

# Security Suite Software for Evolution series and NanoDrop One/One<sup>C</sup> Spectrophotometers

## Frequently asked questions

The Thermo Scientific™ Insight™ Pro and the Thermo Scientific NanoDrop™ One/One<sup>C</sup> PC Control Software are used to control the Thermo Scientific Evolution™ instrument and the NanoDrop One/One<sup>C</sup> instrument, respectively. For laboratories which require adherence to rigorous record-keeping regulations, like US FDA 21 CFR Part 11, the abilities to limit access to software features, require signatures when data is collected or manipulated, and record changes or events for audit purposes are paramount.

To aid in achieving this compliance, the Thermo Scientific Security Suite Software package can be used to record events, control user permissions, and enable the ability to electronically sign data, providing a trail of events.

This software package includes three separate programs:

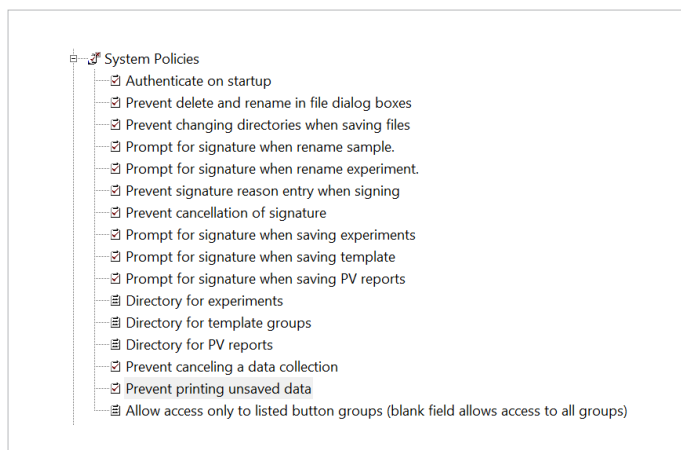
- **Instrument Software**—used to control the instrument, view data and perform calculations.
- **Security Administration**—used to grant or deny user privileges and control signature meanings and system policies.
- **Audit Manager**—used to review audit trail logs, sign audit reports, and verify logs.

Included herein is a list of frequently asked questions surrounding the capabilities of the Security Suite Software package, enabling your lab to comply with 21 CFR Part 11 requirements.

### Does the instrument software require a unique username and password to gain access?

No, the Insight Pro Software and NanoDrop One/One<sup>C</sup> PC Control Software, as well as the security software (Security Administration and Audit Manager), use the Windows User Account of the logged-on user to identify the current operator.

Users can be required to “Authenticate on Startup” as per the configuration of the system policy within the Security Administration Software, ensuring the appropriate user is able to access the software. By default, the Security Administration and Audit Manager Software requires authentication of the user to access the software.



### Can user access to the software or specific functions within the software be restricted?

Yes, through the Security Administration Software, users or groups can be permitted or denied access to the instrument software or other functions within the software.

Below is a list of a few of the available functions that can be restricted:

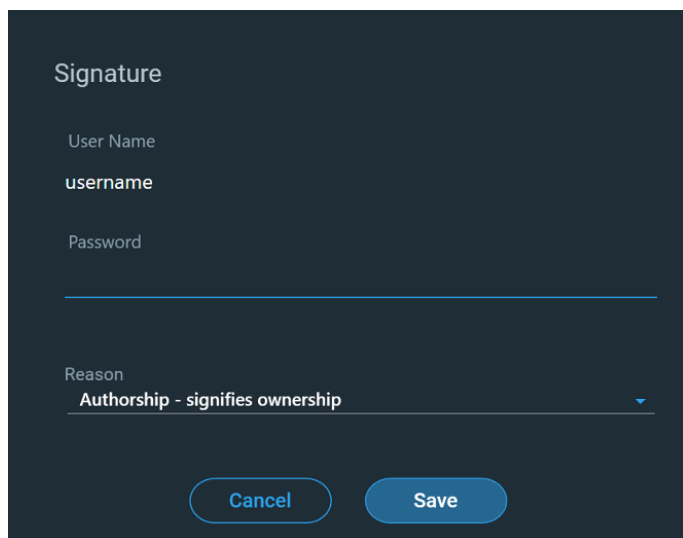
- Ability to run the instrument software
- Ability to re-name experiments
- Ability to edit settings
- Ability to configure reports
- Ability to delete experiments
- And more

### Does the software lock a user out after so many failed attempts of logging into the software?

No, the instrument software, as well as Security Administration and Audit Manager, will not lock a user out after a number of failed attempts.

### What actions require an electronic signature?

The Security Administration Software can be used to define the actions which require an electronic signature. By default, importing data into the History section of the instrument software requires a signature. In the instrument software, any action in which the data was altered, such as performing mathematical functions on the data or using the advanced calculations spreadsheet, requires a signature.



Below is a list of the available functions which can be configured to require a signature:

- Saving an experiment
- Saving a Performance Verification report
- Creating, modifying, or deleting a Custom Method
- Renaming a sample
- Renaming an experiment

### Can signature meanings be assigned?

Yes, signature meanings can be defined within the Security Administration Software and applied when a signature is required within the instrument software. Users or groups can be granted or denied the ability to sign data using specific signature meanings.

Below is a list of default signature meanings which can be assigned to the user:

- **Authorship**—signifies ownership
- **Approval**—the record is approved for use
- **Reviewed**—record contents have been reviewed
- **Revision**—the record has been revised

Additionally, custom signature meanings can be added, given the user has been granted permission with the Security Administration Software to do so.

### Can user roles be defined?

#### Can groups be created in the software?

User roles cannot be altered within the Security Suite Software. User or group Windows accounts are managed separately and can be given permission within the Security Administration Software.

Groups can be created through the Windows user management system and can be permitted or denied certain access controls and the ability to apply specific signature meanings within the Security Administration Software.

#### How is the raw data stored and secured within the software, and how can it be retrieved later?

Data collected within the instrument software is saved as an instrument-specific file (\*.iwbk for the Insight Pro Software and \*.ned for the NanoDrop One/One<sup>c</sup> PC Control Software) within a database format and can be located within the History tab. The database can be backed-up to provide a method of recovery in the event of a computer failure.

Data which was collected using an older version of the instrument software can be imported into the History tab and recalled within the software. This event would be documented in the Audit logs.

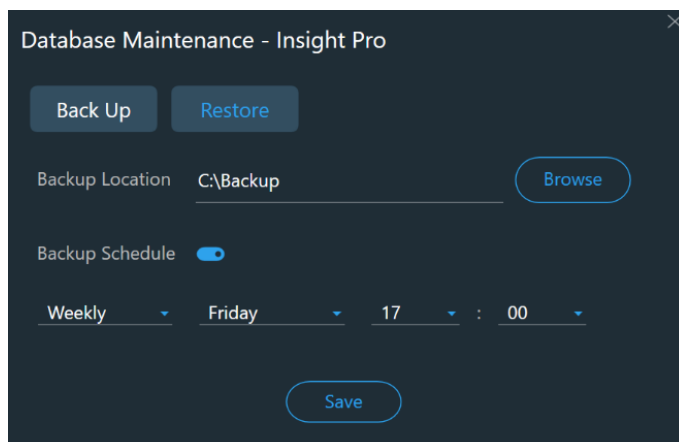
#### Can data from previous versions of the instrument software be migrated to the new software?

Given the software was installed in the same location, the experiments collected in earlier versions of the instrument software are retained in the History.

Additionally, only instrument-specific experiment files (\*.iwbk, \*.ned) can be imported within the instrument software. Any time an experiment file is imported into History, the event is recorded in the audit trail and requires a signature.

#### Is there a backup function for the system?

Yes, the database can be backed-up and restored within the instrument software. By default, the database would need to be backed up manually; however, a time can be selected to allow for automatic backup at a given cadence.



### Can the system be connected to a network?

When using the Insight Pro Software, the database can be set up on a network or a remote server. These capabilities can be controlled within the instrument software. This is not available within the NanoDrop One/One<sup>c</sup> PC Control Software.

### Can the ability to review the audit trail be restricted?

Yes, access to the Audit Manager software as well as the ability to sign records as “Reviewed” can be restricted within the Security Administration software.

### What information is captured in the audit trail?

The audit trail captures information about the operator who initiated the event, a description of the event, the software and computer on which the event occurred, the time of the event, and the severity of the event. Additional comments can be included in the audit logs as well, given the user has been granted this privilege.

### Does the audit trail capture when a user is created/ removed or if the role of a user is changed?

As the audit trail can only capture actions which occur within Audit Manager, Security Administration, the Insight Pro Software, or the NanoDrop One/One<sup>c</sup> PC control software, this event is not logged within Audit Manager.

However, if a user’s rights are changed within Security Administration, such as granting the ability to edit samples names or denying a user access to the instrument software, this event would be logged in the audit trail.

### Can the audit trail be printed?

An Audit Event Report can be saved by a user who has the appropriate privileges using a user-specified date range. The generated report can then be signed, verified, and printed within the Audit Manager software. This report includes the captured signature and date the report was signed in addition to each event log which occurred within the specified timeframe.

### Can audit trails collected from previous software versions be included?

Given the Audit Manager software was installed in the same location as the previous version of the software and the same database for the audit logs was selected, the audit logs from early software versions can be recalled in the Audit Manager software. If the software is installed in a different location or a different database is selected, previous logs from an earlier version of the instrument software will not be included. The Audit Manager software does not allow a user to import or export the logs from a database.

Learn more at [thermofisher.com/uv-vis](https://thermofisher.com/uv-vis)