INFO PAPER

INTUS HARDWARE CHECK

Analysis of the existing INTUS hardware installation

- Analysis of existing INTUS hardware
- Detailed results report
- Recommendations for action
- Support for professional life cycle management

INTUS hardware for time recording and access control is renowned for its reliability. In many cases, INTUS hardware has been installed by customers for more than a decade.

As technology and Security standards are constantly evolving, it is necessary to check from time to time whether the devices used still meet current requirements and support new functions, for example. PCS is committed to ensuring that its customers' security and access control systems are state of the art and function optimally.

This is why PCS offers the INTUS Hardware Check. With this service, it is possible to obtain in-depth transparency of all devices in the running system. How up-to-date is the INTUS hardware? Where is there a need for action? Are current security standards being adhered to? Can the INTUS hardware currently in use be connected to cloud systems?

PCS recommends regularly updating the INTUS hardware used with the latest firmware updates for secure and future-oriented operation. Particular attention should also be paid to the security settings of the INTUS hardware.

Time for security.

pcs

Why is the INTUS Hardware Check useful?

- Overview of the hardware installed in the company
- Checking security-relevant settings, such as z. e.g. encryption of data communication
- Proposals for a future-oriented alignment of the hardware used
- Review of the RFID process used
- Determination of medium-term maintenance and investment requirements and thus forward-looking budget planning for the continuation of the current system

Scope of the INTUS Hardware Check

- Analysis of the existing INTUS Online hardware installation for
  - Hardware used (terminals, controllers, RFID reader)
  - Useful life of the hardware used
  - Up-to-date firmware
  - Security settings
  - Support for new functions
  - RFID technology
  - Battery status
- Results report on the INTUS hardware used with recommendations for the long-term operation of the INTUS system

Note: The INTUS Hardware Check does not include the Checking offline access control, palm vein, UHF and USB readers. This usually requires on-site visits or other services such as RFID migration. As part of the INTUS hardware check, no configuration changes or adjustments are made to either the hardware or the software.

Process description:

- Retrieval of all status pages of the INTUS hardware used
- Analysis of the transmitted data by experienced PCS consultants
- Detailed list of the INTUS hardware used in an overview Excel file
- Detailed results report in PDF format with specific recommendations that can be implemented

Prerequisites:

- Provision of all status pages of the INTUS terminals via remote access to the customer system or independently by the customer using the status page tool provided by PCS.
- If no DEXICON or INTUS COM installation is available: Provision of the IP address list of all INTUS terminals

Investment security and risk management

The INTUS Hardware Check supports professional life cycle management. Analyzing the installed hardware base is the prerequisite for long-term and secure operation of the systems for time recording and access control. It is not always necessary to completely replace the devices. With needs-based maintenance and the use of the latest firmware and RFID technology, the operating time can be significantly extended and data security increased. The INTUS Hardware Check therefore makes a significant contribution to investment security and risk management in the company.

Why is system up-to-dateness important?

PCS recommends the use of up-to-date INTUS hardware and regular firmware updates for Security and future-oriented operation. Switching to a current generation of INTUS terminals with the latest INTUS RemoteConf configuration software offers many long-term advantages:

- Improved security functions, such as AES encryption for secure data transmission
- Investment protection through long-term repair and maintenance capability, support and preparation for the use of further developments
- Faster response times for booking and writing of the identification media
- New functions such as the combination of online and offline access control, e.g. with the INTUS Flex Mechatronics locking systems based on OSS
- Use of the new Lx6 reader generation, for example for parallel use of MIFARE® and LEGIC® RFID technology
- Use of Bluetooth data transmission on the smartphone with the ID.mobile app
- Use of modern identification media
- The latest INTUS hardware generation offers the prerequisites for a cloud connection. This enables more flexible and efficient administration of time and access systems

PCS Systemtechnik GmbH · Pfälzer-Wald-Str. 36 · 81539 Munich · Tel. +49 89 68004 – 0
Ruhrallee 311 · 45136 Essen · Tel. +49 201 89416 – 0
intus@pcs.com · www.pcs.com