



FDA 21 CFR 11 Compliance Checklist of MeltView 2 Software

Introduction

Title 21 of the Code of Federal Regulations Part 11 (21 CFR 11) from United States Food and Drug Administration (FDA) outlines the requirements for an organization to maintain and to submit electronic records with electronic signatures instead of paper records with handwritten records.

The requirements have to be followed to have FDA consider integrity of an organization's management of electronic records and electronic signatures trustworthy.

MeltView 2 Software is designed to support an organization to meet the 21 CFR 11 requirements on handling electronic records generated by MPA100, an automatic melting point apparatus from Stanford Research Systems (SRS).

The following is a list of how MeltView 2 Software implements the requirement of the regulations. The regulations quoted in this document are copied from the following FDA website.

<https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1>

Implementation of 21 CFR 11 requirements in MeltView 2 *Pro* software

Subpart B--Electronic Records

Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

SRS MeltView 2 Software (in *Pro* edition) helps a customer organization to meet the 21 CFR 11 requirements for electronic records of melting point measurements performed using the SRS automatic melting point apparatus, MPA100. The software consists of (1) a database server that stores electronic records and the associated signatures, (2) an administration application (MeltView-Admin) with which users with administrator permission can change user access and signature settings of other users, and (3) a client application (MeltView) with which users with proper permissions can acquire, view, and sign melting point measurement records. These components of the software can run in one computer for simple configuration, or multiple computers for larger organizations.

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Installation qualification, operation qualification and performance qualification protocols will be provided to help the organization to validate the software in its environment.

MeltView 2 Software is designed with data integrity and security in mind. It does not allow users to modify or delete records related to measurement data both at the application level and at the database system level. Normal users only can add new measurement records and signatures to the records. In addition, it is configured to generate independent audit trail records at the database system level automatically whenever changes take place in the database. Because only a database administrator with the master password can make an illegal deletion or modification to the database, the organization should implement an operational procedure to prevent the master password abuse. Furthermore, measurement records are saved along with the hash values. If a measurement record is corrupted with a mismatched hash value, it will be displayed with a mark in the data browser as shown in Figure 1.

Meas. ID	Chemical	Acquired Time	Instrument Serial #	[Left] Clear Temp	[Center] Clear Temp	[Right] Clear Temp	Signed
525	Caffeine	8/24/2005 10:21 AM	78155	236.639	236.829	236.842	
524	Vanillin	8/24/2005 10:00 AM	78154	83.1238	83.2747	83.2681	
523	Phenacetin	8/24/2005 10:10 AM	78154	135.944	136.012	135.978	
522	Caffeine	8/24/2005 10:21 AM	78154	237.203	237.014	237.235	
521	VANILLIN	9/29/2011 12:26 PM	78153	82.834	82.9199	83.0771	
▲ 520	VANILLIN	11/3/2006 10:06 AM	78153	82.5774	82.863	82.8979	✔ Yes
519	Vanillin	8/23/2005 9:53 AM	78153	83.3237	83.0801	82.8962	
518	Phenacetin	9/29/2011 12:36 PM	78153	135.635	135.672	135.459	

Selected row details:

- Summary
- Sample Info
- Configuration
- Results
- Signatures

Summary
Sample: VANILLIN, [No batch #], [No notes]
Configuration: Start Temp: 78.0 C, Stop Temp: 88.0 C, Heating Rate: 1.0 C/min
Results: Clear Points: 82.6 C, 82.9 C, 82.9 C
Signatures: Chulhoon Kim (Review)

Buttons: Sign..., Report..., Open, Close

Figure 1 - The data browser shows the selected row marked as invalid record.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

In MeltView client application (available in MeltView 2 Pro edition), electronic records are displayed in different formats for a viewer's convenience:

- (1) Data browser show a table of measurements, with a detailed view for a selected record.

The screenshot shows the 'Data' browser window. At the top, there are controls for 'Refresh', 'Columns...', and 'Filter...'. Below these are two tabs: 'Measurements' (selected) and 'Signatures'. The main area contains a table with the following data:

Meas. ID	Chemical	Acquired Time	Instrument Serial #	[Left] Clear Temp	[Center] Clear Temp	[Right] Clear Temp	Signed
8389	VANILLIN	8/18/2017 8:07 AM	122999	82.8276	83.0198	82.5452	
8388	Phenacetin	8/18/2017 8:28 AM	122999	135.533	135.452	135.635	
8387	Caffeine	8/18/2017 8:48 AM	122999	236.701	236.671	236.732	Yes
8386	VANILLIN	9/1/2017 9:27 AM	122998	82.9075	83.0002	83.0457	
8385	Phenacetin	9/1/2017 9:46 AM	122998	135.664	135.322	135.575	
8384	Caffeine	9/1/2017 10:17 AM	122998	236.628	236.804	236.629	
8383	VANILLIN	8/26/2017 1:52 PM	122997	83.3496	83.2385	83.2937	

Below the table is a 'Selected row details' section with a tree view on the left and a summary on the right:

- Summary
- Sample Info
- Configuration
- Results
- Signatures

Summary
Sample: Caffeine, [No batch #], [No notes]
Configuration: Start Temp: 232.0 C, Stop Temp: 242.0 C, Heating Rate: 1.0 C/min
Results: Clear Points: 236.7 C, 236.7 C, 236.7 C
Signatures: Matt Kowitt (Review)

At the bottom of the window are buttons for 'Sign...', 'Report...', 'Open', and 'Close'.

Figure 2 - Data browser shows measurement records at the top and detail information on the selected record at the bottom.

(2) Client main window shows detailed information including images and plots.

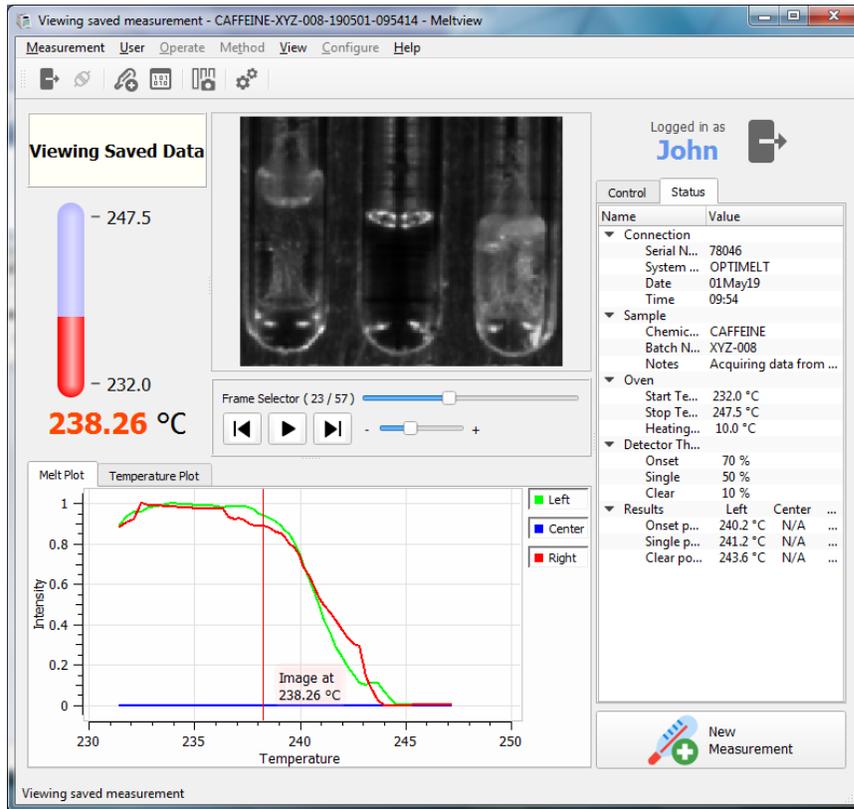


Figure 3 - Main window shows detailed information on a measurement including a melt-movie and a melt-plot.

(3) Audit trail browser shows user activities

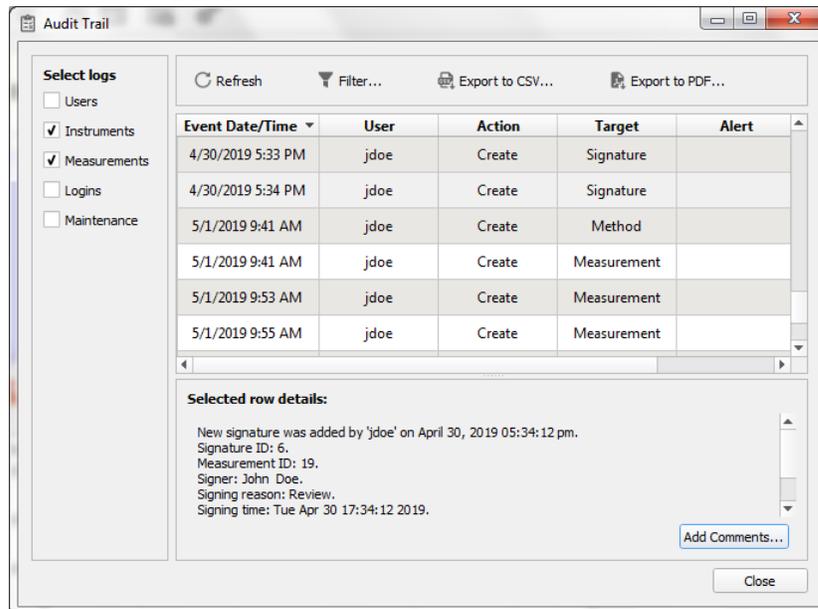


Figure 4 - Audit trail viewer shows user activities at the top and detailed information of a selected row at the bottom.

- (4) A measurement can be exported as a report in Portable Document Format (PDF) for printing or separate electronic storage.
- (5) MeltView 2 Software uses a database management system which allows to use Structured Query Language (SQL) directly to the database. If the agency need to look into specific records in the database, they can audit the database using general database browsing tools.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Users with proper permissions can use client applications to run and sign a measurement, as well as to view electronic signatures and audit trail. All the electronic records are stored in a database server. MeltView-Admin application is equipped with Database backup and restore capability, which can run manually or automatically with a scheduler at regular intervals. If access to electronic records for viewing and signing is no longer required, the database can be saved as a backup and stored during the required retention period without database running on the server. For database security, only database administrators with the master password are allowed to backup, restore, and reset the data base. The organization is responsible for securing the master password to the database system according to the organization's policy, and implementing backup policy for the database.

(d) Limiting system access to authorized individuals.

With the MeltView-Admin application, a user with "Manage Users" permission (administrator) can control how users access to the system. The user administrator assigns an account name to a user, changes expiration date of the account and password, assigns permissions to the account, and locks the account to prevent the user from logging in to the system, if necessary.

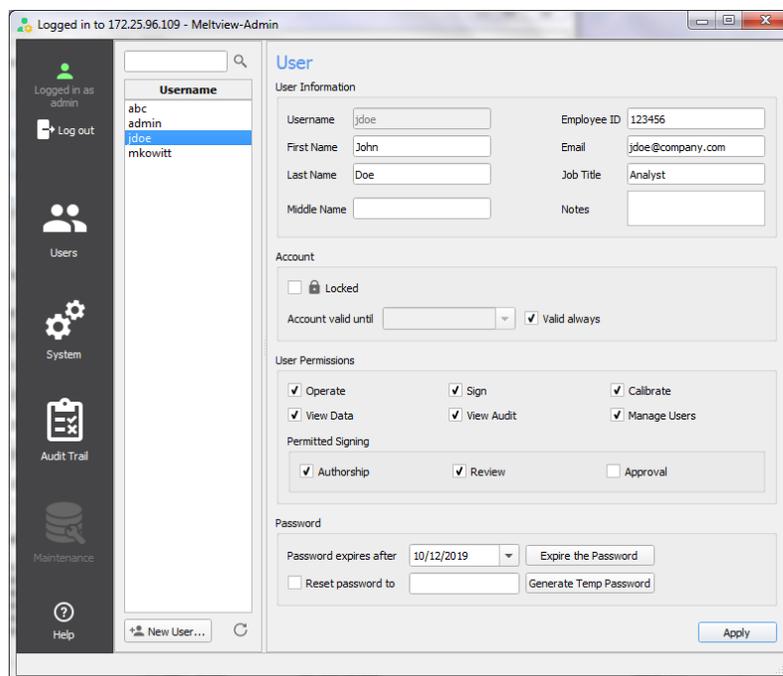


Figure 5 - Administration application shows the user control panel.

A user is required to login to the MeltView client application with required permissions, which are assigned from the administration application, in order to operate an instrument, to run calibration, to view data and audit trails from the database, and to sign a measurement electronically.

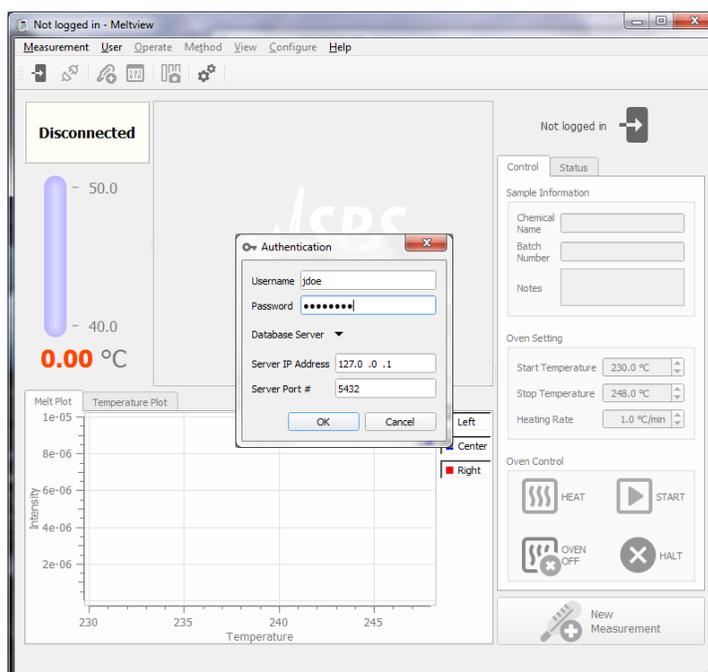


Figure 6 - MeltView-21CFR 11 client application prompts initial user login.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

MeltView 2 software tracks changes in the database, and records them in separate audit trail tables. The audit trail is backed up with the database when the database backup script is run. Regular backups of the database will help the organization retain the electronic records during the required period even against computer failure. It is the organization's responsibility to implement backup policy for the database.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

The MeltView client application monitors the state of a connected instrument, and adjusts the user interface of the application to show only currently allowed actions to choose from based on user permissions. It helps a user take proper steps to complete a task at hand.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

A user is required to log in to the MeltView client application before operating an instrument, browsing electronic records, or viewing the audit trail. The user must have prior authorization before adding an electronic signature to a measurement record.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

The MeltView client application validates the input parameters before starting a measurement, and warns against missing parameters or invalid ones. It also records the measurement process as a movie, which can be reviewed if the measurement has been performed properly.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

These are the organization's responsibility.

Sec. 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

These are not applicable, because MeltView 2 Software is a closed system.

Sec. 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

MeltView 2 Software records signature events with the signer's printed name, the date and time when the signature is executed, and the meaning associated with the signature. User administrators can define organization-specific signature meanings from the MeltView-Admin application.

MeltView client application shows signatures with the required information in different formats for a viewer's convenience:

- (1) Data browser shows a list of signatures filtered with configurable conditions.

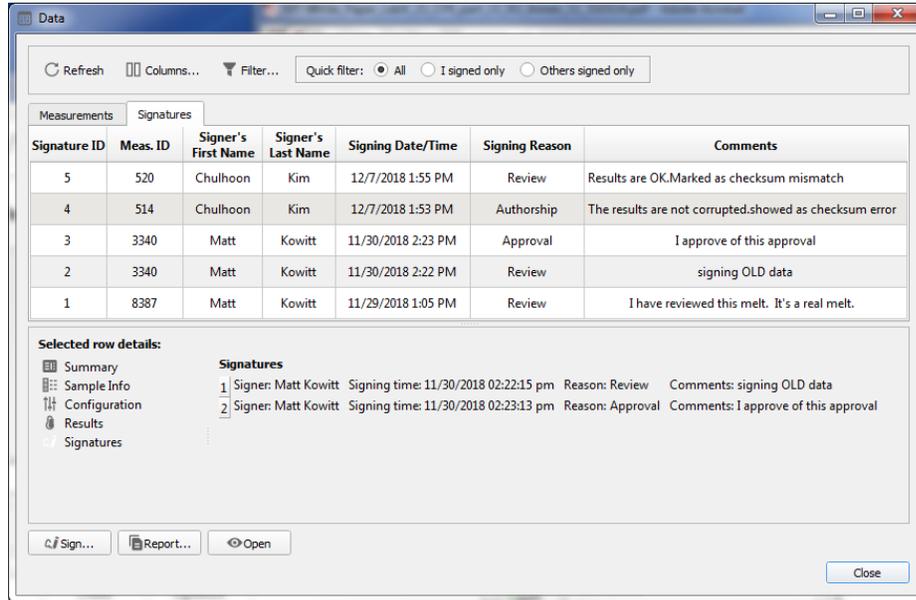


Figure 7 - Data browser in the signature view shows a list of signatures at the top and detailed information on the measurement including the selected signature at the bottom.

- (2) Audit trail browser shows signatures along with other user activities.

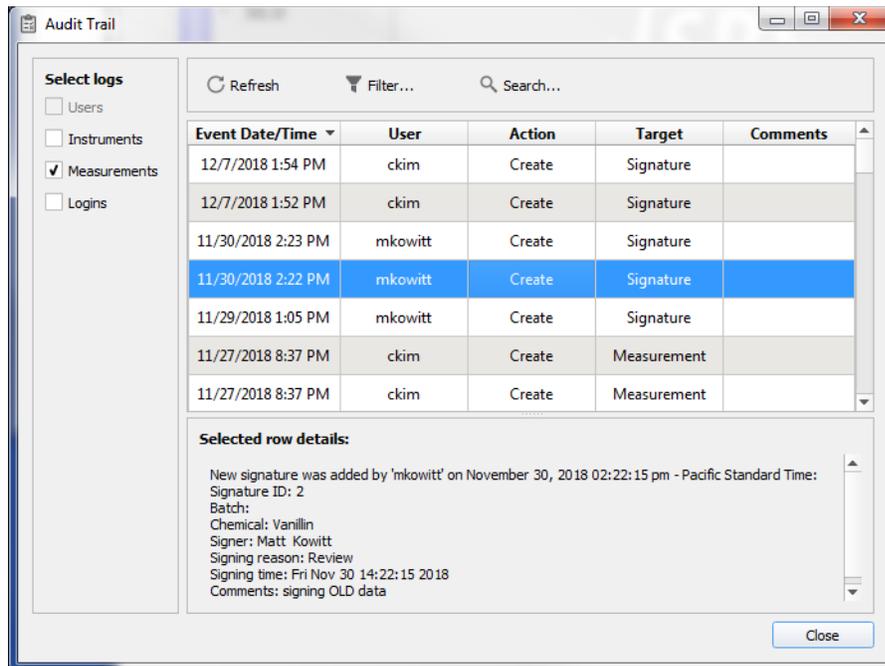


Figure 8 - Audit trail browser shows on a signature and its detailed information.

(3) PDF Reports shows signatures associated with a measurement.



ABC Company

Batch #: . Chemical: Vanillin
Acquired by: Chulhoon Kim. Acquired on: May 06, 2009 01:33:00 pm - Pacific Daylight Time
Instrument: #97204

SIGNATURES:

Digitally signed by Matt Kowitt
Date: November 30, 2018 02:22:15 pm - Pacific Standard Time
Signing reason: Review
Comments: signing OLD data
Signature ID: 2
[fa2d6818ff75b58d65aa5ad18257f592d41acba569320e7dfed734ae62a8bdf6]

Digitally signed by Matt Kowitt
Date: November 30, 2018 02:23:13 pm - Pacific Standard Time
Signing reason: Approval
Comments: I approve of this approval
Signature ID: 3
[a5c78ab8e0d537d4d73b5ee8e9327ac7cc2772d4c8e942bca6d75c729e2f32c0]

Sec. 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

In MeltView 2 Software, every signature is linked to a measurement record. No signatures are duplicated based on signer's name, date and time stamp, and signing reason.

21 CFR part 11 Subpart C--Electronic Signatures

Sec. 11.100 General requirements.

11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

The MeltView-Admin application guarantees the uniqueness of each account name in the system and the corresponding electronic signatures. It is the organization's responsibility not to reuse, or reassign previously created account to another individual.

11.100 (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

11.100 (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

This is the organization's responsibility.

Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

The MeltView client application requires a user to provide user name and password to log in. Once logged in, the user needs to provide the password again each time a document is signed.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

The organization enforces users not to share their user name and password with others.

Because the password of a user account is only known to the genuine owner, the only way to add a signature without knowing the password is to reset the password. Only a user administrator can reset the password of an account and sign on behalf of the genuine user. However, the user administrator must notify the genuine user about password reset, because the user cannot use the previous password.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

MeltView 2 Software does not use biometric signatures.

Sec. 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

Neither MeltView-Admin program nor the database server allow a duplicate user account.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

With MeltView-Admin application, a user with “Manage Users” permission can lock an account, set a password expiration date, and reset password if necessary.

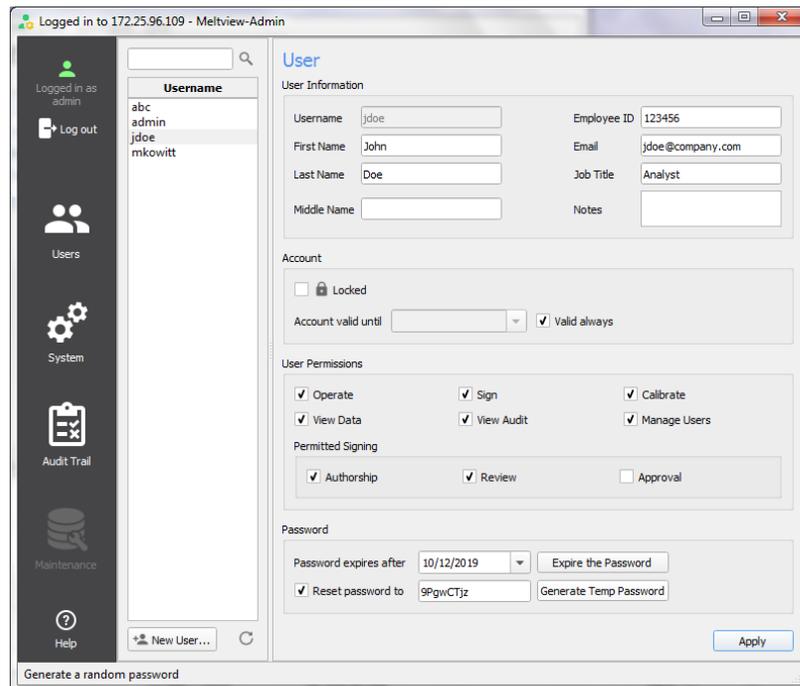


Figure 9 - Administration Application shows the user management panel.

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

An administrator user can lock an account, or change a user's password. A user also can change his or her own password from the MeltView client application.

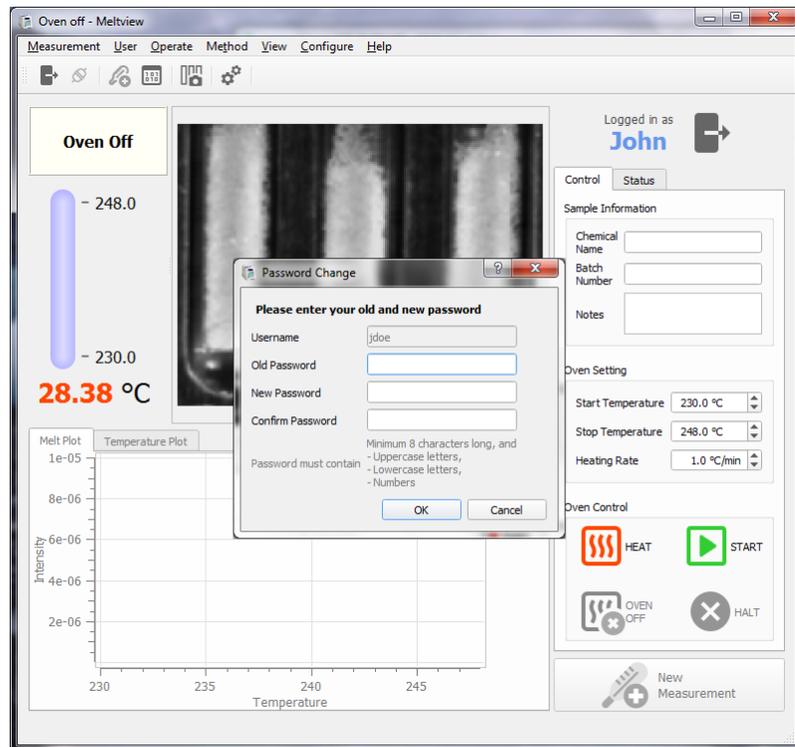


Figure 10 -The client application prompts the password change initiated by the user logged in.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

In MeltView-Admin application, a maximum of incorrect login attempts can be defined.

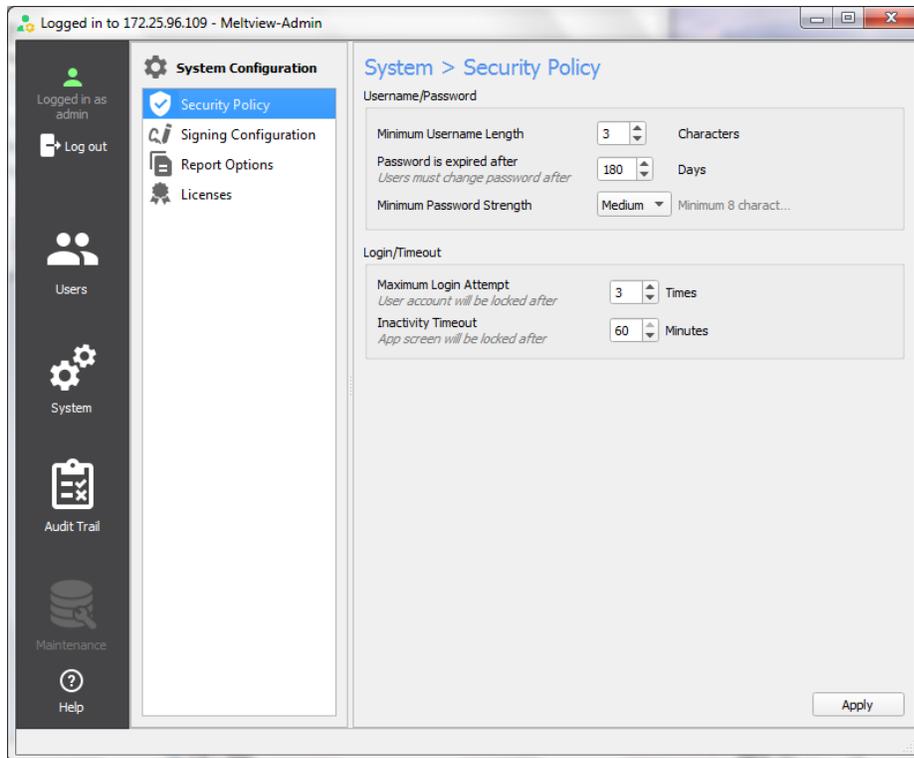


Figure 11 - The administration application shows the security policy panel.

If a user exceeds the maximum number of login attempts, the account will be locked and not available until a user administrator unlocks it. All the login attempts will be recorded in the audit trail. Failed login attempts are clearly marked in the Audit trail browser.

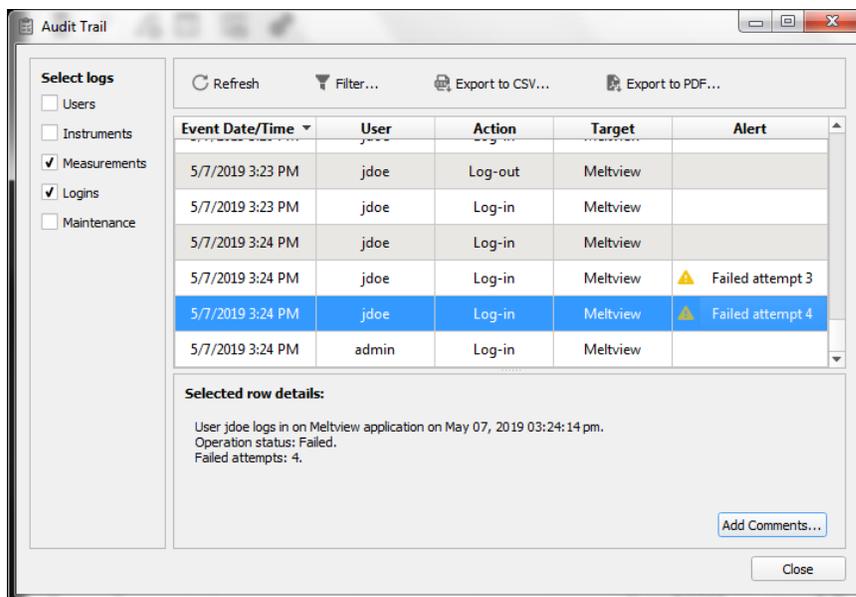


Figure 12 - Failed login attempts are clearly marked in the audit trail browser.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

MeltView 2 Software does not use identification devices.

Summary

FDA 21 CFR 11 contains requirements for an organization to meet when utilizing electronic records and electronic signatures in place of paper records with hand-written signatures. MeltView 2 Software provides the technical controls and features needed to support regulatory compliance for an organization using the SRS MPA100 with electronic recordkeeping.