Net2 - Network Security Recommendations

Overview

In order for your Paxton Net2 system to be as secure as it can be on your site, Paxton recommends that the installer (or IT department) implement IT security mechanisms best practice at each of the 7 layers of Network Open Systems Interconnection (OSI) model.

Implement strong physical security

Implement strong physical security to company premises such as by using Biometrics, token-based authentication, etc. so that an outsider can be stopped before he/she can enter a building with a corporate network.

Implement Network Access Control standards such as IEEE 802.1X authentication for securing LAN and WLAN

This standard enforces security policy by granting only security policy–compliant devices access to network assets when those devices are plugged into a physical LAN port or are connected to a WLAN SSID. This standard not only handles access authentication and authorization functions but even control the data accessed by those specific users by recognizing users, their devices and their network roles. IEE 802.1X is natively supported by all Windows, Mac and Linux machines.

Implement next generation Firewalls to prevent external and internal attacks

Implement a next generation firewall which, in addition to traditional packet based stateful inspection, also performs application layer inspection, intrusion prevention and detection, securing web traffic, etc.

Furthermore, stretch any potentially insecure internal layer 2 VLANs to the firewall and protect access from those VLANs to other trusted/secure VLANs using configurable security policies.

Implement VLANs (Virtual Local Area Networks) for network security and segregation

VLANs allow us to keep data packets from multiple networks (such as departmental networks, critical server networks, etc.) separated. Network segmentation with VLANs creates a collection of isolated networks within a corporate network and reduces the attack surfaces because even if an outsider gets access to a small logical network, he/she won't be able to view or directly attack devices on other VLANs.

Implement strong passwords for Net2 Server application authentication and associated databases. Please see application note APN-1162 for details on how to achieve this.

Have a dedicated machine for Net2 Server

Have a machine dedicated to running Net2 server and not install other software other than network monitoring tools if required.

The physical Net2 server machine should be restricted to authorised personnel only.

Machine safety

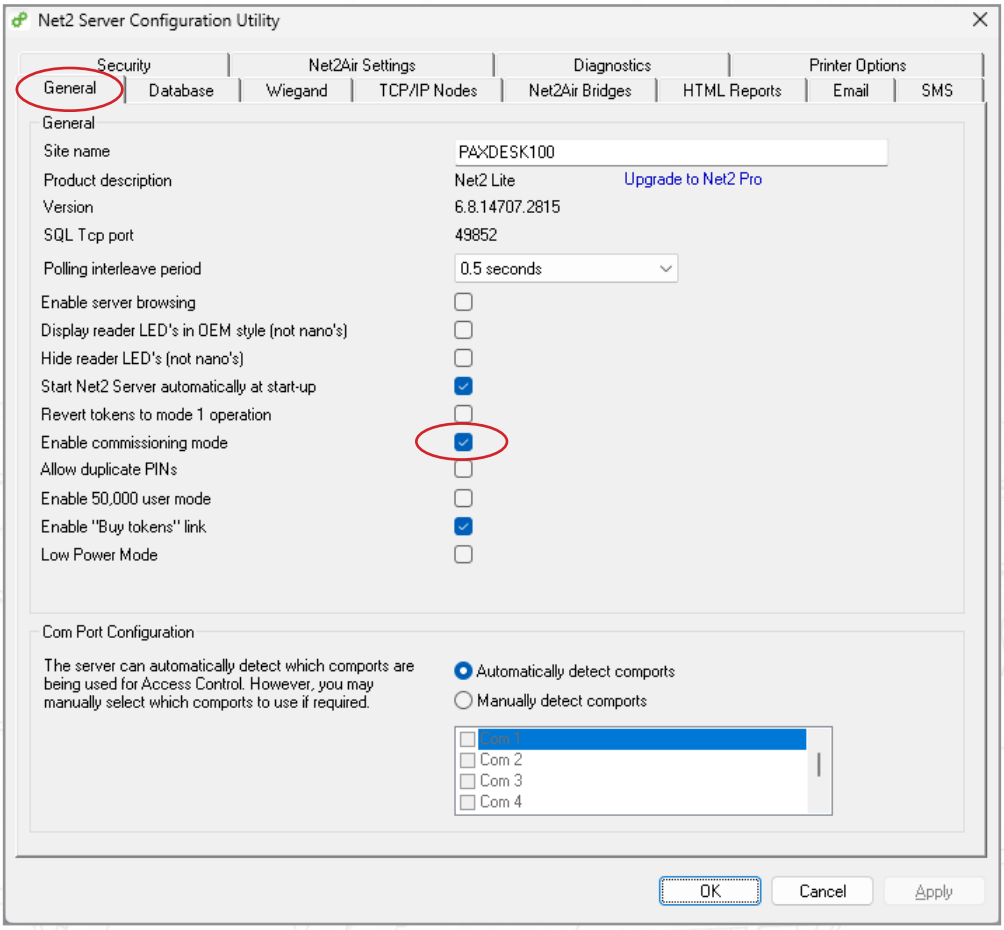
Keep server and client machines updated with latest OS critical updates and ensure virus scanning protection on client machines.

Net2 clients should be installed on machines without email/chat clients to avoid non-intentional malicious code execution via attachments.

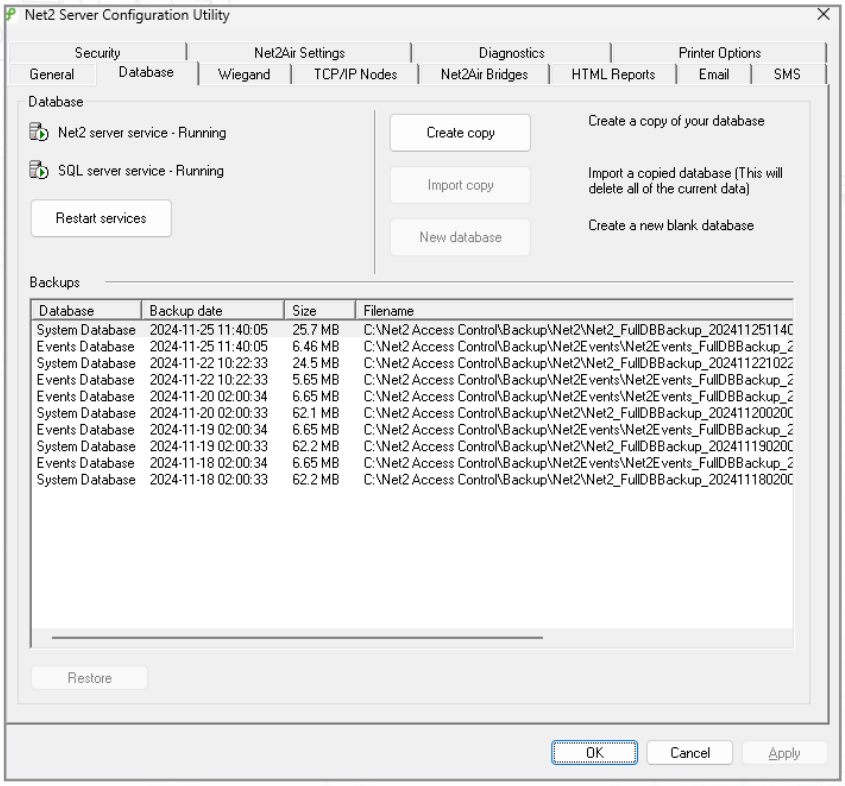
Commissioning Mode

Once you have commissioned your system, it can be locked down by un-checking the **'Enable Commissioning Mode'** box, under the **'General'** tab of the Net2 Configuration Utility.

Please note:
With commissioning mode disabled, it is no longer possible to add or delete ACU's and they will be locked to this server.

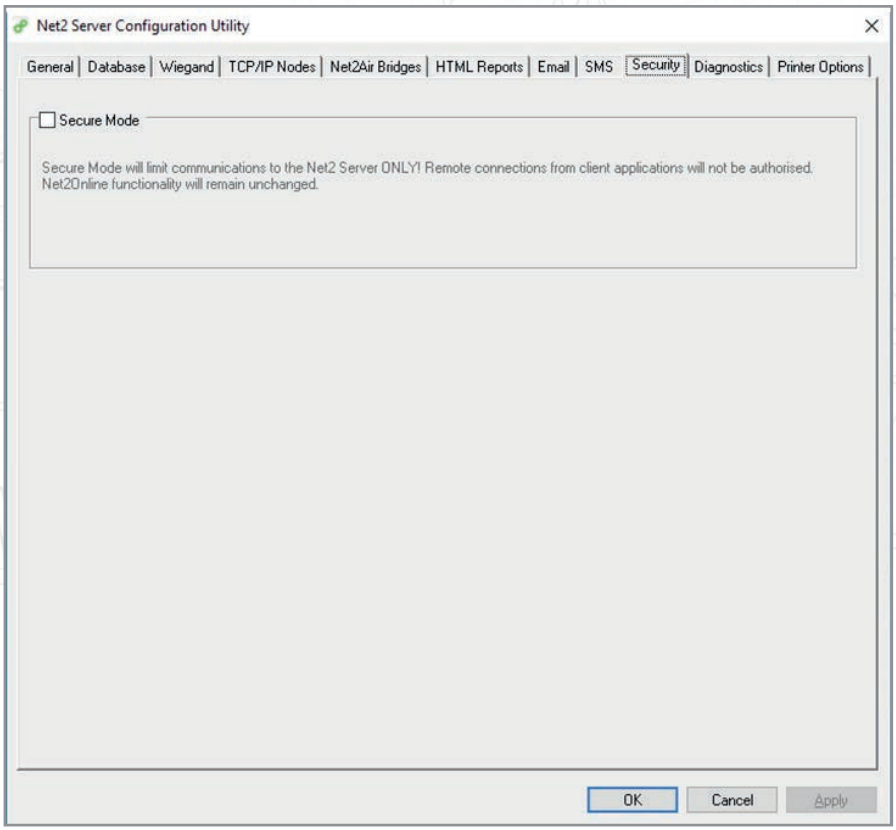


With commissioning mode disabled, options on the **'Database'** tab will also be greyed out in the Net2 Configuration Utility.



Net2 secure mode

For maximum security consider running both the server and client software from the same machine and blocking the TCP SQL server port 1433 for inbound connections. This can be achieved by activating **'Secure Mode'** using the Net2 security tab.



If you require client access, away from the server machine, this can be achieved by using our Net2Online service. This will allow management of users, access and event administration. Site commissioning can only be performed from the server machine.

Alternatively for full use of all client features, use virtualized application software such as VMware horizon to distribute restricted Net2 client applications connected to a Net2 server on a seperate LAN or VLAN.

To allow tokens to be enrolled simply use an existing reader or a reader connected to a wireless Net2 Nano if network cabling not viable. This solution will also allow SDK (Software Development Kit) and Video applications to be isolated in the virtualized desktop and deployed easily, fully administered within the data centre.

What is VMware Horizon? | VDI Software | VMware | UK

Note: VMware horizon does have USB passthrough, but performance is dictated by network speeds and requires testing. This could allow standard desktop reader and webcam use.

Additional Security Steps

1. Implement MAC address filtering on the switch

Implement MAC address filtering on the Entry port. When an unrecognised device connects to a port, the port will be disabled and an alert sent.

2. Isolate the VLAN

Place all the Paxton devices with IP capability on a dedicated VLAN. Isolate this VLAN from the company network to restrict access into areas other than the access control devices.