



MANUAL

INTUS RemoteConf **Configuration and Operation**

G5000-001.16

INTUS RemoteConf

Configuration and Operation

Stand 05/2026

Bestell-Nr. G5000-001.16

PCS Systemtechnik GmbHPfälzer-Wald-Str. 36
81539 München

Tel. +49 89 68004 - 0

<https://www.pcs.com>**PCS Technischer Support**

Telefon: +49 89 68004 - 666

Fax: +49 89 68004 - 562

E-Mail: support@pcs.com

Copying and distribution of this manual, in whole or in parts, is only allowed with prior express authority of **PCS Systemtechnik GmbH**. The information in this manual is subject to changes so that we can maintain the state of the art at all times.

PCS, INTUS, and DEXICON are registered trademarks of PCS Systemtechnik GmbH.

All other product and service names are trademarks of the respective company and organization.

Copyright 2026 by **PCS Systemtechnik GmbH**.

Contents

Safety notes	7
Indications de sécurité importantes	8
1 About this manual	9
1.1 Symbols used in the manual	9
1.2 PCS service tools and manuals	10
1.3 Additional manuals	10
2 Characteristics	11
2.1 Necessary information on the device	11
2.2 INTUS 5200 & INTUS 5205	12
2.3 INTUS 5320-24V/-NT/PoE	13
2.4 INTUS 5500 / 5540 & INTUS 5600	14
2.5 INTUS ACM80e Rack / INTUS ACM80e Wall	15
2.6 INTUS ACM40e	16
3 Security concept	17
3.1 CyberSecurity Measures for the Secure Operation of INTUS Hardware	18
3.2 Reset of Login Credentials	20
3.2.1 Procedure	20
3.2.2 DIP Switch	21
4 Introduction to INTUS RemoteConf	22
4.1 Installing INTUS RemoteConf on a PC	22
4.1.1 Installation on PCs with Microsoft Windows operating system	22
4.1.2 Installation of INTUS RemoteConf with other operating systems	23
4.2 INTUS RemoteConf buttons	24
4.3 Add the terminal to the terminal list	25
4.4 Rearranging the terminal list	26
4.5 PC Firewall	26
4.6 Info button	26
4.7 Activate licence	27
4.8 Device Firmware Update	27
4.9 Simultaneous execution of actions on several terminals	30
4.10 Changed commissioning steps for new devices	30
4.11 Configure Login	31
4.12 Configure data port	31

5	Introduction to the terminal configuration	32
6	Login – log into the terminal	33
6.1	Authorization level.....	33
6.2	Procedure	33
7	Configuration.....	34
7.1	Overview	34
7.2	Save configuration to a file.....	34
7.3	Finalizing the configuration	35
8	The network connection (IP)	36
8.1	WiFi.....	38
8.2	IEEE 802.1X/WPA2-Enterprise.....	39
8.3	Mobile communication	41
9	Data port (Channel A)	43
9.1	TCP protocol settings.....	43
9.2	HTTPS client protocol settings.....	45
9.3	Security settings.....	46
10	The Firewall	47
11	Configuring the LBus	49
11.1	Maximum number of readers	50
11.2	Wiring the INTUS 5200 / 5320 / 5500 / 5540 / 5600	51
11.3	Wiring options of the INTUS ACM40e.....	52
11.4	Wiring options of the INTUS ACM40e with Wiegand module.....	52
11.5	Wiring options of the INTUS ACM80e.....	53
11.6	Point-to-Point wiring the INTUS ACM80e	54
11.7	Multi-Point wiring the INTUS ACM80e	54
11.8	Configuring a reader	55
11.9	Reader type / Easy addressing	56
11.10	Mode of operation	57
11.11	Example ACM40e Wiegand module: 2 LBus readers, 4 Wiegand readers	58
11.12	Example - ACM40e with 16Flex-Licence - 16 wireless connected INTUS Flex devices.....	61
11.13	Example - ACM40e with 16Flex-Licence - Mixed operation with star-shaped connected INTUS readers.....	64
11.14	Example ACM40e with 16Flex-Licence - Mixed operation with bus-wired INTUS readers.....	68

11.15	Example ACM80e with 8 INTUS 700/6xx/350H readers and 8 INTUS Flex devices.....	72
11.16	Example - one INTUS 5500/5540/5600 with LBus1 & LBus2	75
11.17	LBus AES encryption	76
11.17.1	Prerequisites	76
11.17.2	Activating AES encryption.....	76
11.17.3	Configuring the AES key	77
11.17.4	Configuring the customer key	77
11.17.5	Option AES encryption with customer key only.....	78
11.17.6	Changing the customer key	78
11.17.7	Removing a customer key.....	79
11.17.8	AES encryption and OSDP	79
11.18	LBus encryption (PCS proprietary)	80
12	The internal reader.....	81
13	TCL parameters	82
13.1	Settings	82
13.2	Extended user interface	83
13.3	INTUS Sound.....	83
14	Hardware	84
14.1	Display	84
14.2	Magic-Eye (INTUS 5320 only)	84
14.3	Buzzer.....	84
15	Login - Maintenance Group and Password Change	85
15.1	Maintenance group	86
15.2	Changing the password for authorization level	86
16	Time	87
16.1	NTP Client.....	87
16.2	UTC offset – Deviation to UTC time	87
16.3	Daylight saving time switch-over.....	88
17	LBus actions	89
17.1	Overview	89
17.2	Action "Reader firmware update"	90
17.3	Action "Unlock/lock parameter card for reader"	90
17.4	Action "Transfer LBus key to reader"	90
17.5	Action "Reader parameter download"	91

17.6	Action "Custom reader settings configuration"	92
17.6.1	General actions	92
17.6.2	Setting mounting site-specific parameters	93
17.7	Compose sequence of actions	93
18	Service actions for INTUS Flex Air	95
19	Reset	101
20	Upload Logo	103
21	Serial interfaces	104
21.1	Basic settings TTY/BSC	104
21.2	TTY protocol	104
21.3	BSC protocol	105
22	Requirements for firewall settings in network	107
23	Error diagnostics	108
23.1	Reader action test	108
23.1.1	INTUS 3x and 5x	108
23.1.2	INTUS 5540	108
23.1.3	INTUS ACM80e	108
23.1.4	INTUS ACM40e	109
23.2	Automatic self-test	109
23.3	Error diagnostics by log file	111
23.4	Unsuccessful error diagnostics	111
24	Tables of configurable parameters	112
25	License regulations for free software	115
26	List of figures	116
27	Index	118



Safety notes

- All voltages introduced into the device must conform to the following requirements: LPS (Limited Power Source) and SELV (Safety Extra Low Voltage) according to IEC/EN/UL/CSA 60950-1 or ES1 and PS2 according to IEC/EN/UL/CSA 62368-1.
- Always cut off power supply before opening the terminal.
- Only trained technical personnel are authorized to install the terminal and to open the terminal for maintenance purposes. Unauthorized opening and inappropriate repair may cause considerable hazards for the user.
- The terminal is not equipped with a disconnecting terminal from mains (switch) accessible from the outside.
- If a non-detachable mains connection is used, an easily accessible disconnecting terminal (e. g. an automatic circuit-breaker with a maximum rating of 16 A) must be installed.
- If the attached mains cable is used, the mains connector (power plug) must be used as a disconnecting terminal. The socket outlet must therefore be positioned in an easily accessible location.
- If the integrated power supply unit is out of order, please send the terminal to the PCS Technical Support.
- The data cable shielding is grounded at the terminal. If a peripheral terminal operated on a circuit different from that of the terminal is connected, the shielding of the data cables at the peripheral/remote terminal (or computer) must be insulated from the protective conductor.
- Do not connect or disconnect cables during a thunderstorm.
- In all cases of emergency (damage to mains cable or equipment, liquids or foreign substances leaking in, etc.): De-energize the terminal immediately by pulling the power plug or opening the disconnecting terminal. Contact the PCS Technical Support.
- CAUTION! Danger of explosion, if the battery is incorrectly replaced. Only replace batteries with same or equivalent type recommended by PCS, see Terminal Installation Guide.
- Please dispose of used batteries in an environmentally oriented fashion.
- The I/O board is an electrostatic-sensitive device. Do not handle the board but at an electrostatic-free workstation.
- Only qualified PCS personnel is allowed to modify the hard- or software of the device.



Indications de sécurité importantes

- Toutes les tensions dans l'appareil doivent être conformes à des exigences suivantes: LPS (Limited Power Source) et SELV (Safety Extra Low Voltage) en conformité avec IEC/EN/UL/CSA 60950-1 ou ES1 et PS2 en conformité avec IEC/EN/UL/CSA 62368-1.
- Débranchez l'INTUS appareil de l'alimentation électrique avant de l'ouvrir.
- L'INTUS appareil ne doit être installé que par du personnel spécialisé et formé et n'être ouvert qu'à des fins de maintenance. En cas d'ouverture non autorisée et de réparations inappropriées, l'utilisateur s'expose à des risques importants.
- L'INTUS appareil n'est pas équipé d'un dispositif de séparation d'alimentation électrique (interrupteur) accessible de l'extérieur. Débrancher le câble d'alimentation.
- Connecter l'INTUS appareil à une prise secteur mise à la terre.
- Si le fusible sur le bloc d'alimentation électrique est détruite, celle-ci ne doit pas être changée car elle ne peut être détruite que par un défaut appareil sérieux. Il faut dans ce cas envoyer l'appareil en réparation.
- Comme la protection du câble de données sur l'INTUS appareil est reliée à la terre, lors du branchement d'un périphérique qui est alimenté par un autre circuit électrique que celui de l'INTUS appareil, la protection du câble de données sur l'appareil final/le périphérique (ou ordinateur) doit être séparée de la terre.
- Pendant un orage, les câbles de données ne doivent être ni débranchés ni branchés.
- En cas d'urgence (par ex., câble de données ou boîtier endommagés, intrusion de liquides ou de corps étrangers), retirez immédiatement la prise. Contactez PCS Technical Support.
- ATTENTION! Risque d'explosion en cas de remplacement inapproprié de la batterie.
- Remplacement de la batterie uniquement par le même type ou par un type conseillé par PCS.
- Les batteries utilisés doivent être éliminés en respectant l'environnement.
- Les dispositifs électroniques contiennent des pièces ESD à risque. Prenez des mesures adéquates pour la protection des pièces.

Les interventions au niveau du matériel et du logiciel de l'INTUS appareil qui ne sont pas décrites dans ce manuel ne doivent être exécutées que par PCS Service Center.

1 About this manual

This manual covers commissioning, definition and modification of terminal configuration, monitoring of operation, as well as error diagnostics. This manual refers to the following device types:

- INTUS 5205-SNT / INTUS 5205-PoE
- INTUS 5200-24V / INTUS 5200-PoE
- INTUS 5320-24V / INTUS 5320-NT / INTUS 5320-PoE
- INTUS 5500-24V / INTUS 5500-NT / INTUS 5500-PoE
- INTUS 5540-24V / INTUS 5540-NT / INTUS 5540-PoE
- INTUS 5600-24V / INTUS 5600-NT / INTUS 5600-PoE
- INTUS ACM80e Rack / INTUS ACM80e Wall
- INTUS ACM40e
- INTUS 3150/3155

Important NOTE

This manual is valid for the software version V1.16.00.

The following download link to the PCS site

<https://download.pcs.com/irc> offers download of the current software version of INTUS RemoteConf, please see chapter 4.6.

Symbols used in the manual



This warning symbol indicates hazards to your health and life as well as hazards that may cause damage to the terminal or system. You should always read and follow the text next to the symbol.



This symbol points to information that may facilitate your handling of the product and should be noted.

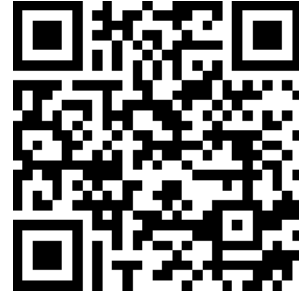


This symbol points to operational instructions.

1.2 PCS service tools and manuals

The following web page offers free download of PCS service tools for installation and maintenance, as well as the respective manuals:

<https://download.pcs.com/service-tools/>



1.3 Additional manuals

- For each terminal and INTUS ACM, there is a manual for installation & maintenance of the device. It provides the information the installer or electrician needs for mounting and installing the devices.
- INTUS Local Setup (order No. G5000-003) – for INTUS 3150/5320/5500/ACM40e/80e and setup via touchscreen for INTUS 5200/5205/5600.
- INTUS TCL Programmer's Manual (order No. G3000-004). This manual describes the TCL programming language. TCL can be used for customized programming of the device.

2 Characteristics

2.1 Necessary information on the device

To configure a device, the following information is absolutely required:

- Configuration of the network
- Configuration of the readers – if the connected readers are not configured by higher-level software.
- Other TCL parameters – if the TCL parameters are not set by higher-level software.

Setting operating parameters

For putting the device into operation, operating parameters must be set in a way that connection to the host computer and to the remote readers is established.

This manual describes how to set the parameters using a PC and the software „INTUS RemoteConf“.

Possibly, your software partner will handle this task.

Setting of operation parameters depends on the software in use.

2.2 INTUS 5200 & INTUS 5205

Interfaces	INTUS 5200	INTUS 5205
Ethernet 10/100BASE-T / WiFi	◆ / ◇	◆
Integrated RFID reader	◆	◆
Barcode scanner	◇	----
Interface module		
2 x DI, digital input (opto-decoupled) 1 x door control DO, switching relay 1x external reader (RS485 interface)	◇	----
Control elements and display		
3,5" projective capacitive touch screen	◆	◆
3,5" TFT colour display, resolution 320 x 240	◆	◆
Status display blue	◆	◆
Membrane keypad with numeric block & 2 function keys	◇	----
User interface	predefined	predefined
Action with INTUS RemoteConf		
Load private customer logo	◆	◆
Load screen masks*	◇	◇
Load audio file	◇	----
Load keyboard file	----	----
Performance features		
Memory	◆ 1 MB ◇ 2 MB	◆ 0.5 MB
Degree of protection IP30 / up to IP64 with sealing kit	◆ / ◇	◆ / --
Buzzer / speaker / heating	◆ / ◇ / ◇	◆ / -- / --
Tamper contact, lock	◆	◆
Power Supply INTUS 5205 / 5200		
INTUS 5200-24 V		
12-24 V + 20 % - 15 % DC; external power supply unit, SELV, L.P.S, ES1, PS2		
INTUS 5205-SNT		
Factory connected cable with plug-in power supply (230VAC)		
INTUS 5200-PoE / 5205-PoE: Power over Ethernet, IEEE 802.3af class2		

◆ Standard; ◇ Option

* loading of screen masks is possible optionally, if mask access was purchased

2.3 INTUS 5320-24V/-NT/PoE

Interfaces

Ethernet 10/100BaseT; RJ45 socket / WiFi	◆ / ◇
Integrated reader	◆
RFID reader Mifare or Legic or Hitag	
DI / DO interfaces	
2 x DI, digital input opto decoupled	◆
2 x DO, digital output (relay)	
Slot for one LBus module with 4 readers via LBus1	◇
Control elements and display	
240 x 64 pixels LC display, black/white with LED backlight	◆
Membrane keyboard, 5 function keys + 2 scroll keys + numeric keypad (10)	◆ / ◇
MagicEye (blue, red, green), 2 LEDs (red, green)	◆
Performance features and mechanics	
Memory 2 MB / 6 MB	◆ / ◇
Master records / bookings with 2 MB	about 13 000 / 26 000
Master records / bookings with 6 MB	about 40 000 / 80 000
Degree of protection IP30, with sealing option up to IP65	◆ / ◇
Buzzer / heating	◆ / ◇
Tamper contact and lock	◆

◆ Standard; ◇ Option

	INTUS 5320-24V	INTUS 5320-NT	INTUS 5320-PoE
Power supply	External power supply unit 24 V; SELV, L.P.S, ES1, PS2	Integrated power supply unit 115 ... 230 V AC	Power over Ethernet, IEEE 802.3af class3

2.4 INTUS 5500 / 5540 & INTUS 5600

Interfaces	5500	5540	5600
Ethernet 10/100BASE-T / WiFi	◆ / ◇	◆ / ◇	◆ / ◇
Integrated RFID reader Mifare, Legic, Hitag	◇	◇	◇
Interface module			
2 x DI, digital input (opto decoupled)	◇	◇	◇
2 x DO, digital output (relay)			
Two slots each for one LBus module, to connect up to 8 readers via LBus1 or LBus2	◇	◇	◇
USB socket for PCS Barcode reader	◇	◇	◇
Control elements and display			
5,7" TFT VGA colour display, 640 x 480 pixels	---	---	◆
4,3" TFT colour display, 480 x 272 pixels	---	◆	---
Display 24 0x 64 pixels, black/white	◆	---	---
Projective capacitive touch screen, with customizable keyboard layout	---	---	◆
Membrane keyboard (numeric block) with 5 programmable function keys	◆	◆	---
MagicEye blue/red/green, 2 LEDs red/green	◆	◆	◆
Action with INTUS RemoteConf			
Load screen masks and customer logo	----	----	◆
Load audio file	◆	◆	◆
Load keyboard file	----	----	◆
Performance features and mechanics	5500 / 5540 & 5600		
Memory 2 MB / 6 MB	◆ / ◇		
Master sets / bookings with 2 MB	ca. 13 000 / 26 000		
Master sets / bookings with 6 MB	ca. 40 000 / 80 000		
IP30 / up to IP 64 with sealing kit	◆ / ◇		
Buzzer / speaker / heating	◆ / ◇ / ◇		
Tamper contact, lock and locking	◆		
Power Supply INTUS 5500 / 5540 & 5600			
INTUS 5500-24V / INTUS 5540-24V / INTUS 5600-24V			
24V ± 20% DC, external power supply unit, SELV, L.P.S, ES1, PS2			
INTUS 5500-NT / INTUS 5540-NT / INTUS 5600-NT			
Integrated power supply unit 115...230 V AC, factory attached power cable			
INTUS 5500-PoE / INTUS 5540-PoE / 5600-PoE			
Power over Ethernet, IEEE 802.3af class3			

◆ Standard; ◇ Option

2.5 INTUS ACM80e Rack / INTUS ACM80e Wall

Interfaces for door control

4 / 8 / 16 access readers, Point-to-Point or MultiPoint	◆ / ◇ / ◇
LBus2 module (option) to connect up to 8 access readers, MultiPoint	◇
16 x digital input (DI) opto-decoupled, dedicated to the reader	◆
16 x digital output (DO) changeover relay 5 A, dedicated to the reader	◆

Interfaces for alarm system, emergency call, general tasks

4 x digital input (DI) opto-decoupled	◆
4 x digital output (DO) changeover relay 5 A, DO4 relay is switchable to bistable changeover relay 2 V	◆

Host interface

Ethernet 10/100BASE-T	◆
-----------------------	---

Performance features and mechanics

Memory 2 MB / 6 MB / 10 MB	◆ / ◇ / ◇
Headcount * / bookings with 2 MB: 35.000/32.000	
Headcount * / bookings with 6 MB: 109.000/101.000	
Headcount * / bookings with 10 MB: 190.000**/170.000	
Tamper contact / Buzzer	◆
CPU ARM9 G45 / 400 MHz	◆

Integrated power supply

Access readers voltage supply 12 V DC (default) / 24 V DC selectable; regulated	◆
Door strike (DO) or system, alarm (DO) - voltage supply 12 V DC (default) / 24 V DC selectable; regulated	◆

Power supply

Integrated 230 V AC toroidal transformer, switchable to 115 V AC	◆
--	---

Safety concept

Increased failure protection of the device: If a component fails or is damaged, only this component will be affected. This is achieved by
Point-to-Point connections to the readers, power supply via the device
2x digital inputs/ outputs provided per reader connection

◆ Standard; ◇ Option

* The headcount is given for access control. For time recording it is reduced by about 50%.

**When using TPI for access control, the number of employees is limited to 99999th.

2.6 INTUS ACM40e

Interfaces

Reader	4 access readers max (2 standard + 2 optional), LBus interfaces for Point-to-Point connection
Door control	8 x DI (opto-decoupled), 4 x DO (switching relays) dedicated to the readers are destined for door control only
System application alarms, burglar alarm systems	4 x DI (opto-decoupled) , 2 x DO (switching relays), 1 x bistable DO (flip-flop)
Host interface	Ethernet 10/100 BaseT via RJ45 socket

Integrated voltage supply

Reader	Reader supply voltage 12 V DC (default) / 24 V DC switchable; regulated
Door opener	Door opener (DO) or system, alarm (DO) supply voltage 12 V DC (default) / 24 V DC switchable; regulated
Emergency power supply INTUS ACM40e-Akku	4 h buffer time or 2.500 operations

Performance feature

Memory	2 MB (default) / 6 MB (option) / 10 MB (option)
--------	---

Power supply

INTUS ACM40e-NT	INTUS ACM40e-Akku	INTUS ACM40e-24	INTUS ACM40e-PoE
Integrated 115 – 230 V industrial power supply unit	Integrated 115 - 230 V industrial power supply unit with accumulator buffering	External power supply unit 12 V DC or 24 V DC (SELV, L.P.S., ES1, PS2)	Power supply via Ethernet (Ultra PoE)

3 Security concept

There is a number of methods to secure the configuration of the terminal and its communication with host and readers.

Authorization level: There are three different authorization levels accessible by passwords

Authorization level	Password (default setting)	
1	111111	Password of level 1
2	14789632	Password of level 1 + 2
3	14589632	Password of level 1 + 2 + 3

Firewall

You are able to grant access rights for individual network users or network groups

INTUS RemoteConf → Configuration > Firewall

Maintenance group

Allows you to assign the device to a specific maintenance group. If the maintenance group is not known, access via PCS Tools is not possible.

INTUS RemoteConf → Configuration > Login

Host interface password

Allows you to enable passwords for accessing the TCL interpreter;

INTUS RemoteConf → Configuration > Channel A

Host interface encryption

Allows you to encrypt communication with the TCL interpreter;

INTUS RemoteConf → Configuration > Channel A

Loss of access credentials

The correct and secure storage of access credentials such as passwords and maintenance groups within the system is the responsibility of the customer.

Loss of passwords may result in security risks, impaired system functionality, additional costs, and project delays.

In order to receive technical support, project management, installation, or similar services, the required passwords must be available at the appropriate time.



Make a note of any change in the maintenance group, new passwords and passphrase (encryption text).

Tables for this purpose are provided in Chapter 24.

If you loose access authorization settings or if you have additional questions, please call us.

Please have the serial number of the terminal ready.

PCS Support: +49 89 68004 - 666

E-mail: support@pcs.com

3.1 CyberSecurity Measures for the Secure Operation of INTUS Hardware

This section provides information about cybersecurity measures to ensure the secure operation of current INTUS terminals, access control managers, and readers. It is intended as a concise supplement to the existing documentation. All relevant information from other official sources should also be taken into account. In case of discrepancies, the more recent version takes precedence. All listed measures are strongly recommended by us.

This section serves as an overview of our recommendations. Detailed instructions and implementation steps can be found in the respective manuals.

General Recommendations: (strongly recommended)

- Use the latest INTUS TCL-Firmwareversion („INTUS Firmware Package“)
- Use the latest version of INTUS RemoteConf
- Use the latest version of INTUS COM
- Use the latest RFID technology
- Use the latest hardware (INTUS RemoteConf devices)
- Use the latest reader firmware

Secure Network Operation:

Internal device firewall (strongly recommended)

We recommend using the device firewall to restrict communication for daily operation (with the application or INTUS COM) and maintenance (HTML status page, INTUS RemoteConf), unless other measures (e.g., VLANs) have been implemented.

Disable IP setup comfort function with INTUS RemoteConf

After initial commissioning of the terminal, the IP setup in INTUS RemoteConf for the terminal/ACM should be disabled. Once the terminal is operational, this setup feature is no longer required.

(If an IP address range change is planned, the terminal has a static IPv4

address, and IPv6 is disabled, temporarily reactivating this feature may be advisable.)

- **Disable AutoClone connection with INTUS RemoteConf (strongly recommended if INTUS COM is not in use)**

Recent versions of INTUS RemoteConf allow the AutoClone service connection to be disabled. This is recommended if INTUS COM is not used.

- **Use IEEE 802.1X for wired Ethernet**

IEEE 802.1X allows network access to be protected at the Ethernet switch level. Only devices that successfully authenticate will be granted access. Since time-tracking terminals are often located in semi-public areas, we recommend enabling this feature.

- **WPA2 Enterprise**

For WLAN-connected terminals, best practice in larger networks is to assign unique WLAN credentials to each device. This enables individual device access to be revoked if necessary.

Protection Against Unauthorized Device Access:

Starting August 1, 2025, devices will be delivered with a new firmware version that requires password changes via the appropriate INTUS RemoteConf tool before use. This prevents security risks associated with default passwords after initial setup and enhances the cybersecurity of your system.

Securing Data Exchange with INTUS COM or Other Applications (Secure Host Communication):

- **Data exchange via HTTP/2**

If supported by the application or when using INTUS COM, we recommend prioritizing this interface option.

- **CA certificate updates via HTTP/2**

When using HTTP/2 for data exchange, enabling this option is recommended. It allows the terminal to update the certificate used for server authentication with ease (supported in INTUS COM).

- **Encryption of host interface using TCP protocol (strongly recommended):**

If supported by the middleware, this feature should be enabled. We recommend using the latest encryption version (V2), to be configured in both INTUS COM and INTUS RemoteConf.



Warning: If login and encryption, as well as the device firewall, are not used during active/passive TCP connection setup, other appropriate protective measures are urgently required (e.g., VLANs in combination with IEEE 802.1X).

Securing data exchange between INTUS readers and INTUS ACM/INTUS terminals:

Encrypt LBus

- To secure communication with the reader, enabling encryption is strongly recommended, provided the connected reader supports this feature.

3.2 Reset of Login Credentials



Important: The exact location of the DIP switches is device-specific and is described in the respective manuals.

3.2.1 Procedure

If the login credentials (maintenance group and passwords) are lost, they can be reset using a switch inside the device.

The procedure is basically identical for all devices; only the position of the DIP switch differs depending on the model (see section 3.2.2).

Proceed as follows:

- 1 Switch off the device in order to open the device housing.
- 2 Toggle the DIP switch intended for reset (switch number 1) using a suitable narrow tool, i.e. change its position (e.g. from ON to OFF or from OFF to ON).
- 3 Close the housing and switch the device on again.

The following settings are reset to factory defaults:

- Maintenance group
- Passwords for all authorization levels

If required, the complete device configuration can subsequently be reset to factory defaults (see Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Before the device can be fully put back into operation, new passwords must be assigned for all authorization levels (see Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**).



The device detects the position of the DIP switch for the reset and performs the reset only if the switch state has changed compared to the last system reboot. Therefore, the DIP switch must not be returned to its original position for normal operation.

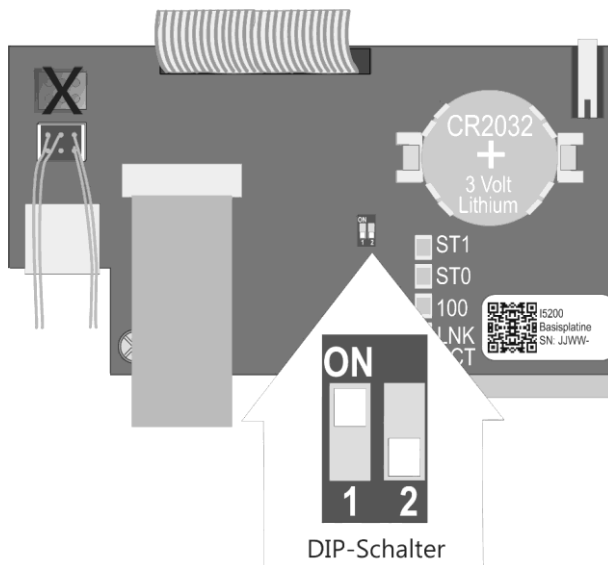
3.2.2 DIP Switch

The reset of the login credentials is triggered via a DIP switch inside the device.

Depending on the device model, the DIP switch is located in different positions. The exact location as well as an illustration of the DIP switch can be found in the device-specific manuals. These manuals also contain instructions for correctly opening and closing the terminal.

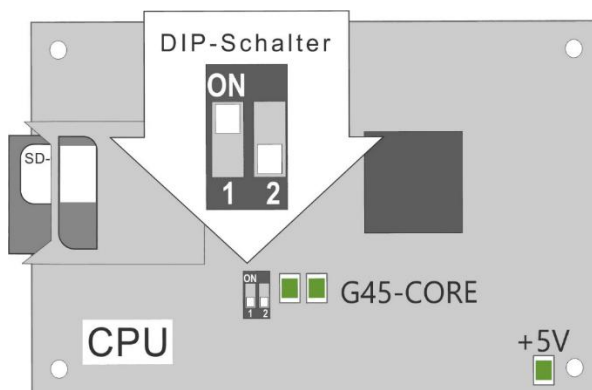
5200s

On all devices of the 5200-series (I5200, I5205), the DIP switch is located at the following position:



All other devices

On all other devices (e.g. I5320, I5500, I5540, I5600, ACM40e, ACM80e Rack, ACM80e Wall), the DIP switch is located at the following position:



The DIP switches may be covered with a protective film. This film must be removed first.

For the reset procedure, please follow the general procedure described in Chapter 3.2.1.

4 Introduction to INTUS RemoteConf



To configure the operating parameters of the terminal via a PC, please use the software „INTUS RemoteConf“.

There are two ways of configuration via PC:

- PC and device are located in the same network segment
- PC and device are connected directly to each other



Figure 4-1: Connection terminal/PC



Before you start INTUS RemoteConf:

Please make sure that the PC is equipped with an IP address. You can check PC settings by prompting “ipconfig”.



WiFi as host interface

Please note the special network settings used if WiFi is set as host interface (chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**).

4.1 Installing INTUS RemoteConf on a PC



To use INTUS RemoteConf, the software Java has to be installed on the PC in any case (see chapter 4.1). Since INTUS RemoteConf V1.04.01, INTUS RemoteConf is offered for download as a package including Windows Installer and optional internal Java runtime environment.

4.1.1 Installation on PCs with Microsoft Windows operating system

For this method, the package "INTUS_RemoteConf-x.xx.xx-WindowsInstaller.zip" is made available on the download page <https://download.pcs.com/irc/>.



Extract the .zip file and start "INTUS RemoteConf-1.04.01 Installer.exe". During installation, you have the option to install the enclosed private free runtime environment on the basis of OpenJDK together with INTUS RemoteConf.

If you do not choose this option, you need to install your own Java runtime environment on the PC (Version 8 or higher), in order to be able to start INTUS RemoteConf.

After installation, INTUS RemoteConf can be started via the Windows Start menu.

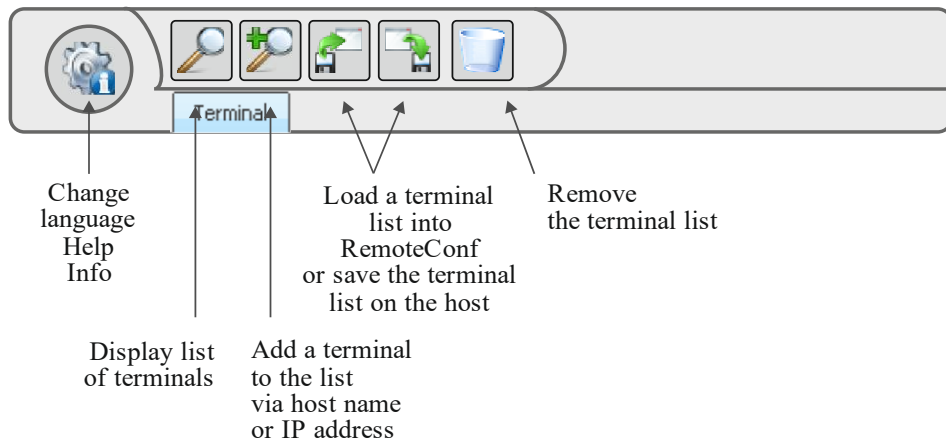
4.1.2 Installation of INTUS RemoteConf with other operating systems

For this method, the package "INTUS_RemoteConf-x.xx.xx-JarOnly.zip" is made available under <https://download.pcs.com/irc/>. This package only contains the Java program "INTUSRemoteConf.jar", without installer or private Java runtime environment.



- You need to install your own Java runtime environment (RJE) on your PC to be able to start INTUS RemoteConf.
- The Java runtime environment should be Version 8 or higher.
- Start INTUS RemoteConf by executing "INTUSRemoteConf.jar".

4.2 INTUS RemoteConf buttons



INTUS RemoteConf provides the following options:

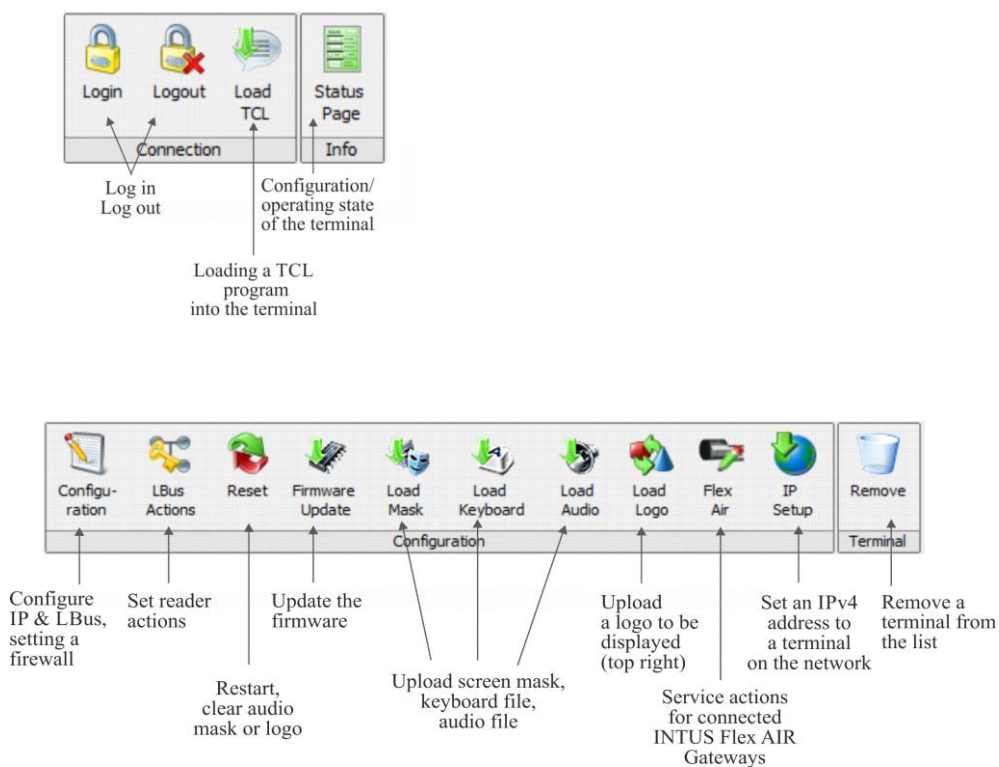


Figure 4-2: INTUS RemoteConf buttons

4.3 Add the terminal to the terminal list

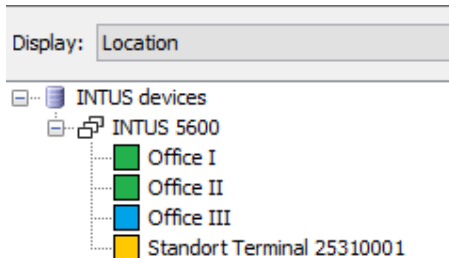


or



Display the terminal in the terminal list by „Search all“ or „Add“ the IP address or host name.

All accessible terminals are displayed



- Terminals highlighted in green are reachable and can be configured.
- Terminals highlighted in blue do not meet the requirements for configuration.
- Terminals highlighted in dark yellow are reachable but require login and data port setup before operation (see Chapter 4.10).



Making the terminals highlighted in blue accessible

A terminal is highlighted in blue if

- IPv6 is not available on PC or terminal. IPv4 is used in this case.
- DHCP is enabled, but a DHCP server does not exist in the sub network
- the IPv4 address of the terminal does not comply with the PC sub network.

In these cases, the button IP Setup is enabled.



The terminal is highlighted in blue, it has to be assigned an address



To display the terminal in the terminal list, please set:

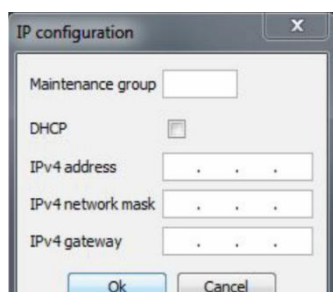


Figure 4-3: IP configuration

Maintenance group, „0“ - default setting.

IP address, select a free IP address from the same subnet of the PC IP address

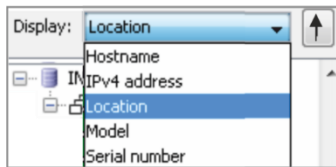
Net mask, as set at the PC

Gateway, set 0.0.0.0, to delete all the entries stored on the terminal



For future use of the terminal without DHCP, your network administrator can provide you with the IP address, the net mask, and the gateway address.

4.4 Rearranging the terminal list



You can rearrange the terminal list.

Figure 4-4: Rearranging the terminal list

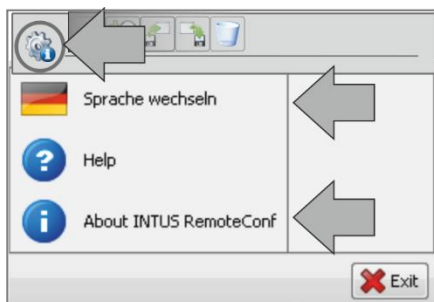
4.5 PC Firewall

In case the PC firewall configuration blocks access of INTUS RemoteConf to the network, proceed as follows:



- 4 Click on the button “allow access”.
- 5 Repeat the search for terminals in the network by clicking on the button “Search all”.

4.6 Info button



English or German

Link to a download page
License terms

Figure 4-5: Info button

4.7 Activate licence

The licence can be loaded via INTUS RemoteConf via Load TCL

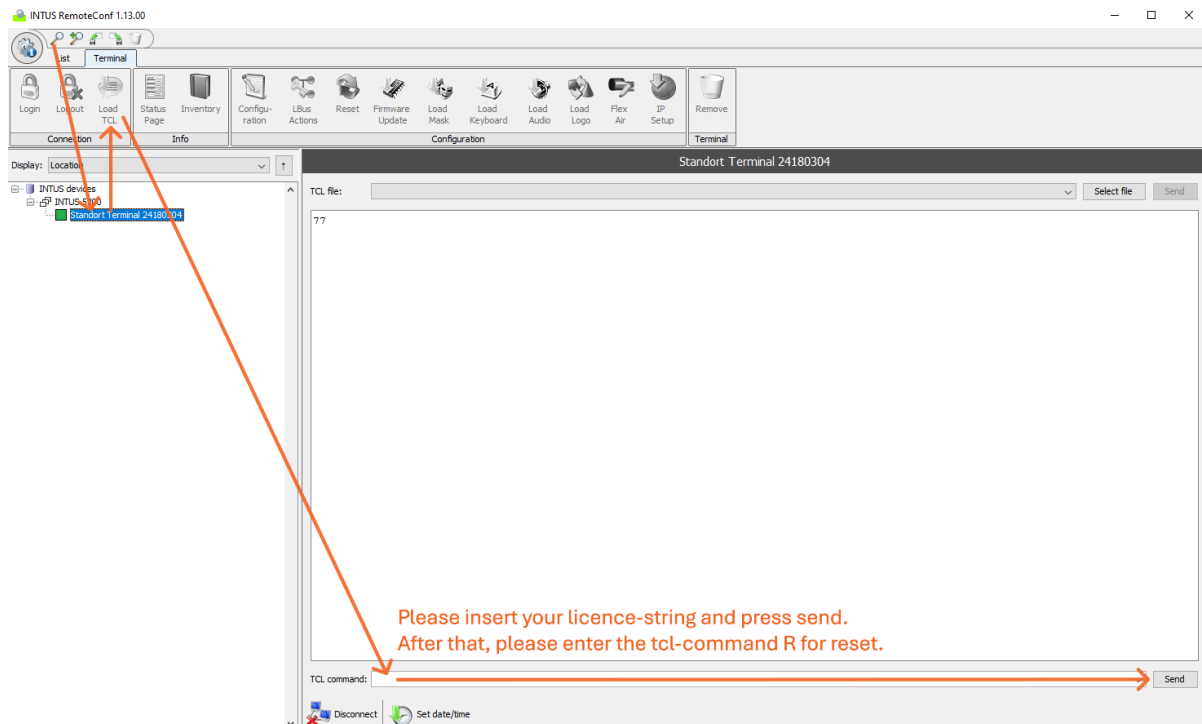


Abbildung 4-1: Activate licence

Then, enter the TCL command R for reset and send it to the terminal.

Alternatively, the string can be sent to the device via INTUS COM through terminal dialog.

4.8 Device Firmware Update

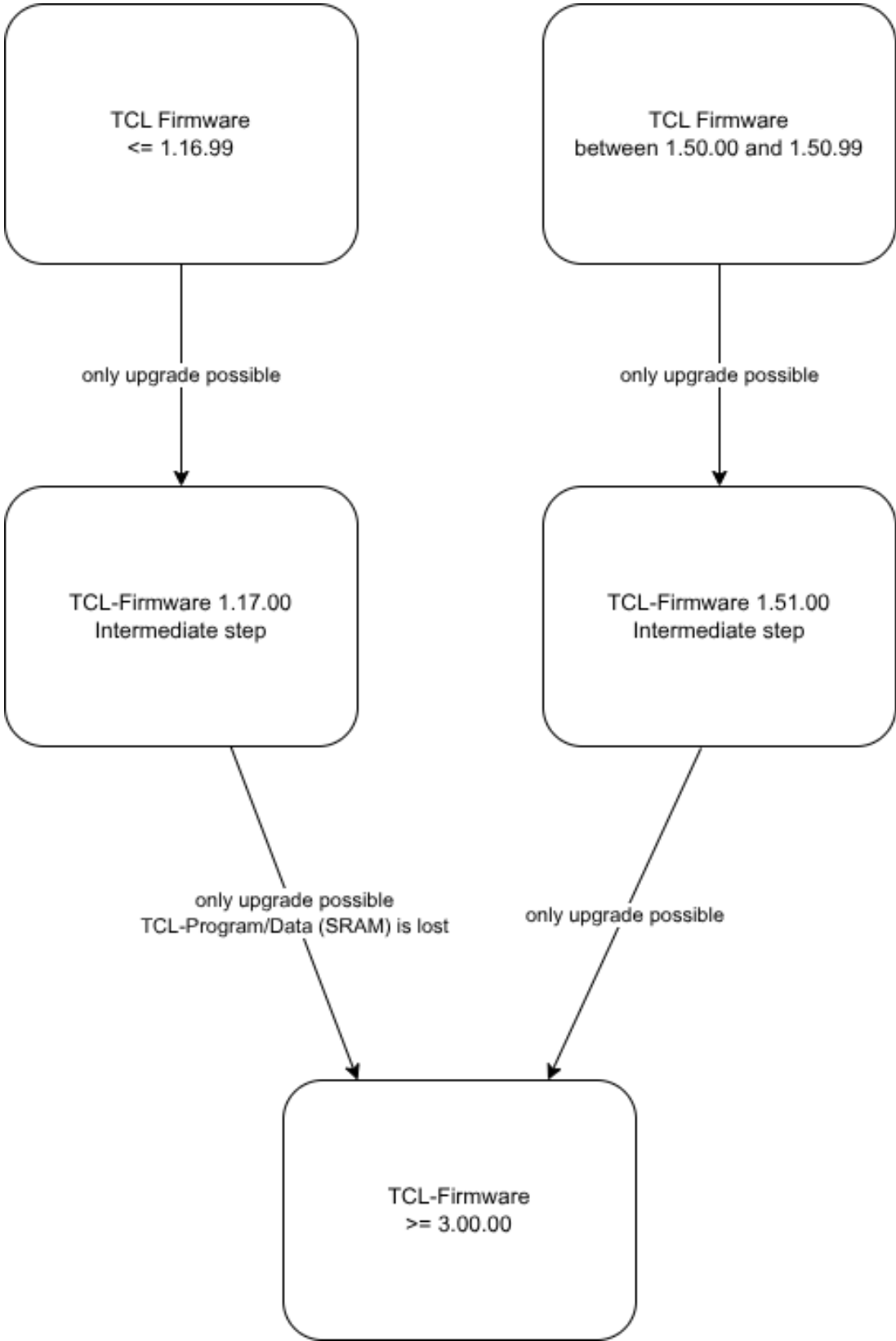
- 1 Log in to the device with authorization level 3.
- 2 Click the "Update firmware" button.
- 3 Select the desired firmware package. Please refer to the following section to check whether intermediate steps are required. Only applies to firmware versions below 3.xx.xx.

This chapter provides an overview of the required steps to update older versions of the INTUS TCL firmware to versions $\geq 3.00.00$.

Firmware version 3.00.00 introduces extensive changes to the update procedure. For this reason, a direct update from older versions to versions $\geq 3.00.00$ is not possible.

Therefore, an intermediate step is required to update the firmware from older versions to versions $\geq 3.00.00$.

Firmware Version	Intermediate Version
<= 1.16.99	1.17.00
Between 1.50.00 and 1.50.99	1.51.00



Notes:

The intermediate versions 1.17.00 and 1.51.00 are not intended for normal operation. They are used solely to install firmware versions $\geq 3.00.00$.

For firmware versions $\geq 3.00.00$, the model is no longer distinguished. Only whether the device is with or without VIG (masks) is relevant.

When resetting the SRAM, transactions may be lost due to the automatically performed cold start if they are still stored in the emergency buffer. Therefore, it must be ensured beforehand that the emergency buffer is cleared by means of an active connection to the higher-level system.

The current firmware version is displayed, for example, in INTUS RemoteConf:

Firmware package:	1.16.00
Version Monitor:	1.16.00
Version TCL:	6.82
Version INTUS Graph:	1.04.02

The current firmware version for your device is available via the [PCS Service Center](#).

If the firmware is not available there, please contact our support team at support@pcs.com.

4.9 Simultaneous execution of actions on several terminals

Many actions in INTUS RemoteConf can be executed at several terminals simultaneously. Some of the functions in INTUS RemoteConf, however, are only possible if one single terminal was selected. In these cases, the buttons are greyed out if several terminals are selected.

The following table offers an overview:

Button	Actions possible at several terminals
Login	yes
Logout	yes
Load TCL	no
Status Page	no
Configuration	no
LBus Actions	yes
Reset	yes
Firmware Update	yes
Load Mask	yes
Load Keyboard	yes
Load Audio	yes
Load Logo	yes
Flex Air	no
IP Setup	no
Remove	yes



Please note: If a button is greyed out in INTUS RemoteConf anyway, it means that at least one of the selected terminals doesn't support the respective function.

4.10 Changed commissioning steps for new devices

INTUS Devices shipped from August 2025 onwards follow a modified commissioning procedure.

In the factory default settings, the data port (see Chapter 9) is deactivated for these devices.

The required commissioning steps can be carried out using INTUS RemoteConf.

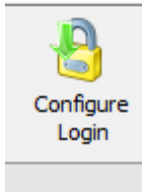
First, the login settings must be configured on the INTUS device. This can be done using "Configuration" (see Chapter 7) or "Set up Login" (see Chapter 4.11).

Setting up the login includes changing the passwords for all three authorization levels so that they no longer match the default passwords.

Once the login has been successfully set up, the color of a terminal in INTUS RemoteConf changes from "dark yellow" to "green".

Afterwards, the data port of the terminal can be configured.
This is done using "Configuration" (Chapter 7) or "Set up Data Port" (see Chapter 4.12).

4.11 Configure Login



- Authorization level 3
- For quick setup or modification of Login settings
- Configuration options are explained in Chapter 6 (Login)

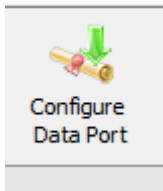


The correct and secure storage of access credentials such as passwords and maintenance groups within the system is the responsibility of the customer.

Loss of passwords may result in security risks, impaired system functionality, additional costs, and project delays.

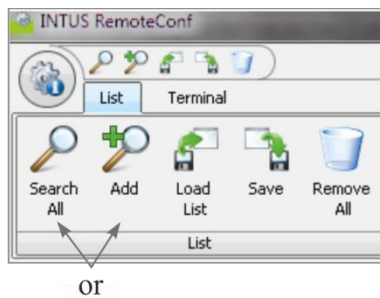
In order to receive technical support, project management, installation, or similar services, the required passwords must be available at the appropriate time.

4.12 Configure data port



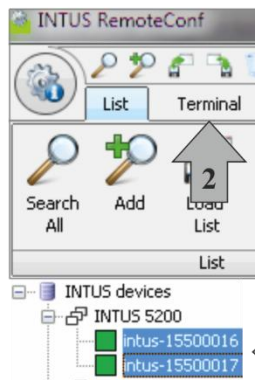
- Authorization Level 3
- For quick setup or modification of Data Port settings.
- The button is grayed out until the login has been set up (see Chapter 4.11).
- Configuration options are explained in Chapter 9 (Data Port – Channel A).

5 Introduction to the terminal configuration



Step 1

Display the terminal list or add the terminal to the list



Step 2

Go to the "Terminal" tab

Step 3

Select one or several terminals from the list



Step 4

Login via Password

Step 5

Select an action



Figure 5-1: Introduction to the terminal configuration

6 Login – log into the terminal

6.1 Authorization level

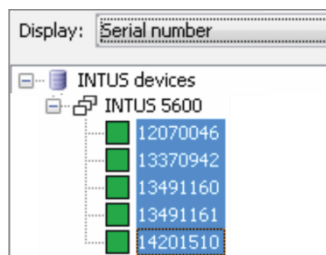
For security reasons, there are three different authorization levels accessible using passwords.

Authorization level	Password (default setting)	
1	111111	Password of level 1
2	14789632	Password of level 1 + 2
3	14589632	Password of level 1 + 2 + 3



You can change the passwords of the authorization levels via “Configuration>Configure Login”.

6.2 Procedure



You have to select one or several terminals from the list first.

Example:

INTUS RemoteConf logs into 5 terminals with the same authorization level.



Select the authorization level.

Maintenance: “0”, default setting

Enter the password, here authorization level 1: 111111.

Figure 6-1: Login



- The authorization level is displayed in a green label after login.
- Login remains until you select Logout or a system reboot is started.
- A time-limited lockout will occur for too many failed authentication attempts during login and when using IP Setup.

7 Configuration



The correct and secure storage of access credentials such as passwords and maintenance groups within the system is the responsibility of the customer.

Loss of passwords may result in security risks, impaired system functionality, additional costs, and project delays.

In order to receive technical support, project management, installation, or similar services, the required passwords must be available at the appropriate time.

7.1 Overview

The configuration is released for the selected terminal after Login.

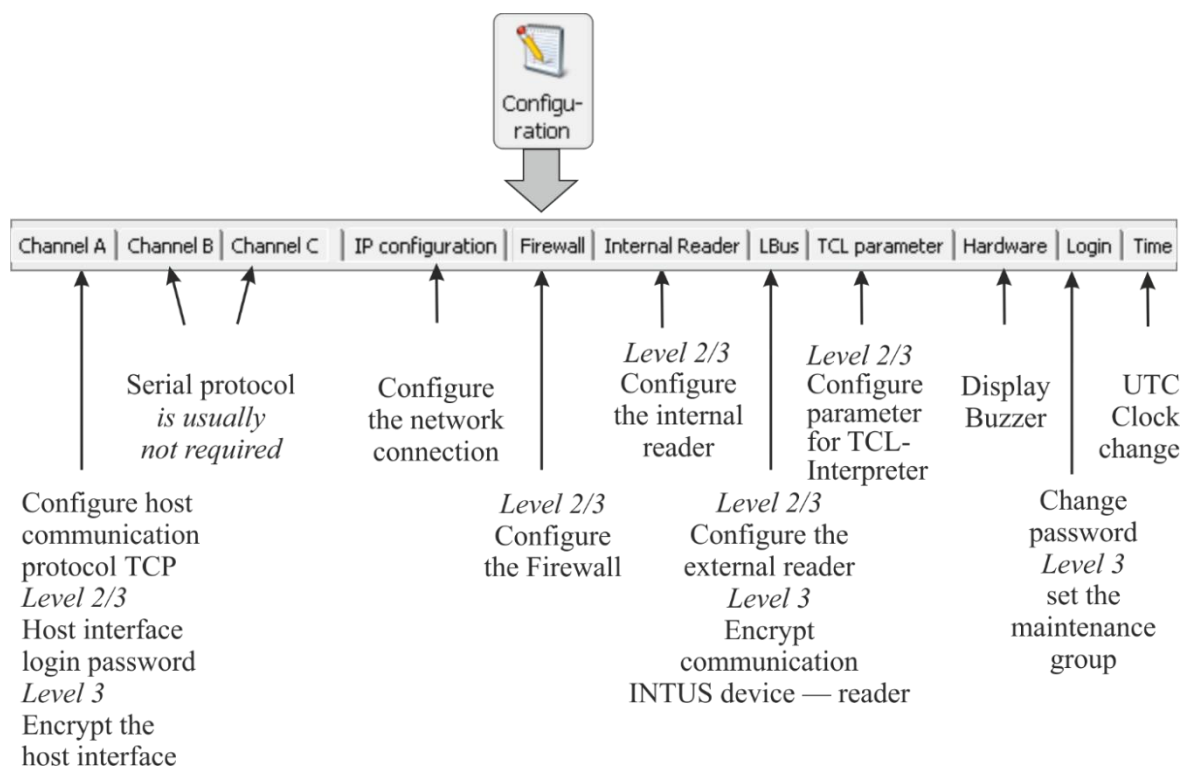


Figure 7-1: Configuration overview



Depending on terminal and interfaces, some items may not be available.

7.2 Save configuration to a file

There is the possibility of saving parts of the configuration to a file for loading it later on. This way you can easily reuse the configuration for this terminal or for other terminals.

Currently, the configuration parts you can select for saving are "Internal reader", "LBus", and "TCL parameters". When loading the saved data later on, you can select which parts of the configuration you want to load/use.



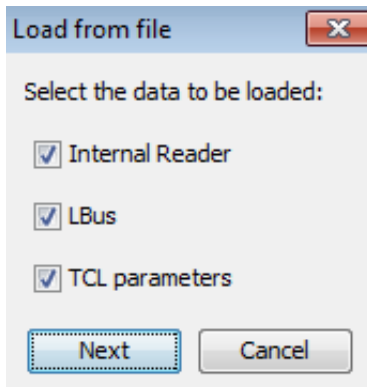
For security reasons, the keys for LBus encryption are not saved to those files. They have to be assigned manually each time.



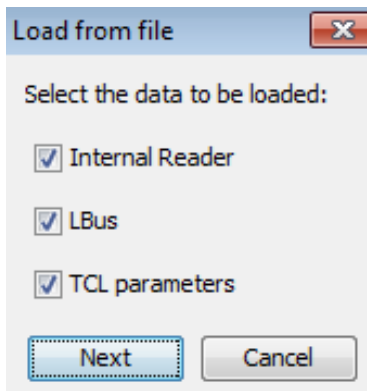
- 1 Click on the button „Save as file“, to save parts of the configuration:



- 2 Select the data you wish to save and choose the folder you want to save the file to:

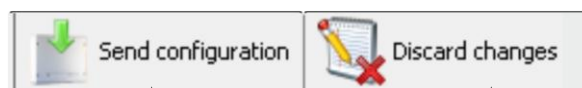


- 3 For loading saved configurations, click on the button „Load from file“ (see above) and select the data to be loaded:



- 4 Afterwards, send the configuration to the terminal, as described in the next chapter.

7.3 Finalizing the configuration



Accept settings and send them to the terminal, the new settings are effective immediately.

Cancel

Figure 7-2: Finalizing the configuration

8 The network connection (IP)



Channel A | Channel B | Channel C | **IP configuration** | Firewall | Internal Reader | LBus | TCL parameter

Location/contact

Location: Standort Terminal 17110029
 Contact: Ansprechpartner
 Characteristics of the terminal

IP options

Default setting
 intus-<serial number>
 If used, select **WiFi**

DHCP hostname: intus-17110029
 Host interface: LAN
 DNS server 1: ::
 DNS server 2: ::
 If used, indicate DNS server

IPv4

☒ Enabled ☒ DHCP
 Default setting
IPv4 - „DHCP“
 The terminal obtains the IPv4 address dynamically from the DHCP Server.

IPv4 address: 192 . 168 . 42 . 127
 IPv4 network mask: 255 . 255 . 255 . 0
 IPv4 gateway: 0 . 0 . 0 . 0

IPv6

☒ Enabled
 Mode: RADV
 Default setting
IPv6 - RADV
 The terminal generates an IPv6 address. In conjunction with IPv4 „DHCP“, further settings are not required.

IPv6 address: 2001::
 IPv6 gateway: ☒ Gateway from RADV
 ::

If necessary enable IEEE802.1X.

Ethernet

Eth-Link: Auto Negotiation
 IEEE 802.1X: ☐ Enabled
 Default setting
 Select IEEE802.1X if required

WLAN

For information about settings for WiFi please see next chapter.

IEEE 802.1X / WPA2-Enterprise

Figure 8-1: The network connection (IP)



Do not disable IPv6 without cause. IPv6 eases communication with the terminal.

IP options

DHCP host name

When the DHCP server is configuring the terminal IP, the terminal transmits the DHCP “host name” (option) to the DHCP server. The host name may consist of up to 18 alphanumeric characters or hyphens.

Please note that the host name has to start with an alphabetic character and must not finish with a hyphen.

By default, the host name is “intus-<serial number>”.

DNS server

A DNS server is only required if the HTTPS client setting is used under „Host Communication“ (see chapter 9).

Generally, the DNS servers are communicated to the terminal via DHCP or RDNSS.

In addition, up to 2 fixed DNS servers (IPv4 or IPv6 address) can be indicated.

A maximum of three DNS servers is used. DNS servers configured via the cellular interface, if any, have the highest priority. This is followed by RDNSS, DHCPv6, and DHCP. The statically configured DNS servers specified here have the lowest priority.

IPv4 / IPv6 address of the terminal



If the terminal is operated with a fixed address, please ask your network administrator for the IP address to be set.

IPv4 net mask

The subnet mask of the local network the terminal is installed on. The default value is 255.255.255.000.

It can be used for most networks. Ask your network administrator for the subnet mask that is to be set.

IPv6 obtains address dynamically

Set the dynamic address:

- **RADV** (default: Router advertisement) - an IPv6 address is generated automatically by the terminal itself according to the specifications of the local router.
- **DHCP** - the IPv6 address is obtained by the stateful DHCP.

IPv4 / IPv6 Gateway

IP address of the router:

Always set this address when host and terminal are in different logical subnets. Ask your network administrator for the IP address to be set.

IPv6 Prefix length

Prefix length (1-128 bits) for the local area network.

Normally, 64 bits is set.

Ethernet

Eth-Link – transfer rate

This parameter configures the transfer rate of the Ethernet link.

Auto-negotiation or a fixed transfer rate 10BASE-T or 100BASE-TX, each with half duplex or full duplex, are available. Auto-negotiation is the default setting.



The setting must be identical on the opposite side, otherwise communication problems may occur!

IEEE 802.1X

Authentication of the terminal in the Ethernet network.

For configuration, please see chapter 8.2.

8.1 WiFi

Valid for the terminals INTUS 5200 & INTUS 5320 & INTUS 5500/ 5540 & INTUS 5600

Your network administrator will provide you with the required information about WiFi.



The screenshot displays the configuration interface for WiFi. It is divided into two main sections: 'IP options' and 'WiFi'.

IP options section:

- DHCP hostname:** A text input field containing 'intus-52PROTO5'.
- Host interface:** A dropdown menu currently set to 'WiFi'.

WiFi section:

- Regulatory domain:** A dropdown menu set to 'Germany'.
- SSID:** A text input field containing 'test_wlan'.
- BSSID:** An empty text input field.
- Security:** A dropdown menu set to 'WPA2-PSK'.
- Wireless password (PSK):** A text input field filled with dots.
- show key:** An unchecked checkbox.
- keep / change:** Two radio buttons, with 'change' being the selected option.

Annotations on the right side of the screenshot:

- Next to the 'Host interface' dropdown: 'Select WiFi'.
- Next to the 'Regulatory domain' dropdown: 'The country code setting sets the frequency range in which the network is operating'.
- Next to the 'SSID' field: 'Name of the WiFi'.
- Next to the 'BSSID' field: 'Definite address of the WiFi'.
- Next to the 'Wireless password (PSK)' field: 'For information on this contact your network administrator'.

Figure 8-2: WiFi

* This information is absolutely necessary. The SSID needs to be configured as visible in the WiFi settings of the Access Points.

** This information is absolutely necessary for WPA2-PSK.

WiFi as host interface

If WiFi is available and WiFi is enabled as host interface, the Ethernet interface serves as a service interface.

The service interface has the following fixed network settings:

- IPv6 is enabled with Link-Local-address
- IPv4 address 192.168.42.127
- IPv4 network mask 255.255.255.0

If the WiFi interface is in this network, the Ethernet interface has the IPv4 address 10.10.42.127.

When using the service interface, actions of INTUS RemoteConf are restricted to:

- Changing the configuration
- Opening the status page

The service interface should be used only during commissioning or for maintenance purposes. During normal operation, no network cable should be connected.

8.2 IEEE 802.1X/WPA2-Enterprise

802.1x / WPA2-Enterprise muss must be configured if

- WiFi Security type WPA2 Enterprise is selected, or
- Ethernet 802.1x is enabled



IEEE 802.1X / WPA2-Enterprise

Authentication: Authentication/Inner authentication is described below.

Anonymous identity:

CA certificate: (not configured) The following requirements are set for the certificates:

- The file contains X.509 certificates only (no key)
- Number of certificates:
 - CA certificate: 1 to 5
 - Client certificate: exactly 1
- PEM or DER coding
- valid Common Name

Inner authentication:

User name:

Password: (not configured) ☐ Show password

User certificate: (not configured) ☒ keep ☐ delete ☐ change

Private key: (not configured) Private key is described below.

Private key password: (not configured) ☐ Show password

☒ keep ☐ delete ☐ change

Figure 8-3: IEEE 802.1X/WPA2-Enterprise

Authentication / inner authentication

The following methods are supported:

- EAP-MD5 (Ethernet 802.1x only)
- EAP-TLS
- EAP-PEAPv0/MD5
- EAP-PEAPv0/MSCHAPv2
- EAP-TTLS/EAP-MD5
- EAP-TTLS/EAP-MSCHAPv2
- EAP-TTLS/PAP
- EAP-TTLS/CHAP
- EAP-TTLS/MSCHAP
- EAP-TTLS/MSCHAPv2

Private key

- The file contains exactly one private key
- PEM or DER coding

With this information, your system administrator should be able to configure the WiFi.



It is possible to reset all settings, security-related information, and passwords via Reset, please see chapter 17.

8.3 Mobile communication



If „Mobile communication“ is used as host interface, the respective settings need to be entered here. The settings depend on your mobile communication provider.

Figure 8-4: Mobile

- APN and PIN need to be entered.
- User name / password depend on your network provider.

Mobile communication as host interface

If Mobile communication is available and Mobile communication is enabled as host interface, the Ethernet interface serves as a service interface.

The service interface has the following fixed network settings:

- IPv6 is enabled with Link-Local-address
- IPv4 address 192.168.42.127
- IPv4 network mask 255.255.255.0

If the intern Mobil communication-modem-interface is in this network, the Ethernet interface has the IPv4 address 10.10.42.127.

When using the service interface, actions of INTUS RemoteConf are restricted to:

- Changing the configuration
- Opening the status page

9 Data port (Channel A)



The default setting is "not configured"; an INTUS device must be set to the communication protocol TCP or HTTPS Client.

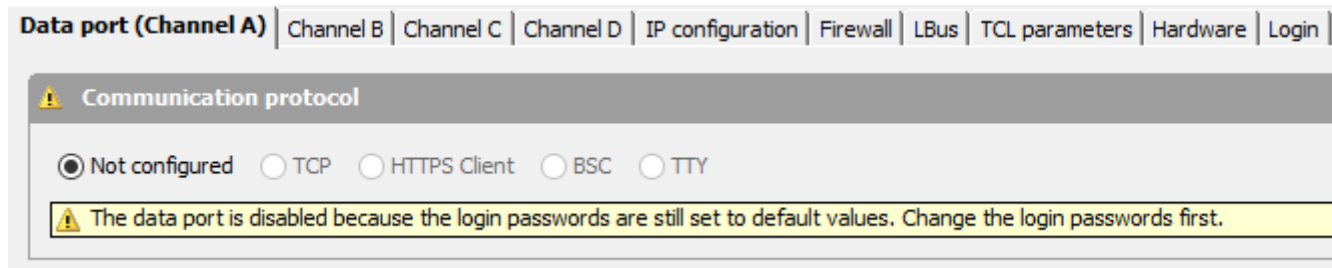


Figure 9-1: Channel A – Not configured

9.1 TCP protocol settings

Connection establishment

Defines the type of connection establishment (client/server):

Passive

Default setting, the terminal (server) opens a TCP port with the defined port number and waits for connection requests from the host (client).

If a connection has been set up and no data transfer has taken place for 1 minute, the terminal sends a "Keepalive" packet to find out whether the connection still exists. This way, an irregular connection breakdown is quickly detected, and rapid switchover from online mode to offline mode is possible.

Passive/RAS

This setting is suitable for TCP/IP connections via ISDN dial-up lines which are automatically released when there is no data traffic while the logical TCP/IP connection is maintained. Like the passive setting above, the passive/RAS value sets the terminal into passive server mode.

However, the intervals between "Keepalive" packets is increased from one minute to two hours in order to reduce communication costs.

Active

If the terminal is operated in active connection establishment mode, the host (server) must open a TCP port with the defined port number, and wait for connection requests from the terminal (client). The terminal periodically repeats its connection requests until a connection can be set up. This method is more secure because connection can only be set up to a host. "Keepalive" packets are sent the same way as in case of the passive setting.

"Keepalive on Demand": If a connection request for the TCL port arrives at a terminal operated in passive server mode although a connection still exists, the request is rejected.

Subsequently, the terminal attempts to find out with a “Keepalive” packet whether there is in fact a connection or whether an irregular connection breakdown occurred.

If a connection no longer exists, the TCP/IP protocol stack of the host will respond to these “Keepalive” packets with a TCP Reset packet and immediately release the connection this way.

If there is no such response from the host, it will take a maximum of 6 minutes before the terminal detects the connection as broken down and allows another connection.

In case of an irregular connection breakdown, the host will in any case receive a rejection (ECONNREFUSED or ECONNABORT) in response to at least one connection request (connect), before the connection can be set up. The implementation on the host must consider this fact and allow a number of connection setup attempts.

The screenshot displays the configuration interface for 'Data port (Channel A)'. The top navigation bar includes links for Channel B, Channel C, Channel D, IP configuration, Firewall, LBus, TCL parameters, Hardware, and Login. The main content area is divided into three sections: 'Communication protocol', 'TCP settings', and 'Security settings'. In the 'Communication protocol' section, 'TCP' is selected. The 'TCP settings' section shows 'Connection establishment' set to 'Passive' and 'Port' set to '3001'. The 'IPv4/IPv6 address' field is empty. The 'Security settings' section shows 'Encryption' set to 'Disabled', a 'Generate key' button, 'Login' set to 'Disabled', and fields for 'Password for simple access' and 'Password for administrative access', both with 'show password' checkboxes. At the bottom, there are fields for 'Transmission record structure: Routing bytes' and 'Record number character for login messages'.

Port

The port number for the terminal connection to the host. The port number is represented by a decimal value.

By default, the port number is set to 3001. Normally, the port number should not be changed. Port number 22, 80 und 3123 are not available.

IPv4 / IPv6 address

The address of the host is only required if connection establishment is set to active. Otherwise, the default value should not be changed.

Default:

IPv4 - 000.000.000.000 or

IPv6 - :: stands for 0000:0000:0000:0000:0000:0000:0000:0000

An IPv4 address can be displayed in IPv6 format, for example

192.168.42.127
 ↓ ↓ ↓ ↓
 0000:0000:0000:0000:0000:ffff:c0a8:2a7f or ::ffff:c0a8:2a7f

9.2 HTTPS client protocol settings

All parameters that can be entered depend on the used software solution of the host. Connections to hosts using certain reverse proxy solutions may require activation of the option "send content length header". This option should only be activated if necessary.



Data port (Channel A) | Channel B | Channel C | Channel D | IP configuration | Firewall | LBus | TCL parameters | Hardware | Login | Time

Communication protocol

☐ Not configured ☐ TCP ☒ HTTPS Client ☐ BSC ☐ TTY

HTTPS Client settings

Hostname:

Port:

Directory:

User name:

Password:

☐ show password

☐ keep ☒ change

CA certificate: Certum Trusted Network CA Load

☐ keep ☒ change

☒ Online update

Upstream: ☒ Send Content-Length Header

Figure 9-2: HTTPS client settings

The URL for communication with the host is created using host name, port, and directory.

For authentication, user name and password are used (basic authentication).

The CA certificate serves for verifying the server certificate.

Certificates in PEM format are accepted. Up to 10 different certificates can be added to a file.

With TCL Firmware 1.08 and later, an automatic update of the CA certificate via the host can be activated using the option "Online update". The software solution of the host needs to support this.

For further information, please see the INTUS TCL manual G3000-004.

9.3 Security settings

Encryption on host interface with TCP protocol

Authorization level 3

It is possible to configure encrypted data transfer between host and TCL interpreter.



Click "Generate key" to enter any encryption text of up to 512 characters. This text is used to generate a key for transmission.

Login on host interface

Authorization level 2/3

You can set a password and routing bytes for the communication with the TCL interpreter (MONIN & MONOUT process).

Password for simple access

The terminal can send records. It only processes "J" records and acknowledgment records.

Password for administrative access

No restrictions are applied.

For more information, please see the INTUS TCL Programming Manual G3000-004.

10 The Firewall

Authorization level 2 / 3



Enable the firewall to prevent unauthorized network access to the terminal. To permit the operation, you have to allow network access to different services as data, maintenance and state.

To permit the operation, the Data and Maintenance services must be enabled for the respective network participants.

Enabling the Status service is optional and not required for operation.

For an explanation of the terms Data, Maintenance, and Status, refer to Chapter 22. The restrictions for the Data service apply specifically when the data port (Channel A) is used in TCP / passive operating mode.

The network address in conjunction with the network mask/prefix defines which and how many network users are granted access authorization for the respective services.

The number of network users is defined by the network mask/prefix and calculated using binary code. The value 255.255.255.255 (IPv4) or 128 (IPv6) means only a single network user has the configured access authorization.

The lowest value is 0.0.0.0 (IPv4) or 0 (IPv6). This means that all network participants, regardless of their network address, are granted the configured access permissions.

Up to five access entries can be defined for IPv4 and IPv6 respectively. If a service request from a network participant does not match any of the defined access entries, the request will be discarded.

For more information on network address and mask please contact your network administrator.

Default setting

Firewall is not configured.

Data port (Channel A) | Channel B | Channel C | Channel D | IP configuration | **Firewall** | LBus | TCL parameters | Hardware | Login | Time

Firewall

☒ Enable firewall

IPv4 network address	IPv4 network mask	Maintenance	Data	State
192 . 169 . 167 . 0	255 . 255 . 255 . 0	☒	☒	☐
192 . 169 . 10 . 33	255 . 255 . 255 . 255	☐	☐	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐

IPv6 address	IPv6 prefix	Maintenance	Data	State
fe80::	/ 64	☒	☐	☒
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐

Figure 10-1: Firewall Configuration - Example

Figure 10-2 shows an example configuration that grants access to Maintenance and Data for all network participants, but does not grant any access to Status. For this purpose, one access entry for IPv4 and one access entry for IPv6 have been configured.

Data port (Channel A) | Channel B | Channel C | Channel D | IP configuration | **Firewall** | LBus | TCL parameters | Hardware | Login | Time

Firewall

☒ Enable firewall

IPv4 network address	IPv4 network mask	Maintenance	Data	State
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☒	☒	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐
0 . 0 . 0 . 0	0 . 0 . 0 . 0	☐	☐	☐

IPv6 address	IPv6 prefix	Maintenance	Data	State
::	/ 0	☒	☒	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐

Figure 10-2: Status not granted

11 Configuring the LBus

Authorization level 2 / 3

- The LBus is an interface to connect external readers.
- When configuring the LBus, the available LBus interfaces with the corresponding board labelling are displayed.
- To improve readability, the term “reader” is used in the following, also if a subterminal is dealt with.
- **HW address** means the reader's address, which must be set manually for each reader. Please refer to the reader's installation guide for information.
- **TCL address** is the logical address of the reader.
- **Point-to-Point (PP)**: When 1x reader is connected to an LBus interface, this is called Point-to-Point (PP) by PCS.
- **Multi-Point (MP)**: When several readers are connected to an LBus interface in a line, the connection type is called Multi-Point (MP) by PCS.



In case of a connection of INTUS Flex readers with the INTUS Flex Gateway: A Gateway can be connected directly "Point-to-Point", but if several cylinders have to be coupled, "Multipoint" must be set in TCL.



No address can be set for the **INTUS 315ro**. Therefore, no Multi-Point connection is possible.

Reader type **OSDP** currently only supports INTUS Flex readers. Other OSDP readers have to be verified and released by PCS!

11.1 Maximum number of readers

Device	Number of readers		Remark
	LBus 1	LBus 2	
INTUS 5200	1	----	Option
INTUS 5320	4	----	
INTUS 5500/5540/5600	8	8	
INTUS ACM80e Rack	8	8	Standard 8 readers Optional 16 readers
INTUS ACM80e Wall	8	8	Standard 4 readers Optional 8 or 16 readers
INTUS ACM40e	8	8	Standard 2 readers Optional 4 readers With ACM40e Wiegand module: + 4 Wiegand readers With 4Flex license*: + 4 INTUS Flex readers With 16Flex license*: +16 INTUS Flex Endgeräte

*With a basic ACM40e configuration without 4Flex license, no INTUS Flex readers can be operated.

11.2 Wiring the INTUS 5200 / 5320 / 5500 / 5540 / 5600

Wiring LBus1/LBus2



Only Multi-Point / Multi-Point cabling is possible for non-ACM devices:

INTUS 5500/5540/5600 each max. 8 readers per interface (option),

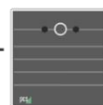
INTUS 5200 one reader per interface (option).

INTUS 5200

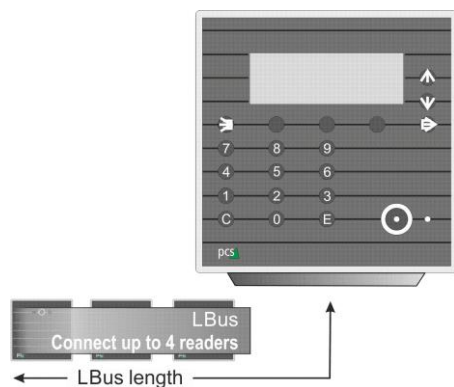


Connection: at most one reader

Distance: up to 10m / 33ft



INTUS 5320



INTUS 5500/5540/5600

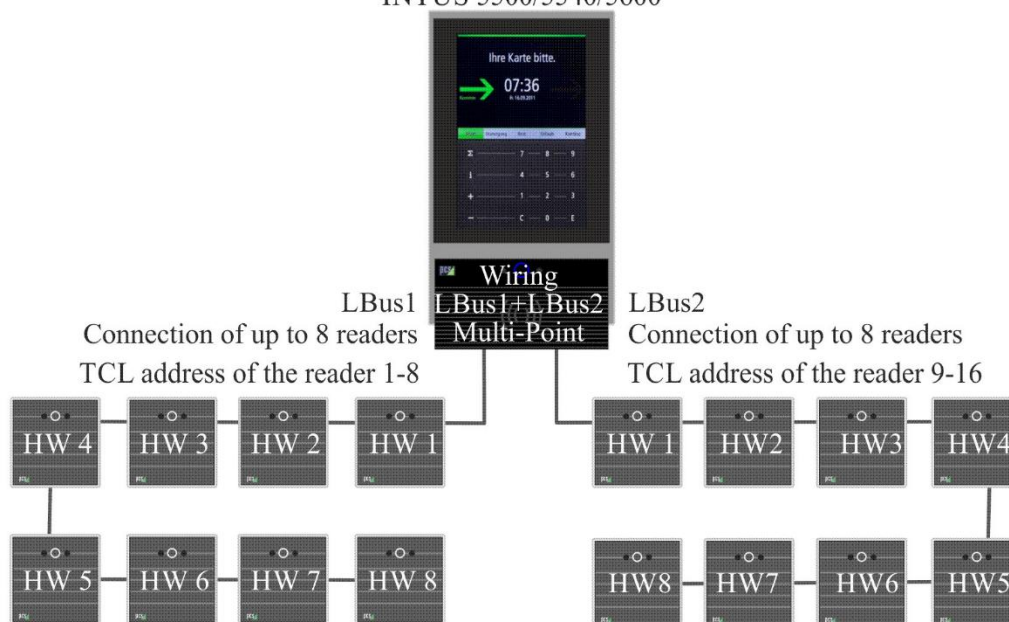
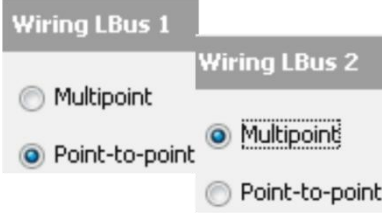
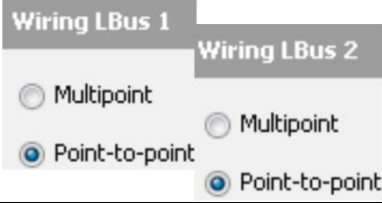
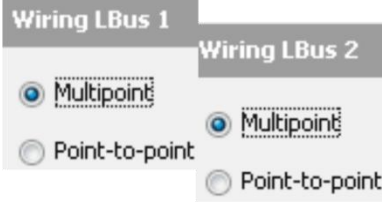


Figure 11-1: Wiring the INTUS 5200 / INTUS 5320 / INTUS 5500 / 5540 / 5600

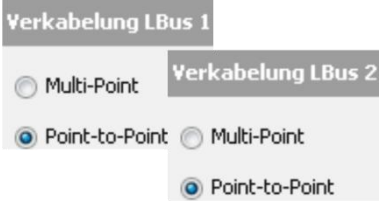


The HW (Hardware) address must be set for each reader, as described in the reader's installation manual.

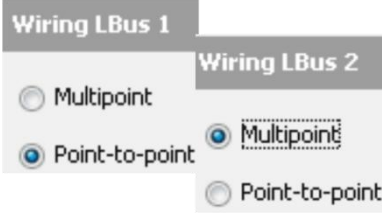
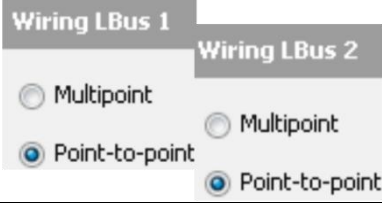
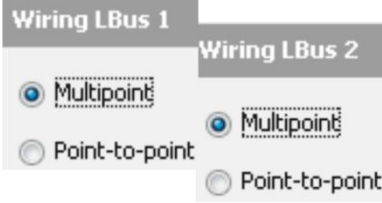
11.3 Wiring options of the INTUS ACM40e

Wiring LBus1 /LBus2	INTUS ACM Reader interface	Connected readers	Reader addressing HW address	
			easy	fixed
	Reader 1 to reader 4 -----	1 x reader per interface Max. 4 readers	1	1 to 4
	Reader 1 to reader 2 Reader 3 to reader 4	1 x reader per interface Max. 4 readers	1	1 to 2 1 to 2
	Reader 1 to reader 2 Reader 3 to reader 4	8 readers max, divided to the reader interfaces	---	1 to 4 1 to 4

11.4 Wiring options of the INTUS ACM40e with Wiegand module

Wiring LBus1 /LBus2	INTUS ACM40e Reader interface	Connected readers	Reader HW address	
			easy	fixed
	Wiegand 1 to 2 Wiegand 3 to 4	4 readers max distributed to the reader interfaces	---	---
	Reader 1 to 2 Wiegand 1 to 4	6 readers max distributed to the reader interfaces	1 ---	1 to 2 ---
	Wiegand 1 to 4 Reader 1 to 2	6 readers max distributed to the reader interfaces	---	---

11.5 Wiring options of the INTUS ACM80e

Wiring LBus1 /LBus2	INTUS ACM Reader interface	Connected readers	Reader addressing HW address	
			easy	fixed
	Reader 1 to Reader 8 -----	1 x reader per interface Max. 8 readers	1	1 to 8
	Reader 1 to Reader 4 Reader 5 to Reader 8	1 x reader per interface Max. 8 readers	1	1 to 4 1 to 4
	Reader 1 to Reader 4 Reader 5 to Reader 8	Max. 16 readers distributed to the reader interfaces	---	1 to 8 1 to 8

INTUS ACM80e with additional LBus2 interface (option)

Wiring LBus1/LBus2



You have to select: Point-to-Point for the interfaces Reader1 to Reader8 / Multi-Point for the LBus2 interface.

11.6 Point-to-Point wiring the INTUS ACM80e

HW address of the reader *

Easy addressing enabled: Reader HW address 1

Fixed reader HW address: LBus1 1 - 8;

LBus1+LBus2 1 - 4 + 1 - 4

TCL address of the reader

LBus1: 1 - 8

LBus1 + LBus2: 1 - 4 + 9 - 12

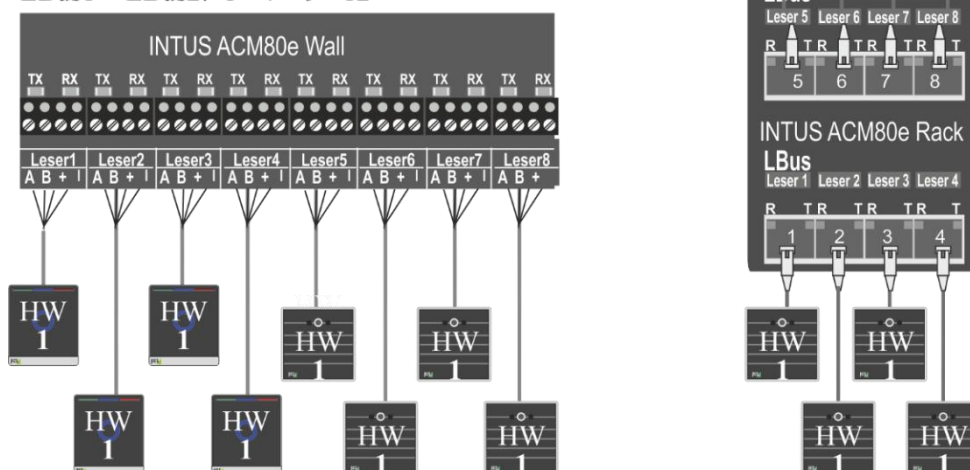


Figure 11-2: Point-to-Point wiring the INTUS ACM80e

11.7 Multi-Point wiring the INTUS ACM80e

Readers can be freely assigned to the interfaces / slots. The distribution of the readers is determined by the specific features of the given installation.

The HW (hardware) address* for each reader can be individually configured in the range from 1 to 8.

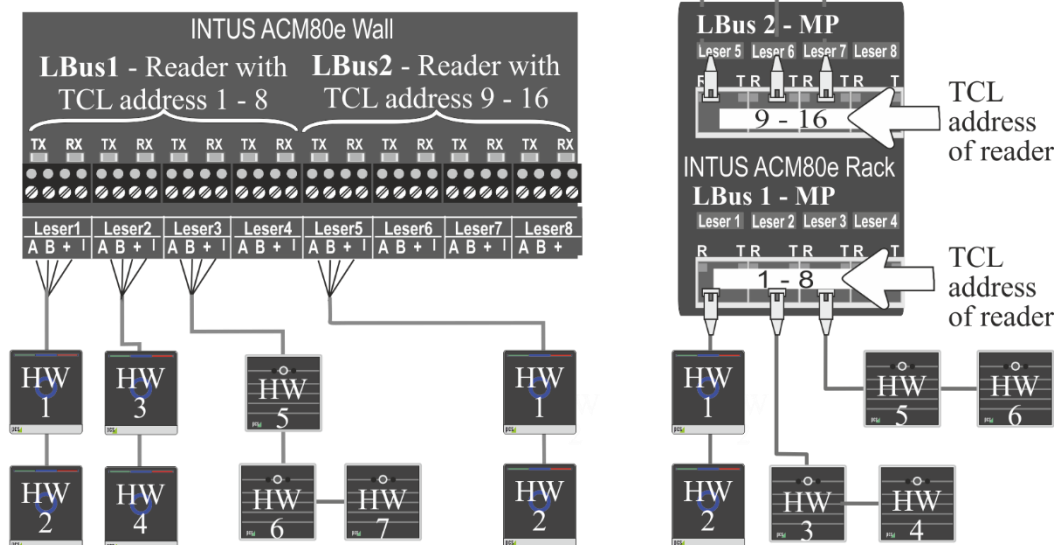


Figure 11-3: Multi-Point wiring the INTUS ACM80e



* The HW (Hardware) address must be set for each reader, as described in the reader's installation manual.

11.8 Configuring a reader



The figure illustrates the configuration process for a reader in the INTUS RemoteConf software, divided into five steps:

- Step 1:** Select **LBus** and set the wiring. The interface shows tabs for Channel A, Channel B, Channel C, IP configuration, Firewall, Internal Reader, **LBus**, and TCL parameter. Under LBus, it indicates "0 readers configured, 16 readers possible". The wiring options for LBus 1 and LBus 2 are shown: Multipoint and Point-to-point. Point-to-point is selected for LBus 1, and Multipoint is selected for LBus 2.
- Step 2:** Select **LBus1** or **LBus2**. The interface shows LBus 1 selected.
- Step 3:** Set the **Reader type**. The interface shows the Reader type options: not configured, INTUS 700/6xx/5x0/4x0/1600/1500/350H (selected), INTUS 300H/340H, INTUS 300L/300M, and INTUS 300ro/315ro. The Easy addressing checkbox is checked. A button labeled "Generate key" is visible.
- Step 4:** Select reader interface. The interface shows the reader interface options: Leser 1, Leser 2, Leser 3, and Leser 4. A table titled "LBus 1/Leser 1" shows the configuration for the selected reader:

TCL address	HW address	Mode of operation	Encryption
1	1	not configured	☐
- Step 5:** Set the mode of operation for the connected reader. The interface shows the mode of operation options: not configured, Mode A (2x16 character display, INTUS 1500, INTUS 610moto), Mode B (Default), and Mode C (Extended keyboard functionality, INTUS 1600-II). Mode B is selected.

The final state shows "LBus (1 readers configured, 16 readers possible)" and "The reader is configured".

Figure 11-4: Reader configuration



INTUS 5200/5320/5500/5540/5600, the 1st step is omitted, since only Multi-Point wiring is possible for LBus1 and LBus2

11.9 Reader type / Easy addressing

The reader is not yet configured by setting the reader type. Communication on the LBus is defined by the reader type.



Valid for the following readers:
 INTUS 700
 INTUS 600/615/620; 600FP
 INTUS 500/500IP/520IP
 INTUS 400/420/400S
 INTUS 1600/1600-II/1500/FP
 INTUS 350H/640H*
 INTUS PS Controller
 INTUS I/O Box

Point-to-Point
 recommended setting



Figure 11-5: Easy addressing

* INTUS 350H and INTUS 640H, setting of the reader type depends on whether an LBus protocol or 340H protocol is configured inside the reader.

The following settings are required:

- LBus protocol “reader type: INTUS 700/6xx/.../350H” is set;
- 340H protocol “reader type: 300H/340H” is set,

Please also see INTUS 350H or INTUS 640H Installation Guide.

Mixed operation is possible when the readers have the same “Reader type” setting. Please always note the length of the LBus at mixed operation!

Easy addressing enabled, INTUS ACM only

For Point-to-Point wiring, simple addressing should be enabled. There mustn't be a conflict between the reader address (1) and the reader identification or TCL address in the access server.

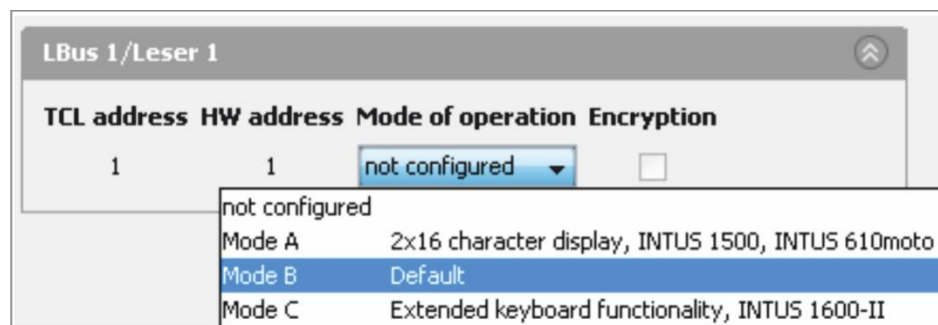
Each external reader is assigned HW address1, which is usually preset. This setting should be checked.

11.10 Mode of operation



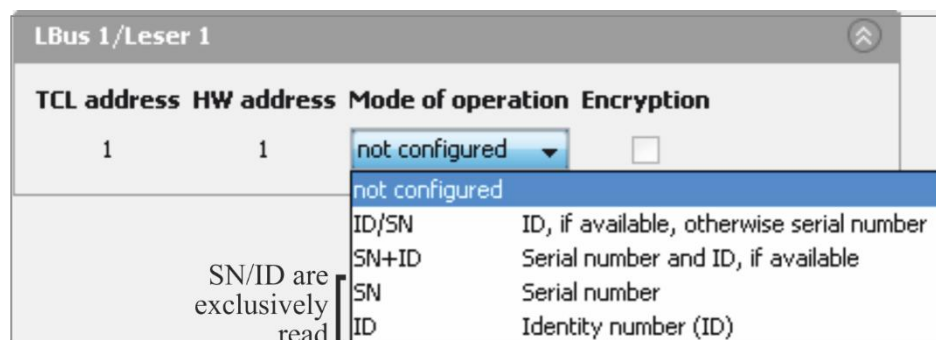
For configuring an external reader, the mode of operation must be specified (not for Wiegand or INTUS Flex (OSDP) readers).

INTUS 700, 600, 615, 620, 500IP, 520IP, 400, 420, 350H, 640H, 600/800FP, INTUS 1600, 1600-II, INTUS PS Controller



Reader	Display formatting		
	Mode A	Mode B	Mode C
	2 x 16 characters	2 x 20 characters	2 x 20 characters + extended keyboard functionality
INTUS 700, 600/615/620, 500IP/520IP, 400/420, 350H, 640H, 600/800FP	-	OK	-
INTUS 1600-II	-	OK	OK
INTUS 1500 / 610Moto	OK	-	-
INTUS 1600	OK	OK	-
INTUS PS Controller	-	OK	-

INTUS 300H, INTUS 340H, INTUS 350H/ 640H (340H protocol)



INTUS 300L, 300M

“Default mode“ should only be changed after having consulted the PCS Technical Support.

11.11 Example ACM40e Wiegand module: 2 LBus readers, 4 Wiegand readers

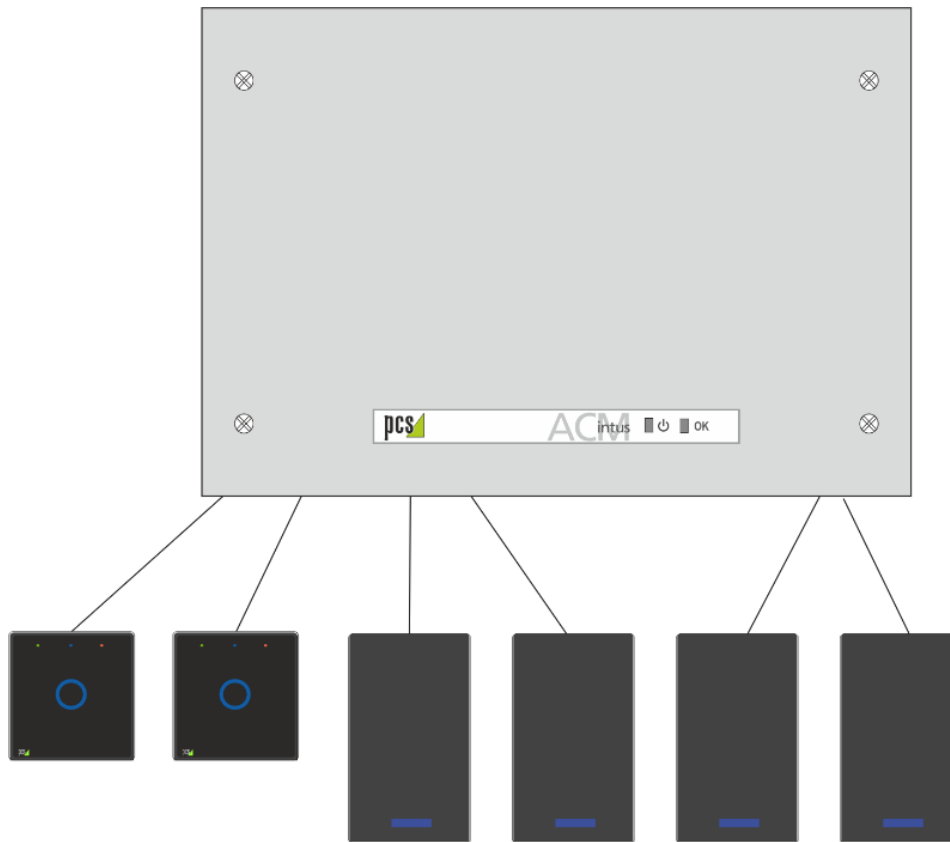


Figure 11-6: ACM40e Wiegand module: 2 LBus readers, 4 Wiegand readers

Settings Wiring PP/PP

Wiring LBus 1
☐ Multi-Point
☒ Point-To-Point

Wiring LBus 2
☐ Multi-Point
☒ Point-To-Point

LBus 1

Reader type:

☐ not configured

☒ INTUS 700/6xx/5x0/4x0/1600/1500/350H

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☐ Wiegand

☐ OSDP

☒ Easy addressing

Generate key (for PCS-proprietary encryption)

Configuration LBus 2

LBus 2

Reader type:

☐ not configured

☐ INTUS 700/6xx/5x0/4x0/1600/1500/350H

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ Wiegand

☐ OSDP

☐ Easy addressing

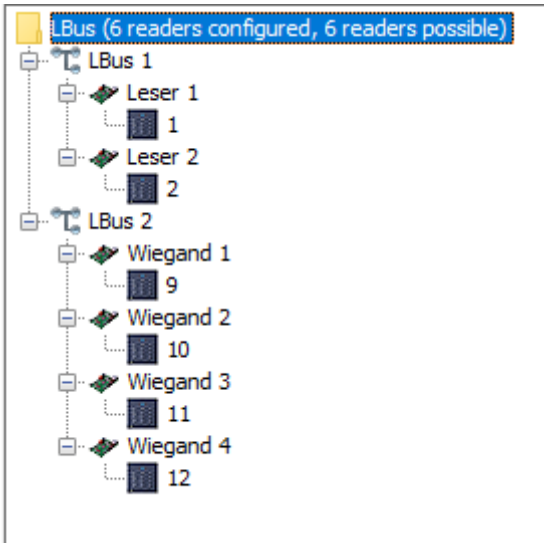
Generate key (for PCS-proprietary encryption)

Configuration of the Reader to "Wiegand 1"

LBus 2/Wiegand 1

TCL address	HW address	Mode of operation	Encryption
9	1	Default mode not configured Default mode Wiegand	☐

Result



11.12 Example - ACM40e with 16Flex-Licence - 16 wireless connected INTUS Flex devices

Star Wiring (configuration MP/MP):

- One INTUS Flex Gateway is connected to "Leser 1" - interface
- One INTUS Flex Gateway is connected to "Leser 3" - interface

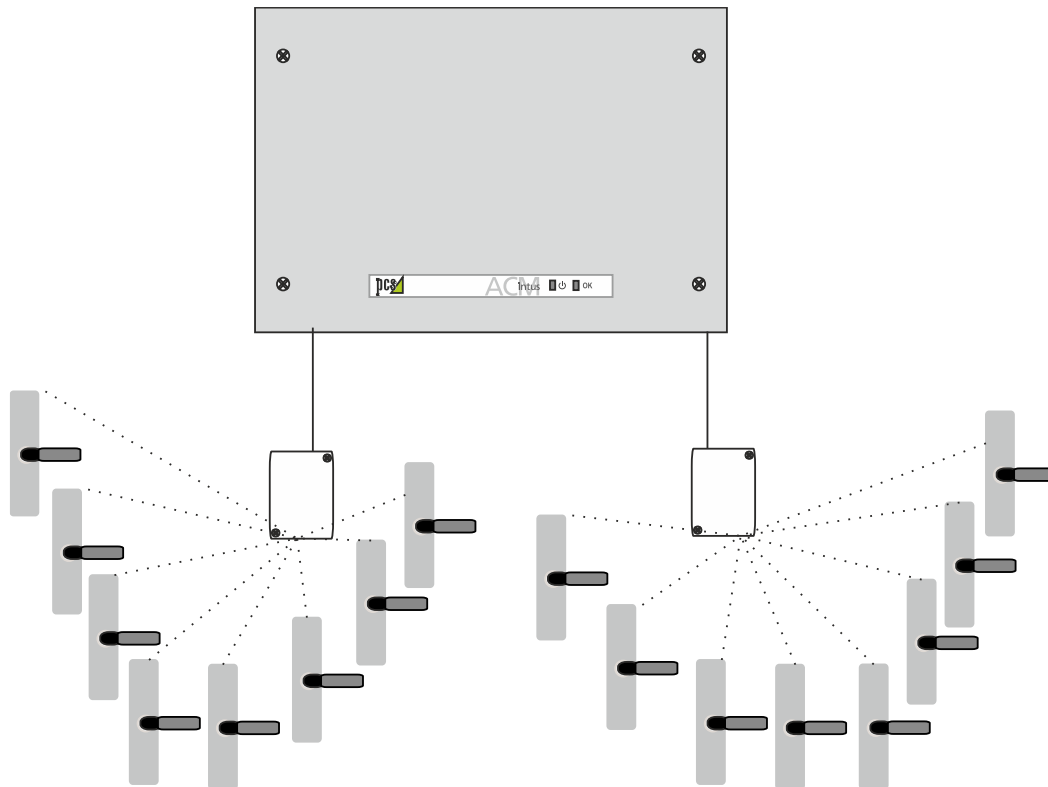


Figure 11-7: example ACM40e with 16 INTUS Flex devices

Setting MP/MP

The screenshot shows a configuration window with two sections: 'Wiring LBus 1' and 'Wiring LBus 2'. Each section contains two radio button options: 'Multi-Point' and 'Point-To-Point'. In both sections, the 'Multi-Point' option is selected, indicated by a filled circle next to the text.

Setting LBus 1 / OSDP

LBus 1

Reader type:

☐ not configured

☐ INTUS 700/6xx/5x0/4x0/1600/1500/350H

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ Easy addressing

Generate key (for PCS-proprietary encryption)

Setting LBus 2 / OSDP

LBus 2

Reader type:

☐ not configured

☐ INTUS 700/6xx/5x0/4x0/1600/1500/350H

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ Easy addressing

Generate key (for PCS-proprietary encryption)

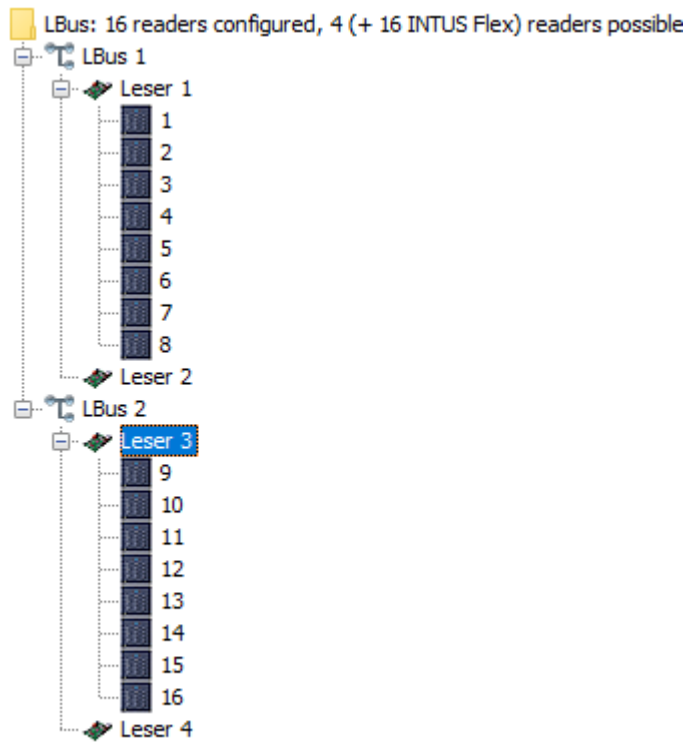
Configuration on "Leser 1"

LBus 1/Leser 1			
TCL address	HW address	Mode of operation	Encryption
1	1	INTUS Flex	☒
2	2	INTUS Flex	☒
3	3	INTUS Flex	☒
4	4	INTUS Flex	☒
5	5	INTUS Flex	☒
6	6	INTUS Flex	☒
7	7	INTUS Flex	☒
8	8	INTUS Flex	☒

Configuration on "Leser 3"

LBus 2/Leser 3			
TCL address	HW address	Mode of operation	Encryption
9	1	INTUS Flex	☒
10	2	INTUS Flex	☒
11	3	INTUS Flex	☒
12	4	INTUS Flex	☒
13	5	INTUS Flex	☒
14	6	INTUS Flex	☒
15	7	INTUS Flex	☒
16	8	INTUS Flex	☒

Result



11.13 Example - ACM40e with 16Flex-Licence - Mixed operation with star-shaped connected INTUS readers

- LBus1: 2 INTUS reader, star-shaped connection. "Leser 1" and "Leser 2".
- LBus2: 2 INTUS Flex Gateways, 8 wireless INTUS Flex devices.
- The first INTUS Flex Gateway is connected to "Leser 3": TCL-addresses 9, 10, 11 and 12.
- The second INTUS Flex Gateway is connected to "Leser 4": TCL-addresses 13, 14, 15 and 16.



MP/MP must be set. With that, no "easy addressing" to LBus 1 is possible (just possible with PP).

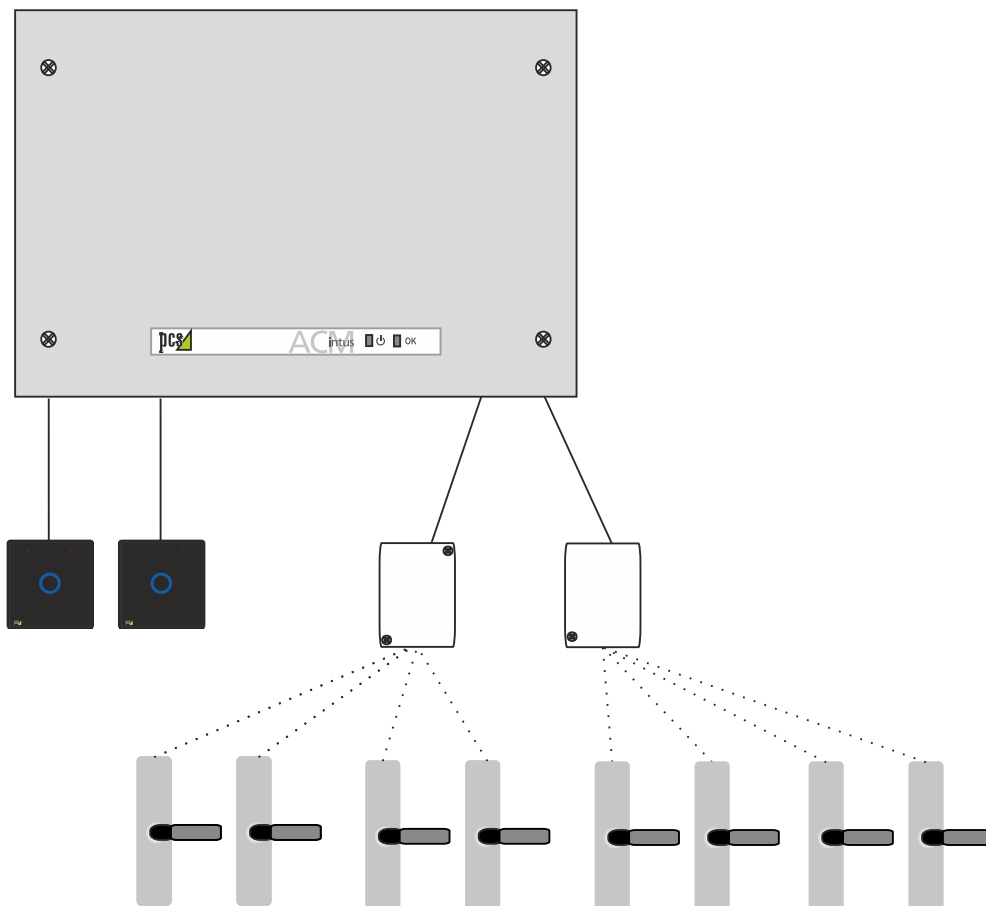
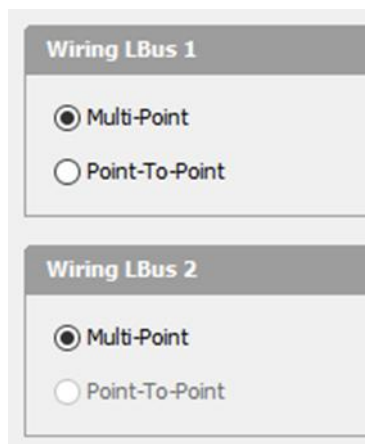


Figure 11-8: ACM 40e, 2 readers, 8 INTUS Flex devices

Setting MP / MP



The screenshot shows two configuration panels, 'Wiring LBus 1' and 'Wiring LBus 2'. Each panel contains two radio button options: 'Multi-Point' (which is selected) and 'Point-To-Point'.

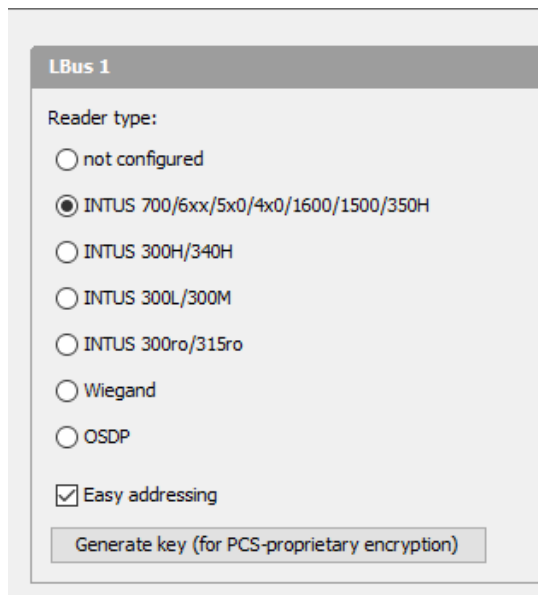
Wiring LBus 1

- ☒ Multi-Point
- ☐ Point-To-Point

Wiring LBus 2

- ☒ Multi-Point
- ☐ Point-To-Point

Setting LBus 1 / INTUS 700/6xx/5x0/4x0/1600/1500/350H



The screenshot shows the 'LBus 1' configuration panel. It includes a 'Reader type:' section with several radio button options. The option 'INTUS 700/6xx/5x0/4x0/1600/1500/350H' is selected. There is also a checkbox for 'Easy addressing' which is checked, and a button labeled 'Generate key (for PCS-proprietary encryption)'.

LBus 1

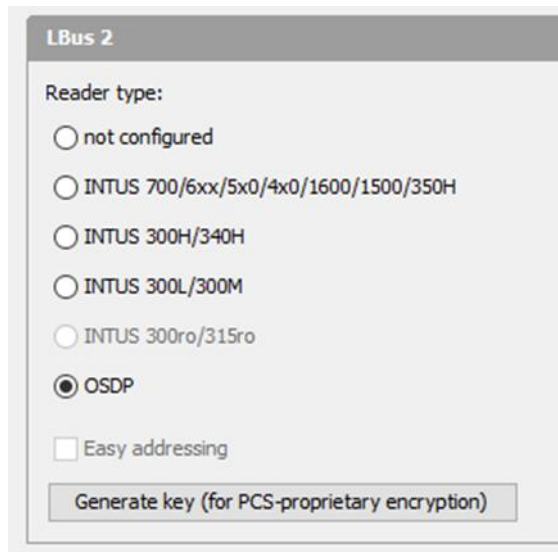
Reader type:

- ☐ not configured
- ☒ INTUS 700/6xx/5x0/4x0/1600/1500/350H
- ☐ INTUS 300H/340H
- ☐ INTUS 300L/300M
- ☐ INTUS 300ro/315ro
- ☐ Wiegand
- ☐ OSDP

☒ Easy addressing

Generate key (for PCS-proprietary encryption)

Setting LBus 2 / OSDP



The screenshot shows the 'LBus 2' configuration panel. It includes a 'Reader type:' section with several radio button options. The option 'OSDP' is selected. There is also a checkbox for 'Easy addressing' which is unchecked, and a button labeled 'Generate key (for PCS-proprietary encryption)'.

LBus 2

Reader type:

- ☐ not configured
- ☐ INTUS 700/6xx/5x0/4x0/1600/1500/350H
- ☐ INTUS 300H/340H
- ☐ INTUS 300L/300M
- ☐ INTUS 300ro/315ro
- ☒ OSDP

☐ Easy addressing

Generate key (for PCS-proprietary encryption)

Configuration on "Leser 1"

LBus 1/Leser 1			
TCL address	HW address	Mode of operation	Encryption
1	1	Mode B	☒
3	3	not configured	☐
4	4	not configured	☐

Configuration on "Leser 2"

LBus 1/Leser 2			
TCL address	HW address	Mode of operation	Encryption
2	2	Mode B	☒
3	3	not configured	☐
4	4	not configured	☐

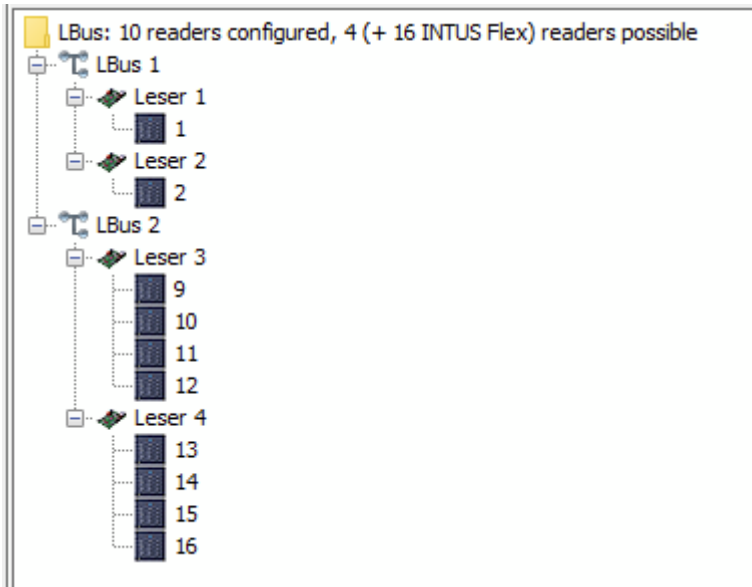
Configuration on "Leser 3"

LBus 2/Leser 3			
TCL address	HW address	Mode of operation	Encryption
9	1	INTUS Flex	☒
10	2	INTUS Flex	☒
11	3	INTUS Flex	☒
12	4	INTUS Flex	☒

Configuration on "Leser 4"

LBus 2/Leser 4			
TCL address	HW address	Mode of operation	Encryption
13	5	INTUS Flex	☒
14	6	INTUS Flex	☒
15	7	INTUS Flex	☒
16	8	INTUS Flex	☒

Result



11.14 Example ACM40e with 16Flex-Licence - Mixed operation with bus-wired INTUS readers

- LBus1: 4 INTUS readers, all 4 on "Leser 1". Bus-wired.
- LBus2: 2 INTUS Flex Gateways, 8 wireless INTUS Flex devices. Bus-wired.
- The first INTUS Flex Gateway is connected to "Leser 3". TCL-addresses 9 and 10.
- The second INTUS Flex Gateway is connected to "Leser 3": TCL-addresses 11 und 12.
- The third INTUS Flex Gateway is connected to "Leser 4": TCL-addresses 13 und 14.
- The fourth INTUS Flex Gateway is connected to "Leser 4": TCL-addresses 15 und 16.

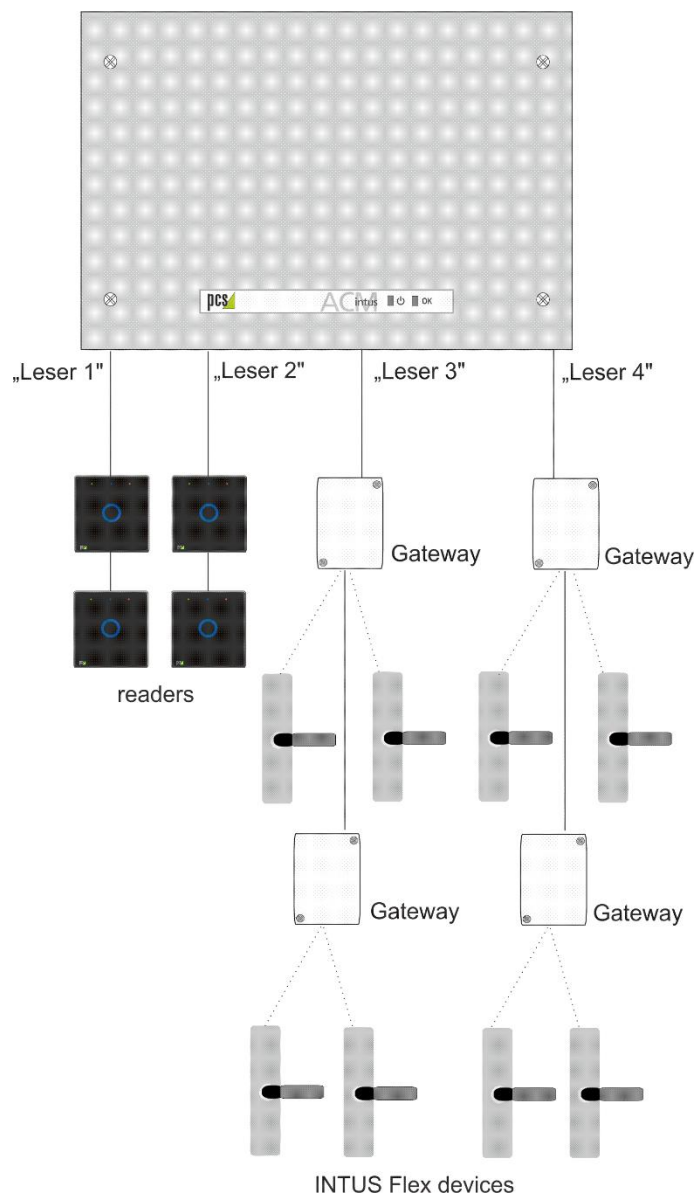


Figure 11-9: ACM40e, 4 readers, 8 INTUS Flex devices

Setting MP / MP

The screenshot shows two configuration panels. The top panel, titled 'Wiring LBus 1', contains two radio button options: 'Multi-Point' (which is selected) and 'Point-To-Point'. The bottom panel, titled 'Wiring LBus 2', also contains two radio button options: 'Multi-Point' (selected) and 'Point-To-Point'.

Setting LBus 1 / INTUS 700/6xx/5x0/4x0/1600/1500/350H

The screenshot shows the 'LBus 1' configuration panel. Under the heading 'Reader type:', there are several radio button options: 'not configured', 'INTUS 700/6xx/5x0/4x0/1600/1500/350H' (selected), 'INTUS 300H/340H', 'INTUS 300L/300M', 'INTUS 300ro/315ro', 'Wiegand', and 'OSDP'. Below these options is a checked checkbox for 'Easy addressing'. At the bottom of the panel is a button labeled 'Generate key (for PCS-proprietary encryption)'.

Setting LBus 2 / OSDP

The screenshot shows the 'LBus 2' configuration panel. Under the heading 'Reader type:', there are several radio button options: 'not configured', 'INTUS 700/6xx/5x0/4x0/1600/1500/350H', 'INTUS 300H/340H', 'INTUS 300L/300M', 'INTUS 300ro/315ro', and 'OSDP' (selected). Below these options is an unchecked checkbox for 'Easy addressing'. At the bottom of the panel is a button labeled 'Generate key (for PCS-proprietary encryption)'.

Configuration on "Leser 1"

LBus 1/Leser 1			
TCL address	HW address	Mode of operation	Encryption
1	1	Mode B	☒
2	2	Mode B	☒

Configuration on "Leser 2"

LBus 1/Leser 2			
TCL address	HW address	Mode of operation	Encryption
3	3	Mode B	☒
4	4	Mode B	☒

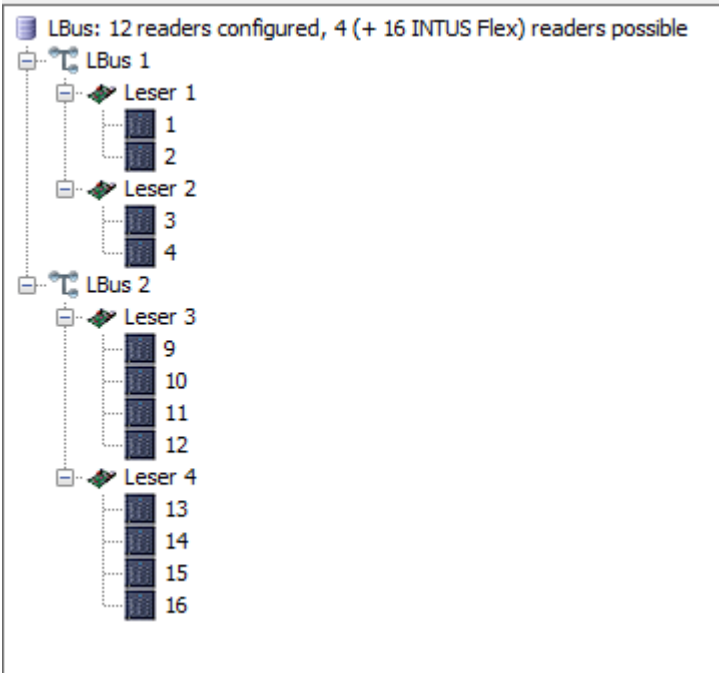
Configuration on "Leser 3"

LBus 2/Leser 3			
TCL address	HW address	Mode of operation	Encryption
9	1	INTUS Flex	☒
10	2	INTUS Flex	☒
11	3	INTUS Flex	☒
12	4	INTUS Flex	☒

Configuration on "Leser 4"

LBus 2/Leser 4			
TCL address	HW address	Mode of operation	Encryption
13	5	INTUS Flex	☒
14	6	INTUS Flex	☒
15	7	INTUS Flex	☒
16	8	INTUS Flex	☒

Results



11.15 Example ACM80e with 8 INTUS 700/6xx/350H readers and 8 INTUS Flex devices

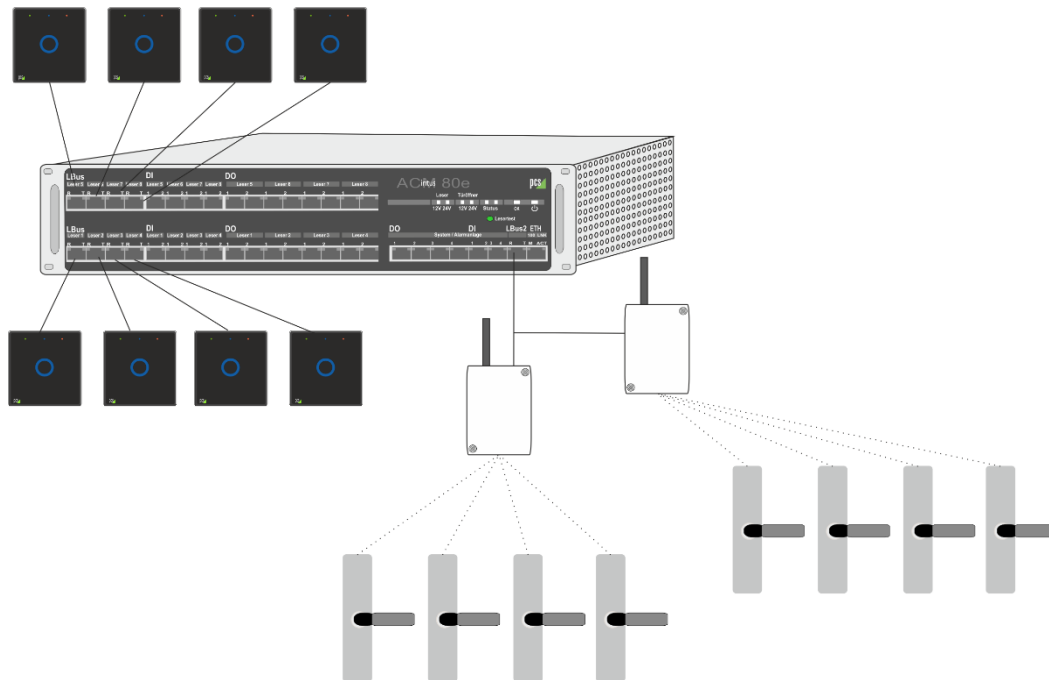


Figure 11-10: ACM80e, 8 INTUS 700/6xx/350H readers and 8 INTUS Flex devices

Setting MP / MP

Wiring LBus 1
☐ Multi-Point
☒ Point-To-Point

Wiring LBus 2
☒ Multi-Point
☐ Point-To-Point

Setting LBus 1 / INTUS 700/6xx/5x0/4x0/1600/1500/350H

LBus 1

Reader type:

☐ not configured

☒ INTUS 700/6xx/5x0/4x0/1600/1500/350H

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☐ OSDP

☒ Easy addressing

Generate key (for PCS-proprietary encryption)

Setting LBus 2 / OSDP

LBus 2

Reader type:

☐ not configured

☐ INTUS 700/6xx/5x0/4x0/1600/1500/350H

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

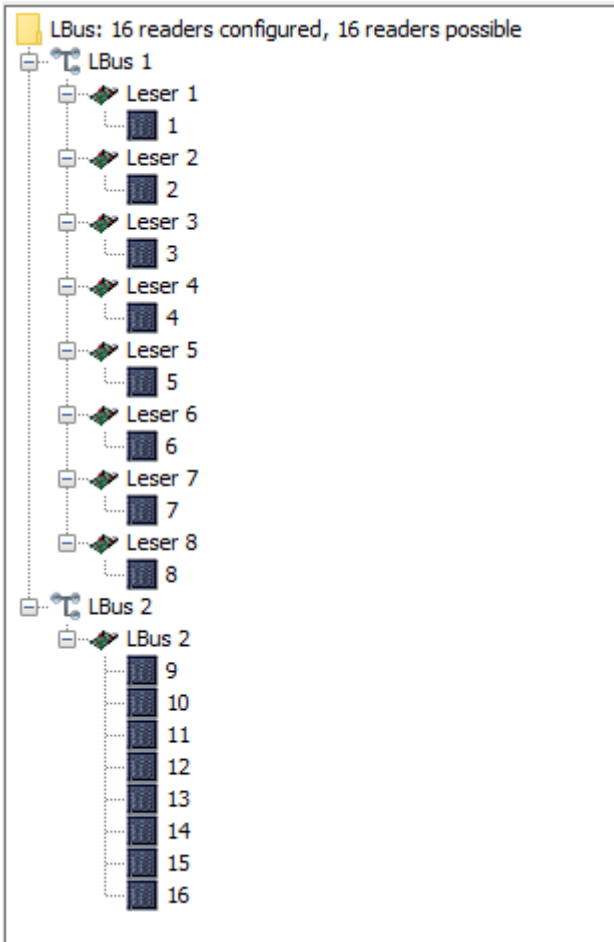
☐ Easy addressing

Generate key (for PCS-proprietary encryption)

LBus 2/LBus 2			
TCL address	HW address	Mode of operation	Encryption
9	1	not configured	☐
10	2	not configured	
11	3	Default mode	all OSDP readers except INTUS Flex
		INTUS Flex	OSDP INTUS Flex only

LBus 2/LBus 2			
TCL address	HW address	Mode of operation	Encryption
9	1	INTUS Flex	☒
10	2	INTUS Flex	☒
11	3	INTUS Flex	☒
12	4	INTUS Flex	☒
13	5	INTUS Flex	☒
14	6	INTUS Flex	☒
15	7	INTUS Flex	☒
16	8	INTUS Flex	☒

Results



11.16 Example - one INTUS 5500/5540/5600 with LBus1 & LBus2

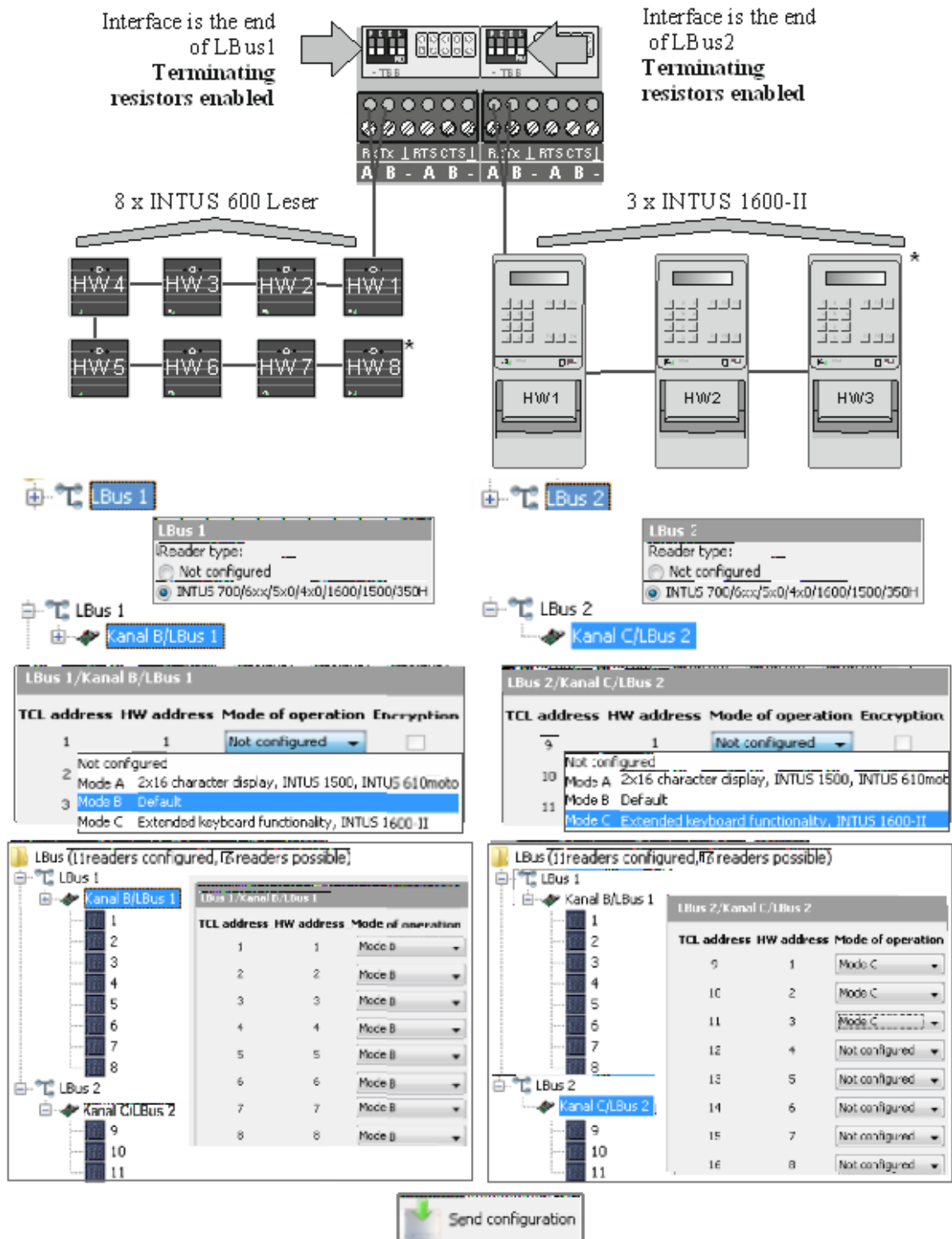


Figure 11-11: One INTUS 5500/5540/5600 with LBus1 & LBus2

The last reader is the end of LBus1 & LBus2: Enable the terminating resistor!



* The reader address (HW) must be set manually to each reader. For more information, please see the Installation Guide of the respective reader.

11.17 LBus AES encryption

Authorization level 3

It is possible to encrypt communication between an LBus reader and the terminal via AES.

11.17.1 Prerequisites

- AES encryption can only be used if supported by the terminal firmware.
- TCL firmware 1.07 and later support this function.
- Further, the reader firmware needs to support AES encryption. This is not valid for reader type Wiegand. Concerning OSDP and INTUS Flex, please see chapter 11.17.8.

11.17.2 Activating AES encryption

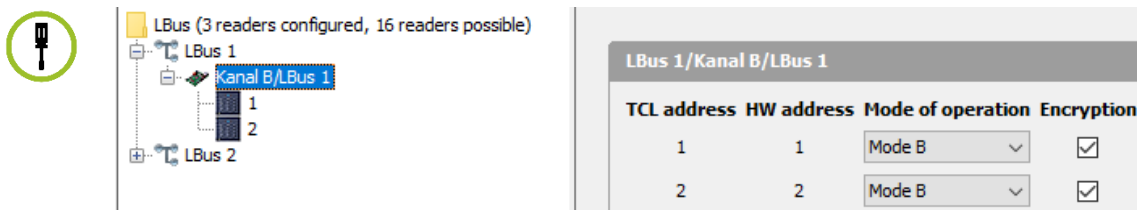


Figure 11-12: Activating AES encryption

- Automatic activation: When establishing communication, the terminal requests from the reader whether it supports AES encryption.
- If the reader supports AES encryption it is automatically activated, even if the checkbox „encryption“ is not marked for this reader.
- By setting the option „Encryption“ at a reader, encrypted communication is forced (either via AES or PCS proprietary – see chapter 11.17.8 ff.).
 - If a reader supports both AES encryption and PCS proprietary encryption, the terminal chooses AES encryption.
 - If the checkbox is activated and a reader doesn't support encryption, the TCL firmware deactivates communication. This means that the reader is no longer active ("KO") and cannot be used for readings.



11.17.3 Configuring the AES key



Figure 11-13: Configuring the AES key

- By default, the TCL firmware uses the so-called device key for AES encryption with a reader.
- Via INTUS RemoteConf, you can load your own customer key to the terminal and the connected readers.

11.17.4 Configuring the customer key



Figure 11-14: Configuring the customer key

- For AES encryption, a new section „Common LBus settings“ was introduced in INTUS RemoteConf V1.05.00.
- Choose your own customer key and load it to the terminal via INTUS RemoteConf.
- The customer key can then be transferred to the connected readers via LBus action "Transfer LBus key to reader" (see chapter 17).

11.17.5 Option AES encryption with customer key only

- There is a checkbox for the option "AES encryption with customer key only".
- The checkbox is not activated: If no customer key is available for a reader, the terminal uses the device key for communication.
- The checkbox is activated: If no customer key is available for a reader, the TCL firmware deactivates communication with this reader, meaning the reader is inactive ("KO") and cannot be used for readings. It is possible, however, to reload the customer key via LBus action "Transfer LBus key to reader"(see chapter 17).

11.17.6 Changing the customer key



Common LBus settings

Customer key for AES encryption: [dots]

☐ show key

☐ keep ☒ change

☐ AES encryption with customer key only

Figure 11-15: Changing the customer key

- The customer key can be changed via INTUS RemoteConf at any time.
- The terminal remembers the last customer key when the key is changed (so-called „old customer key“).
- The new key can be transferred to the connected readers via LBus action „Transfer LBus key to reader (see chapter 17).
- The "old customer key" is deleted by the terminal as soon as all connected readers are using the new customer key.

11.17.7 Removing a customer key



Common LBus settings

Customer key for AES encryption: 00000000000000000000000000000000

☒ show key

☐ keep ☒ change

☐ AES encryption with customer key only

Figure 11-16: Removing a customer key

- The configured customer key can be removed from a terminal/ACM by entering an empty key 00000000000000000000000000000000 (32 times 0) via INTUS RemoteConf.
- Via LBus action „Transfer LBus key to reader (see chapter 17), this empty customer key can be transferred to all readers.

This removes an available customer key from all readers.

11.17.8 AES encryption and OSDP

AES encryption for OSDP readers at a terminal slightly differs from the above-described procedure for general LBus readers:

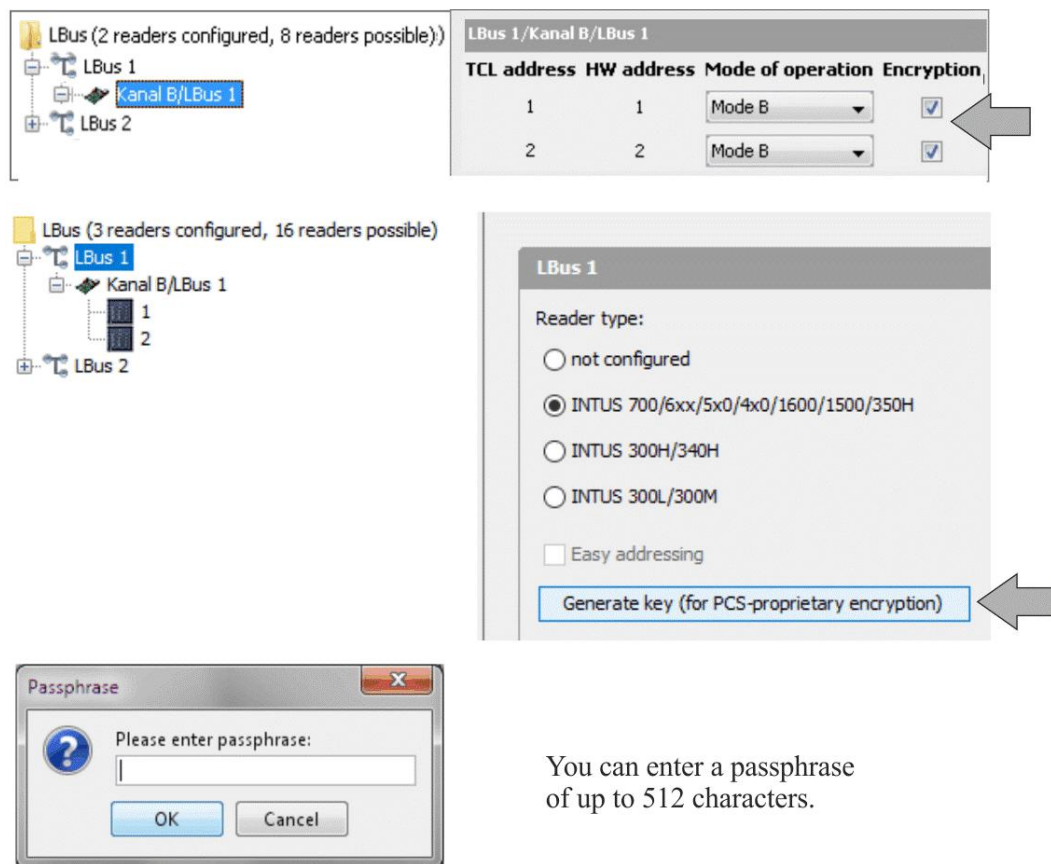
- AES encryption is not automatically activated by the terminal (chapter 11.17.2), but has to be activated explicitly for each reader.
- Since there are no separate „device keys“ for OSDP readers, the terminal uses the key set as „customer key“ in INTUS RemoteConf.
- This is why the setting "AES encryption with customer key only" (chapter 11.17.5) is not relevant for OSDP readers.
- Depending on OSDP reader settings, it may happen that an unencrypted connection or loading of the key via LBus action (see chapter 17) is not supported by the reader.

11.18 LBus encryption (PCS proprietary)

Authorization level 3

You can encrypt the communication between an external reader and the terminal. Since a fixed length is required for the key, a passphrase of up to 512 characters needs to be entered. The key is then created correctly and automatically for facilitating key creation. Currently, encryption is supported by

- INTUS 700/600/620 und INTUS 640H
- INTUS 400/420, INTUS 500/520, firmware version 1.08 and higher,
- INTUS 350H firmware version 1.01 and higher.
- INTUS 1600-II



You can enter a passphrase of up to 512 characters.

Figure 11-17: LBus encryption



Encrypted communication is possible if terminal and reader are encrypted with the same passphrase (key).

If supported by the firmware of the terminal, you are able to load the LBus keys from the terminal to the readers. For more information, see chapter 17.

12 The internal reader

Authorization level 2 / 3

Does not apply to the INTUS ACM



A change of the default setting is usually only required if a barcode reader is connected.

When a barcode reader is installed, it must be activated as "additional barcode reader".



Channel A | Channel B | Channel C | IP configuration | Firewall | **Internal Reader** | LBus | TCL parameter

Reader type: Serial standard

Mode: Default (selected), DNCIN, DNCIN

☒ additional barcode reader

Figure 12-1: Internal reader

Reader type: Serial standard

Reader mode	Comment
Default	Legic® or Mifare® or Hitag® reader with serial connection
DNCIN	Serial reader interface for free use
Default + additional barcode reader	1x proximity reader & 1x barcode reader

Reader type: Clock data (INTUS 5320)

Reader mode	Comment
Omron – code identifier X	Reader with Omron emulation; TCL code identifier „X“
Omron - code identifier Y	Reader with Omron Emulation; TCL code identifier „Y“
Omron - code identifier Z	Reader with Omron Emulation; TCL code identifier „Z“
Barcode (Wand emulation)	Barcode reader

13 TCL parameters

Authorization level 2 / 3



Channel A	Channel B	Channel C	IP configuration	Firewall	Internal Reader	LBus	TCL parameter	Hardware	Logir
Settings <i>Default setting</i>									
Table field [Byte]: 49152 ☐ Save buffer records with record number Number of labels: 1024									
Save buffer [Byte]: 49152 ☒ Load default TCL program on cold boot									
Ack timeout [s]: 26 Size BMI field [byte]: ☒ 88 ☐ 115 Character encoding: ISO8859-1									
Extended user interface <i>Default setting</i>									
TCL binding: table field									
Start offset: 0 Length of field to be synchronized 0									
INTUS Sound <i>Default setting</i>									
Volume [%]: 70									

Figure 13-1: TCL parameters

13.1 Settings

Table field

Default setting is a TF field size of 49152 bytes (48kb).

Save buffer

Default setting is an offline buffer size (\$4 circular buffer) of 49152 bytes (48 kb).



Note that the table field and the offline buffer size should not exceed the capacity of the available SRAM configuration. If the sum of the values exceeds the available SRAM, both the operating parameters will be reduced to their default value of 49152Byte.

Therefore, following a reset, you should check whether your settings have been accepted.

Ack timeout

The logical acknowledgement time defines the period of time within which a record from the offline buffer must be acknowledged by the host; it can be set to a value between 2 and 230 seconds. The default value is an acknowledgement period of 26 seconds. In the TCL system, the acknowledgement period is used to control the MONOUT process via the P3 field.

Save buffer records with record number

If you select this checkbox, a logical record number will be added automatically to the records from the offline buffer. If it is deselected, no logical record number will be prefixed. Further information on the structure of data records from the offline buffer can be found in the P20+22,1 and P10 fields, please see the TCL Programmer's Manual.

Load default TCL program on cold boot

If you deselect this checkbox, the default program will not be executed during a cold boot or ice-cold boot. In this case, the load request '77' will not be sent to the host either.

The default setting is Yes and should not be changed.

Size BMI field

This option allows you to change the size of the B, M, and I fields from the default value of 88 characters to 115 characters (no checkmark in the box), if the readers return records of more than 80 characters.

The default size is 88 characters and should not be changed.

Number of labels

This option allows you to set the number of jump destinations (= labels) in a TCL program to a value between 512 and 4352. The default value is 1024.

Note that each jump destination occupies 4 bytes of SRAM storage. If there is no need for a large number of jump destinations, you should not set an excessively large number for the labels here because the corresponding storage will not be available for the TF field, offline buffer, and TCL program memory (DL).

Character set

If a display is available, you can select the character set that will be preset in the display. The default value is ISO 646 – GERMANY.

13.2 Extended user interface

You can define a range for additional INTUS Graph information. TCL provides this range to INTUS Graph.

Normally, this setting is entered directly in the TCL program.

13.3 INTUS Sound

Authorization level 1 / 2 / 3

The volume of the sound module (option) can be adjusted.

14 Hardware



Figure 14-1: Hardware

14.1 Display

Display contrast

The display contrast for the INTUS 3150/3155/5320/5500 is optimally adjusted by PCS. However, external influences may make it necessary to readjust the setting.



The default setting is 21; the highest possible contrast is 64.

Backlight saver

If the backlight saver function is enabled, the backlight is dimmed after an hour of inactivity (INTUS 5320).

14.2 Magic-Eye (INTUS 5320 only)

Blue brightness: Adjust the brightness of the blue MagicEye LED. Value range is 0-15, default setting is 9.

Brightness is regulated in 3 steps: Off (value 0), normal (values 1 to 9) and high (values 10 to 15).

14.3 Buzzer



You can set the frequency of the buzzer in the range of 300 up to 6000 Hz.

15 Login - Maintenance Group and Password Change



Data port (Channel A) | Channel B | Channel C | Channel D | IP configuration | Firewall | LBus | TCL parameters | Hardware | **Login** | Time

Login

Maintenance group:

The documented default value is currently active on the device!

Password authorization level 1:

☒ show password

The documented default value is currently active on the device!

Password authorization level 2:

☒ show password

The documented default value is currently active on the device!

Password authorization level 3:

☒ show password

The documented default value is currently active on the device!

Options

☒ Allow IP setup via UDP maintenance port

The IP setup is a convenience function exclusively for commissioning and should be deactivated afterwards for security reasons

☒ Allow AutoClone service connection

Figure 15-1: Login



Once the maintenance group or the password have been changed and sent, the display Security setting has documented default value is faded out.

This warning indicates that by changing passwords and maintenance group, the terminal is more secure against unauthorized access.

15.1 Maintenance group

On authorization level 3 you can define a maintenance group.



The value margin is 0 to 65535.

The default setting assigns the device to maintenance group 0.



Always make a note of the maintenance group.

15.2 Changing the password for authorization level

Password changing depends on the authorization level.

On authorization level 3, you can change the password for all levels.



Please make a note of any password change.

16 Time



Figure 16-1: Time

16.1 NTP Client

The terminal now optionally supports synchronization of date/time via NTP (Network Time Protocol). By default, NTP time synchronization is off.



NTP server 1 or NTP server 2: An IP address or a host name can be indicated. NTP time synchronization is activated if the option "from DHCP" is activated and/or a value is set for NTP server 1 or NTP server 2.

From all configured time servers (via DHCP or via INTUS RemoteConf), the most suitable server is chosen for synchronization.



NTP always uses UTC time. It is thus recommended to configure the deviation from UTC time and daylight saving time accordingly.

16.2 UTC offset – Deviation to UTC time

UTC (UTC – world time) is used as a basis.



For a deviation between local time and UTC, enter the direction (eastward or westward) and the number of hours. This value refers to winter time. A positive value means west of UTC, a negative value (with preceding '-') means east of UTC.

Example: Local time in Germany → UTC: Currently (as of 2021) 1 hour east of UTC. The value of "-60" has to be entered as deviation.

16.3 Daylight saving time switch-over



If daylight saving time (DST) switch-over is to be performed automatically by the terminal, you have to set the DST start and end dates in POSIX TZ format.

The POSIX TZ format **Mm.w.d/h** specifies the switching instant as day d of the week w in the month m at hour h.

The day d must be between 0 (Sunday) and 6 (Saturday).

The week w must be between 1 and 5. Week 1 is the first week, in which the weekday d appears. Week 5 selects the last week, in which the weekday d appears. The month m can be adjusted between 1 and 12, the hour h between 0 and 23.

Currently (as of 2021), the following applies to Central Europe:

Start of the daylight saving time: **M3.5.0/02** (last Sunday in March at 2 am)

End of the daylight saving time: **M10.5.0/03** (last Sunday in October at 3 am)

The complete POSIX TZ string for Central Europe is thus:

CET-1CEST-2,M3.5.0/2,M10.5.0/3

17 LBus actions

Authorization level 2 / 3

17.1 Overview

This function enables the terminal, or the ACM, respectively, to perform certain actions on the internal reader, or readers connected via LBus. Several terminals can be selected before the button "LBus action" is clicked on. In this case, the LBus action is simultaneously sent to the selected terminals and the action is performed.



If an LBus action is performed on several terminals, the readers that are not connected to a terminal are left out without error warning.

If the "LBus actions" button is inactive, the terminal firmware does not support LBus actions.



Procedure:

- 1 Push the "LBus actions" button to start.
- 2 Select one of the four actions, or composing a sequence of actions

The action "Custom reader settings configuration" cannot be included in a sequence of actions.



"Custom reader settings configuration" cannot be activated, if more than one terminal is selected.

- 3 Click on „Next“.

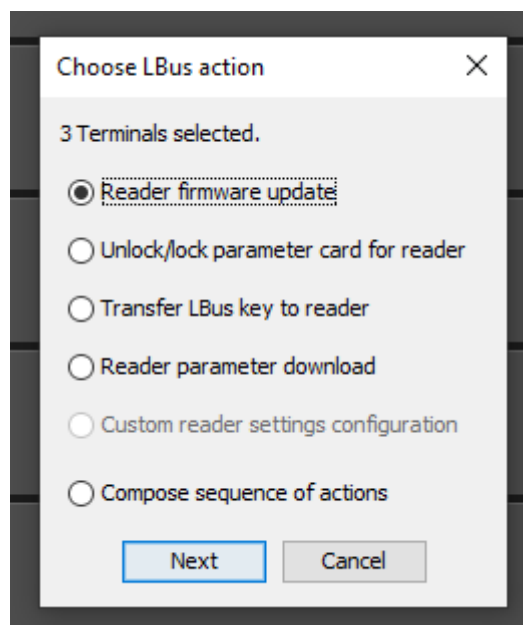


Figure 17-1: Select LBus action(s)

- 4 Select the readers you wish to perform the action on. Depending on the action, further settings may be required. Please see the following chapters.

- 5 After having pushed "Start", the action is performed on each selected reader. While the terminal is performing the LBus action, INTUS RemoteConf shows a status view.
- 6 After the action has been completed, an overview is displayed.

17.2 Action "Reader firmware update"

It may be necessary for certain reasons to update the firmware of the readers connected to the terminal.

The PCS Technical Support provides a file with reader firmware for you individually.



- 1 Select an IRFW file via "Choose IRFW file".
- 2 Select the reader the firmware of which is to be updated.



After the reader firmware was updated from 4.x or 5.x to version 6.x, the reader always has to be reconfigured. This is done via a VX parameter card or via INTUS RemoteConf using an IRPA file (see chapters 17.5 and 17.7).

17.3 Action "Unlock/lock parameter card for reader"

This action executes enabling/disabling of the function „Lock/unlock parameter card“ (see manual “Parameterizing with parameter card”, order No. G3000-21). This enables local enhancement or changes of reader parameters. The parameter card is provided by PCS.



- 1 Select whether you want to lock or unlock.
- 2 Select the reader of which the parameter card is to be locked or unlocked.

17.4 Action "Transfer LBus key to reader"

This action enables transfer of the LBus keys from the terminal to the reader. Also see chapters 11.17 and 11.18.



Select the connected readers to which the keys are to be transferred.



Key transfer is only required at start-up or after changes of the key.

17.5 Action "Reader parameter download"

It may become necessary to configure the readers connected to a terminal via INTUS RemoteConf.

Instead of using a parameter card, a reader parameter download can be performed. For this action, TCL firmware version 1.10.00 or later is required.

PCS Technical Support provides you with an IRPA file for reader parameter download. This file contains the parameters (e. g. VXD) for INTUS readers.

Further, PCS Technical Support will give you an individual IRPA file password for this file.



- 1 In INTUS RemoteConf, select the file via "Choose IRPA file", and enter the IRPA password in the respective field:

The screenshot shows a dialog box with the following elements:

- A text field containing "VXD00-001.02.irpa".
- A button labeled "Choose IRPA file...".
- A label "IRPA file password:" followed by a password input field filled with dots.
- A checkbox labeled "show password" which is currently unchecked.
- Two buttons at the bottom: "Start" (highlighted with a blue border) and "Cancel".

- 2 Select the readers you wish to configure.

The terminal decrypts the data in the IRPA file with use of the IRPA file password, then loads the decrypted parameter data to the selected readers.



After successful parameter download, the functions of parameter cards are blocked for these readers. If required, they can be reactivated any time via LBus action "parameter card" (chapter 17.3).

17.6 Action "Custom reader settings configuration"

Via this dialog, further settings for the connected readers can be configured.

There is a tab for each connected reader. The settings can be entered separately for each reader. Via the button "Send configuration", the settings are transferred to the terminal/ACM.

The screenshot shows the 'Custom reader settings configuration' dialog for 'Reader 1'. The dialog is organized into several sections, each with a title bar and a close button:

- General actions:** Contains two checkboxes: 'Disable administration of custom reader settings' and 'Reset custom reader settings to readers default settings'.
- Reader identification:** Contains a 'Display name' text field (value: 'Main entrance') and a 'Usage' dropdown menu (value: 'Access / Door').
- Mobile Access:** Contains four dropdown menus: 'Mobile Access Mode' (value: 'Wake-Up'), 'Wake-up sensitivity' (value: 'high'), 'BLE range [Min. RSSI, dBm]' (value: '-42'), and 'Access result' (value: 'OK/NOK').
- Apple Wallet:** Contains an 'Authentication mode' dropdown menu (value: 'Express').
- Tamper contact:** Contains a 'Sensitivity' dropdown menu (value: 'Not available').
- Frequency:** Contains two dropdown menus: 'Buzzer frequency' (value: 'Not available') and 'Key tone frequency' (value: 'Not available').
- Brightness:** Contains a 'Keyboard brightness' dropdown menu (value: 'Not available').

Figure 17-1: Custom reader settings configuration

17.6.1 General actions

Reader settings made in RemoteConf are saved to ACMs and terminals. When a reader connected to a terminal/ACM is replaced, the saved settings are loaded to the new reader. If this is not wanted, loading of those settings can be avoided by activating the checkbox "Disable administration of custom reader settings":



Activate the checkbox "**Disable administration of custom reader settings**" and click on "Send configuration". The reader settings are deleted in the terminal/ACM.

- 1 Unplug the reader you wish to replace, and connect the new reader.
- 2 Deactivate the checkbox, so that the ACM/terminal can load and save the settings of the new reader.



Do not activate the checkbox if a reader is to be replaced while keeping the settings of the old reader.

By activating the checkbox **"Reset custom reader settings to default reader settings"**, all settings made in this dialog are reversed.

17.6.2 Setting mounting site-specific parameters

Via the sections **"Reader identification, Mobile Access, Apple Wallet, Tamper contact, Frequency, Brightness"**, site-specific parameters for the readers can be set. Move your mouse over one of the info icons for further information on the settings.

17.7 Compose sequence of actions

In order to ease work, several actions can be composed to a sequence. This way, you don't need to wait at the computer, e. g. until a firmware update is finished, before starting parameter download as another action. Actions of a sequence are processed one after the other by all terminals.

Initially, the list of actions is empty. By adding actions, it can be filled step by step.

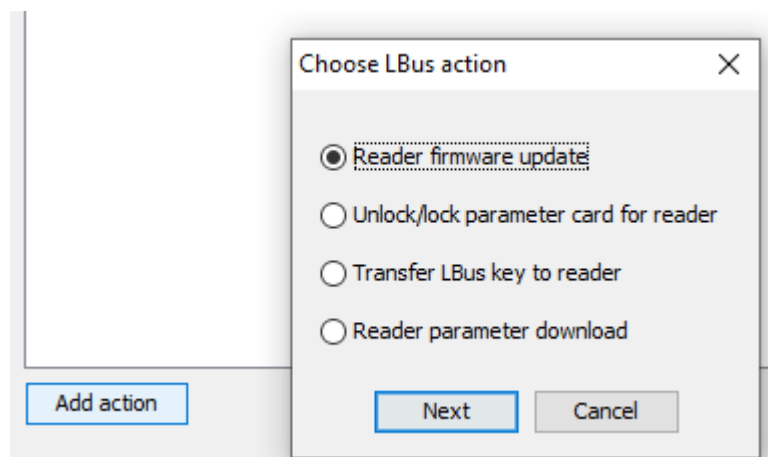


Figure 17-2: Sequence of LBus actions

Each action is processed one after the other by each terminal. Once an action is terminated for all selected readers, the next action is started.

The list may contain up to 99 actions. For each action, readers can be selected individually.

If an error occurs during an action at one of the readers, further actions are not processed at this reader.

Example 1:

For readers 1-8, a firmware update is performed, then parameters are loaded:

Compose sequence of actions

Action	Detail	Readers
1 - Firmware update	INTUS_Leser_Firmware_V6.12.irfw	1-8
2 - Parameter download	VXD00-999.00.irpa	1-8

Example 2:

Example 1 was altered in a way that readers 1-4 are processed, then readers 5-8:

Compose sequence of actions

Action	Detail	Readers
1 - Firmware update	INTUS_Leser_Firmware_V6.12.irfw	1-4
2 - Parameter download	VXD00-999.00.irpa	1-4
3 - Firmware update	INTUS_Leser_Firmware_V6.12.irfw	5-8
4 - Parameter download	VXD00-999.00.irpa	5-8

18 Service actions for INTUS Flex Air

Authorization level 2 / 3

The following actions for INTUS Flex Air are described below:

- Modifying the base address of the INTUS Flex Gateway
- Pairing of INTUS Flex devices onto a INTUS Flex Gateway
- Removal of INTUS Flex Devices from a INTUS Flex Gateway
- Activating the service mode of the INTUS Flex Gateway

View of the current Flex configuration

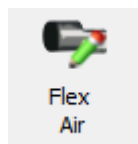


Figure 18-1: Flex Air

The button "Flex Air" takes you to the complete view for the Flex configuration. In this view, the LBus configuration of the ACM is displayed, as well as the currently connected gateways and the INTUS Flex devices connected to the gateways.

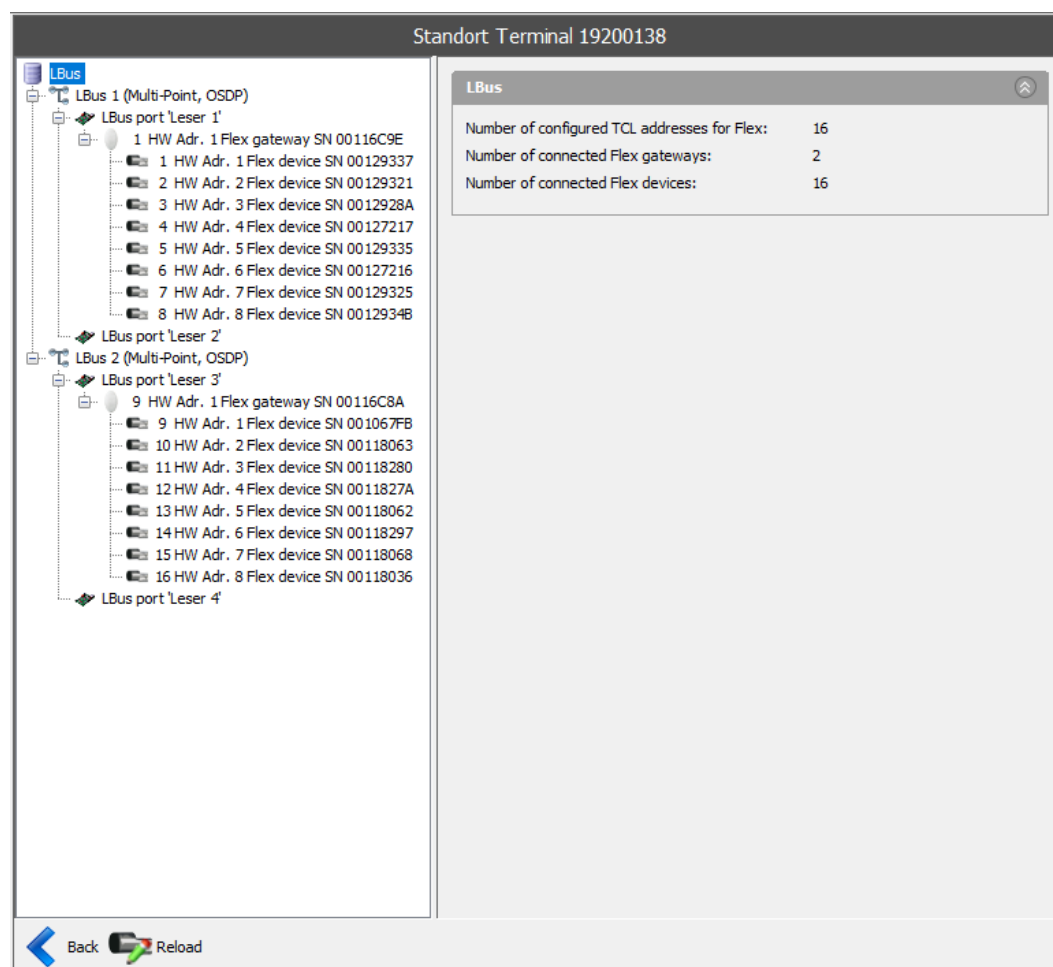


Figure 18-2: View of the Flex configuration

In this example, one ACM40e with 16 Flex devices is configured on two gateways. Here, the two gateways are connected to an ACM and are displayed. RemoteConf has already been used, to connect 16 devices to the gateways.

Changing the base address

To change the base address, all Flex devices must be decoupled. The change of the base address is normally only necessary when you are configuring the gateway for the first time.

To start the process, select a gateway and select the option "Change base address".

Make sure that no devices are connected to a gateway, otherwise the process cannot continue and an error message will be displayed.

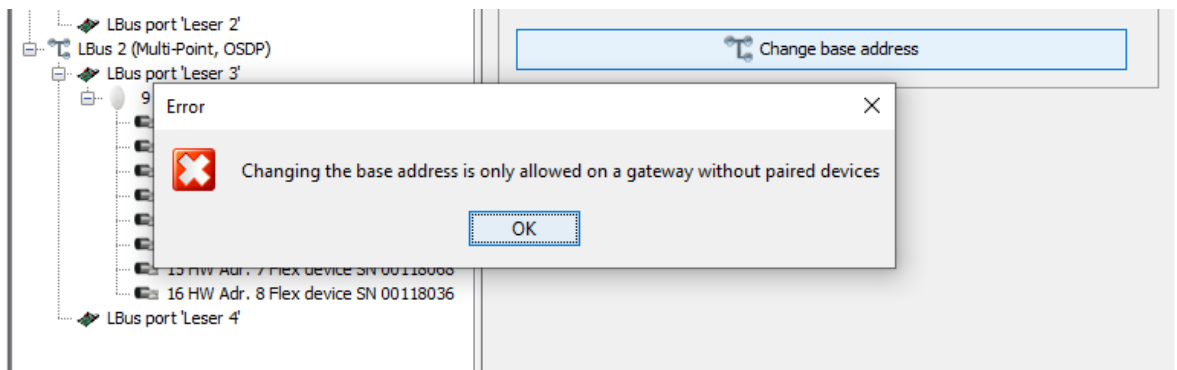


Figure 18-3: Error message - Change base address

When operating multiple gateways on one LBus-Port, ensure that they are configured onto different base addresses, otherwise not all gateways are addressable and can therefore not be displayed.

Remove INTUS Flex devices from INTUS Flex gateway

To remove Flex devices from a gateway, select a Flex device and select the option "Remove flex device from gateway".

In the overall view, a cylinder icon is used for all devices.

In Figure 18-4, the third Flex device (Address 11) has been selected and after confirming the Flex action, the process for removing the device can be completed.

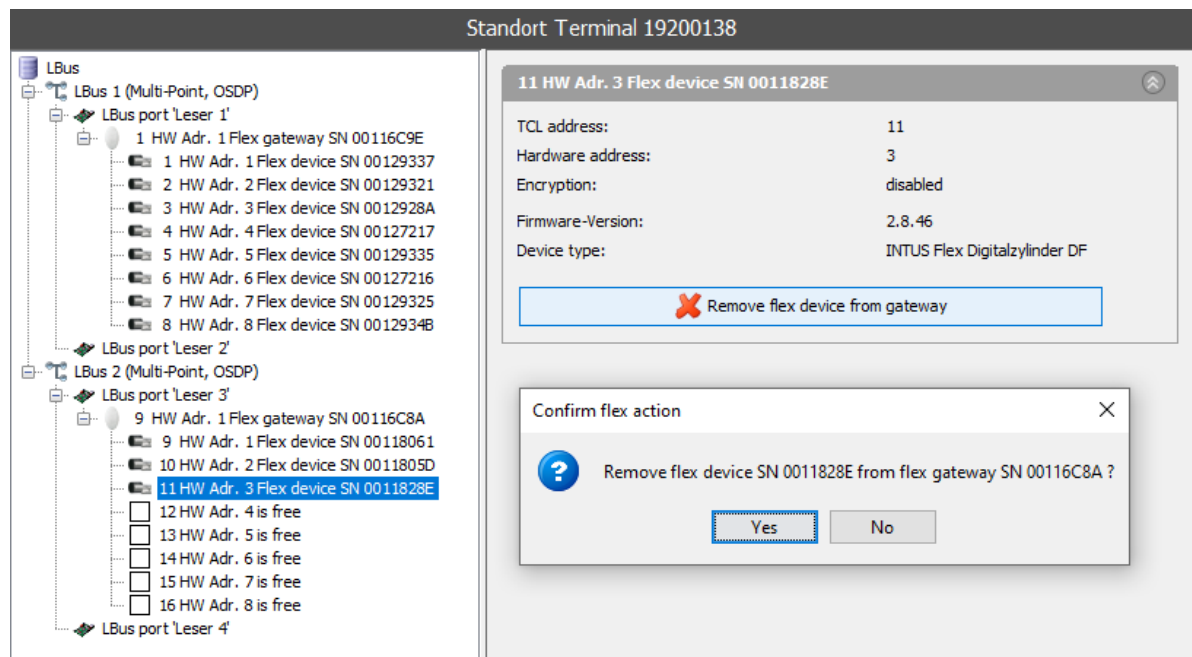


Figure 18-4: Remove flex device from gateway

Pair INTUS Flex devices to INTUS Flex gateway

To pair Flex devices to a gateway, select a free address (white rectangle) and select the option "Pair Flex device".

Before confirming the Flex action to complete the process, hold the service card to the Flex device first.

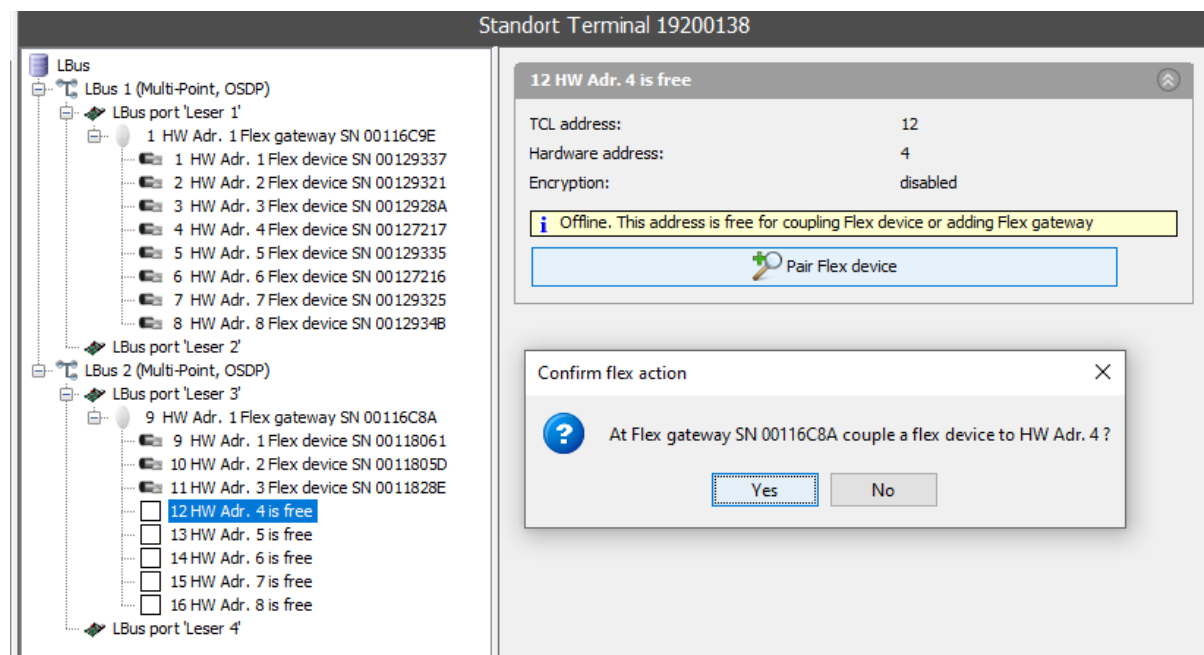


Figure 18-5: Pair Flex device

Modifying the base address

In the following example, a gateway is connected to LBus 2 with the HW-address 9. No other Flex devices are paired. To modify the base address, select a free address. In this example in Figure 18-6, the free address 13 is selected.

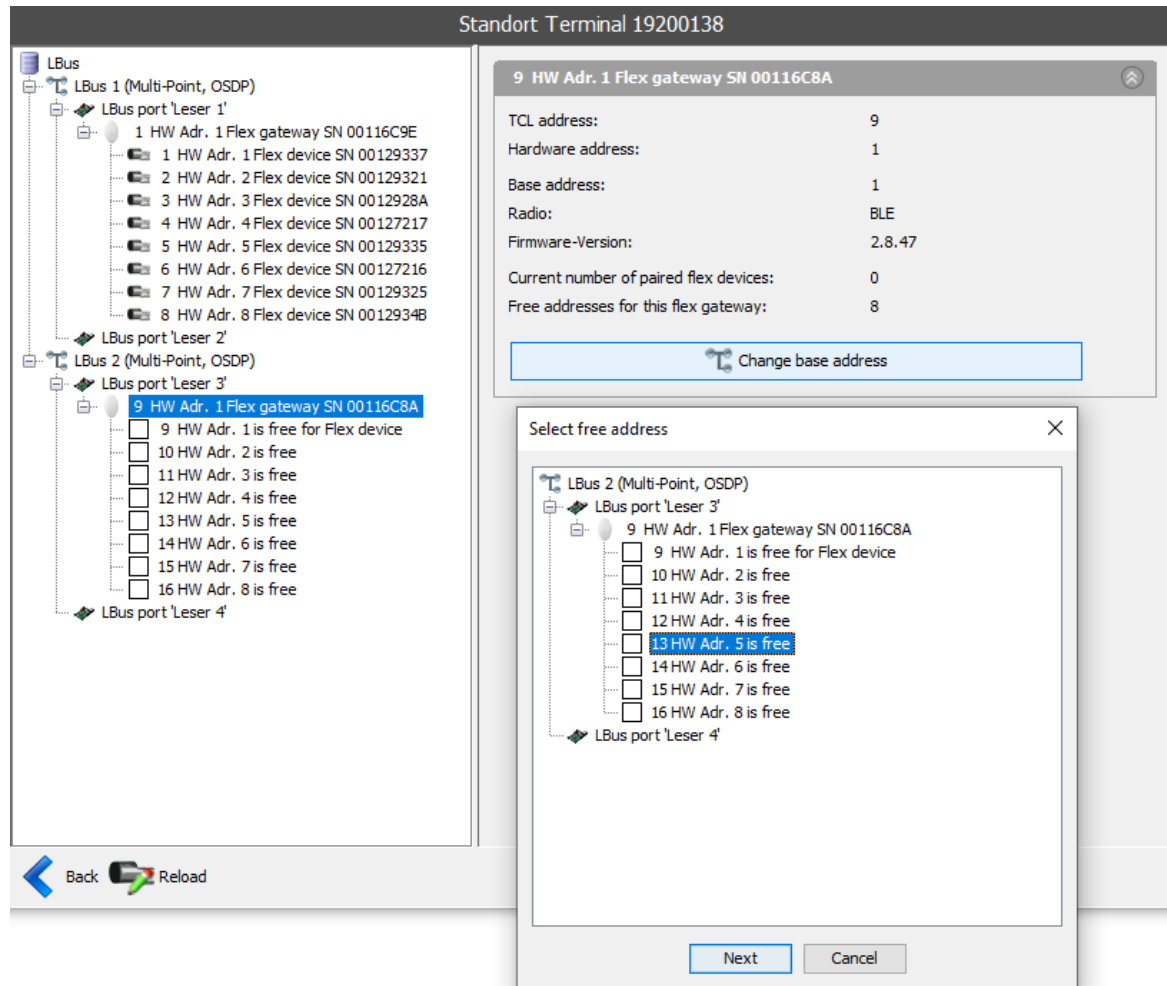


Figure 18-6: Select free address

Modifying the base address with changing the LBus-Port

For this example, the L-Bus configuration has been adapted. LBus 2 is now divided into four readers on port 3 and into four readers on port 4.

To change the gateway from address 9 (Port 3) to address 13 (port 4), proceed as follows:

- Select the applicable configuration, as shown in Figure 18-6 and click "Next" to continue.
- A note is displayed, that the gateway must also be connected to the other port when the changes are made. To complete the process press "yes".

After following these steps, the gateway with address 9 is successfully changed to port 3 (address 13). You can now connect another gateway on address 9, if required.

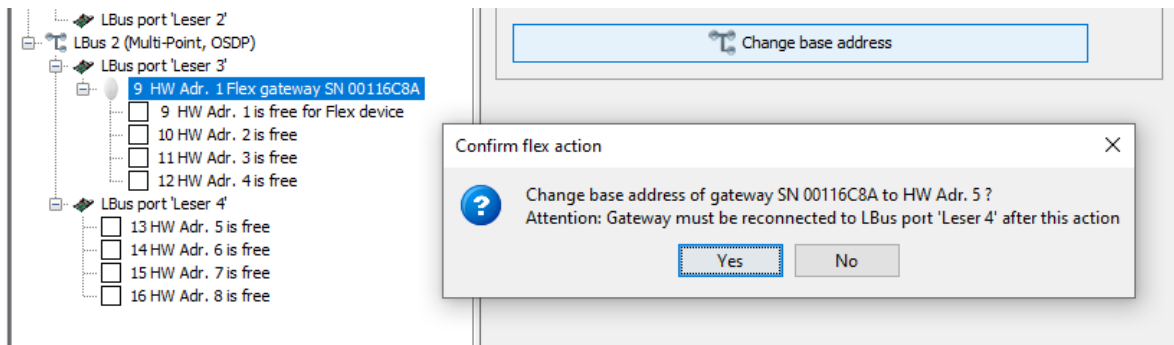


Figure 18-7: Note change base address

The gateway has now been reconfigured to address 13 (HW address 5) but not yet reconnected to the ACM. It is therefore not visible (offline).

It is visible as soon as the gateway is reconnected and the process is complete.

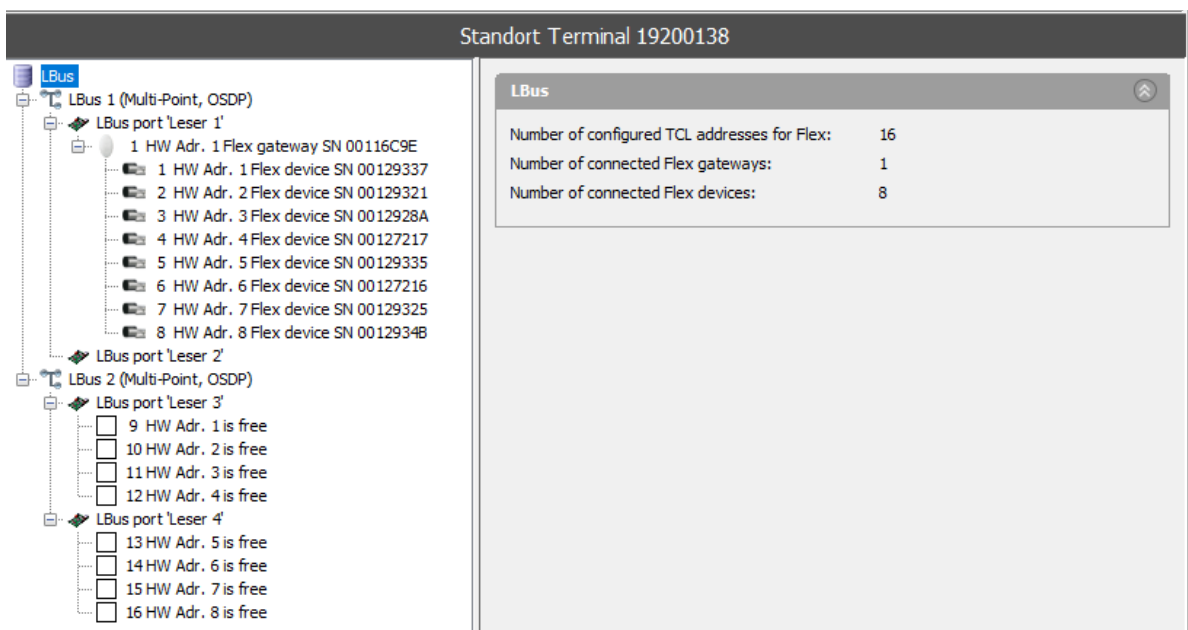


Figure 18-8: Base adresse modified

Activating the service mode of the INTUS Flex Gateway

To activate the service mode of the INTUS Flex Gateway select the Gateway and select the option "Activate service mode".

The Flex Gateway is set to service mode. Details on the service mode can be found in the INTUS Flex Gateway manual (G3800-615).

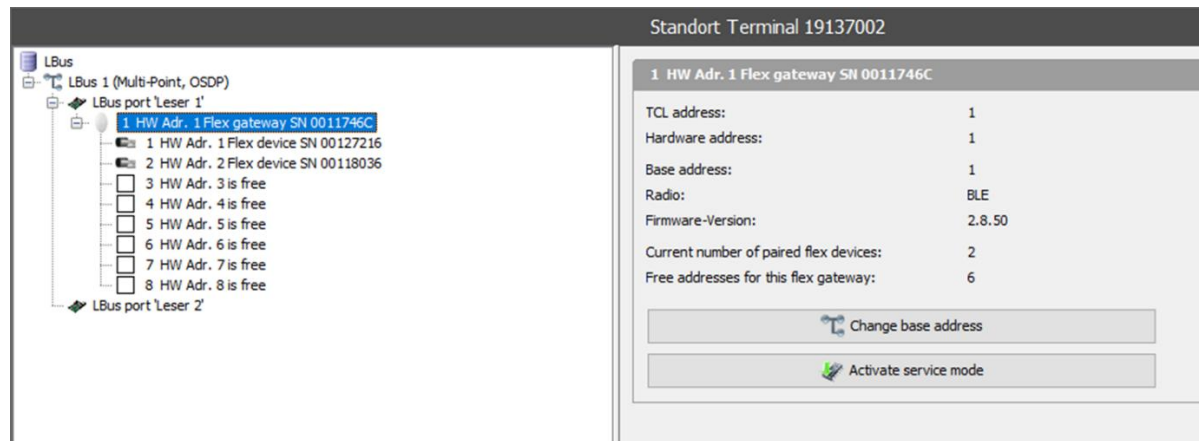


Abbildung 18-1: Activate service mode

19 Reset

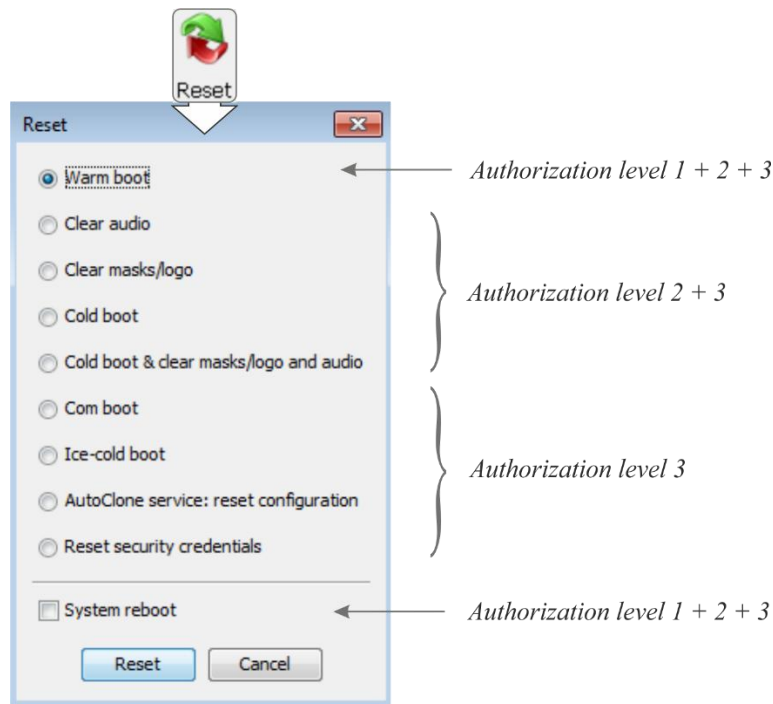


Figure 19-1: Reset

	Warm boot	Cold boot	Com boot	Ice-cold boot
TCL application variables offline buffer	Are preserved	Are cleared	Are cleared	Are cleared
TCL parameters	Are preserved	Are preserved		
TCP/IP parameters	Are preserved	Are preserved	Are preserved	
Audio, masks logo	Are preserved	Are preserved	Are cleared	
Default program	Loaded if no TCL application is available	Loaded	Loaded	Loaded

If a critical system parameter is changed, such as the size of the table field or offline buffer, a cold boot is carried out automatically.



By means of an ice-cold boot you can establish a defined state for the terminal if it does not function correctly.

AutoClone service

This option is only available if the INTUS COM software is used.

Reset security credentials

The configuration of WiFi, IEEE 802.1X and HTTPS client is reset concerning certificates, user names, and passwords. This may be used for deleting internal information from devices before sending them in to PCS Service. Security credentials are also deleted after an ice-cold boot.

20 Upload Logo

Authorization level 2 / 3

Valid for INTUS 5200 & INTS 5205

Valid for INTUS 5600, if the loaded masks allow



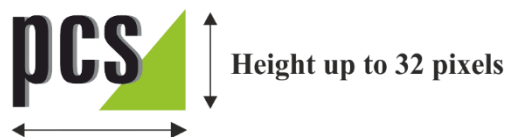
Figure 20-1: Logo upload

The following conditions must be met for a logo to be loaded in the upper right side of the display:



Size of the logo at INTUS 5200 & INTS 5205

At the TPI standard masks (VIG 10-001) for TPI 3.7



Width up to 70 pixels, the data field on the display appears without restrictions

Width up to 100 pixels, the data field on the display is partially overwritten, only shortened weekdays are displayed

Size of the logo at INTUS 5600

Depends on the mask layout.

File format of the logo



21 Serial interfaces



In exceptional cases, the protocol TTY or BSC protocol are required for a serial interface; it can be set via channel A / B / C / D.

21.1 Basic settings TTY/BSC

Baud rate

Depending on the device type, not any baud rate can be set. Possible baud rates are:

1200 / 1800 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200

Data format

Depending on the device type, not any data format can be set.

Date bits: 8 / 7

Parity: none = no parity bit, even = even parity, odd = odd parity.

Buffer size

Receive buffer (byte) / transmit buffer (bytes)

21.2 TTY protocol

TTY is a character stream mode with configurable flow control. The TTY character stream mode includes the following sublevels:

Hardware flow control: Select None or RTS/CTS to define whether or not the terminal is to conform to the RTS/CTS protocol during transmission.

Send

Contains the following parameters for defining the behaviour during the transmission of a character or during the handshakes:

Software flow control (XON/XOFF) enabled: The terminal is to conform to the XON/XOFF protocol during transmission.

Process enabled: Activates the following settings:

CR to EOL: The end-of-line character CR ("0D") is to be translated into other characters.

EOL: You can choose two end-of-line characters which have to be set separately using hexadecimal values. If you set 00 for the second character, CR is translated into one end-of-line character only.

Reception

Contains the following parameters for defining the behaviour during the reception of a character or during the handshakes:

Software flow control (XON/XOFF) enabled: The terminal is to conform to the XON/XOFF protocol during reception.

Process enabled: Ignore EOL enabled: The end-of-line character will not be stored in the input buffer.

EOL 1: Choose the first of two possible end-of-line characters to be used by the host. The EOL character is represented by a hexadecimal value.

Ignore char enabled: You can set the character to be suppressed in hexadecimal format.

EOL to CR enabled: The end-of-line character used by the host is translated into CR ("0D"), the end-of-record character used in TCL. The EOL character used by the host can be configured under EOL 1 and EOL 2.

EOL 2: Allows you to set a second end-of-line character in hexadecimal format. If you set this value to 00, only one end-of-line character is expected and translated into CR.

Erase char: It enables you to suppress certain characters which interfere with TCL (e. g. because of EOL characters or character sets used by the host). You can specify a character (in hexadecimal format) that is used to delete a preceding character. This only makes sense during interactive operation of the terminal. For all other purposes, the value should be set to FF.

EOF / Counter: You can set a hexadecimal character value specifying the number of characters which will be waited for during the delay set under EOL 1 before being passed on.

21.3 BSC protocol

BSC is a packet-oriented protocol that supports protected data transfer. If you select the BSC protocol for a serial interface, the BSC driver is enabled in its slave form.

Group ID / Device ID: Address for the terminal between @ and Z

Poll Timeout (s): Period of time (seconds in decimal format) which may elapse between two poll activities on the partyline before the BSC protocol reports an offline state to the TCL system (which subsequently sets the PO flag). This period of time must elapse after a partyline failure before the offline state is detected.

Data Timeout (ms): Period of time that may elapse from the reception of the first character of a data block to the reception of the last character of the same block (in 100 ms units).

Send delay (ms): Allows you to set a transmission pause (in milliseconds) during which the partyline is to be idle after a protocol telegram was received. This idle period is required to perform the transmit receive switchover on a two-wire partyline and to suppress any PAD characters.

Acknowledge Timeout (ms): Allows you to set a period of time (in units of 10 milliseconds) during which a response is expected from the remote station after a protocol telegram was transmitted.

Number of pad characters: Allows you to set the number of PAD characters appended to a protocol telegram to a value between 0 and 9.

At least one PAD character is required for a two-wire partyline because of the necessary receive-transmit switchover. Additional appended PAD characters may be required for a complex partyline structure involving intermediate stations (bridges and routers).

The default setting is 1 PAD character.

It should not be taken for granted that the receive station will actually receive the PAD characters or that no additional PADs will be appended for driver or line reasons.

Also, the receive station should be able to equally process PAD characters with 7F and with FF hexadecimal coding. The transmit delay (see above) should always be set in such a way that an additional PAD character can be tolerated beside the set PAD characters.

If the BSC driver detects that settings fail to make sense, the settings are automatically corrected. To check if a setting was accepted as specified after a reset, you should perform a second reset via the Reset: Yes menu option and then check the setting in the Setup.

EOL: Select the sentence ending mark. The default setting is 00

22 Requirements for firewall settings in network

The operation of the terminal in network can be separated in three categories:

- Standard operation (download of master data, upload of booking data, if necessary)
- Status request (particularly HTML status page)
- Maintenance (configuration change, firmware update)

For these functions, different TCP/UDP connections are required which are documented in this appendix.

In addition, the common ports for DHCP, DHCPv6, Ping (ICMP, ICMPv6) are required, if necessary.

TCP connections are reporting the direction of connection establishment only.

It is assumed that further data packets are accepted (stateful firewall).

Configuring the data port, you can set the direction of connection establishment (standard = passive) and the port number (standard = 3001).

Connection establishment	Protocol	Source port	Destination port	Note
Host → Terminal	TCP	*2)	<as configured>4*)	Connection establishment passive or passive/RAS
Terminal → Host	TCP	*3)	<as configured>4*)	Connection establishment active
PCStatus request → Terminal	TCP	*2)	80	
PCMaintenance ↔ Terminal	UDP	57005	57005	
	UDP	48879	57005	
PCMaintenance → Terminal	TCP	*2)	3121	

1) Terminals supporting IPv6 only

2) Selected by the operating system; depending on used software, possibly limited

3) Selected by the terminal

4) Configuration > Channel A > TCP settings > Port

23 Error diagnostics

23.1 Reader action test

This test serves for checking the functionality of the device hardware and the connected external readers (good/faulty readings).

23.1.1 INTUS 3x and 5x

A reader action test can be performed directly on the device in local setup via "Test> Reader action". Please see the manual "INTUS Local Setup".

23.1.2 INTUS 5540

Via the download link in chapter 1.2 you will find a program for testing the connected readers.

23.1.3 INTUS ACM80e

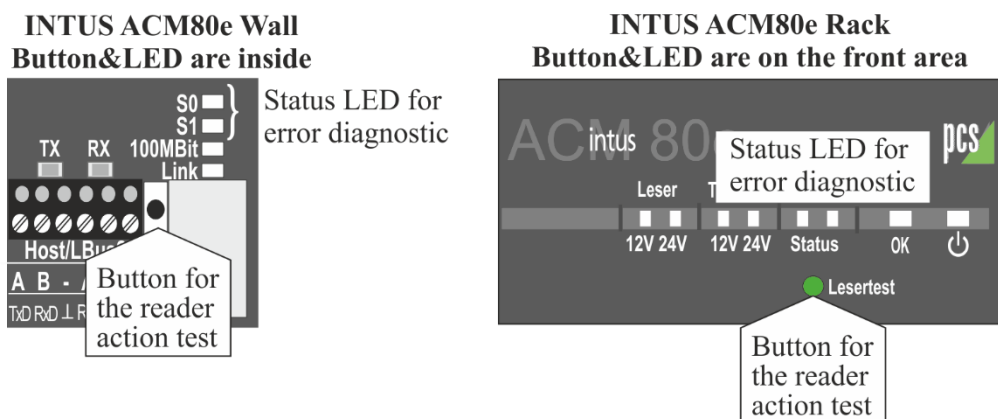


Figure 23-1: Reader action test, INTUS ACM80e

Start the reader action test as follows

Disconnect the INTUS ACM80e from power supply.

Re-connect the INTUS ACM80e to power supply, and immediately press and hold down the "Reader test" button until there are two short beeps.

After a short while, the status LEDs begin to blink. The device is now in reader action test mode.

Each reader is activated, each reading is displayed:

- **Good reading**, the relays at the reader and the relays inside the device are activated for three seconds. The green LED and the buzzer are activated at the reader.
- **Bad reading**, the red LED and the buzzer are activated at the reader.

To terminate the reader action test:

Disconnect the INTUS ACM from power supply and re-connect it to power supply.

23.1.4 INTUS ACM40e

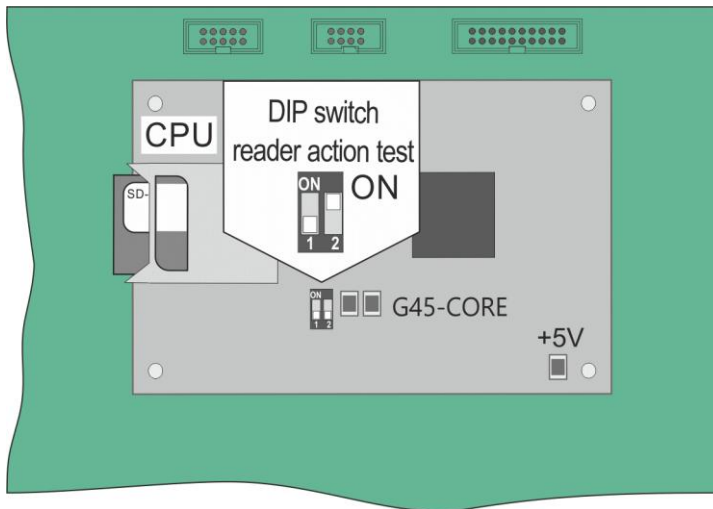


Figure 23-2: Reader action test, INTUS ACM40e

Start the reader action test

Disconnect the INTUS ACM40e from power supply. Set the right DIP switch (2) on the CPU to ON and switch on the ACM40e. Wait till the device is ready to operate. The device is in reader action test mode.

Each reader is activated, each reading is displayed:

- **Good reading**, the relays at the reader and the relays inside the device are activated for three seconds. The green LED and the buzzer are activated at the reader.
- **Bad reading**, the red LED and the buzzer are activated at the reader.

Terminate the reader action test

Disconnect the INTUS ACM40e from power supply. Set the DIP switch (2) to OFF again.

23.2 Automatic self-test

The device performs an automatic self-test and initialization procedure after the mains supply is switched on or after a reset is carried out.

During self-configuration or initialization, the system may notice a lack of system resources or a severe system error. In this case, the message is announced as follows:

- The buzzer sounds at each terminal if the cover is connected to the basic unit.
- At INTUS ACM via the status LEDs and the buzzer
- S0 - status LED on, S1 - status LED blinks and the buzzer sounds at the same time. See figure above for the positions of status LEDs
- At INTUS 5500 and INTUS 5320 terminals with display, the following message is displayed during initialization: SYSTEM ERROR: X

SYSTEM ERROR:	Status LED flashes, buzzer sounds	Cause and correction
G	7x	Mismatch between TCL firmware and text file INTUS.TXT containing the language-dependent message and setup texts. Use INTUS RemoteSetup to update the firmware.
H	8x	The host connection could not be opened. Correction: Attempt an ice-cold boot. If this is unsuccessful, there is a hardware problem that must be repaired.
I	9x	The hardware configuration could not be loaded from the EEPROM. Correction: Reproduce the INTUS ACM40 with the production and maintenance software. If unsuccessful, there possibly is a hardware defect.
J	10x	The number of requested software timers exceeds the number of software timers that were created. Internal software error which should not occur.
K	11x	An internal memory request for creating a table in the DRAM failed. The cause may be that too large a buffer was specified for the serial channels. Correction: Ice-cold boot and reconfiguration. If unsuccessful, there possibly is a hardware defect.
L	12x	A software module was unable to register for de-initialization. Internal software error which should not occur.
M	13x	Insufficient memory while creating a real-time component. Correction as under "11x".
N	14x	Insufficient memory while creating a ring buffer. Correction as under "11x".
O	15x	Error in SRAM management. Internal error which should not occur.
P	16x	Error in SRAM management. Internal error which should not occur.
Q	17x	Insufficient memory while creating a real-time process. Correction as under "11x".
R	18x	Configured offline buffer too large. This error should generally be avoided by an automatic reconfiguration, reducing offline buffer size to the default setting of 48 kB. Correction: Ice-cold start and reconfiguration; the offline buffer and the table field should be configured in a way that at least 30 kB remain for the DL download area.



In the case of system errors, in contrast to breakdowns due to defective hardware, INTUS RemoteConf is still usable.

You can thus correct configuration errors by performing an ice-cold boot. Carried out under "Reset", please see chapter 17.

23.3 Error diagnostics by log file



The log files are saved:

%AppData%\ INTUS\RemoteConf

If RemoteConf0.log exceeds 512 KB, the RemoteConf0.log is renamed in RemoteConf1.log. A new RemoteConf0.log is created ("log file rotation").

When a second INTUS RemoteConf is started, the log file is called RemoteConf0.log.1.

Up to 4 files can be created:

- RemoteConf0.log
- RemoteConf1.log
- RemoteConf0.log.1
- RemoteConf1.log.1

Any device-specific entry in the log file begins with the serial number of the device.

23.4 Unsuccessful error diagnostics

Please contact the PCS Technical Support if you fail to locate and eliminate a failure:

E-mail: support@pcs.com

Make sure you have the following information ready:

- Precise description of the failure
- Firmware version number and configured parameters, both displayed on the status page of INTUS RemoteConf.

24 Tables of configurable parameters

The following tables list the most important configurable parameters including their default values.

Please record the new values for all the settings that you have changed during installation, so that you can refer to these values when contacting the PCS Technical Support.

IP configuration - network connection

Parameter		Default setting	Changed to
Location		Location terminal <serial number>	
Contact		Contact	
Hostname		intus-<serial number>	
Host interface		LAN	
IPv4		DHCP	
IPv4 without DHCP	IPv4 address	192.168.042.127	
	IPv4 network mask	255.255.255.000	
	IPv4 gateway	0 . 0 . 0 . 0	
IPv6		RADV	
IPv6 Manual setting	IPv6 address	*2001:0000:0000:0000: 0000:0000:0000:0000	
	IPv6 prefix	64	
IPv6 DHCP	IPv6 gateway	RADV	
	IPv6 gateway address	*2001:0000:0000:0000: 0000:0000:0000:0000	
ETH-Link		Auto-negotiation	
IEEE 802.1X		Not activated	

Channel A - Host communication TCP

Parameter		Default setting	Changed to
Connection establishment		Passive	
Port		3001	
Connection establishment: active	IPv4 or IPv6 address	0 . 0 . 0 . 0 or *0000:0000:0000:0000: 0000:0000:0000:0000	

** 2001:: is displayed

TCL parameters

Parameter	Default setting	Changed to
Table field (bytes)	49152	
Offline buffer (bytes)	49152	
Acknowledge time (s)	26	
Offline buffer records with record number	NO	
Load default TCL program on cold boot	Yes	
Size BMI field (bytes)	88	
Number of labels	1024	
Character encoding	ISO6464-DE	

Tables for security settings*Channel A - Host interface access*

Parameter	Default setting	Changed to
Encryption Authorization level 3	disabled	
Login		
Password for simple access Authorization level 2/3	disabled	
Password for administrative access	disabled	
Transmission record structure		
Routing bytes Authorization level 2/3	disabled	
Record character for login messages	disabled	

Firewall IPv4

Network address	Network mask	Data	Maintenance	State
. . .	. . .			
. . .	. . .			
. . .	. . .			
. . .	. . .			
. . .	. . .			

Firewall IPv6

Network address	Prefix	Data	Maintenance	State

Change maintenance group & password / LBus Key

Parameter		Default setting	Changed to
Login	Maintenance group Authorization level 3	0	
	Password Authorization level 1	111111	
	Password Authorization level 2	14789632	
	Password Authorization level 3	14589632	
LBus 1	LBus1 – Key Authorization level 3	without	
LBus 2	LBus2 – Key Authorization level 3	without	

25 License regulations for free software

The TCL firmware includes free licensed software. The free software was developed by third parties and is protected by copyright laws and international copyright treaties.

The license regulations in the English original version are displayed directly in INTUS RemoteConf.

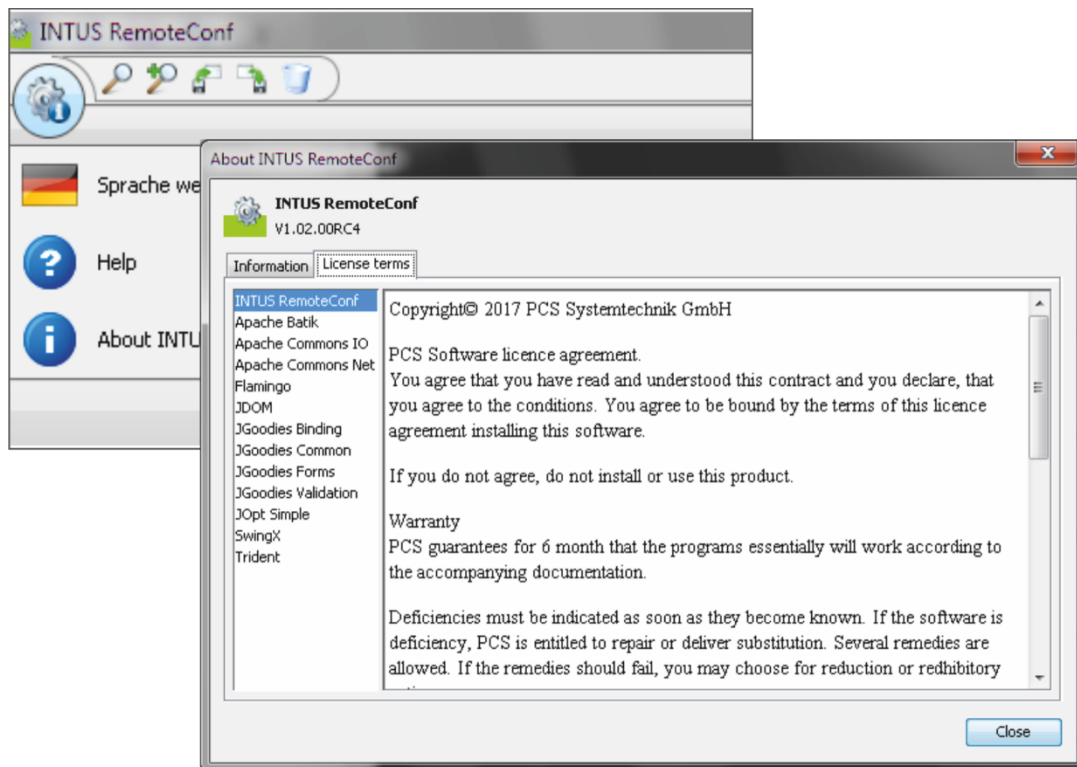


Figure 25-1: License regulations

The free software is provided free of charge. You are entitled to use the free software in accordance with the license regulations specified above. Where these license regulations are in conflict with the PCS Systemtechnik GmbH license regulations for software, the license regulations specified above shall have priority as far as free software is concerned.

PCS Systemtechnik GmbH accepts no liability for defects if the free software infringes on third-party intellectual property rights.

On request and for a fee, which doesn't exceed distribution costs, PCS Systemtechnik GmbH offers to deliver or to make available a complete machine-readable copy of source code at common media for electronic data exchange. This offer is valid within a period of three years after the purchase of this product. You get the source code from PCS Technical Support or www.pcs.com/services/download

26 List of figures

Figure 4-1: Connection terminal/PC	22
Figure 4-2: INTUS RemoteConf buttons	24
Figure 4-3: IP configuration	25
Figure 4-4: Rearranging the terminal list	26
Figure 4-5: Info button	26
Abbildung 4-1: Activate licence	27
Figure 5-1: Introduction to the terminal configuration	32
Figure 6-1: Login	33
Figure 7-1: Configuration overview	34
Figure 7-2: Finalizing the configuration	35
Figure 8-1: The network connection (IP)	36
Figure 8-2: WiFi	38
Figure 8-3: IEEE 802.1X/WPA2-Enterprise	40
Figure 8-4: Mobile	41
Figure 9-1: Channel A – Not configured	43
Figure 9-2: HTTPS client settings	45
Figure 10-1: Firewall Configuration - Example	48
Figure 10-2: Status not granted	48
Figure 11-1: Wiring the INTUS 5200 / INTUS 5320 / INTUS 5500 / 5540 / 5600	51
Figure 11-2: Point-to-Point wiring the INTUS ACM80e	54
Figure 11-3: Multi-Point wiring the INTUS ACM80e	54
Figure 11-4: Reader configuration	55
Figure 11-5: Easy addressing	56
Figure 11-6: ACM40e Wiegand module: 2 LBus readers, 4 Wiegand readers	58
Figure 11-7: example ACM40e with 16 INTUS Flex devices	61
Figure 11-8: ACM 40e, 2 readers, 8 INTUS Flex devices	64
Figure 11-9: ACM40e, 4 readers, 8 INTUS Flex devices	68
Figure 11-10: ACM80e, 8 INTUS 700/6xx/350H readers and 8 INTUS Flex devices	72
Figure 11-11: One INTUS 5500/5540/5600 with LBus1 & LBus2	75
Figure 11-12: Activating AES encryption	76
Figure 11-13: Configuring the AES key	77
Figure 11-14: Configuring the customer key	77
Figure 11-15: Changing the customer key	78
Figure 11-16: Removing a customer key	79
Figure 11-17: LBus encryption	80
Figure 12-1: Internal reader	81
Figure 13-1: TCL parameters	82
Figure 14-1: Hardware	84
Figure 15-1: Login	85
Figure 16-1: Time	87
Figure 17-1: Select LBus action(s)	89
Figure 17-1: Custom reader settings configuration	92
Figure 17-2: Sequence of LBus actions	93
Figure 18-1: Flex Air	95

Figure 18-2: View of the Flex configuration 95

Figure 18-3: Error message - Change base address 96

Figure 18-4: Remove flex device from gateway 97

Figure 18-5: Pair Flex device 97

Figure 18-6: Select free address 98

Figure 18-7: Note change base address 99

Figure 18-8: Base adresse modified 99

Abbildung 18-1: Activate service mode 100

Figure 19-1: Reset 101

Figure 20-1: Logo upload 103

Figure 23-1: Reader action test, INTUS ACM80e 108

Figure 23-2: Reader action test, INTUS ACM40e 109

Figure 25-1: License regulations 115

27 Index

- Authorization level 17
- AutoClone service 98
- Blue marked 24
- BSC 101
- Buttons 23
- Buzzer sounds 106
- Characteristics 12
- Cold boot 97
- Configuration 31
 - Overview 31
- Connection establishment 39
- Daylight saving time 84
- Display contrast 80
- DNS-Server 34
- Encryption 76
- Error 107
- Finalizing 32
- Firewall 43
- Host communication 39, 108
- Host name 34
- HTTPS Client 41
- HW 71
- Ice-cold boot 97
- IEEE 802.1X 36
- Indications de sécurité 8
- Internal reader 77
- IPv4 34
- IPv6 34
- Key 76
- LBus
- Device types 52
 - Licensed software 111
 - Log file 107
 - Logging 30
 - Logo 99
 - Maintenance group 82
 - Mode 53
 - Mode of operation 53
 - Net mask 34
 - Operating parameters 11
 - Parameter tables 108
 - Passphrase 76
 - Password 82
 - Password changing 82
 - PC Firewall 25
 - PCS-Hotline 18
 - RADV 34
 - Reader action test 104
 - Reset 97
 - Safety concept 17
 - Setup
- BSC 101
- TTY 100
 - Symbols 9
 - TCL parameter 78, 109
 - Time 83
 - TTY 100
 - UTC 83
 - WiFi 35
 - WPA2-Enterprise 36

Any questions?

Call us.

PCS Hotline: +49 (0)89/68004-666

Email: support@pcs.com

We try to make our manuals as useful as possible. Please don't hesitate to call us and tell us if there is anything we can improve. Thank you in advance for your effort.

Sincerely: PCS Systemtechnik GmbH

Zeit für Sicherheit.



PCS Systemtechnik GmbH
Pfälzer-Wald-Str. 36
81539 München
Tel. +49 89 68004-0
intus@pcs.com
www.pcs.com

Ruhrallee 311
45136 Essen
Tel. +49 201 89416-0

