NOX Systems

Security Whitepaper

Version 20.0

Version	Author	Changes	Date
19.0	Christian Tyllesen	NIS2 segment added	28.05.2024
20.0	Christian Tyllesen	OSDP encryption added	08.07.2024

ARAS Security A/S
+45 7027 4090
info@aras.dk
www.aras.dk

Table of Content

Introduction to NOX Software releases

EOL System software

Software release ≤R6 is End-of-life and is no longer supported and will not be updated by NOX Systems.

It is recommended to update the NOX CPU's to R8 (11.xx) to ensure the newest security technology and continued support and updates.

Valid from system version R7

The NOX central unit software is designed to comply with the newest IT security standards.

For this purpose, all Data transmission is encrypted (except NOX TIO device) and the connection is authenticated at the network layer.

In addition, the user must authenticate to the system using a user code or username/password.

If the central unit with the stored data falls into unauthorized hands, the data stored on the CPU cannot be read without valid authentication.

Safety measures:

- Use of TLS 1.2
- Protection against brute force attacks
- Protection against man-in-the-middle-attacks
- Optional customer-specific certificates for TLS authentication
- Configuration data in the CPU is stored encrypted
- System files in the CPU are checked for validity using encryption
- PC applications use Code Signing

Recommendations for high security installations (Class 3 and 4)

- Use of SL4 (authentication using username and password)
- Use of a password to view the configuration
- Use of complex password rules
- Activation of only the necessary network services in the system
- No use of NOX TIO devices with control functions (no encryption)
- Limitation of User Interfaces to what is absolutely necessary
- Use of time profiles to limit user validity

NOX and SIMS, common ports in use

Direction	Application	Description	From	To	Port	Configurable	Security	Standard setting
NOX Inbound								
	NOX Config	General System configuration	Software	Central unit	4322	No	Encrypted	Open
	NOX Config	NOX Loader	Software	Central unit	6251	No	Encrypted	Open
	NOX Config	Terminal Window	Software	Central unit	4321	No	Encrypted	Open
	NOX PC Control	User interface for Windows PC	Software	Central unit	4322	No	Encrypted	Open
	NOX PC TPA	User interface for Touch Screen w. graphics	Software	Central unit	4322	No	Encrypted	Open
	NOX Smartphone App	User interface for Smartphones and MacOS	Software	Central unit	4325	Yes	Encrypted	Closed
	NOX SSH Server	User interface, for simple integrations	Software	Central unit	22	Yes	Encrypted	Closed
	NOX Modbus Server	Integration with HVAC/CTS Systems	Software	Central unit	502	Yes	None	Closed
	NOX SNMP Trap Receiver	SNMP trap receiver from selected communities	Software	Central unit	162	No	None	Closed
	NOX TIO	User interface, Telnet/Text messages	Software	Central unit	4001	Yes	None	Closed
	NOX in Network Configuration	Several NOX Central units in the same network	Secondary Central	Main Central	8981	No	Encrypted	Closed
NOX Outbound								
	NTP	Time synchronization via NTP Server	Central unit	Service	123	No	None	Closed
	Modbus Client	Integration med HVAC/CTS Systems	Central unit	Service	502	Yes	None	Closed
	SMTP	E-mail dispatcher directly from NOX Central Unit	Central unit	Service	587	Yes	Encrypted	Closed
	NOX Smartphone App	NOX Push notifications: push.noxsystems.com	Central unit	Service	4324	No	Encrypted	Closed
	NOX TIO	User interface, Telnet/Text messages	Central unit	Service	4001	Yes	None	Closed
	SmartIntego	Wireless doors for NOX	Central unit	Gatenode	2101	No	None	Closed
	SIA IP	Alarm transmission	Central unit	ARC	30001	Yes	Optional	Closed
SIMS Inbound								
	SIMS Client	Client for managing SIMS connected NOX Central units	Client PC	SIMS Server	2010	Yes	Encrypted	Open
SIMS Outbound								
	SIMS Server	Connection to NOX Central units	SIMS Server	Central unit	4322	No	Encrypted	Open
	NOX License Server	NOX Systems Licens server: license.noxsystems.com	SIMS Server	Service	8777	No	Encrypted	Open

NOX Hardware

NOX BUS

The NOX bus is of the RS-485 Standard type.

The NOX bus uses obfuscation/blurring of data when communicating between the CPU and NOX devices, developed by NOX Systems.

All messages change form each time they are used, and it is therefore very complicated to simulate/emulate a message and play it back on the NOX bus.

The NOX bus is part of the NOX system and has no influence on the IT infrastructure, it is carried out as an independent part of the NOX installation itself.

If the bus is interrupted, the NOX system will generate a sabotage alarm for all missing units.

When attempting to manipulate data packets, these will be ignored as they do not contain the correct data structure.

OSDP BUS

The OSDP bus can be protected with a 128bit AES encryption, it is optional, and it is not enabled by default.

NB. Requieres NOX System ≥ 10.51L (R8) and CMO FW > 30

NOX Central units in Network

NOX in network conditions consists of 2 or more NOX CPUs that communicate via TCP/IP.

The communication is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85

From R7 (Version 10.0) 256-bit AES encryption is used.

Communication takes place on the following ports: 8981

The port is locked and cannot be changed.

NOX Redundant CPU

NOX Redundant CPU, consists of 2 NOX CPUs that communicate via TCP/IP, they are duplicated 1 to 1, and share physical buses, so that when one restarts or crashes, the other takes over without interruption. All communication between primary and secondary CPU takes place without encryption.

Communication takes place on the following ports: 8982

NOX PC Control

NOX PC Control is operating software that can access the NOX CPU via TCP/IP.

The communication is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85

From R7 (Version 10.0) 256-bit AES encryption is used.

From version 10.0, it is possible to opt for higher security through certificate-based authentication, or username and password authentication.

The software can be installed on all Windows versions, 32 bit and 64 bit, from Windows 7 onwards.

The prerequisite for fully functional software is pre-installation of .NET 2.0 (included in .NET 3.5.1)

Communication takes place on the following ports: 4322
The port is locked and cannot be changed.

NOX PC TPA

NOX PC TPA is operating software that can access the NOX CPU via TCP/IP.

The communication is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85

From R7 (Version 10.0) 256-bit AES encryption is used.

From version 10.0, it is possible to opt for higher security through certificate-based authentication, or username and password authentication.

The software can be installed on all Windows versions, 32 bit and 64 bit, from Windows 7 onwards.

The prerequisite for fully functional software is pre-installation of .NET 2.0 (included in .NET 3.5.1)

Communication takes place on the following ports: 4322

The port is locked and cannot be changed.

NOX Logger

NOX Logger is a small piece of software that can run independently of NOX Config or NOX PC Control, the features of this program is to collect logs in real-time through NoxDLL.dll.

The communication is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85 (NOX Logger 3.0)

From R7 (Version 10.0) 256-bit AES encryption is used.

From version 10.0, it is possible to opt for higher security through certificate-based authentication, or username and password authentication. (NOX Logger 4.0)

The software can be installed on all Windows versions, 32 bit and 64 bit, from Windows 7 onwards.

The prerequisite for fully functional software is pre-installation of .NET 2.0 (included in .NET 3.5.1)

Communication takes place on the following ports: 4322

The port is locked and cannot be changed.

NOX Config

NOX Config is configuration software that can access the NOX CPU via TCP/IP.

The communication is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85

From R7 (Version 10.0) 256-bit AES encryption is used.

From version 10.0, it is possible to opt for higher security through certificate-based authentication, or username and password authentication.

The software can be installed on all Windows versions, 32 bit and 64 bit, from Windows 7 onwards.

The prerequisite for fully functional software is pre-installation of .NET 2.0 (included in .NET 3.5.1)

Communication takes place on the following ports: 4321, 4322, 6251

The ports are locked and cannot be changed.

NOX SIMS V6

SIMS is a Server/Client software solution for multi-central and graphic solutions with the possibility of integration through SQL Server. SIMS stands for Security Information Management System.

Server:

The communication between SIMS Server and NOX CPUs is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85

From R7 (Version 10.0) 256-bit AES encryption and TLS 1.2 (SSL) are used.

From version 10.0, it is possible to opt for higher security through certificate-based authentication, or username and password authentication.

The software can be installed on all Windows versions, 32 bit and 64 bit, from Windows 7 onwards.

The prerequisite for fully functional software is pre-installation of .NET 2.0 (included in .NET 3.5.1) and .NET 4.5

Communication takes place on the following ports: 4322, 8777
The ports are locked and cannot be changed, if there is no access to port 8777, possible license updates must be transferred manually.

Client:

The communication between SIMS Client and SIMS Server is protected with a 128 bit AES encryption.

The software can be installed on all Windows versions, 32 bit and 64 bit, from Windows 7 onwards.

The prerequisite for fully functional software is pre-installation of .NET 2.0 (included in .NET 3.5.1) and .NET 4.5

Communication only takes place with the SIMS Server on the following ports: 2010

Port 2010 is recommended but can be freely changed.

iNOX & NOX for Android, MacOS

iNOX and NOX for Android are Smartphone apps that can access the NOX CPU via TCP/IP.

The communication is protected with a 384 bit Blowfish encryption, in all Firmware versions up to and including Version 9.85

From R7 (Version 10.0) 256-bit AES encryption is used.

From version 10.0, it is possible to opt for higher security through certificate-based authentication, or username and password authentication.

Communication takes place on the following ports: 4325

The port is recommended but can be freely changed.

NOX SSH

NOX SSH is only SSH Server, the communication can be chosen to be between 256 bit to 4096 bit Diffie Hellman, Private Key auth or Public Key auth.

For further information, refer to the Rebex website, www.rebex.net, Rebex File Server -> Features -> SSH Server

NOX PCIF (General protection of PC Interface)

Brute force prevention (Prevent repeated attempts with wrong code over IP)

In R6 (<9.85x):

The IP Interface follows the specified number of attempts and time, which is selected in NOX Config under "General -> General Settings -> User -> MMI Lockings", when the number of attempts is reached, the IP Interface is blocked for the relevant Source IP for the number of minutes specified (default time = 3 minutes).

In R7 (>10.0):

SL3: (Backward compatible code-only mode)

The IP Interface follows the specified number of attempts and time, which is selected in NOX Config under "General -> General Settings -> User -> MMI Lockings", when the number of attempts is reached, the IP Interface is blocked for the relevant Source IP for the number of minutes specified (default time = 3 minutes).

SL4: (High security, authentication through username and password, TLS 1.2)

1. It is recommended to use passwords with high complexity. The requirement for complexity is set up in NOX Config under "General -> General Settings -> Network access/Encryption -> Password rules"

2. For each incorrect login attempt, a delay of 1 ms is set, this increases up to 1 second, so it will take a disproportionately long time to "guess" the code. This delay is only removed by correct login.

The combination of complex codes and delay is considered a particularly secure protection against brute force attempts.

NOX Code policy (operating devices on NOX BUS)

The default configuration locks all control panels for 3 minutes upon 5 incorrect code entries, subsequently locks all panels for 5 minutes upon entry of the 6th incorrect entry. It is described in the Danish “Forsikring og Pension” (F&P) guidelines for Automatic Burglar Alarm facilities that it must be like this.

In NOX it is programmable, so if you want a stricter code policy it is possible.
We advise against relaxing the policy, as this means that the facility no longer meets F&P's requirements.

NOX Card + PIN code policy (CMx interfaces on NOX BUS)

f the PIN code is entered incorrectly, the default setting is that nothing happens.
It is a programmable feature and is not subject to rules such as the above from F&P.

In practice, this means that if you want a card to be blocked after 3 incorrect PIN entries, it is possible.

A blocked card can subsequently be opened by a person who can edit users through PC Control.

Dataflow/Bandwidth consumption

SIMS Server -> SIMS Client

The communication between SIMS Server and SIMS Client consists of encrypted data, mostly events (text), it requires almost no bandwidth.

There is a greater need when connecting a SIMS client to the SIMS Server for the first time, as floor plans are transferred. These drawings are cached on the client, and are synchronized on a new connection if changes have taken place.

Every time there is an event in the NOX System, this is sent to the SIMS Server, from where it is forwarded to active clients. Each event consists of max. 1 kB of data, an event is a setting, alarm, motion, etc.

The recommended bandwidth between SIMS Server and SIMS Client is 2 Mbit/s, which will cover the vast majority of cases, as it corresponds to 256 events per second. For larger SIMS installations with >50 NOX CPUs, a higher bandwidth may be necessary.

NOX CPU -> SIMS Server

The communication between NOX CPU and SIMS Server consists of encrypted data, mostly events (text), it requires almost no bandwidth.

Every time there is an event in the NOX System, this is sent to the SIMS Server. Each event consists of max. 1 kB of data, an event is a setting, alarm, motion, etc.

The recommended bandwidth between NOX CPU and SIMS Server is 0.5 Mbit/s, which will cover the vast majority of cases, as it corresponds to 64 events per second.

NOX CPU -> NOX Config/NOX PC Control

The communication between NOX CPU and NOX Config/NOX PC Control consists of encrypted data, mostly events (text), it requires almost no bandwidth.

Every time there is an event in the NOX System, this is sent to active clients. Each event consists of max. 1 kB of data, an event is a setting, alarm, motion, etc.

The recommended bandwidth between NOX CPU and SIMS Server is 0.5 Mbit/s, which will cover the vast majority of cases, as it corresponds to 64 events per second.

External Application -> NOX

There are many types of incoming connection options for NOX, common to them is that they are typically text-based, therefore they require almost no bandwidth. Some of these options also offer encryption (SSH/SDK). Since it is variable what you want to send to NOX, it will be necessary to make an assessment on a case-by-case basis. However, our experience is that 2 Mbit/s will be enough in 99 out of 100 cases.

NIS2 with NOX and SIMS

The EU has tightened the requirements for companies and authorities in the area of Cyber and Information Security, at the same time the EU has expanded the scope of which types of companies will be affected in the future. NIS2 (Network and Information Systems version 2) is aimed at Electronic communication networks, devices that process digital data, or systems that store data.

NOX

NOX are Certified and approved systems according to EN50131 Class 3, the highest security class in the EU.
In connection with the use of NOX in a company, it is important to know that it is only about securing the communication with the central unit, since the central unit is the only network-connected unit in a NOX system. As it appears from this document, all essential network communication is encrypted, and therefore NOX will be able to be included as a secure unit in a possible NIS2 assessment.
All Automatic burglar alarm and access control components are connected to an RS-485 BUS where the communication protocol is secured with a proprietary algorithm invented by NOX Systems.

SIMS

If a company wants to use SIMS (Multi Central Management platform for NOX), the same case applies as above. It is all about securing the communication with the central unit, since the central unit is the only network-connected unit in a NOX system.
SIMS is a Windows-based application which will be installed on a server and can be included in the customer's patching and maintenance plans on an equal footing with the company's other IT systems.

General recommendations

It is recommended to only use network technologies that support encrypted communication, the individual network technologies are described in detail in this document. In connection with the establishment of access control, we recommend using encrypted OSDP communication for readers, in combination with DESFire EV2/EV3 and Secure File reading as card technology, in this way the greatest possible security is achieved on card and reader, which at the same time prevents copying of cards and possibly "man-in-the-middle attack". All NOX Burglar alarm and access control components that are part of a Certified installation must maintain a security level corresponding to that of the customer or possibly 3rd party set level and class. If there is a need for further elaboration, or a need for a non-binding discussion about the safety on NOX systems, you can always contact us.

Principle drawing of NOX and SIMS installation in a typical environment