






VENUS 21 CFR Part 11

User's Guide

P/N 6604796-01, Rev B

 System Settings	▼ Access restrictions	
 Error Settings	Checksum Verification	Disabled
 Security Settings	File Validation	Disabled
	Function Protection	Disabled
	▼ Miscellaneous	
	Audit Trail	Disabled
	Authentication System	Operating System
	List Used Files	Enabled

Contents

1	About	4
1.1	About this Document	4
1.2	Terms and Definitions	4
2	Overview	6
2.1	21 CFR Part 11.10 Compliance	7
2.1.1	Controls for Closed Systems: 21 CFR Part 11.10	7
2.1.2	Validation (a)	7
2.1.3	Readability (b)	8
2.1.4	Archived Record Protection (c)	8
2.1.5	System Security (d)	9
2.1.6	Audit Trail (e)	9
2.1.7	Sequencing (f)	9
2.1.8	Authority (g)	10
2.1.9	Location Checks (h)	10
2.1.10	Education/Training (i)	11
2.1.11	Written Policies (j)	11
2.1.12	Document Controls/Audit Trails (k (1))	11
2.1.13	Document Controls/Audit Trails (k (2))	12
2.2	User Groups	12
2.2.1	Lab Operator	12
2.2.2	Lab Operator 2	12
2.2.3	Lab Method Programmer	12
2.2.4	Lab Service	12
2.2.5	Lab Remote Service	12
2.3	Hamilton Security Settings	13
2.3.1	Checksum Verification	13
2.3.2	Function Protection	13
2.3.3	File Validation	13
2.3.4	Audit Trail	14
2.3.5	Authentication System	14
2.3.6	List Used Files	14
2.4	Hamilton Company Electronic Records	15
3	Setup	16
3.1	Enabling 21 CFR Part 11 Features	16

3.1.1	During VENUS Installation	16
3.1.2	After VENUS Installation	18
3.2	Configuring User Accounts.....	19
3.2.1	Hamilton Authentication	20
3.2.2	Operating System.....	22
4	Features	25
4.1	Validating Files	25
4.1.1	Validating Labware Definitions	25
4.1.2	Validating HSL Libraries	26
4.1.3	Validating Submethod Libraries and Methods/Layouts	26
4.1.4	Validating Liquid Classes.....	27
4.2	View Design History.....	27
4.2.1	Labware Definition Design History.....	28
4.2.2	HSL Library Design History	28
4.2.3	Submethod Library, Method, Layout Design History	28
4.2.4	Liquid Class Design History.....	28
5	Troubleshooting.....	29
5.1	Users.cfg is not signed for this system.....	29

1 About

1.1 About this Document

Revision History:

Version	Revision	Release Date	Description
01	A	04/2020	First draft
02	A	05/2020	Removed watermark
01	B	09/2020	Official release

All efforts have been made to ensure the accuracy of the contents of this manual.

Hamilton Company can assume no responsibility for any errors in this manual or their consequences. If any errors are found, please contact Hamilton Company.

Reproduction of any part of this manual in any form whatsoever without the express written consent of Hamilton Company is forbidden. The contents of this manual are subject to change without notice.

Copyright© 2020 Hamilton Company. All rights reserved.

Microlab® is a registered trademark of Hamilton Company.

NIMBUS® is a registered trademark of Hamilton Company.

The Microlab® STAR™, STAR^{PLUS}, STAR^{LET}, NIMBUS®, and NIMBUS HD, will be referred to as STAR and NIMBUS (respectively) for the remainder of this manual.

For the latest revisions of Hamilton manuals, drivers, and software, contact Hamilton support.

1.2 Terms and Definitions

Agency: Food and Drug Administration

Bilateral Identification: A method of verifying an individual's identity based on a user ID and password system.

Biometric Identification: A method of verifying an individual's identity based on measurement of the individual's physical features or repeatable actions where those features or actions are both measurable and unique to that individual.

Checksum: A system by which the authenticity of a file can be checked based on its binary code. The checksum value is updated every time a file is legitimately saved. If the checksum doesn't match when the file is reopened, the file has been improperly modified and the file is blocked from use. This system protects files from being improperly modified.

Closed System: An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Electronic Records: Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature: A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Method Files: A method in VENUS is defined by the .med, .stp, .lay, .sub, .res, and .hsl files. These six files are necessary for running a method in VENUS.

SOP: Standard operating procedure.

Trace Files: The file generated by VENUS for every runtime event. The trace file contains all the events of the run, date, time and user ID information.

Validation: Confirmation by examination and provision of objective evidence that the system specifications conform to user needs and intended uses, and that all requirements can be consistently fulfilled.

Vector/VENUS Software: Vector software, or VENUS, is the software designed for Hamilton robotic instrumentation control. The software provisions for 21 CFR Part 11 apply to all instruments controlled by the software, including the STAR.

2 Overview

Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES). Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable, and equivalent to paper records.

Laboratory implementation and compliance with the 21 CFR Part 11 regulation requires a program combining GLP (Good Laboratory Practice) with compliant instrument software and secure LIMS database management. Hamilton's Vector/VENUS software contains the tools necessary for 21 CFR Part 11-compliant operation of its robotic liquid handling instruments. This document describes the specific features of VENUS that enable compliant instrument operation, along with areas of laboratory responsibility.

Table 2-1: VENUS compliance summary

Requirements	Software Feature	21 CFR Part 11.10 Section
Controlled system access	VENUS uses the security tools provided in Windows 2000/XP/7/10 for five defined user groups	a, d
	VENUS functional protections	d, g
Files accessible and printable in a human-readable form	Files can either be printed as text or from the correct viewer	b
Electronic records protected and maintained throughout the records retention period	User ID and date/time stamps are applied to every electronic record when it is saved	g
	Changes to records are monitored by checksum	g
	Hamilton maintains backward compatibility when reasonable	b, c
	VENUS is compatible with database software programs for version control for complete audit trails	e

Requirements	Software Feature	21 CFR Part 11.10 Section
Documentation	Hamilton documentation for robotic instruments is controlled through an ISO-9001-compliant change control process consistent with 21 CFR Part 11 regulation	k (1)
Training	Hamilton provides ISO-9001-compliant training with certification of training for users	i

2.1 21 CFR Part 11.10 Compliance

This section lists each part of 21 CFR Part 11.10 and describes which parts VENUS directly supports, as well as those parts that individual laboratories are responsible for. Each part of 21 CFR Part 11.10 is quoted directly for reference.

2.1.1 Controls for Closed Systems: 21 CFR Part 11.10

“Persons who used 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:”

This requirement defines an electronic record as protected for closed systems. The subsequent requirements apply to all records created on a closed system, whether or not it is validated or formally recognized by the organization. The following subsections address more specific requirements.

Hamilton instruments are controlled by closed computer systems. A closed system is one to which access is controlled by persons responsible for the content of the electronic records on that system. Each section of 21 CFR Part 11.10 is included here, followed by an explanation of VENUS’s compliance approach and the implementation responsibilities of the end user.

2.1.2 Validation (a)

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

This part refers to the validation of the electronic signature system to be used. The electronic signature system must be able to restrict access to various levels of functionality, identify when (and by whom) a change is made to an electronic record, and whether these changes were validated. VENUS uses the security tools of the Windows operating systems, which allow for different user groups within an organization to have different levels of access to

the software. The files are user ID and date/time stamped whenever they are saved. In addition, these files are checksum-protected, which prevents inappropriate modification. Figure 2–1 shows an error message generated when a checksum-protected file has been inappropriately modified. This message will appear when the user attempts to reopen the file.

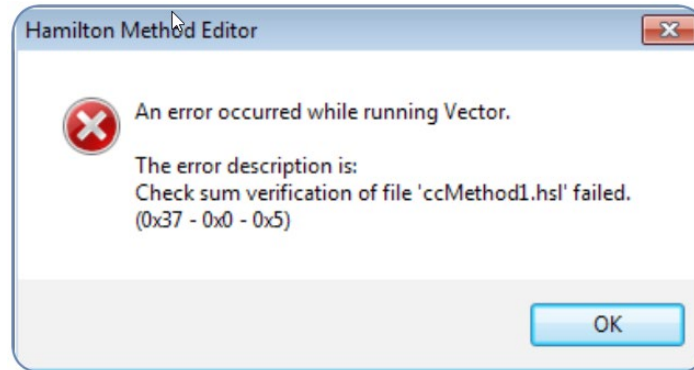


Figure 2–1: Checksum-protected file modification error

2.1.3 Readability (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.”

All records must be readily generated in either electronic or human readable form, along with the procedures used to create the records. This means all trace files must be retrievable along with the method files used to create these trace files. Organizations need to maintain electronic records as defined by agency-defined retention periods. Obsolete hardware and software versions do not need to be maintained, as long as all the records are retrievable after updating to new versions.

VENUS files are either binary or ASCII text. ASCII is easily printed in human-readable form with a text program. Other file types can be viewed and printed with the correct viewer or converted to ASCII and printed. Hamilton maintains backward compatibility of method files between software revisions when reasonable. In the event a software revision no longer supports an archived method, the appropriate software version must be maintained to support the archived record.

2.1.4 Archived Record Protection (c)

“Protection of records to enable their accurate and ready retrieval throughout the records retention period.”

This part is similar to part (b), requiring maintained electronic files throughout the data retention period—however, this rule is not limited to retrieval of data. The method must be able to be processed as originally done. Hamilton maintains backward compatibility of method files between software revisions when reasonable. Even if the current software version on the instrument does not support the archived method, records associated with the archived methods can still be viewed and are protected.

2.1.5 System Security (d)

“Limiting system access to authorized individuals.”

System access can be limited by current bilateral identification systems, such as user ID and passwords, or by a single biometric identification. User access must be defined and limited to various levels of the software. This security can be applied by through Windows security tools. System access for VENUS is controlled through the Windows operating systems, which allow access to various levels of the software based on the user group membership of the user that is logged in. If a user with an insufficient access level attempts to enter restricted sections of the software, an error message is displayed and the user is blocked from inappropriate access.

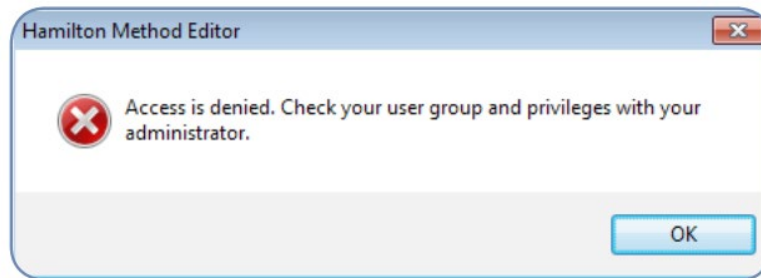


Figure 2-2: Access denied error

2.1.6 Audit Trail (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 shall be available for agency review and copying.”

Complete audit trail documentation is outside the scope of VENUS, and must be maintained by laboratory practices.

2.1.7 Sequencing (f)

“Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.”

The purpose of operational system checks is to verify that operations are not performed out of sequence as defined by the method. It is the agency's intent that such checks be performed by the computer system. Method checkpoints can be written into the program to direct the user and ensure that certain events have taken place before continuing with the method, such as all labware being in position. However, fulfilling this is a laboratory procedure and is not enforced within VENUS.

2.1.8 Authority (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.”

Five user groups are defined in VENUS, each with a distinct level of access. The groups are summarized in Table 2–2, with more detail on each group provided in section [2.2](#). Methods can be controlled by saving validated methods in an access-controlled directory. Lab Operator and Lab Operator 2 user groups should be denied access to directories containing non-validated methods while having read-only access to validated method directories. Additional protection is supplied by the checksum system for all records, which protects files from inappropriate modification. The user ID and time/date stamp are applied to every electronic record when it is saved.

Table 2–2: VENUS user groups

User Group	Allowed Function
Lab Operator	Allowed to run validated methods
Lab Operator 2	Allowed to run validated methods and move labware using the Layout Editor
Lab Method Programmer	Allowed to change methods, labware, and sequences
Lab Service	Allowed full access in order to install and service the system
Lab Remote Service	Allowed to read data only

2.1.9 Location Checks (h)

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

This requirement is applicable to a source of data (such as a plate reader) that can receive commands from more than one system, such as on a network. The instrument or device sending data would have to question the source of the command to ensure that only the authorized instrument is the actual source of the commands. Hamilton instruments have hardwired connections to the computer. For unique instruments, location checks are unnecessary. In the event of identical instruments under control by the same computer, the node identity of the second instrument must be changed from the default setting during installation, creating a unique address for each of the identical instruments and differentiating the systems to the computer. Correct instrument identification is verified during instrument installation.

2.1.10 Education/Training (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.”

Hamilton Company supplies training and application support as necessary to assist in developing and maintaining application performance. After training with a Hamilton representative, each trainee receives a certificate of training completion. This certificate can be used to document adequate training for use of a Hamilton instrument. Internal training programs and documentation need to be developed and documented by the end user laboratory.

2.1.11 Written Policies (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.”

This is a laboratory procedure, separate from Hamilton instrumentation.

2.1.12 Document Controls/Audit Trails (k (1))

“Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.”

This rule applies to the system documentation, which describes how a system operates and is maintained. System documentation includes, but is not limited to, operation manuals, help files, SOPs, access information, operating system manuals and privilege logs. This rule only pertains to documentation that can be changed by individuals within an organization. Documentation of Hamilton instrumentation, can only be changed by Hamilton:

- Software manuals
- Hardware manuals
- Technical bulletins
- Service bulletins
- Help files

Laboratories do not need to control these documents. While laboratories do not need a change control procedure for these documents, they are responsible for archiving and making them accessible to the appropriate users. Laboratories are also responsible for protecting their own documents regarding Hamilton instrumentation. Hamilton regulates the distribution of, access to and use of system documentation by ISO-9001 compliant procedures.

2.1.13 Document Controls/Audit Trails (k (2))

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

This rule refers to the same documents referenced in the previous section. Hamilton maintains an internal change control process for documentation by procedures that are consistent with the 21 CFR Part 11 guidelines. Laboratories are responsible for the change control process of their internal documents.

2.2 User Groups

When using user-restricted access through Function Protection (see section [2.3.2](#)), access rights are granted based on membership in one of the following user groups. These groups have the same labeling and access rights between Operating System (Windows login) and Hamilton Authentication (VENUS login) methodologies.

2.2.1 Lab Operator

Lab Operators can run methods. If File Validation is enabled, they may only run validated methods. They are not able to make any changes to any files, validate files, or access the System Configuration Editor.

2.2.2 Lab Operator 2

A user with in the Lab Operator 2 group can run a method and may move elements in deck layout files. If File Validation is enabled, they may only run validated methods. If File Validation is enabled, moving elements on the system layout will set the layout to “not validated” and prevent users in the Lab Operator and Lab Operator 2 groups from running it.

Lab Operator 2 users cannot make any changes to any non-layout files, validate files, or access the System Configuration Editor.

2.2.3 Lab Method Programmer

Lab Method Programmers can edit any VENUS files, or create new ones. They can also validate files and run both validated and non-validated methods, but they cannot access the System Configuration Editor.

2.2.4 Lab Service

Lab Service has the same permissions as Lab Method Programmers, and they can also access the System Configuration Editor and make changes.

2.2.5 Lab Remote Service

Lab Remote Service users can only view data.

2.3 Hamilton Security Settings

This section describes the VENUS settings that support 21 CFR Part 11.10 compliance in detail. These settings are accessed through the System Configuration Editor.

2.3.1 Checksum Verification

VENUS files contain checksums and last modified timestamps. A checksum is a value representing the sum of the correct digits in a piece of stored or transmitted digital data (such as a Labware Definition or method file in VENUS), against which later comparisons can be made to detect corruptions or modifications in the data. This value is updated each time the file is saved using a VENUS-associated application like the Labware and Method Editors, but it does not change if the file is manipulated by external means, like Notepad.

When Checksum Verification is enabled, VENUS files are tested for valid checksums whenever they are opened. If the checksum of one or more files is not valid, an error message is displayed and the method fails to open or execute.

Checksum Verification also detects when VENUS files have been edited outside of Hamilton software, which would circumvent other security settings and indicates file tampering may have occurred. Additionally, this functionality will detect file corruption, unrelated to tampering.

2.3.2 Function Protection

Function Protection allows the access rights of users to be limited via use of an authentication system. Two options are available for defining user roles: Hamilton Authentication and Operating System. Refer to section [2.3.5](#) for details.

Function Protection is required in order to use File Validation. This functionality defines the roles used to determine who has rights to perform various Validation functions or run non-validated methods. Additionally, this function can be used to deny access or editing functionality to various VENUS components; refer to section [2.2](#) for details on user group permissions.

2.3.3 File Validation

File Validation notifies the user whether the method they are attempting to run (including all associated VENUS files) has been validated or not. File Validation is only available if Function Protection is enabled (see section [2.3.2](#)).

File Validation serves as a means to restrict which methods can be executed by a particular user group, allowing for the methods and associated files to require “validation” (a form of “release” or “production” labeling) by an authorized method developer prior to being run by Lab Operators. This prevents Lab Operators from using methods, libraries, labware definitions, and other VENUS files that have not been fully validated for use in production.

2.3.4 Audit Trail

The Audit Trail requests a change description whenever a particular action is performed within the VENUS software, including the Labware and CO-RE Liquid Editors. This information, as well as the username and timestamp, can be retrieved by selecting “View Design History” in the corresponding application.

Two options are available when enabling Audit Trail. The “Validation Only” option only requests and records audit trail information when the user has opted to validate a file. The “Always” option requests and records audit trail information when the user has opted to validate a file or save a file.

The Audit Trail creates a record of when a file was modified or validated, increasing traceability. This record can be opened and printed to a PDF using “View Design History”.

2.3.5 Authentication System

The Authentication System sets the method by which user account credentials are determined for user access. The two options available are Hamilton Authentication and Operating System. To ensure compliance with 21 CFR Part 11, it is required that Function Protection via the Operating System Authentication option be enabled. This would allow IT to require periodic resets of passwords for the users. The Hamilton Authentication option does not allow for such a functionality and is therefore not fully compliant.

2.3.5.1 Hamilton Authentication

The Hamilton Authentication option allows for the creation of user accounts for individual users. Once enabled, opening Run Control, Method Editor, or any other Hamilton software will require the user to enter a valid username and password to continue.

2.3.5.2 Operating System

The Operating System option allows these same roles to be defined using Windows Local Users and Groups by assigning a user's login to a particular group. As this uses the Windows login credentials to determine access rights, there are no additional username/password prompts.

2.3.6 List Used Files

The List Used Files setting lists all the VENUS files that are associated with the method being run, including libraries, layouts, and labware files. This information is printed to the end of the method trace file.

The list of used files serves to enhance traceability of all components used in a method, but also serves to help identify any files requiring validation during test runs by a Method Programmer, if File Validation is being used.

2.4 Hamilton Company Electronic Records

Operation of a Hamilton instrument involves multiple file types or electronic records, which need to be protected under 21 CFR Part 11. These can be input files for method development and runtime, or output files, which are created by the software during runtime.

- Input Files
- Labware Definitions
- Liquid Class Definitions
- Method Files
- System configuration files
- Output Files
- Trace files

Barcode and worklist files are not protected by VENUS. These files may be created and used by programs outside of Hamilton's control. Further protection of these files for full compliance must be accomplished by laboratory practices.

3 Setup

The general steps for setting up VENUS for 21 CFR Part 11 compliance are as follows:

1. Enable the function protections in VENUS.
2. Define user groups, and assign users to these groups with unique user IDs and passwords.
3. Define SOPs and practices for complete laboratory compliance.

This chapter covers the first two steps in this procedure. It is the responsibility of the laboratory to define SOPs and practices for areas of 21 CFR Part 11 compliance that VENUS cannot support. These areas may include the following:

- Maintaining archives of old methods and software revisions throughout the records maintenance period
- Implementing practices or additional software sufficient for a complete audit trail of records
- Maintaining internal documentation on any Hamilton instrumentation

3.1 Enabling 21 CFR Part 11 Features

The 21 CFR Part 11 functionality in VENUS can be enabled during or after VENUS installation via the System Configuration Editor.

3.1.1 During VENUS Installation

During installation, a dialog with 21 CFR Part 11 options will be displayed with “Use file checksums to validate files” enabled and everything else unselected. This enables Checksum Verification (see section [2.3.1](#)) and is usually left enabled regardless of whether or not any of the other security options are needed. Selecting “Restrict functionality by user logon” will enable Function Protection (section [2.3.2](#)) and Authentication System (section [2.3.5](#)), while enabling “Record (all) file names in the runtime trace” enables List Used Files (section [2.3.6](#)).

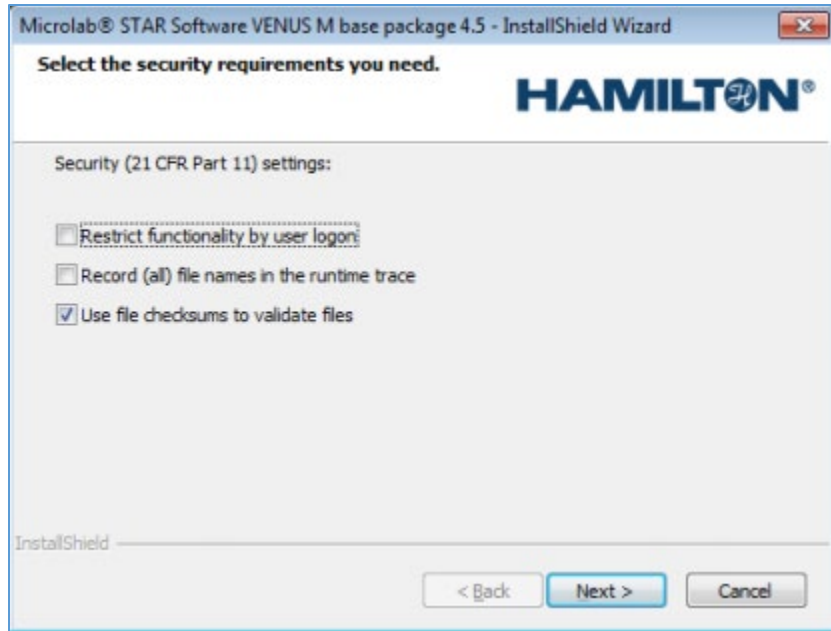


Figure 3–1: First 21 CFR Part 11 installation dialog

If “Restrict functionality by user logon” is enabled, another dialog will appear while continuing installation.

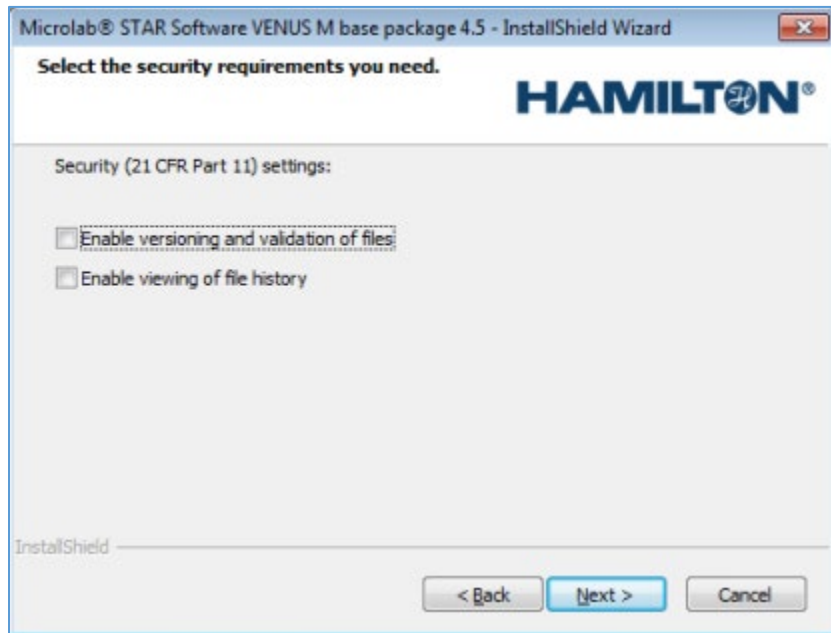


Figure 3–2: Second 21 CFR Part 11 installation dialog

This second dialog can be used to enable the following features:

- File Validation (section [2.3.2](#)): “Enable versioning and validation of files”
- Audit Trail (section [2.3.4](#)): “Enable viewing of file history”.

If Audit Trail is enabled, one more 21 CFR Part 11 dialog will appear with the option to turn on Audit Trail for all changes saved by enabling “Force audit trail for all file changes”, instead of only when validating files.

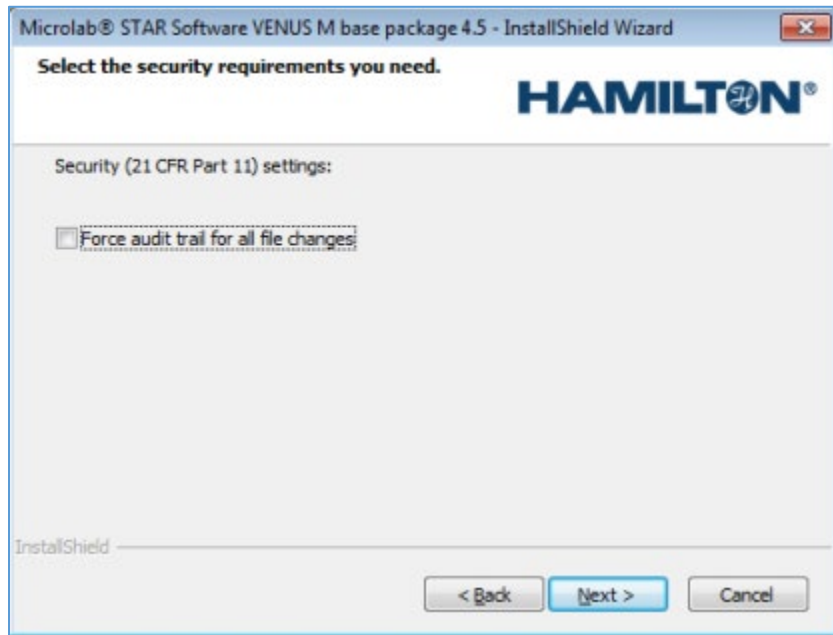


Figure 3–3: Third 21 CFR part 11 installation dialog

3.1.2 After VENUS Installation

Features that support 21 CFR Part 11 compliance can be enabled or disabled in the System Configuration Editor after installation.

1. **Open the System Configuration Editor.** From the Method Editor, click Tools > System Configuration Editor.
2. **Select the Security Settings tab** on the left.
3. **Enable the desired 21 CFR Part 11 features** in the right panel.

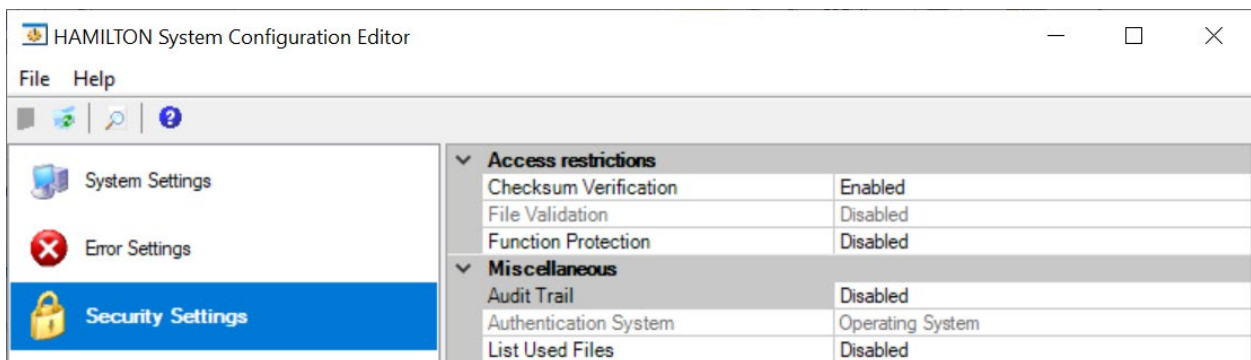


Figure 3–4: Enabling security settings for 21 CFR Part 11

4. **Click Save** or select File > Save changes.

Alternatively, close the System Configuration Editor and save the changes using the dialog shown in Figure 3–5.

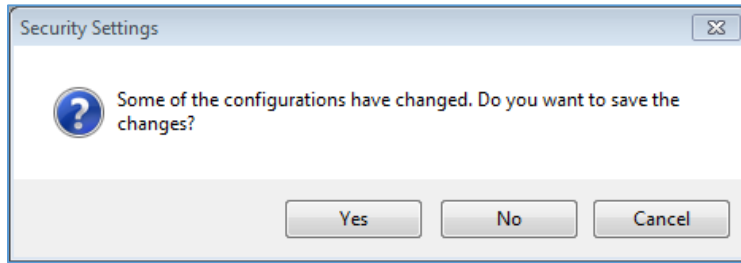


Figure 3–5: Save security setting changes dialog

5. **If Function Protection was enabled, click Yes in the dialog shown in Figure 3–6.**

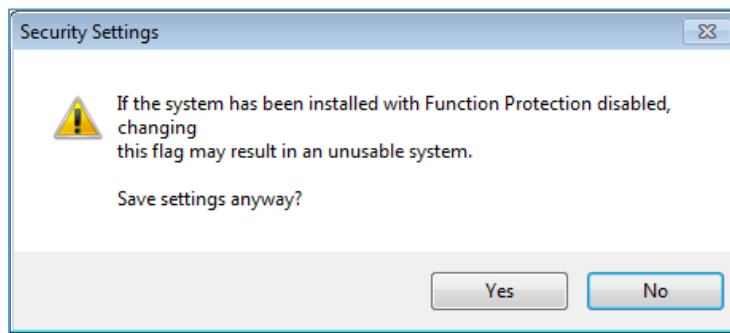


Figure 3–6: Function Protection warning

6. **When prompted, close any other Hamilton applications that may be open and click Yes.**

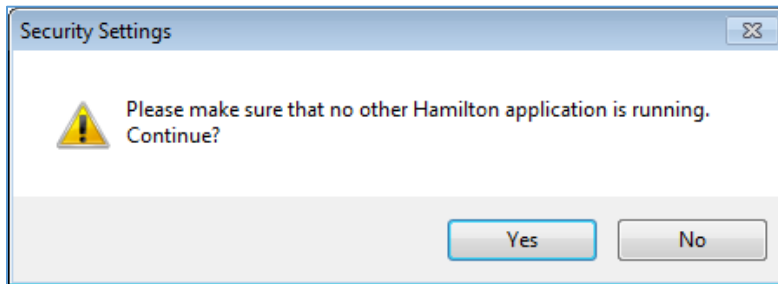


Figure 3–7: Disable Hamilton applications warning

3.2 Configuring User Accounts

After enabling Function Protection, individual accounts must be configured for the users based on the desired access restrictions. The configuration process differs between Hamilton Authentication and Operating System authentication options, but the rights assigned to each group name is the same across both options. Refer to section [2.2](#) for details on the user groups.

3.2.1 Hamilton Authentication

User accounts defined via the Hamilton Authentication method are configured in the **System Configuration Editor**. Once Hamilton Authentication is enabled, the default administrator account must be used to access the System Configuration Editor and create new accounts.

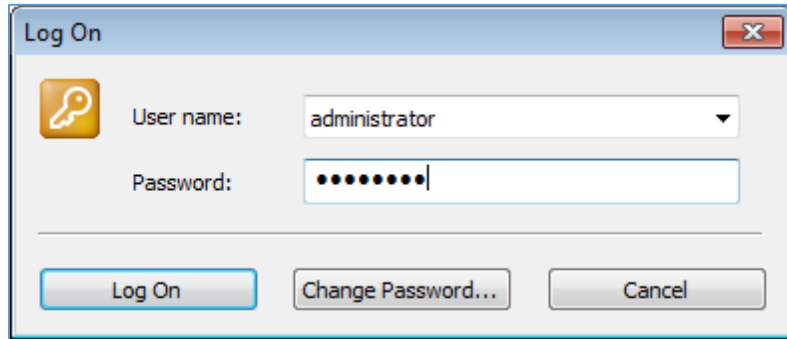


Figure 3–8: Default administrator login

The default admin username is “administrator” with the password “Hamilton” or “hamilton” depending on the version of VENUS installed.

1. **Open the System Configuration Editor.** Open the Method Editor, log in using the “administrator” account, and click Tools > System Configuration Editor.
2. **Select the Manage Users tab** on the left.

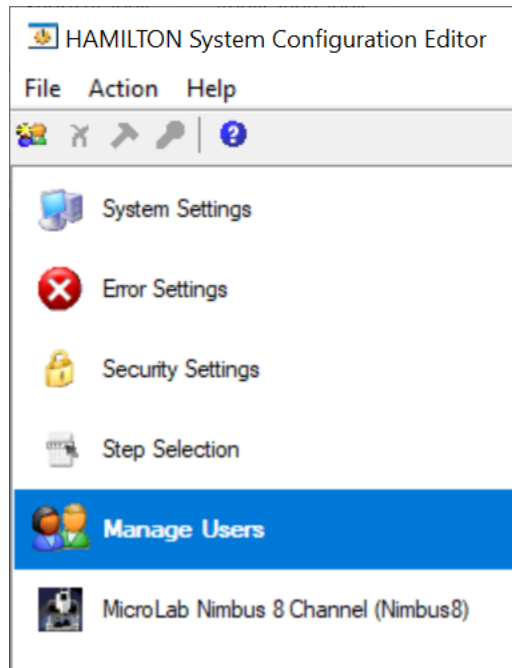


Figure 3–9: Manage Users tab

3. **Create as many new users as needed** by clicking the Create new User button.

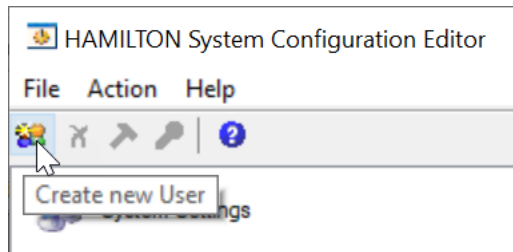


Figure 3–10: Creating new users

4. **Assign each user to the appropriate user group.** Click the desired user to highlight it, then select its group in the Permissions panel.

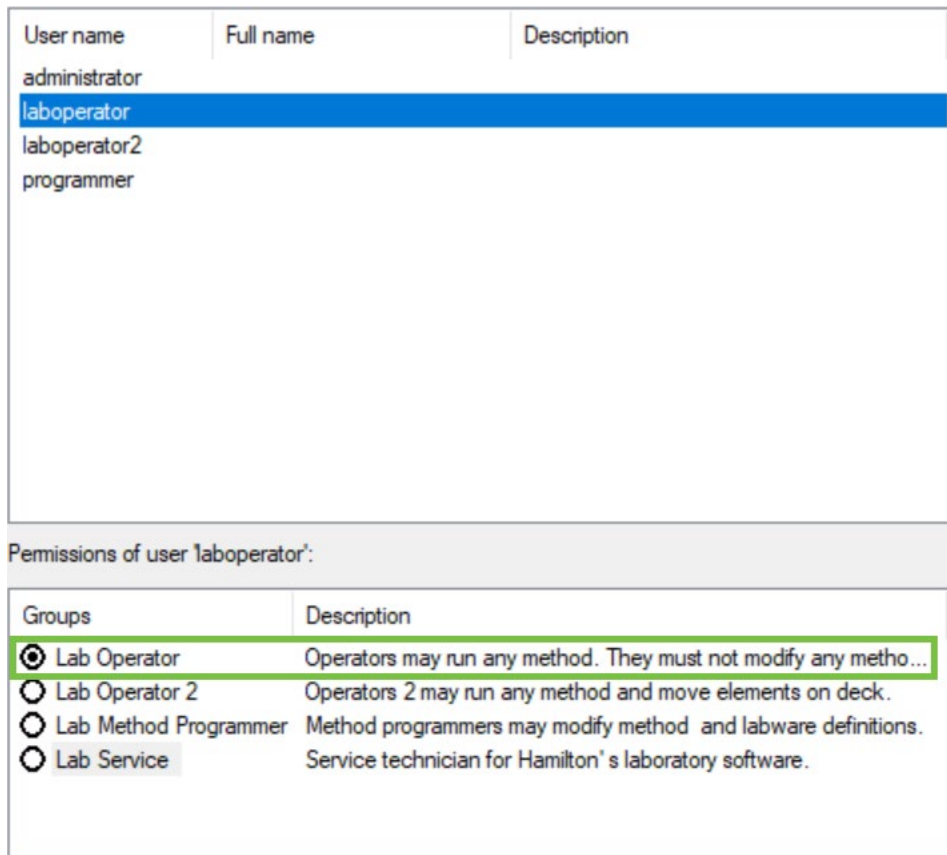


Figure 3–11: Assigning a user group

5. **Right-click a user to change their user information**, such as their name or password.

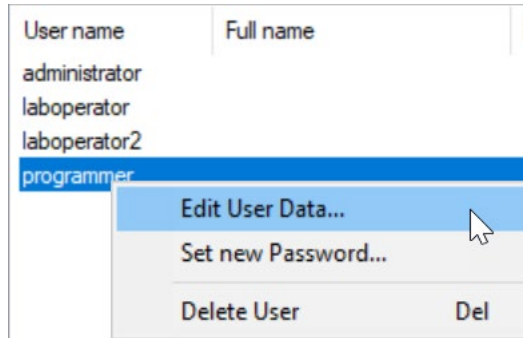


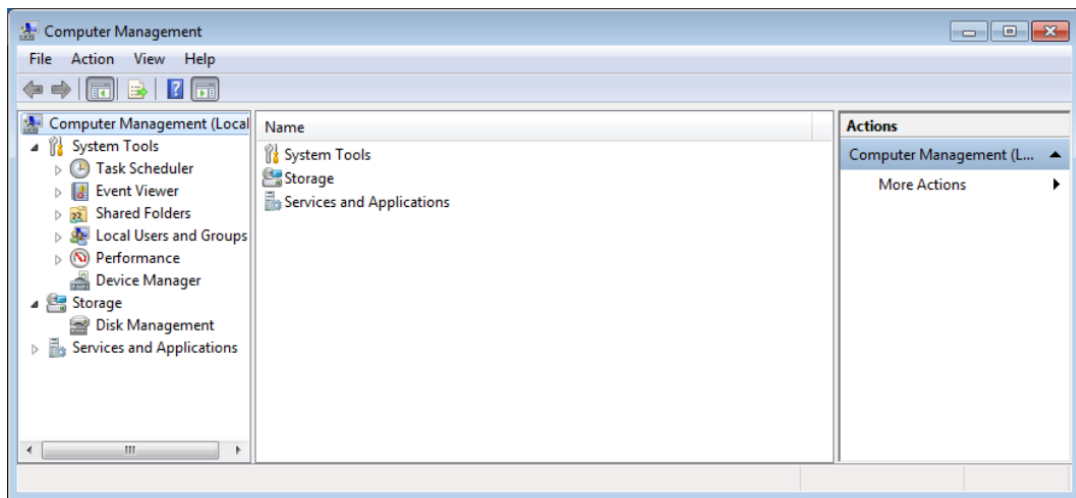
Figure 3-12: Editing user information

6. **Close the System Configuration Editor when finished.** New user accounts are saved as they are created, so they do not need to be saved manually.

3.2.2 Operating System

User accounts defined via the Operating System authentication method are configured in the Windows Local Users and Groups screen.

1. **Open the File Explorer, right-click This PC, and select Manage.** The Computer Management window will appear.



2. **Navigate to System Tool > Local Users and Groups > Groups.** The user groups will appear in the middle panel.

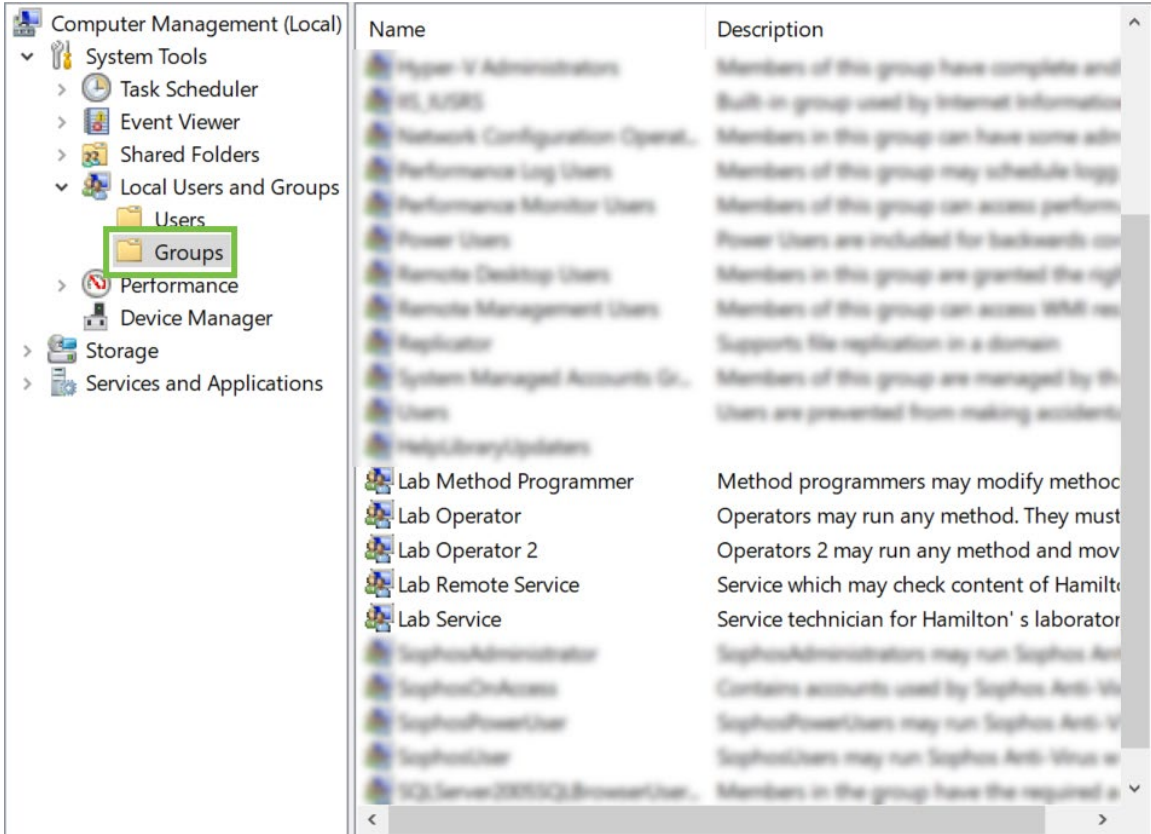


Figure 3–13: User groups in Computer Management window

3. Add users to the appropriate groups as needed:

- a. Double-click the group to open its properties.

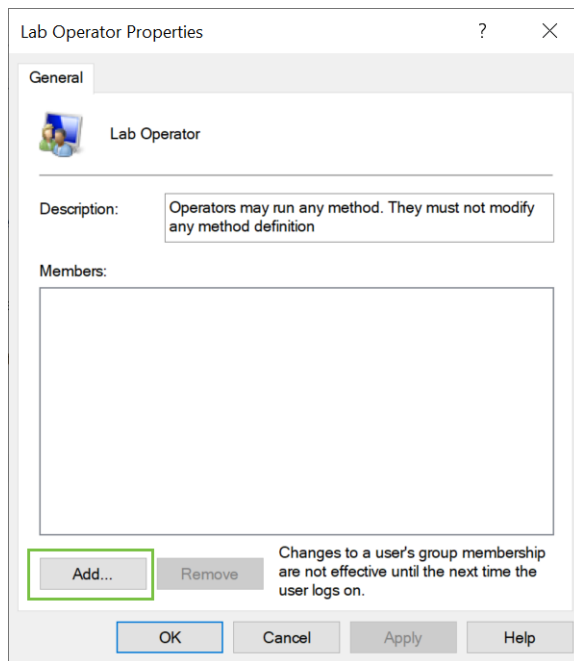


Figure 3–14: User group properties

- b. Click Add. The Select Users dialog appears.
- c. Type the desired username in the format DOMAIN\username in the field labeled "Enter the object names to select". Click Check Names to verify that the username is correctly entered.

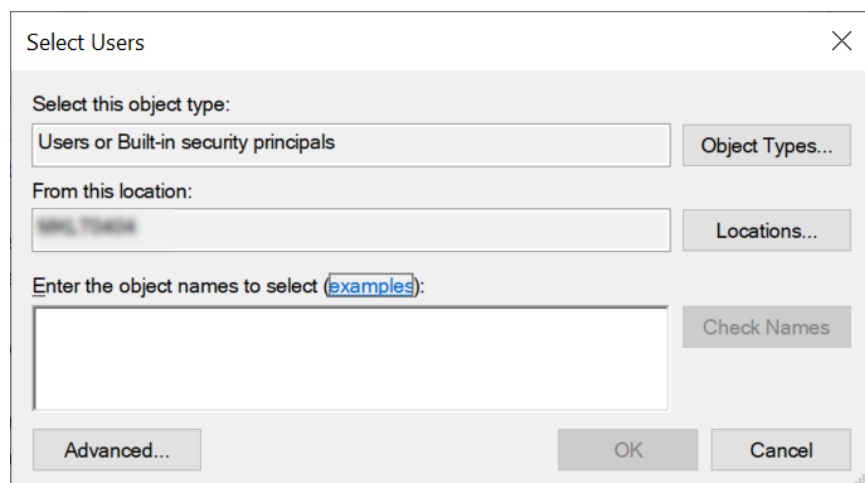


Figure 3–15: Adding users

- d. Click OK in the Select Users and user properties dialogs.
4. **Log out, then log in and back in** for the new permissions to take effect.

If an error occurs when using Check Names, contact your IT department to assist with assigning users to the local groups.

4 Features

4.1 Validating Files

When using **List Used Files**, the end of the trace will show the associated files and those requiring validation, such as method and submethod library files, layouts, liquid classes, and labware definitions.

```

18:46:39> SYSTEM : End method - start;
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Labware\Example\12 Column Trough.tml
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Labware\Example\ek_2034_12col_dw_reservoir.ctr
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Labware\Example\EK_2034_12col_DW_reservoir_col.rck
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Labware\ML_STAR\CO-RE-GRIP\core grip tool 1000ul model.ctr
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Labware\ML_STAR\CO-RE-GRIP\CORE Grip Tool 1000uL Model.rck
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Labware\ML_STAR\Tips\ST_L_NE_stack.rck
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Library\Alpha Numeric Conversion\Alpha Numeric Conversion.hs_
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Library\Alpha Numeric Conversion\Alpha Numeric Conversion.hsi
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Library\Alpha Numeric Conversion\Alpha Numeric Conversion.stp
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Library\ASWStandard\TraceLevel\TraceLevel.hsl
18:46:39> SYSTEM : End method - progress; Object not validated: File C:\Program Files (x86)\HAMILTON\Library\ASWStandard\TraceLevel\TraceLevel.t

```

Figure 4–1: Validation trace info

Non-validated components are listed as “Object not validated” in the first section of the list of used files. Some files, such as .res and .hsl files with the same name as the method, are all part of the method itself, and will therefore be validated automatically when the method or layout is validated.

If File Validation is enabled after installation, some preexisting files may need to be opened using the corresponding editor for validation if the file was not originally validated.

4.1.1 Validating Labware Definitions

1. **Open the Labware Editor.** From the Method Editor, click Tools > Labware Editor.
2. **Click File > Open and browse for the file to validate.**
3. **Click File > Validate.** The validation dialog appears.

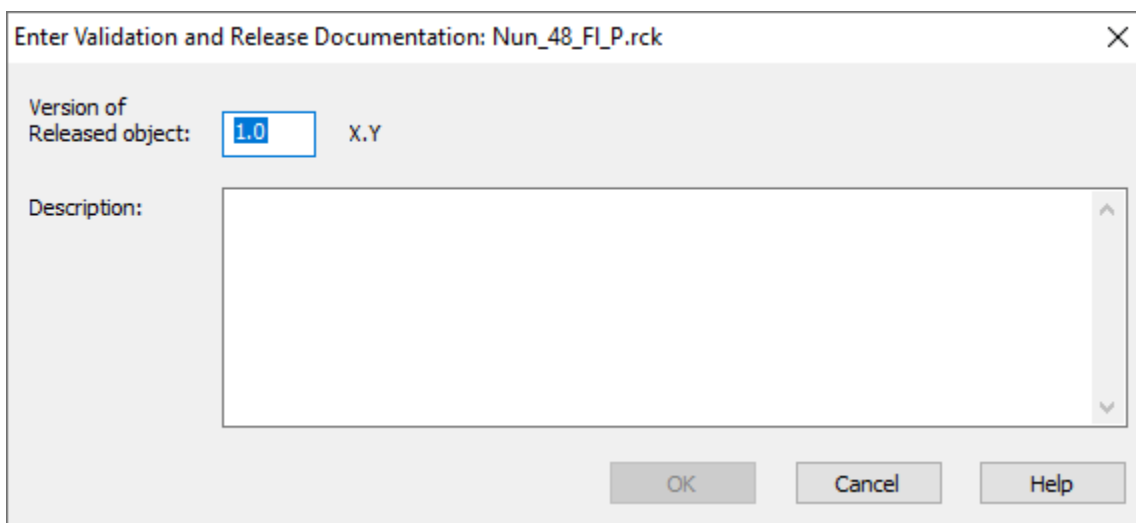


Figure 4–2: Labware validation dialog

4. **Enter the version number and an appropriate description.** Click OK when finished.

4.1.2 Validating HSL Libraries

1. **Open the HSL Method Editor** (HxHSLMetEd) from the Hamilton\Bin directory.
2. **Click File > Open and browse for the file to validate.**
3. **Click File > Validate.** The validation dialog appears.

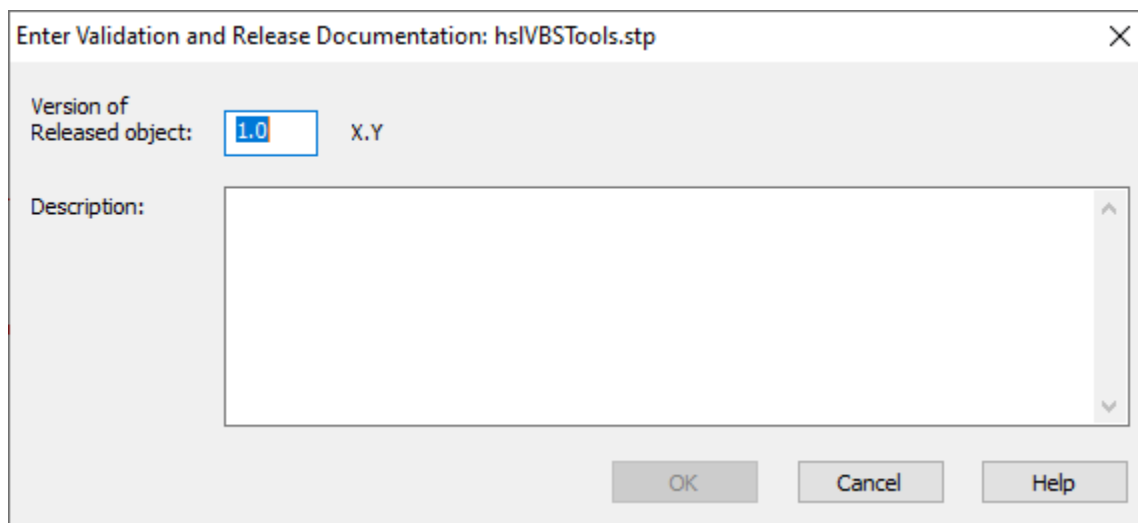


Figure 4–3: HSL Library validation dialog

4. **Enter the version number and an appropriate description.** Click OK when finished.

4.1.3 Validating Submethod Libraries and Methods/Layouts

1. **Open the Method Editor.**
2. **Click File > Open and browse for the file to validate.**
3. **Click File > Validate from the view of the file to validate.** Layouts and methods are validated separately, and the validation applies to the view that is active when the validation dialog opens.

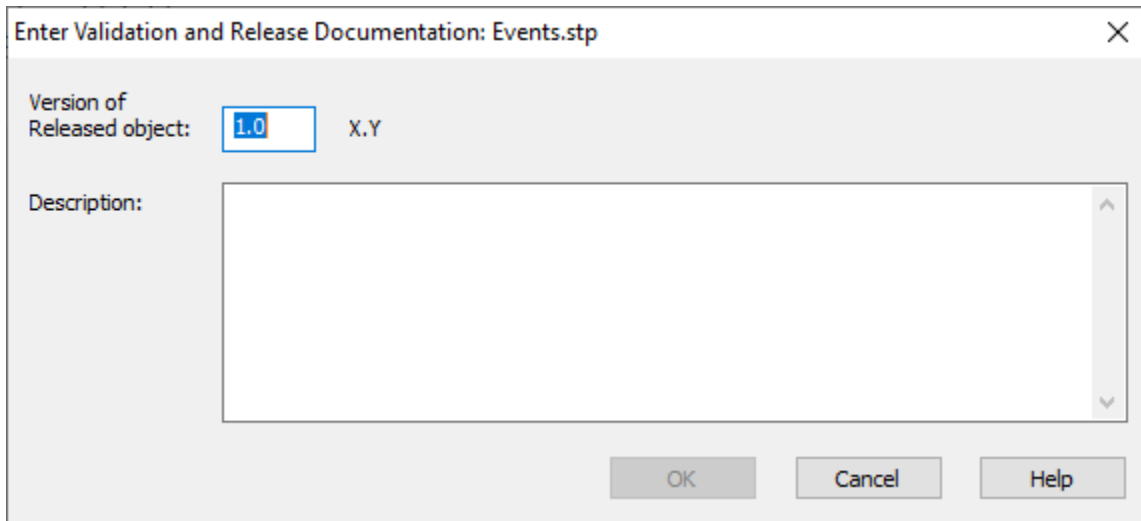


Figure 4-4: Submethod library validation dialog

4. **Enter the version number and an appropriate description.** Click OK when finished.

4.1.4 Validating Liquid Classes

1. **Open the CO-RE Liquid Editor.**
2. **Right-click the desired Liquid Class and click Validate.** The validation dialog appears.

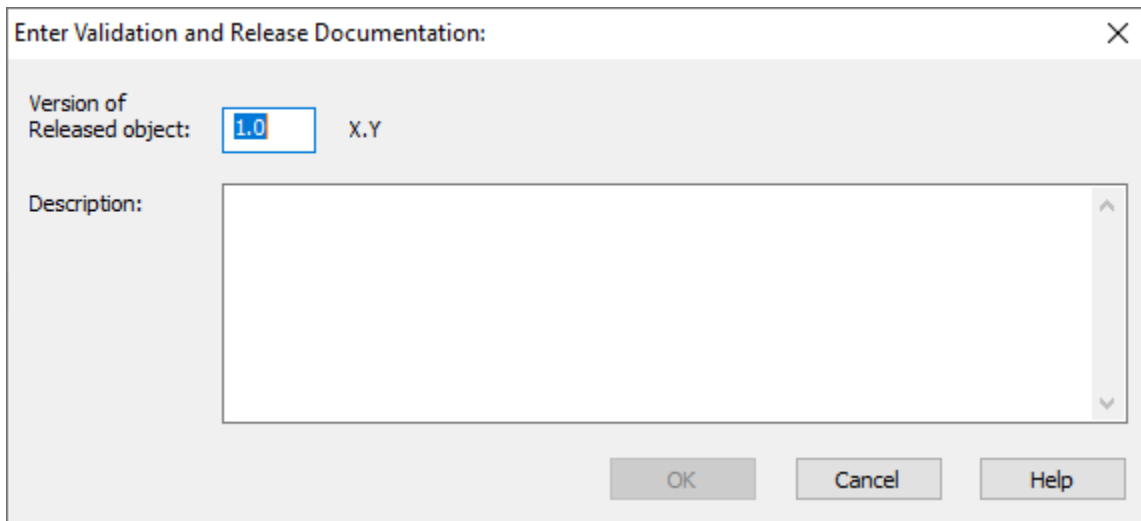


Figure 4-5: Liquid Class validation dialog

3. **Enter the version number and an appropriate description.** Click OK when finished.

4.2 View Design History

The Design History of a file can be viewed by opening it in the corresponding editor.

4.2.1 Labware Definition Design History

1. **Open the Labware Editor.** From the Method Editor, click Tools > Labware Editor.
2. **Click File > Open and browse for the desired labware.**
3. **Click File > View Design History.**

4.2.2 HSL Library Design History

1. **Open the HSL Method Editor (HxHSLMetEd)** from the Hamilton\Bin directory.
2. **Click File > Open and browse for the desired HSL library.**
3. **Click File > View Design History.**

4.2.3 Submethod Library, Method, Layout Design History

1. **Open the Method Editor.**
2. **Click File > Open and browse for the desired file.**
3. **Click File > View Design History from the view of the desired file to validate.** The design history of the file in the view that is active will open.

4.2.4 Liquid Class Design History

1. **Open the CO-RE Liquid Editor.**
2. **Right-click the desired Liquid Class and click View Design History.**

5 Troubleshooting

5.1 Users.cfg is not signed for this system

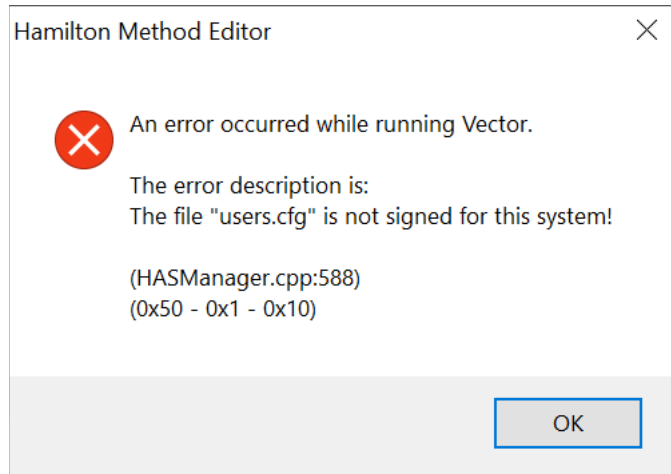


Figure 5–1: Users.cfg error

This error typically occurs when the Users.cfg file is corrupt. This can occur due to the time zone being changed after installing VENUS.

Solution

1. **Close all Hamilton applications.**
2. **Open the Windows Task Manager and end any running HxUserManager.exe processes.**

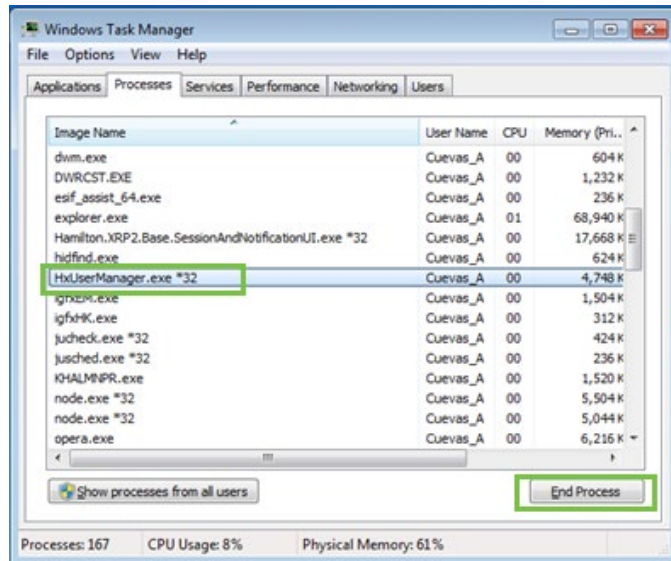


Figure 5–2: Closing HxUserManager.exe

3. **Delete [installation directory]\HAMILTON\Config\Users.cfg.**

If the Authentication System is set to Operating System, the issue should be fixed. If using Hamilton Authentication, continue to the next step.

4. **Disable Function Protection from the registry:**

a. In the Start Menu, search for and open regedit.exe.

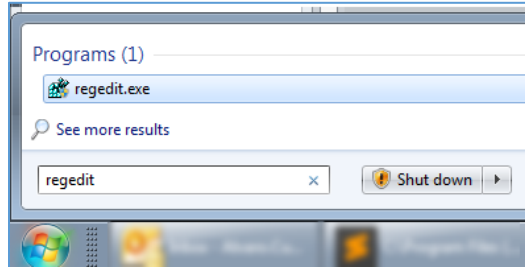


Figure 5-3: Opening the Registry Editor

b. In the Registry Editor, navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Phoenix\Environment.

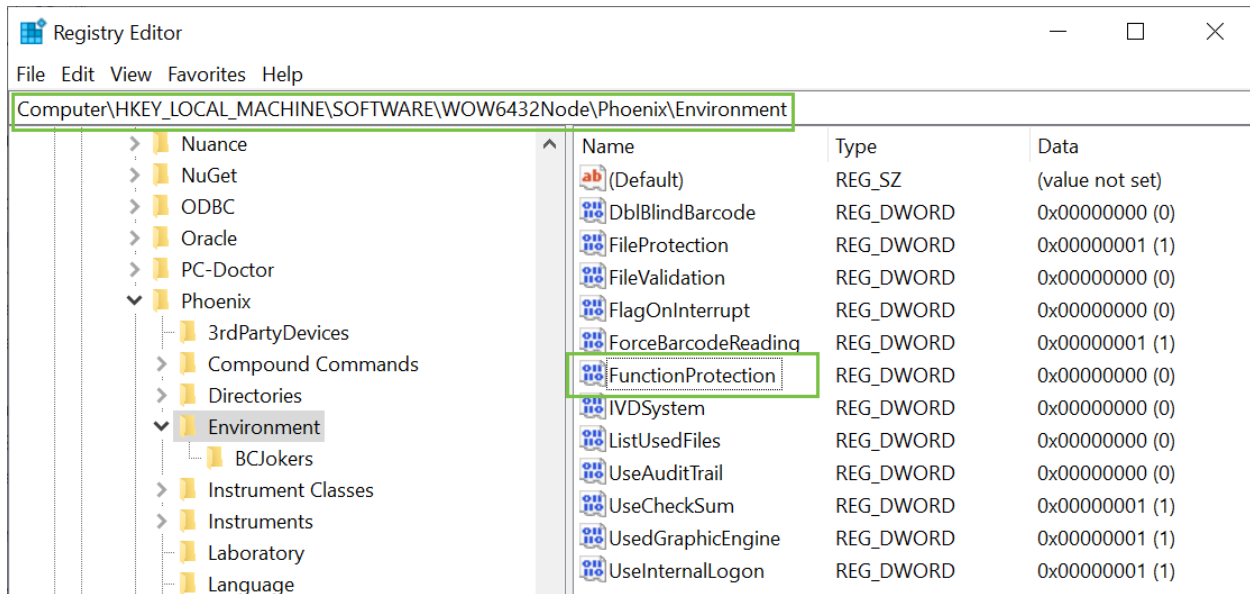


Figure 5-4: Opening Function Protection

c. Double-click FunctionProtection.

d. In the Edit Value dialog, set the “Value data” field to 0 and click OK.

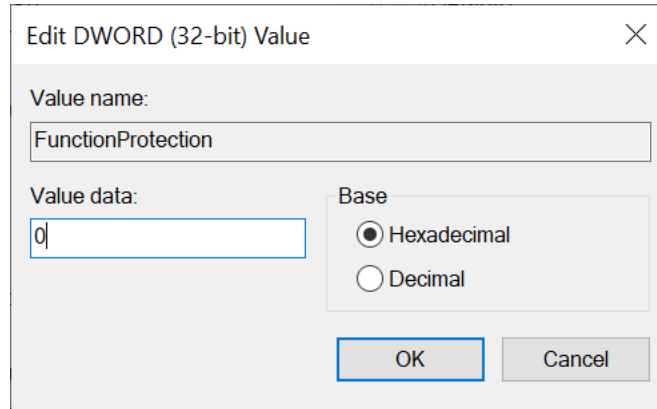


Figure 5–5: Disabling Function Protection through the Registry Editor

5. **Open the System Configuration Editor.** From the Method Editor, click Tools > System Configuration Editor. Close or click Cancel on any login prompts.
6. **Create a new administrator account:**
 - a. Select the Manage Users tab on the left.
 - b. Click the “Create new User” button.

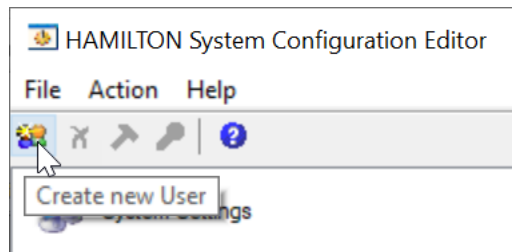


Figure 5–6: Creating a new user

- c. Enter “administrator” for the username and “hamilton” for the password.
- d. Set the user group to Lab Service.
- e. Enable Function Protection if needed under Security Settings.