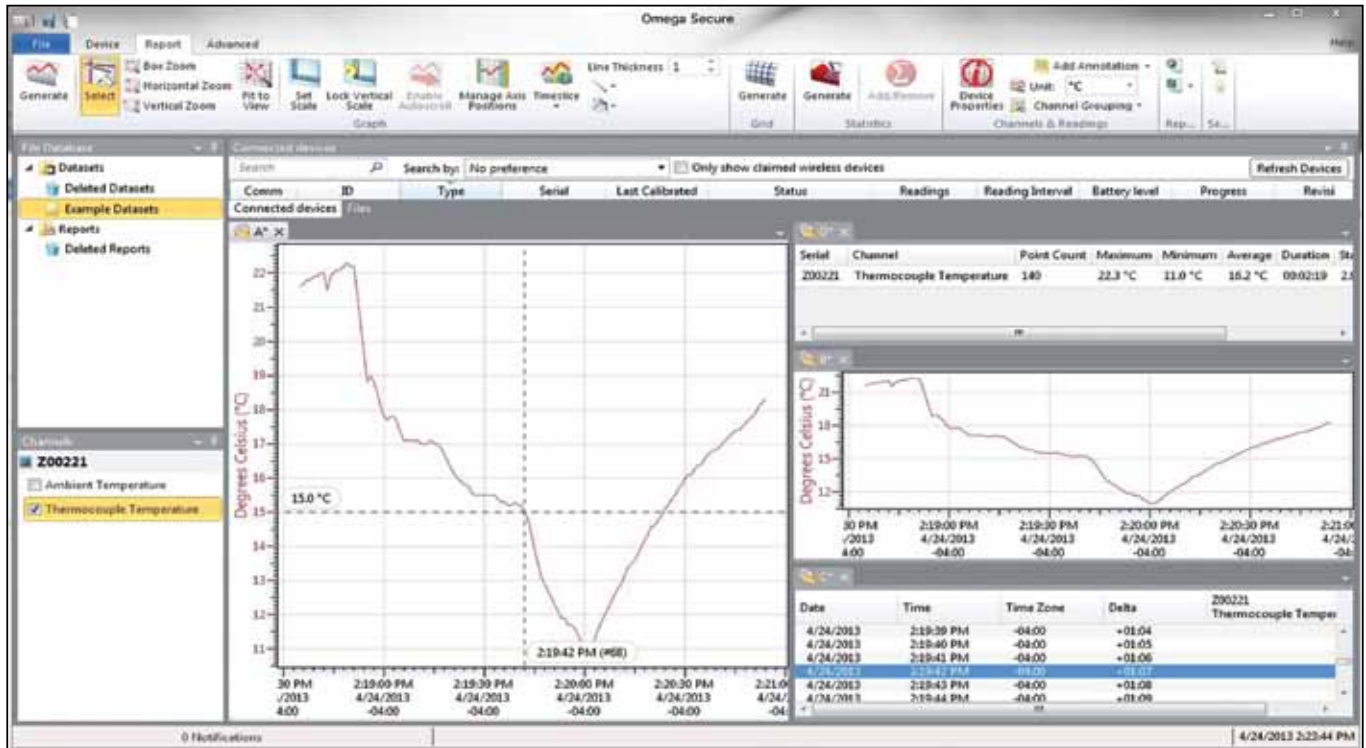


# Secure Software



## For Use with OM-CP Series Data Loggers

### OM-CP-SVP-SYSTEM



- **Install, Validate and Operate One Software Program Universally**
- **Compatible with Most OM-CP Series Data Loggers**
- **Time and Cost Saving Validation Package—Stands up to Interrogation from Auditors**
- **Automatic Data Security and Audit Trail**
- **Sophisticated User Maintenance**
- **Traceability with Customizable Electronic Signatures and Audit Trails**
- **Aids in Compliance with FDA 21 CFR Part 11/820 and GxP Guidelines**

#### Applications

- **Pharmaceutical**
- **Medical**
- **Hospitals**
- **FDA Regulated Organizations**
- **Temperature Mapping**

The OM-CP-SVP-SYSTEM Secure Software aids customers in compliance with 21 CFR Part 11 requirements. The software ensures standards in which electronic files are considered equivalent to

paper records, saving time and effort. OM-CP-SVP-SYSTEM Secure Software contains criteria such as electronic signatures, access codes, secure data files, and an audit trail which meet the requirements of 21 CFR Part 11 and help provide data integrity. IQ/OQ/PQ (Installation/Operational Qualification/Performance Qualification) protocols are included with the purchase of the OM-CP-SVP-SYSTEM Secure Software to validate that the software has been installed and is operating correctly. The layout of the secure software is similar to the OM-CP Series Data Logger Standard Software, allowing users to easily learn the additional features.

The Windows® based software package allows the user to effortlessly collect, display and analyze data. A variety of powerful tools provide the ability to examine, export, and print professional looking data with just a click of the mouse.

#### **Logger Auto-Detection—Saves Time, Secures Data**

The software automatically detects loggers as soon as they are plugged into the computer. With minimal user involvement, drivers are then

installed, data is downloaded, and a graph of the data is rendered on screen.

#### **Linked Data—Saves Time and Effort**

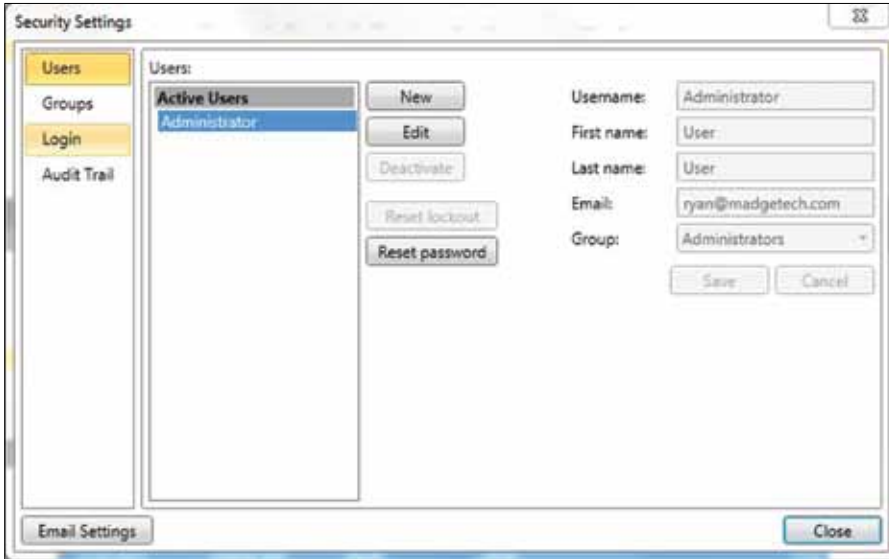
Graphs and data grids can now be linked, allowing the user to quickly and easily modify multiple views of the same information. Make a change to the data grid and the information on the linked graph synchronizes immediately and automatically!

#### **Multiple Data Sets—Makes Mapping a Breeze**

Mapping data has never been so easy—or fast! Now data from multiple loggers can be easily combined in a single data grid by simply dragging and dropping data sets, creating a side by side comparison of data for each logger.

#### **Software Overview—Security Settings**

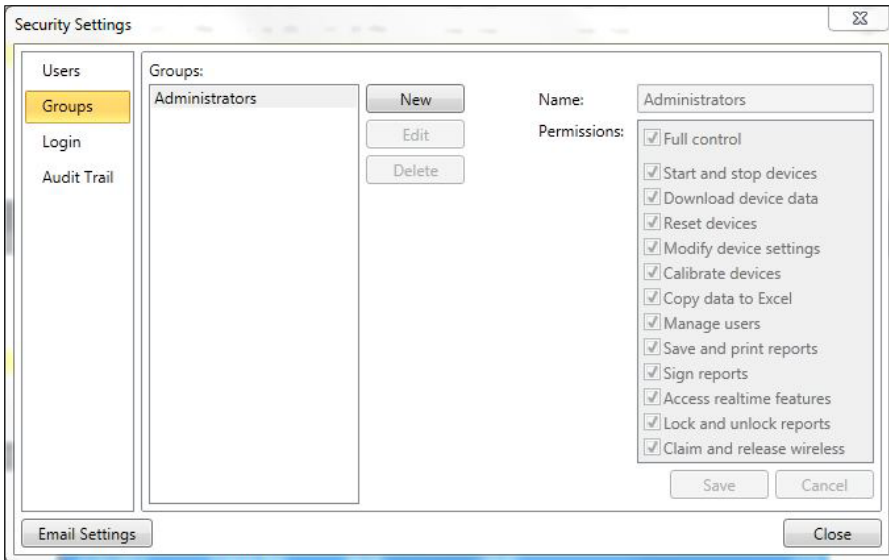
On the following pages are an overview of the important 21 CFR Part 11 compliance features in the OM-CP-SVP-SYSTEM Secure Software. Each feature is important in securing data and ensuring tampered data is recognized by the OM-CP-SVP-SYSTEM Secure Software.



The screenshot shows the 'Users' tab in the Security Settings window. On the left, a sidebar contains 'Users', 'Groups', 'Login', and 'Audit Trail', with 'Users' selected. The main area is titled 'Users:' and contains a list of 'Active Users' with 'Administrator' selected. To the right of the list are buttons for 'New', 'Edit', 'Deactivate', 'Reset lockout', and 'Reset password'. Further right, form fields are provided for 'Username' (Administrator), 'First name' (User), 'Last name' (User), 'Email' (ryan@madgetech.com), and 'Group' (Administrators). 'Save' and 'Cancel' buttons are at the bottom right. An 'Email Settings' button is at the bottom left, and a 'Close' button is at the bottom right.

## Administrator and User Settings

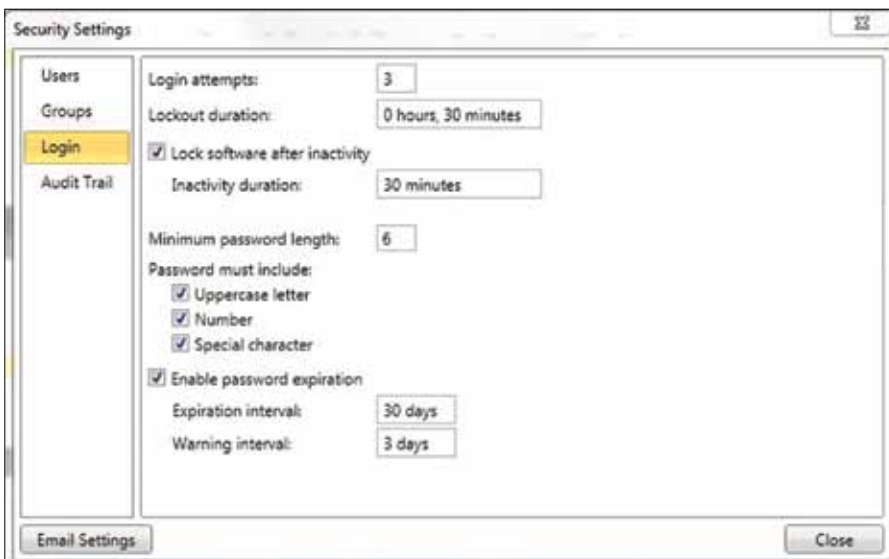
Users can be given two levels of access, either administrator or user. Administrators have access to all the security settings, while users only have access to communicate with the data loggers and analyze data.



The screenshot shows the 'Groups' tab in the Security Settings window. The sidebar has 'Groups' selected. The main area is titled 'Groups:' and contains a list with 'Administrators' selected. To the right are buttons for 'New', 'Edit', and 'Delete'. Further right, the 'Name' field is 'Administrators' and the 'Permissions' list includes: Full control, Start and stop devices, Download device data, Reset devices, Modify device settings, Calibrate devices, Copy data to Excel, Manage users, Save and print reports, Sign reports, Access realtime features, Lock and unlock reports, and Claim and release wireless. 'Save' and 'Cancel' buttons are at the bottom right. An 'Email Settings' button is at the bottom left, and a 'Close' button is at the bottom right.

## Groups

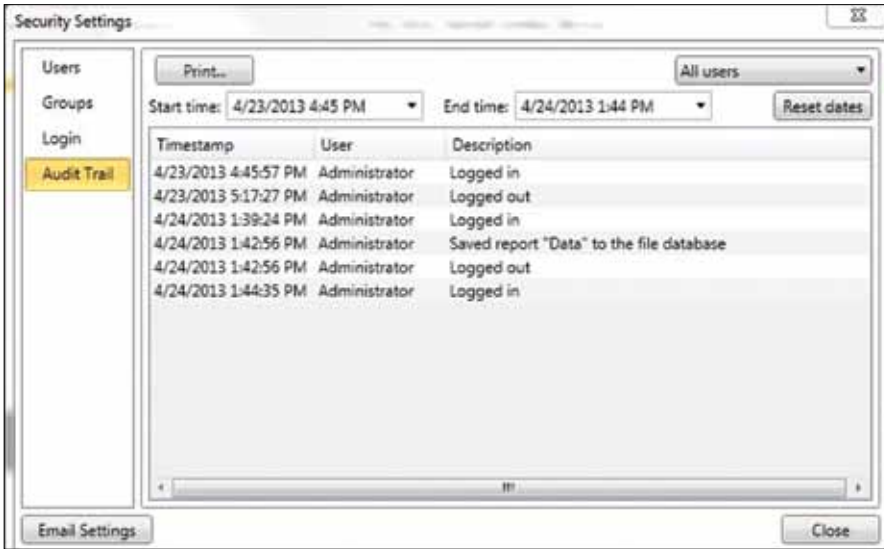
Users and Administrators can be assigned to Groups and can be easily maintained using a variety of permissions.



The screenshot shows the 'Login' tab in the Security Settings window. The sidebar has 'Login' selected. The main area contains settings for login attempts (3), lockout duration (0 hours, 30 minutes), and a checkbox for 'Lock software after inactivity' which is checked. Below this is 'Inactivity duration' (30 minutes), 'Minimum password length' (6), and 'Password must include' options: 'Uppercase letter', 'Number', and 'Special character', all checked. There is also a checkbox for 'Enable password expiration' which is checked, with 'Expiration interval' (30 days) and 'Warning interval' (3 days) fields. An 'Email Settings' button is at the bottom left, and a 'Close' button is at the bottom right.

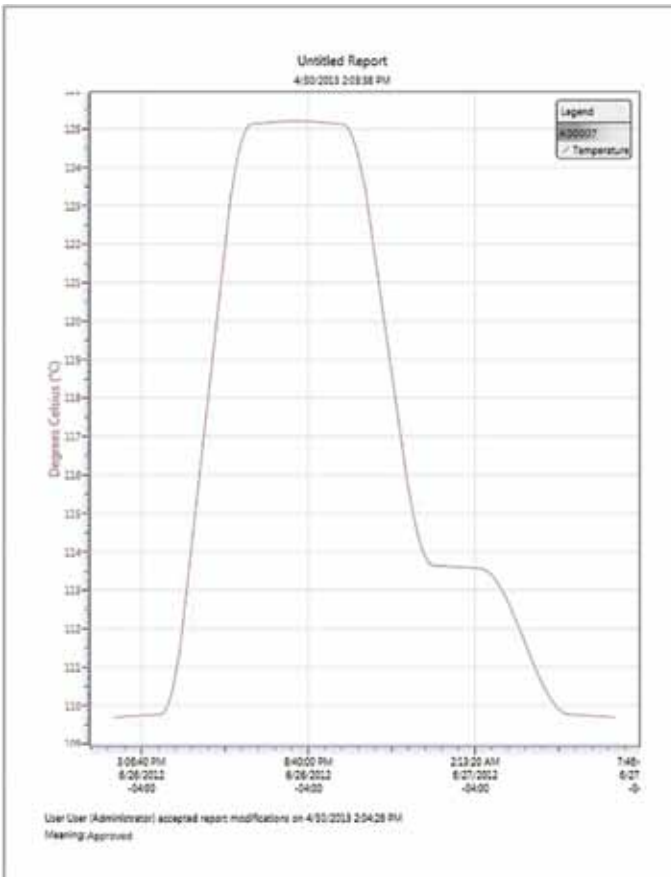
## Login

Login attempts and lockout duration can be assigned within the Login tab. There are numerous password and account settings for the administrator to set such as the complexity of the password and status of each user account. The user management tab is only available to administrative users.



### Audit Trail

An Audit Trail is kept automatically with information such as who has logged in and out, what files were downloaded, saved, printed etc. Each record is date and time stamped and includes the user information.



### Electronic Signature

By clicking the Electronic Signature button, users and administrators can add electronic signatures. The electronic signature contains the printed name of the signer, date and time of the signing and the meaning of the signing.



## 21 CFR PART 11 Requirement Checklist

21 CFR Part 11 Requirement	Does OM-CP-SVP-SYSTEM Secure Software Comply?	No Additional Action Required to Comply?	Comments
The system must be capable of being validated.	Yes	No	The customer must execute the IQ/OQ/PQ to validate that the software is installed correctly and that it operates properly.
It must be possible to discern invalid or altered records.	Yes	Yes	The file format used in the Secure software is proprietary and cannot be opened in any other piece of software. Only .MTFFS files are able to be saved and/or opened by the OM-CP-SVP-SYSTEM Secure software.
The system must be capable of producing accurate and complete copies of electronic records on paper.	Yes	Yes	The OM-CP-SVP-SYSTEM Secure software allows the graph and all data records to be printed on paper. In addition, device status, data file statistics, audit trails and other pertinent information may be printed.
The system must be capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA.	Yes	Yes	All data files may be transferred by e-mail or other means to other users of OM-CP-SVP-SYSTEM Secure software, or printed to a secure document in another format such as PDF.
Records must be readily retrievable throughout their retention period.	Yes	Yes	All data downloaded from a device are automatically saved to an internal secure database, these data cannot be altered, but is always available for the user to generate a visual representation of the data in grid, graph, and statistic format.
System access must be limited to authorized individuals.	Yes	No	The OM-CP-SVP-SYSTEM Secure software ensures that only users with a valid User ID and password can gain access to the software. End-user SOPs should be developed and maintained to ensure that users do not share their unique user ID and or password.
The system must be capable of producing a secure, computer-generated, time-stamped audit trail that records the date and time of operator entries and actions that create, modify or delete electronic records.	Yes	Yes	The OM-CP-SVP-SYSTEM Secure software maintains an audit trail file on any salient operation performed on the system. The audit trail is secure and encrypted and contains all operations performed by date, time and operator.
Upon making a change to an electronic record, original information is still available.	Yes	Yes	Changes cannot be made to raw data datasets; however, reports generated by the user may be changed as desired.
Electronic records audit trails are retrievable throughout the record's retention period.	Yes	Yes	All audit trails are saved as a part of the record and cannot be deleted or modified in any way.

## 21 CFR PART 11 Requirement Checklist

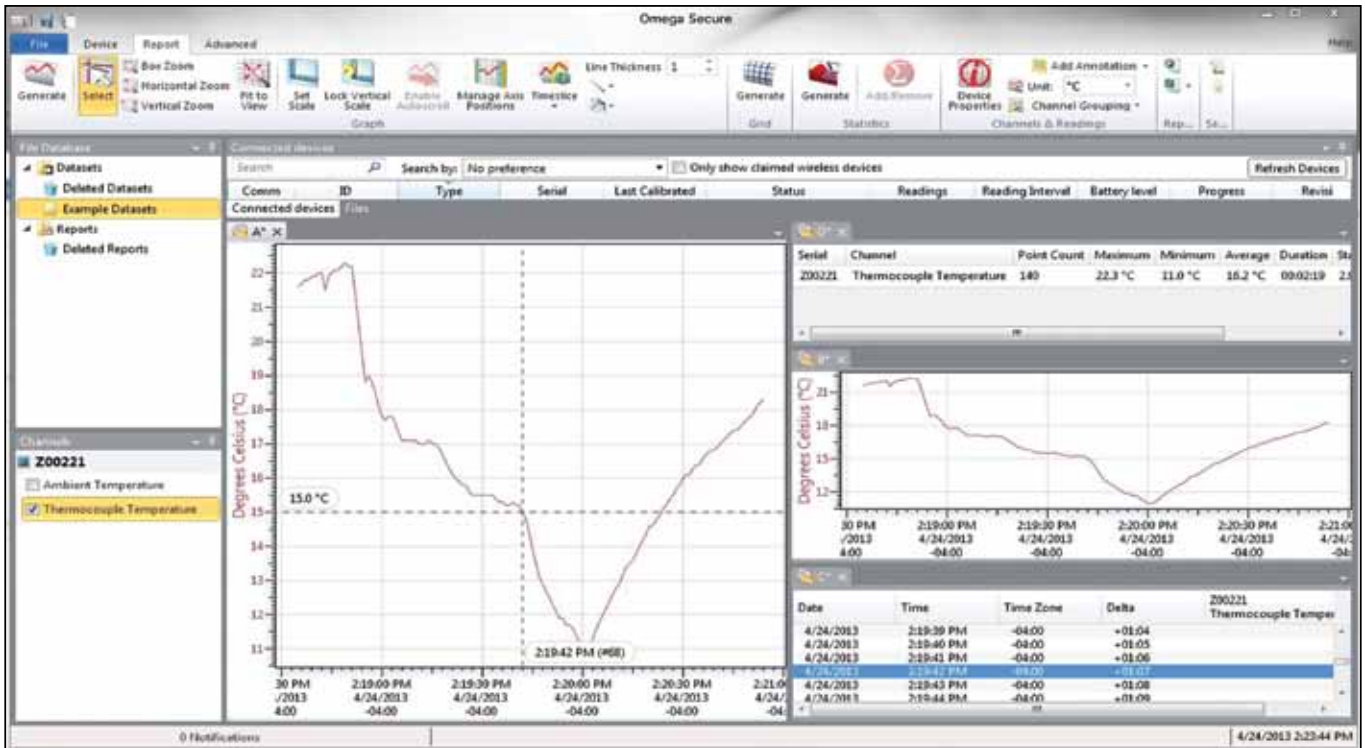
21 CFR Part 11 Requirement	Does OM-CP-SVP-SYSTEM Secure Software Comply?	No Additional Action Required to Comply?	Comments
The audit trail is available for review and reproduction by the FDA.	Yes	Yes	The OM-CP-SVP-SYSTEM Secure software allows the Audit Trail to be printed or transferred electronically for review and reproduction by the FDA.
When any sequence of system steps is important, that sequence must be enforced by the system.	No	No	The OM-CP-SVP-SYSTEM Secure software does not require any specific sequence of steps or order of operation. The customer is responsible for defining, writing and enforcing any SOPs that require a sequence of steps.
The system should ensure that only authorized individuals can use it, electronically sign records, access the operation or computer system input or output device, alter a record, or perform other operations.	Yes	No	OM-CP-SVP-SYSTEM Secure software requires unique User IDs and passwords to login to the system. Different features are available to different users depending on their level of access. These levels may be defined and created by the user. Defined SOPs should be implemented so the PC requires an authorized login and directs that users cannot share their unique user IDs and or passwords.
The system should be able to check the validity of the source of any data or instructions if it is a requirement of the system that input data or instructions can only come from certain input devices.	Yes	Yes	OM-CP-SVP-SYSTEM Secure software will only accept input and communicate with OM-CP Series data loggers using proprietary communication protocol. Each OM-CP Series data logger is uniquely identified by an electronic serial number.
(Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals.)			
A documented training, including on the job training for system users, developers, IT support staff should be available.	Yes	No	Users may provide their own training through testing and the support of OM-CP-SVP-SYSTEM Secure software documentation package.
A written policy that makes individuals fully responsible for actions initiated under their electronic signatures should be in place.	No	No	It is the responsibility of the customer to provide a written policy that informs individual users that they are responsible for all actions taken while under their login.
The distribution of, access to, and use of systems operation and maintenance documentation should be controlled.	Yes	No	The customer is responsible for obeying the licensing terms and distribution of the software and documentation that supports OM-CP-SVP-SYSTEM Secure software.
A formal change control procedure for system documentation that maintains a time sequenced audit trail of changes should be in place.	Yes	Yes	The OM-CP-SVP-SYSTEM Secure software operations document is revision controlled.

## Signed Electronic Records

21 CFR Part 11 Requirement	Does OM-CP-SVP-SYSTEM Secure Software Comply?	No Additional Action Required to Comply?	Comments
Signed electronic records should contain the following related information: <ul style="list-style-type: none"> <li>• Printed name of the signer</li> <li>• Date and time of signing</li> <li>• Meaning of the signing</li> </ul>	Yes	No	This name of the signer, the date and time of signing and the meaning of the signing are contained in all electronically signed records and all printed material. The customer is required to define the meaning of signing the document.
The above information should be shown on displayed and printed copies of the electronic record.	Yes	Yes	All the above information is displayed and printed on all copies of records.
Signatures should be linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification.	Yes	Yes	Signatures are linked to the original record and cannot be cut, copied, or transferred.

## Electronic Signatures (General)

21 CFR Part 11 Requirement	Does OM-CP-SVP-SYSTEM Secure Software Comply?	No Additional Action Required to Comply?	Comments
Electronic signatures must be unique to each authorized individual.	Yes	Yes	The OM-CP-SVP-SYSTEM Secure software will not allow the user to duplicate electronic signatures. It is recommended that SOPs include a statement clearly defining that only one person is linked to each user ID. The administrator must define the unique user IDs, the user must define their own unique password.
The reuse or reassignment of electronic signatures should be discouraged.	Yes	No	The end user SOPs should state that user IDs are not to be re-used or reassigned to anyone else. User IDs should be inactivated and a new ID created.
The identity of the individual should be verified before an electronic signature is allocated.	Yes	No	The end user SOP should state that the identity of the individual is verified before an ID is assigned. Once a new user is created, an email will be sent to the administrator and user verifying his/her own unique login password. Once verified the OM-CP-SVP-SYSTEM Secure software will identify the individual in the future via the user ID and password. The user will be required to enter their username and password.



### Electronic Signatures (Non-Biometrics)

21 CFR Part 11 Requirement	Does OM-CP-SVP-SYSTEM Secure Software Comply?	No Additional Action Required to Comply?	Comments
Signatures must be made up of at least two components such as an identification code and password, or an identification card and password.	Yes	Yes	To electronically sign a record, the username and password need to be entered.
The users password must be executed at each signing when several signings are made during a continuous session.	Yes	Yes	OM-CP-SVP-SYSTEM Secure software requires the password to be executed at each signing.
If signings are not done in a continuous session, both components of the electronic signature should be executed with each signing.	Yes	Yes	To electronically sign a record, the username and password need to be entered at each signing.
Non-biometric signatures should only be used by their genuine owners.	Yes	No	Users should put in place SOPs requiring that combination of user IDs and password only be made known to the genuine owner.
Attempts to falsify an electronic signature must require the collaboration of at least two individuals.	Yes	No	Users should put in place SOPs that forbid users from disclosing their unique user ID and password.

## Controls for Identification Codes and Passwords

21 CFR Part 11 Requirement	Does OM-CP-SVP-SYSTEM Secure Software Comply?	No Additional Action Required to Comply?	Comments
Controls to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password, are in place.	Yes	Yes	OM-CP-SVP-SYSTEM Secure software will not allow duplicate user IDs.
Procedures must be in place to ensure the validity of identification codes and that they are periodically checked.	Yes	No	The end user's SOP should state that the System Administrator is to periodically maintain active accounts and disable inactive accounts. OM-CP-SVP-SYSTEM Secure software allows the administrator to set accounts to expire automatically.
Passwords should periodically expire and need to be revised.	Yes	No	OM-CP-SVP-SYSTEM Secure software allows the administrator to give the user options to make user passwords expire as well as set warnings to notify the user in advance as to when the password is scheduled to be reset. The customer SOP should determine how often and/or when passwords expire.
Procedure for recalling identification codes and passwords if a person leaves or is transferred should be developed.	Yes	No	Passwords cannot be recalled; the administrator can reset the password. The SOP should state that the administrator can only reset a password if the password is lost or stolen, or the user leaves or is transferred.
A procedure for electronically disabling an identification code or password if it is potentially compromised or lost should be in place.	Yes	No	The OM-CP-SVP-SYSTEM secure software will allow user accounts to be temporarily or permanently disabled. The customer's SOPs will designate an administrator to have this responsibility. Only administrators can change user account settings.
A procedure for detecting attempts at unauthorized use and for informing security should be in place.	Yes	No	The OM-CP-SVP-SYSTEM Secure software will detect attempts at unauthorized use. All attempts are recorded and marked clearly in the audit trail. SOPs should be implemented so that a designated user is responsible for reviewing the audit trail for any suspicious activity.
A procedure for reporting repeated or serious attempts at unauthorized use to management should be in place.	Yes	No	The OM-CP-SVP-SYSTEM Secure software will detect attempts at unauthorized use. All serious or repeated attempts are emailed to the designated administrator(s). SOPs should be implemented so that a designated user is responsible for reviewing the audit trail for any suspicious activity.

### To Order

Model No.	Description
OM-CP-SVP-SYSTEM	FDA 21 CFR Part 11 compliant IQ/OQ/PQ secure software validation workbook and software package (unlimited users, license per computer). Compatible with Windows XP/Vista/7/8 (32-bit and 64-bit). Supports all OM-CP Series Data Loggers except OM-CP-SVR101.

**Ordering Example:** OM-CP-SVP-SYSTEM FDA 21 CFR Part 11 compliant IQ/OQ/PQ secure software validation workbook and software package (unlimited users, license per computer).