# Security Configuration Guide

Catalogue

# 1 Introduction

Akuvox company strives to apply cybersecurity best practices in the design, development, and testing of our devices to minimize the risk of defects that could be exploit in an attack. However, the entire vendor supply chain and end-user organization must be involved in securing a network, its devices, and the services it supports. A secure environment depends on its users, processes, and technology. The purpose of this guide is to help you keep your network, devices, and services secure.

The most obvious threats to an Akuvox device are physical sabotage, vandalism, and tampering. To protect a product from these threats, it's important to select a vandal-resistant model or casing, to mount it in the recommended manner, and to protect the cables. Akuvox recommend using auxiliary products to enhance security, such as tamper-proof switches (if applicable to the selected product) or Akuvox security relays.

From an IT/network perspective, Akuvox devices are network endpoints just like computers and mobile phones. Although Akuvox network devices do not include functions that allow users to access potentially harmful websites, open malicious email attachments, or install untrusted applications, they are still network devices with interfaces that can expose vulnerabilities to connected systems. This guide focuses on minimizing the attack surface of such risks.

The guide provides technical advice for anyone involved in deploying Akuvox devices mentioned below. It includes a recommended baseline configuration as well as a hardening guide that takes the evolving threat landscape into account. You may need to consult the product's user manual to learn how to configure specific settings. Please refer to https://knowledge.akuvox.com/docs for additional documentation.

## Scope

This guide applies applies to devices with firmware version xx.xx.10.x and above.
The products covered in this guide are collectively referred to as "Akuvox devices."

| | | | | | |
|---|---|---|---|---|---|
| **Door Phone** | | | | | |
| S539 | S532 | X916 | X915 | X912 | R29 |
| R28 | R20K | R20B | E21 | R25A | R20A |
| E18 | E16 | E12 | E11 | E20S | |
| **Indoor Monitor** | | | | | |
| S567 | S565 | S563 | S562 | S560 | IT88 |
| C319 | X933 | IT82 | C316 | C315 | C313 |
| **2-Wire Intercom** | | | | | |
| R20K-2 | R20A-2 | E12S-2 | C313W-2 | | |
| **Access Control** | | | | | |
| EC33 | A094 | A08 | A05 | A03 | A02 |
| A01 | | | | | |

# 2 Device Access and Configuration Tools

## 2.1 Access directly through a web browser

Akuvox devices have a web server that allows Administrators/users to access the device via a web browser. The web interface is intended for configuration, maintenance, and troubleshooting. It's not intended for daily operations, for example as a client to view video.

## 2.2 Other configuration tools

Akuvox provides several additional tools for partial device configuration:

- SDMC Device Management System
- PCManager Device Configuration Tool
- IPScanner Device Scanning Tool

If a device is connected to these tools, they are authorized to modify the device's configuration, either partially or fully. For more information about these tools, please visit https://knowledge.akuvox.com/docs/.

# 3 Protection levels

| Levels | Description |
|---|---|
| * | **Minimum Hardening Level**: Encourages all users to follow these guidelines. |
| ** | **Intermediate Hardening Measures**: Enhances security beyond the minimum level with moderate resource investment. |
| *** | **Advanced Hardening Measures**: Designed for enterprise use, targeting high-risk users who are priority attack targets. |

# 4 General Rules

These guidelines apply to all Akuvox devices.

## 4.1 Factory default settings*

Before you configure your device, make sure that it's in a factory default state. It's also important to reset the device to factory default settings when you need to clear it from user data or decommission it. Please read the user manual to learn how to restore the device to its default factory Settings.

## 4.2 Upgrade to latest Akuvox FW (Firmware)*

When vulnerabilities are discovered in the device itself, most are either non-critical or have a very high exploitation cost. Occasionally, critical vulnerabilities may be identified, requiring patches for the device, computers, and system services. Patching software is an important aspect of cybersecurity. Attackers will often try to exploit commonly known vulnerabilities and may succeed if they gain network access to an unpatched service. Make sure you always use the latest Akuvox FW since it may include security patches for known vulnerabilities. The release notes for a specific version may explicitly mention a critical security fix, but not all general fixes.

Download the latest firmware file to your computer. The latest version is available for free at https://knowledge.akuvox.com/docs/firmware-7, or you can contact the relevant technical support to

obtain the latest version. Before upgrading the firmware, please carefully read the release notes and create a backup of your configuration.

### 4.3 Use a strong password *

After logging in with the default account and password for the first time, the device will require a mandatory password change to ensure a strong password is set. It is also recommended to set up security questions in case the password is forgotten, allowing for password recovery.

In multi-device installations, devices can use either the same password or unique passwords. Using the same password simplifies management, but it increases the risk if the security of one device is compromised.

### 4.4 Configure date and time settings*

From a security perspective, it's important that you set the correct date and time. This ensures that that system logs are correctly time-stamped. It is recommended to synchronize the device clock with a Network Time Protocol (NTP) server.

Using public NTP or NTS servers, such aspool.ntp.org , or obtaining time form My2N can be an alternative for individuals and small organizations that can't facilitate local time server instances themselves.

### 4.5 Limit internet exposure**

We don't recommend that you expose the Akuvox device as a public web server, or that you in any other way give unknown clients network access to the device. Akuvox recommends using appropriate networking tools to restrict access from the Internet to local networks only.

### 4.6 Limit network exposure*

Akuvox devices require network access to other devices and systems. It is recommended to limit access to the network to only the necessary systems and personnel. The use of virtual and/or physical network isolation is advised.

### 4.7 Information Sharing*

Do not share your Akuvox device login credentials or any services you use. When sharing configuration files, ensure that sensitive information is removed. And do not share system logs or network captures.

## 5 Intercom

### 5.1 Calls

#### 5.1.1 SIP Accounts

- When using a SIP PBX for calls, enable authentication and avoid anonymous accounts. *
- Use SIPs (SIP configured with the TLS transport protocol) and SRTP for secure calls. ***
- Import and validate the SIP PBX certificate. ***

#### 5.1.2 General Settings

- Disable auto-answer if not required. *
- If there are no specific requirements, enable SIP HACKING protection. *

### 5.2 Access control

- Use time-based profiles. Avoid allowing 24/7 access if not necessary. *
- Disable public key-based door unlocking if not required. *
- Disable facial recognition for access if not in use. *
- Disable private key-based door unlocking if not necessary. *
- Disable Bluetooth-based door unlocking if not in use. *
- Disable NFC-based door unlocking if not in use. *
- Disable RFID-based door unlocking if not required. *
- Disable HTTP-based door unlocking if not in use. **
- Disable DTMF-based door unlocking if not necessary. **
- Disable QR code-based door unlocking if not needed. **
- When enabling RFID-based access, use encrypted cards for better security. *
- If HTTP-based access is required, set a strong authentication password. **
- If DTMF-based access is necessary, configure it with a 4-digit mode. **

### 5.3 Streaming media

#### 5.3.1 ONVIF/RTSP/MJPEG **

- Disable RTSP/MJPEG/ONVIF services if not in use.*
- If only video functionality is required, disable the audio stream.*
- When using the RTSP feature, enable Digest Authentication and configure a strong password.**
- It is recommended to configure an authorized IP address list for additional security.*

#### 5.3.2 Motion Detection

- If unused, disable motion detection. *

### 5.4 HTTP API

- If unused, disable the HTTP API service. *
- Enable authentication and use strong passwords (preferably different from the administrator account password). *
- Use Digest Authentication. **

## 6 Hardware

- After installation, enable tamper alarm functionality. *
- It is recommended to use a Security Relay to prevent unauthorized lock-picking. **
- *For the PIN interface keypad display mode, it is best to select the "Disorder" mode. *

# 7 Operations and Maintenance

- Do not enable the Remote Debug Server if it is not required. *
- Avoid enabling automatic configuration updates unless necessary. *
- Do not enable the packet capture function unless needed. *

## 8 About this document

This guide explains how to enhance device security and serves as a reference for deployment teams handling local network policies, configurations, and standards. All settings described in this document can be found on the product's configuration webpage. For detailed descriptions, please refer to: https://knowledge.akuvox.com/docs/intercom-manual.

This document has been carefully prepared. If you notice any inaccuracies or omissions, please inform your Akuvox representative. The Akuvox Support Team assumes no responsibility for any technical or typographical errors in this document and reserves the right to make changes to the product and manual without prior notice.

The Akuvox Support Team makes no warranties of any kind concerning the materials in this document, including but not limited to implied warranties of merchantability and fitness for a particular purpose.

The Akuvox Support Team shall not be liable for any incidental or consequential damages arising from the provision, performance, or use of these materials. This product is intended solely for its specified purposes.

## 9 Contact information

Contact Us For more information about the product,
please visit us at www.akuvox.com or feel free to contact us by Sales email: sales@akuvox.com
Technical support email: support@akuvox.com
Telephone: +86-592-2133061 ext.7694/8162
We highly appreciate your feedback about our products.