# Advanced public address server and license

PRA-APAS | PRA-APAL


**en** Release notes 1.10

# Table of contents

# 1 Introduction

## 1.1 Document history

| Release date | Documentation version | Reason |
|---|---|---|
| 12-05-2021 | V1.00 | 1st edition |
| 11-03-2022 | V1.10 | 2nd edition |

## 1.2 Release history

| Release date | Documentation version | Reason |
|---|---|---|
| 2021.06 | V1.0.31 | 1st official release |
| 2021.12 | V1.0.32 | Public intermediate release |
| 2022.03 | V.1.1.0 | 2nd official release |

## 1.3 Scope

The release notes give an overview of new functionalities compared to the previous release. It reports known limitations and possible workarounds.

## 1.4 Installation and configuration information

The PRA-APAS Advanced public address server and PRA-APAL Advanced public address license are products of the PRAESENSA system. Detailed installation and configuration instructions are provided in the installation manual and configuration manual of PRAESENSA and an additional dedicated Advanced public address server manual. All manuals can be downloaded in different languages from www.boschsecurity.com in the PRAESENSA product section.

When a PRAESENSA system is installed for voice alarm purposes, take notice of the installation and configuration directions in the checklist for compliance to the EN 54-16 and EN 54-4 standards. The checklist can be found at the end of the installation manual.

**Notice!**
The PRA-APAS is not certified to operate as a device for evacuation purposes. The device is designed for commercial use cases.

# 2 Supported products

## 2.1 Release 1.00

The PRA-APAS is only operational in combination with a PRA-SCL and compatible with the following PRAESENSA products:

| | |
|---|---|
| PRA-SCL | System controller, large |
| PRA-AD604 | Amplifier, 600W 4-channel |
| PRA-AD608 | Amplifier, 600W 8-channel |
| PRA-EOL | End-of-line device |
| PRA-MPS3 | Multifunction power supply, large |
| PRA-CSLD | Desktop LCD call station |
| PRA-CSLW | Wallmount LCD call station |
| PRA-CSE | Call station extension |
| PRA-ANS | Ambient noise sensor |
| PRA-ES8P2S | Ethernet switch, 8xPoE, 2xSFP |
| PRA-SFPSX | Fiber transceiver, multimode |
| PRA-SFPLX | Fiber transceiver, single mode |

## 2.2 Release 1.10

Same list of supported products as *Release 1.00, page 5*.

- A general security leak has been closed: update of security fix Apache log4j to 2.17.1.
- Twenty languages are now available for the graphic user interface. Refer to *Supported languages, page 6*.
- Implementation of auto-resize for text boxes and tiles to react on different lengths of text strings in other languages.
- Implementation of a bug fix in PA settings. It is now possible to leave the start chime empty if no start chime is required.
- Adjustment of the software to a new Amazon Polly Text-to-Speech feature. As a general new service, Amazon Polly offers Neural Text-to-Speech (NTTS). For 23 NTTS voices across 13 languages, Amazon Polly customers can choose a voice either as an NTTS or as a Standard voice.
- Addition of an indication for the 3000 characters limit to the text editor area for Text-to-Speech and announcement scrips.
- A user cannot change their own role anymore. As such, an integrator cannot downgrade their role and lock themselves out by mistake.

**Refer to**

- *Supported languages, page 6*
- *Release 1.00, page 5*

# 3 Notices

This chapter presents system characteristics that are normal, or even intended, but possibly not expected.

## 3.1 One PRA-APAL allows for one active operator

The number of enabled PRA-APAL Advanced public address licenses limits the number of active operators. When the number of possible simultaneous users exceeds the number of licenses, any additional user, who wants to login, will get a pop-up message. He is informed to make a choice. He can either refrain from continuing or he will logout another user to get access himself. To avoid this potential conflict, it is recommended to add one PRA-APAL for each active operator.

## 3.2 GUI is optimized for the use with 10” touch panel PCs

For better performance, the operator should use a touch panel PC with a 10” screen. A laptop PC with mouse pad is the best choice for the installer to work in the Settings menu during the system configuration.

## 3.3 Supported languages

English (US) is supported in Software and user interfaces.

Additional languages added with release 1.10:
- Danish (DK).
- Czech (CZ).
- German (DE).
- Greek (GR).
- Spanish (ES).
- Finnish (FI).
- French (FR).
- Hungarian (HU).
- Italian (IT).
- Korean (KR).
- Norwegian (NO).
- Dutch (NL).
- Polish (PL).
- Brazilian Portuguese (BR).
- Russian (RU).
- Slovakian (SK).
- Swedish (SE).
- Turkish (TR).
- Simplified Chinese (CN).
- Traditional Chinese (TW).

## 3.4 One PRA-APAS per IP network can connect to one System controller

The PRA-APAS is not a multi-controller solution. It is impossible to connect more than one System controller to a single PRA-APAS. It is also impossible to connect several PRA-APAS to one single System controller and it is not allowed to connect multiple PRA-APAS to multiple PRA-SCL on the same IP network.

## 3.5 OMNEO control is not compatible with the APAS

OMNEO control does not support AES67 audio streams, because it would clean up the AES67 audio streams every 30 seconds. Therefore OMNEO control cannot be used in combination with the PRA-APAS and there is also no need to use the combination.

## 3.6 After a restart it takes several minutes to reestablish BGM

It is intended to run the PRA-APAS 24/7. If a power circle of the PRA-APAS is done, it takes up to two minutes before basic functionality is operational again. The reestablishment of the online audio streams and BGM might take additional five minutes.

## 3.7 Automatic logout after 15 minutes of inactivity

For security reasons an operator is automatically logout after 15 minutes of inactivity.

## 3.8 Manual time settings will restart the server

After a manual change of the time settings the server will restart, which will take about 100 seconds. After the restart a new login is required.

## 3.9 Start playing the message takes too long after the pre-chime

The message is played within 2.5 seconds, after the pre-chime ended. If the pause seems too long, configure another pre-chime. Most likely the reverberation time of the chosen pre-chime is unsuitable for the use with the PRA-APAS.

## 3.10 Firefox does not allow for login anymore

When the operator tries to access the browser of the PRA-APAS for login, he receives the fault message **Secure connection failed**. This issue is related to a particular installation of Firefox (or policy in it). It usually happens when Firefox internal certificate trust store is corrupted. Please refer to the Troubleshooting chapter of the Configuration manual.

# 4 Known limitations

These system functions are implemented but with limitations. In some cases, workarounds are given.

## 4.1 Music control of the same BGM zone with CST and APAS

It is possible to control the same BGM zone with the PRA-APAS and a Call station with the following remarks:

– Online radio streams of the PRA-APAS are send to the PRAESENSA network without transmitting the name of the source. In the **Music** menu of the Call station, the LCD will display **unknown source**.
– The PRA-APAS Graphic user interface follows volume changes of the BGM zone made by the Call station. Only if the control window of the same BGM zone is already open, the page needs to be refreshed to update the Volume slider.

## 4.2 It is not recommended to use Safari in combination with the APAS

With Safari iOS 14.0, it is expected that:

– The silence period between pre-chime and message might be six seconds.
– When pre-listening to an announcement, the first 1.5 seconds of the recording might be missing, but the announcement will be completely played to the areas.

– If you are unable to pre-listen to announcements at all:

1. Check that PRA-APAS website is listed in the Safari browser > **Preferences** > **Websites** > **Auto-Play**.
2. Select **Allow All Auto-Play**.

**Notice!**
Use Google Chrome or Microsoft Edge for better performance with an iPAD.

# 5 Security precautions

PRAESENSA is an IP-connected, networked Public Address and Voice Alarm system. In order to ensure that the intended functions of the system are not compromised, special attention and measures are required during installation and operation to avoid tampering of the system. Many of such measures are provided in the PRAESENSA configuration manual and installation manual, related to the products and the activities described. This section provides an overview of precautions to be taken, related to network security and access to the system.

- Follow the installation instructions with respect to the location of equipment and the permitted access levels. See section Location of racks and enclosures of the PRAESENSA installation manual. Make sure that call stations that address very large areas (critical) and operator panels that are configured for alarm functions only have restricted access using a special procedure, such as being mounted in an enclosure with lockable door or by configuration of user authentication on the device. The availability of the user authentication function will be announced.
- It is highly recommended to operate PRAESENSA on its own dedicated network, not mixed with other equipment for other purposes. Other equipment may be accessible by unauthorized people, causing a security risk. This is especially true if the network is connected to the Internet.
- It is highly recommended that unused ports of network switches are locked or disabled to avoid the possibility that equipment is connected that may compromise the system. This is also the case for PRAESENSA call stations that are connected via a single network cable. Make sure that the connector cover of the device is in place and properly fixed, to avoid that the second network socket is accessible. Other PRAESENSA equipment should be installed in an area that is only accessible by authorized people to avoid tampering.
- PRAESENSA uses secure OMNEO for its network connections, using encryption and authentication for all control and audio data exchange, but the system controller allows the configuration of unsecure Dante or AES67 audio connections as an extension of the system, both as inputs and as outputs. These Dante/AES67 connections are not authenticated and not encrypted and form a security risk, as no precautions are taken against malicious or accidental attacks via their network interfaces. For highest security, these Dante/AES67 devices should not be used as part of the PRAESENSA system. If such inputs or outputs need to be used, use unicast connections only. Only Dante devices should be used that support Device Lock. Device Lock allows you to lock and unlock supported Dante devices using a 4-digit PIN (Personal Identification Number). Make sure that the devices are locked when in normal operation. Dante Controller is needed to set the PIN and setup the connections. Alternatively use Dante Domain Manager.
- For security reasons, by default the PRA-ES8P2S Ethernet switch is not accessible from the Internet. When the default (special link-local) IP-address is changed to an address outside the link-local range (169.254.x.x/16), then also the default (published) password must be changed. But even for applications on a closed local network, for highest security the password may still be changed. See section Ethernet switch, chapter Installation of the PRAESENSA installation manual.
- The PRA-ES8P2S network switch supports SNMP. By convention, most SNMPv1-v2c equipment ships from the factory with a read-only community string set to "public". This also applies to the PRA-ES8P2S. For security reasons SNMP should be disabled. If SNMP must be enabled, for example to use the Bosch Network analysis tool OMN-DOCENT, use SNMPv3. SNMPv3 provides much better security with authentication and privacy. Select the authentication level SHA and encryption via AES. To configure the switch accordingly,

see section Ethernet switch, chapter Installation of the PRAESENSA installation manual. The system controller webserver uses secure HTTPS with SSL. The web server in the system controller uses a self-signed security certificate. When you access the server via https, you will see a Secure Connection Failed error or warning dialog indicating that the certificate was signed by an unknown authority. This is expected and to avoid this message in the future you have to create an exception in the browser.

- Make sure that new user accounts for system configuration access use sufficiently long and complex passwords. The user name must have between 5 and 64 characters. The password must have between 4 and 64 characters.
- The PRAESENSA system controller provides an Open Interface for external control. Access via this interface requires the same user accounts as for system configuration access. In addition, the system controller generates a certificate to setup the TLS (secure) connection between the system controller and the Open Interface client. Download the certificate and open/install/save (depending on browser type) the crt-file. Activate the certificate on the client PC. See section System security of the PRAESENSA configuration manual.
- System access to the devices of this system is secured through the OMNEO security user name and passphrase of the system. The system uses a self-generated user name and long passphrase. This can be changed in the configuration. The user name must have between 5 and 32 characters and the passphrase must have 8 to 64 characters. To update the firmware of the devices, the firmware upload tool requires this security user name and passphrase to get access.
- In case a PC for event logs is used (PRAESENSA logging server and viewer), make sure that the PC is not accessible by unauthorized persons.

**Bosch Security Systems B.V.**
Torenallee 49
5617 BA Eindhoven
Netherlands
**www.boschsecurity.com**


**Building solutions for a better life.**

202203141637