No**' was pressed the client database closes and automatically prompts for a [Login](#) User Id.



output to a printer

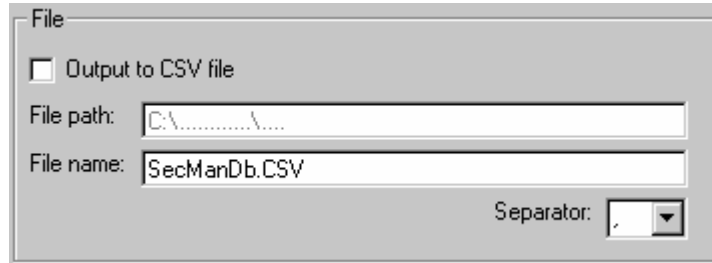
The Printer area allows the User to setup the printer output features. If the 'Output to printer' field is checked the printer is the selected output format. This indicates the User will create a printed output of the selected elements. indicates selected elements will NOT be output via the printer. The User can change the following printer output features.



output to a .CSV file

The File area allows the User to setup the file output features. If the 'Output to file' field is checked a .CSV file is the selected output format. This indicates that the selected elements will be output in an electronic format. indicates selected elements will NOT be output in an electronic format.

The User can change the following file output features.



 **Click to display the relevant configuration details.**

select Print categories

The Print categories area list the elements available to output, that consists of the Users, Security items, and Security zones areas. They correspond to the tabs in the Security Manager Window with the addition of User group access rights, Retired users and management.

An output will ONLY be produced if output type is specified by selecting either,

- Output to printer
- Output to CSV file

Note

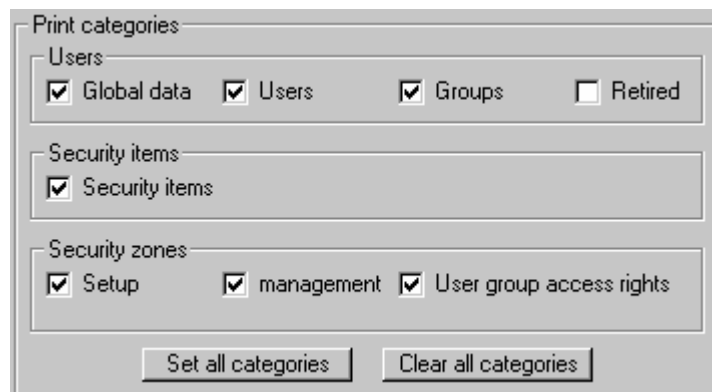
If the **Output to printer** and **Output to CSV file** are checked, a printed copy, and a .csv file version will be produced.

Select elements to output by

- 1 Clicking the element check box required. indicates the element is selected and an output will be produced. indicates it is NOT selected.

Example

The graphic illustrates an output is created for everything except the 'Retired users'.



- 2 By pressing the 'Set all categories' button, an output type, including all the categories is produced. Pressing the 'Clear all categories' deselects the categories.

Cancel Print

Press this button to cancel the operation.

Enable Security on EurothermSuite PC's

This function locks or unlocks the Master UNC Path to the master database. It also locks the Security Manager and Project databases together if both are located in the same directory.

If security is enabled the Master UNC Path cannot be edited and any changes to the Security Manager database are stored in the project database.

If security is enabled the 'Enable security on EurothermSuite PC's' option has a check mark along side, if there is NOT a check mark security is disabled.

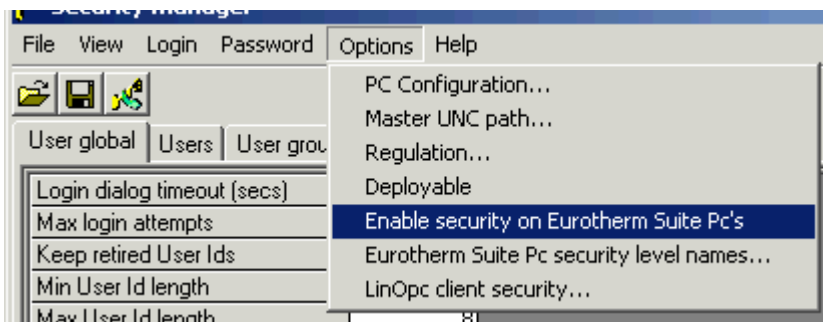
How to Enable/Disable Security on EurothermSuite PC's

The following instructions will enable or disable the security of the computer resident on the current security configuration.

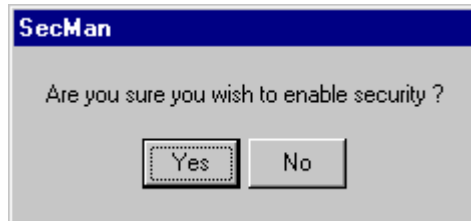
- 1 Select 'Options > Enable security on EurothermSuite PC's' from the Menu Bar.

Note

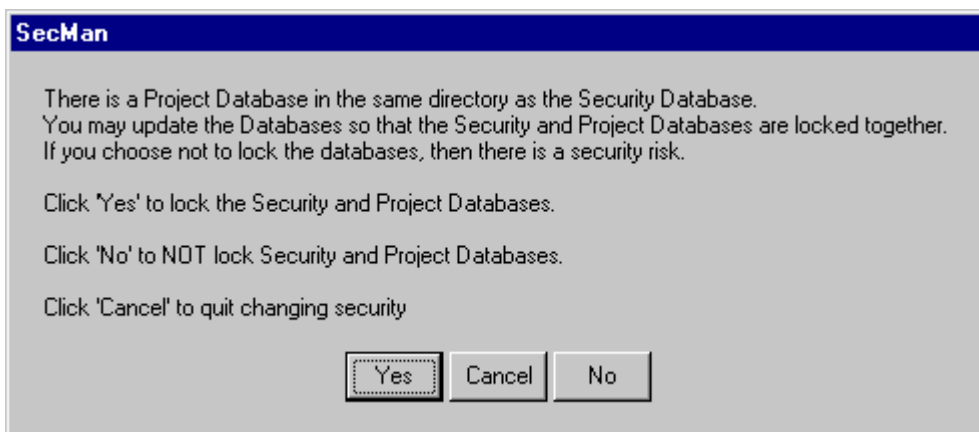
The 'Enable Security on EurothermSuite PC's' is disabled by default (NO check mark). If enabled a check mark is visible.



- 2 A dialog window to appears. Press 'Yes' to confirm or 'No' to cancel the operation.



- 3 If the Project (project.mdb) and Security Manager databases are NOT located in the same directory, security is enable/disabled without the warning below. If the databases are located in the same directory the following dialog window is displayed. Read the information and take the appropriate action.



It is recommended that...
the User selects 'Yes' to ensure the Project (project.mdb) and Security Manager (SecManDb.ujx) databases remain associated.

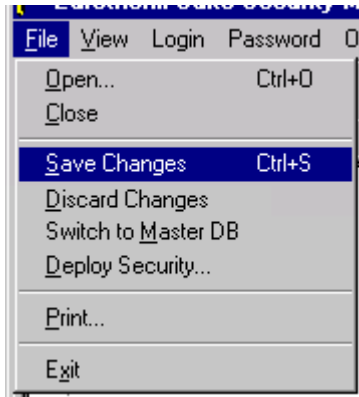
Save Changes

This function allows the User to save the configuration changes to the active database at the current location.

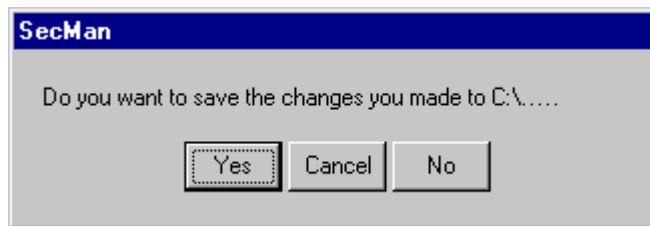
It is recommended that...
changes are saved at regular intervals.

Save changes by,

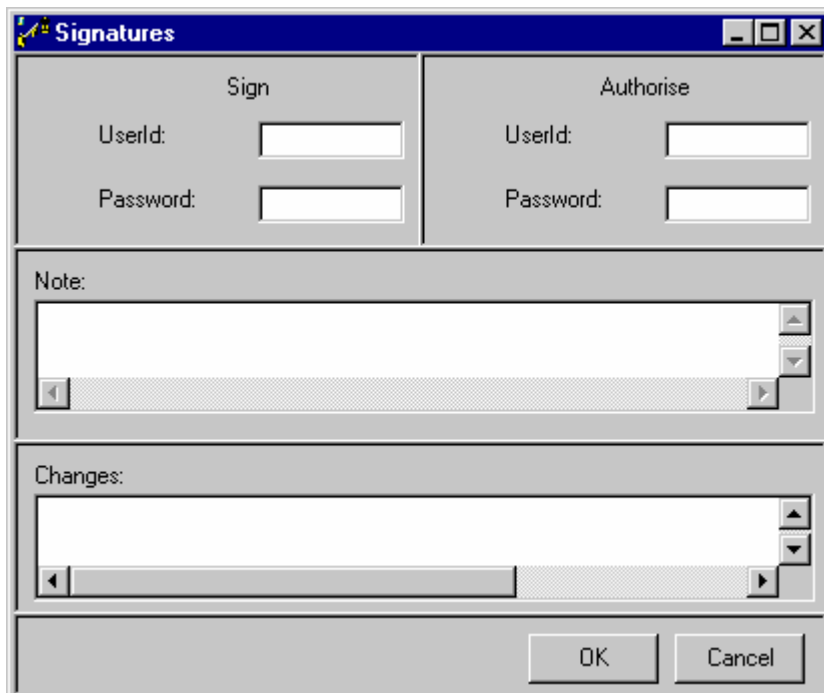
- 1 Selecting **'File > Save'** from the Menu Bar.
 - Alternatively, click the Save toolbutton.



- 2 The save changes dialog window appears, press **'Yes'** to save any changes, and **'Cancel'** to return to the current Security Manager window. Select **'No'** to discard any changes made since the last save and revert to a blank Security Manager window.



- 3 If the 'Sign', 'Authorise' and/or 'Note' Management Data and Access Rights are configured a window is displayed with the appropriate fields available. Press **'OK'** to save any changes, and **'Cancel'** to return to the current Security Manager window

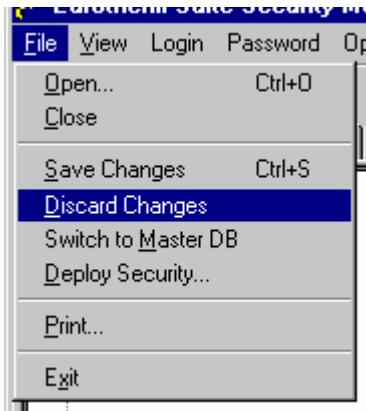


Discard Changes

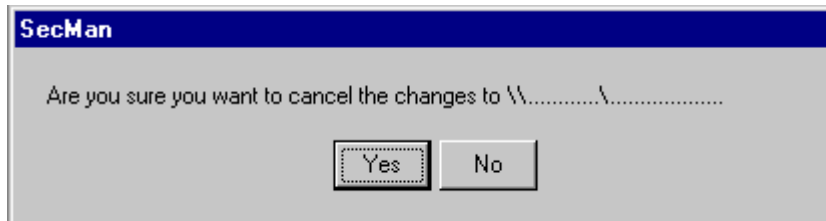
This function allows the User to abandon the changes made and return the database to the last saved configuration.

The previously saved database configuration can be retrieved by,

- 1 Selecting '**File > Discard Changes**' from the Menu Bar.



- 2 The dialog window below appears. Click 'Yes' to ignore all changes made since the previous save. Select 'No' to return to the current database configuration, retaining the changes.



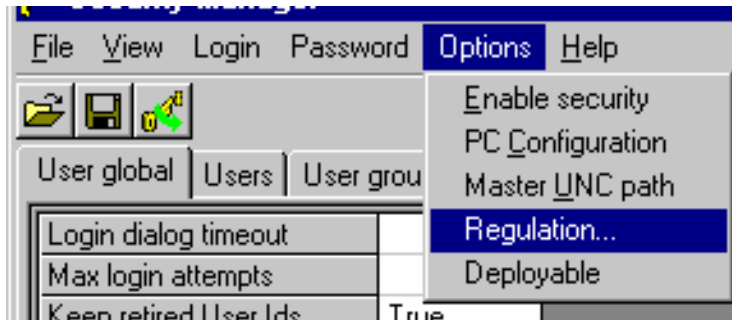
Defining the Regulation

When setting the level of Regulation required a dialog window will appear. The required Regulation is configured by simply selecting the required Regulation from the drop down list provided.

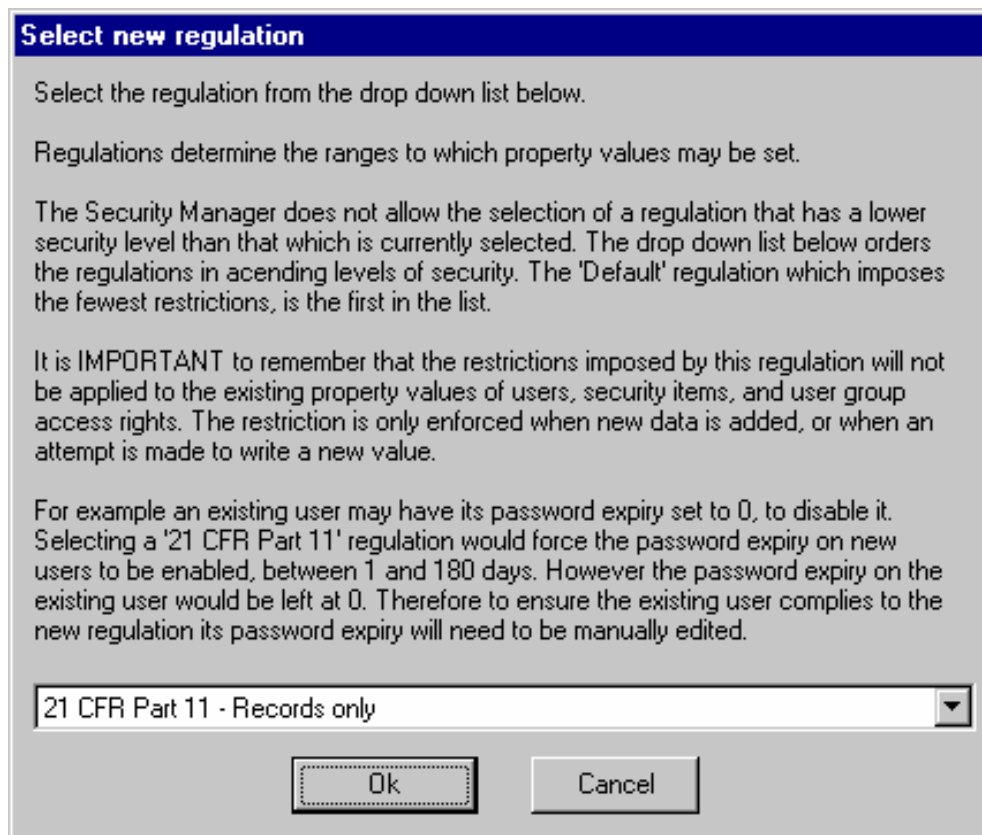
Beware
once accepted (**Ok** button) a level of Regulation can **ONLY** be increased.

The User **MUST** know if the system needs to comply to a level of Regulation.

- 1 Select '**Options > Regulation**' from the Menu Bar. A dialog window appears.



- 2 Read the information displayed and then at the prompt select the **Regulation** required.
 - Default
This imposes the fewest restrictions on the parameters in the system.
 - 21 CFR Part 11 Records only
This causes Security item types to Audit Trail changes.
 - 21 CFR Part 11 Signatures
This causes Security item types to comply with ALL constraints imposed by 21 CFR Part 11, including the Audit Trail and Electronic Signature security features.



- 3 Click the **Ok** button to confirm the selection or **Cancel** to change in Regulation and return to the Security Manager Window.

edit the User global tab parameters

How to configure the User global?

User global parameters define the properties of all Users of the database, including Users on client databases.

To configure the User global

- 1 Firstly, ensure the User global information is displayed. If these options are not, click the User global tab.
- 2 Then, configure the fields appropriately.
 - Change the [Login dialog timeout parameter](#)
 - Change the [Maximum login attempts parameter](#)
 - Change the [keep retired User Ids parameter](#)
 - Change the [minimum User Id length parameter](#)
 - Change the [maximum User Id length parameter](#)
 - Change the [minimum password length parameter](#)
 - Change the [maximum password length parameter](#)
 - Change the [Password reuse period parameter](#)

Finally, save changes and [deploy to Security item\(s\)](#), using the  to start the deployment wizard.

Note

Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

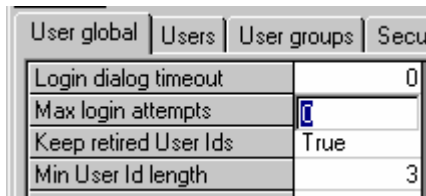
change the maximum login attempts

Change the numeric value to increase or decrease amount of consecutive failed logins that may be attempted before the being automatically disqualified (locked out).

- 1 Click the editable 'Maximum login attempts' field.

Note

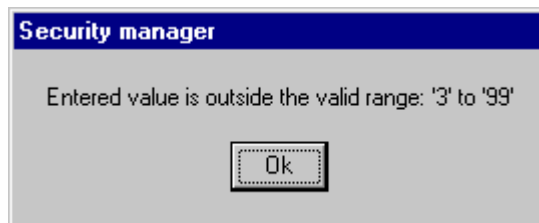
The existing value is highlighted. If the value is NOT highlighted double click in the field.



- 2 Enter the value that does not exceed the selected [Regulatory value constraints](#).

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.



- 3 Finally [save changes](#).

change the minimum password length

Change this field to increase or decrease the minimum number of characters used for ALL passwords in the database.

- 1 Click the editable 'Minimum User Id length' field.

Note

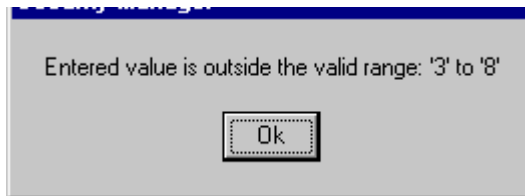
The existing value is highlighted. If the value is NOT highlighted double click in the field.

User global	Users	User groups	Secu
Login dialog timeout			0
Max login attempts			0
Keep retired User Ids		True	
Min User Id length			3
Max User Id length			8
Min password length			8
Max password length			8

- 2 Enter a value of between 3 and 8. Enter a new value of between 3 and 8 which does not exceed the selected [Regulatory value constraints](#).

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.



- 3 Finally [save changes](#).

change the minimum User Id length

Change this field to increase or decrease the minimum number of characters used for ALL User Id's in the database.

- 1 Click the editable 'Minimum User Id length' field.

Note

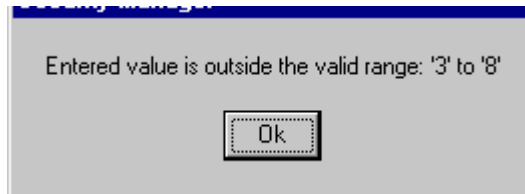
The existing value is highlighted. If the value is NOT highlighted double click in the field.

User global	Users	User groups	Securi
Login dialog timeout			0
Max login attempts			0
Keep retired User Ids		True	
Min User Id length			3
Max User Id length			8
Min password length			8
Max password length			8

- 2 Enter a value of between 3 and 8 which does not exceed the selected [Regulatory value constraints](#).

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.



- 3 Finally [save changes](#).

change the maximum password length

Change this field to increase or decrease the maximum number of characters used for ALL passwords in the database.

- 1 Click the editable 'Maximum User Id length' field.

Note

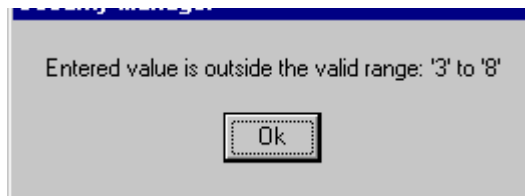
The existing value is highlighted. If the value is NOT highlighted double click in the field.

User global	Users	User groups	Secu
Login dialog timeout			0
Max login attempts			0
Keep retired User Ids		True	
Min User Id length			3
Max User Id length			8
Min password length			3
Max password length			8
Password reuse period			0

- 2 Enter a value of between 3 and 8 which does not exceed the selected [Regulatory value constraints](#).

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.

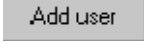


- 3 Finally [save changes](#).

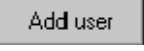
edit the User tab parameters

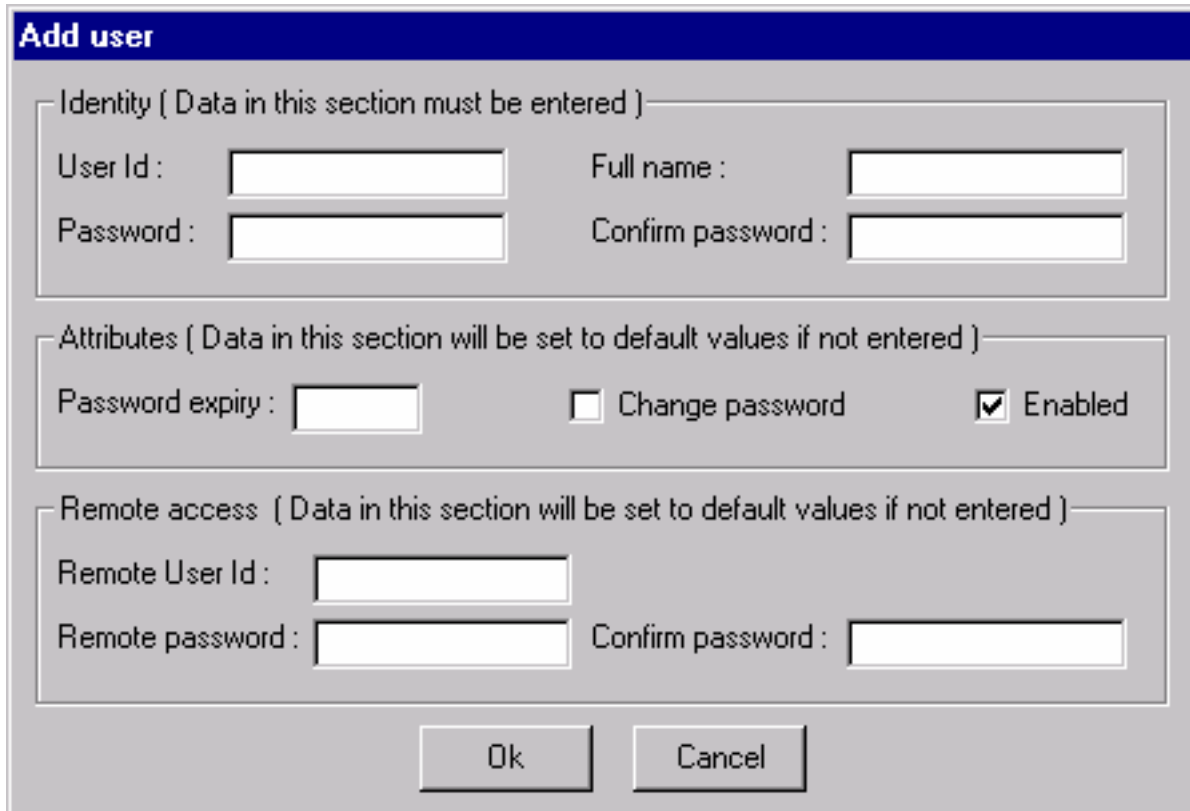
How to add a User

A User account is added to enable the User to perform certain functions within the system, one of which is Security Manager itself. Only Users with sufficient account Access Rights can modify the security database.

A User is added by pressing the  that displays the **Add User** dialog box.

Add a User by

- 1 Pressing  displays the **Add User** dialog box below.



Add user

Identity (Data in this section must be entered)

User Id : Full name :

Password : Confirm password :

Attributes (Data in this section will be set to default values if not entered)

Password expiry : Change password Enabled

Remote access (Data in this section will be set to default values if not entered)

Remote User Id :

Remote password : Confirm password :

Ok Cancel

- 2 Complete All the *Identity* fields and any other appropriate fields, being aware of the constraints configured in the User global tab.

Note

The constraints are defined in the [Security Manager Regulatory Defaults](#) table.

- 3 Press '**OK**' to add a User or '**Cancel**' to ignore the changes and return to the **User** tab.

Note




Only unsaved Users accounts can be removed (accounts added AFTER the LAST save), but ONLY by using the [File > Discard Changes](#) option. This also causes **ALL** unsaved changes to be removed, including the User.

- 4 Finally [save changes](#).
 - If satisfied, the User can now be [allocated to a User group](#).

How to configure the User?

User accounts for each User must be configured, in order to access the security database of Security item assigned to a corresponding Security zone.

To configure a User

- 1 Firstly, ensure the User group information is displayed. If these options are not, click the User group tab.
- 2 Then, [add a User](#) using . This displays a dialog box allowing the input of the User Id name and relevant system information.
 - When a number of Users have been added, the User tab can show [all or just the active Users](#)
 - If a User becomes locked out of the database, use the  to [re-enable a User](#).
- 3 When the User accounts have been added, configure the fields appropriately.
 - [Change the User Id parameter](#)
 - [Change the Password parameter](#)
 - [Change the Change Password parameter](#)
 - [Change the Password expiry parameter](#)
 - [Change the Remote UserId parameter](#)
 - [Change the Remote Password parameter](#)
 - [Change the Fullname parameter](#)
 - [Change the System parameter](#)
 - [Change the Retired parameter](#)
 - [Change the Enabled parameter](#)
 - [Change the Login attempts parameter](#)
 - [Change the Locked out parameter](#)
 - [Change the Reason parameter](#)
- 4 Finally, save changes and [deploy to Security item\(s\)](#), using the  to start the deployment wizard.

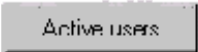
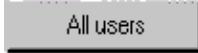
Note

Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

How to show Active or All Users

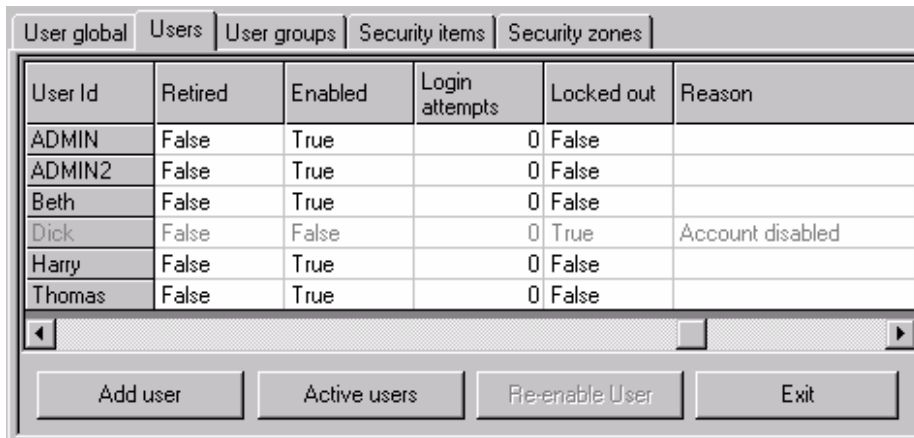
The function of this button allows the User to display [ALL Users](#) or just the [Active Users](#) in the User Id column.

Display Active or All users by

- 1 Clicking  and observe the list of User Id's as it is reduced to show just the **Active Users**. The button now reads .

Note

If the tab was already showing just the **Active Users**, pressing the 'All User' button causes the list of User Id's to expand and show **ALL Users**, including disqualified Users.



User Id	Retired	Enabled	Login attempts	Locked out	Reason
ADMIN	False	True	0	False	
ADMIN2	False	True	0	False	
Beth	False	True	0	False	
Dick	False	False	0	True	Account disabled
Harry	False	True	0	False	
Thomas	False	True	0	False	

- 2 Finally [save changes](#).

re-enable a User

The function of this button allows the User with sufficient access rights to the Security database to enable an automatically disabled User. A User may require re-instating if automatically locked, due to the,

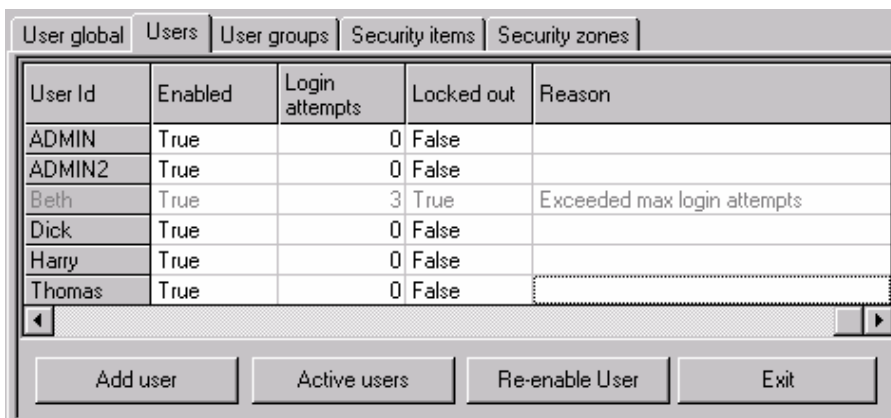
- User account has been disabled ('Enabled' field reads 'False', Reason field reads 'Account disabled')
- login attempts have been exceeded
- password has expired

Example

A User who has exceeded the maximum login attempts as configured in the User Global tab is an automatically disabled User.

Re-enable a disqualified User by

- 1 Selecting the automatically disabled User from the list of Users in the User Id column.



User Id	Enabled	Login attempts	Locked out	Reason
ADMIN	True	0	False	
ADMIN2	True	0	False	
Beth	True	3	True	Exceeded max login attempts
Dick	True	0	False	
Harry	True	0	False	
Thomas	True	0	False	

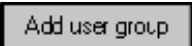
- 2 Then clicking the 'Re-enable User' button. The User is now enabled.

edit the User group tab parameters

add a User group

Assuming this tab is accessible, all User's are displayed in the left hand column. A new column is created each time a group is added. The group name is displayed at the top of each column.

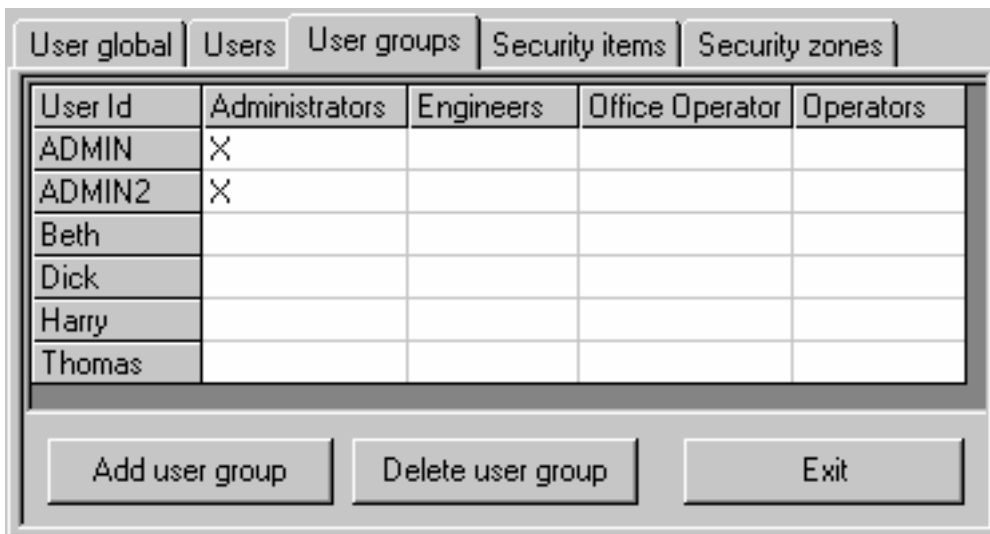
Add a User group by

- 1 Pressing  to display the **Add User Group** dialog box.



- 2 Select a User Group name from the drop down and edit or simply type in a new User Group name.
- 3 Press **Ok** to add the User group or **Cancel** to ignore the changes and return to the **User Group** tab.

Note
If **Ok** was selected observe the User Group name is added to the tab.



- 4 Finally [save changes](#).
 - If satisfied with the creation of the User Group, allocate [Security Items](#) or [User Groups](#). If NOT satisfied groups can be deleted, see [How to delete a User group](#).

How to configure the User group?

User groups must be configured to represent each category of User in the system.

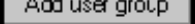

To configure the User groups

The fields in this tab are check fields.

- 1 Firstly, ensure the User group information is displayed. If these options are not, click the User group tab.

Note

A selection of default User Groups already exists in the Security database.

- 2 Then, [add a User group](#) using . This displays a dialog box allowing the input of the User group name.
 - Once accepted, [delete a User group](#) if it has been incorrectly created.
- 3 When the User groups have been added, [allocate each User to appropriate group\(s\)](#).
- 4 Finally, save changes and [deploy to Security item\(s\)](#) using the  to start the deployment wizard.

Note

Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

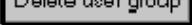
delete a User group

Assuming this tab is accessible, all User's are displayed in the left hand column. The group name is removed from the window after deletion.

Note

All User accounts assigned to the deleted User group ONLY will remain in the database, but will lose any privileges configured for that User group.

Delete a User group by

- 1 Pressing  displays the **Delete User Group** dialog box.
Alternatively, select the group from the main display.



- 2 Select a User Group name from the drop down or simply type in the User Group name.
- 3 Press '**OK**' to delete the User group or '**Cancel**' to ignore the changes and return to the **User Group** tab.

Note

If '**OK**' was selected observe the User Group name is removed to the tab.

User Id	Administrators	Engineers	Office Operator	Operators
ADMIN	X			
ADMIN2	X			
Beth				
Dick				
Harry				
Thomas				

Buttons: Add user group, Delete user group, Exit

4 Finally [save changes](#).

- If satisfied with deletion of the User Group, [allocate a User to a group](#) If NOT satisfied a group can be added, see [How to add a User group](#).
- Use the to remove a group added by error.

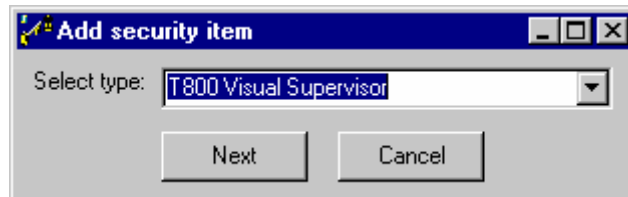
edit the Security items tab parameters

add a Security item

Security items are added to correspond with all configured Security items within the security configuration. The addition of items is executed using the **Add security item** which reveals the **add Security item** dialog box.

Add Security items by,

- 1 Pressing **Add security item** to display the first of 2 dialog boxes.
- 2 At this dialog box select the Security item type required from the drop down list.



- 3 Press **Next** to display the second of the 2 dialog boxes.
- 4 Complete the appropriate fields.

Note

Each Security item is automatically enabled to receive a deployment of the security database. This can be disabled by clicking in the Enabled for Deployment check box and removing the check mark.

- Adding a 5000 Series, enter a unique 'Security item name' and 'Address or Host name'. An item name **MUST** be added whereas the Address or Host name can be entered at a later date.
- Adding a EurothermSuite PC, enter a unique 'Security item name' and 'Project path'. An item name **MUST** be added whereas the path can be entered at a later date.
- Adding Review or QuickChart software, enter a unique 'Security item name' and 'Project path'. An item name **MUST** be added whereas the Computer Name and Database path can be entered at a later date.
- Adding a T800 Visual Supervisor, enter a unique 'Security item name', 'Lin port name' and 'Lin db name'. An item name **MUST** be added whereas the port and database names can be entered at a later date.
- Adding a Windows Domain, enter a unique 'Security item name'. Specify whether this Security item can configure Users globally in a domain, select the *Domain* radio button, or locally from a PC, select the *PC* radio button. An item name **MUST** be added whereas *Domain* or *PC* selection and the *Name* field can be entered at a later date.

It is recommended that...

both the Security item name and the Domain/PC name are the same, as this is referenced within Security Manager.

Note

The Windows Domain Security Item displays additional warnings concerning the reconciliation of Passwords and Password expiry dates when deployed.



All Security item information can be modified at a later date using the **Modify security item**.

- 5 Press **Previous** to return to the item type prompt, **Finish** to accept the new Security item information, or **Cancel** to abandon the activity and return to the Security items tab.
- 6 Finally [save changes](#).
 - If satisfied now [allocate the Security item](#). If NOT satisfied [delete the Security item](#).

How to configure the Security items?

Security items must be configured to represent each Security item type in a Security zone.


To configure the Security items

- 1 Firstly, ensure the Security items information is displayed. If these options are not, click the Security items tab.
- 2 Then, [add a Security item](#). If a Security item has been incorrectly created,
 - [Delete a Security item](#)
 - [Modify a Security item](#).
- 3 Finally, save changes and [deploy to Security item\(s\)](#), using the  to start the deployment wizard.
 - Alternatively, use  toolbutton.


Note

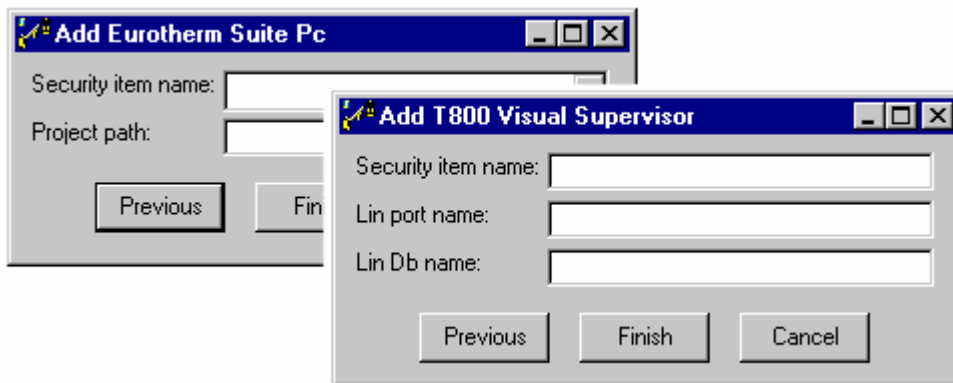
Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

modify a Security item

Sometimes during the process of adding Security items certain information is not available and therefore cannot be entered. This information can be added using the .

Modify a Security item by,

- 1 Clicking the Security item and pressing the . This will displays a dialog box identical to the **Add Security item** dialog box enabling the entry of the required information.

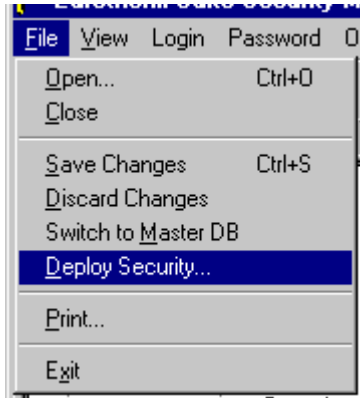


- 2 Enter any changes and press '**Ok**' to confirm the information or '**Cancel**' to reject the operation and return to the Security item tab.

deploy to selected Security items

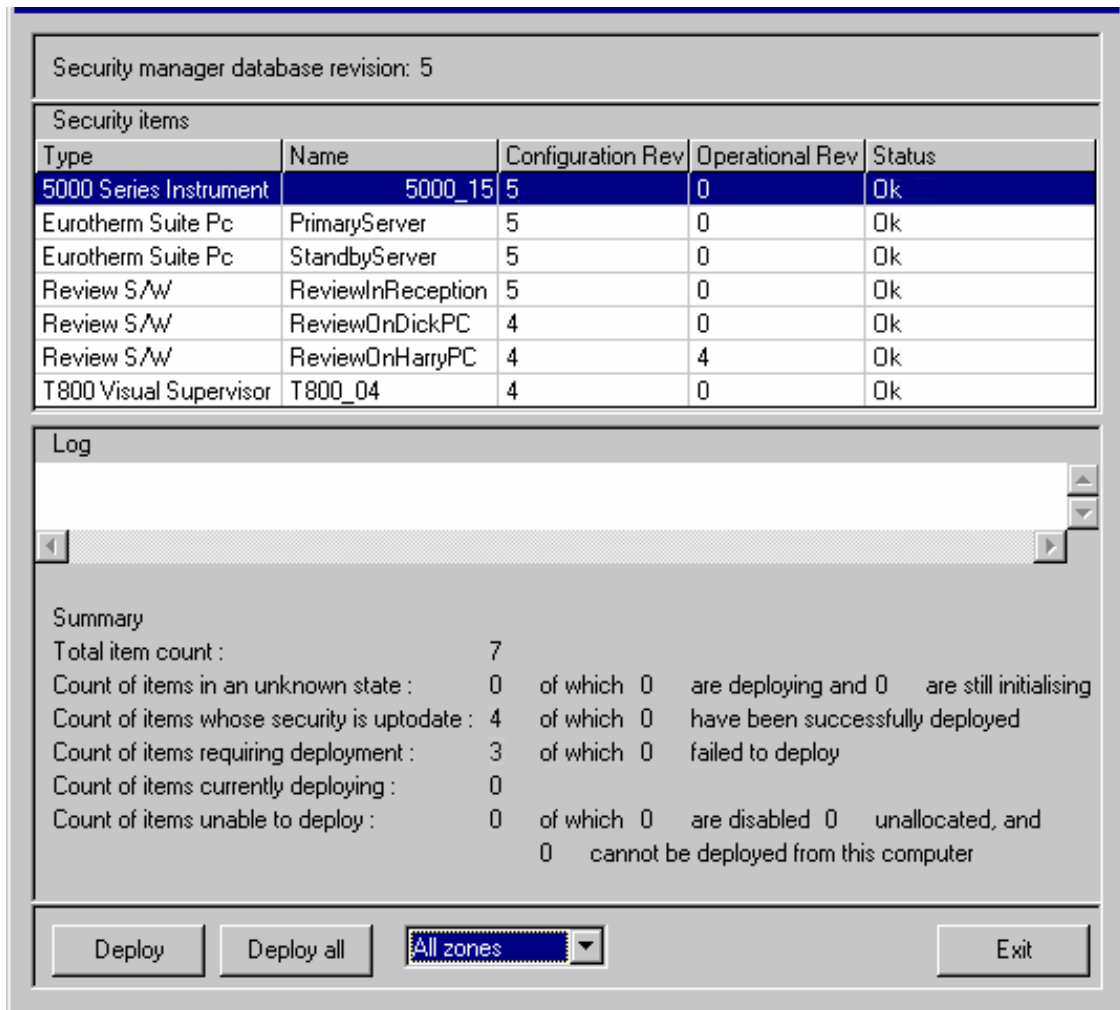
The deployment of the master Security database can be initiated by either

- Clicking the  on the Toolbar,
- Clicking the  available via the Security items tab, or
- Selecting 'Menu Bar > File > Deploy Security'.



Deploy to selected Security items

- 1 After selecting to 'Deploy Security' using one of methods indicated above, the Deploy Security window is displayed.



- 2 Click the 'Deploy' or 'Deploy All' button to continue.

Note

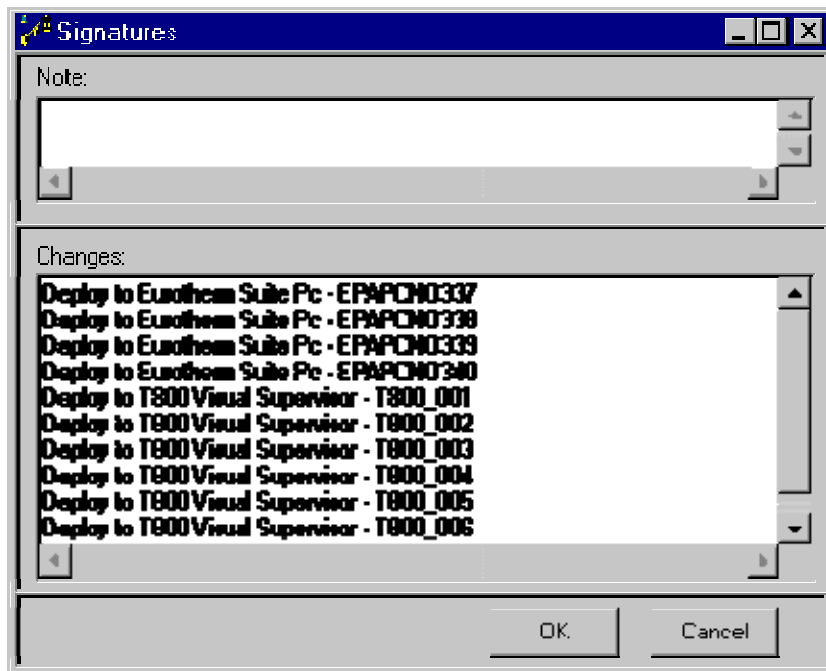
These buttons can be used in conjunction with the Zones drop down list if available.

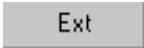


A 'Save' dialog window appears listing the destination of the deployed master security database.

Note

If the 'Notes' and/or 'Sign' features have been enabled for the User, appropriate fields are included in the save window. A 'Note' field allows information to be added and the 'Sign' field allows for the input of 'Electronic Signatures'.



- Press 'OK' to confirm the deployment to the selected Security items.
 - Press 'Cancel' to return to the Security item tab.
- 3 After confirming the destination to the selected Security items the Deploy Security dialog window reappears. It now shows the attempted reconciliation's and downloads to the selected items in the 'Log' field of the window.
 - 4 Press  to return to the Deploy Security window.

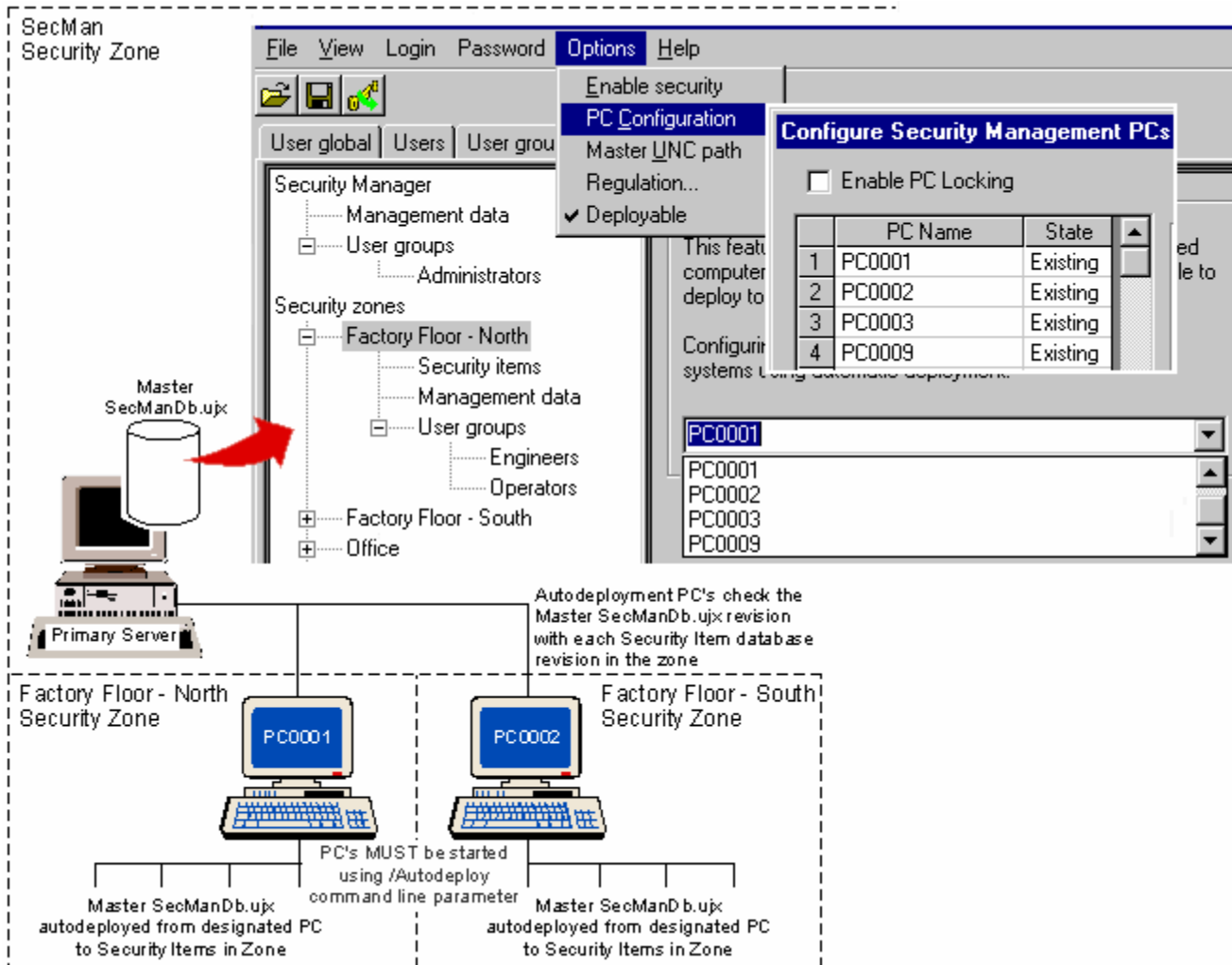
What is Deployment?

Deployment is a method of automatically gathering remote node 'Security databases', collating and updating the master database with the latest relevant information and downloading it to selected Security item nodes. It is divided into 'Reconciliation' and 'Download' steps.

- Reconciliation collates the operational revisions from selected databases and retains them in the Security Manager master database. The configuration revision of the master database is updated and allocated the next highest number.
- Download issues the latest configuration revision of the master database back to the selected client databases.

Example 4 - Deployment Computer configuration

With the correct master SecManDb.ujx configuration and start up of the Security Manager database on the specified Deployment Computer.



edit the Security zones tab parameters

add a Security zone

A new Security zone allows the User to configure different Management Data applicable to the User group (Users) requirements. All zones are displayed in the navigation pane. Any zone with allocated groups or items can be expanded (+) and collapsed (=). The Properties pane lists each zone in alphabetical order.

Note
Zones can ONLY be added when the zone list is displayed in the Properties pane.

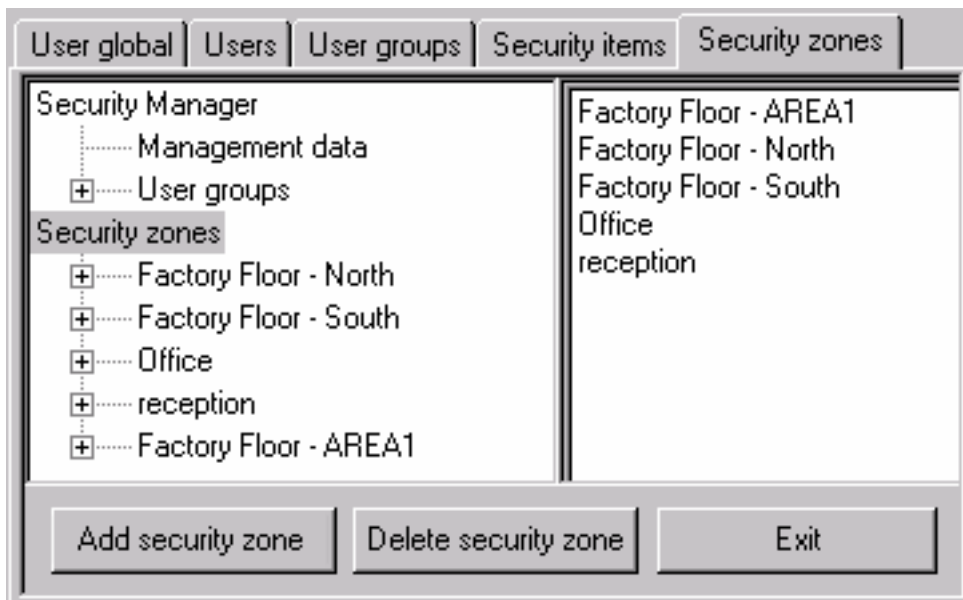
Add a zone by

- 1 Clicking  to display the **Add Security zone** dialog box.



- 2 Select a Security zone name from the drop down and edit or simply type in a new Security zone name.
- 3 Press **Ok** to add the Security zone or **Cancel** to ignore the changes and return to the **Security zone** tab.

Note
If **Ok** was selected observe the Security zone name is added to the tab



- 4 Finally [save changes](#).
 - Now allocate '[Security items](#)' or '[User groups](#)' or alternatively [delete a Security Zone](#)'.

How to configure the Security zone?

Security zones must be configured in order to define (set-up),

- Security item [Management Data](#)
- User group [Access Rights](#).

Renaming a Security zone

To configure a Security zone

- 1 Firstly, ensure the Security zones information is displayed. If these options are not, click the Security zones tab.
- 2 Then, [add a Security zone](#) using . This displays a dialog box allowing the input of the Security zone name.
 - Once accepted, [delete a Security zone](#) if it has been incorrectly created.
- 3 Next, [allocate Security items](#).
- 4 Now, [allocate User groups](#).
- 5 If required, [configure a Deployment computer](#)
 - [Configure Management Data for Security items](#)
 - [Security Manager Management Data](#)
 - [5000 Series Management Data](#)
 - [PC Management Data](#)
 - [QuickChart Software Management Data](#)
 - [Review Software Management Data](#)
 - [T800 Visual Supervisor Management Data](#)
 - [Windows Domain Management Data](#)
 - [Configure Access Rights for User groups](#)
 - [Security Manager Access Rights](#)
 - [5000 Series Access Rights](#)
 - [PC Access Rights](#)
 - [QuickChart Software Access Rights](#)
 - [Review Software Access Rights](#)
 - [T800 Visual Supervisor Access Rights](#)
 - [Windows Domain Access Rights](#)
- 6 Finally, save changes and [deploy to Security item\(s\)](#), using the  to start the deployment wizard.

Note

Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

allocate Security items

Allocating Security items to Security zones is an additional form of security grouping. The intention is to group items that require the same Management Data configuration so,

- allocated User groups have the ability to use enabled Management Data, and
- all Security items within the zone of identical type inherit the configured Management Data.


Security items can NOT be allocated to more than 1 zone.

Allocate Security items by


- 1 Opening a Security zone from the Navigation pane. When the zone is expanded Security items and User groups are displayed.

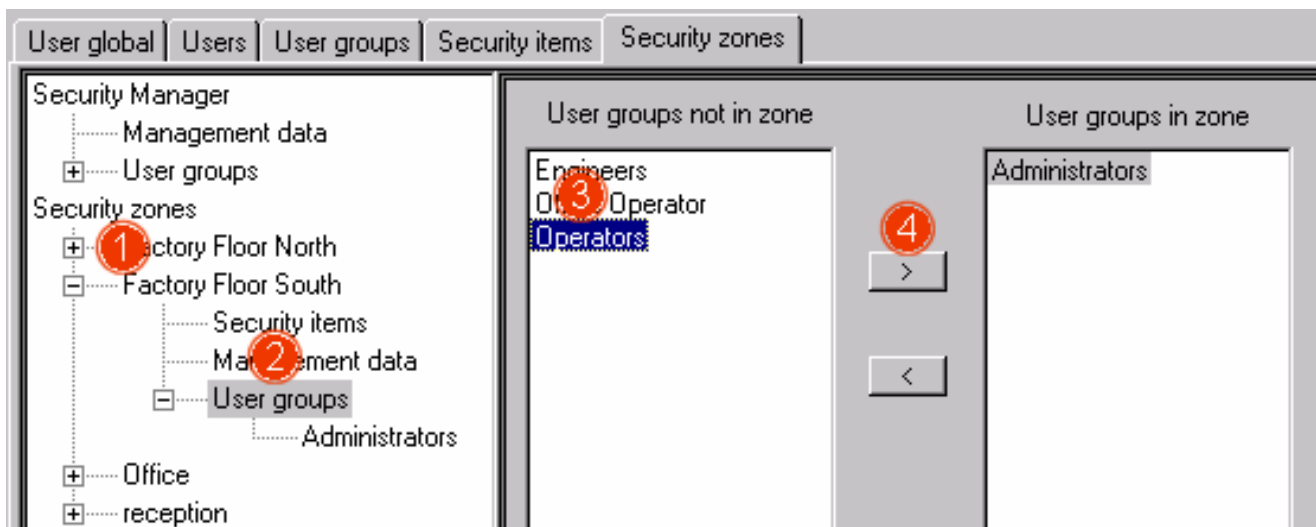
Note

Before any groups or items have been allocated the Properties pane is blank, requesting items are allocated.

- 2 In the Navigation pane click the **Security items** heading. Observe the Properties pane divides into 2 columns, a list of all the Security items
 - 'not in zone' (left hand column), (Unallocated)
 - 'in zone' (right hand column is initially empty). All allocated items are displayed in this column.
- 3 Click on a Security item from the 'not in zone' column.
- 4 Press the  to move the selected Security item to the 'in zone' column.

Note

Press the  to move the Security item back to the 'not in zone' column.



- 5 After successfully allocating the Security items to the appropriate Security zones, [save changes](#) and proceed with configuring the User operations.

allocate User groups

Allocating User groups to Security zones is an additional form of security grouping. When User groups are allocated to a Security zone, they inherit the configured Access Rights.


A single User group may be allocated to any number of zones.

Allocate User groups by


- 1 Opening a Security zone from the Navigation pane.

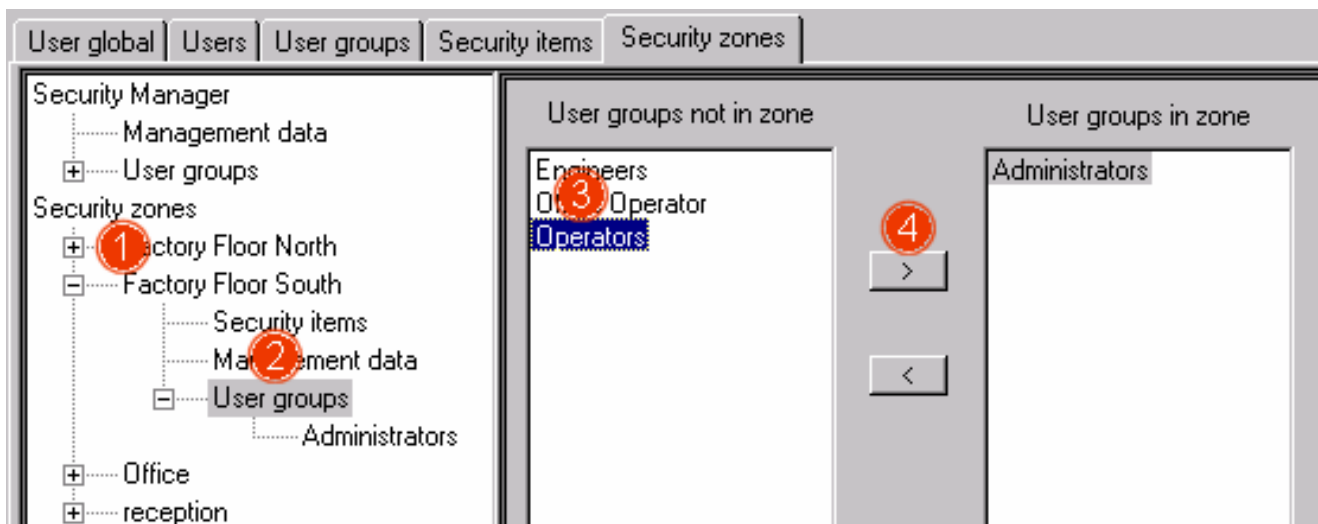
Note

Before any groups have been allocated the Properties pane is blank and requests the allocation of User groups.

- 2 In the Navigation pane click the **User groups** heading.
- 3 Observe the Properties pane divides into 2 columns, a list of all the User groups
 - 'not in zone' (left hand column), (Unallocated)
 - 'in zone' (right hand column is initially empty). All allocated groups are displayed in this column.
- 4 Click on a User group from the 'not in zone' column.
- 5 Press the  to move the selected User group to the 'in zone' column.

Note

Press the  to move the user group back to the 'not in zone' column.



After successfully allocating the User groups to the appropriate Security zones, [save changes](#) and proceed with configuring the User operations.

rename a Security zone

After a Security zone has been added, the specifics of it may change. The changes may now not clearly identify the Security zone.

To rename a Security zone

- 1 Select the required Security zone from the navigation pane. This will show the Security zone name in the Properties pane, to the right of the navigation pane.
- 2 Simply, replace the existing Security zone name by typing the new Security zone name in the Security zone name field at the top of the Properties pane.

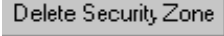
Note

Security zones names must be unique. Any attempt to duplicate Security zone names will display a failure dialog, and cancel the operation.

delete a Security zone

Deleting a Security zone removes the configured Management Data and Access Rights for the allocated groups and items. If Security items or User groups are allocated to only this deleted zone they need to be re-allocated and all configurations revert to the default parameters. If allocated to another Security zone, ONLY the Management Data corresponding to the deleted zones is removed. The User can delete Security zones using the Delete Security zone button. This function removes the zone from the 'Database'.

Delete a Security zone by

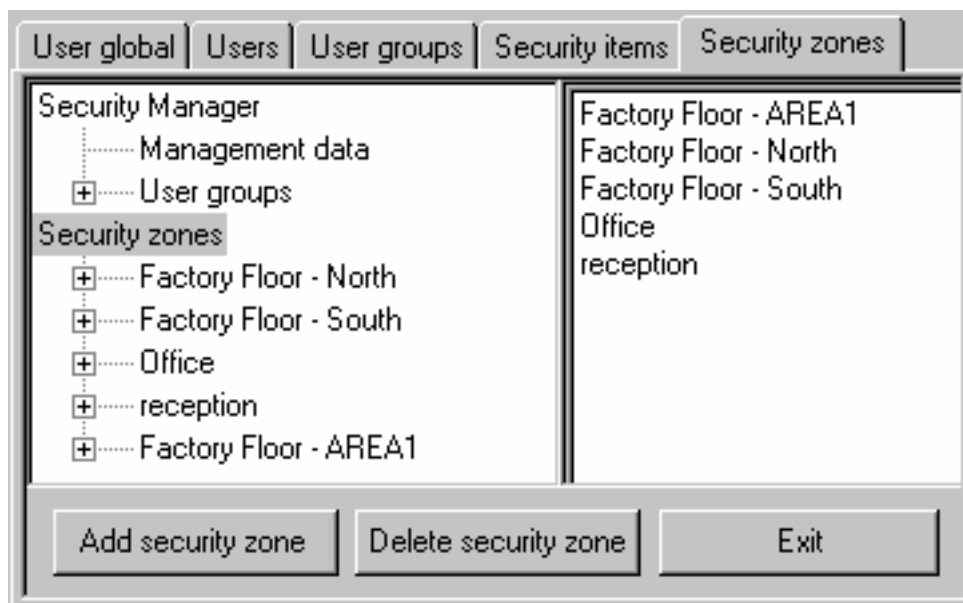
- Pressing  displays the **Delete Security zone** dialog box.
Select a Security zone name from the drop down or simply type in the Security zone name.

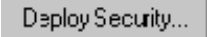


- Press **'OK'** to delete the Security zone or **'Cancel'** to ignore the changes and return to the **User Group** tab.

Note

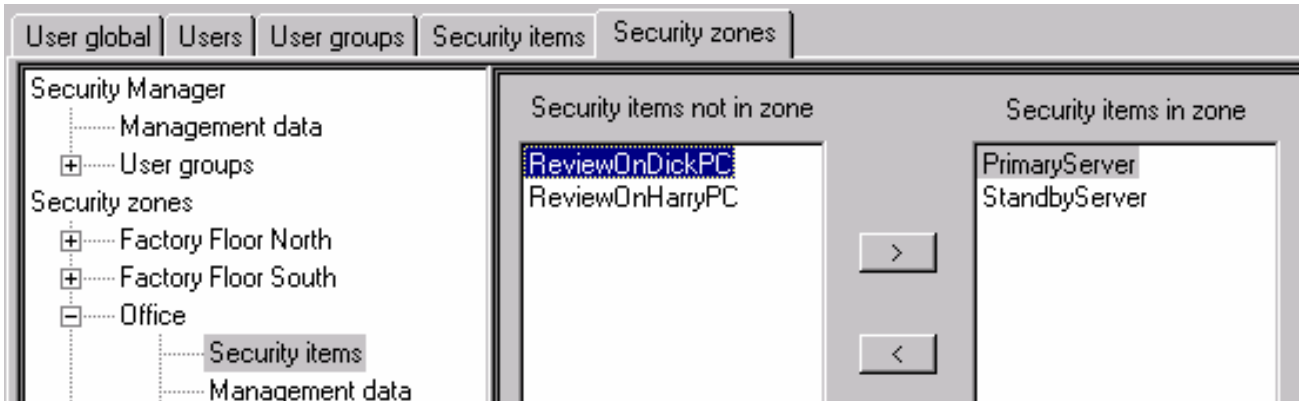
If **'OK'** was selected observe the Security zone name is removed to the tab.



- Press the  button.
- Finally [save changes](#).

Example 1 - Allocating Security items / User groups

If Security items and User groups have been added, selecting the heading in the left hand pane which displays a column of items or groups 'not in zone' and a column of items 'in zone' in the right hand pane.

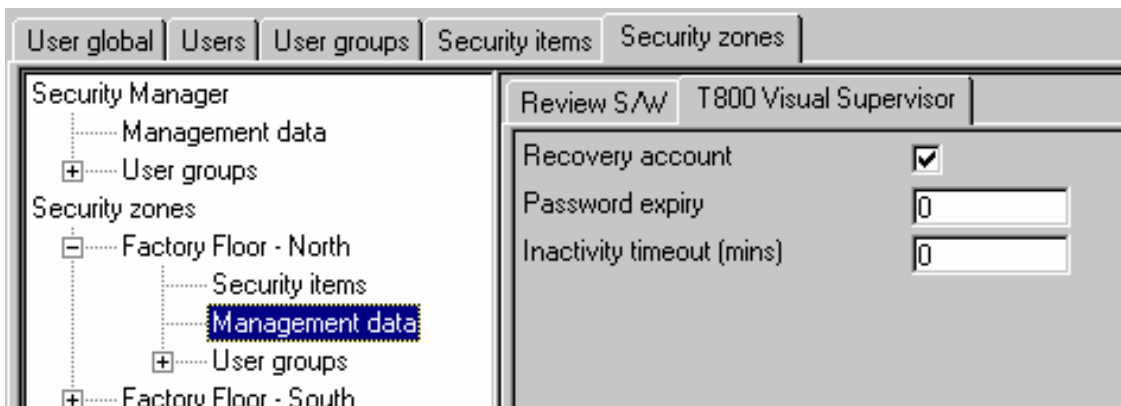


Note

If User groups have been added selecting a User groups heading in the left-hand pane displays a table of unallocated and allocated groups within the selected zone in the right hand pane.

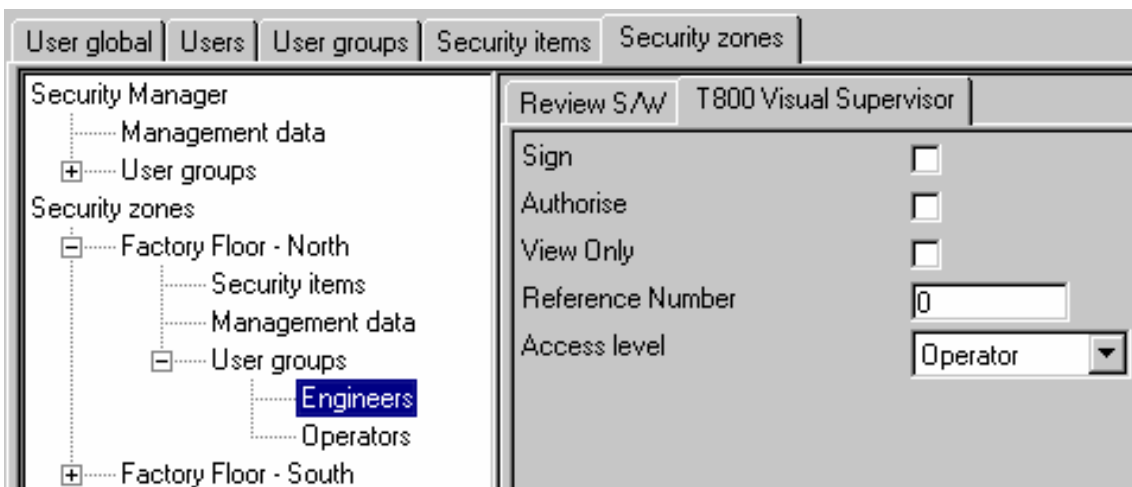
Example 2 - Management Data

Selecting a zone name in the left hand pane displays the allocated item types and configured Management Data in the right hand pane.



Example 3 - Access Rights

If selecting a User group name (accessed via 'Zone name > User group > User group name') in the left hand pane the item types and configured access rights (if allocated) are shown in the right hand pane.



edit the Security Manager permissions

configure the Security Manager management data

The Security Manager Utility management data is configured to enable valid Users access to change only a limited level of data. This means enabling or disabling specific features to ensure the Project can be monitored and maintained as desired. Management data can be configured from any Security item containing either the master or client database.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.*

To configure this

If the Security Manager zone Management Data is selected in the Navigation pane, the SecMan tab displays the configurable management data in the Properties pane, as follows

 [Audit trail](#)

 [Signing](#)

 [Authorisation](#)

 [Recovery user](#)

configure the Security Manager access rights

The Security Manager Utility access rights are configured to enable valid responsible Users, generally Administrators, and access to configure the access rights.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.*

To configure this

If the Administrators User group is selected in the Navigation pane, the SecMan tab displays the configurable access rights in the Properties pane, as follows

 [Sign](#)

 [Authorise](#)

 [Inactivity timeout \(ms\)](#)

 [Change own password](#)

 [Change own expired password](#)

 [View security data](#)

 [Edit user global data](#)

 [Edit user data](#)

 [Edit user group data](#)

 [Edit security item data](#)

 [Edit zone configuration data](#)

 [Edit zone management data](#)

 [Edit zone access rights data](#)

 [Edit Security Manager setup](#)

 [Edit Deployable flag](#)

 [Deploy Security](#)

edit the 5000 Series permissions

configure the 5000 Series management data










The 5000 Series Security item is configured to enable the User sufficient features in order to perform all expected tasks within the constraints of the selected Regulation. It is used to enable or disable features of the security configuration.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master Security database.*

To configure this

Selecting a zone name from the Navigation pane displays the 5000 Series Security item tab with the following fields in the Properties pane.

-  [Record Logins](#)
-  [Login Timeout \(mins\)](#)
-  [With unapplied changes](#)
-  [Require Signing](#)
-  [Require Authorisation](#)
-  [Enable Audit Trail](#)
-  [Disable Service Account](#)
-  [Login by User List](#)
-  [Password change on Expiry](#)

configure the 5000 Series access rights























The 5000 Series Security item is configured to enable the User sufficient access rights to perform all expected tasks. It is used to control and monitor the operations covering multiple areas of the security configuration.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.*

To configure this

Select a zone name from the Navigation pane displays the 5000 Series Security item tab with the following fields in the Properties pane.

-  [Connect from Remote](#)
-  [Edit Own Password](#)
-  [Change Alarm Setpoints](#)
-  [Acknowledge Alarms](#)
-  [Edit Maths Constants](#)
-  [Reset Maths](#)
-  [Preset Totalisers](#)
-  [Preset Counters](#)
-  [Start/Reset Timers](#)
-  [Set Clock](#)
-  [Adjust Inputs](#)
-  [Archiving Control](#)
-  [Save/Restore](#)
-  [Paste/Delete Files](#)
-  [Full Configuration](#)
-  [Full Security](#)
-  [Batch Control](#)
-  [Can Sign](#)
-  [Can Authorise](#)
-  [Event Permission 1 to 5](#)
-  [Edit Output Channel Default](#)
-  [Action Demand Writes](#)

edit the 6000 Series permissions

configure the 6000 Series management data










The 6000 Series Security item is configured to enable the User sufficient features in order to perform all expected tasks within the constraints of the selected Regulation. It is used to enable or disable features of the security configuration.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pull-down '**File > Switch to MasterDB**' to open the master Security database.

To configure this

Selecting a zone name from the Navigation pane displays the 6000 Series Security item tab with the following fields in the Properties pane.

-  [Record Logins](#)
-  [Login Timeout \(mins\)](#)
-  [With unapplied changes](#)
-  [Require Signing](#)
-  [Require Authorisation](#)
-  [Enable Audit Trail](#)
-  [Disable Service Account](#)
-  [Login by User List](#)
-  [Password change on Expiry](#)

configure the 6000 Series access rights








The 6000 Series Security item is configured to enable the User sufficient access rights to perform all expected tasks. It is used to control and monitor the operations covering multiple areas of the security configuration.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pull-down '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a zone name from the Navigation pane displays the 6000 Series Security item tab with the following fields in the Properties pane.

-  [Connect from Remote](#)
-  [Edit Own Password](#)
-  [Change Alarm Setpoints](#)
-  [Acknowledge Alarms](#)
-  [Edit Maths Constants](#)
-  [Reset Maths](#)
-  [Preset Totalisers](#)
-  [Preset Counters](#)
-  [Start/Reset Timers](#)
-  [Set Clock](#)
-  [Adjust Inputs](#)
-  [Archiving Control](#)
-  [Save/Restore](#)
-  [Paste/Delete Files](#)
-  [Full Configuration](#)
-  [Full Security](#)
-  [Batch Control](#)
-  [Can Sign](#)
-  [Can Authorise](#)
-  [Event Permission 1 to 5](#)
-  [Edit Output Channel Default](#)
-  [Action Demand Writes](#)
-  [Perform Upgrade](#)

edit the EurothermSuite PC permissions

configure the PC management data

The EurothermSuite PC Security item is configured to enable the User sufficient features in order to perform all expected tasks within the constraints of the selected Regulation. It is used to enable or disable features of the security configuration.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a zone name from the Navigation pane displays the EurothermSuite PC Security item tab with the following fields in the Properties pane.

-  [Audit trail](#)
-  [Signing](#)
-  [Authorisation](#)
-  [Alarm signing](#)
-  [Alarm authorisation](#)
-  [Confirmation](#)
-  [Notes](#)
-  [Auto Logon](#)
-  [Log Invalid Times](#)
-  [Audit Ports](#)
-  [Lockout Level](#)

configure the PC access rights






















The EurothermSuite PC Security item is configured to enable the User sufficient access rights to perform all expected tasks. It is used to control and monitor the operations covering multiple areas of the security configuration.









It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a User group name from the Navigation pane displays the EurothermSuite Security item tab with the following fields in the Properties pane.

-  [Sign](#)
-  [Authorise](#)
-  [Print](#)
-  [TagEdit](#)
-  [Operator Point Display](#)
-  [Export Historical Trend](#)
-  [Faceplate Configurator](#)
-  [Inactivity timeout \(ms\)](#)
-  [Display access level](#)
-  [Synchronise Files](#)
-  [Override Server Redundancy](#)
-  [Task Switch](#)
-  [Operator group global](#)
-  [Debug](#)
-  [Operator groups](#)
-  [Trend global](#)
-  [AlarmHistMaxItems](#)
-  [Trends](#)
-  [Recipe](#)
-  [Global Alarm Acknowledge](#)
-  [Faceplate Modify](#)

-  [Change Language](#)
-  [Offline data writes](#)
-  [IO data writes](#)
-  [System User writes](#)
-  [Custom1 to Custom5](#)
-  [Custom6 to Custom10](#)
-  [downloaded Recipes](#)
-  [Tag Security Area](#)

edit the QuickChart software permissions

configure the QuickChart software management data

The QuickChart software Security item is configured to enable the User sufficient features in order to perform all expected tasks within the constraints of the selected Regulation.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a zone name from the Navigation pane displays the blank QuickChart software Security item tab in the Properties pane.

 [Signing](#)

configure the QuickChart software access rights

The QuickChart software Security item is configured to enable the User sufficient access rights to perform all expected tasks. It is used to control and monitor the operations covering multiple areas of the security configuration.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a User group name from the Navigation pane displays the QuickChart software Security item tab with the following fields in the Properties pane.

 [Create Chart](#)

 [Chart Open/Close](#)

 [Modify Chart](#)

 [Save Chart](#)

 [Chart Setup](#)

 [Administration](#)

 [Chart Annotate](#)

 [Chart Review](#)

 [Chart Approve](#)

 [Chart Release](#)

 [Print](#)

 [Print Setup](#)

 [Export Data](#)

 [Export Setup](#)

 [Inactivity timeout \(ms\)](#)

edit the Review software permissions

configure the Review software management data

The Review software Security item is configured to enable the User sufficient features in order to perform all expected tasks within the constraints of the selected Regulation. It is used to enable or disable features of the security configuration.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a zone name from the Navigation pane displays the EurothermSuite PC Security item tab with the following fields in the Properties pane.

 [Signing](#)

configure the Review software access rights

The Review software Security item is configured to enable the User sufficient access rights to perform all expected tasks. It is used to control and monitor the operations covering multiple areas of the security configuration.

It is recommended that...

a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a User group name from the Navigation pane displays the Review software Security item tab with the following fields in the Properties pane.

 [Transfer Files](#)

 [Chart Setup](#)

 [Chart Open/Close](#)

 [Modify Chart](#)

 [Save Chart](#)

 [Administration](#)

 [File Services](#)

 [Chart Annotate](#)

 [Chart Review](#)

 [Chart Approve](#)

 [Chart Release](#)

 [Print](#)

 [Print Setup](#)

 [Export Data](#)

 [Export Setup](#)

 [Inactivity timeout \(ms\)](#)

edit the T800 Visual Supervisor permissions

configure the T800 Visual Supervisor management data

The T800 Visual Supervisor is configured to enable the User sufficient features to perform all expected tasks.


It is recommended that...

a client database should **ONLY** be edited in *exceptional circumstances*. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Select a zone name from the Navigation pane displays the T800 Visual Supervisor tab with the following fields in the Properties pane.

 [Recovery account](#)

 [Password Expiry](#)

 [Inactivity timeout \(ms\)](#)

configure the T800 Visual Supervisor access rights

The T800 Visual Supervisor is configured to enable the User sufficient access rights to perform all expected tasks.

It is recommended that...

a client database should **ONLY** be edited in *exceptional circumstances*. Use the pulldown '**File > Switch to MasterDB**' to open the master database.

To configure this

Selecting a User group name from the Navigation pane to displays the T800 Visual Supervisor tab with the following fields in the Properties pane.

 [Sign](#)

 [Authorise](#)

 [View Only](#)

 [Admin only](#)

 [FTP](#)

 [Remote](#)

 [User1 to User4](#)

 [Reference Number](#)

 [Access level](#)

edit the Windows Domain permissions

configure the Windows Domain Management Data

The Windows Domain Management Data is configured to enable valid Users access to change only a limited level of data. This means enabling or disabling specific features to ensure the Project can be monitored and maintained as desired.

Management data can be configured from any Security item containing either the master or client database.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.*

To configure this

Select a zone name from the Navigation pane, to display the Windows Domain Security item tab with the following fields in the Properties pane.

 [Administrator UserId](#)

 [Administrator Password](#)

 [Password Expiry](#)

 [Deploy existing users](#)

 [Delete retired users](#)

configure the Windows Domain Access Rights

The Windows Domain Security item is configured to enable the User sufficient access rights to perform all expected tasks. It is used to control and monitor the operations covering multiple areas of the security configuration.

It is recommended that...

*a client database should **ONLY** be edited in exceptional circumstances. Use the pulldown '**File > Switch to MasterDB**' to open the master database.*

To configure this

Select a zone name and User group from the Navigation pane, to display the Windows Domain Security item tab with the following fields in the Properties pane.

 [Groups](#)

Configure Security item parameters

configure the Access level access rights

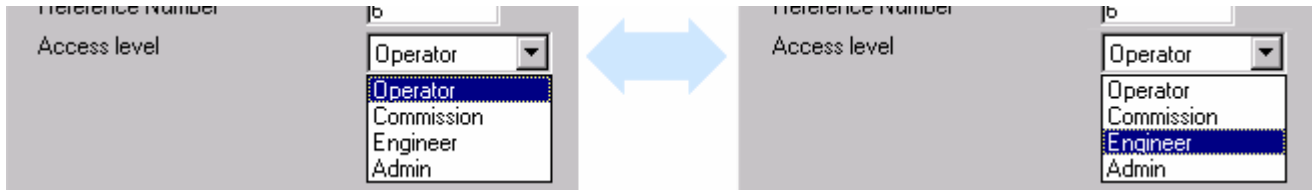
This field allows the User to specify the security Access level required to read or write to T800 Visual Supervisor item types. Any User attempting to use the T800 Visual Supervisor's MUST have Access Rights that are equal or greater than the value entered in this field.

The Access level drop down list displays the Operator, Commission, Engineer and Admin levels.

This is configured in the database for T800 Visual Supervisor Security items.

To configure this

- 1 Select the type of access level required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Acknowledge Alarms access rights

This check box allows or does not allow the Users assigned to the selected User group to acknowledge the presence of an alarm.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to acknowledge the alarm. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Acknowledge Alarms** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Action Demand Writes access rights

This check box allows or does not allow the Users assigned to the selected User group to overwrite master communications values,

■ by job action

■ by the User Screens 'Operator' key, if the Master Communications option is fitted

It has 2 states, - True or - False. If the check box is set to True the User group is allowed overwrite master comms values. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Action Demand Writes** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Adjust Inputs access rights

This check box allows or does not allow the Users assigned to the selected User group to change the process values of selected channels.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the process values of selected channels. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Adjust Inputs** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Admin only access rights

This field allows or does not allow Administrator Users to perform tasks that exceed the responsibility.

This is configured in the database for T800 Visual Supervisor Security items.

To configure this

- 1 Click the **Admin only** checkbox.

indicates the Administrator User can perform tasks within the Administrator responsibility only.

indicates the Administrator User is permitted perform tasks that exceed the Administrators responsibility.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Administration access rights

This check box allows or does not allow the Users to use the Automatic Print Setup, Maintain Database, Auto Backup/Transfer Setup, Instrument Setup, Security Setup, and all Options menu item commands.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the setup commands and all Options menu item commands. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Administration** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Administrator Password field

This field allows the generation of a Windows Domain Administrator password to accompany the Windows Domain Administrator User account. The Windows Domain Administrator User account is defined in the Administrator UserId field.

This is configured in the database for Windows Domain Security item type.

To configure this

- 1 Click the Administrator Password field.
- 2 At the keyboard, enter the required Password and press the return key.

Note

If attempting to leave this field blank Security manager automatically configures a default password, ADMIN – case sensitive.

configure the Administrator UserId field

This field allows the generation of a Windows Domain Administrator User account. It has sufficient privilege for Security Manager to login and configure the security of a Windows domain. If the UserId field is left blank, Security Manager will complete the changes using the currently logged on User. This UserId requires a password that is defined in the Administrator Password field.

This is configured in the database for Windows Domain Security item type.

To configure this

- 1 Click the Administrator UserId field.

- At the keyboard, enter the required UserId and press the return key.

Note

If Security Manager does not have sufficient privilege, deployment will fail.

configure the Alarm authorisation field

This field allows the input of a specified alarm priority level that when reached or exceeded will require an approval signature. This signature will accompany the Alarm signing signature that authenticated the alarm acknowledgement, which will automatically be requested even if NOT configured.

A default value of '0' indicates this feature is disabled with '1' being the lowest priority level and '15' being the highest.

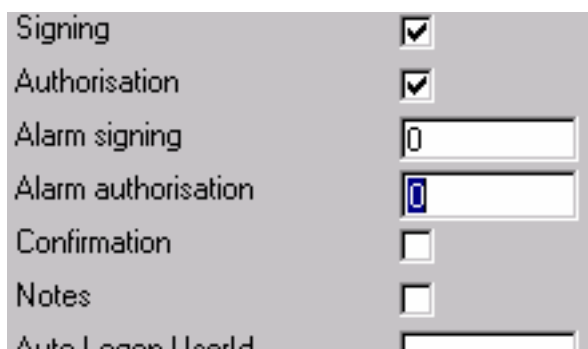
This is configured in the database for EurothermSuite PC Security item type.

To configure this

- Select in the **Alarm authorisation** field.

Note

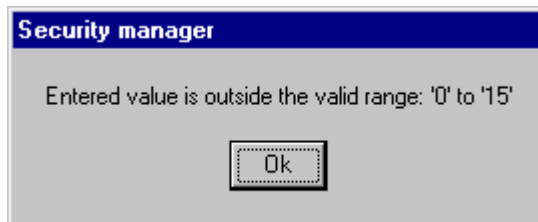
If the value is NOT highlighted double click in the field.



- Using the keyboard, enter a new value and press the return key.

Note

A dialog window appears if a value outside the constraints is entered. Read the dialog and click 'Ok', the field reverts to its previous setting.



- Finally, [save changes](#) and proceed to the next task.

configure the Alarm signing field

This field allows the input of a specified alarm priority level that when reached or exceeded will require a signature to authenticate the alarm acknowledgement.

A default value of '0' indicates this feature is disabled with '1' being the lowest priority level and '15' being the highest.

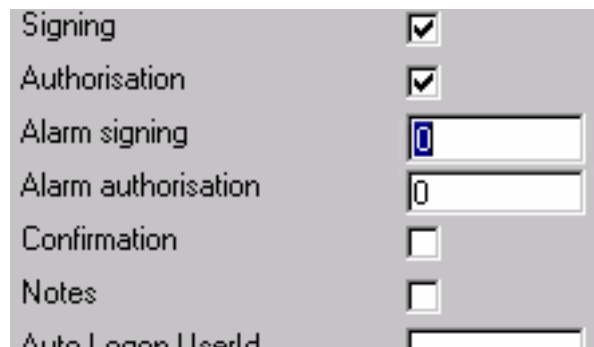
This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select in the **Alarm signing** field.

Note

If the value is NOT highlighted double click in the field.



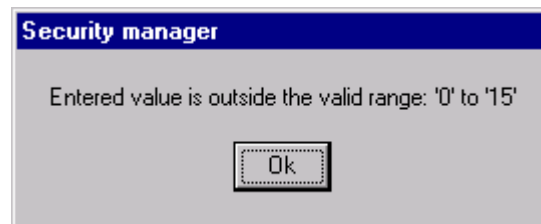
The screenshot shows a configuration window with several options. The 'Alarm signing' option is highlighted in blue. The options are:

Signing	<input checked="" type="checkbox"/>
Authorisation	<input checked="" type="checkbox"/>
Alarm signing	<input type="text" value="0"/>
Alarm authorisation	<input type="text" value="0"/>
Confirmation	<input type="checkbox"/>
Notes	<input type="checkbox"/>
Auto Login User Id	<input type="text"/>

- 2 Using the keyboard, enter a new value and press the return key.

Note

A dialog window appears if a value outside the constraints is entered. Read the dialog and click 'Ok' the field reverts to its previous setting.



- 3 Finally, [save changes](#) and proceed to the next task.

configure the AlarmHistMaxItems access rights

This field allows the selection of a type of confirmation via a drop down list, needed to accept changes to the number of retrieved alarms from the alarm history via the 'InTouch WindowViewer'.

InTouch WindowViewer > Alarm History

The **AlarmHistMaxItems** enables the User to increase the maximum number of alarms retrieved from the alarm history server from 500 to 32767, data retrieval timeout permitting.

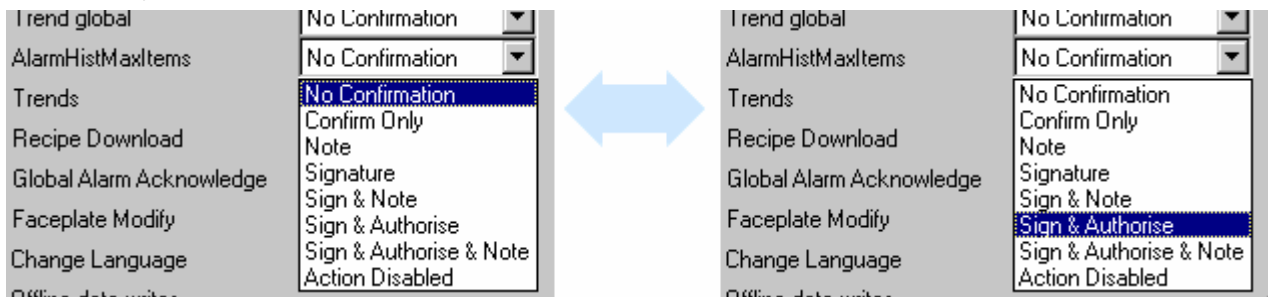
Note

The **Action Disabled** access right ONLY prevents the User changing the number of retrieved alarms to greater than 500.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Archiving Control access rights

This check box allows or does not allow the Users assigned to the selected User group to configure the archiving strategy of 5000 Series configuration data.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to configure the archiving strategy. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Archiving Control** check box.



indicates that the User group is allowed to use this action.



indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Audit Ports

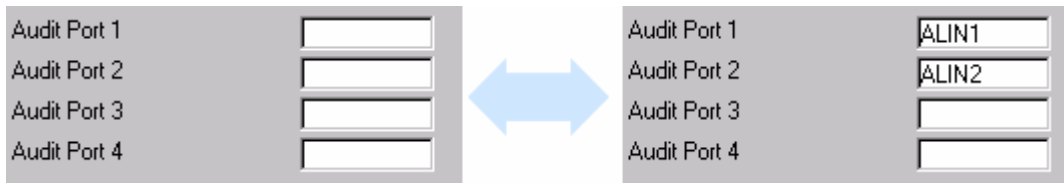
These fields enable the configuration of up to 4 Local Instrument Networks (LINs) for remote Audit Trail purposes. Each Audit Port field stores events and alarms in local .uhh files sent from all T800 Visual Supervisors that communicate via that network.

Each LIN Network is designated using it's network port name in the appropriate Audit Port field. Generally Audit Port 1 is designated the first ALIN port (e.g. ALIN1) and Audit Ports 2, 3 and 4 the other ports (if available).


This is configured in the database for EurothermSuite PC Security item type.

To configure this

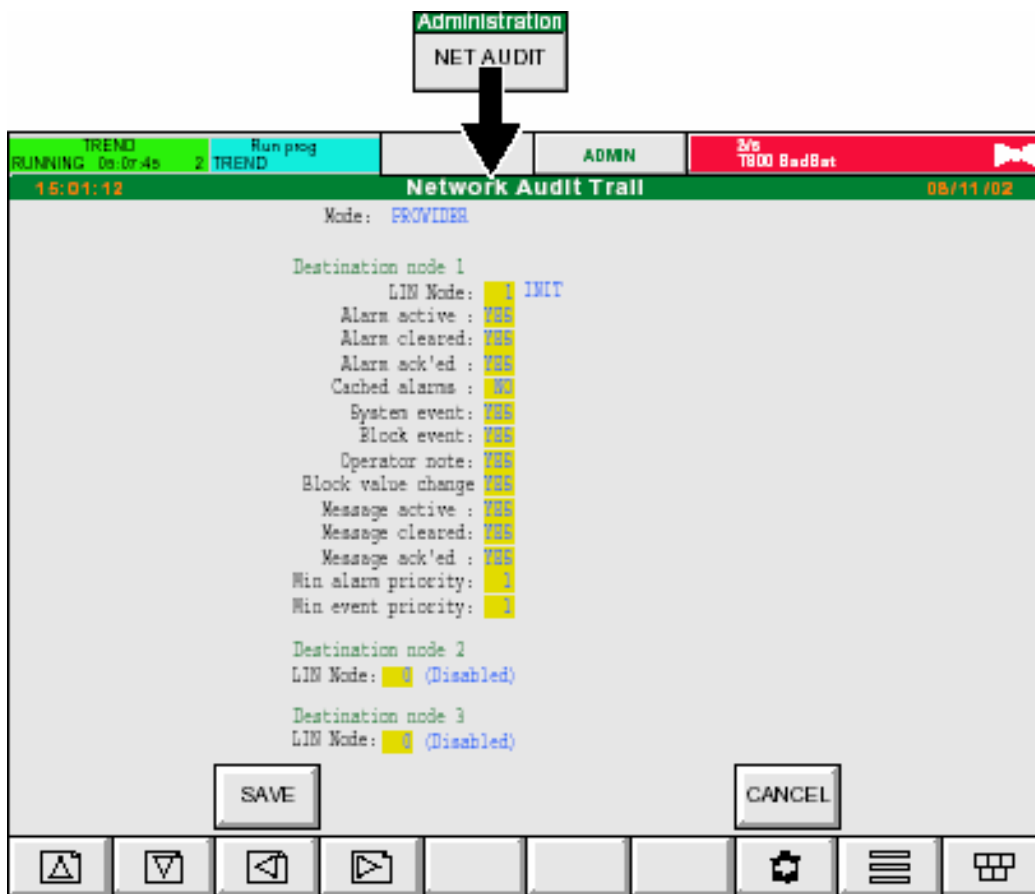
- 1 Firstly find the network port name.
- 2 Locate Security item node name in the Network folder and then trace back to the Network level.
- 3 Enter the network port name in the appropriate Audit Port field.



- 4 Ensure all T800 Visual Supervisors in the network are configured appropriately.

At each instrument open the Administration menu by operating the  (menu) button (at the bottom right of the screen) then

SYSTEM > ADMIN > NET AUDIT keys



Edit the configuration as appropriate and press **Save**.

Finally, [save changes](#) and proceed to the next task.

configure the Audit Trail field

This check box allows or does not allow the Users to request the future logging of events and alarms generated by an action when the **Default Regulation** is selected

Options > Regulations

The other **Regulations** are pre-configured (Read only fields) to record information in the Audit Trail.

The events and alarms are logged in tamper proof data storage files in a History folder in the same directory as the Security database.

Note

The default value limits of the field are subject to [Regulatory defaults](#).

It has 2 states, - True or - False. If the check box is set to (True - 21 CFR Part 11 compliant), events will be logged in the Audit Trail. If false, the Audit Trail will NOT log any events in the selected zone.

This is configured in the database for the Security Manager, EurothermSuite PC, and 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Audit Trail** check box.

indicates the Audit Trail is enabled in this Security item type.

indicates it is disabled.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Authorisation field

This check box allows or does not allow the Users to request a Authorisation Signature for the selected Security item type.

It has 2 states, True or - False. If the check box is set to True, an Authorisation Signature will be requested that ONLY Users groups with Authorise access rights allocated to this Security zone can complete before the changes can take effect. If False, an Authorisation Signature will NOT be requested.

Note

If Sign is configured as - False a User will still be requested to Sign for unsaved changes IF the Authorisation field is configured as - True.

The security configuration may request both an authentication and an authorisation signature before the changes can be implemented. An authorisation signature is used to approve the changes that have been authenticated.

This is configured in the database for the Security Manager, EurothermSuite PC, and 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Authorisation** check box.

indicates that approval will be requested in the Computer Security item type in this Security zone.

indicates it will NOT be requested.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Authorise access rights

This check box allows or does not allow the Users to sign as authorisation. This authorisation is to verify the User accepting (see [Sign](#)) the changes and also to implement the changes.

Note

The 5000 Series Instruments also use the Authorise feature, but is indicated as '**Can Authorise**' number of retrieved alarms to greater than 500.

It has 2 states, - True or - False. If the check box is set to True the User is allowed to sign as authorisation. If False, the User group has been denied the access rights.

Note

If Sign is configured as False a User will still be requested to Sign for unsaved changes IF the Authorise field is configured as True.

This is configured in the database for Security Manager, EurothermSuite PC, T800 Visual Supervisor, 5000 and 6000 Series instrument and Review Security items types.

To configure this

- 1 Click the **Authorise** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

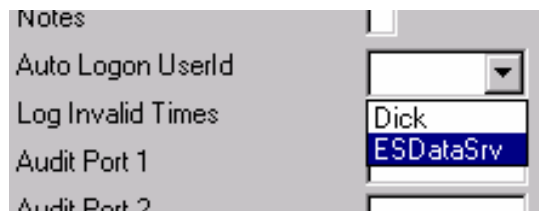
configure the Auto Logon UserId field

This field allows the input of a specified system User Id that can automatically login when the Computer Security item type is accessed. A system User Id is configured in the [System field](#) at the User tab.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click in the **Auto Logon UserId** field. This displays a drop down list.
- 2 Select a User Id from the available list.
- 3 Finally, [save changes](#) and proceed to the next task.

**configure the Batch Control access rights**

This check box allows or does not allow the Users assigned to the selected User group to define configured channels for batch control (if the option is fitted).

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to define configured channels for batch control. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Batch Control** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Change Alarm Setpoints access rights

This check box allows or does not allow the Users assigned to the selected User group to edit alarm setpoint parameters.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to edit alarm setpoint parameters. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the Change Alarm Setpoints check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Change Language access rights

This field allows the selection of a type of confirmation via a drop down list, needed before the 'InTouch WindowViewer' can convert to the selected language.

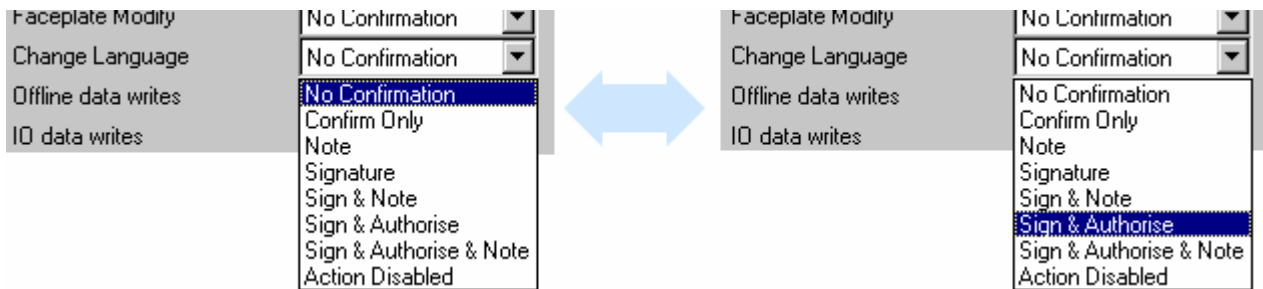
Note

This feature is dependant on the availability of appropriate software language files (.dll's).

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Change Password on Expiry access rights

This check box allows or does not allow the Users assigned to the selected User group one chance only, to modify their own password at the instrument before it expires.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to modify their own password at the instrument before it expires. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the Change Password on Expiry check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Change own expired password access rights

This check box allows or does not allow the Users to change their own password that has already expired.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change their expired password. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the **Change own expired** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Change own password access rights

This check box allows or does not allow the Users to change their own password.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change their current password. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager. It is also used in the 5000 and 6000 Series Instruments, but is described as Edit Own Password.

To configure this

- 1 Click the **Change own password** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Chart Annotate access rights

This check box allows or does not allow the Users to add notes to an open chart.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Chart Annotate command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Chart Annotate** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Chart Approve access rights

This check box allows or does not allow the Users to add approval comments to an open chart.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Chart Approve command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Chart Approve** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Chart Open/Close access rights

This check box allows or does not allow the Users assigned to the selected User group to open and close charts using the menu item, **File > Open**.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to open and close charts. If False then only the chart(s) on screen when Review was last used will be visible, or only the chart opened via a command line argument.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Chart Open/Close** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Chart Release access rights

This check box allows or does not allow the Users to add release comments to an open chart.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Chart Release command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Chart Release** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Chart Review access rights

This check box allows or does not allow the Users to add any review comments to an open chart.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Chart Review command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Chart Review** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Chart Setup access rights

This check box allows or does not allow the Users assigned to the selected User group to edit the chart setup, including Point Properties.

Note

This field will NOT allow Charts to be Saved or created.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to create and amend charts. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Chart Setup** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Confirmation field

This check box allows or does not allow the Users to enable or disable any future request for confirmation.

It has 2 states, - True or - False. If the check box is set to True, a level of confirmation via a drop down list (defined for each User group) will be requested and MUST be completed before the changes can take effect. If False, confirmation will NOT be requested by the Security item type in this Security zone.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click in the **Confirmation** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Connect from remote access rights

This check box allows or does not allow the Users assigned to the selected User group to configure the manual archiving of 5000 Series configuration data to a remote host.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to configure the manual archiving to a remote host. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the Connect from remote check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Create Chart access rights

This check box allows or does not allow the Users assigned to the selected User group to make new charts by reading .uhh/.pkd files. This also includes changes made via Point Properties.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to create charts. If False, the User group has been denied the access rights.

This is configured in the database for the QuickChart software item type.

To configure this

- 1 Click the **Create QuickChart** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Custom1 to Custom5 access rights

These fields allow or do not allow Users to perform a customer-defined function.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click the **Custom1** or appropriate checkbox.

indicates the User perform a customer-defined function.

indicates the User is not permitted to perform a customer-defined function.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Custom6 to Custom10 access rights

This field allows the selection of a type of confirmation required for completing a Custom6 to Custom10 customer defined function. It is available via a drop down list, needed when attempting to save changes to this Security item type.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Debug access rights

This field allows the selection of a type of confirmation via a drop down list, needed before Debugging Script Errors in the 'InTouch WindowViewer'.

InTouch WindowViewer > About/Help/Information > Script Errors

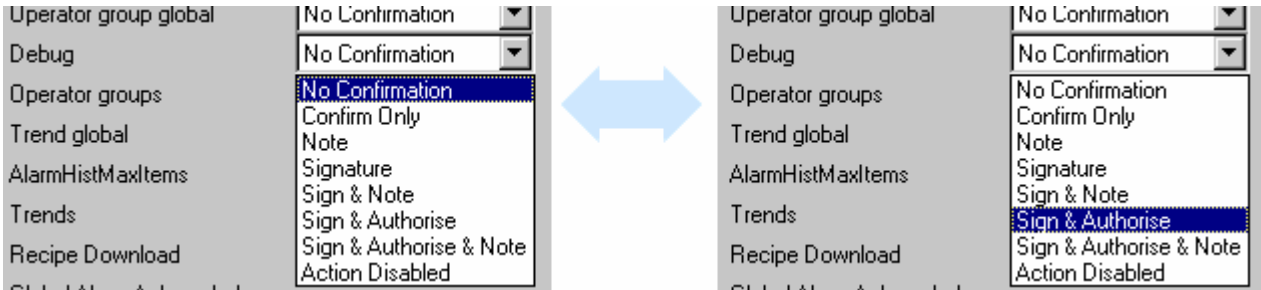
Note

The Debug feature tracks certain scripts and output information, including all writes and the 'Point Page' to the Wonderware Logger.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Delete retired users field

This field allows or does not allow Users retired by Security Manager will be deleted from the Windows domain.

This is configured in the database for Windows Domain Security item type.

To configure this

- 1 Click the **Delete retired users** checkbox.

indicates that Users retired by Security Manager will be deleted from the Windows domain.

indicates that Users retired by Security Manager will not be deleted from the Windows domain.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Deploy Security access rights

This check box allows or does not allow the Users to deploy a Security database overriding a - False Deployable Flag check box.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to deploy a Security database even if the Deployable Flag check box is - False. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click in the **Deploy Security** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Deploy existing users field

This field allows or does not allow the deployment of the database.
This is configured in the database for Windows Domain Security item type.

To configure this

- 1 Click the Deploy existing users checkbox.



indicates that deployment is permitted to a user already configured in the Windows domain.



indicates that deployment is not permitted to a user already configured in the Windows domain.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Disable Service Account field

This check box allows or does not allow the Users assigned to the selected User group to disable the Service User Account feature.

IMPORTANT NOTE

The Account is designed for use by Service Engineers ONLY.

The Service account check box has 2 states, - True or - False. If the field is set to True the Service account is disabled. If the field is set to False, a Service Engineers has full access to all instrument functions and to areas of memory for diagnostic purposes.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the Disable Service Account check box.



indicates that the Service Account is NOT configured.



indicates an account has been stored to enable access for a Service Engineers.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Display access level field

This field provides security to mimics by allowing the User to specify the security access level. To display a mimic any value entered in this field MUST be greater than that configured in the 'Display Navigation Tool' in the 'Standard Navigation' Utility. Alternatively allocating a 'display block' to the mimic will display it.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click the Display access level field.

Note

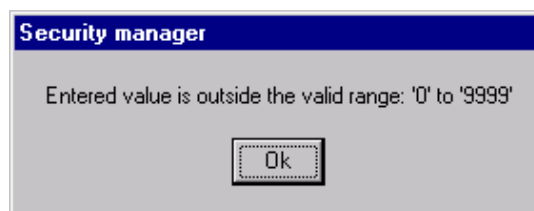
If the value is NOT highlighted double click in the field.



- 2 At the keyboard, enter a new value and press the return key.

Note

A dialog window appears if a value outside the constraints is entered. Read the dialog and click 'Ok', the field reverts to its previous setting.



- 3 Finally, [save changes](#) and proceed to the next task.

configure the Edit Deployable Flag access rights

This check box allows or does not allow the Users to select which Security item databases can be deployed.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change any Security Manager data configuration in the Utility. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click in the **Edit Deployable flag** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit Maths Constants access rights

This check box allows or does not allow the Users assigned to the selected User group to edit any constant value of one or more maths channels, (if configured with function 'Constant',) of units fitted with the Maths option.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to edit any constant value of units fitted with the Maths option. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Edit Maths Constants** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit Output Channel Default access rights

This check box allows or does not allow the Users assigned to the selected User group to edit the default value of any output channel if the Master Communications option is fitted. Normally the defaults are used only when the source channel is 'In Error'.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the default value of any output channel. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the Edit Output Channel Default check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit Security Manager setup access rights

This check box allows or does not allow the Users to change any Security Manager data configuration.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change any Security Manager data configuration in the Utility. If False, the User is denied access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click in the Edit Security Manager setup check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit security item data access rights

This check box allows or does not allow the Users to change the Security data on the Security item tab.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the Security data on the Security item tab. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the Edit security item data check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit user data access rights

This check box allows or does not allow the Users to change the Security data on the User tab.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the Security data on the User tab. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the **Edit user data** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit user global data access rights

This check box allows or does not allow the Users to change the Security data on the User global tab.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the Security data on the User global tab. If False, the User is denied access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click in the **Edit user global data** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit user group data access rights

This check box allows or does not allow the Users to change the Security data on the User global tab.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the Security data on the User group tab. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the **Edit user group data** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit zone access rights data access rights

This check box allows or does not allow the Users to change the User groups access rights on the Security zone tab.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to change the access rights for a User group. This does NOT include the access rights in the Security Manager zone. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the Edit zone access rights check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit zone configuration data access rights

This check box allows or does not allow the Users to change the User groups and Security items are in which Security zones. User groups can also add and remove Security zones.

Note

Only User groups can be changed in the Security Manager zone.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to include and exclude User groups and Security items in Security zones, although only User groups can be changed in the Security Manager zone. User groups can also add and remove Security zones. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the Edit zone configuration data check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Edit zone management data access rights

This check box allows or does not allow the Users to change the Security item management data on the Security zone tab.

Note

Although only User groups can be changed in the Security Manager zone.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to include and exclude User groups and Security items in Security zones and also add and remove Security zones. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the Edit zone management data check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Event Permission access rights

These check boxes allow or does not allow the Users assigned to the selected User group to login in order to initiate a 5000 Series event.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to login in order to initiate a 5000 Series event. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Event Permission** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Export Data access rights

This check box allows or does not allow the Users to use the Export command, excluding Export Range that must be enabled in Modify Chart View.

Note

Export Setup must be enabled to modify the other export data.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Export Data command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Export Data** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Export Historical Trend access rights

This check box allows or does not allow the Users assigned to the selected User group to export the currently viewed historical Trend in the 'InTouch WindowViewer Historical Data' window as a .CSV file.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed export the currently viewed historical Trend page. If False, the User group has been denied the access rights.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click the Export Historical Trend check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Export Setup access rights

This check box allows or does not allow the Users to configure the export parameters, excluding Export Range that must be enabled in Modify Chart View.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Export Setup command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Export Setup** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the FTP access rights

This field allows or does not allow Users access to and from a remote network site.

This is configured in the database for T800 Visual Supervisor Security items.

To configure this

- 1 Click the **FTP** checkbox.

indicates the User can have access to and from a remote network site.

indicates the Administrator User is not permitted to access a remote network site.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Faceplate Configurator access rights

This check box allows or does not allow the Users assigned to the selected User group to create and save mimic faceplates in the 'InTouch WindowViewer'.

Note

Pressing 'CTRL+SHIFT+F' when running 'InTouch WindowViewer' displays the Faceplate Configurator page.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to create and save mimic faceplates. If False, the User group has been denied the access rights.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click the Faceplate Configurator check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Faceplate Modify access rights

This field allows the selection of a type of confirmation via a drop down list, needed for accepting changes to a Faceplate via the 'InTouch WindowViewer'.

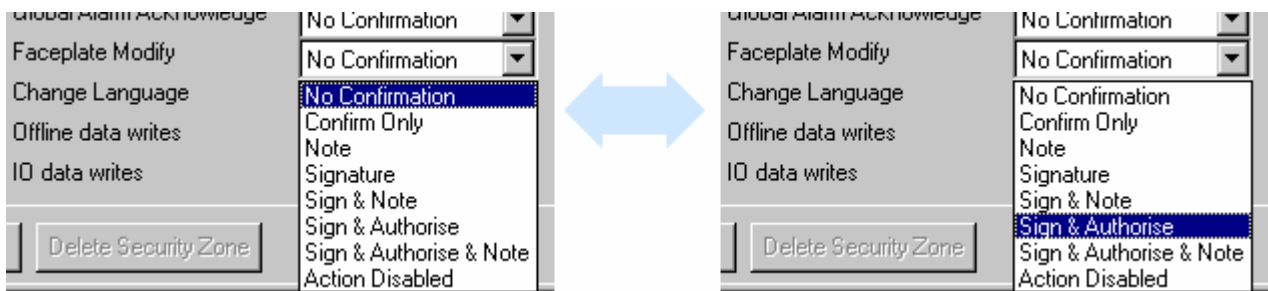
IMPORTANT NOTE

The 'Faceplate Configurator' field **MUST** be enabled before attempting to modify the Faceplates.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the File Services access rights

This check box allows or does not allow the Users to use the File Services command that is a password-controlled interface with defined instruments.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the File Services command. If False, the User group has been denied the access rights.

This is configured in the database for the Review software item type.

To configure this

- 1 Click the **File Services** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Full Configuration access rights

This check box allows or does not allow the Users assigned to the selected User group to amend the major channel/alarm option in the 5000 Series configuration.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to read and write to the major channel/alarm option in an existing configuration. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Full Configuration** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Full Security access rights

This check box allows or does not allow the Users assigned to the selected User group to create and amend the access permissions of other Users to the 5000 Series configuration.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed full access to the security functions, including adding and amending Users and the access permissions for an existing configuration. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Full Security** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

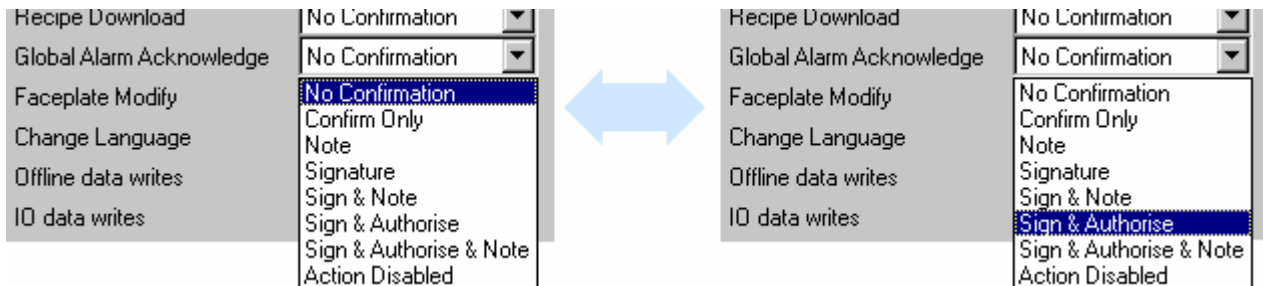
configure the Global Alarm Acknowledge access rights

This field allows the selection of a type of confirmation via a drop down list, needed for acknowledging the presence of a project wide alarm via the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Groups access rights

This field defines the Windows Domain groups for each Security Manager User group, as required.

This is configured in the database for Windows Domain Security item type.

To configure this

- 1 Click the **Group** field.
- 2 At the keyboard, enter the required Group name and press the return key.

Note
If any Windows Domain group does not exist, deployment will fail.

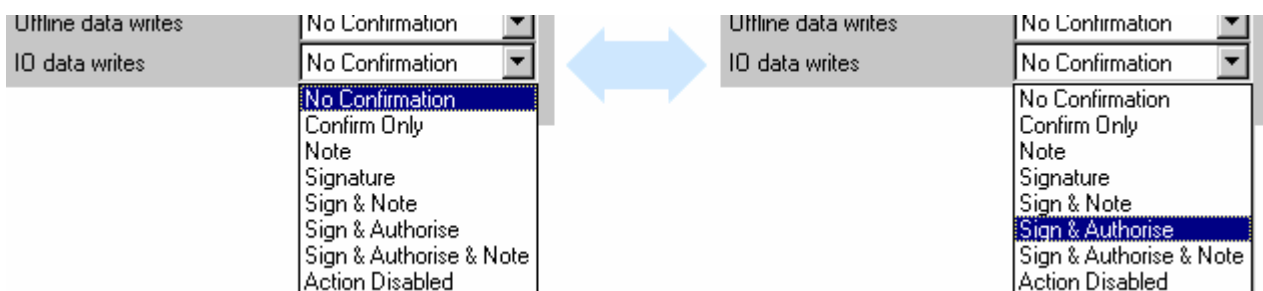
configure the IO data writes access rights

This field allows the selection of a type of confirmation via a drop down list, needed when attempting to save changes to this Security item type.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Inactivity timeout field

This field allows the input of the number of minutes the selected Security item types can be left idle before the current User is logged out.

Note

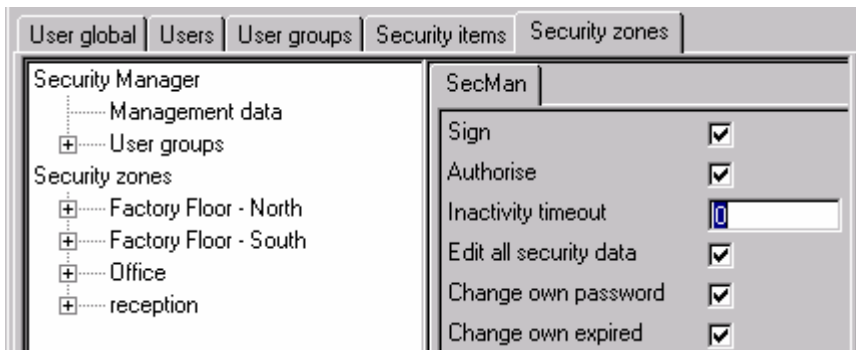
The default value limits of the field are subject to [Regulatory defaults](#) alarms to greater than 500.

To configure this

- 1 Click in the **Inactivity timeout** field.

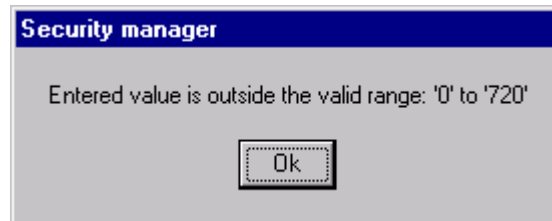
Note

If the value is not highlighted double click in the field.



- 2 Enter a new value and press the return key.

A dialog window appears if a value outside the constraints is entered. Read the dialog and click 'Ok', the field reverts to its previous setting.



If required enter an adjusted value.

- 3 Finally, [save changes](#) and proceed to the next task.

configure the Lockout Level field

This field allows or does not allow Users to configure the available actions when the EurothermSuite PC does not have a current user logged in.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Log Invalid Times field

This check box allows or does not allow the recording of invalid time stamps in the Audit Trail.

It has 2 states, - True or - False. If the check box is set to True, the Audit Trail records all time stamps NOT corresponding with that of the master database. If False, the feature is disabled.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click in the **Log Invalid Times** check box.
 indicates that the action is enabled.
 indicates the feature is disabled.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Login by User List field

This check box allows the User to specify that a User can Login to the 5000 Series instrument by either selecting a User Id from a drop down list or by simply typing in the appropriate User Id and Password.

It has 2 states, - True or - False. If the check box is set to True, a login User Id is selected from a drop down list. If False, a login User Id has to be typed in.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Login by User List** check box.
 indicates the feature is enabled in this Security item type.
 indicates it is disabled.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Login timeout field

This field allows the input of the number of minutes the Security item type in the Security zone can be left idle before the current User is automatically logged out.

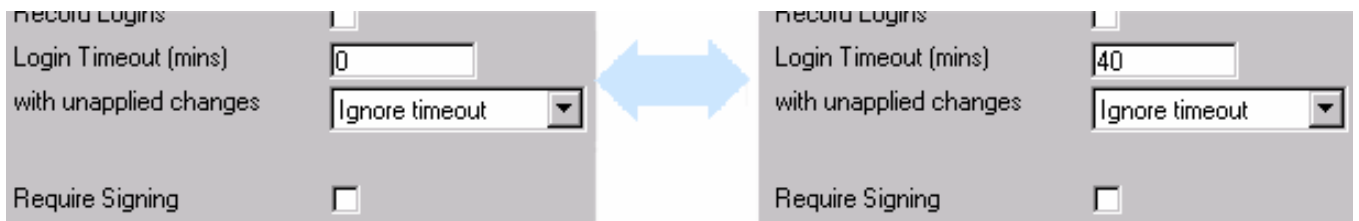
The **Login timeout** as configured for the 5000 and 6000 Series instrument Security item type is used in conjunction with the **'with unapplied changes'** configuration. This defines the consequences to any unsaved changes when the specified time has elapsed (see ['with unapplied changes'](#)).

Note
The default value limits of the field are subject to [Regulatory defaults](#).

To configure this

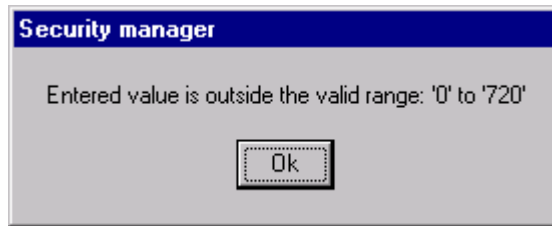
- 1 Click the **Login timeout** field.

Note
If the value is NOT highlighted double click in the field.



- 2 Enter a new value and press the return key.

A dialog window appears if a value outside the constraints is entered. Read the dialog and click 'Ok', the field reverts to its previous setting.



If required enter an adjusted value.

- 3 Finally, [save changes](#) and proceed to the next task.

configure the Modify Chart View access rights

This check box allows or does not allow the Users assigned to the selected User group to,

- use the Zoom
- use the Chart Go to
- use the scroll functions
- change the view settings in Print Setup and Export dialog
- switch between chart and spreadsheet view.

Note

This field will NOT allow changes to the Page Setup or Layout parameters.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the various view commands. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Modify Chart View** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Notes field

This check box allows or does not allow the Users to enable or disable any future request for input of additional comments concerning the changes to the Security database.

It has 2 states, - True or - False. If the check box is set to True the User MUST enter comments concerning the changes to the Security database. If False, the field is NOT displayed and additional comments will NOT be requested.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click in the **Notes** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task

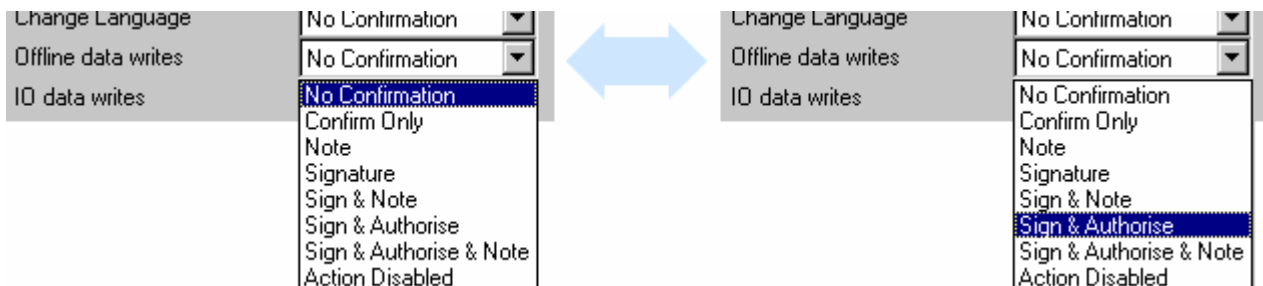
configure the Offline data writes access rights

This field allows the selection of a type of confirmation via a drop down list, needed when attempting to save changes to this Security item type that is currently offline.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Operator Point Display access rights

This check box allows or does not allow the Users assigned to the selected User group to display a reduced information format 'Operator Point' page (if defined) in the 'InTouch WindowViewer'.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to display a reduced information format 'Operator Point' page. If False, the User group has been denied the access rights.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click the Operator Point Display check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

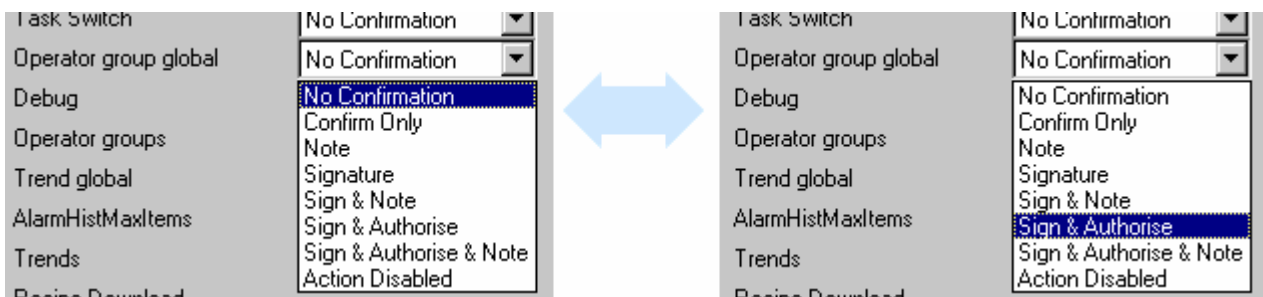
configure the Operator group global access rights

This field allows the selection of a type of confirmation via a drop down list, needed to accept changes to other Users configured operator group configurations in the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

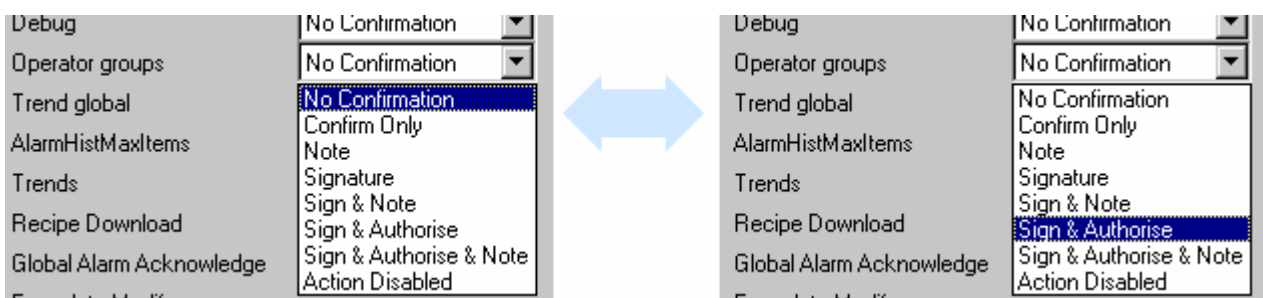
configure the Operator groups access rights

This field allows the selection of a type of confirmation via a drop down list, needed to accept only changes to their own configured operator group configurations in the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

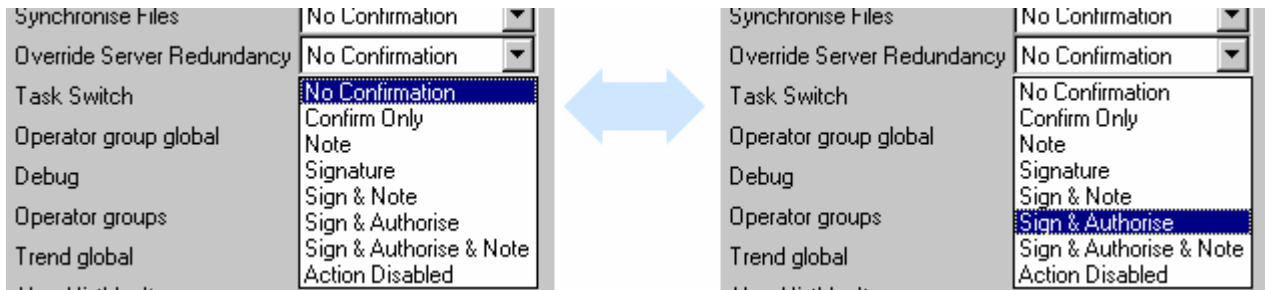
configure the Override Server Redundancy access rights

This field allows the selection of a type of confirmation via a drop down list, needed before switching from a server that has detected the 'LINOPC' watchdog has ceased to a second specified server in the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Password Expiry field

This field allows the input of a specified period in days until a User password will expire for the selected Security item type.

Note
The default value limits of the field are subject to [Regulatory defaults](#).

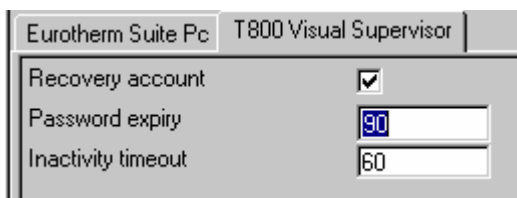
The Password expiry period is configured in the databases for the Security Manager, 5000 Series and T800 Visual Supervisor instruments Security items.

Note
The Password expiry period does NOT apply to passwords received via Security deployment.

To configure this

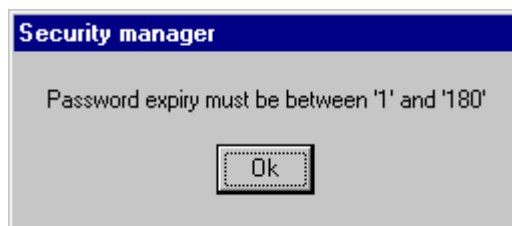
- 1 Click the **Password expiry** field.

Note
If the value is NOT highlighted double click in the field.



- 2 At the keyboard, enter a new value and press the return key.

Note
If a value outside the constraints is entered, a dialog window appears Read the dialog and click 'Ok' to return this field to its previous setting.



- 3 Finally, [save changes](#) and proceed to the next task.

configure the Paste/Delete Files access rights

This check box allows or does not allow the Users assigned to the selected User group to copy, paste and delete specified configurations.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to copy, paste and delete specified configurations. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Paste/Delete Files** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Perform Upgrade access rights

This field allows or does not allow the User to perform an update to the instrument software.

This is configured in the database for the 6000 Series instrument Security item.

To configure this

- 1 Click the **Perform Update** checkbox.

indicates the User can update the instrument software.

indicates the User is not permitted to update the instrument software.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Preset Counters access rights

This check box allows or does not allow the Users assigned to the selected User group to preset counter values (if the option is fitted) either directly from the configuration page or by setting a counter job.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to preset counter values, if the option is fitted. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Preset Counters** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Preset Totalisers access rights

This check box allows or does not allow the Users assigned to the selected User group to preset totaliser values (if the option is fitted) either directly from the configuration page or by setting a totaliser job.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to preset totaliser values, if the option is fitted. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Preset Totalisers** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Print Setup access rights

This check box allows or does not allow the Users to configure the print parameters, excluding Print Range that must be enabled in Modify Chart View.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to use the Print Setup command. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Print Setup** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Print access rights

This check box allows or does not allow the Users assigned to the selected User group to print selected pages from the 'InTouch WindowViewer' or charts and spreadsheets from Review software.

Note

Review software requires that to modify the Print Range in the print setup dialog the Modify Chart View must be enabled. Print Setup must be enabled to modify other print data.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to print. If False, the User group has been denied the access rights.

This is configured in the database for EurothermSuite PC, Review and QuickChart software Security item types.

To configure this

- 1 Click the **Print** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

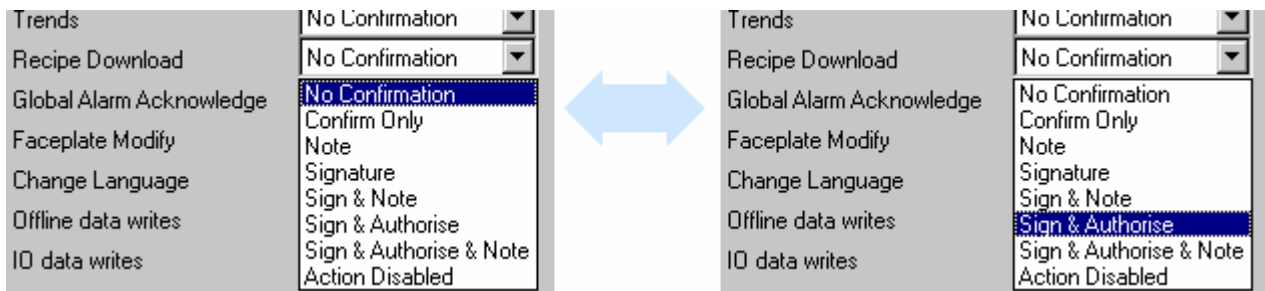
configure the Recipe Download access rights

This field allows the selection of a type of confirmation via a drop down list, needed before a recipe can be downloaded to a specified location.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Record Logins field

This check box allows or does not allow the Users assigned to the selected User group to any future login or logout message appearing on the chart only when the **Default Regulation** is selected

Options > Regulations

The other **Regulations** are pre-configured to record this information in the Audit Trail.

Note

The default value limits of the field are subject to [Regulatory defaults](#).

It has 2 states, - True or - False. If the check box is set to (True - 21 CFR Part 11 compliant), any login or logout message will occur on the chart. It will include the date, time, MAC address of the remote viewing device and login name. If False, the Audit Trail will NOT log any events in the selected zone.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Record Logins** check box. indicates the feature is enabled in this Security item type. indicates it is disabled.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Recovery account field

This check box allows or does NOT allow the Users assigned to the selected User group to enable or disable the T800 Visual Supervisor Recovery account feature.

It is recommended that...

this field is set to True, to ensure it is always possible to retrieve a corrupt database.

It has 2 states, - True or - False. If the field is set to True a User can access a T800 Visual Supervisor item type that has ALL Users '**Locked out**', '**Disabled**' or '**Retired**' using a blank User Id. The User will login with full access rights. If the field is set to False, the '**Recovery account**' is disabled.

Note

If this feature has NOT been enabled, the instrument must be returned to the supplier where recovery of the account can be attempted.

This is configured in the database for T800 Visual Supervisor Security item type.

To configure this

- 1 Click the **Recovery account** check box.
 - indicates that the User may shutdown the Export Historical Trend view in the T800 Visual Supervisor item type.
 - indicates the Users has insufficient access rights.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Recovery user field

This check box allows or does not allow the Users to enable or disable the 'Recovery user ' account.

It has 2 states, - True or - False. If the field is set to True a User can access the database that has ALL Users 'Locked out', 'Disabled' or 'Retired' using a blank User Id. The User can login with full Access Rights. If the field is set to False, the Recovery user account is disabled.

This is configured in the database for the Security Manager.

To configure this

- 1 Click the **Recovery user** check box.

indicates that the Recovery user is configured in the Computer Security item type.

indicates it is NOT configured.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Reference Number access rights

This field allows the User to enter a **Reference Number** between '0' and '65535' that corresponds to a number entered in software scripts used within T800 Visual Supervisor.

As the Reference Number within Security Manager is configured per User group, ALL Users within that User group inherit the specified **Reference Number**. Therefore, a User assigned to numerous User groups may have numerous reference numbers corresponding to areas within T800 Visual Supervisor software scripts.

Note

If a User is assigned to numerous User groups only the Users highest '**Reference Number**' is deployed, ignoring all the Users other reference numbers that may cause the software scripts to operate incorrectly.

It is recommended that...

*to avoid problems when using the '**Reference Number**' field, each User should also have their own individual User group with only the '**Reference Number**' configured.*

This is configured in the database for T800 Visual Supervisor Security item type.

To configure this

- 1 Click the **Reference Number** field.

Note

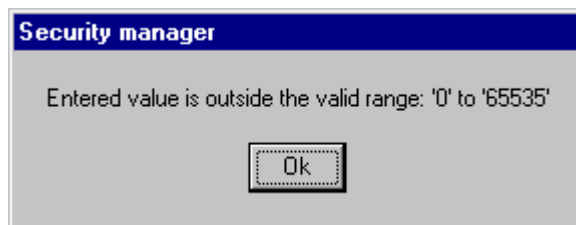
If the value is not highlighted double click in the field.



- 2 At the keyboard, enter a new value and press the return key.

Note

If a value outside the constraints is entered, a dialog window appears Read the dialog and click '**OK**' to return this field to its previous setting.



- 3 Finally, [save changes](#) and proceed to the next task.

configure the Remote access rights

This field allows or does not allow Users remote access to this Security item type, in this Security zone.

This is configured in the database for T800 Visual Supervisor Security items.

To configure this

- 1 Click the **Remote** checkbox.



indicates the User can remotely access this Security item type, in this Security zone.



indicates the User is not permitted to remotely access this Security item type, in this Security zone.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Reset Maths access rights

This check box allows or does not allow the Users assigned to the selected User group to reset applicable maths function,

- from the maths channel configuration page
- by setting a maths job

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to reset applicable maths function. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Reset Maths** check box.



indicates that the User group is allowed to use this action.



indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Save Chart access rights

This check box allows or does not allow the Users to save the new view of a file that has been modified by one of the actions allowed in [Modify Chart View](#).

Note

This command is automatically enabled if Chart Setup access right is True.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to save the new view of a file. If False, the User group has been denied the access rights.

This is configured in the database for the Review and QuickChart software item type.

To configure this

- 1 Click the **Save Chart** check box.



indicates that the User group is allowed to use this action.



indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Save/Restore access rights

This check box allows or does not allow the Users assigned to the selected User group to saving or restoring 5000 Series configurations. User Screens can be imported and exported if the User Screens option is fitted.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to save or restore a configuration. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Save/Restore** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Set Clock access rights

This check box allows or does not allow the Users assigned to the selected User group to set the time and date functions.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to set the time and date functions. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Set Clock** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Sign access rights

This check box check box allows or does not allow the Users to sign for unsaved changes at the Security item type in the Security zone.

Note

If **Sign** is configured as False a User will still be requested to Sign for unsaved changes IF the Authorise field is configured as True.

Note

The 5000 Series Instruments also use the Sign feature, but is referred to as '**Can Sign**'.

It has 2 states, - True or - False. If the check box is set to True the User is allowed to sign. If False, the User group has been denied the access rights.

This is configured in the database for Security Manager, EurothermSuite PC, T800 Visual Supervisor, 5000 and 6000 Series instrument Security items types.

To configure this

- 1 Click the **Sign** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Signing field

This check box allows or does not allow the Users assigned to the selected User group to request a Authentication Signature for the selected Security item type when the **Default** or **21 CFR Part 11 - Records Regulation** is selected via

Options > Regulations

The **21 CFR Part 11 - Signature Regulation** is pre-configured (Read only field) to request signatures before performing the action.

Note

The default value limits of the field are subject to [Regulatory defaults](#).

It has 2 states, - True or - False. If the check box is set to True, an Authentication Signature will be requested that ONLY Users groups with Sign access rights allocated to this Security zone can complete before the changes can take effect. If False, an Authentication Signature will NOT be requested.

This is configured in the database for all Security items types.

To configure this

- 1 Click the **Signing** check box.

indicates that an Authentication Signature will be requested by this Security item type in this Security zone.

indicates it will NOT be requested.

Note

This is also referred to as the 'Sign for Annotation' field in the Review and QuickChart software Security items types.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Start/Reset Timers access rights

This check box allows or does not allow the Users assigned to the selected User group to start and reset the timer (if the option is fitted) either directly from the configuration page or by setting a timer job.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to control the timer, if the option is fitted. If False, the User group has been denied the access rights.

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Click the **Start/Reset Timers** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the Synchronise Files access rights

This field allows the selection of a type of confirmation via a drop down list, needed before deploying (pressing CTRL+SHIFT+H keys) the latest version of selected files to specified locations using the 'InTouch WindowViewer'.

InTouch WindowViewer > About/Help/Information > Synchronise Files

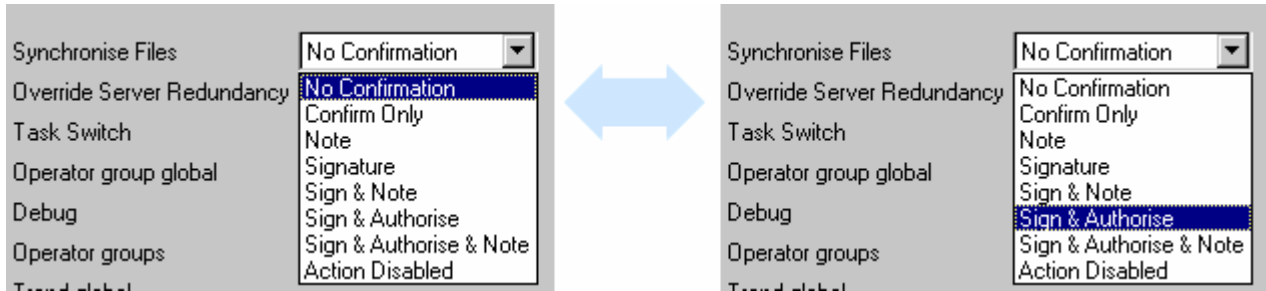
Note

The feature mimics the **File Reconcile Utility** by deploying the latest version of selected files to specified locations.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the System User writes access rights

This field allows the selection of which field writes are logged for system Users, as defined in the User tab.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of system reporting required from a drop down list, as described above.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the Tag Security Area access level fields

These Tag Security Area access level fields are used to associate [Tag Security Areas](#), created using 'Project Organiser', with defined access level enumeration's.

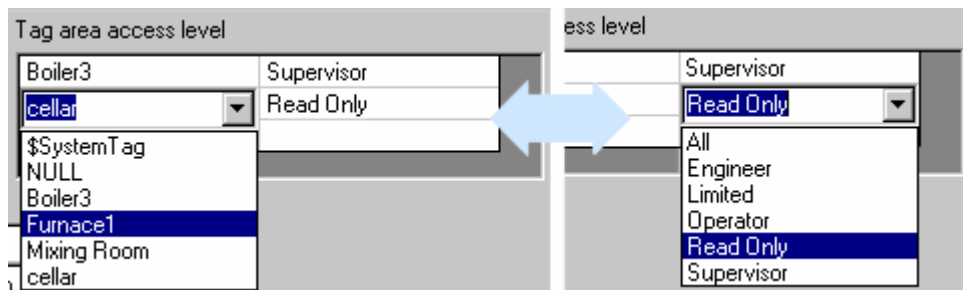
Remember

Tags can ONLY be edited by Users with Access Levels equal or greater than the selected value.

Example: Tag Security Area Access Levels

To configure this

- 1 Select the **Tag Security Area** from the drop down list in the last available field. A row is automatically added when the last field in either column is configured.



- 2 Select the appropriate Access Level from the drop down list in the corresponding right hand field.
- 3 Finally, [save changes](#) and proceed to the next task.

configure the TagEdit access rights

This check box allows or does not allow the Users assigned to the selected User group to edit Tags in the

- On-line 'Tag Browser' (in Plant Units, Alarm Groups and Networks)
- menu item on the 'Point Page menu' via the 'InTouch WindowViewer'

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to edit Tags in the Online 'Tag Browser'. If False, the User group has been denied the access rights.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Click the **TagEdit** check box.
 - indicates that the User group is allowed to use this action.
 - indicates the Users assigned to the selected User group will have insufficient access rights.
- 2 Finally, [save changes](#) and proceed to the next task.

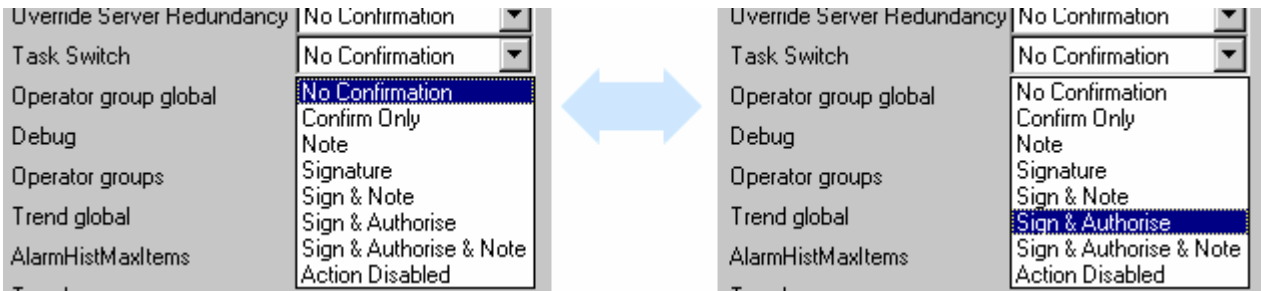
configure the Task Switch access rights

This field allows the selection of a type of confirmation via a drop down list, needed when accessing the operating system environment (pressing ALT+TAB keys) via the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the Transfer Files access rights

This check box allows or does not allow the Users assigned to the selected User group to transfer data into the Review database by any of the manual routes.

Note
The Automatic Backup/Transfer continues irrespective of permissions of current user.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to transfer the data to the Review database. If False, the User group has been denied the access rights.

This is configured in the database for the Review software item type.

To configure this

- 1 Click the **Transfer Files** check box.
 - indicates that the User group is allowed to use this action.
 - indicates the Users assigned to the selected User group will have insufficient access rights.
- 2 Finally, [save changes](#) and proceed to the next task.

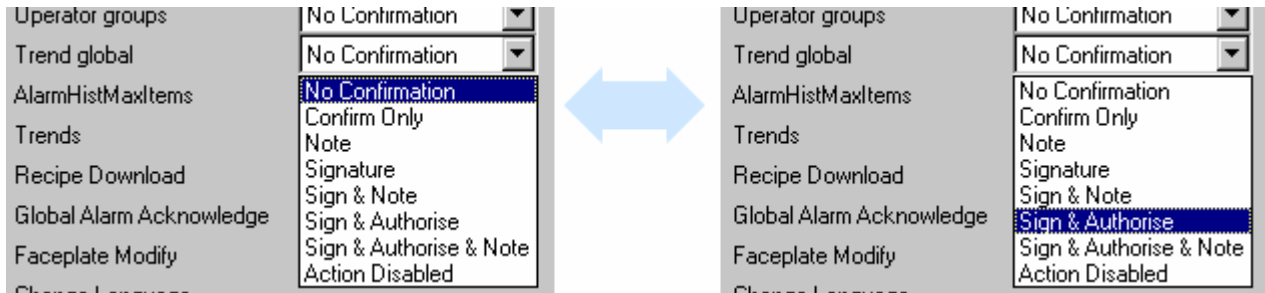
configure the Trend Global access rights

This field allows the selection of a type of confirmation via a drop down list, needed to accept changes to other Users configured Trend data in the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

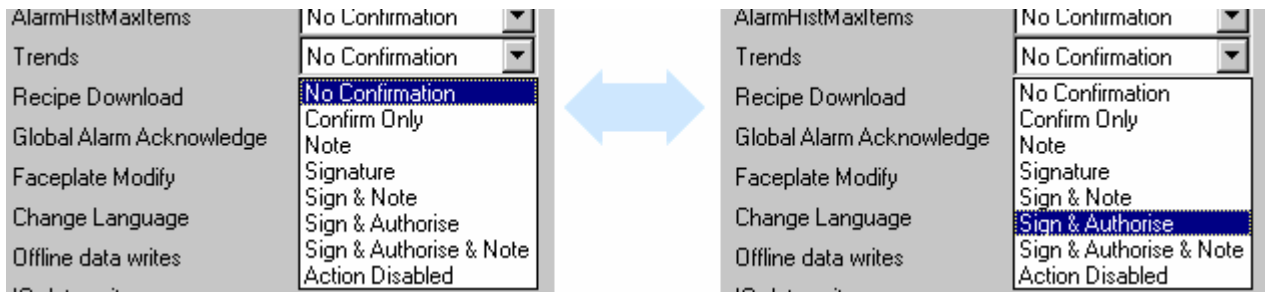
configure the Trends access rights

This field allows the selection of a type of confirmation via a drop down list, needed to accept only changes to their own configured Trend data in the 'InTouch WindowViewer'.

This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Select the type of confirmation required from a drop down list, as described above.



- 2 Finally, [save changes](#) and proceed to the next task.

configure the User1 to User4 access rights

This field allows or does not allow the indicated User to perform a customer-defined function.

This is configured in the database for T800 Visual Supervisor Security items.

To configure this

- 1 Click the **User1** or appropriate checkbox.
 - indicates the User perform a customer-defined function.
 - indicates the User is not permitted to perform a customer-defined function.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the View Only access rights

This check box allows or does not allow the Users assigned to the selected User group to enable or disable write access to the controllable features in all T800 Visual Supervisor Security items in the zone. This ensures the Users in the User group can only view the instrument information.

This is configured in the database for T800 Visual Supervisor Security items.

To configure this

- 1 Click the **View Only** checkbox.

indicates that Users in this User group can ONLY VIEW the controllable features.

indicates the Users can edit controllable features.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the View Security Data access rights

This check box allows or does not allow the Users to view and print all Security data.

It has 2 states, - True or - False. If the check box is set to True the User group is allowed to view and print all Security data. If False, the User group has been denied the access rights.

This is configured in the database for the Security Manager Security item type.

To configure this

- 1 Click the **View Security Data** check box.

indicates that the User group is allowed to use this action.

indicates the Users assigned to the selected User group will have insufficient access rights.

- 2 Finally, [save changes](#) and proceed to the next task.

configure the With unapplied changes field

This field allows or does not allow the Users assigned to the selected User group to specify the consequences to any unsaved changes when the **Login timeout period** has elapsed.

The drop down list displays the **Discard Changes** and **Ignore timeout**.

It is recommended that...

*this is configured as **Discard Changes**, as this will ensure that when the [Login timeout period](#) has elapsed the instrument will automatically logout, whereas if configured as **Ignore timeout**, changes to the instrument values are retained but the database remains open and is susceptible to access from unauthorised Users.*

This is configured in the database for 5000 and 6000 Series instrument Security items.

To configure this

- 1 Select **Discard Changes** or **Ignore timeout** from a drop down list, as described above.
- 2 Finally, [save changes](#) and proceed to the next task.

configure the downloaded Recipes field

These field enables a [system User Id](#) ('ESDataSrv' system User Id can be created when adding a Computer Security item for this purpose) to be assigned to a selected Recipe. A Recipe is downloaded to a known location, then the designated User Id is allowed to start the Recipe, which thereafter is controlled by the system.

Note

Remember to configure the type of confirmation via a drop down list required to allow the [Recipe Download](#) to proceed.

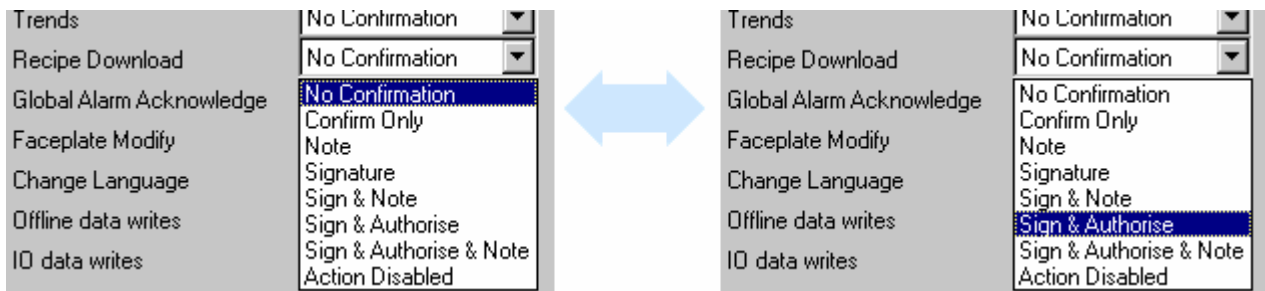
This is configured in the database for EurothermSuite PC Security item type.

To configure this

- 1 Enter the following data, into the first blank left hand field.

<File Name including full path name>/<Unit>/<Recipe>

A row is automatically added when the last field in either column is configured.



- 2 Select the system User Id designated to start the Recipe from the drop-down in the appropriate right hand field.
- 3 Finally, [save changes](#) and proceed to the next task.

Editing parameters

change the User Id

This is a Read Only column but is incremented when Users are added.

change the Password field

This field is edited within the constraints configured in the User Global tab, to change the password before the User can access a Security database.

Note
When changing the password at a client database, confirmation is required by a second authorised User.

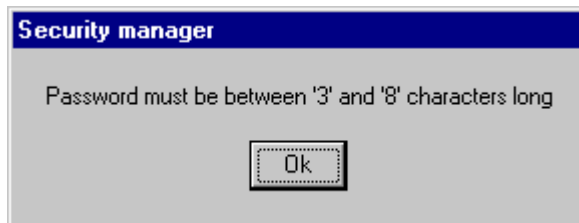
- 1 Select the appropriate Users '**Password**' field.

Note
If the value is NOT highlighted double click in the field.

User Id	Password	Change password	Pa exp
ADMIN	xxxxxxx	False	
ADMIN2	xxxxxxx	False	
Beth	xxxxxxx	False	
Dick	xxxxxxx	False	
Harry	xxxxxxx	False	
Thomas	xxxxxxx	False	

- 2 Enter a new case-sensitive password value which does not exceed the selected [Regulatory value constraints](#) and press the return key.

Note
If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field. Click '**OK**' to return this field to its previous setting and then attempt the change again.



- 3 Read the information on the dialog window requesting password re-entry, and confirm by clicking the '**OK**' button.



- 4 In the same field as before enter the identical password again.

Note
Passwords are displayed as 'xxxxxxx'.

- 5 Finally [save changes](#).

change the Change Password field

This field is edited to enable/disable the need for a User to change the password when attempting to login for the first time.

- 1 Select the appropriate Users 'Change password' field.
- 2 Select the appropriate indicator.

Note

If False, the User will NOT be requested to change the [Password](#). If True, when the User next attempts to [login](#) a prompt appears requesting a change of password.

User Id	Password	Change password	Password expiry (days)	R
ADMIN	*****	False	0	U
ADMIN2	*****	False	0	
Beth	*****	False	0	
Dick	*****	False	0	
Harry	*****	True	0	
Thomas	*****	False	0	

- 3 Finally [save changes](#).

change the Password expiry time period

Change this field to increase or decrease the minimum number of days until a password expires and requires changing.

- 1 Select the appropriate Users 'Password expiry' field.

Note

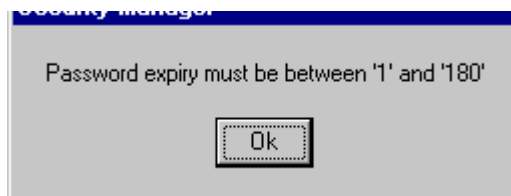
If the value is NOT highlighted double click in the field.

User Id	Change password	Password expiry (days)	Remote User Id
ADMIN	False	0	
ADMIN2	False	0	
Beth	False	0	
Dick	False	0	
Harry	False	0	
Thomas	False	0	

- 2 Enter a value which does not exceed the selected [Regulatory value constraints](#) and press the return key.

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field. Click 'OK' to return this field to its previous setting and then attempt the change again.



- 3 Finally [save changes](#).

change the Remote User Id

This field is edited to enable the User access to a Security database via a 5000 Series instrument.

- 1 Select the appropriate Users 'Remote User Id' field.

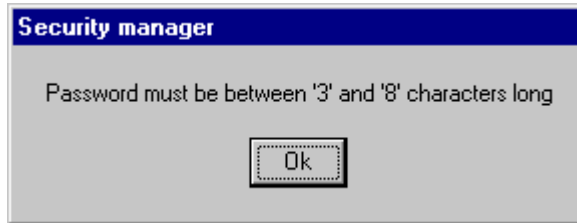
Note

If a value is NOT highlighted double click in the field.

- 2 Enter a value which does not exceed the selected [Regulatory value constraints](#) and press the return key.

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field. Click 'OK' to return this field to its previous setting and then attempt the change again.



- 3 Finally [save changes](#)

change the Remote password field

This field is edited within the constraints configured in the Minimum and Maximum Password Length fields on the User Global tab, to change the password before the User can access a Security database via a 5000 Series instrument.

- 1 Select the appropriate Users '**Remote password**' field.

Note

If a value is NOT highlighted double click in the field.

- 2 Enter a new case-sensitive password value which does not exceed the selected [Regulatory value constraints](#) and press the return key.

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field. Click 'OK' to return this field to its previous setting and then attempt the change again.

- 3 Read the information on the dialog window requesting password re-entry, and confirm by clicking the 'OK' button.



- 4 In the same field as before enter the identical password again.

Note

Passwords are displayed as 'xxxxxxx'.

- 5 Finally [save changes](#)

change the Enabled

Change the Enabled field to indicate the User has been denied access to the Security database.

- 1 Select the appropriate Users Enabled field.
- 2 Select appropriate indicator.

Note

True indicates a User account as Active. False identifies a User account as Locked out.

User Id	System	Retired	Enabled	Lo att
ADMIN	False	False	True	
ADMIN2	False	False	True	
Beth	False	False	True	
Dick	False	False	False	
Harry	False	False	True	
Thomas	False	False	False	

- 3 Finally [save changes](#).

change the Fullname

Change the Fullname field to enter an appropriate name for the User account.

- 1 Select the appropriate Users 'Fullname' field.

Note

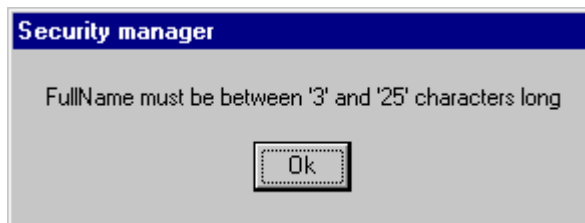
If the value is NOT highlighted double click in the field.

User Id	Remote User Id	Remote password	FullName	System	R
ADMIN		*****	ADMIN	False	Fa
ADMIN2		*****	ADMIN2	False	Fa
Beth		*****	Elizabeth	False	Fa
Dick		*****	Dick MyPro	False	Fa
Harry		*****	Harry	False	Fa
Thomas		*****	Thomas	False	Fa

- 2 Enter a value which does not exceed the selected [Regulatory value constraints](#) and press the return key.

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field. Click 'OK' to return this field to its previous setting and then attempt the change again.



- 3 Finally [save changes](#).

change the System field

Change this field to identify an account used to perform system functions.

- 1 Select the appropriate **'System'** field.
- 2 Select appropriate indicator.

Note
True indicates the account is used by the system. False identifies it as a User account.

User Id	FullName	System	Retired
ADMIN	ADMIN	False	False
ADMIN2	ADMIN2	False	False
Beth	Elizabeth	False	False
Dick	Dick	<input type="checkbox"/>	False
Harry	Harry	<input type="checkbox"/>	False
Thomas	Thomas	False	False

- 3 Finally [save changes](#).

change the Retired field

Change this field to terminate the selected User account, thus preventing the selected User access to the Security database.

- 1 Select the **'Retired'** field associated with the User who is to be terminated.
- 2 Select **'True'** from the drop down list.

All records of Retired accounts compliant to the Default Regulation are removed, whereas records of Retired accounts compliant to the 21 CFR Part 11 are retained, (greyed out in the User tab).

Beware

There is NO confirmation requested for this action.
SO MAKE SURE !

Note

Only accounts Retired AFTER the LAST save can be re-instated. These Retired accounts can be re-instated using the [File > Discard Changes](#) option. This causes ALL unsaved changes to be discarded, thus re-instating the terminated account.

User Id	FullName	System	Retired	Enabled
ADMIN	ADMIN	False	False	True
ADMIN2	ADMIN2	False	False	True
Beth	Elizabeth	False	False	True
Dick	Dick	False	<input type="checkbox"/>	True
Harry	Harry	False	<input checked="" type="checkbox"/>	True
Thomas	Thomas	False	False	True

- 3 Finally [save changes](#).

change the Reason field

This is a Read Only column automatically describing the cause that resulted in the User to be Locked out.

This field automatically describes the cause that resulted in the User to be Locked out.

If there is a number of reasons ONLY 1 is displayed at a time but each MUST be dealt with before the User can access the Security database.

User Id	Login attempts	Locked out	Reason
ADMIN	0	False	
ADMIN2	0	False	
Beth	0	False	
Dick	0	True	Account disabled
Harry	0	False	
Thomas	0	False	

A User can be Locked out if the,

- User account has been disabled ('Enabled' field reads 'False', Reason field reads 'Account disabled')
- login attempts have been exceeded
- password has expired
- User account has been Retired ('Retired' field reads 'True' Reason field reads 'Account retired')

change the Login dialog timeout

Change the numeric value to increase or decrease the amount of time a Login prompt window will remain displayed before automatically logging out.

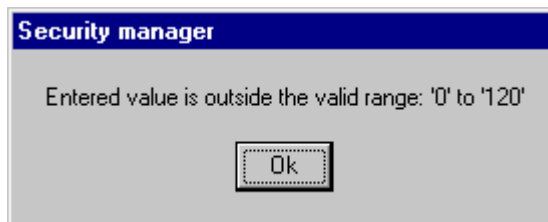
- 1 Click the editable 'Login dialog timeout' field.

Note
The existing value is highlighted. If the value is NOT highlighted double click in the field.

User global	Users	User groups	Security items	Security zones
Login dialog timeout				
Max login attempts				
Keep retired User Ids				
Min User Id length				

- 2 Enter the value that does not exceed the selected [Regulatory value constraints](#).

Note
If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.



- 3 Finally [save changes](#).

change the keep retired User Id

Change this field to allow User Ids and Passwords to be stored in the Project database or to be erased when the User is configured as retired.

- 1 Click the 'Keep retired User Ids' field to reveal the True/False menu.
- 2 Select either
 - True, to retain ALL User accounts and remain compliant with 21 CFR part 11 guidelines, or
 - False, to allow retired User accounts to be erased.

Note

All records of Retired accounts compliant to the Default Regulation are removed, whereas records of Retired accounts compliant to the 21 CFR Part 11 are retained, (greyed out in the User tab).

- 3 Finally [save changes](#).

change the Password reuse period

Change this field to increase or decrease the minimum number of days before an expired password may be used again.

- 1 Click the editable 'Password reuse period' field.

Note

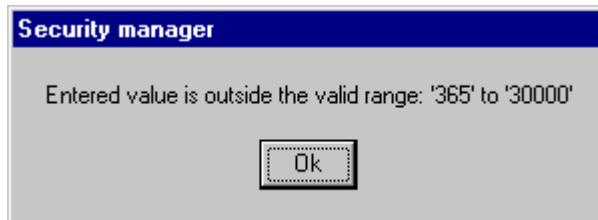
The existing value is highlighted. If the value is NOT highlighted double click in the field.

User global	Users	User groups	Secu
Login dialog timeout			0
Max login attempts			0
Keep retired User Ids			True
Min User Id length			3
Max User Id length			8
Min password length			3
Max password length			8
Password reuse period			0

- 2 Enter the value that does not exceed the selected [Regulatory value constraints](#).

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.



- 3 Finally [save changes](#).

change the maximum User Id length

Change this field to increase or decrease the maximum number of characters used by for ALL User Id's in the database.

- 1 Click the editable 'Maximum User Id length' field.

Note

The existing value is highlighted. If the value is NOT highlighted double click in the field.

User global	Users	User groups	Secur
Login dialog timeout			0
Max login attempts			0
Keep retired User Ids			True
Min User Id length			3
Max User Id length			
Min password length			3
Max password length			8

- 2 Enter a value of between 3 and 8 which does not exceed the selected [Regulatory value constraints](#).

Note

If a value entered exceeds the constraints, a dialog window appears. Read the dialog indicating the constraints of the field and then click 'OK' to return this field to its previous setting.



- 3 Finally [save changes](#).

Default accounts

These accounts are allocated to the default 'Administrators' User group in the Security Manager zone.

Note
Earlier Security Manager versions use the User Id - EPA (NOT case-sensitive), Password - EPAEPA (case-sensitive).

Default Account 1

User Id - ADMIN (NOT case-sensitive), Password - ADMIN (case-sensitive).

Default Account 2

User Id - ADMIN2 (NOT case-sensitive), Password - ADMIN2 (case-sensitive).

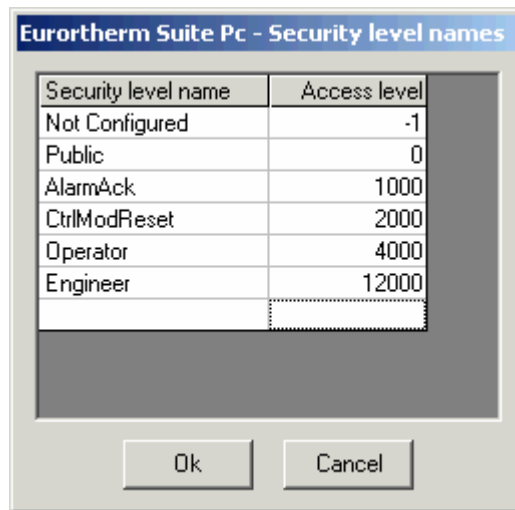
The default Access Rights vary depending on the Regulation selected.

Incorrect User Id or Password

An incorrect **User Id** or **Password** results in the display of the Invalid User Id/Password dialog box. It timeouts after approximately 30 seconds or can be closed by clicking the 'Ok' button.

Access Level enumeration's

Numeric values may be entered instead of the enumerations.



TagEdit and ESDataSrv user account

When TagEdit is used with the configuration tools the User does not have to login, instead TagEdit uses the system User Id, ESDataSrv. The ESDataSrv account can be created when adding a Security item. Therefore if security is enabled, it is necessary give ESDataSrv the necessary Access Levels to the Tag Security Areas.

What is a Tag Security Area?

Tags are assigned to Tag Security Areas (formerly Security Areas) using TagEdit. When User groups are allocated to Security zones they can be assigned an Access Level to selected Tag Security Areas. This determines what privileges the User has when writing to Tags within the selected Tag Security Area.

Example 1 - Tag Security Area Access Levels

This table shows that Users in User group 1 have Operator Access Levels which is sufficient the edit Tag1 and Tag3 in Tag Security Area 3 and Tag5 and Tag6 in Tag Security Area 6, but insufficient to edit Tag2 in Tag Security Area 2.

User group Access Level	Tag	Location	Tag Security Area	Tag Access Level
Operator (UG1)	Tag1, and Tag3	PC_12	Tag Security Area 3	Operator (8000)
Operator (UG1)	Tag2	PC_12	Tag Security Area 2	Engineer (16000)
Operator (UG1)	Tag5 and Tag6	PC_4	Tag Security Area 6	Read only (0)

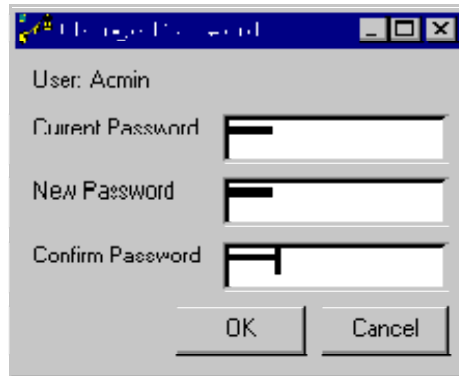
Change Password

This section assumes that a User is currently logged in. This field permits the current Users password to be changed. The current Users password can be changed by,

- 1 Selecting '**Password > Change Password**' from the [Menu bar](#).



- 2 When this option is selected, the current User Id is shown at the top of the blank prompt window. Select the Current Password field and enter the correct **Current Password**.
- 3 Select the **New Password** field and enter a new **Password**.
- 4 The new password must be confirmed by entering the identical, case-sensitive password in the **Confirm Password** field.



- 5 When all fields have been completed, accept the changes by clicking '**OK**'. To discard and return to the previous password select '**Cancel**'.

delete a Security item

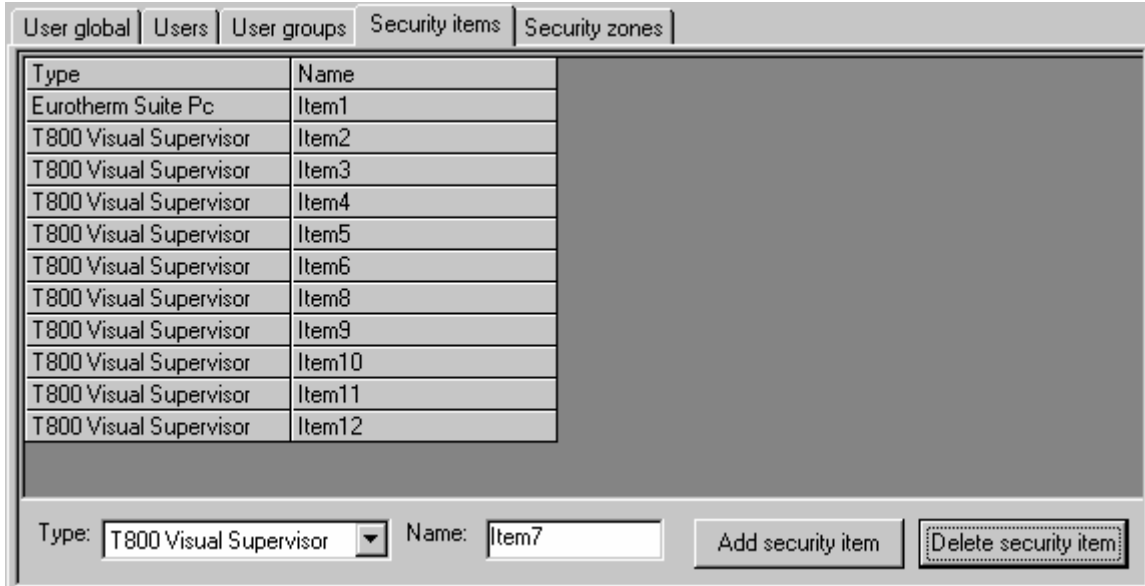
This function removes the object and all its configured parameters from the database.

Delete a Security item by,

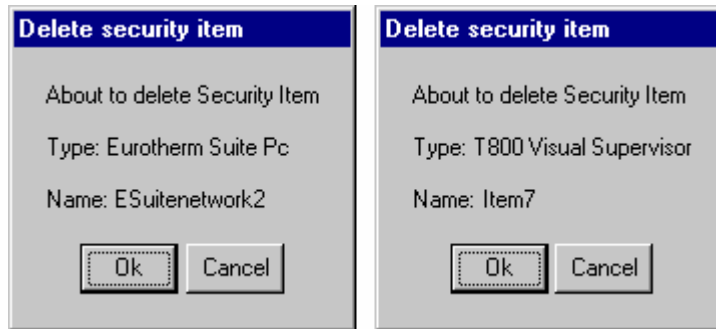
- 1 Selecting the item that is not required.

Note

The Security item type and name are displayed in the relevant fields.



- 2 Press the **Delete security item**.
- 3 A confirmation dialog window appears. Press '**Ok**' to delete the item or '**Cancel**' to reject the operation and return to the Security item element.



Note

If '**Ok**' was selected observe the item has been removed.

- 4 Finally [save changes](#).

Address

Displays the Security item address. This describes the location of the Security item security database by either Project path (Eurotherm Suite PC), Computer Name and Security database path (Review and QuickChart Software), IP address or Host Name (5000 and 6000 Series instrument) or 'Lin port name' and 'Lin db name' (T800 Visual Supervisor instrument).

Security items display field

Displays all configured Security items, including item specific data such as the Type (Computer, Software and instruments), Name (Security item name), Configuration Rev (last deployed master security database revision), Operational Rev (latest revision of the local security database) and the Status (Specific errors status).

recover a Security Database*Recover Security Manager/PC Security Database*

A Recovery User account is essential to recover an unusable security database. It relies on an Administrator enabling the Security Manager [Recovery User](#) account before the Security database becomes inaccessible.

Beware

If the Recovery User account is NOT configured at any time before the system becomes inaccessible, the Recovery User account will NOT be available.

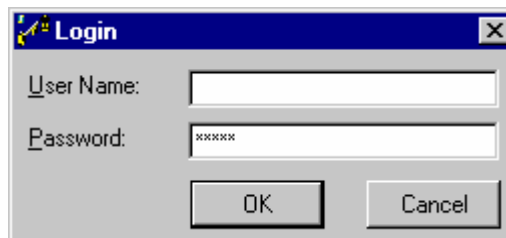
The database has an Recovery User account that allows a User to login to a database that does NOT have sufficient active Administrator accounts with full Access Rights. If the database has insufficient active Administrator accounts this could be due to,

- passwords expiring or being forgotten
- exceeding the Maximum Login attempt limits
- disabled Administrator accounts

Recover an unusable Security Manager/PC Security Database

If the **Recovery User account** has already been configured it will be possible to recover an unusable Security database. Use the following instructions in order to do so.

- 1 Contact supplier stating the problem. The supplier will issue a time restricted (1 day), date dependent password.
- 2 Open and login to the database before the 1-day limit expires. Do NOT use a User Id and enter the special issued password.



- 3 The database will open enabling the User to re-instate sufficient accounts reactivating the security project.

Recover T800 Visual Supervisor Security Database

A Recovery User Account is essential to recover an unusable database. It relies on an Administrator enabling the [T800 Recovery account](#) before the Security database becomes inaccessible.

Beware

If the Recovery User account is NOT configured at any time before the system becomes inaccessible, the Recovery User account will NOT be available.

If configured the T800 Visual Supervisor has a Recovery account that allows a User to login to a T800 Security database that does NOT have sufficient active Administrator accounts with full access rights. If this item has insufficient active Administrator accounts this could be due to,

- passwords expiring or being forgotten.
- exceeding the Maximum Login attempt limits.
- disabled Administrator accounts.

Recover an unusable T800 Security database

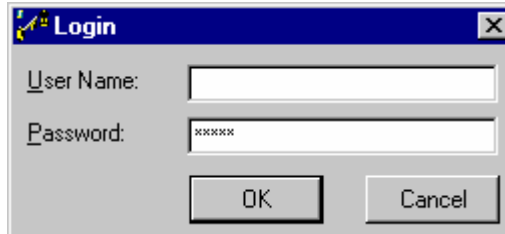
If the **Recovery account** has already been configured it will be possible to recover an unusable Security database. Use the following instructions in order to do so.

- 1 At the instrument, press the 'RECOVER' button (this temporarily replaces the 'USERS' button), to display a window containing a number. The number is derived from instrument specific data, date and time.

Note

Write down the number.

- 2 Contact supplier stating the problem and instrument specific number. The supplier will issue a time restricted (1 hour), date dependent password.
- 3 Open and login to the instrument before the 1 hour time limit expires. Do NOT use a User Id and enter the special issued password.



- 4 This will open the Security database, enabling the User to re-instate sufficient accounts, therefore reactivating the Security database.

Cancel PC Configuration



Operate this button to stop the computer configuration procedure and revert to the current Security Manager Window. A prompt appears if there is unsaved changes, select as appropriate.

Customise Security Manager

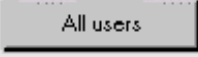
How to show Active or All Users

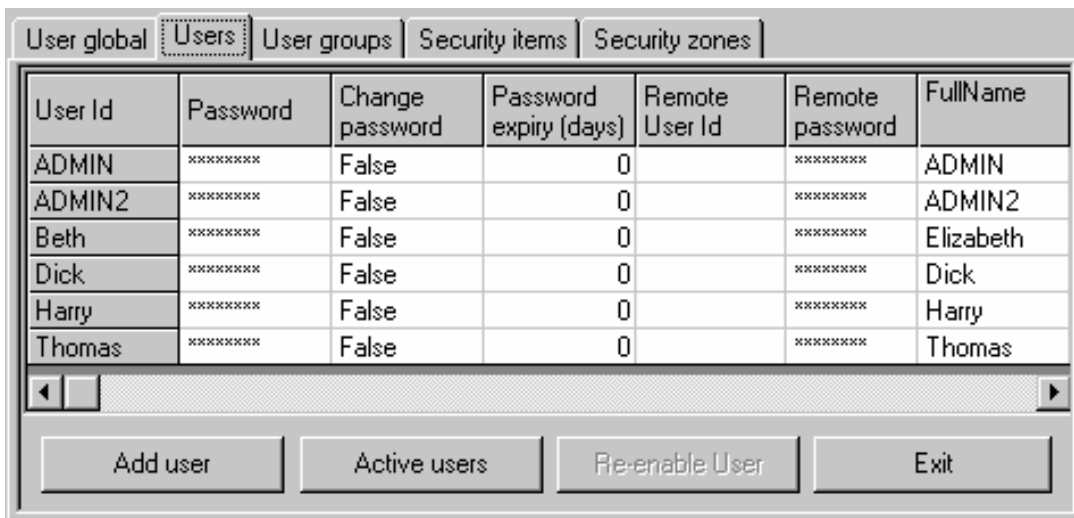
The function of this button allows the User to display [ALL Users](#) or just the [Active Users](#) in the User Id column.

Display Active or All users by

- 1 Clicking  and observe the list of User Id's as it is reduced to show just the **Active Users**. The button now reads .

Note

If the tab was already showing just the **Active Users**, pressing the  causes the list of User Id's to expand and show **ALL Users**, including disqualified Users.



- 2 Finally [save changes](#).

How to hide/show toolbar

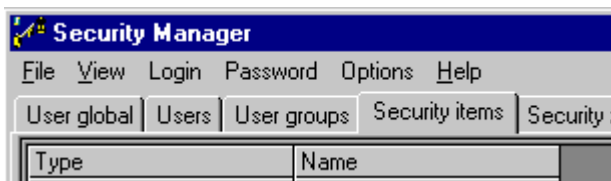
The Toolbar stores 2 icons that enable quick access to the Open and Save options. It is displayed by default and is located at the top of the Security Manager window. A check mark along side this option in the View pulldown indicates it is currently displayed.

Hide/show this bar by,

- 1 Select '**View > Toolbar**' from the Menu Bar.



- 2 The Toolbar is removed from the window.



- 3 To display the Toolbar, repeat the instructions.

How to hide/show status bar

The Status Bar displays Security Manager database status information, including location, current user, security status, date and time. It is displayed by default and is located along the foot of the Security Manager window. A check mark indicates it is currently displayed.

To hide/show this bar by,

- 1 Selecting '**View > Status Bar**' from the Menu Bar.



- 2 The Status Bar is removed from the window.



- 3 Repeat the instructions to display the Status Bar.

EurothermSuite Pc's security level names

This function shows the **Security level** names and the corresponding **Access level** values. The **Security level** name is used to define the level of security required by a User when attempting to edit a Tag. However, editing these fields is permitted.

Beware
 editing these fields will require further configuration of the Project Database, and may not benefit the security configuration.

To add a new EurothermSuite Pc security level,

- 1 Select '**Options > EurothermSuite Pc's security level names**' from the Menu Bar. A dialog window appears.

It is recommended that...
the existing access level values remain as shown. However, editing the Security level name, may clarify security levels for each unique system.

- 2 Double-click the next available **Security level name** field and enter the required text.
- 3 Double-click the corresponding **Access level** field and enter the required value.
- 4 Press 'Ok' to reveal the confirmation dialog. Press Yes to confirm the new EurothermSuite Pc Security parameters.

Note
 The EurothermSuite Pc Security parameters can be removed, simply by deleting the **Security level name** text and corresponding **Access level** value. Confirmation will be required.

Regulatory Defaults

Regulatory Defaults

Each Security Manager field has a defined range dependant on the selected Regulation. Any value that deviates from the Regulatory defaults will a breach of the defined Regulations, creating a system that now does NOT comply with those Regulations.

Security Manager Regulatory Defaults

This table lists the Regulatory defaults for SecMan security item.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 Records		21 CFR Part 11 Signatures	
	Default	Range	Default	Range	Default	Range
<i>User Global</i>						
Login Dialog Timeout (secs)	0	0 30 000	0	0 30 000	0	0 120
Max login attempts	0	0 30 000	3	3 99	3	3 99
Keep retired user ids	True	True / False	True (Locked)		True (Locked)	
Minimum user id length	3	3 8	6	3 8	6	3 8
Maximum user id length	8	3 8	8	3 8	8	3 8
Minimum password length	3	3 8	6	3 8	6	3 8
Maximum password length	8	3 8	8	3 8	8	3 8
Password Reuse Period (days)	0	0 30 000	365	365 30 000	365	365 30 000
<i>User</i>						
User Id	Read Only User Id		Read Only User Id		Read Only User Id	
Password	3	3 8	6	3 8	6	3 8
Change Password	False	True / False	False	True / False	False	True / False
Password Expiry	0	0 30 000	90	1 180	90	1 180
Remote User Id	blank	0 20	blank	0 20	blank	0 20
Remote Password	3	3 8	6	3 8	6	3 8
Fullname	blank	0 25	blank	0 25	blank	0 25
System	False	True / False	False	True / False	False	True / False
Retired	False	True / False	False	True / False	False	True / False
Enabled	True	True / False	True	True / False	True	True / False
Login Attempts	Incrementing Value (Locked)		Incrementing Value (Locked)		Incrementing Value (Locked)	
Locked Out	True / False (Locked)		True / False (Locked)		True / False (Locked)	
Reason	Description (Locked)		Description (Locked)		Description (Locked)	
<i>User Group</i>						
<i>There are no Regulatory requirements for this Section</i>						
<i>Security item</i>						
<i>There are no Regulatory requirements for this Section</i>						
<i>Security Zone</i>						
<i>There are no Regulatory requirements for this Section</i>						

5000 Series Instrument Regulatory Defaults

This table lists the Regulatory defaults for 5000 Series security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 - Records		21 CFR Part 11 - Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Record Logins	False	True / False	True (Locked)		True (Locked)	
Login Timeout	0	0 - 99	15	1 - 99	15	1 - 99
with unapplied changes	Ignore Timeout	Ignore Timeout / Discard Changes	Discard Changes	Ignore Timeout / Discard Changes	Discard Changes	Ignore Timeout / Discard Changes
Require Signing	False	True / False	False	True / False	True (Locked)	
Require Authorisation	False	True / False	False	True / False	False	True / False
Enable Audit Trail	False	True / False	True (Locked)		True (Locked)	
Disable Service Account	False	True / False	False	True / False	False	True / False
Login by User Id	True	True / False	True	True / False	True	True / False
Password Change on Expiry	True	True / False	True	True / False	True	True / False
<i>Access Rights</i>						
Connect from remote	False	True / False	False	True / False	False	True / False
Edit own password	True	True / False	True	True / False	True	True / False
Change alarm setpoints	False	True / False	False	True / False	False	True / False
Acknowledge alarms	True	True / False	False	True / False	False	True / False
Edit Maths Constants	False	True / False	False	True / False	False	True / False
Reset Maths	False	True / False	False	True / False	False	True / False
Preset Totalisers	False	True / False	False	True / False	False	True / False
Start/Reset Timers	False	True / False	False	True / False	False	True / False
Set Clock	False	True / False	False	True / False	False	True / False
Adjust Inputs	False	True / False	False	True / False	False	True / False
Archiving Control	False	True / False	False	True / False	False	True / False
Save/Restore	False	True / False	False	True / False	False	True / False
Paste/Delete	False	True / False	False	True / False	False	True / False
Full Configuration	False	True / False	False	True / False	False	True / False
Full Security	False	True / False	False	True / False	False	True / False
Batch Control	False	True / False	False	True / False	False	True / False
Can Sign	False	True / False	False	True / False	False	True / False
Can Authorise	False	True / False	False	True / False	False	True / False
Event Permission (x 5)	False	True / False	False	True / False	False	True / False
Edit Output Channel Default	False	True / False	False	True / False	False	True / False
Action Demand Writes	False	True / False	False	True / False	False	True / False

6000 Series Instrument Regulatory Defaults

This table lists the Regulatory defaults for 6000 Series security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 Records		21 CFR Part 11 Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Record Logins	False	True / False	True (Locked)		True (Locked)	
Login Timeout	0	0 99	15	1 99	15	1 99
with unapplied changes	Ignore Timeout	Ignore Timeout / Discard Changes	Discard Changes	Ignore Timeout / Discard Changes	Discard Changes	Ignore Timeout / Discard Changes
Require Signing	False	True / False	False	True / False	True (Locked)	
Require Authorisation	False	True / False	False	True / False	False	True / False
Enable Audit Trail	False	True / False	True (Locked)		True (Locked)	
Disable Service Account	False	True / False	False	True / False	False	True / False
Login by User Id	True	True / False	True	True / False	True	True / False
Password Change on Expiry	True	True / False	True	True / False	True	True / False
<i>Access Rights</i>						
Connect from remote	False	True / False	False	True / False	False	True / False
Edit own password	True	True / False	True	True / False	True	True / False
Change alarm setpoints	False	True / False	False	True / False	False	True / False
Acknowledge alarms	True	True / False	False	True / False	False	True / False
Edit Maths Constants	False	True / False	False	True / False	False	True / False
Reset Maths	False	True / False	False	True / False	False	True / False
Preset Totalisers	False	True / False	False	True / False	False	True / False
Start/Reset Timers	False	True / False	False	True / False	False	True / False
Set Clock	False	True / False	False	True / False	False	True / False
Adjust Inputs	False	True / False	False	True / False	False	True / False
Archiving Control	False	True / False	False	True / False	False	True / False
Save/Restore	False	True / False	False	True / False	False	True / False
Paste/Delete	False	True / False	False	True / False	False	True / False
Full Configuration	False	True / False	False	True / False	False	True / False
Full Security	False	True / False	False	True / False	False	True / False
Batch Control	False	True / False	False	True / False	False	True / False
Can Sign	False	True / False	False	True / False	False	True / False
Can Authorise	False	True / False	False	True / False	False	True / False
Event Permission (x 5)	False	True / False	False	True / False	False	True / False
Edit Output Channel Default	False	True / False	False	True / False	False	True / False
Action Demand Writes	False	True / False	False	True / False	False	True / False
Perform Update	False	True / False	False	True / False	False	True / False

EurothermSuite PC Regulatory Defaults

This table lists the Regulatory defaults for EurothermSuite PC security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 Records		21 CFR Part 11 Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Audit Trail	True	True / False	True (Locked)		True (Locked)	
Signing	True	True / False	True	True / False	True (Locked)	
Authorisation	True	True / False	True	True / False	True	True / False
Alarm Signing	0	0 15	0	0 15	0	0 15
Alarm Authorisation	0	0 15	0	0 15	0	0 15
Confirmation	False	True / False	False	True / False	False	True / False
Notes	False	True / False	False	True / False	False	True / False
Auto Logon User Id	Blank (User Id needed)		Blank (User Id needed)		Blank (User Id needed)	
Log Invalid Times	False	True / False	False	True / False	False	True / False
Audit Ports (x4)	Blank (Port name needed)		Blank (Port name needed)		Blank (Port name needed)	
Lockout Level		None		None		None
<i>Access Rights</i>						
Sign	False	True / False	False	True / False	False	True / False
Authorise	False	True / False	False	True / False	False	True / False
Print	False	True / False	False	True / False	False	True / False
TagEdit	False	True / False	False	True / False	False	True / False
Operator Point Display	False	True / False	False	True / False	False	True / False
Export Historical Trend	False	True / False	False	True / False	False	True / False
Inactivity Timeout (secs)	0	0 30 000	15	1 720	15	1 720
Display access level	0	0 9999	0	0 9999	0	0 9999
Synchronise Files	Each of the access rights in this part require the selection of a level of confirmation the default is No Confirmation					
Override Server Redundancy						
Task Switch						
Operator group global	<u>Level of Confirmation</u>		<u>Level of Confirmation</u>		<u>Level of Confirmation</u>	
	No Confirmation Confirm Only Note Signature Sign & Note Sign & Authorise Sign & Authorise & Note Action Disabled		No Confirmation Confirm Only Note Signature Sign & Note Sign & Authorise Sign & Authorise & Note Action Disabled		No Confirmation Confirm Only Note Signature Sign & Note Sign & Authorise Sign & Authorise & Note Action Disabled	
Debug						
Operator groups						
Trend global						

	Default		21 CFR Part 11 Records		21 CFR Part 11 Signature	
	Default	Range	Default	Range	Default	Range
AlarmHistMaxItems						
Trends						
Recipe Download						
Global Alarm Acknowledge						
Faceplate Modify						
Change Language						
Offline data writes						
IO data writes						
System User writes						
Recipes		Needs appropriate configuration		Needs appropriate configuration		Needs appropriate configuration
Tag Security Area						

QuickChart Software Regulatory Defaults

This table lists the Regulatory defaults for QuickChart software security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 - Records		21 CFR Part 11 - Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Sign for Annotation	False	True / False	False	True / False	True (Locked)	
<i>Access Rights</i>						
Create QuickChart	False	True / False	False	True / False	False	True / False
Open QuickChart	True	True / False	True	True / False	True	True / False
Modify Chart View	True	True / False	True	True / False	True	True / False
Save QuickChart	False	True / False	False	True / False	False	True / False
Chart Setup	False	True / False	False	True / False	False	True / False
Administration	False	True / False	False	True / False	False	True / False
Chart Annotate	False	True / False	False	True / False	False	True / False
Chart Review	False	True / False	False	True / False	False	True / False
Chart Approve	False	True / False	False	True / False	False	True / False
Chart Release	False	True / False	False	True / False	False	True / False
Print	True	True / False	True	True / False	True	True / False
Print Setup	True	True / False	True	True / False	True	True / False
Export Data	True	True / False	True	True / False	True	True / False
Export Setup	True	True / False	True	True / False	True	True / False
Inactivity Timeout (secs)	0	0 - 30 000	15	1 - 720	15	1 - 720

Review Software Regulatory Defaults

This table lists the Regulatory defaults for Review software security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 - Records		21 CFR Part 11 - Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Sign for Annotation	False	True / False	False	True / False	True (Locked)	
<i>Access Rights</i>						
Transfer Files	False	True / False	False	True / False	False	True / False
Chart Setup	False	True / False	False	True / False	False	True / False
Chart Open/Close	True	True / False	True	True / False	True	True / False
Modify Chart View	True	True / False	True	True / False	True	True / False
Save Chart	False	True / False	False	True / False	False	True / False
Administration	False	True / False	False	True / False	False	True / False
File Services	False	True / False	False	True / False	False	True / False
Chart Annotate	False	True / False	False	True / False	False	True / False
Chart Review	False	True / False	False	True / False	False	True / False
Chart Approve	False	True / False	False	True / False	False	True / False
Chart Release	False	True / False	False	True / False	False	True / False
Print	True	True / False	True	True / False	True	True / False
Print Setup	True	True / False	True	True / False	True	True / False
Export Data	True	True / False	True	True / False	True	True / False
Export Setup	True	True / False	True	True / False	True	True / False
Inactivity Timeout (secs)	0	0 - 30 000	15	1 - 720	15	1 - 720

T800 Visual Supervisor Regulatory Defaults

This table lists the Regulatory defaults for T800 security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 - Records		21 CFR Part 11 - Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Recovery User	True	True / False	True	True / False	True	True / False
Password Expiry	0	0 - 180	90	1 - 180	90	1 - 180
Inactivity Timeout (secs)	0	1 - 720	15	1 - 720	15	1 - 720
<i>Access Rights</i>						
Sign	False	True / False	False	True / False	False	True / False
Authorise	False	True / False	False	True / False	False	True / False
View Only	False	True / False	False	True / False	False	True / False
Reference Number	0	0 - 65535	0	0 - 65535	0	0 - 65535
Access Level	Operator	Op. - Admin	Operator	Op. - Admin	Operator	Op. - Admin

Windows Domain Regulatory Defaults

This table lists the Regulatory defaults for Windows Domain security items.

IMPORTANT NOTE
Grey fields indicate a Read Only parameter.

	Default		21 CFR Part 11 - Records		21 CFR Part 11 - Signature	
	Default	Range	Default	Range	Default	Range
<i>Management Data</i>						
Administrator UserId	Needs appropriate configuration		Needs appropriate configuration		Needs appropriate configuration	
Administrator Password	0	0 - 180	90	1 - 180	90	1 - 180
Password Expiry	0	1 - 720	15	1 - 720	15	1 - 720
Deploy Existing Users	True	True / False	True	True / False	True	True / False
Deploy Retired Users	True	True / False	True	True / False	True	True / False
<i>Access Rights</i>						
Groups	True	True / False	True	True / False	True	True / False
	Needs appropriate configuration					

Other Information

What is a Master Database?

The master database is defined by the [Master UNC \(Universal Naming Convention\) path](#) configured using 'Options > Master UNC path' pulldown. Generally the master database is resident on a shared computer, where the Project was initially created.

Example

`\\< shared Security item Computer name >\< directory >\< project folder >`

Note

The computer name can be found by selecting
Start > Settings > Control Panel > Network > Identification

To give the computer, or to be more accurate the hard drive (C:), 'shared' access

- 1 Select the computer hard drive icon, right click and select '**Properties > Sharing tab**'.
- 2 Click the '**Shared as**' radio button and type '**C\$**' into the '**Shared name**' field.
- 3 Press '**OK**' to accept or '**Cancel**' to exit the operation.

What is a Client Database?

This is a deployed copy of the master database. Generally it is resident on Security item nodes in the security configuration.

Replication of a **client** database is NOT permitted and if attempted the User is requested to switch to the master security database before continuing.

What is the PC Name/Code?

The computer Name is the computer identification name.

The computer Code is a hexadecimal address value of the computer.

These parameters are displayed when selecting a database ('Enable PC locking' MUST be enabled).

LIN Information

Default LIN User Names

Unless the item being written to was added using the '.w' qualifier, LINOPC will use the OPC group name as the User name.

If it is not already known, it is possible to determine the OPC group names that have been created in LINOPC by running the LINOPC Groups application.

Some clients may not specify a group name in which case LINOPC automatically creates group names of the form AutoGroup<nn>.

If these applications are also using 'Fully qualified addresses' it will be necessary to add these group names into the 'defaccss.CSV' file. For the clients that have group names automatically created the user name AutoGroup will need to be added, and will apply to all these clients.

After installation 'defaccss.CSV' will normally be configured with the lines

```
LinToolsOpc.<Logged in NT user>.<PC node name> , RW  
TheGroup, RW
```

This defines the access for the clients LINTools and OPCScope.

Default LIN Access

If the client is addressing the LIN Blocks using Fully qualified addresses then LINOPC will not have a Tag Security Area for the block, and consequently will be unable to determine if the User has sufficient Access Level when writing to the blocks. LIN Tools and OPC Scope are examples of such clients.

In this instance LINOPC uses the default LIN access defined in the 'defaccss.CSV' file. Each line of this file has the following format.

```
<User name>, <RO | RW>
```

Where

RO = Read only

RW = Read write

LINOPC looks for this file first in the active Project folder, and then in the folder containing the Linopc.exe file.

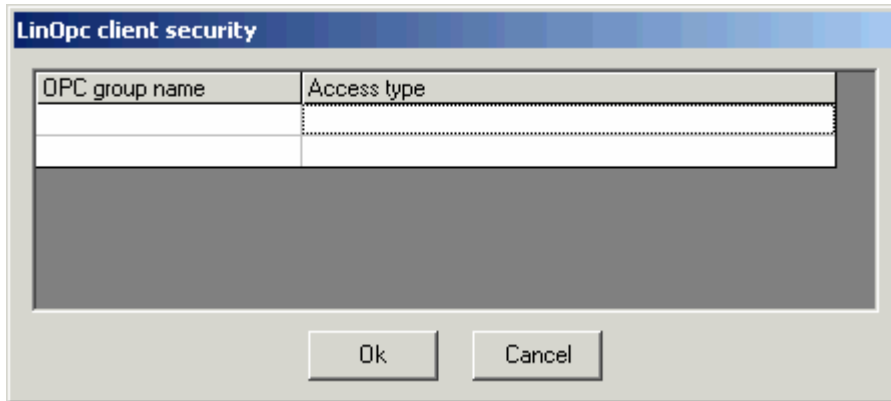
If LINOPC has to use the security defined in this file then a user will be granted either 'RO' or 'RW' access, irrespective of the block being written.

LINOPC Client Security

This function shows existing **OPC Group** names and the corresponding **Access Type**. Additional groups can be added, simply by entering the required group name text and selecting the appropriate **OPC Access type**. The **OPC Group** name is used to define the security for groups of Third-Party clients.

To add OPC Group security,

- 1 Select '**Options > LINOPC Client Security**' from the Menu Bar. A dialog window appears.



- 2 Double-click the next available **LINOPC Group name** field and enter the required text.
- 3 Double-click the corresponding **Access level** field and select the required Access type.
 - NONE (No access)
 - RO (Read only access)
 - RW (Read write access – everything logged)
 - RWE (Read write access – only errors logged)
 - RWN (Read write access – nothing logged)
- 4 Press 'Ok' to reveal the confirmation dialog. Press Yes to confirm the new LINOPC Security parameters.

Note

The LINOPC Security parameters can be removed, simply by deleting the **LINOPC Group name** text and the corresponding **Access type** value. Confirmation will be required.

LINOPC Security specifics

Online LIN data is accessed through the LINOPC server. This program provides an OPC interface to the LIN Blocks. Through this interface LIN items are always referred to by their Fully Qualified Address (FQA) (see [Default LIN Access](#)):-

<Port name>”NN:<Lin DB name>.<Block name>[.<Field name> | .<Sub field name> | .<Qualifier>]

where,

NN = LIN node address in hex.

Or if a Project database is available, items may be referred to using their Tags,

<Tag name>[.<Field name>][.<Sub field name>][.<Qualifier>]

By default, LINOPC takes the OPC group name to which the item was added as the User name. However if the item has the '.w' qualifier, the [LIN User Name](#) is extracted from the string that is written to the item.

For example, if a client wishes to write the value '55.6' to the 'PV' field of the 'Tag' 'PID01', the client adds the item

[PID01.PV]

and writes '55.6' to it. In this instance LINOPC uses the OPC group name the item was added to as the User.

Alternatively if the client wished to specify User 'Jack' on computer, i.e. 'OpStn1', signed for the change, the item could be added with the '.w' qualifier.

[PID01.PV.w]

A '.w' string value which has the following syntax would then be expected.

[<PC Node>],[<User data>],[<Access level>],[<Qualifier>],[<Value type>]:<Value>[0]

Where

<User data> [Logged on user] / [Signing user] / [Authorising user]

Currently only the [Logged on user] or the [Signing user] is used. The Access Level is checked against the [Signing 'User'] if present.

<Access level> If this value is specified it overrides the Users Access Level to the Tag defined in the security database.

<Qualifier> not used

<Value type> <s | d | f | x | o>

<s> = string

<d> = integer

<f> = floating point

<x> = hex

o> = octal

In this example it would be: -

OpStn1, /Jack/, , ,f,55.6

Tag and LINBlock specifics

If the system includes Tags and LINBlocks it is important to have an understanding of the following features and how they relate to the elements of the Security Manager.

- [Tag Security Areas](#)

User groups are given Access Levels to Tag Security Areas. This determines the privileges required in order to write to the Tags in the Tag Security Areas in the selected Security zone. The Access Levels are defined as part of the Access Rights given to a User group.

Note

In systems that precede the Security Manager, these were known as Security Areas. When upgrading systems it is IMPORTANT not to confuse Tag Security Areas with Security zones.

- [Tag Profile Configurator](#)

The fields in a LIN block referenced by a Tag have a number of properties, including flags to indicate Electronic Signatures are required. By default these properties are contained in the template that describes the block. However, the Tag Profile Configurator can redefine these properties so that they are unique for each Tag.

- [LINOPC Security](#)

LINOPC applies its own security check to confirm that a client has the Access Level necessary to write to an online LINBlock. This is based on user names and Tag Security Areas. However some client processes do not refer to LINBlocks by their Tags, and do not explicitly specify user names, LINTools and OPCScope are two examples. The installation sets up the necessary information for known clients, however where a new OPC client is being integrated it is necessary to understand how LINOPC deals with security.

- [TagEdit and ESDataSrv user account](#)

When TagEdit is activated from one of the Project Developer tools, the User is not required to login. In this mode TagEdit uses ESDataSrv the default system User Id. ESDataSrv is one of the default accounts supplied with the Security database and must be given access to the Tag Security Areas to ensure TagEdit has the privilege to perform writes when security is enabled.

Tag Profile Configurator specifics

Each field associated with a Tag has actions relating to security which must be completed before any changes can take effect.

By default these values are defined on a block type basis, however this configurator allows new pseudo LIN Block types to be created. The new types have the same LIN Template, i.e. fields as the original type, but security and other attributes stored in the Project Database can be changed from the default values. The new type is identified using the block type name, e.g. 'PID' plus a PointDisp name other than default, e.g. Boiler. Once the new type has been created in the Tag Profile Configurator the PointDisp field can be changed in TagEdit. Opening Tag Profiles in the Project folder runs this configurator which can also be used to configure various other field properties.

Tag Security Areas specifics

Each field in a block referenced by a Tag has an Access Level (a numeric value between 0 and 32767). A User wishing to write to that field would require an Access Level of at least this value.

Each Tag can be assigned to a single Tag Security Area only. When Users login to a security item they are given an Access Level over each of the Tag Security Areas, that determines which fields in each Tag can be written to.

create a Tag Security Area (Project Organiser)

Project Organiser must be used to create Tag Security Areas and configure the relevant Tags.

Refer to...
Project Organiser help file for full instructions.

Project Organiser is used to create Tag Security Areas and configure the relevant Tags. **Security Manager** is then used to assign User Access Rights to **Tag Security Areas**, allowing assigned Users to write to the Tags of that Tag Security Area. There are 2 default **Tag Security Areas**.

- \$SystemTag
 provides access to the LIN Write Failure flag. This is generated and viewed in **InTouch** when a write to a LIN server fails due to an invalid reference or insufficient security. This Tag Security Area includes all system Tags, for example, all Tags used to clear down the LIN write error counts. These Tags all require an Access Level of 10000.
- UNALLOCATED (NULL)
 allows **engineer** security access to Tags NOT assigned to a **Tag Security Area**. **Security Manager** is used to assign the **Unallocated (NULL) Tag Security Area** to those User Groups. This Tag Security Area includes all Tags that have not been assigned to a Tag Security Area.

Note
Tags can only be assigned to a single Tag Security Area.

This is configured by,

In the **Project Organiser**

- 1 Open the Project folder, and then Tag Security Areas.

Note
 If creating the first Tag Security Area the Editor Contents Region is empty.

- 2 Create the **Tag Security Area** to break the Project down into sufficient identifiable groups,
 - Right click to show the floating menu and select **New > Tag Security Area**.
 The command displays the *New Tag Security Area* dialog. In the *Tag Security Area Name* field, enter a short (12 characters maximum) easily identifiable name for the *Tag Security Area* containing any of the following characters a z, A Z, 0 9, &, _, -.

Tip!
For clarity, try to use an easily identifiable name for an object, i.e. Boiler3 (Tag Security Area).

- 3 Select **OK** to accept the *Tag Security Area* name. Press **Cancel**, **X**, or **Esc**. on the keyboard to abort the operation.
- 4 Refresh the display, (**View > Refresh** (F5)) when complete.

In the **Security Manager**,

- 5 Configure the permission for the relevant Tag Security Area by selecting the appropriate level of security from the enumerated picklist of Access Levels.
 The Access Level a User has in each Tag Security Area is configured by the Security Manager. An Access Level determines a minimum level of security permitted before the Tags it contains can be edited by a User assigned to a User group on a computer.
 The User group Tag Security Area Access Level is configured in a table, which allows the Access Levels to be defined.
 - Clicking in the left-hand column offers a picklist showing the configured Tag Security Areas.
 - Clicking in the right hand column offers an enumerated picklist of Access Levels.

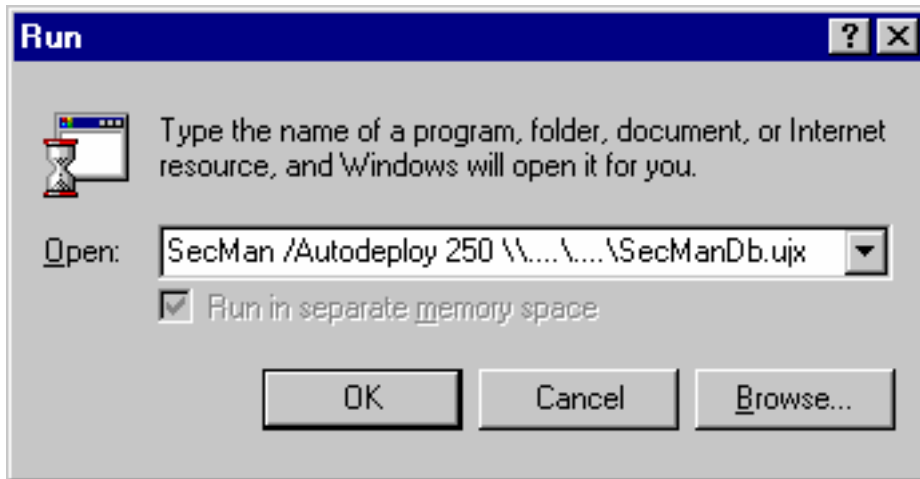
Command Line Parameters

Path to SecManDb.ujx Command line parameter

This Command line parameter should only be used to define the location of the Security database when operating the Security Manager through the Command line prompt.

This can be configured in a string with other Command line parameters.

Command line prompt example

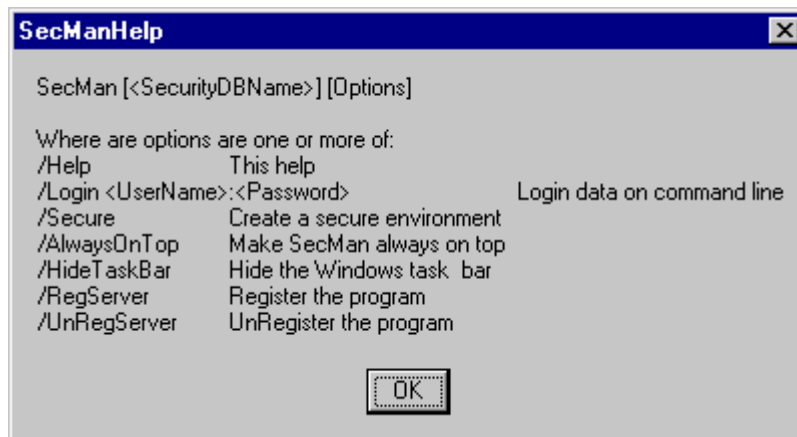


This Command line parameter will run the Security Manager Utility and load the defined SecManDb.ujx database.

Command Line parameters

Security Manager can also be operated and MUST be started at the Deployment Computer using Command Line parameters.

The following image indicates the parameters that can be configured using the command line prompt. All parameters are single space separated.



IMPORTANT NOTE

This graphic is displayed using the /Help Command line parameter, it shows the parameters with the exception of the /AutoDeploy Command line.

/RegServer Command line parameter

This Command line parameter should rarely be used, as the correct information should have already been configured when Security Manager was installed.

Command line prompt example

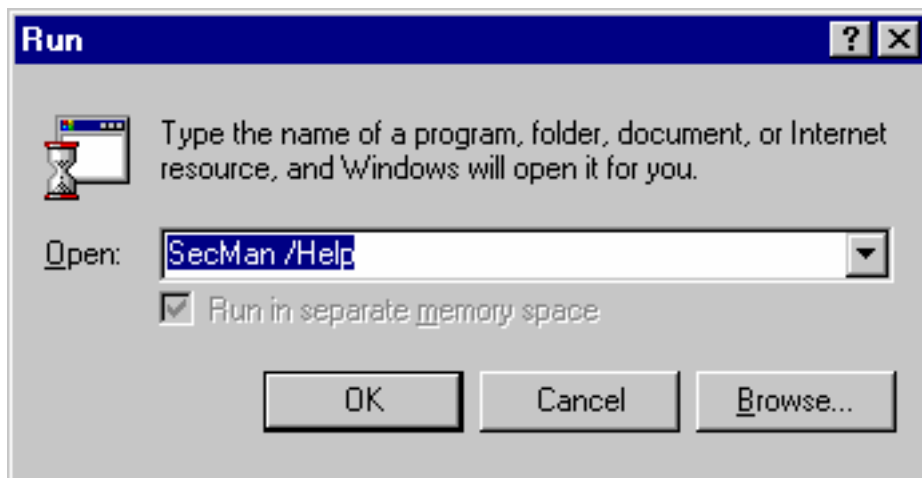


This Command line parameter will enter Security Manager registry data to allow the user to double click the SecManDb.ujx to open the database.

/Help Command line parameter

This Command line parameter will display the following list of available Command line parameters.

Command line prompt example



Note

This graphic is displayed using the /Help Command line parameter, it lists each additional parameter. An /AutoDeploy Command line parameter has also been included.

/Login Command line parameter

This can be configured in a string with other Command line parameters.

Command line prompt example



This Command line parameter will automatically enter defined User Id and Password in the Login prompt.

/Secure Command line parameter

This can be configured in a string with other Command line parameters.

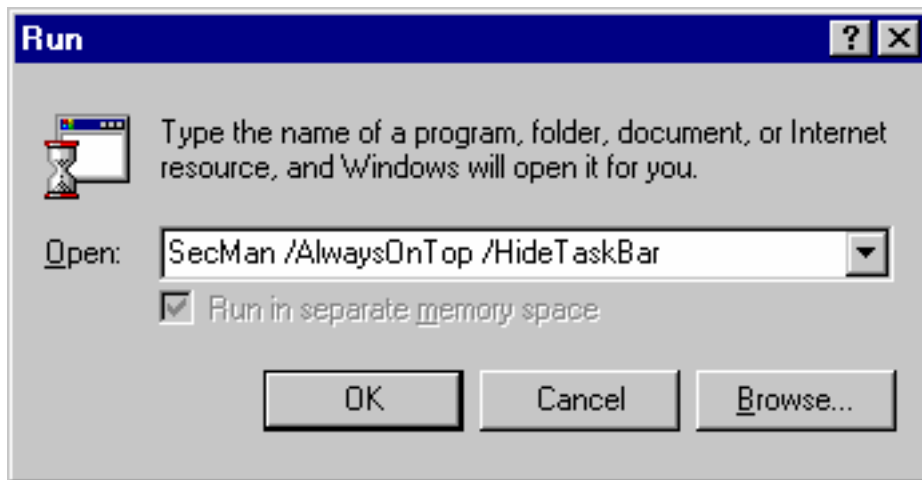
Command line prompt example



This Command line parameter will stop any means of saving data by disabling the **File > Open** and **File > Close** options, the **Help** option, including the **About** dialog.

/HideTaskBar Command line parameter

This Command line parameter can be configured in a string with other Command line parameters.

Command line prompt example

This Command line parameter will ensure that when Security Manager is the Windows Task Bar, and any operations associated with it are NOT displayed on screen.

/Autodeploy Command line parameter

The Autodeploy function can be started from a Deployment computer either by the Command line prompt or via a shortcut to the Master Security database.

It is recommended that...

*the shortcut method is used, as this will cancel the need to enter the **/Autodeploy Command line parameter** each time in order to start Security Manager.*

For this facility to operate successfully, the Deployment computer MUST be,

- specified in the Security zone
- listed in the PC Configuration table (**Options** pulldown)
- and the Deployable flag MUST be checked (**Options** pulldown)

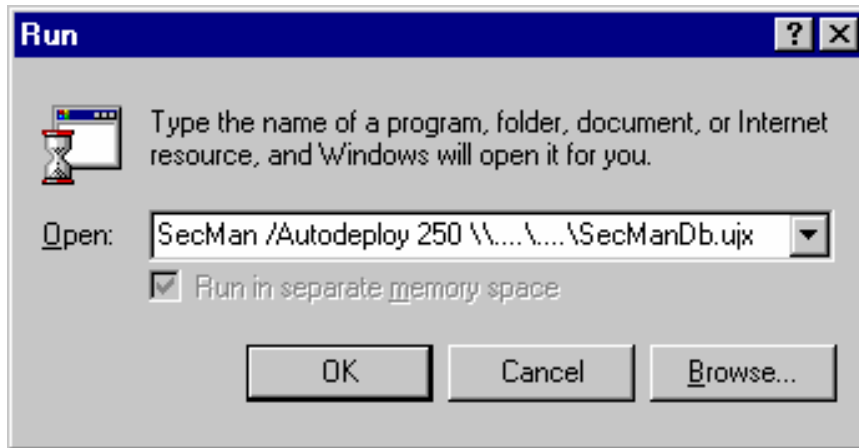
It can be configured in a string with other Command line parameters.

This Command line parameter will,

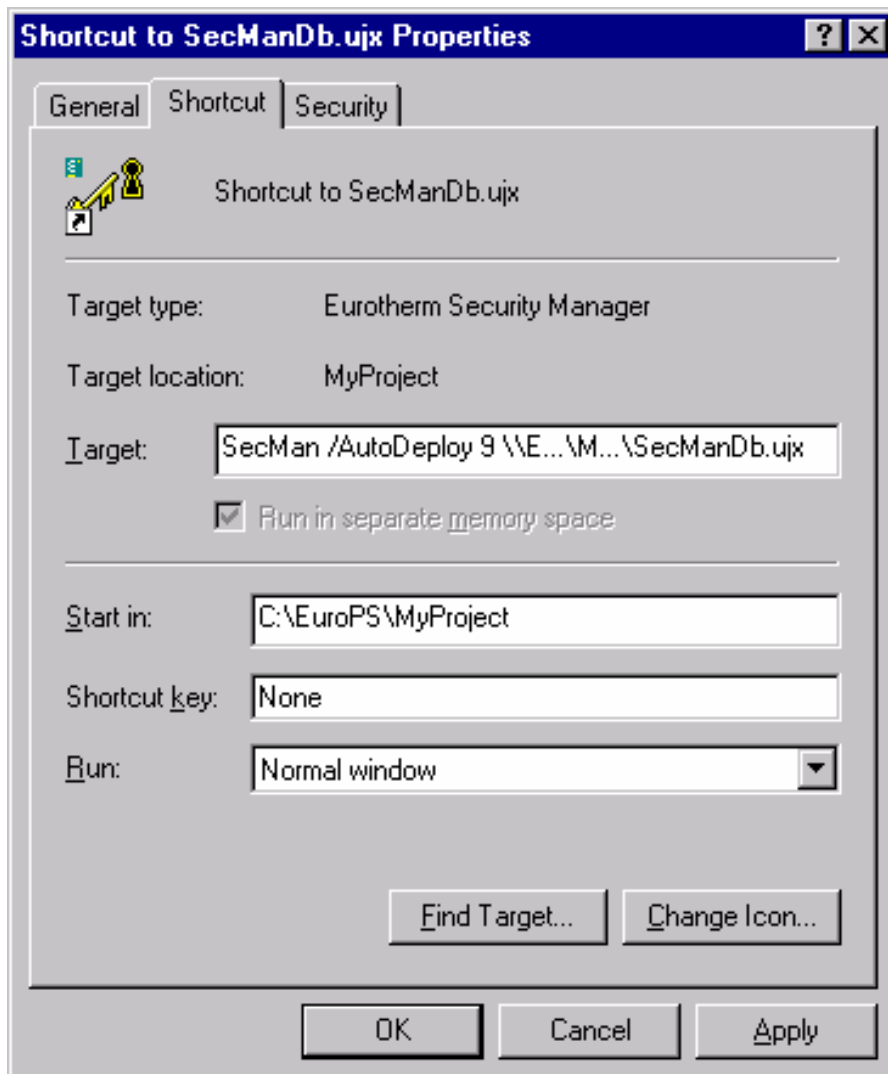
- display the deployment dialog with full use of the Deploy and the 'Deploy All/Zone' buttons
- compare the Master Security database revision to that of the Security items in the Security zone, and reconcile and deploy where necessary

It is recommended that...

a sufficient time, specified in the command line, is allowed for the Autodeploy comparison to complete. Any value greater than 60 secs can be applied, but a default 300 secs is assumed if a value is not offered. The value must be changed according to the complexity of the system, with a minimum of 5 mins in a system comprised of 5000 Series instruments.

Command line prompt examples

"SecMan" /AutoDeploy 60 "\\EuroPS\MyProject\SecManDb.ujx"

Shortcut example**IMPORTANT NOTE**

The /Autodeploy Command line parameter,
"SecMan" /AutoDeploy 60 "\\EuroPS\MyProject\SecManDb.ujx"
 MUST be entered in the *Target* field of the *shortcut properties dialog box*.

/UnRegServer Command line parameter

This Command line parameter should rarely be used, as the correct information should have already been configured when Security Manager was installed.

Command line prompt example



This Command line parameter will remove Security Manager registry data that will stop the user from opening the database.

Audit Trail Information

Security Manager Audit Trail

This enables event and alarm trace-ability in the form of tamper-proof data storage files. A new file is created each time the database is opened. It is assigned a filename derived from the Database name (SecMan), computer name, Year/Month/Day, an issue number, and a .uhh extension.



SecMan_PrimaryServer_20030915_000002.UHH

The Audit Trail is saved to the History directory in the Project folder.

Each time an event or alarm occurs at an item configured in the database, an entry containing additional data is added to the Security Manager Audit Trail. There are 4 event types each recording different information,

- Non operator
These are system or universal events that record Date, Time, and Action, Previous and New values (if appropriate).
- Permitted
These are events caused by User accessing nodes on the system. The Date, Time, Action, User Id and/or User name, Previous and New values (if appropriate) are recorded.
- Signed
These are events that require the User to enter a password to accept the changes. An optional Reason note accompanies these events.
- Signed and authorised
These events require 2 different User signatures. The first to sign (accept) a change and the second to authorise (confirm) the change. The authorisation signature is accompanied by the Users Fullname description.

The Security Manager Audit Trail can be viewed and printed using the Review software.

Audit Trail events

An event is defined as the following:

- Login/Logout.
- Exceeded Login attempts.
- Any saved configuration changes to the database.
- Synchronise/Deploy the master database.
- Security configuration audit.
- Starting other applications.
- Event alert failure.

Audit Trail event details

Each event is accompanied by the following data,

- Time stamp.
- Current User Id and Fullname.
- Signing User Id and Fullname (if required).
- An authorised User Id and Fullname (if required).
- A description of the changes as part of an electronic signature (if required).

Examples

Example 1 - Each User in their own User group solution

Consider a system that comprises 2 Security item nodes (2 T800 Visual Supervisor's - T800_01, and T800_02) and 4 Users (U1, U2, U3, and U4) each having access to both Security items.

This example has a unique User group for each User (UG1, UG2, UG3, and UG4) and a unique Security zone configuration (Z1 and Z2) for each Security item.

This solution gives the maximum flexibility but as shown in the table below there are 10 (ten) different sets of security data that need to be edited, 2 sets of Management Data plus 8 sets of Access Rights. This may become complicated when attempting to edit the system configuration.

Security zone	Security item	Security data
Z1	T800_01	Zone 1 Management Data configuration UG1 Access Rights UG2 Access Rights UG3 Access Rights UG4 Access Rights
Z2	T800_02	Zone 2 Management Data configuration UG1 Access Rights UG2 Access Rights UG3 Access Rights UG4 Access Rights

Example 2 - All Users in a single User group solution

If after deciding that the Security items in the system have identical Management Data and all Users need the same Access Rights, this solution is applicable. All Users in a single User group.

This example has 1 set of User group Access Rights allocated to 1 set of Security zone Management Data, as shown below.

Note

Users familiar with the 'Security Configurator' can use the rules that apply to that utility when a single Security zone is being configured.

This solution gives the minimum flexibility but as shown in the table below there is the minimum amount of security data that needs to be edited, which makes it easier to manage.

Security zone	Security item	Security data
Z1	T800_01 & T800_02	Zone 1 Management Data configuration UG1 Access Rights

Example 3 - Simple Management Data and Access Rights solution

Typically the required solution is likely to be somewhere between example 1 and 2, where a number of Users need identical Management Data but different Access Rights configurations.

Most systems have different types of Users, Operators (UG1) and Engineers (UG2). This solution results in the configuration shown below.

Note
Users familiar with the 'Security Configurator' can use the rules that apply to that utility when a single Security zone is being configured.

Security zone	Security item	Security data
Z1	T800_01 & T800_02	Zone 1 Management Data configuration UG1 with Operator Access Rights UG2 with Engineer Access Rights

Example 4 - Complex Management Data and Access Rights solution

Now consider a system that comprises 8 Security items (6 computer's - PC_1, PC_2, PC_3, PC_4, PC_5, and PC_6, and 2 T800 Visual Supervisor's - T800_01, and T800_02) and 8 Users - 2 supervisors, 2 engineers and 4 operators.

The Security items divide into 4 Security Zones on the basis that they need different Management Data. An initial theory of User groups would be 1 User group per role (Access Rights), per Security zone. This solution results in twelve (12) User groups in total, shown below.

Security zone	Security item	Security data
Z1	PC_1 & PC_2	Zone 1 Management Data configuration UG1 with Operator Access Rights UG2 with Engineer Access Rights UG3 with Supervisor Access Rights
Z2	PC_3 & PC_4	Zone 2 Management Data configuration UG4 with Operator Access Rights UG5 with Engineer Access Rights UG6 with Supervisor Access Rights
Z3	PC_5 & T800_01	Zone 3 Management Data configuration UG7 with Operator Access Rights UG8 with Engineer Access Rights UG9 Supervisor Access Rights
Z4	PC_6 & T800_02	Zone 4 Management Data configuration UG10 with Operator Access Rights UG11 with Engineer Access Rights UG12 with Supervisor Access Rights

Example: Modified Complex single Access Rights solution

- This is a variation of this configuration.

Example 4a - Modified Complex Management Data and Access Rights solution

Now consider the same system as the [Complex Management Data and Access Rights solution](#) with the following changes.

If

- Both Supervisors have the same Access Rights across all the Security zones (UG6, UG9 and UG12 are redundant).
- Engineer 1 is responsible for Security zone 1 and Engineer 2 is responsible for Security zones 2, 3 and 4 (UG8 and UG11 are redundant).
- Operators 1 and 2 are responsible for Security zones 1 and 2 and Operators 3 and 4 are responsible for Security zones 3 and 4 (UG4 and UG10 are redundant).

Now only 5 User groups are required and not twelve (12). The fact that UG3, UG5 and UG7 are allocated to both Z3 and Z4 still is correct. This means the Management Data between Z3 and Z4 are different (e.g. Z3 has a need for Electronic Signatures and Z4 does not). This was the original reason for putting Security items into different zones, see below.

Security zone	Security item	Security data
Z1	PC_1 & PC_2	Zone 1 Management Data configuration UG1 with Operator Access Rights UG2 with Engineer Access Rights UG3 with Supervisor Access Rights
Z2	PC_3 & PC_4	Zone 2 Management Data configuration UG1 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Rights
Z3	PC_5 & T800_01	Zone 3 Management Data configuration UG7 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Rights
Z4	PC_6 & T800_02	Zone 4 Management Data configuration UG7 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Levels

Example: Modified Complex single Access Rights solution

- To see a variation of this configuration.

Example 4b - Modified Complex Single Access Rights solution

Example: Modified Complex Management Data and Access Rights solution

This example is a more structured approach to the problem of allowing all Operators outside Z1 to operate the emergency shutdown with the addition of Security Zone, Z5, and Operator group UG14 with Operators O5 and O6.

The solution is simply to add Operators O5 and O6 to UG13 to give them emergency shutdown Access Rights in Z1. Hence only 1 User group emergency shutdown Access Rights need to be edited to affect all Operators.

Security zone	Security item	Security data
Z1	PC_1 & PC_2	Zone 1 Management Data configuration UG1 with Operator Access Rights UG2 with Engineer Access Rights UG3 with Supervisor Access Rights UG13 with Emergency Operator Access Rights
Z2	PC_3 & PC_4	Zone 2 Management Data configuration UG1 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Rights
Z3	PC_5 & T800_1	Zone 3 Management Data configuration UG7 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Rights
Z4	PC_6 & T800_02	Zone 4 Management Data configuration UG7 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Levels
Z5	T800_03	Zone 5 Management Data configuration UG14 with Operator Access Rights

Example: Modified Complex single Access Rights solution

- To see a variation of this configuration.

Example 4c - Modified Complex Multiple Access Rights solution

Example: Modified Complex single Access Rights solution

This example adopts a different approach to the problem of allowing all Operators outside Z1 to operate the emergency shutdown and has additional Security Zone, Z5, and Operator group UG14 with Operators O5 and O6.

The solution is simply to allocate UG14 to Z1 with the correct emergency shutdown Access Rights. However if the emergency shutdown Access Rights change, the Access Rights in Z1/UG7 and Z1/UG14 will both need to be edited.

Security zone	Security item	Security data
Z1	PC_1 & PC_2	Zone 1 Management Data configuration UG1 with Emergency Operator Access Rights UG2 with Engineer Access Rights UG3 with Supervisor Access Rights UG7 with Emergency Operator Access Rights UG14 with Emergency Operator Access Rights
Z2	PC_3 & PC_4	Zone 2 Management Data configuration UG1 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Rights
Z3	PC_5 & T800_01	Zone 3 Management Data configuration UG7 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Rights
Z4	PC_6 & T800_02	Zone 4 Management Data configuration UG7 with Operator Access Rights UG5 with Engineer Access Rights UG3 with Supervisor Access Levels
Z5	T800_03	Zone 5 Management Data configuration UG14 with Operator Access Rights

Example: Modified Complex single Access Rights solution

- To see a variation of this configuration.

Example 5 - Tag Security Areas configuration solution

Consider a system that comprises 2 Security items (PC_1 and T940_01), where some of the blocks in T940_01 are used to control a boiler and the rest are used to control a furnace.

There are 2 Users groups, Furnace engineers and Boiler engineers who when login to the PC_1 have an Engineers Access Level to the Tags controlling their blocks and an Operators Access Level to the rest.

Note
Users familiar with the 'Security Configurator' can use the rules that apply to that utility when a single Security zone is being configured.

Using EurothermSuite Configurator (ESConfig)

- 1 [Declare the Tag Security Area names.](#)

Using TagEdit

The TagEdit Utility may be accessed from the Tag Browser area in any Developer Tool Utilities.

Allocate the Tags to the Tag Security Area.

Using Security Manager

Create the Users.

Create User groups, (i.e. 'UG1' and 'UG2') and assign Users to each group.

Create a computer Security item (i.e. 'PC_1').

Create a Security zone (i.e. Zone1('Z1')).

Allocate the Security item to Zone1 (i.e. 'PC_1' to 'Z1').

Allocate both User groups to Zone1 (i.e. 'UG1' and 'UG2' to 'Z1').

Edit the Access Rights for each User group, and the Tag Security Area Access Level accordingly.

The instructions above are portrayed in this table.

Security zone	Security item	Security data
Z1	PC_1	Zone 1 Management Data configuration UG1 with Operator access to Furnace Tag Security Area. Engineer access to Boiler Tag Security Area. UG2 with Operator access to Boiler Tag Security Area. Engineer access to Furnace Tag Security Area.

Example 6 - Typical System configuration solution

This is an example of a Typical System configuration.

Consider a system that comprises 2 Security zones, each containing a computer that communicate via an ALIN or Ethernet link. Z1 includes PC_1 and T940_01, where some of the blocks in the instrument are used to control a boiler (Tag Security Area - PID1) and some are used to control a furnace (Tag Security Area - PID2) and Z2 includes PC_2.

There are 4 Users (U1, U2, U3, and U4) divided between 3 Users groups, Administrators (UG1 includes U1), Engineers (UG2 includes U2 and U3) and Operators (UG3 includes U4).

Security zone	Security item	Security data
Z1	PC_1 & T940_01	<p>Zone 1 Management Data configuration</p> <p>UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility ONLY.</p> <p>UG2 with Engineer access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2.</p> <p>UG3 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p>
Z2	PC_2	<p>Zone 2 Management Data configuration</p> <p>UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility ONLY.</p> <p>UG2 with Engineer access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2.</p> <p>UG3 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p>

By changing the configuration, UG2 can be restricted to Operator when accessing the Furnace, Tag Security Area – PID2 and UG3 can be restricted to Operator when accessing the Boiler, Tag Security Area – PID1.

Security zone	Security item	Security data
Z1	PC_1 & T940_01	<p>Zone 1 Management Data configuration</p> <p>UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility ONLY.</p> <p>UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p> <p>UG3 with Operator access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2.</p>
Z2	PC_2	<p>Zone 2 Management Data configuration</p> <p>UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility ONLY.</p> <p>UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p> <p>UG3 with Operator access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area -- PID2.</p>

By changing the configuration, it could also be possible to restrict the access to the Furnace, Tag Security Area - PID2 and the Boiler, Tag Security Area - PID1 depending on where the login has taken place.

Security zone	Security item	Security data
Z1	PC_1 & T940_01	<p>Zone 1 Management Data configuration</p> <p>UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility ONLY.</p> <p>UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p> <p>UG3 with Engineer access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2.</p>
Z2	PC_2	<p>Zone 2 Management Data configuration</p> <p>UG1 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p> <p>UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p> <p>UG3 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.</p>

21 CFR Part 11

The 21 CFR (Code of Federal Regulations) Part 11 guidelines can be found on the FDA (Food and Drug Administration) web-site at the address below.

www.access.gpo.gov/nara/cfr/waisidx_02/21cfr11_02.html

A system can only be 21 CFR Part 11 compliant if enabled regulatory features do NOT exceed the regulatory parameter limits.

.CSV Files



These are text files. .csv files can be viewed using Microsoft Excel.

Delete

Operating this button after selecting a computer will remove it from the list of computers that can access the master database.

Confirmation is required if at 'existing' status.

Navigation pane

This half of the window always lists the Security zones and User groups in alphabetical/numerical order. All items and groups are found using the  and  symbols.

The selection of a heading within this pane displays the appropriate information in the Properties pane.

Login attempts

This field displays an instantaneous record indicating the number of continuous login failures attempted by each Active User.

The field is reset to '0' following a successful login.

Note

Any User exceeding the login attempts configured in the Maximum Login Attempts field on the User Global tab will be automatically Locked out. This will be indicated in the Reason column.

Locked out

This field displays an automatic record indicating whether the User may access the database.

True indicates the User is Locked out (User Id row will be greyed out in the User tab). False identifies the User is NOT disqualified.

A User can be locked out at the Administrator's discretion by

- Setting 'Enabled' from 'False' to 'True'

or automatically if

- exceeded the login attempts,
- the password has expired.

Enabled

This field is edited to indicate the User account is denied access to the Security database.

True indicates a User account as Active. False identifies a User account as Locked out. (see [change the Enabled field](#)) as indicated with 'Account disabled' displayed in the Locked out reason column.

Enabled

This is a Read Only column indicating,

- True, the Security item is enabled for Deployment,
- False, the Security item is not enabled for Deployment.

Enable PC Locking

When this box is checked ONLY the listed computer's may access the database.

Exit Button

Operating this button terminates the Security Manager Utility, returning to the Project Folder.

Fullname

This field is edited to enable the Security database to identify a User when used in conjunction with the corresponding password.

This field is initially blank but MUST be completed to enable the User to Login (see [change the Fullname field](#)). The name entered MUST always be unique.

Note

The default Password MUST also be changed to enable the User to Login.

This field can only be configured within the selected [Regulatory value constraints](#) determined in the User Global tab.

File name field

When the .CSV file is the selected output format, the saved electronic file is assigned a default SecManDb.CSV file name.

The default SecManDb.CSV file name can be edited to enable the User to use a unique file name prior to pressing 'OK'.

File path field

When the .CSV file is the selected output format, the file path defines the location of the saved electronic file.

This field can be edited to save electronic copies of the selected elements to a specified location prior to pressing 'OK'.

Name

Displays the assigned Security item name. This is the name as shown in the Project Folder.

Project Folder > Networks > network directory.

Password

This column stores the password, displayed as 'xxxxxxx', associated with each User needing access to a Security database.

The password must first be changed at this location before the User can access a Security database (see [change the Password field](#)), but can be changed at any time with confirmation by 2 authorised Users.

It is recommended that...
passwords contain at least 1 printable non-alpha character.

This field can only be configured within the selected [Regulatory value constraints](#) determined in the User Global tab.

PC List

This field displays the computer name, code and State of computers selected to access the master database.

The 'State' field can be 'Add' - awaiting confirmation, 'Delete' - awaiting confirmation or 'Existing' - confirmation received.

Password expiry

This field is edited to increase or decrease the minimum number of days until a password expires and requires changing (see [change the Password expiry time field](#)). When the password has expired the User is Locked out of the Security database.

Note

An account that has been locked out due exceeding the password expiry period can be re-enabled by changing the Password (see [change the Password field](#)), and setting this field to a revised password expiry period (see [change the Password expiry time field](#)).

This field can only be configured within the selected [Regulatory value constraints](#).

This is a 21 CFR part 11 compliant feature.

Regulation

This function allows the selection of a Regulation. Each Regulation determines the levels of restriction set on the ranges for each of the parameter values within the Utility.

These Regulations are imposed on Security Manager Utility, Series 5000 instruments, computer's, and T800 instruments when the database is deployed.

It is recommended that...

this option is defined as early as possible, as any parameter value existing before a Regulation is selected will NOT be effected. However any subsequent configuration will be restricted by the [Regulation constraints](#).

Type

Displays the Security item type, i.e. EurothermSuite PC, Review and QuickChart Software, 5000 and 6000 Series or T800 Visual Supervisor instruments.

Recipe

A recipe can be either;

- ingredients (elements needed for production) or
- machine setup parameters or
- steps in batch processing.

Reason

This is a Read Only column automatically describing the cause which resulted in the User to be Locked out.

If there is a number of reasons ONLY 1 is displayed at a time but each MUST be dealt with before the User can access the Security database.

A User can be Locked out if, the

- User account has been disabled ('Enabled' field reads 'False', Reason field reads 'Account disabled').
- login attempts have been exceeded,
- password has expired,
- User account has been Retired ('Retired' field reads 'True' Reason field reads 'Account retired').

User Id

This column lists the configured Security Manager User accounts. Current disqualified (Locked out, Disabled, or Retired) Users are greyed out.

This is a Read Only column but is incremented when Users are added.

User Id column

List's ALL User Id's (accounts).

System

This field is edited to identify an account used to perform system functions.

Note

An 'ESDataSrv' system account can be created when adding a computer Security item.

If the field indicates True the system User account can only initiate system functions. After initiating operations are performed by the system. False identifies the it as a User account (see [change the System field](#)).

Note

Users cannot Login using these parameters.

Remote User Id

This column lists the configured remote User accounts which require access to the Security database via a 5000 Series instrument.

Each field is edited to allow the creation of a Remote User Id (see [change the Remote User Id field](#)) that can access the Security database via a 5000 Series instrument.

Remote password

This column stores the Remote password, displayed as 'xxxxxxx', associated with each User requiring access to a Security database via a 5000 Series instrument.

The Remote password must first be changed at this location before the User can access a Security database via a 5000 Series instrument (see [change the Password field](#)), but can be changed at any time.

It is recommended that...

passwords contain at least 1 printable non-alpha character.

This field can only be configured within the selected [Regulatory value constraints](#) determined in the User Global tab.

Retired

This field is used to terminate the selected User account, thus preventing the selected User access to the Security database.

True indicates the User account has been terminated. False (default) indicates a current active User account (see [change the Retired field](#)).

Beware

21 CFR Part 11 Regulations state that Retired User Ids MUST be retained. Although systems configured to the *Default Regulations* will be able remove all Retired User account parameters if the *Keep Retired User Ids (User Global tab)* reads *False*.

Development Tools

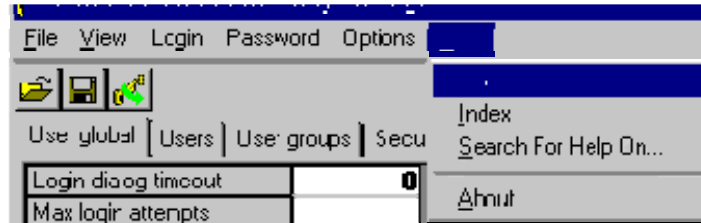
The required software programs used to develop a system.

Contents

With the selection of this menu option, the **'Help'** file is displayed with the **'Contents'** command as the priority.

To display this

- 1 Select the **'Help > Contents'** from the Menu Bar.



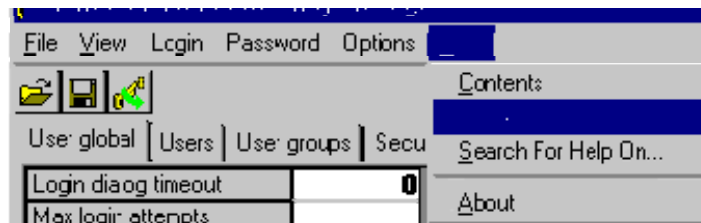
- 2 The Security Manager On-line Help document appears in a new window. Use standard windows Help operations to use the On-line Help.

Index

With the selection of this menu option, the **'Help'** file is displayed with the **'Index'** command as the priority.

To display this

- 1 Select **'Help > Index'** from the Menu Bar.



- 2 The Security Manager On-line Help document appears in a new window. Use standard windows operations to use the On-line Help.

Search For Help On

With the selection of this menu option, the **'Help'** file is displayed with the **'Search'** command as the priority.

To display this

- 1 Select **'Help > Search For Help On'** from the Menu Bar.



- 2 The Security Manager On-line Help document appears in a new window. Use standard windows operations to use the On-line Help.

About

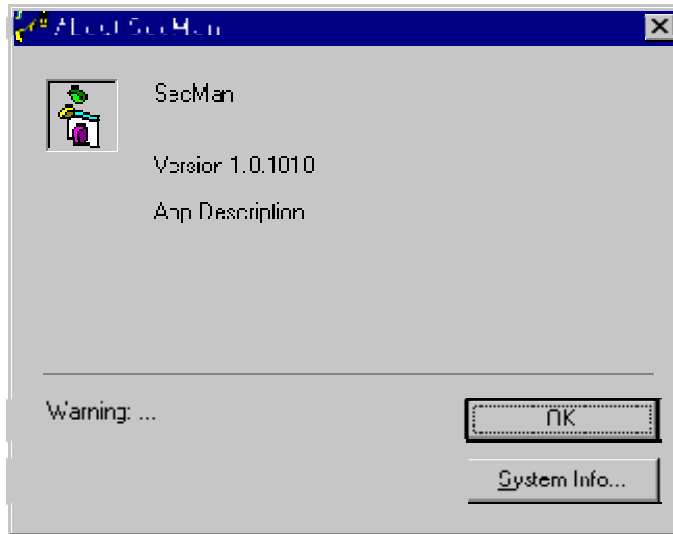
With the selection of this menu option, information about the utility is displayed including the name, version number, and description.

Display the utility details by,

- 1 Selecting 'Help > About' from the Menu Bar.



- 2 The About dialog window appears.



- 3 Select the 'OK' button to return to the previous window.

Security Status

This part of the Status Bar shows the current state of database.

Security Manager Database Location

This part of the Status Bar shows the full path location of the opened database.

Security Manager Database icon



Time

This part of the Status Bar shows the current time.

Date

This part of the Status Bar shows the current date.

OK

Press this button to confirm the selected command.

Security Manager help

To get help on using Security Manager, click the shortcuts:

 [Security items](#)

 [Security zone](#)

 [User global](#)

 [Users](#)

 [User group](#)

 **Click on a Security Manager window region to get help!**

Getting specific help:

Sometimes you can see more specific help by clicking the object of interest, then pressing the <F1> key on the keyboard.

Index

.		
.csv file	31	
.pkd file	81	
.uhh file	81, 146	
5		
5000 Series	17, 61, 128	
5000 Series instruments	17, 128	
5000 Series Regulatory Defaults	128	
6		
6000 Series Instrument Regulatory Defaults	129	
A		
About	159	
Access level		
configure	69	
Access level	69	
Access Rights	59, 60, 61, 63, 65, 66, 67, 69, 70, 73, 76, 77, 78, 79, 80, 81, 82, 84, 88, 89, 91, 95, 96, 97, 98, 99, 101, 102, 149	
Access Rights data	86	
Access Rights solution	148, 149, 150, 151	
Acknowledge Alarms		
configure	69	
Acknowledge Alarms	69	
Action Demand Writes		
configure	69	
Action Demand Writes	69	
Add		
Security item	49	
Security zone	54	
User	43	
User group	46	
Add	15	
Add	43	
Add	46	
Add	49	
Add	54	
Add User group button	15	
Address	121	
Adjust Inputs		
configure	70	
Adjust Inputs	70	
Administration		
configure	70	
Administration	70	
Administrator	15	
Alarm		
configure	72	
Alarm	72	
Alarm authorisation field		
configure	71	
Alarm authorisation field	71	
AlarmHistMaxItems		
configure	73	
AlarmHistMaxItems	73	
All Users	14, 45, 125, 147	
Allocate		
User	16	
Allocate	16	
Allocate	56	
Allocate	57	
Allocate	59	
Allocate Security items	56, 59	
Allocate User groups	57	
Archiving Control		
configure	73	
Archiving Control	73	
Audit Ports		
configure	74	
Audit Ports	74	
Audit Trail field		
configure	75	
Audit Trail field	75	
Authorisation field		
configure	75	
Authorisation field	75	
Authorise		
configure	76	
Authorise	76	
Auto Logon UserId field		
configure	76	
Auto Logon UserId field	76	
Auto deploy Command line parameter	91, 95, 96, 97, 98, 99	
B		
Batch Control		
configure	76	
Batch Control	76	
C		
Cancel PC Configuration	124	
Change		
Change Password field	111	
Enabled	113	
Fullname	113	
keep retired User Id field	116	
Login dialog timeout	115	
maximum login attempts	40	
maximum password length	42	
maximum User Id length	117	
minimum password length	41	
minimum User Id length	41	
Password expiry time period	111	
Password field	110	
Password reuse period	116	
Reason field	115	
Remote password field	112	
Remote User Id	112	
Retired field	114	
System field	114	
User Id	110	
Change	40	
Change	41	
Change	41	
Change	42	
Change	77	
Change	77	
Change	77	
Change	77	
Change	78	

Change	78	Audit Ports	74
Change	108	Audit Trail field	75
Change	110	Authorisation field	75
Change	110	Authorise	76
Change	111	Auto Logon UserId field	76
Change	111	Batch Control	76
Change	112	Change Alarm Setpoints	77
Change	112	Change Language	77
Change	113	Change own	78
Change	113	Change own expired	78
Change	114	Chart Annotate	78
Change	114	Chart Approve	79
Change	115	Chart Open/Close	79
Change	115	Chart Release	79
Change	116	Chart Review	80
Change	116	Chart Setup	80
Change	117	Confirmation field	80
Change	119	Connect	81
Change Alarm Setpoints configure	77	Create Chart	81
Change Alarm Setpoints	77	Debug	82
Change Language configure	77	Disable Service Account field	83
Change Language	77	Display access level field	83
Change own configure	78	downloaded Recipes field	109
Change own	78	Edit	85, 86
Change own expired configure	78	Edit Deployable Flag	84
Change own expired	78	Edit Maths Constants	84
Change password	77	Edit Output Channel Default	84
Change Password	111	Edit user data	85
Change Password field change	111	Edit zone	86, 87
Change Password field	111	Edit zone configuration data	87
Chart Annotate configure	78	Event Permission	87
Chart Annotate	78	Export Data	88
Chart Approve configure	79	Export Historical Trend	88
Chart Approve	79	Export Setup	88
Chart Open/Close configure	79	Faceplate	89
Chart Open/Close	79	Faceplate Configurator	89
Chart Release configure	79	File Services	90
Chart Release	79	Full Configuration	90
Chart Review configure	80	Full Security	90
Chart Review	80	Global Alarm Acknowledge	91
Chart Setup configure	80	Inactivity timeout field	92
Chart Setup	80	IO data writes	91
Close	27	Log Invalid Times field	93
Command Line parameters	140	Login	93
Complex Management Data	148, 149	Login timeout field	94
Configure		Modify Chart View	95
Access level	69	Notes field	95
Acknowledge Alarms	69	Offline data writes	95
Action Demand Writes	69	Operator	96
Adjust Inputs	70	Operator group global	96
Administration	70	Operator Point Display	96
Alarm	72	Override Server Redundancy	97
Alarm authorisation field	71	Paste/Delete Files	98
AlarmHistMaxItems	73	Preset Counters	98
Archiving Control	73	Preset Totalisers	98
		Print Setup	99
		QuickChart software	65
		Recipe Download	99
		Record	100
		Recovery	101
		Recovery account field	100
		Reference Number	101
		Reset Maths	102
		Save Chart	102
		Save/Restore	103
		Set Clock	103

Sign.....	103	Configure.....	88
Signing field	104	Configure.....	89
Start/Reset Timers	104	Configure.....	89
Synchronise Files.....	105	Configure.....	90
T800 Visual Supervisor	67	Configure.....	90
Task.....	106	Configure.....	90
Transfer Files.....	106	Configure.....	91
Trend Global	107	Configure.....	91
Trends.....	107	Configure.....	92
View Only.....	108	Configure.....	93
View Security Data.....	108	Configure.....	93
With unapplied	108	Configure.....	94
Configure	19, 60, 61, 63	Configure.....	95
Configure	65	Configure.....	95
Configure	65	Configure.....	95
Configure	66	Configure.....	96
Configure	66	Configure.....	96
Configure	67	Configure.....	96
Configure	67	Configure.....	97
Configure	69	Configure.....	97
Configure	69	Configure.....	98
Configure	69	Configure.....	98
Configure	70	Configure.....	98
Configure	70	Configure.....	99
Configure	71	Configure.....	99
Configure	72	Configure.....	99
Configure	73	Configure.....	100
Configure	73	Configure.....	100
Configure	74	Configure.....	101
Configure	75	Configure.....	101
Configure	75	Configure.....	102
Configure	76	Configure.....	102
Configure	76	Configure.....	103
Configure	76	Configure.....	103
Configure	77	Configure.....	103
Configure	77	Configure.....	104
Configure	77	Configure.....	104
Configure	78	Configure.....	105
Configure	78	Configure.....	105
Configure	78	Configure.....	106
Configure	79	Configure.....	106
Configure	79	Configure.....	106
Configure	79	Configure.....	107
Configure	80	Configure.....	107
Configure	80	Configure.....	108
Configure	80	Configure.....	108
Configure	81	Configure.....	108
Configure	81	Configure.....	109
Configure	82	Configure Access Rights	25
Configure	82	Configure Management Data	24
Configure	83	configure the 6000 Series access rights	62
Configure	83	configure the 6000 Series management data.....	62
Configure	84	configure the Admin only access rights	70
Configure	84	configure the Administrator Password field	70
Configure	84	configure the Administrator UserId field	71
Configure	85	configure the Custom1 to Custom5 access rights	81
Configure	85	configure the Custom6 to Custom10 access rights	81
Configure	85	configure the Delete retired users field	82
Configure	86	configure the Deploy existing users field	83
Configure	86	configure the FTP access rights	89
Configure	86	configure the Groups fields	91
Configure	87	configure the Lockout Level field	92
Configure	87	configure the Perform Upgrade access rights	98
Configure	87	configure the Remote access rights	102
Configure	88	configure the User1 to User4 access rights.....	107
Configure	88	configure the Windows Domain Access Rights	68

configure the Windows Domain Management Data.....	68
Configuring	
Database.....	5
Deployment computer.....	19
Configuring.....	5
Configuring.....	19
Confirmation field	
configure.....	80
Confirmation field.....	80
Connect	
configure.....	81
Connect.....	81
Contents.....	158
Create.....	81
Create Chart	
configure.....	81
Create Chart.....	81
CSV file.....	35

D

Database	
Configuring.....	5
Database.....	5
Database.....	34
Database.....	121
Database.....	122
Debug	
configure.....	82
Debug.....	82
Default accounts.....	118
Delete	
Security item.....	120
Security zone.....	58
User group.....	47
Delete.....	47
Delete.....	58
Delete.....	120
Delete.....	154
Deploy	
selected Security items.....	51
Deploy.....	20, 21
Deploy.....	51
Deploy.....	82
Deploy Security.....	20, 21, 82
Deploy Security Window.....	21
Deployable.....	22, 84
Deployment computer	
configure.....	19
Deployment computer.....	19
Deployment computer.....	53
Deployment Computer configuration.....	53
Disable Service Account field	
configure.....	83
Disable Service Account field.....	83
Discard Changes.....	38
Display access level field	
configure.....	83
Display access level field.....	83
Downloaded Recipes field	
configure.....	109
Downloaded Recipes field.....	109

E

Each User.....	147
Edit	
configure.....	85, 86
Edit.....	85
Edit.....	85
Edit.....	86
Edit.....	86
Edit Deployable Flag	
configure.....	84
Edit Deployable Flag.....	84
Edit Maths Constants	
configure.....	84
Edit Maths Constants.....	84
Edit Output Channel Default	
configure.....	84
Edit Output Channel Default.....	84
Edit user data	
configure.....	85
Edit user data.....	85
Edit zone	
configure.....	86, 87
Edit zone.....	86
Edit zone.....	87
Edit zone configuration data	
configure.....	87
Edit zone configuration data.....	87
Element selection.....	32
Enable PC Locking.....	155
Enable Security.....	36
Enabled	
change.....	113
Enabled.....	36
Enabled.....	113
Enabled.....	113
Enabled.....	155
Enabled.....	155
ESDataSrv user account.....	118
EurothermSuite PC Regulatory Defaults.....	130
EurothermSuite Pc s security level names.....	126
Event Permission	
configure.....	87
Event Permission.....	87
Example	53, 59, 118, 147, 148, 149, 150, 151, 152, 153
Example 4a.....	149
Example 4b.....	150
Example 4c.....	151
Exit.....	28, 155
Exit Button.....	155
Expiry.....	77
Export Data	
configure.....	88
Export Data.....	88
Export Historical Trend	
configure.....	88
Export Historical Trend.....	88
Export Setup	
configure.....	88
Export Setup.....	88

F

Faceplate	
configure.....	89
Faceplate.....	89

configure 95
 Modify Chart View..... 95

N

Notes field
 configure 95
 Notes field..... 95

O

Offline data writes
 configure 95
 Offline data writes 95
 OK 159
 Open 26
 Opening
 Security Manager 4
 Opening 4
 Opening 26
 Operator
 configure 96
 Operator 96
 Operator group global
 configure 96
 Operator group global 96
 Operator Point Display
 configure 96
 Operator Point Display 96
 Options pulldown 9
 Output
 printer 34
 Output 34
 Output 35
 Output 84
 Override Server Redundancy
 configure 97
 Override Server Redundancy 97
 Overview
 Security Manager 2
 Overview 2

P

Password9, 12, 78, 97, 110, 111, 116, 156
 Password expiry 97, 111, 113, 156
 Password expiry time period
 change 111
 Password expiry time period 111
 Password field
 change 110
 Password field 110
 Password pulldown 9
 Password reuse period
 change 116
 Password reuse period 12
 Password reuse period 116
 Paste/Delete Files
 configure 98
 Paste/Delete Files..... 98
 Path
 SecManDb.ujx Command line parameter 140
 Path 140
 PC 63, 123, 155, 156
 PC Configuration 123

PC List 156
 Preset Counters
 configure 98
 Preset Counters..... 98
 Preset Totalisers
 configure 98
 Preset Totalisers..... 98
 Print 31, 99
 Print Setup
 configure 99
 Print Setup..... 99
 Printer
 output 34
 Printer 34
 Pulldown 8

Q

QuickChart Software
 configure 65
 QuickChart Software 17
 QuickChart Software 65
 QuickChart Software 65
 QuickChart Software 131

R

Reason115, 156
 Reason field
 change 115
 Reason field..... 115
 Recipe Download
 configure 99
 Recipe Download 99
 Record
 configure 100
 Record 100
 Recover
 unusable Security Manager/PC Security 121
 unusable T800 Security 122
 Recover 121
 Recover 122
 Recover Security Manager/PC Security Database 121
 Recover T800 Visual Supervisor Security Database 121
 Recovery
 configure 101
 Recovery 101
 Recovery account field
 configure 100
 Recovery account field 100
 Recovery User Account 14
 Re-enable
 User 45
 Re-enable 45
 Re-enable User Button 14
 Reference Number
 configure 101
 Reference Number 101
 RegServer Command line parameter 141
 Regulation 156
 Regulatory Defaults127, 128, 131
 Remote 81
 Remote password.....112, 157
 Remote password field
 change 112

Remote password field 112

Remote User Id
change 112

Remote User Id 112

Remote User Id 157

Remove/show status bar 126

Remove/show toolbar 125

Rename a Security zone 57

Reset Maths
configure 102

Reset Maths 102

Retired 114, 157

Retired field
change 114

Retired field 114

Review Software 18, 66, 132

Review Software Regulatory Defaults 132

S

Save Changes 37

Save Chart
configure 102

Save Chart 102

Save/Restore
configure 103

Save/Restore 103

Search
Help On 158

Search 158

Search For Help On 158

SecManDb.ujx 140

SecManDb.ujx path Command line parameter 140

Secure Command line parameter 142

Security item data 85

Security items
add 49

delete 120

modify 50

Security items 17

Security items 49

Security items 50

Security items 85

Security items 120

Security Manager
Opening 4

Overview 2

Security Manager 2

Security Manager 3

Security Manager 4

Security Manager 7

Security Manager 60

Security Manager 60

Security Manager 85

Security Manager 127

Security Manager 146

Security Manager 159

Security Manager Audit Trail 146

Security Manager Database icon 159

Security Manager help 160

Security Manager Regulatory Defaults 127

Security Manager setup 85

Security Manager Utility 3

Security Manager Window 7

Security Zones
add 54

delete 58

Security Zones 23

Security Zones 54

Security Zones 58

Select Print categories 35

Selected Security items
deploy 51

Selected Security items 51

Set Clock
configure 103

Set Clock 103

Show Active 45, 125

Show Active Users 45, 125

Sign
configure 103

Sign 103

Signing field
configure 104

Signing field 104

Simple Management Data 148

Single User group solution 147

Start/Reset Timers
configure 104

Start/Reset Timers 104

Status bar 8

Switch
MasterDB 34

Switch 34

Switch 106

Synchronise Files
configure 105

Synchronise Files 105

System 114, 157

System field
change 114

System field 114

System User writes 105

T

T800 Visual Supervisor
configure 67

T800 Visual Supervisor 67

T800 Visual Supervisor 67

T800 Visual Supervisor Regulatory Defaults 133

T800 Visual Supervisor specifics 18

Tag 105, 118, 138, 139, 152

Tag Profile Configurator specifics 138

Tag Security Area 105, 118, 139, 152

Tag Security Area Access Levels 105, 118

Tag Security Areas configuration solution 152

Tag Security Areas specifics 139

TagEdit 106, 118

Task
configure 106

Task 106

Their own User group solution 147

Transfer Files
configure 106

Transfer Files 106

Trend Global
configure 107

Trend Global 107

Trends
configure 107

Trends 107

Typical System configuration solution..... 153

U

UnRegServer Command line parameter.....	145
Unusable Security Manager/PC Security	
Recover.....	121
Unusable Security Manager/PC Security.....	121
Unusable T800 Security	
Recover.....	122
Unusable T800 Security.....	122
User	
add.....	43
allocate.....	16
Re-enable.....	45
User.....	11, 13, 15
User.....	16
User.....	43
User.....	45
User.....	46
User.....	47
User.....	59
User.....	85
User.....	86
User.....	86
User.....	93
User.....	101
User.....	110
User.....	147
User.....	157
User Global.....	11, 86
User global data.....	86
User group	
add.....	46
Definition.....	15
delete.....	47
User group.....	15

User group.....	15
User group.....	15
User group.....	46
User group.....	47
User group.....	59
User group.....	86
User group data.....	86
User Id	
change.....	110
User Id.....	110
User Id.....	157
User List field.....	93

V

View Only	
configure.....	108
View Only.....	108
View pulldown.....	9
View Security Data	
configure.....	108
View Security Data.....	108

W

Welcome.....	1
What is	
User Group.....	15
What is.....	15
Windows Domain.....	18
Windows Domain Regulatory Defaults.....	133
Windows Domain specifics.....	19
With unapplied	
configure.....	108
With unapplied.....	108

Inter-Company sales and service locations

AUSTRALIA Sydney

Eurotherm Pty. Ltd.
Telephone (+61 2) 9838 0099
Fax (+61 2) 9838 9288
E-mail info.au@eurotherm.com

AUSTRIA Vienna

Eurotherm GmbH
Telephone (+43 1) 7987601
Fax (+43 1) 7987605
E-mail info.at@eurotherm.com

BELGIUM & LUXEMBURG Moha

Eurotherm S.A./N.V.
Telephone (+32) 85 274080
Fax (+32) 85 274081
E-mail info.be@eurotherm.com

BRAZIL Campinas-SP

Eurotherm Ltda.
Telephone (+5519) 3707 5333
Fax (+5519) 3707 5345
E-mail info.br@eurotherm.com

DENMARK Copenhagen

Eurotherm Danmark AS
Telephone (+45 70) 234670
Fax (+45 70) 234660
E-mail info.dk@eurotherm.com

FINLAND Abo

Eurotherm Finland
Telephone (+358) 22506030
Fax (+358) 22503201
E-mail info.fi@eurotherm.com

FRANCE Lyon

Eurotherm Automation SA
Telephone (+33 478) 664500
Fax (+33 478) 352490
E-mail info.fr@eurotherm.com

GERMANY Limburg

Eurotherm Deutschland GmbH
Telephone (+49 6431) 2980
Fax (+49 6431) 298119
E-mail info.de@eurotherm.com

HONG KONG & CHINA

Eurotherm Limited North Point
Telephone (+85 2) 28733826
Fax (+85 2) 28700148
E-mail info.hk@eurotherm.com

Guangzhou Office

Telephone (+86 20) 8755 5099
Fax (+86 20) 8755 5831
E-mail info.cn@eurotherm.com

Beijing Office

Telephone (+86 10) 6567 8506
Fax (+86 10) 6567 8509
E-mail info.cn@eurotherm.com

Shanghai Office

Telephone (+86 21) 6145 1188
Fax (+86 21) 6145 1187
E-mail info.cn@eurotherm.com

INDIA Chennai

Eurotherm India Limited
Telephone (+9144) 2496 1129
Fax (+9144) 2496 1831
E-mail info.in@eurotherm.com

IRELAND Dublin

Eurotherm Ireland Limited
Telephone (+353 1) 4691800
Fax (+353 1) 4691300
E-mail info.ie@eurotherm.com

ITALY Como

Eurotherm S.r.l.
Telephone (+39 31) 975111
Fax (+39 31) 977512
E-mail info.it@eurotherm.com

KOREA Seoul

Eurotherm Korea Limited
Telephone (+82 31) 2738507
Fax (+82 31) 2738508
E-mail info.kr@eurotherm.com

NETHERLANDS Alphen a/d Rijn

Eurotherm B.V.
Telephone (+31 172) 411752
Fax (+31 172) 417260
E-mail info.nl@eurotherm.com

NORWAY Oslo

Eurotherm A/S
Telephone (+47 67) 592170
Fax (+47 67) 118301
E-mail info.no@eurotherm.com

POLAND Katowice

Invensys Eurotherm Sp z o.o.
Telephone (+48 32) 218 5100
Fax (+48 32) 217 7171
E-mail info.pl@eurotherm.com

SPAIN Madrid

Eurotherm España SA
Telephone (+34 91) 661 6001
Fax (+34 91) 661 9093
E-mail info.es@eurotherm.com

SWEDEN Malmo

Eurotherm AB
Telephone (+46 40) 384500
Fax (+46 40) 384545
E-mail info.se@eurotherm.com

SWITZERLAND Wollerau

Eurotherm Produkte (Schweiz) AG
Telephone (+41 44) 787 1040
Fax (+41 44) 787 1044
E-mail info.ch@eurotherm.com

UNITED KINGDOM Worthing

Eurotherm Limited
Telephone (+44 1903) 268500
Fax (+44 1903) 265982
E-mail info.uk@eurotherm.com
Web www.eurotherm.co.uk

U.S.A Leesburg VA

Eurotherm Inc.
Telephone (+1 703) 443 0000
Fax (+1 703) 669 1300
E-mail info.us@eurotherm.com
Web www.eurotherm.com

ED52



Invensys

EUROTHERM

EUROTHERM LIMITED

Faraday Close, Durrington, Worthing, West Sussex, BN13 3PL

Telephone: +44 (0)1903 268500 Facsimile: +44 (0)1903 265982

e-mail: info.uk@eurotherm.com

Website: <http://www.eurotherm.co.uk>