FL mGuard 1000 series FAQ

1) Will the new 1000 series platform replace the existing mGuard platform?

No. Existing customers who are satisfied with the functionality of the RS2000 and RS4000 series can continue to purchase these products that fulfill the existing application. The FL mGuard 1000 series is geared toward companies that do not have designated security experts, but are looking for secure networks with easy NAT and fundamental security. The main differences are:

- The FL mGuard 2000/2005 devices are for companies that want to implement low-cost, secure, and simple remote maintenance.
- The FL mGuard 4000/4004 devices are for companies that have their own security experts in the company. For example, the application has a high number of implemented devices and requires central management for applications where the security requirements are higher, such as Deep Packet Inspection or hosting their own industrial VPN solution.

2) Is the FL mGuard 1102/1105 certified according to IEC 62443?

At the time of development, the team in Germany was not certified to IEC 62443. Therefore, it is not formally allowed to say that the product was developed according to IEC 62443. Many leading IT companies such as Apple, Microsoft, Cisco and CheckPoint are also not certified according to IEC 62443.

3) Will our product be certified according to IEC 62443 later?

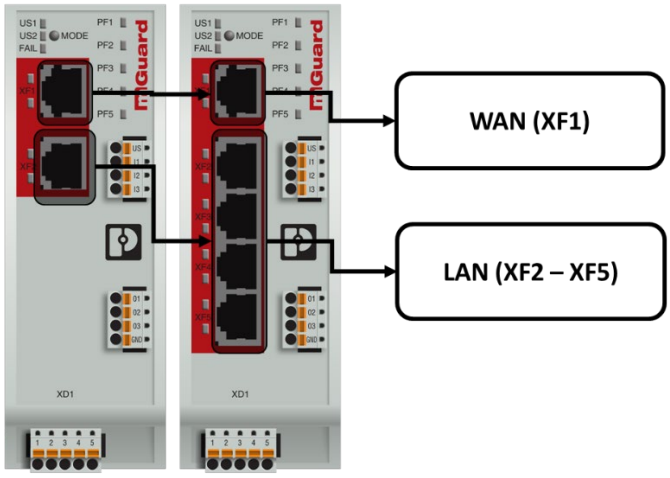
Yes. If a certified product according to IEC 62443 is a mandatory requirement from our target group, we will launch a corresponding certified product on the market.

4) Will the new mGuard 1000 series have UL?

Yes, the 1000 series has safety approval under standard UL 61010. This is a more recent standard (in effect since April 1, 2016) than the familiar UL 508.

5) How do you identify the Machine (LAN) and Plant (WAN) ports in the 1000 series mGuard?

The device's WAN port is physically labeled as XF1, and the LAN ports are XF2 through XF5 depending on your device. See image below for reference:



6) **Are the FL mGuard 1105 integrated ports managed?**

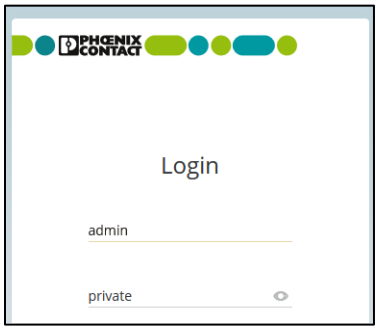
No, the FL mGuard 1105 comes with a 4-port unmanaged switch.

7) **How do I login to the 1000 series mGuard out of the box?**

The easiest way to login to the web-based management page of the mGuard is to connect to one of the LAN ports (XF2 – XF5), open a web browser, and use the out-of-the-box IP address https://192.168.1.1.

8) **What is the out-of-the-box login information?**

Access the mGuard web-based management page with the following information:



9) **Why does the device no longer have SSH for configuration management?**

It is a security entry-level product. A beginner typically does not use SSH. If, however, a machine configures the devices automatically in the future, a RESTful API interface is provided.

10) **Can I protect 5 different networks with only one FL mGuard 1105?**

No, the FL mGuard 1105 firmware can connect, protect, and filter data packets between two network zones only.

11) **Why is the SD card slot no longer in the front?**

The SD Card for the mGuard 1000 series was placed on the back of the hardware following physical security recommendations and feedback from customers to make it “harder to access”. Additionally, our other networking lines have successfully adopted this placement.

12) **Will the FL mGuard 1102/1105 still get VPN functionality?**

Yes, the VPN function is planned for Spring of 2021. The new approach is that the configuration of a VPN connection is to be considerably simplified for a non-expert. Details of the new VPN approach will be released by the product specialist as soon as it is available.

13) **If the FL mGuard 1102/1105 has VPN, will it then connect to the PROFICLOUD / mGuard Secure Cloud services?**

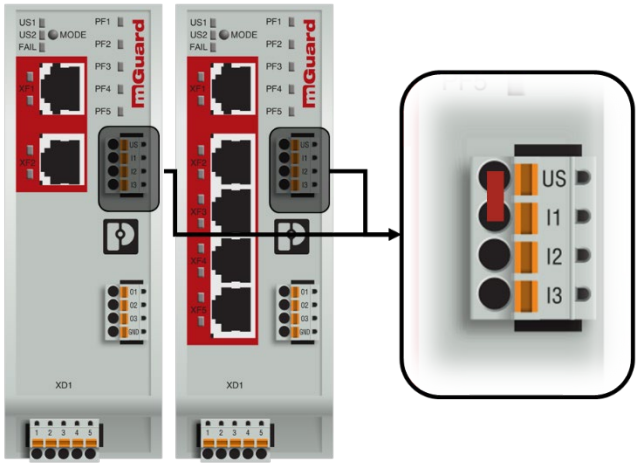
There is no current timetable for the new 1000 series mGuard to be supported in the available Phoenix Contact cloud services.

14) **Are the 1000 series mGuard supported in the mGuard Device Manager (MDM) software?**

The new 1000 series mGuard will be compatible in the next release of the MDM software. The new MDM release is expected in Winter 2020.

15) How do you enable the Easy Protect Mode?

The 1000 series mGuard will be booted in Easy Protect Mode if the jumper showed in the image is wired before powering the mGuard. The connector is physically labeled XG1.



16) Is the Easy Protect Mode on the new 1000 series mGuard the same as a data diode?

At first glance, the function of the data diode and the Easy Protect Mode are very similar. In detail, however, they are very different and serve completely different application scenarios.

Easy Protect Mode: In Easy Protect Mode, an mGuard 1000 is not as restrictive as a data diode. Although requests from Zone B to Zone A are blocked, if responses from Zone B are requested from Zone A, they are forwarded. This is the difference. For many industrial applications, however, this security approach is enough and more practice-oriented than the use of expensive data diodes.

Data diode: The data diode channels data streams in only one direction, e.g., from Zone A to B but not from Zone B to A. It becomes complicated when applications or protocols from Zone A require an answer or an acknowledgement of receipt from Zone B. Despite the simple basic idea, data diodes are therefore very complex and expensive products that are used in very sensitive applications with extremely high security requirements. For example, in public authorities or power plants.

17) What measures did Phoenix Contact take to develop secure firmware for the FL mGuard 1000 series?

The mGuard 1000 series uses a hardened Linux system based on Secure Embedded Operating System (SEOS). Some measures are:

- No unused software packages on the system which follows the principle of minimal required software
- Hardened bootloader
- Kernel and service components are configured accordingly and following security aspects
- The storage of the configuration and all user data is encrypted
- The firmware update and files are signed for proper integrity and authenticity validation to the firmware

18) What measures did Phoenix Contact take to harden the network interfaces in the FL mGuard 1000 series?

- HTTPS access to device only via secure integrated reverse proxy
- Anti-spoofing for own and forwarded network traffic

- Support for only modern encryption algorithms (according to 'moz://a recommended configurations')
- Anti DoS measures for the mGuard and devices to be protected
- Measures against brute force and password timing attacks
- Constant monitoring of all components used for security vulnerabilities by our Product Security Incident Response Team (PSIRT)

19) Is the mGuard 1000 series covered under the LLW requirements?

Yes. To attain the LLW for the new 1000 series or any other mGuard devices, you will need to purchase additional products in accordance with Phoenix Contact USA's recommendations for power supply and surge suppression protection. For more information, visit www.phoenixcontact.com/llw.

For more information, visit www.phoenixcontact.com/mguard1000.