

Net2 aanbevelingen voor netwerkbeveiliging

Overzicht

Om ervoor te zorgen dat uw Net2 toegangscontrole systeem zo veilig mogelijk is dient u uw netwerk te beveiligen. Uw installateur of IT afdeling kan u adviseren om beveiligingsmechanisme te gebruiken op ieder van de 7 lagen van het OSI (Open Systems Interconnection) model.

Implementeer toegangscontrole

Implementeer toegangscontrole op ruimtes met netwerk apparatuur zodat een buitenstaander geen toegang heeft tot deze ruimten. Zo voorkomt u dat buitenstaanders toegang krijgen tot uw netwerk.



Gebruik netwerk authenticatie standaarden zoals IEEE 802.1X om uw LAN en WLAN te beveiligen

Deze beveiligingsstandaard laat alleen LAN en WLAN netwerkapparatuur op uw netwerk toe die voldoen aan de IEEE802.1X beveiligingsstandaard. Deze standaard behandelt niet alleen toegangsauthenticatie- en autorisatiefuncties, maar beheert zelfs de gegevens die door die specifieke gebruikers en apparaten geraadpleegd worden. IEEE802.1x wordt standaard ondersteund door alle Windows, Mac en Linux machines.

Gebruik de nieuwe generatie firewalls (NGFW) om externe en interne aanvallen te voorkomen

De nieuwe generaties firewall (NGFW) omvatten (naast de traditionele firewall techniek 'state full packet inspection'): Application layer inspection, Intrusion Prevention System (IPS), Anti-Malware Prevention, Deep Packet Inspection (DPI) etc.

Configureer mogelijk onveilige layer 2 VLAN's naar uw firewall. En voorkom dat u vanuit veilige VLAN's de onveilige layer 2 VLAN's kunt benaderen door gebruik te maken van een beveiligingsbeleid.

Gebruik VLAN's (Virtual Local Area Networks) voor netwerk beveiliging en scheiding

Met VLAN's kunt u op één fysiek netwerk uw netwerken scheiden van elkaar, zo kunt u een netwerk hebben voor bijvoorbeeld uw camera's, toegangscontrole of computers. Met netwerk segmentatie via VLAN's creëert u losstaande netwerken. Wanneer een iemand ongeoorloofde toegang heeft tot één VLAN kan er vanuit daar geen aanval gedaan worden op de overige VLAN's. Hiermee beperkt u een aanval op uw netwerk tot één VLAN.

Gebruik een sterk wachtwoord om uw Net2 systeembeheerder account mee te beveiligen. Meer informatie over hoe u uw software kunt beveiligen vindt u via: paxton.info/4167

Heb een separate PC voor Net2 Software

Gebruik een separate PC of Windows omgeving waar u Net2 op installeert. Zorg ervoor dat alleen geautoriseerd personeel toegang heeft tot deze PC om mogelijk misbruik tegen te gaan.

Maak ook gebruik van een antivirus, anti-malware of firewall op deze PC om de veiligheid van uw PC te verhogen.

Beveiliging van de PC

Zorg ervoor dat de server of PC waar Net2 op geïnstalleerd is voorzien is van de laatste Windows (security) updates. Hiermee verhoogt u de beveiliging van uw Windows omgeving doordat bekende veiligheidsrisico's gedicht zijn. Door uw Windows omgeving te beveiligen zorgt u er ook voor dat Net2 beter beschermd is voor aanvallen van buitenaf.

Maak ook gebruik van een antivirus, anti-malware of firewall op uw PC, en zorg ervoor dat deze regelmatig geüpdatet wordt. Door uw antivirus programma en firewall programma te updaten word uw PC beschermt tegen die nieuwste virussen en malware.

Om de veiligheid verder te verhogen is het te adviseren om automatisch uitloggen in te stellen op de PC of Net2. Hierdoor is het niet meer mogelijk om toegang te krijgen tot de software wanneer een gebruiker vergeet uit te loggen en de PC onbeheerd achterlaat.

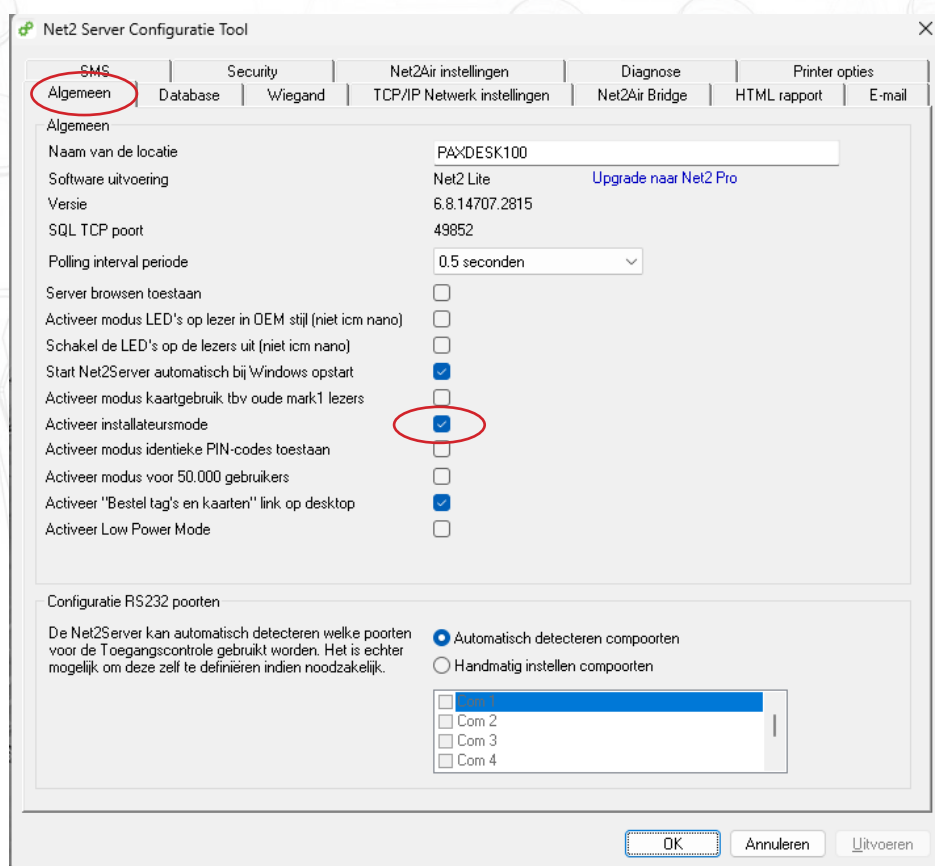
Installeursmode

Wanneer u het Net2 systeem in bedrijf heeft gesteld kunt u een extra beveiligings laag toevoegen op de controllers. Dit doet u door de installeursmode uit te vinken via de Net2 Configuration Utility.

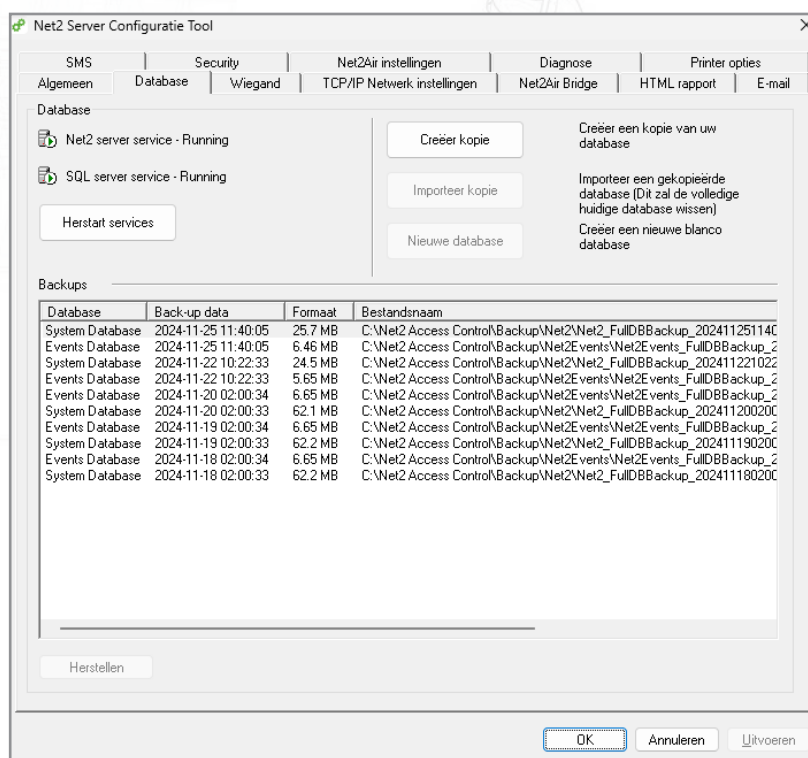
Wanneer installeursmode is uitgeschakeld zullen de controllers alleen communiceren met deze database en kunnen niet verbonden worden aan een andere database.

Let op:

Wanneer installeursmode is uitgeschakeld, is het niet meer mogelijk om controllers te detecteren en is het niet meer mogelijk om een kopie van de database te maken.



Omdat de controllers alleen met deze database communiceren is het advies om back-ups te maken van de database.

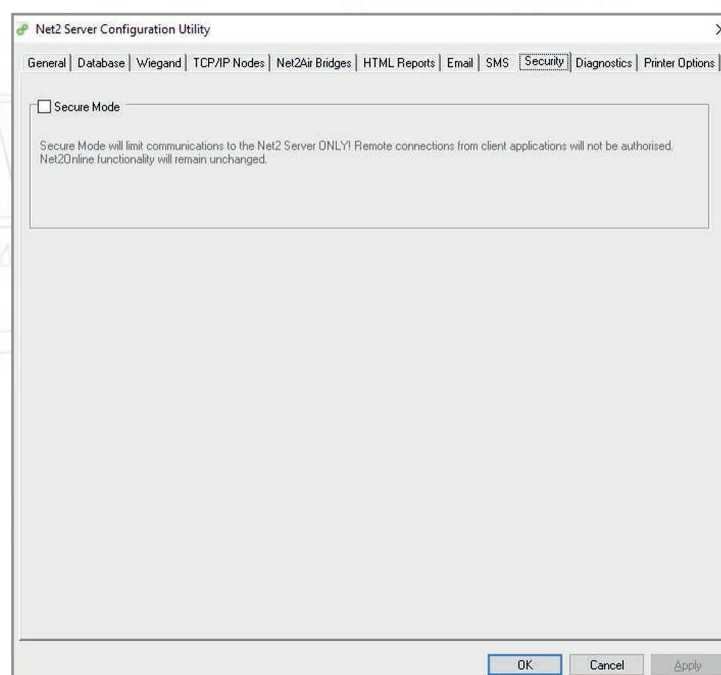


Net2 secure mode

Voor een optimale beveiliging van uw systeem adviseren wij om de Net2 Client op dezelfde PC te gebruiken als de Net2 (Lite of Pro) software.

Door Net2 Secure mode te activeren wordt de communicatie naar de Net2 database beperkt doordat de SQL TCP poort 1433 dicht gezet voor verbinding van buitenaf. Hierdoor is het niet meer mogelijk om de Net2 Client vanaf een LAN of WAN te gebruiken.

Wanneer u Net2 Secure mode inschakelt kunt u de Net2Online webbased client en Connect app blijven gebruiken voor het beheer op afstand. Om Net2 Online te gebruiken is een internetverbinding en de Pro software vereist.



Wilt u toch de volledige Net2 Client gebruiken op meerdere PC's in uw netwerk. Dan kunt u gebruik maken van desktop virtualisatie zoals VMware Horizon. Met deze software draaien virtuele desktops in een virtuele machine op een gecentraliseerde server. De Net2 software wordt op de virtuele machine geïnstalleerd en afhankelijk van de rechten van een gebruiker wordt in zijn virtuele desktop de Net2 applicatie weergegeven. Hierdoor kunt u Net2 beheren vanuit een andere LAN of VLAN.

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

Virtual Desktop Infrastructure (VDI) is het hosten van desktopomgevingen op een centrale server. Het is een vorm van desktopvirtualisatie omdat de desktopimages beschikbaar zijn in een virtuele machine (VM) en via het netwerk beschikbaar zijn voor gebruikers. De gebruikers kunnen daarvoor een pc of ander device gebruiken, zoals een tablet of thin client.

Let op: VMware horizon is voorzien van USB passthrough zodat u mogelijk de standaard Net2 desktooplezer(514-326-NL) kunt gebruiken. Dit dient wel voor implementatie getest te worden.

Indien de desktooplezer in uw omgeving niet functioneert kunt u de OEM desktop lezer met keyboard uitgang(214-326-NL) gebruiken. Deze desktooplezer functioneert als toetsenbord en is beter geschikt voor deze toepassingen. U kunt er daarnaast voor kiezen om een kaartlezer die aangesloten is op een deurcontroller in te stellen als desktooplezer om kaarten en tags te programmeren.

Extra netwerk beveiliging

1. Maak gebruik van MAC adresfiltering op de switch

Stel MAC adresfiltering in op uw netwerk switch. Dit zorgt ervoor dat alleen de MAC adressen van uw apparaten verbinding kunnen maken met het netwerk. Mocht er een onbekend MAC adres verbinding proberen te maken met het netwerk dan wordt de poort op de switch uitgeschakeld en kunt u afhankelijk van uw switch configuratie een melding ontvangen.

Voor alle netwerkkabels die zich buiten het gebouw bevinden is het de adviseren om MAC adresfiltering te gebruiken om ervoor te zorgen dat onbekende apparaten geen toegang krijgen tot uw netwerk van buitenaf.

2. Segmenteer de VLAN's

Installeer alle Paxton IP apparaten zoals deurcontrollers, Entry buitenposten en Entry binnenposten om hetzelfde VLAN. Zorg ervoor dat er vanuit dit VLAN geen verbinding mogelijk is naar andere delen van het netwerk. Mocht iemand ongeoorloofd toegang hebben tot dit VLAN dan kan er vanuit daar geen aanval gedaan worden op de rest van het netwerk.