PRAESENSA

Public Address and Voice Alarm System

en Release notes 1.20

Table of contents

1	**Introduction**	**4**
1.1	Document history	**4**
1.2	Release history	**4**
1.3	Scope	**4**
1.4	Installation and configuration information	**4**
2	**Supported products**	**5**
2.1	Release 1.00	**5**
2.2	Release 1.10	**5**
2.3	Release 1.20	**6**
3	**Compliance to voice alarm standards**	**7**
3.1	Release 1.00	**7**
3.2	Release 1.10	**7**
3.3	Release 1.20	**7**
4	**Notices**	**8**
4.1	Documentation and software download	**8**
4.2	Load measurement	**8**
4.3	Audio equalizer	**8**
4.4	Minimum message length	**8**
4.5	Logging server compatibility	**8**
4.6	System controller redundancy configuration	**8**
4.7	Brightness adjustment	**8**
4.8	Network snapshot	**8**
5	**Missing functions**	**9**
5.1	System controller	**9**
6	**Known limitations**	**10**
6.1	Firmware upload to call station fails	**10**
6.2	Dante multicast	**10**
6.3	Scheduled calls	**10**
6.4	Load measurement	**10**
6.5	Firmware upgrade	**10**
6.6	Enable Network Time Protocol (NTP)	**10**
6.7	Smart safety link	**10**
6.8	Dante audio outputs	**11**
6.9	Multiple redundant System controllers	**11**
6.10	DHCP server	**11**
7	**Security precautions**	**12**

1 Introduction

1.1 Document history

Release date	Documentation version	Reason
2019.12.19	V1.00	1st edition
2020.05.15	V1.10	2nd edition
2020.06.18	V1.10_01	Chapter updated: 3.2
2020.09.29	V1.20	Chapters updated: 1.1, 1.2, 6.8, 6.9. New chapters: 2.3, 3.3, 5.1, 6.10.

1.2 Release history

Release date	Released version	Reason
2019.12.06	1.00	1st official release
2020.05.18	1.10	2nd official release
2020.09.30	1.20	Official release

1.3 Scope

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

1.4 Installation and configuration information

PRAESENSA products are delivered with a quick installation guide (QIG) for basic step-by-step installation instructions. Detailed installation and configuration instructions are provided in the installation manual and configuration manual of PRAESENSA. Both 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.

2 Supported products

2.1 Release 1.00

The following PRAESENSA products can be installed and configured:

PRA-SCL	System controller, large
PRA-AD608	Amplifier, 600 W 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-ES8P2S	Ethernet switch, 8xPoE, 2xSFP
PRA-SFPSX	Fiber transceiver, multimode
PRA-SFPLX	Fiber transceiver, single mode

The following products can be used without need for configuration:

PRA-PSM24	Power supply module 24 V
PRA-PSM48	Power supply module 48 V

The following products are already described in the installation manual and/or the configuration manual, but are not yet available:

PRA-SCM	System controller, medium
PRA-SCS	System controller, small
PRA-AD604	Amplifier, 600 W 4-channel

2.2 Release 1.10

Same list as *Release 1.00, page 5*, but now the PRA-AD604 is part of the set that can be installed and configured.

Added functionality:

- Support of PRA-AD604 4-channel, 600 W amplifier.
- System controller redundancy.
- Fault simulation of an amplifier channel to force amplifier to spare channel.
- Dimming of Call station LCD and LEDs.
- Configurable audio delay for every amplifier channel.

2.3 Release 1.20

Same (list) of supported products as *Release 1.00, page 5* and *Release 1.10, page 5*.

Added functionality:

- The configuration webpages are available in additional languages: Czech, German, Spanish, English, French, Italian, Dutch, Korean, Polish, Portuguese, Russian, Slovakian, simplified Chinese.
- UL amplifier mode is added to system settings. When the amplifiers run in this mode, they comply to the requirements of UL with regards to temperature limitations.
- In a system with System controller redundancy, the Dante audio routing for inputs and/or outputs is synchronized with the redundant System controller. The Dante audio routing is configured for the duty System controller. As soon as the backup System controller takes over the Dante audio routing is automatically recreated.
- Fixes have been applied to the following security vulnerabilities of the configuration web interface. These changes only affect the web interface which is only used during configuration of the system:
  - In the web configuration of the System controller a Cross-Site Request Forgery (CSRF) vulnerability has been found. This has been solved by adding verification data to the web pages.
  - In the web configuration of the System controller a Cross-site Scripting (XSS) vulnerability has been found. This has been solved by sanitizing the data that is received from the web pages better to avoid that script data is fed back to the browser.
  - Additional HTTP headers are added to the web pages giving instructions to the browser in helping to avoid cross-site attacks.

3 Compliance to voice alarm standards

3.1 Release 1.00

This software release in combination with the following products is certified for compliance to EN 54-16 and EN 54-4. See 0560-CPR-182190000 and Declaration of Performance GO002945v1.

PRA-SCL	System controller, large
PRA-AD608	Amplifier, 600 W 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-ES8P2S	Ethernet switch, 8xPoE, 2xSFP
PRA-SFPSX	Fiber transceiver, multimode
PRA-SFPLX	Fiber transceiver, single mode

3.2 Release 1.10

Same list as in *Release 1.00, page 7*, but now the PRA-AD604 is included.
This software release in combination with the previous described products is certified for compliance to EN 54-16 and EN 54-4. See 0560-CPR-182190000 and Declaration of Performance GO002945v1.
The same combination is also tested and found compliant to ISO 7240-16 and ISO 7240-4.

PRAESENSA is certified according the DNV-GL type approval. This is valid for the listed products and the power supply module PRA-PSM48.

3.3 Release 1.20

Same (list) as *Release 1.00, page 5* and *Release 1.10, page 5*.
No new changes and/or additions.

4 Notices

System characteristics that are normal, or even intended, but possibly not expected.

4.1 Documentation and software download

Multi-lingual PRAESENSA product documentation and software is available from www.boschsecurity.com > PRAESENSA product section. An additional download area for PRAESENSA software and English documentation is here: https://licensing.boschsecurity.com/publicaddress.

4.2 Load measurement

The amplifier loudspeaker load measurement is part of the configuration (Diagnose > Amplifier loads). It is an essential step in the system configuration to do a load measurement to check whether the amplifier channels and the amplifier are not overloaded. Without this check, the amplifier channel volume is automatically set to -12 dB to protect the amplifier from unexpected overload conditions in case of an alarm situation.

4.3 Audio equalizer

The DSP audio equalizers have an internal headroom of 18 dB. Do not use audio equalizer settings with an accumulated gain of more than 18 dB at any frequency, as this will cause audio clipping for full scale input signals. It is good practice to do most of the frequency response corrections by attenuation of prominent frequency bands.

4.4 Minimum message length

The minimum message length for repeating messages is 500 ms.

4.5 Logging server compatibility

In release 1.10 the Open Interface of the System controller was updated, incompatible with the Logging Server of release 1.00. To continue receiving diagnostic events from the System controller, the Logging Server with the Open Interface .NET library must be updated to release 1.10.

4.6 System controller redundancy configuration

When a second System controller is added to a system for redundancy, the second System controller must be reset to factory default.

4.7 Brightness adjustment

The brightness adjustment of the PRA-CSLD and PRA-CSLW LCD and PRA-CSE LEDs is only supported on devices with HW version 01/01 and higher.

4.8 Network snapshot

A new network snapshot is required after a device was added, removed or replaced.
A system with redundant cabling and network supervision enabled, requires a new network snapshot after a device was added, removed or replaced.
Until this is not done, the fault in the new device will not be reported.

5 Missing functions

System functions that are mentioned in the documentation, but have been postponed.

5.1 System controller

PRA-SCS System controller small and PRA-SCM System controller medium are postponed to a later release. System controller large (PRA-SCL) performs effectively equal or better than the smaller versions.

6 Known limitations

System functions that are implemented but with limitations. In some cases workarounds are given.

6.1 Firmware upload to call station fails

The MTU (Maximum Transmission Unit) of the call stations is 1468. When the MTU of the PC network adapter that is used is set to a lower value than 1472 (1468 + 4), the data packets are split across different frames; the FWUT (Firmware Upload Tool) cannot handle this and will disconnect.
Check the actual MTU value of the network adapter by opening a **cmd-**window (with administrator rights) and enter:

netsh interface ipv4 show subinterface

If the MTU value is too low, it can be increased temporarily to a higher value by entering:

netsh interface ipv4 set subinterface
"<name of interface>" mtu=1500
store=persistent
Then try again.

6.2 Dante multicast

Only use Dante unicast streams between a Dante device and the system controller to prevent multicast addressing conflicts, that can result in audio distortion or not being able to setup a call.

6.3 Scheduled calls

If a scheduled call is activated by a button of a call station extension, the scheduled time intervals are ignored and the call starts immediately. Scheduled calls can only be started from a control input.

6.4 Load measurement

When a load measurement on an amplifier channel is done with a shorted loudspeaker line, the web page will indicate: “Not measured”. Remove the short circuit and redo the load measurement.

6.5 Firmware upgrade

Before using the firmware upgrade tool, make sure the released PRAESENSA firmware files have been installed also.
In some rare cases the upgrade of a device will not be successful in the first attempt. If this occurs please retry for the device for which it failed.

6.6 Enable Network Time Protocol (NTP)

NTP is configured on the “Time settings” page. Enable “Set time automatically (NTP)” and press submit. Wait for the reboot system page; this will take a few seconds. Press “System reboot” to activate NTP. If you navigate away to another configuration page too early and don’t wait for the reboot system page, a non-responsive web page will show "Loading" and NTP will remain disabled.

6.7 Smart safety link

Smart safety link does not support System controller redundancy. In combination with PRAESENSA and Bosch fire detection systems a Smart safety link communication is possible.

When a backup System controller will take over the duty System controller, an evacuation call, that was activated by a Smart safety link connection is stopped and not restarted. The missing functionality will be added to the next software release of the Bosch fire detection system.

6.8 Dante audio outputs

A system with System controller redundancy does not support secure Dante 4-digit PIN (Personal Identification Number) on the Dante audio outputs.
You might want to use Dante audio outputs to interface with 3rd party devices like amplifiers or devices for recording purposes. When control is switched from duty system controller to redundant System controller, the transmit of the Dante output channels of the duty system controller is moved to the redundant System controller in order to make the Dante audio outputs redundant.
The persistent Dante audio channels cannot be authenticated and not encrypted, so they form a security risk, as no precautions are taken against malicious or accidental attacks via their network interfaces. For highest security, these Dante output channels in combination with System controller redundancy should **not be used** as part of the PRAESENSA system.

6.9 Multiple redundant System controllers

Release 1.10 and 1.20 are tested with one duty and one redundant System controller. There is no built-in limit, and it is possible to add multiple redundant System controllers. A system setup with more than one redundant System controller was not tested and proper operation cannot be confirmed.

6.10 DHCP server

When the DHCP server is not available when the system starts it can happen that some devices do not receive an DHCP IP-address and will remain in link-local. The consequence is that these devices do not connect to the System Controller. If the System Controller does not receive a DHCP IP-address it cannot connect to the system devices. It is strongly recommended to have the DHCP server available when the system starts.

7 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 4.1 of the PRAESENSA installation manual. Make sure that critical* call stations 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**.
  * Call stations, that address very large areas, are considered as critical.
  ** Availability of the user authentication function is to 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 14.5 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 14.5 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 7.2 of the PRAESENSA configuration manual.
- 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.

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

202009291156