

Setting up Viridi integration with Paxton Net2 Server

Overview

Integrating Viridi biometric readers with the Paxton Net2 system is made possible by using UNIS4 and QEManager (the software required can be downloaded [here](#)).

The installation and configuration steps to follow are:

1. Install Net2 (view application notes [here](#))
2. Install UNIS4
3. Install QEManager

Versions of software used in this documentation:

Net2 – 5.04.6918.5578

UNIS4 – 4.2.7.18

QEManager – 1.3.1.3



Install Net2 and configure the door controller for Wiegand use

1. Reader type -> Wiegand reader
2. Token data format – Wiegand 26 bit
3. Reader operating mode -> Token Only

ACU serial number: 65239487

Door name:

Door group:

Door open time: seconds

Unlock the door during:

☐ Only unlock the door once a user has been granted access

☐ Silent operation

Unlock relay 2 during:

Reader 1 | Reader 2 | Alarm | Events | Fire alarm inputs | Multizone Intruder | Access rights | Camera integration

Reader details

Name:

Reader type:

Keypad type:

Token data format:

Operating mode

Reader operating mode:

☐ Timed operating modes - This allows for different reader operation during a selected timezone.

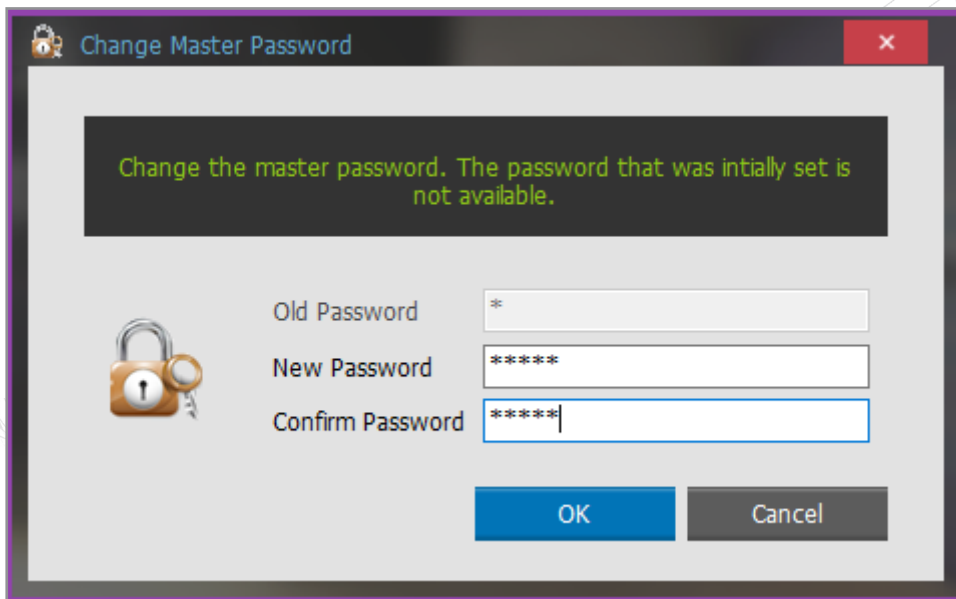
During this timezone:

This reader will operate as:

Reader action - This is what will happen when a valid access is granted.

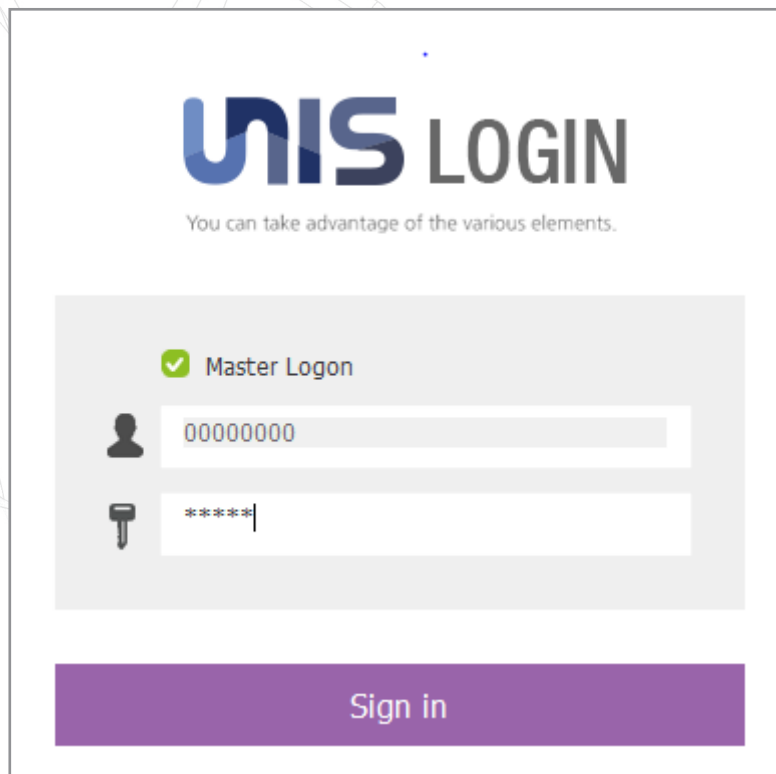
Installing and setting up UNIS4

1. Install UNIS4 (please refer to the Paxton Integrations page for the latest available versions).
2. When using UNIS for the first time create a new password



A screenshot of a 'Change Master Password' dialog box. The title bar says 'Change Master Password' with a red close button. Inside, a green message box states: 'Change the master password. The password that was initially set is not available.' Below this, there is a padlock icon. To the right of the icon are three input fields: 'Old Password' (containing a single asterisk), 'New Password' (containing six asterisks), and 'Confirm Password' (containing six asterisks). At the bottom right are 'OK' and 'Cancel' buttons.

3. Login to UNIS by selecting Master and entering the new password



A screenshot of the 'UNIS LOGIN' screen. The header features the 'UNIS LOGIN' logo and the tagline 'You can take advantage of the various elements.' Below the header, there is a section titled 'Master Logon' with a green checkmark icon. Under this section, there are two input fields: one for a username (containing '00000000') and one for a password (containing six asterisks). At the bottom of the screen is a large purple 'Sign in' button.

8. To send the Wiegand settings to the Virdi readers, select a Terminal and Bit Length and click on Send to Terminal.

Set Wiegand

Set wiegend in out format and import and export from the terminal

Wiegand Out Wiegand In

Code	Name
0001	26 bit Wiegand

Input info

Code: 0001

Name: 26 bit Wiegand

Register Modify Delete

Basic info

Terminal: 0001 : Test Reader

Bit Length: St. 26bit

Port State: Active Low

Send Fail: Not Anything

Output Type: UserID

Read from Terminal Send to Terminal

Custom Size: 1

Site Code: 0

Fail Data: 0

Intervar Time(us): 0

Width Time(us): 0

Set Field

Field	Value
1	E
17	
33	
49	
65	
81	
97	
113	
16	
32	0
48	
64	
80	
96	
112	
128	

Set Parity

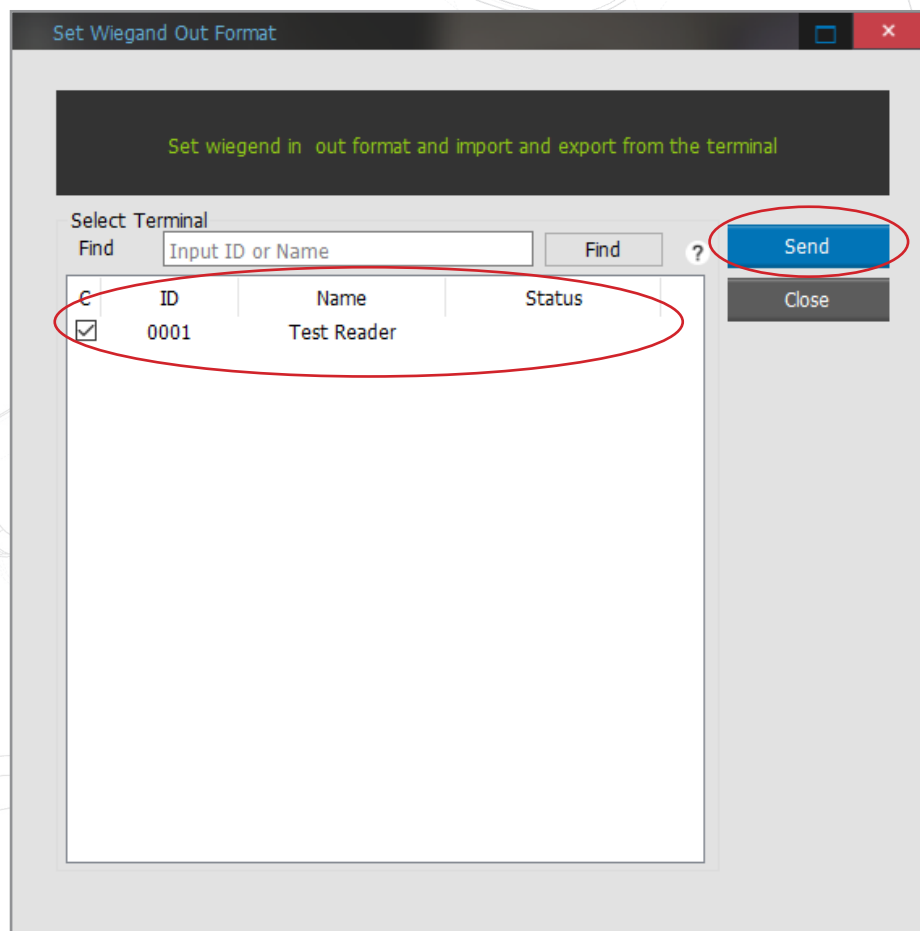
Field	Value
1	
17	
33	
49	
65	
81	
97	
113	
16	
32	
48	
64	
80	
96	
112	
128	

Field Type

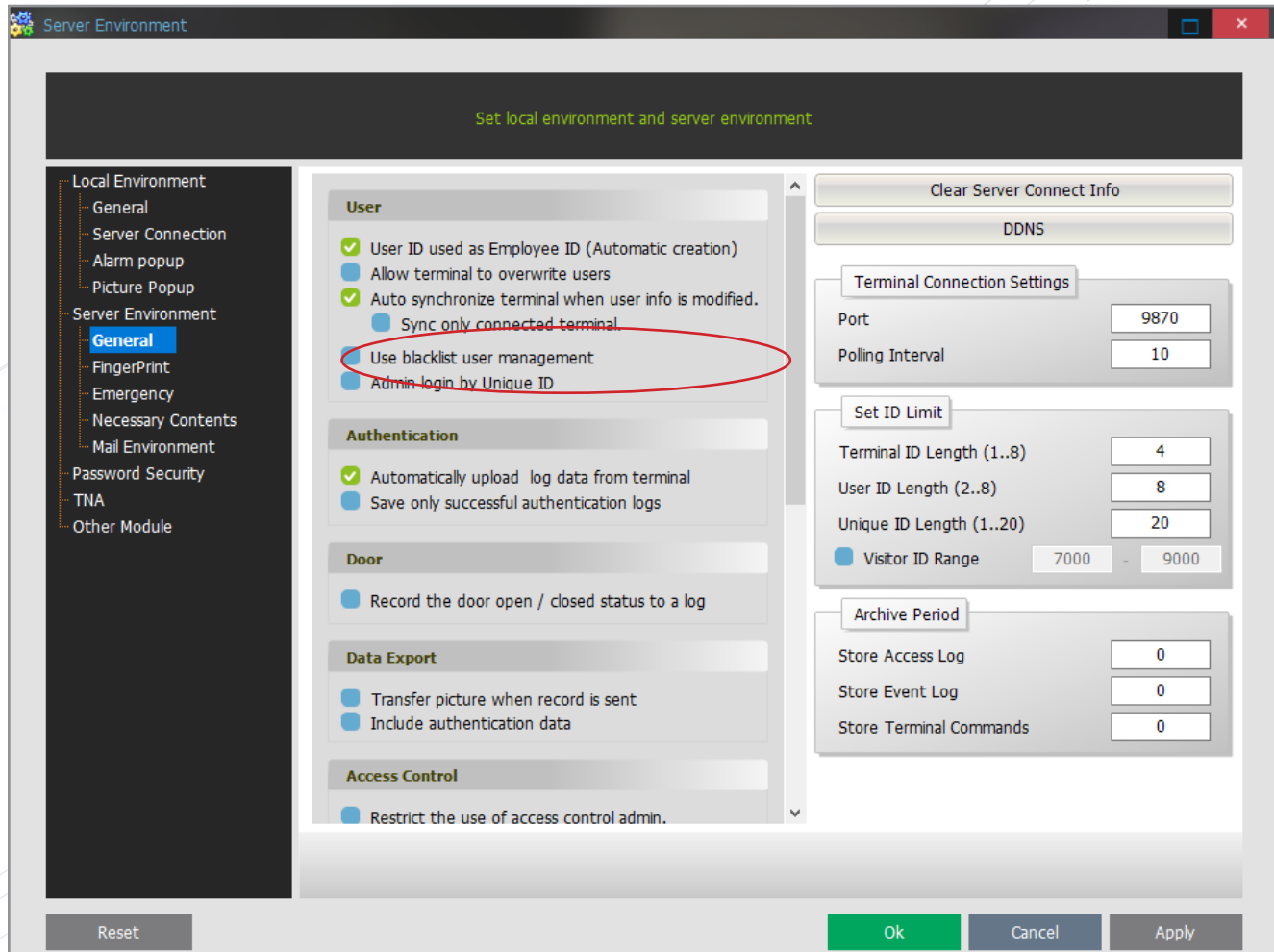
- S Site Code
- D Data(ID)
- 0 Fixed 0
- 1 Fixed 1
- O Odd Parity
- E Event Parity
- Point

Ready

9. Select all the readers and click on Send

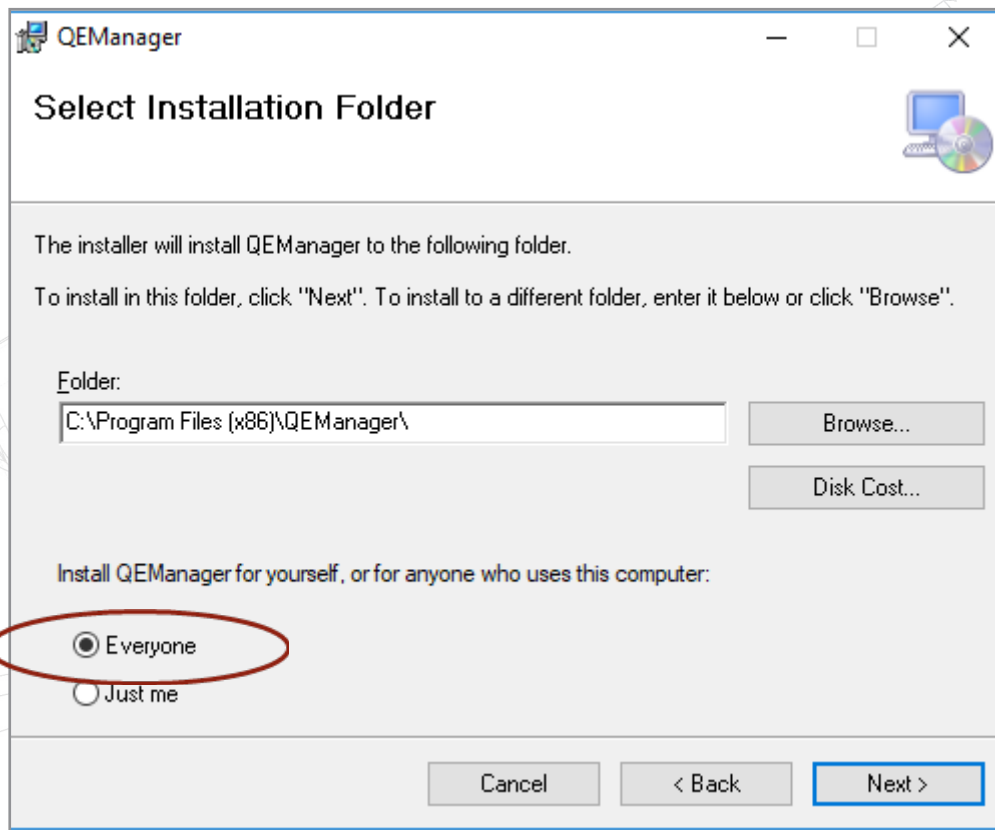


10. To setup real-time synchronizing of users, Go to Environment Settings (menu is hidden away on the right side of the screen. Move the mouse cursor to the right border of the UNIS screen to view the menu).
11. Under Environment -> General -> Users - ensure the option to "Auto synchronize terminal when userinfo is modified" is selected. Click Apply.

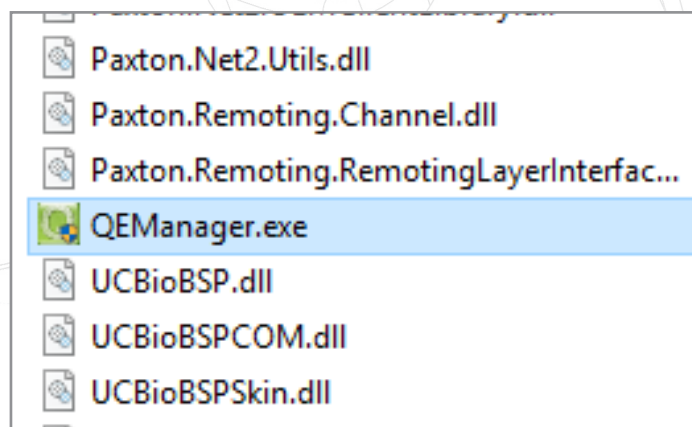


Installing and setting up QEManager

1. When installing QEManager select install for Everyone



- Go to C:\Program Files (x86)\QEManager, right click on QEManager.exe and send to your desktop (create a shortcut)



- To run QEManager, right click the shortcut on the desktop and select Run as Administrator
- Enter the password for Net2:

Environments

UNIS Connect Info

UNIS Server
 Server IP: 127.0.0.1
 Server Port: 9871

UDB Server
 UDB IP: 127.0.0.1
 UDB Port: 9872

ODBC: UNIS
 DB ID: unisuser
 DB Pwd: *****

Paxton Info

Net2 Connect Info
 IP Address: 127.0.0.1
 Port: 8025
 ID: System engineer
 Password: *****

Ok Cancel

- To view if the connection has succeeded, double click on the QEManager icon in the taskbar (hidden)

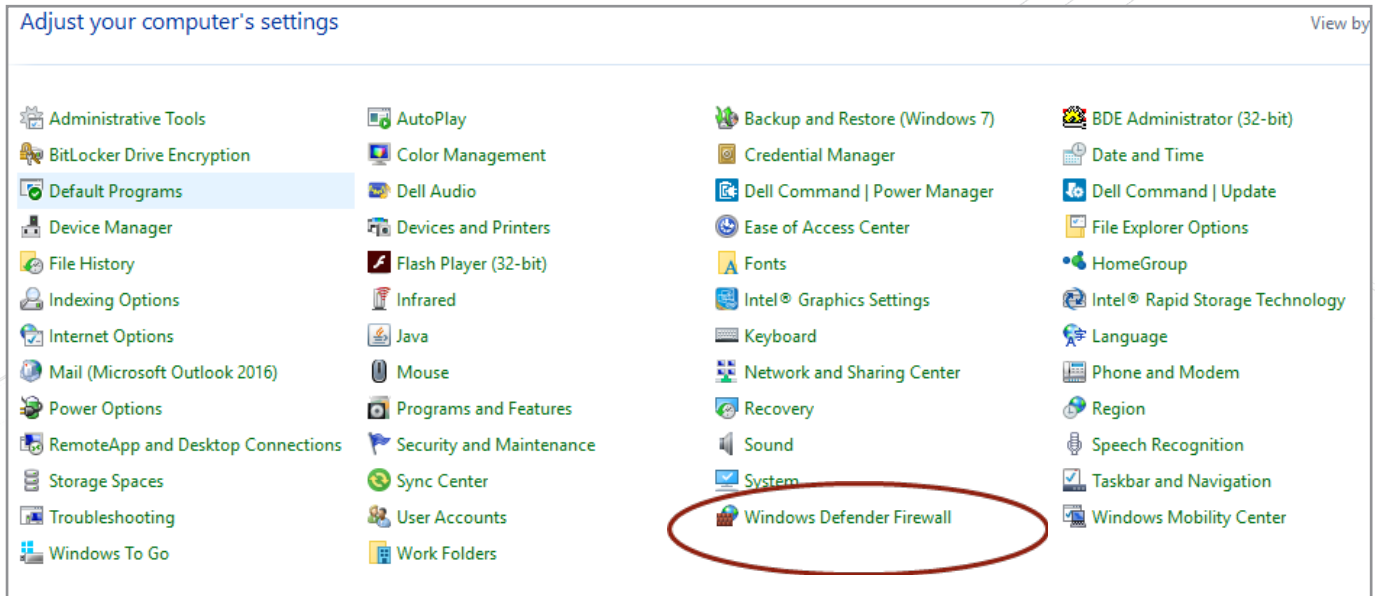
Quick Enroll Manager

Type	DateTime	UID	Message
Info	2018-07-09 12:31:...	0	Connect Paxton Net2..OK
Info	2018-07-09 12:31:...	0	Load General Database..OK
Info	2018-07-09 12:31:...	0	Load General Database..
Info	2018-07-09 12:31:...	0	Init FP Info..
Info	2018-07-09 12:31:...	0	Load System Database..OK
Info	2018-07-09 12:31:...	0	Load System Database..
Info	2018-07-09 12:31:...	0	Connect Auth Server..OK
Info	2018-07-09 12:31:...	0	Connect Auth Server..
Info	2018-07-09 12:31:...	0	Connect UDB Server..OK
Info	2018-07-09 12:31:...	0	Connect UDB Server..
Info	2018-07-09 12:31:...	0	Load MultiLanguage..
Info	2018-07-09 12:31:...	0	Load Local Config..
Info	2018-07-09 12:31:...	0	Create directory
Info	2018-07-09 12:31:...	0	Load System Config..
Info	2018-07-09 12:31:...	0	Start!

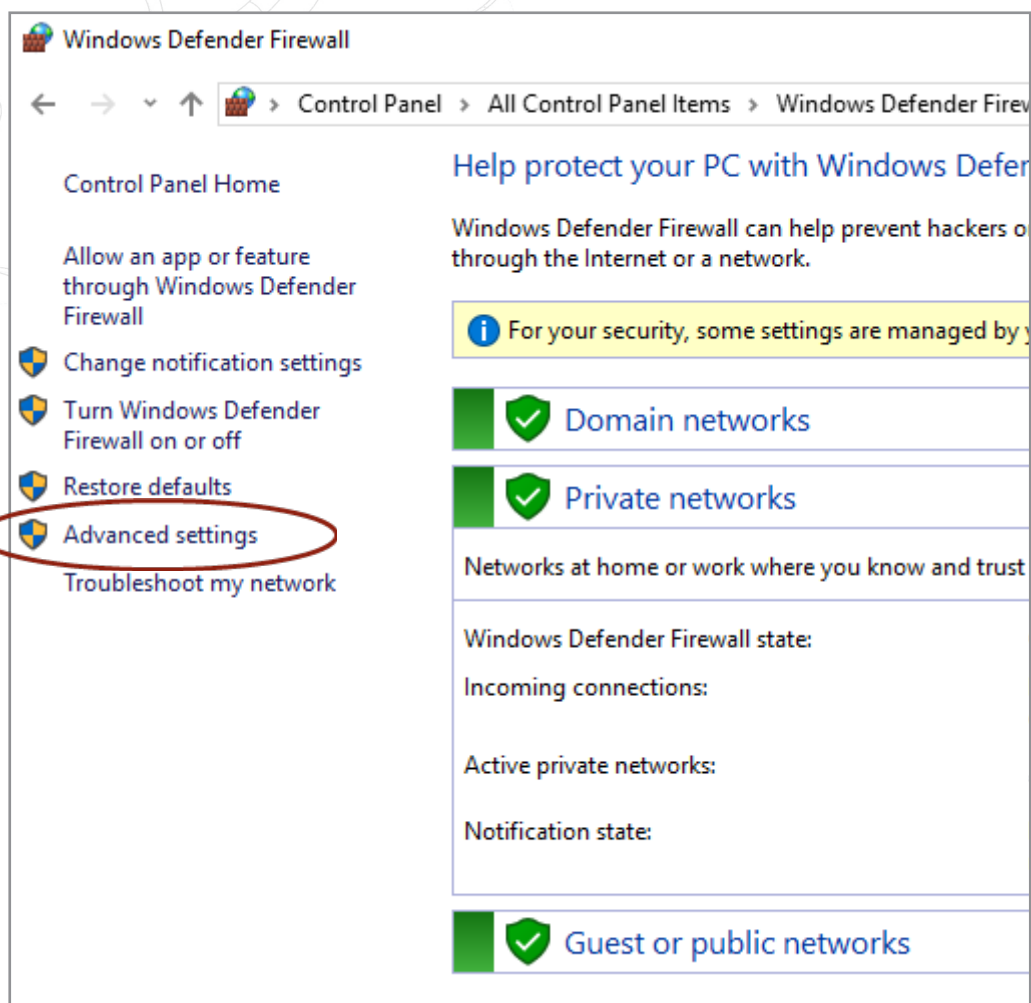
PAXTON v1.3.1.3 Clear

Opening ports in the Firewall

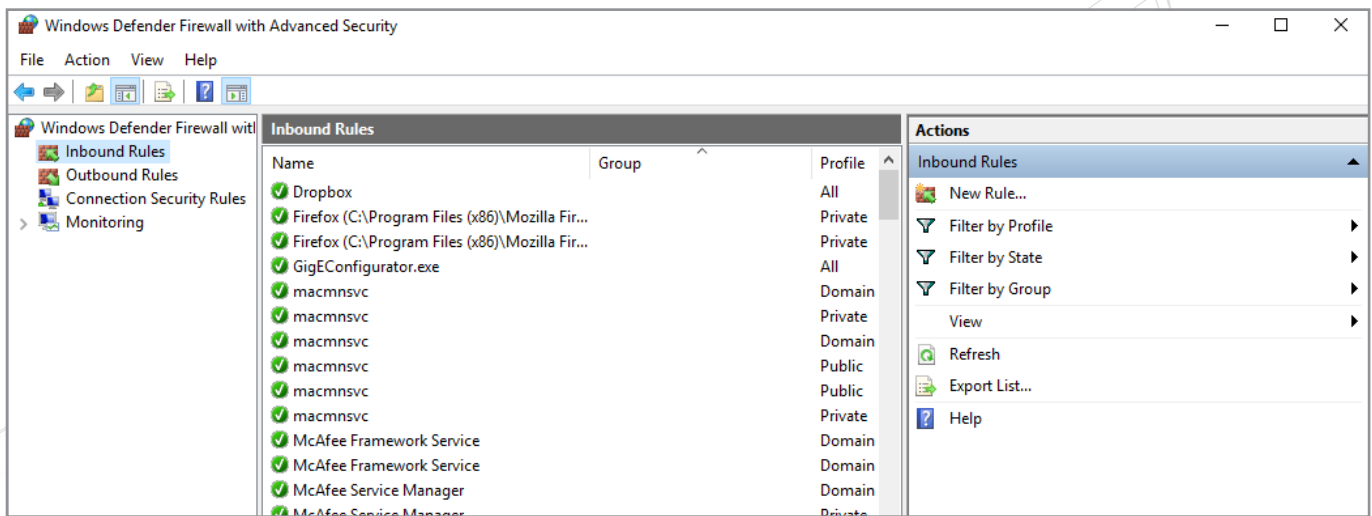
- Ports 9870, 9871, 9872, 9873, 9874, 9875 needs to be allowed for incoming and outgoing
- Go to Control Panel and click on Windows Defender Firewall



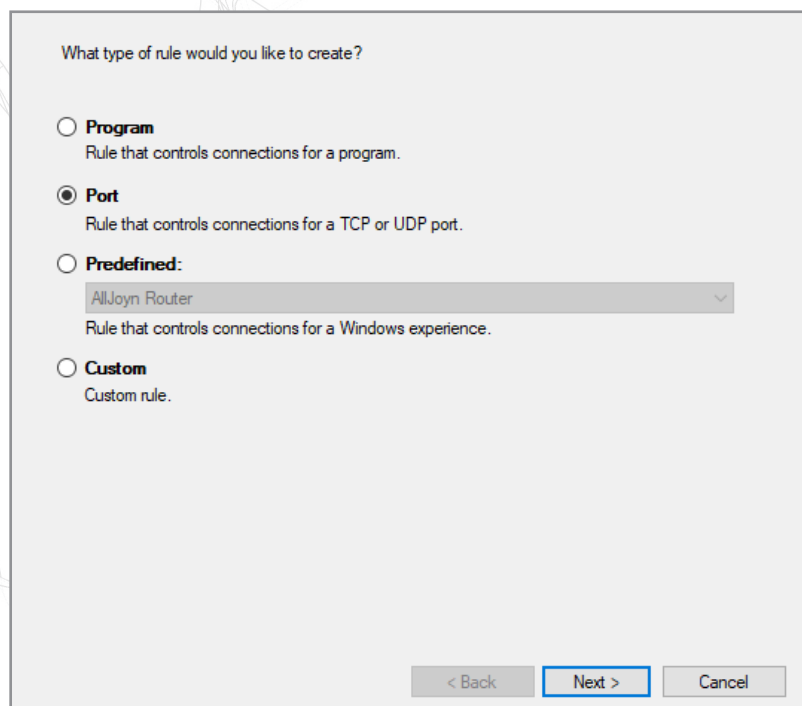
- Click on Advanced settings



- Now we are going to create 2 Firewall rules for UNIS: Inbound and Outbound
- Inbound rule: Click on Inbound rule and then click on New Rule



- Select Port:



- Enter the ports to be allowed: 9870 -9875

Does this rule apply to TCP or UDP?

☒ TCP
☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports
☒ Specific local ports:
Example: 80, 443, 5000-5010

< Back Next > Cancel

- Make sure that Allow the Connection is selected

What action should be taken when a connection matches the specified conditions?

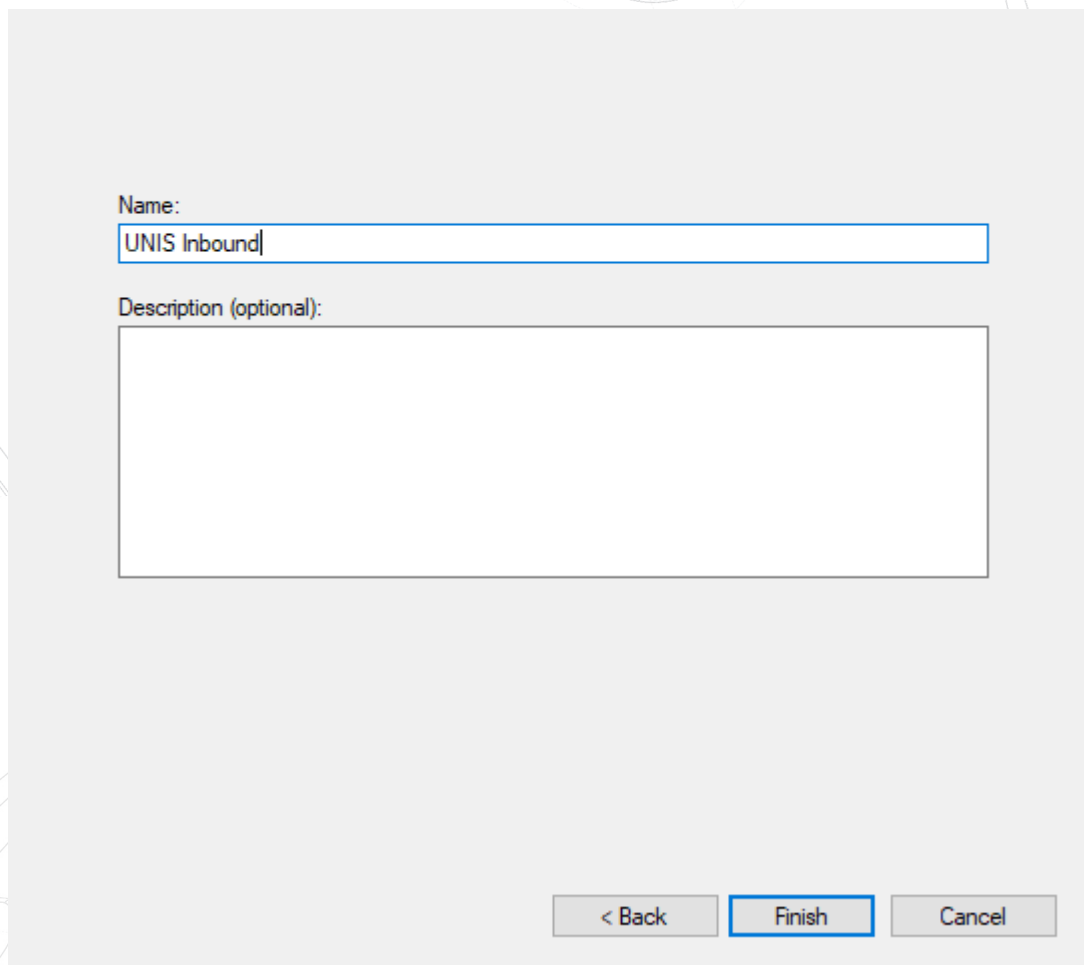
☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Block the connection**

< Back Next > Cancel

- Enter a name for the rule and click on Finish.



A screenshot of a light gray dialog box with a white background. At the top, the label "Name:" is followed by a text input field containing the text "UNIS Inbound". Below this, the label "Description (optional):" is followed by a larger, empty text area. At the bottom right of the dialog, there are three buttons: "< Back", "Finish" (which is highlighted with a blue border), and "Cancel".

- Repeat these steps for Outbound rules.

Installing the Virdi USB Take-on reader drivers

- Before starting to enrol users, ensure that the USB drivers have been installed for the Take-on reader.

Enrolling fingerprints out of Net2

- To add user's fingerprints, click on add user in the Net2 Software
- Add all relevant information such as first name, surname, department, and access level. Click on the Auto PIN button to create a unique 4-digit PIN and retype the PIN number in the Token Number field.
- Select Fingerprint Verification from the Token Type dropdown box.

Add user

Please select the type of token which you wish to issue

Token type: Default New type

First name: Joe

Middle name:

Surname: Soap

Department: Visitors

Access level: Working hours

Telephone:

Fax:

Valid from: 09/07/2018

Expires end: 09/07/2018

Address 1:

Address 2:

Town:

County:

Post code:

Home telephone:

Home Fax:

Mobile:

Card template:

Get picture

Capture Picture

Email:

Position:

Start date:

Car registration:

Notes:

Personnel number:

PIN: 5139 Auto PIN

Token number: 5139

Token type: Fingerprint verification ...

☐ When I click 'Add user' reload the token type default values

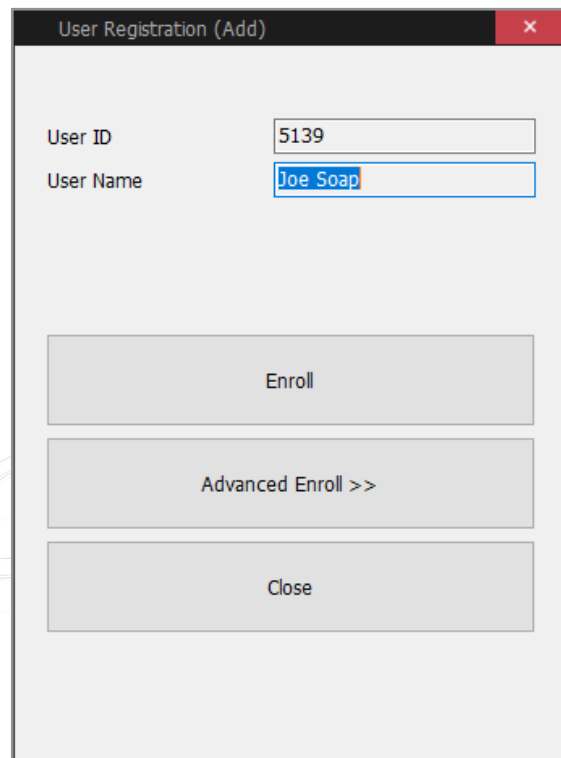
☒ When I click 'Add user' retain the previous record values

Print card

Close

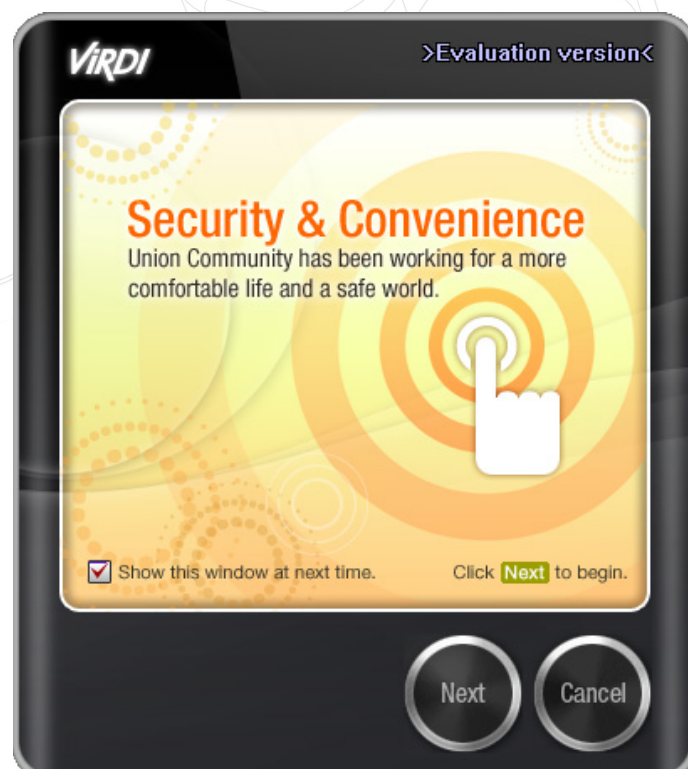
Add user

- Click on the Add User button which will save the user and open the VirDI User Registration screen for the fingerprints.
- Click the Enrol button

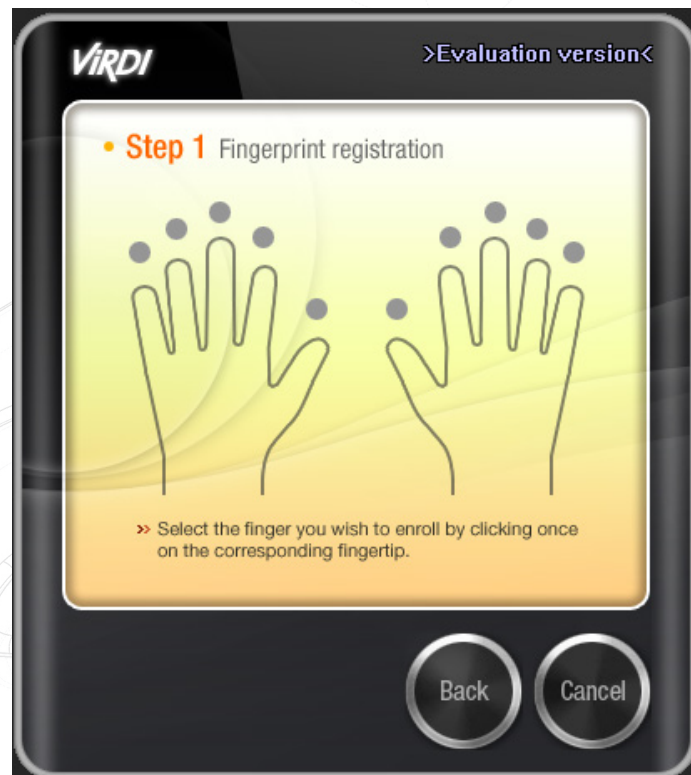


A screenshot of a 'User Registration (Add)' dialog box. It has a title bar with a close button. Inside, there are two input fields: 'User ID' with the value '5139' and 'User Name' with the value 'Joe Soap'. Below the fields are three buttons: 'Enroll', 'Advanced Enroll >>', and 'Close'.

- Click on next



- Select the finger to enrol (it is good practice to do at least 1 finger from both hands)



- Once the fingerprint enrolment is completed, the fingerprint will be displayed as a token in the user's profile

Soap, Joe

First name: Joe

Surname: Soap

Department: Visitors


Telephone: Fax:

Personnel number:

Valid from: 09/07/2018 ☐ Expires end: Never expires

Access rights | **Tokens** | Other details | Memo | Events | Current validity | Anti-passback | Multizone Intruder

PIN: 5139 Card template: None


5139

Token has not been used in the past 12 months

Setting up Viridi integration with Paxton Net2 Client

- Fingerprints can now also be enrolled from a client PC. The following software needs to be installed on the client PC:
 - Net2 Software – same version as which is used on the Server
 - QEManager - same version as which is used on the Server
- The installation of QEManager for a client is the same as for the Server (see instructions earlier in the document)
- Right click on QEManager in the taskbar and select Settings.
- By default, all the IP addresses will point to the local machine (localhost IP of 127.0.0.1). Change all the IPs to the IP address of the PC running the Server software.

The screenshot shows the 'Environments' dialog box with two main sections: 'UNIS Connect Info' and 'Paxton Info'. In the 'UNIS Connect Info' section, the 'Server IP' and 'UDB IP' fields are both set to '127.0.0.1' and are circled in red. The 'Server Port' is '9871' and the 'UDB Port' is '9872'. To the right, there are fields for 'ODBC' (set to 'UNIS'), 'DB ID' (set to 'unisuser'), and 'DB Pwd' (set to '*****'). The 'Paxton Info' section has a 'Net2 Connect Info' sub-section where the 'IP Address' is '127.0.0.1' (circled in red), the 'Port' is '8025', the 'ID' is 'System engineer', and the 'Password' is '*****'. At the bottom right are 'Ok' and 'Cancel' buttons.

UNIS Connect Info	
UNIS Server	
Server IP	127.0.0.1
Server Port	9871
UDB Server	
UDB IP	127.0.0.1
UDB Port	9872
ODBC	UNIS
DB ID	unisuser
DB Pwd	*****

Paxton Info	
Net2 Connect Info	
IP Address	127.0.0.1
Port	8025
ID	System engineer
Password	*****