Eurotherm®

by Schneider Electric

Security Management & Control Software

Security Manager

User Guide

HA028131

July 2019 (Issue 8)

© 2019

All rights are strictly reserved. No part of this document may be reproduced, modified, or transmitted in any form by any means, nor may it be stored in a retrieval system other than for the purpose to act as an aid in operating the equipment to which the document relates, without prior written permission of the manufacturer.

The manufacturer pursues a policy of continuous development and product improvement. The specifications in this document may therefore be changed without notice. The information in this document is given in good faith, but is intended for guidance only. The manufacturer will not accept responsibility for any losses arising from errors in this document.

SECURITY MANAGER
USER GUIDE
Table of Contents

1 INTRODUCTION

1.1 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,

- Computers 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
- Eycon™ 10/20 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.

1.1.1 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.

EFFECTIVITY

This document refers to Security Manager version 1.12

1.1.2 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

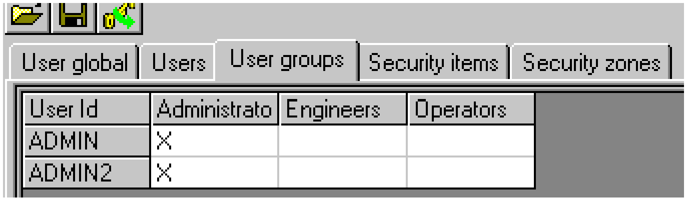
For a full description of these features refer to Tag and LINBlock specifics.

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

- 5000 Series instruments
- 6000 Series instruments
- QuickChart Software
- Review Software
- T800/Eycon™10/20 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.

2 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

2.1 SOFTWARE INSTALLATION REQUIREMENTS

Listed below are the software installation requirements, which should be installed before installing the 6000 Series Tools.

Application	Requirement
6000 Series Tools - Security Manager - Bridge	Microsoft Visual C++ 2015 Redistributable Update 3
	Microsoft .NET Framework 4.7
	Microsoft .NET Framework 3.5

2.2 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 > Eurotherm > 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.

2.3 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 on any Security item node. The SecManDb.ujx icon represents the Security Manager Utility.

SecManDb.ujx

It is recommended that a client database should be edited only in exceptional circumstances. Use the pulldown 'File > Switch to MasterDB' to open the master database.

Important Note: With improved security capability, i.e. 6000 with Secure FTP, the user may experience initial communications being blocked. Please ensure both the Security Manager application (SecMan.exe) and Security Manager's Service (SecManSrv.exe) have both been approved and allowed through your system firewall(s). For further information, please refer to your security application's user documentation or consult your local system administrator.

To open Security Manager,

1. At the computer,

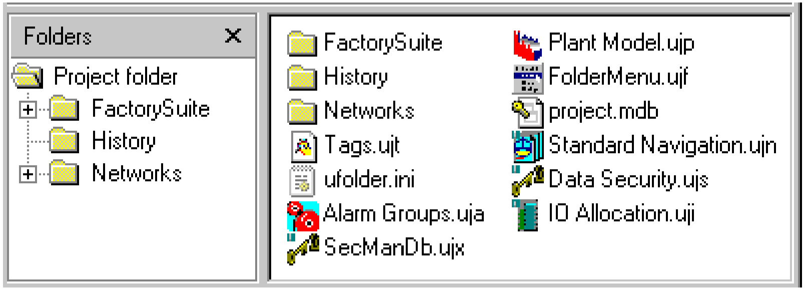
A Standalone Utility

- 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.



2. In the Project Folder, open the Utility (SecManDb.ujx icon) using the (or **'File** > **Open...'**).

- Alternatively, double-click the SecManDb.ujx icon.

3. 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.

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.

4. Now, configure the database.

2.3.1 Configure a Database

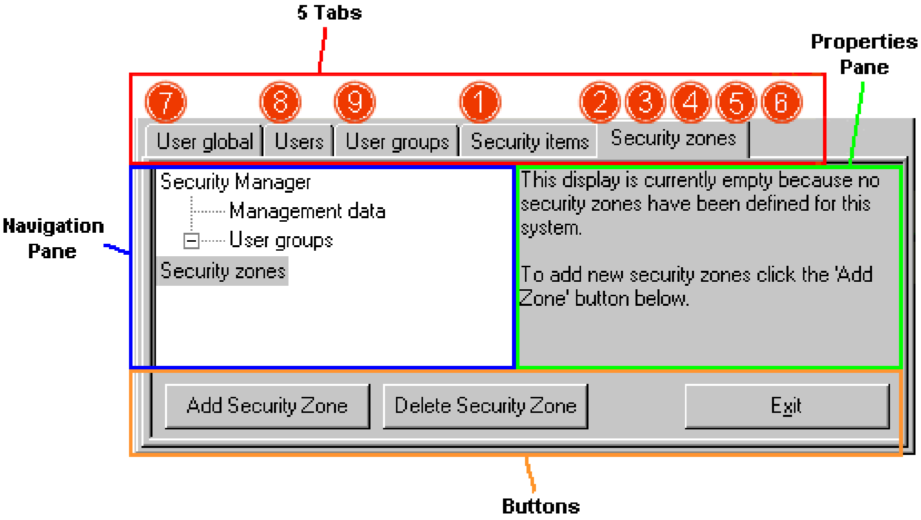
To simplify the configuration of the database it has been divided into security elements, each represented by a tab. There are no definitive rules about how to structure security, but it is important remember there is usually more than 1 possible configuration. Users and Security items are easy to create 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.



This display is currently empty because no security zones have been defined for this system.

To add new security zones click the 'Add Zone' button below.

2.3.2 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 1 - EACH USER IN THEIR OWN USER GROUP SOLUTION

Consider a system that comprises 2 Security item nodes (2 T800 Visual Supervisors - 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 Supervisors - 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 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 4B - MODIFIED COMPLEX SINGLE 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 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 4C - MODIFIED COMPLEX MULTIPLE 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 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.

2. Allocate the Tags to the Tag Security Area.

Using Security Manager

3. Create the Users.
4. Create User groups, (i.e. 'UG1' and 'UG2') and assign Users to each group.
5. Create a computer Security item (i.e. 'PC_1').
6. Create a Security zone (i.e. Zone1('Z1')).
7. Allocate the Security item to Zone1 (i.e. 'PC_1' to 'Z1').
8. Allocate both User groups to Zone1 (i.e. 'UG1' and 'UG2' to 'Z1').
9. 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	Zone 1 Management Data configuration UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility **ONLY**. UG2 with Engineer access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2. UG3 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.
Z2	PC_2	Zone 2 Management Data configuration UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility **ONLY**. UG2 with Engineer access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2. UG3 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.

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	Zone 1 Management Data configuration UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility **ONLY**. UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2. UG3 with Operator access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2.
Z2	PC_2	Zone 2 Management Data configuration UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility **ONLY**. UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2. UG3 with Operator access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area -- PID2.

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	Zone 1 Management Data configuration UG1 with Administrator access to all Tags NOT assigned to a Tag Security Area and can edit Security Manager Utility **ONLY**. UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2. UG3 with Engineer access to Boiler, Tag Security Area - PID1. Engineer access to Furnace, Tag Security Area - PID2.
Z2	PC_2	Zone 2 Management Data configuration UG1 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2. UG2 with Engineer access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2. UG3 with Operator access to Boiler, Tag Security Area - PID1. Operator access to Furnace, Tag Security Area - PID2.

.

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 be edited only 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

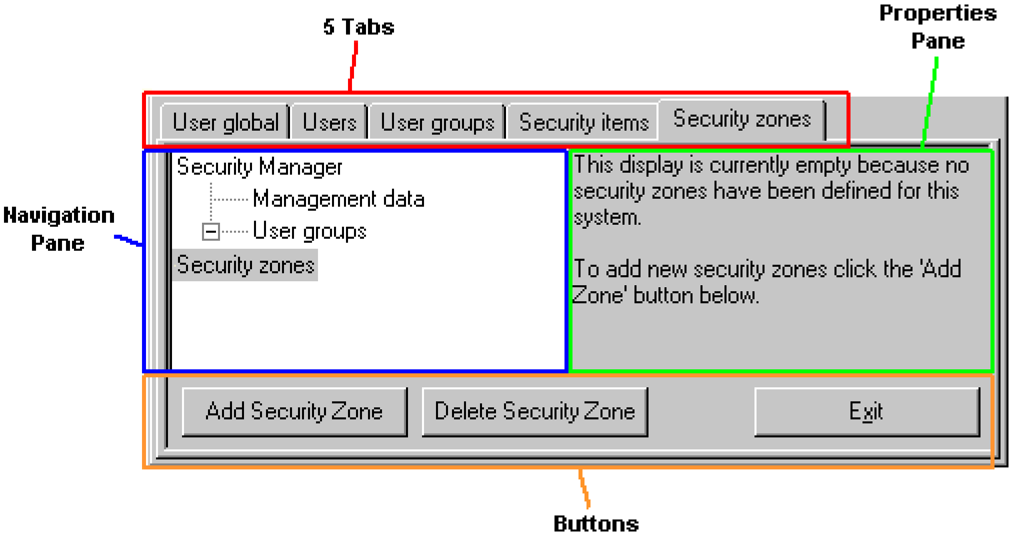
Accounts can be deleted from the database only if using the **Default Regulation** constraints and the **Keep Retired User Id** field on the User global tab reads ‘False’. Any other configuration will store account details allowing the database to automatically check that accounts are unique when added. 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.

3 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.



This display is currently empty because no security zones have been defined for this system.

To add new security zones click the 'Add Zone' button below.

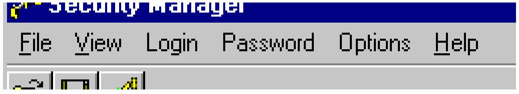
3.1 MENU REGIONS

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

3.1.1 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.

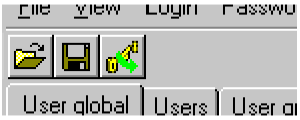
The Menu bar contains the following items,



3.1.2 Toolbar

The Toolbar hosts icon buttons that enable quick access to a limited number of Edit and View commands. It is displayed by default at the top of the Editor screen.

The Toolbar contains the following items,



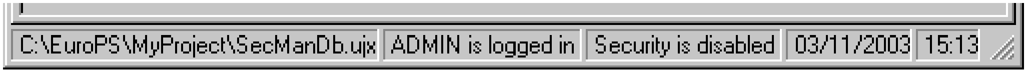
Note

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

3.1.3 Status Bar

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

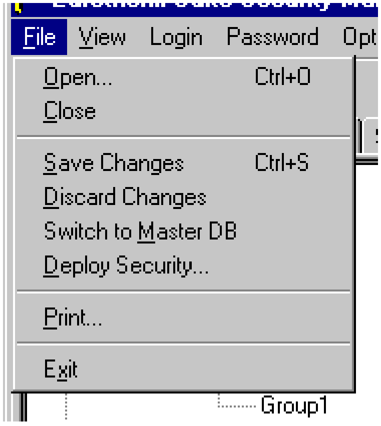
The Status bar contains the following items,



C:\EuroPS\MyProject\SecManDb.ujx | ADMIN is logged in | Security is disabled | 03/11/2003 | 15:13

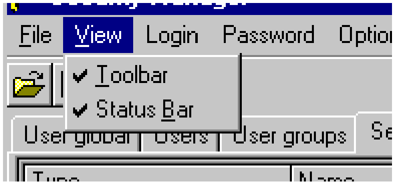
3.1.4 File pulldown

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



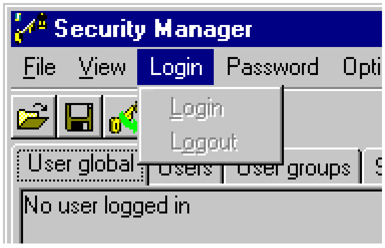
3.1.5 View pulldown

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



3.1.6 Login pulldown

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



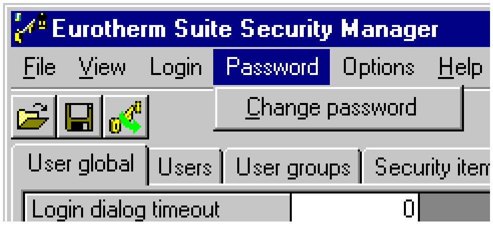
No user logged in

The Login pulldown menu offers the following functions,

- Login
- Logout

3.1.7 Password pulldown

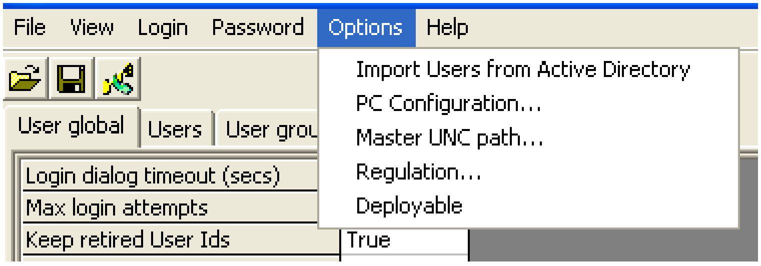
The Password pulldown menu offers the opportunity to change the current Users password. This is achieved via the Change Password option.



Login dialog timeout 0

3.1.8 Options pulldown

The Options pulldown menu allows the User to manipulate the security of the Security Manager master database itself.

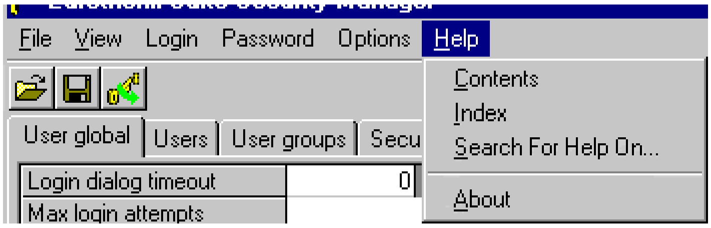


3.1.9 Help pulldown

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.



3.2 TABS

3.2.1 User global

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

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 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 MAXIMUM LOGIN ATTEMPTS FIELD

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 KEEP RETIRED USER IDS FIELD

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 FIELD

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 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 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 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.

BUTTONS

3.2.2 USERS TAB

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.

DISPLAY FIELDS

User Id
Password
Change Password
Password Expiry
Remote User Id
Remote Password
Fullname
System
Retired
Enabled
Login Attempts
Locked Out
Reason

BUTTONS

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/Eycon™ 10/20 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 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.

Note
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.

3.2.3 User Groups Tab

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.
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

DECIDING ON USER GROUPS

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

- each User in his or her 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 correspond with a role within a Security zone. The role of the User group is defined by the Access Rights configured for each User group 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.

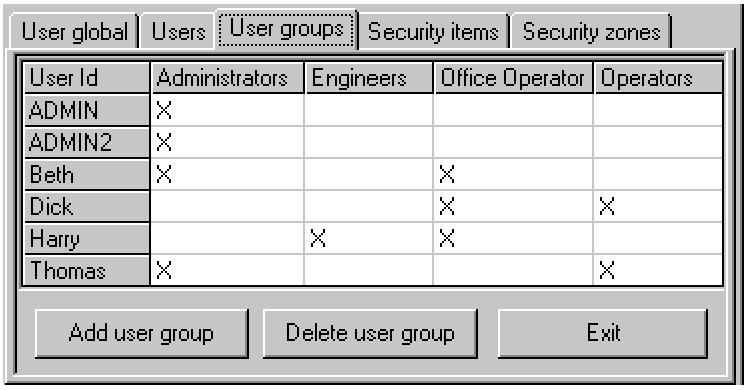
ALLOCATE A USER TO A GROUP

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.

3.2.4 Security items tab

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.

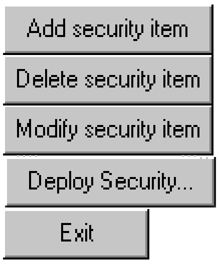
WHAT IS THE SECURITY ITEMS TAB?

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



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, Visual supervisor 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 recorders, T800/ Eycon™10/20 Visual Supervisors 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.

VISUAL SUPERVISOR

After a security database has been downloaded to a Visual Supervisor, it will reject any other databases unless they have been generated from the same source. To enable the 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

Because Windows prevents 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 Visual Supervisor 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

The Configuration of 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.

IMPORTANT NOTE

Each Deployment Computer MUST start the Security Manager Utility using the /Autodeploy Command line parameter

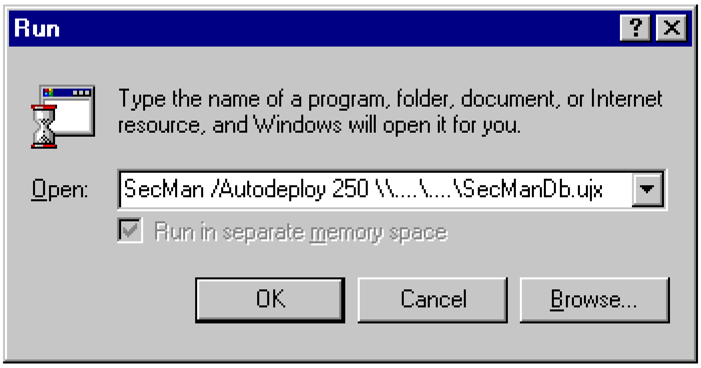
Configure a Deployment zone by:

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
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.
From the drop down list select the PC for that Security zone.
Finally save changes.

Now at the Deployment Computer

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

Command line prompt example



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /Autodeploy 250 \\....\....\SecManDb.ujx

☑ Run in separate memory space

"SecMan" /AutoDeploy 60 "\\EuroPS\MyProject\SecManDb.ujx"
"SecMan" /AutoDeploy 300 "SecManDb.ujx"

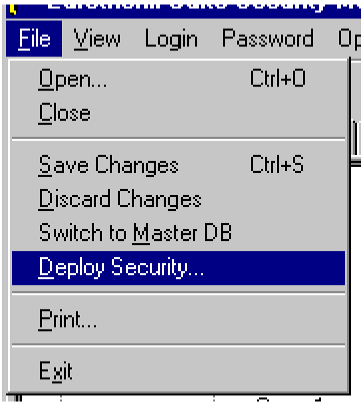
Note

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 Deploy Security... 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.

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, Deploy Security... from the Security items tab, or from the **‘File > Deploy Security’**.

Display fields

Security items
Log

Buttons

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

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

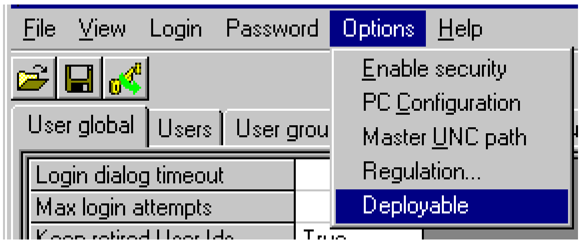
This function allows non-privileged Users to replicate the database to an individual destination or groups of Security items without requesting a signature.

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

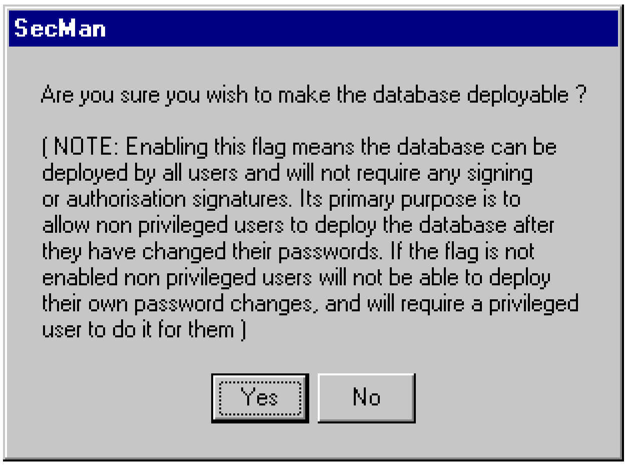
A check mark beside the option indicates it is a currently deployable database.

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.


SecMan

Are you sure you wish to make the database deployable ?

(NOTE: Enabling this flag means the database can be deployed by all users and will not require any signing or authorisation signatures. Its primary purpose is to allow non privileged users to deploy the database after they have changed their passwords. If the flag is not enabled non privileged users will not be able to deploy their own password changes, and will require a privileged user to do it for them)

3.2.5 Security zones tab

WHAT IS A SECURITY ZONE?

A Security zone is a grouping of Security item(s) and/or User group(s) and may not necessarily 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)

BUTTONS

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/ Eycon™10/20 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.

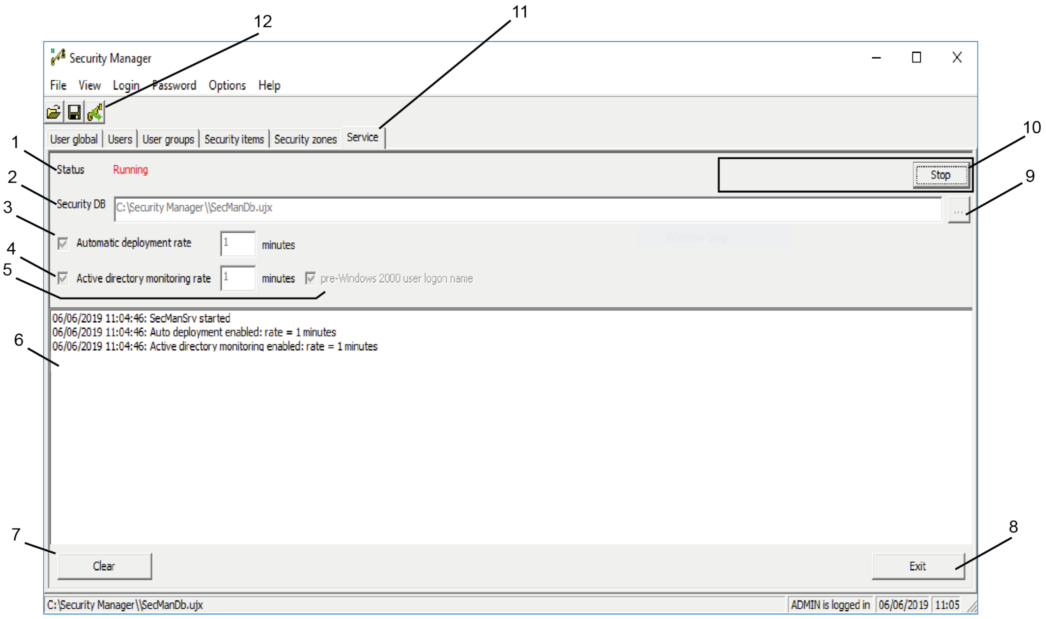
- Security Manager Access Rights
- EurothermSuite PC Access Rights
- Review Software Access Rights
- QuickChart Software
- 5000 Series Access Rights
- T80/ Eycon™10/200 Visual Supervisor Access Rights
- Windows Domain Access Rights

3.2.6 Service tab

WHAT IS THE SERVICE TAB?

The Service tab provides and allows;

- the Service function to be installed as an autonomous PC service
- users to control the installed Service, for example Stop, Start and Uninstall
- the display of the current Service status, in addition to a log of the Service activity and events deployed
- the configuration of Service functions *Auto deployment* and *Active Directory monitoring*



Status Running

Security DB C:\Security Manager\\SecManDb.ujx

☑ Automatic deployment rate 1 minutes

☑ Active directory monitoring rate 1 minutes ☑ pre-Windows 2000 user logon name

```
06/06/2019 11:04:46: SecManSrv started
06/06/2019 11:04:46: Auto deployment enabled: rate = 1 minutes
06/06/2019 11:04:46: Active directory monitoring enabled: rate = 1 minutes
```

C:\Security Manager\\SecManDb.ujx | ADMIN is logged in | 06/06/2019 | 11:05

Service Status

1 Service status

The following Status types exists:

Uninstalled The Security Manager Service has not been installed.

Running The Security Manager Service is running as an autonomous PC service.

Stopped The Security Manager Service has been stopped by an approved user. During the *Stopped* status the Service will not perform monitoring or deployment.

2 Security DB The text box displays the file path of the Security database used by the Service

Note: Ensure the Security Manager Service is *Stopped* (button 10) before opening an existing or creating a new Security DB file.

Check boxes:

3 Automatic deployment rate Check to enable Automatic Deployment, see *enable and configure Automatic deployment*.

Automatic deployment rate - Minutes Enter a time value (measured in minutes)

4 Active Directory monitoring rate Check to enable Active Directory monitoring, see *enable and configure Active Directory monitoring*.

Active Directory monitoring rate – Minutes Enter a time value (measured in minutes)

5 pre-Windows 2000 user logon name Check to enable pre-Windows 2000 user logon name, see *pre-Windows 2000 user logon name*.

Window

6 Event Log window — Displays a historical list of actions performed by the Service.

Buttons and Tabs

7 Clear — Deletes the log file and clears the Event log window (6).

8 Exit — Selecting *Exit* will close the Security Manager application.

Note: However if the Service has been installed, correctly configured and left in *Running* status the Service will continue to run in the background, while the PC remains on.

9 — Click to select the Security DB file location.

10 Stop — Selecting *Stop* will stop Security Manager Service and if enabled Automatic monitoring and Deployment.

Note: When stopped the service can be configured.

Start — Select *Start* to run the Security Manager Service.

Uninstall — Select *Uninstall* to remove the Service.

Note: Once removed, all changes to the Security Manager's configuration will need to be deployed manually using the *Deploy* button (12).

Install — Select *Install* to install the Service.

The *Install* button only appears if the status is *Uninstalled*, see Status (1). Selecting the *Install* button displays the *Security Manager - Install service* dialog, to continue installing the Service complete the dialog by adding the relevant Service Account details - see *How to install and configure the Service*.

11 Service tab — The *Service* tab in the Security Manager application.

12 — Select the *Deploy* button to manually deploy the Security Manager configuration.

HOW TO INSTALL AND CONFIGURE THE SERVICE?

The Security Manager's Service configuration comprises of;

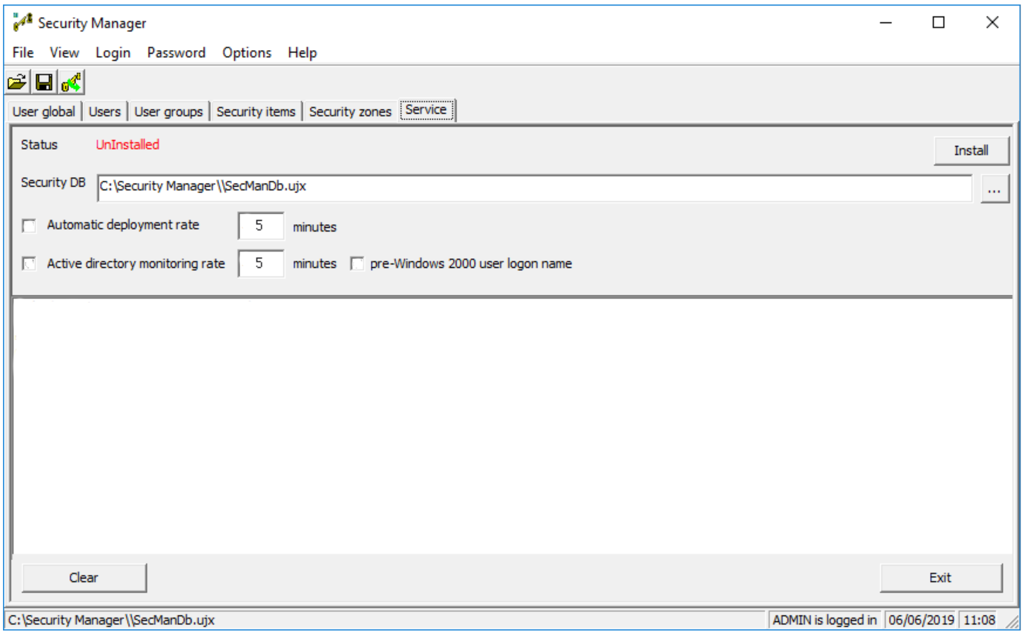
- Installing the Service function as a PC service
- Configuring a User account for the Service to run on, autonomously
- Enabling and configuring Service functions *Auto deployment* and *Active Directory monitoring*

To Install the Service, (Run as Administrator)

Note: The following instructions assume the latest version of Security Manager is installed.

1. Save and Close the Security Manager application, if open.
2. Start the Security Manager application using the *Run as Administrator* option.
3. Depending on the Operating System (OS), approve and allow any OS permissions to continue.
4. The *Login* dialog displays. Complete the *User Name*, *Password* fields to log in.
5. Select the *Service* tab from the Security Manager application.

   The Service Manager application displays the Service.


Security Manager
File View Login Password Options Help
User global | Users | User groups | Security items | Security zones | Service
Install
...
Clear
Exit

Status UnInstalled

Security DB C:\Security Manager\\SecManDb.ujx

□ Automatic deployment rate 5 minutes

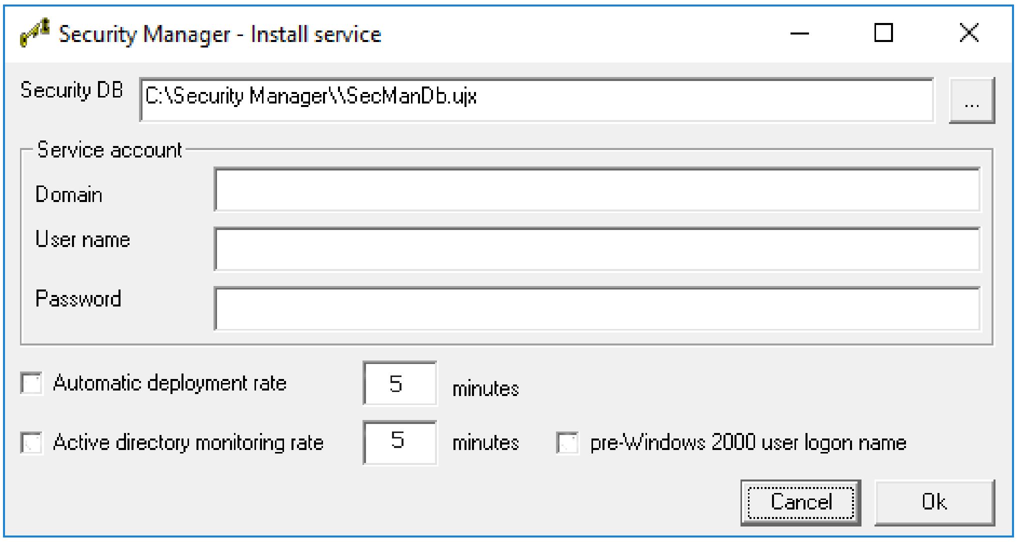
□ Active directory monitoring rate 5 minutes □ pre-Windows 2000 user logon name

C:\Security Manager\\SecManDb.ujx | ADMIN is logged in | 06/06/2019 | 11:08

   If the *Install* button is not visible and the status is *Unknown*, Security Manager is not running as Administrator.

6. Select the *Install* button (top right).

   The *Service Manager - Install service* dialog appears



Security DB C:\Security Manager\\SecManDb.ujx

Service account

Domain

User name

Password

□ Automatic deployment rate 5 minutes

□ Active directory monitoring rate 5 minutes □ pre-Windows 2000 user logon name

7. Complete the *Install Service* dialog with the following details to configure the Service:

Security DB	The text box displays the default file path location of the Security database. Change as required.
Service account	The user account details entered (*Domain*, *User name* and *Password)* specifies the account the Service will run under. Note: The user account must have the 'Run as Service' privilege.
Domain	Enter domain name. If left blank, it will assume it is a local user.
User name	Enter a User name.
Password	Enter the corresponding password, ensure it is correct.
Check boxes	
Active Deployment Rate	See *Configuring Service functions,* for futher information.
Active Directory monitoring rate	
Pre-Windows 2000 user logon name	

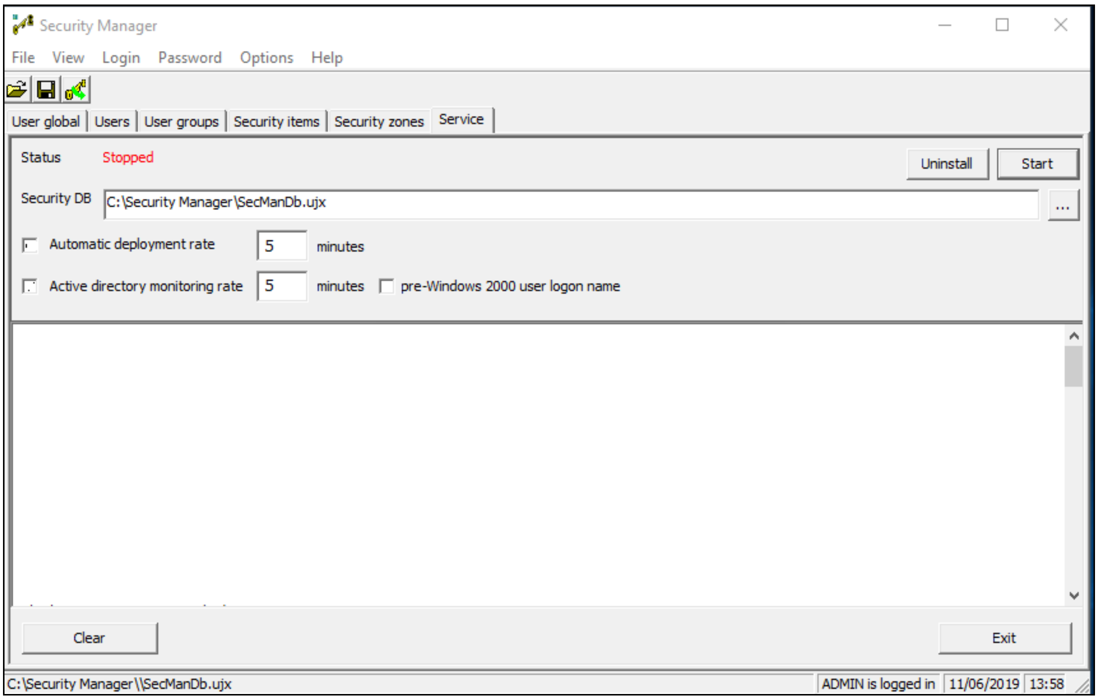
NOTE: The User name entered in the Service account configuration must have Administration rights and 'Run as Service' privileges. Also, the password must be correct and entered correctly, as the dialog only confirms the User account exist, it does not verify and authenticate all the user details configured, meaning the Service will still install but may not run and warn of an incorrect configuration.

8. Select and click Ok, on the *Install Service* dialog to complete the Service Installation,

The Security manager application will display when installed;

Status: *Stopped*

Buttons present (top right): *Uninstall* and *Start*)


Security Manager
File View Login Password Options Help
User global | Users | User groups | Security items | Security zones | Service
Uninstall
Start
...
Clear
Exit

Status Stopped

Security DB C:\Security Manager\SecManDb.ujx

□ Automatic deployment rate 5 minutes

□ Active directory monitoring rate 5 minutes □ pre-Windows 2000 user logon name

C:\Security Manager\\SecManDb.ujx | ADMIN is logged in | 11/06/2019 | 13:58

Configuring Service functions

Once the Service has been installed the following functions may need to be configured if required;

- Auto deployment, see *enable and configure Automatic deployment*
- Active Directory monitoring, see *enable and configure Active Directory monitoring*
- pre-Windows 2000 user logon name, see *enable Active Directory pre-Windows 2000 User logon names*

Note: To gain access to the Service check box functions ensure the Service status is *Stopped*, The Service check box functions are unaccessible when the Service is running.

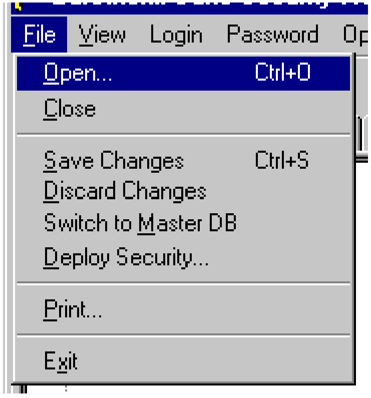
4 HOW TO...

4.1 OPEN

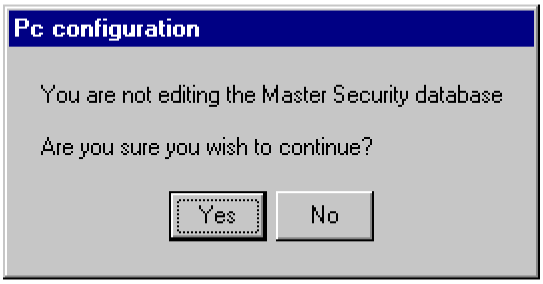
This function allows the User to find and open a database from the security configuration.

It is recommended that, if a database is already open, any changes are saved before another database is opened.

Open a database by,
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 SecMan Db.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.


Pc configuration

You are not editing the Master Security database

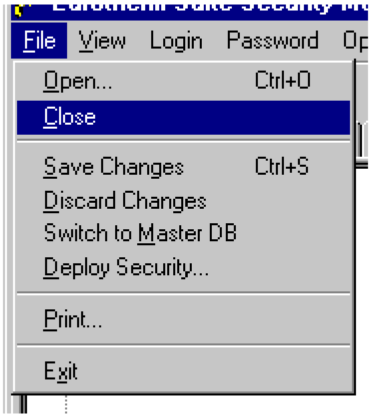
Are you sure you wish to continue?

The user is prompted to Login. After a successful login the selected Security Manager database appears.

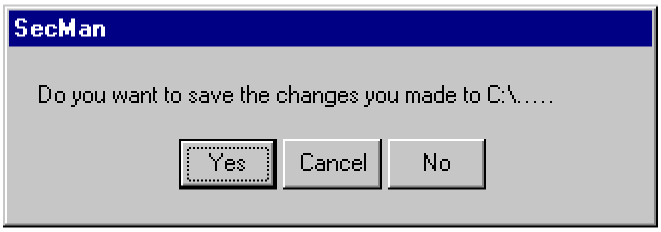
4.2 CLOSE

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.

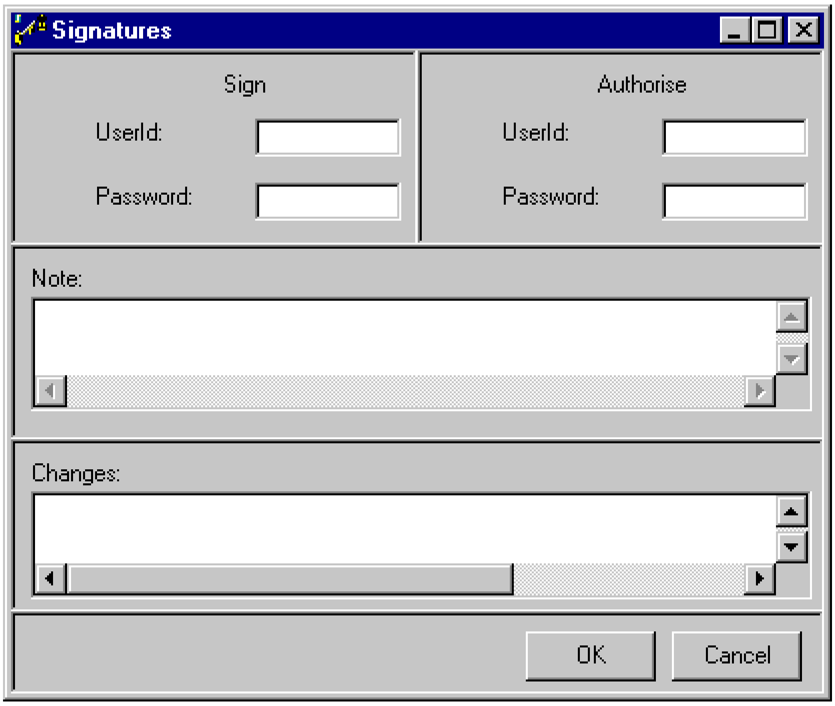


2. The save changes dialog window appears, press '**Yes**' to save any changes, and '**Cancel**' to return to the current Security Manager window. Select '**No**' to discard any changes made since the last save and revert to a blank Security Manager window.


SecMan

Do you want to save the changes you made to C:\.....

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


Signatures

Sign
UserId:
Password:

Authorise
UserId:
Password:

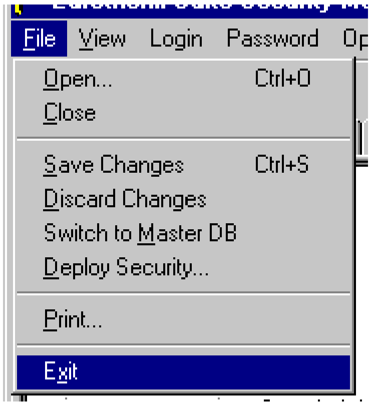
Note:

Changes:

4.3 EXIT

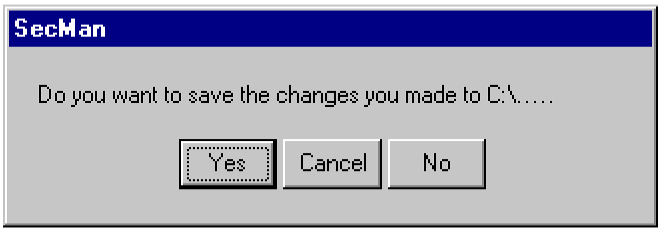
This function is similar to the '**Close**' option. It terminates this Utility and returns to the Project Folder. Exit the Utility by,

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



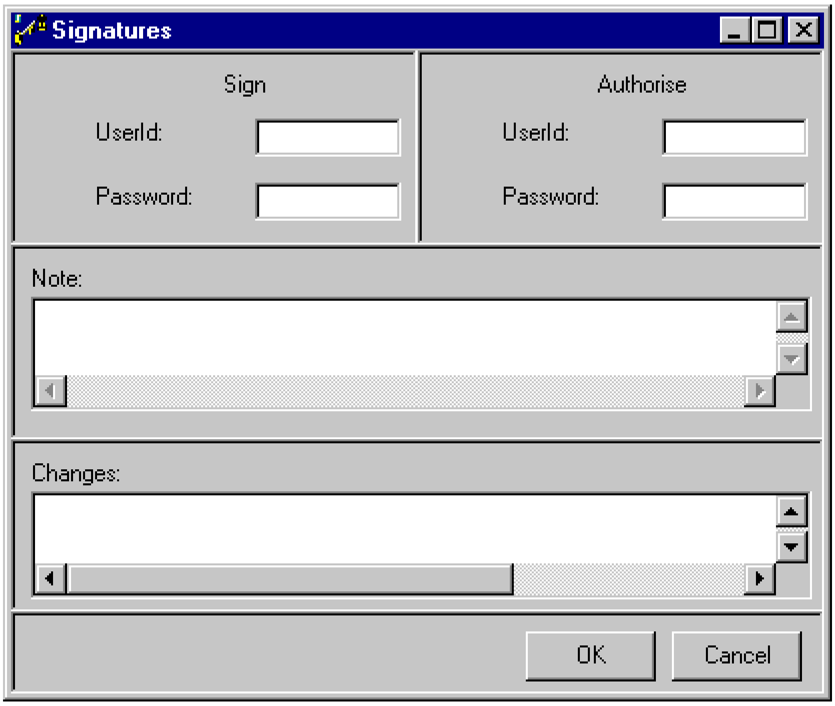
- If changes have not yet been saved a dialog window appears.

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.



Do you want to save the changes you made to C:\.....

- 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.

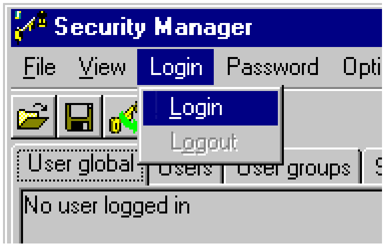


- Click '**OK**' if satisfied with the information or '**Cancel**' to discard **ALL** changes made. The dialog window and the Utility closes. The Project Folder is now active.

4.4 LOGIN

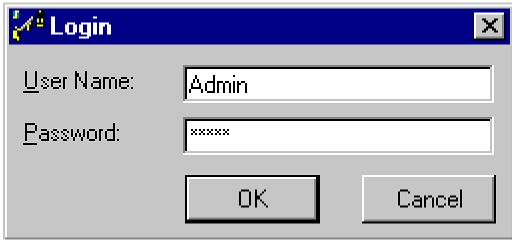
The function enables the User to access a database using a valid User Id and password.
To login,

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



No user logged in

- 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.



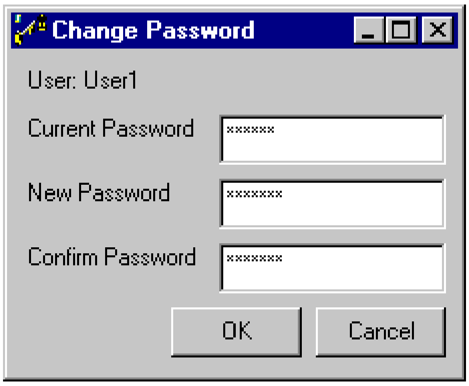
User Name: Admin

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.



User: User1

Current Password ******

New Password *******

Confirm Password *******

- 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

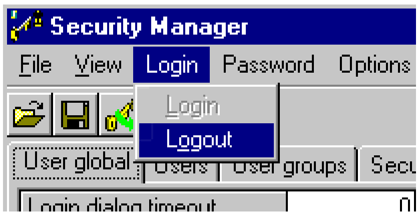
For security purposes passwords are '**always**' displayed as '**xxxxxxxx**' irrespective of the constraints specified in the User global tab.

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

4.5 LOGOUT

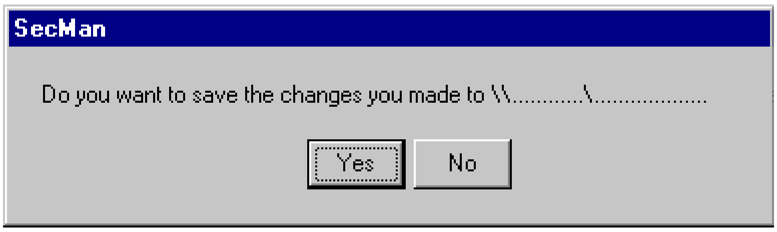
This function enables the User to close of the database, returning to the blank Security Manager Window, after saving or discarding changes if requested.
To logout,

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



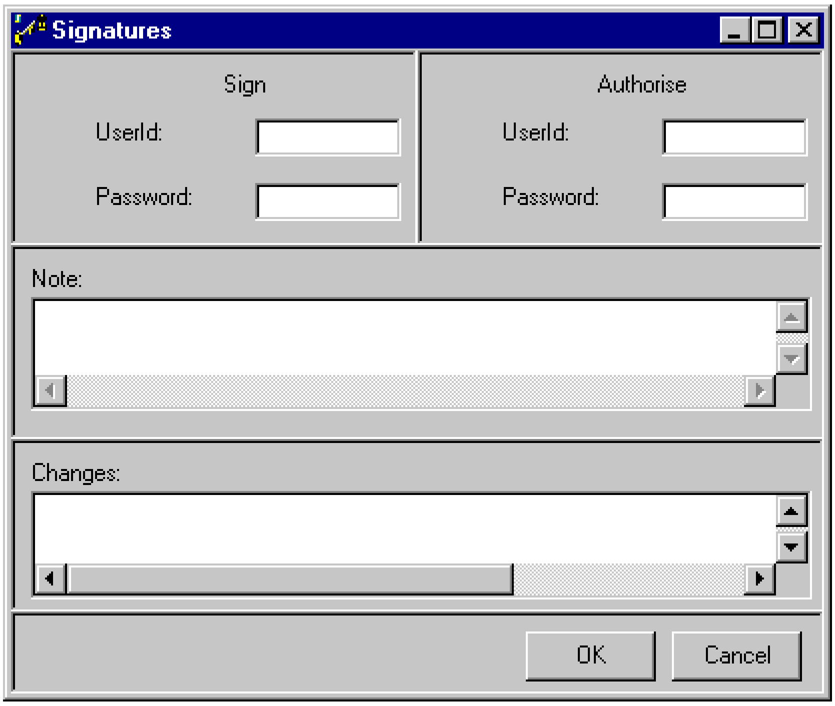
- A blank Security Manager window appears if no changes exist.
- If changes have not yet been saved a dialog window appears.

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.



Do you want to save the changes you made to \\...........\..................

- 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.

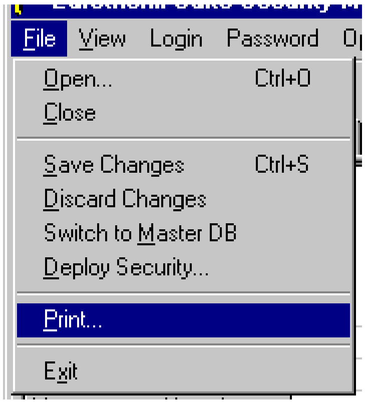
4.6 PRINT

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

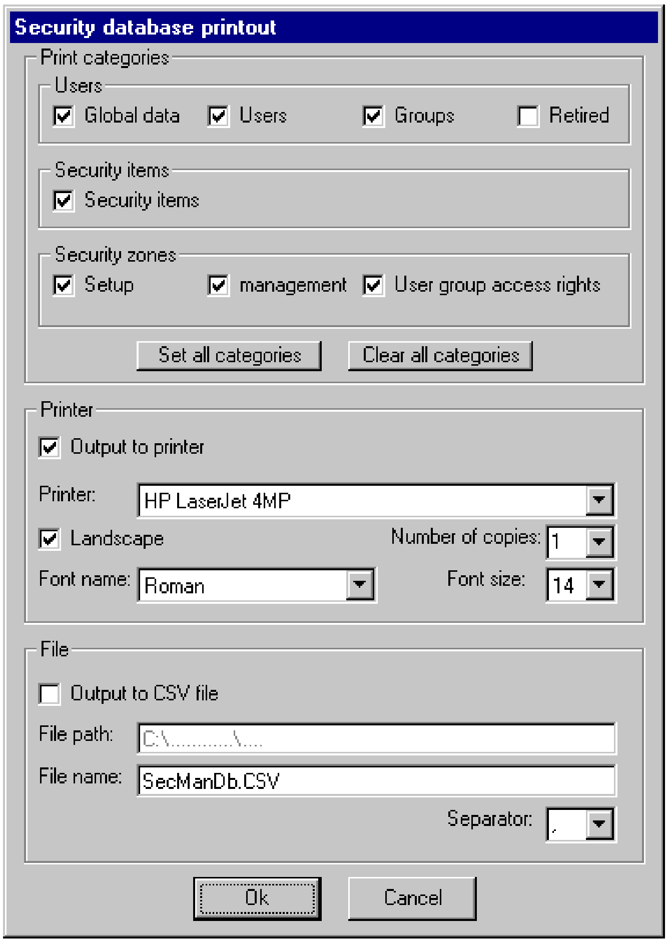
- Print categories
- Printer
- File

An output of the selected categories is produced by,

1. Selecting ‘**File** > **Print’** from the Menu Bar.



2. The Print dialogue window is displayed allowing the User to select elements and set up the printer or file options.



Security database printout

Print categories

Users: ☑ Global data ☑ Users ☑ Groups □ Retired

Security items: ☑ Security items

Security zones: ☑ Setup ☑ management ☑ User group access rights

Printer

☑ Output to printer

Printer: HP LaserJet 4MP

☑ Landscape

Number of copies: 1

Font name: Roman

Font size: 14

File

□ Output to CSV file

File path: C:\...........\....

File name: SecManDb.CSV

Separator: ,

3. After the Print dialogue window is setup, press ‘**Ok**’ to print or ‘**Cancel**’ to abandon the print instructions and return to the current Security Manager window.

4.6.1 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.

4.6.2 Element selection

If the element check box is
☑an output will be produced
but, if
□an output will NOT be.

4.6.3 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.

4.6.4 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.

4.6.5 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.

4.6.6 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.

4.6.7 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.

4.6.8 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.

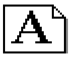
It is recommended that in order to ensure the printed text is readable, the font size is set to 6 or above.

4.6.9 Number of copies field

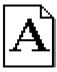
When the printer is the selected output format, the number of printed copies can be altered.
The User can select between 1 and 99 copies from the drop-down list.

4.6.10 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 .

4.6.11 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.

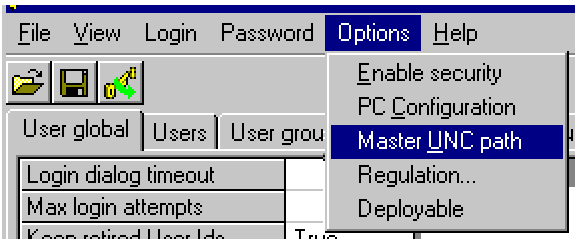
If the 'Separator: , ▾' is selected, Microsoft Excel separates the information into multiple columns.

If the 'Separator: Tab ▾ ' 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.

4.6.12 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.

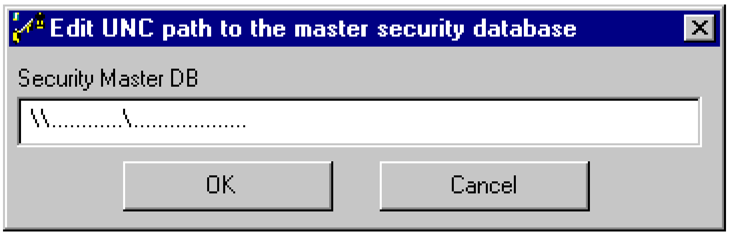
1. Select **'Options** > **Master UNC Path'** from the Menu Bar.



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.

5. Enter the correct path and press the '**Update UNC path**' button.

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

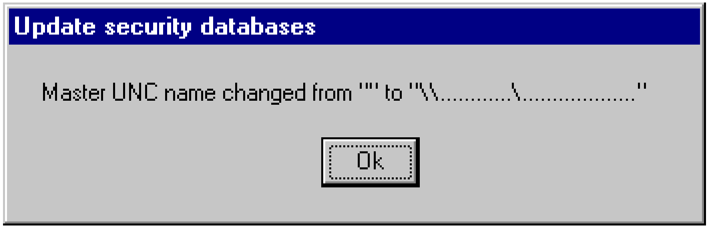


Edit UNC path to the master security database

Security Master DB

\\............\...................

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.


Update security databases

Master UNC name changed from "" to "\\............\.................."

6. After the path has been successfully, updated press ‘**Close**’ to return to the current security database window.

4.7 SWITCH TO MASTERDB (DATABASE)

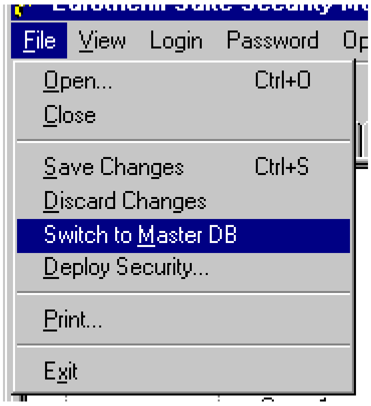
This function allows the User to switch from editing a Security Manager client database to the master database. This feature will automatically,

- 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.

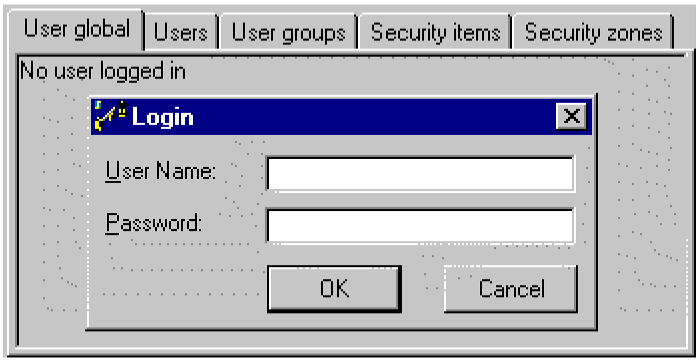
Switch to the master database by,

1. Selecting **‘File** > **Switch to MasterDB’** from the Menu Bar.



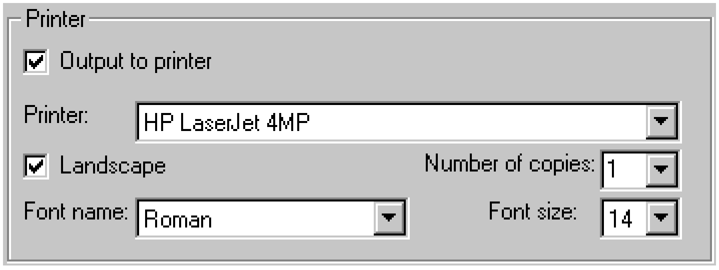
2. If the database detects unsaved changes, the save prompt appears. Press ‘**Yes**’ to save changes and continue, ‘**No**’ to discard changes and continue, or ‘**Cancel**’ to revert to the current client security configuration.

If ‘**Yes**’ or ‘**No**’ was pressed the client database closes and automatically prompts for a Login User Id.


No user logged in

4.8 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.



Printer

☑ Output to printer

Printer: HP LaserJet 4MP

☑ Landscape

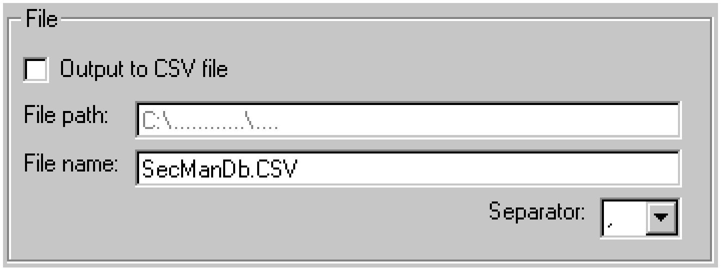
Number of copies: 1

Font name: Roman

Font size: 14

4.8.1 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.



File

□ Output to CSV file

File path: C:\............\....

File name: SecManDb.CSV

Separator: ,

4.8.2 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,

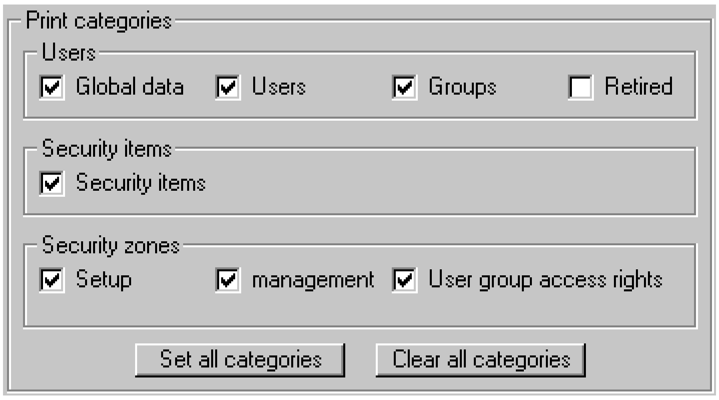
- Output to printer
- Output to CSV file

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’.



Print categories

Users

☑ Global data ☑ Users ☑ Groups □ Retired

Security items

☑ Security items

Security zones

☑ Setup ☑ management ☑ User group access rights

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.

4.9 ENABLE SECURITY ON EUROTHERMSUITE PCS

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.

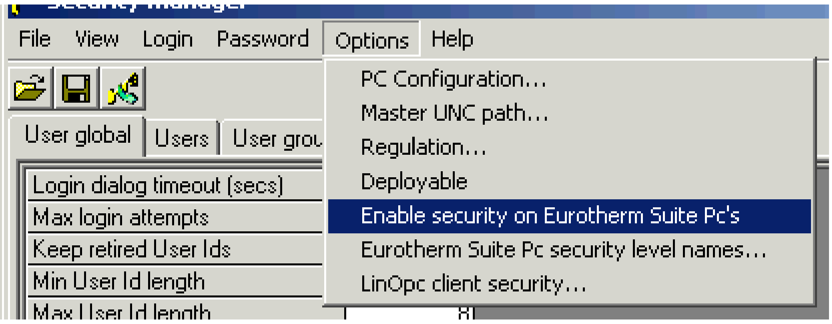
4.9.1 How to Enable/Disable Security on EurothermSuite PCS

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

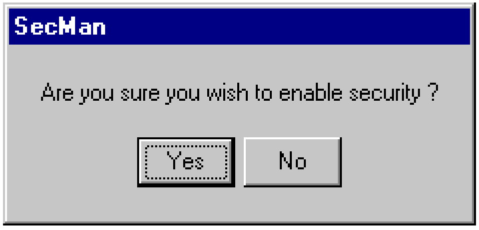
1. Select **‘Options** > **Enable security on EurothermSuite PC's’** from the Menu Bar.

Note

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

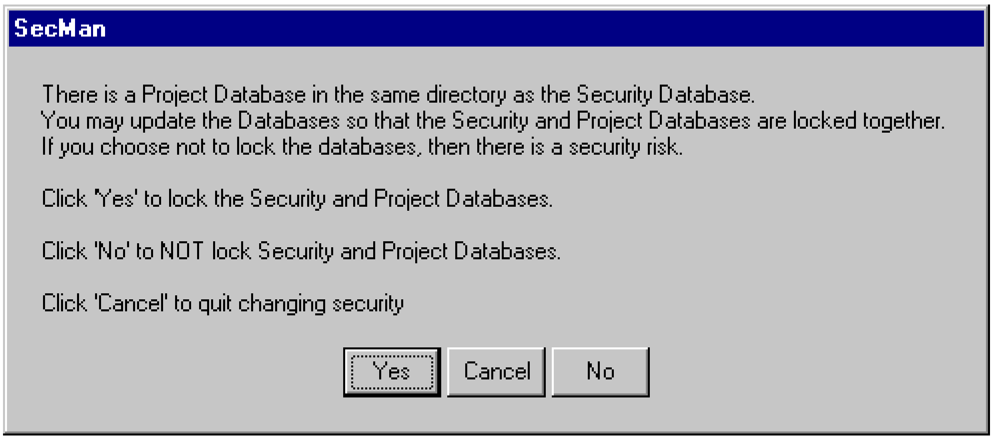


2. A dialog window to appears. Press ‘**Yes**’ to confirm or ‘**No**’ to cancel the operation.



Are you sure you wish to enable security ?

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.



There is a Project Database in the same directory as the Security Database.
You may update the Databases so that the Security and Project Databases are locked together.
If you choose not to lock the databases, then there is a security risk.

Click 'Yes' to lock the Security and Project Databases.

Click 'No' to NOT lock Security and Project Databases.

Click 'Cancel' to quit changing security

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

4.10 SAVE CHANGES

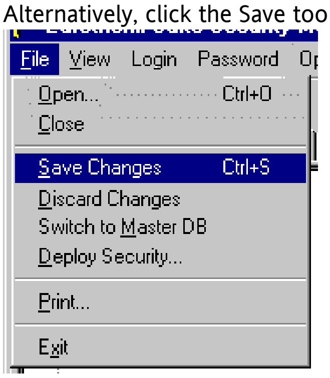
This function allows the User to save the configuration changes to the active database at the current location.

It is recommended that changes are saved at regular intervals.

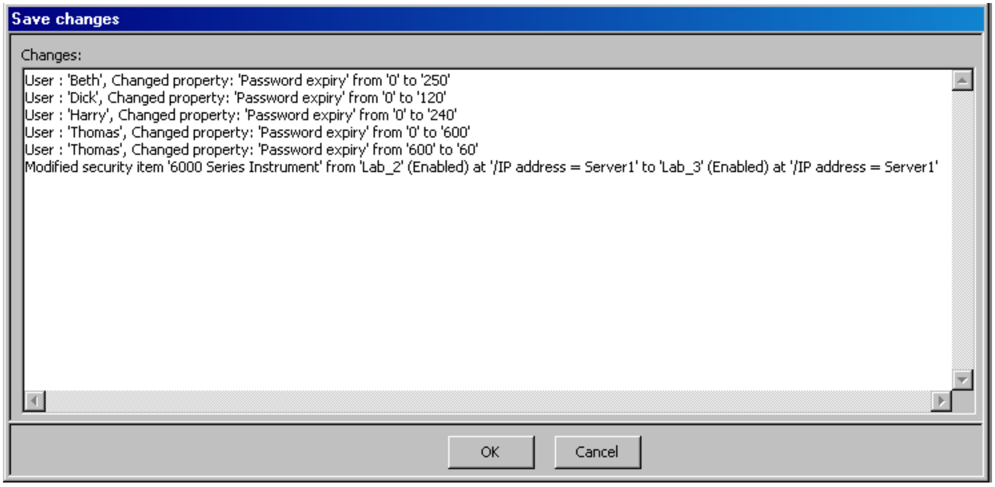
Save changes by,

1 Selecting '**File** > **Save'** from the Menu bar.

Alternatively, click the Save toolbutton.

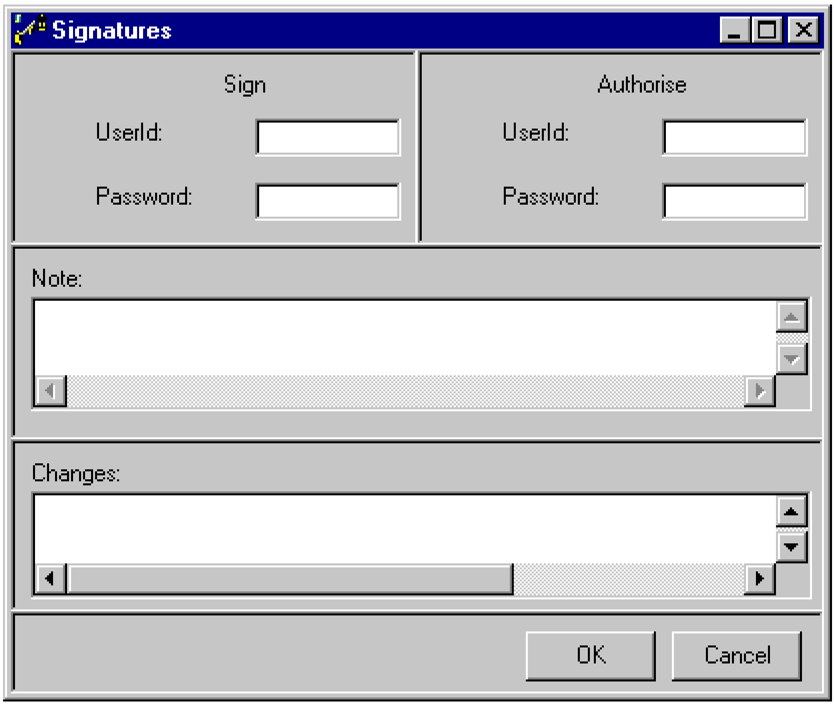


2 The save changes dialog window appears, press '**OK'** to save any changes. Press '**Cancel'** to return to the current Security Manager window without saving changes.



```
User : 'Beth', Changed property: 'Password expiry' from '0' to '250'
User : 'Dick', Changed property: 'Password expiry' from '0' to '120'
User : 'Harry', Changed property: 'Password expiry' from '0' to '240'
User : 'Thomas', Changed property: 'Password expiry' from '0' to '600'
User : 'Thomas', Changed property: 'Password expiry' from '600' to '60'
Modified security item '6000 Series Instrument' from 'Lab_2' (Enabled) at '/IP address = Server1' to 'Lab_3' (Enabled) at '/IP address = Server1'
```

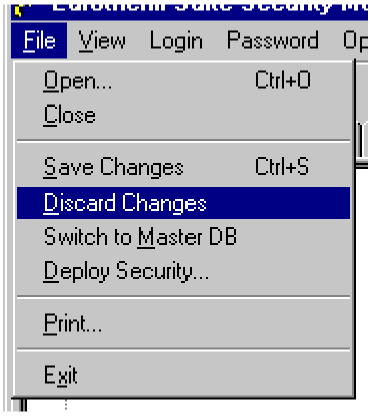
If the 'Sign', 'Authorise' and/or 'Note' Management Data and Access Rights have been configured via the Regulation menu, a window is displayed with the appropriate fields available. Press '**OK'** to save any changes, and '**Cancel'** to return to the current Security Manager window



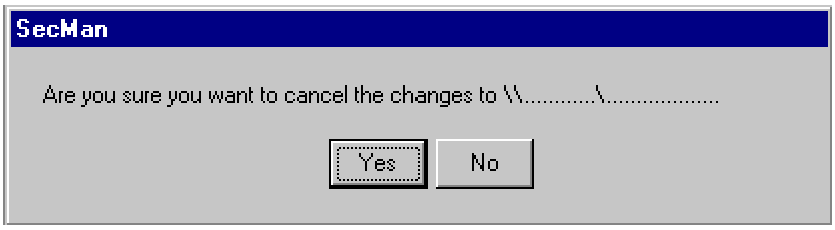
4.11 DISCARD CHANGES

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.



SecMan

Are you sure you want to cancel the changes to \\...........\..................

4.12 DEFINE THE REGULATION

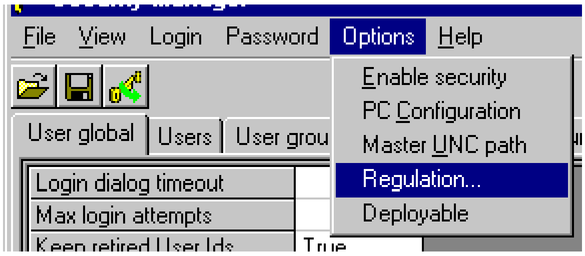
When setting the level of Regulation required a dialog window will appear. The required Regulation is configured by simply selecting the required Regulation from the drop down list provided.

Note

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

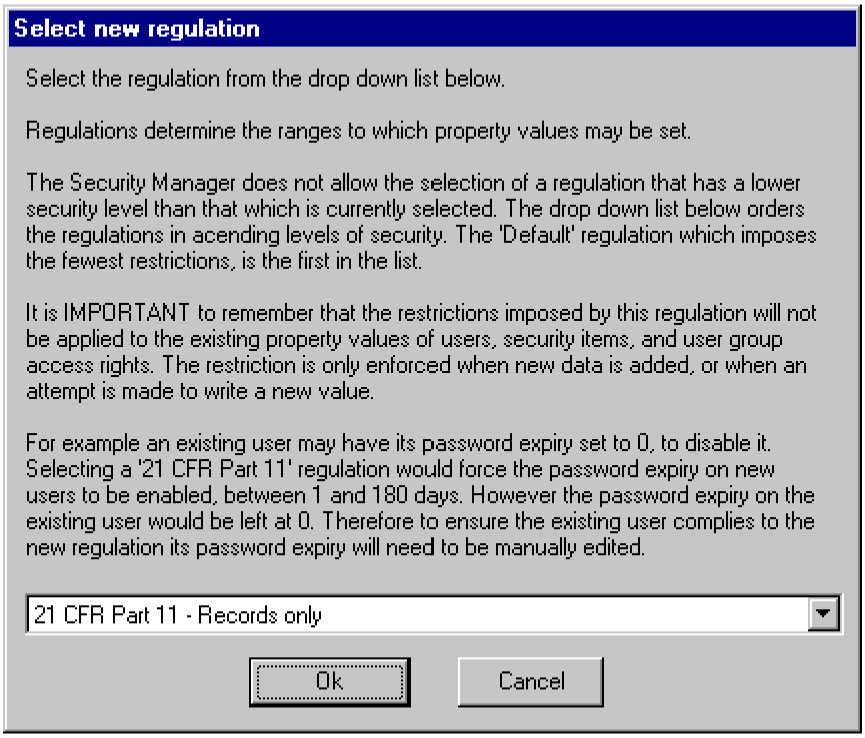
  This imposes the fewest restrictions on the parameters in the system.

- 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.



Select new regulation

Select the regulation from the drop down list below.

Regulations determine the ranges to which property values may be set.

The Security Manager does not allow the selection of a regulation that has a lower security level than that which is currently selected. The drop down list below orders the regulations in acending levels of security. The 'Default' regulation which imposes the fewest restrictions, is the first in the list.

It is IMPORTANT to remember that the restrictions imposed by this regulation will not be applied to the existing property values of users, security items, and user group access rights. The restriction is only enforced when new data is added, or when an attempt is made to write a new value.

For example an existing user may have its password expiry set to 0, to disable it. Selecting a '21 CFR Part 11' regulation would force the password expiry on new users to be enabled, between 1 and 180 days. However the password expiry on the existing user would be left at 0. Therefore to ensure the existing user complies to the new regulation its password expiry will need to be manually edited.

21 CFR Part 11 - Records only

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

4.13 EDIT THE USER GLOBAL TAB PARAMETERS

4.13.1 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

Note
This parameter only applies to the T800 and Eycon™ 10/20 Visual supervisors.

- 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

3. 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.

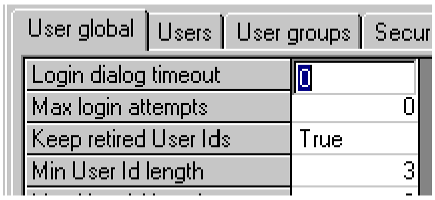
4.14 CHANGE THE LOGIN DIALOG TIMEOUT

Change the numeric value to increase or decrease the amount of time a Login prompt window will remain displayed before automatically logging out.

Note
This timeout value applies ONLY to Visual Supervisor Login dialogues.

1. Click the editable ‘Login dialog timeout’ field.

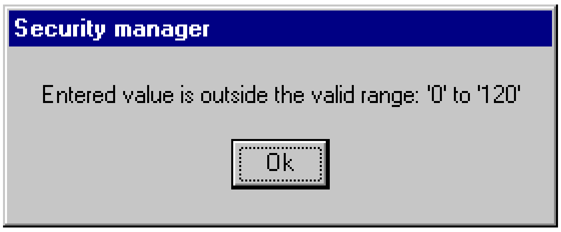
Note
The existing value is highlighted. If the value is NOT highlighted double click in the field.



Login dialog timeout	0
Max login attempts	0
Keep retired User Ids	True
Min User Id length	3

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.


Security manager

Entered value is outside the valid range: '0' to '120'

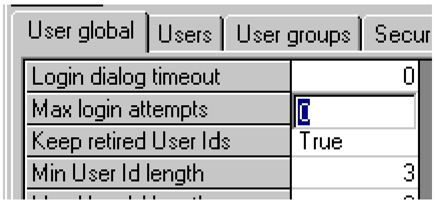
3. Finally save changes.

4.15 CHANGE THE MAXIMUM LOGIN ATTEMPTS

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

1. Click the editable ‘Maximum login attempts’ field.

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

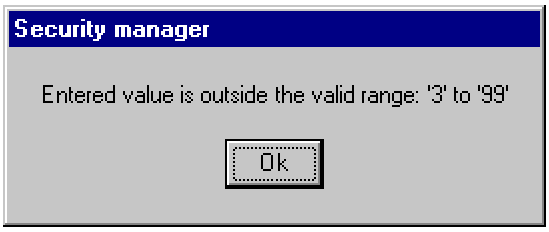


Login dialog timeout	0
Max login attempts	0
Keep retired User Ids	True
Min User Id length	3

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.


Security manager

Entered value is outside the valid range: '3' to '99'

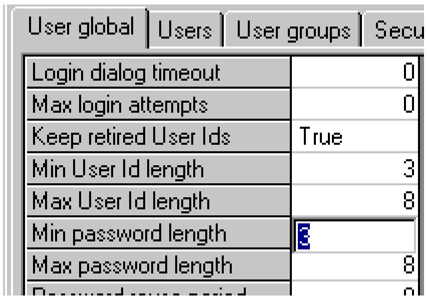
3. Finally save changes.

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

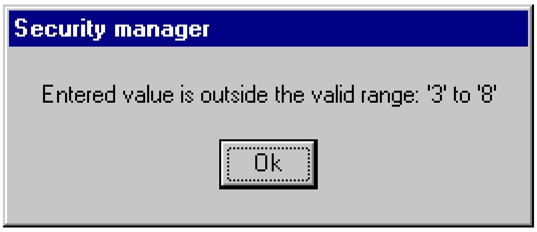


Login dialog timeout	0
Max login attempts	0
Keep retired User Ids	True
Min User Id length	3
Max User Id length	8
Min password length	3
Max password length	8

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.


Security manager

Entered value is outside the valid range: '3' to '8'

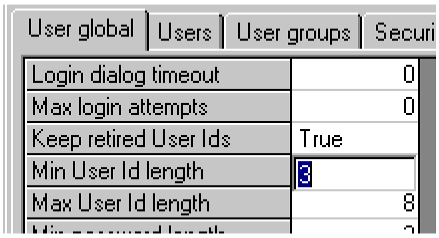
3. Finally save changes.

4.17 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.

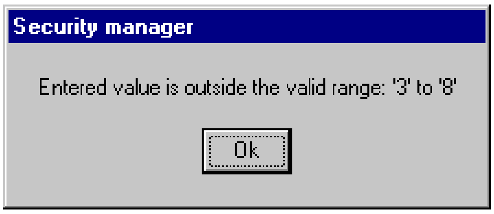
> **Note**
> The existing value is highlighted. If the value is NOT highlighted double click in the field.



Login dialog timeout	0
Max login attempts	0
Keep retired User Ids	True
Min User Id length	3
Max User Id 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.


Security manager

Entered value is outside the valid range: '3' to '8'

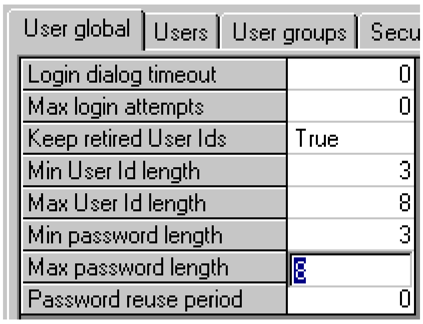
3. Finally save changes.

4.18 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.

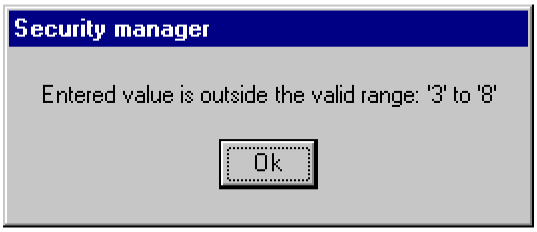
> Note: If the value is NOT highlighted double click in the field.



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.


Security manager

Entered value is outside the valid range: '3' to '8'

3. Finally save changes.

4.19 EDIT THE USER TAB PARAMETERS

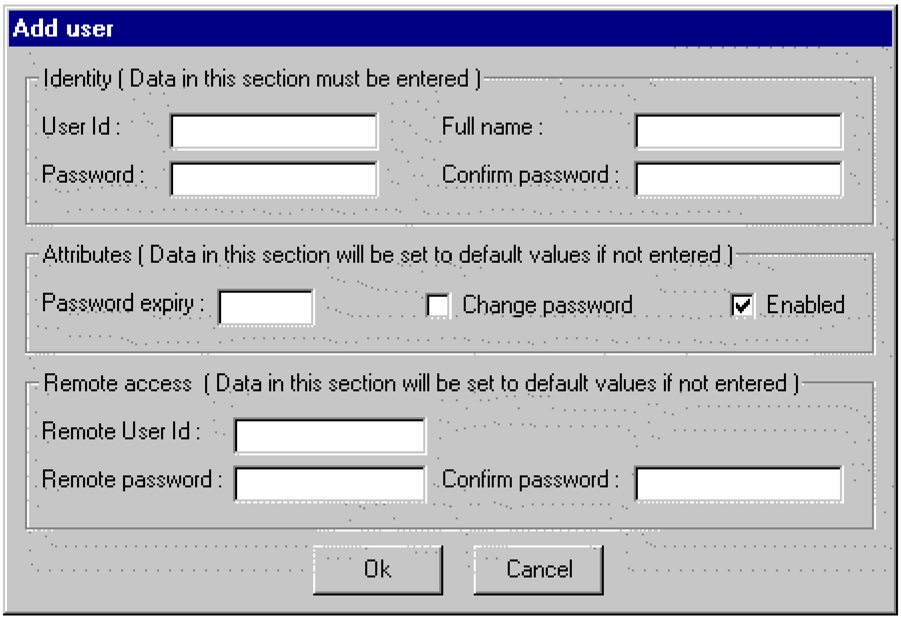
How to add a User

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.

Note:
In order to access Security Manager, Eurotherm Suite®, Review etc. software using a Remote Desktop (RDP) session, the user must also be added to the group able to run an RDP session (help from the user's local IT department may be needed).

Add a User by

1. Pressing Add user 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 **<u>ALL</u>** unsaved changes to be removed, including the User.

4. Finally save changes.

- If satisfied, the User can now be allocated to a User group.

4.20 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.

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 Add user. 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 Re-enable User 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 Domain 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.

4.20.1 How to show Active or All Users

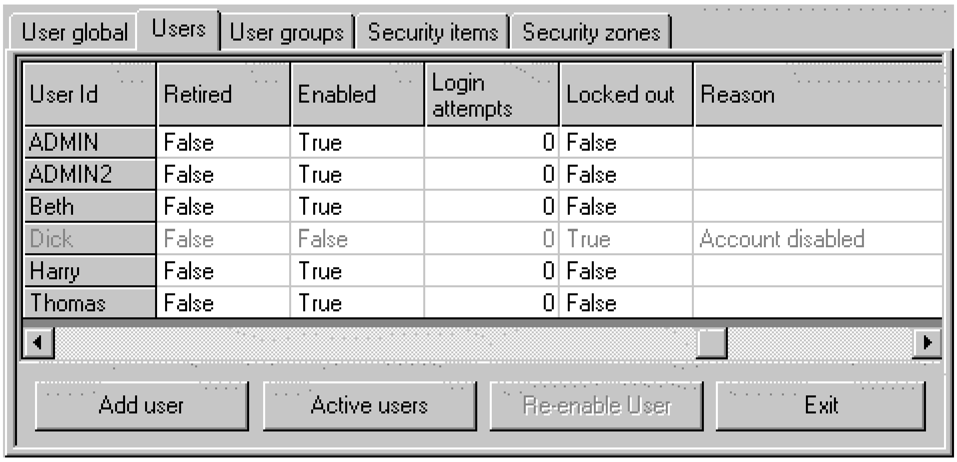
The function of this button allows the User to display ALL Users or just the Active Users in the User Id column.

DISPLAY ACTIVE OR ALL USERS BY

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

Note

If the tab was already showing just the **Active Users**, pressing All users 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.

4.21 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,

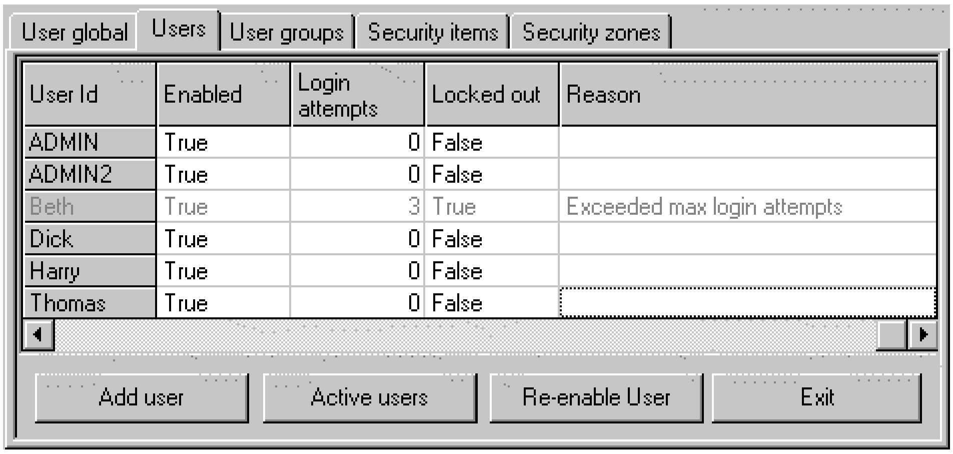
- User account has been disabled ('Enabled' field reads 'False', Reason field reads 'Account disabled')
- login attempts have been exceeded
- password has expired

Example

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

4.21.1 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.

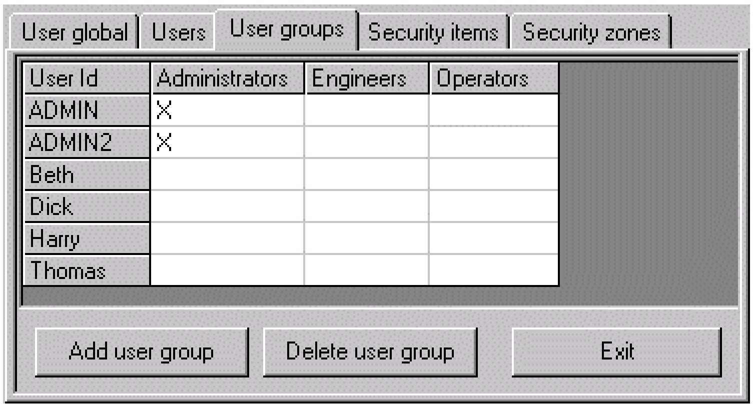
The User is now enabled.

4.22 EDIT THE USER GROUP TAB PARAMETERS

4.22.1 add a User group

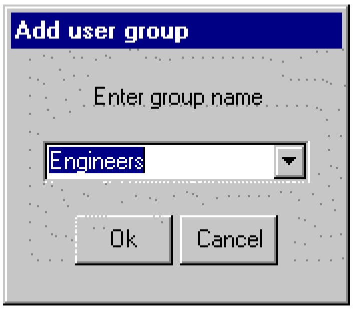
Assuming this tab is accessible, all User's are displayed in the left hand column. A new column is created each time a group is added. The group name is displayed at the top of each column.

ADD A USER GROUP BY



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

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

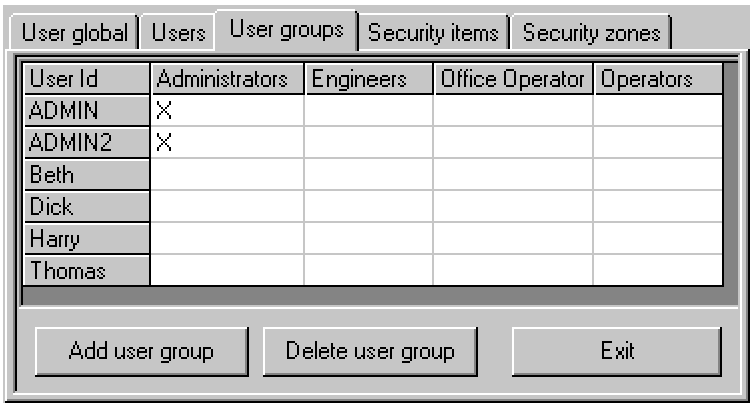


Engineers

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.



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

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.

4.23 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

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 Add user group. 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.

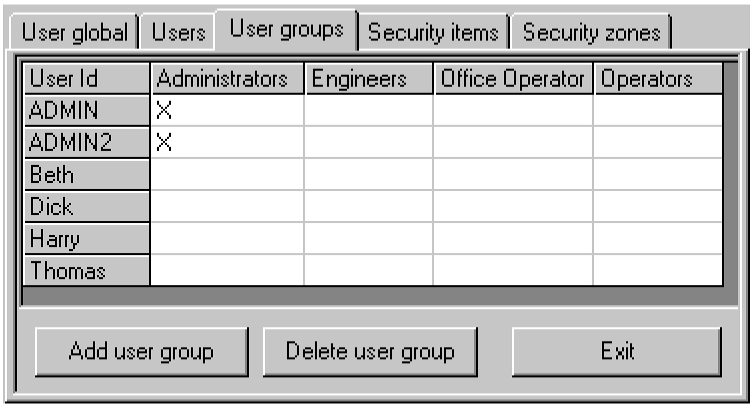
> **Note**
> Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

4.24 DELETE A USER GROUP

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

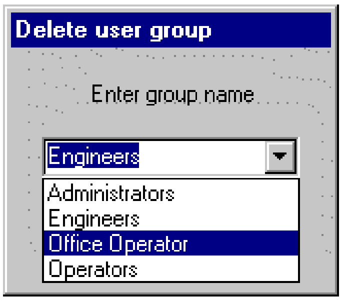
Note
All User accounts assigned to the deleted User group ONLY will remain in the database, but will lose any privileges configured for that User group.

Delete a User group by



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

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



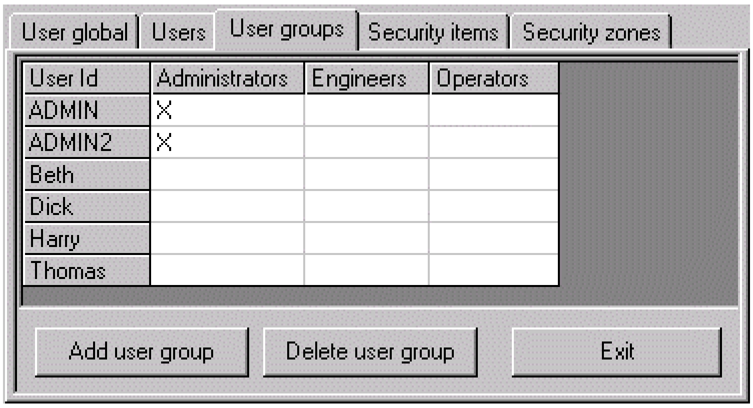
Engineers

Administrators
Engineers
Office Operator
Operators

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	Operators
ADMIN	X		
ADMIN2	X		
Beth			
Dick			
Harry			
Thomas			

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 Delete user group to remove a group added by error.

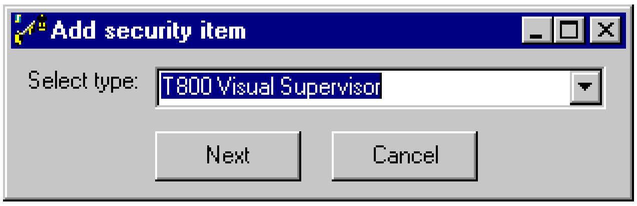
4.25 EDIT THE SECURITY ITEMS TAB PARAMETERS

4.25.1 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.



Select type: T800 Visual Supervisor

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 6000 Series, enter a unique 'Security item name' and 'I/P Address or Host name'. Furthermore, adding a 6000 Series instrument with Secure File Transfer Protocol (SFTP) enabled, requires additional configuration and involves the loading of a SFTP public key. For further information see *6000 Series Instrument (SFTP) - Add/Modify Security item*.
- 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 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.

4.26 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 Deploy to start the deployment wizard.
   - Alternatively, use toolbutton.

Note

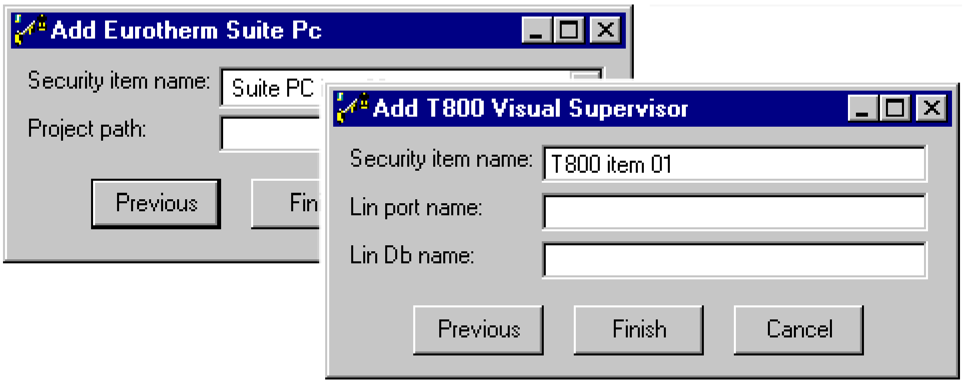
Starting the Deployment wizard will replicate the master Security database to selected items in the security configuration.

4.27 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 security item.

Modify a Security item by,

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


Add Eurotherm Suite Pc

Security item name: Suite PC

Project path:

Add T800 Visual Supervisor

Security item name: T800 item 01

Lin port name:

Lin Db name:

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

4.28 6000 SERIES INSTRUMENT (SFTP) - ADD/MODIFY SECURITY ITEM

As additional instruments are added to an infrastructure, they will need to be added into the Security Manager application.

The **Add 6000 Series Instrument** dialog enables Security Manager users to add a 6000 Series instrument as a security item and configure:

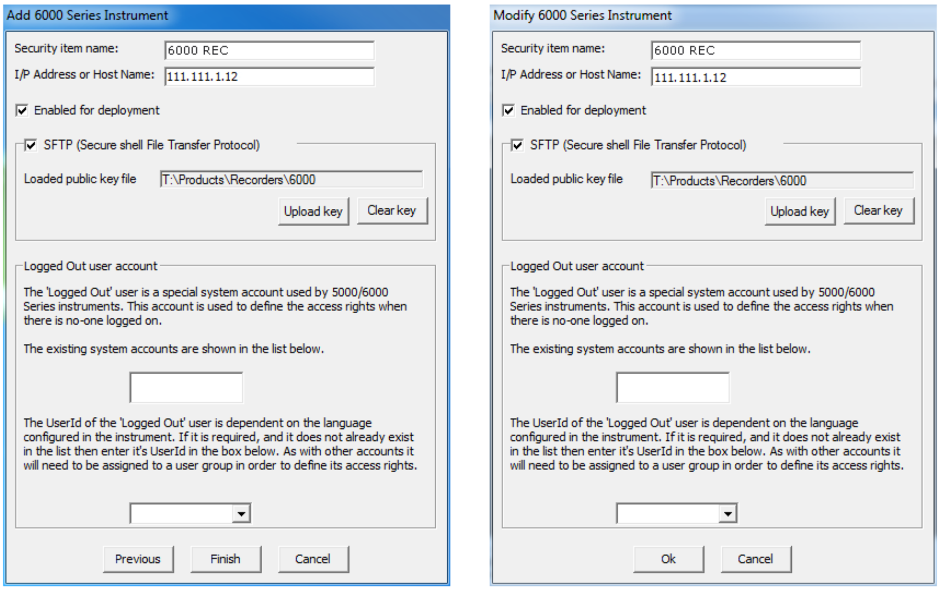
- the Security item name and IP address or Host Name
- the Secure FTP (SFTP) option, if utilized and import the SFTP public Key
- the 6000 Series Logged Out users' access rights

The **Modify 6000 Series Instrument** dialog allows users to edit existing security items.

To display the:

- **Add 6000 Series Instrument** dialog, select the *Security item*s tab > select *Add security item* button > select *6000 Series Instrument* option from the *Add security item* dialog > click *Next*. The *Add 6000 Series Instrument* dialog appears.
- **Modify 6000 Series Instrument** dialog, select the *Security items* tab > select from the existing security items list *Type*: *6000 Series Instrument* > select the *Modify security item* button. The *Modify 6000 Series Instrument* dialog appears.

Add and Modify 6000 Series Instrument dialogs



Add 6000 Series Instrument

Security item name: 6000 REC

I/P Address or Host Name: 111.111.1.12

☑ Enabled for deployment

☑ SFTP (Secure shell File Transfer Protocol)

Loaded public key file: T:\Products\Recorders\6000

Upload key | Clear key

Logged Out user account

The 'Logged Out' user is a special system account used by 5000/6000 Series instruments. This account is used to define the access rights when there is no-one logged on.

The existing system accounts are shown in the list below.

The UserId of the 'Logged Out' user is dependent on the language configured in the instrument. If it is required, and it does not already exist in the list then enter it's UserId in the box below. As with other accounts it will need to be assigned to a user group in order to define its access rights.

Previous | Finish | Cancel

Modify 6000 Series Instrument

Security item name: 6000 REC

I/P Address or Host Name: 111.111.1.12

☑ Enabled for deployment

☑ SFTP (Secure shell File Transfer Protocol)

Loaded public key file: T:\Products\Recorders\6000

Upload key | Clear key

Logged Out user account

The 'Logged Out' user is a special system account used by 5000/6000 Series instruments. This account is used to define the access rights when there is no-one logged on.

The existing system accounts are shown in the list below.

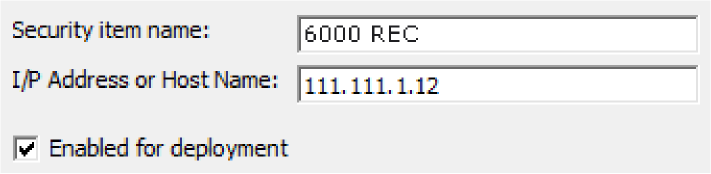
The UserId of the 'Logged Out' user is dependent on the language configured in the instrument. If it is required, and it does not already exist in the list then enter it's UserId in the box below. As with other accounts it will need to be assigned to a user group in order to define its access rights.

Ok | Cancel

The Add 6000 Series Instrument (left figure) and Modify 6000 Series Instrument (right figure) dialogs are similar.

The dialog has three sections to add, configure or modify the 6000 Series security items;

Security item Name & Address



Security item name: 6000 REC

I/P Address or Host Name: 111.111.1.12

☑ Enabled for deployment

Security item name	Add or modify the security item name. (The Security item name should be unique).
IP Address or Host Name	Add or modify the instruments' IP address or Host name.
Enabled for deployment (check box)	Select to make the security item deployable.

Secure FTP (SFTP)

When a 6000 Recorder is shipped, Secure FTP (SFTP) will be enabled by default.

Any application or device that needs to communicate, transfer data and files to a 6000 recorder with SFTP enabled will need to be SFTP configured. The configuration requires the uploading of the target recorder's SFTP public key.

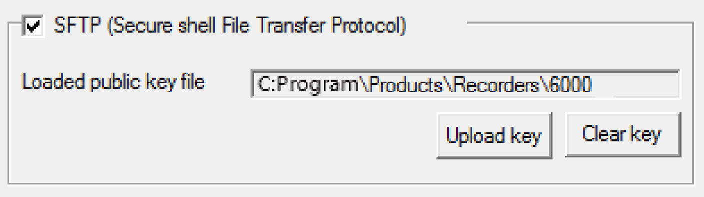
To obtain the recorder's SFTP public key, log in to the 6000 as an Engineer and select the *Export Public Key* option. This will copy the public key (sshkey.pub) to the *User* folder (or saved directly to an inserted USB stick). If saved in the *User* folder the public key can either be copied directly onto a USB stick, or copied using an FTP client (i.e. FileZilla).

If the file format is correct it will upload, if incorrect an error dialog will appear.

IMPORTANT NOTE: If the SFTP public key format is valid but from a different 6000 instrument, the upload will succeed but Security Manager will fail to communicate with the instrument and a connection error will be recorded in the service Log.

Each SFTP public key is unique and specific to the 6000 instrument that generates it, so when adding or modifying a 6000 Series security item, ensure the SFTP public key being uploaded originates from the same 6000 recorder.

Note: All changes to the configuration of the public key are logged to the UHH audit trail.



☑ SFTP (Secure shell File Transfer Protocol)

Loaded public key file: C:Program\Products\Recorders\6000

SFTP (Secure Shell File Transfer Protocol), check box

To enable Secure FTP, check the SFTP (Secure shell File Transfer Protocol) check box.

Once this option is checked, the 6000 recorder's SFTP public key will be required. Ensure you have a copy available to upload.

Note: If Secure FTP is disabled the loaded public key text and associated buttons will be disabled and greyed out.

Loaded public key file

Displays the location and file path of the Secure FTP public key file that has been uploaded.

Upload key (button)

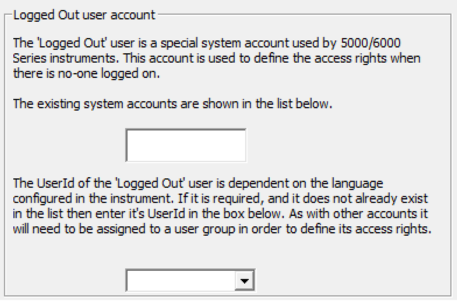
When selected, opens a browser to select the public key file.

Clear key (button)

When selected, deletes the existing SFTP public key file.

For example, if an incorrect SFTP public key is loaded, or a 6000 recorder's public key has been generated (renewed), then the existing one in Security Manager will be out of date and will require deleting.

Logged Out user account



Logged Out user account

The 'Logged Out' user is a special system account used by 5000/6000 Series instruments. This account is used to define the access rights when there is no-one logged on.

The existing system accounts are shown in the list below.

The UserId of the 'Logged Out' user is dependent on the language configured in the instrument. If it is required, and it does not already exist in the list then enter it's UserId in the box below. As with other accounts it will need to be assigned to a user group in order to define its access rights.

Drop down menu:

Existing system accounts

Select from the *Logged Out user account* drop down menu the system account to set the access rights and available recorder functions when no one is logged on to the recorder.

User ID

Select the user from the *User ID* drop down menu, to configure as an identifiable 'logged out' user. The User ID is dependant on the language configured in the instrument, if a User ID does not exist, enter one. The User ID will need to be assigned to a User group to define access rights.

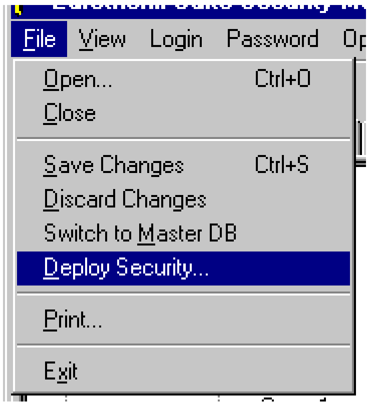
Add 6000 Series dialog buttons:

Previous	Select to cancel the *Add 6000 Series Instrument* panel and returns to the initial *Add security item* panel.
Finish	Select to finish adding a 6000 Series Instrument.
Cancel	Select to cancel and dismiss the *Add 6000 Series Instrument* panel and returns to Security Manager's panel.

Modify 6000 Series dialog buttons:

Ok	Select to commit and enter any modifications made to a 6000 Series security item.
Cancel	Select to cancel and dismiss the *Modify 6000 Series Instrument* dialog and return to Security Manager's panel.

4.29 DEPLOY TO SELECTED SECURITY ITEMS



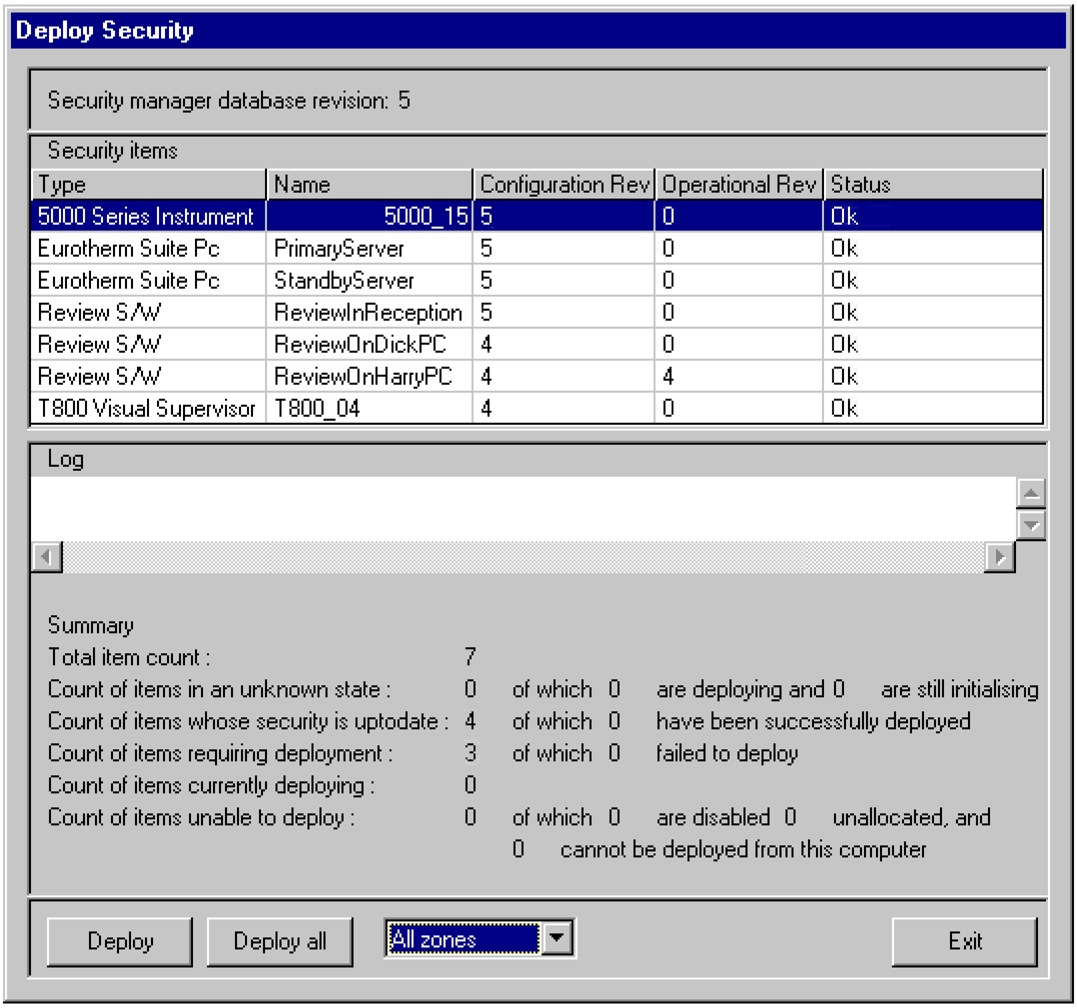
The deployment of the master Security database can be initiated by either

- Clicking the on the Toolbar,
- Clicking the ‘Deploy Security’ button available via the Security items tab, or
- Selecting **‘Menu Bar > File > Deploy Security...’**.

1. After selecting ’**Deploy Security**’ using one of methods indicated above, the Deploy Security window is displayed.

Note

If more than 100 users are deployed to a 5000/6000 recorder, the deployment could fail.



Deploy Security

Security manager database revision: 5

Security items

Type	Name	Configuration Rev	Operational Rev	Status
5000 Series Instrument	5000_15	5	0	Ok
Eurotherm Suite Pc	PrimaryServer	5	0	Ok
Eurotherm Suite Pc	StandbyServer	5	0	Ok
Review S/W	ReviewInReception	5	0	Ok
Review S/W	ReviewOnDickPC	4	0	Ok
Review S/W	ReviewOnHarryPC	4	4	Ok
T800 Visual Supervisor	T800_04	4	0	Ok

Log

Summary
Total item count : 7
Count of items in an unknown state : 0 of which 0 are deploying and 0 are still initialising
Count of items whose security is uptodate : 4 of which 0 have been successfully deployed
Count of items requiring deployment : 3 of which 0 failed to deploy
Count of items currently deploying : 0
Count of items unable to deploy : 0 of which 0 are disabled 0 unallocated, and
0 cannot be deployed from this computer

2. Click the appropriate ‘Deploy’ or ‘Deploy all’ button to continue.

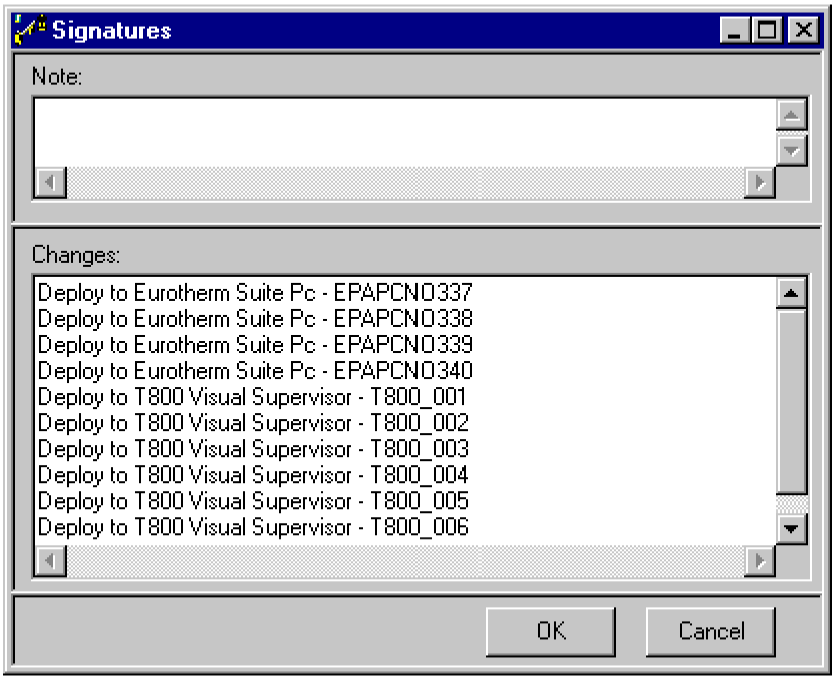
Note

This button 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’.



Deploy to Eurotherm Suite Pc - EPAPCN0337
Deploy to Eurotherm Suite Pc - EPAPCN0338
Deploy to Eurotherm Suite Pc - EPAPCN0339
Deploy to Eurotherm Suite Pc - EPAPCN0340
Deploy to T800 Visual Supervisor - T800_001
Deploy to T800 Visual Supervisor - T800_002
Deploy to T800 Visual Supervisor - T800_003
Deploy to T800 Visual Supervisor - T800_004
Deploy to T800 Visual Supervisor - T800_005
Deploy to T800 Visual Supervisor - T800_006

- 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 Exit to return to the Deploy Security window.

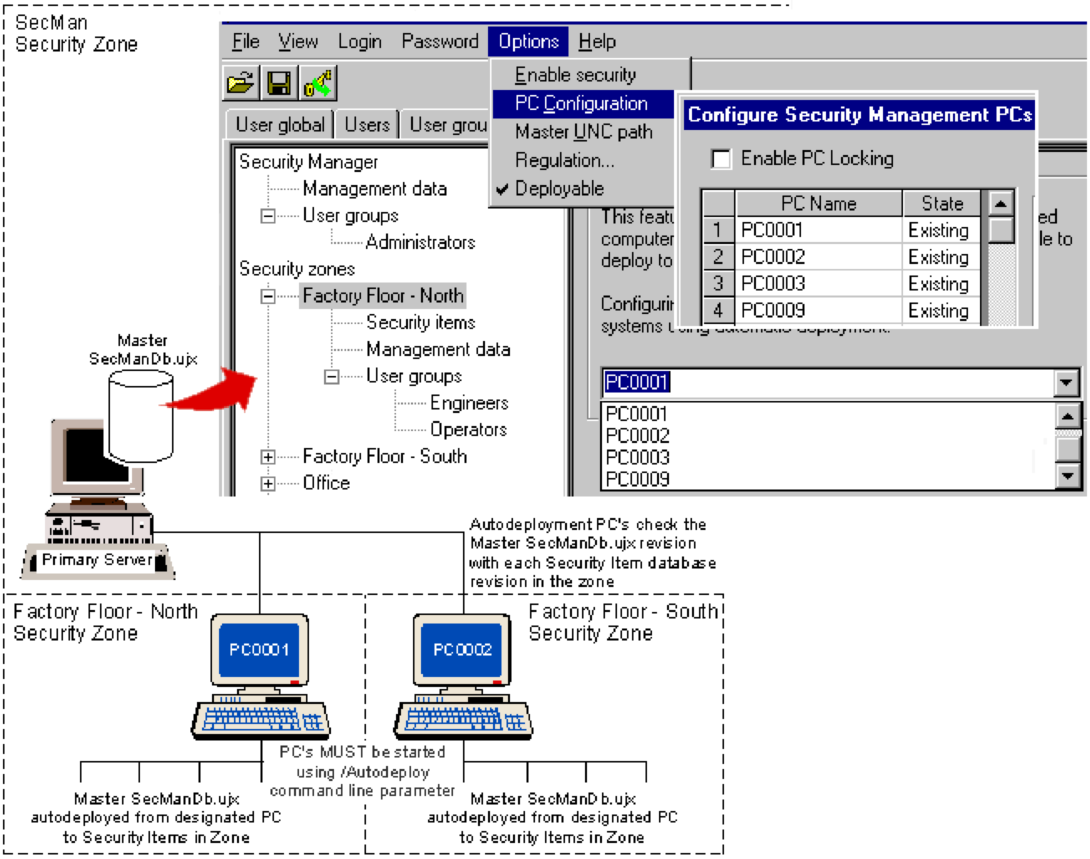
4.29.1 What is Deployment?

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 - DEPLOYMENT COMPUTER CONFIGURATION

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



	PC Name	State
1	PC0001	Existing
2	PC0002	Existing
3	PC0003	Existing
4	PC0009	Existing

4.30 EDIT THE SECURITY ZONES TAB PARAMETERS

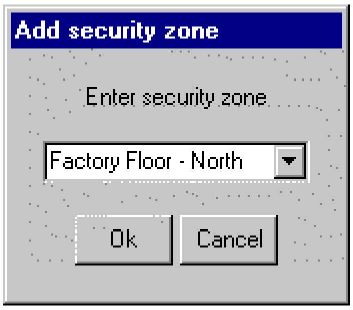
4.30.1 add a Security zone

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 be added only when the zone list is displayed in the Properties pane.

Add a zone by

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



Add security zone

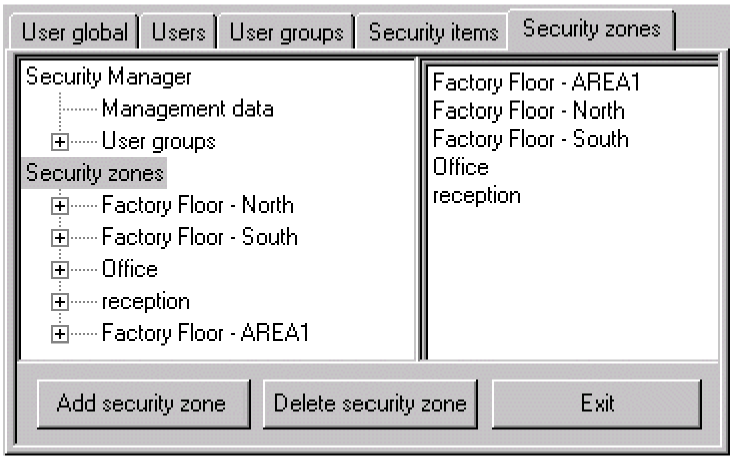
Enter security zone

Factory Floor - North

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



Security Manager
- Management data
- ⊞ User groups

Security zones
- ⊞ Factory Floor - North
- ⊞ Factory Floor - South
- ⊞ Office
- ⊞ reception
- ⊞ Factory Floor - AREA1

Factory Floor - AREA1
Factory Floor - North
Factory Floor - South
Office
reception

4. Finally save changes.

- Now allocate ‘Security items’ or ‘User groups’ or alternatively delete a Security Zone’.

4.31 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.

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 Add Security Zone. 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
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
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.

4.32 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

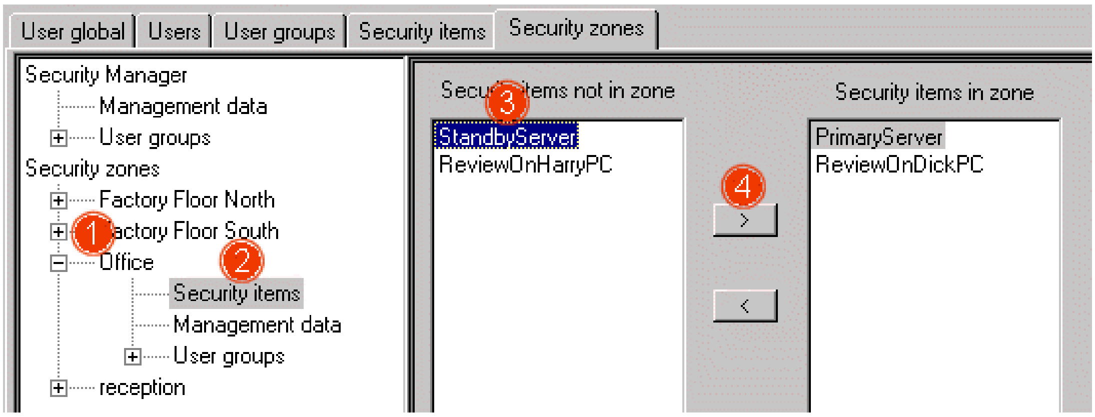
- 'not in zone' (left hand column), (Unallocated)
- 'in zone' (right hand column is initially empty). All allocated items are displayed in this column.

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.

4.33 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.

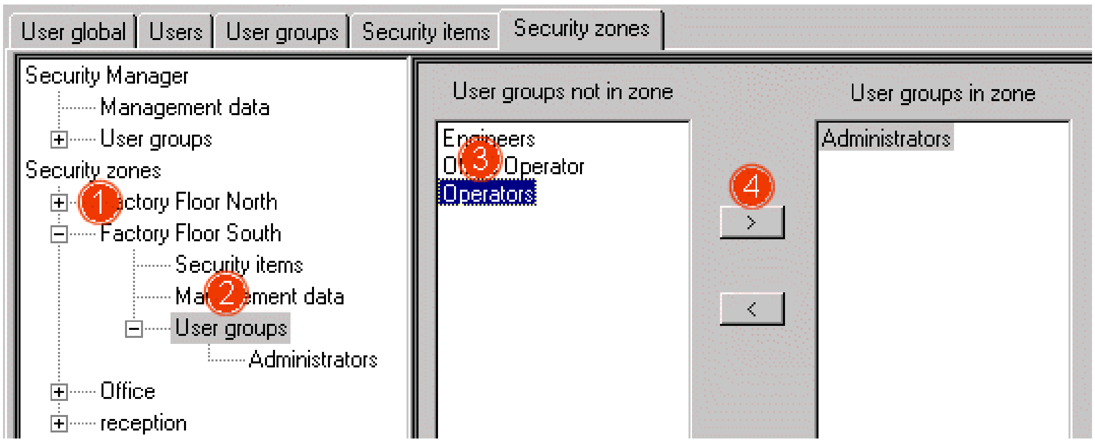
2. In the Navigation pane click the **User groups** heading.
   Observe the Properties pane divides into two columns, a list of all the user groups

- 'not in zone' (left hand column), (Unallocated)
- 'in zone' (right hand column is initially empty). All allocated groups are displayed in this column

3. Click on a User group from the 'not in zone' column.

4. 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.



5. After successfully allocating the User groups to the appropriate Security zones, save changes and proceed with configuring the User operations.

4.34 RENAME A SECURITY ZONE

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

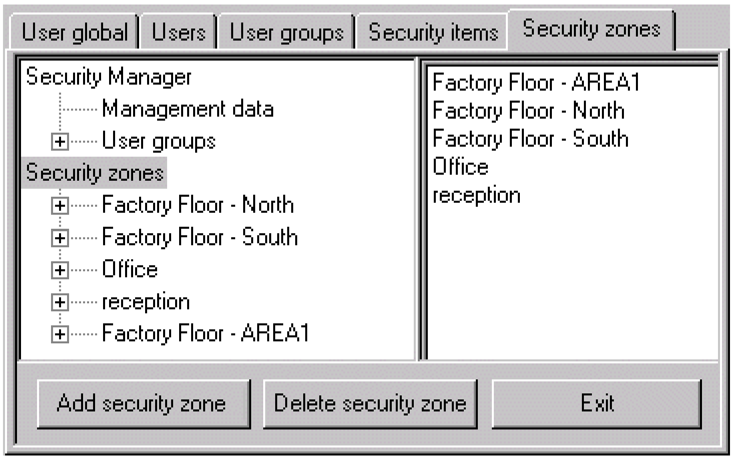
> **Note**
> Security zones names must be unique. Any attempt to duplicate Security zone names will display a failure dialog, and cancel the operation.

4.35 DELETE A SECURITY ZONE

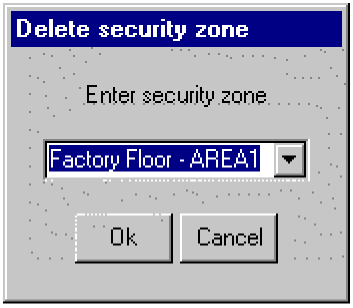
Deleting a Security zone removes the configured Management Data and Access Rights for the allocated groups and items. If Security items or User groups are allocated to only this deleted zone they need to be re-allocated and all configurations revert to the default parameters. If allocated to another 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



1. 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.

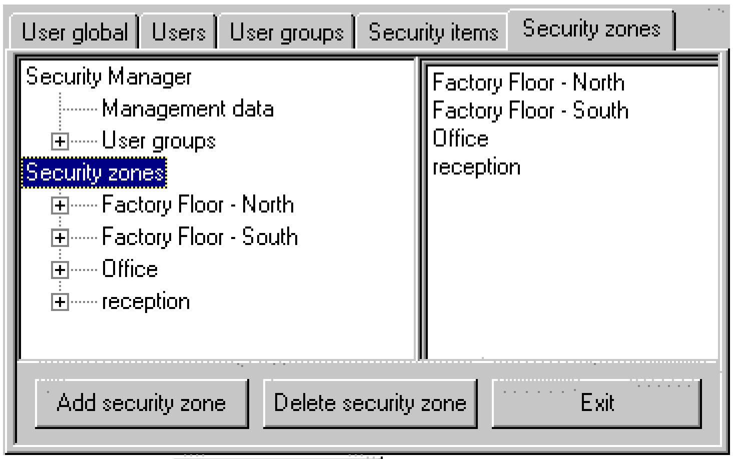


Enter security zone
Factory Floor - AREA1

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

Note

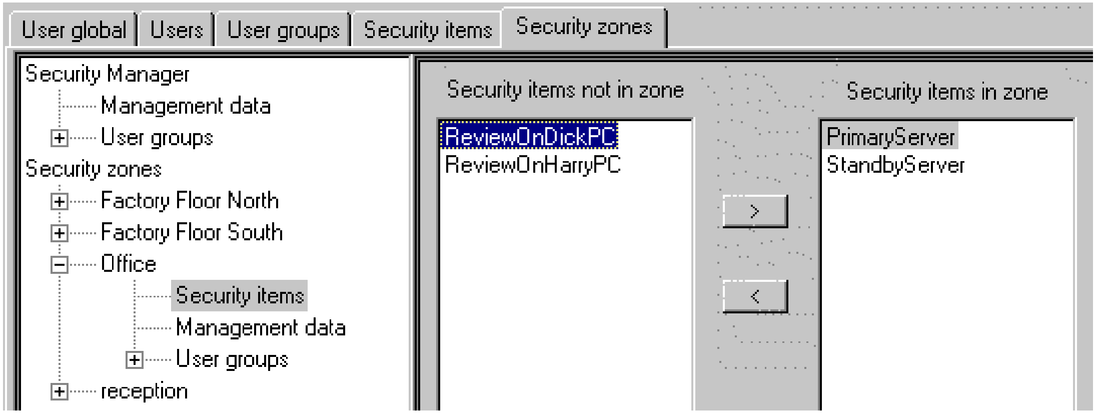
If '**Ok**' was selected observe the Security zone name is removed to the tab.



3. Press the button.
4. Finally save changes.

4.35.1 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.



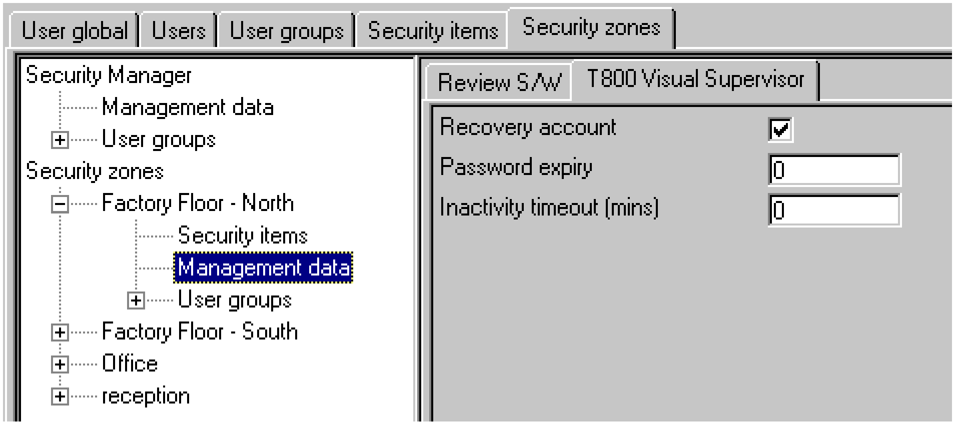
Security items not in zone	Security items in zone
ReviewOnDickPC	PrimaryServer
ReviewOnHarryPC	StandbyServer

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.

4.35.2 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.



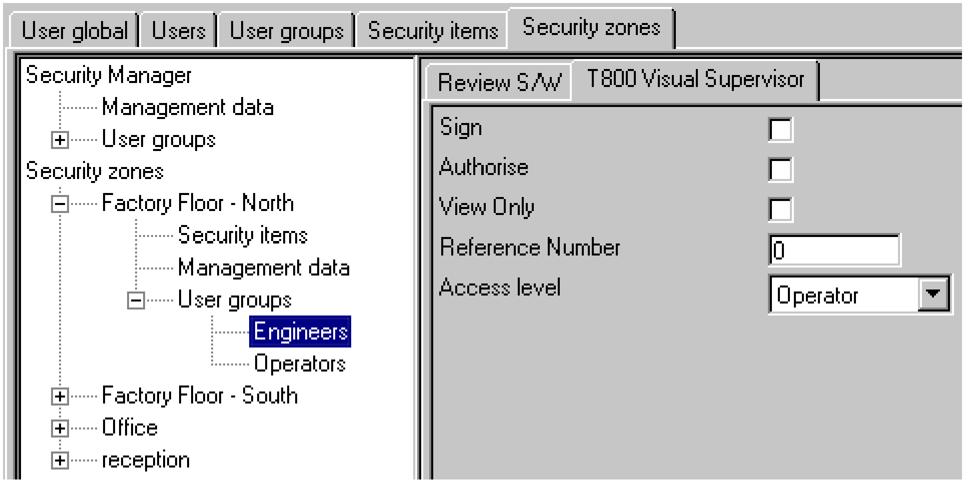
Recovery account ☑

Password expiry 0

Inactivity timeout (mins) 0

4.35.3 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.



Sign □

Authorise □

View Only □

Reference Number 0

Access level Operator

edit the Security Manager permissions

4.36 EDIT THE SERVICE TAB PARAMETERS

4.36.1 Install the Service

At Installation you can configure the following items:

- the Security Manager's Service user account details (Domain, User name, Password)
- the Service functions *Auto deployment, Active Directory monitoring* and *pre-Windows 2000 user logon name*

For further details, see *How to install and configure the Service*.

4.36.2 enable and configure Automatic deployment

Once the Security Manager's Service is configured and the *Automatic deployment* function is enabled and configured the Service will:

- deploy the Security Manager's database configuration automatically, to and from all Security items (known as *Deployment*)
- deploy repeatedly, at a configurable time interval measured in minutes. For example an *Automatic deployment rate* of 10 minutes would result in the Service deploying security events every 10 minutes
- remove the need to manually deploy (though still available)

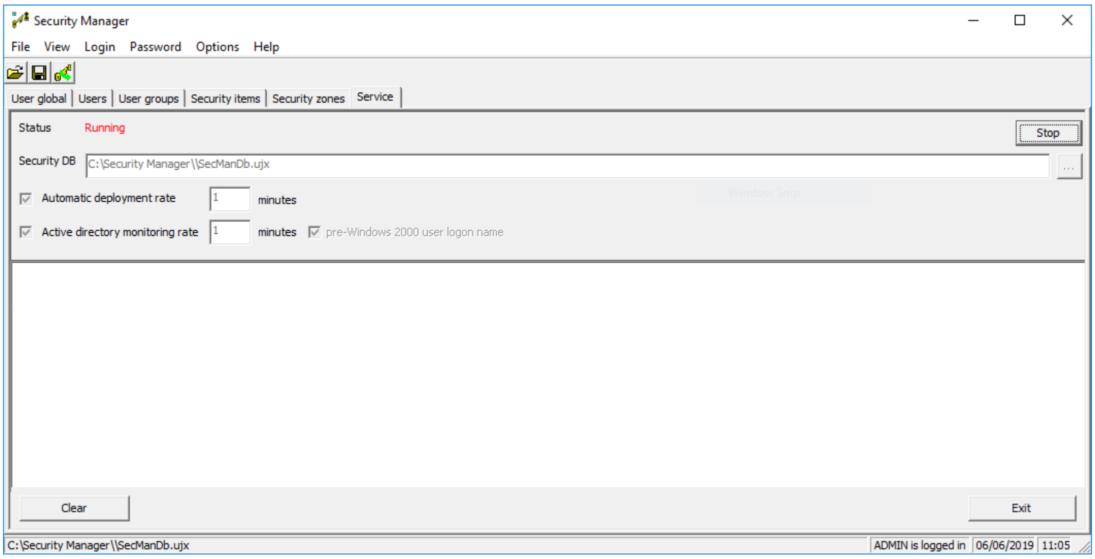
The *Automatic deployment rate* is the time interval (measured in minutes), each time the Service:

- checks the security version on all security items against the Security Manager's Master DB
- deploys any changes to both security items and any back to the Master DB

The *Automatic deployment rate* is measured in minutes, is user configurable and by default is 5 minutes.

For example, a user locking themselves out on their local recorder would be reconciled back up to Security Manager database, and in turn the Service would deploy the user 'lock out' change to all other configured security items, at the configured time interval.

To enable and configure Automatic deployment



Status Running

Security DB C:\Security Manager\\SecManDb.ujx

☑ Automatic deployment rate 1 minutes

☑ Active directory monitoring rate 1 minutes ☑ pre-Windows 2000 user logon name

C:\Security Manager\\SecManDb.ujx | ADMIN is logged in | 06/06/2019 | 11:05

1. With the Service running, select and click *Stop*.
2. Select and check the following check box, located below the Security DB text box:
   - Automatic deployment rate
3. Enter a time value (in minutes), to the right of the *Automatic deployment rate* check box. (The default is 5 minutes).
4. Click the *Start* button (top right) to apply the change and start the Service running.

4.36.3 enable and configure Active Directory monitoring

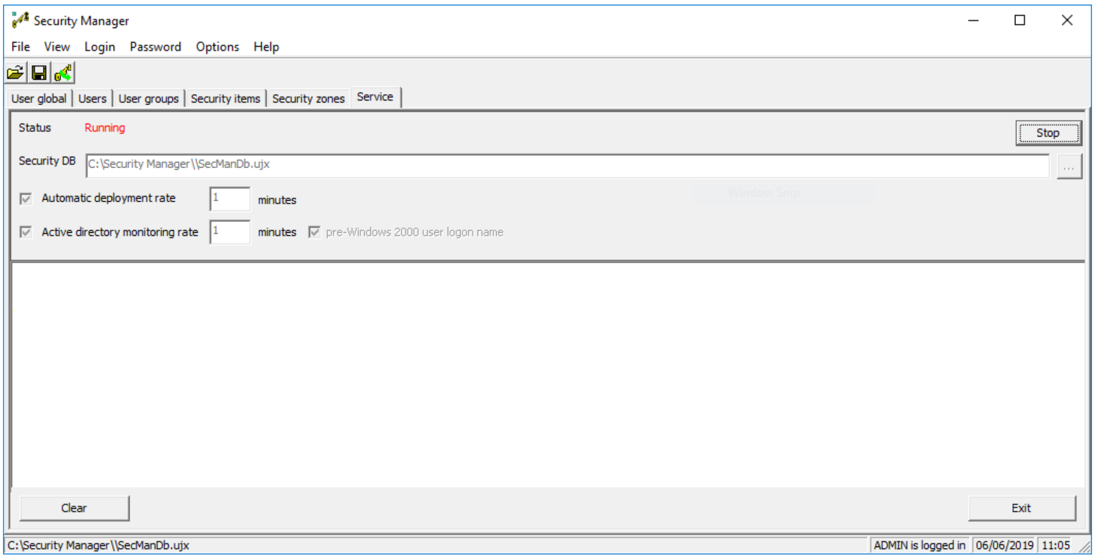
Note: The following feature is only applicable if you have created a User group that is linked to an Active Directory.

Once the Security Manager Service is installed and the *Active Directory monitoring* function been enabled the Service will:

- Automatically monitor the Active Directory used to import users into the Security Manager database (see *Import Users from Active Directory*)

The *Active Directory monitoring rate* is the time interval between each time the Service checks the linked directory for any changes. The rate is measured in minutes and is user configurable. (The default is 5 minutes).

To enable and configure Active Directory monitoring


Security Manager
File View Login Password Options Help
User global | Users | User groups | Security items | Security zones | Service
Stop
...
Clear
Exit

Status Running

Security DB C:\Security Manager\\SecManDb.ujx

☑ Automatic deployment rate 1 minutes

☑ Active directory monitoring rate 1 minutes ☑ pre-Windows 2000 user logon name

C:\Security Manager\\SecManDb.ujx | ADMIN is logged in | 06/06/2019 | 11:05

1 With the Service running, select and click *Stop*.

2 Select and check the following check box, located below the Security DB text box;

- Active Directory monitoring rate

3 Enter a time value (in minutes), the default is 5 minutes.

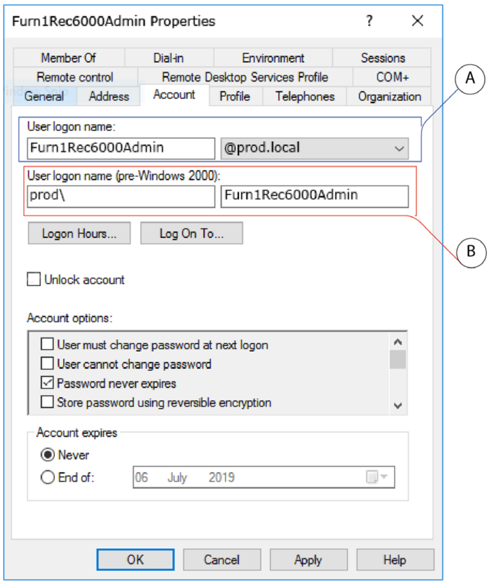
4 Click the *Start* button (top right) to apply the change and start the Service running.

4.36.4 enable Active directory pre-Windows 2000 User logon names

Users, or more specifically User Accounts can be imported into the Security Manager application from a Active Directory, see *Import Users from Active Directory*.

Active Directory user accounts have 2 variations of User logon name;

- User logon name (A in below image)
- User logon name (pre-Windows 2000) - (B in below image)



User logon name:
Furn1Rec6000Admin @prod.local

User logon name (pre-Windows 2000):
prod\ Furn1Rec6000Admin

□ Unlock account

Account options:

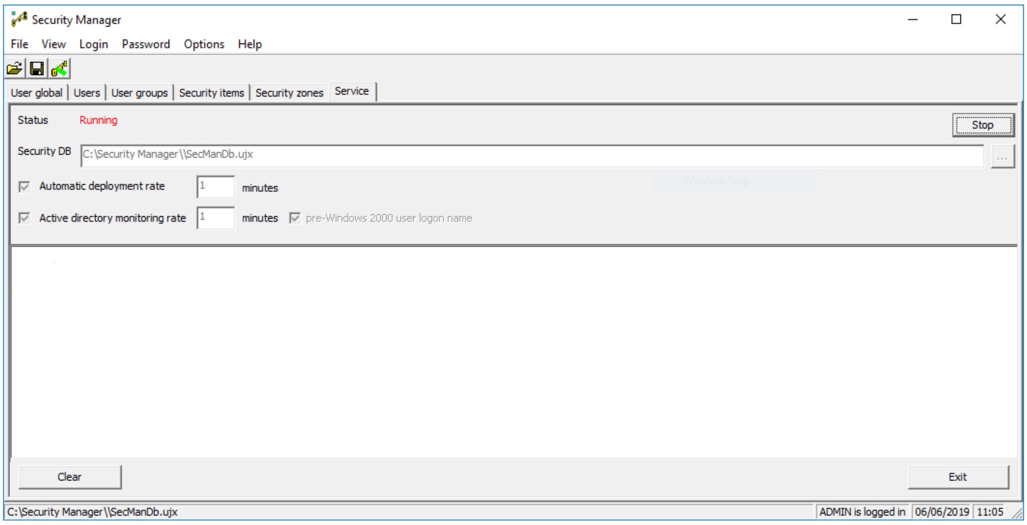
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: 06 July 2019

The *pre-Windows 2000 user logon name* function allows the Security Manager to only refer to and use the pre Windows 2000 User logon name and details. (See option B in above image).

Note: The pre-Windows 2000 user logon name, also requires the option Active Directory monitoring to be enabled.

To enable the pre-Windows 2000 user logon name



Status Running

Security DB C:\Security Manager\\SecManDb.ujx

☑ Automatic deployment rate 1 minutes

☑ Active directory monitoring rate 1 minutes ☑ pre-Windows 2000 user logon name

C:\Security Manager\\SecManDb.ujx | ADMIN is logged in | 06/06/2019 | 11:05

1. With the Service running, select and click *Stop*.
2. Select and check the following check boxes, located below the *Security DB* text box;
   - Active Directory monitoring rate
   - pre-Windows 2000 user logon name, to use only the pre Windows 2000 Logon name
3. Click the Start button (top right) to apply the change and start the Service running.

4.37 EDIT THE SECURITY MANAGER PERMISSIONS

4.37.1 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 be edited only 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

4.37.2 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 be edited only 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

4.37.3 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 be edited only 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

4.37.4 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 be edited only 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 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 be edited only 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 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

4.37.5 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 be edited only 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

4.37.6 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 be edited only 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 be edited only 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)

4.37.7 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 be edited only 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 be edited only 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)

4.37.8 edit Visual Supervisor permissions

CONFIGURE THE T800 OR EYCON™ 10/20 VISUAL SUPERVISOR MANAGEMENT DATA

The Visual Supervisor is configured to allow the user access to sufficient features to perform all expected tasks.

> It is recommended that a client database should be edited only in exceptional circumstances. Use the pulldown '*File* > Switch to MasterDB' to open the master database.

To configure this

Selecting a zone name from the Navigation pane displays the Visual Supervisor tab with the following fields in the Properties pane.
Recovery account
Password Expiry
Inactivity timeout (ms)

CONFIGURE THE T800 OR EYCON™ 10/20 VISUAL SUPERVISOR ACCESS RIGHTS

The Visual Supervisor is configured to grant the user sufficient access rights to perform all expected tasks.

> It is recommended that *a* client database should be edited only 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 displays the 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

4.37.9 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 be edited only 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 be edited only 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

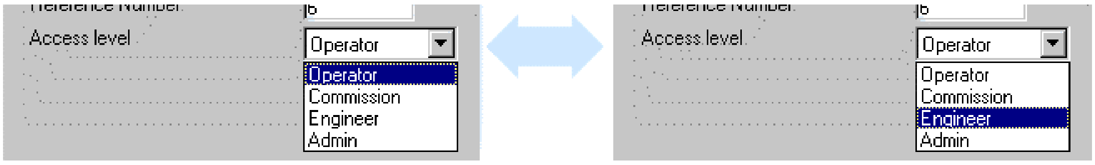
4.38 CONFIGURE SECURITY ITEM PARAMETERS

4.38.1 configure the Access level access rights

This field allows the User to specify the security Access level required to read or write to Visual Supervisor item types. Any User attempting to use the 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 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.

4.38.2 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.

4.38.3 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.

4.38.4 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.

4.38.5 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 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.

4.38.6 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.

4.38.7 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.

4.38.8 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.
2. At the keyboard, enter the required UserId and press the return key.

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

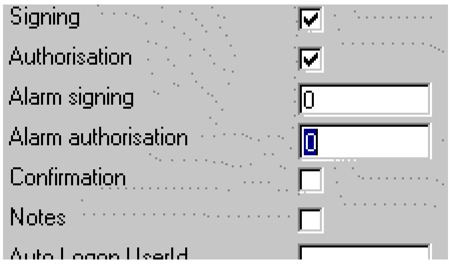
4.38.9 Configure the Alarm authorisation field

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

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

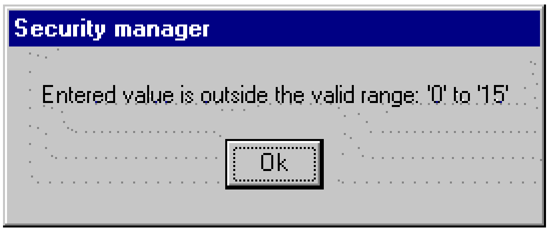
Note
If the value is NOT highlighted double click in the field.



Signing ☑
Authorisation ☑
Alarm signing 0
Alarm authorisation 0
Confirmation □
Notes □
Auto Logon UserId

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.



Entered value is outside the valid range: '0' to '15'

3. Finally, save changes and proceed to the next task.

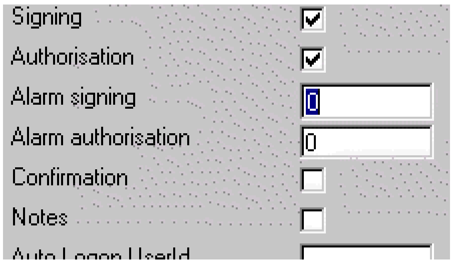
4.38.10 Configure the Alarm signing field

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.

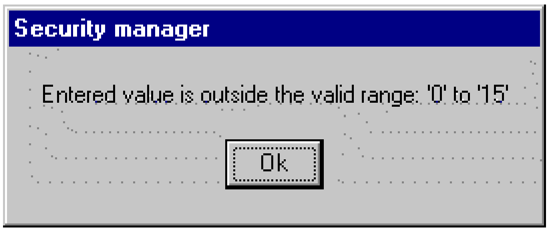
> **Note**
> If the value is NOT highlighted double click in the field.



Signing ☑
Authorisation ☑
Alarm signing 0
Alarm authorisation 0
Confirmation □
Notes □
Auto Logon UserId

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.



Security manager

Entered value is outside the valid range: '0' to '15'

3. Finally, save changes and proceed to the next task.

4.38.11 Configure the AlarmHistMaxItems access rights

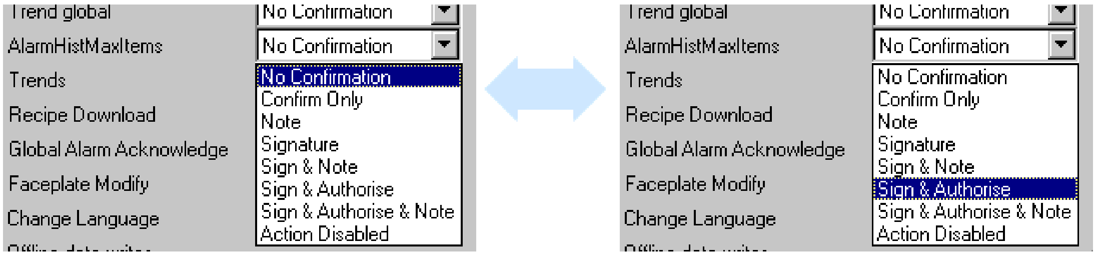
This field allows the selection of a type of confirmation via a drop down list, needed to accept changes to the number of retrieved alarms from the alarm history via the 'InTouch WindowViewer'.
InTouch WindowViewer > Alarm History
The **AlarmHistMaxItems** enables the User to increase the maximum number 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.



Trend global No Confirmation
AlarmHistMaxItems No Confirmation
Trends
Recipe Download
Global Alarm Acknowledge
Faceplate Modify
Change Language

2. Finally, save changes and proceed to the next task.

4.38.12 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, 'ticked' (True) or un-ticked (False). If the check box is ticked the User group is allowed to configure the archiving strategy. If not ticked, 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.

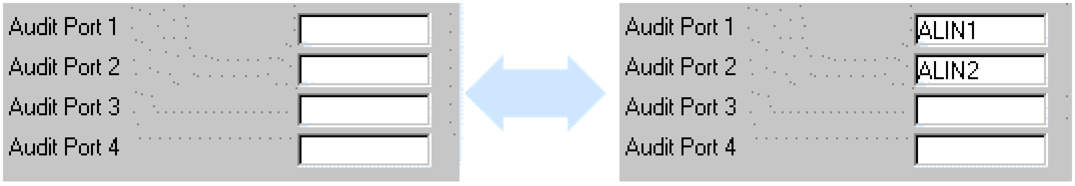
2. Finally, save changes and proceed to the next task.

4.38.13 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 Visual Supervisors that communicate via that network. Each LIN Network is designated using its 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

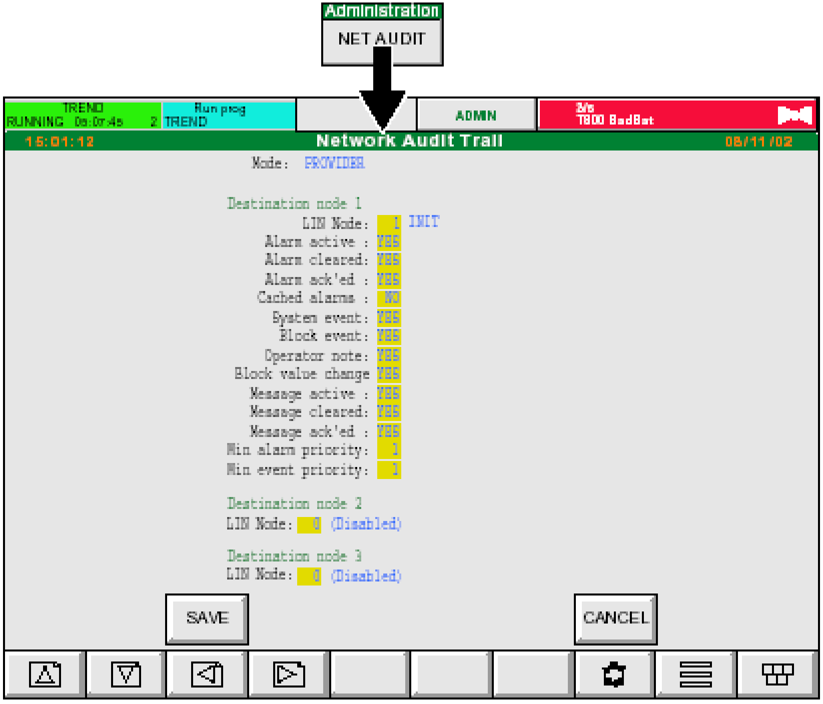
Firstly find the network port name.
Locate Security item node name in the Network folder and then trace back to the Network level.
Enter the network port name in the appropriate Audit Port field.



Audit Port 1
Audit Port 2
Audit Port 3
Audit Port 4

Audit Port 1 ALIN1
Audit Port 2 ALIN2
Audit Port 3
Audit Port 4

Ensure all 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**



Node: PROVIDER

Destination node 1
LIN Node: 1 INIT
Alarm active : YES
Alarm cleared: YES
Alarm ack'ed : YES
Cached alarms : NO
System event: YES
Block event: YES
Operator note: YES
Block value change YES
Message active : YES
Message cleared: YES
Message ack'ed : YES
Min alarm priority: 1
Min event priority: 1

Destination node 2
LIN Node: 0 (Disabled)

Destination node 3
LIN Node: 0 (Disabled)

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

5. Finally, save changes and proceed to the next task.

4.38.14 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.

4.38.15 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.

4.38.16 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/ Eycon™10/20 Visual Supervisor, 5000 and 6000 Series recorders and Review Security item 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.

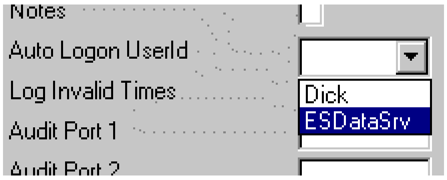
2. Finally, save changes and proceed to the next task.

4.38.17 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.

4.38.18 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.

4.38.19 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.

4.38.20 Configure the Change Language access rights

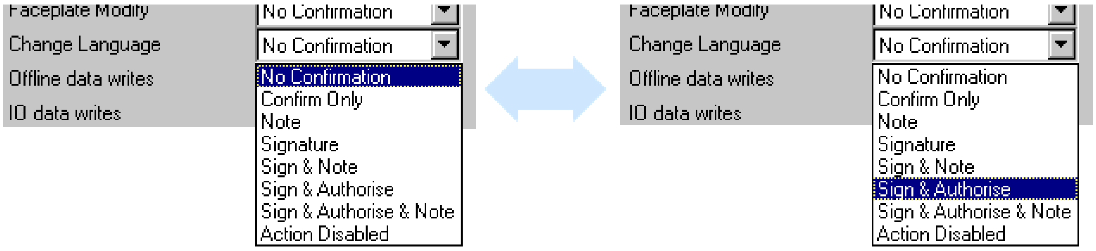
This field allows the selection of a type of confirmation via a drop down list, needed before the 'InTouch WindowViewer' can convert to the selected language.

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.

4.38.21 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.

4.38.22 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.

4.38.23 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.

4.38.24 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.

4.38.25 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.

4.38.26 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.

4.38.27 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.

4.38.28 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.

4.38.29 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.

4.38.30 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

4.38.31 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.

4.38.32 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.

4.38.33 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.

4.38.34 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.

4.38.35 Configure the Debug access rights

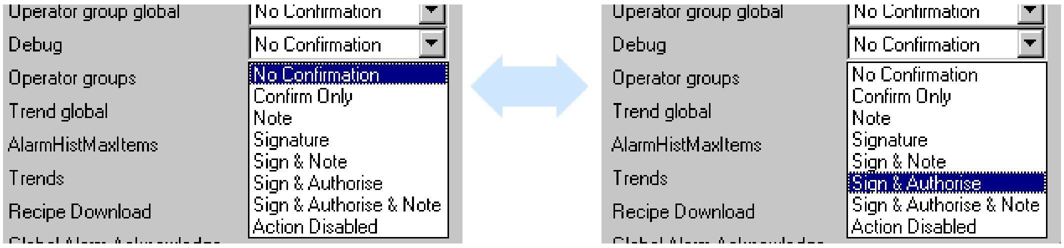
This field allows the selection of a type of confirmation via a drop down list, needed before Debugging Script Errors in the 'InTouch WindowViewer'.
InTouch WindowViewer > About/Help/Information > Script Errors

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.



Operator group global: No Confirmation
Debug: No Confirmation
Operator groups
Trend global
AlarmHistMaxItems
Trends
Recipe Download

No Confirmation
Confirm Only
Note
Signature
Sign & Note
Sign & Authorise
Sign & Authorise & Note
Action Disabled

2. Finally, save changes and proceed to the next task.

4.38.36 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.

4.38.37 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.

4.38.38 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.

4.38.39 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.

It is recommended that the field is set to ‘false’. This ensures that the account is enabled.

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.

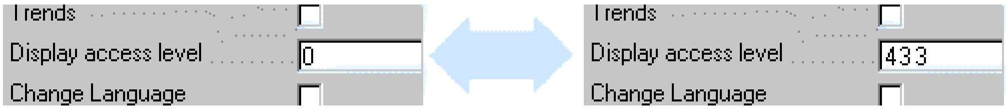
4.38.40 Configure the Display access level field

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.

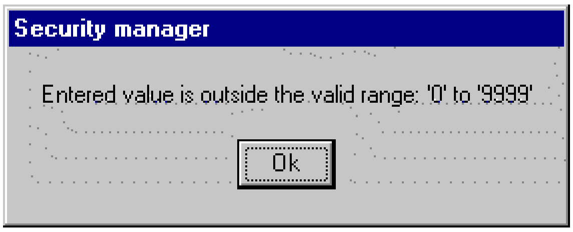


Trends □
Display access level 0
Change Language □

Trends □
Display access level 433
Change Language □

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.



Security manager

Entered value is outside the valid range: '0' to '9999'

3. Finally, save changes and proceed to the next task.

4.38.41 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.

4.38.42 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.

4.38.43 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.

4.38.44 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.

4.38.45 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.

4.38.46 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.

4.38.47 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.

4.38.48 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.

4.38.49 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.

4.38.50 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.

4.38.51 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.

4.38.52 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.

4.38.53 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.

4.38.54 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.

4.38.55 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.

4.38.56 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 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.

4.38.57 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.

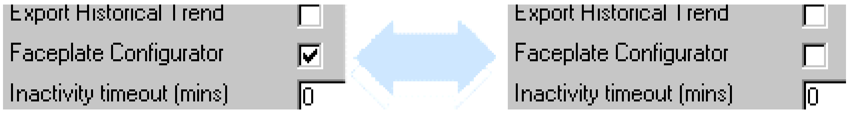
It has 2 states, ☑- True or □- False. If the check box is set to True the User group is allowed to create and save mimic faceplates. If False, the User group has been denied the access rights.
This is configured in the database for EurothermSuite PC Security item type.

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.



Export Historical Trend □
Faceplate Configurator ☑
Inactivity timeout (mins) 0

Export Historical Trend □
Faceplate Configurator □
Inactivity timeout (mins) 0

2. Finally, save changes and proceed to the next task.

4.38.58 Configure the Faceplate Modify access rights

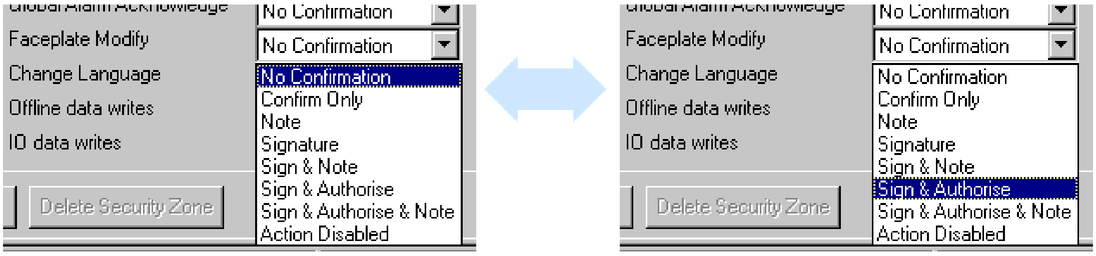
This field allows the selection of a type of confirmation via a drop down list, needed for accepting changes to a Faceplate via the 'InTouch WindowViewer'.

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.



Global Alarm Acknowledge No Confirmation
Faceplate Modify No Confirmation
Change Language
Offline data writes
IO data writes

2. Finally, save changes and proceed to the next task.

4.38.59 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.

4.38.60 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.

4.38.61 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.

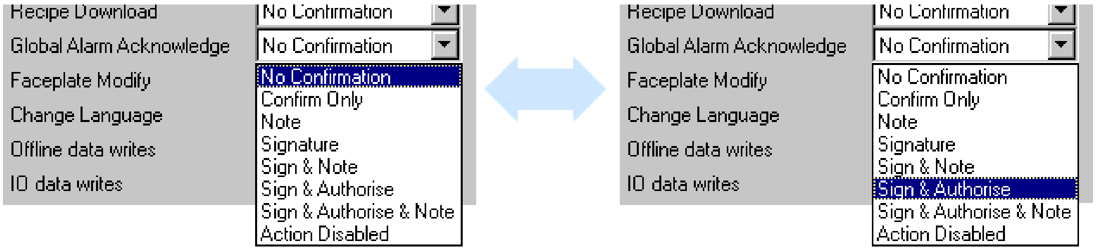
2. Finally, save changes and proceed to the next task.

4.38.62 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.

4.38.63 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.

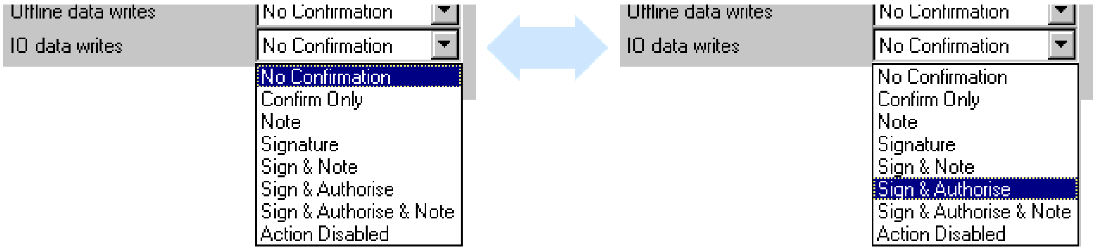
Note
If any Windows Domain group does not exist, deployment will fail.

4.38.64 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.



Offline data writes No Confirmation
IO data writes No Confirmation

Offline data writes No Confirmation
IO data writes No Confirmation

2. Finally, save changes and proceed to the next task.

4.38.65 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

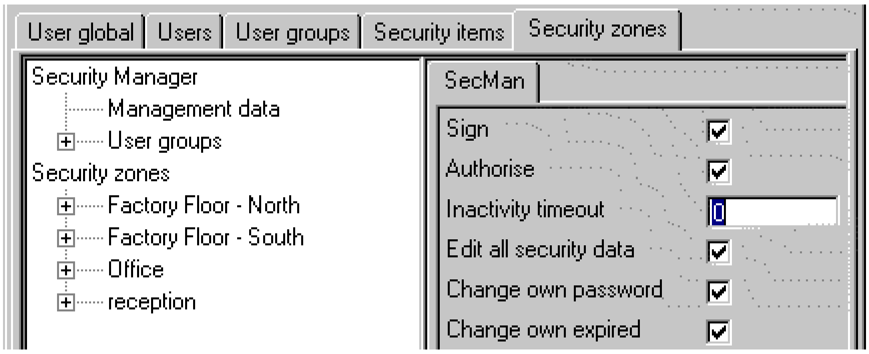
The default value limits of the field are subject to Regulatory defaults.

To configure this

1. Click in the **Inactivity timeout** field.

Note

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



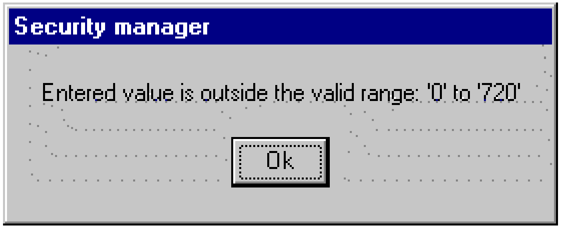
Security Manager
- Management data
- User groups

Security zones
- Factory Floor - North
- Factory Floor - South
- Office
- reception

Sign ☑
Authorise ☑
Inactivity timeout 0
Edit all security data ☑
Change own password ☑
Change own expired ☑

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.



Entered value is outside the valid range: '0' to '720'

If required enter an adjusted value.

3. Finally, save changes and proceed to the next task.

4.38.66 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.

4.38.67 Configure the Log Invalid Times field

This check box allows or does not allow the recording of invalid time stamps in the Audit Trail.

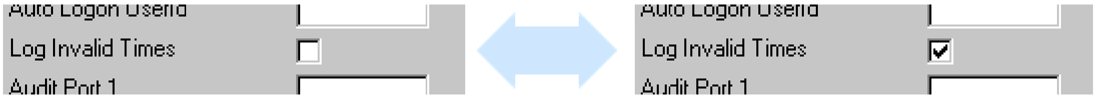
It has 2 states, ☑- True or □- False. If the check box is set to True, the Audit Trail records all time stamps NOT corresponding with that of the master database. If False, the feature is disabled.
This is configured in the database for EurothermSuite PC Security item type.

To configure this

1. Click in the **Log Invalid Times** check box.

☑ indicates that the action is enabled.

□ indicates the feature is disabled.



Auto Logon UserId
Log Invalid Times □
Audit Port 1

Auto Logon UserId
Log Invalid Times ☑
Audit Port 1

2. Finally, save changes and proceed to the next task.

4.38.68 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.

4.38.69 Configure the Login timeout field

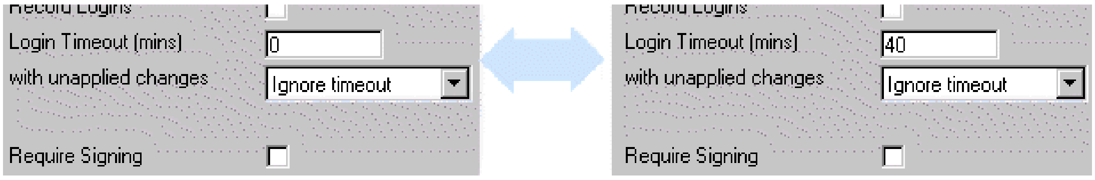
This field allows the input of the number of minutes the Security item type in the Security zone can be left idle before the current User is automatically logged out.
The **Login timeout** as configured for the 5000 and 6000 Series instrument Security item type is used in conjunction with the '**with 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.

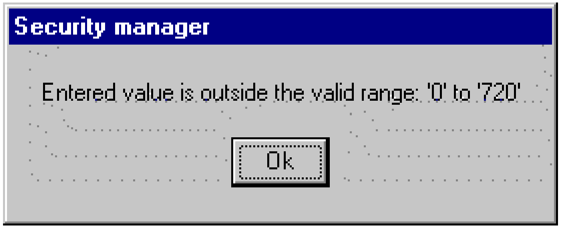


Record Logins
Login Timeout (mins) 0
with unapplied changes Ignore timeout
Require Signing □

Record Logins
Login Timeout (mins) 40
with unapplied changes Ignore timeout
Require Signing □

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.



Security manager

Entered value is outside the valid range: '0' to '720'

If required enter an adjusted value.

3. Finally, save changes and proceed to the next task.

4.38.70 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.

4.38.71 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.

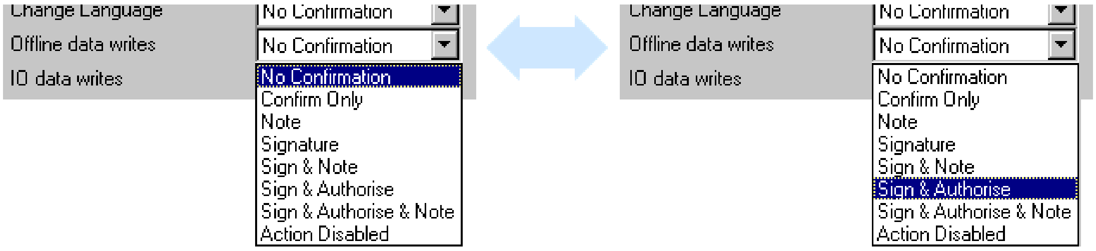
2. Finally, save changes and proceed to the next task

4.38.72 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.

4.38.73 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.

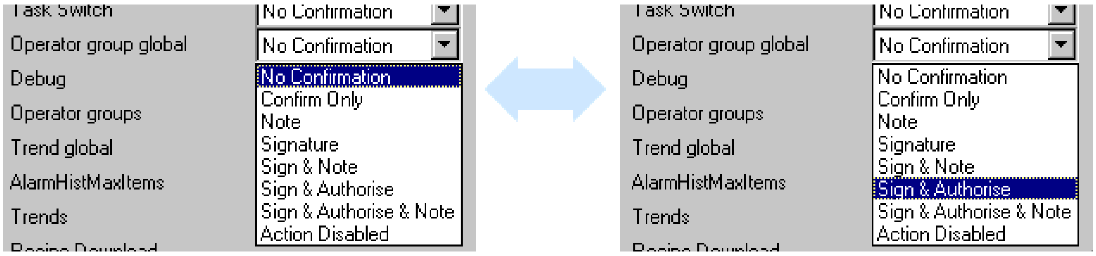
2. Finally, save changes and proceed to the next task.

4.38.74 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.



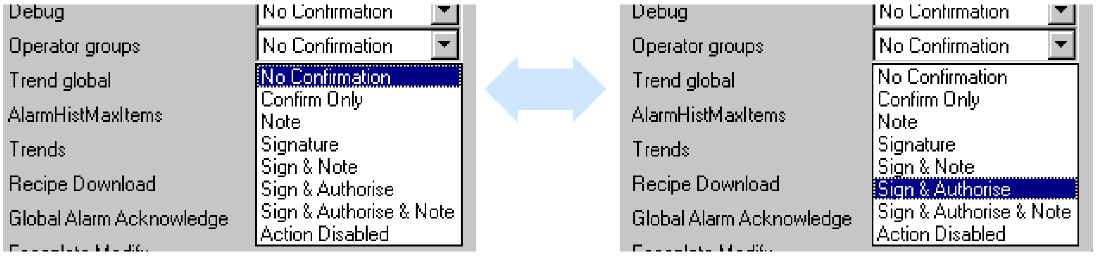
2. Finally, save changes and proceed to the next task.

4.38.75 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.



Debug: No Confirmation
Operator groups: No Confirmation

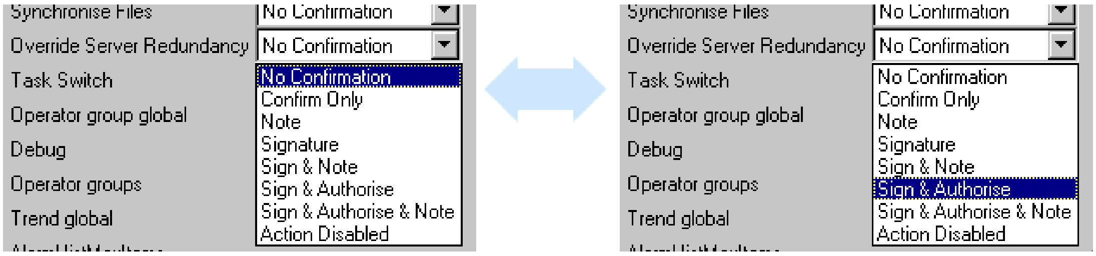
2. Finally, save changes and proceed to the next task.

4.38.76 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.



Synchronise Files: No Confirmation
Override Server Redundancy: No Confirmation

2. Finally, save changes and proceed to the next task.

4.38.77 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.

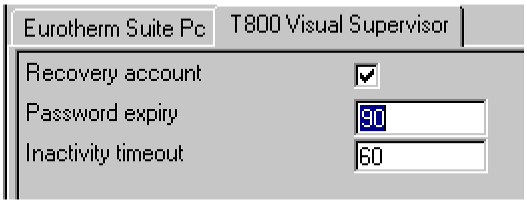
The Password expiry period is configured in the databases for the Security Manager, 5000 Series and Visual Supervisor instruments Security items.

Note
The Password expiry period does NOT apply to passwords received via Security deployment.

To configure this

1. Click the **Password expiry** field.

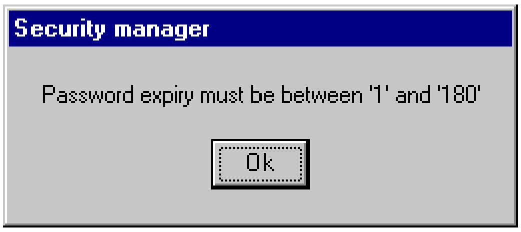
Note
If the value is NOT highlighted double click in the field.



Recovery account ☑
Password expiry 90
Inactivity timeout 60

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.


Security manager

Password expiry must be between '1' and '180'

3. Finally, save changes and proceed to the next task.

4.38.78 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.

4.38.79 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.

4.38.80 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.

4.38.81 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.

4.38.82 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.

4.38.83 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.

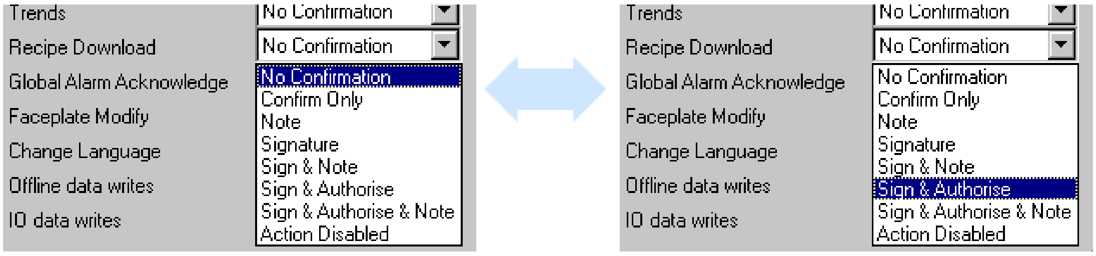
2. Finally, save changes and proceed to the next task.

4.38.84 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.

4.38.85 Configure the Record Logins field

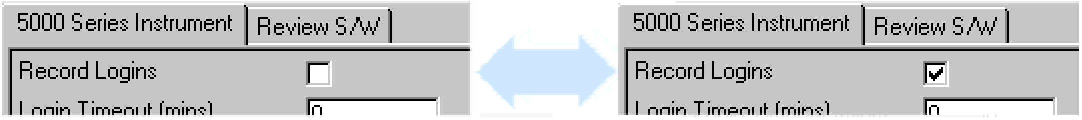
This check box allows or does not allow the Users assigned to the selected User group to any future login or logout message appearing on the chart only when the **Default Regulation** is selected
Options > Regulations
The other **Regulations** are pre-configured to record this information in the Audit 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.



5000 Series Instrument | Review S/W
Record Logins ☐
Login Timeout (mins) 0

5000 Series Instrument | Review S/W
Record Logins ☑
Login Timeout (mins) 0

2. Finally, save changes and proceed to the next task.

4.38.86 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 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 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 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 Visual Supervisor item type.

☐ indicates the Users has insufficient access rights.

2. Finally, save changes and proceed to the next task.

4.38.87 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.

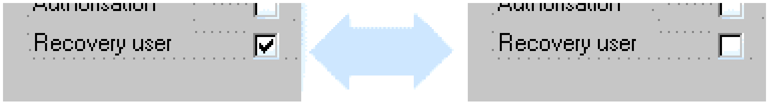
This is configured in the database for the Security Manager.

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.



Recovery user ☑

Recovery user □

2. Finally, save changes and proceed to the next task.

4.38.88 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 a 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 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.

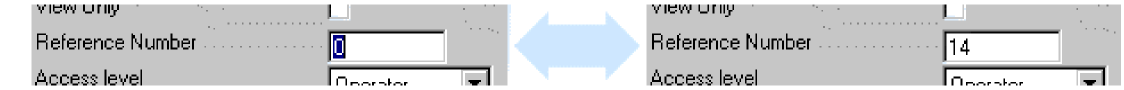
This is configured in the database for Visual Supervisor Security item types.

To configure this

1. Click the **Reference Number** field.

Note

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



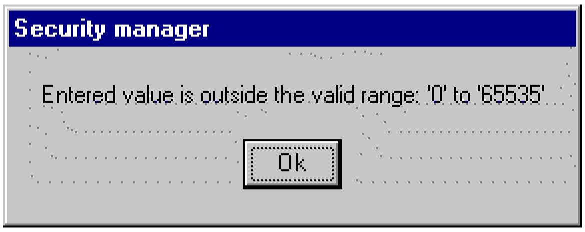
Reference Number 0

Reference Number 14

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.



Security manager

Entered value is outside the valid range: '0' to '65535'

3. Finally, save changes and proceed to the next task.

4.38.89 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 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.

4.38.90 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.

4.38.91 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.

4.38.92 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.

4.38.93 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.

4.38.94 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, / Eycon™10/20 Visual Supervisor, 5000 and 6000 Series recorder Security item 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.

4.38.95 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.

4.38.96 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.

4.38.97 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 CRTL+SHIFT+H keys) the latest version of selected files to specified locations using the 'InTouch WindowViewer'. InTouch WindowViewer > About/Help/Information > Synchronise Files

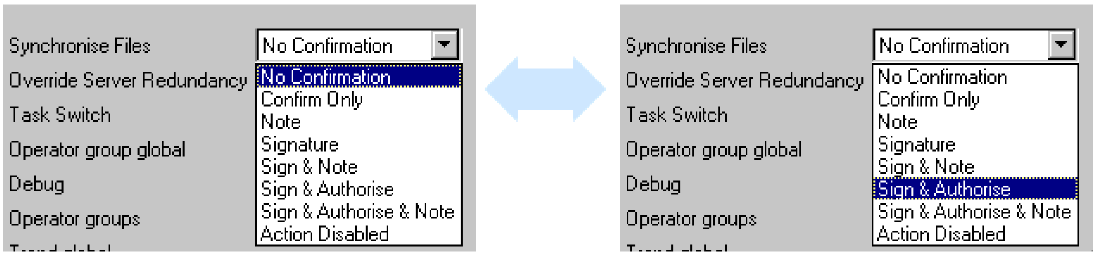
Note

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.

4.38.98 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.

4.38.99 Configure the Tag Security Area access level fields

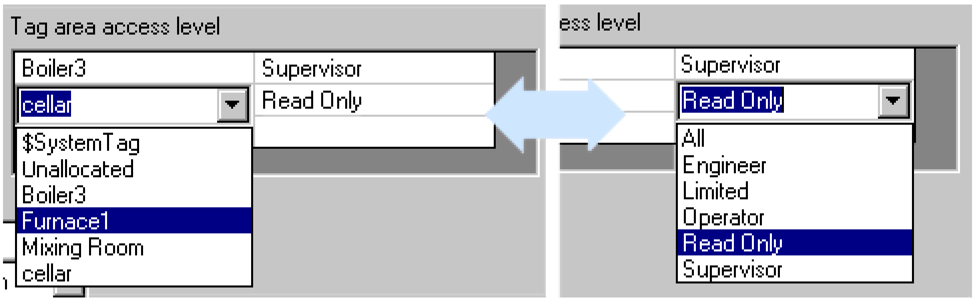
These Tag Security Area access level fields are used to associate Tag Security Areas, created using '**Project Organiser**', with defined access level enumeration's.

Note

Remember, Tags can ONLY be edited by Users with Access Levels equal or greater than the selected value.

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.

4.38.100 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.

4.38.101 Configure the Task Switch access rights

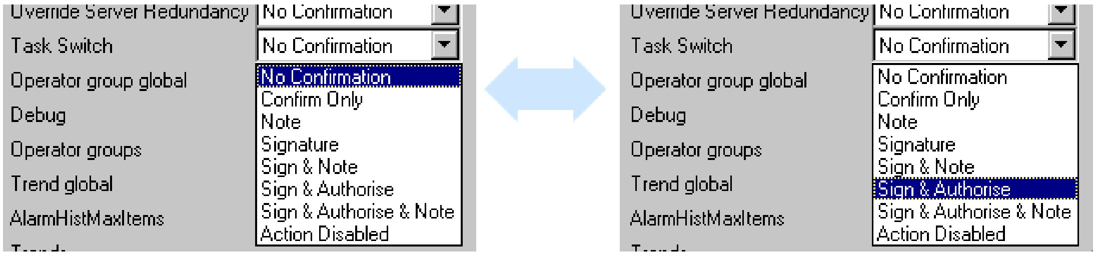
This field allows the selection of a type of confirmation via a drop down list, needed when accessing the operating system environment (pressing ALT+TAB keys) via the ‘InTouch WindowViewer’.

It is recommended that the action remains disabled at all times

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.

4.38.102 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.

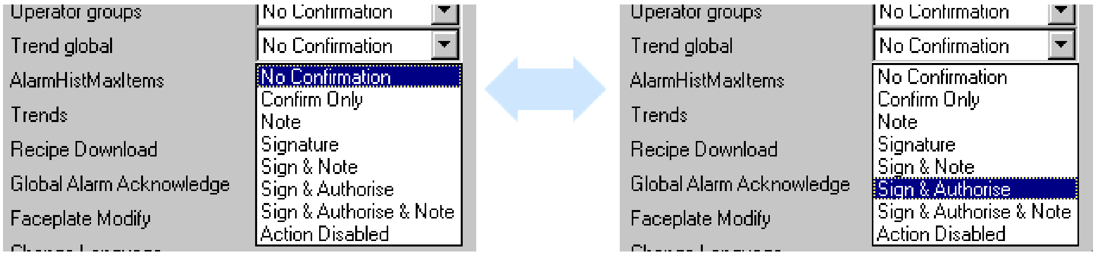
2. Finally, save changes and proceed to the next task.

4.38.103 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.



Operator groups: No Confirmation
Trend global: No Confirmation

No Confirmation
Confirm Only
Note
Signature
Sign & Note
Sign & Authorise
Sign & Authorise & Note
Action Disabled

AlarmHistMaxItems
Trends
Recipe Download
Global Alarm Acknowledge
Faceplate Modify

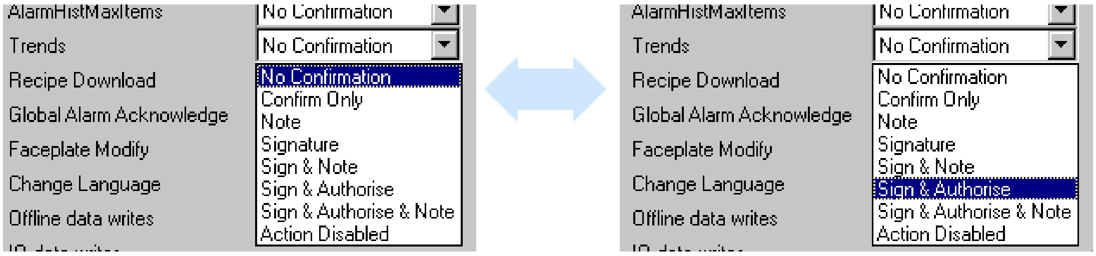
2. Finally, save changes and proceed to the next task.

4.38.104 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.



AlarmHistMaxItems: No Confirmation
Trends: No Confirmation

No Confirmation
Confirm Only
Note
Signature
Sign & Note
Sign & Authorise
Sign & Authorise & Note
Action Disabled

Recipe Download
Global Alarm Acknowledge
Faceplate Modify
Change Language
Offline data writes

2. Finally, save changes and proceed to the next task.

4.38.105 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 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.

4.38.106 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 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.

4.38.107 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.

4.38.108 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.

4.38.109 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.

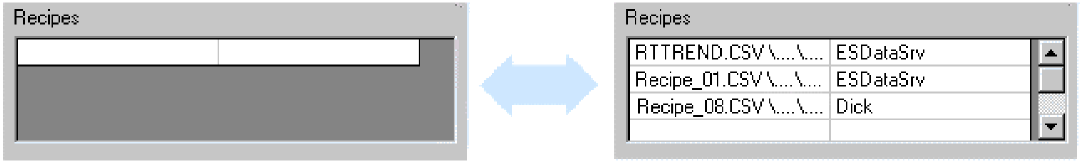
> **Note**
> Remember to configure the type of confirmation via a drop down list required to allow the Recipe Download to proceed.

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.



RTTREND.CSV \....\....	ESDataSrv
Recipe_01.CSV \....\....	ESDataSrv
Recipe_08.CSV \....\....	Dick

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.

5 EDITING PARAMETERS

5.1 CHANGE THE USER ID

This is a Read Only column but is incremented when Users are added.

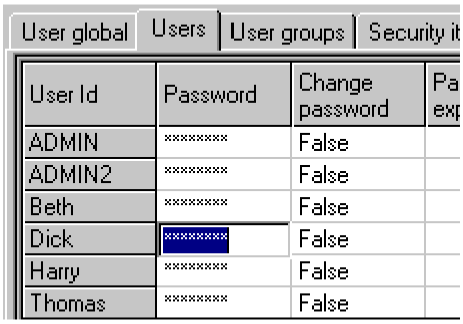
5.2 CHANGE THE PASSWORD FIELD

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 User's '**Password**' field.

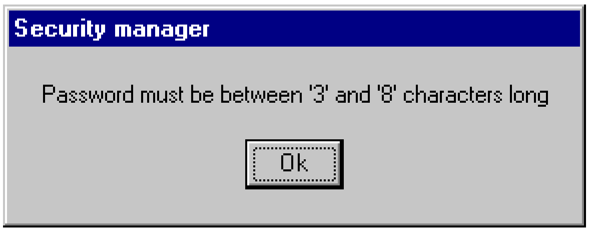
Note
If the value is NOT highlighted double click in the field.



User Id	Password	Change password	Pa exp
ADMIN	xxxxxxxxx	False	
ADMIN2	xxxxxxxxx	False	
Beth	xxxxxxxxx	False	
Dick	xxxxxxxxx	False	
Harry	xxxxxxxxx	False	
Thomas	xxxxxxxxx	False	

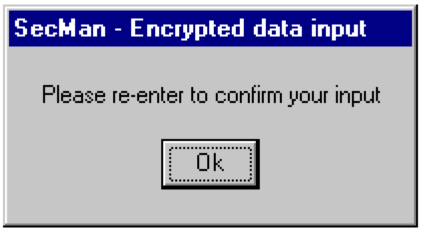
2. Enter a new case-sensitive password value which does not exceed the selected Regulatory value constraints and press the return key.

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.



Password must be between '3' and '8' characters long

3. Read the information on the dialog window requesting password re-entry, and confirm by clicking the '**Ok**' button.



Please re-enter to confirm your input

4. In the same field as before enter the identical password again.

Note
Passwords are displayed as '**xxxxxxxx**'.

5. Finally save changes.

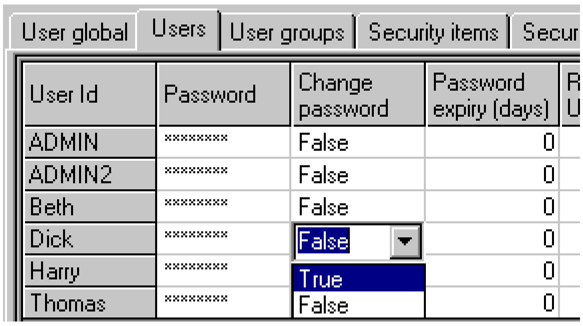
5.3 CHANGE THE CHANGE PASSWORD FIELD

This field is edited to enable or disable the need for a User to change the password when he or she next attempts to login to a security database on a PC.

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 to a security database on a PC, a prompt appears requesting a change of password.



User Id	Password	Change password	Password expiry (days)	R U
ADMIN	********	False	0	
ADMIN2	********	False	0	
Beth	********	False	0	
Dick	********	False	0	
Harry	********	True	0	
Thomas	********	False	0	

3. Finally save changes.

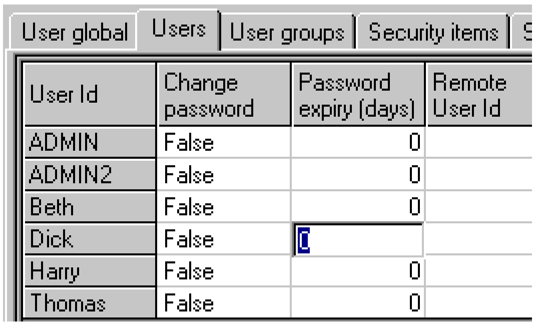
5.4 CHANGE THE PASSWORD EXPIRY TIME PERIOD

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.

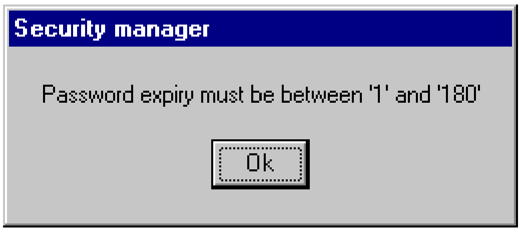


User Id	Change password	Password expiry (days)	Remote User Id
ADMIN	False	0	
ADMIN2	False	0	
Beth	False	0	
Dick	False	0	
Harry	False	0	
Thomas	False	0	

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.



Password expiry must be between '1' and '180'

3. Finally save changes.

5.5 CHANGE THE REMOTE USER ID

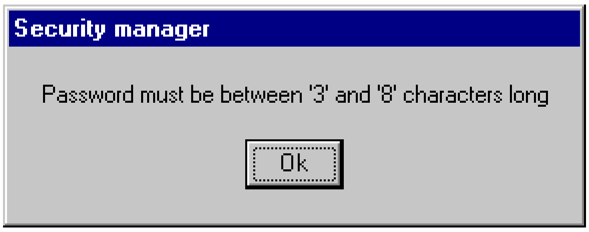
This field is edited to enable the User access to a Security database via a 5000 Series instrument.

1. Select the appropriate User's '**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.


Security manager

Password must be between '3' and '8' characters long

3. Finally save changes

5.6 CHANGE THE REMOTE PASSWORD FIELD

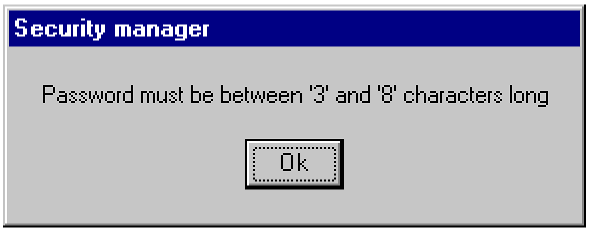
This field is edited within the constraints configured in the Minimum and Maximum Password Length fields on the User Global tab, to change the password before the User can access a Security database via a 5000 Series instrument.

1. Select the appropriate User's '**Remote password**' field.

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

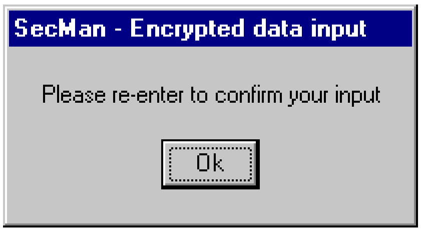
2. Enter a new case-sensitive password value which does not exceed the selected Regulatory value constraints and press the return key.

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.


Security manager

Password must be between '3' and '8' characters long

3. Read the information on the dialog window requesting password re-entry, and confirm by clicking the '**Ok**' button.


SecMan - Encrypted data input

Please re-enter to confirm your input

4. In the same field as before enter the identical password again.

Note
Passwords are displayed as '**xxxxxxxx**'.

5. Finally save changes

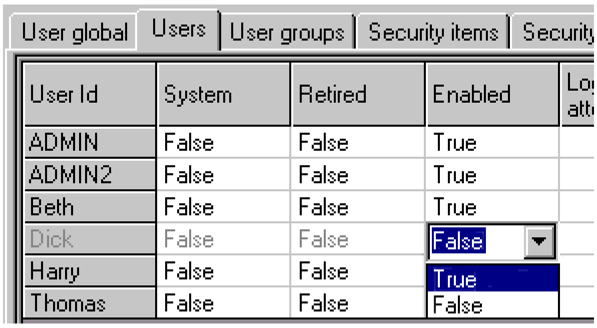
5.7 CHANGE THE ENABLED FIELD

Change this 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		
Thomas	False	False		

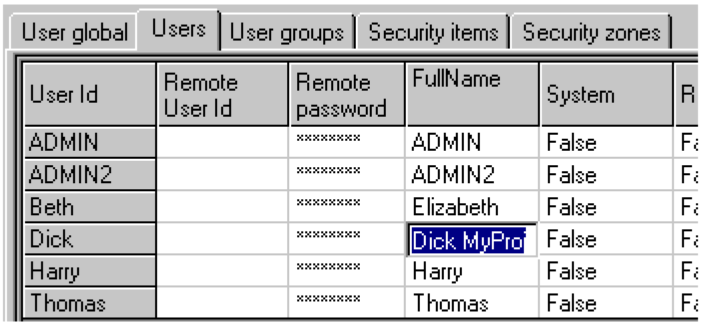
3. Finally save changes.

5.8 CHANGE THE FULLNAME FIELD

Change this field to enter an appropriate name for the User account.

1. Select the appropriate Users '**Fullname**' field.

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

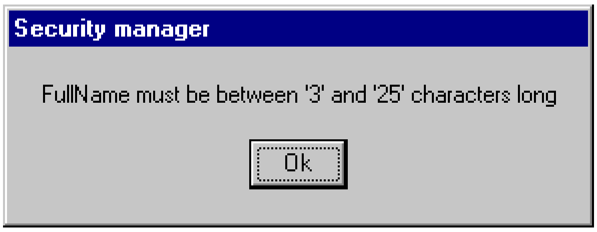


User Id	Remote User Id	Remote password	FullName	System	R
ADMIN		********	ADMIN	False	Fa
ADMIN2		********	ADMIN2	False	Fa
Beth		********	Elizabeth	False	Fa
Dick		********	Dick MyPro	False	Fa
Harry		********	Harry	False	Fa
Thomas		********	Thomas	False	Fa

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 'r;**Ok**' to return this field to its previous setting and then attempt the change again.



Security manager

FullName must be between '3' and '25' characters long

3. Finally save changes.

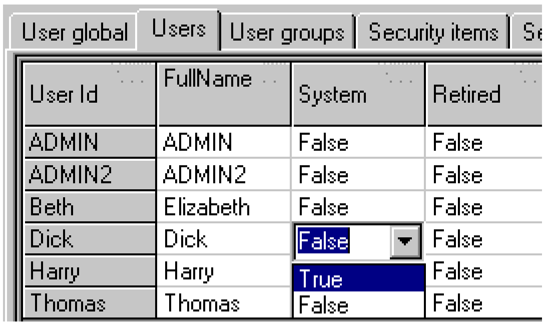
5.9 CHANGE THE SYSTEM FIELD

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	False	False
Harry	Harry	True	False
Thomas	Thomas	False	False

3. Finally save changes.

5.10 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.

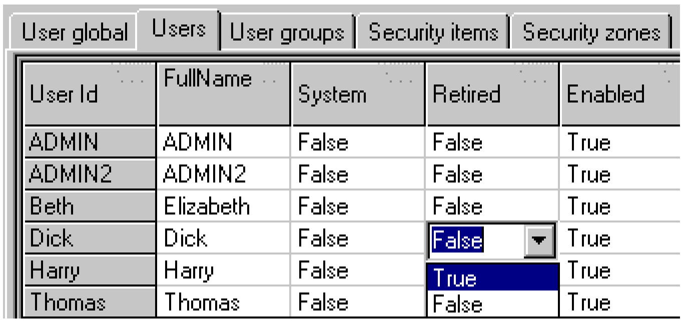
All records of Retired accounts compliant to the Default Regulation are removed, whereas records of Retired accounts compliant to the 21 CFR Part 11 are retained, (greyed out in the User tab).

Note

The effect is immediate (i.e. there is NO confirmation requested for this action.)

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.

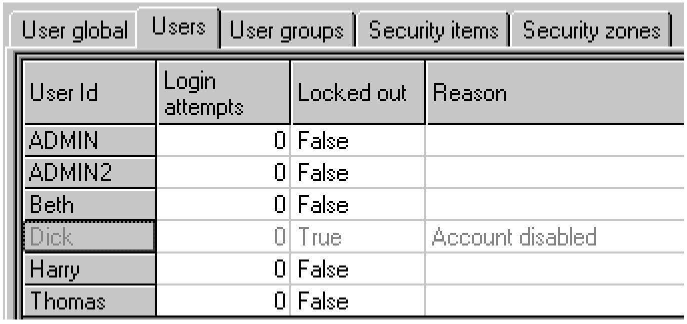


User Id	FullName	System	Retired	Enabled
ADMIN	ADMIN	False	False	True
ADMIN2	ADMIN2	False	False	True
Beth	Elizabeth	False	False	True
Dick	Dick	False	False	True
Harry	Harry	False	True	True
Thomas	Thomas	False	False	True

3. Finally save changes.

5.11 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

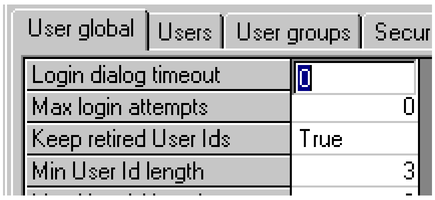
5.12 CHANGE THE LOGIN DIALOG TIMEOUT

Change the numeric value to increase or decrease the amount of time a Login prompt window will remain displayed before automatically logging out.

Note
This timeout value only applies to the T800/ Eycon™ 10/20 Visual Supervisor Login dialog.

1. Click the editable ‘Login dialog timeout’ field.

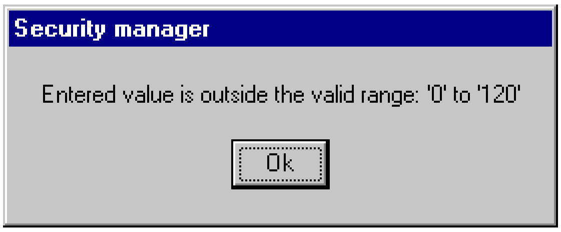
Note
The existing value is highlighted. If the value is NOT highlighted double click in the field.



Login dialog timeout	0
Max login attempts	0
Keep retired User Ids	True
Min User Id length	3

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.


Security manager

Entered value is outside the valid range: '0' to '120'

3. Finally save changes.

5.13 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.

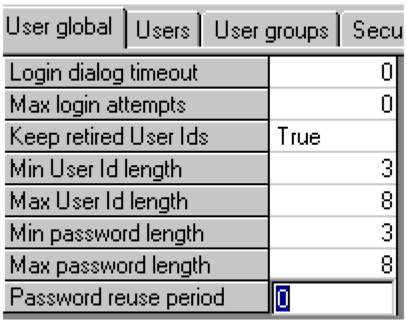
5.14 CHANGE THE PASSWORD REUSE PERIOD

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.

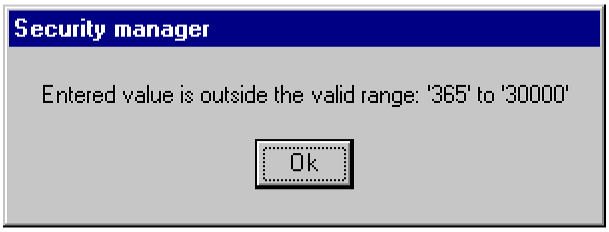


Login dialog timeout	0
Max login attempts	0
Keep retired User Ids	True
Min User Id length	3
Max User Id length	8
Min password length	3
Max password length	8
Password reuse period	0

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.


Security manager

Entered value is outside the valid range: '365' to '30000'

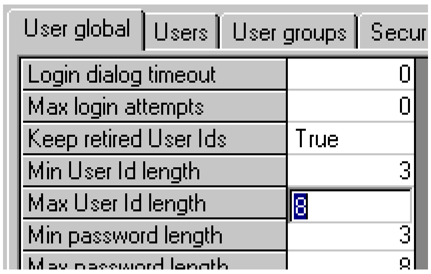
3. Finally save changes.

5.15 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.

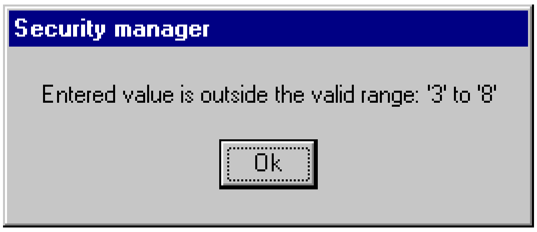
Note
The existing value is highlighted. If the value is NOT highlighted double click in the field.



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

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.



Entered value is outside the valid range: '3' to '8'

3. Finally save changes.

6 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).

6.1 DEFAULT ACCOUNT 1

User Id - ADMIN (NOT case-sensitive), Password - ADMIN (case-sensitive).

6.2 DEFAULT ACCOUNT 2

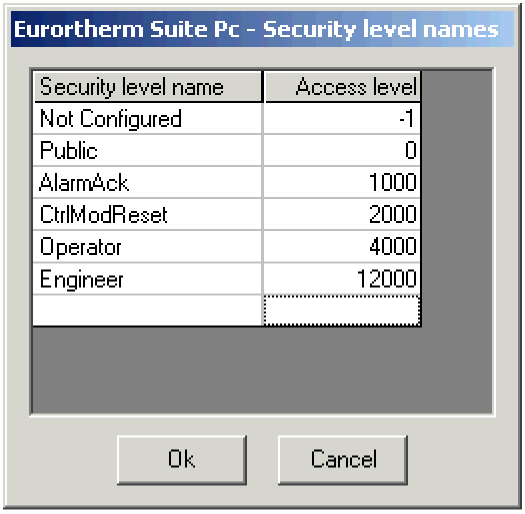
User Id - ADMIN2 (NOT case-sensitive), Password - ADMIN2 (case-sensitive).
The default Access Rights vary depending on the Regulation selected.

6.3 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.

6.4 ACCESS LEVEL ENUMERATIONS

Numeric values may be entered instead of the enumerations.


Eurotherm Suite Pc - Security level names

Security level name	Access level
Not Configured	-1
Public	0
AlarmAck	1000
CtrlModReset	2000
Operator	4000
Engineer	12000

6.5 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.

6.5.1 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.

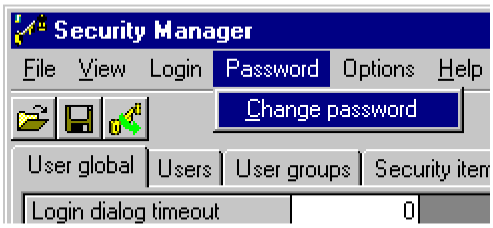
User group Access Level	Tag	Location	Tag Security Area	Tag Access Level
Operator (UG1)	Tag1, and Tag3	PC_12	Tag Security Area 3	Operator (8000)
Operator (UG1)	Tag2	PC_12	Tag Security Area 2	Engineer (16000)
Operator (UG1)	Tag5 and Tag6	PC_4	Tag Security Area 6	Read only (0)

7 PASSWORD MENU

7.1 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,

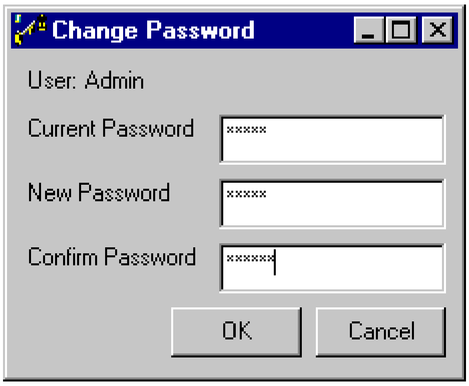
1. Selecting **'Password** > **Change Password'** from the Menu bar.



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.



User: Admin

Current Password xxxxx

New Password xxxxx

Confirm Password xxxxxx

5. When all fields have been completed, accept the changes by clicking '**OK**'. To discard and return to the previous password select '**Cancel**'.

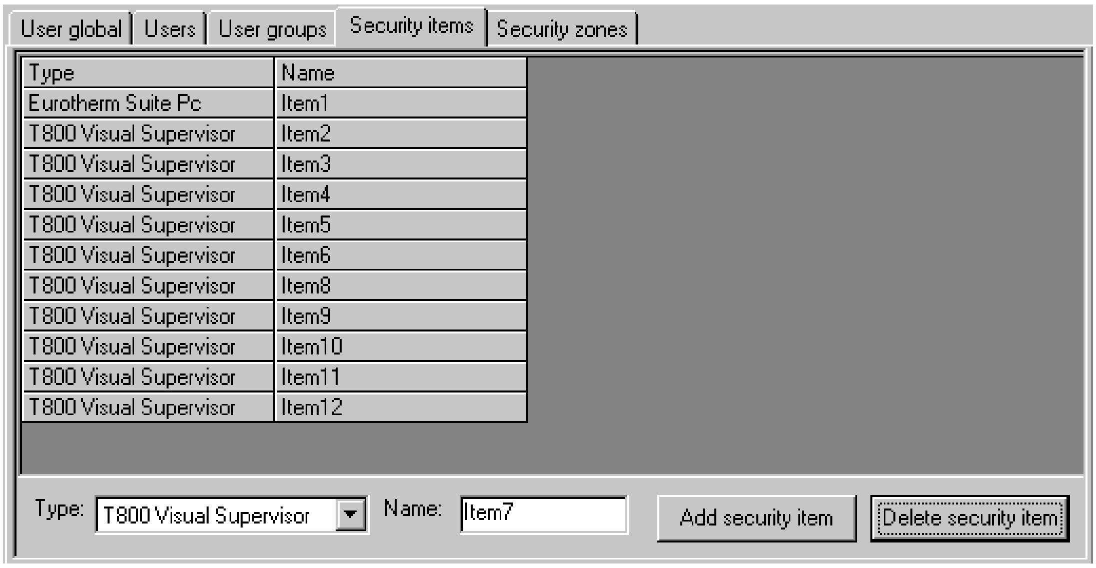
8 DELETE A SECURITY ITEM

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.



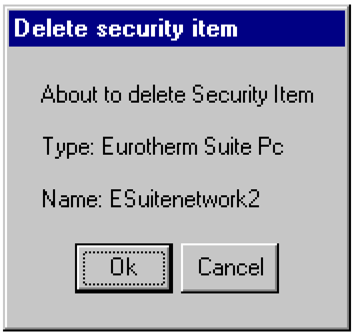
Type	Name
Eurotherm Suite Pc	Item1
T800 Visual Supervisor	Item2
T800 Visual Supervisor	Item3
T800 Visual Supervisor	Item4
T800 Visual Supervisor	Item5
T800 Visual Supervisor	Item6
T800 Visual Supervisor	Item8
T800 Visual Supervisor	Item9
T800 Visual Supervisor	Item10
T800 Visual Supervisor	Item11
T800 Visual Supervisor	Item12

Type: T800 Visual Supervisor

Name: Item7

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.

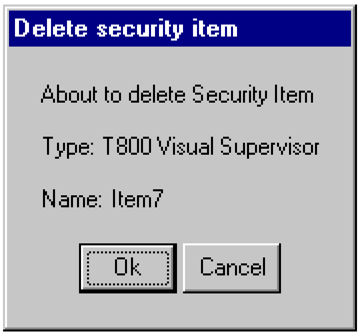


Delete security item

About to delete Security Item

Type: Eurotherm Suite Pc

Name: ESuitenetwork2



Delete security item

About to delete Security Item

Type: T800 Visual Supervisor

Name: Item7

Note
If '**Ok**' was selected observe the item has been removed.

4. Finally save changes.

8.1.1 Address

Displays the Security item address. This describes the location of the Security item security database by either Project path (EurothermSuite 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' (Visual Supervisor instruments).

8.1.2 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).

8.1.3 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.

Note
If the Recovery User account is NOT configured at any time before the system becomes inaccessible, the Recovery User account will NOT made be available.

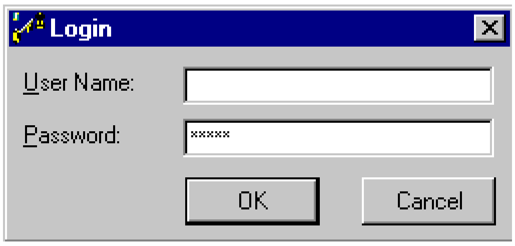
The database has an Recovery User account that allows a User to login to a database that does NOT have sufficient active Administrator accounts with full Access Rights. If the database has insufficient active Administrator accounts this could be due to,

- passwords expiring or being forgotten
- exceeding the Maximum Login attempt limits
- disabled Administrator accounts

8.1.4 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 the 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 opens enabling the User to re-instate sufficient accounts reactivating the security project.



8.1.5 Recover Visual Supervisor Security Database

A Recovery User Account is essential to recover an unusable database. It relies on an Administrator enabling the Visual Supervisor Recovery account before the Security database becomes inaccessible.

Note
If the Recovery User account is NOT configured at any time before the system becomes inaccessible, the Recovery User account will NOT made be available.

If configured the Visual Supervisor has a Recovery account that allows a User to login to a 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 having been forgotten.
- the Maximum Login attempt limits being exceeded.
- Administrator accounts being disabled.

8.1.6 Recover an unusable Visual supervisor Security database

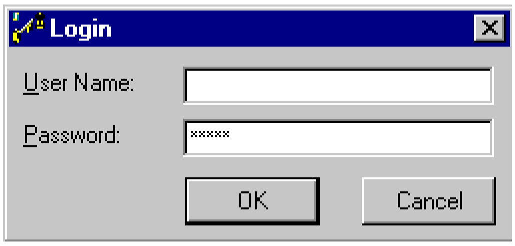
If the **Recovery account** has already been configured it will be possible to recover an unusable Security database. Use the following instructions in order to do so.

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.



Password: *****

4. This opens the Security database, enabling the User to re-instate sufficient accounts, therefore reactivating the Security database.

9 PC CONFIGURATION

This function enables the User to restrict the use of the master security database. This database is unrestricted until the 'Enable PC Locking' field is checked, after which the database is restricted to the list of computer's in the '**PC Configuration**' dialog window. This is also a default list of computers for use with the AutoDeployment zone.

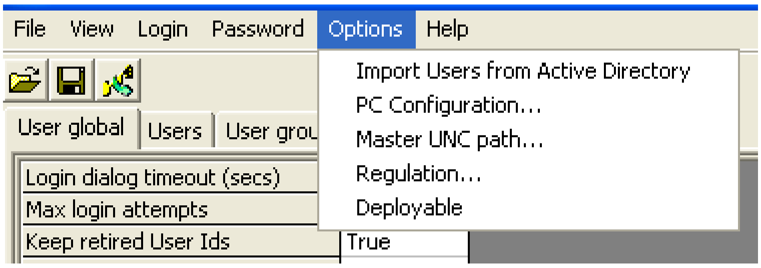
If the 'Enable PC Locking' field is selected before any computer's have been added a dialog window appears warning that this function is NOT enabled.

9.1 TO SETUP THE PC CONFIGURATION

When PC Configuration is selected, a dialog window appears. It is configured by adding computer's to a list, deleting them from the list, enabling computer locking and confirming the operation.

The User needs to know the PC Name, and PC Code of the computer before attempting to add it to the list.

1. Select **'Options** > **PC Configuration'** from the Menu Bar.



2. A dialog window to appears. Firstly, make sure the 'Enable PC Locking' is disabled. Using the keyboard enter the PC Name and PC Code in the appropriate fields and press the 'Add PC' button. If attempting to add the computer currently in use click the 'Add this PC' button.

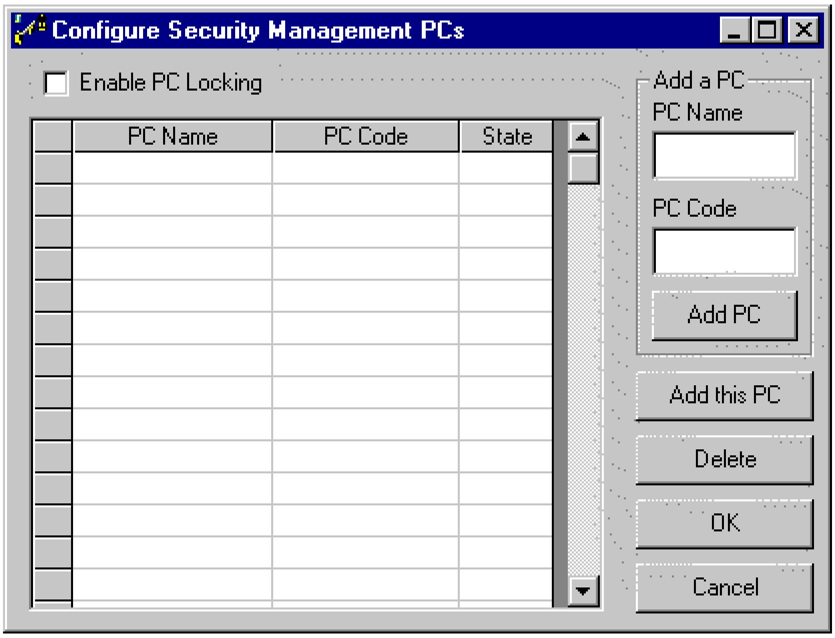
3. Observe the computer Name and Code have been entered in the list. ALL computers on the list remain at 'ADD' status until confirmed.

Note

Any computer at the '**ADD**' status may be deleted without confirmation.

4. Press '**Ok**' to confirm and update the computer's status from 'add' to 'existing'.

- Use the Cancel button to ignore the changes.



9.2 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.

10 CUSTOMISE SECURITY MANAGER

10.1 HOW TO SHOW ACTIVE OR ALL USERS

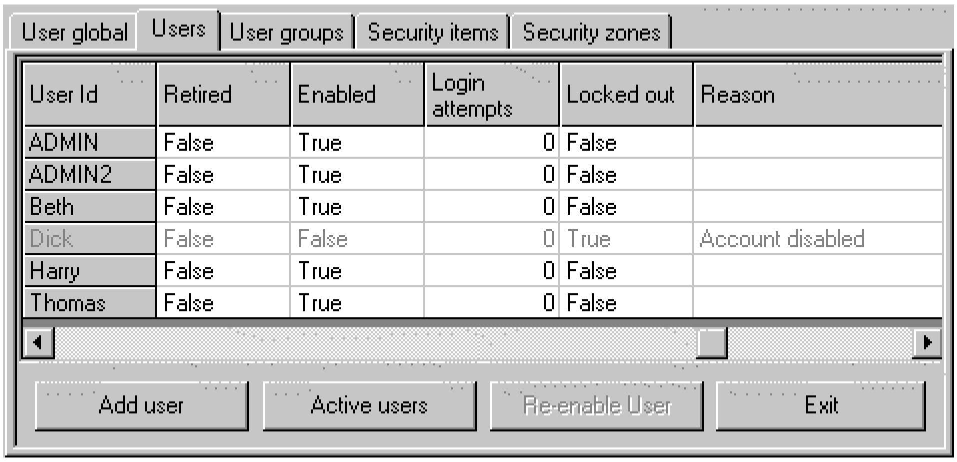
The function of this button allows the User to display ALL Users or just the Active Users in the User Id column.

Display Active or All users by

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

Note

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



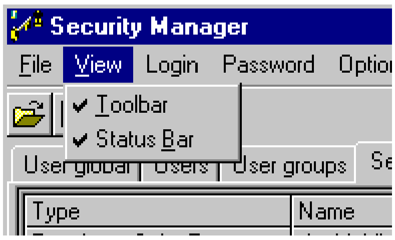
User Id	Retired	Enabled	Login attempts	Locked out	Reason
ADMIN	False	True	0	False	
ADMIN2	False	True	0	False	
Beth	False	True	0	False	
Dick	False	False	0	True	Account disabled
Harry	False	True	0	False	
Thomas	False	True	0	False	

2. Finally save changes.

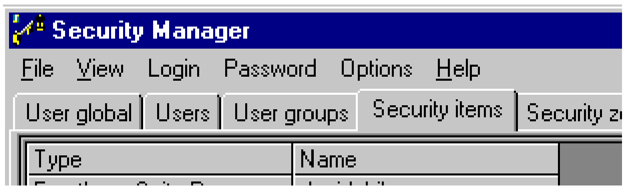
10.2 HOW TO HIDE/SHOW TOOLBAR

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.



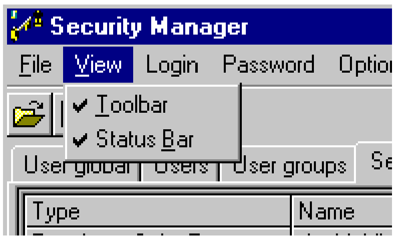
3. To display the Toolbar, repeat the instructions.

10.3 HOW TO HIDE/SHOW STATUS BAR

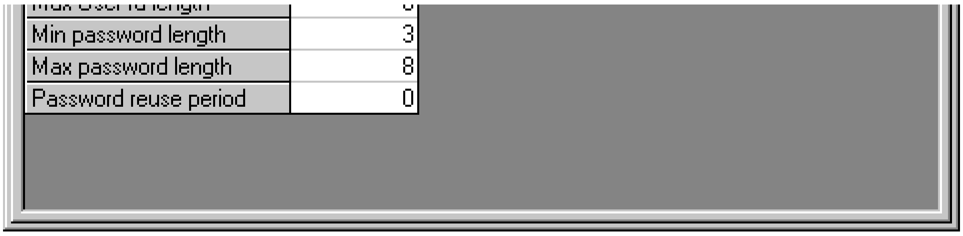
The Status Bar displays Security Manager database status information, including location, current user, security status, date and time. It is displayed by default and is located along the foot of the Security Manager window. A check mark indicates it is currently displayed.

To hide/show this bar by,

1. Selecting **'View** > **Status Bar'** from the Menu Bar.



2. The Status Bar is removed from the window.



Min password length	3
Max password length	8
Password reuse period	0

3. Repeat the instructions to display the Status Bar.

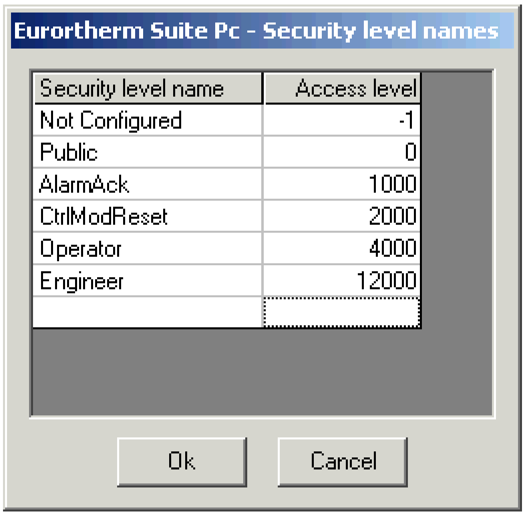
11 EUROTHERMSUITE PC SECURITY LEVEL NAMES

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.

Note
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.



Eurortherm Suite Pc - Security level names

Security level name	Access level
Not Configured	-1
Public	0
AlarmAck	1000
CtrlModReset	2000
Operator	4000
Engineer	12000

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.

12 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.

12.1 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
User Global						
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
User						
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)	
User Group						

There are no Regulatory requirements for this Section

Security item

There are no Regulatory requirements for this Section

Security Zone

There are no Regulatory requirements for this Section

12.2 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
Management Data						
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
Access Rights						
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

12.3 6000 SERIES INSTRUMENT REGULATORY DEFAULTS

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
Management Data						
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
Access Rights						
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	True /	False	True /

		False		False		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

12.4 EUROTHERMSUITE PC REGULATORY DEFAULTS

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
Management Data						
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	
Access Rights						
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	**Level of Confirmation** No Confirmation Confirm Only Note Signature Sign & Note Sign & Authorise Sign & Authorise & Note Action Disabled	**Level of Confirmation** No Confirmation Confirm Only Note Signature Sign & Note Sign & Authorise Sign & Authorise & Note Action Disabled	**Level of Confirmation** No Confirmation Confirm Only Note Signature Sign & Note Sign & Authorise Sign & Authorise & Note Action Disabled

Debug			
Operator groups			
Trend global			
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			

12.5 QUICKCHART SOFTWARE REGULATORY DEFAULTS

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
Management Data						
Sign for Annotation	False	True / False	False	True / False	True (Locked)	
Access Rights						
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

12.6 REVIEW SOFTWARE REGULATORY DEFAULTS

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
Management Data						
Sign for Annotation	False	True / False	False	True / False	True (Locked)	
Access Rights						
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

12.7 VISUAL SUPERVISOR REGULATORY DEFAULTS

This table lists the Regulatory defaults for T800/Eycon™10/20 Visual Supervisor 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
Management Data						
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
Access Rights						
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

12.8 WINDOWS DOMAIN REGULATORY DEFAULTS

This table lists the Regulatory defaults for Windows Domain security items.

> **IMPORTANT NOTE**
> **G**rey fields indicate a Read Only parameter.

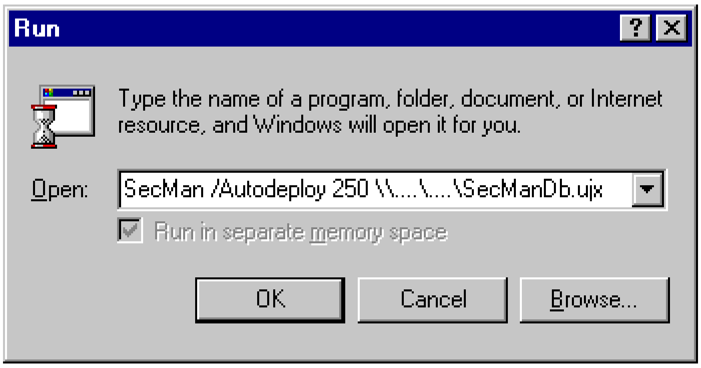
	Default		**21 CFR Part 11 - Records**		**21 CFR Part 11 - Signature**	
	Default	Range	Default	Range	Default	Range
Management Data						
Administrator UserId	Needs appropriate configuration		Needs appropriate configuration		Needs appropriate configuration	
Administrator Password	0	0 - 180	90	1 - 180	90	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
Access Rights	True	True / False	True	True / False	True	True / False
Groups	Needs appropriate configuration					

13 COMMAND LINE PARAMETERS

13.1 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

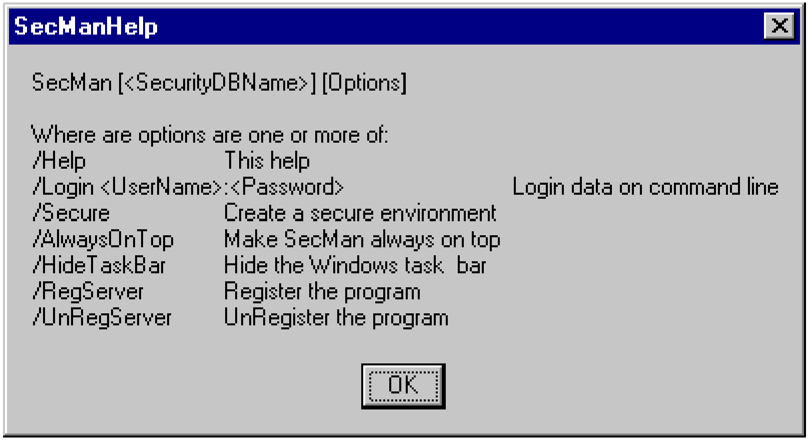


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /Autodeploy 250 \\....\....\SecManDb.ujx

☑ Run in separate memory space

This Command line parameter will run the Security Manager Utility and load the defined SecManDb.ujx database. 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.



```
SecMan [<SecurityDBName>] [Options]

Where are options are one or more of:
/Help                 This help
/Login <UserName>:<Password>              Login data on command line
/Secure               Create a secure environment
/AlwaysOnTop          Make SecMan always on top
/HideTaskBar          Hide the Windows task  bar
/RegServer            Register the program
/UnRegServer          UnRegister the program
```

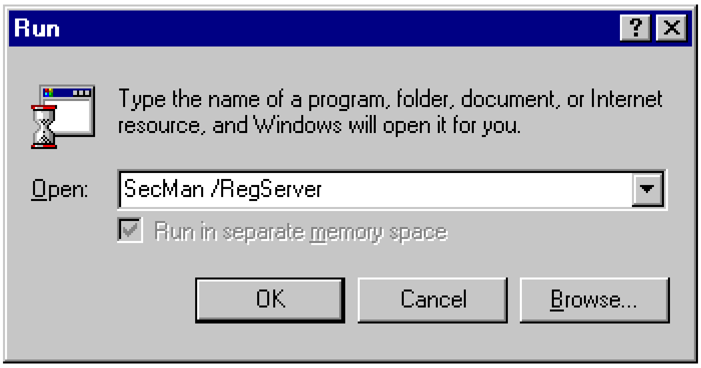
NOTE

This graphic is displayed using the /Help Command line parameter, it shows the parameters with the exception of the /AutoDeploy Command line.

13.2 /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



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /RegServer

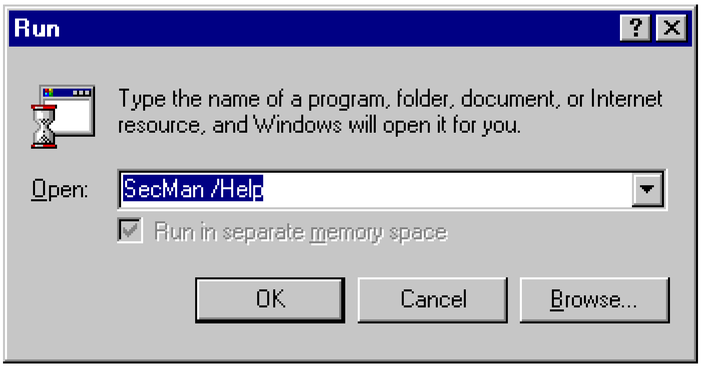
☑ Run in separate memory space

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



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /Help

☑ Run in separate memory space

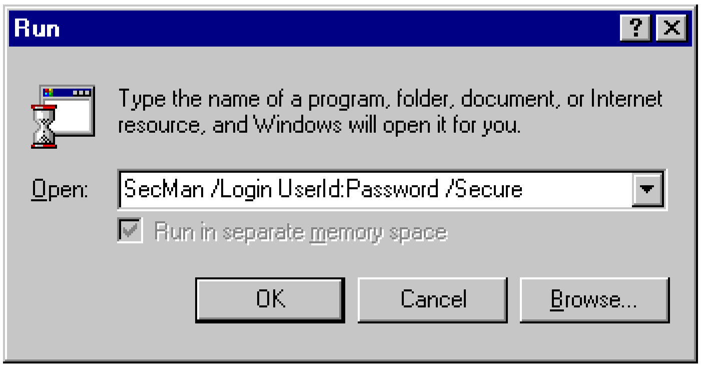
Note

This graphic is displayed using the /Help Command line parameter, it lists each additional parameter. An /AutoDeploy Command line parameter has also been included.

13.3 /LOGIN COMMAND LINE PARAMETER

This can be configured in a string with other Command line parameters.

Command line prompt example



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /Login UserId:Password /Secure

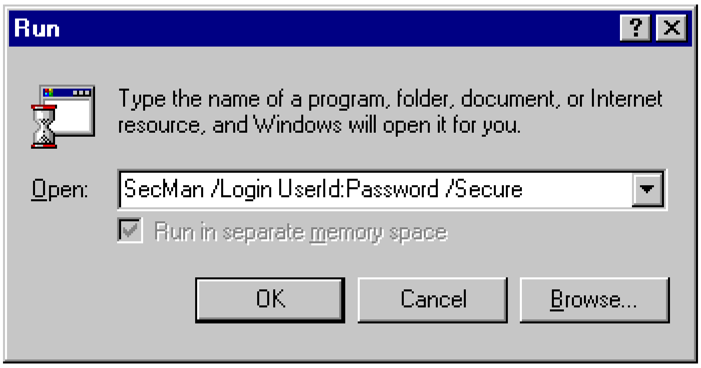
☑ Run in separate memory space

This Command line parameter will automatically enter defined User Id and Password in the Login prompt.

13.4 /SECURE COMMAND LINE PARAMETER

This can be configured in a string with other Command line parameters.

Command line prompt example



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
☑ Run in separate memory space
OK
Cancel
Browse...

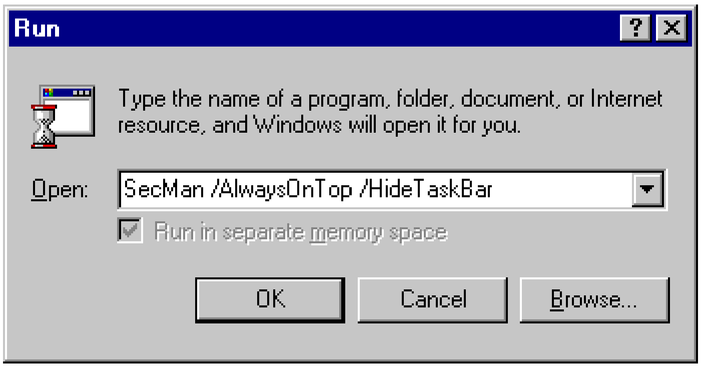
```
SecMan /Login UserId:Password /Secure
```

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.

13.5 /HIDETASKBAR COMMAND LINE PARAMETER

This Command line parameter can be configured in a string with other Command line parameters.

Command line prompt example



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
☑ Run in separate memory space
OK
Cancel
Browse...

```
SecMan /AlwaysOnTop /HideTaskBar
```

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.

13.6 /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,

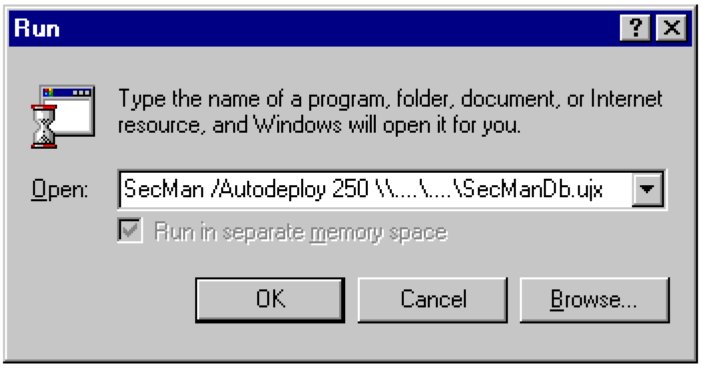
- specified in the Security zone
- listed in the PC Configuration table (**Options** pulldown)
- and the Deployable flag MUST be checked (**Options** pulldown)

It can be configured in a string with other Command line parameters.
This Command line parameter

- displays the deployment dialog with full use of the Deploy and the 'Deploy All/Zone' buttons
- compares the Master Security database revision with 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



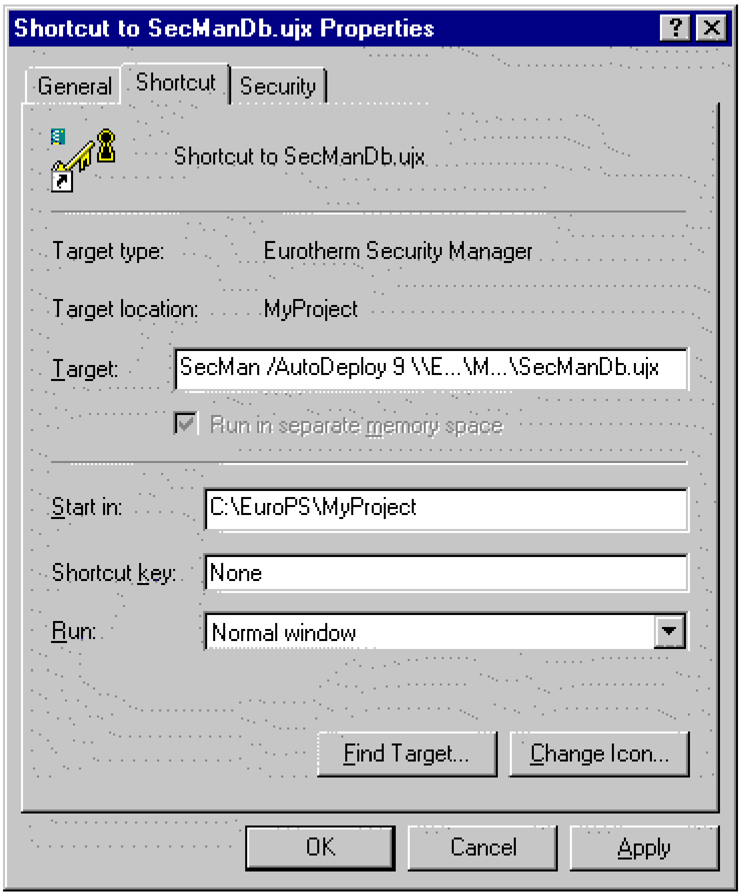
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /Autodeploy 250 \\....\....\SecManDb.ujx

☑ Run in separate memory space

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

Shortcut example



Shortcut to SecManDb.ujx

Target type: Eurotherm Security Manager

Target location: MyProject

Target: SecMan /AutoDeploy 9 \\E...\M...\SecManDb.ujx

☑ Run in separate memory space

Start in: C:\EuroPS\MyProject

Shortcut key: None

Run: Normal window

IMPORTANT NOTE

The /Autodeploy Command line parameter,

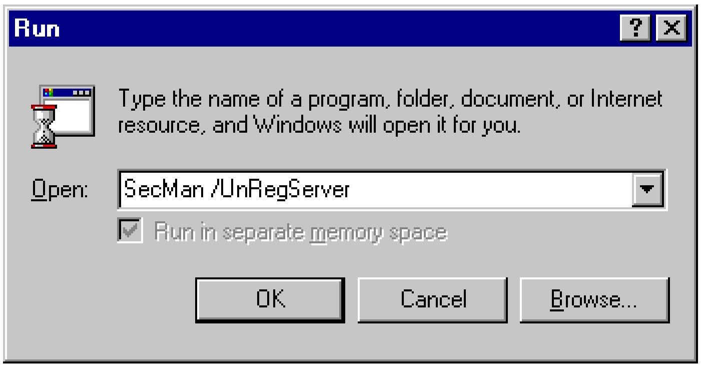
"SecMan" /AutoDeploy 60 "\\EuroPS\MyProject\SecManDb.ujx"

MUST be entered in the Target field of the shortcut properties dialog box.

13.7 /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



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SecMan /UnRegServer

☑ Run in separate memory space

This Command line parameter will remove Security Manager registry data that will stop the user from opening the database.

14 AUDIT TRAIL INFORMATION

14.1 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.

14.2 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.

14.2.1 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).

14.3 21 CFR PART 11

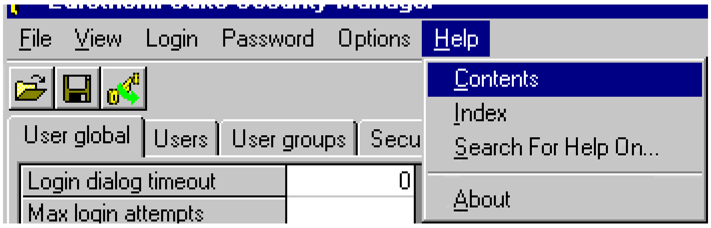
The 21 CFR (Code of Federal Regulations) Part 11 guidelines can be found on the FDA (Food and Drug Administration) web-site at the address below.
www.access.gpo.gov/nara/cfr/waisidx_02/21cfr11_02.html
A system can only be 21 CFR Part 11 compliant if enabled regulatory features do NOT exceed the regulatory parameter limits.

15 HELP MENU

15.1 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.

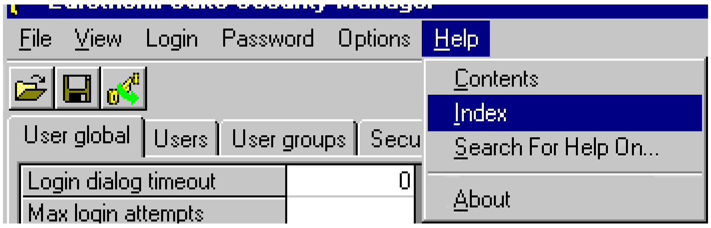


2. The Security Manager On-line Help document appears in a new window. Use standard windows Help operations to use the On-line Help.

15.2 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.

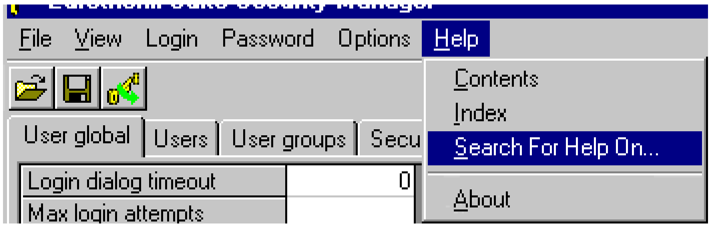


2. The Security Manager On-line Help document appears in a new window. Use standard windows operations to use the On-line Help.

15.3 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.



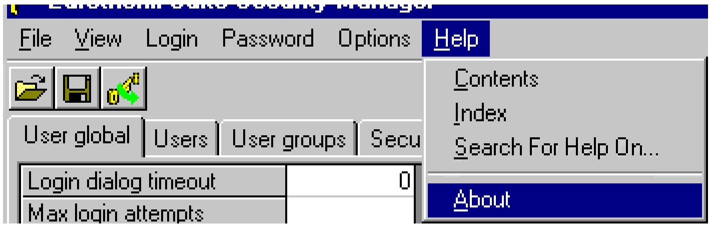
2. The Security Manager On-line Help document appears in a new window. Use standard windows operations to use the On-line Help.

15.4 ABOUT

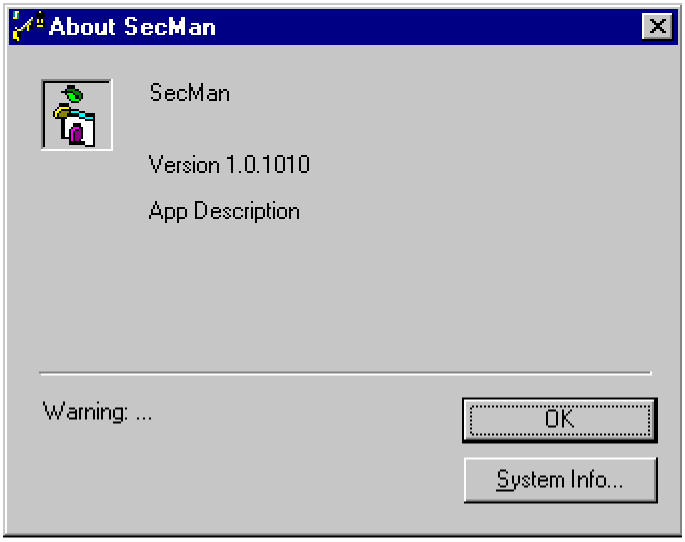
With the selection of this menu option, information about the utility is displayed including the name, version number, and description.

Display the utility details by,

1. Selecting **‘Help > About’** from the Menu Bar.



2 The About dialog window appears.


About SecMan

SecMan

Version 1.0.1010

App Description

Warning: ...

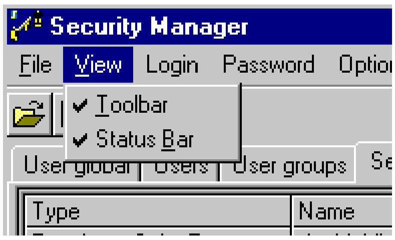
3 Select the ‘**OK**’ button to return to the previous window.

16 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.

16.1 HOW TO HIDE/SHOW STATUS BAR

1. Open the View menu and click on the Status bar item to 'untick' it.



2. The Status Bar is removed from the window.
3. Repeat the instructions to display the Status Bar.

16.2 STATUS BAR ITEMS

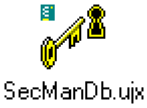
16.2.1 Security Status

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

16.2.2 Security Manager Database Location

This part of the Status Bar shows the full path location of the opened database.

16.2.3 Security Manager Database icon



16.2.4 Time

This part of the Status Bar shows the current time.

16.2.5 Date

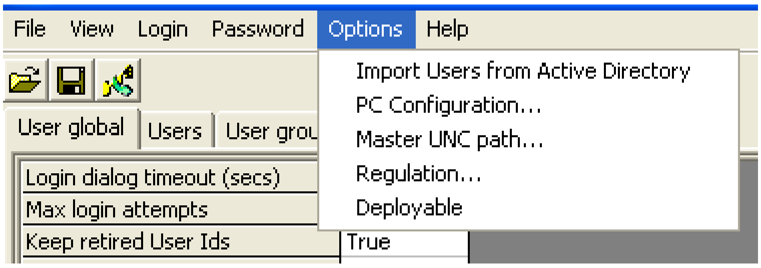
This part of the Status Bar shows the current date

17 ACTIVE DIRECTORY

17.1 IMPORT USERS FROM ACTIVE DIRECTORY

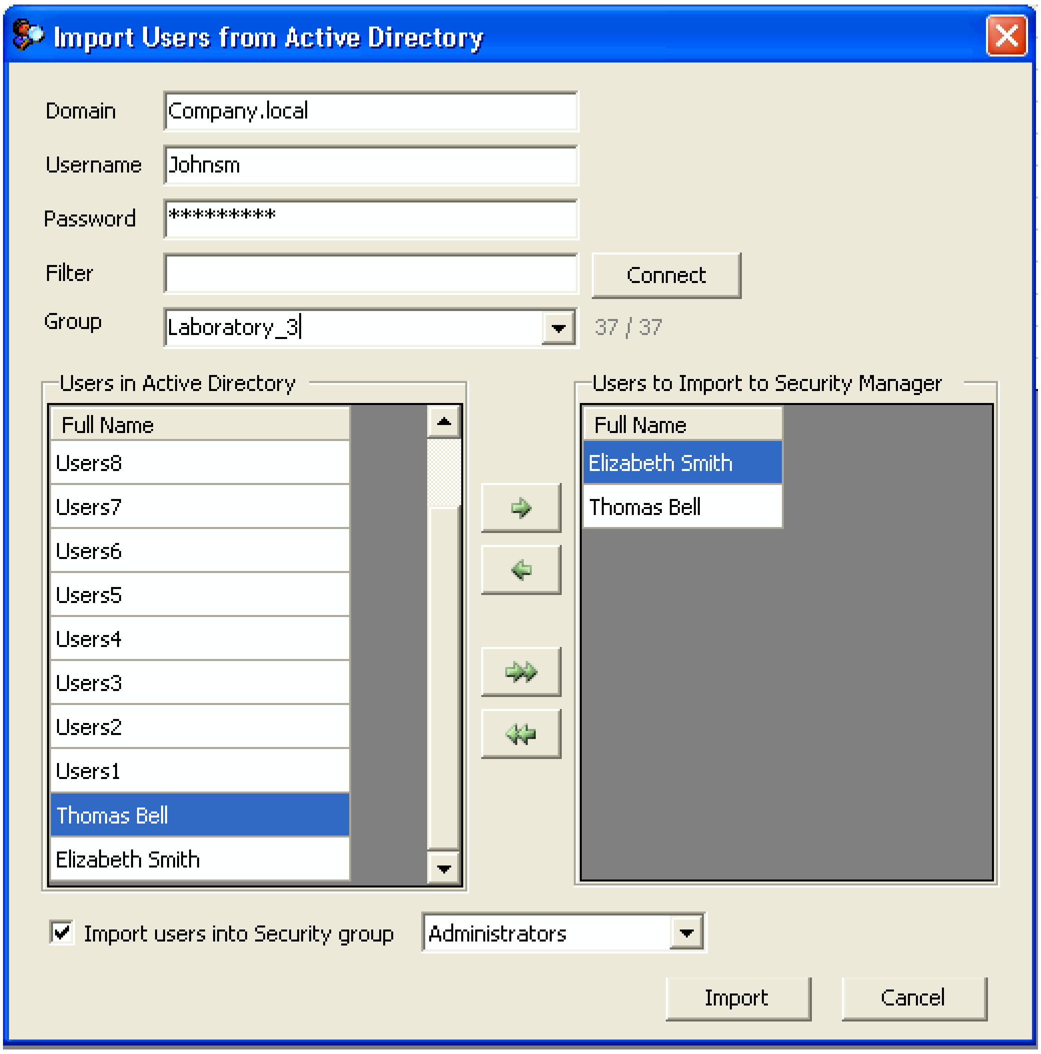
To import existing User Accounts from the Domain Server Active directory;

1. Select **'Options** > **Import Users from Active Directory'** from the Menu Bar.



2. A dialog window appears. Enter the **'Domain' DNS server name**, **'Username'** and **'Password'** and select **'Connect'**

IMPORTANT
When importing users into 'Security Manager' from an active directory Domain server, the DNS Domain name must be specified for the Domain server and NOT an IP address or NETBIOS name. If the IP address is entered it will not be possible to authenticate users at the 'Instrument' level.



Domain: Company.local
Username: Johnsm
Password: *********
Filter:
Group: Laboratory_3

☑ Import users into Security group: Administrators

3. Once 'connection' with the domain server is established, the **'Group'** field will contain a pick-list to select the required user group. The screen shot above shows the **'Laboratory_3' Group** is selected, and the users contained within it are shown in the **'Users in Active Directory'** selection box.

4. Select each required user and transfer them to the '**Users to Import to Security Manager'** box by using the transfer arrow;' ➡ '.

5. Enter a '**Tick**' into the '**Import users into Security group'** box and then select the appropriate '**security group'** from the pick-list

6. Finally click the **'Import'** button. All selected users will then be imported into '**Security Manager'.**

Note
All imported users will appear in the 'Users' page of 'Security Manager' including the Domain server name for each user.

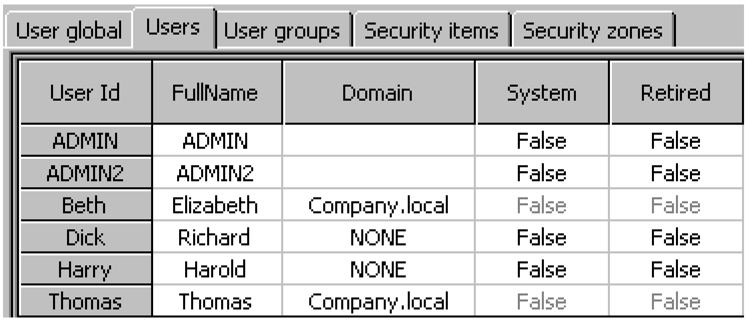
17.2 CHANGE THE DOMAIN PARAMETER

This parameter contains the Domain server name. The Domain name must be entered using the 'Import Users from Active Directory' facility found in the '**Options**' menu.

Note
Active Directory is the system which provides your network logon credentials to access network resources, applications and web sites requiring authentication

1. If the parameter is 'blank' or states 'NONE', the user account is 'local' to 'Security Manager' only.
2. If the parameter contains a Domain name, the user account has been imported from a company Domain server using the 'Import Users from Active Directory' facility.

Note
For users with a Domain name, they will always be enabled for deployment to a 6000 series recorder supporting Active Directory, unless 'retired' from 'Security Manager'



User Id	FullName	Domain	System	Retired
ADMIN	ADMIN		False	False
ADMIN2	ADMIN2		False	False
Beth	Elizabeth	Company.local	False	False
Dick	Richard	NONE	False	False
Harry	Harold	NONE	False	False
Thomas	Thomas	Company.local	False	False

3. Finally save changes.

18 OTHER INFORMATION

18.1 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.

18.2 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.

18.3 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).

18.4 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.

18.5 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.

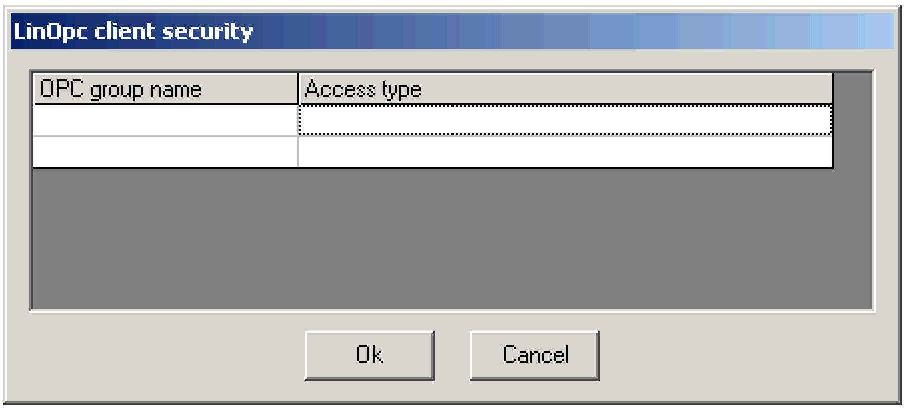
If LINOPC has to use the security defined in this file then a user will be granted either 'RO' or 'RW' access, irrespective of the block being written.

18.6 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.

18.6.1 To add OPC Group security,

1. Select **'Options** > **LINOPC Client Security'** from the Menu Bar. A dialog window appears.



LinOpc client security

OPC group name	Access type

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.

18.6.2 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 be 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

18.7 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.

18.7.1 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.

18.7.2 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.

18.7.3 create a Tag Security Area (Project Organiser)

Project Organiser must be used to create Tag Security Areas and configure the relevant Tags.

Note: 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**.

3. 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, &, _, -.

For clarity, try to use an easily identifiable name for an object, i.e. Boiler3 (Tag Security Area).

4. Select **OK** to accept the Tag Security Area name. Press **Cancel**, ☒, or **Esc**. on the keyboard to abort the operation.

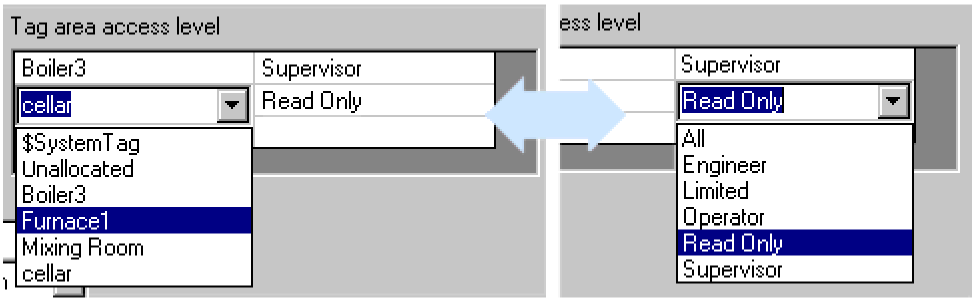
5. Refresh the display, (**View** > **Refresh** (F5)) when complete.

In the Security Manager,

6. 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.



.CSV FILES

These comma separated variable (.csv) text files can be viewed using (for example) 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 by the Administrator's setting 'Enabled' from 'False' to 'True'

or automatically if

- The number of permitted login attempts has been exceeded or,
- 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.

DOMAIN NAME

This field contains the Domain server name for user accounts associated with 'Active Directory'. If the field is blank, or states 'NONE', the user account has been established using Security Manager rather than the Domain server.
If the field contains a Domain name, or if it is required to import user accounts from a Domain server, the user account must be imported using the 'Import Users from Active directory' facility.
Note: Active directory is a system which provides network logon credentials to allow the user access to network resources, applications and web sites requiring authentication.

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 as shown in the Project Folder.
Project Folder > Networks > network directory.

PASSWORD

This column stores the password, displayed as '**xxxxxxxx**', 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 recorders, computers, and T800/ Eycon™ 10/20 Visual Supervisors 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 recorders or Visual Supervisor instruments.

RECIPE

A recipe can be;

- 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 one 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 ‘**xxxxxxxx**’, 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).

Note

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.

Index

Scan for local contacts

Eurotherm Ltd
Faraday Close
Durrington
Worthing
West Sussex
BN13 3PL
Phone: +44 (0) 1903 268500
www.eurotherm.com

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

© 2019 Eurotherm Limited. All Rights Reserved.