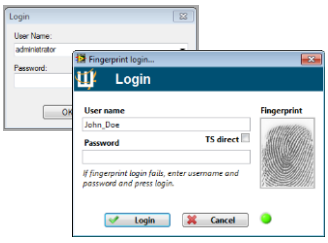
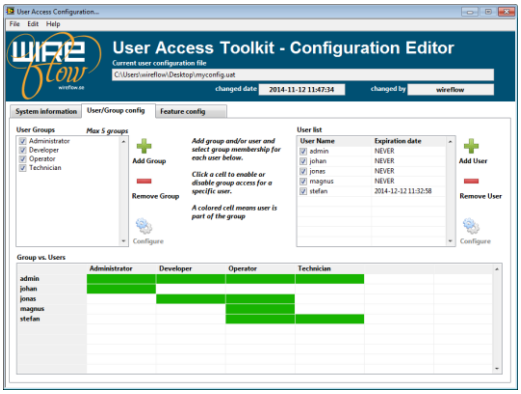
wireflow

AC0082-001, rev B

UAT - TestStand Integration User Manual





Contents

Support information 2
Technical support and Product information 2
WireFlow headquarters 2
Important information 2
Copyright 2
EULA 2
Introduction 6
Requirements 6
Quick Start 6
TestStand Login 7
Installation 7
Step-by-step for first time installation 7
Step-by-step to enroll a user with fingerprints 15
UAT configuration 20
TestStand installation 20
TestStand integration configuration 20
Configuration 22
UAT configuration 23
The menus 23
System information 24
User configuration 25
Troubleshooting 30
Error codes 30
Technical support and Professional services 31

Support information

Technical support and Product information

www.wireflow.se

WireFlow headquarters

WireFlow AB
Theres Svenssons gata 10
SE-417 55 Göteborg

Please see appendix “Technical support and Professional services” for more information.

Important information

Copyright

EULA

END-USER LICENSE AGREEMENT FOR
WireFlow UAT-TestStand Integration (AC0082)

IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM DOWNLOAD/INSTALL: WireFlow's End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and WireFlow, for the WireFlow software product(s) identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the program between you and WireFlow, (referred to as "licenser"), and it supersedes any prior proposal, representation, or understanding between the parties. If you do not agree to the terms of this EULA, do not download, install or use the SOFTWARE PRODUCT.
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1 GRANT OF LICENSE

The SOFTWARE PRODUCT is licensed as follows:

1.1 Installation and Use

WireFlow grants you a personal, non-transferable and non-exclusive right to use the copy of the Software provided with this EULA on your computer running a validly licensed copy of the operating system for which the SOFTWARE PRODUCT was designed.

1.2 Backup Copies

You may also make copies of the SOFTWARE PRODUCT as may be necessary for backup and archival purposes.

1.3 Evaluation Version

For clarity in the case of Trial Licenses, if You do not pay the applicable license fees prior to the conclusion of any applicable Trial Period, you have no right or license, express or implied, to further use the SOFTWARE PRODUCT in any manner thereafter.

2 DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

2.1 Maintenance of Copyright Notices

You must not remove or alter any copyright notices on any and all copies of the SOFTWARE PRODUCT.

2.2 Distribution

You may not distribute registered copies of the SOFTWARE PRODUCT to third parties. Evaluation versions available for download from WireFlow's websites may be freely distributed.

2.3 Prohibition on Reverse Engineering, Decompilation, and Disassembly

You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

2.4 Rental

You may not rent, lease, or lend the SOFTWARE PRODUCT.

2.5 Support Services

WireFlow may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Any supplemental software code provided

to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this EULA.

2.6 Compliance with Applicable Laws

You must comply with all applicable laws regarding use of the SOFTWARE PRODUCT.

2.7 Export Laws

The export of the SOFTWARE PRODUCT from the country of original purchase may be subject to control or restriction by applicable local law. Licensee is solely responsible for determining the existence and application of any such law to any proposed export and for obtaining any needed authorization. Licensee agrees not to export the SOFTWARE PRODUCT from any country in violation of applicable legal restrictions on such export.

3 TERMINATION

Without prejudice to any other rights, WireFlow may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT in your possession.

4 COPYRIGHT

All title, including but not limited to copyrights, in and to the SOFTWARE PRODUCT and any copies thereof are owned by WireFlow or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by WireFlow.

4.1 Third party software.

The SOFTWARE PRODUCT may include software under license from third parties (“Third Party Software” and “Third Party License”). Any Third Party Software is licensed to you subject to the terms and conditions of the corresponding Third Party License. Generally, the Third Party License is located in a separate file such as license.txt or a readme file.

5 NO WARRANTIES

WireFlow expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is provided 'As Is' without any express or implied warranty of any kind, including but not limited to any warranties of merchantability, noninfringement, or fitness of a particular purpose. WireFlow does not warrant or assume responsibility for the accuracy or

completeness of any information, text, graphics, links or other items contained within the SOFTWARE PRODUCT. WireFlow makes no warranties respecting any harm that may be caused by the transmission of a computer virus, worm, time bomb, logic bomb, or other such computer program. WireFlow further expressly disclaims any warranty or representation to Authorized Users or to any third party.

6 HIGH RISK ACTIVITIES

The SOFTWARE PRODUCT is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the SOFTWARE PRODUCT could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). WireFlow and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

7 LIMITATION OF LIABILITY

In no event shall WireFlow be liable for any damages (including, without limitation, lost profits, business interruption, or lost information) rising out of 'Authorized Users' use of or inability to use the SOFTWARE PRODUCT, even if WireFlow has been advised of the possibility of such damages. In no event will WireFlow be liable for loss of data or for indirect, special, incidental, consequential (including lost profit), or other damages based in contract, tort or otherwise. WireFlow shall have no liability with respect to the content of the SOFTWARE PRODUCT or any part thereof, including but not limited to errors or omissions contained therein, libel, infringements of rights of publicity, privacy, trademark rights, business interruption, personal injury, loss of privacy, moral rights or the disclosure of confidential information.

8 CONTACT

All questions about this EULA shall be directed to: info@wireflow.se.

WireFlow AB
Theres Svenssons gata 10
SE-417 55 Göteborg
Sweden

Introduction

The WireFlow “UAT - TestStand Integration” product is a TestStand plugin that enables TestStand to use the WF-2111 fingerprint reader for authentication.

Users are managed using the User Access Toolkit management GUI.

Requirements

- LabVIEW runtime 2012 or higher
- Fingerprint reader (WF2111) + Windows Device driver
- TestStand

Quick Start

Once the UAT - TestStand Integration has been installed for the desired TestStand version, the standard TestStand login dialog is replaced by a fingerprint enabled dialog.

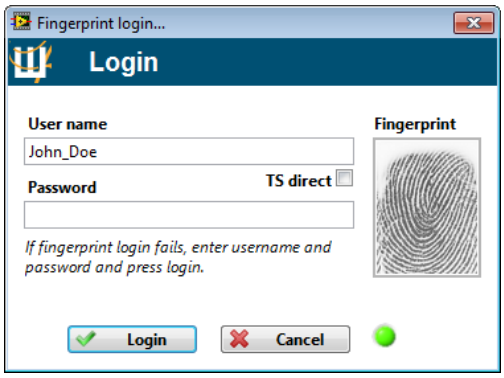


Figure 1. UAT-TestStand Login dialog

When the dialog, see Figure 1, is shown just place the finger on the fingerprint read and wait for the UAT to login the user in TestStand. If the fingerprint is not recognized, it is always possible to use the fallback of user name and password.

It is even possible to use TestStand defined users, in this case the TS direct checkbox must be checked. This means that the user name and password are passed directly to TestStand and never involves UAT.

The groups in UAT should match the groups that are defined in TestStand, and once the user is logged in he/she will get access rights according to the group membership in TestStand.

The installed UAT-TS applications can be found in the Windows start menu under “UAT-TestStand Integration”

TestStand Login

If the UAT TestStand integration add-on is installed it means that every time TestStand starts or whenever a login is invoked (from a sequence or from the TestStand menus), the UAT- TestStand Login dialog is shown instead of the standard TestStand dialog.

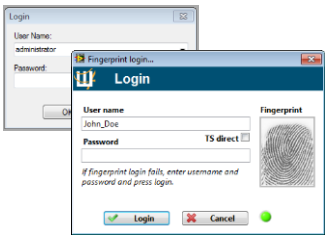


Figure 2. The standard TestStand dialog is replaced by the UAT dialog

This dialog connects to the UAT user database and uses this information to manage users in TestStand, as well as performing login when UAT successfully identifies the user.

NOTE: For the fingerprint to work it has to be enabled and activated for the users (described later in this document).

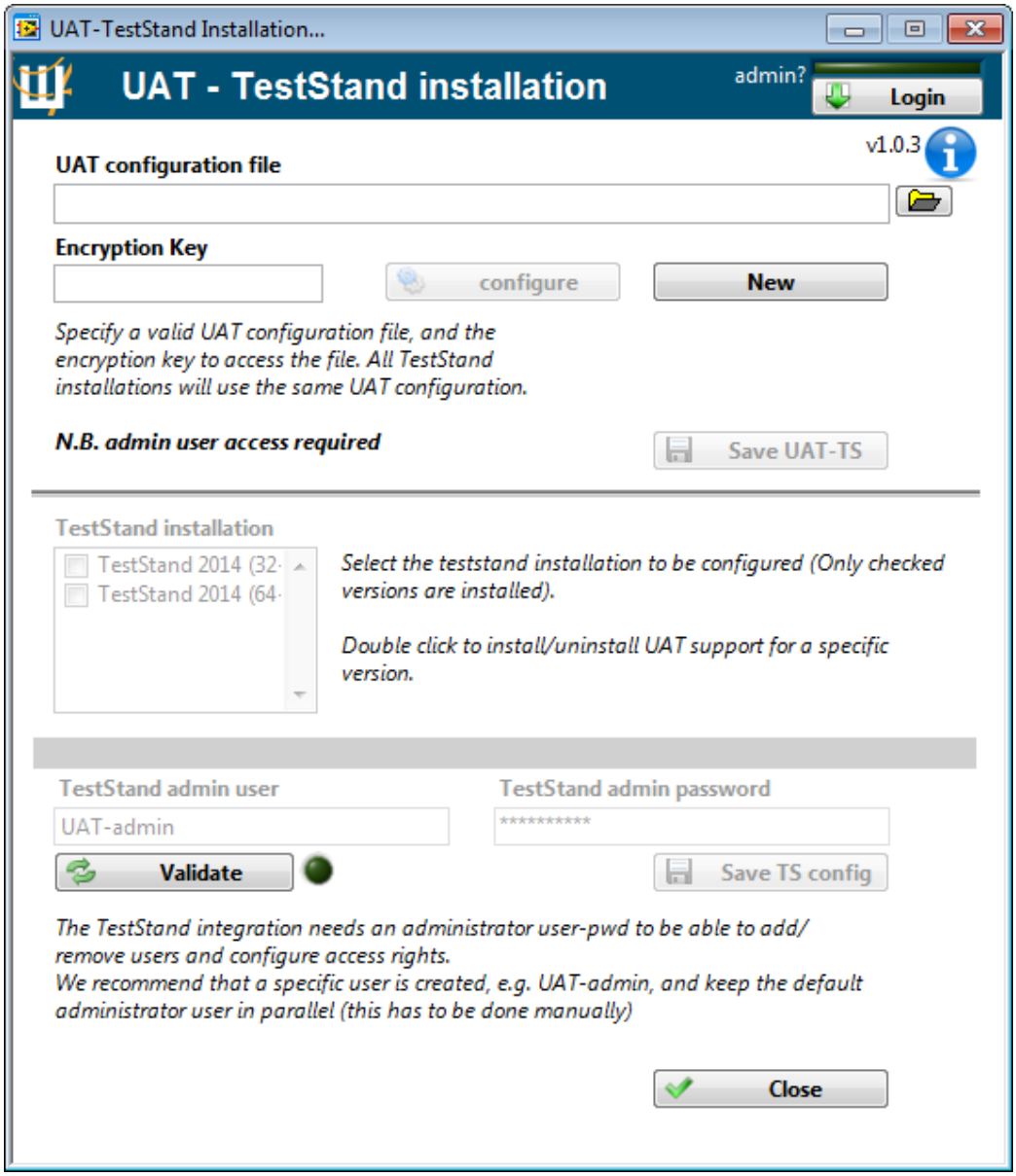
Installation

Step-by-step for first time installation

First time installation of the UAT – TestStand Integration is done using the supplied setup.exe. Run setup.exe and follow the instructions. Two applications are installed and can be accessed in the Windows start menu in the UAT-TS integration folder.

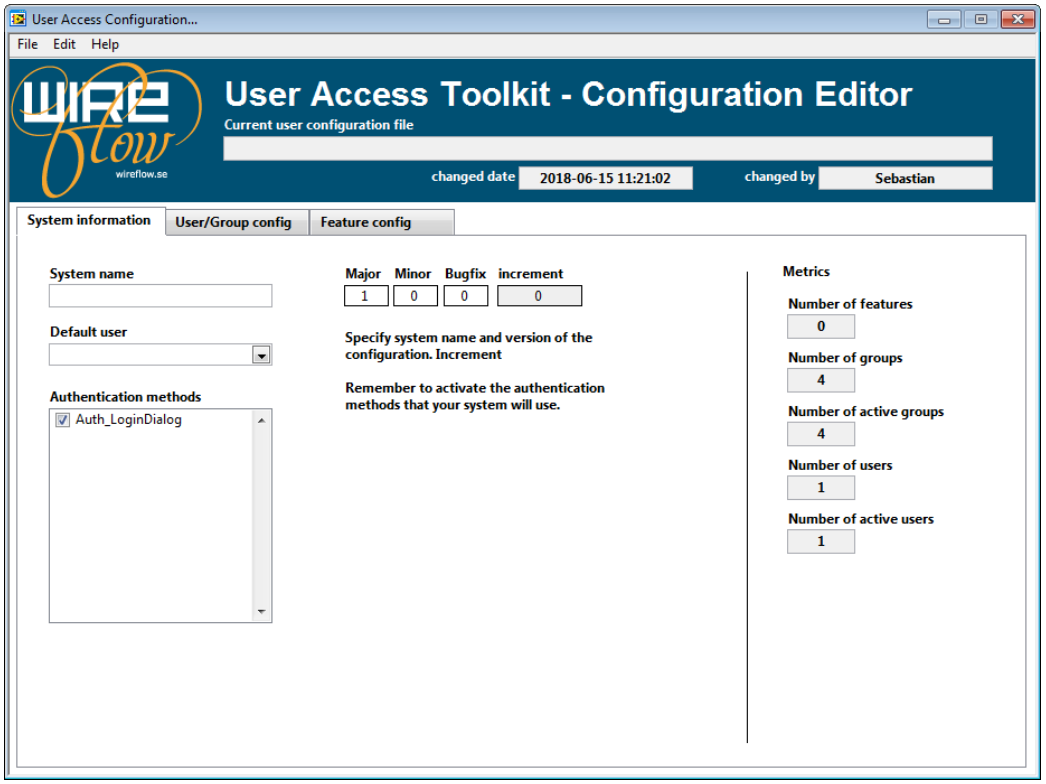
- UAT-TS_Installation
- UAT-TS_Configurator

Once the application is installed, the UAT-TS_Installation application pops up and lets the user do initial configuration of the system.

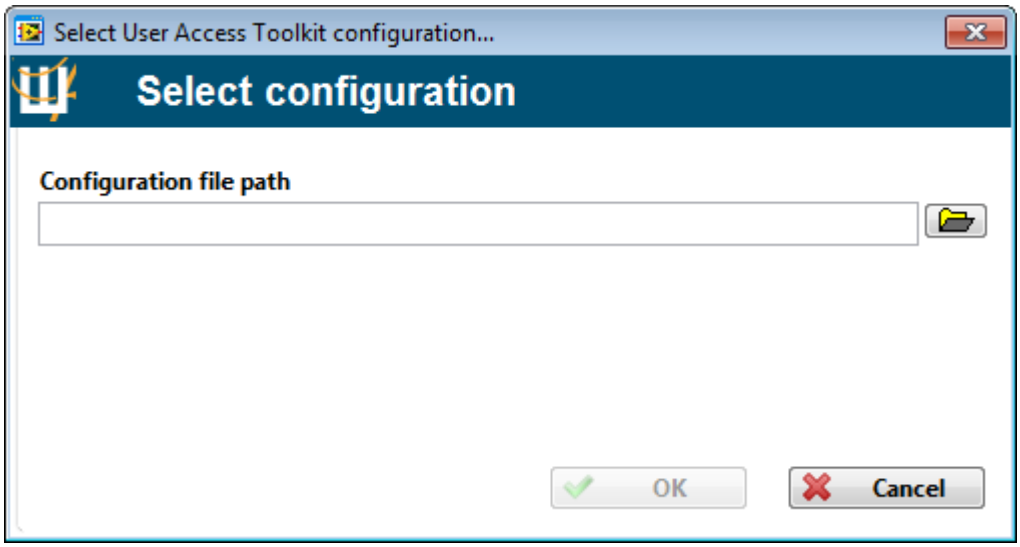


Click New to create a UAT configuration file. An encryption key dialog appears.

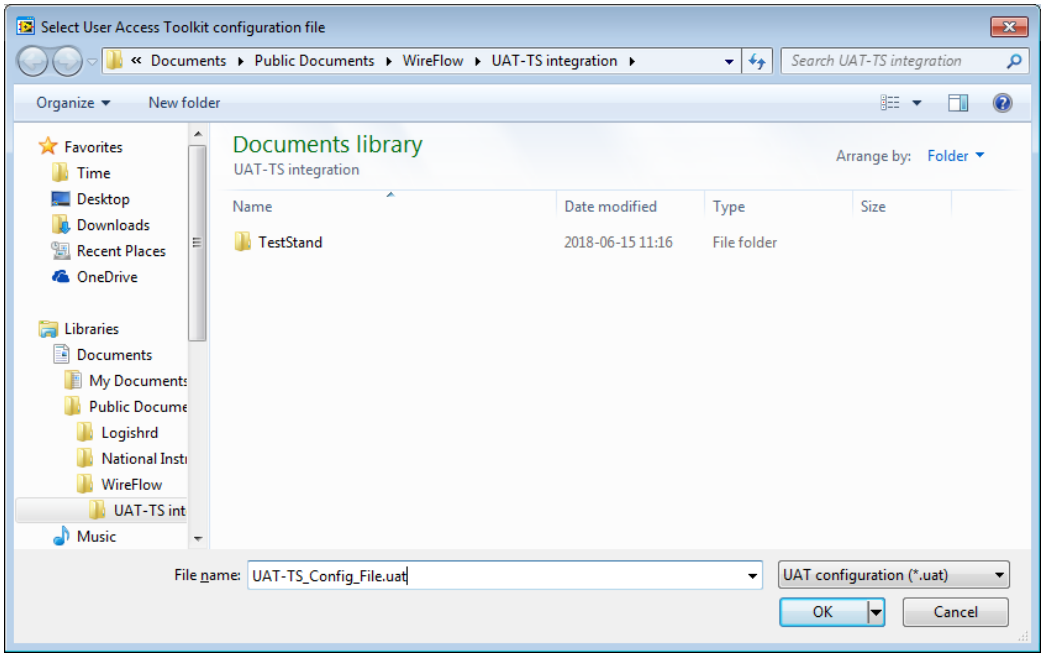
Write an encryption key twice and click OK. The User Access Toolkit – Configuration Editor appears.



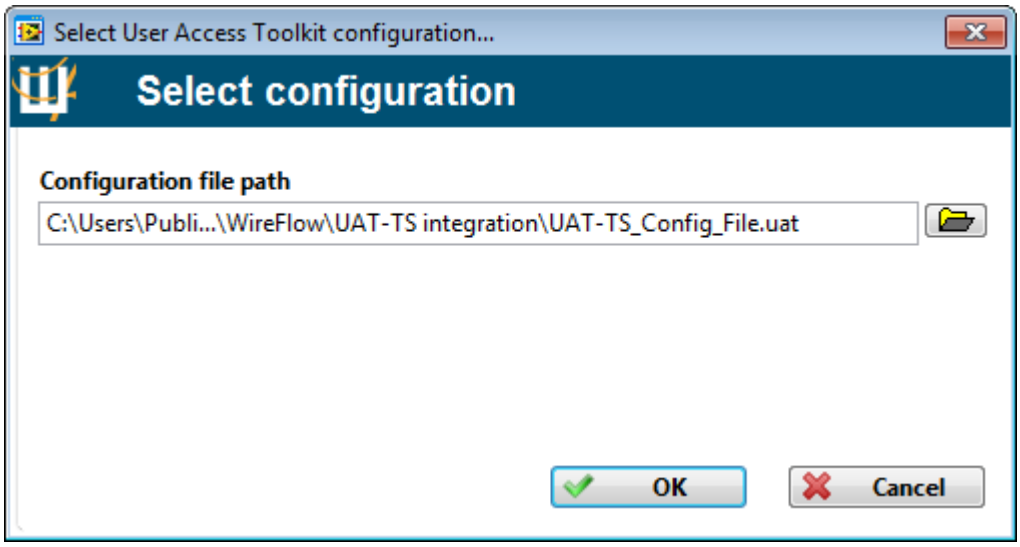
Click File – Save. A configuration file path dialog appears.



Click the open button to specify a new filename (.uat).



Click OK.

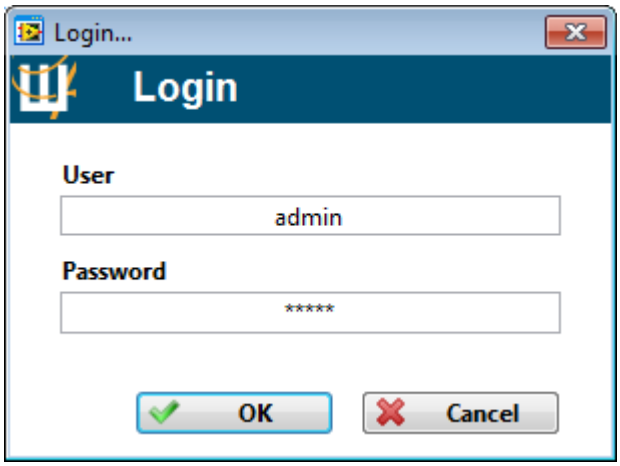


Click OK.

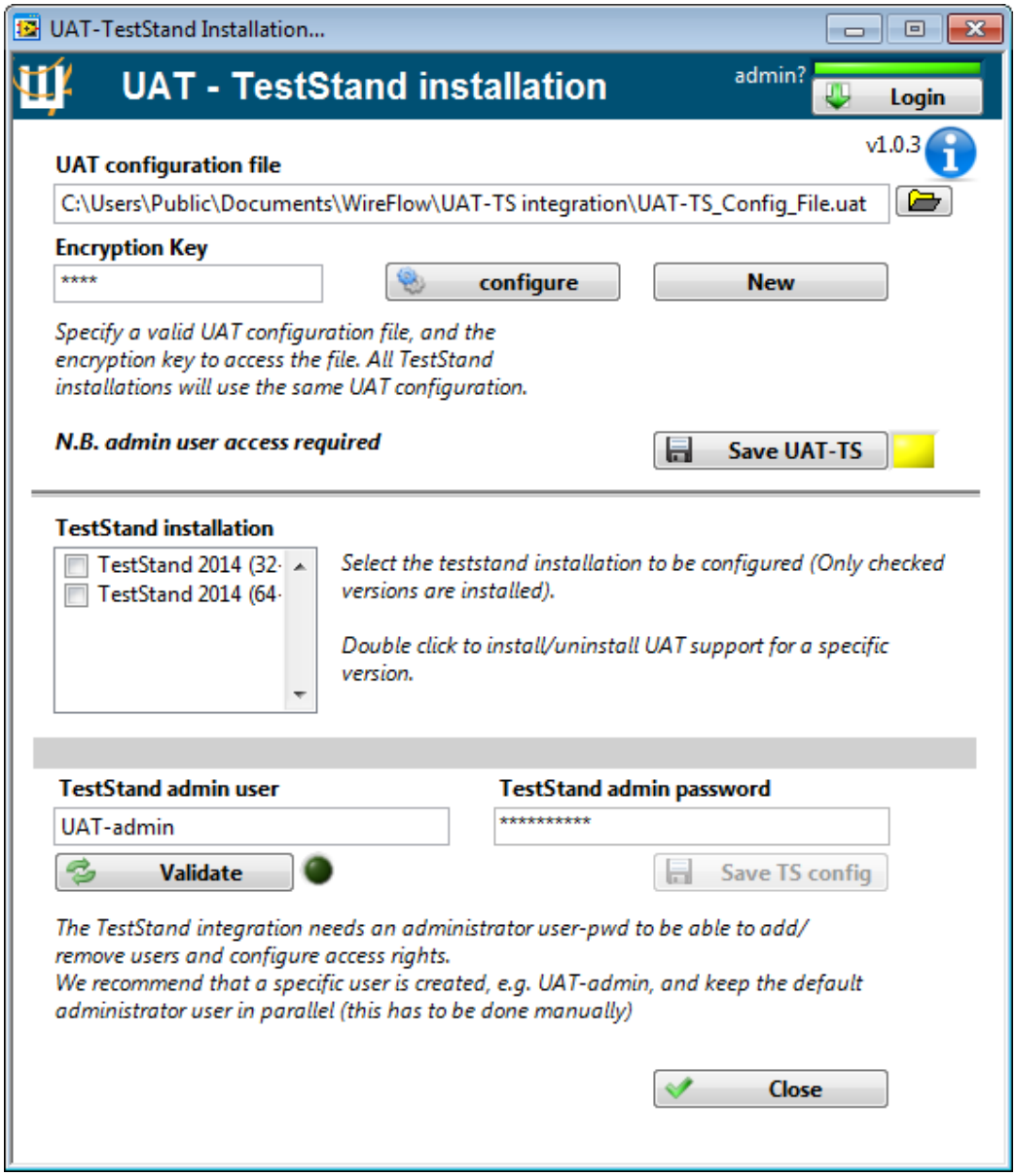
Optional: add or manage the groups and users. You can return at any time using the configure button or the UAT-TS_Configurator application.

Close the window to return to UAT-T_Installation. An encryption key dialog appears.

Enter the encryption key that you created earlier. Click OK. A login dialog appears.

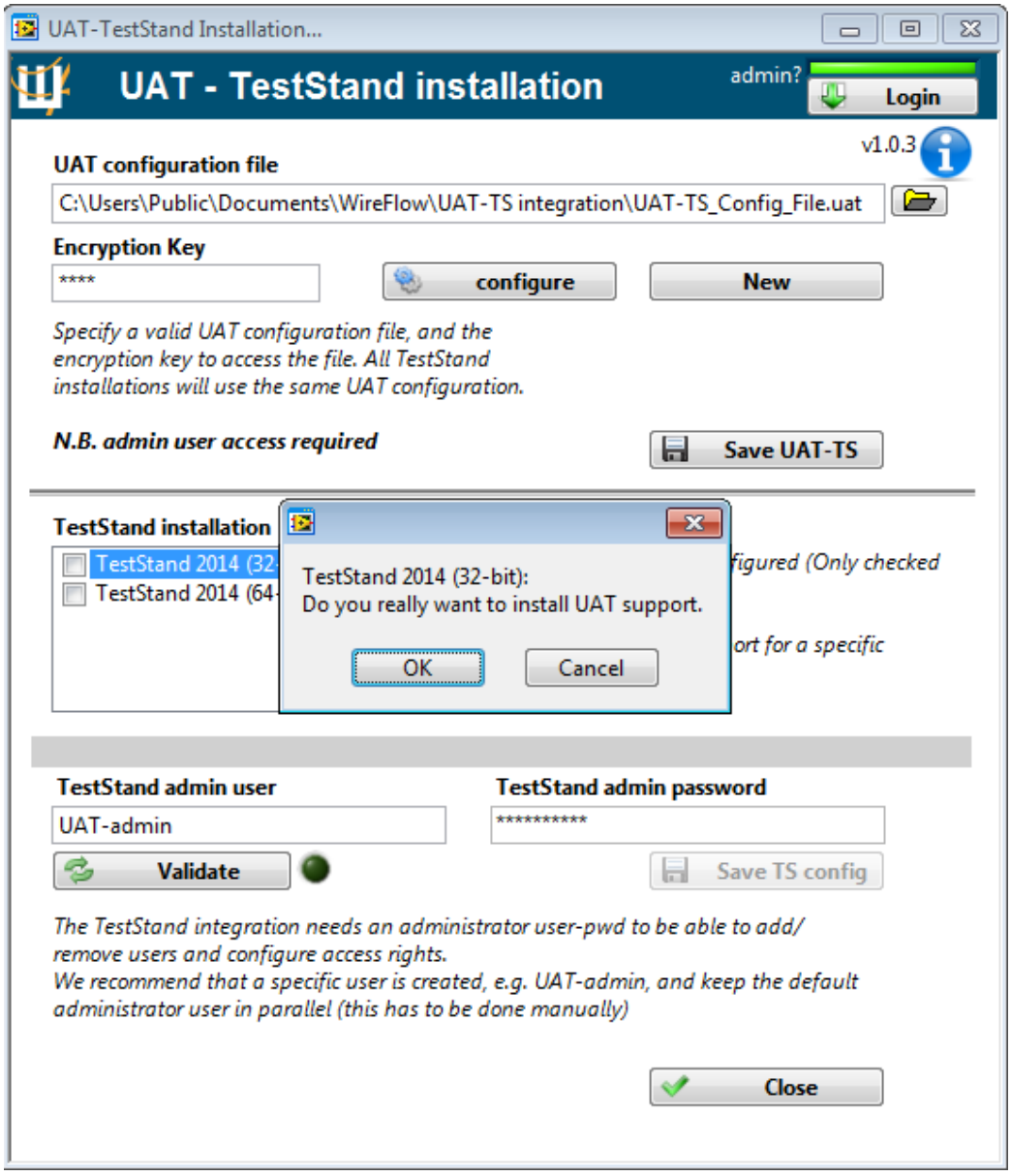


Enter the user and password. The default user/pass is admin/admin. Click OK. The UAT-TS_Installation window appears.

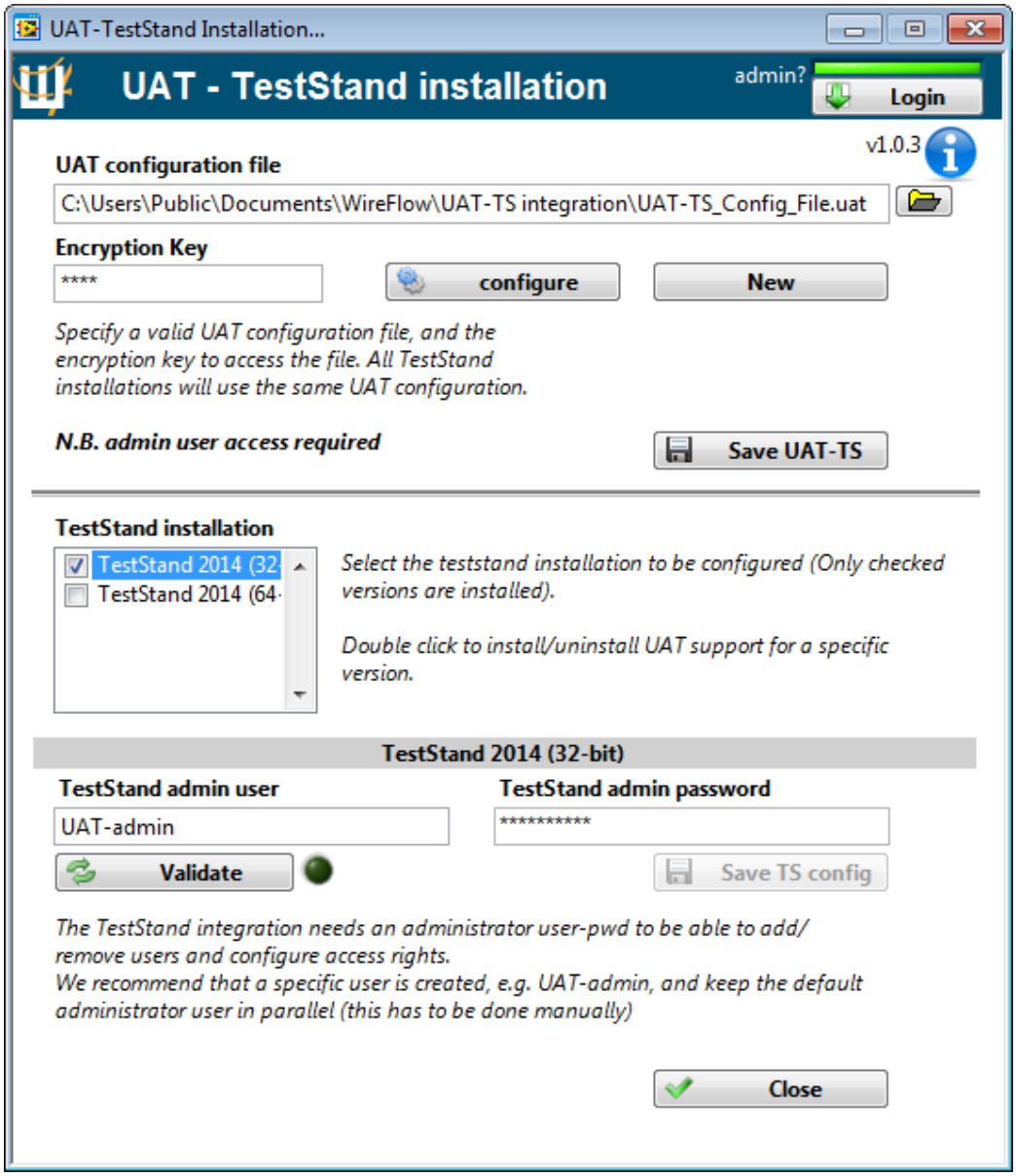


Click Save UAT-TS to save the User Access Toolkit connection to TestStand.

Double-click on a TestStand version in the TestStand installation list to install UAT support for that TestStand version. A confirmation dialog appears.

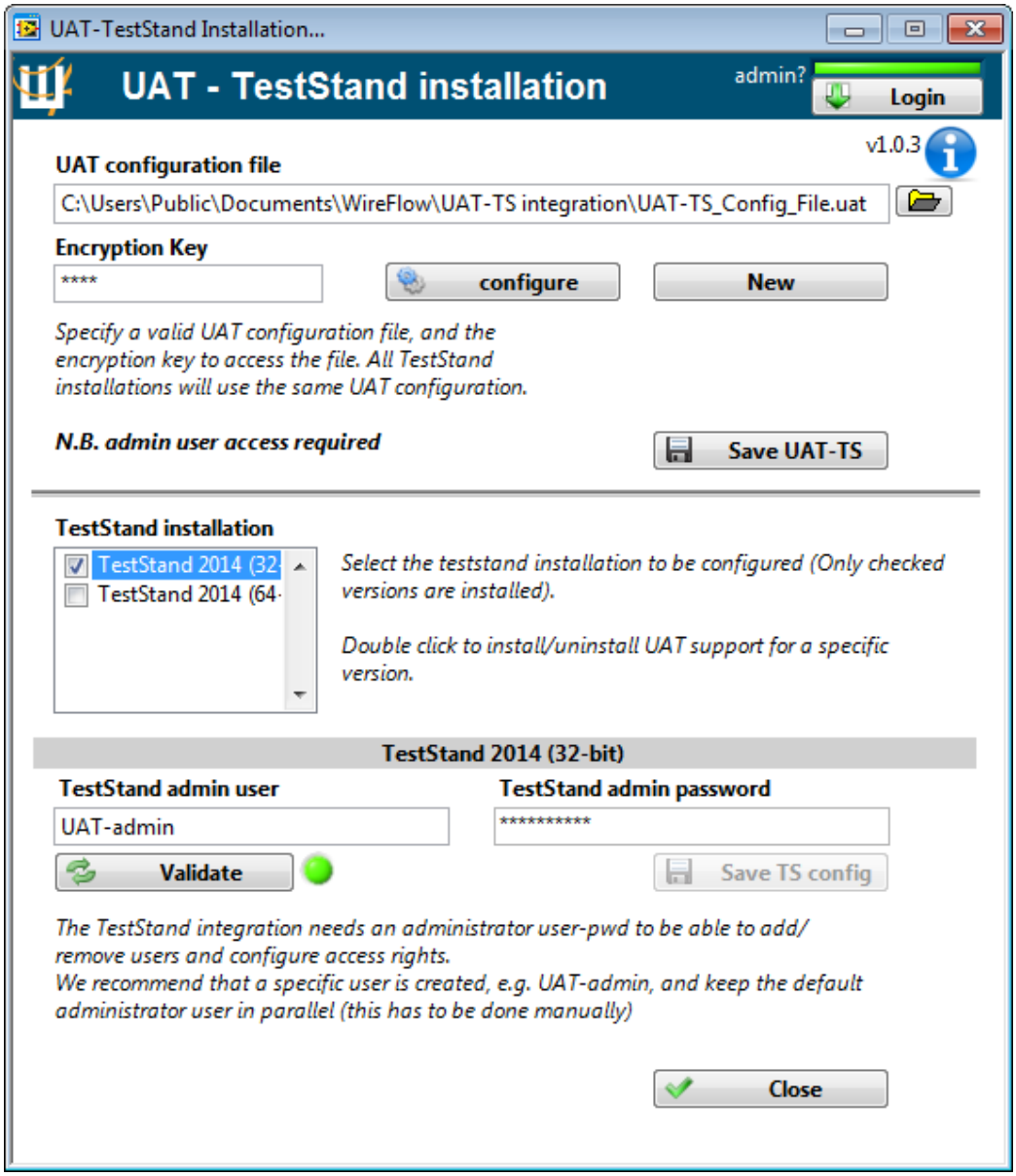


Click OK to confirm and return.



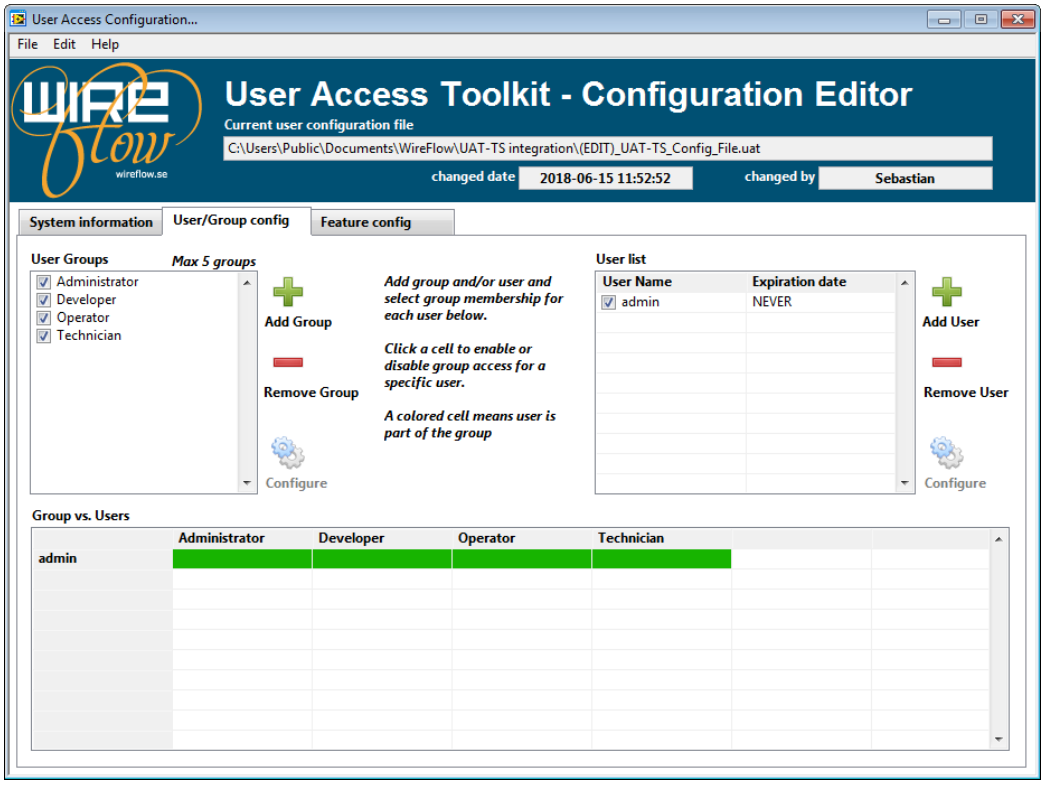
Click Validate to validate the default UAT-admin TestStand user.

The Boolean indicator lights up to indicate success.

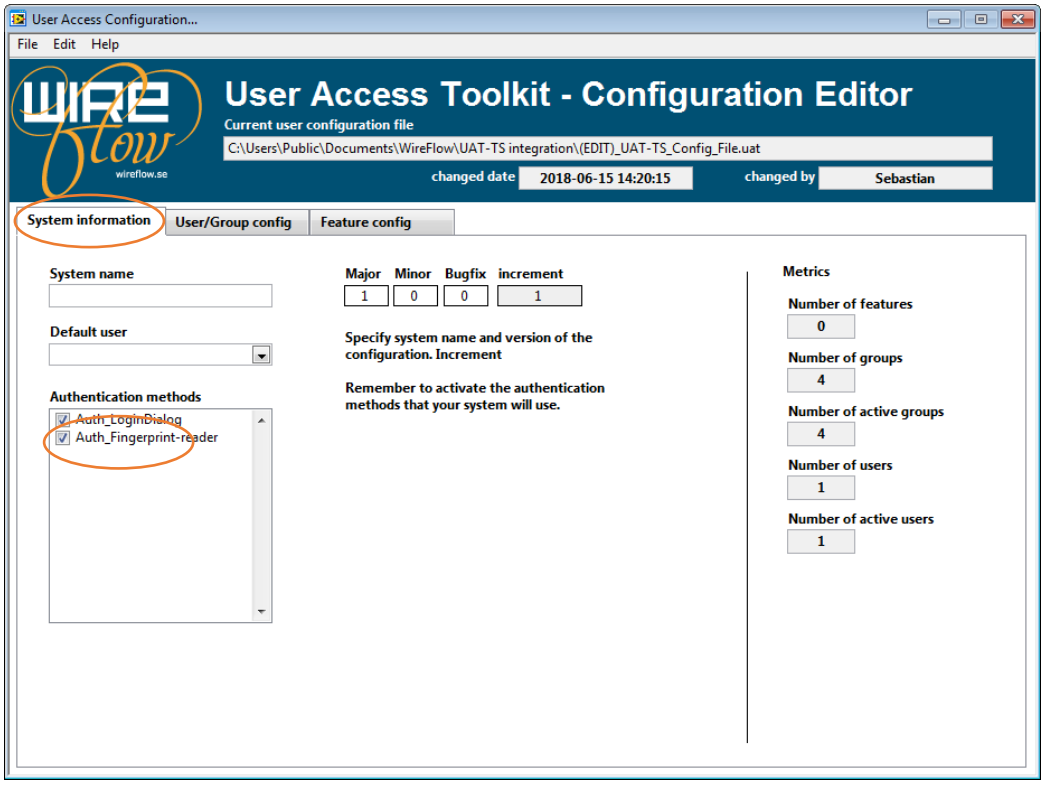


Step-by-step to enroll a user with fingerprints

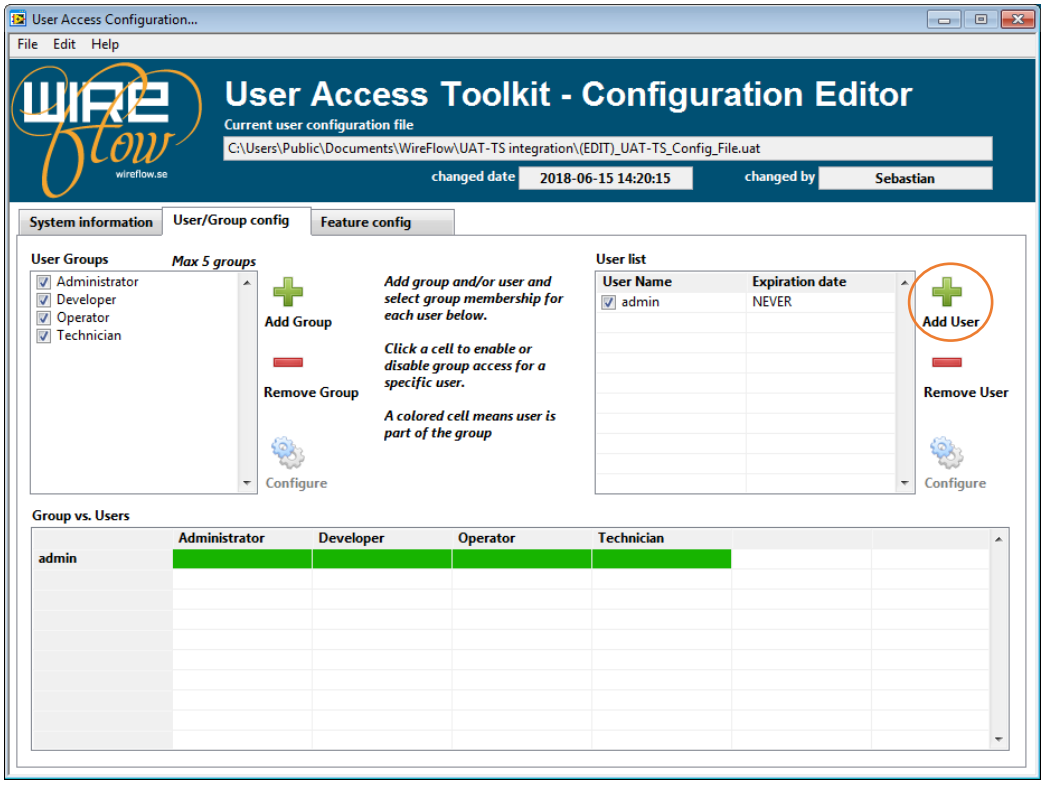
Click configure to open the User Access Toolkit.



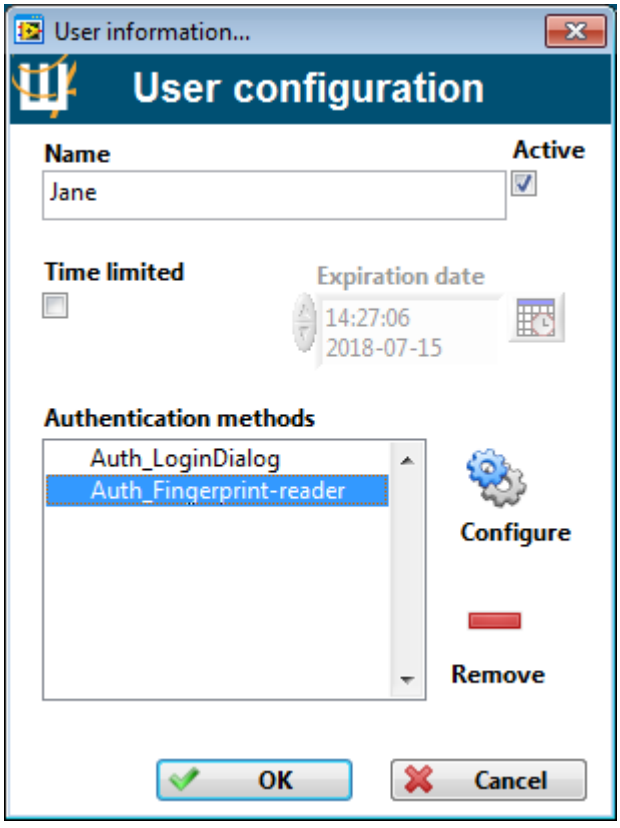
Click the System information tab and make sure that Auth_Fingerprint-reader is checked.



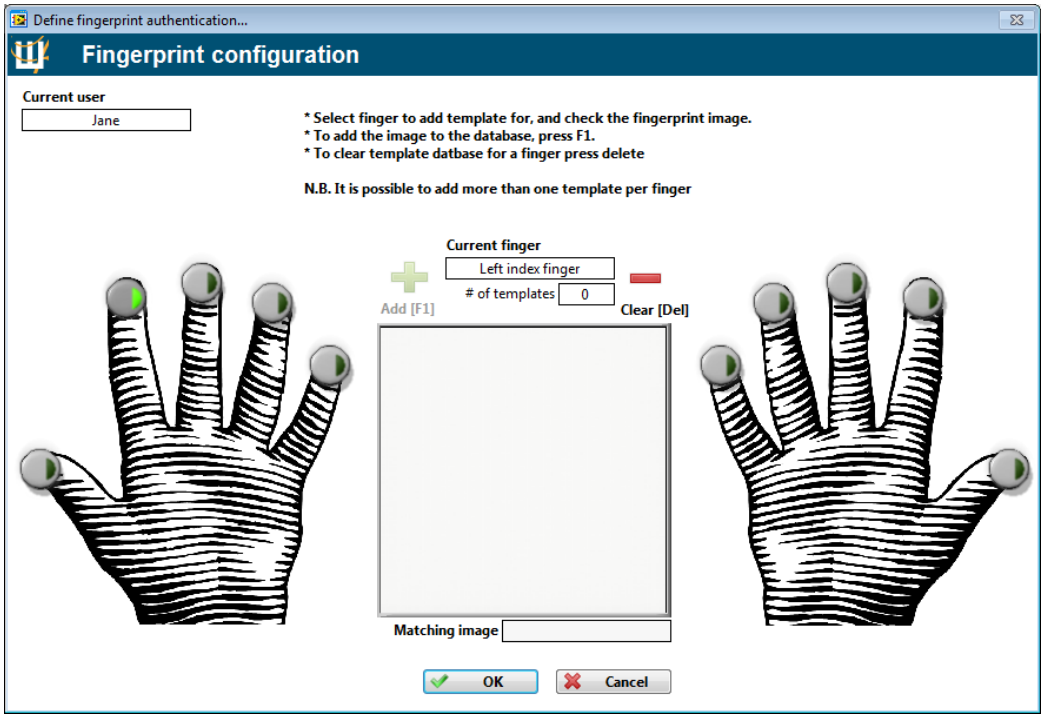
Go to the User/Group config tab and click add User.



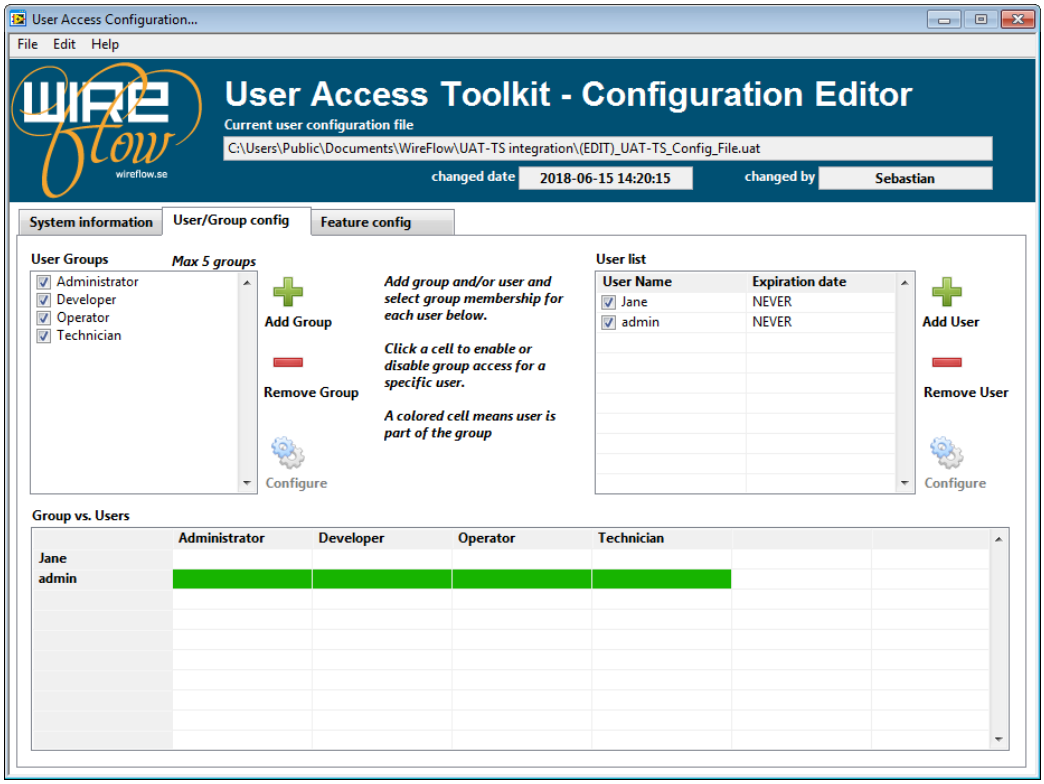
The User configuration dialog appears. Write a name, select Auth_Fingerprint-reader and click Configure.



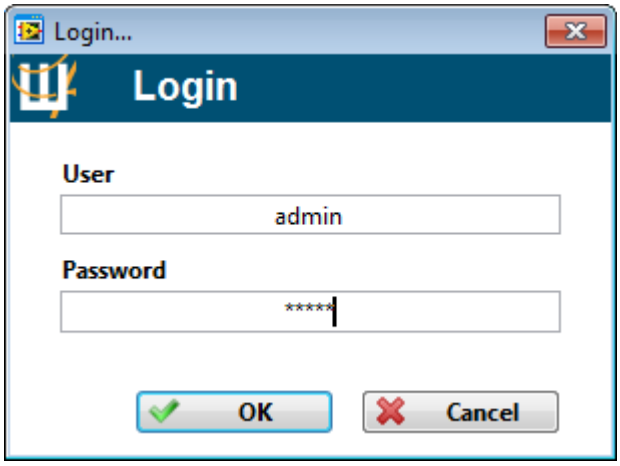
The fingerprint configuration dialog appears.



Place a finger on the fingerprint reader, click Add [F1] and then OK. Click OK again go get back to the user access toolkit main screen. Note the new user in the user list.



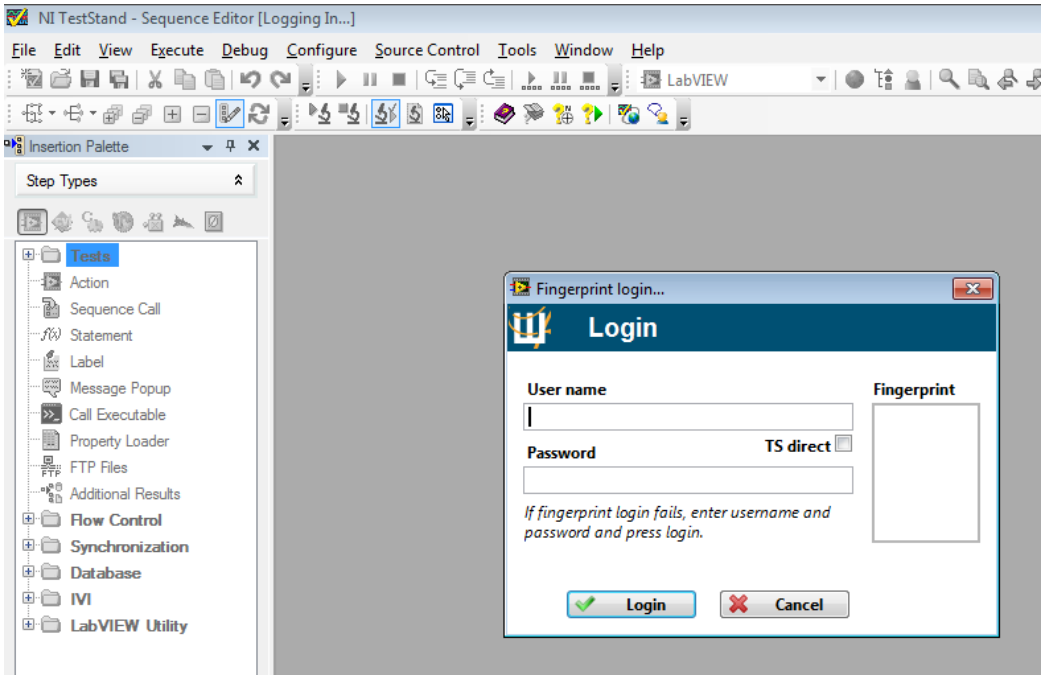
Click File – Save. Close the window. A login dialog appears.



Enter the user and password (default admin/admin) and click OK to return to UAT-TS_Installation. Click Save UAT-TS to save the User Access Toolkit connection to TestStand.

Click Close to exit the application.

Open TestStand.



Place the finger on the fingerprint reader to log in.

UAT configuration

The top section in the GUI is used to setup the UAT connection, and contains the following items.

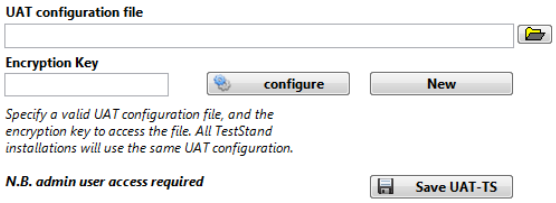


Figure 3. UAT configuration

- UAT configuration file
  - Specifies the UAT configuration to be used. This can be placed on a network share to use the same user configuration on several test stations. At runtime each test station uses a local cached copy of this file.
- Encryption key
  - The key used to access the UAT configuration file (the file is encrypted).
- Configure
  - Open the UAT configuration GUI for configuration
  - Requires an admin user (according to the UAT configuration) to be able to edit configuration (default user/password the first time UAT –TS is installed is admin/admin).
- New
  - If we install the UAT-TS for the very first time we have to create a new UAT configuration (default admin/password is admin/admin).
- Save UAT-TS
  - Updates this test station configuration with info about location of UAT configuration and Keys.

TestStand installation

Next Section in the GUI is the TestStand installation.

Figure 4. List of TestStand installations

This section lists all config folders detected for different TestStand versions, and by double clicking on an item UAT – TestStand integration can be enabled/disabled for a specific TestStand version (indicated by a checkmark).

TestStand integration configuration

At the bottom is a section where the TestStand integration is configured.

Figure 5. TestStand integration configuration

UAT-TS needs a TestStand administrator account in order for the UAT configuration to be able to synch users/group with TestStand. WF recommends a specific admin user just for UAT-TS integration, as this user is never used outside the UAT-TS configuration.

Enter the name and password for the UAT-admin to be used (default is UAT-admin), and when Save TS config is pressed, the application checks with TestStand if the user exists

If it doesn't exist, the system tries to add the user using the default TestStand admin account. If the default admin user is not valid, a dialog asks for TestStand admin credentials to be used.

The username and password is then stored in another encrypted configuration file.

Use the Validate button to check if the entered credentials are actually valid.

Configuration

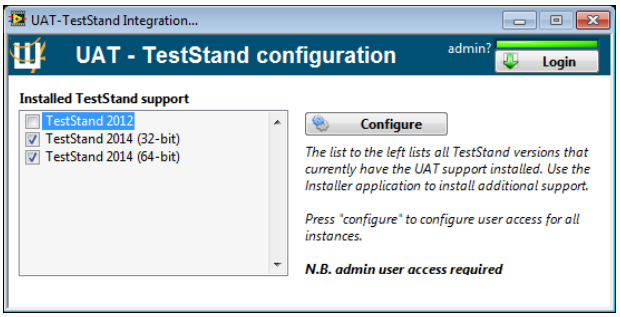


Figure 6. The UAT-TS_Configurator application

When everything is up and running we still might have to add new users, change credentials etc. To do this we can use the included Configuration application (UAT-TS_Configurator). This application is a stripped down version of the Installation application, and does not show any path details since it should only access the current configuration.

To the left is a list of the currently installed TestStand versions, and once an admin user is logged in, it is possible to press Configure to add users, change credentials or user groups.

Since the UAT - TestStand Integration uses locally cached files during runtime, it is possible to edit the configuration from any computer with access to the network-share. This means that the test-stations could be given read-only access to the network share and that a separate PC could be used to manage all users/test stations in the system.

NOTE. When the UAT configuration panel is open no other instances can access the shared configuration, and has to use the cached configuration data. Therefore don't forget to close the UAT configuration editor.

UAT configuration

This section is a modified excerpt from the User Access Toolkit manual, which can be downloaded in full from www.wireflow.se .

This application can edit the configuration in terms of authentication methods, users and groups.

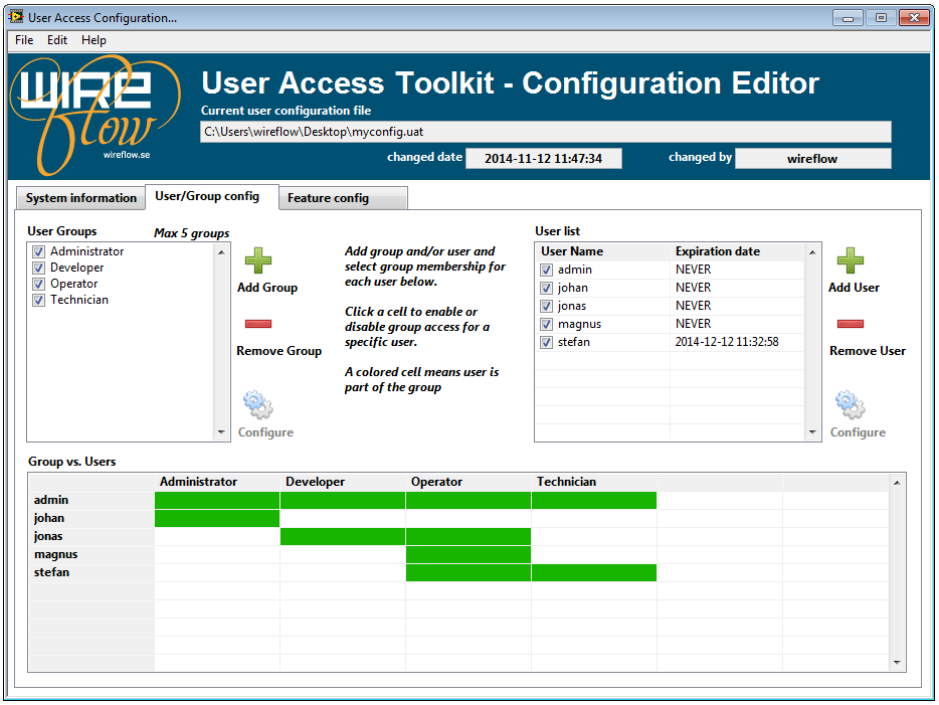


Figure 7. The configuration UI

The configuration panel has three configuration pages

- System information
  - General system info and configuration overview
  - Import and export of configurations
- User/Group config
  - Add, remove, enable or disable users
  - Configure expiration and credentials for users.
  - Add, remove, enable or disable groups
  - Configure user group access
- Feature config (**not used in the TestStand add-on**)
  - Add or remove features
  - Configure feature access for different groups

Using these pages it is possible to configure access for users in the system.

The menus

Opening, saving and creating new configurations is done through menu actions.

This section briefly describes the available menu selection

File:New...	Creates a new User Access Toolkit configuration from scratch (with only the root admin user at the start)
File:Open...	Opens an existing configuration, prompting the user for a password to load the file. If the password is not correct the configuration is not loaded
File:Save...	Saves the current configuration to file, prompting the user for a password to save the file. N.B. the password must match the password used in the application, otherwise the application cannot read the configuration data.
File:Save As...	Saves a copy of the current configuration to a new file, prompting the user for a password to save the file. N.B. only available if configuration UI launched with empty path.
File:Exit	Exits the application
Edit:Revert	Reverts all edits to the last loaded state
Help:Show Context Help	Opens the context help window

System information

At the top of the panel, in the WireFlow banner, general file information is displayed;

- Current user configuration file = path to the configuration currently edited.
- changed date = date/time when the configuration file was saved.
- changed by = user (in the system) that last saved the configuration

Figure 8. UAT WireFlow banner field

The first thing to do when creating a new configuration is to define what type of authentications the application should use.

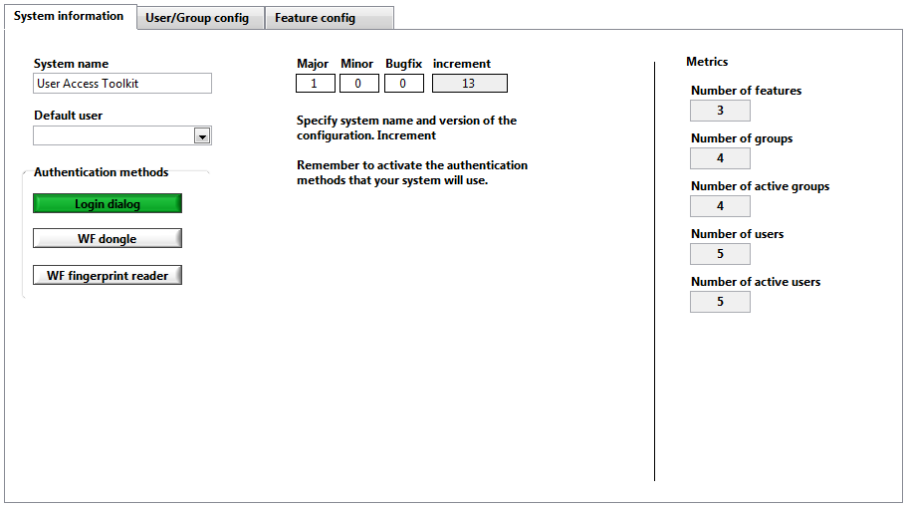


Figure 9. System information page

When an authentication method is enabled, the button is green, e.g. 

, and the option is enabled in the user configuration panel (see Figure 12). The TestStand add-on can only use Login-dialog and the WF fingerprint reader, i.e. the dongle is currently not supported.

System name is only informational, but can be read by the API for information to the end user.

If default user is set, this will be the user that is activated when the configuration is applied when a session is initiated.

The default user should never be an admin user, and will not be activated when configuration is applied.

The right hand side of the information page shows some metrics for the system, like number of groups, users and features.

User configuration

Without a valid user configuration the UAT cannot perform login or access checks.

Configuring a user involves giving the user a unique name, set the user credentials and optionally setting an expiration date as well as group membership.

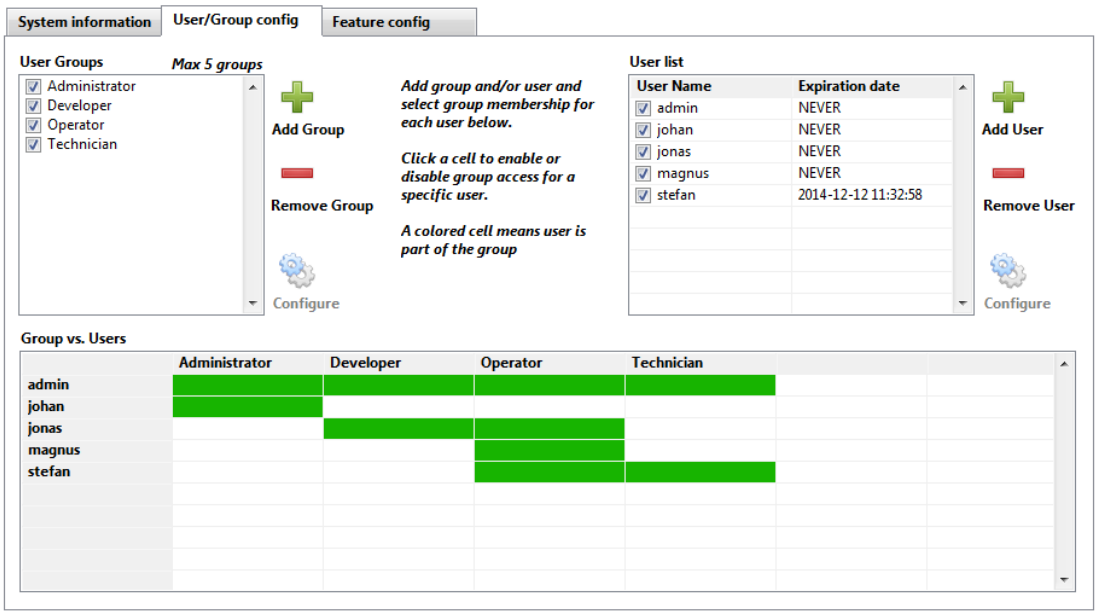


Figure 10. User configuration

Figure 10 shows the configuration of user and groups;

- The "User Groups" shows the groups in the system and their active state.
- The "User list" shows the current users in the system and their active state as well as the expiration date
- "Group vs. User" shows and defines the group membership for each user in the system. Groups are in columns and users are in rows.

The checkboxes to the left of a user or group name can be used to disable or enable the selected item (disabling is not possible for the default admin user or admin group):

- Disabling a user means that the user cannot access the system, but that the user information is still stored in the configuration data.
- Disabling a group means that all users that are member of that group loose the access right defined for that group.

Exactly how a group/user can be configured is described in more detail in the following subchapters.

Adding a new group

To add a new group, press 

and give the new group a name and optionally set the group inactive (group name cannot contain spaces, and while name is invalid the OK button will be disabled).

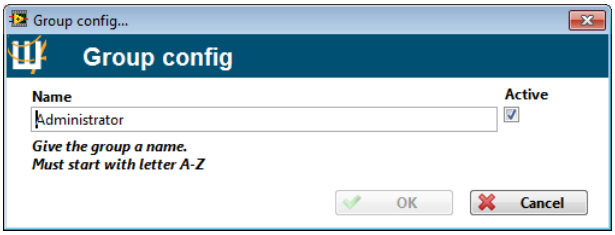


Figure 11. Group configuration dialog.

Removing an existing group

To remove an existing group, select one or more groups in the group list and press Remove Group and either accept or cancel the deletion. The default admin group cannot be removed.

Renaming a group

To rename a group, double-click the group name or press the Configure button next to the group list, and change the name in the Group config dialog.

Adding a new user

To add a new user, press Add User and fill in the information in the pop-up. A checkmark to the left of an authentication type means that the authentication is configured.

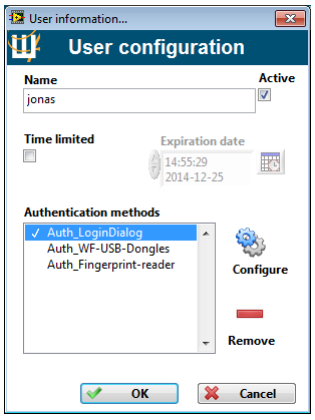


Figure 12. User configuration dialog

- Name
  - Must be a unique name and can only contain the characters:
    - a-z, A-Z, 0-9, _-().@
- Active
  - Sets the user to be active or inactive. Can also be set from the user list
- Time limited
  - If the user account is time limited, set this checkbox and fill in the Expiration date
- Expiration date

    - Expiration date is only active if the “Time limited” checkbox is set.
- Authentication methods
    - List of the currently active authentication methods and their status. A checkmark before an authentication indicates that it is configured and ready to be used.
- Configure
    - Opens up a dialog to configure the selected authentication method.

Login dialog authentication

Login dialog is the most basic user validation. To configure a user with the login dialog option, we have to specify the password.

Figure 13. Specifying user password for login dialog

The configuration dialog we have to specify the new password, and if “Hide characters” is selected we have to specify the password twice. When the “Confirm New Password” and “New Password” matches (or if Hide characters is unchecked) the OK button is activated.

The password is hashed using the SHA-256 algorithm, and the only thing that is saved to configuration is the username and the hash. Since the SHA-256 algorithm is one-direction, it is impossible to reveal the password from the hash value.

Fingerprint reader credentials

Even if the fingerprint authentication works on many LabVIEW platforms, the configuration of the user has to be performed on a desktop version of LabVIEW. Configuration requires a connected WF fingerprint reader.

Configuring a user for fingerprint access means that we have to take a number of captures of one or more fingers.

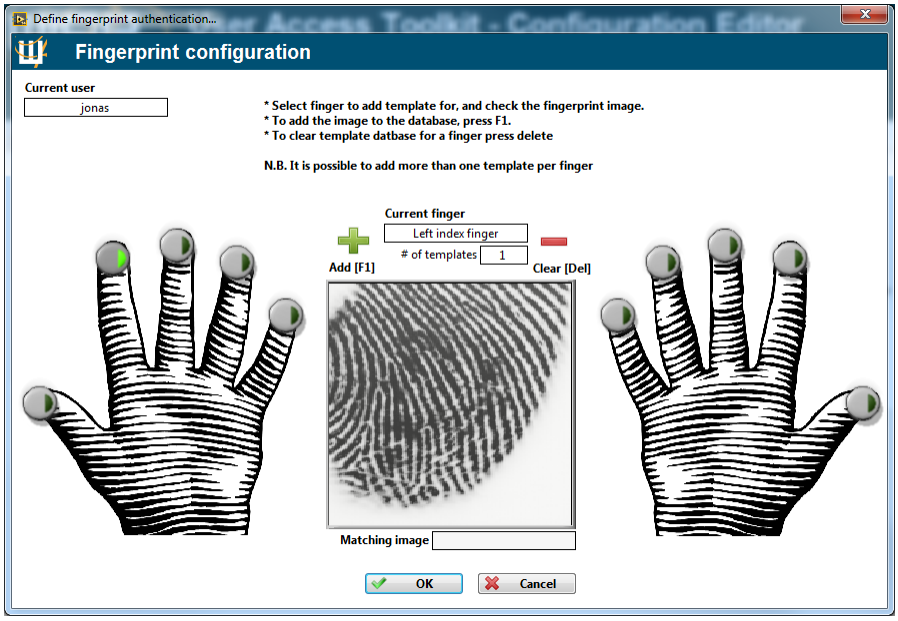


Figure 14 Fingerprint authentication setup

The setup panel in Figure 14 is used to configure the fingerprint access for a user in the User Access Toolkit. The basic usage is;

1. Select finger to use by pressing a Boolean at one of the fingertips.
2. Once the image is good enough the Add [F1] button will be activated. Press the button (or press F1 on the keyboard) to add a new template image to the database
3. The "# of templates" counter indicates how many templates that is currently stored for the selected finger.
    a. Adding more templates can result in better image matching, but can also result in more false positives.
4. Once a finger has a template added, the finger will be automatically detected and displayed in the Matching image string indicator

To delete the template(s) for a specific finger, press Clear [Del].

Removing an existing user

To remove an existing user, select one or more users in the user list and press Remove User and either accept or cancel the deletion. The default admin user cannot be removed.

Reconfigure an existing user.

To change the expiration date as and/or credentials or other user information, press Configure or double-click on the user name, and that will open the same dialog as when a new user is added (see Figure 12).

Troubleshooting

Error codes

The toolkit can return the following custom error codes, in the configuration UIs.

Code	Source text	Explanation
6400	Invalid block size for cypher!	The cypher algorithm cannot use this block size (internal error).
6401	Invalid Key size for cypher!	The cypher algorithm cannot use this key size (internal error).
6402	Unrecognized configuration format! Make sure a valid configuration is selected.	UAT is initializes with an unrecognized configuration format! Older versions of UAT might not read new UST config versions.
6403	Invalid configuration data! Check encryption password and make sure a valid configuration is selected.	The configuration data is invalid after decryption, check password and that a valid configuration is selected.
6404	Write Key failed! Check parent key value.	Update of USB dongle key value failed.
6405	User "%s" don't exist!	Unknown user name (internal error)
6406	User access toolkit is not initialized!	UAT has to be initialized before any checks can be performed.
6407	Programmatic login not possible with authentication "%s"!	The current authentication doesn't support programmatic login (internal error)
6408	Group "%s" don't exist!	Unknown user group name (internal error)
6409	Feature name "%s" not found!	Unknown feature name (internal error)
6410	Group "%s" already exists!	The user group name already exists in configuration (internal error)
6411	Invalid feature name "%s"	The name of the feature is invalid (internal error).
6412	User "%s" already Exists!	The user name already exists in the system (internal error).
6413	Authentication failed; User: %s Expired: %s	Optional error if a login fails
6414	Feature "%s" not active for the current user "%s".	Optional error for an unsupported feature.
6415	Validation failed; User "%s" Expired: %s	Optional error if a validation fails
6416	Current user "%s" is not a member of the expected groups.	Optional error for user-group check

6417	Current user "%s" is not an administrator!	Optional error if not an admin user.
6418	Attribute "%s" was not found!	Optional error if attribute not found.
6419	Authentication type is invalid!	The specified authentication type is invalid (internal error)

Technical support and Professional services

For support please check LabVIEW Tools network for updates and/or send an email to support@wireflow.se