Eurotherm®

by Schneider Electric

21 CFR Pt 11

An Introduction to 21 CFR Pt 11

Issue 5

October 2017
HA028067U000

Contents

Introduction to 21 CFR Pt 11

Introduction

This document is an introduction to the requirements of 21 CFR Pt 11 and the functions offered by the EurothermSuite, QuickChart and Review software, the T800 Visual Supervisor, Eycon-10 and Eycon-20 LIN instruments, and the Series 5000 and Series 6000 security items.

Windows Domain security items allows Security Manager to configure users either locally on a PC or globally in 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 Domain name or a PC but it is not necessary.

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

This document describes specific terminology used in 21 CFR Pt 11 standards, that are applicable to all products.

Access control

User Accounts

A user can have any of the following states:

- *Current user*: user is granted access to different functions according to his/her group and its extended access rights.
- *Disabled user*: Security system has disabled the user account because of three failed attempts at entering password or password has expired. The administrator can change a disabled user to either a current or a retired user.
- *Retired user*: the administrator can change a current or disabled user to a retired user. Retired user info will be maintained on the system to prevent an account being reused.

User name

- Users are identified by a User ID and a User Name. User ID is used as the login name and is shorter than the User name.
- User ID and User names must be unique.
- The system is capable of keeping track of all retired accounts.
- Maximum user name lengths is 25 characters.
- Minimum user ID length is three characters.

Administrator functionality

Administrator rights will allow the administrator to:

- New users to be added with default password
- Retire user accounts. Retired user cannot be recreated so ‘uniqueness’ remains with account checks.
- Disable/Enable User accounts
- Modification of existing user account. This will (apart from your own) require confirmation from second administrator.

Password control

- Not viewable in a human readable form at any stage.
- Minimum length of password will configurable between three and eight characters.
- Users are prevented from using previous passwords.
- User IDs and passwords can’t be the same.
- New user account passwords (set up by an administrator) expire.
- Printable characters are valid for passwords with at least one non-alpha character.
- User password can only be changed by the user. Requires authorisation if password is changed by an administrator.
- Password expiry forces users to change their password.
- User accounts are automatically disabled if their password expire.
- Password is disabled if a configurable number of continuous incorrect logins are detected.
- The login dialogue will display time remaining before the password expires. Password expiry alert facility will occur when 14 days or less are left.

Automatic user logout

The current user is automatically ‘logged out’ if there is no user activity after a specified time period.

This time period is configurable per system.

T800 Visual Supervisor and Eycon-10 and Eycon-20 Instrument Access control

The default access system will remain the non-user-based system (i.e. the simple 4-level system). Once converted to the user based access system it may not be converted back.

Administrator must change access control to user based and configure users. On creation of the user based access system, the same default accounts as on V3.3 will be generated except that the ADMIN and ENGINEER user will be granted both Signing and Authorisation privileges. It also creates a second administrator, ADMIN2 with the same access right as ADMIN. This then provides two users so that authorisation may be performed.

The default accounts will expire after 1 year unless passwords are changed.

Up to 100 accounts may be present on the T800 Visual Supervisor, Eycon-10 and Eycon-20 instruments. Account details will not be held in the file system but in E^2PROM and the account information cannot be erased.

The Visual Supervisor will maintain a history of up to 200 retired USER IDs. Once a user account has been retired it shall not be possible to re-create that user account.

CAUTION

If the history of 200 Retired users is exhausted, then each time a new account is generated the oldest 'retired' user is purged from the records and that user no longer subject to the uniqueness checks. This feature is only available with the Auditor option.

Global Properties

The following information is set universally for all users.

- User ID is configurable with a minimum of three, maximum of eight and default of six characters. For non-auditor option minimum length is two characters with default of two.
- Password is configurable with a minimum of three, maximum of eight and default of six characters. Password must include at least one non-alpha character and it can't be the same as the USER ID. For non-auditor option minimum length is zero characters with default of zero.
- Password Expiry has a configurable period up to 365 days and default of 90 days. It is not possible to change the password to itself, i.e. make a null change, nor can it be set to the password previous to the current one (to prevent toggling between two passwords). On logging in a user is presented with an indication of the number of days until password expiry (if configured). If the number of days to expiry is less than or equal to 14 a flashing message will also be presented. If a user has not changed their password within the configured period the account will be disabled. T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments offers two options for recovering after a password expiry. It can be set to allow the user to change the password on the next login or alternatively the account may become current after administrator changes the password.
- Max failed logins is configurable with a minimum of 1, maximum of 99 and default of 3. This means if failed logins set to 3, the account will be disqualified on the 4th attempt if bad, else the login will be successful. The account may only be re-enabled by changing of the password by administrators. This feature is not available for non-auditor option. T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments can be configured to generate an alarm if a user is disabled by failed log attempts.
- User timeout has a configurable period from 1 to 720 minutes. Current logged in user will be automatically logged off once the user time out has expired. For non-auditor option minimum is 0 with default of 0.

User Specific properties

For 21 CFR Part 11 only each user account may have a number of configurable attributes as follows:

- Sign: the ability to issue an electronic signature.
- Authorise: The ability to authorise an electronic signature.
- View Only – Restricted to 'read' operations (i.e. not edit) at the specified access level. This allows a user to see more data but not to modify that data. In particular an administrator with this attribute will be able to view the access system but not to modify it.

Administrators and Account Management

- An administrator shall be capable of disabling another users account, and subsequently re-enabling it provided this change is also authorised by another administrator. A disabled account maybe re-enabled with the ENABLE button, this will retain the password and number of failed logins and password expiry time.
- Any account that has been disabled (either by the administrator or automatically because of login failure) shall be highlighted in red.
- An account whose password has expired will be highlighted in Orange.
- An administrator enables an account by changing the password.
- Any administrator password change (including original account creation) will cause the account to expire on next login forcing the user to change password before performing any activity.
- An administrator shall not be capable of changing the user ID or user name once it has been created and saved. Accounts that have been created but not yet saved will be highlighted in green.
- The access system will track every major change (i.e. the SAVE button) and auto-increment a revision number. The current revision number, plus the signature associated with the SAVE may be viewed with a new REVISION button.

Comparison of Access Systems

The following table compares the user based access systems between existing software (V3.3), this spec without 21 CFR Part 11 option (V4.0), and with 21 CFR Part 11 option (T800 Visual Supervisor later than V4.0-21CFR and Eycon-10/Eycon-20 V1.2). Where a value is given in brackets that indicates a default value.

Feature	*V3.3*	*V4.0*	*21CFR version*
E^2PROM Storage	No	Yes	Yes
Maximum User Accounts	100	100	100
User ID Minimum Length	2	2-8 (2)	3-8 (6)
Password Minimum Length	0	0-8 (0)	3-8(6)
Non-alpha required in password	No	No	Yes
Password change rules (not User ID, + toggle)	No	No	Yes
Password Expiry Periods in days (0 = no expiry)	0	0, 1-365 (0)	1-365 (90)
Maximum Failed logins before account disabled (0 = no disabling)	0	0-99 (0)	1-99 (3)
Unique User Names	No	No	Yes
Number of retired users in unique User ID + name checks.	0	0	200
Eurotherm SERVICE account	Read/Write	Read/Write	Read Only
Eurotherm Engineering accounts	Yes	Yes	No
RECOVERY Account	No	Yes	Option (Yes)
User Attributes (Sign, Authorise, View Only, Max Password Expiry)	No	No	Yes
Disabled Accounts highlighted in Red	No	Yes	Yes
Provisional (unsaved) Accounts highlighted in Green	Yes	Yes	Yes
Master/Slave Account System Option	No	No	Yes (Master)

EurothermSuite Access control

EurothermSuite Security is handled by the Security Manager utility (SecMan), which satisfies 21 CFR part 11 requirement. SecMan is used to globally define the security configuration for a system. Where a system includes remote security items, for example PC workstations, T800 Visual Supervisors, Eycon-10, Eycon-20, Series 5000 or Series 6000 instruments, SecMan will be used to deploy the security data required by these nodes.

SecMan will exist as a standalone executable.

The primary data configured by SecMan are: -

- Users – Individual user accounts.
- User groups – Collections of users who have the same access rights to the system.
- Security items – Objects protected by security. Typically these are instruments, PCs, or programs that require users to logon before they can use them.
- Security zones – Collections of security items, for which user groups have the same access rights.

Security Manager Utility

EurothermSuite Security Manager Utility is independent of the EurothermSuite. It allows the user account file to be configured and deployed to designated Operations Viewer nodes on the network. The utility also fulfils the requirements of EurothermSuite, QuickChart and Review and Windows Domainsoftware, the T800 Visual Supervisor, Eycon-10 and Eycon-20 LIN instruments, and the Series 5000 and Series 6000 security items.

There are two options: High security and standard security. Phase 1 only supports High security option. This option forces values of certain parameters to have a specific range which will make the product 21 CFR Part 11 compliant.

All security changes are treated as events and will be stored in the audit trail.

There are no limits to the number of current and retired users.

To access the utility a login will be required. Users without administrator rights will only be able to change their own passwords.

Global Properties

The following information is set universally for all users.

- Login dialogue timeout has a configurable period from 0 to 120 seconds. Default is zero, which disables the features.
- Maximum login attempts are configurable with a minimum of 3, maximum of 99 and default of 3. This means if failed logins set to 3, the account will be disqualified on the 4th attempt if bad, else the login will be successful. The account may only be re-enabled by the administrator setting the Maximum login attempts count to zero.
- Keep retired User IDs ensures that retired User IDs are not deleted. This field can't be changed for 21 CFR Part 11 systems.
- Minimum User ID length is configurable with a minimum of three, maximum of eight and default of six characters.
- Maximum User ID length is configurable with a minimum of three, maximum of eight and default of eight characters.
- Minimum Password length is configurable with a minimum of three, maximum of eight and default of six characters.
- Maximum Password length is configurable with a minimum of three, maximum of eight and default of eight characters.
- Password reuse period defines the period after which a password can be reused. The minimum period is 1 year.

Users

User accounts are created and given access rights to the various security items in the system, one of which is SecMan itself. Each user account has the following attribute, which need to be configured by the administrator.

- User ID is configurable with a minimum of three, maximum of eight and default of six characters.
- Password is configurable with a minimum of three, maximum of eight and default of six characters. Password must include at least one non-alpha character and it can't be the same as the USER ID.
- 'Password must change' will be automatically set to true when the password is changed by administrator. Administrator can set this flag to true to force a user to enter a new password.
- Password expiry has default of 90 and maximum of 180. It can be changed by administrator.
- Remote User ID is intended for 5000 series, Future.
- Remote password is intended for 5000 series, Future.
- Full name has a maximum of 25 characters and must be unique.
- 'System' identifies an account, which is used by the system to perform system functions; it cannot be used by a user to logon. For example on an EurothermSuite PC, System accounts are most commonly used to download recipes. This means a user may be given the right to start a recipe, but not the direct access to the tags referenced by the recipe. When the recipe is executed the writes are performed under a system account that has access to the tags referenced by the recipe.
- Retired is to true by the administrator. Once an account is retired it can't be re-enabled. There is no limit to the number of retired users.
- Enabled field is used by the administrator to temporarily to lockout an account.
- Login attempts show the number of continuous failures. A successful login resets the count to zero.
- Locked out shows whether a user has been locked out by login failure, password expiry, etc.
- Locked out reason field shows the reason why a user is locked out.

User groups

The User page allows user groups to be defined and to be allocated to groups. A user may be allocated to more than one group. This allows giving a user different access level in different security zones. There is no limit to the number of users and user groups.

Security Items and Areas

In a medium or large plant it is usual to have several areas where not all individuals at the plant have the same status in all areas. The user accounts have a set of {Areas, Privileges} assigned to them. A single password file will hold all the mappings.

Individual instruments will not support areas directly but the User Account Utility will allow instruments to be mapped into areas using the instrument node number. A consequence of this is that an instrument can only be in one area.

EurothermSuite PCs will support multiple areas.

Security Items page will be used to define objects which users can login to and get access rights. With the existing systems a security item can be a thought of as a node such as EurothermSuite, QuickChart and Review software, the T800 Visual Supervisor, Eycon-10 and Eycon-20 LIN instruments, and the Series 5000 and Series 6000 security items.

Windows Domain security items.

Security Zones: **From the Security zones page, user groups' access right is set for each security zone.**

Security Manager is a permanent security zone, which defines the access control within the Security Manager.

User access rights to SecMan

The following information is set for each user level:

- Edit security data - Enable user right to edit all security data.
- Audit security data - Enable user right to audit all security data.
- View security data – Enable the user right to view all security data.
- Change own password - Enable user right to edit their own passwords.
- Sign - Enable user right to sign changes.
- Authorise - Enable user right to authorise changes.
- Inactivity timeout - Inactivity timeout in minutes before SecMan locks up.

If a user fails to login to an account with any of the rights 1 to 5, he will have no access to the Security database (SecManDb).

The following information is set for EurothermSuite nodes.

- Sign
- Authorise
- Inactivity timeout
- Task Switch
- Operator group global
- Operator groups
- Trends
- Display access level
- Shutdown view
- Change language
- Synchronise files
- Override server redundancy
- Faceplate configurator
- Print
- Debug
- TagEdit
- Operator Point Display
- Recipe
- Tag area access level

The following information is set for Visual Supervisor nodes. This feature is not available in phase 1.

- Sign
- Authorise
- Access level

SecMan Electronic signature

The enabling of the electronic signature feature is configurable. If it is enabled the user may be required to enter signing and authorisation signatures for any of the following events

- Updating the Security database (SecManDb)
- Deploying Security database (SecManDb)

If signatures are required then only users with the Sign / Authorise access rights to SecMan will be allowed to do so.

SecMan Audit trail

The following events will cause audit trail messages to be written to tamper resistant .uhh files: -

- Login/Logout
- Exceeded login attempts.
- Saving configuration changes to the master Security database (SecManDb).
- Deployment of Security database (SecManDb)
- Security configuration audit
- Failure to generate an event alert

All messages will include the Security database (SecManDb) revision.

SecMan Password uniqueness

Each time a user password is changed it is stored in a password history. This allows SecMan to ensure that a new password is unique within the password reuse period.

The only exception to this rule is when an administrator is changing someone else's password and the 'Password must change' flag is set. In this instance the administrator can enter a non-unique password.

Access to the Security database

The security information will be held in a single encrypted database for the whole system. The Security Manager will be able to access the database over a network using standard file sharing.

The database will have a 'Locked to PCs' feature that, when enabled, will limit the access to the database to a defined group of PCs. The method of locking the database to PCs will not be published, and users should be aware that any change to the hardware on the PC might cause the utility to no longer function on that PC.

For backup purposes it will be normal to have at least two PCs enabled. Recovery of the file can only be achieved by returning the file to the manufacturer.

The utility will start with the feature 'Locked to PCs' turned off and a default account. The feature can only be turned on from a PC that the utility can run on. Disabling the feature will require authorisation.

Deploying Security database

On deploying the security database to EurothermSuite nodes the following will happen:-

- If a security database doesn't exist then the security database is copied into the remote node.
- If a security database already exists then the existing database is synchronised with the master.

Security Manager's management data

SecManDb contains one permanent zone by default it is called 'Security Manager'. This zone contains the 'Security manager' security item, which will appear on the tabbed display in the right hand pane. As for the other security item types, this shows the access rights Users / 'User groups' have to the Security Manager, which comprise the following.

- Audit trail - If this is enabled SecMan will generate audit trail messages.
- Signing - If this is enabled SecMan will require a signature before it allows a property to be updated that requires signing.
- Authorisation - If this is enabled SecMan will require a authorisation signature before it allows a property to be updated that requires authorisation.
- Recovery user - If this is enabled it will be possible to login as a recovery user. This feature is used where the user is unable to login for some reason (e.g. the passwords have been forgotten, the accounts have expired). The recovery user has full access rights and is logged in using a blank User ID, and a password supplied by Eurotherm.
- Disaster recovery user - If this is enabled SecMan will automatically enable the recovery user feature if it detects that it is no longer possible to administer the system.
- Change own expired password – Allows users to edit their own expired passwords.

Security Manager Recovery

It is possible for the security system to become unusable if sufficient accounts are locked out for various reasons such as passwords expiring or being forgotten.

To cope with this SecMan has a special user account, known as the recovery user. The recovery user has full access to the security data. To login as the recovery user requires a special password to be supplied by Eurotherm that expires within an hour.

This recovery strategy is as follows:

- Contact Eurotherm for a special password, which is date dependent. The special Password expires after an hour.
- Login with a blank User ID and the special password.
- Once logged in then the user has full access to the Security Manager.
- If this recovery strategy is turned off by the users then there will be no recovery strategy available except for the security database to be returned to Eurotherm.

T800 Visual Supervisor, Eycon-10 and Eycon-20 Loss of Privileges Recovery

If the customer fails to maintain the account system properly it is possible that they may end up in a situation where they have locked themselves out of access to certain parts of the system.

Scenarios include:

- All administrator accounts expire. No access to user accounts can be made.
- All administrator password/accounts are ‘forgotten’. No access to user accounts can be made.
- All accounts with signing and or authorisation either expire or are ‘forgotten’. No access to signing and/or authorisation components can be granted. If the cause of loss of access due to ‘forgetting’ passwords and/or user IDs, access will remain locked and the recovery strategy not available. The situation may be forced by making erroneous log-ins to the administrators until their accounts are disabled.
- No pair of accounts with signing and or authorisation at ADMIN level is still current. No access to signing and/or authorisation components can be granted. In the case of password expiry the accounts may be enabled by logging in with the old password, then changing the password. The recovery account will still be enabled under these circumstances.

This recovery strategy is as follows:

- A message will be displayed on the access screen indicating that this situation has arisen.
- A new button ‘RECOVER’ will replace the ‘USERS’ button.
- Pressing the RECOVER button will present a new page, which will display a number. This number (derived from instrument specific information) together with the date and time must be relayed to Eurotherm who will issue a password. The password will be formed of alphanumeric characters. This password may then be used within one hour of the above screen being first displayed to allow a recovery user access. The recovery user will be able to:
- Have full access to the account system to create and enable accounts (without any further authorisation). The status pane will continue to indicate ‘LOCKED’ throughout.
- On exit from the access system the user will be logged out, preventing access to any further parts of the system.
- If this recovery strategy is turned off by the users then there will be no recovery strategy available except for the instrument to be returned to Eurotherm.

Central Security configuration (*Phase 2*)

For systems with a number of T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments and Operations Viewer, going round every unit and changing the password (forced by the expiry date feature) will be very time consuming.

Where the users are the same across all the T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments units, having the facility to set up the security from a single node and deploying it to other nodes will be required.

Accounts will be centrally managed via the Security Manager. It will have the ability to deploy new user accounts or change the state of user accounts on remote PCs/instruments via the network.

The central password file will be locked to a single machine, but can be moved to other PCs with appropriate authorisation. The User Account Utility will be able to be run from more than one PC but will change the password file on the current master PC. This will allow the operators to change their passwords from their own PCs. Control of which PC holds the master version of the file will be for the customer to implement.

The processes of exporting the account information is be implemented by transfer of files from the Master to the Slave. There shall be 2 files transferred, the first shall contain all the account information of existing and deleted (or retired) users in an encrypted format and the second that be an authorisation file (also encrypted) that shall contain a cross-reference (with checksum) to the account information, plus administration authorisation (i.e. login), plus a time stamp.

T800 Visual Supervisor, Eycon-10 and Eycon-20 central security configuration

It is possible to transfer the account information to/from T800 Visual Supervisor, Eycon-10 and Eycon-20. These can be configured as:

- Master Account Systems: A system that may fully manage its accounts and export its account information to another.
- Slave Account Systems: A system that may not create/delete/retire accounts but only import its account information from another, but not export.

Disk Export from a Master Account System: From the account management facility it is possible to export the account information onto a floppy disk which may then be imported onto a slave account system.

Network export from Master Account Systems on a T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments.

It is possible to configure the master account system to export its account system across the network to up to 32 (i.e. same as number of EDBs) slave account systems.

This is a T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments that does not have account edit capabilities, but is capable to importing an account information from a Master Account (21 CFR part 11 only). A slave account system may be “bound” to one particular master. The master may optionally supply a key to an unbound slave system; this key must then always be used to make any update to slave system, thus preventing other nodes from over-writing the access system.

A slave account system will not perform any of the following:

- Add user accounts
- Delete/Retire user accounts
- Manually disable user accounts
- Change the attributes of a user account
- Change any of the global account features
- Change user passwords (to enable accounts)
- Enact the recovery strategy if required

It may however do the following:

- Change to a master account system (subject to usual signatures where appropriate). This will unbind the account system.

A Slave Account system shall ‘poll’ to see if new account information has been downloaded. If the appropriate files are present then the process of account update commences. This will comprise the following steps:

- Validation of the authorisation file. Validation will comprise
  - Asserts the authorisation file has syntactically legal contents
  - Assert the authorisation file correctly identifies the account information file.
  - Assert the authorisation file can ‘log in’ with administrator rights on the slave.
  - Assert the update is within five minutes (value TBD) of the issuing of the authorisation file at the master.
  - Generate an account update failed event if any of the above fail.
  - Assert that the authorisation file locking key matches (if any key previously supplied).
- If authorised then the downloaded information will supersede the existing information. The following rules will apply
  - If a download user has a new password, and then the number of failed retries will be reset to 0, the password expiry reset and if the account was automatically disabled then it will be re-enabled.
  - If a downloaded user has the same password, password expiry and failed login count will not be reset
  - If a downloaded user has been manually disabled, the account will now be disabled.
  - If a downloaded user is enabled, whereas the local account had been disabled, the account will not be re-enabled.
  - If a download user did not previously exist a new account will be created.
- The downloaded files will be deleted.

Note
If the new account system invalidates (disables or deletes/retires) the currently logged in user no immediate action will be taken. The user shall remain logged in, but shall not be able to log in again once logged out.

Disk Import from Master Account Systems:

From the Master account management facility it is possible to export the account information onto a floppy disk which may then be imported onto a slave account system.

On a slave T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments system, an administrator is capable of importing an account system from floppy disk (generated on a master account system). This shall import using the above strategy, but must be imported within 1 hour of original export.

Audit Trail

The Audit trail will contain all events and alarms. There are four types of event messages: Non Operator, Permitted, signed, signed and Authorised. Each event type records a slightly different set of information in the Audit Trail.

- Non operator event which is either system events or universal events record.
  Date/Time, Action, Previous and new value (where appropriate)
- Permitted events, where the user has logged in the audit trail messages will have the following fields: (User information is added)
  Date/Time, Action, User ID and/or User name (depending on output device), Previous and new value (where appropriate).
- Signed is where a user has to prove that he is the person logged in by re-entering his password. Signed additionally will have an optional Reason note.
- Signed and Authorised is where a second user has to enter his/her user ID and password. Signed and Authorised additionally has the Authorisation individual with full user name.

T800 Visual Supervisor, Eycon-10 and Eycon-20 Audit Trail

Elements of Audit Trail

The Audit trail will contain all events and alarms that may be recorded into the alarm history.

The following new (or modified) elements are added to the audit trail.

- All existing events will be recorded with the USER ID (max eight characters) of the currently logged in user if the event is generated directly by a user action.
- If the user is an implied user, the USER ID will appear in brackets (e.g. '(FREDBL)' as opposed to 'FREDBL'). The brackets indicate the logged in user at the event time.
- If the user action required authorisation it shall be recorded with the ID of the person who authorised (max eight characters) it in addition to the person who instigated it.
- If a reason (maximum 16 characters) is supplied as part of an electronic signature this shall also be recorded with the event.
- Events generated on another Visual Supervisor (if other Visual Supervisors are configured to direct their events to that Visual Supervisor). Such events will be recorded as text only, but will be recorded with the node number from which they originated.
- Operator notes are extended from 16 to 24 characters for SVGA displays. Operator notes are not subject to authorisation, nor do they have reason text associated with them, as they do not affect planed operation or configuration in any way.
- LIN dB value changes will be recorded with value before and value requested to be written. NOTE: This may not be the value actually written (it could for example be clipped), however it will be the value seen by the person signing and the person authorising the change.
- A dB stopping event will be generated (in addition to the existing dB stopped event). This allows detection in logging files of lost events due to dB being stopped but not re-started.
- Each time a file from the filing system is read an event shall be recorded with a checksum of the file – this enables any changes in file contents to be noted in the audit trail.

The following access system events shall be added:

- Addition of new user
- Deletion of user
- Disabling of account due to failed logins
- Disabling of account due to password expiry
- Manual (Administrator) disabling of account
- User password change
- Administrator change of password

System Changes

The table below identifies the system audit trail events that are generated and any values recorded with the changes (if applicable). **If the event is not listed here it is not included in the audit trail.**

Event	*Values*	*Existing*	*Notes*
Manual Clock change	New Time/date	Yes	
Password expiry time	USER ID	No	
Failed login Count	USER ID	No	
Inactivity timeout	USER ID	No	
Minimum password length	USER ID	No	
Minimum User ID Length	USER ID	No	
Password change	USER ID	No	
Account disable	USER ID	No	
Account enable	USER ID	No	
Account delete/retire	USER ID	No	Event is ‘delete’ on non-21 CFR part 11 and ‘retire’ on 21 CFR part 11
Account purge	USER ID	No	
Recovery account disable/enable		No	
Master account enable/disable		No	
Access system save	Revision Number (V4.1 onwards & 21 CFR part 11 Only)	No	No details of the changes. (21 CFR part 11 Only)
Account system import		No	No details of changes (of who if across ALIN).
Account system import reject due to authorisation file expiry		No	(21 CFR part 11 Only)
Account system import reject due ‘other’ errors with authorisation file		No	No details of error (file is not user generated). (21 CFR part 11 Only)
Signature fail (due to incorrect user ID/password)		No	(21 CFR part 11 Only)
Authorisation fail (due to incorrect user ID/password)		No	(21 CFR part 11 Only)
Account system bound to master.		No	(21 CFR part 11 Only)
Account system unbound from master.		No	(21 CFR part 11 Only)
Comms set up		No	No details of comms set up changes.
Date, time and duration formats	New format	No	(21 CFR part 11 Only)

Event	*Values*	*Existing*	*Notes*
Soft reset (self-test)		No	(21 CFR part 11 Only)
Language change	New language	No	(21 CFR part 11 Only)
Self-test relay change (Health or run)	New value	No	(21 CFR part 11 Only)
Network audit trail save	Revision Number (V4.1 onwards & 21 CFR part 11 Only)	No	No details of set up change.
Electronic Signature save	Revision Number (V4.1 onwards & 21 CFR part 11 Only)	No	No details of the changes. (21 CFR part 11 Only)
Electronic Signature update (import) from disk.		No	No details of the changes. (21 CFR part 11 Only)
File checksum on read	File name	No	May be truncated on ¼ VGA. This may be used to imply a change.

The following changes are not covered by the audit trail:

- Display panel brightness settings changes
- Display panel timeouts changes (except access logout)
- Language change
- Date/time display format
- General file copy/downloads/delete/changes – These are only observed by virtue of checksum reports initially, and subsequently full file configuration management.

Application Changes

The table below identifies the application audit trail events that are generated and any values recorded with the changes (if applicable). **If the event is not listed here it is not included in the audit trail.**

Event	*Values*	*Existing*	*Notes*
Program, Recipe, dB SAVE	Filename	Yes	Does not include event for over-write of existing file.
Program, Recipe, dB DELETE	Filename	Yes	
Program change whilst running	Program Name Segment Name Value change	No	For any change to a running program all 3 events are generated in the listed sequence.
Program Iterations changes prior to RUN	SPP_CTRL.Num It tag Old Value New Value	No	21 CFR part 11 Only
Block field change	Field Tag Old Value New Value	No Yes	Only ‘tagged’ variables. On non 21 CFR part 11 systems
Alarm priority change	Alarm Tag Old Value New Value	No	21 CFR part 11 Only
Block delete	Block name	No	Database Stopped. Non 21 CFR part 11 Only
Block create	Block name	No	Database Stopped. Non 21 CFR part 11 Only
Hot/Cold start strategy enable/disable		No	
Hot/Cold start times	New time	No	

Review of Audit Trail

The Audit trail will be reviewable on all existing audit trail output devices : alarm history, trends, printer and logging files.

The Audit trail is internally buffered in DRAM and each output device maintains its own 'pointer' into the buffer to log events at its own rate. If the output device fails to consume the event before the buffer is overrun then that device will 'Lose' that event. The internal buffer can have up to 250 entries.

The time stamps for Audit trail messages are given in the local time of the T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments, except for cached block alarm updates (excluding the software alarm) with time synchronisation configured. In this case the time will be the time at the originating node, unless the time stamp is deemed to be potentially 'unsound' in which case local T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments time will be used. If the time is deemed 'unsound' and local time is used then times and dates will be displayed/printed/logged with '*' as the delimiter (this may be configured to be another character is required), e.g. `12:45:03 27/09/02` will be shown as `12*45*03 27*09*02`. The time on a remote node will be considered 'unsound' under any of the following conditions:

- There is no known time synchronisation at the remote node (all existing instruments will be perceived as having no time synchronisation).
- The local T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments is configured for time synchronisation, but is not currently in sync.
- The local T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments is in synchronisation, but the last change was 'large' and a time drift is still in place and is more than two seconds.
- Recovery from a communications outage.

The specific details of each output device is listed below:

Alarm History

Initial entry to alarm history is as per version 3.3. Pressing the 'down' key will convert the alarm history into a multi-line per entry display displaying all other elements of the record.

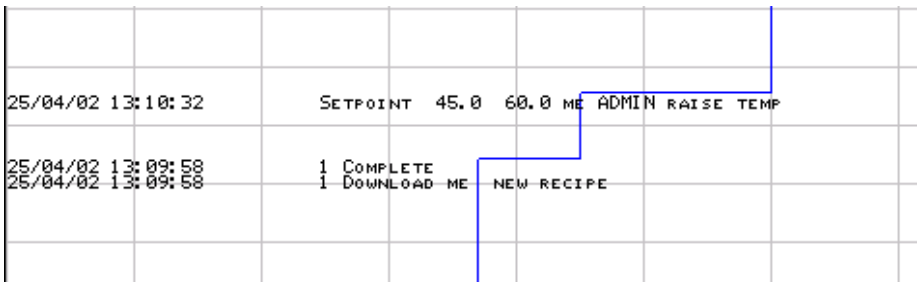
		TYPE	ACTIVE	CLEAR	ACK
Setpoint	45.0	60.0	25/04/02 13:10:32	-------- --------	-------- --------
raise temp			me ADMIN		
1	Complete		25/04/02 13:09:58	-------- --------	-------- --------
1	Download		25/04/02 13:09:58	-------- --------	-------- --------
new recipe			me		
T800	Load		25/04/02 13:06:32	-------- --------	-------- --------
Raise temp			me TheBoss		
me	Log On		25/04/02 12:53:23	-------- --------	-------- --------
			me		
Database Started			25/04/02 12:53:10	-------- --------	-------- --------

It should be noted that sometimes text will be truncated (even on the SVGA) on the alarm history (e.g. Tagnames > 16 characters). Where this happens the fact that text has been truncated will be highlighted. The full text can be seen using the event log.

Trends

The data on trends will the same, except that where a User ID can be associated with an event that USER ID will be appended to the end of the event text. For 21 CFR part 11 systems any authorisation and reason shall also be attached.

It should be noted that sometimes text will be truncated (even on the SVGA) on the trends (e.g. tag names > 16 characters). Where this happens the fact that text has been truncated will be highlighted. The full text can be seen using the event log.



Printer

By default the printer will add any USER ID associated with an event to the end of the text.

```
25/04/02 12:53:23          me Log On          me
25/04/02 13:06:32        T800 Load            me       TheBoss  Raise temp
25/04/02 13:09:58           1 Download        me                new recipe
25/04/02 13:09:58           1 Complete
```

For custom text the USER ID will be a new field available to add into custom formatting of alarms and events. For 21 CFR part 11 systems any authorisation and reason may also be attached.

Logging Files

As trends, it will also include full user name.

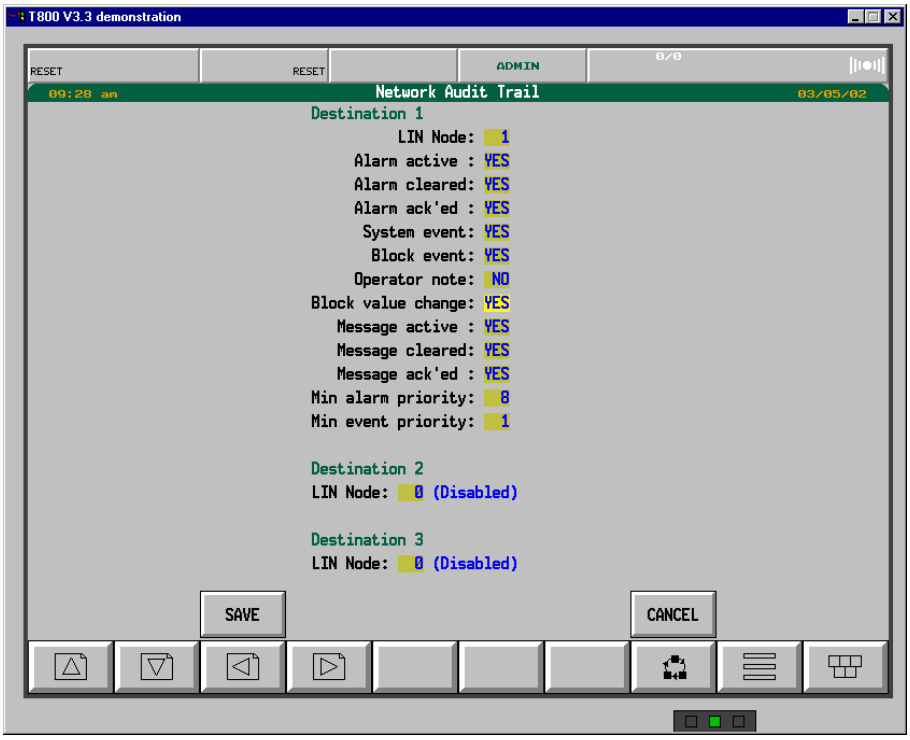
Event Log

A new facility is provided to view the audit trail / event log on screen in an equivalent manner to that presented on the printer, logging or trends. This page is capable of displaying all buffered events (up to 500). It is possible to see all text (maybe with line breaks) using this facility. This facility will also be available when the application is not loaded hence providing full visibility of the audit trail at all times.

Remote Recording of Audit Trail

The Audit trail generated on the T800 Visual Supervisor, or Eycon-10/Eycon-20 may be configured to be directed to up to three remote loggers. The remote logger initially includes EurothermSuite, and subsequently to another T800 Visual Supervisor (phase 2) or Eycon-10/Eycon-20.

Each logger will receive every audit trail event in sequence. Each logger will have the facility to re-synchronise its recording of the audit trail to its last known event (provided the internal Visual Supervisor buffer has not over-run). If the buffer has over-run then a specific over-run event may be generated.



Import and Export of Audit Trail configuration

The network Audit trail configuration may be imported or exported using the floppy disk cloning facility. Only ADMIN level users may clone in or out. The cloned in data will not take effect without a power cycle.

Configuration File Administration

The configuration file administration function is designed to ‘deter and detect’ unauthorised changes to the configuration.

This function is to be achieved in two distinct phases.

Currently it provides the file checksum (identified above) in the audit trail to allow manual checking of the audit trail to identify if any key element has changed since last used. The checksum will include the file name, which implies if a file is copied to a new name it will have a different checksum. In addition for those elements of the configuration that are editable on the instrument (programmer, recipe and database), these shall be prohibited from running if they have been edited without saving. For a programmer this only includes program edits prior to running. For a database it only includes function block manager edits when stopped.

The second phase will include a complete on-instrument configuration file administration facility. This is to be achieved by:

1. Providing the facility to designate certain file types (identified by their file extension) as ‘regulated’.

Note
This will apply only to files on the local ‘E’ drive; there will be no (local) regulation of files on other drives or nodes.

2. Providing the facility to register individual regulated files on the instrument. Once registered, a file may be set up to be either enabled or disabled. Access to a regulated file will be inhibited unless (a) the file has been registered, (b) it has not been modified since registration and (c) it is currently enabled. This will prevent an unapproved file from being used in any way until it is explicitly authorised from the front panel by an appropriate user.
3. Allowing re-registration of a file, which has legitimately changed, maintaining a (local) revision number.

EurothermSuite Audit Trail

Elements of Audit Trail

The Audit trail will contain all events and alarms generated by EurothermSuite. Audit Trail is recorded into the alarm history.

To provide for a centralised audit trail, EurothermSuite allows Operation Servers to be a central audit trail server. Instruments are able to send audit trail events over the LIN network to two servers.

Audit trails will be stored in a 'tamperproof' format .uhh. This format will be common across multiple Eurotherm products. This file will be accessible in a human-readable form via an E-review Active X.

Event Log providers will be able to send its audit trails over the LIN network (via Arcnet or Ethernet media). The provider will buffer events in case of floods of events or if the network has failed. If the buffer overflows then that will be recorded as an event. Each event log message will have a unique ID across all nodes. This will allow viewing software to identify if two messages are the same.

The following new (or modified) elements are added to the audit trail.

- Each Operations server stores the Audit trail in an .uhh with a unique file name (e.g. includes node name and date). The UHH file are viewable and printable via EReview
- The Operations server will be capable as acting as an Event log Consumer. It will be able to cope with up to 60 nodes sending it events.
- The audit trail can be recorded at more than one node for redundant operation.
- All existing events will be recorded with the USER ID and full User name of the currently logged in user if the event is generated directly by a user action.
- If the user action required authorisation it shall be recorded with the ID and full user name of the person who authorised it in addition to the person who instigated it.
- If a reason is supplied as part of an electronic signature this shall also be recorded with the event.
- Events generated by a Visual Supervisor will be recorded and will include the node name from which they originated.
- System events such as starting an application will be audit trailed.

In general the PC time stamp the remote audit trails with the message time stamp. If the message time stamp is suspicious then the PC time will be used for time stamping the message, and the message text will be followed by the message time and what is bad about the time. The bad time can be caused by:

- Provider and recipient not synchronised
- Provider is out by too much
- The provider have been off-line, therefore the time stamp may be from a previous day.
- The provider doesn't have a time stamp.

Security Manager Audit Trail

Security Manager creates its own tamperproof Audit trail file which is held in the projects History directory. Audit trail includes login, logout, loading and unloading the Security database (SecManDb) and any changes to the Security database.

Application Changes

The table below identifies the application Audit trail events that are generated and any values recorded with the changes (if applicable). **If the event is not listed here it is not included in the audit trail.**

Event	*Values*	*Notes*
Block field change	Field Tag	
	Old Value	
	New Value	
Recipe Download		

Review of Audit Trail

The Audit trail is reviewed on alarm history, trends, printers and logging files.

Time Synchronisation

It is possible to configure a time synchronisation service from a EurothermSuite system to synchronise the clock in the T800 Visual Supervisor, Eycon-10 or Eycon-20.

To provide time synchronisation throughout the system, one or more 'Time and Date' master systems will regularly broadcast this data. The TOD_DIAG functionality will be supported in NTSE and LIN instruments such as T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments and T940(X).

It is expected that in most large systems the PCs will be the time masters. On the PC the ES time master process (NTSE) will derive its time from the PC clock. The PC clocks will be kept in synchronisation using the Windows Time Services (See below). If the PC clocks need to be synchronised to an external source (e.g. rugby clock), it is assumed that this will be provided by the project or customer.

Windows time services

When the local clock offset has been determined, the following algorithm is used to adjust the time:

- If the local clock time of the client is behind the current time received from the server, W32Time will change the local clock time immediately.
- If the local clock time of the client is more than three minutes ahead of the time on the server, W32Time will change the local clock time immediately. ***Changing the time on a logging system backwards is a 'recipe for disaster'.*** Review can only accept one sample per instance of time. In the case of backward time, Review will discard the oldest data.
- If the local clock time of the client is less than three minutes ahead of the time on the server, W32Time will quarter or halve the clock frequency for long enough to bring the clocks into sync. If the client is less than 15 seconds ahead, it will halve the frequency; otherwise, it will quarter the frequency. The amount of time the clock spends running at an unusual frequency depends on the size of the offset that is being corrected.

The synchronisation requests shall be issued every 15 minutes. Time synchronisation mode changes can only take place while the LIN database is running. If a LIN dB is unloaded the LIN instrument shall remain in the mode it was when unloaded, i.e. if it was a time master/slave it shall remain as a time master/slave.

Provided the modified time remains within three minutes the time shall be maintained as a monotonically increasing value (i.e. time will not go backwards, nor shall there be any step function in the value of time). This means every second shall occur but the duration of the 'second' will be less (or greater) than one second until time is completely synchronised. This 'drift' at a rate of between 75%-125% of "real" time.

If the time synchronisation request is outside the above band, it shall be considered a 'gross' time change. Such a change shall happen as a step with no smoothing of time. All such changes will be recorded with events in the Audit Trail.

T800 Visual Supervisor, Eycon-10 and Eycon-20 Instrument Time Changes

If a time synchronisation service is currently running it shall not be possible to manually change the clock from the T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments (i.e. neither from function blocks, such as the header block nor from the front panel CLOCK function).

Time synchronisation services shall be deemed not to be running if no request has been received or the last such request was more than 15 minutes 20 seconds ago.

Electronic Signatures

T800 Visual Supervisor, Eycon-10 and Eycon-20 Instruments Electronic Signatures

Components subject to potential electronic signatures may be configured to be one of three classes.

None – No signature required

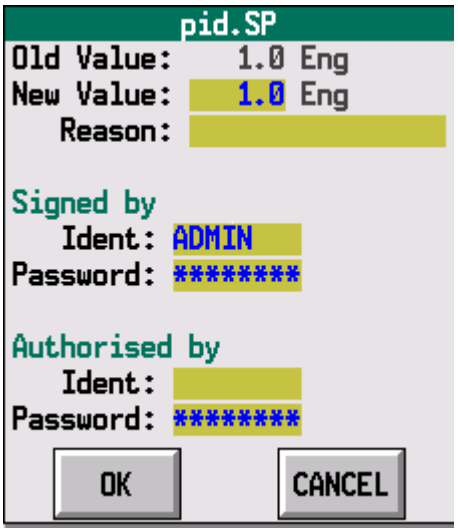
Confirmation – A Simple OK/CANCEL dialogue is presented before the action is carried out (if OK pressed).

Sign – Requires entry of User ID (defaulted to currently logged in user) and password. This need not be the same as the current logged in user.

Sign & Authorise – Requires a signature (see above), plus another user with Authorisation privileges to enter both User ID and Password.

When a button or value subject to signature is pressed a pop-up shall be presented provided that the logged in user has sufficient access level and has signing rights. If they do not have signing rights the value cannot be changed. The title of the pop-up is the button legend (if a button) or the tag of the value (if a LIN database value), or the description if a system value.

The pop-up contains a field for the user to re-enter his/her password. If authorisation is required fields for user ID and password shall also be present. In both cases 'Reason' field with up to 16 characters is available to give a reason for the action. The value change or button press shall not be actioned until all required signature components have been successfully completed and the OK button pressed. An audit trail entry shall be generated containing all the above data.



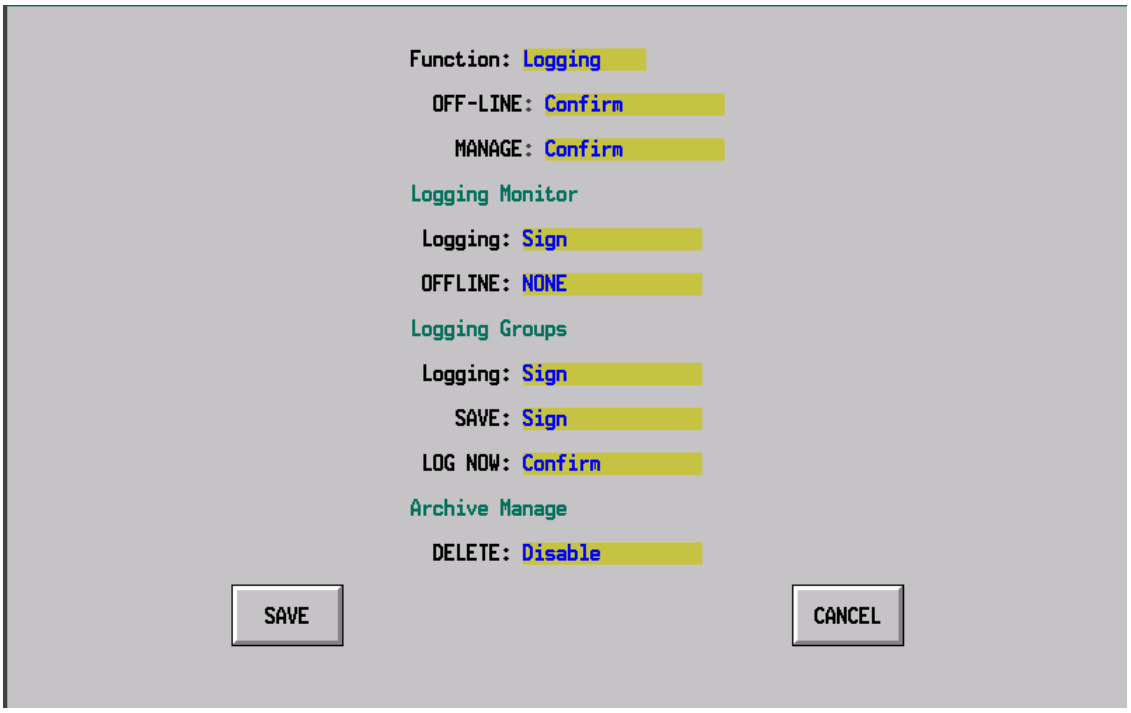
Configuration of System Actions

All system actions may be configured to use any of the three classes of electronic signature component or to be disabled.

Only administrators shall be capable of configuring this feature.

The configuration data shall be stored in E^2PROM and not in the file system and hence shall be tamperproof.

Specific T800 Visual Supervisor editors are provided to enable selection of the appropriate signature class.



Electronic signatures only take effect on power-up (after having been SAVED) or on a manual LOAD.

A button is provided to reset to the factory defaults for signatures.

Initial Conditions for System Component Electronic Signatures

On shipment all system component electronic signatures will be disabled. An administrator with the authorisation of another administrator shall be capable of enabling system component electronic signatures.

Once enabled all components will assume the default values listed below. It shall then NOT be possible to ever turn off signatures globally.

Note
Requiring administrator sign and authorise ensures that sufficient users exist to perform all default operations when enabled.

System Electronic Signature Components

The following system actions are subject to electronic signature configuration and shall have the default values identified below. The defaults are chosen to sign for any change, which modifies values, and Authorisation for any other that may affect the plant and finally none for purely cosmetic changes.

Unless stated otherwise each action may be configured to be one of the following ordered values:

- None
- Confirm
- Signature (Sign)
- Sign & Authorise (AUTH)
- DISABLED

Values of minimum and maximum are given in the table below where applicable; if no limits are given then the full range of values is available. In particular, the option 'DISABLED' is not available where it could render the system unusable if set.

Agent/Feature(s)		*Default, (Min,Max)*	*Audit Trail*
Access			
	SAVE	AUTH, (Sign,DISABLED)	
	PROPERTIES	AUTH, (Sign,DISABLED)	
	MAINT	AUTH, (Sign,DISABLED)	
	RETIRE	AUTH, (Sign,DISABLED)	
Application Manager			
	LOAD	AUTH, (None,AUTH)	
	LD+RUN	AUTH, (None,AUTH)	
	START	AUTH, (None,AUTH)	
	STOP	AUTH, (None,AUTH)	
	SAVE	AUTH, (None,AUTH)	
	SAVE AS	AUTH, (None,AUTH)	
	DELETE	AUTH, (None,AUTH)	
Alarms			
	ACK (pri 6-10)	None, (None,Sign)	
	ACK (pri 11-15)	None, (None,Sign)	
	ACK_ALL	Sign	
	ARCHIVE	Sign	
Batch			
	LOAD	Sign, (None,AUTH)	
	START	Sign, (None,AUTH)	
	HOLD	Sign	
	RESTART	Sign	
	ABORT	Sign	
	RESET	Sign	
	SAVE AS	AUTH	
	CREATE	AUTH	
Clock			
	SET	AUTH	
	Hour +1	None	

Agent/Feature(s)		*Default, (Min,Max)*	*Audit Trail*
	Hour –1	None	
Cloning			
	EXPOR	None	None
	IMPORT	AUTH	
Comms			
	SAVE	AUTH	
	HARDWARE	AUTH	None
Diags			
	RESET	Confirm	None
E-Sig Configuration			
	SAVE	AUTH, (Sign,AUTH)	
	LOAD	AUTH, (Sign,AUTH)	
File Manager			
	COPY	None	
	DELETE	None	
FBlock Manager			
	Edit Fields	AUTH	
	Alarm Priority Edits	AUTH	
	SAVE	AUTH	
Internationalisation			
	CHANGE	None, (None, AUTH)	None
Logging			
	LOG NOW	None	
	OFF-LINE	Signature, (None,AUTH)	
	MANAGE	Confirm	None
	Group Start/.Stop	Signature	
	Device Start/Stop	Signature	
	DELETE	AUTH	None
	SAVE	AUTH	
Network Audit Trail			
	SAVE	AUTH, (None,AUTH)	
Overview			
Panel			
	SAVE	None, (None,AUTH)	None
Programmer			
	LOAD	Sign, (None,AUTH)	
	RUN	Sign, (None,AUTH)	
	RUN FROM	Sign	
	HOLD	Sign	

Agent/Feature(s)		*Default, (Min,Max)*	*Audit Trail*
	ABORT	AUTH	
	SKIP	Sign	
	SAVE	AUTH	
	SAVE AS	AUTH	
	DELETE	AUTH	
	ACCEPT (schedule)	Sign	
	CLEAR (schedule)	Sign	
	NEW	AUTH	
	Edit in HOLD (current)	Sign	
	Edit in HOLD (other)	Sign	
Recipe			
	LOAD	Confirm	
	CAPTURE	None	
	DOWNLOAD	Sign	
	ABORT	Sign	
	SAVE	AUTH	
	SAVE AS	AUTH	
	CREATE	AUTH	
	DELETE	AUTH	
	Monitor SP live edit	Sign	
	Monitor PV live edit	Sign	
	Monitor point live edit	Sign	
Start up			
	SAVE	AUTH, (None,AUTH)	None

Configuration of User Screens

The following user screen components may be configured to have electronic signatures or simple OK/CANCEL style confirmations.

- Buttons
- Value Changes

These will be subject to the usual access level checks, plus any optional electronic signature.

In addition action buttons may include one or more of any of the following actions:

'ENABLE' (or 'ENA') – Taking a single argument which is a Boolean value (bool or subfield type); if FALSE the button will be disabled.

'DISABLE' (or 'DIS') – Taking a single argument which is a Boolean value (bool or subfield type); if TRUE the button will be disabled.

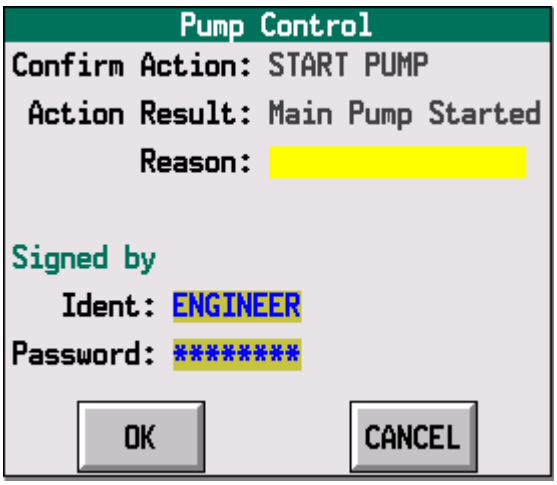
'NOTE' – This will generate a text note (<= 24 characters) into the audit trail (just as if manually typed in via the front panel using the 'NOTE' facility). Such a note may include signature information but *cannot* be marked with an authorisation – the EVENT (see below) must be used if authorisation is required.

'EVENT' – This will generate a text event (<= 16 characters) into the audit trail (just as if manually typed in via the front panel using the 'NOTE' facility).

If a button is configured with an electronic signature (or confirmation), the text from the **first** NOTE or EVENT in the action list of the button will also be displayed in the pop-up.

Example:

```
ENABLE:"[Pid.ModeAct.AutoAct]",ST:"[Pid.Mode]:=MANUAL;",NOTE:"Set to Manual"
```



Setpoint Programmer

The set-point programmer operations will be slightly more restricted if using the 21 CFR part 11 only. The restrictions are as follows:

- Edited but unsaved programs may not be run.
- The editing of running programs shall follow the following rules:

V4.0 It shall not be possible to edit a running program. If the facility is required in conjunction with 21 CFR part 11 then a user screen with the appropriate block fields should be constructed.

V4.1 Programs are edited in the normal manner subject to electronic signatures and with the audit trail restrictions detailed below.

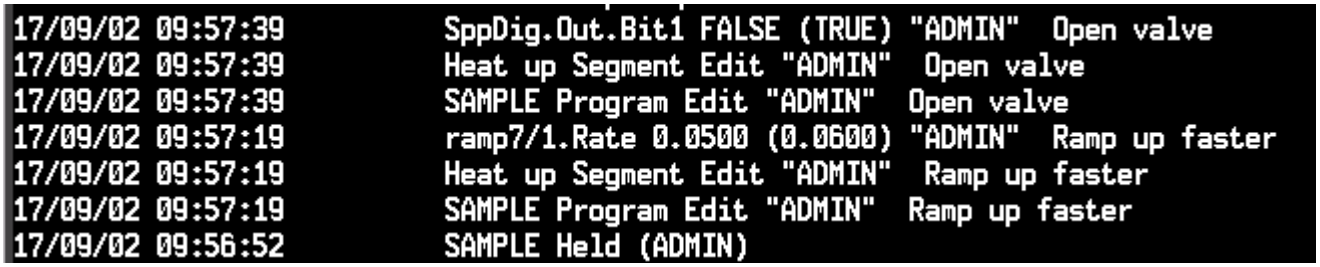
Editing of Running Programs

For 21 CFR-part 11 systems (V4.1 onwards) running programs may be edited in an analogous manner to non-21 CFR part 11 systems, i.e. without requiring a SAVE before a RUN.

The Audit trail for the editing of a 'cell' shall comprise three alarm log entries, 1) an event indicating which program has been edited, 2) an event indicating which segment has been edited and 3) and event indicating which value has been edited. The value changes will be recorded in parentheses '()' if they are 'expected' values.

'Expected' values are values that would be set if this edit is executed, i.e. the program is allowed to execute to this segment. There are a number of reasons why an 'expected' value may never occur, such as 1) the program is aborted before the edited segment is reached, 2) this edit is over-written by another edit to the same value. This means that for a current segment edit the new value is in parentheses '()' – implying that we expect this to be the new value. For past or future segments both values will be in parentheses '()'. Expected values will have at most six significant characters.

See below for examples. The program is called 'SAMPLE' and the segments are 'Heat up' and 'Cool down'. The changes are against the LIN database block field Tags and not against the text in the program editor (i.e. ramp1.TgtSP as opposed to 'Temperature').



Index

Scan for local contents

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

HA028067U000 Issue 5 (CN35935)