Hardware Security

As an access control company, the security of our hardware and IoT products is our number one priority. We are aligned with international standards such as ETSI en 303 645 requirements for IoT. The implementation of secure hardware is an essential part of our products, as we believe that for software to be secure, the underlying hardware must have built in security.

We ensure that our devices do not come with preset passwords that could be easily guessed or exploited by attackers. Instead, we implement secure password mechanisms that require users to create strong, unique passwords to access the device.

In addition, we make sure our products are securely updateable, in order to let the customer apply our regularly released updates and patches to fix any security vulnerabilities and ensure that our products are secure.

Another essential security feature is the fact that we ensure that sensitive security parameters are securely stored, and that our devices communicate securely to protect personal data from unauthorised access. For this goal, we use strong cryptographic algorithms, and we protect data stored and transmitted from unauthorised access and modification via secure means including encryption or secure elements.

We also minimise exposed attack surfaces, by disabling unnecessary interfaces, implementing secure coding standards, and performing regular reviews and pentests to our devices. This includes having strong physical security controls to prevent unauthorised access or tampering, and having all security features enabled by default. Lastly, resiliency is built into our solutions taking into account the possibility of outages of data network and power.

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, Salto assumes no responsibility for any errors or typos that the downloadable version may contain.

Part of the content of this document may have been generated or assisted by artificial intelligence tools. This document may also include automatic or manual translations provided exclusively for informational purposes, which may contain errors or inaccuracies. Salto does not guarantee the accuracy, quality, or reliability of such content or translations, including those generated by AI.

The User is responsible for verifying the information contained in this document and, in case of doubt, must refer to the original English version, which shall prevail in the event of any discrepancy. Other language versions are provided for informational purposes only.

Although Salto makes reasonable efforts to review the content of its downloadable documents, they may contain errors or omissions. Salto assumes no liability arising from the User's use, interpretation, or decisions made based on the information contained in this document, which is used at the User's sole responsibility.

For more detailed information on the use of artificial intelligence, translations, and applicable limitations of liability, please refer to the "Terms of Use of our Website".

As Salto reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.

Copyright ©2026 SALTO Systems S.L. All rights reserved