

# Net2 APN-1180-ZA

# Setting up Virdi integration with Paxton Net2 Server

#### Overview

Integrating Virdi biometric readers with the Paxton Net2 system is made possible by using UNIS4 and C / Janager (the software required can be downloaded <u>here).</u>

The installation and configuration steps to follow is:

- 1) Install Net2 (view application notes <u>here</u>)
- 2) Install UNIS4
- 3) Install QEManager

Versions of software used in this documentation:

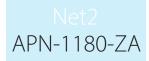
Net2 - 5.04.6918.5578 UNIS4 - 4.2.7.18 QEManager - 1.3.1.3

# 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		1
Door name	New Biometric door	Apply
Door group	(none) V	Cancel
Door open time	3 ÷ seconds	
Unlock the door during	At no time	Open door
	Only unlock the door once a user has been granted access	Identify
	Silent operation	
Unlock relay 2 during	At no time 🗸 🗸	
Reader 1   Reader 2   Alarm   Event Reader details Name	s   Fire alarm inputs   Multizone Intruder   Access rights   Camera integration	]
Reader type	Wiegand reader	~
	-	
Keypad type	None	~
Token data format	Wiegand 26 bit 🗸 🗸	New format
Operating mode		
Reader operating mode	Token only V	
Timed operating modes - This allow	rs for different reader operation during a selected timezone.	
During this timezone:	All day, every day $\sim$	
This reader will operate as:	🔇 Inactive 🗸	
Reader action - This is what will happe	n when a valid access is granted.	
	Relay 1 opens for door open time	

Figure 1 - configure a Net2 Plus controller for Wiegand readers



# Installing and setting up UNIS4

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

8	Change Master	Password			×
	Change the	master password. Ti not av	ne password that w vailable.	vas intially set is	
		Old Password	*		
	0	Olu Passworu			
		New Password	****		
	<b>1</b>	Confirm Password	****		
			ОК	Cancel	

Figure 2 - Create new password for UNIS

Login to UNIS by selecting Master and entering the new password

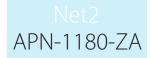
You can take advantage of the various elements.	
Master Logon     0000000	
Sign in	
Sign in	

Figure 3 - Login as Master



- Under the Main Menu tab, select Settings (menu is hidden away on the right side of the screen. Move the mouse curser to the right border of the UNIS screen to view the menu).
- Select -> Wiegand Format Setting
- In the Wiegand Format Setting, in the Input info section, create a 26-bit Wiegand format.
- Click on register to create.

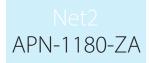
Set wegend in out format and report from the terminal         Wiegand Out       Wiegand In         Code       Name         001       26 bit Wiegand         Input info       Output Type         Output Type       UserID         Set Ridd       1         Set Ridd	et Wiegand	the state of the state former to			
Code       Name         0001       26 bit Wiegand         Bit Length       Unused       Custom Size         Port State       Active Low       Site Code         Send Fail       Not Anything       Fail Data       0         Output Type       UserID       Untervar Time(us)       0         Vidth Time(us)       0       0       0         Name       26 bit Wiegand       1       1       1       1         Set Fail       Not Anything       Fail Data       0       0         Name       26 bit Wiegand       Set Fail       0       0       0         Set Fail       Not Anything       Fail Data       0       0       0         Name       26 bit Wiegand       1	Wiegand Out Wiegand In		and import and export from th	e terminal	
Port State       Active Low       Site Code       0         Send Fail       Not Anything       Fail Data       0         Output Type       UserID       Intervar Time(us)       0         Name       26 bit Wiegand       Set Fild       1       1       1       1         Set Fild       Set Fild       1 <td< td=""><td></td><td></td><td>~</td><td>Read from Terminal</td><td>Send to Terminal</td></td<>			~	Read from Terminal	Send to Terminal
Send Fal       Not Anything       Fal Data       0         Output Type       UserID       Intervar Time(us)       0         Name       26 bit Wiegand       Set Fald       1		Bit Length	Unused $\lor$	Custom Size	1 ~
Input info       Output Type       UserID       Intervar Time(us)       0         Name       26 bit Wiegand       Set Field       1		Port State	Active Low $\sim$	Site Code	0
Input info       Width Time(us)       0         Code       0001       Set Field       1 <td></td> <td>Send Fail</td> <td>Not Anything <math>\sim</math></td> <td>Fail Data</td> <td>0</td>		Send Fail	Not Anything $\sim$	Fail Data	0
Code       0001         Name       26 bit Wiegand         Register       Modify         Delete       1         49       1         65       1         97       1         113       1         113       1         113       1         114       1         115       1         117       1         118       1         119       1         111       1         113       1         114       1         115       1         116       1         17       1         18       1         19       1         10       1         1112       1         111       1         111       1         111       1         111       1         111       1         111       1         111       1         111       1         111       1         111       1         1111       1         11111 <td></td> <td>Output Type</td> <td>UserID ~</td> <td>Intervar Time(us)</td> <td>0</td>		Output Type	UserID ~	Intervar Time(us)	0
Name       26 bit Wiegand         Register       Modify       Delete         1				Width Time(us)	0
1       1       16         17       1       16         17       1       16         13       1       16         49       1       16         65       1       16         80       16         81       1       16         97       1       16		1 17 34 49 65 81 97		16 32 48 64 80 96 112	<ul> <li>Site Code</li> <li>Data(ID)</li> <li>Fixed 0</li> <li>Fixed 1</li> <li>Odd Parity</li> <li>Event Parity</li> </ul>
		1     1       17     1       33     1       49     1       65     1       81     1       97     1		32       48       64       96       112	
Ready		113		128	



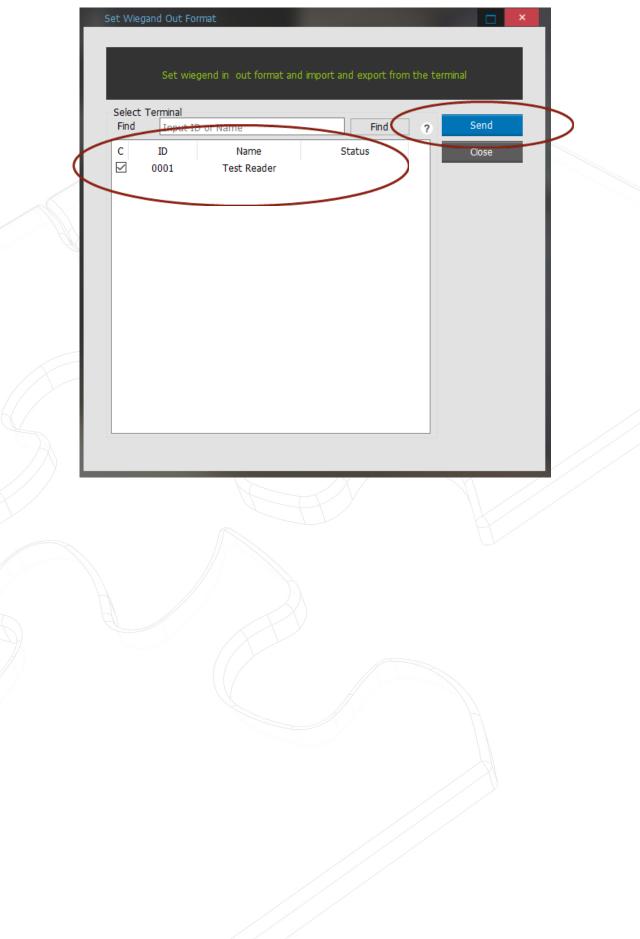
To send the Wiegand settings to the Virdi readers, select a Terminal and Bit Length and click on Send to Terminal

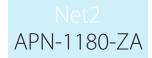
t Wiegand	Set wiegend in out format a	ind import and export from th	ie terminal	
Wiegand Out     Wiegand       Code     Name       0001     26 bit Wiegand	In Basic info	0001 : Test Reader 🗸 🗸	Read from Terminal	Send to Terminal
20 Dic Wiegand	Bit Length Port State Send Fail	St. 26bit ~ Active Low ~ Not Anything ~	Custom Size Site Code Fail Data	1 ~ 0 0
Input info Code 0001 Name 26 bit Wiegand	Output Type	UserID ~	Intervar Time(u: Width Time(us)	
Name 26 bit Wiegand Register Modify Delete			16 32 48 64 80 96 112 128	S       Site Code         D       Data(ID)         0       Fixed 0         1       Fixed 1         O       Odd Parity         E       Event Parity         Point
	Set Parity 1 17 33 49 65		16 32 48 64 80	
eady	81 97 97 113 97 97 97 97 97 97 97 97 97 97 97 97 97		96 96 112 128	

Ready



Select all the readers and click on Send





- 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 curser to the right border of the UNIS screen to view the menu).
- Under Environment -> General -> Users ensure the option to "Auto synchronize terminal when user info is modified" is selected. Click Apply.

Local Environment	User	Clear Server Connect Info
- Server Connection - Alarm popup - Picture Popup Server Environment - General - FingerPrint	<ul> <li>User ID used as Employee ID (Automatic creation)</li> <li>Allow terminal to overwrite users</li> <li>Auto synchronize terminal when user info is modified.</li> <li>Sync only connected terminal.</li> <li>Use blacklist user management</li> <li>Admin login by Unique ID</li> </ul>	DDNS Terminal Connection Settings Port 9870 Polling Interval 10
Emergency Necessary Contents Mail Environment Password Security TNA	Authentication  Automatically upload log data from terminal  Save only successful authentication logs	Set ID Limit         Terminal ID Length (18)         User ID Length (28)         8         Unique ID Length (120)         20
Other Module	Door Record the door open / closed status to a log	Visitor ID Range 7000 - 9000
	Data Export Transfer picture when record is sent Transfer picture authentication data	Store Access Log     0       Store Event Log     0       Store Terminal Commands     0
	Access Control Restrict the use of access control admin.	

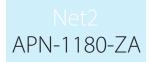
# Installing and setting up QEManager

- When installing QEManager select install for Everyone

🛃 QEManager	_	- 🗆 X
Select Installation Folder		
The installer will install QEManager to the following folder.		
To install in this folder, click "Next". To install to a different folde	er, enter it below	or click "Browse".
<u>F</u> older:		
C:\Program Files (x86)\QEManager\		Browse
		Disk Cost
Install QEManager for yourself, or for anyone who uses this c	omputer:	
Everyone		
O Just me		
Cancel	< Back	Next >

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

	Paxton.Net2.Utils.dll
-	Paxton.Remoting.Channel.dll
	Paxton.Remoting.RemotingLayerInterfac
	💽 QEManager.exe
	UCBioBSP.dll
	UCBioBSPCOM.dll
	UCBioBSPSkin.dll

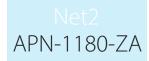


- To run QEManager, right click the shortcut on the desktop and select Run as Administrator
- Enter the password for Net2:

Environments						×
UNIS Connect In	nfo					^
UNIS Server		UDB Server				
Server IP	127.0.0.1	UDB IP	127.0.0.1	ODBC	UNIS	]
Server Port	9871	UDB Port	9872	DB ID	unisuser	]
				DB Pwd	******	
					·	·
Paxton Info						
Net2 Connect Inf	fo					
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)

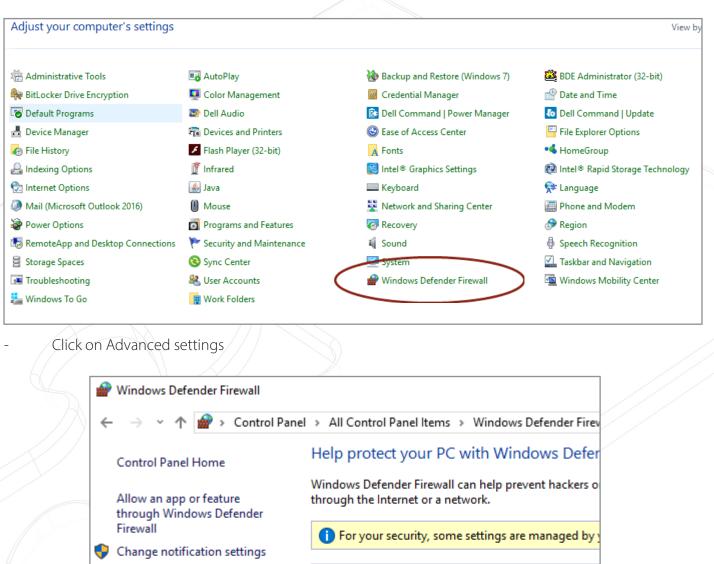
Туре	DateTime	UID	Message	
Info	2018-07-09 12:31:	0	Connect Paxton Net2OK	
Info	2018-07-09 12:31:	0	Load General DatabaseOK	
Info	2018-07-09 12:31:	0	Load General Database	
Info	2018-07-09 12:31:	0	Init FP Info	
Info	2018-07-09 12:31:	0	Load System DatabaseOK	
Info	2018-07-09 12:31:	0	Load System Database	
Info	2018-07-09 12:31:	0	Connect Auth ServerOK	
Info	2018-07-09 12:31:	0	Connect Auth Server	
Info	2018-07-09 12:31:	0	Connect UDB ServerOK	
Info	2018-07-09 12:31:	0	Connect UDB Server	
Info	2018-07-09 12:31:	0	Load MutiLanguage	
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



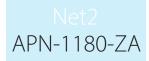
Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network





- 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

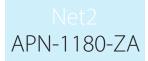
P Windows Defender Firewall wit	th Advanced Security	~			_	×
ile Action View Help						
• 🔿 🙋 📰 🗟 🚺						
Windows Defender Firewall wit	Inbound Rules			Actions		
🔣 Inbound Rules 🚮 Outbound Rules	Name	Group	Profile ^	Inbound Rules		
The Connection Security Rules	Oropbox		All Private	🚉 New Rule		
🌉 Monitoring	<ul> <li>Firefox (C:\Program Files (x86)\M</li> <li>Firefox (C:\Program Files (x86)\M</li> </ul>		Private	Filter by Profile		
	🔮 GigEConfigurator.exe		All	Filter by State		
	macmnsvc     macmnsvc		Domain Private	Filter by Group		
	Macmisve Warmachinsve		Domain	View		
	🔮 macmnsvc		Public	Refresh		
	macmnsvc     macmnsvc		Public Private	Export List		
	McAfee Framework Service		Domain	<table-cell> Help</table-cell>		
	McAfee Framework Service		Domain			
	McAfee Service Manager		Domain Private			
	Port     Rule that controls con     Predefined:     AllJoyn Router	nections for a program. nections for a TCP or UDP port. nections for a Windows experien	ce.			
	d.					

	Does this rule apply to TCP or UDP?		
	TCP     UDP		
	Does this rule apply to all local ports o	or specific local ports?	
	O All local ports		
		9870-9875 Example: 80, 443, 5000-5010	
		< Back Next > Cancel	
Maka sura t	hat Allow the Connection is		
Make sure t	hat Allow the Connection is		
Make sure t	hat Allow the Connection is		
Make sure t			
Make sure t	What action should be taken when a	s selected	
Make sure t	What action should be taken when a	s selected	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is	a connection matches the specified conditions? re protected with IPsec as well as those are not. secure	
Make sure t	<ul> <li>What action should be taken when a</li> <li>Allow the connection This includes connections that are</li> <li>Allow the connection if it is This includes only connections the will be secured using the settings</li> </ul>	a connection matches the specified conditions?	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections th will be secured using the settings Rule node.	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	<ul> <li>What action should be taken when a</li> <li>Allow the connection This includes connections that are</li> <li>Allow the connection if it is This includes only connections the will be secured using the settings</li> </ul>	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections th will be secured using the settings Rule node.	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	
Make sure t	What action should be taken when a Allow the connection This includes connections that are Allow the connection if it is This includes only connections the will be secured using the settings Rule node. Customize	a connection matches the specified conditions? re protected with IPsec as well as those are not. <b>secure</b> nat have been authenticated by using IPsec. Connections	



Enter a name for the rule and click on Finish.

	Name:			
	UNIS Inbound			
	Description (optional):			
		< Back Finis	h Cancel	
peat the	se 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		1.110-2-		×
Please select the type of token v	which you wish to issue			^
I lease select the type of token type	Default		~	New type
First name	Joe	Get picture		
Middle name		Capture Picture		
Surname	Soap			
Department	Visitors ~			
Access level	Working hours $\sim$			
Telephone				
Fax		Email		
Valid from	09/07/2018 🔹	Position		
Expires end	09/07/2018 🔹	Start date		
Address 1		Car registration		
Address 2		Notes		~
Town				
County				
Post code			<	>
Home telephone		Personnel number		
Home Fax		PIN	5139	Auto PIN
Mobile		Token number	5139	
Card template	~	Token type	💽 Fingerprint v	verification 🗸
<u></u>				
<ul> <li>When I click 'Add user' reload</li> <li>When I click 'Add user' retain</li> </ul>				
Print card			Close	Add user
			0036	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

User Registration (Add)

Click on next

		5120		
	User ID User Name	5139 Joe Soap		
$\geq$				
		Enroll		
	Ac	dvanced Enroll >>		
4				
		Close		
L	$\times$			
		$\square$		4
ſ	Virdi		>Evaluation version	1<
	Virdi	<u></u>	>Evaluation version	۱ <b>۲</b>
	····//			1<
		ty & Con		١٢
	Securi Union Commo	ty & Con unity has been w ife and a safe wo	venience	к
	Securi Union Commo	ty & Con unity has been w ife and a safe wo	venience	ι<
	Securi Union Commo	ty & Con unity has been w ife and a safe wo	venience	ιĸ
	Securi Union Commo	ty & Con unity has been w ife and a safe wo	venience	IK
	Securi Union Commo	ty & Con unity has been w ife and a safe wo	venience	
	Securi Union Commu comfortable I	ife and a safe wo	orking for a more orking the second s	X
	Securi Union Commo	ife and a safe wo	venience	
	Securi Union Commu comfortable I	ife and a safe wo	orking for a more orking for a more ord.	
	Securi Union Commu comfortable I	ife and a safe wo	orking for a more orking the second s	
	Securi Union Commu comfortable I	ife and a safe wo	orking for a more orking for a more ord.	

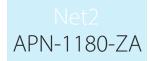


Select the finger to enrol (it is good practice to do at least 1 finger from both hands)



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 Vis
Telephone	Fax
Personnel number	
8	Valid from Expires end
	09/07/2018   Never expires
Access rights Tokens Other d	etails   Memo   Events   Current validity   Anti-passback   Multizone Intruder
PIN 5139 Auto PI	Card template None ~
	New token
	Delete
5139	Lost token
	Found token
	Change token type
	Change token type
Token has not been used in the pa	st 12 months
Capture Picture Get picture	e Delete picture Bar user Delete record Print card Export vcf Apply



# Setting up Virdi 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.

nvironments					
UNIS Connect 1	Info				
UNIS Server		UDB Server		_	
Server I	127.0.0.1		127.0.0.1	ODBC	UNIS
Server Port	9871	UDB Port	9872	DB ID	unisuser
				DB Pwd	*******
Paxton Info					
Net2 Connect Ir	nfo				
IP Add ess	127.0.0.1	$\supset$			
Port	8025				
ID	System engineer				
Password	****				
					Ok Cancel
			NX.		