NITGEN® EvTools

Evaluation Program for Stand-Alone Fingerprint Recognition Device

---

User Manual

Version 2.03

Nitgen EvTools

Serial Number:

Specifications can be changed without notice.

Nitgen EvTools

History

Date	Version	History
2003 – 09	0.9	Initial Version
2010 – 02	2.00	All structure modified # FIM40/FIM50 series added # Old/New/ISO/ANSI Template added # Packet Tracer Option added # Packet Creator added # Auto window resizing function added
2011 – 01	2.02	# Emulation Mode added # GPIO Configuration, GPIO Test added
2012 – 03	2.03	# Document error is fixed

Table of Contents

1. Introduction

The evaluation program “EvTools™” which is shown above, is mainly designed to test and evaluate functions of NITGEN&COMPANY’s embedded modules.

To begin with, connectivity between PC and embedded module should be prepared correctly with external power supply for the module.

Operation Environment

- Windows NT, 2000, XP, Vista, 7

Supported Devices

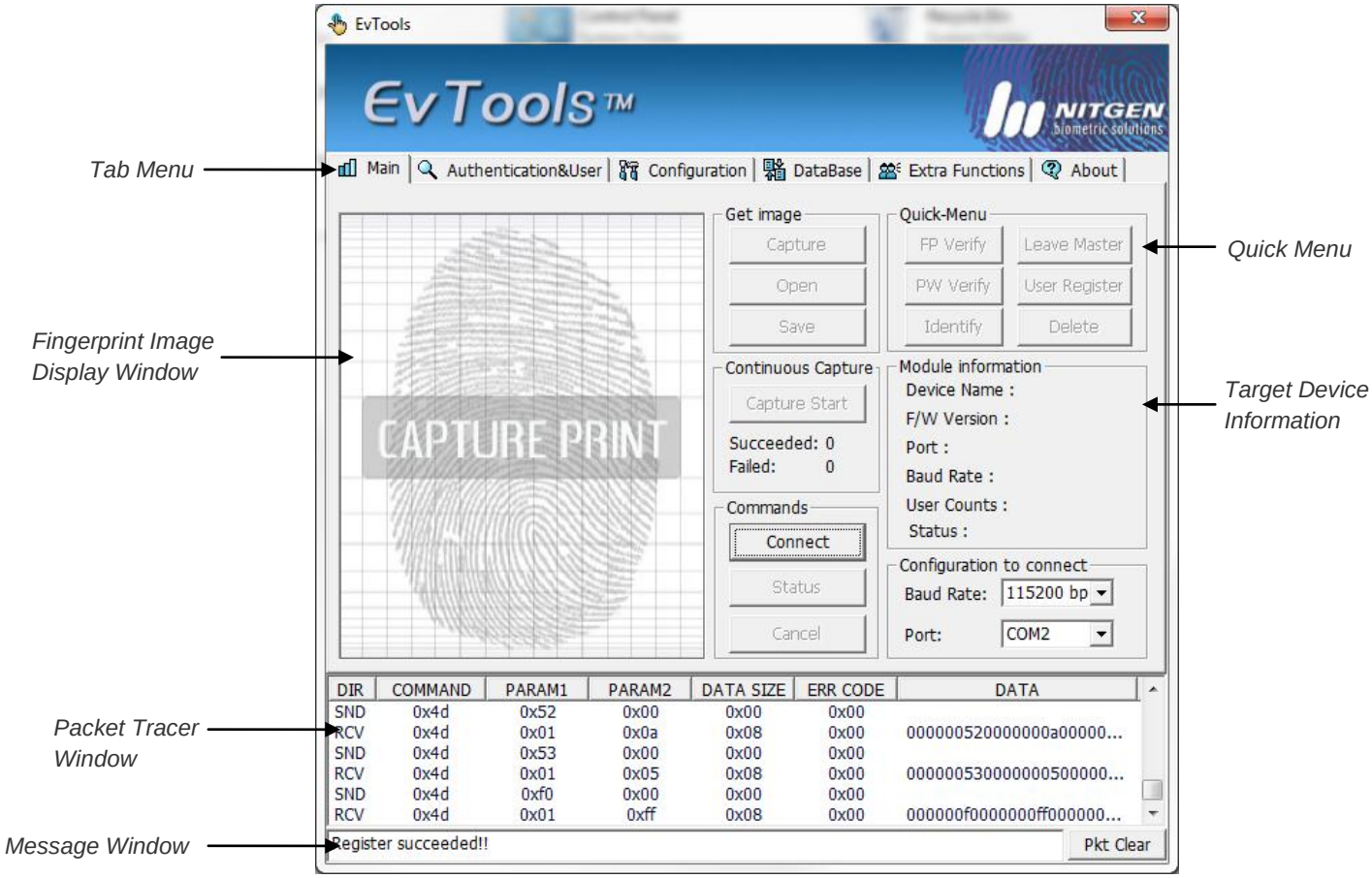
- FIM20 Series
  - FIM2030-HV
  - FIM2040-HV
- FIM22 Series
  - FIM2210-HV
  - FIM2260-HV
- FIM30 Series
  - FIM3030-HV/LV
  - FIM3040-HV/LV
  - FIM3200-HV
  - FIM1200-HV
- FIM40 Series
  - FIM4060-HV
  - FIM4110-HV
  - FIM4120-HV
  - FIM4140-HV
- FIM50 Series
  - FIM5060-HV/LV
  - FIM5110-HV
  - FIM5120-HV
  - FIM5140-HV/LV
  - FIM5260-HV
  - FIM5360-HV/LV

Supported Communication methods

- RS-232C
  - 9 pin (Female) / 9 pin (Female) cross type cable required

2. Program Layout

2.1. Evaluation Program Formation

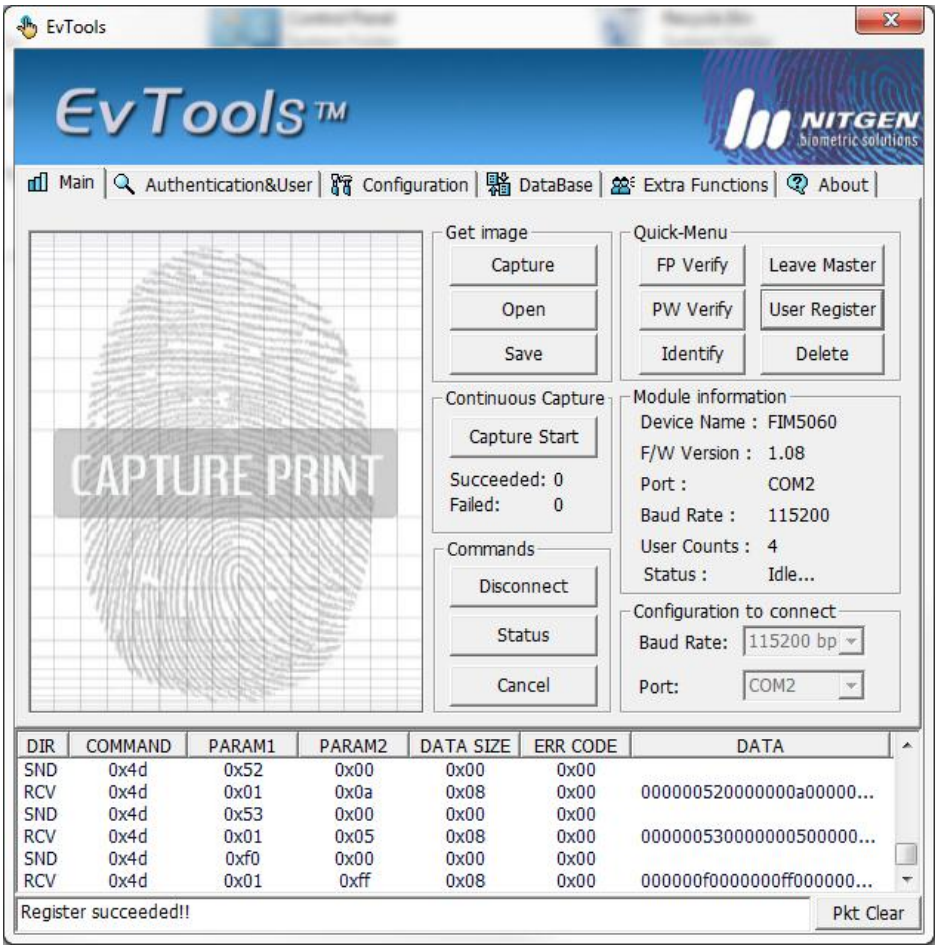


[Figure 1] EvTools Main Window

Tabs separate each section to test various functions in EvTools

3. Function Explanation

3.1. Main Window



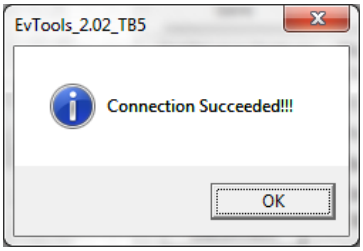
[Figure 2] Connected Main Window

3.1.1. Commands & Configuration to connect

Accurate “Baud-Rate” and “Port” Values in “Configuration to connect” should be configured to make connection between EvTools and devices.

Main Window will be displayed like [Figure 2] when connection has been made successfully by “Connect” button in “Commands” and [Figure 3] will be appeared.

Then, module’s information will be displayed and buttons also will be activated to start test.



[Figure 3] "Succeed" Message

All packets can be checked by "Packet Tracer" which is located on the bottom side of main window. For this reason, tester could be able to check status of EvTools and modules.

Tester also could obtain a status of module via "Status" button. Received message from module will be shown on the Message Window and "Status" section in "Module Information".

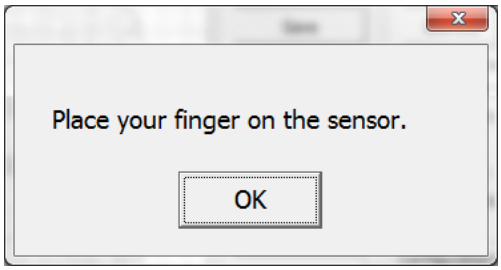
To cancel current operation, tester could be able to stop the operation via "Cancel" button.

"Status" and "Cancel" buttons are contained all windows of EvTools.

3.1.2. Get Image

Fingerprint Images could be checked and stored by "Capture", "Open", "Save" functions.

- Capture: [Figure 4] will be appeared when clicked the button. After that, place your finger on the sensor area then click "OK" to capture fingerprint image. Then, fingerprint image will be displayed on the "Fingerprint Image Display Window".



[Figure 4] "Place finger" Message

- Open: "RAW", "BMP", "WSQ (Wavelet Scalar Quantization Gray File)" formatted files could be checked by "Fingerprint Image Display Window" of Main Window.

- Save: Images that captured by sensor or loaded from image files could be stored by "Save" button with selected format and name. "RAW", "BMP", "WSQ" formats are supported.

3.1.3. Continuous Capture

This function is designed that fingerprint images will be captured and drawn on the screen continuously until stop the operation. And it checks the result of capture routine then, succeeded and failed count will be recorded on the screen.

“Capture Start” text will be changed to “Capture End” when clicking the button. Also, clicking the button again to stop operation and change the text to “Capture Start”.

Any functions like disconnection are not able to use when operate this function. Therefore, Continuous Capture should be stopped essentially to use other functions.

3.1.4. Quick-Menu

This menu contains simplified functions which are mostly used in EvTools.

- FP Verify: This function is used to compare template extracted from the captured fingerprint with enrolled template that have a same ID.
- PW Verify: This function is used to compare password stored in the module with entered password that have a same ID.
- Identify: This function is used to compare template extracted from the captured fingerprint with all fingerprint templates in database of the device.
- Enter Master: Tester could obtain master authority by clicking this button to use certain functions which are required master authority like enrollment and deletion. Tester could use “FP Verify” master authentication only in the “Quick-Menu”. Master authority will be obtained directly if no master in the module.
- User Register: Tester could enroll user-authority account directly with randomized account ID. Master authority required. For details, please refer to the “3.2.7. User Registration”.
- Delete: This function is used to delete certain account. Master authority required.

3.1.5. Module Information

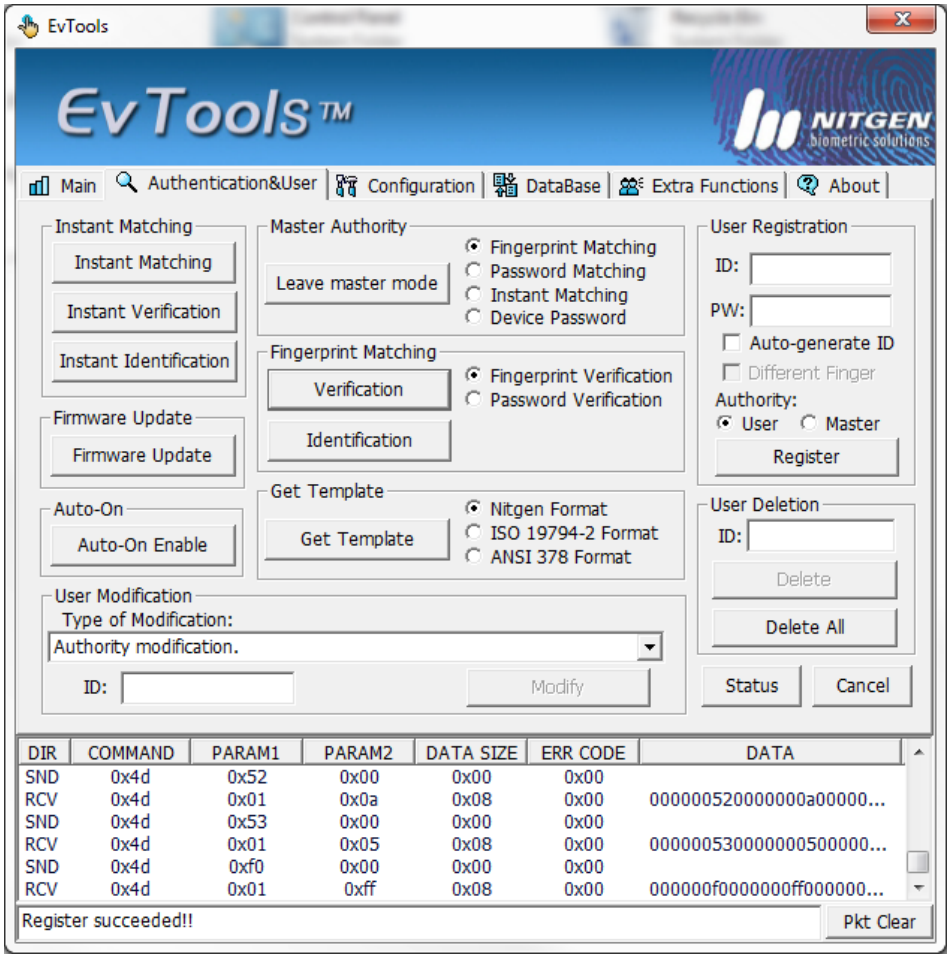
This menu contains the information of connected module.

Displayed item is,

- The name of module
- Firmware version
- Currently connected port number
- Currently connected baud-rate
- A number of accounts which are registered in module
- Current module status

These values will be updated directly if statement modification (i.e. system option modification) is occurred.

3.2 Authentication & User Window



[Figure 5] Authentication & User Window

◈ *Connection is required to access this menu.*

3.2.1. Master Authority

Tester could obtain master authority via this function.

Master authority will be obtained directly if no master and no Device Password in the module. Then, button text will be changed to “Leave Master Mode”.

On the other hand, if master account or Device Password is already registered, tester should choose an option to progress master authentication.

- Fingerprint Matching: This function is used to compare template extracted from the captured fingerprint with enrolled template of master account that have a same ID.

- Password Matching: This function is used to compare password of master account stored in the module with entered password that have a same ID.

- Instant Matching: This function is used to compare template data of master account which is stored outside of the module with template extracted from the captured fingerprint. Template data file could be created by “Get Template” function.
  - This function is not supported in FIM30 Series.

- Device Password: Device Password can be used for master authentication without master FP or password. It can be registered in “Configuration Window” with master authority. Although master accounts are not registered in the module, tester should progress master authentication if Device Password is registered in the module.

3.2.2. Fingerprint Matching

This menu consists of matching functions to compare registered data in the module with entered data.

- Fingerprint Verification: This function is used to compare template extracted from the captured fingerprint with enrolled template that have a same ID.

- Password Verification: This function is used to compare password stored in the module with entered password that have a same ID.

- Identification: This function is used to compare template extracted from the captured fingerprint with all fingerprint templates in database of the device.

3.2.3. Get Template

This function is used to make encrypted fingerprint template data from sensor. Then, encrypted data will be stored to selected format.

- Nitgen Format: This format is developed by Nitgen&Company. It is optimized to all Nitgen's products. It has fixed size.

- ISO 19794-2 Format: This format is based on the ISO 19794-2 standard. It has variable size.
  - This function is supported in firmware version 1.46 or higher in FIM30 series, firmware version 1.90 or higher in FIM20 series and all FIM22/FIM40/FIM50 series.

- ANSI 378 Format: This format is based on the ANSI standard. It has variable size.
  - This function is supported in firmware version 1.46 or higher in FIM30 series, firmware version 1.90 or higher in FIM20 series and all FIM22/FIM40/FIM50 series.

3.2.4. Instant Matching

This function is used to compare template data which is stored outside of module with other template data.

- Instant Matching: This function is used to compare template data which is stored outside of the module with template extracted from the captured fingerprint. Template data file could be created by "Get Template" function. In this function, database of the module is will not be searched.
  - Tester should select the type of template data file before image capture in FIM30 Series. Correct type should be selected to make correct result.

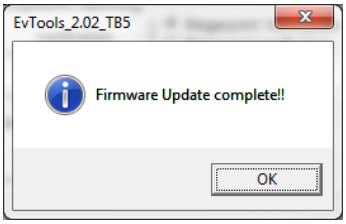
- Instant Verification: This function is used to compare template data which is stored outside of the module with selected account's template in the database of the module. The sensor will not be operated.
  - This function is not supported in FIM30 Series.

- Instant Identification: This function is used to compare template data which is stored outside of the module with whole database's templates of the module.
  - This function is not supported in FIM30 Series.

3.2.5. Firmware Update

This function is used to update firmware to currently connected device.

The firmware update progress will be started automatically when firmware file is selected. Then, [Figure 6] will be appeared if firmware updating has done successfully. Before finished, please do not turn off the module and avoid cancelation.



[Figure 6] "Update Succeeded" Message

3.2.6. Auto-On

Tester's fingerprint will be captured and authenticated automatically when this function is enabled.

The button text will be changed to "Auto-On Disable" when clicking button. Then, Auto-On operation is started. After that, module will send a result of identification to EvTools if fingerprint is detected and captured.

Other functions can not be able to use during Auto-On enabled. For this reason, Auto-On function should be released to use other functions.

This function is available at FIM22/FIM40/FIM50 series only.

3.2.7. User Registration

This function is used to register new account into the module.

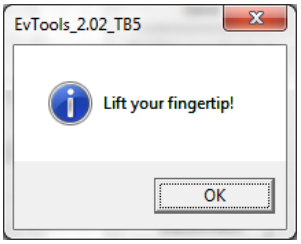
Various options are available and are shown below.

- Auto-generate ID: ID value will be created from lower number (i.e. 0000, 0001, 0002, 0003 …) and stored automatically. Password will not be registered.

- Different Finger: If this option is selected, first entered fingerprint and second entered fingerprint can be different.
  - This function is not available at FIM40/FIM50 series.

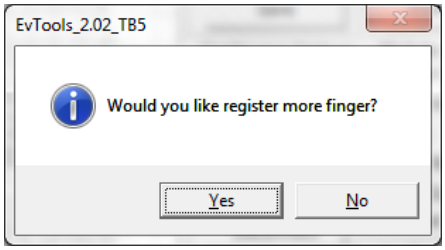
- Authority: Authority can be selected; User or Master.

When register new account, fingerprint should be entered twice. After the first fingerprint captured, [Figure 7] will be appeared. At this moment, tester should detach finger and place on the sensor again to avoid registration failure. Because, it is a meaningless process that a comparison with same fingers.



[Figure 7] After the first fingerprint capturing

Up to ten fingerprints are allowed to register in FIM40/FIM50 series. Fingerprints will be registered step by step and twice entering is required per each finger. When a fingerprint was registered successfully, tester should decide register more or not in [Figure 8].



[Figure 8] Register additional fingerprint or not

On the one hand, if “Yes” was selected in [Figure 8], registration routine for next fingerprint will be started. On the other hand, if “No” was selected in [Figure 8], entered fingerprints will be saved in the module. However, tester will not register fingerprints anymore when ten fingerprints were entered. In this case, entered ten fingerprints will be saved in the module and done.

3.2.8. User Modification

This function is used to modify selected user information. Account’s ID should be entered firstly to progress this function.

Various options are available shown below.

- Authority modification: Change the authority of selected account. Different authority value should be entered to modify the authority successfully. Error will be returned if same authority

value has been entered. To set master authority, please input “1” and to set user authority, please input “0”.

- Password modification: Change the password of selected account.

- User Security Level modification: Apply the personal security level to selected account. Basically, all accounts are using system configuration values; Verification Security Level, Identification Security Level. However, personal security level could be configured by this function. This value is independent of system configuration values.
  - Verification Matching should be selected to use personal security level.
  - Accurate fingerprint input is required to pass the authentication if value of security level is higher than default. On the other hand, authentication will be succeeded easily if value of security level is lower than default.
  - The range of value is 1 ~ 9.

- 1st finger template modification with same finger from host: Change the first fingerprint’s templates of selected account to same fingerprint’s template data which is stored outside of the module.
  - Two same fingerprint’s template data files required.
  - This function will be failed if selected template data was different finger from selected account’s template data which is stored in the module.

- 1st finger template modification with different finger from host: Change the first fingerprint’s templates of selected account to fingerprint’s template data which is stored outside of the module.
  - Two template data files required.
  - Any fingerprint’s template data will be accepted.

- 2nd finger template modification with same finger from host: Change the second fingerprint’s templates of selected account to same fingerprint’s template data which is stored outside of the module.
  - Two same fingerprint’s template data files required.
  - This function will be failed if selected template data was different finger from selected account’s template data which is stored in the module.
  - This function can be used in “4 Template Mode” only.

- 2nd finger template modification with different finger from host: Change the second fingerprint’s templates of selected account to fingerprint’s template data which is stored outside of the module.
  - Two template data files required.

- Any fingerprint's template data will be accepted.
- This function can be used in "4 Template Mode" only.

❖ 1st finger template modification with same finger from sensor: Change the first fingerprint's templates of selected account to same fingerprint's template data extracted from captured fingerprint.
- Two same fingerprint entries required.
- This function will be failed if extracted template data was different finger from selected account's template data which is stored in the module.

❖ 1st finger template modification with different finger from sensor: Change the first fingerprint's templates of selected account to fingerprint's template data extracted from captured fingerprint.
- Two fingerprint entries required.
- Any fingerprint's entry will be accepted.

❖ 2nd finger template modification with same finger from sensor: Change the second fingerprint's templates of selected account to same fingerprint's template data extracted from captured fingerprint.
- Two same fingerprint entries required.
- This function will be failed if extracted template data was different finger from selected account's template data which is stored in the module.
- This function can be used in "4 Template Mode" only.

❖ 2nd finger template modification with different finger from sensor: Change the second fingerprint's templates of selected account to fingerprint's template data extracted from captured fingerprint.
- Two fingerprint entries required.
- Any fingerprint's entry will be accepted.
- This function can be used in "4 Template Mode" only.

This function is available at FIM20/22/30 series only. But, only 1st finger can be modified in FIM30 series.

3.2.9. User Deletion

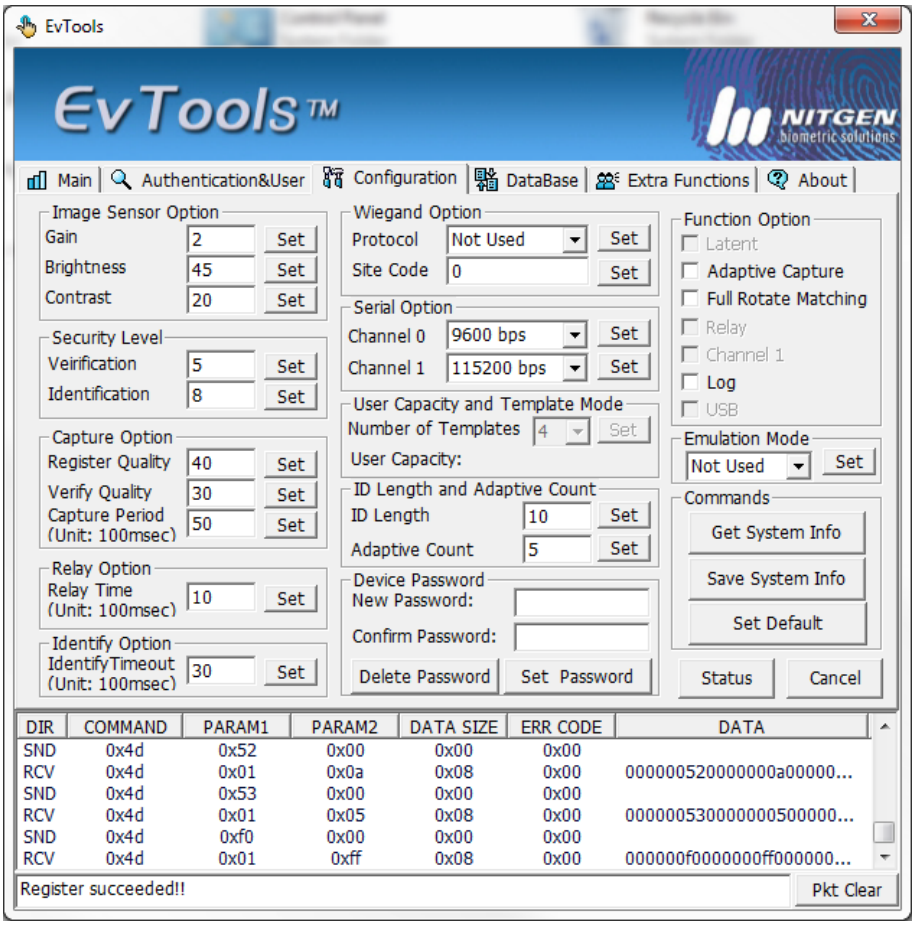
This function is used to delete selected account.

Selected account information could be deleted by clicking "Delete" button.

All accounts could be deleted by clicking "Delete All" button.

Please be careful. Deleted accounts will not be restored.

3.3 Configuration Window



[Figure 9] Configuration Window

◈ *Connection and Master Authority are required to access this menu.*

3.3.1. Introduction

This window can be used to confirm and change various system configuration values.

Master Authority is essentially required to access this menu.

Configuration values will be loaded and shown automatically on the screen when “Configuration” tab has been selected.

3.3.2. Image Sensor Option

This menu is related with captured image's quality. Image quality can be improved by modification of Gain, Brightness and Contrast.

- Gain: Image's gain can be configured. High value means thick image.
  - Default Value: 2
  - Range: 1, 2, 4

- Brightness: Image's brightness can be configured.
  - Default Value: 45
  - Range: 0 ~ 99

- Contrast: Image's Contrast can be configured.
  - Default Value: 20
  - Range: 0 ~ 99

3.3.3. Security Level

Verification, Identification Security Level can be configured in this menu.

Accurate fingerprint input is required to pass the authentication if value of security level is higher than default. On the other hand, authentication will be succeeded easily if value of security level is lower than default.

- Verification: 1 to 1 authentication Security Level can be configured.
  - Default Value: 5
  - Range: 1 ~ 9

- Identification: 1 to N authentication Security Level can be configured.
  - Default Value: 8
  - Range: 6 ~ 9

3.3.4. Capture Option

This menu is related with sensor's operation.

- Register Quality: This configuration is used to set limitation of image's quality in registration. Next to capturing, image's quality is provided from template extraction routine. Capturing will not be succeeded if image's quality was lower than this configuration value.
  - Default Value: 40
  - Range: 40 ~ 100

- Verify Quality: This configuration is used to set limitation of image's quality in verification. Capturing will not be succeeded if image's quality was lower than this configuration value.
  - Default Value: 30
  - Range: 30 ~ 100

- Capture Period: This configuration is used to set timeout of sensor's capturing. For example, next to ID entering in verification, the sensor will be waiting an entry of fingerprint for the time; this value.
  - Default Value: 50
  - Range: 1 ~ Unlimited
  - Unit: 100ms

3.3.5. Relay Option

- Relay Time: This configuration is used to set length of relay's opened or closed period.
  - Default Value: 10
  - Range: 1 ~ 100
  - Unit: 100ms
  - "Relay" check box in "Function Option" menu should be checked to user this function.
  - This function is always available in FIM40/FIM50 series regardless of "Relay" check box.
  - This function is not available in FIM30 series.

3.3.6. Identify Option

- Identify Timeout: this configuration is used to set timeout of template searching in identification.
  - Default Value: 255
  - Range: 5 ~ 255
  - Unit: 100ms

3.3.7. Wiegand Option

Authentication result can be printed out by Wiegand Protocol.

- Protocol: This configuration is used to set type of Wiegand Protocol and to set use or not.
  - Default Value: 26Bit
  - Range: Not Used, 26Bit, 34Bit.

- Site Code: This configuration is used to set Site Code which is a member of Wiegand Protocol.
  - Default Value: 0
  - Range: 0 ~ 255 in 26Bit, 0 ~ 65535 in 34Bit

This function is not available at FIM30 series.

3.3.8. Serial Option

Baud-Rate can be configured in this menu.

Although default configuration is Channel 0 enable with 9,600bps and Channel 1 disable, Channel 0 and Channel 1 can be enabled and configured from 9,600bps to 115,200bps.

In FIM40/FIM50, Channel 0 is operated as a TTL Level UART and Channel 1 is operated as a RS-232 Level UART. Both Channels are also always enabled.

After applying the changed Baud-Rate value, EvTools should be reconnected to apply the Baud-Rate and to enable to save the value; changed value cannot be saved directly until a reconnection is made.

If shut-down module's power-supply after applying the changed Baud-Rate without saving, changed value will not be saved. Then it will be connected with before Baud-Rate next time.

3.3.9. User Capacity and Template Mode

This configuration is used to set a number of templates per account; "2" (two templates, one fingerprint usage) or "4" (four templates, two fingerprint usage).

The default value is "2".

Also, User Capacity will show maximum account capacity of the module.

This configuration is available at FIM20/FIM30/FIM22 series only.

3.3.10. ID Length and Adaptive Count

This configuration is used to set ID length and number of adaptive capture.

- ID Length: Account's ID length can be configured.
  - Default Value: 10
  - Range: 4 ~ 15
- Adaptive Count: Maximum number of adaptive capture can be configured.
  - Adaptive Capture: Automatic sensor configuration adjustment function. In this mode, the module is capturing images several times to apply proper sensor configuration values.
  - Default Value: 5
  - Range: 0 ~ 255

This configuration is available at FIM40/FIM50 series only.

3.3.11. Function Option

This configuration is consists of items which could be configured as enable or disable only.

- Latent: This is a remained fingerprint recognize function.
  - Default Value : Disable
  - This configuration is available at FIM2030, FIM2040, FIM3030, and FIM3040 only.

- Adaptive Capture: Automatic sensor configuration adjustment function. In this mode, the module is capturing images several times to apply proper sensor configuration values.
  - Default Value: Disable
  - This configuration is available at FIM2030, FIM2040, FIM3030, FIM3040, FIM2260, FIM4060, and FIM5060 only.

- Full Rotate Matching: When this function is enabled, fully rotated fingerprint (up to 360 degrees) could be recognized.
  - Default Value: Disable
  - This configuration is available at firmware version 1.46 or higher in FIM30 series, firmware version 1.90 or higher in FIM20 series and all FIM22/FIM40/FIM50 series.

- Relay: Whether Relay will be used or not could be configured.
  - Default Value: Disable

- Channel 1: Whether Channel 1 will be used or not could be configured.
  - Default Value: Disable
  - This configuration is available at FIM20/FIM30/FIM22 series only.

- Log: Whether Log will be stored in the module or not could be configured.
  - Default Value: Enable

3.3.12. Device Password

This function is used to set Device Password.

Device Password can be used for master authentication without master fingerprint or password. It can be created only in master mode.

The password's length is limited up to 16 characters. Also the value of "New Password" and "Confirm Password" should be same to register password successfully.

To delete Device Password, just click "Delete Password" button.

3. 3. 13. Emulation Mode

FIM40/50 Series could be used as FIM20/30 Series through this function.

This function is only available in FIM40/50 Series and this will not be operated if account is registered in the module.

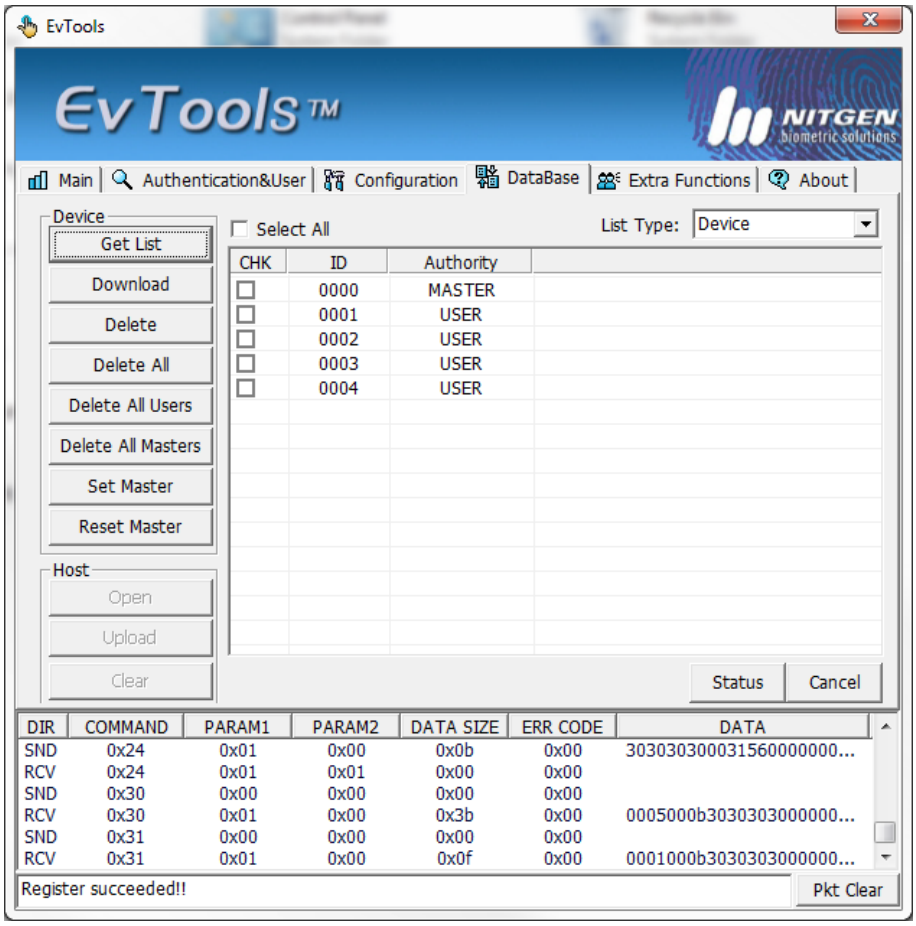
Please be careful to use this function because available protocols are different in each emulation mode.

Available protocols in each module could be confirmed by the ComProtocol document.

3.3.14. Commands

- Get System Info: Read and display current module's system configuration values.
- Save System Info: Save current system configuration values to keep permanently.
- Set Default: Change current system configuration values to default values.

3.4. Database Window



[Figure 10] Database Window

◈ *Connection and Master Authority are required to access this menu.*

3.4.1. Introduction

This window is used to transfer database between device and host. The database also could be modified and deleted.

To handle device's database, the List Type should be selected to "Device". On the other hand, to handle host's database, the List Type should be selected to "Host".

This window is not available at FIM30 series.

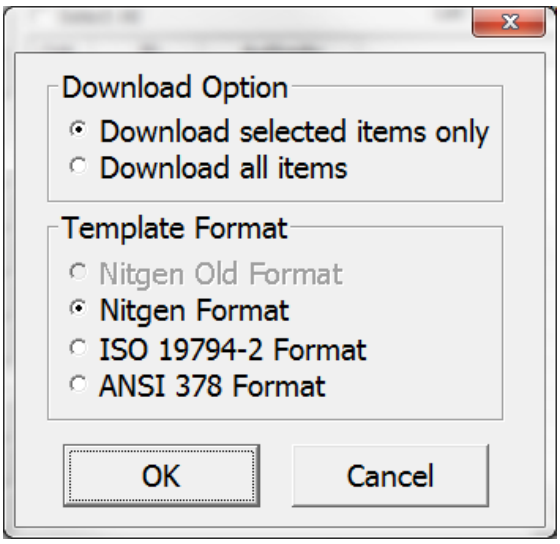
3.4.2. Device – Get List

All enrolled accounts will be displayed on the screen. The one column is account's ID and other column is authority field for a master distinction.

3.4.3. Device – Download

This function is used to get account record composed of registered account's ID, password, encrypted fingerprint template, authority and registered time from the module and save it as a file.

To get several account records of the module, tester should check "CHK" of account to download selected account record only or should check "Select all" to download whole account records. Then, [Figure 11] will be appeared.



[Figure 11] Download Option

- Download Option: Tester could be able to choose a type of download; Download selected items only or Download all items.
- Template Format: Tester could be able to choose a type of template format.
  - Nitgen Old Format: This format is prepared for compatibility with old version modules; firmware version 1.89 or lower in FIM20 series, firmware version 1.45 or lower in FIM30 series.
  - Nitgen Format: This format is currently used in all Nitgen&Company's modules. It is a standard format of whole module products.
  - ISO 19794-2 Format: ISO 19794-2 standard format.
  - ANSI 378 Format: ANSI 378 standard format.

After clicking "OK", database files will be stored in the folder where "EvTools.exe" is stored. Account's ID will be used as a filename.

3.4.4. Device – Delete

This function is used to delete selected account by clicking “Delete” button from the module permanently.

3.4.5. Device – Delete All

This function is used to delete whole accounts by clicking “Delete All” button from the module permanently.

3.4.6. Device – Delete All Users

This function is used to delete accounts which have a user authority by clicking “Delete All Users” button from the module permanently.

3.4.7. Device – Delete All Masters

This function is used to delete accounts which have a master authority by clicking “Delete All Masters” button from the module permanently.

3.4.8. Device – Set Master

This function is used to change selected account’s authority to master authority. If master account was selected, error message will be returned.

3.4.9. Device – Reset Master

This function is used to change selected account’s authority to user authority. If user account was selected, error message will be returned.

3.4.10. Host – Open

This function is used to open account records which are stored by “Device-Download” button and to display loaded account’s information.

Detail of account’s information is consists of ID, authority, stored time as a file and a size of file.

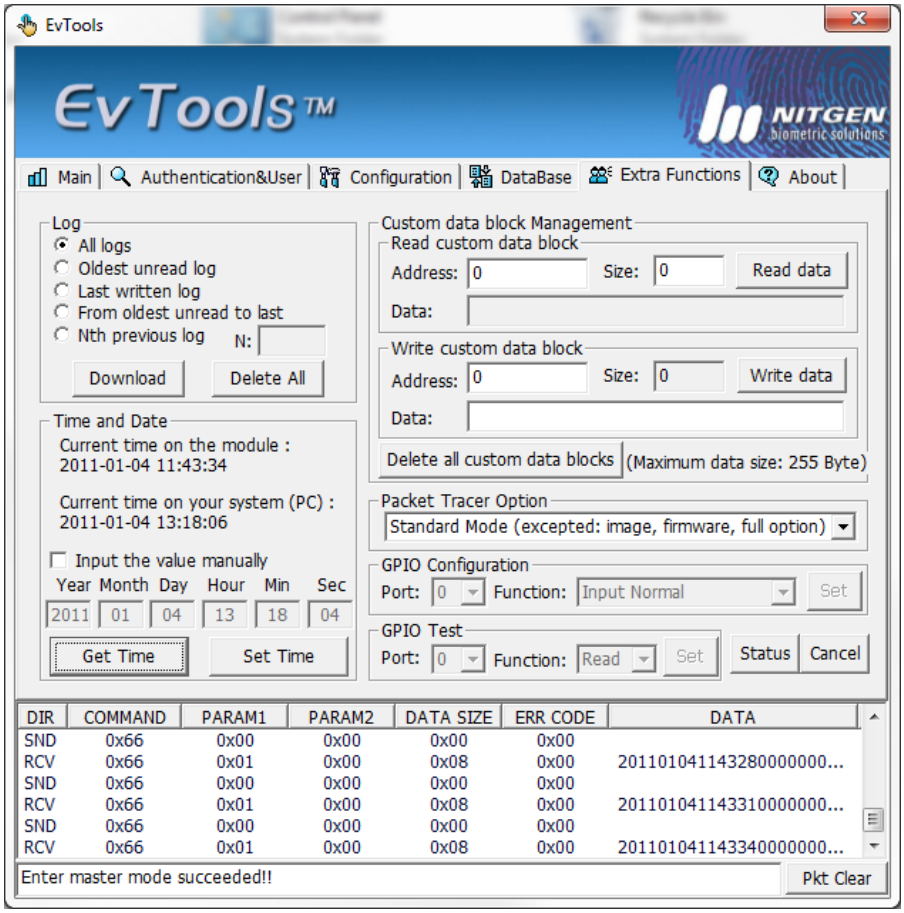
3.4.11. Host – Upload

This function is used to upload selected accounts to the module.

3.4.12. Host – Clear

This function is used to clear the list of loaded accounts.

3.5. Extra Functions Window



[Figure 12] Extra Functions Window

◆*Connection and Master Authority are required to access this menu.*

3.5.1. Introduction

This window is used to provide various additional functions; Log, Time & Date, Custom Block, I/O Control and even Packet Tracer Option.

3.5.2. Log – Log Download

Log data stored in the module can be saved as a file. To save log of the module, Log configuration should be enabled in Configuration Window.

Various options are available to store log data.

- All Logs: Whole log data of the module will be stored.
- Oldest unread log: Oldest unread log data of the module will be stored.
- Last written log: Last written log data of the module will be stored.
- From oldest unread to last: Whole unread log data of the module will be stored.
- Nth previous log: Nth log data will be stored.
  - Tester should write an index of log data.
  - Range: 0 ~ 8191
  - "0" means the oldest log data and "8191" means the last log data.

Downloading period depend on a number of logs.

3.5.3. Log – Delete All

This function is used to delete whole log data of the module.

3.5.4. Time and Date – Get Time

This function is used to read the time and date from the module and display it on the "Current time on the module".

The time and date of the module will be renewed when EvTools makes a connection with the module.

To keep real-time in the module, external real-time clock should be attached.

3.5.5. Time and Date – Set Time

This function is used to apply time and date to the module.

Time and date could be configured manually via "Input the value manually" check box. Configured time and date also can be applied when clicking "Set Time" button with enabled "Input the value manually" check box.

On the other hand, current PC's time and data will be applied when clicking "Set Time" button without "Input the value manually" selection.

3.5.6. Custom data block Management

All modules have a pre-allocated memory area for user application support.

It is possible to write/read application specific data on the memory.

Custom data could be written byte by byte and could read several bytes at once. These custom data will not be erased if modules were turned-off; however, data overwriting is not allowed.

Maximum size of data transferring at once is 256 bytes.

- Read custom data block: Tester should input the start address of data to load firstly. Then, input the size of the data. Finally, clicking “Read custom data” button to read selected data.

- Write custom data block: First of all, input the start address of custom data block and write data on the data section. Then, clicking “Write custom data” button to write selected data.

- Delete all custom data blocks: Delete whole custom data block.

◈ *The size of Custom Data Block depend on the module. Tester should refer to the ComProtocol document before custom data block usage.*

3.5.7. Packet Tracer Option

Packet Tracer is a tool that it used to observe received and transmitted packets between EvTools and modules.

It can be configured through this configuration.

- Standard Mode: Almost all packets can be checked and confirmed; however, some packets; Image Drawing, Firmware Uploading and Full-Option Loading, are excepted because these packets tend to transfer several times in a short period of time.
- Show all packets: whole packets will be displayed.
- Packet Tracer function disabled: Do not use Packet Tracer.

3.5.8. GPIO Configuration

GPIOs(General Purpose Input and Output) can be configured through this function. Please refer to “Appendix F” of “ComProtocol” document to confirm various options and operating rules of GPIOs.

Configured values can be stored permanently by Save System Info of Configuration window.

This function is available at FIM40/FIM50 series only.

3.5.9. GPIO Test

GPIOs can be controlled via this function when selected GPIO is configured as normal input or output in FIM40/FIM50 series.

- Read: Selected GPIO should be configured as “Input Normal” to read the value of the port. In the other case, “Invalid Parameter!!” will be returned.
- High: Selected GPIO should be configured as “Output Normal” to make high level.
- Low: Selected GPIO should be configured as “Output Normal” to make low level.

Even though I/O function is supported in FIM20/FIM22 and FIM30, this version of EvTools is not suitable to test old I/O function efficiently. Please use old version of EvTools to test old I/O function.

3.6. About Window

This window shows the information of EvTools. Tester also could be able to make a packet to send the module directly for test purpose in Packet Creator.

[Figure 13] About Window

3.6.1. Packet Creator

This function is used to make a packet by hand to transfer to the module. Tester should refer to "ComProtocol" document to use this function correctly. Because certain routines are requiring a number of packet transferring to finish the work.

Tester also should use hex characters only and "0x" should be omitted.

3.7. Additional Features

3.7.1. Packet Tracer

Packet Tracer is a tool that it used to observe received and transmitted packets between EvTools and modules.

It can be configured by Packet Tracer Option in User Window.

If packet contains data, the data will be shown in the data column. Please refer to “ComProtocol” document to analyze the data.

Whole Packet Tracer’s list area could be cleared by clicking “Pkt Clear” button.

3.7.2. Message Window

Various results of the commands and current status are displayed on the Message Window.

It is located on the bottom of Main Window.

3.7.3. EvTools Logo

This is an EvTools logo. Tester could be able to access Nitgen&Company’s webpage directly by clicking the logo.

Also, the webpage could be accessed by clicking logo in the About Window.

3.7.4. Low Resolution Support Function

If the monitor’s resolution is 800 * 600 or lower, EvTools window would become smaller (logo will be disappeared). However, EvTools can be sliced if resolution was smaller than 640 * 480.

Appendix A. Support Information

NITGEN&COMPANY CO., LTD.

B-12F PaxTower Nonhyun-dong, Gangnam-gu,
Seoul, 135-010 Korea

Tel: +82-2-556-7115

Fax: +82-2-556-7118

E-mail: Customer@nitgen.com