2N

2N IP products with 2N OS inside
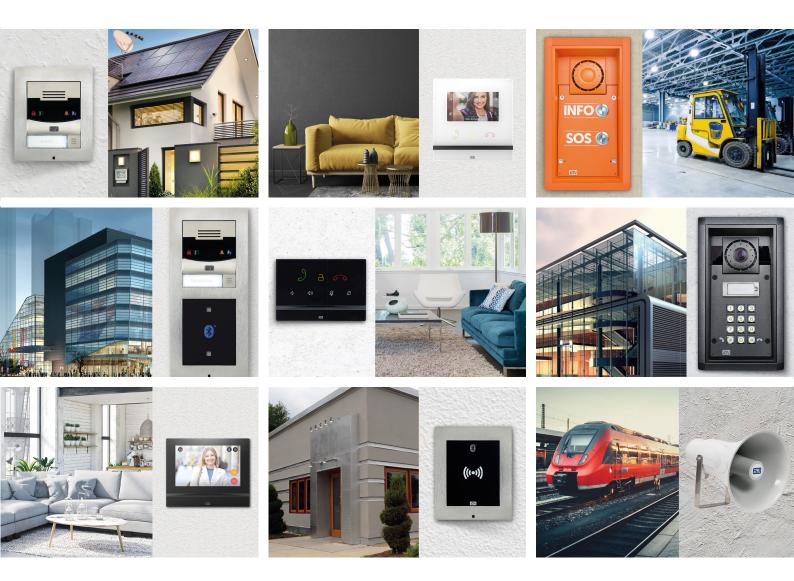
Table of contents

1.   Introduction

2N strives to apply cybersecurity best practices in the design, development and testing of our devices to minimize the risk of flaws that could be exploited in an attack. However, securing a network, its devices, and the services it supports requires active participation by the entire vendor supply chain, as well as the end-user organization. A secure environment depends on its users, processes, and technology. Therefore, we created this guide to support you in securing your network, devices and services.

The guide provides technical advice for anyone involved in deploying below mentioned 2N devices. It establishes a baseline configuration as well as a hardening guide that deals with the evolving threat landscape.

You may need the product's Configuration Manual to learn how to configure specific settings. See wiki.2n.cz for additional documentation.

Document applies to devices with firmware 2.29.0.

Products covered, referred to as "2N device" in scope of this document:
2N® IP Verso, 2N® IP Solo, 2N® IP Vario, 2N® IP Force, 2N® IP Safety, 2N® IP Uni, 2N® IP Base, 2N® IP Audio Kit, 2N® Indoor Talk, 2N® Indoor Compact, 2N® Indoor View, 2N® SIP Speaker Horn, 2N® SIP Audio Converter, 2N Access Unit and 2N Access Unit 2.0.

2.   System & Environment

2.1.   Direct Web Browser Access

2N devices have a web server that allows users to access the device using a web browser. The web interface is intended for configuration, maintenance and trouble shooting. It is not intended to be used for daily operation such as a client to view video. System users should never be allowed to access web configuration. Always log out when you are done with configuration.

2.2.   Other configuration tools

2N provides some additional tools for partial configuration of the device:

> 2N® Access Commander
>
> My2N cloud
>
> 2N® Network Scanner

If a device is connected to these tools, they have the right to change its configuration, partially or in whole. For more information on these tools visit www.2n.cz or [wiki.2n.cz.](wiki.2n.cz)

Configuration can also be changed by inserting complete or partial configuration file using HTTP API. See below recommendation on securing the HTTP API.

2.3.   2N devices in a network environment

The most apparent threats to a network device are physical sabotage, vandalism and tampering. To protect the product from these threats, it is important to select a vandal-resistant model or casing, to mount it in the recommended way, and to protect the cables. 2N recommends using auxiliary products increasing the security, like tamper switch (if available for selected product) or 2N® Security Relay.

From an IT/network perspective, the 2N device is a network endpoint similar to business laptops, desktops and mobile devices. Unlike a business laptop, a 2N network device does not have users visiting potentially harmful websites, opening malicious email attachments, or installing untrusted applications. However, it is a network device with an interface that may expose the system to risks. This guide focuses on reducing the exposure area of these risks.

2.4.   Limit Internet exposure

It is not recommended to expose the 2N device as a public web server, allowing unknown clients to get network access to the device. 2N recommends restricting access to local network from internet using appropriate networking tools.

2.5.   Limit local network exposure

Functionality of the 2N devices will require network access to other devices and systems. It is recommended to limit the access to this network to only necessary systems and personnel. Using virtually and/or physically isolated network is recommended.

2.6.   Information sharing

Do not share your login credentials to 2N device or any of the services used. Do not share configuration file without removing sensitive information first. Do not share syslog or network captures. Do not share your license keys or security codes provided by 2N with the product.

3. Protection levels

This guide uses different protection levels depending on organization type, size and needs.

Level	Description
*	Minimal level of hardening, all users are encouraged to follow these guidelines.
**	Measures increasing the level of security above the minimal level using moderate resources.
***	Measures relevant for corporate use, users with high risk of focused attack.

4. General

These guidelines apply to devices in general.

4.1. Factory default settings *

Before the first use of the device, make sure that the product is in a known factory default state. Read the manual how to factory default the device.

4.2. Upgrade to the latest firmware *

When new vulnerabilities are discovered, most are either not critical or are very costly to exploit. Occasionally a critical vulnerability is discovered, and device, computer, and systems services need to be patched. Patching software and firmware is an important process of cybersecurity. An attacker will often try to exploit common (known) vulnerabilities, and if they gain network access to an unpatched service, they may succeed. Make sure you always use the latest firmware because it may include security patches for known vulnerabilities. The release notes for a specific firmware may explicitly mention a critical security fix but not all the general ones.

Download the latest firmware file to your computer. The latest version is always available free of charge at www.2n.cz. Devices connected to the Internet can be upgraded directly from their web configuration. Before upgrading the firmware, study its release notes carefully and create a backup of configuration.

4.3. Set strong device password *

The device uses one level of access which is administrator level. The password needs to be set for the device to access its configuration. Make sure to use a strong password and keep it protected. On a multi-device installation, the devices can have the same password or unique passwords. Using the same password simplifies management but increases the risk if one device's security is compromised.

4.4. Set time and date *

From a security perspective, it is important that the date and time are correct so that, for example, the system logs are time-stamped with the right information.

It is recommended that the device clock be synchronized with a Network Time Protocol (NTP) server. For individuals and small organizations that do not have a local NTP server, a public NTP server may be used. Check with your Internet service provider or use a public NTP server such as pool.ntp.org.

5. Services

This section describes individual services of 2N devices with recommendations for their safe use.

5.1. Phone

5.1.1. SIP accounts

When using SIP PBX for calling, use authentication, refrain from using anonymous accounts *
When using SIP PBX for calling, use filtering of IP addresses *
Use SIPs (configured as TLS transport protocol for SIP) and SRTP for calling ***
Use user certificates ***

5.1.2. Calls

Do not enable incoming calls when not needed *

5.1.3. Local calls

Local calls use 2N own discovery protocol to enable calling on device name of the counterpart instead of IP address.
Disable local calls when not used *
When using local calls use strong Access Key *

5.1.4. Audio

Disable DTMF transfer using other method than SIP INFO *

5.1.5. Keypad

Do not enable calling on Virtual numbers if not used *
Do not enable telephone mode if not used *
If used, set maximal number length to the lowest value needed for operation to prevent dialing outside intended destination group *

5.2. Streaming

5.2.1. RTSP

Do not enable if not used *
If used only for video, disable streaming of audio *
Do not enable anonymous access *
Set a strong password for RTSP access *
Set list of authorized IP addresses **

5.2.2. Multicast

Do not enable if not used multicast streaming or receiving *

5.2.3. Informacast

Do not enable if not used *
If using Informacast service, only allow services which you need **

5.2.4. FTP

Do not enable if not used *
Use authentication for access to FTP server **

5.2.5. Angelcam

Do not enable if not used *

5.3. ONVIF

Disable WS discovery if not using ONVIF **
Do not enable Calling to AXIS Camera Station if not used *
Create ONVIF users with appropriate user right levels and strong passwords *

5.4. E-mail

Do not enable if not used *
Use SMTP server requiring authentication *
Verify server identity using certificates ***

5.5. HTTP API

Disable API services you are not using *
Use TLS *
Use authentication *
Use Digest authentication **

5.6. Web server

Disable remote access unless access from outside of LAN is needed *
Set minimal TLS version to 1.2 *
Set server certificate ***

5.7. SNMP

Do not enable if not used *

5.8. Network

Disable Restore Network Settings By Buttons *
Use dedicated VLAN ***
Use 802.1x to verify device identity ***

5.9. Autoprovisioning

Disable updates of configuration *
Disable updates of firmware *
If used, apply certificates and username/password ***
Disable TR069 if not used *

6.   Access control

Enable Limit Failed Access Attempts to prevent brute force
attacks on access control *
If using PIN codes for access control require at least 4 digits *
Change default 00 code *
Use user PIN codes instead of PIN shared among multiple users **
If using RFID for access control, use encrypted cards **
If using PIN for access control use scramble keypad on touch screen of IP Verso **
Enforce multifactor authentication **

7.   Specific guidelines for 2N® LTE Verso

Do not enable SIP if not used *
Do not enable web server if not used *

8.   Intellectual property rights

2N and the mother company Axis AB has intellectual property rights relating to
technology embodied in the product described in this document. In particular, and
without limitation, these intellectual property rights may include one or more of the
patents listed at www.axis.com/patent.htm and one or more additional patents or
pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About"
in the product's user interface for more information.

9.   About this document

This guide explains how to harden devices and it can also be used as collateral
for deployment teams dealing with local network policy, configurations and
specification.

All settings described in this document are available in the product's configuration
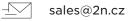web. For detailed description see wiki.2n.cz.

This document has been prepared carefully, if you identify any inaccuracies or
omissions, please inform a 2N representation. 2N TELEKOMUNIKACE a.s. is not
responsible for any technical or typographical errors in this document and reserves
the right to make changes to the product and manuals without prior notice.

2N TELEKOMUNIKACE a.s. makes no warranty of any kind with regard to the material
contained within this document, including, but not limited to, the implied warranties
of merchantability and fitness for a particular purpose.

2N TELEKOMUNIKACE a.s. shall not be liable nor responsible for incidental or
consequential damages in connection with the furnishing, performance or use of
this material. This product is only to be used for its intended purpose.

10. Contact information

2N TELEKOMUNIKACE a.s.
Modřanská 621/72
143 01 Prague 4
Czech Republic

✉ sales@2n.cz ☎ (+420) 225 271 111

11. Support

For technical assistance, please contact your 2N reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response.

If you are connected to the Internet, you can visit:
> www.2n.cz -   download user documentation and software updates.
> wiki.2n.cz -   find answers to resolved problems in the FAQ database. Search by product, category or phrase.