

Complying with

# FDA - 21 CFR part 11

## Electronic Records & Signatures

Unitronics' UniStream modular, all-in-one PLC+HMI controllers offer a cost-effective solution for Life Science manufacturers requiring compliance with the FDA 21 CFR Part 11.

UniLogic, the comprehensive application programming environment for UniStream controllers, offers features that enable the system to be validated to the 21 CFR Part 11 regulations, including:

- Program version control and revision history tracking
- User access control and administration
- Record keeping for changes to configuration, operator actions and alarms
- Data storage and export to generate audit trails

This document discusses the Unitronics UniStream PLC+HMI control tools for creating applications that are compliant with the 21 CFR Part 11 regulations.

### Version control of electronic data records and audit trail in UniLogic software

The UniLogic programming environment provides comprehensive tools for complying with regulations regarding version control of electronic data records as specified by 21 CFR Part 11. UniLogic software utilities enable the identification of changes in a UniStream program, including to the hardware configuration, ladder logic or HMI design. UniLogic automatically logs all project changes each time a new program is downloaded to a UniStream controller; the amended object, type of change, time stamp, and the user identification (electronic signature) are recorded. The logged data is encrypted and saved in the project database. The data can then be displayed in a clear list, enabling full traceability regarding the changes in the project program.

Access to the programmed project can be restricted to ensure only authorized users make changes. Downloading a new program to a controller can also be restricted to authorized users by assigning user names and a passwords. The code can be downloaded independently of a complete project, enhancing the application security. To ensure complete security, access to the computer on which the UniLogic application is installed must be controlled by the operating system's built-in passwords and encryption mechanisms.



---

## Audit trails of operator entries and actions recordings

The UniStream controller provides tools for security, tracks alarms, and logs operator actions and other operational data, enabling an audit trail. Using the data table functionality, the UniStream controller program can record any action that is performed by the system user or operator. The recording can include the identification of the user, the action that was performed and a time stamp. The data is stored in a log file in a proprietary file format or a CSV file.

Using the UniStream Alarms widget, an alarm log can be recorded by the controller. The program can require that alarms are acknowledged by an authorized user, who must enter their user name and password. The alarms, time stamp and user acknowledgment are logged in a proprietary file format or a CSV file.

Similarly, the Trends functionality can be used to track and log application data, which can be uploaded by authorized users to other database systems for data acquisition purposes. Changes to the logged values in these database files do not overwrite previous values. Furthermore, these files cannot be edited while they are stored in the UniStream controller.

It is important to emphasize that once application-related electronic records have been exported from the Unitronics UniStream and UniLogic environment, they should be protected using the database application, operating system or other security mechanism.

Detailed instructions and consulting on programming a 21 CFR Part 11-compliant application as well as UniLogic programming examples can be provided free of charge by Unitronics technical support specialists.

Note:

We reserve the right to make changes or modify the contents of this document without prior notice. Unitronics does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.



---

## HMI user administration and signing

In accordance with FDA 21 CFR Part 11, access to the HMI should be restricted to users with appropriate authorization. In order to comply with this regulation, the program for the UniStream controller should include the implementation multilevel access control. The user name and password entered to access the system acts as the electronic signature of a user or a system operator. User name and passwords corresponding to different access rights can be predefined using data table functionality, in order to limit certain system actions to specified users. Using data tables also allows the administrator to perform periodic password updates to enhance the access control protection.

As the controller program is a proprietary code, it is not possible to access the PLC/HMI program without the provided software.

Furthermore, it is possible to control access to the HMI and controller by either disabling specific communication ports or restricting their use to certain users. Physical barriers (e.g. rooms or cabinets with locked doors) should also be used, in order to limit access to the PLC+HMI and the computer on which the UniLogic software is installed.



### International Headquarters

P.O.B. 300, Ben Gurion Airport 7019900, Israel  
Tel : +972 3 977 88 88, fax : +972 3 977 88 77

[www.unitronics.com](http://www.unitronics.com)  
[global.sales@unitronics.com](mailto:global.sales@unitronics.com)