

Cyber Security at Solar-Log™

Whitepaper

More and more digital and networked solutions are being used in our infrastructure, increasing the risk of disruptions and undesirable external influences.

As we are part of this sensitive infrastructure with our products, the topic of cyber security is a top priority for us. We are actively working to always offer the highest standard, but we are also dependent on the cooperation of our customers and partners.

There are three points that deserve special attention and we would like to explain them to you here:

Current firmware

One component in the area of cyber security is to install the latest firmware on our Solar-Log™ devices. In addition to new implementations, one focus of our firmware updates is the topic of security and stability.

Only with the latest firmware are all the latest security updates guaranteed and the device is protected accordingly.

For this purpose, we have always provided the latest firmware for you on our [Solar-Log™ Firmware Download](#) homepage. The new version of the Solar-Log™ Base firmware 6.3.0_172 is available there and on our firmware update server. Details on compatibility and an overview of the improvements can be found in the [release notes for the firmware](#).

ISO/IEC 27001 Certificate

Actually every aspect of our daily lives is increasingly affected by digitalisation and can become a worthwhile goal in this respect. Especially the ever-increasing expansion of decentralised energy generation systems can only succeed through the use of digital solutions. This also requires sophisticated protection mechanisms and a regular check of the mechanisms used for their effectiveness. Solar-Log™ is committed to supporting its partners in the market in tackling this ongoing task.

We are aware of our responsibility as part of the energy infrastructure, especially due to the strong growth in our plant portfolio to over 19.5 GWp of installed plant capacity today. In order to take this into account externally, we have subjected our processes and procedures with regard to IT security issues to a review and successfully completed certification in accordance with ISO/IEC 27001.

Our partners can be sure that their infrastructure is secure and can also prove to other inspection bodies that their partners, who are used in the infrastructure, take the topic of IT security seriously and regularly question themselves anew.

We are happy to provide you with the [ISO/IEC 27001 certificate here](#).

Password protection

The requirements for the protection of personal data are very high. Security mechanisms supposedly limit the user's convenience, but this is usually only superficial. The damage caused by a data leak is in most cases immensely greater and requires elaborate measures to contain it.

Devices used in network infrastructures must provide a variety of security mechanisms. The configuration of these devices should always be done from a security point of view. Two areas can be defined here.

First, existing password functions on devices must be set for access protection. Solar-Log™ offers this option for its devices and explains how to use this function on the device and in the documentation accompanying the product.

For the greatest possible protection against unauthorised access to the device, the password should be set during the initial installation and fulfil the requirements for passwords that are common today:

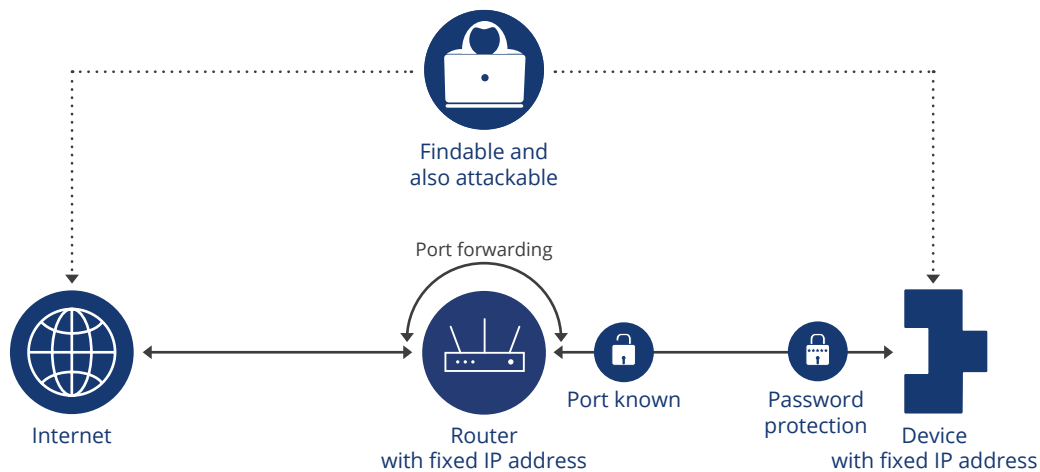
- No single words or word phrases
- At least 9 characters
- Combination of upper case letters / lower case letters / digits and special characters
- The password should not be openly attached to the unit and should only be known to authorised persons.
- Use a separate password for each device.



Internet providers randomly assign the IP addresses of the routers in your network, which are changed daily. These IP addresses can be compared to house numbers or house addresses. If the location of a house is known, unauthorised access is only prevented by locked doors. In the network, the router takes over the security function of the door. However, this door can be open through port releases. If one now knows the

IP address and the open port, the device assigned to the port can be accessed without problems. Some services require such access to the network, but one should pay attention to a minimum number of open ports (doors) and secure the services and devices behind them with additional passwords or other mechanisms.

If the IP address of the router is set permanently, a port is opened and a fixed IP address is defined for the device in the network, which can then be reached via this port, the device can be found and attacked via the Internet. Thus, all system data or personal data provided by the device are potentially available to an attacker or security-relevant settings, e.g. network settings for active and reactive power control, can be changed, which can possibly lead to devastating effects on the infrastructure.



Therefore, as a user, you should take the two points explained very seriously and pay attention to the necessary configuration.

Solar-Log™ devices have extensive mechanisms to secure the device in the network against unauthorised access. As we always focus on IT security and data protection, we are constantly developing our security mechanisms. For the intended operation of the Solar-Log™ with connected portal, no network access from the Internet to the local network is necessary. This ensures that the Solar-Log™ devices are not visible on the internet when used as intended.

If it is necessary to access the Solar-Log™ via the Internet, we strongly recommend that this access is set up by an IT specialist. This specialist is able to completely secure access from unauthorised access, for example by using VPN mechanisms.