

Advanced public address server and license

PRA-APAS | PRA-APAL

Table of contents

1	Introduction	4
1.1	Release history	4
1.2	Scope	4
1.3	Installation and configuration information	4
2	Release overview	5
2.1	Release 1.31	5
2.2	Release 1.30	5
2.3	Release 1.20	5
2.4	Release 1.10	5
2.5	Release 1.00	6
3	Notices	7
3.1	One PRA-APAL allows for one active operator	7
3.2	GUI is optimized for the use with 10" touch panel PCs	7
3.3	Supported languages	7
3.4	One PRA-APAS per IP network can connect to one System controller	7
3.5	OMNEO control is not compatible with the APAS	8
3.6	After a restart it takes several minutes to reestablish BGM	8
3.7	Automatic logout after 15 minutes of inactivity	8
3.8	Manual time settings will restart the server	8
3.9	Start playing the message takes too long after the pre-chime	8
3.10	Firefox does not allow for login anymore	8
4	Known limitations	9
4.1	Music control of the same BGM zone with CST and APAS	9
4.2	Do not use Safari in combination with the APAS	9
5	Security precautions	10

1 Introduction

1.1 Release history

Release date	Version	Reason
2021-07	1.00	Official release.
2022-03	1.10	Official release.
2023-11	1.20	Official release.
2024-11	1.30	Official release.
2026-07	1.31	Official release.

1.2 Scope

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

1.3 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.keenfinity-group.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 Release overview

2.1 Release 1.31

- Fixed an issue with the web music sources that stopped playing.
- Improved backup functionality. Users can now export and import backups that contain large media files, not limited to 10 GiB of size a processing time of 30 minutes.
- Updated the time zone database.

2.2 Release 1.30

- Added support for the PRA-SCS System controller, small. The same functionalities as the large system controller apply, with the following exceptions:
 - The minimum number of Audio input offset is 9.
 - The maximum number of AES67 Audio channels is 8.
- A scheduled paused event is no longer automatically activated after a configuration change. The paused event remains paused until the user intentionally activates it.
- The APAS web server connection supports TLS 1.3. The PRA-APAS can still use lower TLS versions, if 3rd party servers, such as streaming music sources, do not support TLS 1.3.
- The maximum call priority is now 223, instead of 200. The minimum call priority remains 32.
- The logout time is now 12 hours, instead of one hour. The automatic logout after 15 minutes of inactivity remains.
- Improved cyber security due to updated firewall rules and security patches.

**Notice!**

Software release version **1.30** appears as release version **1.2.1-1688** for the firmware.

2.3 Release 1.20

Same list of supported products as Release 1.00, page 6.

Added functionalities

- Text-to-Speech support by Microsoft Azure added. Microsoft Azure expands the selection of available languages and voices. Choose either Amazon Polly or Microsoft Azure as required.
- Flags in the introductory screen reassigned correctly.
- Bug that occurred during scheduler operation fixed. Now, if you pause a scheduled event for a specific announcement and edit it during that pause, the original event is removed and not restarted.

2.4 Release 1.10

Same list of supported products as Release 1.00, page 6.

Added functionalities

- 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 7.
- 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.

2.5

Release 1.00

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

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

As of release 1.10, the languages supported by the PRA-APAS user interface are:

- American English
- British English
- Danish
- German
- Spanish
- French
- Italian
- Hungarian
- Dutch
- Norwegian
- Polish
- Brazilian Portuguese
- Slovakian
- Finnish
- Swedish
- Turkish
- Czech
- Greek
- Russian
- Simplified Chinese
- Traditional Chinese
- Korean.

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

The PRA-APAS is not a multi-controller solution. As such:

- It is impossible to connect more than one system controller to a single PRA-APAS.
- It is impossible to connect several PRA-APAS to one single system controller.

- It is not allowed to connect multiple PRA-APAS to multiple system controllers 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, they receive 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. Refer to the Troubleshooting chapter of the User 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 sent 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 Do not 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. To make sure that the intended functions of the system are not compromised, special attention and measures are required during installation and operation. The PRAESENSA configuration manual and installation manual provide many security measures related to the products and the activities described. This section provides an overview of precautions 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. Refer to the chapter *Location of racks and enclosures* in the PRAESENSA installation manual for more information. Make sure to restrict access to call stations that address very large areas and to operator panels configured for alarm functions. To do so, mount them in an enclosure with a lockable door or configure user authentication on the device.
- It is highly recommended to operate PRAESENSA on its own dedicated network. Do not mix the system with equipment with other purposes. The extra equipment can 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 to lock or disable unused ports on network switches to avoid the possibility that connected equipment can compromise the system. This is also the case for PRAESENSA call stations connected through a single network cable. Make sure the connector cover of the device is in place and fixed to avoid access by a second network socket. Install other PRAESENSA equipment in an area that is only accessible by authorized people to avoid tampering.
- Use an Intrusion Protection System (IPS) with port security where possible to monitor the network for malicious activity or policy violations.
- PRAESENSA uses secure OMNEO for its network connections. All control and audio data exchange use encryption and authentication. 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. This forms a security risk, as no precautions are taken against malicious or accidental attacks through their network interfaces. For highest security, these Dante/AES67 devices should not be used as part of the PRAESENSA system. If you need such inputs or outputs, use unicast connections.
- The following switches report their power faults and network connection status directly to the PRAESENSA system controller through SNMP:
 - From PRAESENSA software version 1.50 onwards, the PRA-ES8P2S switch and the Cisco IE-5000-12S12P-10G switch/router.
 - From PRAESENSA software version 2.30 onwards, the Cisco IE-9320-22SC4X-A switch/router.
 - From PRAESENSA software version 2.40 onwards, the PRA-ES8E8S switch.The switches can be daisy-chained without an OMNEO device between them for connection supervision. Both PRAESENSA switches are preconfigured for this purpose.
- For security reasons, the PRA-ES8P2S and the PRA-ES8E8S Ethernet switches are not accessible from the Internet by default. When the default (special link-local) IP-address is changed to an address outside the link-local range (169.254.x.x/16), the default (published) password must be changed. Even for applications on a closed local network, for highest security, the password must still be changed. Refer to the *Ethernet switch* chapter in the PRAESENSA installation manual for more information.
- To enable SNMP, for example to use the analysis tool Network Docent, use SNMPv3. SNMPv3 provides much better security with authentication and privacy. Select the authentication level SHA and encryption via AES. Refer to the *Ethernet switch* chapter in the PRAESENSA installation manual for more information.

- 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 a minimum of five characters and a maximum of 16 characters. The password must contain the characters as defined in the **System settings**. For more information, refer to the System settings chapter of the PRAESENSA configuration manual.
- The PRAESENSA system controller provides an Open Interface for external control. Access through this interface requires the same user accounts as for the 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 the crt-file. Activate the certificate on the client PC. Refer to the System security chapter in the PRAESENSA configuration manual for more information.
- System access to the devices of this system is secured via 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.
- Use secure VoIP protocols (SIPs) whenever possible, including verification through VoIP server certificate. Only use non-secure protocols when the SIP server (PBX) does not support secure VoIP. Only use VoIP audio in the protected sections of the network, because the VoIP audio is not encrypted.
- Anyone with the ability to dial one of the extensions of the system controller can make an announcement in the PRAESENSA system. Do not allow external numbers to dial the system controller extensions.

Find all documentation and software related at <https://www.keenfinity-group.com/> in the **Downloads** section of the PRAESENSA products.

Whenever you think you have identified a vulnerability or any other security issue related to a product or service, refer to <https://www.keenfinity-group.com/x/en/support/product-security/>

Electro Voice Dynacord B.V.

Achtseweg Zuid 173

5651 GW Eindhoven

The Netherlands

www.keenfinity-group.com

© Electro Voice Dynacord 2026