

EasyView QA

SPECIFICATION

1 Glossary

Administrator	General term: A person having special access, or other, rights in a system.
EasyView Administrator	A person having special operational rights in EasyView.
EasyView policies	Settings in EasyView governing administrator rights, login and signing functionality and responses.
Login to EasyView	EasyView administrators must log in to EasyView Administrator accounts
Login to System	Owner defined log in rules can be in effect at system (OS) level.
Migrate record	Move EasyView database to other system.
Operator	A person having access rights as a “Windows user” but not as an EasyView administrator..
Owner	A person having all necessary rights to install and maintain a system.
Project	An EasyView term for a pre-programmed set of commands and parameters that govern the acquisition of data and how it is displayed.
System policy	Settings in the OS, governing user rights and login procedures.
User	A Windows term for a person having the right to use a windows account. Access rights are defined by the owner.
Windows Administrator	A person with unrestricted rights in Windows.

2 Software categorisation

EasyView QA is a COTS (IEEE term: Commercial Off-the-shelf Software) and GAMP Category 3 software.

I.e. “it is defined by a market-driven need, its fitness for use has been demonstrated by a broad spectrum of commercial user”.

3 Computer requirements

EasyView QA requires a reasonably fast computer. The following is a list of recommended hardware and properties.

1. Processor speed > 200MHz
2. RAM > 64MB
3. Available disk space > 32MB
4. Graphics accelerator 4MB
5. Monitor resolution > 1280 x 1024

4 OS requirements

To take full advantage of the safety and data integrity safeguard features incorporated in EasyView QA, it is mandatory that it be installed in a MS Windows XP, Windows 2000 or NT4 environment.

5 Installation

1. Installation must be performed in Windows by a person who has Windows administrator privileges and “owner rights”.
The system should normally be run with reduced access rights e.g. user accounts.
2. It is the responsibility of the “owner” to ensure that correct and sufficient safety barriers are in force. I.e. operators should use operator accounts with no more rights than absolutely necessary.

6 User accounts in Operator mode

User accounts are created by the Windows administrator. Usage of an account that has access to EasyView QA (without logging on to EasyView privileged accounts) is in “Operator mode”. It is limited to the following tasks in EasyView QA:

1. Open recordings for viewing
2. Zoom in and out in views (rescale axes)
3. Change colour and widths of graphs
4. Show/hide graphs
5. Create diagram tabs
6. Change names of diagram tabs
7. Remove diagram tabs
8. Activate/Deactivate “extended features”
9. Edit Notes
10. Acknowledge alarms
11. Print views
12. Start, Stop and/or up-load recordings if granted by administrator of Projects.

N.B. that none of these operations affect data numerically. No data can be added, deleted or altered.

7 Passwords

1. All operations, beyond those allowed the operator, are password protected.
2. Passwords must have a length not shorter than 7 characters.
3. Passwords must be assigned to all EasyView administrators.
4. All passwords can be altered by administrators with the right to create administrator accounts.
5. Passwords can be programmed to expire after a set period.
6. An EasyView QA administrator can at all times change his own password.

8 EasyView Administrator Accounts

EasyView administrator accounts are defined by a “User name”, “Full name” and a password. They are protected by passwords. Each account is assigned a globally unique identifier in the form of a 38 character long string.

EasyView administrator accounts can have varying privileges.

The first and foremost account is that created by the “owner” at the time of installation

This “Owner” account is allowed to create new administrator accounts with suitable privileges.

Selectable privileges are:

Create accounts	This privilege should be limited to as few persons as possible but not fewer than two.
Review documents	This is an “electronic signature”. See FDA “21 CFR part 11”
Approve documents/ Issue Approval Form	Approval signatures may be either electronic (See FDA “21 CFR part 11”) or handwritten. The choice is a “policy setting”; See 9.1. An electronic approval signature or issue of an Approval Form will also lock the document, preventing further modifications.
Managing of recordings and “projects”.	See separate table in the manual.

1. Login to Administrator accounts demands a user name and a password.
2. Logins are noted in the Audit Trail
3. Password expiry settings are never or after a programmed number of days
4. All administrators are automatically logged out after a set period of inactivity.
5. Unauthorised attempts to log in are recorded in the System Audit Trail
6. A programmable number of unauthorised attempts to log in, can disable the account and notification of this can, if so ordered, be sent via e-mail.
7. Only Administrators with “create accounts” rights can re-open closed accounts.

9 EasyView QA Policy settings

The following features can be activated and programmed by EasyView Administrators with “Create accounts” rights.

	<i>Policy</i>	<i>Action/Argument</i>
1	Approve documents using electronic signature Approve documents using handwritten signature.	Select either.
2	Automatic Inactivity log out	Activate/no of minutes
3	Automatic disabling of account after failed login attempts	Activate/no of attempts
4	Notify e-mail recipient of disabled account	Activate/E-mail address
5	All logins are recorded in the Audit trail	Activate
6	All failed login attempts are recorded in the Audit trail	Activate

Password expiry is set in each account: never or after a programmed number of days

10 Electronic records

EasyView QA creates, manages and “handles” measurement and other data as recordings or documents. These documents meet the specifications of electronic records in FDA “21 CFR part 11”.

The EasyView documents contain measurement data, meta data, audit trail, name of the responsible administrator and, where applicable, electronic signatures.

The Administrator responsible for recorder settings will be noted as responsible for the document regardless of who actually created it. See Projects 16

All EasyView QA documents are kept in a secure, password protected, database.

- Retention period** The “owner” must ascertain that the storage medium meets his demands.
- Record migration** Record migration in the form of databases must be handled at the “owner” level where it is the responsibility of the owner to ensure system integrity and security.
- Recording import** Only copies of EasyView secure documents can be “imported”. They must be “exported” by an EasyView QA and have intact encryption and contain the audit trail and signatures where applicable.
Conventional import to EasyView QA is not possible
- Recording export** Documents can be copied to other EasyView QA systems. These copies are encrypted using the ECB and contain the Audit trail and applicable signatures.
It is normally not possible to export data to non-EasyView QA systems. Customised secure non-EasyView export plug-ins can be made available.

5. **Secure records** EasyView QA will only accept data via its built in logger drivers. Recordings from a non-QA EasyView will not open in EasyView QA.
- When a document is opened it is “checked out”. Other users will only be able to open a write-protected copy of the document. If, for some reason, this document is not subsequently closed correctly, it will remain “checked out” until the same user opens it and closes it again.

11 Document integrity

Each EasyView QA document is identified by OS account; Responsible Administrator; Title; Date and Time. It is also assigned a 38 character long globally unique identifier. All EasyView QA documents are kept in a secure, password protected, ODBC compliant database. They are stored in the form of tamper-proof data packages. These data packages can only be accessed by EasyView QA.

12 Electronic signatures

1. Electronic signatures in EasyView QA are of two kinds: Reviewed and Approved.
2. Only Reviewed documents can be Approved.
3. Any modification forces a new Review signature before Approval is made possible.
4. An Approved document is locked and cannot be modified.
5. Electronic signatures can only be entered by administrators with signature (Approve or Review) privileges.
6. Administrators with signature privileges must supply their user name and password when signing.
7. Electronic signatures are shown in the record, in electronic or printed form, with meaning (Approve or Review), full name and date, time and time zone of the signing.
8. When signing, EasyView QA informs the signer that the signature is legally binding.
9. All signings are noted in the Record Audit Trail.
10. Unsuccessful attempts at signing are, if so ordered , noted in the Audit trail.
11. A programmable number of unsuccessful attempts may disable the account. A notifying e-mail can be sent as a result of such a disabling.

13 Handwritten signatures

The EasyView QA policy settings allow “hybrid” configuration. I. e. the documents are electronic but approval signatures will be handwritten.

Approval will in these cases result in the issue of a printed form.

1. The “Electronic Record Approval” form can only be issued from “Reviewed” documents.
2. Any modification forces a new Review entry before Approval is made possible.
3. Issuing the Approval form locks the document.
4. Only Administrators with approval rights can issue the Approval forms.
5. Administrators with signature privileges must supply their user name and password when approving.
6. The Approval form shows full name and date, time and time zone of the signer.
7. Issue of the Approval form is noted in the Record Audit Trail.
8. Unsuccessful attempts at issuing the approval form are noted in the Audit trail.
9. A programmable number of unsuccessful attempts may disable the account. A notifying e-mail can be sent as a result of such a disabling.

14 Audit Trails

EasyView QA maintains two types of Audit trails: the (global) System Audit Trail and the Record Audit trail.

The **System Audit Trail** records all EasyView QA account transactions:

Account creation, modification of Account rights, disabling of accounts.

The **Record Audit Trail** records all the actions that affect the recording. These are:

Change channel label, Change transform, Change transform unit, Change channel time skew, Change start time, Edit formulas, Approve document, Review document.

1. All entries in the audit trails include the, at the time logged in, user/administrator.
2. All entries are time stamped.
3. Time and date formats follow those specified in the Windows control panel.
4. Audit trails are not editable by the user.
5. Audit trails are at all times viewable and printable
6. All entries are sequentially added.

15 Record printouts

The electronic record, in the form of an EasyView QA document, can in full or selected parts be printed on paper. All pages of a printout contain the 38 character Document identifier; Responsible Administrator; Signatures with reason, date, time and time zone.

Selectable parts are:

1. Active diagram tab
2. Active info-table tab
3. Selected plug-ins. (See main manual.)
4. Record Audit Trail

16 Projects

EasyView QA projects (see main manual) can only be created by EasyView QA Administrators. It is possible for an EasyView QA administrator to allow operators to Start and/or Stop and/or Offload a recording. It is up to the project responsible to judge whether projects should thus be made available to Operators.

Within a dedicated single role system, it is only possible to fetch off-line data using the same project that initiated the collection of data.

The Administrator should be aware of the possibility to inadvertently use the wrong project in multi-role, multi-logger, multi-project environments and thus have as few projects open to the operator as possible.

17 Removed EasyView Pro features

The following features of the EasyView Pro are not consistent with 21 CFR part 11 and data and document integrity and are therefore not present in EasyView QA:

1. Operator channels
2. Data Import
3. Data Export
4. Logger Boot
5. New document
6. Open view in new document
7. EasyTerm