DYNACORD

PROMATRIX 9000

Security precautions

en Safety and security information

Table of contents

1 Security precautions

Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:

- General information: https://www.boschsecurity.com/xc/en/support/product-security/
- Security advisories, that is a list of identified vulnerabilities and proposed solutions: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

PROMATRIX 9000 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 PROMATRIX 9000 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.

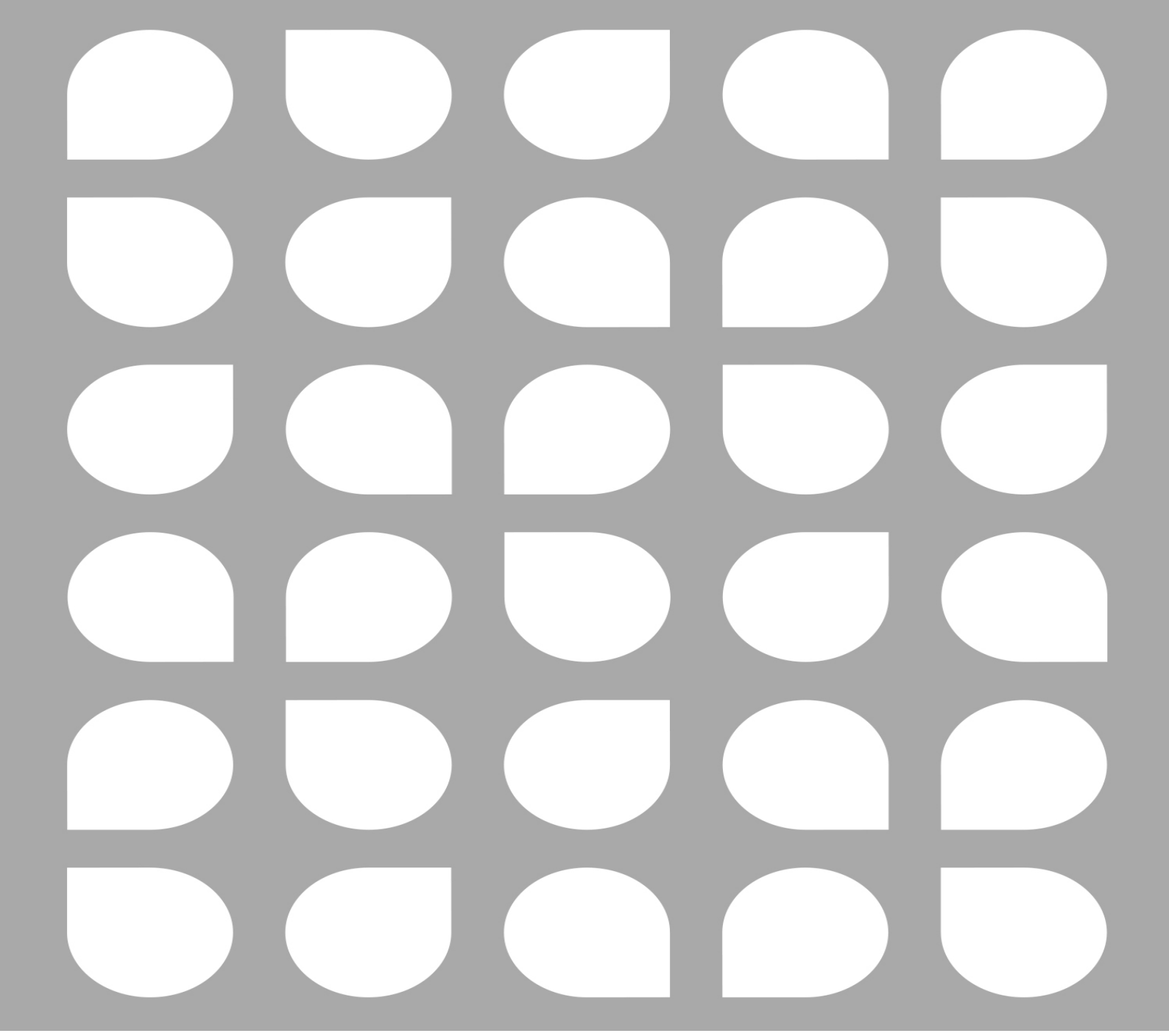
- Follow the installation instructions with respect to the location of equipment and the permitted access levels. Refer to the chapter *Location of racks and enclosures* in the PROMATRIX 9000 Installation manual for more information. Make sure that call stations that address very large areas and operator 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.
- It is highly recommended to operate PROMATRIX 9000 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 PROMATRIX 9000 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 PROMATRIX 9000 equipment should be installed 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.
- PROMATRIX 9000 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. They form 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 PROMATRIX 9000 system. If such inputs or outputs are needed, use unicast connections.

- 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. Refer to the *Ethernet switch* chapter in the PROMATRIX 9000 Installation manual for more information.
- To enable SNMP, for example to use the Dynacord 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. Refer to the *Ethernet switch* chapter in the PROMATRIX 9000 Installation manual for more information.
- From PROMATRIX 9000 software version 1.50 onwards, the PRA-ES8P2S switches and the CISCO IE-5000 series switches report their power fault and network connection status directly to the PROMATRIX 9000 system controller through SNMP. The switches can be daisy-chained without an OMNEO device between them for connection supervision. The PRA-ES8P2S is preconfigured for this purpose from custom firmware version 1.01.05 onwards.
- 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 PROMATRIX 9000 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 PROMATRIX 9000 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 (PROMATRIX 9000 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 www.dynacord.com in the **Downloads** section of the PROMATRIX 9000 products.

Whenever you think you have identified a vulnerability or any other security issue related to a Bosch product or service, contact the Bosch Product Security Incident Response Team (PSIRT): https://psirt.bosch.com.



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

202404241631