

Introducing the New Incucyte® 21 CFR Part 11 Software Module

With Incucyte® 21 CFR Part 11 Software You Can:

- Track all system and user actions with a global audit event log
- Guarantee secure and configurable login and password procedures with Windows Authentication
- Configure full system access with user permissions and exclusive user roles
- Trace protocol deviations and create mandatory audit trail entry selections
- Customize authentication actions to fit your laboratories exact requirements
- Filter, sort, search, and export all audit log entries

Compliant and User Friendly

The Incucyte® 21 CFR Part 11 Software Module is a software package providing comprehensive security and electronic record keeping functionality. Support your compliance needs while still keeping Incucyte's software intuitive and easy to use.



Specifications

Audit Trail	Electronic Records (continued)	Electronic Signatures
<p>11.10 (a) The ability to discern invalid or altered records.</p> <p>Incucyte® was developed and validated under a development process. Incucyte® utilizes watermarks and metadata files to discern invalid or altered records. Any files that have been directly tampered with will be prevented from running.</p>	<p>11.10 (g) Only authorized individuals can control actions executed by the equipment through the software.</p> <p>Multiple permission levels are provided to ensure each authorized user is only able to perform the required control over the system that they need.</p>	<p>11.50 The operator, date, time, and action are to be included as part of a human-readable electronic record.</p> <p>The username, date/time stamp, and action performed are all stored in data files, the database, and the global audit log, and can be exported to a PDF report.</p>
<p>11.10(b) Record generation and exporting is provided in a human readable format.</p> <p>Data can be exported for electronic record keeping in multiple formats such as text, image, or video files. Entire experiments can be archived for record keeping.</p>	<p>11.10 (h) Only valid actions and data files are inputted into the system.</p> <p>Incucyte® is a secure system providing the only access that enables users to interact with the equipment. Incucyte® applies watermarks to ensure only untampered images created by Incucyte® can be analyzed on the system.</p>	<p>11.70 Electronic signatures are locked with the recorded action. Records cannot be falsified.</p> <p>Incucyte® utilizes Windows Authentication preventing tampering with User IDs. The username and date/time stamp are stored in data files, the database, and printed on the report. Both the data file and reports are read-only and cannot be modified.</p>
<p>11.10 (c) Records are protected within the software.</p> <p>Incucyte® images are written once cannot be rewritten. Data can only be accessed from within the Incucyte® software.</p>	<p>11.10 (i) Customized education for users to properly run the equipment and the software.</p> <p>Sartorius professional support teams provide demonstrations for users on how to utilize all the Incucyte® 21 CFR Part 11 Software Module features.</p>	<p>11.100 Only unique users are allowed access to the system and able to sign for electronic signatures.</p> <p>Incucyte® utilizes Windows Authentication for both ease of use and to ensure the security and singularity of User IDs.</p>
<p>11.10(d) Limiting system access to authorized individuals.</p> <p>Incucyte® has security features that allow Admin Users to customize individual user roles for both access and specific system permissions.</p>	<p>11.10 (j) Hold individuals accountable and responsible for actions initiated under their electronic signature</p> <p>Incucyte® utilizes Windows Authentication to perform secure electronic signing.</p>	<p>11.200 Two distinct identification components are used for both continuous and non-continuous sessions.</p> <p>Incucyte® utilizes Windows Authentication enabling only an Admin User to provide unique User IDs and password control for access to the system and recording of actions.</p>
<p>11.10(e) Audit trails are secure, human-readable, and contain the relevant information about the instrument and analysis activities.</p> <p>The Incucyte® audit trail is stored in a secure database recording the date, time, operator, and specific action that was performed. The audit trail can be viewed and filtered within the software as well as exported as a PDF.</p>	<p>11.10 (k) (1) Documentation is available for system operation and maintenance.</p> <p>Sartorius provides documentation for the general usage and maintenance of the equipment along with guidance for setting up the Incucyte® 21 CFR Part 11 Software Module.</p>	<p>11.300 System provides secured unique user and password controls.</p> <p>Incucyte® utilizes Windows Authentication to provide and maintain secure control over User IDs and passwords.</p>
<p>11.10 (f) Only permitted actions in the correct sequence are authorized during equipment usage.</p> <p>Incucyte® provides sequential layout and wizards to guide the user on equipment usage. Users can only control the equipment through the software.</p>	<p>11.10(k)(2) Documentation and the source code for the software is under a version control system.</p> <p>Engineering and hardware are under a version control system.</p>	
	<p>11.30 Ensure the authenticity, integrity, and confidentiality of electronic records.</p> <p>Incucyte® is designed to run as a closed system. Both the equipment and the data can only be accessed through the Incucyte® user interface by authorized users.</p>	
		<p style="background-color: #ffff00;">Part Numbers</p> <p>BA-04876 Incucyte® 21 CFR Part 11 Software Module</p>

Germany:
Sartorius Lab Instruments
Phone +49 551 308 0

USA:
Sartorius Corporation
Phone +1 631 254 4249
Toll-free +1 800 635 2906

 **Learn more:** www.sartorius.com/incucyte-21-cfr-part-11

 **For questions, email:** LPS.OPM.NA@sartorius.com