

Lambda 365

Security Software Guide



Release History

Part Number	Release	Software Version	Publication Date
09931300	D	UV Express Security Software 4.0.1	September 2016

Notices

The information contained in this document is subject to change without notice.

Except as specifically set forth in its terms and conditions of sales, PerkinElmer makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

PerkinElmer shall not be liable for errors contained herein for incidental consequential damaged in connection with furnishing, performance or use of this material.

Copyright Information

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this publication may be reproduced in any form whatsoever or translated into any language without the prior, written permission of PerkinElmer, Inc.

Copyright © 2016 PerkinElmer, Inc.

Trademarks

Registered names, trademarks, etc. used in this document, even when not specifically marked as such, are protected by law.

PerkinElmer is a registered trademark of PerkinElmer, Inc.

Table of Contents

I.	Introduction	1
1.	21 CFR Part 11 Compliance	1
	1.1 Subpart A. General Provisions	1
	1.2 Subpart B. Electronic Records	4
	1.3 Subpart C. Electronic Signatures	8
2.	Security Program.....	11
II.	Overview of Windows Administration	13
1.	Basic Network concepts	13
2.	Network Terms	13
	2.1 Server and Client.....	13
	2.2 Supported configurations.....	14
III.	Network System	15
1.	Pre-Installation.....	15
	1.1 User Account Design.....	16
2.	Software Installation.....	18
	2.1 Installation of Security Sever Software.....	18
	2.2 Installation of UV Express and UV Express Security Software	26
	2.3 Setting IP address	31
	2.4 Folder Permissions.....	33
	2.5 Setting Windows Firewall	42
3.	Operating Security Server	45
	3.1 Set [Account]	50
	3.2 Set [Software List]	52
	3.3 Set [Access Control]	53
	3.4 Set [Signature Meanings]	55
4.	Operating UV Express Software	57
	4.1 Operating UV Express Software.....	57
	4.2 Changing Methods	60
	4.3 Lockout for unattended operation.....	61
	4.4 Deleting Spectra	62
	4.5 Retrieve the deleted spectra.....	62
5.	Event Log	63

IV. Local System	68
1. Pre-Installation.....	68
1.1 User Account Design.....	68
2. Software Installation.....	70
2.1 Installation of Security Sever Software.....	70
2.2 Installation of UV Express and UV Express Security Software	78
2.3 Setting IP address	82
2.4 Folder Permissions.....	83
2.5 Setting Windows Firewall	90
3. Operating Security Server	93
3.1 Set [Account]	98
3.2 Set [Software List]	100
3.3 Set [Access Control]	101
3.4 Set [Signature Meanings]	103
4. Operating UV Express Software	105
4.1 Operating UV Express Software.....	105
4.2 Changing Methods	109
4.3 Lockout for unattended operation.....	110
4.4 Deleting Spectra	110
4.5 Retrieve the deleted spectra.....	111
5. Event Log	112

I. Introduction

This document explains how PerkinElmer's UV Express Security software assists in meeting the regulation of 21 CFR Part 11 for electronic records and electronic signatures.

1. 21 CFR Part 11 Compliance

Title 21 CFR Part 11 of the Code of Federal Regulations includes the Food and Drug Administration's (FDA) guidelines on electronic records and electronic signatures in the United States. 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.

1.1 Subpart A. General Provisions

Sec. 11.1. Scope

- (a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.*
- (b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.*
- (c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as*

required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

- (d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.*
- (e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.*
- (f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.*

Sec. 11.2. Implementation

- (a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.*
- (b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:*
 - 1) The requirements of this part are met; and*
 - 2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of*

transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3. Definitions

1. *The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.*
2. *The following definitions of terms also apply to this part:*
 - 1) *Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).*
 - 2) *Agency means the Food and Drug Administration.*
 - 3) *Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.*
 - 4) *Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*
 - 5) *Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.*
 - 6) *Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.*
 - 7) *Electronic signature means 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.*
 - 8) *Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The acts of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.*

- 9) *Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.*

1.2 Subpart B. Electronic Records

Sec. 11.10. Controls for closed systems

Person who use 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:

- (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

All records are stored in encrypted. Access is controlled by User Name and secret password.

- (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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.*

If the user of UV Express Security software has the authority to save data, they can save it in its own file format. (*.dgd, *.dkdt, *.dbdt, *.dqdt, *.dsrdt, *.dskdt, *.dsqdt, *.dthdt, *.dcdt, *.dpdt, and *.dvdt). This file includes experiment information, signature history and data modification history, etc. Spectrum data can be exported as CSV file, standard ASCII and JCAMP format but a CSV file cannot be imported into UV Express software. The system owner must determine which file format should be maintained and saved.

- (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.**

The data created by UV Express Security software is saved in the designated folders and these data can be read. The system owner must determine how the files will be archived

and backup and have the procedure to ensure that retrieval records can be read.

(d) Limiting system access to authorized individuals.

The only administrator can allocate who is authorized to access the system. It is possible for an administrator to give each user the authority to access the system in Microsoft Windows 7 Professional and Ultimate. To access the system, the user should be given a unique user name and a password.

(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 and shall be available for agency review and copying.

Event log contains the User name, time stamp and all data log when the data file was created, modified or deleted, the new value, the old value, and the type of modification. Change to the data file do not obscure previously saved information. All logs can be review and printed for inspection purposes.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Enforced sequencing is carried out in the application: The system can be set up to enforce the carrying out of certain tasks to ensure correct sequencing. Examples of these are: running standards during an analysis, mandatory data entry and calibrating the instrument.

(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.

Security Server Software manages the authority to use the system and electronic signature for the electronic records.

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

UV Express Security software will only read recognized PerkinElmer file formats. During installation the instrument serial number is recognized. Instrument model and serial number are stored with all data collected.

(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.

It is the responsibility of customer and should be part of the system's procedural compliance. Electronic or hardcopy documentation is provided.

(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.

It is the responsibility of customer and should be part of the system's procedural compliance.

(k) Use of appropriate controls over systems documentation including:

- 1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*
- 2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*

It is the customer's responsibility to maintain appropriate controls of the installed system and this should be part of the system's procedural compliance.

Sec. 11.30. Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in

11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

The UV Express Security software implementation requires the use of a closed system as we do not employ data encryption on our data files with this software. For Windows 7 Professional and Ultimate, security is embedded in the UV Express software structure and set up through the Windows 7 security feature. The Windows log-in and password, in conjunction with the password reverification required when a user starts UV Express, provide a way to control access to the UV Express software and a spectrophotometer. By following the guidelines in this document, you can achieve compliance with 21 CFR Part 11 as it pertains to a closed system.

Although data encryption is not used, the system administrator may choose to store the data in a secure folder such that only authorized users may access data according to their privileges. These privileges must be controlled by a unique user name and password combination.

If compliance is desired in an open system, those responsible for maintaining system records must take adequate measures to ensure that UV Express complies.

Sec. 11.50. Signature manifestations

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- 1) The printed name of the signer;*
- 2) The date and time when the signature was executed;*
- 3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*

UV Express security software implement as follows:

- 1) The printed name is the User Name.
- 2) The data and time are recorded. PerkinElmer users the PC's log data format and includes time zone information.
- 3) The meaning of each signature event is recorded and stored in the history record with

the User Name of the signer E-signatures are configurable. Signature is selected by the security server software.

(b) The items identified in paragraphs a1, b1, and c1 of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

The history record for the method or results stores this information. This record can be viewed on screen and printed.

Sec. 11.70. Signature/record linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

The digital signature is stored in the same data file or report that is signed. Because the signature is stored in the same file as the electronic record, all digital signatures produced by UV Express are directly linked to the electronic record. A check of an electronic record can verify whether the signature is valid. An invalid signature could be caused by a record that was never signed or a record that was modified after it was signed.

If an invalid signature was attached to an electronic record, or if the record was tampered with, simply checking the signature on the electronic file will reveal the problem.

1.3 Subpart C. Electronic Signatures

Sec. 11.100. General requirements

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

No two users can have the same User Name and secret password combination.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

It is the responsibility of the customer to include this as part of the system's procedural compliance.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

1) The certification shall be submitted in paper form and signed with a traditional signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

2) Persons using electronic signature shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

It is the responsibility of the customer to include as part of the system's procedural compliance.

Sec. 11.200. Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

1) Employ at least two distinct identification components such as an identification code and password.

i. When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

ii. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

2) Be used only by their genuine owners;

3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Digital signature used by UV Express is based on the user's ID and Password based on non-biometrics. This signature is encrypted in the data file and cannot be opened in any other application software.

Sec. 11.300. Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

No two users can have the same User Name and secret password combination. When a user leaves the company the system will not allow that particular User Name to be reused by anyone else. This should be made part of the system's procedural compliance.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

UV Express has the facility to allow password ageing. New passwords are checked according to the administrator settings for password ageing. The password aging intervals must be defined by the security server software an administrator and should be part of the system's procedural compliance.

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

The system allows an administrator to disable access via the compromised User Name. This should be part of the system's procedural compliance. The system administrator can issue temporary and permanent replacement access

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Regular review of the log is customer/client responsibility, and should be part of the system's procedural compliance.

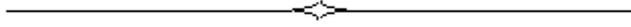
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Devices such as tokens or cards are not used by UV Express.

2. Security Program

UV Express Security Software is provided to run in Network PC and Local environment. This runs as service under Windows and enforces the security policies defined with the Security Server Program. UV Express Security automatically tracks changes to data file. As mathematical processing or renaming occurs, the changes are saved in the data history information. It also handles the data history, method history and electronic signatures. The data used in UV Express Security software is binary code based and cannot be opened in any other application software.

- i. Security Server software provides the functions for setting up the privilege and access control of application software, measurement method and etc. The audit trail function is included in the Event Viewer and each audit trail can be viewed.
- ii. UV Express software is the program to run the Lambda 365 meeting the regulation of 21 CFR Part 11 for electronic records and electronic signatures.



II. Overview of Windows Administration

1. Basic Network concepts

PerkinElmer Security Server software is designed to run in a networked or local environment. The security functionality of Security Server is fundamentally linked to the security features of your Windows network operation system. Understanding of some of the concepts and terms may give you more confidence in using the Security Server software.

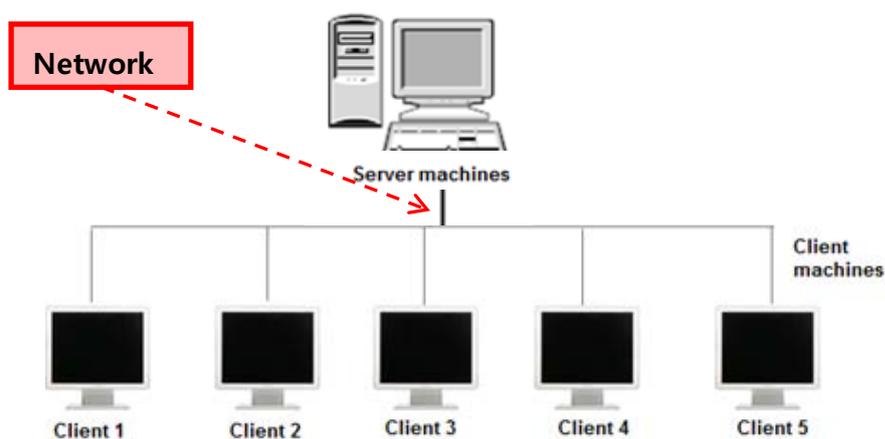
2. Network Terms

2.1 Server and Client

A network server is a computer or device that provides information or services to other computers on a network.

A client is the requesting program or user in a client-server relationship.

Client-server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request.



2.2 Supported configurations

You can use Security Server to set and enforce security policies in network:

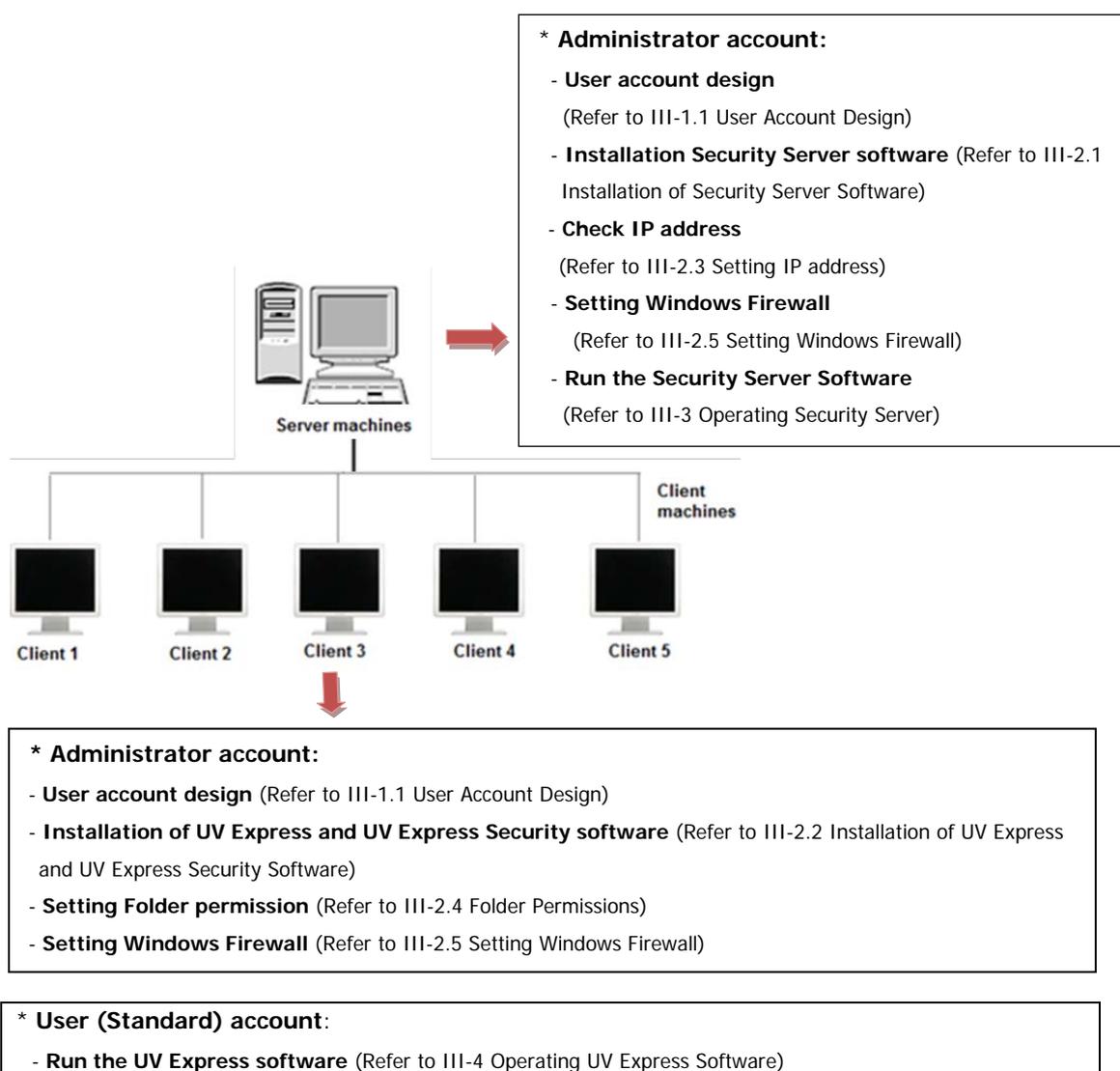
In the Network System, Security Server is installed on Windows 7 that is a member of the domain. The client application is installed on multiple workstations that are members of the domain. The client workstations run Windows 7 Professional and Ultimate.

In the stand-alone configuration (Local System), Security Server is installed and run along with the client application on a single non-networked computer that acts as both client and server. This computer runs Windows 7 Professional and Ultimate. Stand-alone configurations are intended for small laboratories with no network facilities.

III. Network System

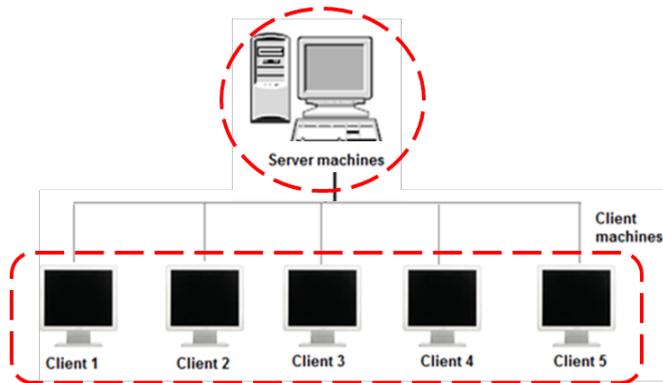
1. Pre-Installation

Before installing the UV Express Application, the local administrator needs to designate users or groups and assign their authority of access. Users and Groups are designated in the Control Panel of the Windows Operating System. You need to set up user accounts in each computer in the workgroup, not just on a server. Each user must have the same user name and password on each computer in the workgroup.



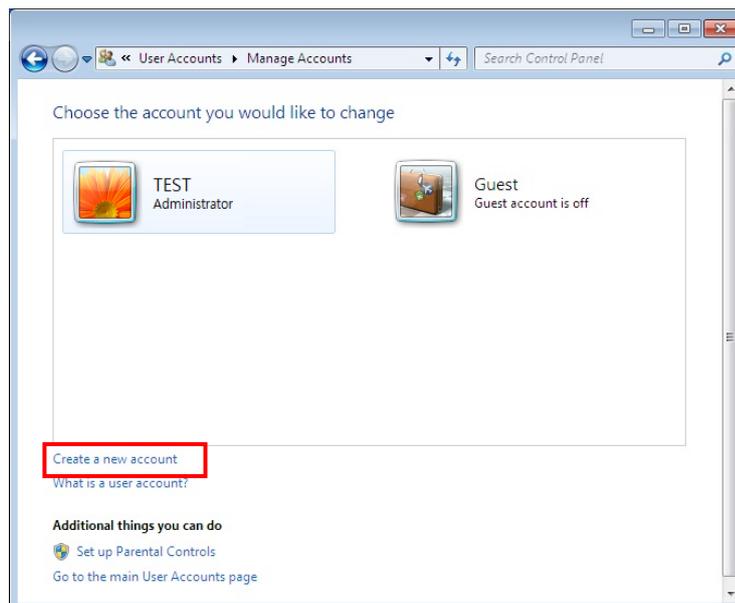
1.1 User Account Design

NOTE: *User account design should be same name on the Administrator account both the Server and the Client computer.*

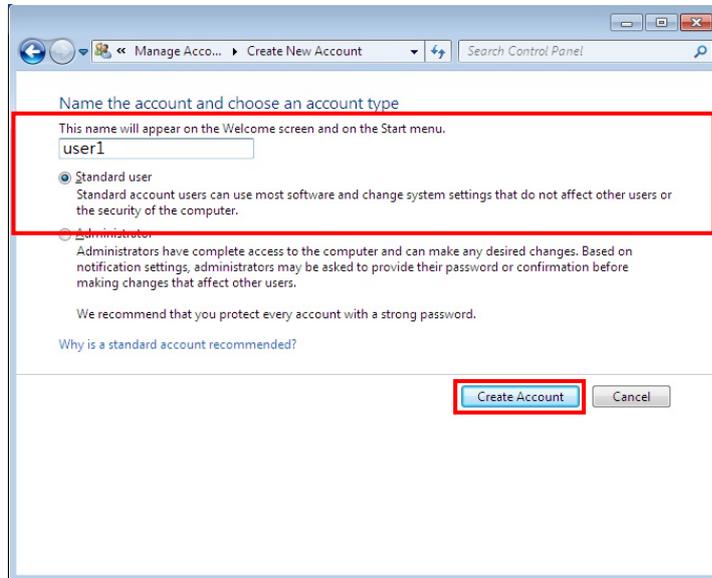


1.1.1 Create the User account(s) in Windows 7

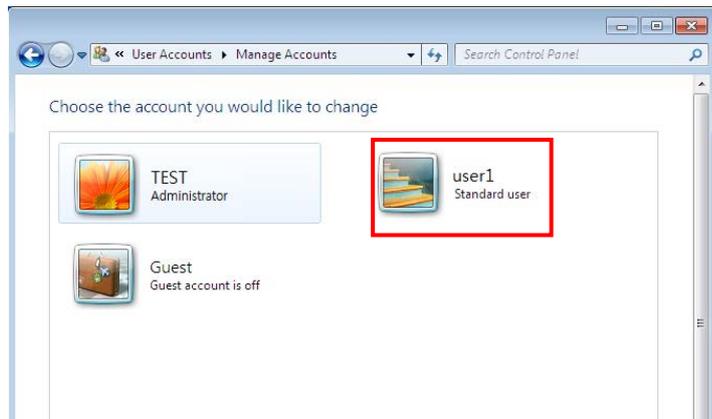
1. Log on to the computer as an administrator of server computer.
2. Select **Control Panel > User Accounts** from the **Start** menu in the Windows operating System.
3. Click **Manage another account > Create a new account**.



4. Enter the Name (ex. user1) of the new account, select **Standard user** and click **Create Account**.



5. Verify the new account was created correctly.

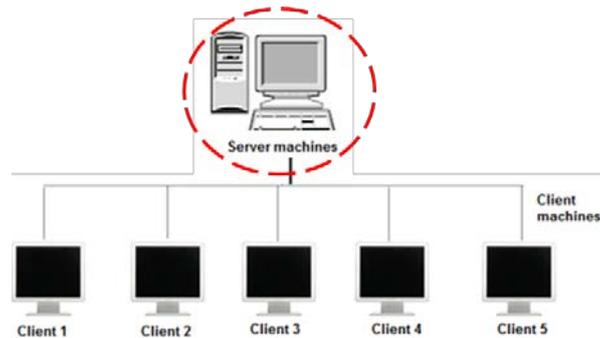


6. Additional accounts can be created in the same way as above.
7. The procedure for creating user account is complete.
8. Reboot and log on to the computer as an administrator.
9. Log on the computer as an administrator of client computer. Create the user account same as sever computer following procedure from #2 to #8.

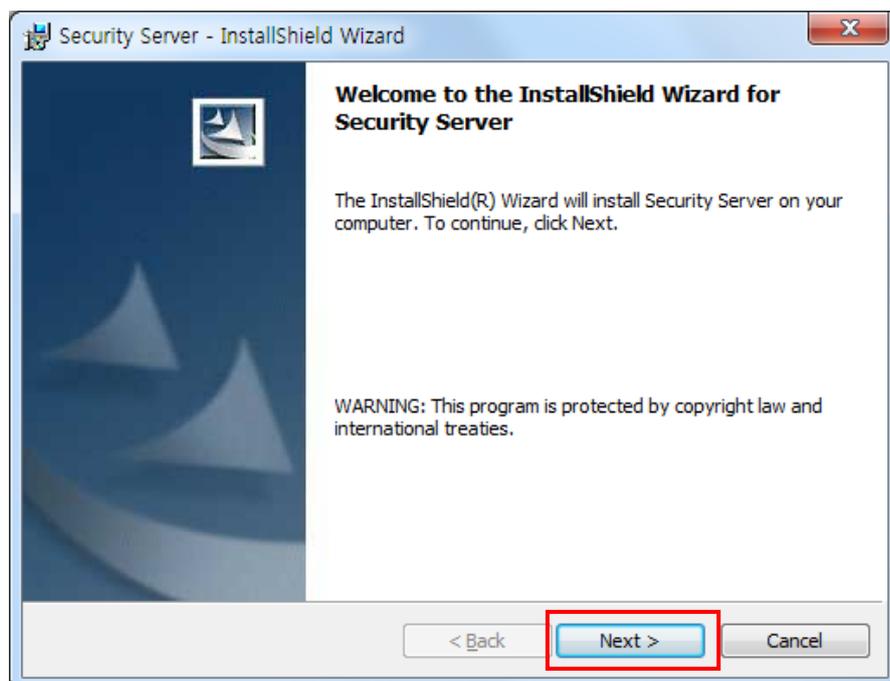
2. Software Installation

2.1 Installation of Security Sever Software

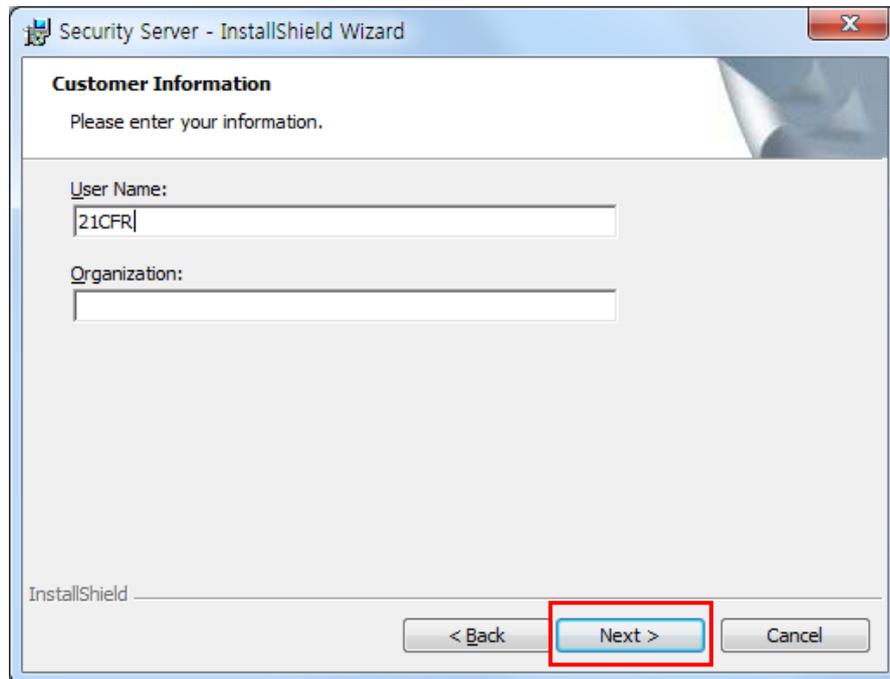
NOTE: *Security Server Software should be installed on the Server computer.*



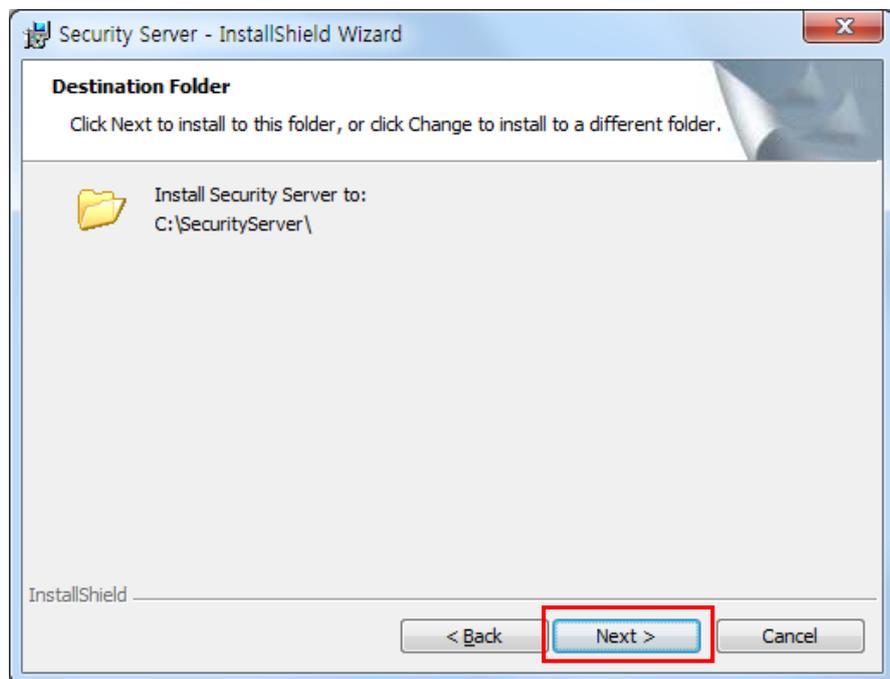
1. Log on to the computer as an Administrator account of the Server computer.
2. Input the **Security Server software** CD into the CD drive. Security Server Software is installed automatically. The default installation folder is "C:\ SecurityServer".
3. If the automatic setup window is not shown, click **Setup.exe** in the CD.
4. Security Server InstallShield® Wizard starts. Click **Next**.



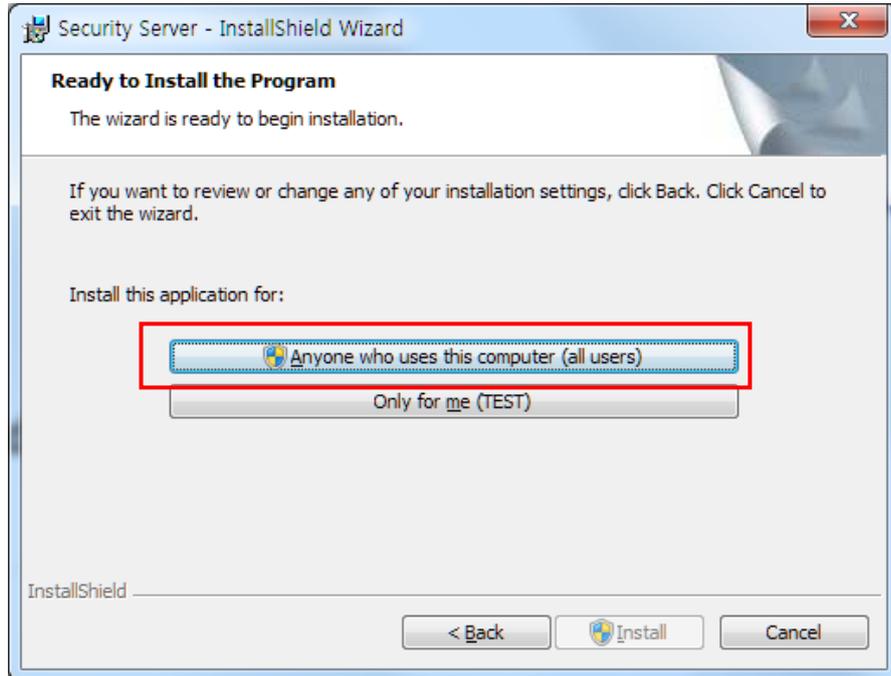
5. Enter your information and Click **Next**.



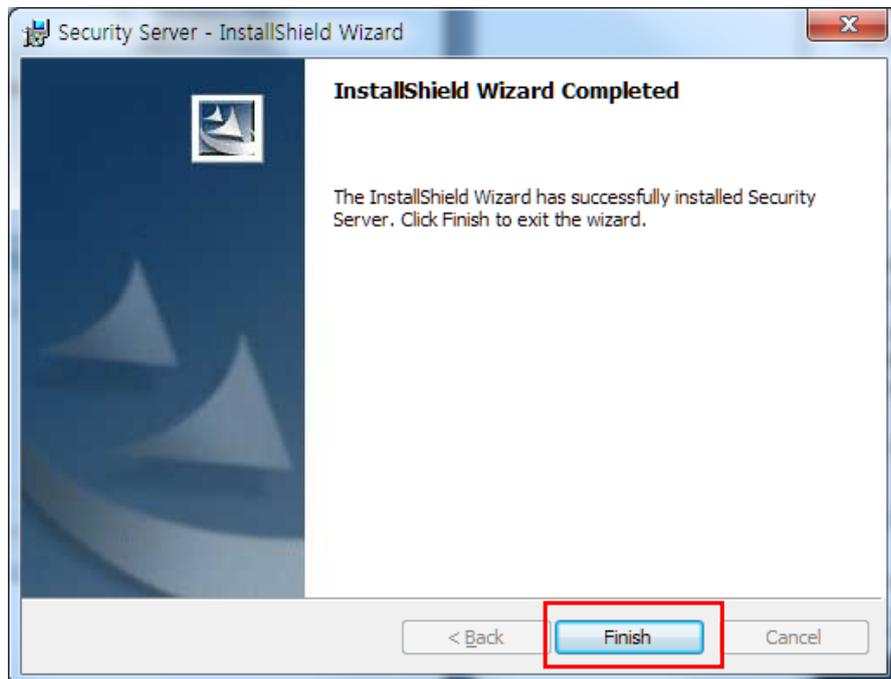
6. Click **Next**.



7. Click **Anyone who uses this computer (all users)**.



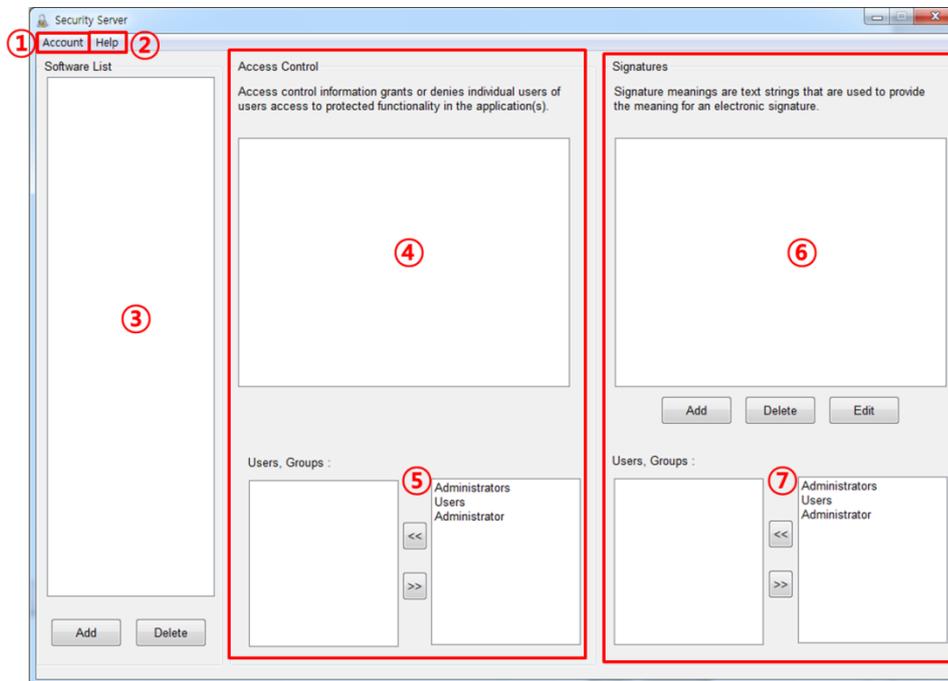
8. After the setup is complete successfully, click **Finish**.



9. After the Security Server software installation is complete, the icon  will be created on the Desktop.

2.1.1 Security Server Software Interface

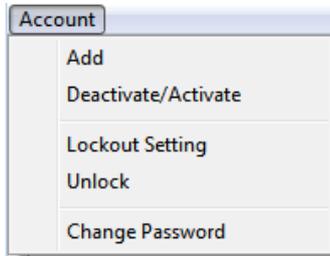
Describes the unique display features of the security software.



- ① Account: Control to set / change user account and password.
- ② Help: Display the security software Guide and version of Security Server.
- ③ Software List: Register the software to be used (UV Express).
- ④ Access Control: Display the software function of the selected software in the Software List section. (File, Edit, Math, Measure, View, Math, etc.)
- ⑤ Users, Groups: Select user account(s) to be given the access permission to each function in the Access control section.
- ⑥ Signature: Set electronic signature. (Default-Authorship, Responsibility, Approval, Review, etc.)
- ⑦ Users Group: Select user account(s) who will have the authority to apply each signature.

2.1.1.1 Account

- The Account menu includes commands to perform account functions as shown in the following table.

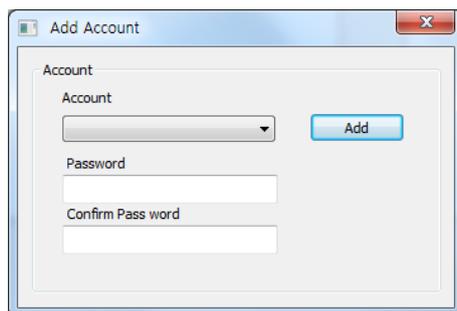


Command	Function
Add	Add new user account
Deactivate/Activate	Deactivate or activate the user account
Lockout Setting	Set the lockout function
Unlock	Unlock the user account and set new password
Change Password	Change the password of user account

Add

- Use the Add command to add a new user account.
- Procedure

1. To add a new user account, select user account and enter a password. Click **Add**.



NOTE: Password must be of minimum 6 characters and include at least one letter and a number each.

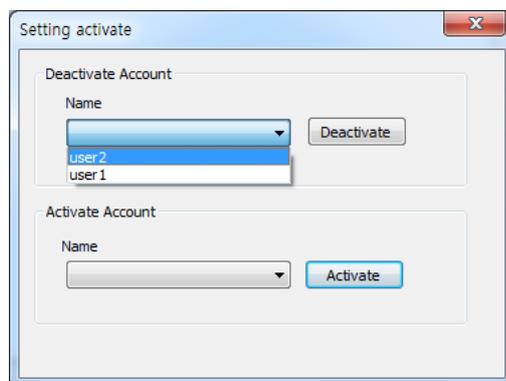
NOTE: When the new user logs on for the first time they will be forced to change their password.

Deactivate/Activate

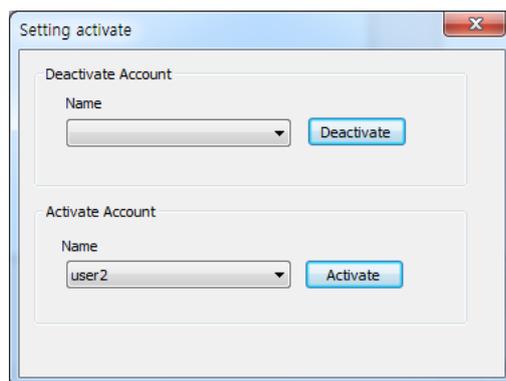
- Use the Deactivate command to deactivate and prevent an activated user account from accessing the UV Express software.
- Use the Activate command to activate and allow a deactivated user account to access the UV Express software.

■ Procedure

1. To deactivate a registered user account, click the “Name” drop-down list in the “Deactivate account” section, and then the currently activated accounts are listed.
2. Select the account to be deactivated and then click **Deactivate**.

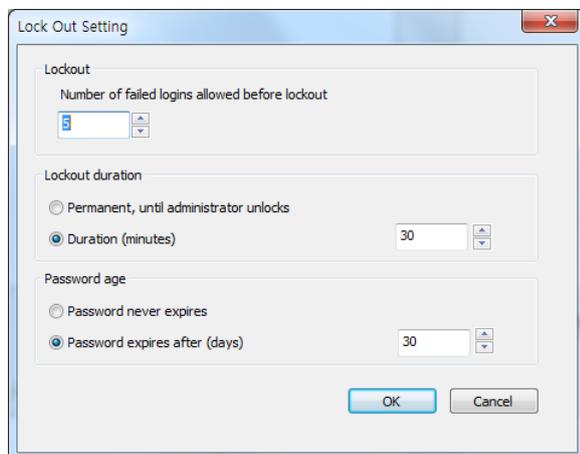


3. To activate a registered user account out of deactivated accounts, click the “Name” drop down list in the “activate account” section and the currently deactivated accounts are listed.
4. Select the deactivated account to be activated and then click **Activate**.



Lockout Setting

- Use the Lock out setting command to set the number of failed logins, lockout duration and password age.



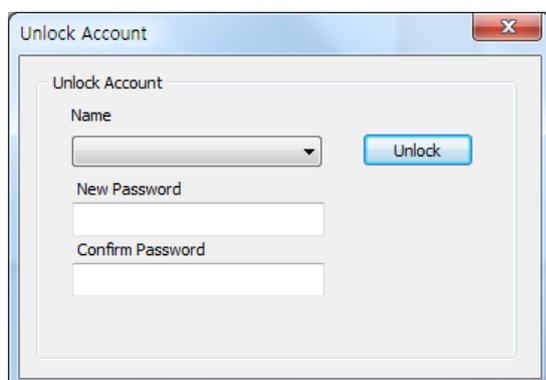
- Lockout: In executing the UV Express software or signing the measured file, enter the limit number of failed logins. Once locked out, execute the Unlock function and set a new password.
- Lockout duration: Set the time (minutes) when the UV Express software is closed in case that there is no action after it is executed.
- Password age: Set the password expiration (days). Alarm message is displayed from 3 days before the password is expired.

Unlock Account

- Use the Unlock Account command to unlock the user account when user failed logins over setting lockout number and set the new password.

- Procedure

1. To unlock user account, select user account and enter the new password and click **unlock**.

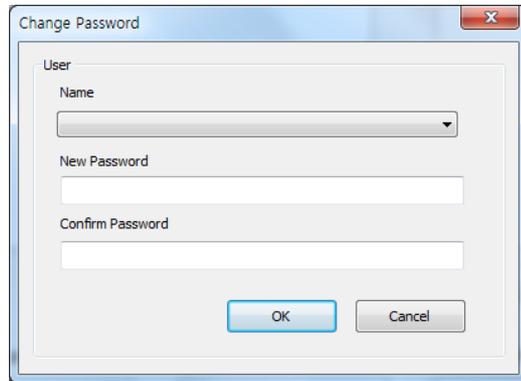


Change Password

- Use the Change Password command to change the user account password.

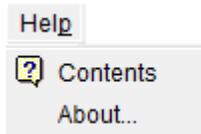
- Procedure

1. To change password, select user account and enter the new password and click **OK**.



2.1.1.2 Help

- The Help menu contains the Help contents for Security Server Software.



Command	Function
Contents	Open the Security Software Guide as PDF file
About...	Display the version of Security Server Software

Contents

- Contents links to external document of the Security Software Guide.

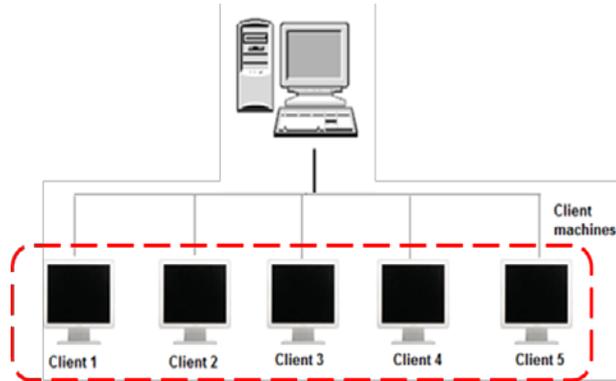
About

- About Security Server contains information on the version of the software.

2.2 Installation of UV Express and UV Express Security Software

NOTE: *UV Express and UV Express Security software should be installed on a client computer.*

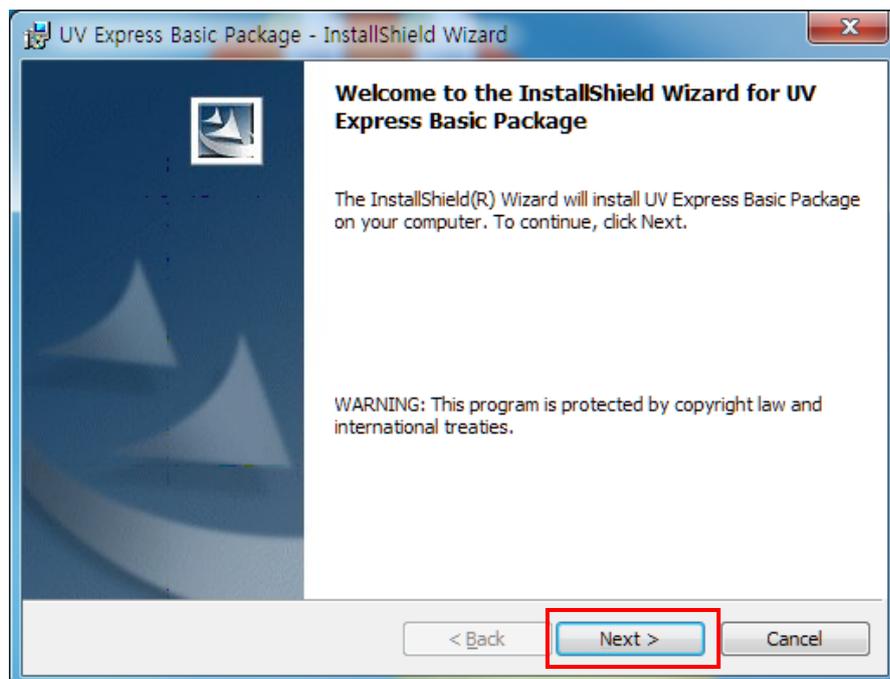
1. Log on as an Administrator account on a Client computer.



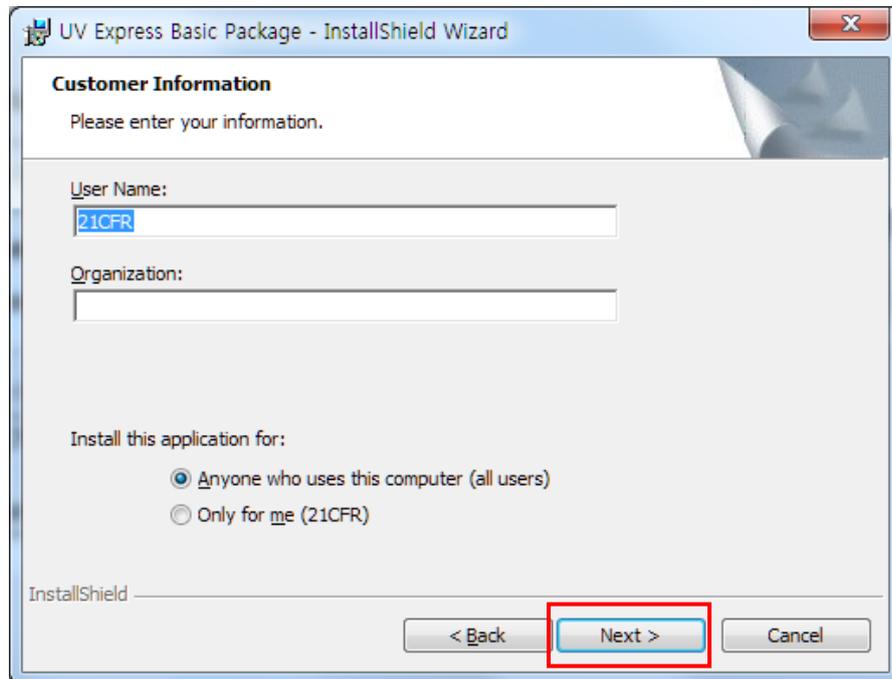
2. Input the **UV Express software** CD into the CD drive. UV Express software is installed automatically. The default installation folder is "C:\UV Express".

NOTE: *If UV Express Software has already been installed, please skip the procedures #2-9 and then, UV Express Security software only needs to be installed on a client computer.*

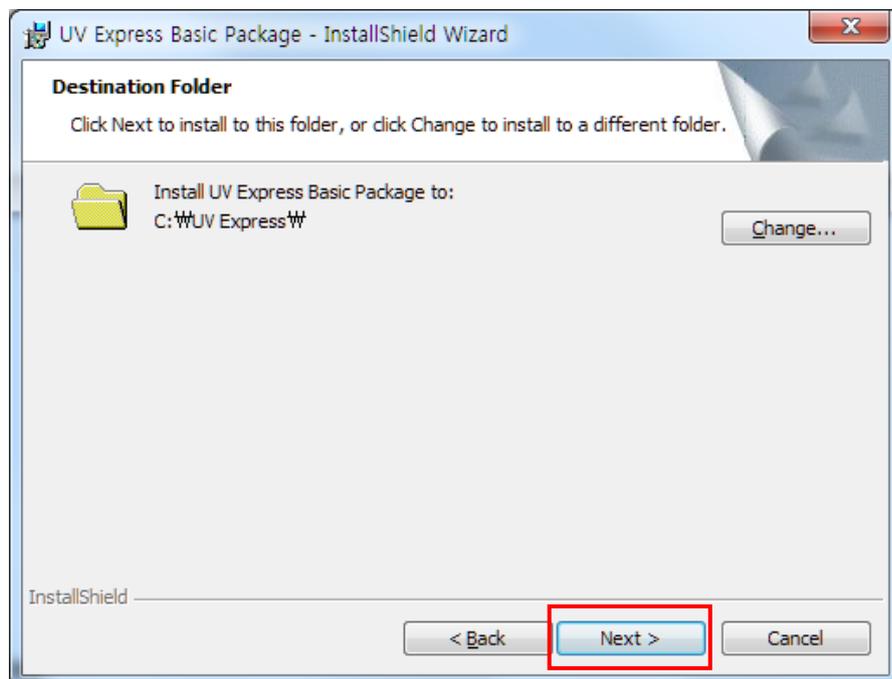
3. If the automatic setup window is not shown, click **Setup.exe** in the CD.
4. UV Express InstallShield® Wizard starts. Click **Next**.



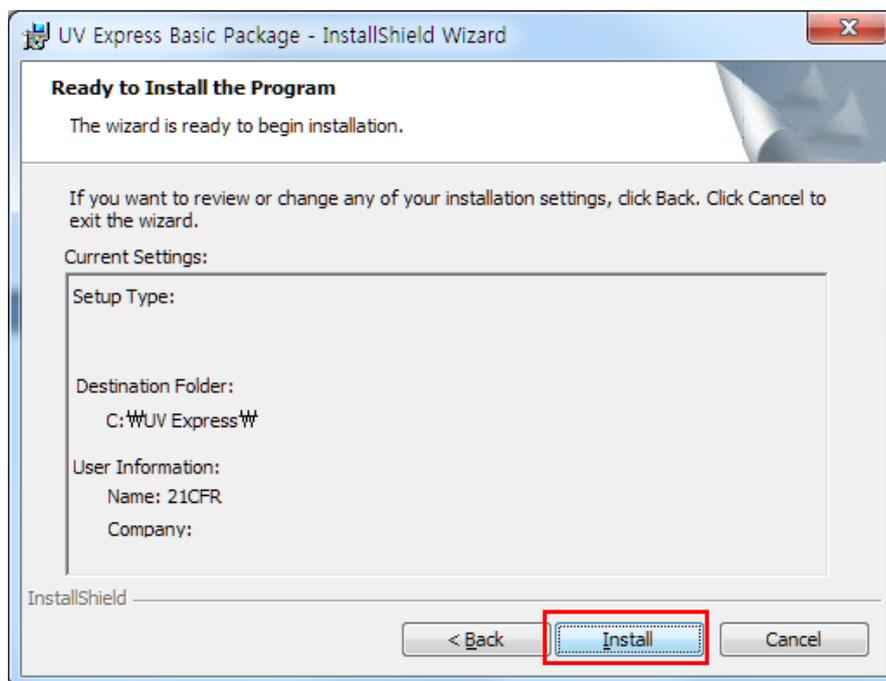
5. Enter your information and click **Next**.



6. Click **Next**.

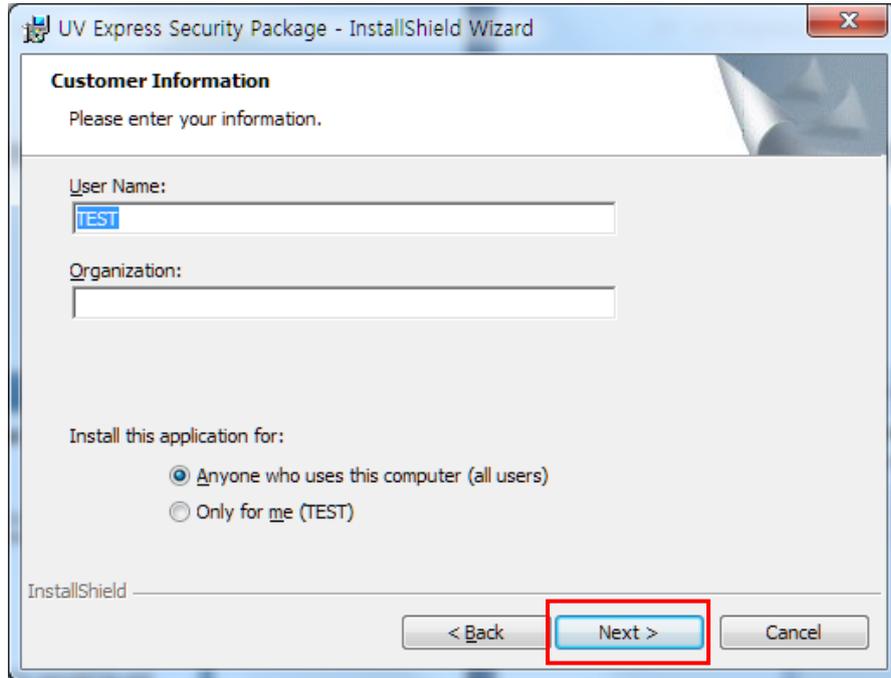


7. Click **Install**.

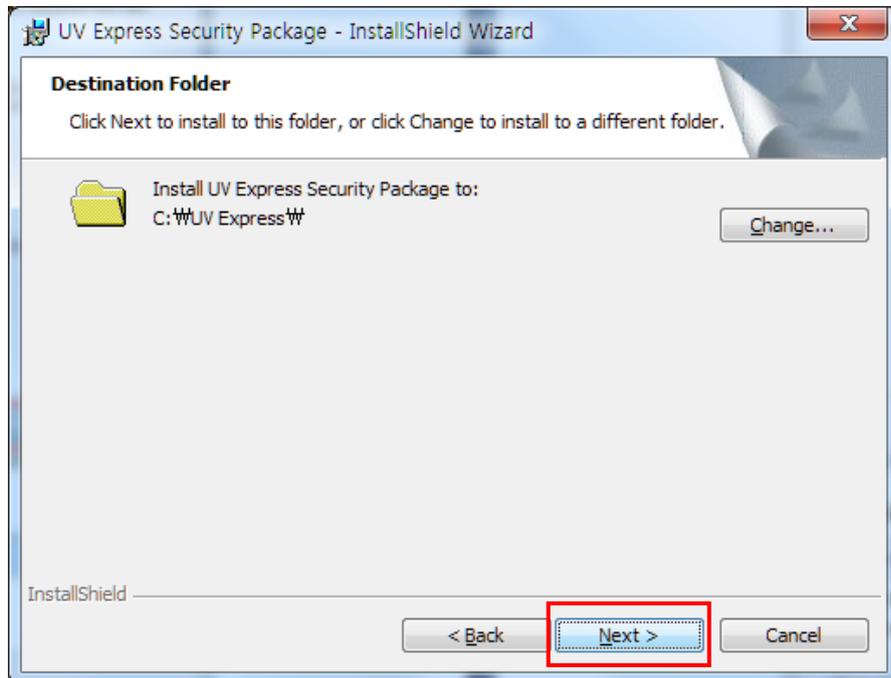


8. After the setup is complete successfully, click **Finish**.
9. After the UV Express Software installation is complete, the UV Express folder  will be created on the Desktop.
10. Input the **Security software** CD into the CD drive. UV Express Security software is installed automatically. The default installation folder is "C:\UV Express".
11. If the automatic setup window is not shown, click **Setup.exe** in the CD.
12. UV Express Security InstallShield® Wizard starts. Click **Next**.

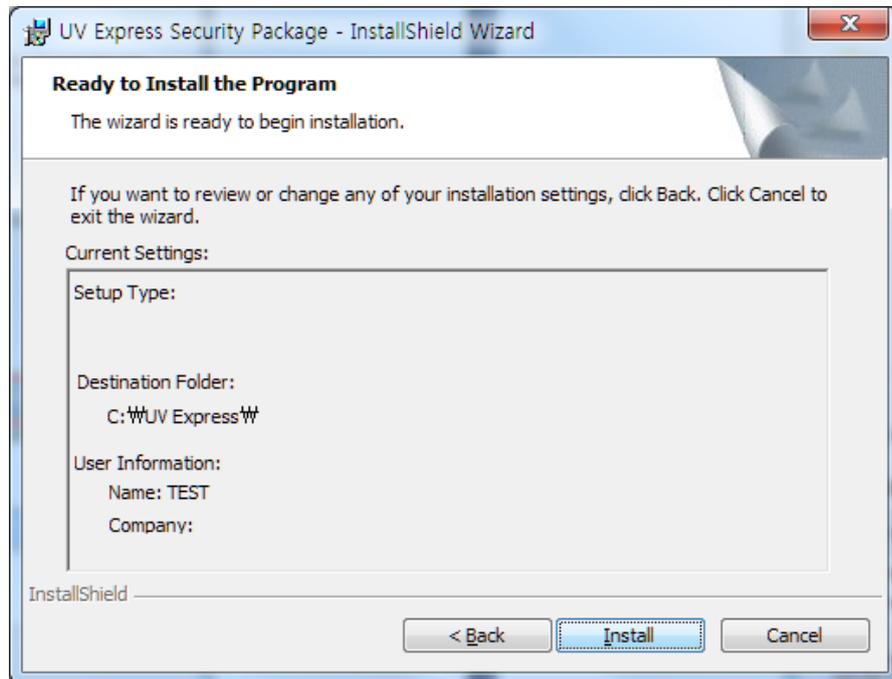
13. Enter your information and click **Next**.



14. Click **Next**.



15. Click **Install**.



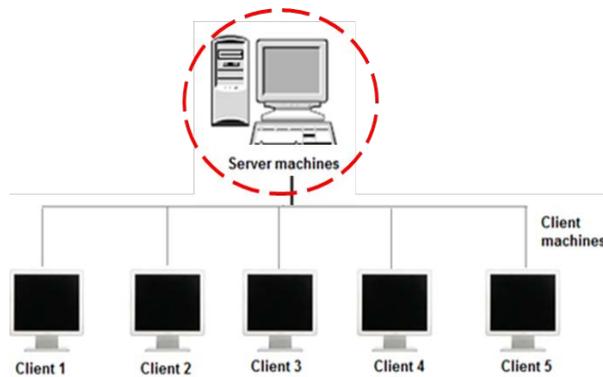
16. After the setup is complete successfully, click **Finish**.

2.3 Setting IP address

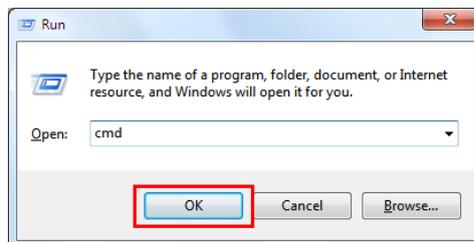
The IP Address of the Server computer should be addressed in the Client computer for networking as follows.

2.3.1 Check the Server computer IP address

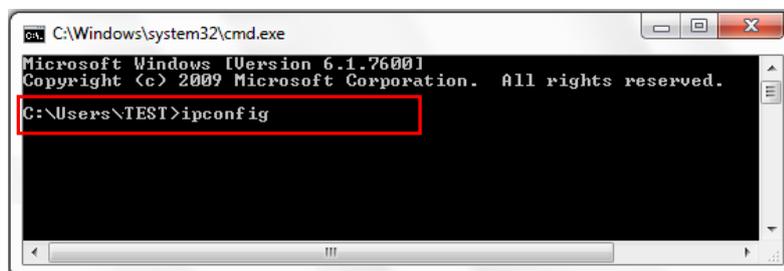
1. Log on to the computer as an Administrator account of the Server computer.



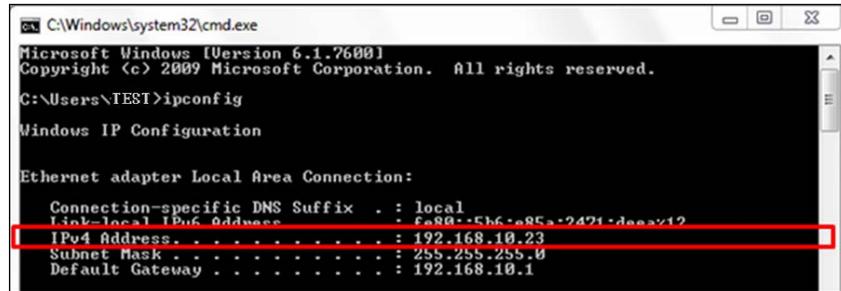
2. Press and hold the "Windows" key and then press the R key to open Run, and after writing "cmd", click **OK**.



3. Type "ipconfig" and press the **Enter** key.



4. Check the Server computer's IP address: ex. 192.168.10.23.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\TEST>ipconfig

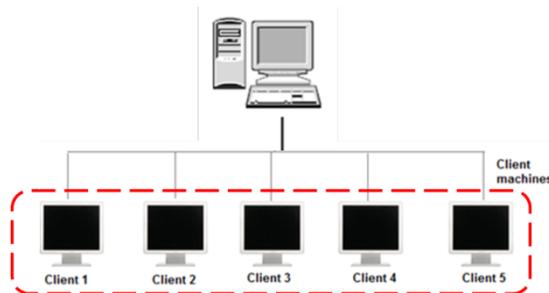
Windows IP Configuration

Ethernet adapter Local Area Connection:

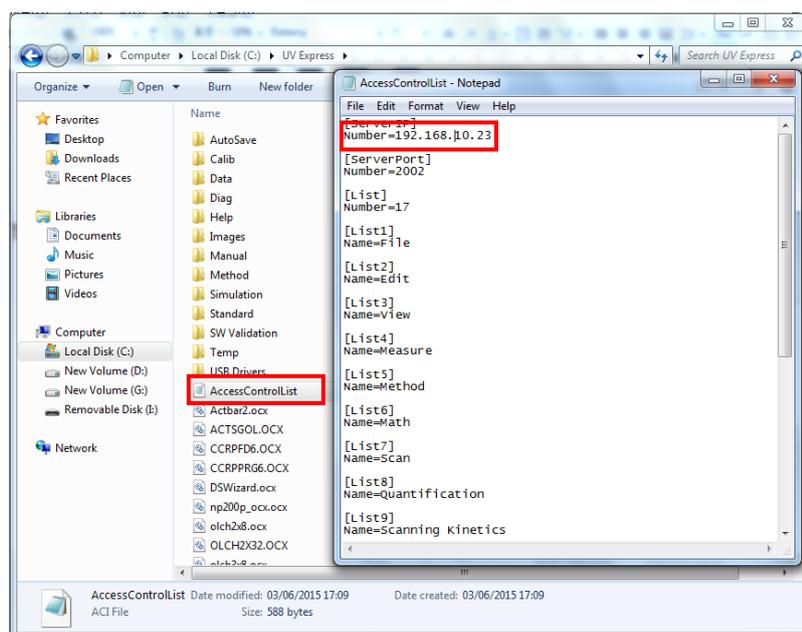
    Connection-specific DNS Suffix  . : local
    Link-local IPv6 Address . . . . . : fe80::5b6-e85a-2421-d0eay12
    IPv4 Address. . . . . : 192.168.10.23
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
```

2.3.2 Input the Server IP address information in the Client computer

1. Log on as an Administrator account on a Client computer.



2. Open the "C:\\" directory, and click the "UV Express" folder. Open **AccessControlList.aci** file on the notepad and type the above Server IP address instead of the currently set IP address. Click **File** and Save the modified server IP address.



2.4 Folder Permissions

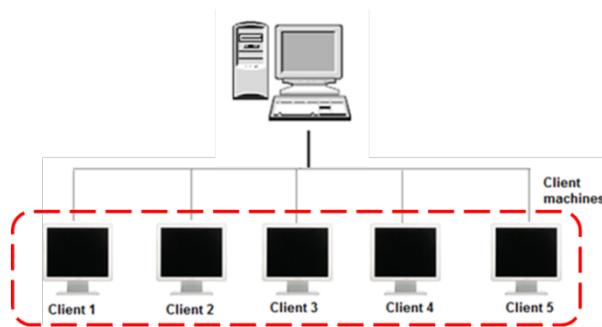
The Administrator account is already present on the PC. This gives the administrator full access to the whole system, including the ability to delete and rename files, and run any application, and change user and file/folder permissions.

In order for data files to be protected, data saved in this protected folder can only be accessed by authorized users. This all permissions of file and folder follow the Windows system's procedural compliance.

2.4.1 Setting the "Write" permission to the "UV Express" folder

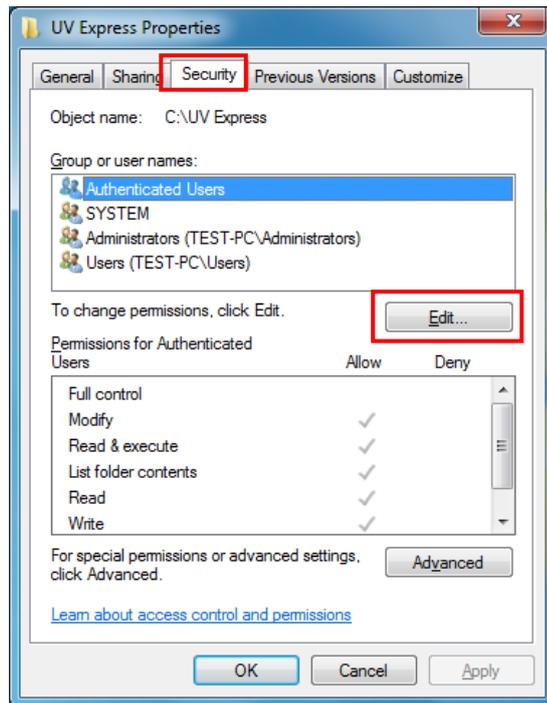
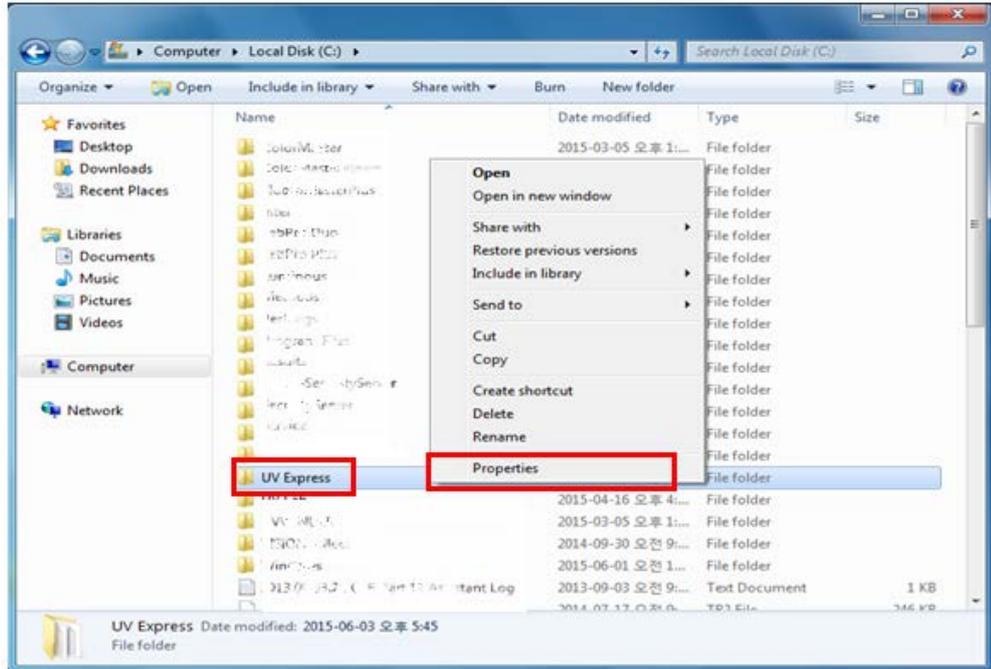
Note: *User(s) should be granted the "Write" permission to run the UV Express security software. To set up write access permission is carried out only on the Client computer's Administrator account.*

1. Log on to a Client computer as an Administrator account.

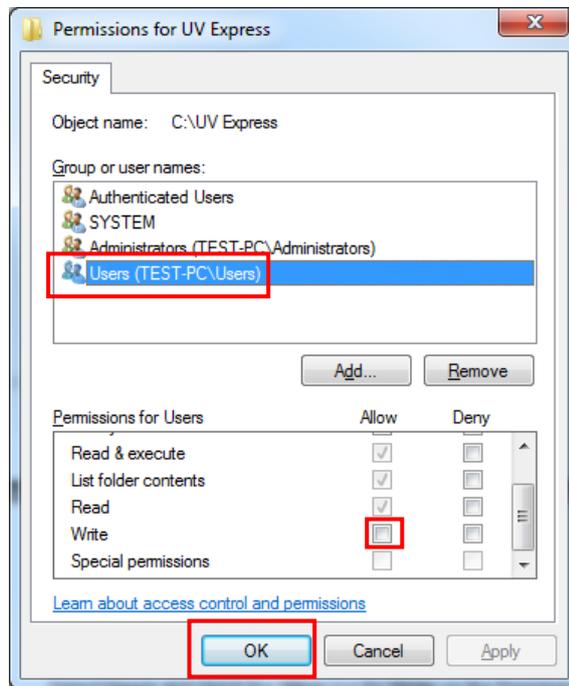


2. Open the "C:\\" directory, and right-click the "**UV Express**" folder, and then click **Properties**.

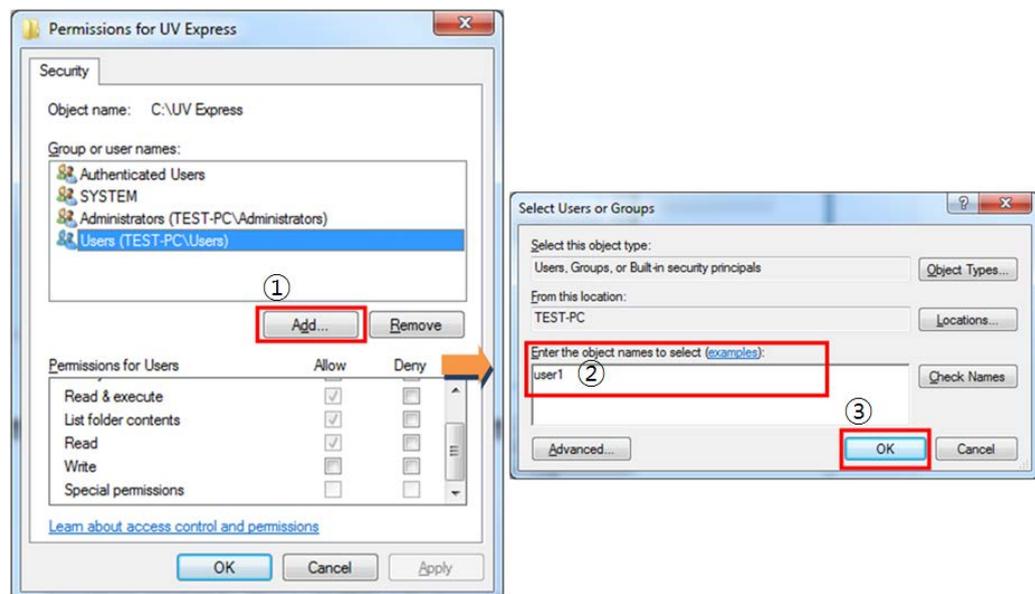
3. Click **"Security"** tab and click **Edit**.



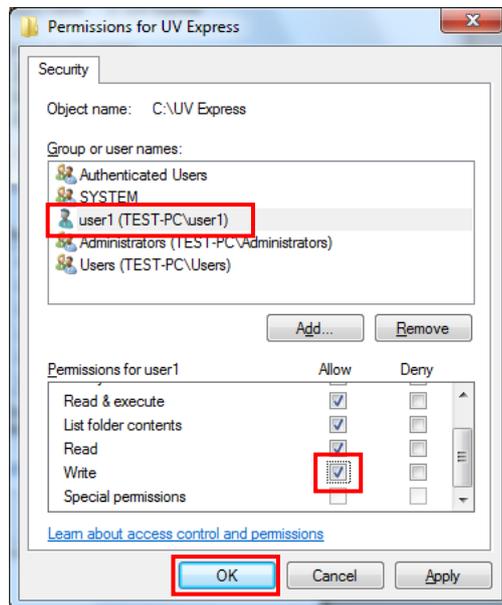
4. Select **Users** and check the **Allow** box for **Write** on the Permissions for Users window and click **OK**.



5. To allow a specific account (e.g. user 1) the write permission, not all **Users**, set as below.



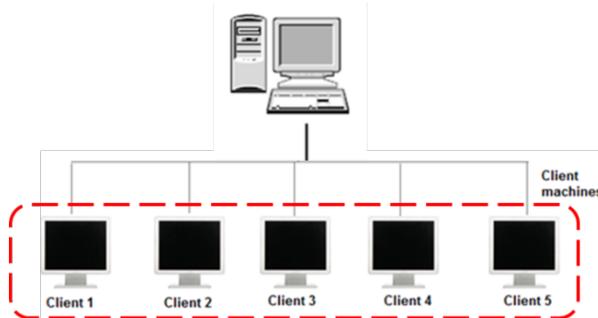
6. Select **user1** and check the **Allow** box for **Write** on the Permissions for User1 window and click **OK**.



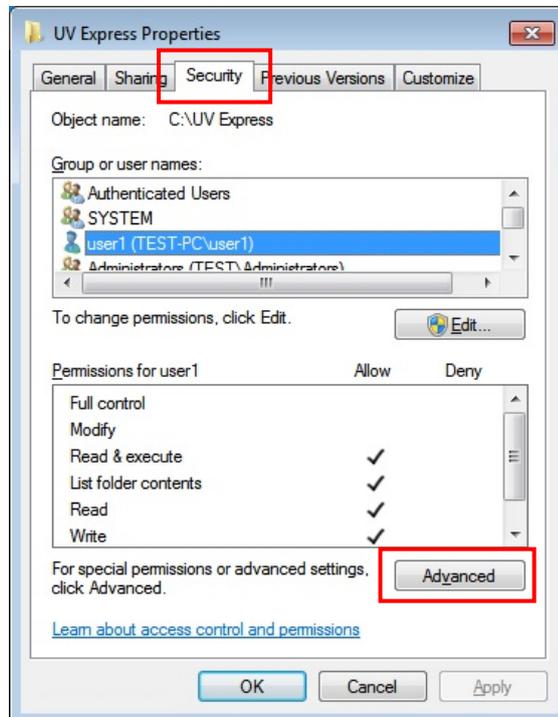
2.4.2 Setting the "Delete and Change" prevention to the "UV Express" folder

NOTE: To prevent user from deleting or changing the UV Express folder (C:\UV Express) and its subfolders and files, the delete permission should be set as **Deny**. It can be set with Administrator's account in the Client computer.

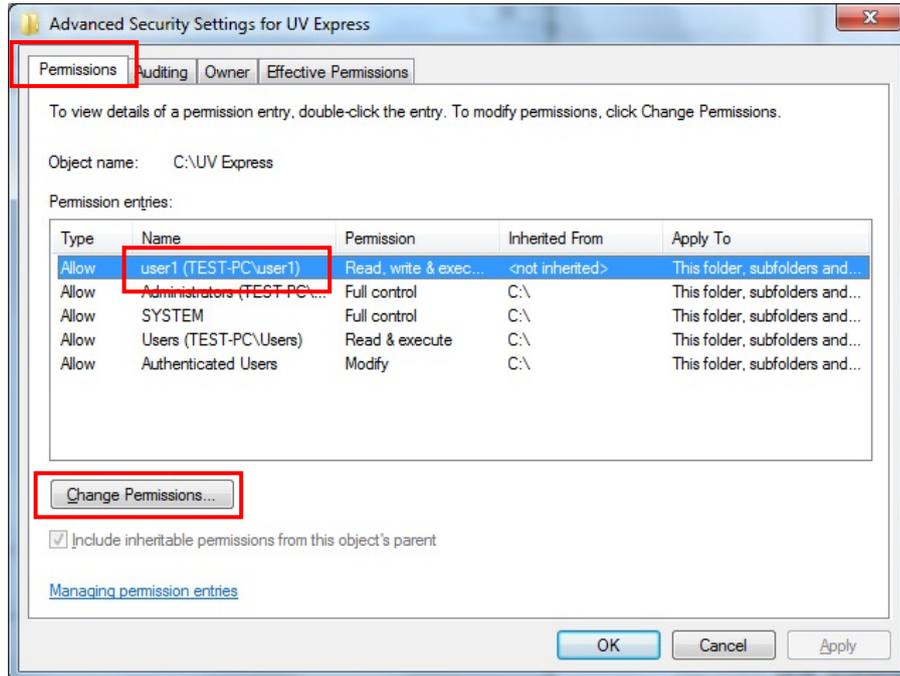
1. Log on a Client computer as an Administrator account.



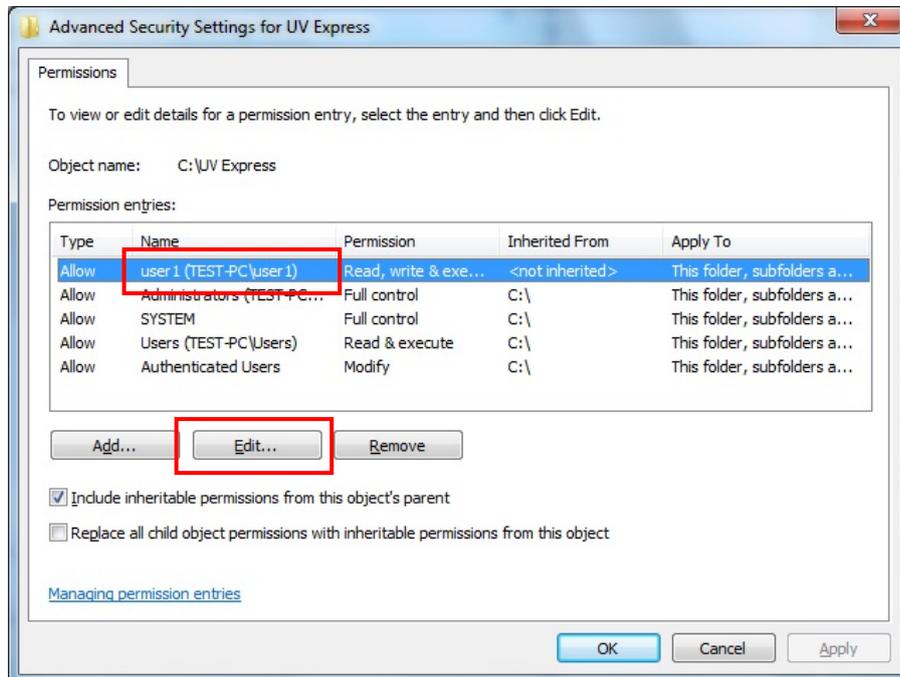
2. Open the "C:\\" directory, and right-click the "UV Express" folder, and then click **Properties**.
3. Select **Security** tab in the Properties window and click **Advanced**.



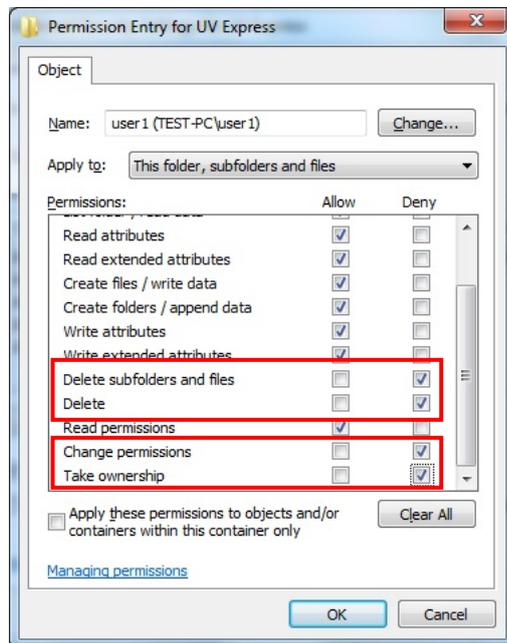
4. Select the **permissions** tab and “**user1**” and click **Change Permissions**.



5. Select “**user1**” in the permissions window and click **Edit**.



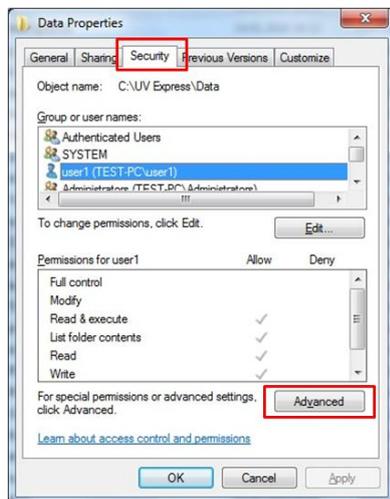
- Under permissions for **Delete subfolders and files**, **Delete**, **Change permissions** and **Take ownership**, select or check **Deny** and click **OK**.



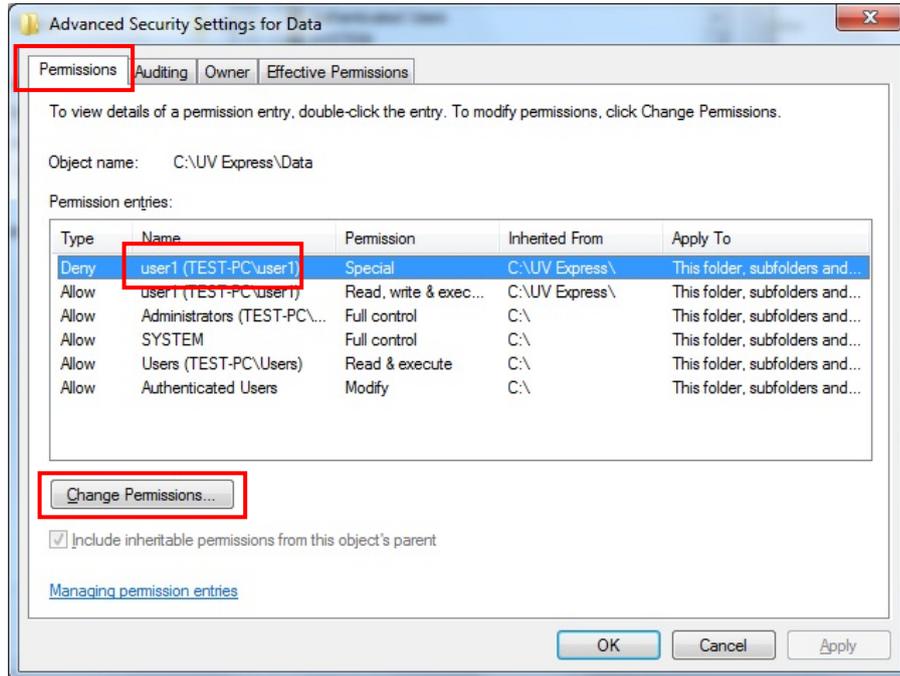
2.4.3 Setting the "Overwrite" prevention to the "Data" folder

NOTE: To prevent user from overwriting data into the Data folder (C:\UV Express\Data) , the **Create Folders / append data** permission should be set as **Deny**. It can be set with Administrator's account in the Client computer.

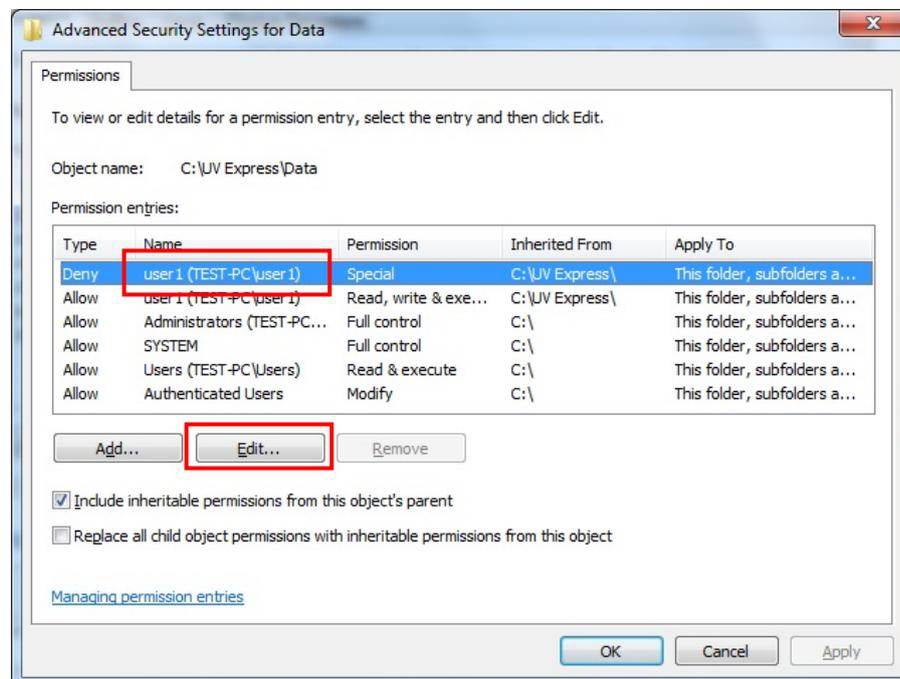
- With the Administrator's account logged on, open the "C:\ UV Express" directory, and right-click on the "**Data**" folder and then click **Properties**.
- Select **Security** tab in the properties window and click **Advanced**.



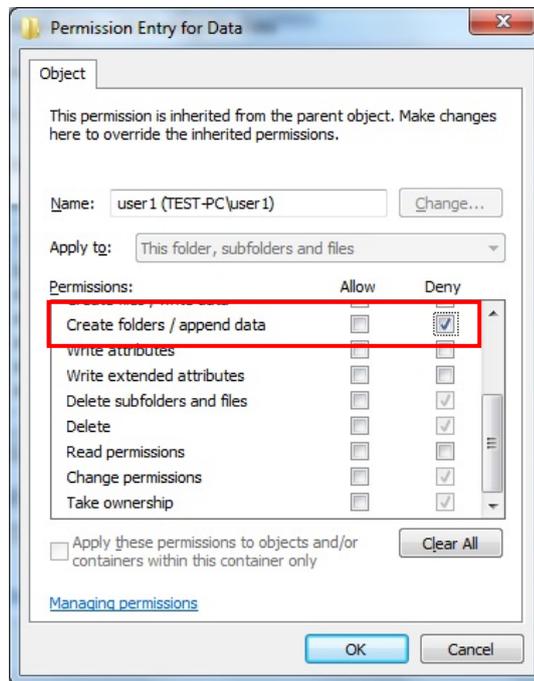
3. Select the **permissions** tab and “**user1**” and click **Change Permissions**.



4. Select “**user1**” in the permissions window and click **Edit**.



5. Under permissions for **Create folders/ append data**, select or check the **Deny** and click **OK**.



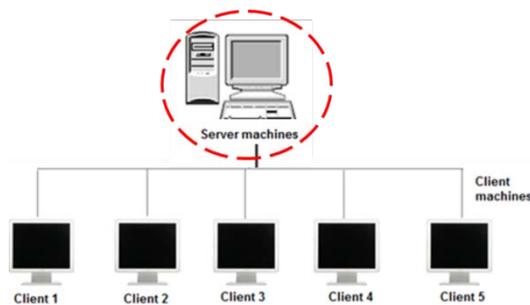
2.5 Setting Windows Firewall

Windows Firewall is a program to prevent malicious software from gaining access to your PC through the Internet or a network. In the Network System, if the windows Firewall programs is turned on and the programs for UV Express Security software are blocked, it should be set to allow the programs to communicate through the Windows Firewall.

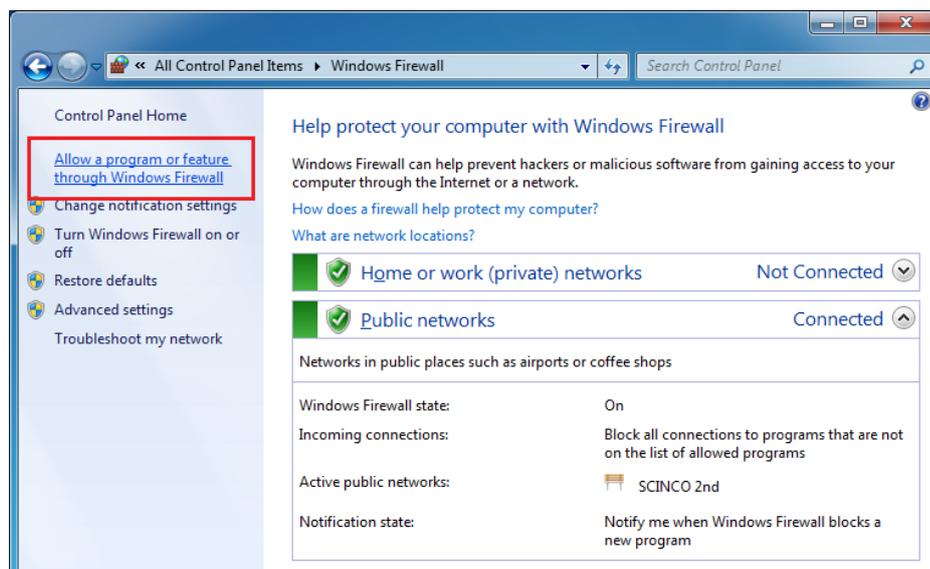
NOTE: *In case that user uses other firewall programs, it should also be set to allow the programs for UV Express Security software to communicate through those firewall programs.*

2.5.1 UV Express access through the Windows Firewall

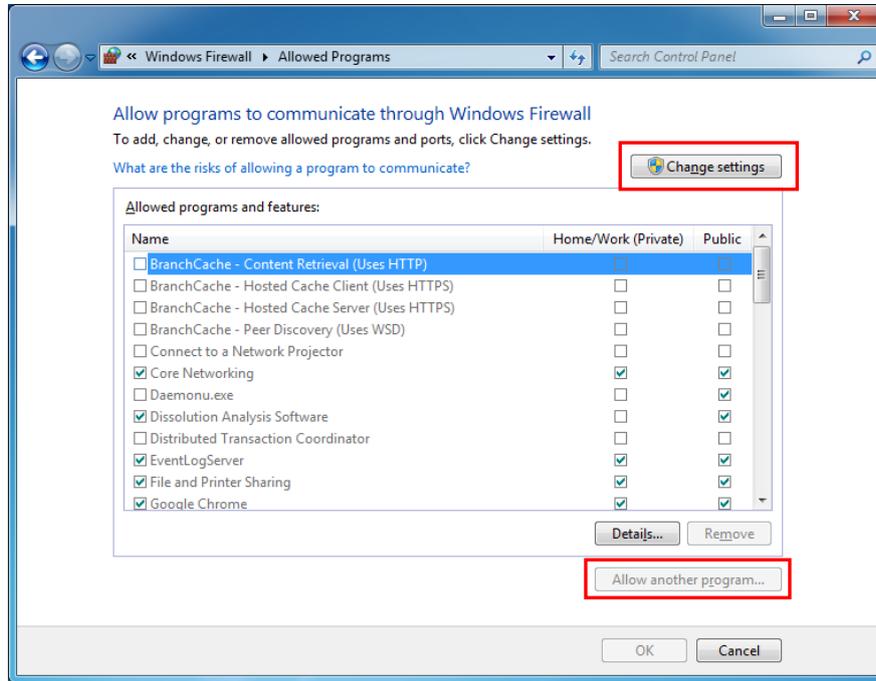
1. Log on as an Administrator account on the Server computer.



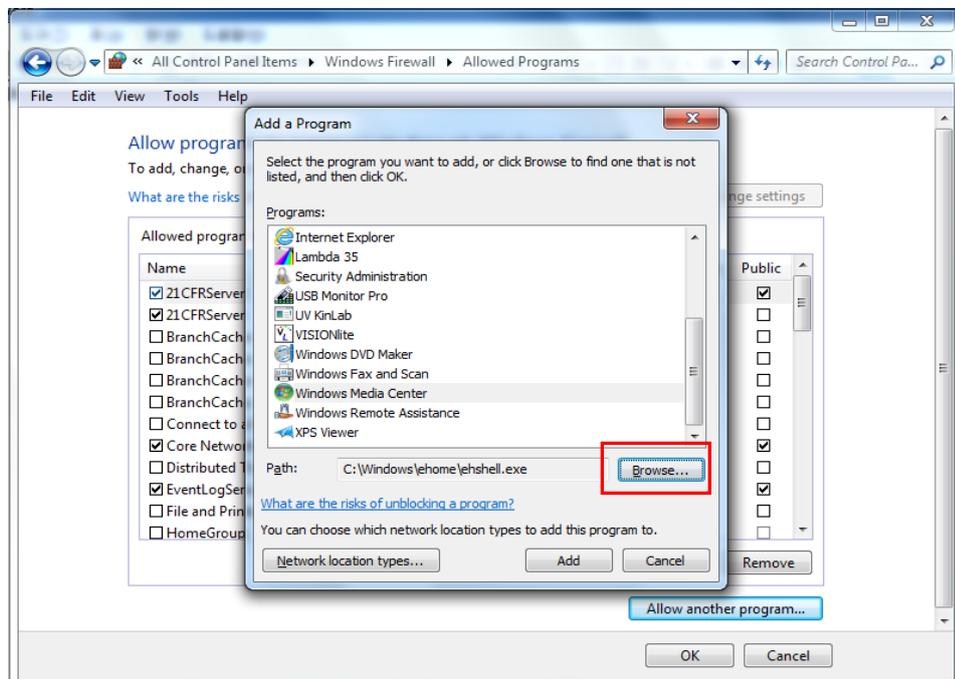
2. Select **Control Panel** from the Start menu in the windows operating system. And the click **Windows Firewall**.
3. Click **Allow programs to communicate through Windows Firewall**.



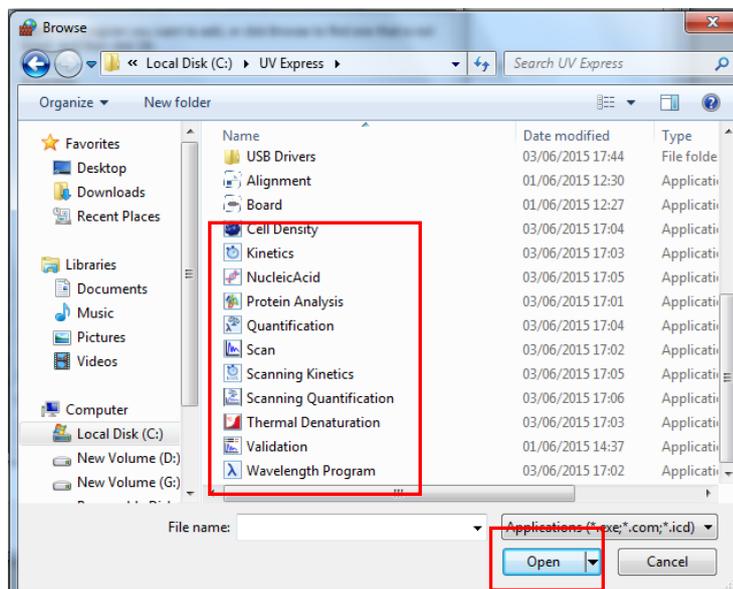
4. Select **"Change settings"** , and then the "Allow another program" button is activated. Click **"Allow another program"**.



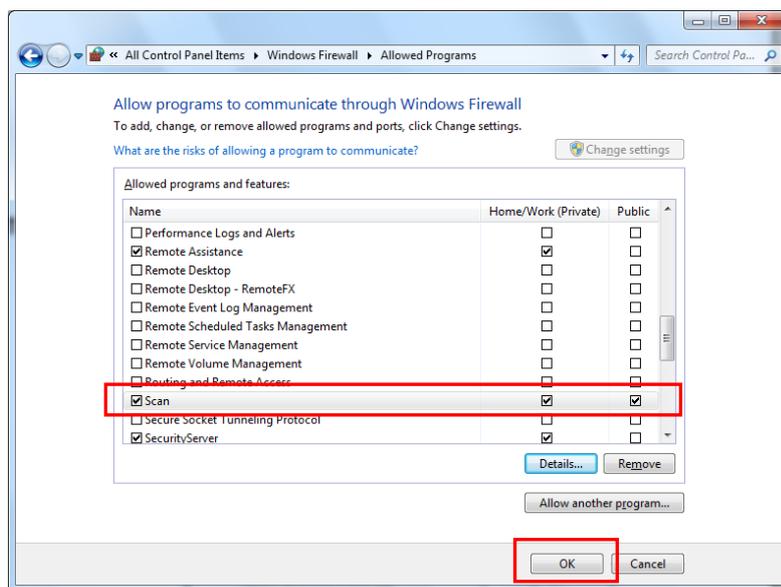
4. Click **Browse...**



- Open each executable measurement modes.



- After selecting **the entire measurement mode of UV Express** (such as **Scan**) and check **Home/Work (Private)** and **public**, then click **OK**.

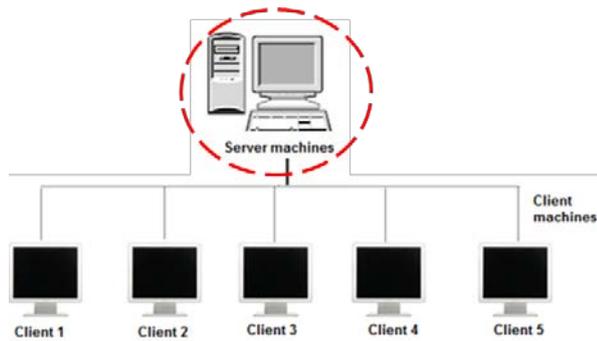


- Set to allow the **Security Server software** to communicate through Windows Firewall following procedures #5~7.
- Log on as an Administrator account of Client computer.
- Referring to procedures #2~#7, it should be set to allow **the entire mode of UV Express programs** for security software to communicate through the Windows Firewall of the Client computer.

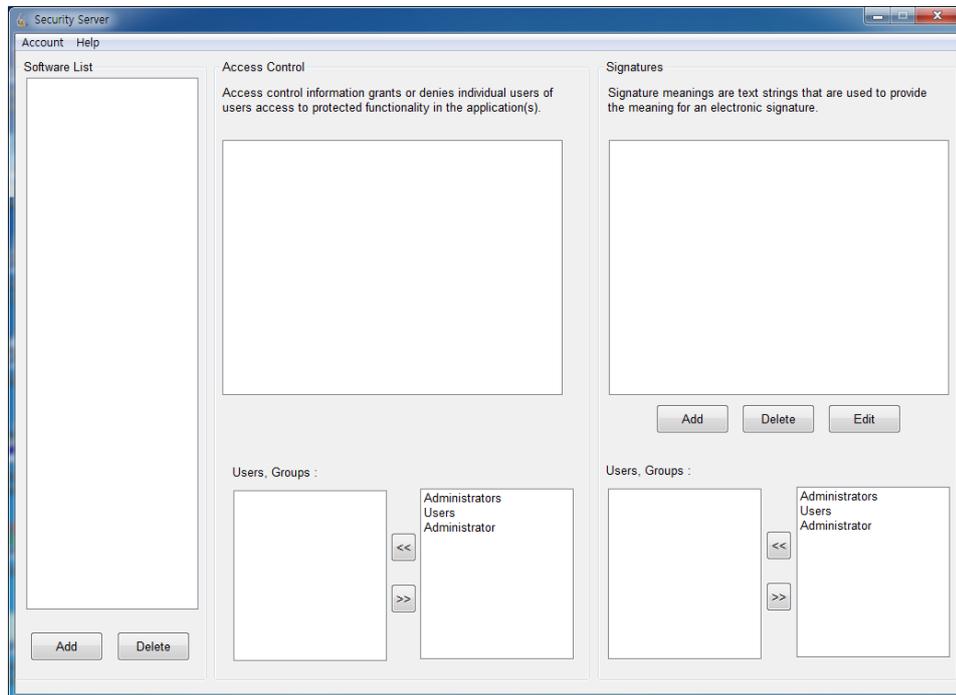
3. Operating Security Server

NOTE: *Security Server cannot be executed under the User account because the authority and permission have to be controlled by Administrator only.*

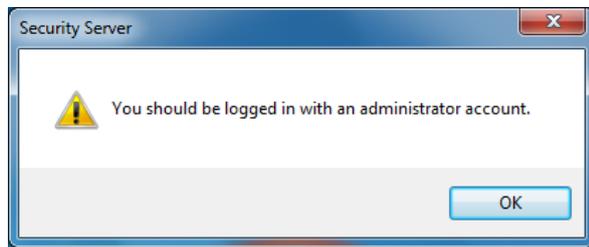
NOTE: *In the network system, to run the security program properly, the Administrator account of the Server computer should be kept logged-on.*



1. Run the **Security Server** software  , then Security Server window will appear.

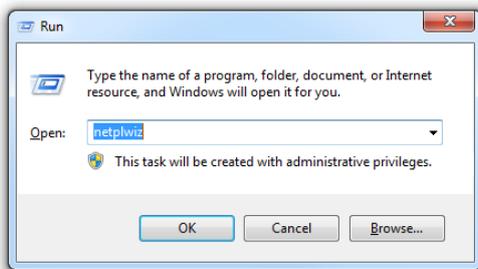


2. In case that the message pops up as below, proceed with the following steps to get the administrator account logged in properly.

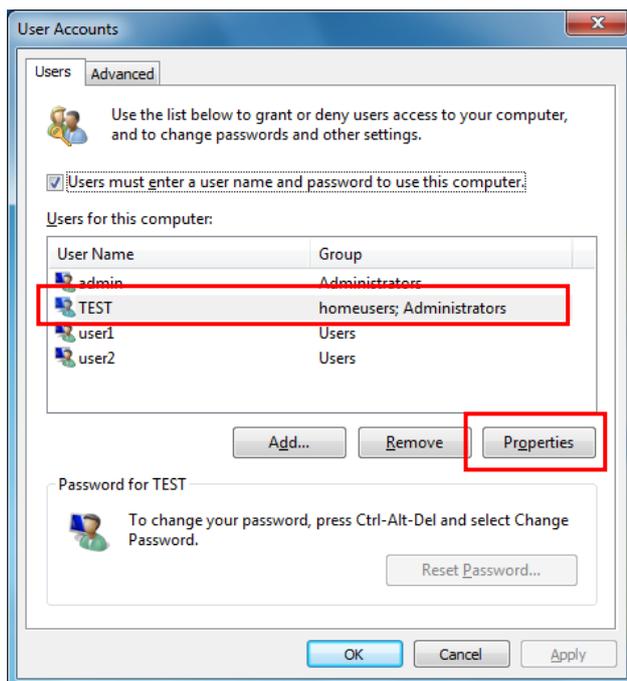


NOTE: *The account has to be grouped in proper type, e.g., Administrator or Standard user (Local account). If the account is involved in unintended group like homeusers, the access to software could be denied.*

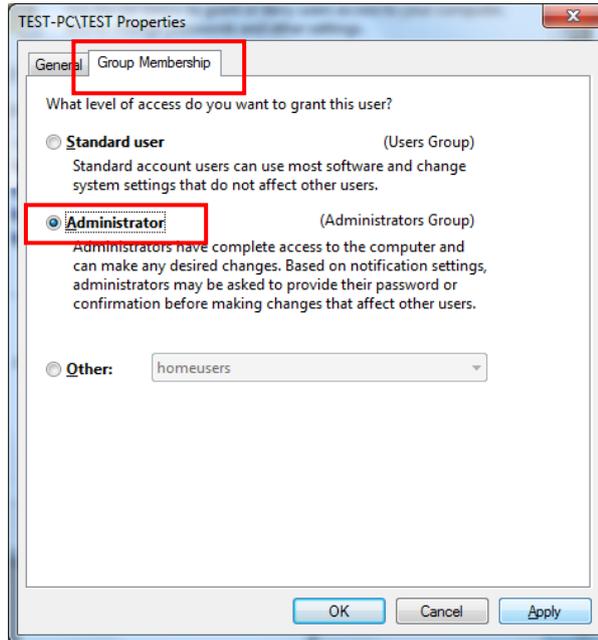
3. Press and hold the "Windows" key and then press the R key to open Run. After writing "netplwiz", click **OK**.



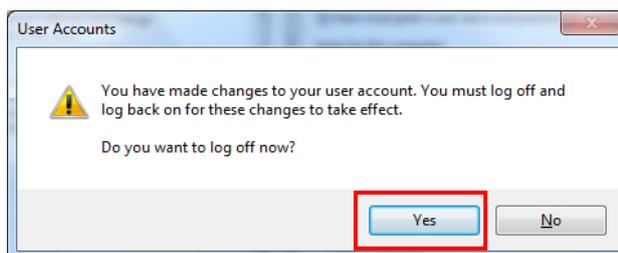
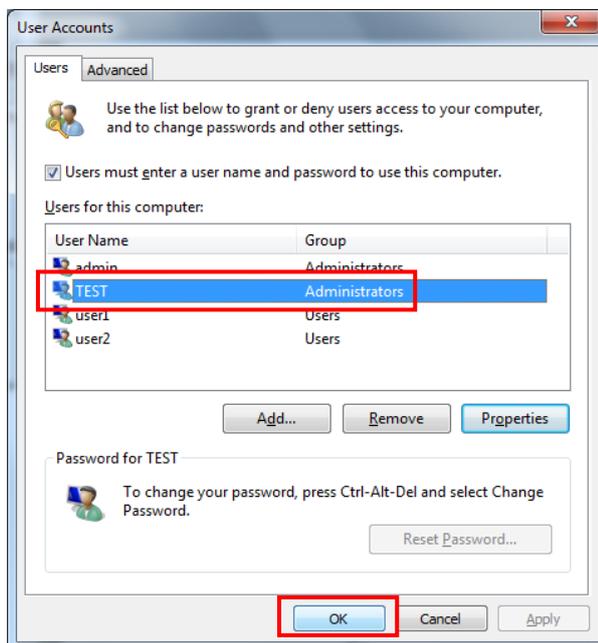
4. If the user is grouped other than Administration, i.e., homeusers, select user and click **Properties**.



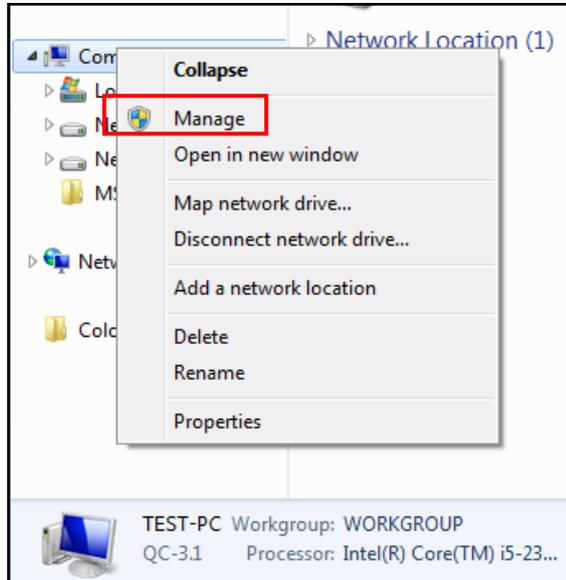
5. Select **Group Membership** and check **Administrator**. Click **Apply** and **OK**.



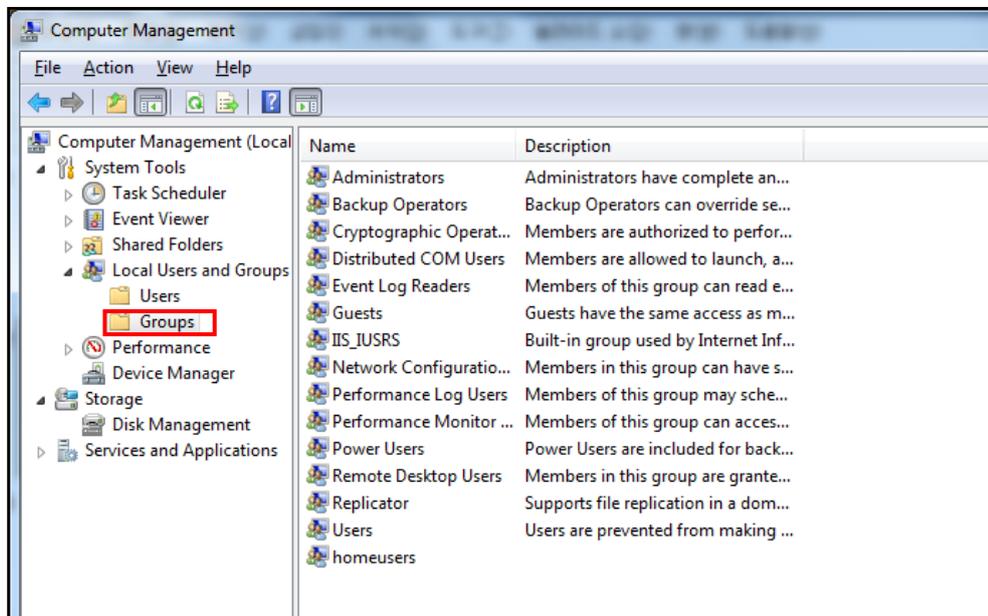
6. Confirm the group is properly modified. After the following message appear, Click **Yes** to restart computer.



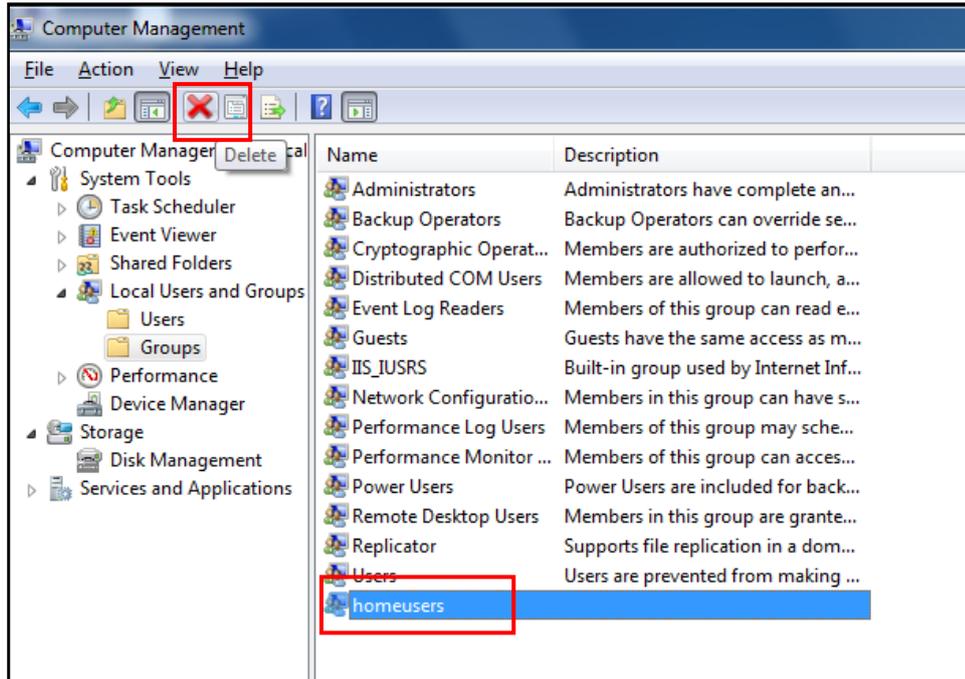
7. Despite all that, if accessing to Security Server is still denied, the unwanted group (homeusers) has to be deleted itself. Right-click on **Computer** and then click **Manage**.



8. Open **Groups** in Local Users and Groups.

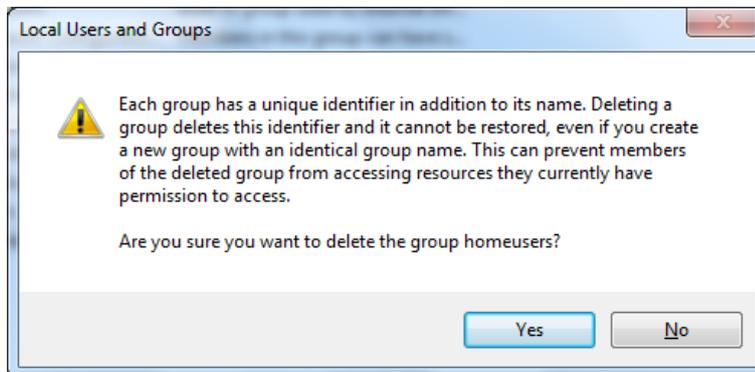


9. Select **homeusers** and click **Delete** icon.



10. The following box will appear. Click **Yes** to delete homeusers group.

NOTE: *Other functions of windows system could be affected by deleting this homeusers group. Carefully consider the deletion.*

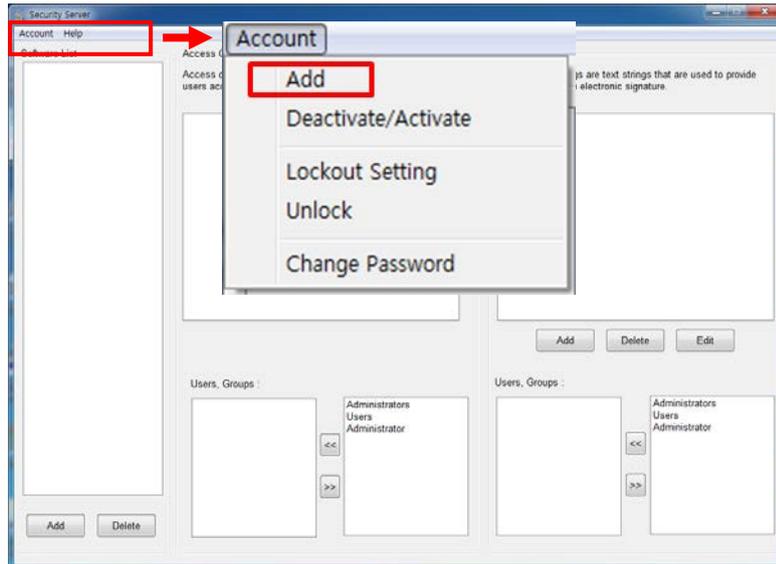


11. Restart the computer and execute the Security Server.

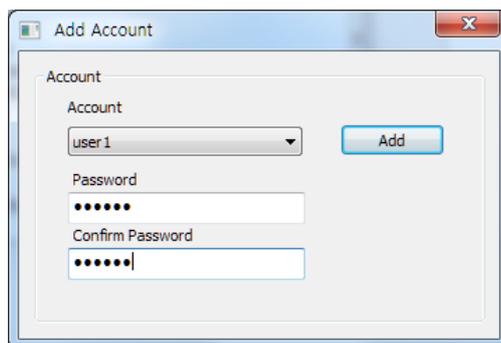
3.1 Set [Account]

On UV Express security software, user's account(s) should be added in the Security Server software following the procedures below.

1. Select **Account** of the Security Server window. Click **Add**.



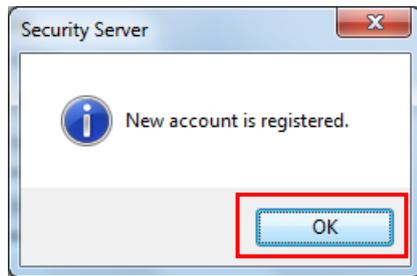
2. As the Add Account window appears, select **account** and set the password. Click **Add**.



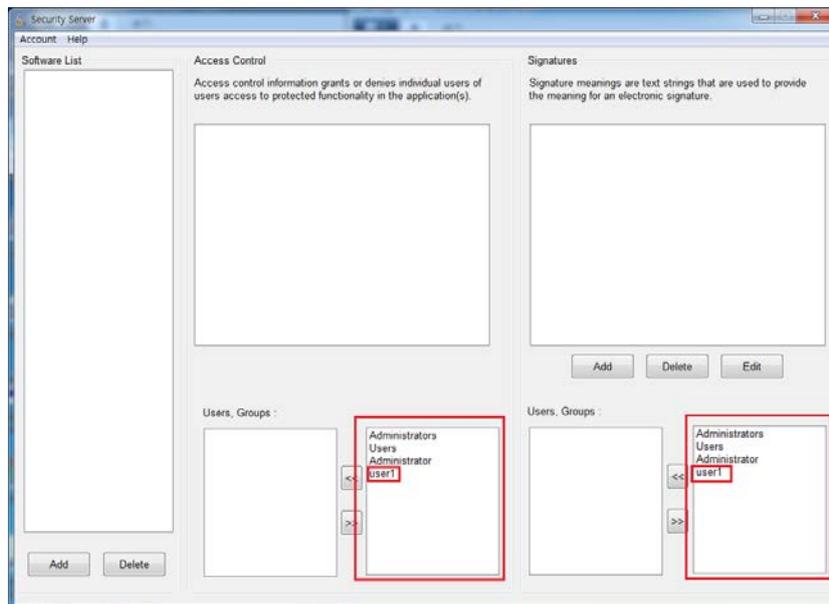
NOTE: Password must be of minimum 6 characters and include at least one letter and a number each.

NOTE: When the new user logs on for the first time, they will be forced to change their password.

3. The following message will appear, and then click **OK**.



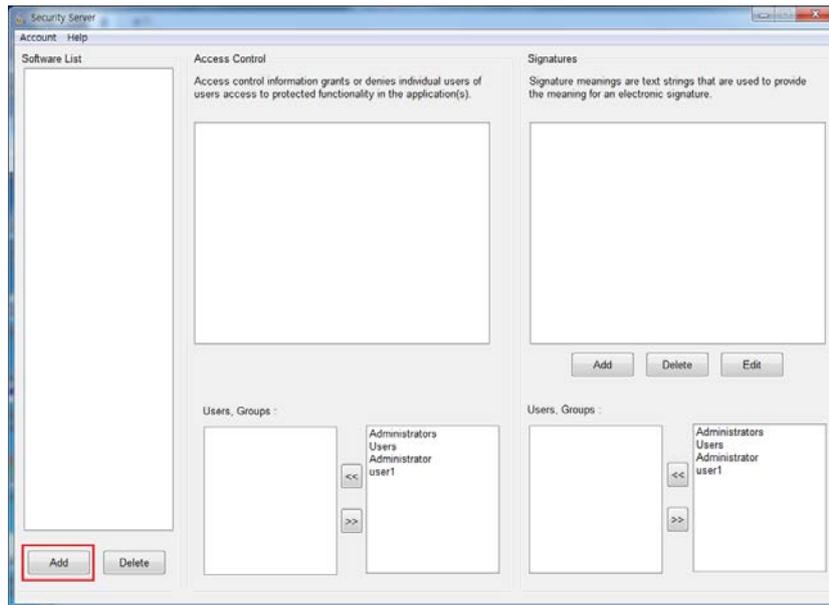
4. Confirm the account was listed on **Users, Groups**.



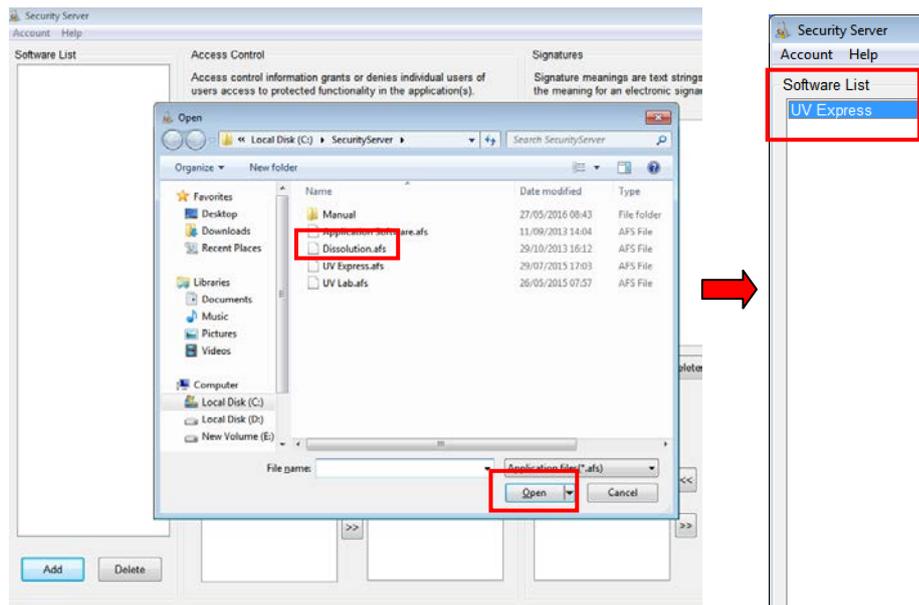
3.2 Set [Software List]

In order to set Access Control for UV Express security software functions, the software must be registered on the Software List in advance. Set the Software List as follows.

1. Click **Add** in the Software List section of the Security Server window.



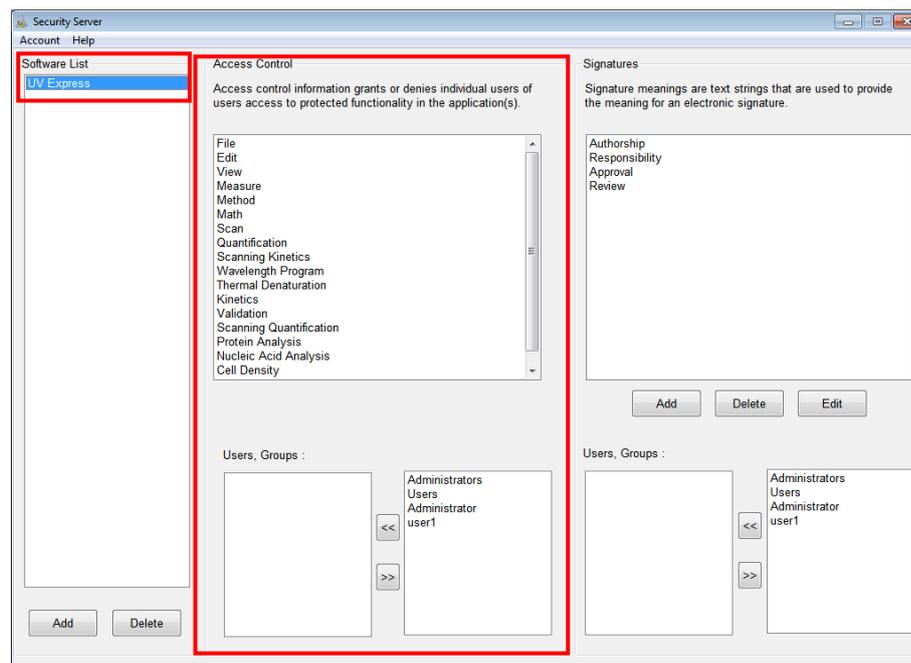
2. As the open window appears, select **UV Express.afs** and click **Open**. Then, the UV Express will appear in the Software List.



3.3 Set [Access Control]

Access Control assigns users the authority to access various functions in the UV Express security software. Set access controls as follows.

1. Click on the **UV Express** in the Software List. And then items are displayed in each section.



Each 'function' corresponds to a menu item in the main menu of the UV Express software or a specific command. See the UV Express software Users Guide for more details.

File : Allows user to access each command in the File menu.

Edit : Allows user to access each command in the Edit menu.

View : Allows user to access each command in the View menu.

Measure : Allows user to access each command in the Measure menu.

Method : Allows user to access each command in the Method menu.

Math : Allows user to access each command in the Math menu.

Scan : Allows user to access Scan mode executable program.

Quantification : Allows user to access Quantification mode executable program.

Scanning Kinetics : Allows user to access Scanning Kinetics mode executable program.

Wavelength Program : Allows user to access Wavelength Program mode

executable program.

Thermal Denaturation : Allows user to access Thermal Denaturation mode executable program.

Kinetics : Allows user to access Kinetics mode executable program.

Validation : Allows user to access Validation functions. Validation Software is optional.

Scanning Quantification : Allows user to access Scanning Quantification mode executable program.

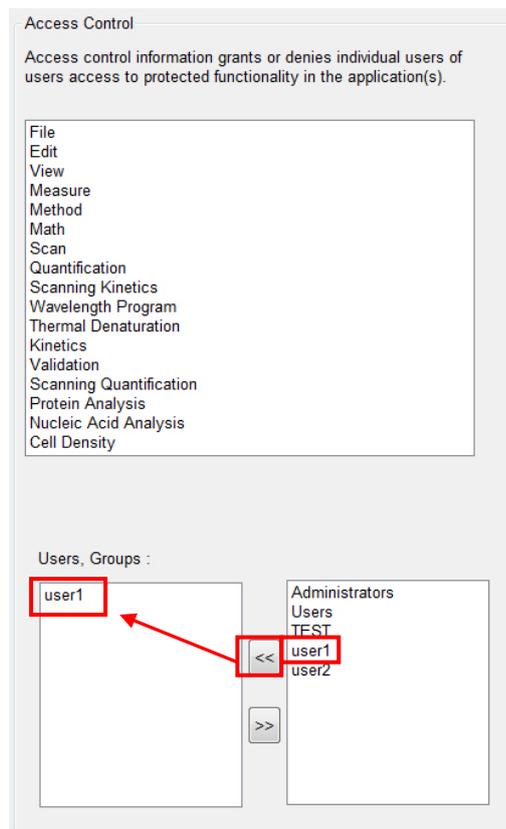
Protein Analysis : Allows user to access Protein Analysis mode executable program.

Nucleic Acid Analysis : Allows user to access Nucleic Acid Analysis mode executable program.

Cell Density : Allows user to access Cell Density mode executable program.

Multicomponent Analysis : Allows user to access Multicomponent Analysis mode executable program.

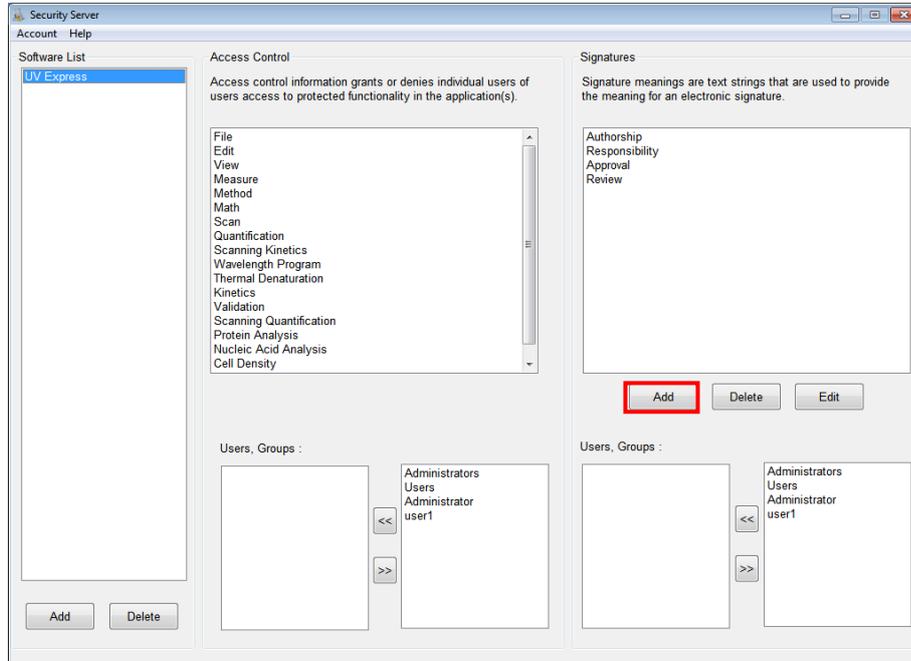
2. Select the user account(s) to be given the access permission to each and click .



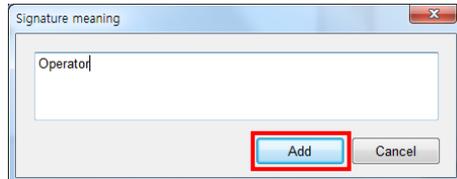
3.4 Set [Signature Meanings]

Set the signature meanings for users as follows.

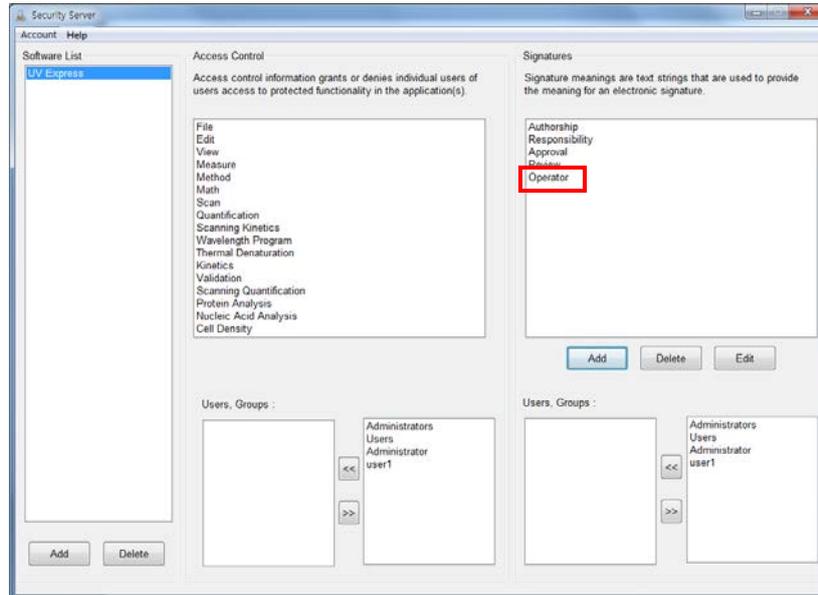
1. To create a new signature, click **Add** in the Security Server window.



2. Enter the name for the new signature meaning and click **Add**.

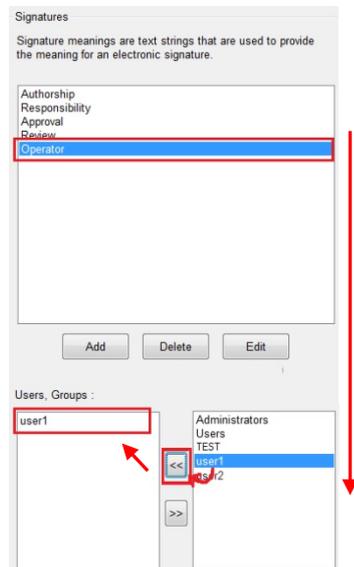


3. The created signature meaning is shown in the Security Server window.



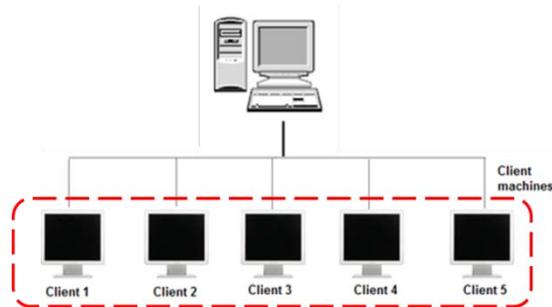
4. Users for each signature are listed in the "Users, Groups" section. Select a signature and select users who will have the authority to apply the selected signature using

<< , >> in the Users, Groups section.



4. Operating UV Express Software

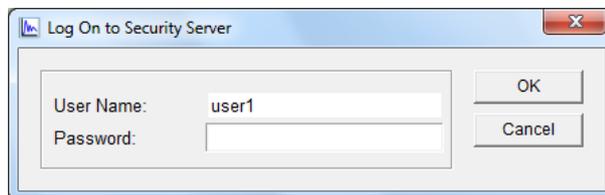
4.1 Operating UV Express Software



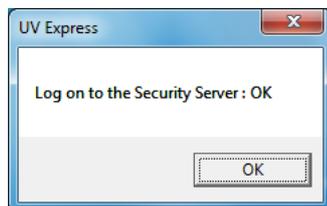
1. Log on to a client computer as a **Standard user account**.

NOTE: *UV Express software cannot be executed under a Windows "Computer Administrator" account because the administrator account has the authority to modify and delete data.*

2. Execute one of the measurement modes of UV Express software, and then 'Log on to Security Server' message will appear. Enter the registered User Name and Password of the account and click **OK**.



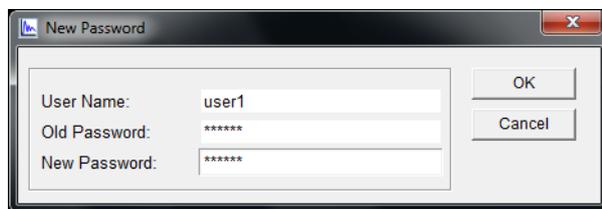
3. If the password is correct, the following message will appear, and then click **OK**.



4. If it is the first time to log on to UV Express security software, the following message will appear and click **OK**.

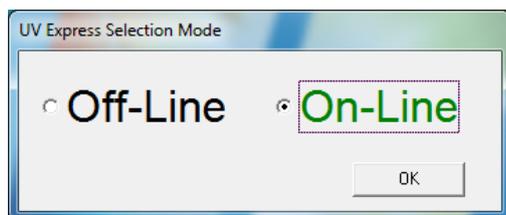


5. Enter the old password (assigned password by administrator) and a new password, and then click **OK**.



NOTE: Password must be of minimum 6 characters and include at least one letter and a number each.

6. The "Password successfully changed" message will appear, and then click **OK**.
7. Log on again with the changed password. If the instrument is connected and ready to measure, click **On-Line** or **Off-Line**.



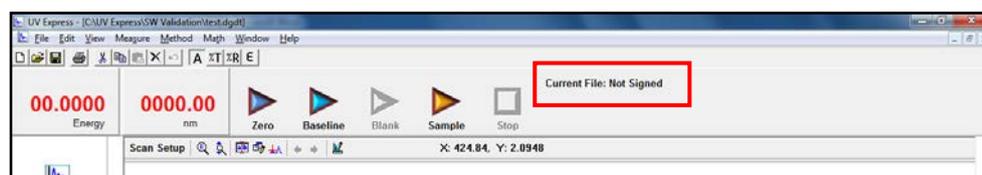
8. A user's access to each menu is determined by the privileges given to each user account. In the following example, user1 was given access to log on and execute the **Scan** mode of UV Express software with the file, method, measure and signature menu.

9. Open an existing sample data or measure the sample. Save a data.

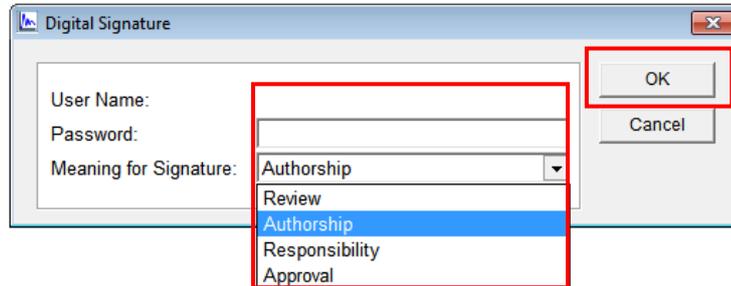
NOTE: If the data is not saved, signatures cannot be applied. Ensure that data is saved first.

NOTE: Data must be saved in a folder which the user has been granted the access to.

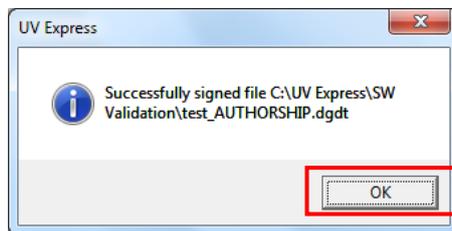
10. Apply a signature to measured or archived data by clicking **Current File** on the window.



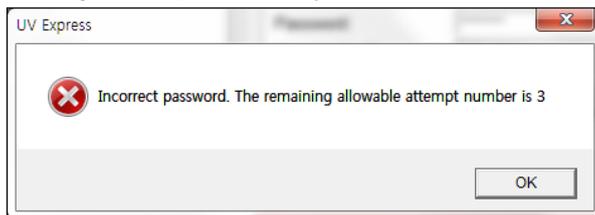
11. In the Digital Signature dialog box, enter User Name and Password, select the signature meaning, and click **OK**.



12. After the Signature is complete, the following message will appear. Click **OK**.

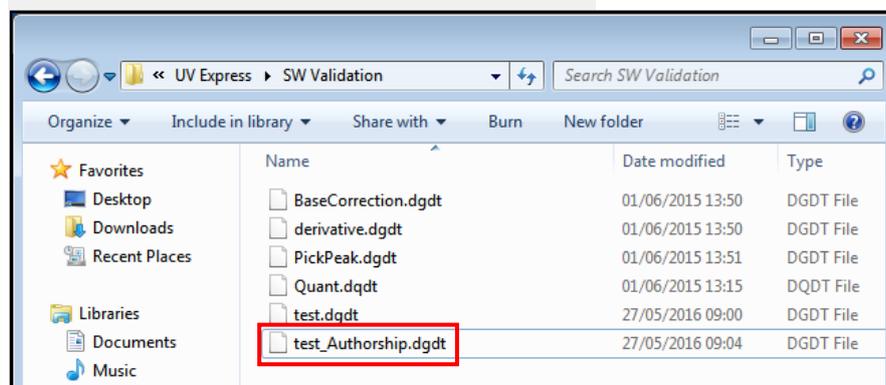


NOTE: *If you enter any incorrect password, the below message will appear. Your account is locked out when you exceed the limit number of failed logins and it can be unlocked by setting a new password by the administrator.*

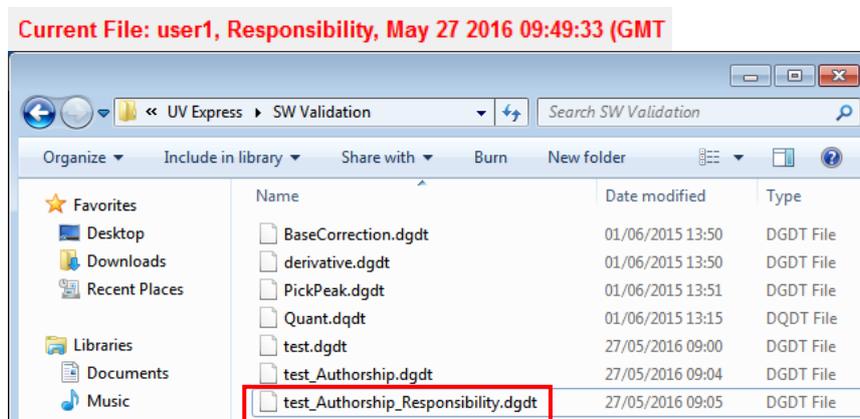


13. The signature record is shown in the main window and the signed data is saved as a new file.

Current File: user1, Authorship, May 27 2016 09:49:00 (GMT -8:00)



14. If the second signature is applied to the data file, it is saved as a new file again as shown below.

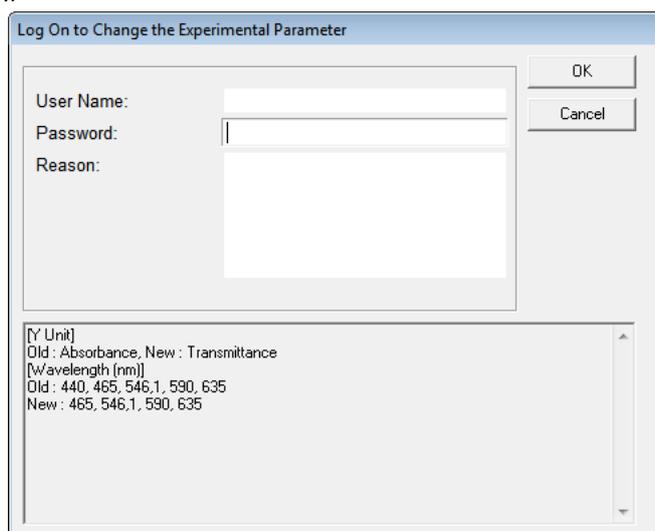


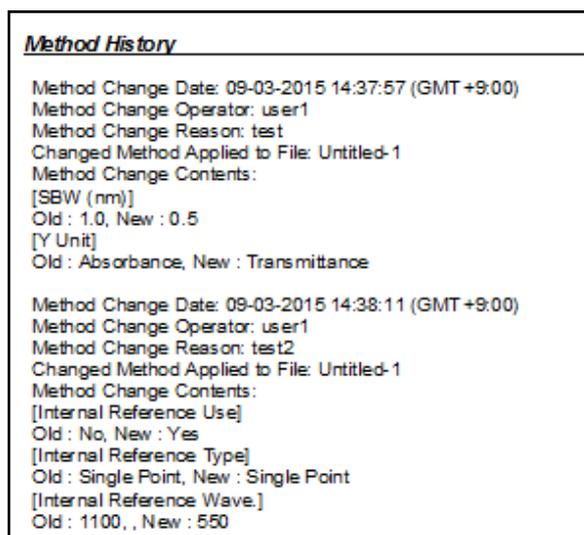
15. Click **Print** to view the saved data using a printed report.

4.2 Changing Methods

If any Method is changed or data is modified in the signed file, user has to enter the User Name and Password to change methods. After typing the reason, click **OK** to save the changed data. The method change history could be checked in the print window.

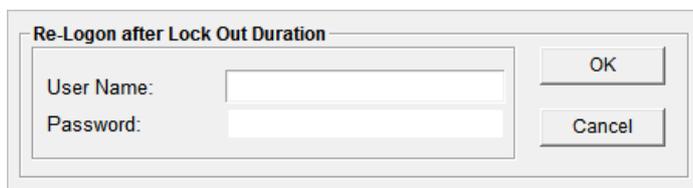
NOTE: *Be sure that if the method or data is modified, the data is needed to be saved and signed again.*





4.3 Lockout for unattended operation

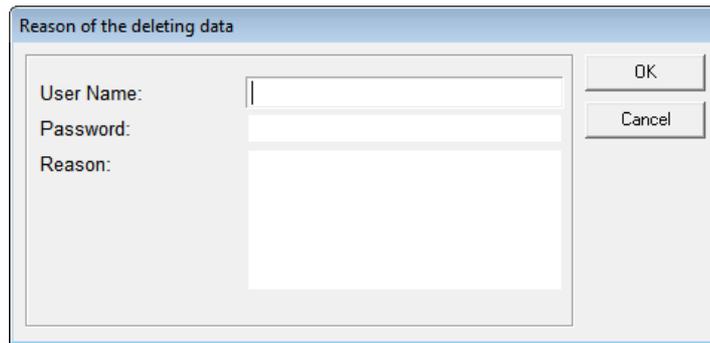
This function is performing automatic lockout after some set time of inactivity. The automatic lockout time (Lockout duration) is set in the security server software by the administrator. If there is no action in the set time after the UV Express security software is executed, it is locked out and the following message will appear. Enter the User Name and Password to unlock the UV Express security software again.



NOTE: *Your account is locked out when you exceed the limit number of failed logins and it can be unlocked by setting a new password by the administrator.*

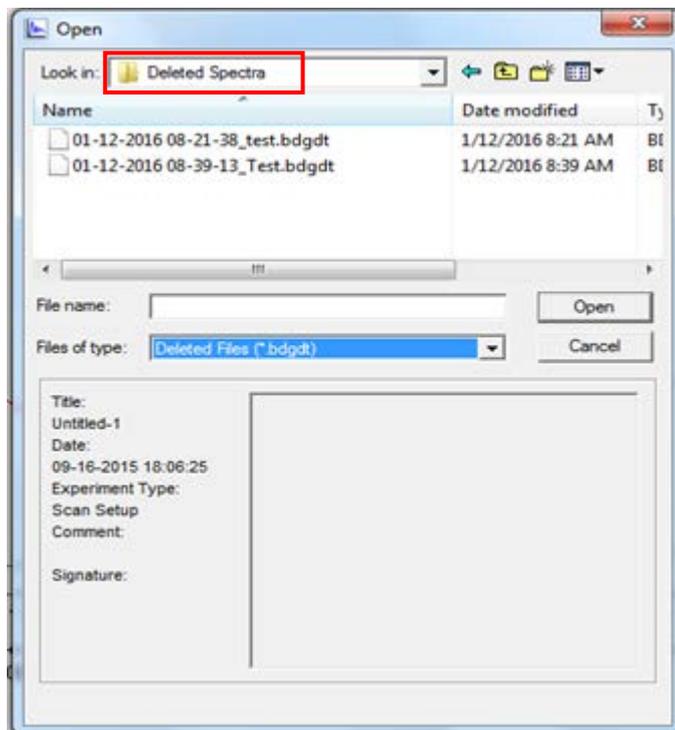
4.4 Deleting Spectra

If a user deletes an acquired spectrum from the sample measurement result, it is mandatory to enter the User Name and Password in the 'Reason of the deleting data' message box. Deleted data is stored in the 'Deleted Spectra' folder. (C:\UV Express\Deleted Spectra).



4.5 Retrieve the deleted spectra

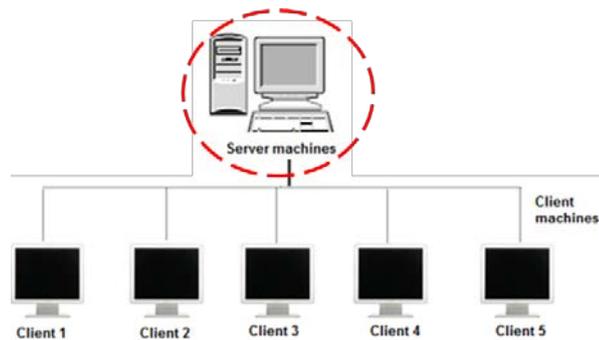
1. In order to retrieve and re-analyze the deleted spectrum in the UV Express security software, click **Open** in the menu and select the deleted file [* .b+ file extension (e.g. *.bdgdt)] in the '**Deleted Spectra**' folder.



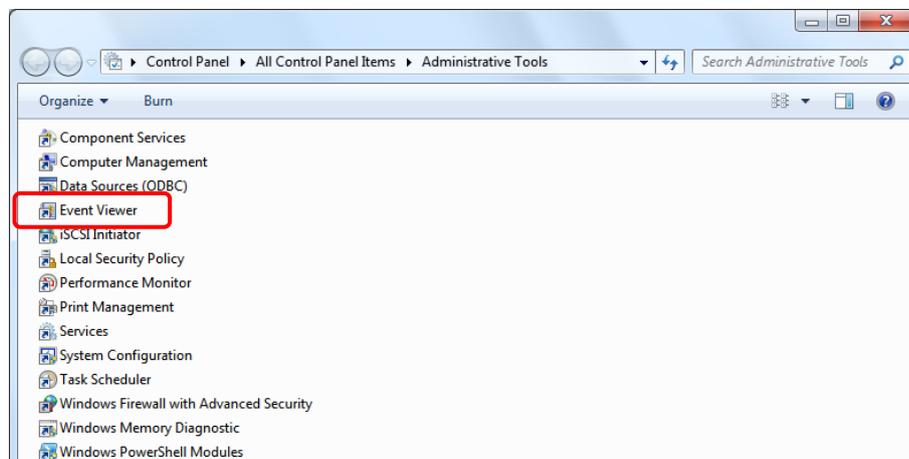
5. Event Log

The Logs of Changes are displayed in the Windows Event Viewer to trace the history of all setup changes in the Security Server and UV Express Security software.

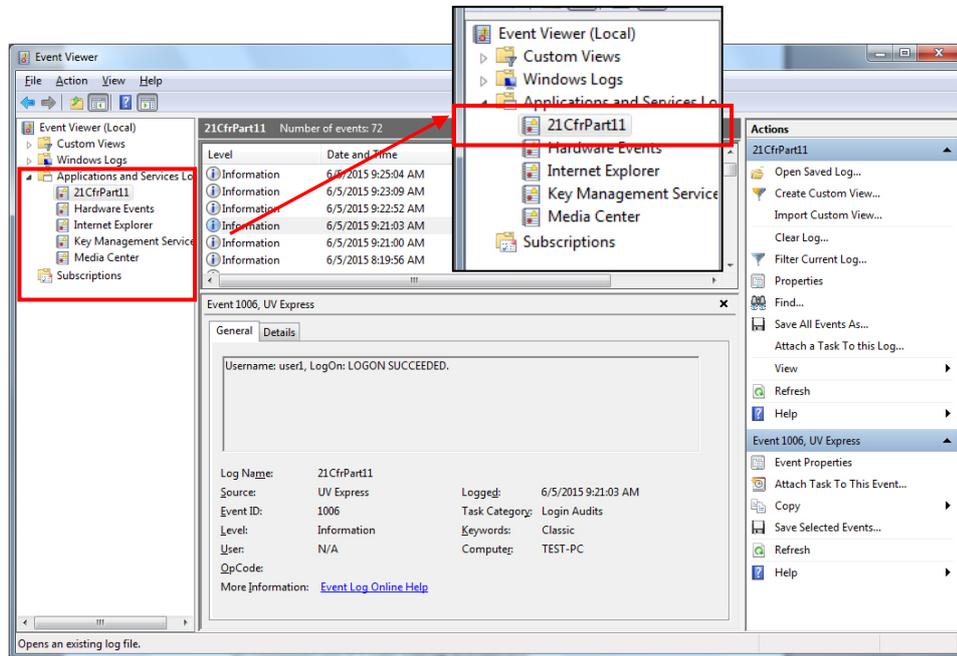
NOTE: *In the network system, they are shown in the server PC.*



1. Click **Start > Control Panel**.
2. Open **Administrative Tools > Event Viewer**.



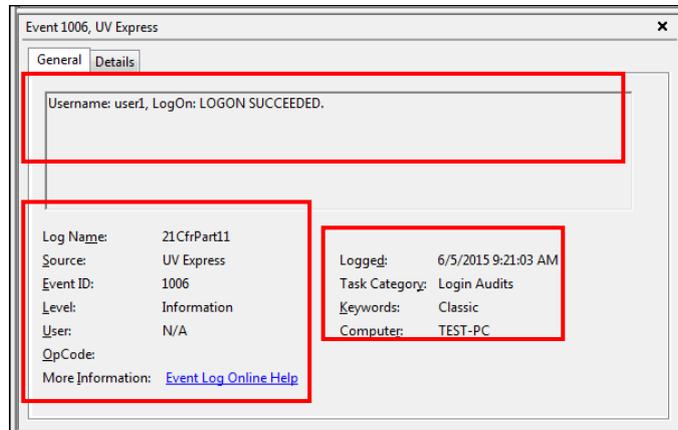
- The Event View contents are displayed. Expand the **Applications and Services Logs** folder, and then select **21CfrPart11**.



- The event logs of the windows applications related to the UV Express Security Software are listed in the **21CfrPart11** section. Select a particular event log in the list.

Level	Date and Time	Source
Information	6/5/2015 9:25:04 AM	UV Express
Information	6/5/2015 9:23:09 AM	UV Express
Information	6/5/2015 9:22:52 AM	UV Express
Information	6/5/2015 9:21:03 AM	UV Express
Information	6/5/2015 9:21:00 AM	UV Express
Information	6/5/2015 8:19:56 AM	Security Administrati...
Information	6/5/2015 8:19:46 AM	Security Administrati...
Information	6/5/2015 8:19:04 AM	Security Administrati...
Information	6/5/2015 8:18:53 AM	Security Administrati...

5. You can see more detailed information (Username, software, event, date, time, etc). Some of types of the events are described as follows.



a) Description of Security Server

Account and Permission modified : Change the account settings.

- Ex.1) Username: Administrator. Added "UV Express" to Application Software.
 Ex.2) Username: Administrator. Deleted "UV Express" from Application Software.
 Ex.3) Username: Administrator. Changed the Lockout Setting.
 Ex.4) Username: Administrator. Changed the password : "user1".
 Ex.5) Username: Administrator. Added "user1: in the users list.
 Ex.6) Username: Administrator. Deactivated the user account: "user1".
 Ex.7) Username: Administrator. Activated the user account: "user1".
 Ex.8) Username: Administrator. Unlocked : "user1".
 Ex.9) Username: Administrator. Added "user1" to "Review" Signature Permission.
 Ex.10) Username: Administrator. Deleted "user1" from "Review" Signature Permission.
 Ex.11) Username: Administrator. Added "user1" to "Wavelength Program" Access Permission.
 Ex.12) Username: Administrator. Deleted "user1" from "Wavelength Program" Access Permission.

b) Description of UV Express

Performance : Note the serial number of instrument with every operation.

- Ex.) Username: user 1. "Scan" was performed. Instrument : Lambda 365. Serial number : 365K5050403.

Account modified : Change the account settings.

- Ex.) Username: user1, Scan: Password successfully changed.

Logon : Execute the UV Express software.

- Ex.1) Username: user1, LogOn: **LOGON SUCCEEDED**.
 Ex.2) Username: user1, LogOn: **LOGON FAILED**.
 Ex.3) Username: user1. Scan(Log On) : The ID is not registered.

- Ex.4) Username: user1. Scan(Log On) : Incorrect password. The remaining allowable attempt number is 1.
- Ex.5) Username: user1. Scan(Log On) : User has entered wrong password over the lock out number and account is disabled.
- Ex.6) Username: user1. Quantification : User does not have permission to access the Quantification.

Re-logout : Re-access UV Express software after lockout time.

- Ex.1) Username: user 1, Scanning Kinetics : **RELOGON SUCCEEDED**.
- Ex.2) Username: user 1, Scanning Kinetics : **RELOGON FAILED**.
- Ex.3) Username: user1. Scan(Relog On) : Incorrect password. The remaining allowable attempt number is 2.
- Ex.4) Username: user1. Scan(Relog On) : User has entered wrong password over the lock out number and account is disabled.
- Ex.5) Username: user 1, Scanning Kinetics : **RELOGON** succeeded for change the method.

Created : Save data to new file or create the sample.

- Ex.1) Username: user1. The file "C:\UV Express\Data\time.dkdt" was **created**.
- Ex.2) Username: user1. The data "Sample1" was **created**. The file "C:\UV Express\Data\Untitled-1.dgdt".
- Ex.3) Username: user 1. The data "Sample1 + 1.0000" was **created**. The file "C:\UV Express\Data\data1.dgdt".

Modified : Save the modified data or save as different name.

- Ex.1) Username: user1. The file "C:\UV Express\Data\time2.dkdt" was **modified**.
- Ex.2) Username: user1. Protein Analysis : The delete all was undone. The file "C:\UV Express\Data\Untitled-1.dpdt".
- Ex.3) Username: user1. Protein Analysis : The data Sample 1 was pasted. The file "C:\UV Express\Data\Untitled-1.dpdt".
- Ex.4) Username: user1. Protein Analysis : The data Sample 1 was copied. The file "C:\UV Express\Data\Untitled-1.dpdt".
- Ex.5) Username: user1. The data "Sample 1 + Sample 2" was modified. The original data is "Sample 1, Sample 2". The file is "C:\UV Express\Data\Untitled-1.dgdt".
- Ex.6) Username: user1. The file "C:\UV Express\Data\Untitled-1_Approval.dgdt" was modified. The original file is "C:\UV Express\Data\Untitled-1.dgdt".
- Ex.7) Username: user1. Scan : Method change reason - Test.
[Internal Reference Use]
Old : No, New : Yes

[Internal Reference Type]

New : Single Point

[Internal Reference Wave.]

New : 300.

Deleted : Save the delete a single data or all the data.

Ex.1) Username: user1. The data "sample 1" was **deleted**. The file C:\UV Express
\Data\data1.dgdt.

Ex.2) Username: user1. The data "Sample 1" was deleted. The file is Untitled-1.

Ex.3) Username: user1. Deleted all data. The file is Untitled-1.

Signature : Provide the electronic signature.

Ex.) Username: user 1. The file "C:\UV Express\Data\time.dkdt" was **signed**.

Reason : Review.

Log off : Close the UV Express software.

Ex.) Username: user 1, successfully exited or **logged off** the application.

Validation: Check the instrument's status (Wavelength, Photometric, Resolution,
Stray Light, Noise and Stability) only in Validation software.

Ex.) Username : user 1. The data "**Noise**" was created. The file Untitled-1

IV. Local System

1. Pre-Installation

Before installing the UV Express Application, the administrator needs to designate users or groups and assign their authority of access. In the Local System, UV Express software with the security function can be run on a user account, not on the Administrator account. To set up account design and write access is possible only on the Administrator account in the Local System.



*** Administrator account:**

- **User account design** (Refer to IV-1.1 User Account Design)
- **Installation Security Server software & UV Express and UV Express Security Software** (Refer to IV-2 Software Installation)
- **Check IP address** (Refer to IV-2.3 Setting IP address)
- **Setting Folder Permission** (Refer to IV-2.4 Folder Permission)
- **Setting Windows Firewall** (Refer to IV-2.5 Setting Windows Firewall)
- **Run the Security Server Software** (Refer to IV-3 Operating Security Server)

*** User account:**

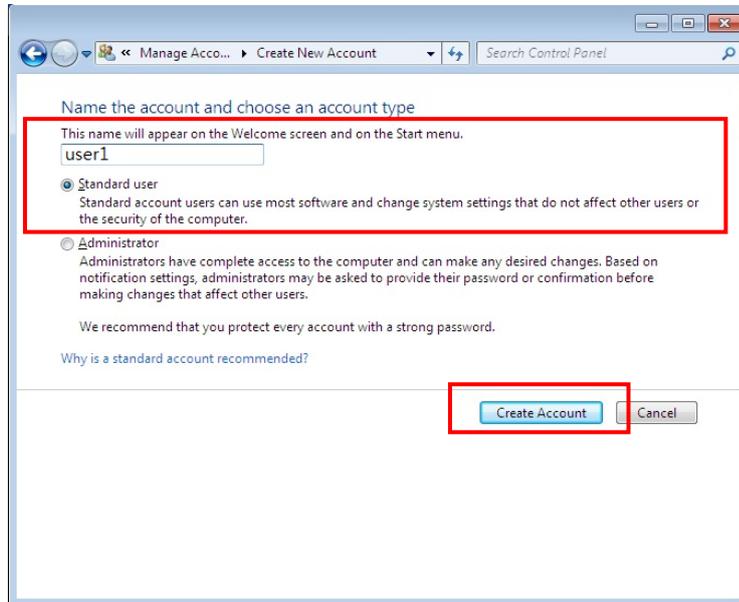
- **Run the UV Express software** (Refer to IV-4 Operating UV Express Software)

1.1 User Account Design

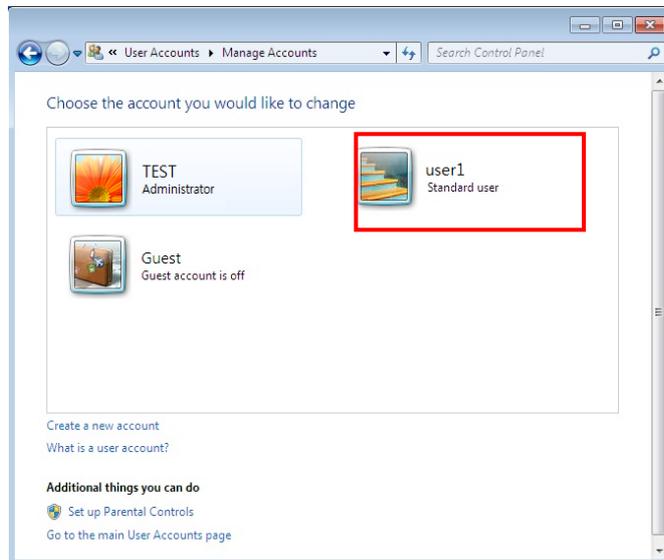
1.1.1 Create the User account(s) in Windows 7

1. Log on to the computer as an administrator.
2. Select **Control Panel > User Accounts** from the **Start** menu in the Windows operating System.
3. Click **Manage another account > Create a new account**.

4. Enter the Name (ex. user1) of the new account, select **Standard user** and click **Create Account**.



5. Verify the new account was created correctly.



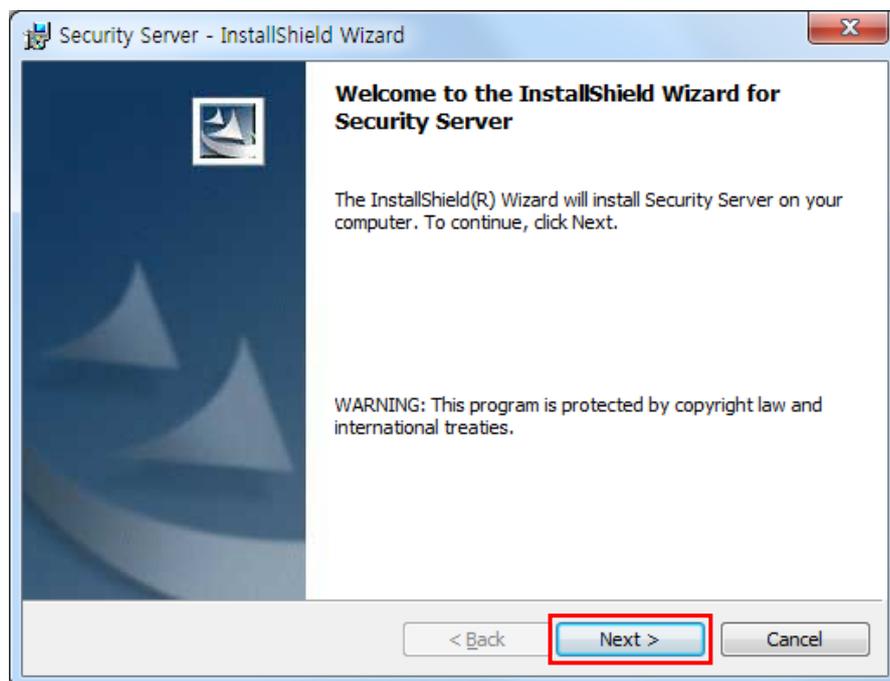
6. Additional accounts can be created in the same way as above.
7. The procedure for creating user account is complete.
8. Reboot and log on to the computer as an administrator.

2. Software Installation

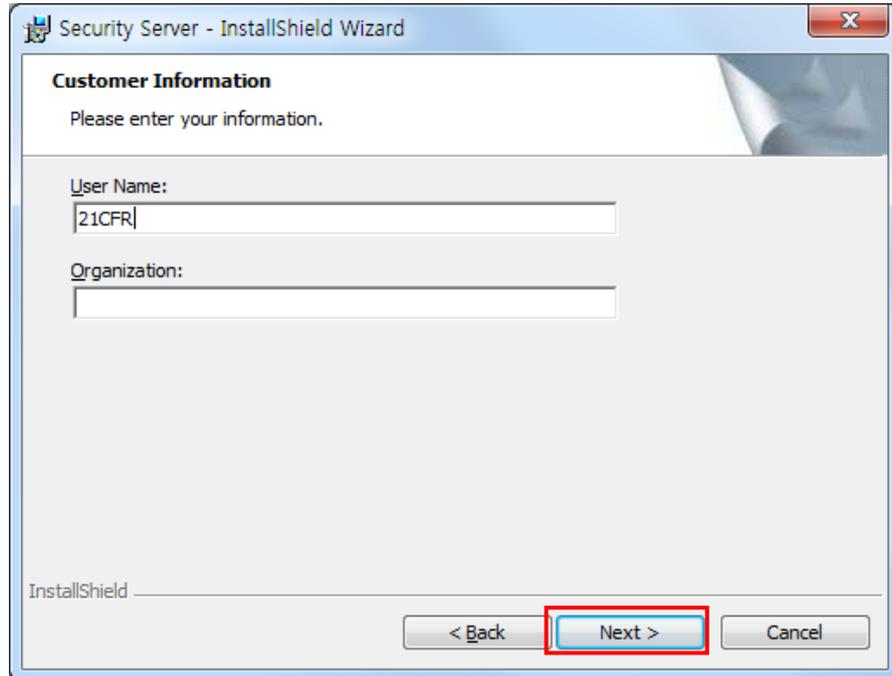
In the local system you should install three separate software, which are Security Server, UV Express and UV Express Security software on the Administrator account. However, the UV Express and UV Express Security software is running only in the Standard User account.

2.1 Installation of Security Sever Software

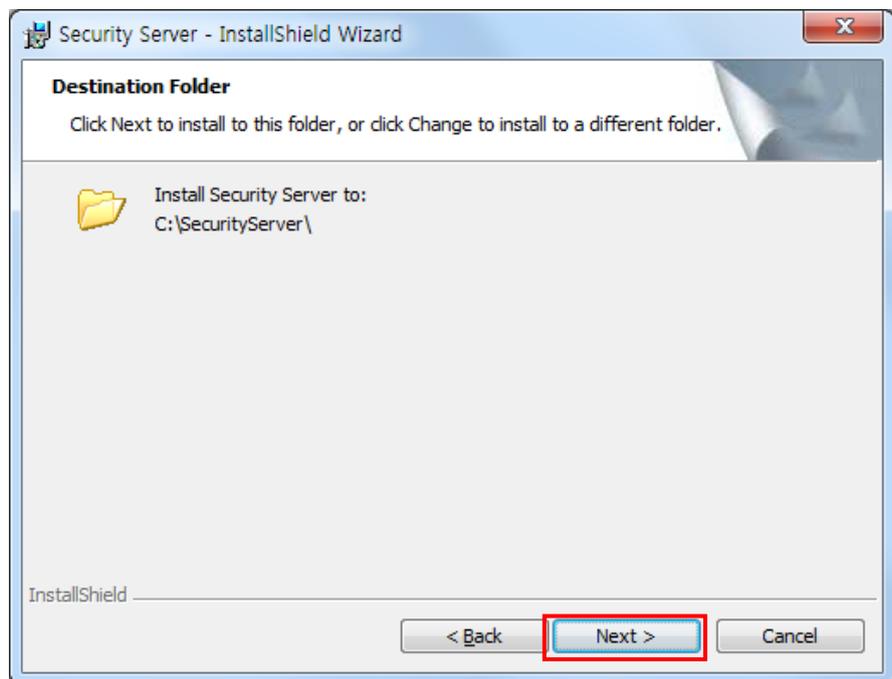
1. Log on to the computer as an Administrator account.
2. Input the **Security Server software** CD into the CD drive. Security Server Software is installed automatically. The default installation folder is "C:\ SecurityServer".
3. If the automatic setup window is not shown, click **Setup.exe** in the CD.
4. Security Server InstallShield® Wizard starts. Click **Next**.



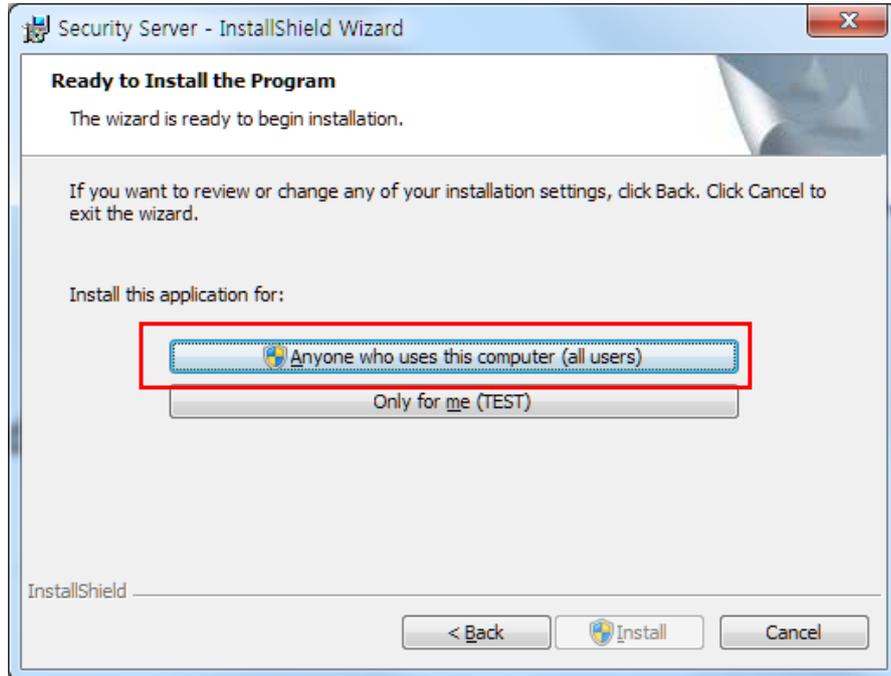
5. Enter your information and Click **Next**.



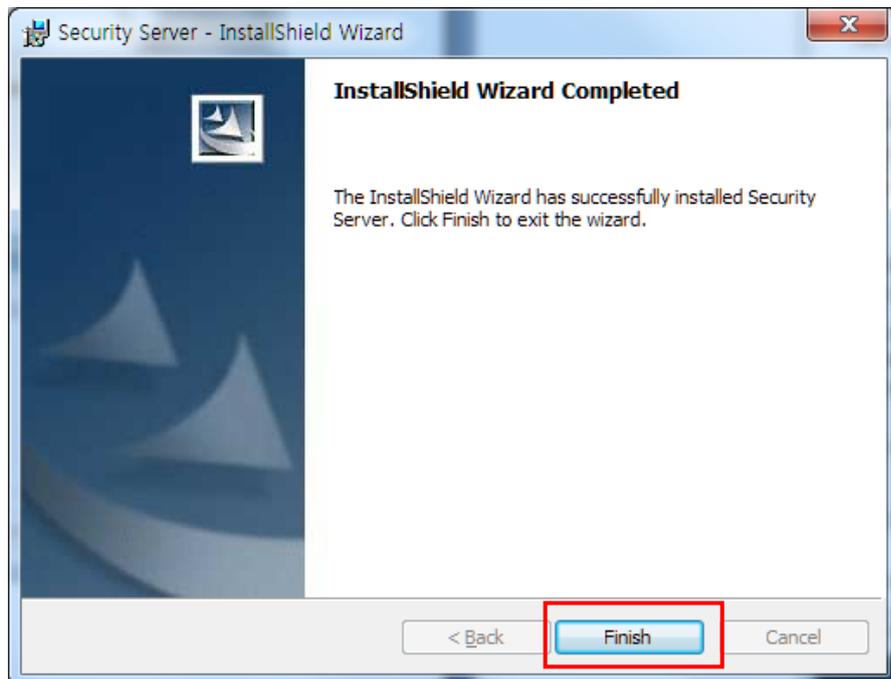
6. Click **Next**.



7. Click **Anyone who uses this computer (all users)**.



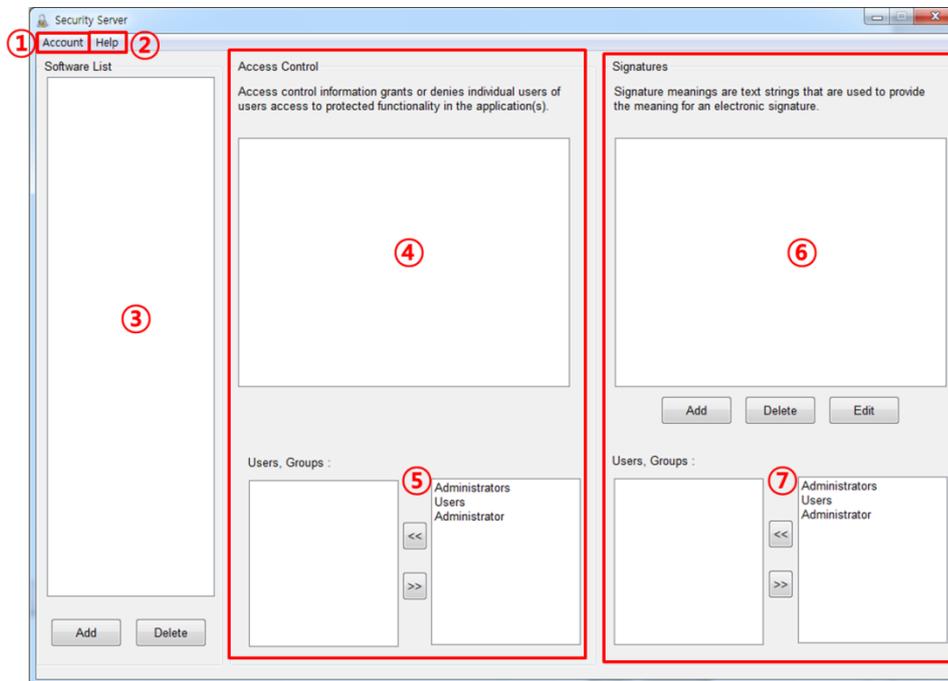
8. After the setup is completed successfully, click **Finish**.



9. After the Security Server software installation is complete, the icon  will be created on the Desktop.

2.1.1 Security Server Software Interface

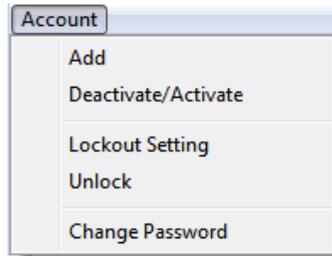
Describes the unique display features of the security software.



- ① Account: Control to set / change user account and password.
- ② Help: Display the security software Guide and version of Security Server.
- ③ Software List: Register the software to be used (UV Express).
- ④ Account Control: Display the software function of the selected software in the Software List section. (File, Edit, Math, Measure, View, Math, etc.)
- ⑤ Users, Groups: Select user account(s) to be given the access permission to each function in the Access control section.
- ⑥ Signature: Set electronic signature. (Default-Authorship, Responsibility, Approval, Review, etc.)
- ⑦ Users Group: Select user account(s) who will have the authority to apply each signature.

2.1.1.1 Account

- The Account menu includes commands to perform account functions as shown in the following table.

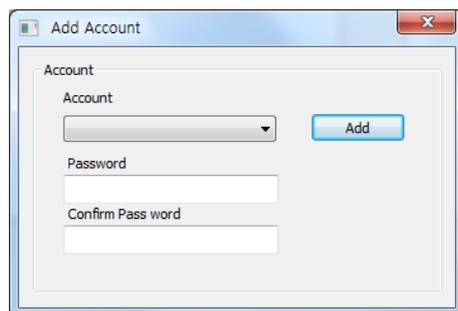


Command	Function
Add	Add new user account
Deactivate/Activate	Deactivate or activate the user account
Lockout Setting	Set the lockout function
Unlock	Unlock the user account and set new password
Change Password	Change the password of user account

Add

- Use the Add command to add a new user account.
- Procedure

1. To add a new user account, select user account and enter a password. Click **Add**.



NOTE: Password must be of minimum 6 characters and include at least one letter and a number each.

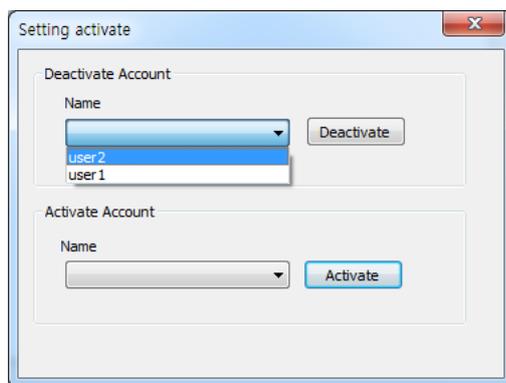
NOTE: When the new user logs on for the first time, they will be forced to change their password.

Deactivate/Active

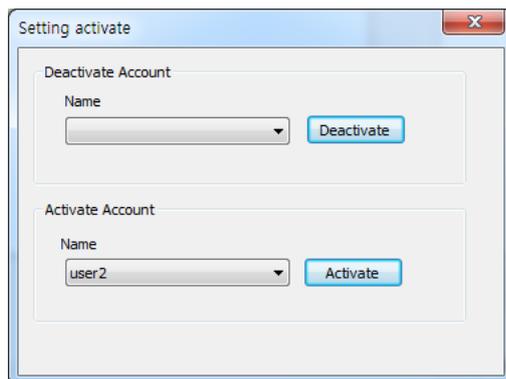
- Use the Deactivate command to delete deactivate and prohibit an activate user account to access the UV Express software.
- Use the Active command to activate and allow a deactivate user account to access the UV Express software.

■ Procedure

1. To deactivate a registered user account, click the “Name” drop-down list in the “Deactivate account” section, and then the currently activated accounts are listed.
2. Select the account to be deactivated and then click **Deactivate**.

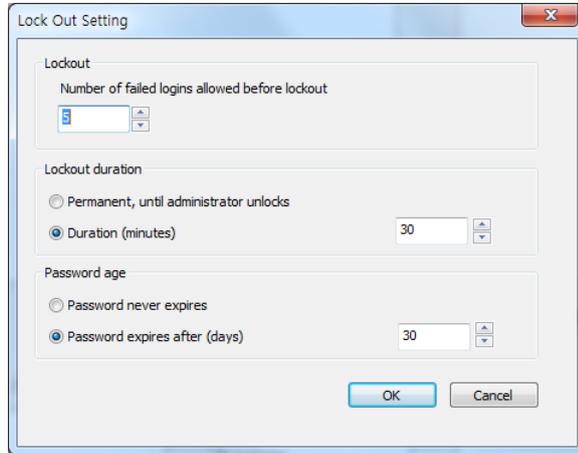


3. To activate a registered user account out of deactivated accounts, click the “Name” drop down list in the “activate account” section, and then the currently deactivated accounts are listed.
4. Select the deactivated account to be activated and then click **Activate**.



Lockout Setting

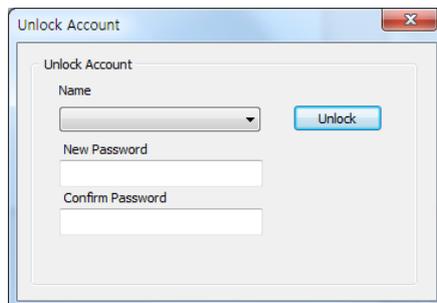
- Use the Lock out setting command to set the number of failed logins, lockout duration and password age.



- Lockout: In executing the UV Express software or signing the measured file, enter the limit number of failed logins. Once locked out, execute the Unlock function and set a new password.
- Lockout duration: Set the time (minutes) when the UV Express software is closed in case that there is no action after it is executed.
- Password age: Set the password expiration (days). Alarm message is displayed from 3 days before the password is expired.

Unlock Account

- Use the Unlock Account command to unlock the user account when user failed logins over setting lockout number and set the new password.
- Procedure
 1. To unlock user account, select user account and enter the new password and click **unlock**.

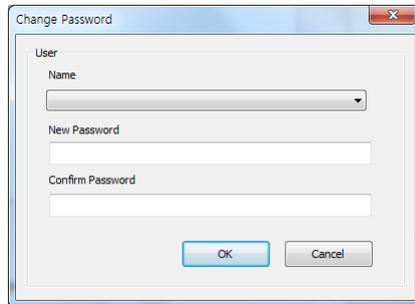


Change Password

- Use the Change Password command to change the user account password.

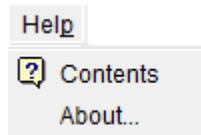
- Procedure

1. To change password, select user account and enter the new password and click **OK**.



2.1.1.2 Help

- The Help menu contains the Help contents for UV Express Software.



Command	Function
Contents	Open the Security Software Guide as PDF file
About...	Display the version of Security Server Software

Contents

- Contents links to external document of the Security Software Guide.

About

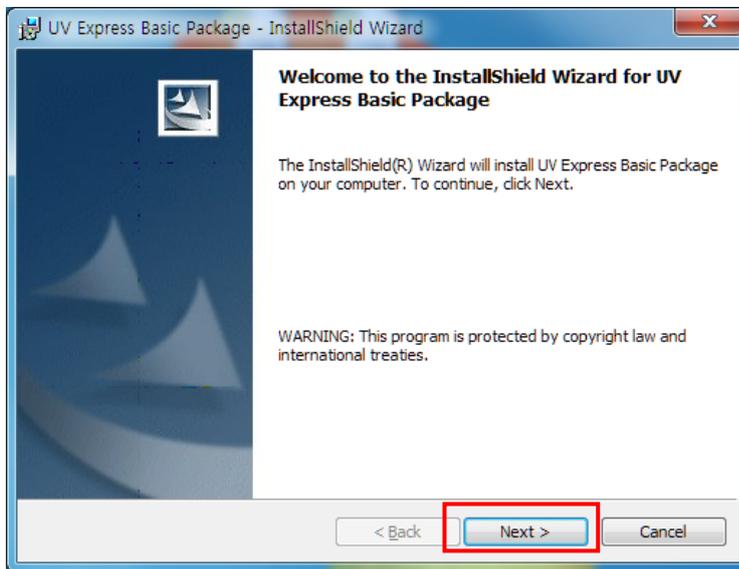
- About Security Server contains information on the version of the software.

2.2 Installation of UV Express and UV Express Security Software

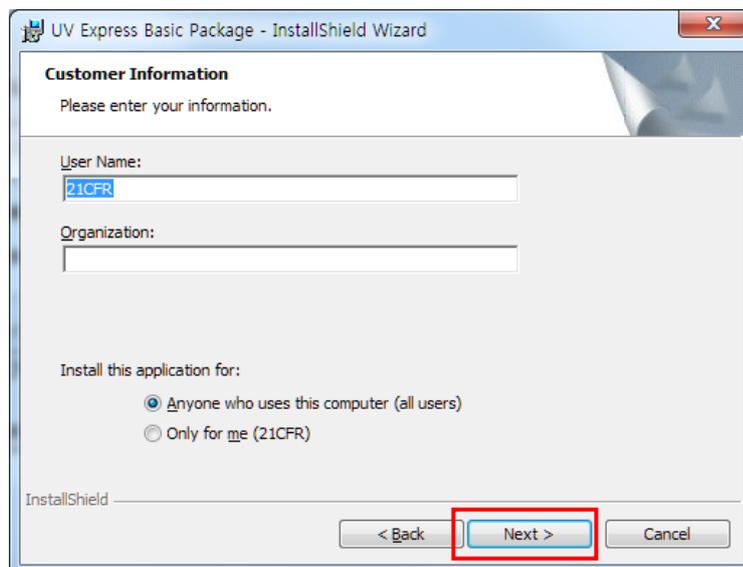
1. Log on as an Administrator account.
2. Input the **UV Express software** CD into the CD drive. UV Express software is installed automatically. The default installation folder is "C:\UV Express".

NOTE: *If UV Express Software has already been installed, please skip the procedures #2-9 and then, UV Express Security software only needs to be installed on the computer.*

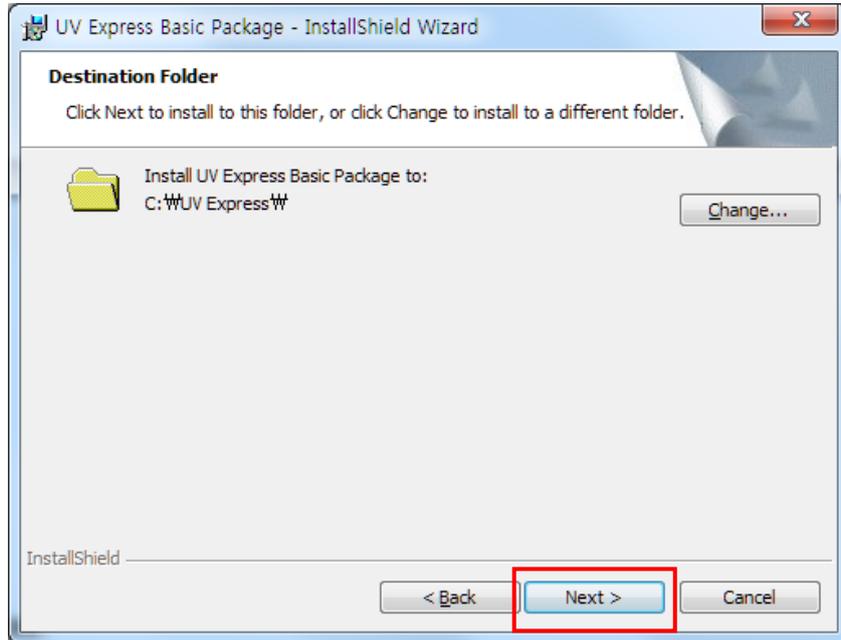
3. If the automatic setup window is not shown, click **Setup.exe** in the CD.
4. UV Express InstallShield® Wizard starts. Click **Next**.



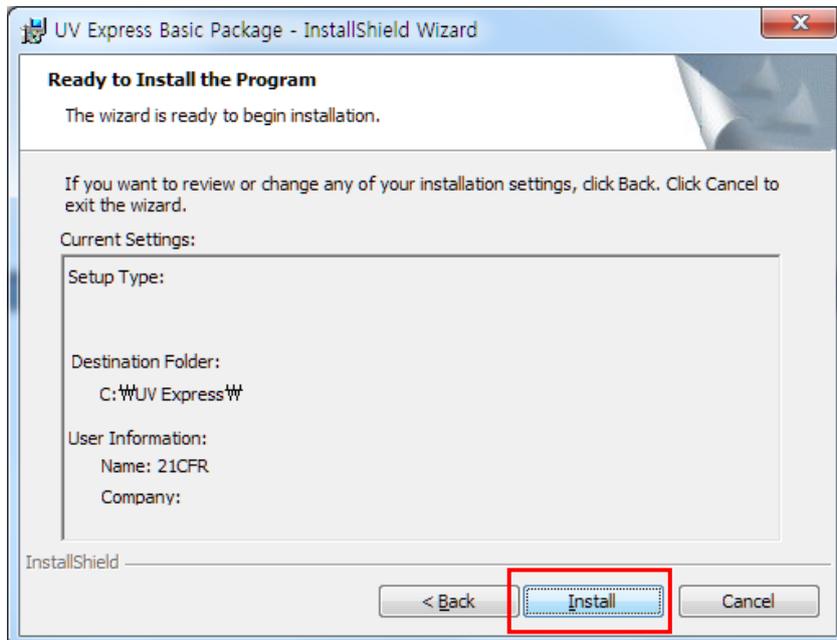
5. Enter your information and click **Next**.



6. Click **Next**.



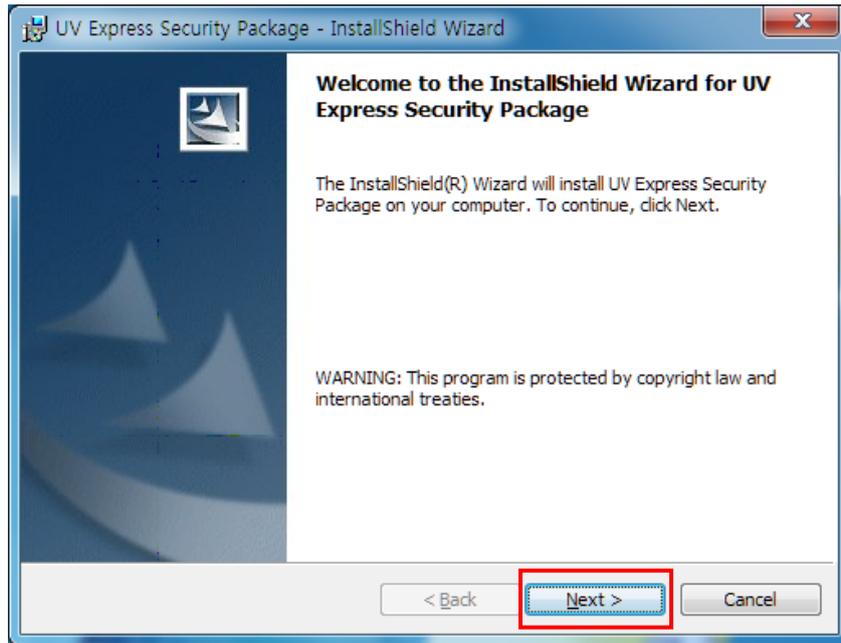
7. Click **Install**.



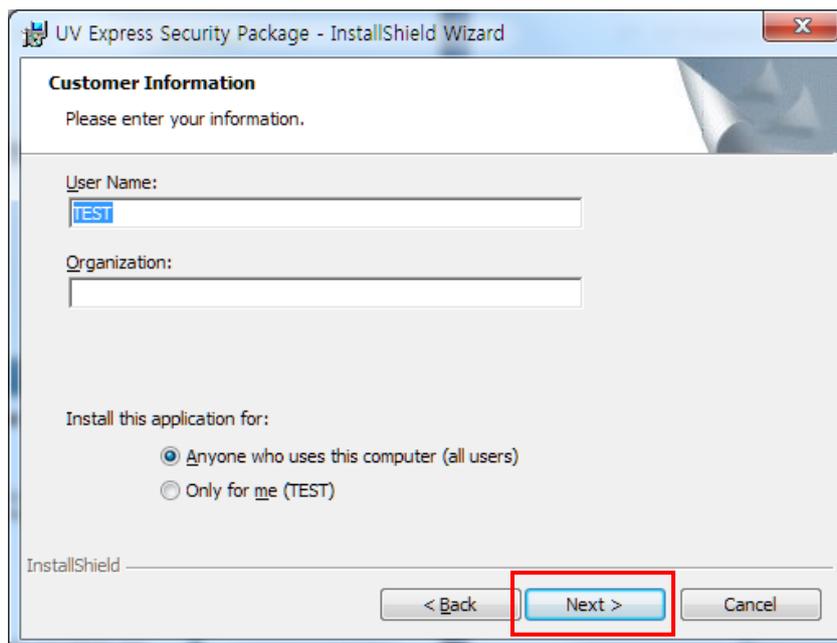
8. After the setup is complete successfully, click **Finish**.
9. After the UV Express Software installation is complete, the UV Express folder will be created on the Desktop.



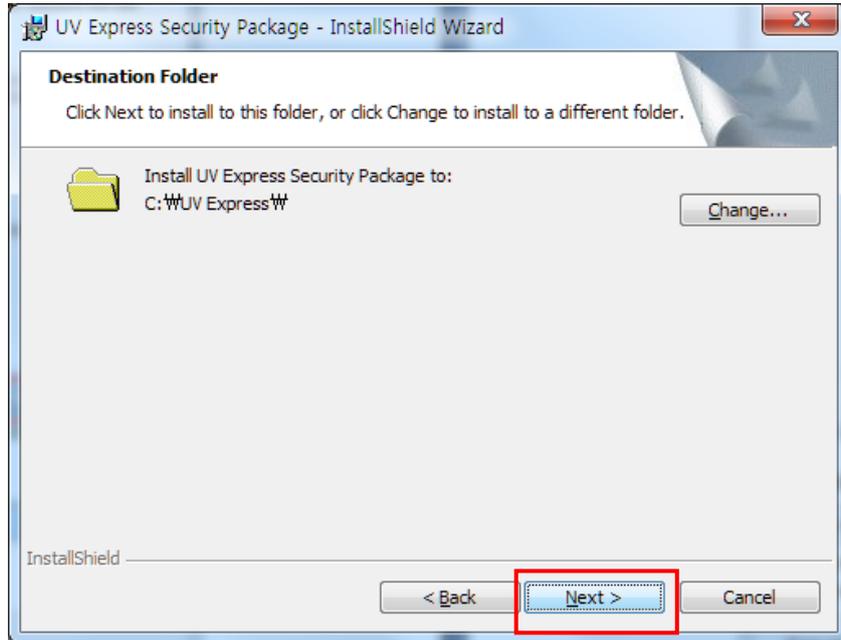
10. Input the **Security software** CD into the CD drive. UV Express Security software is installed automatically. The default installation folder is "C:\UV Express".
11. If the automatic setup window is not shown, click **Setup.exe** in the CD.
12. UV Express Security InstallShield® Wizard starts. Click **Next**.



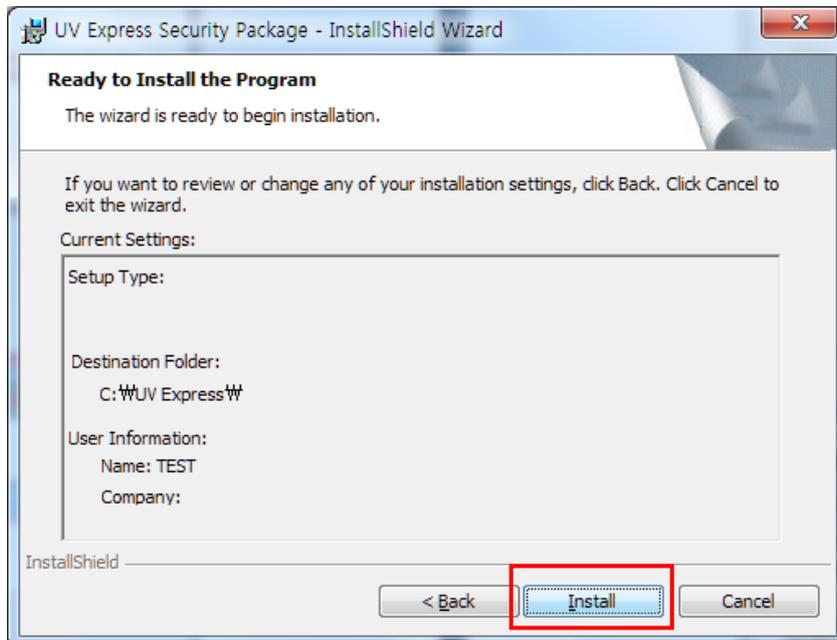
13. Enter your information and click **Next**.



14. Click **Next**.



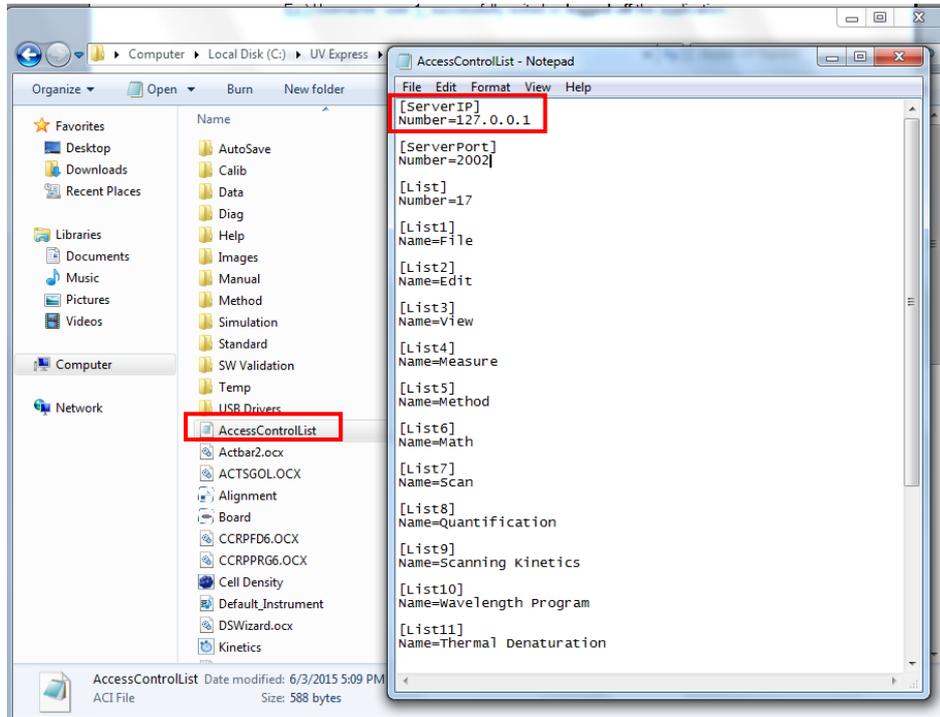
15. Click **Install**.



16. After the setup is complete successfully, click **Finish**.

2.3 Setting IP address

Open the "C:\\" directory, and click the "UV Express" folder. Open AccessControlList.aci file on the notepad and save the modified IP address as 127.0.0.1.



2.4 Folder Permissions

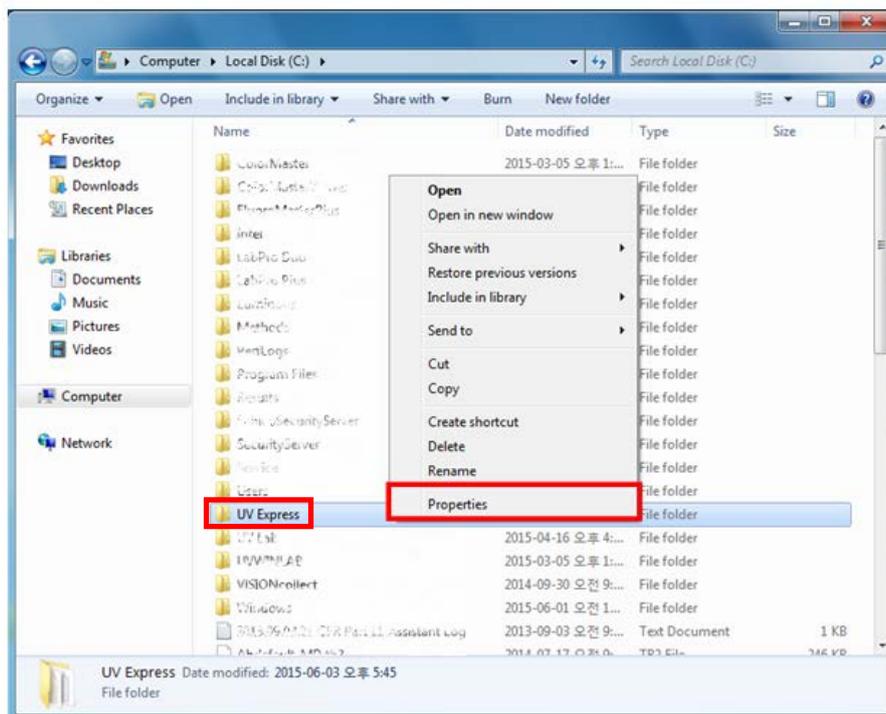
The Administrator account is already present on the PC. This gives the administrator full access to the whole system, including the ability to delete and rename files, and run any application, and change user and file/folder permissions.

In order for data files to be protected, data saved in this protected folder can only be accessed by authorized users. This all permissions of file and folder follow the Windows system's procedural compliance.

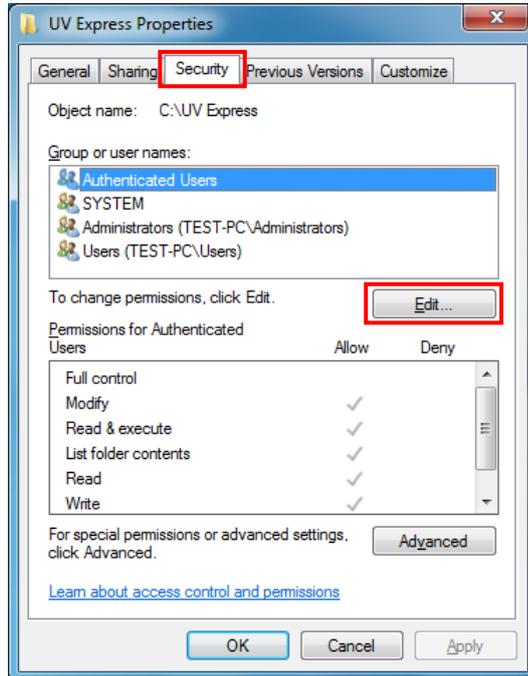
2.4.1 Setting the "Write" permission to the "UV Express" folder

NOTE: *User(s) should be granted the "Write" permission to run the UV Express security software.*

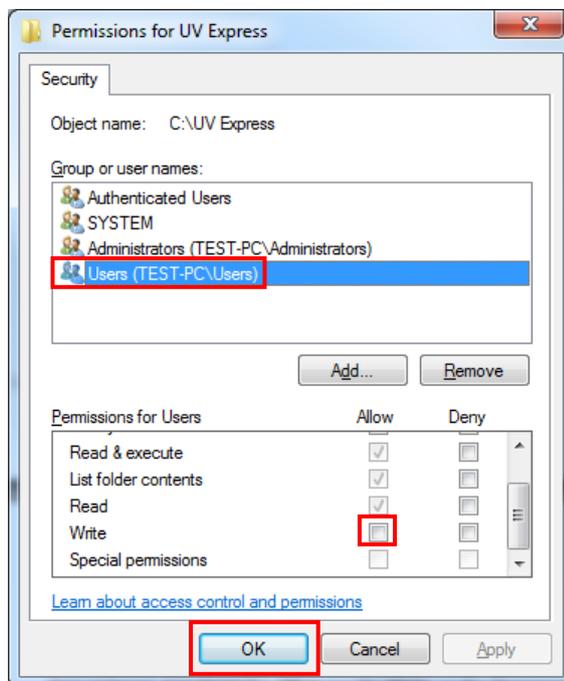
1. Open the "C:\\" directory, and right-click the "UV Express" folder, and then click **Properties**.



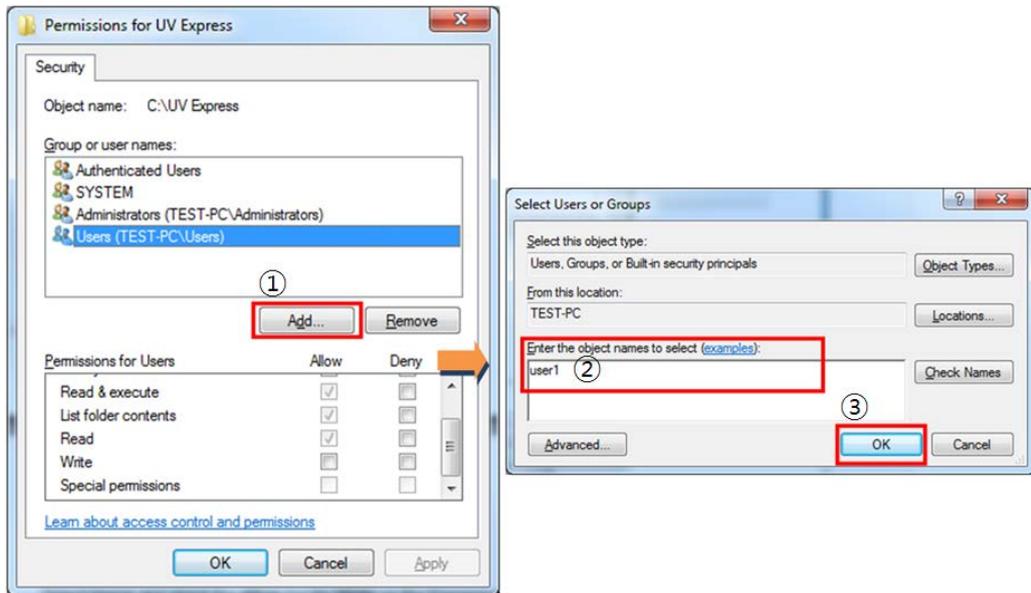
2. Click **"Security"** tab and click **Edit**.



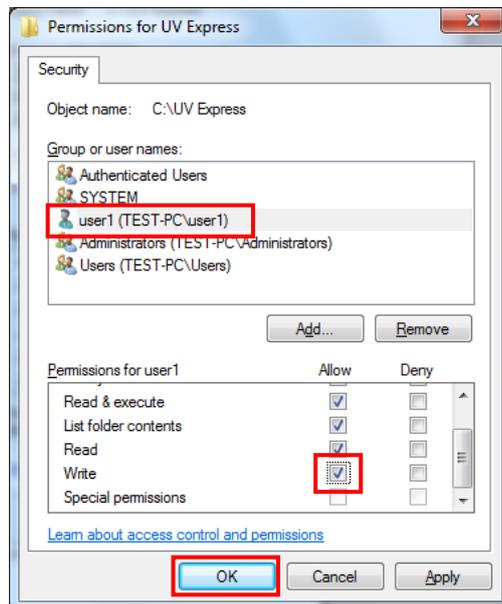
3. Select **Users** and check the **Allow** box for **Write** on the Permissions for Users window and click **OK**.



4. To allow a specific account (e.g. User 1) the write permission, not all **Users**, set as below.



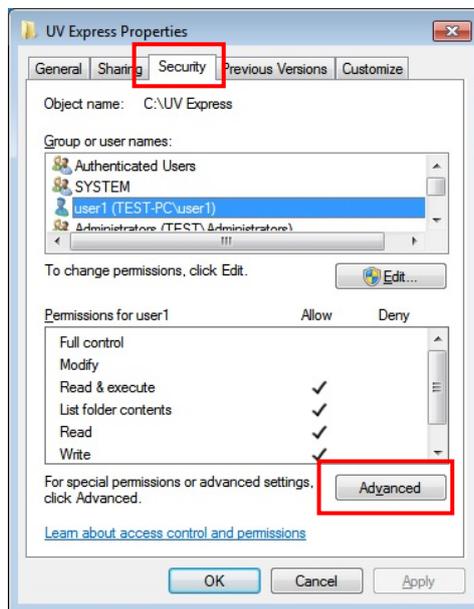
5. Select **user1** and check the **Allow** box for **Write** on the Permissions for user1 window and click **OK**.



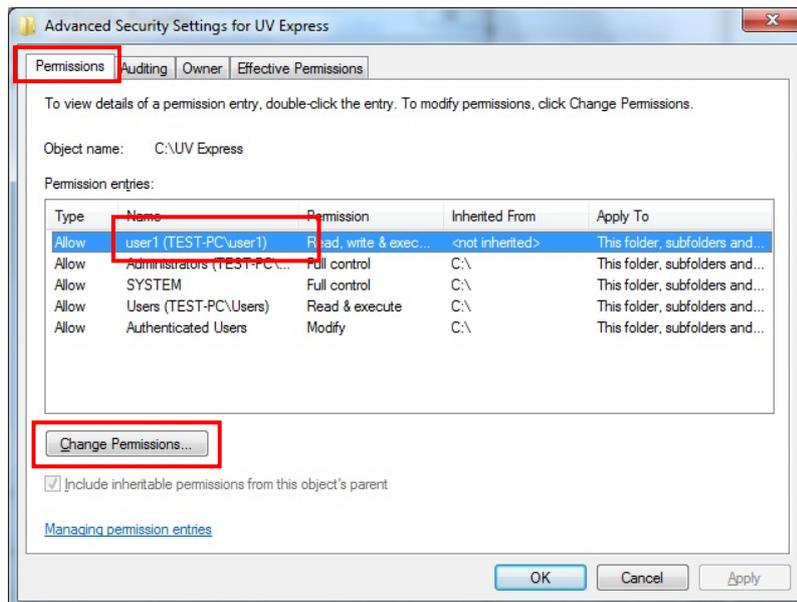
2.4.2 Setting the "Delete and Change" prevention to the "UV Express" folder

NOTE: To prevent user from deleting or changing the UV Express folder (C:\UV Express) and its subfolders and files, the delete permission should be set as **Deny**. It can be set with Administrator's account.

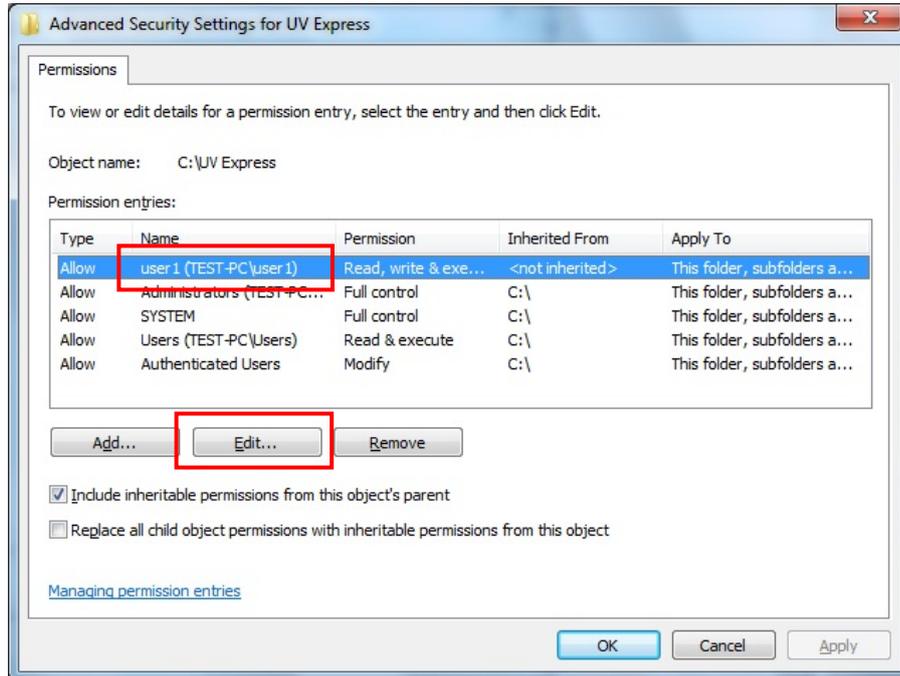
1. Open the "C:\\" directory, and right-click the "**UV Express**" folder, and then click **Properties**.
2. Select **Security** tab in the Properties window and click **Advanced**.



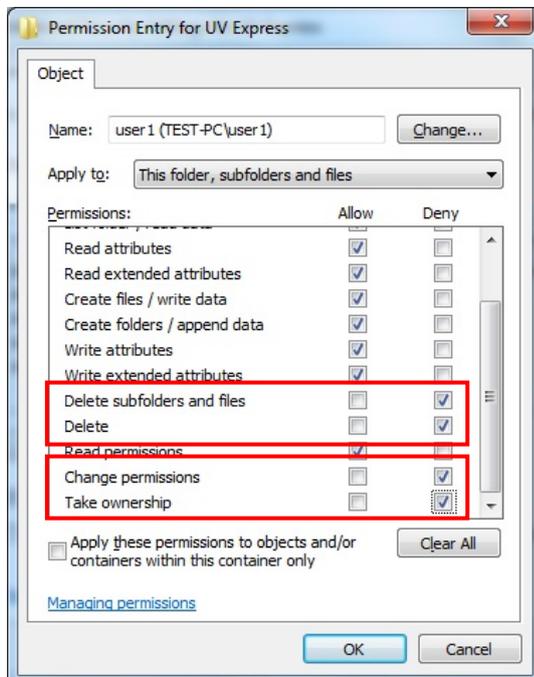
3. Select the **permissions** tab and "**user1**" and click **Change Permissions**.



4. Select "user1" in the permissions window and click **Edit**.



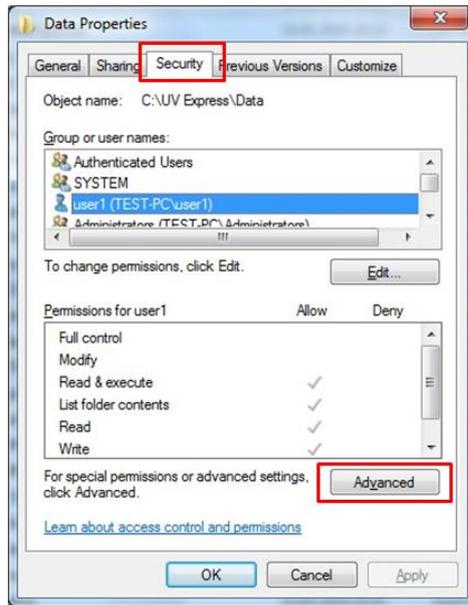
5. Under permissions for **Delete subfolders and files**, **Delete**, **Change permissions** and **Take ownership**, select or check **Deny** and click **OK**.



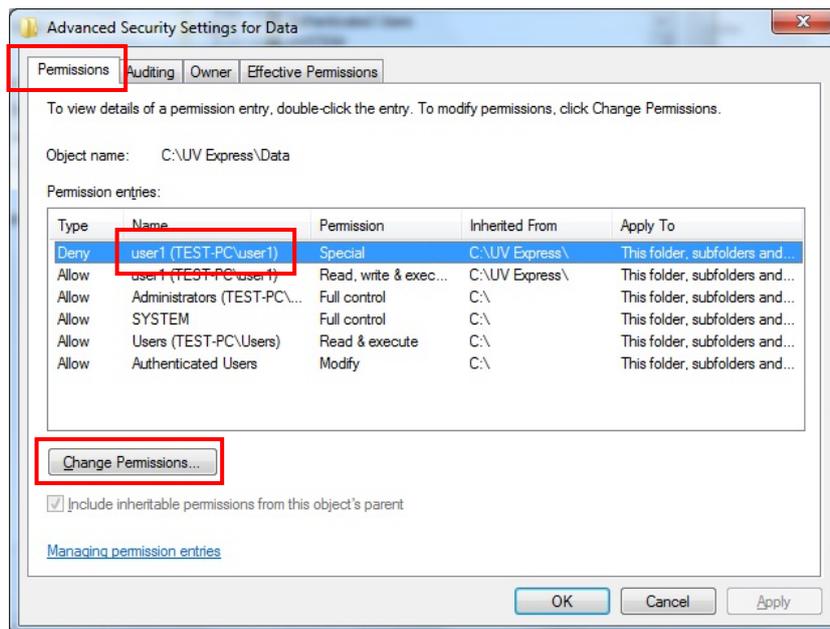
2.4.3 Setting the "Overwrite" prevention to the "Data" folder

NOTE: To prevent user from overwriting data into the Data folder (C:\UV Express\Data), the **Create Folders / append data** permission should be set as **Deny**. It can be set with Administrator's account.

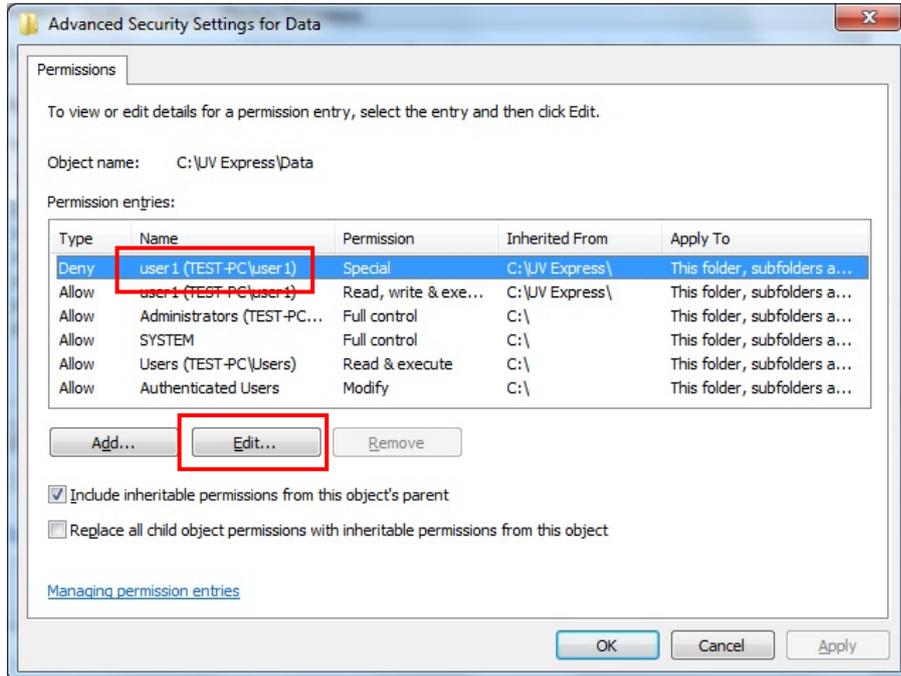
1. With the Administrator's account logged on, open the "C:\ UV Express" directory, and right-click on the "**Data**" folder and then click **Properties**.
2. Select **Security** tab in the properties window and click **Advanced**.



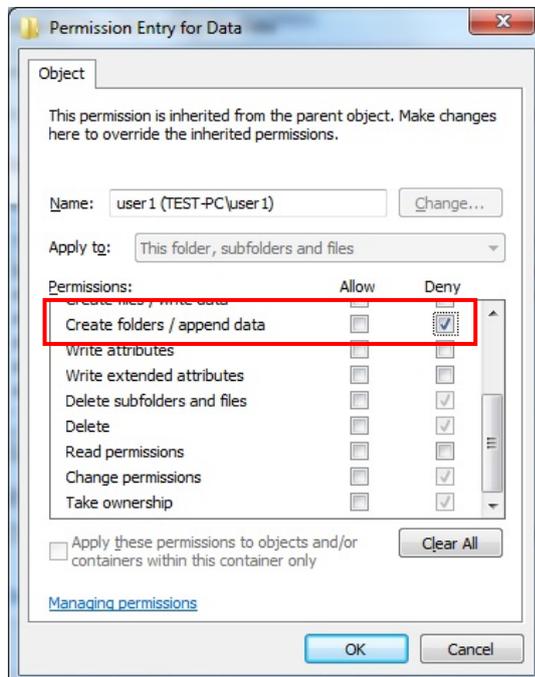
3. Select the **permissions** tab and "**user1**" and click **Change Permissions**.



4. Select "user1" in the permissions window and click **Edit**.



5. Under permissions for **Create folders/ append data**, select or check the **Deny** and click **OK**.



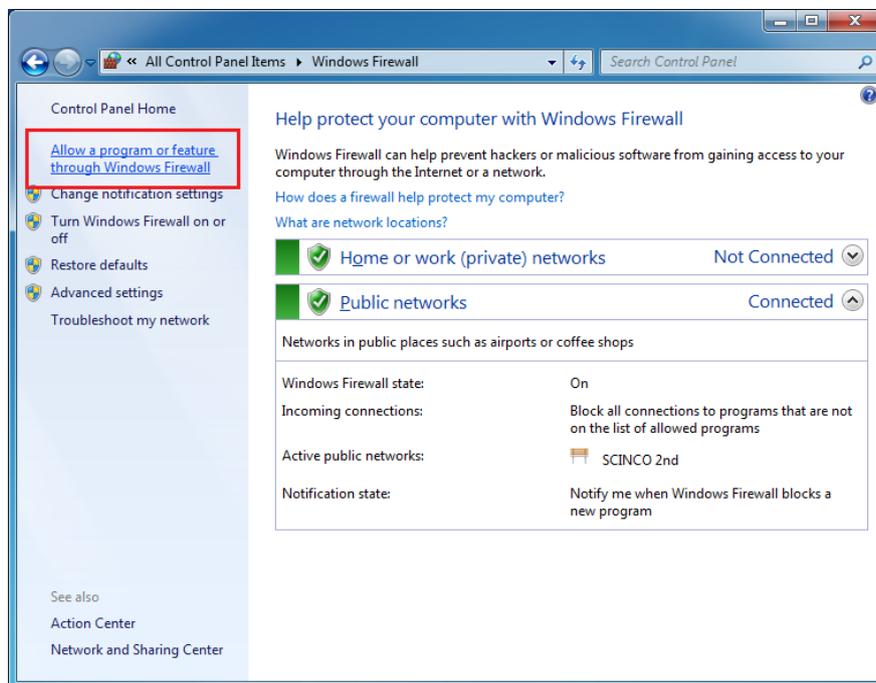
2.5 Setting Windows Firewall

Windows Firewall is a program to prevent malicious software from gaining access to your PC through the Internet or a network. If the windows Firewall programs is turned on and the programs for UV Express Security software are blocked, it should be set to allow the programs to communicate through the Windows Firewall.

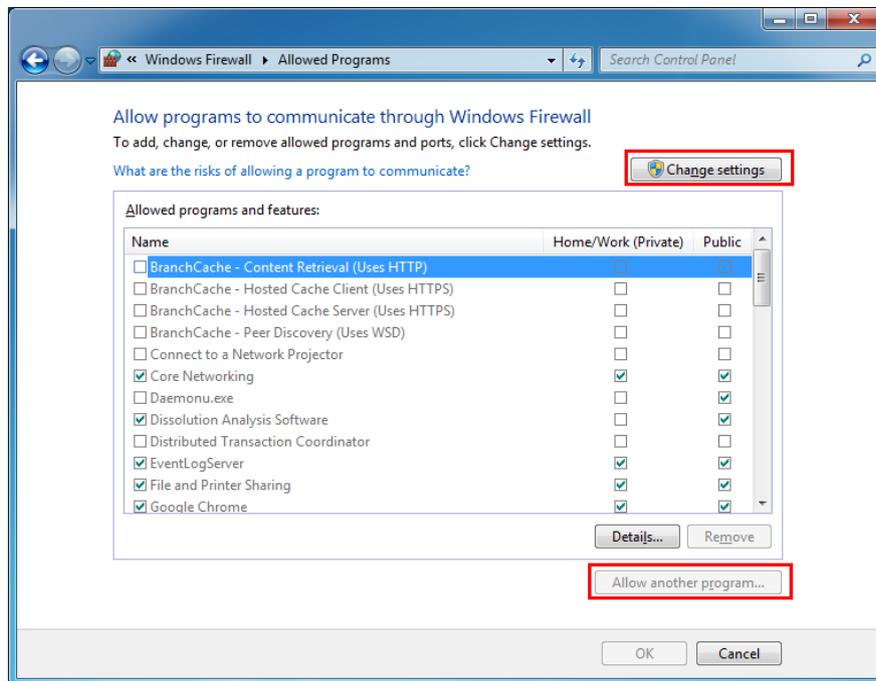
NOTE: *In case that user uses other firewall programs, it should also be set to allow the programs for UV Express Security software to communicate through those firewall programs.*

2.5.1 UV Express access through the Windows Firewall

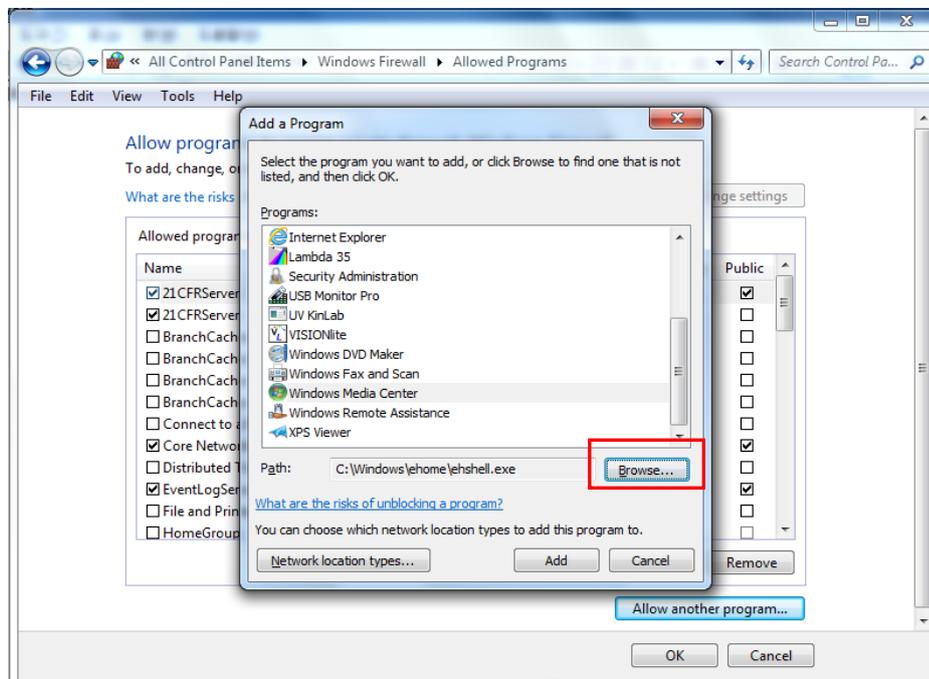
1. Log on as an Administrator account.
2. Select **Control Panel** from the Start menu in the windows operating system. And the click **Windows Firewall**.
3. Click **Allow programs to communicate through Windows Firewall**.



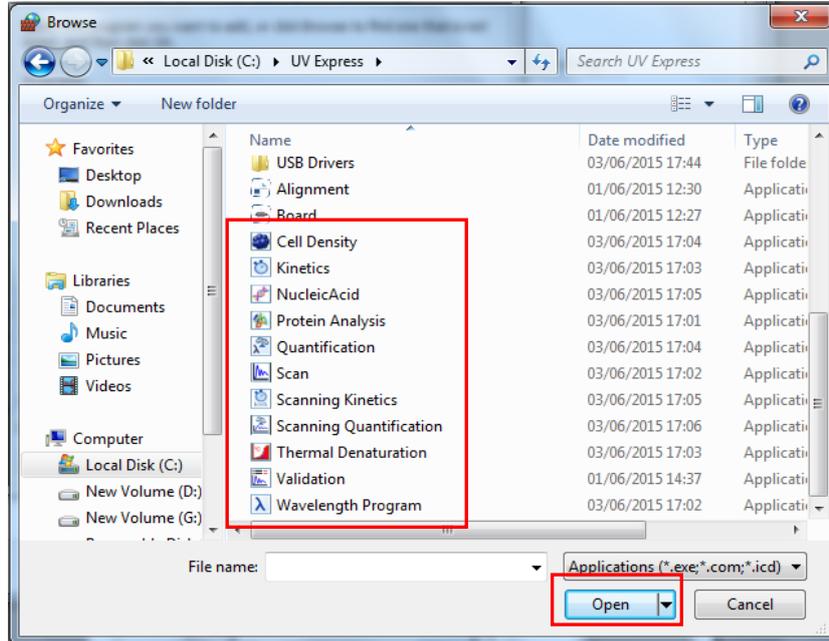
4. Select **“Change settings”** and the **“Allow another program”** button is activated. Click **“Allow another program”**.



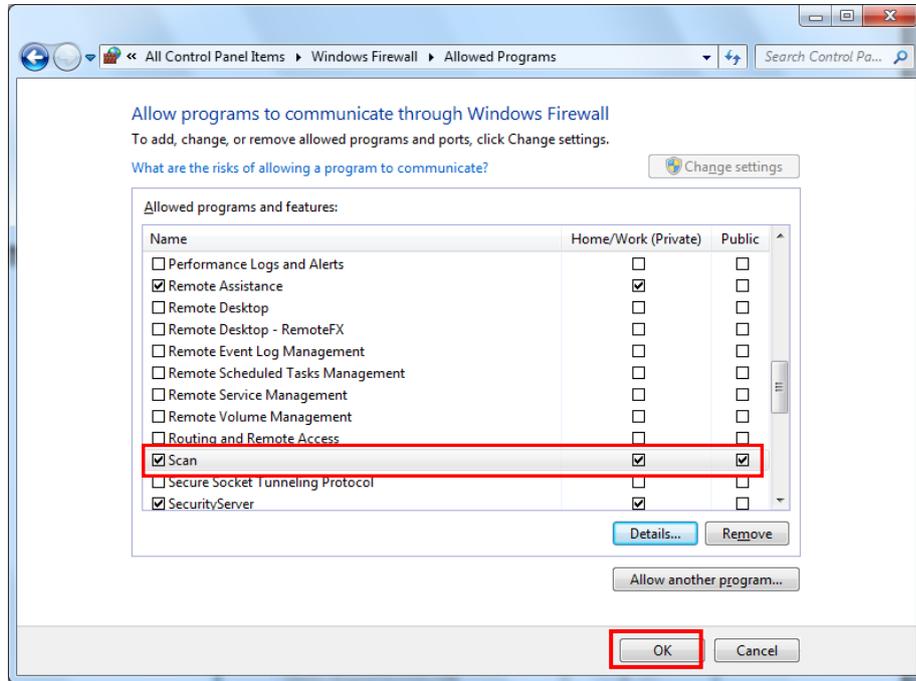
5. Click **Browse...**



- Open all of executable file of UV Express modes.



- After selecting **the entire mode of UV Express** (such as **Scan**) and check **Home/Work (Private)** and **public**, and then click **OK**.



- Set to allow the **Security Server software** to communicate through Windows Firewall following procedures #5~7.

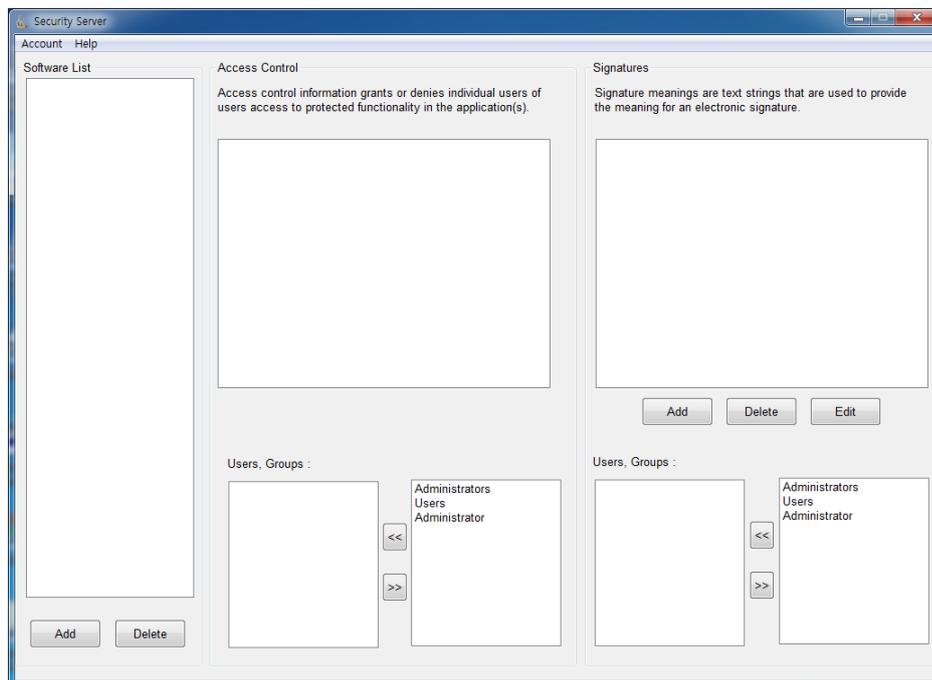
3. Operating Security Server

NOTE: *The user must be logged on as an administrator account of computer in the Local System.*

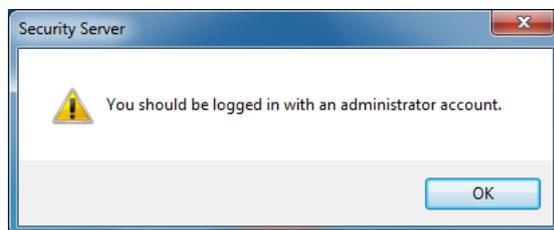
NOTE: *Security Server cannot be executed under the User account because the authority and permission have to be controlled by Administrator only.*



1. Run the **Security Server** software, then Security Server window will appear.

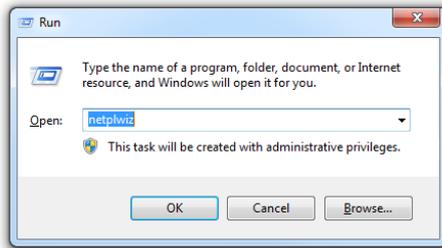


2. In case that the message pops up as below, proceed with the following steps to get the administrator account logged in properly.

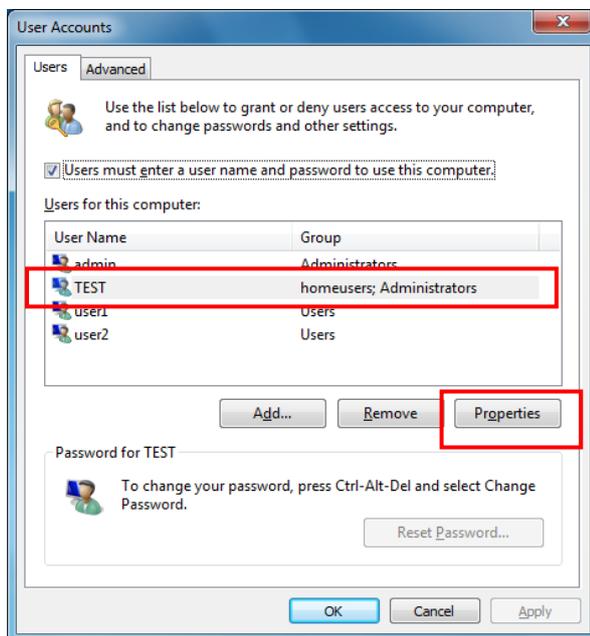


NOTE: *The account has to be grouped in proper type, e.g., Administrator or Standard user (Local account). If the account is involved in unintended group like homeusers, the access to software could be denied.*

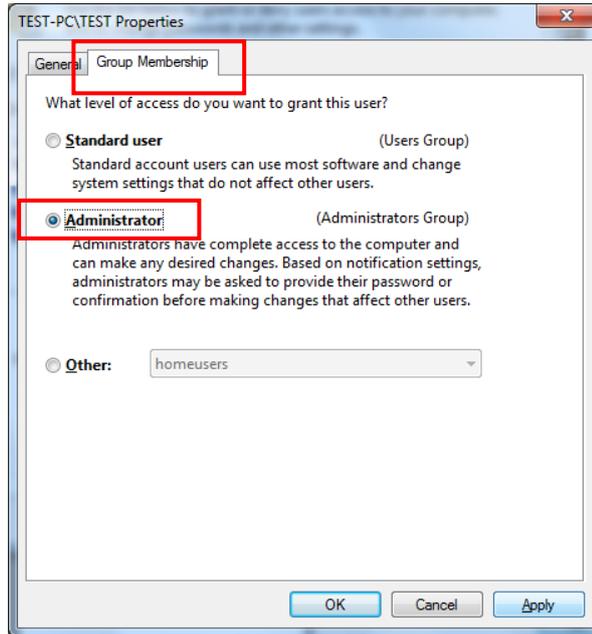
3. Press and hold the "Windows" key and then press the R key to open Run. After writing "netplwiz", click **OK**.



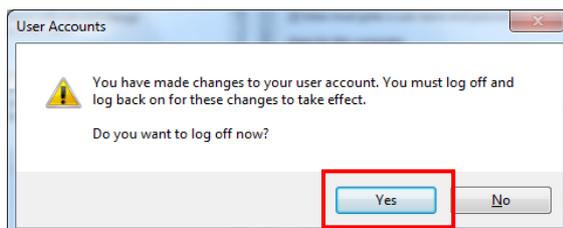
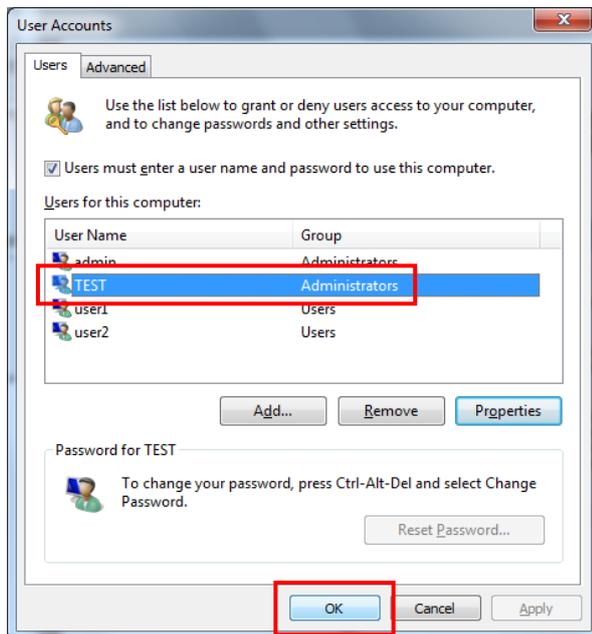
4. If the user is grouped other than Administration, i.e., homeusers, select user and click **Properties**.



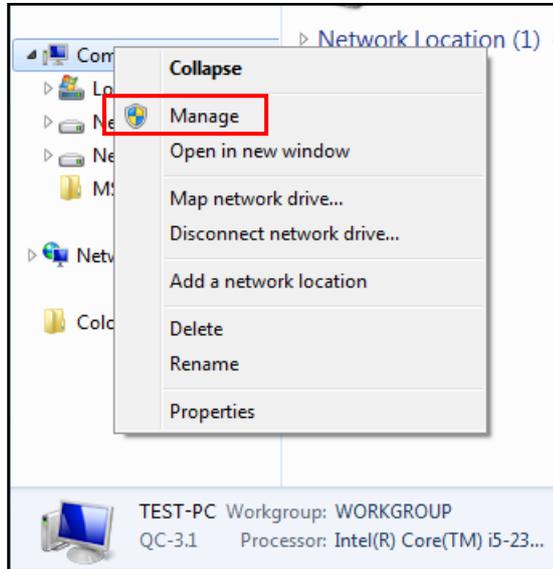
5. Select **Group Membership** and check **Administrator**. Click **Apply** and **OK**.



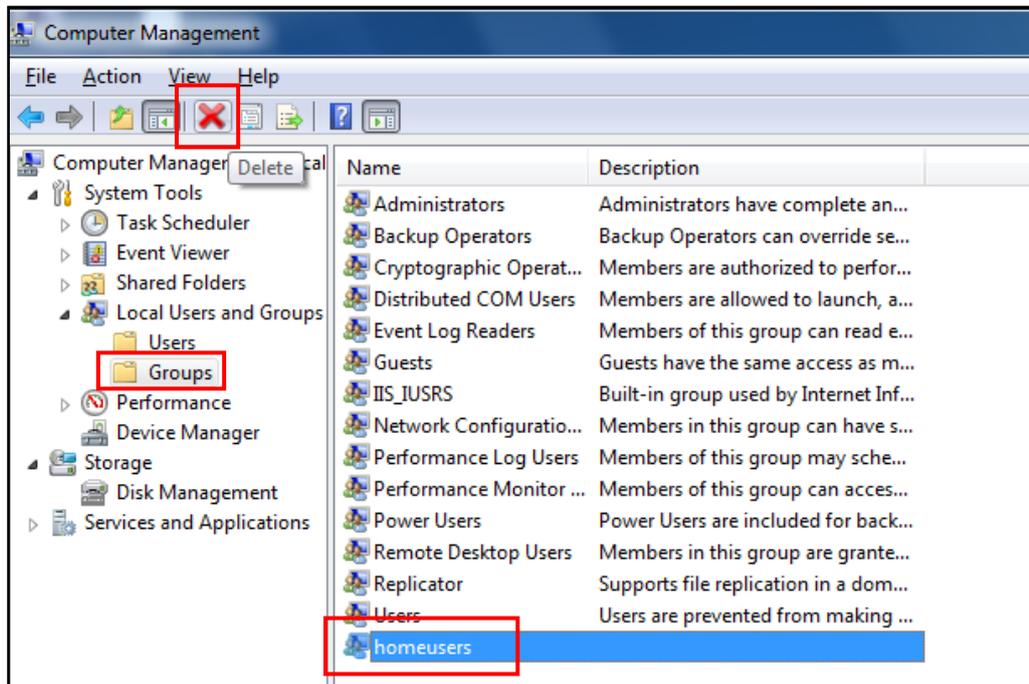
6. Confirm the group is properly modified. After the following message appear, Click **Yes** to restart computer.



7. Despite all that, if accessing to Security Server is still denied, the unwanted group (homeusers) has to be deleted itself. Right-click on **Computer** and then click **Manage**.

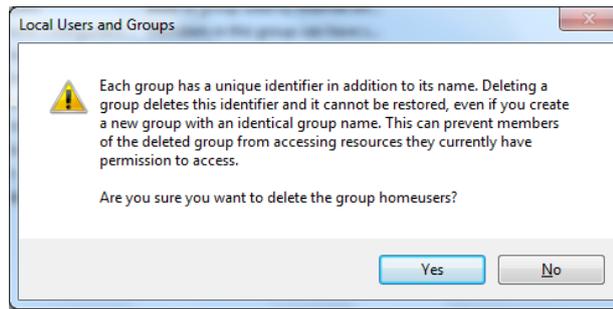


8. Open **Groups** in Local Users and Groups. Select **homeusers** and click **Delete** icon.



9. The following box will appear. Click **Yes** to delete homeusers group.

NOTE: Other functions of windows system could be affected by deleting this homeusers group. Carefully consider the deletion.

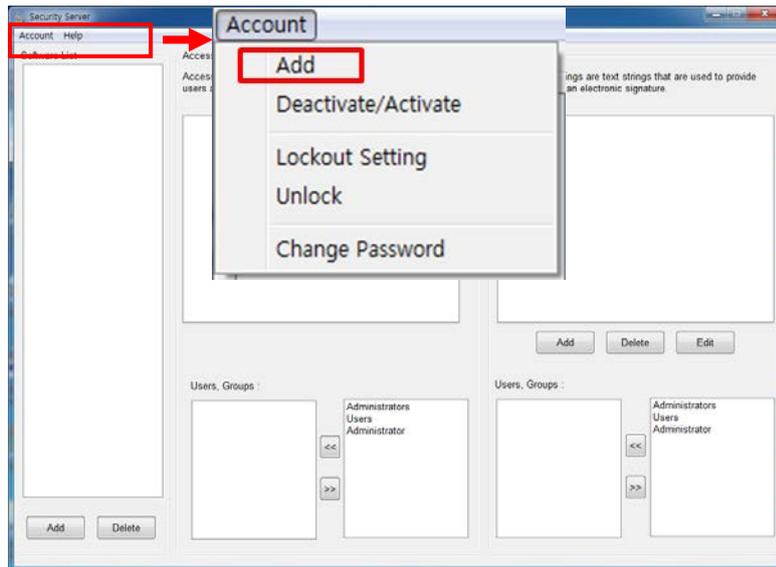


10. Restart the computer and execute the Security Server.

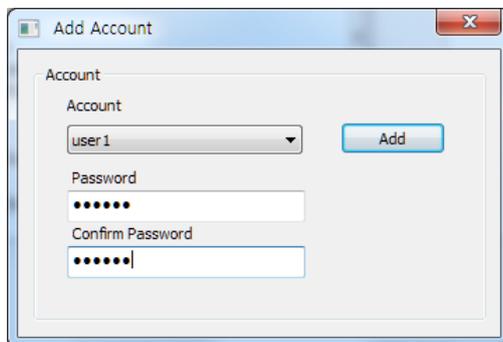
3.1 Set [Account]

To UV Express software, user's account(s) should be added in the Security Server program following the procedures below.

1. Select **Account** of the Security Server window. Click **Add**.



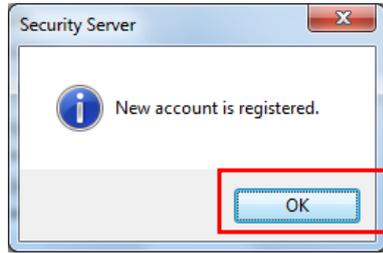
2. As the Add Account window appears, select account and set the password. Click **Add**.



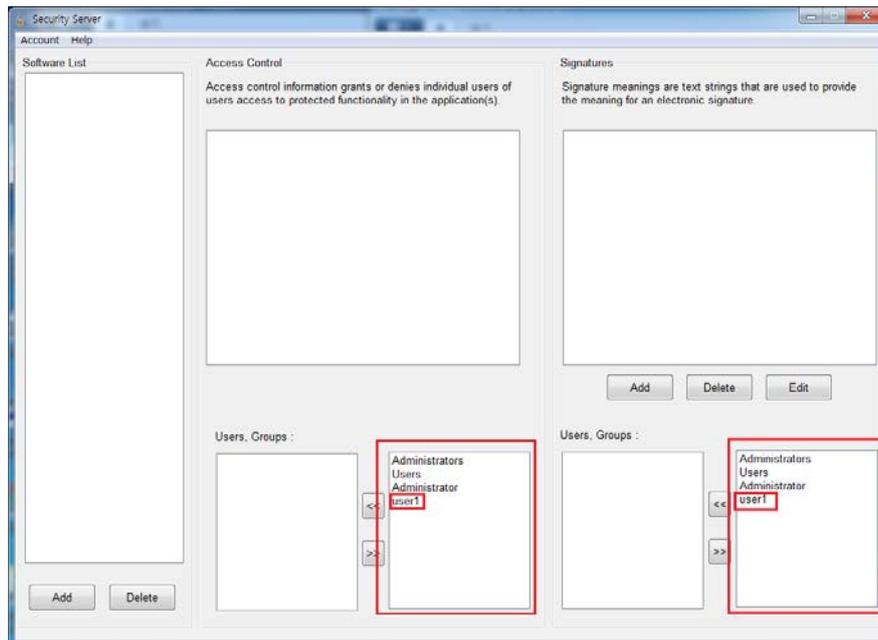
NOTE: Password must be of minimum 6 characters and include at least one letter and a number each.

NOTE: When the new user logs on for the first time, they will be forced to change their password.

3. The following message will appear, and then click **OK**.



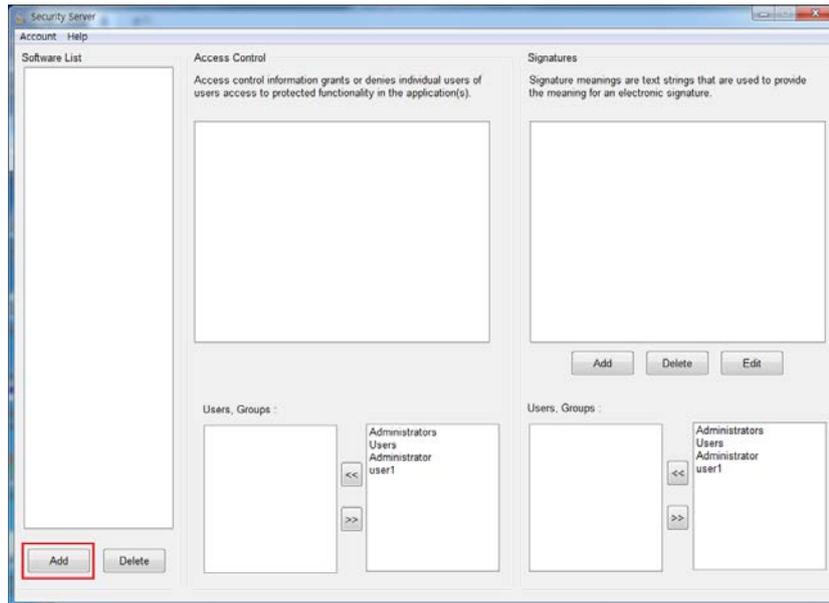
4. Confirm the account was listed on **Users, Groups**.



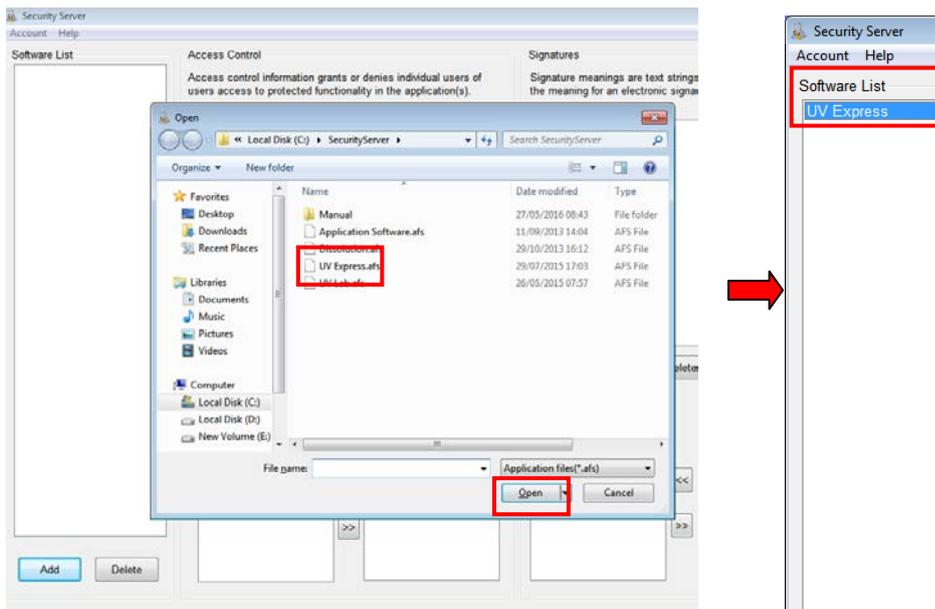
3.2 Set [Software List]

In order to set Access Control for UV Express software functions, the software must be registered on the Software List in advance. Set the Software List as follows.

1. Click **Add** in the Software List section of the Security Server window.



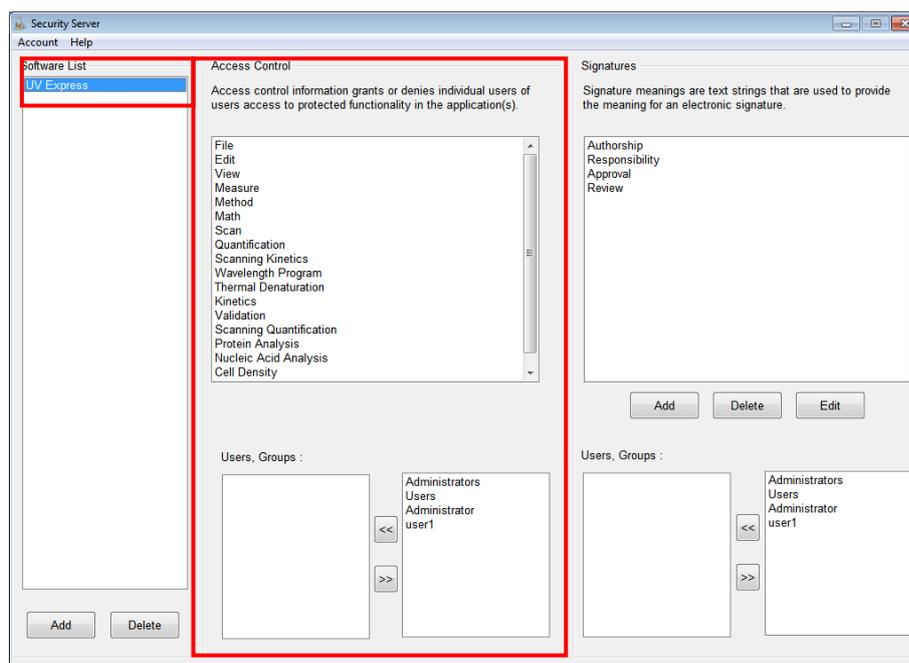
2. As the Open window appears, select **UV Express.afs** and click **Open**. Then, the UV Express will appear in the Software List.



3.3 Set [Access Control]

Access Control assigns users the authority to access various functions in the UV Express software. Set access controls as follows.

1. Click on the **UV Express** in the Software List. And then items are displayed in each section.



Each 'function' corresponds to a menu item in the main menu of the UV Express software or a specific command. See the UV Express software Users Guide for more details.

File : Allows user to access each command in the File menu.

Edit : Allows user to access each command in the Edit menu.

View : Allows user to access each command in the View menu.

Measure : Allows user to access each command in the Measure menu.

Method : Allows user to access each command in the Method menu.

Math : Allows user to access each command in the Math menu.

Scan : Allows user to access Scan mode executable program.

Quantification : Allows user to access Quantification mode executable program.

Scanning Kinetics : Allows user to access Scanning Kinetics mode executable program.

Wavelength Program : Allows user to access Wavelength Program mode

executable program.

Thermal Denaturation : Allows user to access Thermal Denaturation mode executable program.

Kinetics : Allows user to access Kinetics mode executable program.

Validation : Allows user to access Validation functions. Validation Software is optional.

Scanning Quantification : Allows user to access Scanning Quantification mode executable program.

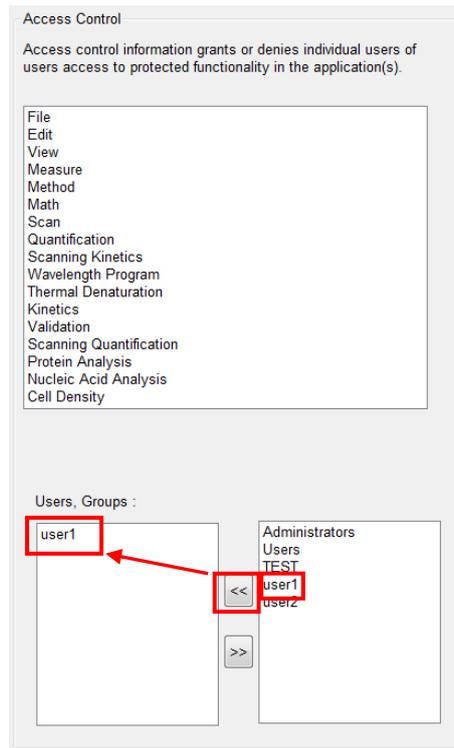
Protein Analysis : Allows user to access Protein Analysis mode executable program.

Nucleic Acid Analysis : Allows user to access Nucleic Acid Analysis mode executable program.

Cell Density : Allows user to access Cell Density mode executable program.

Multicomponent Analysis : Allows user to access Multicomponent Analysis mode executable program.

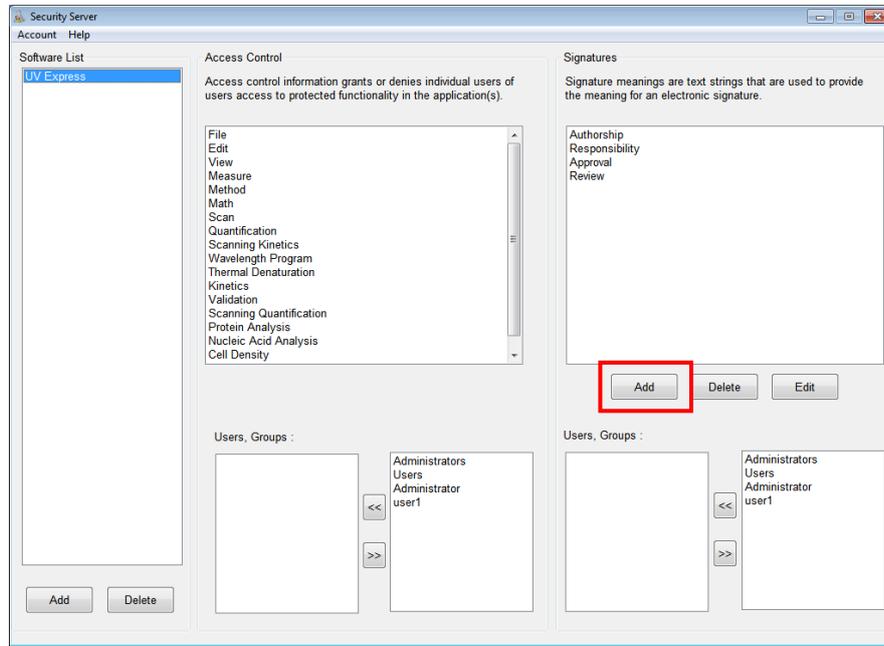
2. Select the user account(s) to be given the access permission to each and click .



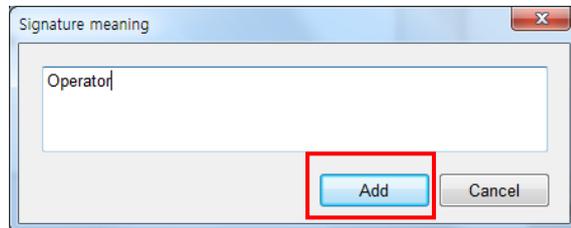
3.4 Set [Signature Meanings]

Set the signature meanings for users as follows.

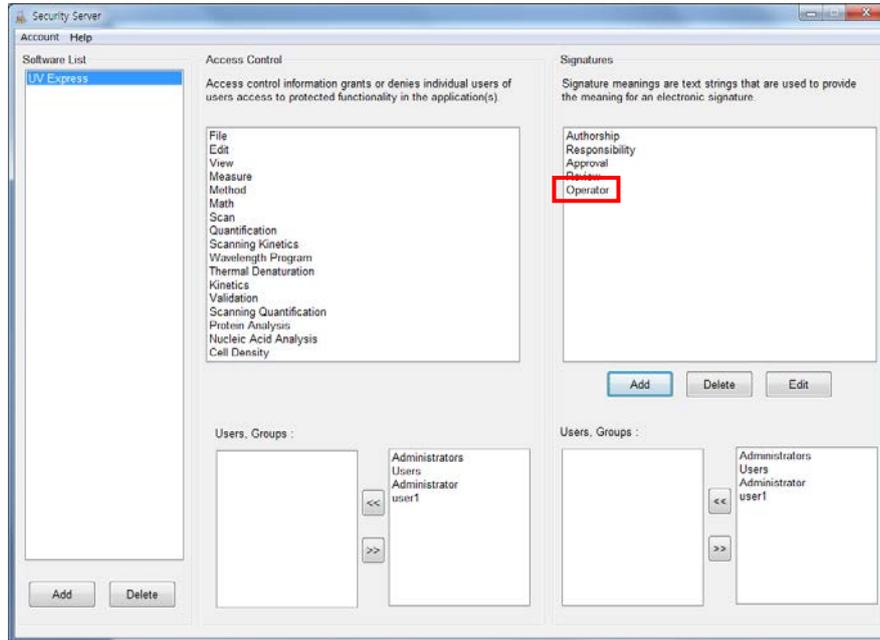
1. To create a new signature, click **Add** in the Security Server window.



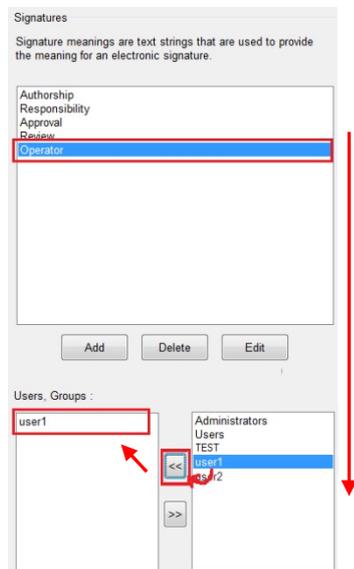
2. Enter the name for the new signature meaning and click **Add**.



3. The created signature meaning is shown in the Security Server window.



4. Users for each signature are listed in the "Users, Groups" section. Select a signature and select users who will have the authority to apply the selected signature using << , >> in the Users, Groups section.



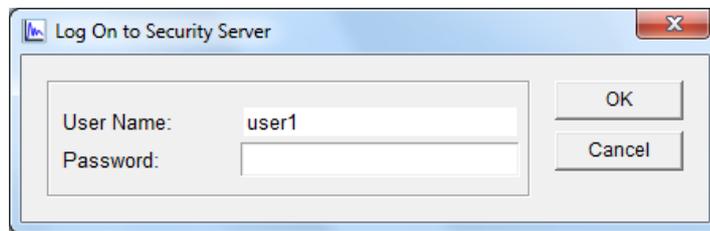
4. Operating UV Express Software

4.1 Operating UV Express Software

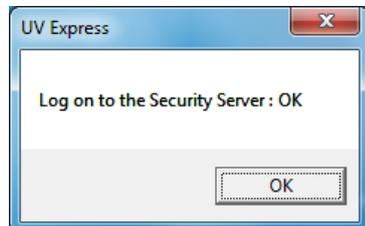
1. Log on to a client computer as a **Standard user account**.

NOTE: *UV Express software cannot be executed under a Windows "Computer Administrator" account because the administrator account has the authority to modify and delete data.*

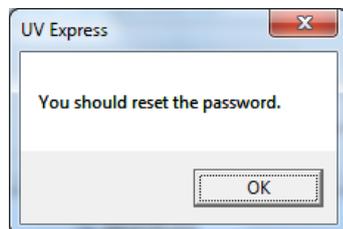
2. Execute one of the measurement modes of UV Express software, and then 'Log on to Security Server' message will appear. Enter the registered User Name and Password of the account and click **OK**.



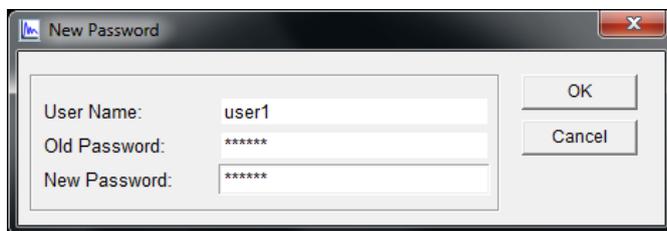
3. If the password is correct, the following message will appear, and then click **OK**.



4. If the log on is the first time, the password has to be reset which has to be differed from given password by administrator.



5. Enter the old password on the old password (assigned password by administrator) and a new password, and then click **OK**.

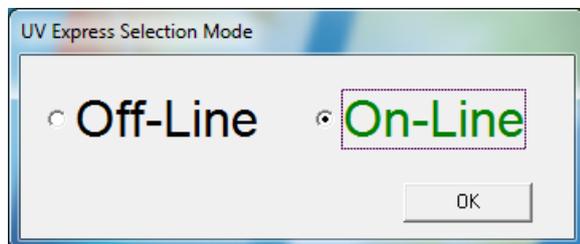


NOTE: Password must be of minimum 6 characters and include at least one letter and a number each.

6. Click **OK**.



7. Log on again with the changed password. If the instrument is connected and ready to measure, click **On-Line** or **Off-Line**.



8. A user's access to each menu is determined by the privileges given to each user account. In the following example, user1 was given access to log on and execute the **Scan** mode of UV Express software with the file, method, measure and signature menu.
9. Open an existing sample data or measure the sample. Save a data.

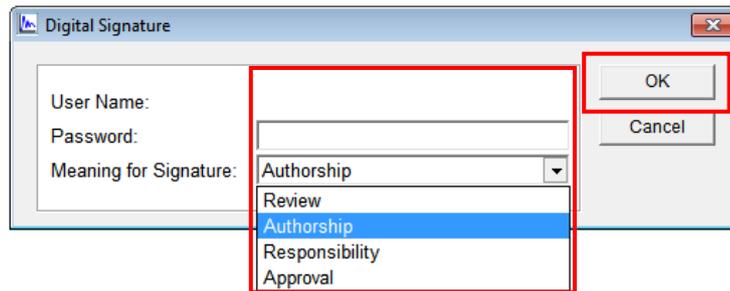
NOTE: If the data is not saved, signatures cannot be applied. Ensure that data is saved first.

NOTE: Data must be saved in a folder which the user has been granted the access to.

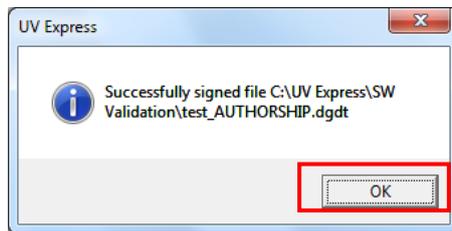
10. Apply a signature to measured or archived data by clicking **Current File** on the window.



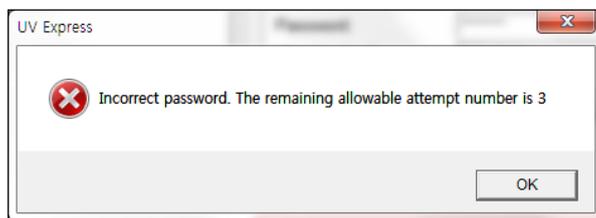
11. In the Digital Signature dialog box, enter the User Name and Password, select the signature meaning, and click **OK**.



12. After the Signature is complete, the following message will appear, and then click **OK**.

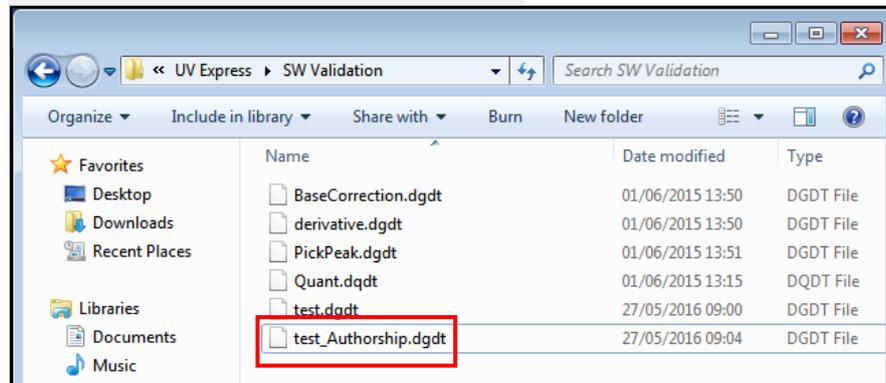


NOTE: If you enter any incorrect password, the below message will appear. Your account is locked out when you exceed the limit number of failed logins and it can be unlocked by setting a new password by the administrator.



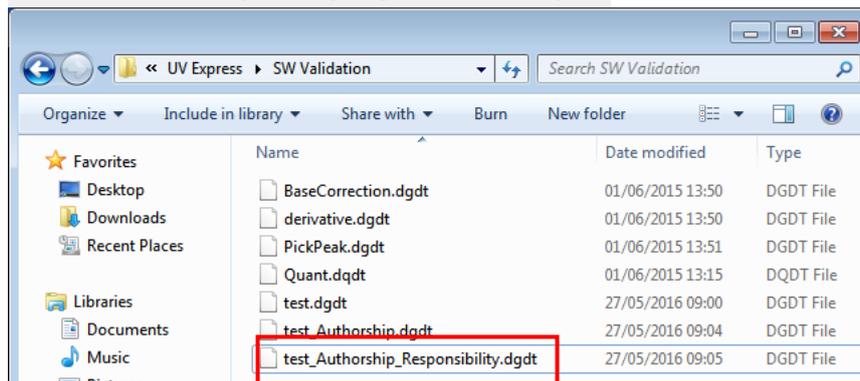
13. The signature record is shown in the main window and the signed data is saved as a new file.

Current File: user1, Authorship, May 27 2016 09:49:00 (GMT -8:00)



14. If the second signature is applied to the data file, it is saved as a new file again as shown below.

Current File: user1, Responsibility, May 27 2016 09:49:33 (GMT



15. Click **Print** to view the saved data using a printed report as shown below.

4.2 Changing Methods

If the Method is changed or data is modified in the signed file, user has to enter the User Name and Password to change methods. After typing the reason, click **OK** to save the changed data. The method change history could be checked in the print window.

NOTE: *Be sure that if the method or data is modified, the data is needed to be saved and signed again.*

Log On to Change the Experimental Parameter

User Name:

Password:

Reason:

OK

Cancel

[Y Unit]
Old: Absorbance, New: Transmittance
[Wavelength (nm)]
Old: 440, 465, 546, 1, 590, 635
New: 465, 546, 1, 590, 635

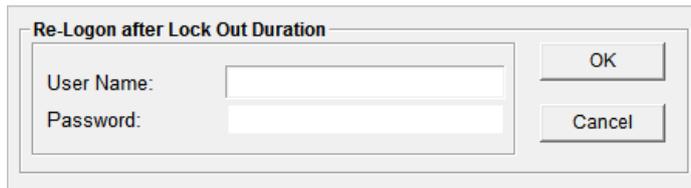
Method History

Method Change Date: 09-03-2015 14:37:57 (GMT +9:00)
Method Change Operator: user1
Method Change Reason: test
Changed Method Applied to File: Untitled-1
Method Change Contents:
[SBW (nm)]
Old: 1.0, New : 0.5
[Y Unit]
Old: Absorbance, New : Transmittance

Method Change Date: 09-03-2015 14:38:11 (GMT +9:00)
Method Change Operator: user1
Method Change Reason: test2
Changed Method Applied to File: Untitled-1
Method Change Contents:
[Internal Reference Use]
Old: No, New : Yes
[Internal Reference Type]
Old: Single Point, New : Single Point
[Internal Reference Wave.]
Old: 1100., New : 550

4.3 Lockout for unattended operation

This function is performing automatic lockout after some set time of inactivity. The automatic lockout time (Lockout duration) is set in the security server software by the administrator. If there is no action in the set time after the UV Express security software is executed, it is locked out and the following message will appear. Enter the User Name and Password to unlock the UV Express security software again.

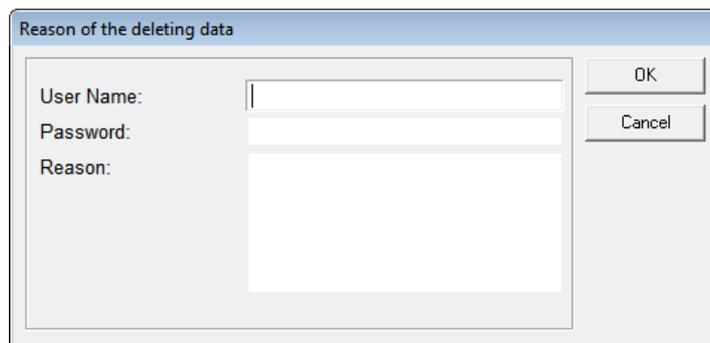


A dialog box titled "Re-Login after Lock Out Duration". It contains two input fields: "User Name:" and "Password:". To the right of these fields are two buttons: "OK" and "Cancel".

NOTE: *Your account is locked out when you exceed the limit number of failed logins and it can be unlocked by setting a new password by the administrator.*

4.4 Deleting Spectra

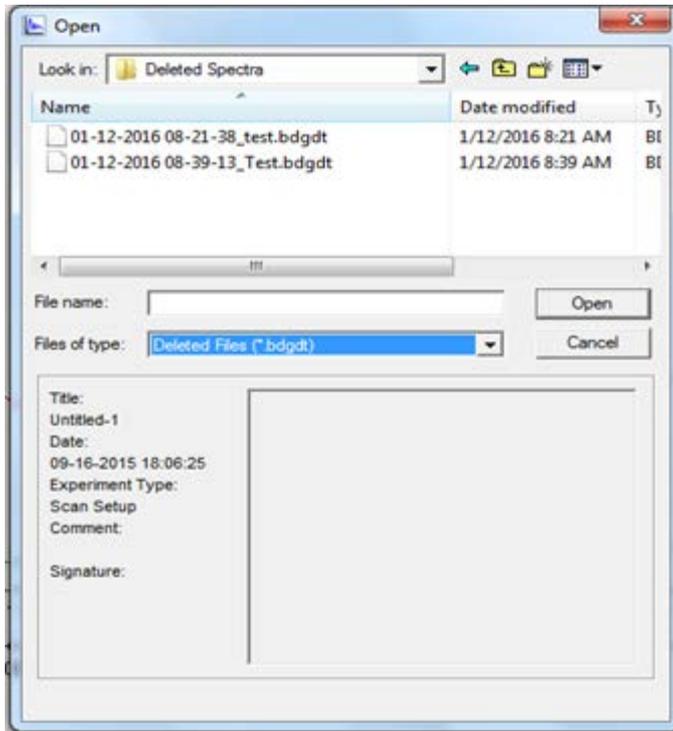
If a user deletes an acquired spectrum from the sample measurement result, it is mandatory to enter the User Name and Password in the 'Reason of the deleting data' message box. Deleted data is stored in the 'Deleted Spectra' folder. (C:\UV Express\Deleted Spectra).



A dialog box titled "Reason of the deleting data". It contains three input fields: "User Name:", "Password:", and "Reason:". To the right of these fields are two buttons: "OK" and "Cancel".

4.5 Retrieve the deleted spectra

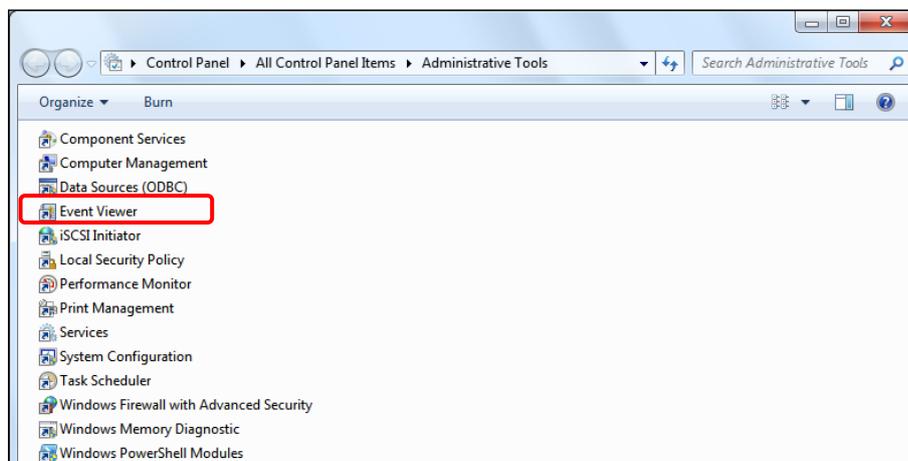
1. In order to retrieve and re-analyze the deleted spectrum in the UV Express security software, click **Open** in the menu and select the deleted file [* .b+ file extension (e.g. *.bdgdt)] in the **'Deleted Spectra'** folder.



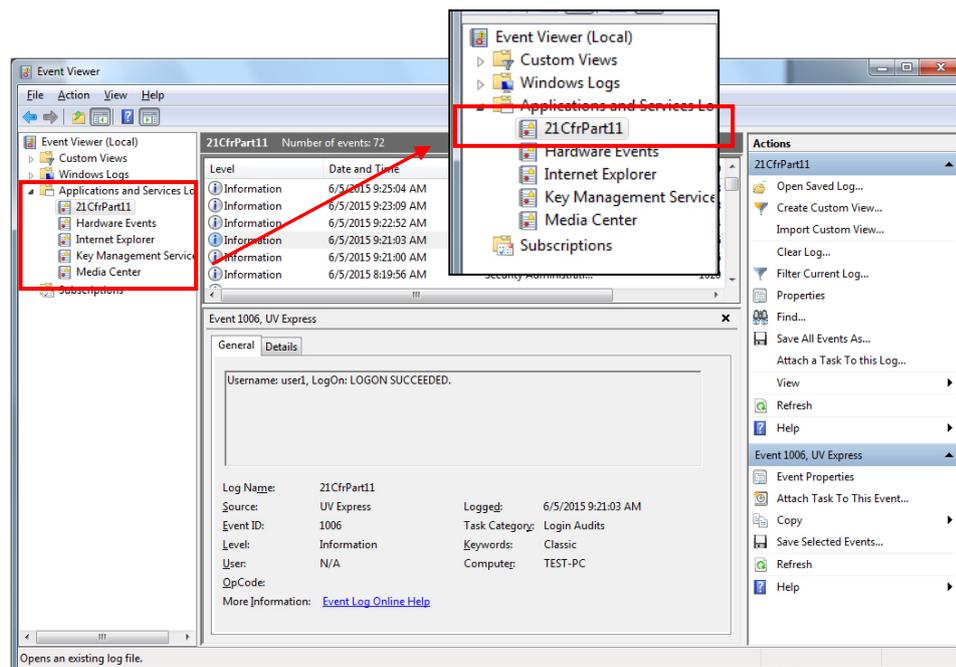
5. Event Log

The Logs of Changes are displayed in the Windows Event Viewer to trace the history of all setup changes in the Security Server and UV Express Security software.

1. Click **Start > Control Panel**.
2. Open **Administrative Tools > Event Viewer**.



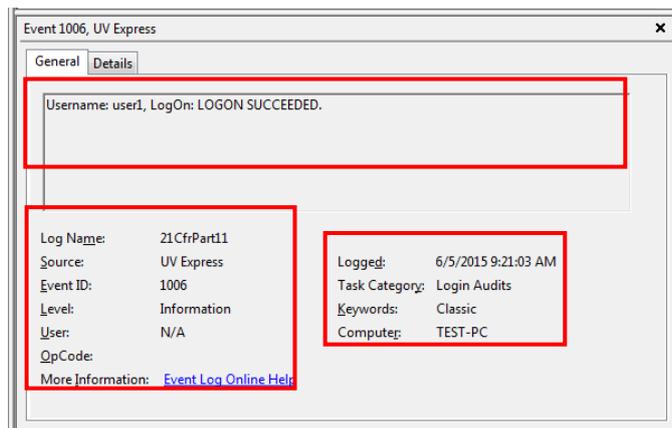
3. The Event View contents are displayed. Expand the **Applications and Services Logs** folder, and then select **21cfrPart11**.



4. The event logs of the windows applications related to the UV Express Security Software are listed in the 21CfrPart11 section. Select a particular event log in the list.

Level	Date and Time	Source
Information	6/5/2015 9:25:04 AM	UV Express
Information	6/5/2015 9:23:09 AM	UV Express
Information	6/5/2015 9:22:52 AM	UV Express
Information	6/5/2015 9:21:03 AM	UV Express
Information	6/5/2015 9:21:00 AM	UV Express
Information	6/5/2015 8:19:56 AM	Security Administrati...
Information	6/5/2015 8:19:46 AM	Security Administrati...
Information	6/5/2015 8:19:04 AM	Security Administrati...
Information	6/5/2015 8:18:53 AM	Security Administrati...

5. You can see more detailed information (Username, software, event, date, time, etc.). Some of types of the events are described as follows.



a) Description of Security Server

Account and Permission modified : Change the account settings.

- Ex.1) Username: Administrator. Added "UV Express" to Application Software.
- Ex.2) Username: Administrator. Deleted "UV Express" from Application Software.
- Ex.3) Username: Administrator. Changed the Lockout Setting.
- Ex.4) Username: Administrator. Changed the password : "user1".
- Ex.5) Username: Administrator. Added "user1: in the users list.
- Ex.6) Username: Administrator. Deactivated the user account: "user1".
- Ex.7) Username: Administrator. Activated the user account: "user1".
- Ex.8) Username: Administrator. Unlocked : "user1".
- Ex.9) Username: Administrator. Added "user1" to "Review" Signature Permission.
- Ex.10) Username: Administrator. Deleted "user1" from "Review" Signature Permission.
- Ex.11) Username: Administrator. Added "user1" to "Wavelength Program" Access Permission.
- Ex.12) Username: Administrator. Deleted "user1" from "Wavelength Program" Access Permission.

b) Description of UV Express

Performance : Note the serial number of instrument with every operation.

Ex.) Username: user 1. "Scan" was performed. Instrument : Lambda 365. Serial number : 365K5050403.

Account modified : Change the account settings.

Ex.) Username: user1, Scan: Password successfully changed.

Logon : Execute the UV Express software.

Ex.1) Username: user1, LogOn: **LOGON SUCCEEDED**.

Ex.2) Username: user1, LogOn: **LOGON FAILED**.

Ex.3) Username: user1. Scan(Log On) : The ID is not registered.

Ex.4) Username: user1. Scan(Log On) : Incorrect password. The remaining allowable attempt number is 1.

Ex.5) Username: user1. Scan(Log On) : User has entered wrong password over the lock out number and account is disabled.

Ex.6) Username: user1. Quantification : User does not have permission to access the Quantification.

Re-logon : Re-access UV Express software after lockout time.

Ex.1) Username: user 1, Scanning Kinetics : **RELOGON SUCCEEDED**.

Ex.2) Username: user 1, Scanning Kinetics : **RELOGON FAILED**.

Ex.3) Username: user1. Scan(Re-log On) : Incorrect password. The remaining allowable attempt number is 2.

Ex.4) Username: user1. Scan(Re-log On) : User has entered wrong password over the lock out number and account is disabled.

Ex.5) Username: user 1, Scanning Kinetics : **RELOGON** succeeded for change the method.

Created : Save data to new file or create the sample.

Ex.1) Username: user1. The file "C:\UV Express\Data\time.dkdt" was **created**.

Ex.2) Username: user1. The data "Sample1" was **created**. The file "C:\UV Express\Data\Untitled-1.dgdt".

Ex.3) Username: user 1. The data "Sample1 + 1.0000" was **created**. The file "C:\UV Express\Data\data1.dgdt".

Modified : Save the modified data or save as different name.

Ex.1) Username: user1. The file "C:\UV Express\Data\time2.dkdt" was **modified**.

Ex.2) Username: user1. Protein Analysis : The delete all was undone. The file "C:\UV Express\Data\Untitled-1.dpdt".

- Ex.3) Username: user1. Protein Analysis : The data Sample 1 was pasted. The file "C:\UV Express\Data\Untitled-1.dpdt".
- Ex.4) Username: user1. Protein Analysis : The data Sample 1 was copied. The file "C:\UV Express\Data\Untitled-1.dpdt"
- Ex.5) Username: user1. The data "Sample 1 + Sample 2" was modified. The original data is "Sample 1, Sample 2". The file is "C:\UV Express\Data\Untitled-1.dgdt".
- Ex.6) Username: user1. The file "C:\UV Express\Data\Untitled-1_Approval.dgdt" was modified. The original file is "C:\UV Express\Data\Untitled-1.dgdt".
- Ex.7) Username: user1. Scan : Method change reason - Test.
- [Internal Reference Use]
- Old : No, New : Yes
- [Internal Reference Type]
- New : Single Point
- [Internal Reference Wave.]
- New : 300.

Deleted : Save the delete a single data or all the data.

- Ex.1) Username: user1. The data "sample 1" was **deleted**. The file C:\UV Express \Data\data1.dgdt.
- Ex.2) Username: user1. The data "Sample 1" was deleted. The file is Untitled-1.
- Ex.3) Username: user1. Deleted all data. The file is Untitled-1.

Signature : Provide the electronic signature.

- Ex.) Username: user 1. The file "C:\UV Express\Data\time.dkdt" was **signed**.
Reason : Review.

Log off : Close the UV Express software.

- Ex.) Username: user 1, successfully exited or **logged off** the application.

Validation: Check the instrument's status (Wavelength, Photometric, Resolution, Stray Light, Noise and Stability) only in Validation software.

- Ex.) Username : user 1. The data "**Noise**" was created. The file Untitled-1

