



MANUAL

INTUS RemoteConf **Konfiguration und Betrieb**

D5000-001.16

INTUS RemoteConf

Konfiguration und Betrieb

Stand 05/2026

Bestell-Nr. D5000-001.16

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

Die Vervielfältigung und Veröffentlichung des vorliegenden Handbuchs, auch auszugsweise, ist nur mit ausdrücklicher Genehmigung der **PCS Systemtechnik GmbH** erlaubt.

Um stets auf dem Stand der Technik bleiben zu können, behalten wir uns Änderungen vor.

PCS, INTUS und DEXICON sind eingetragene Marken der PCS Systemtechnik GmbH. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen und Organisationen.

©2026 PCS Systemtechnik GmbH

Inhaltsverzeichnis

Sicherheitshinweise	7
1 Über dieses Handbuch	8
1.1 Verwendete Symbole	8
1.2 PCS-Service-Tools und -Handbücher	9
1.3 Weitere Handbücher	9
2 Merkmale	10
2.1 Notwendige Informationen zum Terminal	10
2.2 INTUS 5200 & 5205	11
2.3 INTUS 5320-24V/-NT/PoE	12
2.4 INTUS 5500 / 5540 & INTUS 5600	13
2.5 INTUS ACM80e Rack / INTUS ACM80e Wand	14
2.6 INTUS ACM40e	15
3 Sicherheitskonzept.....	16
3.1 CyberSecurity-Maßnahmen für sicheren Betrieb von INTUS Hardware	17
3.2 Reset der Zugangsdaten für den Login.....	20
3.2.1 Ablauf.....	20
3.2.2 DIP-Schalter.....	20
4 Einstieg in INTUS RemoteConf.....	22
4.1 Installation von INTUS RemoteConf auf dem PC	22
4.1.1 Installation auf PCs mit Microsoft Windows-Betriebssystemen.....	22
4.1.2 Ausführen von INTUS RemoteConf auf anderen Betriebssystemen.....	23
4.2 Schaltflächen von INTUS RemoteConf	24
4.3 Terminal zur Terminalliste hinzufügen	25
4.4 Terminalliste neu ordnen.....	26
4.5 PC-Firewall	26
4.6 Info-Schaltfläche	26
4.7 Lizenz freischalten	27
4.8 Geräte Firmwareupdate	27
4.9 Gleichzeitiges Ausführen von Aktionen an mehreren Terminals.....	30
4.10 Geänderte Inbetriebnahme von Neugeräten.....	30
4.11 Login einrichten.....	31
4.12 Datenport einrichten.....	31
5 Einstieg in die Konfiguration.....	32

6	Login – Einloggen ins Terminal.....	33
6.1	Berechtigungsstufen	33
6.2	Vorgehen	33
7	Konfiguration.....	34
7.1	Übersicht.....	34
7.2	Konfiguration als Datei speichern	34
7.3	Konfiguration beenden.....	36
8	Netzwerkanschluss (IP) konfigurieren.....	37
8.1	WLAN	39
8.2	IEEE 802.1X/WPA2-Enterprise.....	41
8.3	Mobilfunk.....	43
9	Datenport (Kanal A) einstellen	44
9.1	Einstellungen Protokoll TCP	44
9.2	Einstellungen Protokoll HTTPS Client.....	46
9.3	Sicherheitseinstellungen	47
10	Firewall konfigurieren	48
11	LBus konfigurieren	50
11.1	Maximal mögliche Anzahl Leser	51
11.2	Verkabelung beim INTUS 5200/5320/5500/5540/5600.....	52
11.3	Verkabelungsmöglichkeiten beim INTUS ACM40e.....	53
11.4	Verkabelungsmöglichkeiten beim INTUS ACM40e mit Wiegand-Modul	53
11.5	Verkabelungsmöglichkeiten beim INTUS ACM80e.....	54
11.6	Point-to-Point-Verkabelung des INTUS ACM80e.....	55
11.7	MultiPoint-Verkabelung des INTUS ACM80e.....	55
11.8	Leser konfigurieren	56
11.9	Lesertyp / einfache Adressierung.....	57
11.10	Betriebsart.....	58
11.11	Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser.....	59
11.12	Beispiel ACM40e mit 16Flex-Lizenz - 16 funkverbundene INTUS Flex-Endgeräte	62
11.13	Beispiel: ACM40e mit 16Flex-Lizenz - Mischbetrieb mit sternförmig angeschlossenen INTUS Lesern	66
11.14	Beispiel: ACM40e mit 16Flex-Lizenz - Mischbetrieb mit busverdrahteten INTUS Lesern	70
11.15	Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten	74

11.16	Beispiel: ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2.....	77
11.17	LBus AES-Verschlüsselung	78
11.17.1	Voraussetzungen	78
11.17.2	Aktivierung der AES-Verschlüsselung	78
11.17.3	Konfiguration der AES-Schlüssel	79
11.17.4	Kundenschlüssel konfigurieren	79
11.17.5	Option AES-Verschlüsselung nur mit Kundenschlüssel	80
11.17.6	Kundenschlüssel ändern.....	80
11.17.7	Kundenschlüssel entfernen.....	81
11.17.8	AES-Verschlüsselung bei OSDP	81
11.18	LBus-Verschlüsselung (PCS-proprietär)	82
12	Internen Leser einstellen.....	83
13	TCL Parameter einstellen	84
13.1	Einstellungen	84
13.2	Erweiterte Benutzerschnittstelle	85
13.3	INTUS Sound.....	85
14	Hardware	86
14.1	Display	86
14.2	Magic-Eye (nur INTUS 5320).....	86
14.3	Hupe	86
15	Login – Wartungsgruppe und Passwörter ändern.....	87
15.1	Wartungsgruppe	87
15.2	Passwort der Berechtigungsstufe ändern	88
16	Zeit.....	89
16.1	NTP Client.....	89
16.2	UTC offset - Abweichung zur UTC Zeit.....	90
16.3	Sommer/Winterzeitumschaltung	90
17	LBus-Aktionen.....	91
17.1	Überblick.....	91
17.2	Aktion "Firmwareupdate für Leser"	92
17.3	Aktion "Parametrierkarte am Leser freigeben/sperrern"	92
17.4	Aktion "LBus-Schlüssel an Leser übertragen"	92
17.5	Aktion "Leser Parameter Download"	93
17.6	Aktion "Leserspezifische Einstellungen konfigurieren"	94
17.6.1	Allgemeine Aktionen	95

17.6.2	Einstellungen von montageortspezifischen Parametern	95
17.7	Aktionsfolge zusammenstellen.....	95
18	Serviceaktionen für INTUS Flex Air	98
19	Reset	105
20	Logo laden	107
21	Serielle Schnittstelle.....	108
21.1	Basiseinstellungen TTY/BSC	108
21.2	TTY-Protokoll	108
21.3	BSC-Protokoll	109
22	Firewall-Einstellungen im Netzwerk	111
23	Fehlerdiagnose	112
23.1	Leser-Aktionstest	112
23.1.1	INTUS 3xxx und 5xxx	112
23.1.2	INTUS 5540	112
23.1.3	INTUS ACM80e	112
23.1.4	INTUS ACM40e	113
23.2	Automatische Selbsttests.....	113
23.3	Fehlerdiagnose über Log-Dateien.....	115
23.4	Erfolglose Fehlerdiagnose	116
24	Tabellen für die Parameter.....	117
25	Lizenzbestimmungen der freien Software	120
26	Abbildungsverzeichnis	121
27	Index	123



Sicherheitshinweise

- Es dürfen nur Spannungen ins Gerät geführt werden, die folgende Anforderungen erfüllen: LPS (Limited Power Source) und SELV (Safety Extra Low Voltage) entsprechend IEC/EN/UL/CSA 60950-1 oder ES1 und PS2 entsprechend IEC/EN/UL/CSA 62368-1.
- Das Gerät vor dem Öffnen von der Stromversorgung trennen.
- Das Gerät darf nur von unterwiesenem Fachpersonal installiert und nur zu Wartungszwecken geöffnet werden. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen.
- Das Gerät ist nicht mit einer von außen zugänglichen Trennvorrichtung von der Stromversorgung (Schalter) ausgestattet.
- Bei einem festen Netzanschluss muss eine leicht zugängliche Trennvorrichtung (Leitungsschutzschalter mit maximal 16A) installiert werden.
- Erfolgt der Netzanschluss über das Netzkabel, muss der Netzstecker als Trennvorrichtung benutzt werden. Die Steckdose muss leicht zugänglich sein.
- Sollte die Sicherung des integrierten Netzteiles zerstört sein, senden Sie bitte das Terminal zur Reparatur an den PCS Support.
- Da die Abschirmung der Kabel am INTUS Gerät geerdet ist, muss beim Anschluss eines Peripheriegerätes, das an einem anderen Stromkreis als das INTUS Gerät betrieben wird, die Abschirmung der Kabel am Peripherie-/Endgerät (oder Rechner) vom Schutzleiter getrennt sein.
- Während eines Gewitters dürfen die Kabel weder angeschlossen noch gelöst werden.
- In Notfällen (z. B. beschädigtes Netzkabel oder Gehäuse, Eindringen von Flüssigkeiten oder Fremdkörpern) ist das Gerät sofort stromlos zu machen (Netzstecker ziehen bzw. Trennvorrichtung öffnen). Verständigen Sie den PCS Support.
- VORSICHT! Explosionsgefahr bei unsachgemäßem Austausch der Batterie.
- Ersatz der Batterie nur durch denselben oder einen von PCS empfohlenen gleichwertigen Typ, siehe Handbuch Installation & Wartung.
- Gebrauchte Batterien sollten umweltgerecht entsorgt werden.
- Die Platine enthält gefährdete ESD-Bauteile. Treffen Sie geeignete Maßnahmen zum Schutz der Platine.
- Eingriffe in die Hard- und Software, die nicht in diesem Handbuch beschrieben sind, dürfen nur durch PCS Fachpersonal vorgenommen werden.

1 Über dieses Handbuch

Das vorliegende Handbuch gibt dem Betreiber und Instandhalter die notwendigen Informationen für die Inbetriebnahme, die Festlegung und Änderung der Konfiguration des Terminals, die Betriebsüberwachung und die Fehlerdiagnose. Es gilt für folgende Terminaltypen:

- 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 Wand
- INTUS ACM40e
- INTUS 3150/3155

Das vorliegende Handbuch ist gültig für die Software Version V1.16.



Über die Info-Schaltfläche, siehe Kapitel 4.6, gelangen Sie direkt zur Download-Seite für INTUS RemoteConf: <https://download.pcs.com/irc>. Hier kann die aktuelle Software-Version von INTUS RemoteConf heruntergeladen werden.

Verwendete Symbole



Dieses Symbol warnt vor Gefahren für Gesundheit und Leben sowie vor Gefahren, die zu Schäden des Geräts oder des Systems führen können. Den Text neben diesem Zeichen sollten Sie in jedem Fall lesen und beachten!



Dieses Symbol weist auf Informationen hin, die für den Umgang mit dem Gerät wichtig sind und beachtet werden müssen.



Dieses Symbol weist auf eine Handlungsanweisung hin.

1.2 PCS-Service-Tools und -Handbücher

Auf folgender Seite stehen Ihnen PCS-Service-Tools für Inbetriebnahme und Wartung der INTUS Terminals und die dazugehörigen Handbücher kostenlos zum Download zur Verfügung:



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

1.3 Weitere Handbücher

- Ein Handbuch für die Installation und Wartung des jeweiligen Geräts. Der Monteur und Elektriker findet darin ausführliche Informationen über Montage, Anschlüsse, Schnittstellen und die Umgebungsbedingungen.
- INTUS Lokaler Setup (Bestell-Nr. D5000-003) – für INTUS 3150/5320/5500/ACM40e/80e und Setup über Touchscreen für INTUS 5200/5205/5600
- INTUS 3000 Programmierhandbuch TCL (Bestellnummer D3000-004). Dieses Handbuch beschreibt die Programmiersprache TCL, mit der sich das INTUS Gerät für den individuellen Einsatz programmieren lässt.

2 Merkmale

2.1 Notwendige Informationen zum Terminal

Um ein Gerät mit INTUS RemoteConf konfigurieren zu können, sind folgende Informationen unbedingt erforderlich:

- Netzwerkkonfiguration bzw. Hostschnittstelle
- Leserkonfiguration – falls die angeschlossenen Leser nicht von einer übergeordneten Software konfiguriert werden.
- Sonstige TCL Parameter – falls die TCL Parameter nicht von einer übergeordneten Software konfiguriert werden.

Parameterwerte konfigurieren

Um ein Terminal in Betrieb zu nehmen, müssen die Betriebsparameter eingestellt werden, damit die Verbindung zum Leitrechner (Host) und zu den externen Lesern funktioniert.

Im vorliegenden Handbuch wird die Konfiguration der Parameterwerte mittels eines PCs und der Software „INTUS RemoteConf“ erläutert.

Gegebenenfalls übernimmt Ihr Softwarepartner diese Aufgabe für Sie.

Wie die Parameterwerte eingestellt werden, ist abhängig von der eingesetzten Softwarelösung.

2.2 INTUS 5200 & 5205

Schnittstellen	INTUS 5200	INTUS 5205
Ethernet 10/100BASE-T / WLAN	◆ / ◇	◆
Integrierter RFID-Leser	◆	◆
Barcode Leser	◇	----
Interface Modul		
2x digitaler Eingang DI, optoentkoppelt 1x Türsteuerung DO (Wechsler Relais) 1x Externer Leser (RS485 Schnittstelle)	◇	----
Bedienelement und Anzeige		
3,5“ Projiziert-kapazitiver Touchscreen	◆	◆
3,5“ TFT Farbdisplay Auflösung 320x240	◆	◆
Statusanzeige blau	◆	◆
Folientastatur, 10-er Block 2 Funktionstasten	◇	----
Benutzeroberfläche	vordefiniert	vordefiniert
Aktion mit INTUS RemoteConf		
Eigenes Kundenlogo laden	◆	◆
Bildschirmmaske laden*	◇	◇
Audiodatei laden	◇	----
Tastaturbelegung laden	----	----
Leistungsmerkmale		
Datenspeicher	◆ 1MB ◇ 2MB	◆ 0,5MB
Schutzart IP30 / mit Dicht-Kit bis IP 64	◆ / ◇	◆ / --
Signalgeber / Lautsprecher / Heizung	◆ / ◇ / ◇	◆ / -- / --
Sabotagekontakt, Schloss	◆	◆
Stromversorgung INTUS 5205 / 5200		
INTUS 5200-24V 12-24V +20% -15% DC, externes Netzteil; SELV, L.P.S, ES1, PS2		
INTUS 5205-SNT Werkseitig angeschlossenes Kabel mit Steckernetzteil (230V AC)		
INTUS 5200-PoE/ 5205-PoE Power over Ethernet, IEEE 802.3af class2		

◆ Standard; ◇ Option

* Das Laden der Bildschirmmaske ist optional möglich, wenn die Maskenfreeschaltung gekauft wurde

2.3 INTUS 5320-24V/-NT/PoE

Schnittstellen	
Ethernet 10/100BaseT; RJ45 Buchse/WLAN	◆ / ◇
Integrierter RFID-Leser Mifare, Legic, Hitag	◇
DI/DO Schnittstellen	
2 x digitaler Eingang DI, optoentkoppelt 1 x digitaler Ausgang DO (Relais)	◆
1 Steckplatz für ein LBus-Modul à 4 Leser über LBus1	◇
Bedienelement und Anzeige	
Display 240 x 64 Pixel, schwarz-weiß	◆
Folientastatur (10-er Block) mit 5 programmierbaren Funktionstasten / mit 10-er Block	◆ / ◇
MagicEye (blau/rot/grün), 2 LEDs (rot/grün)	◆
Leistungsmerkmale und Mechanik	
Speicher 2 MB / 6 MB	◆ / ◇
Stammsätze / Buchungen mit 2 MB	ca. 13 000 / 26 000
Stammsätze / Buchungen mit 6 MB	ca. 40 000 / 80 000
Schutzart IP30 / mit Dicht-Option bis IP65	◆ / ◇
Signalgeber / Heizung	◆ / ◇
Sabotagekontakt, Schloss und Verriegelung	◆

◆ Standard; ◇ Option

	INTUS 5320-24V	INTUS 5320-NT	INTUS 5320-PoE
Stromversorgung	externes Netzteil 24 V; SELV, L.P.S, ES1, PS2	Integriertes Netzteil 115...230 V AC	Power over Ethernet, IEEE 802.3af class3

2.4 INTUS 5500 / 5540 & INTUS 5600

Schnittstellen	5500	5540	5600
Ethernet 10/100BASE-T / WLAN	◆ / ◇	◆ / ◇	◆ / ◇
Integrierter RFID-Leser Mifare, Legic, Hitag	◇	◇	◇
Barcode Leser	◇	◇	◇
Interface Modul			
2 x digitaler Eingang DI, optoentkoppelt	◇	◇	◇
2 x digitaler Ausgang DO (Relais)			
2 Steckplätze für je ein LBus Modul á 8 Leser über LBus1 bzw. LBus2	◇	◇	◇
USB-Buchse für PCS Barcodescanner	◇	◇	◇
Bedienelement und Anzeige			
5,7" TFT VGA Farbdisplay, 640x480 Pixel	---	---	◆
4,3" TFT Farbdisplay, 480x272 Pixel	---	◆	---
Display 240x64 Pixel, schwarz-weiß	◆	---	---
Projiziert-kapazitiver Touchscreen, mit wählbarem Tastaturlayout	---	---	◆
Folientastatur (10-er Block) mit 5 programmierbaren Funktionstasten	◆	◆	---
MagicEye (blau/rot/grün), 2 LEDs (rot/grün)	◆	◆	◆
Aktion mit INTUS RemoteConf			
Bildschirmmaske und Kundenlogo laden	----	----	◆
Audiodatei laden	◆	◆	◆
Tastaturbelegung laden	----	----	◆
Leistungsmerkmale und Mechanik	5500 / 5540 & 5600		
Speicher 2MB / 6MB	◆ / ◇		
Stammsätze / Buchungen mit 2MB	ca. 13 000 / 26 000		
Stammsätze / Buchungen mit 6MB	ca. 40 000 / 80 000		
Schutzart IP30 / mit Dicht-Kit bis IP 64	◆ / ◇		
Signalgeber / Lautsprecher / Heizung	◆ / ◇ / ◇		
Sabotagekontakt, Schloss und Verriegelung	◆		
Stromversorgung INTUS 5500 / 5540 & 5600			
INTUS 5500-24V / INTUS 5540-24V / INTUS 5600-24V 24V ± 20% DC, externes Netzteil; SELV, L.P.S, ES1, PS2			
INTUS 5500-NT / INTUS 5540-NT / INTUS 5600-NT Integriertes Netzteil 115...230V AC, werkseitig angeschlossenes Netzkabel			
INTUS 5500-PoE / INTUS 5540-PoE / 5600-PoE Power over Ethernet, IEEE 802.3af class3			

◆ Standard; ◇ Option

2.5 INTUS ACM80e Rack / INTUS ACM80e Wand

Schnittstellen zur Türsteuerung

4 / 8 / 16 Zutrittsleser, Point-to-Point oder MultiPoint	◆ / ◇ / ◇
LBus2 Modul für bis zu 8 weitere Zutrittsleser (MultiPoint)	◇
16 x digitaler Eingang (DI) optoentkoppelt, Lesern zugeordnet	◆
16 x digitaler Ausgang (DO) Wechsler-Relais 5A, Lesern zugeordnet	◆

Schnittstellen für Alarmanlage, Sirene, Systemanwendungen

4 x digitaler Eingang (DI) optoentkoppelt	◆
4 x digitaler Ausgang (DO) Wechsler-Relais 5A, DO4 umschaltbar auf bistabiles Wechsler-Relais 2A	◆

Leitrechner (Host) Schnittstelle

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

Leistungsmerkmale und Mechanik

Speicher 2MB / 6MB / 10MB	◆ / ◇ / ◇
Mitarbeiter* / Buchungen mit 2MB: 35.000 / 32.000	
Mitarbeiter* / Buchungen mit 6MB: 109.000** / 101.000	
Mitarbeiter* / Buchungen mit 10MB: 190.000** / 170.000	
Sabotagekontakt / Hupe	◆
CPU ARM9 G45 / 400MHz	◆

Integrierte Stromversorgung

Leser-Versorgungsspannung 12V DC (Voreinstellung) / 24V DC umschaltbar; geregelt	◆
Türöffner (DO)- bzw. System, Alarm (DO) - Versorgungsspannung 12V DC (Voreinstellung) / 24V DC umschaltbar; geregelt	◆

Stromversorgung

integrierter 230V AC Ringkerntrafo, umschaltbar auf 115V AC	◆
---	---

Sicherheitskonzept

Erhöhte Ausfallsicherheit des Geräts: Bei Beschädigung einer Komponente ist nur diese Komponente betroffen. Dies wird erreicht durch Leser-Anschluss Point-to-Point, Stromversorgung über das Gerät, die Bereitstellung von 2 digitalen Ein- und Ausgängen pro Leser-Anschluss.

◆ Standard; ◇ Option

* Die Anzahl der Mitarbeiter ist für die Zutrittskontrolle angegeben. Bei Zeiterfassung reduziert sie sich um ca. 50%.

** Bei Verwendung von TPI zur Zutrittskontrolle ist die Anzahl der Mitarbeiter auf 99.999 begrenzt.

2.6 INTUS ACM40e

Schnittstellen

Leser	Max. 4 Zutrittsleser (2 Standard + 2 optional), über LBus-Schnittstellen für Point-to-Point-Anschluss
Türsteuerung	8 x DI (optoentkoppelt), 4 x DO (Wechsler-Relais) zur Kontrolle von 4 Türen; den Lesern zugeordnet, und nur für die Türsteuerung geeignet
Systemsteuerung für Alarm, Meldelinie	4 x DI (optoentkoppelt), 2 x DO (Wechsler-Relais), 1 x bistabiler DO (Wechsler-Relais)
Host	Ethernet 10/100 BaseT über RJ45 Buchse

Integrierte Spannungsversorgung

Leser	Leser-Versorgungsspannung 12 V DC (Voreinstellung) / 24 V DC umschaltbar; geregelt
Türöffner DO	Türöffner (DO)- bzw. System, Alarm (DO) - Versorgungsspannung 12 V DC (Voreinstellung) / 24 V DC umschaltbar; geregelt
Notstromversorgung INTUS ACM40e-Akku	4 h Pufferzeit bzw. 2500 Aktionen

Leistungsmerkmale

Speicher	2 MB (Standard) / 6 MB (Option) / 10 MB (Option)
----------	--

Stromversorgung

INTUS ACM40e-NT	INTUS ACM40e-Akku	INTUS ACM40e-24	INTUS ACM40e-PoE
Integriertes 115 – 230 V Industrienetzteil	Integriertes 115 -230 V Industrienetzteil mit Akkupufferung	Externe Spannungsquelle 12 V DC oder 24 V DC (SELV, L.P.S., ES1, PS2)	Stromversorgung über Ethernet (Ultra PoE)

3 Sicherheitskonzept

Die Konfiguration des Terminals, die Kommunikation mit dem Host und den Lesern lässt sich folgendermaßen absichern:

Berechtigungsstufen: Es gibt drei Berechtigungsstufen, die über Passwörter zugänglich sind.

Berechtigungsstufe	Passwort (voreingestellt)	
1	111111	Passwort der Stufe 1
2	14789632	Passwort der Stufe 1 + 2
3	14589632	Passwort der Stufe 1 + 2 + 3

Firewall

Es ist möglich, Zugangsberechtigungen für einzelne Netzwerkteilnehmer oder Netzwerkgruppen freizuschalten:

INTUS RemoteConf → Konfiguration > Firewall

Wartungsgruppe

Das Terminal kann einer bestimmten Wartungsgruppe zugeordnet werden. Bei Unkenntnis der Wartungsgruppe ist kein Zugang mit den PCS-Tools möglich.

INTUS RemoteConf → Konfiguration > Login

Passwort der Hostschnittstelle

Es ist möglich, Passwörter für den Zugang (Login) einzurichten;

INTUS RemoteConf → Konfiguration > Kanal A

Verschlüsselung der Hostschnittstelle

Es ist möglich, die Kommunikation mit dem TCL Interpreter zu verschlüsseln;

INTUS RemoteConf → Konfiguration > Kanal A

Verlust von Zugangsdaten

Die korrekte und sichere Speicherung von Zugangsdaten wie z. B. Passwörtern und Wartungsgruppen im System liegen in der Verantwortung des Kunden.

Ein Verlust der Passwörter kann zu Sicherheitsrisiken, zur Gefährdung der Systemfunktion, Folgekosten und Zeitverzug führen.

Um technischen Support, eine Projektleitung, Installation oder Ähnliches erhalten zu können, müssen die Passwörter zum entsprechenden Zeitpunkt vorliegen.



Notieren Sie in jedem Fall bei einer Änderung neue Passwörter sowie gegebenenfalls die Passphrase (den Verschlüsselungstext).

Hierfür finden Sie Tabellen in Kapitel 24. Informationen zum **Reset der Zugangsdaten für den Login** finden Sie in Kapitel 3.2.

Wenn Sie versäumt haben, die Änderung bzw. Einstellung der Zugangsberechtigung zu notieren oder weitere Fragen haben, rufen Sie uns an.

Halten Sie bitte die Seriennummer des Terminals bereit.

PCS-Hotline: +49 89 68004-666

E-Mail: support@pcs.com

3.1 CyberSecurity-Maßnahmen für sicheren Betrieb von INTUS Hardware

In diesem Abschnitt wollen wir Sie über die Maßnahmen für einen sicheren Betrieb der aktuellen INTUS Terminals, Zutrittskontrollmanager und Leser informieren. Der Abschnitt ist als kompakte Ergänzung zur bestehenden Dokumentation zu sehen, wobei auch die Hinweise in allen anderen Informationsquellen zu beachten sind. Im Zweifelsfall hat die aktuellere Version Gültigkeit. Alle aufgelisteten Maßnahmen werden von uns dringlichst empfohlen.

Hier geben wir Ihnen die Möglichkeit, einen Überblick über unsere Empfehlungen zu gewinnen. Die entsprechenden Details und Maßnahmen können Sie den Handbüchern entnehmen.

Allgemeine Empfehlungen: (dringend empfohlen)

- Aktuelle INTUS TCL-Firmwareversion („INTUS Firmware-Paket“) verwenden
- Aktuelle Version von INTUS RemoteConf verwenden
- Aktuelle Version von INTUS COM verwenden
- Aktuelle RFID-Technologie verwenden
- Aktuelle Hardware (INTUS RemoteConf-Geräte) verwenden
- Aktuelle Leserfirmware verwenden

Sicherer Betrieb im Netzwerk:

- Interne Gerätefirewall (dringend empfohlen)
- Wir empfehlen, die Gerätefirewall zu nutzen, um die Kommunikation für den täglichen Betrieb (mit der Applikation oder INTUS COM) sowie für die Wartung (HTML Statusseite, INTUS RemoteConf) einzuschränken, sofern keine anderen Maßnahmen (z. B. VLANs) umgesetzt sind.
- IP-Setup-Komfortfunktion mit INTUS RemoteConf deaktivieren
- Nach der Erstinbetriebnahme des Terminals sollte der IP-Setup in INTUS RemoteConf für das Terminal/ACM gesperrt werden. Sobald das Terminal in

Betrieb ist, wird diese Komfortfunktion für die Erstinbetriebnahme nicht mehr benötigt.

- (Sofern ein Wechsel des IP-Adressbereichs geplant ist, das Terminal eine feste IPv4-Adresse hat und IPv6 deaktiviert ist, ist es sinnvoll, diese Option vorübergehend wieder zu aktivieren.)
- AutoClone-Verbindung mit INTUS RemoteConf deaktivieren (dringend empfohlen ohne INTUS COM)
- In INTUS RemoteConf gibt es in neueren Versionen die Möglichkeit, die Verbindung zum AutoClone-Dienst zu deaktivieren. Dies ist bei einer Nicht-Verwendung von INTUS COM empfohlen.
- IEEE 802.1X bei kabelgebundenem Ethernet nutzen
- Mittels IEEE 802.1X kann der Zugang zum Netzwerk vom Ethernet-Switch geschützt werden; nur Geräte, die sich authentifizieren, erhalten nach einer positiven Autorisierung entsprechenden Zugang.
Da sich Zeiterfassungsterminals meist in einem halböffentlichen Bereich befinden, empfehlen wir dieses Feature zu nutzen.
- WPA2 Enterprise
- Sofern Terminals via WLAN angebunden werden, ist es in größeren Netzwerken Best Practice, wenn jedes Gerät eigene Zugangsdaten zum WLAN-Netzwerk besitzt. Nur so ist es möglich, ein dediziertes Gerät zu sperren.

Schutz vor unerlaubtem Zugriff auf die Geräte:

Ab 01. August 2025 werden die Geräte mit einer neuen Firmware-Version ausgeliefert, welche eine Änderung der Passwörter mit dem entsprechenden INTUS RemoteConf vor Nutzung voraussetzt. Dies verhindert die Gefährdung der Geräte durch die Standardpasswörter nach der erstmaligen Inbetriebnahme und verbessert so die Cybersicherheit Ihres Systems.

Schutz des Datenaustauschs mit INTUS COM bzw. einer anderen Applikation (sichere Verbindung mit dem Host):

- Datenaustausch per HTTP/2
- Sofern die Applikation dies unterstützt oder INTUS COM im Einsatz ist, empfehlen wir, dieser Schnittstellenoption den Vorzug zu geben.
- CA-Zertifikats-Updates per HTTP/2
- Sofern der Datenaustausch per HTTP/2 erfolgt, ist angeraten, diesen zu aktivieren. So kann das Zertifikat, mit dem das Terminal den Server authentifiziert, einfach getauscht werden (INTUS COM Unterstützung ist gegeben).

- Verschlüsselung der Hostschnittstelle bei TCP-Protokoll (dringend empfohlen)
- Sofern die Middleware dieses Feature unterstützt, sollte es aktiviert werden. Die Empfehlung ist, die neuste Version der Verschlüsselung (V2) zu verwenden und in INTUS COM und INTUS RemoteConf zu setzen.



- Achtung: Werden beim aktiven/passiven TCP-Verbindungsaufbau weder Login und Verschlüsselung noch die Gerätefirewall genutzt, sind dringend andere geeignete Maßnahmen zum Schutz des Datenaustauschs erforderlich (z. B. VLANs in Verbindung mit IEEE802.1X).

Schutz des Datenaustauschs zwischen INTUS Leser und INTUS ACM/INTUS Terminal:

- LBus verschlüsseln

Zur Absicherung der Kommunikation mit dem Leser wird dringend empfohlen, die Verschlüsselung zu aktivieren, sofern der angeschlossene Leser dies unterstützt.

3.2 Reset der Zugangsdaten für den Login



Wichtig: Die genaue Lage der DIP-Schalter ist geräteabhängig und wird in den jeweiligen Handbüchern beschrieben.

Diese Reset-Funktionalität ist nur aktiv, wenn im Gerät eine INTUS Firmware Paket Version 3.00 oder höher installiert ist.

3.2.1 Ablauf

Falls die Zugangsdaten (Wartungsgruppe und Passwörter) für den Login verloren gegangen sind, können Sie diese über einen Schalter im Gerät zurücksetzen. Der Vorgang ist bei allen Geräten grundsätzlich identisch; lediglich die Lage des DIP-Schalters unterscheidet sich je nach Modell (siehe 3.2.2)

Dazu ist folgendermaßen vorzugehen:

- 1 Schalten Sie das Gerät aus, um das Gehäuse des Gerätes zu öffnen.
- 2 Schalten Sie den für den Reset vorgesehenen DIP-Schalter (Nummer 1) (sanft mit einem schmalen Werkzeug) um, d.h. die Position wechseln; z. B. von ON auf OFF oder von OFF auf ON.
- 3 Schließen Sie das Gehäuse und schalten Sie das Gerät wieder ein.

Dadurch werden folgende Einstellungen auf Werkseinstellungen zurückgesetzt:

- Wartungsgruppe
- Passwörter für alle Berechtigungsstufen

Falls gewünscht kann anschließend die vollständige Gerätekonfiguration auf Werkseinstellungen zurückgesetzt werden (siehe Kapitel 19).

Bevor das Gerät wieder vollständig in Betrieb genommen werden kann, müssen neue Passwörter für alle Berechtigungsstufen vergeben werden (siehe Kapitel 6.1).



Das Gerät merkt sich die Position des DIP-Schalters für den Reset und löst diesen nur aus, wenn sich der Zustand beim System-Reboot gegenüber dem letzten System-Reboot geändert hat.

Der DIP-Schalter muss somit für den normalen Betrieb **nicht** wieder zurück auf die Ausgangsposition geändert werden.

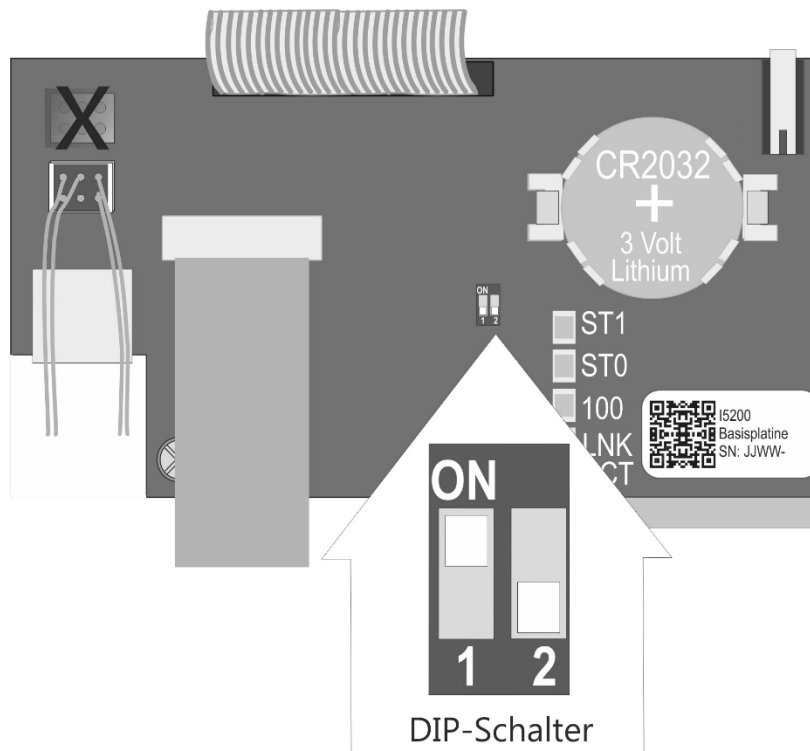
3.2.2 DIP-Schalter

Der Reset der Zugangsdaten wird über einen DIP-Schalter im Gerät ausgelöst.

Je nach Gerätemodell befindet sich der DIP-Schalter an unterschiedlicher Stelle. Die genaue Lage sowie eine Abbildung des DIP-Schalters finden Sie in den gerätespezifischen Handbüchern. Dort finden Sie ebenfalls die Beschreibung zum fachgerechten Öffnen und Schließen des Terminals.

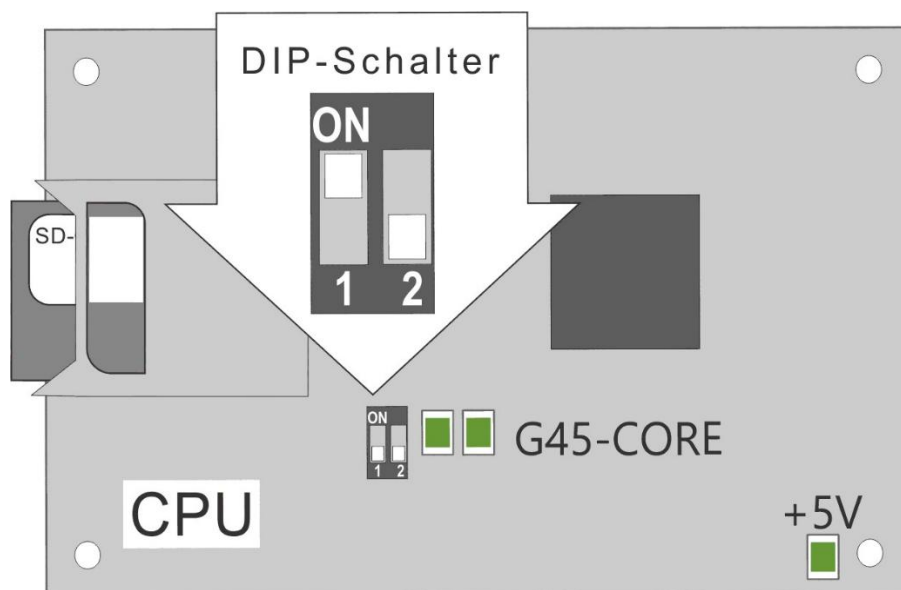
5200er

Bei allen Geräten der 5200er-Serie (I5200, I5205) befindet sich der DIP-Schalter an folgender Stelle:



Alle anderen Geräte

Bei allen übrigen Geräten (z. B. I5320, I5500, I5540, I5600, ACM40e, ACM80e Rack, ACM80e Wand) befindet sich der DIP-Schalter an folgender Stelle:



Die DIP-Schalter können mit der **Schutzfolie** versehen sein. Diese muss zuerst entfernt werden.

Für den Reset folgen Sie bitte dem allgemeinen Ablauf im Kapitel 3.2.1.

4 Einstieg in INTUS RemoteConf

Alle Betriebsparameter des Gerätes werden mit der Software „INTUS RemoteConf“ an einem PC konfiguriert.

Es gibt zwei Möglichkeiten:

- PC und Gerät befindet sich im selben Netzwerk-Segment
- PC und Gerät sind direkt miteinander verbunden



Abbildung 4-1: Anbindung PC/Terminal



Bevor Sie INTUS RemoteConf starten: Bitte stellen Sie unbedingt sicher, dass der PC über eine IP-Adresse verfügt. Mit „ipconfig“ in der Eingabeaufforderung können Sie die Einstellungen am PC kontrollieren.



WLAN als Hostschnittstelle

Bitte beachten Sie die Netzwerk-Einstellungen, wenn WLAN als Hostschnittstelle eingerichtet ist, siehe Kapitel 8.1.

4.1 Installation von INTUS RemoteConf auf dem PC

Um INTUS RemoteConf ausführen zu können, muss in jedem Fall die aktuelle Software Java auf dem PC installiert sein.

Ab INTUS RemoteConf V1.04.01 wird INTUS RemoteConf auch als Paket mit Windows Installer und optionaler interner Java-Laufzeitumgebung zum Download angeboten.

4.1.1 Installation auf PCs mit Microsoft Windows-Betriebssystemen

Für diese Möglichkeit steht das Paket



"INTUS_RemoteConf-x.xx.xx-WindowsInstaller.zip" auf der Download-Seite <https://download.pcs.com/irc/> zur Verfügung. Entpacken Sie die .zip-Datei und führen Sie die Datei "INTUS RemoteConf-x.xx.xxInstaller.exe" aus. Sie haben bei der Installation die Option, eine kostenlose mitgelieferte (private) Laufzeitumgebung basierend auf OpenJDK mit INTUS RemoteConf zusammen zu installieren.

Falls diese Option nicht gewählt wird, müssen Sie selbst eine Java-Laufzeitumgebung (Version 8 oder neuer) Ihrer Wahl auf dem PC installieren, damit INTUS RemoteConf gestartet werden kann.

Nach der Installation kann INTUS RemoteConf über das Windows Start-Menü gestartet werden.

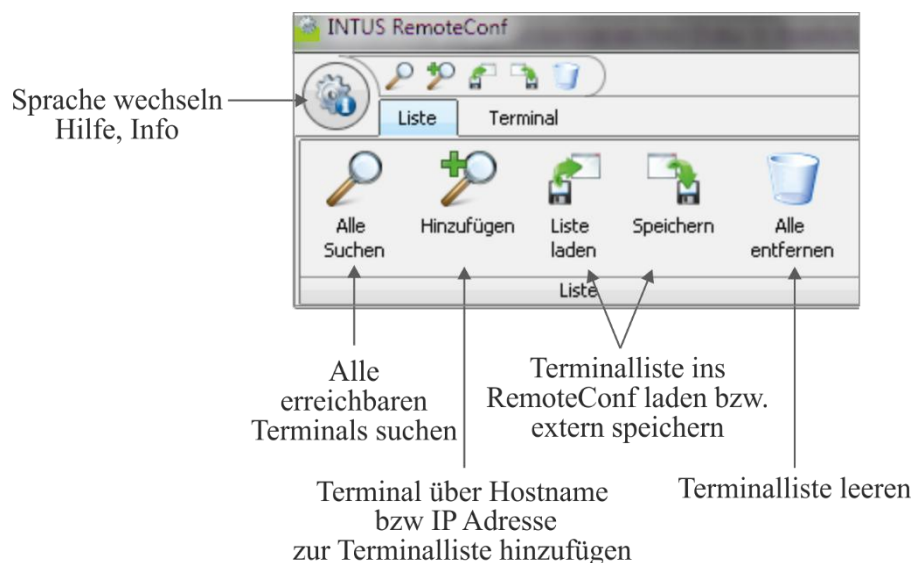
4.1.2 Ausführen von INTUS RemoteConf auf anderen Betriebssystemen

Für diese Möglichkeit steht das Paket "INTUS_RemoteConf-x.xx.xx-JarOnly.zip" unter <https://download.pcs.com/irc/> zur Verfügung. Dieses Paket enthält nur das Java Programm "INTUSRemoteConf.jar", ohne Installer oder private Java-Laufzeitumgebung.



- Sie müssen daher selbst eine Java-Laufzeitumgebung (JRE) Ihrer Wahl auf dem PC installieren, damit INTUS RemoteConf gestartet werden kann.
- Die Java Laufzeitumgebung sollte eine Version 8 oder neuer sein.
- Starten Sie INTUS RemoteConf durch Ausführen von "INTUSRemoteConf.jar".

4.2 Schaltflächen von INTUS RemoteConf



INTUS RemoteConf bietet folgende Möglichkeiten:

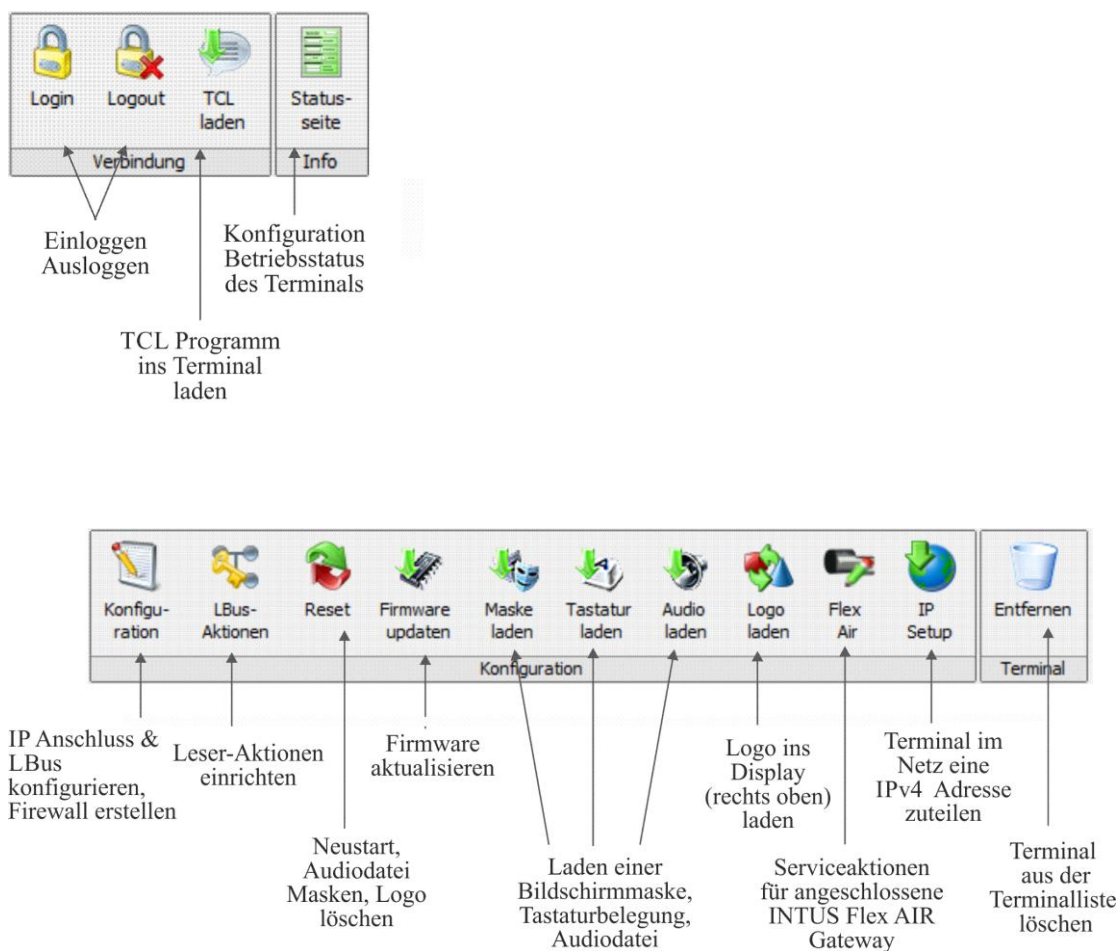


Abbildung 4-2: Schaltflächen in RemoteConf

4.3 Terminal zur Terminalliste hinzufügen

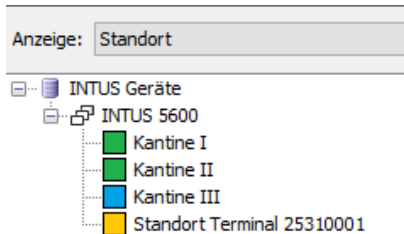


oder



Terminal in der Terminalliste anzeigen:
„Alle Suchen“ oder „Hinzufügen“
(manuelle Eingabe von IP Adresse
oder Hostname).

Alle erreichbaren Terminals werden angezeigt.



- Grün markierte Terminals sind erreichbar und können konfiguriert werden.
- Blau markierte Terminals sind für die Konfiguration nicht ausreichend.
- Dunkelgelb markierte Terminals sind erreichbar, benötigen jedoch vor Betrieb eine Einrichtung des Logins und Datenports (siehe Kapitel 4.11 und 4.12).

Blau markierte Terminals für INTUS RemoteConf erreichbar machen

Ein Terminal wird blau markiert, wenn

- IPv6 beim PC oder Terminal nicht vorhanden ist und deshalb IPv4 verwendet wird.
- Das Terminal nutzt DHCP und ein DHCP Server fehlt im Subnetz.
- IPv4 Adresse des Terminals passt nicht zum Subnetz des PCs.

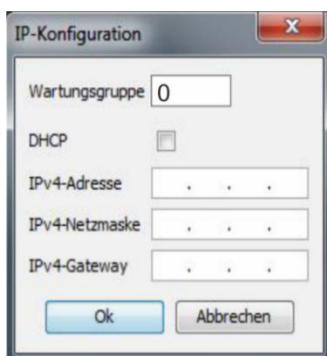
In diesen Fällen ist die Schaltfläche *IP Setup* aktiv.



Das Terminal ist blau markiert, dem Terminal muss eine Adresse zugewiesen werden.



Folgende Angaben werden benötigt, um das Terminal in die Liste aufzunehmen:



Wartungsgruppe, „0“ - Voreinstellung.

IP-Adresse, freie IP-Adresse aus dem Subnetz der IP-Adresse des PCs

Netzmaske, wie am PC eingestellt

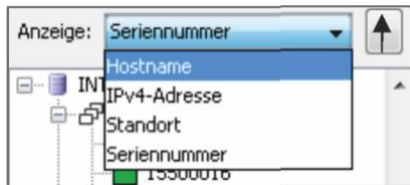
Gateway, auf 0.0.0.0 setzen, um vorhandene Einträge im Terminal zu löschen

Abbildung 4-3: IP-Konfiguration



Soll das Terminal zukünftig ohne DHCP verwendet werden, informiert Sie der Netzverwalter über IP-Adresse, Netzmaske und Gateway-Adresse.

4.4 Terminalliste neu ordnen



Die Terminalliste kann neu geordnet werden.

Abbildung 4-4: Terminalliste ordnen

4.5 PC-Firewall



Falls die PC-Firewall so konfiguriert ist, dass INTUS RemoteConf nicht auf das Netzwerk zugreifen kann, gehen Sie folgendermaßen vor:

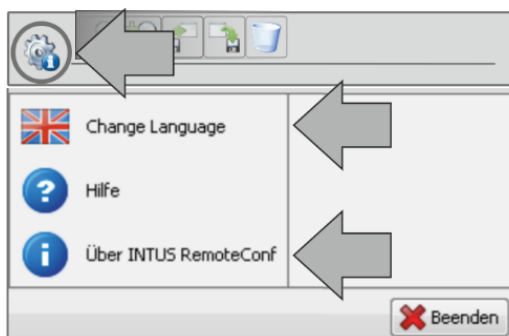


„Zugriff zulassen“ anklicken.

Abbildung 4-5: PC-Firewall

Wiederholen Sie anschließend die Suche im Netzwerk mit INTUS RemoteConf.

4.6 Info-Schaltfläche



Deutsch oder Englisch

Link zur Download Seite
Lizenzvereinbarungen

Abbildung 4-6: Info-Schaltfläche

4.7 Lizenz freischalten

Die Lizenz kann über INTUS RemoteConf über *TCL laden* eingespielt werden.

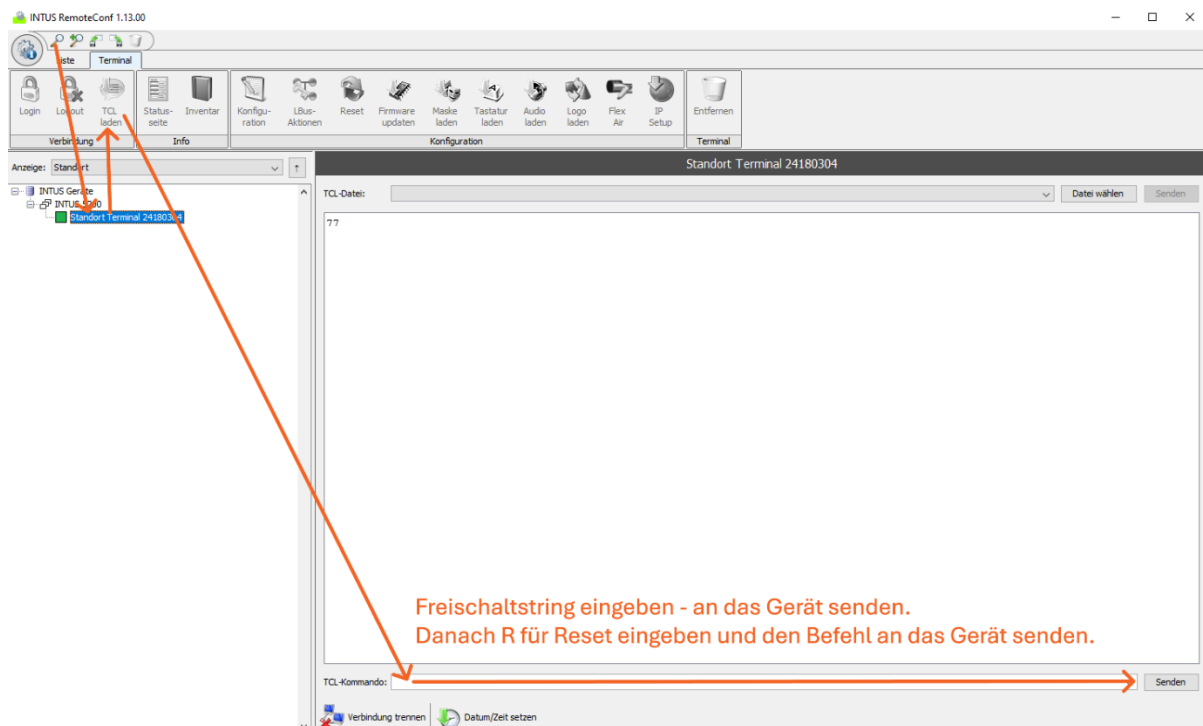


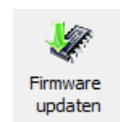
Abbildung 4-7: Lizenz freischalten

Anschließend die TCL-Anweisung R für Reset eingeben und an das Terminal senden.

Alternativ dazu kann der String über INTUS Com via Dialog mit Terminal an das Gerät geschickt werden.

4.8 Geräte Firmwareupdate

- 1 Loggen Sie sich auf das Gerät mit der Berechtigungstufe 3 an.
- 2 Klicken Sie auf den Button "Firmware updaten".
- 3 Wählen Sie das gewünschte Firmwarepaket aus. Beachten Sie bitte im nachfolgenden Absatz ob ggfs. Zwischenschritte notwendig sind. Nur bei Firmware kleiner als 3.xx.xx!

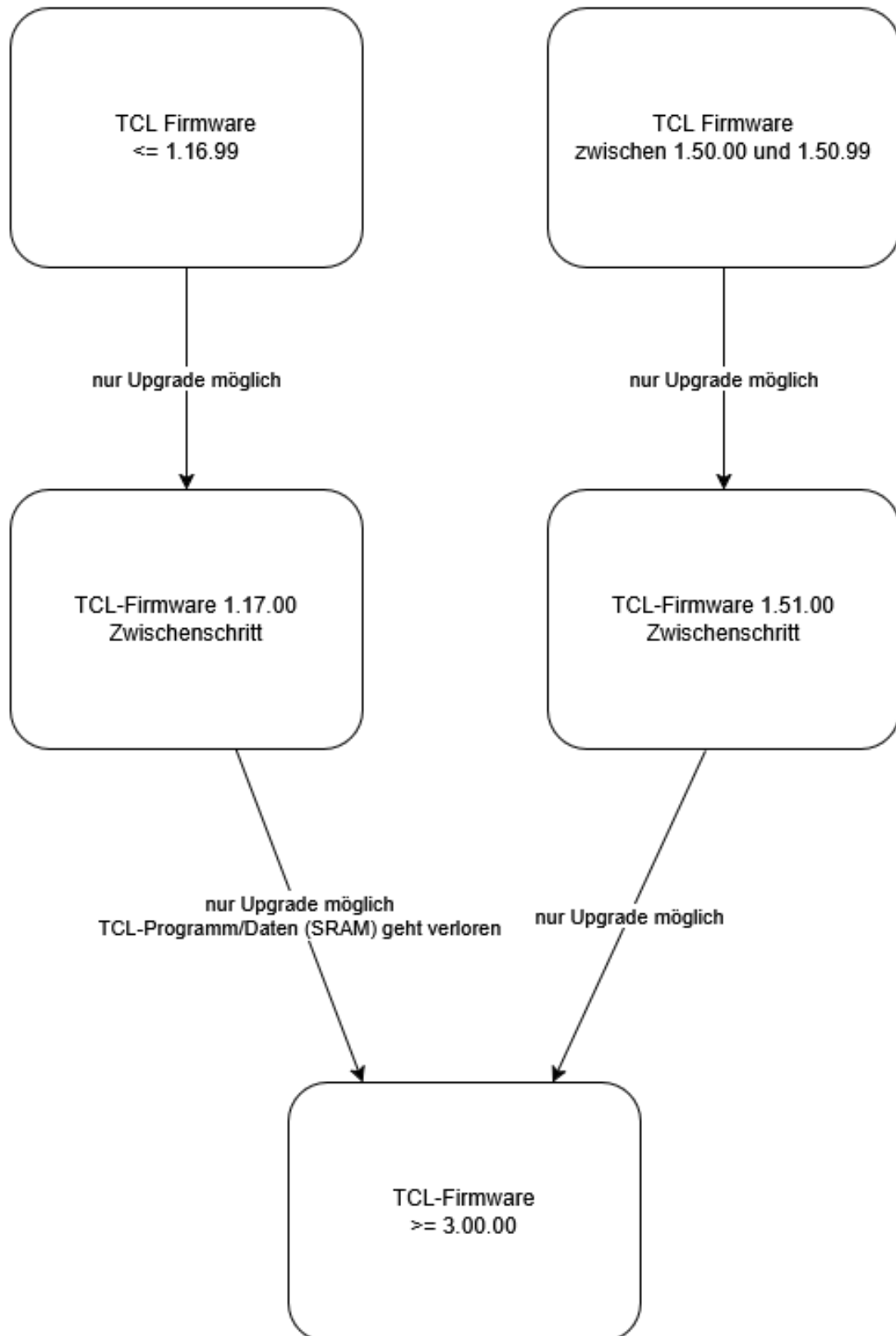


Dieses Kapitel gibt eine Übersicht über die notwendigen Schritte zum Update von älteren Versionen der INTUS TCL Firmware auf Versionen $\geq 3.00.00$.

Die Firmware Version 3.00.00 enthält umfangreiche Änderungen an der Update-Prozedur. Deswegen ist von älteren Versionen kein direktes Update auf Versionen $\geq 3.00.00$ möglich.

Um die Firmware von älteren Versionen auf Versionen $\geq 3.00.00$ zu aktualisieren, ist deswegen ein Zwischenschritt notwendig.

Firmware Version	Zwischenschritt Version
$\leq 1.16.99$	1.17.00
Zwischen 1.50.00 und 1.50.99	1.51.00



Hinweise:

- Die Zwischen-Versionen 1.17.00 und 1.51.00 sind nicht für den normalen Betrieb gedacht. Sie dienen nur dazu eine Firmware $\geq 3.00.00$ zu installieren.
- Bei Firmware Versionen $\geq 3.00.00$ wird nicht mehr nach Modell unterschieden. Nur ob mit oder ohne VIG (Masken).
- Beim Zurücksetzen des SRAM kann es dazu kommen, dass Buchungen durch den automatisch durchgeführten Kaltstart verloren gehen, wenn sie noch im Notpuffer vorhanden sind. Ein Entleeren des Notpuffers durch eine aktive Verbindung zum übergeordneten System ist somit davor sicherzustellen

Die aktuelle Firmware-Version wird z.B. in INTUS RemoteConf angezeigt:

Firmware-Paket:	1.16.00
Version Monitor:	1.16.00
Version TCL:	6.82
Version INTUS Graph:	1.04.02

Die aktuelle Firmwareversion für Ihr Gerät erhalten Sie über das [PCS Service Center](#).

Sollte die Firmware dort nicht verfügbar sein, wenden Sie sich bitte an unseren Support unter support@pcs.com.

4.9 Gleichzeitiges Ausführen von Aktionen an mehreren Terminals

Viele der Aktionen in RemoteConf können an mehreren ausgewählten Terminals gleichzeitig ausgeführt werden.

Einige der Funktionen in INTUS RemoteConf sind aber nur möglich, wenn ein einzelnes Terminal ausgewählt wurde. In diesen Fällen wird die Schaltfläche deaktiviert, wenn mehrere Terminals ausgewählt sind.

Die folgende Tabelle gibt eine Übersicht:

Schaltfläche	Aktionen an mehreren ausgewählten Terminals möglich
Login	ja
Logout	ja
TCL laden	nein
Statusseite	nein
Konfiguration	nein
LBus-Aktionen	ja
Reset	ja
Firmware updaten	ja
Maske laden	ja
Tastatur laden	ja
Audio laden	ja
Logo laden	ja
Flex Air	nein
IP Setup	nein
Entfernen	ja



Ist eine Schaltfläche in INTUS RemoteConf dennoch deaktiviert, so liegt dies daran, dass mindestens eines der ausgewählten Terminals die Funktion nicht unterstützt.

4.10 Geänderte Inbetriebnahme von Neugeräten

INTUS Geräte die ab August 2025 ausgeliefert werden, haben ein geändertes Vorgehen zur Inbetriebnahme.

In der Werkseinstellung ist der Datenport (siehe Kapitel 9) für diese Geräte deaktiviert.

Die notwendigen Schritte zur Inbetriebnahme können Sie mit INTUS RemoteConf durchführen.

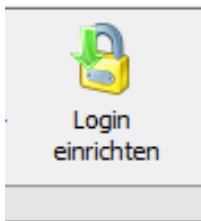
Zuerst muss eine Einrichtung der Login-Einstellungen im INTUS Gerät erfolgen. Die Einrichtung des Logins erfolgt mit "Konfiguration" (Kapitel 7) oder mit "Login einrichten" (siehe Kapitel 4.11)

Die Einrichtung des Logins beinhaltet, dass die Passwörter der drei Berechtigungsstufen geändert werden, so dass sie nicht mehr den jeweiligen Standard-Passwörtern entsprechen.

Ist der Login eingerichtet, so ändert sich die Farbe eines Terminals in INTUS RemoteConf von "dunkelgelb" auf "grün".

Anschließend kann der Datenport des Terminals eingerichtet werden. Die Einrichtung des Datenports erfolgt mit "Konfiguration" (Kapitel 7) oder "Datenport einrichten" (siehe Kapitel 4.12)

4.11 Login einrichten



- Berechtigungsstufe 3
- Für die schnelle Einrichtung oder Änderung der "Login" Einstellungen.
- Die Einstellungsmöglichkeiten werden in Kapitel 6 (Login) beschrieben



Die korrekte und sichere Speicherung von Zugangsdaten wie z. B. Passwörtern und Wartungsgruppen im System liegen in der Verantwortung des Kunden.

Ein Verlust der Passwörter kann zu Sicherheitsrisiken, zur Gefährdung der Systemfunktion, Folgekosten und Zeitverzug führen.

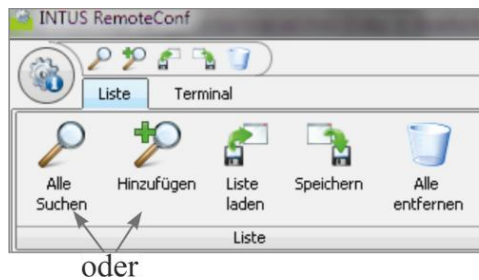
Um technischen Support, eine Projektleitung, Installation oder Ähnliches erhalten zu können, müssen die Passwörter zum entsprechenden Zeitpunkt vorliegen.

4.12 Datenport einrichten



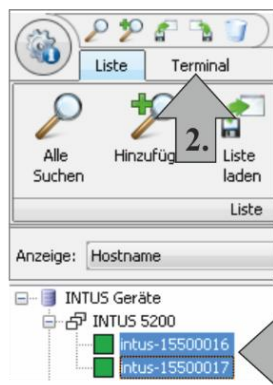
- Berechtigungsstufe 3
- Für die schnelle Einrichtung oder Änderung der "Datenport" Einstellungen.
- Die Schaltfläche ist ausgegraut, solange der Login nicht eingerichtet ist (siehe Kapitel 4.11)
- Die Einstellungsmöglichkeiten werden in Kapitel 9 (Datenport - Kanal A) erklärt

5 Einstieg in die Konfiguration



1. Schritt

Terminalliste aufrufen bzw.
Terminal zur Terminalliste
hinzufügen



2. Schritt

Zum Register „Terminal“ wechseln

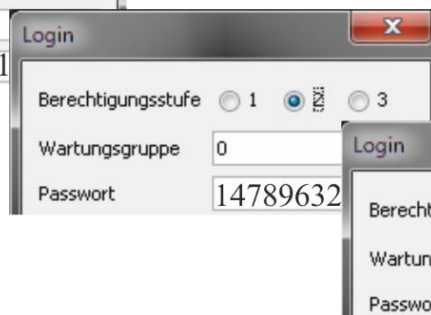
3. Schritt

Ein oder mehrere Terminals
in der Terminalliste auswählen



4. Schritt

Login über Passwort



5. Schritt

Aktion auswählen



Abbildung 5-1: Einstieg in die Konfiguration

6 Login – Einloggen ins Terminal

6.1 Berechtigungsstufen

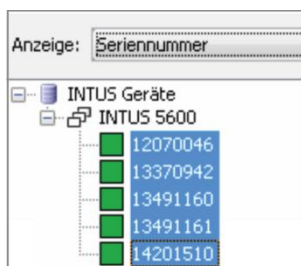
Aus Sicherheitsgründen gibt es drei Berechtigungsstufen, die über Passwörter zugänglich sind.

Berechtigungsstufe	Passwort (voreingestellt)	
1	111111	Passwort der Stufe 1
2	14789632	Passwort der Stufe 1 + 2
3	14589632	Passwort der Stufe 1 + 2 + 3



Über „Konfiguration>Login einrichten“ müssen die Passwörter der Berechtigungsstufen geändert werden.

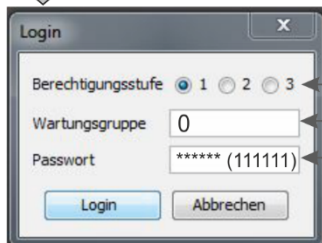
6.2 Vorgehen



Vor dem Login müssen ein oder mehrere Terminals aus der Liste ausgewählt werden.

Beispiel:

INTUS RemoteConf loggt sich an 5 Terminals mit der gleichen Berechtigungsstufe ein.



Berechtigungsstufe auswählen.

Wartungsgruppe: „0“ - Voreinstellung.

Passwort eingeben,
hier Berechtigungsstufe 1; Passwort 111111.

Abbildung 6-1: Einloggen

- Die Berechtigungsstufe wird nach dem Einloggen am Terminal angezeigt (im grünen Kästchen).
- Nach dem Einloggen bleibt Login so lange bestehen, bis ein Logout oder ein System-Reboot durchgeführt wird.
- Bei zu vielen fehlgeschlagenen Authentifizierungsversuchen während der Anmeldung und bei der Verwendung von IP Setup erfolgt eine zeitlich begrenzte Sperre.

7 Konfiguration



Die korrekte und sichere Speicherung von Zugangsdaten wie z. B. Passwörtern und Wartungsgruppen im System liegen in der Verantwortung des Kunden.

Ein Verlust der Passwörter kann zu Sicherheitsrisiken, zur Gefährdung der Systemfunktion, Folgekosten und Zeitverzug führen.

Um technischen Support, eine Projektleitung, Installation oder Ähnliches erhalten zu können, müssen die Passwörter zum entsprechenden Zeitpunkt vorliegen.

7.1 Übersicht

Nach dem Login ist die Konfiguration freigegeben.

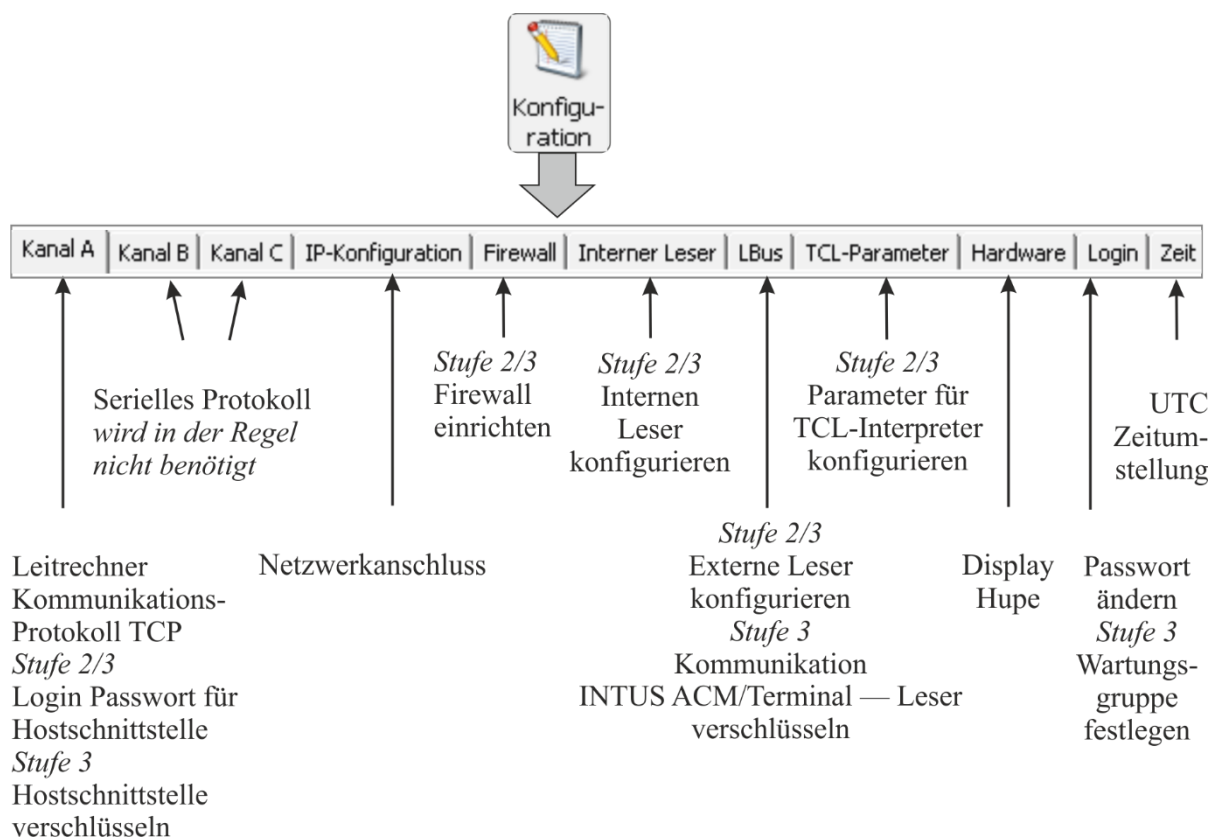


Abbildung 7-1: Übersicht Konfiguration



Abhängig vom Gerät und den verfügbaren Schnittstellen können manche Parameter nicht gültig sein.

7.2 Konfiguration als Datei speichern

Sie haben die Möglichkeit, Teile der Konfiguration in eine Datei abzuspeichern und später diese Datei wieder zu laden. So können Sie auf einfache Art für das aktuelle Terminal wie auch für andere Terminals diese Konfiguration wiederverwenden.

Derzeit speicherbare Teile der Konfiguration sind die Bereiche "Interner Leser", "LBus", und "TCL-Parameter". Diese können beim Speichern ausgewählt werden.

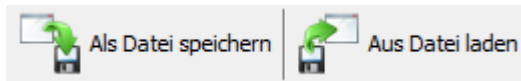
Beim späteren Laden der Datei können Sie wiederum auswählen, welche der zuvor gespeicherten Datenbereiche geladen/verwendet werden sollen.



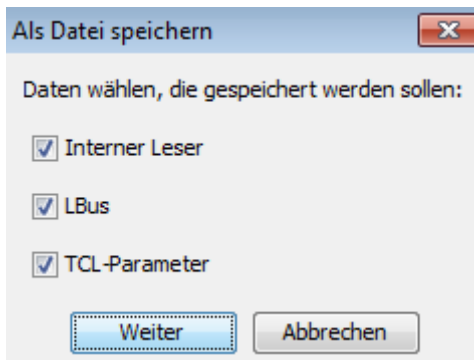
Die Schlüssel zur LBus-Verschlüsselung sind aus Sicherheitsgründen nicht Teil der in der Datei gespeicherten LBus-Konfiguration und müssen jeweils neu vergeben werden.



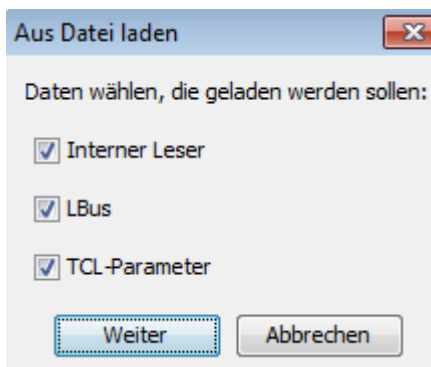
- 1 Klicken Sie auf die Schaltfläche „Als Datei speichern“, um Teile der Konfiguration zu speichern:



- 2 Wählen Sie die zu speichernden Daten aus und wählen Sie den Ablageort der Datei:



- 3 Zum Laden von gespeicherten Konfigurationen klicken Sie auf die Schaltfläche „Aus Datei laden“ (siehe oben) und wählen Sie die Daten aus, die geladen werden sollen:



- 4 Danach senden Sie die Konfiguration, wie im nächsten Kapitel beschrieben, an das Terminal.

7.3 Konfiguration beenden



Einstellungen übernehmen
und an das Terminal senden.
Die neuen Einstellungen sind
sofort gültig.

Abbruch

Abbildung 7-2: Konfiguration beenden

8 Netzwerkanschluss (IP) konfigurieren



Kanal A	Kanal B	Kanal C	IP-Konfiguration	Firewall	Interner Leser	LBus	TCL-Parameter
Standort/Kontakt							
Standort:		Standort Terminal 17110029		Merkmale des Terminals festlegen			
Kontakt:		Ansprechpartner					
IP-Optionen							
DHCP-Hostname:		intus-17110029		Voreinstellung intus-<seriennummer>			
Hostschnittstelle:		LAN ▾		Gegebenenfalls WLAN auswählen			
DNS-Server 1:		::		Gegebenenfalls DNS-Server angeben			
DNS-Server 2:		::					
IPv4							
☒ Aktiviert		☒ DHCP		Voreinstellung IPv4 „DHCP“ Das Gerät bezieht die IPv4 Adresse dynamisch vom DHCP Server			
IPv4-Adresse:		192 . 168 . 42 . 127					
IPv4-Netzmaske:		255 . 255 . 255 . 0					
IPv4-Gateway:		0 . 0 . 0 . 0					
IPv6							
☒ Aktiviert				Voreinstellung IPv6 „RAADV“ Das Gerät generiert eine IPv6 Adresse. In Verbindung mit IPv4 „DHCP“ sind weitere Einstellungen nicht erforderlich.			
Modus:		RAADV ▾					
IPv6-Adresse:		2001::					
IPv6-Gateway:		☒ Gateway aus RADV					
		::					
Ethernet							
Eth-Link:		Auto Negotiation ▾		Voreinstellung Gegebenenfalls IEEE 802.1X auswählen			
IEEE 802.1X:		☐ Aktiviert					
WLAN							
Informationen zu den Einstellungen für das WLAN finden Sie im anschließenden Kapitel							
IEEE 802.1X / WPA2-Enterprise							

Abbildung 8-1: Netzanschluss konfigurieren



IPv6 sollte nicht ohne Grund deaktiviert werden. IPv6 erleichtert die Kommunikation mit dem Terminal.

IP-Optionen

DHCP- Hostname

Bezieht das Terminal seine IP-Konfiguration von einem DHCP-Server, so sendet es diesem auch DHCP „Hostname“ (Option).

Der DHCP Hostname kann bis zu 18 Stellen lang sein und aus alphanumerischen Zeichen sowie dem Bindestrich bestehen. Dabei ist zu beachten, dass er mit einem Buchstaben beginnt und nicht mit einem Bindestrich endet.

Die Voreinstellung ist intus-<Seriennummer>.

DNS-Server

Ein DNS-Server wird z. B. benötigt, wenn bei „Host Kommunikation“ die HTTPS Client Einstellung verwendet wird (siehe Kapitel 9).

In der Regel werden dem Terminal die DNS-Server per DHCP oder RDNSS mitgeteilt.

Zusätzlich können hier bis zu 2 feste DNS-Server (IPv4 oder IPv6 Adresse) angegeben werden.

Es werden maximal 3 DNS-Server verwendet. Höchste Priorität haben die gegebenenfalls über Mobilfunk konfigurierten DNS-Server. Dann folgen RDNSS, DHCPv6 und DHCP. Niedrigste Priorität haben die hier konfigurierten festen DNS-Server.

IPv4 / IPv6 Adresse



Soll das Terminal mit einer festen Adresse betrieben werden, informieren Sie sich beim Netzverwalter über die einzustellende IP-Adresse.

IPv4 Netzmaske

Subnetz-Maske des lokalen Netzes, in dem das Terminal installiert ist.

Die Voreinstellung ist 255.255.255.000. Sie ist für die meisten Netze brauchbar. Informieren Sie sich beim Netzverwalter über die einzustellende Subnetz-Maske.

IPv6 Adresse dynamisch beziehen

Einstellung bei dynamischer Adressvergabe:

- RADV (router advertisement; Voreinstellung) das Terminal generiert sich gegebenenfalls automatisch eine IPv6 Adresse gemäß den Vorgaben des lokalen Routers.
- DHCP - es wird über stateful DHCP eine IPv6 Adresse bezogen.

IPv4 / IPv6 Gateway

IP-Adresse des Routers:

Diese Adresse muss immer dann eingestellt werden, wenn Leitrechner und Terminal in verschiedenen logischen Subnetzen hängen. Informieren Sie sich beim Netzverwalter über die einzustellende IP-Adresse.

IPv6 Präfixlänge

Länge des Präfixes (1-128Bit) des lokalen Netzes.

In der Regel werden 64Bit (Voreinstellung) zugewiesen.

Ethernet

Eth-Link (Geschwindigkeit)

Mit diesem Parameter wird die Geschwindigkeit festgelegt.

Auto Negotiation oder feste Übertragungsrate (10BASE-T, 100BASE-TX jeweils half duplex oder full duplex) stehen zur Auswahl.

Die Voreinstellung ist Auto Negotiation.



Diese Einstellung muss mit der Gegenseite übereinstimmen, ansonsten kommt es zu Kommunikationsproblemen!

IEEE 802.1X

Authentifizierung des Terminals im Ethernet-Netzwerk.

Informationen zur Konfiguration finden Sie in Kapitel 8.2.

8.1 WLAN

Gültig für die Terminals INTUS 5200 & INTUS 5320 & INTUS 5500/ 5540 & INTUS 5600.

Alle Information zum WLAN erhalten Sie von ihrem Netzwerkverwalter.

IP-Optionen

DHCP-Hostname: intus-52PROTO5

Hostschnittstelle: WLAN WLAN auswählen

WLAN

Regulierungsbereich:* World Die Ländercode-Einstellung legt den Frequenzbereich fest, in dem das Netzwerk arbeitet.

SSID * Name des WLANs

BSSID: Eindeutige Adresse des WLANs

Sicherheitstyp: WPA2-PSK

Netzwerkschlüssel (PSK):** (nicht) Informieren Sie sich beim Netzwerkverwalter

☐ Schlüssel anzeigen

☒ beibehalten ☐ ändern

Abbildung 8-2: WLAN

* Diese Angaben sind unbedingt erforderlich. Die SSID muss in den WLAN-Einstellungen des Access Points als sichtbar konfiguriert sein.

** Unbedingt erforderlich bei WPA2-PSK.

WLAN als Hostschnittstelle

Ist im Terminal WLAN vorhanden und WLAN als Hostschnittstelle aktiviert, dient die Ethernet-Schnittstelle als Service-Schnittstelle.

Die Service-Schnittstelle hat folgende feste Netzwerk-Einstellungen:

- IPv6 ist aktiviert mit Link-Local-Adresse
- IPv4 Adresse 192.168.42.127
- IPv4 Netzmaske 255.255.255.0

Falls sich die WLAN-Schnittstelle in diesem Netzwerk befindet, hat die Ethernet-Schnittstelle die IPv4 Adresse 10.10.42.127.

Bei Verwendung der Service-Schnittstelle sind die Aktionen von INTUS RemoteConf beschränkt auf:

- Konfiguration ändern
- Statusseite abrufen

Die Service-Schnittstelle sollte nur bei der Inbetriebnahme oder im Wartungs-Fall verwendet werden. Im normalen Betrieb sollte kein Netzkabel angeschlossen sein.

8.2 IEEE 802.1X/WPA2-Enterprise

802.1X/WPA2-Enterprise muss konfiguriert werden, wenn:

- WLAN-Sicherheitstyp WPA2-Enterprise ausgewählt ist oder
- Ethernet 802.1X aktiviert ist



IEEE 802.1X / WPA2-Enterprise

Authentifizierung: ---

Anonyme Identität: ☐

CA-Zertifikat: (nicht konfiguriert)

Innere Authentifizierung: * ---

Benutzername:

Passwort: (nicht konfiguriert)

Client-Zertifikat: (nicht konfiguriert)

Privater Schlüssel: (nicht konfiguriert)

Passwort privater Schlüssel: (nicht konfiguriert)

☐ Passwort anzeigen

An die Zertifikate werden folgende Anforderungen gestellt:

- Die Datei enthält nur X.509 Zertifikate (keine Schlüssel)
- Anzahl der Zertifikate:
CA-Zertifikat: 1 bis 5
Client-Zertifikat: genau 1
- PEM oder DER-Kodierung
- Gültiger Common Name

☒ beibehalten ☐ ändern

☒ Die Datei enthält genau einen privaten Schlüssel

☒ Base64 oder DER-Kodierung

☐ beibehalten ☐ löschen ☐ ändern

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

Authentifizierung / Innere Authentifizierung

Es werden folgende Methoden unterstützt:

- EAP-MD5 (nur bei Ethernet 802.1X)
- 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

Anforderung an „Privater Schlüssel“

- Die Datei enthält genau einen privaten Schlüssel
- PEM oder DER-Kodierung

Mit diesen Informationen sollte ihr Systemadministrator das WLAN konfigurieren können.



Über Reset ist es möglich, alle Einstellungen, sicherheitsrelevante Informationen und Passwörter zurückzusetzen, siehe Kapitel 19.

8.3 Mobilfunk



Einstellungen für Mobilfunk müssen angegeben werden, wenn als Host-Schnittstelle "Mobilfunk" konfiguriert ist.

Die Werte, die Sie hier eintragen müssen, hängen von Ihrem Mobilfunk-Anbieter ab.

The screenshot shows a configuration window titled 'Mobilfunk'. It has four input fields: 'APN:', 'Benutzername:', 'Passwort:', and 'PIN:'. The 'PIN:' field contains the text '(konfiguriert)'. Below these fields, there is a checkbox labeled 'PIN anzeigen' which is unchecked. To its right, there are two radio buttons: 'beibehalten' (selected) and 'ändern' (unselected).

Abbildung 8-4: Mobilfunk

- Die Eingabe von APN und PIN ist erforderlich.
- Benutzername/Passwort hängen vom jeweiligen Netzbetreiber ab.

Mobilfunk als Hostschnittstelle

Ist im Terminal Mobilfunk vorhanden und Mobilfunk als Hostschnittstelle aktiviert, dient die Ethernet-Schnittstelle als Service-Schnittstelle.

Die Service-Schnittstelle hat folgende feste Netzwerk-Einstellungen:

- IPv6 ist aktiviert mit Link-Local-Adresse
- IPv4 Adresse 192.168.42.127
- IPv4 Netzmaske 255.255.255.0

Falls sich die interne Mobilfunk-Modem-Schnittstelle in diesem Netzwerk befindet, hat die Ethernet-Schnittstelle die IPv4 Adresse 10.10.42.127.

Bei Verwendung der Service-Schnittstelle sind die Aktionen von INTUS RemoteConf beschränkt auf:

- Konfiguration ändern
- Statusseite abrufen

Die Service-Schnittstelle sollte nur bei der Inbetriebnahme oder im Wartungs-Fall verwendet werden. Im normalen Betrieb sollte kein Netzkabel angeschlossen sein.

9 Datenport (Kanal A) einstellen

Default-Einstellung ist "nicht konfiguriert", ein INTUS Gerät muss auf Kommunikationsprotokoll TCP oder HTTPS Client eingestellt werden.

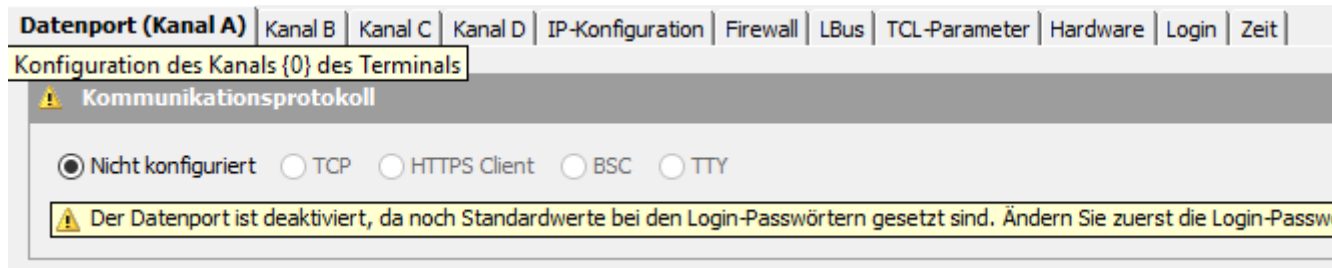


Abbildung 9-1: Kanal A - Nicht konfiguriert

9.1 Einstellungen Protokoll TCP

Verbindungsaufbau

Steuert die Art (Client/Server) des Verbindungsaufbaus:

passiv

Voreinstellung. Das Terminal (Server) öffnet einen TCP Port mit der eingestellten Port-Nummer und wartet auf Verbindungsanforderungen des Leitrechners (Client).

Ist eine Verbindung aufgebaut und hat 1 Minute lang kein Datentransfer stattgefunden, so sendet das Terminal ein "Keep Alive" Paket, um festzustellen, ob die Verbindung noch besteht.

Dadurch wird ein ungeordneter Verbindungsabbruch rasch entdeckt und die schnelle Umschaltung zwischen einem Online- und Offline-Modus ermöglicht.

passiv/RAS

Diese Einstellung ist für TCP/IP-Verbindungen über ISDN-Wählleitungen geeignet, die bei ausbleibendem Datenaufkommen automatisch wieder abgebaut werden, ohne dass auch die logische TCP/IP-Verbindung getrennt wird: Der Wert passiv/RAS versetzt das Terminal – genauso wie der oben beschriebene Wert passiv – in den passiven Server-Modus, aber die Zeitspanne zwischen den "Keep-Alive" Paketen wird von einer Minute auf zwei Stunden erhöht, sodass die Kommunikationskosten auf Wählleitungen gesenkt werden.

aktiv

Beim Betrieb mit dem Wert aktiv muss der Leitrechner (Server) einen TCP Port mit der eingestellten Port-Nummer öffnen und auf Verbindungsanforderungen des Terminals (Client) warten. Das Terminal wiederholt seine Verbindungsanforderungen periodisch so lange, bis eine Verbindung hergestellt werden kann. Dieses Verfahren bietet eine höhere Sicherheit, da die Verbindung nur zu einem Leitrechner aufgebaut werden kann. "Keep Alive" Pakete werden wie beim Wert passiv versendet.

"Keep Alive on Demand": Wenn beim Terminal, das im passiven Server-Modus betrieben wird, eine Verbindungsanforderung für den TCL Port eintrifft, obwohl noch

eine Verbindung besteht, wird die Anforderung abgelehnt. Anschließend versucht das Terminal durch ein "Keep-Alive" Paket festzustellen, ob diese Verbindung in der Tat noch existiert oder ob sie bereits ungeordnet abgebrochen wurde. Wenn die Verbindung nicht mehr besteht, wird der TCP/IP Protokollstack des Leitrechners auf diese "Keep-Alive" Pakete mit einem TCP Reset Paket antworten und damit die Verbindung sofort beenden.

Bleibt diese Antwort des Leitrechners aus, dauert es maximal 6 Minuten, bevor das Terminal die Verbindung als abgebrochen erkennt und eine andere Verbindung zulässt.

Bei einer ungeordnet abgebauten Verbindung wird der Leitrechner in jedem Fall mindestens eine Verbindungsanforderung (connect) mit einer Ablehnung (ECONNREFUSED oder ECONNABORT) beantwortet bekommen, bevor die Verbindung aufgebaut werden kann.

Dieser Tatsache muss die Implementierung auf dem Leitrechner Rechnung tragen und eine Reihe von Verbindungsaufbauversuchen zulassen.

Datenport (Kanal A) | Kanal B | Kanal C | Kanal D | IP-Konfiguration | Firewall | LBus | TCL-Parameter | Hardware | Login | Zeit

Kommunikationsprotokoll

☐ Nicht konfiguriert ☒ TCP ☐ HTTPS Client ☐ BSC ☐ TTY

TCP-Einstellungen

Verbindungsaufbau: Port:

IPv4/IPv6-Adresse:

Sicherheitseinstellungen

Verschlüsselung: ☒ deaktiviert ☐ TCL ☐ TCL-V2

Login: ☒ deaktiviert ☐ MONOUT ☐ transparent

Passwort für einfachen Zugriff:

☐ Passwort anzeigen

Passwort für administrativen Zugriff:

☐ Passwort anzeigen

Sendedatensatz-Format: Routingbytes:

Satznummernzeichen für Login-Meldungen:

Port

Port-Nummer der Leitrechnerverbindung des Terminals, der Wert ist dezimal dargestellt. Die Voreinstellung ist 3001.

Die Port-Nummer sollte normalerweise nicht verändert werden. Port 22, 80 und 3123 sind nicht möglich.

IPv4 / IPv6-Adresse

Leitrechneradresse; ist nur erforderlich, wenn beim Verbindungsaufbau aktiv gewählt wurde. Die Voreinstellung sollte ansonsten nicht verändert werden.

Voreinstellung

IPv4 - 000.000.000.000 bzw.

IPv6 - :: steht für 0000:0000:0000:0000:0000:0000:0000:0000

Eine IPv4-Adresse kann auch im IPv6-Format angezeigt werden, zum Beispiel

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

9.2 Einstellungen Protokoll HTTPS Client

Alle einzutragenden Parameter hängen von der eingesetzten Software-Lösung des Hosts ab. Bei Verbindungen zu Hosts, die gewisse Reverse-Proxy Lösungen einsetzen, kann es notwendig sein, die Option "Content-Length Header senden" zu aktivieren. Diese Option sollte nur aktiviert werden, falls dies notwendig ist.



Abbildung 9-2: HTTPS Client Einstellungen

Die URL zur Kommunikation mit dem Host wird aus Hostname, Port und Verzeichnis gebildet.

Zur Authentifizierung gegenüber dem Host werden Benutzername und Passwort verwendet (Basic Authentication).

Das CA-Zertifikat dient der Prüfung des Server-Zertifikats.

Es werden Zertifikate im PEM-Format akzeptiert. In der Datei dürfen bis zu 10 einzelne Zertifikate zusammengefasst werden.

Ab Geräte-Firmware 1.08 kann mittels der Option "Online-Update" ein automatisches Update des CA-Zertifikats durch den Host aktiviert werden. Die eingesetzte Software-Lösung des Hosts muss dies unterstützen.

Nähere Informationen hierzu finden Sie auch im INTUS TCL Programmierhandbuch D3000-004.

9.3 Sicherheitseinstellungen

Verschlüsselung der Hostschnittstelle bei Protokoll TCP

Berechtigungsstufe 3

Es ist möglich, den verschlüsselten Datentransfer zwischen Host und TCL Interpreter einzustellen.



Über "Schlüssel erzeugen" können Sie den Passphrase mit maximal 512 Zeichen eingeben. Daraus wird ein Schlüssel für die Übertragung generiert.

Login auf der Hostschnittstelle

Berechtigungsstufe 2/3

Es ist möglich, ein Passwort sowie Routingbytes für die Kommunikation mit dem TCL Interpreter (MONIN und MONOUT Prozess) einzustellen.

Passwort für einfachen Zugriff

Das Terminal kann Datensätze versenden, verarbeitet aber nur „J“- Datensätze und Quittungssätze.

Passwort für administrativen Zugriff

Es gibt keine Einschränkungen.

Nähere Informationen hierzu finden Sie im INTUS TCL Programmierhandbuch D3000-004.

10 Firewall konfigurieren

Berechtigungsstufe 2 / 3



Durch das Aktivieren der Firewall wird ein unberechtigter Netzwerkzugriff auf das Terminal verhindert. Um einen Betrieb zu ermöglichen, müssen die Dienste Daten und Wartung jeweils für Netzwerkteilnehmer freigegeben werden. Die Freigabe des Dienstes Status ist optional und wird für den Betrieb nicht benötigt.

Für eine Erklärung der Begriffe Daten, Wartung und Status siehe Kapitel 22.

Die Einschränkungen für den Dienst Daten sind genau dann aktiv, wenn der Datenport (Kanal A) im Betriebsmodus TCP / passiv genutzt wird.

Die Netzadresse in Verbindung mit der Netzwerkmaske bzw. Präfix legen fest, wie viele und welche Netzwerkteilnehmer Zugangsberechtigungen für die jeweiligen Dienste erhalten.

Die Anzahl der Netzwerkteilnehmer wird dabei von der Netzwerkmaske bzw. Präfix vorgegeben, sie errechnet sich mit Hilfe des Binärcodes. Der größte Wert beträgt 255.255.255.255 (IPv4) bzw. 128 (IPv6). Das heißt, nur ein Netzwerkteilnehmer hat die eingestellten Zugangsberechtigungen.

Der kleinste Wert beträgt 0.0.0.0 (IPv4) bzw. 0 (IPv6). Das heißt, alle Netzwerkteilnehmer unabhängig von ihrer Netzadresse haben die jeweils eingestellten Zugangsberechtigungen.

Jeweils 5 Freigabe-Einträge für IPv4 bzw. IPv6 können hinterlegt werden. Wenn für eine Dienst-Anfrage eines Netzwerkteilnehmers keine der Freigaben-Einträge zutrifft, dann wird diese Anfrage verworfen.

Weitere Informationen über Netzadresse und Netzwerkmaske erhalten Sie von Ihrem Netzwerkverwalter.

Voreinstellung

Die Firewall ist nicht konfiguriert.

The screenshot shows the 'Firewall' configuration page. At the top, there is a navigation bar with tabs: Datenport (Kanal A), Kanal B, Kanal C, Kanal D, IP-Konfiguration, **Firewall**, LBus, TCL-Parameter, Hardware, Login, and Zeit. Below the navigation bar, the 'Firewall' section is active. It contains a checkbox labeled 'Firewall aktivieren' which is unchecked. Below this, there are two tables for configuring firewall rules.

IPv4-Netzadresse	IPv4-Netzmaske	Wartung	Daten	Status
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-Adresse	IPv6-Präfix	Wartung	Daten	Status
fe80::	/ 64	☒	☐	☒
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐

Abbildung 10-1: Firewall Beispiel-Konfiguration

In Abbildung 10-2 finden Sie als Beispiel eine Konfiguration, die den Zugriff auf Wartung und Daten für alle Netzwerkteilnehmer freigibt, aber den Zugriff auf den Status gar nicht freigibt.

Dazu wurde ein Freigabe-Eintrag für IPv4 und ein Freigabe-Eintrag für IPv6 eingetragen.

The screenshot shows the 'Firewall' configuration page with the same navigation bar as in the previous image. The 'Firewall aktivieren' checkbox is checked. The configuration tables are as follows:

IPv4-Netzadresse	IPv4-Netzmaske	Wartung	Daten	Status
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-Adresse	IPv6-Präfix	Wartung	Daten	Status
::	/ 0	☒	☒	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐
::	/ 64	☐	☐	☐

Abbildung 10-2: Status nicht freigegeben

11 LBus konfigurieren

Berechtigungsstufe 2 / 3

Zur Verbesserung der Lesbarkeit wird nachfolgend der Begriff „Leser“ verwendet, auch wenn es sich um INTUS Flex Endgeräte handelt

- Ein LBus ist die Schnittstelle zum Anschluss von externen Lesern.
- Bei der LBus-Konfiguration werden die verfügbaren LBus-Schnittstellen mit der entsprechenden Platinenbeschriftung angezeigt.
- **HW-Adresse** bezeichnet die Leseradresse, die bei jedem Leser manuell eingestellt werden muss. Informationen finden Sie in der Installationsanleitung des Lesers.
- **TCL-Adresse** ist die logische Adresse des Lesers.
- **Point-to-Point (PP)**: Wird 1 Leser an eine LBus-Schnittstelle angeschlossen, wird dies bei PCS Point-to-Point (PP) genannt
- **MultiPoint (MP)**: Werden mehrere Leser als Reihe an eine LBus-Schnittstelle angeschlossen, wird dies bei PCS MultiPoint (MP) genannt.



Im Falle des Anschlusses von INTUS Flex Endgeräten mittels des INTUS Flex Gateways: Ein Gateway kann zwar direkt "Point-to-Point" angeschlossen sein, wenn aber mehrere Zylinder gekoppelt werden sollen, muss in TCL "MultiPoint" eingestellt werden.



Beim INTUS 315ro lässt sich keine Adresse einstellen. Daher ist für diesen Leser kein MultiPoint Anschluss möglich.

Der Lesertyp OSDP unterstützt derzeit nur die INTUS Flex Endgeräte. Andere OSDP-Leser müssen durch PCS geprüft und freigegeben werden!

11.1 Maximal mögliche Anzahl Leser

Gerät	Anzahl der Leser		Bemerkung
	LBus 1	LBus 2	
INTUS 5200	1	----	Option
INTUS 5320	4	----	
INTUS 5500/5540/5600	8	8	
INTUS ACM80e Rack	8	8	Standard 8 Leser, Option 16 Leser
INTUS ACM80e Wand	8	8	Standard 4 Leser, Option 8 bzw. 16 Leser
INTUS ACM40e	8	8	Standard 2 Leser, Option 4 Leser Mit ACM40e Wiegand-Modul: + 4 Wiegand Leser Mit 4Flex-Lizenz*: + 4 INTUS Flex Endgeräte Mit 16Flex-Lizenz*: +16 INTUS Flex Endgeräte

* Mit einem ACM40e in der Grundausstattung, also ohne INTUS Flex-Lizenz, können keine INTUS Flex Endgeräte betrieben werden.

11.2 Verkabelung beim INTUS 5200/5320/5500/5540/5600

Verkabelung LBus1/LBus2



Nur die Einstellung MultiPoint / MultiPoint ist für nicht-ACM-Geräte möglich:

INTUS 5500/5540/5600 jeweils max. 8 Leser pro Schnittstelle (Option)

INTUS 5200 ein Leser pro Schnittstelle (Option)

INTUS 5200

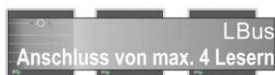
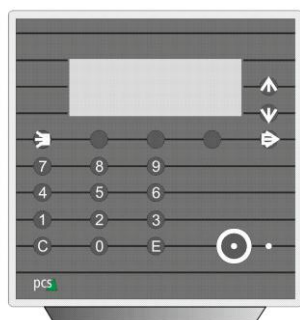


Anschluss: maximal ein Leser

Entfernung: maximal 10m



INTUS 5320



← LBus-Länge

INTUS 5500/5540/5600

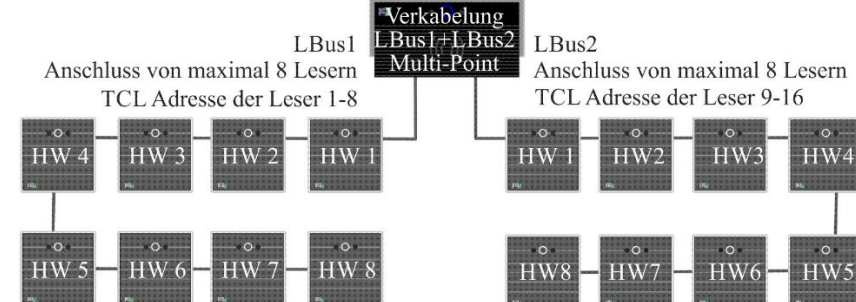


Abbildung 11-1: Verkabelung beim INTUS 5200/5320/5500/5540/5600



Die HW(Hardware)-Adresse muss bei jedem Leser eingestellt werden. Informationen hierzu finden Sie im Installationshandbuch des Lesers.

11.3 Verkabelungsmöglichkeiten beim INTUS ACM40e

Verkabelung LBus1 /LBus2	INTUS ACM40e Leserschnitt- stelle	Leser pro Schnittstelle	Leser HW-Adresse	
			einfache	feste
Verkabelung LBus 1 ☐ Multi-Point ☒ Point-to-Point Verkabelung LBus 2 ☒ Multi-Point ☐ Point-to-Point	Leser 1 bis Leser 4 -----	Jeweils 1 Leser pro Schnittstelle Max. 4 Leser	1	1 bis 4
Verkabelung LBus 1 ☐ Multi-Point ☒ Point-to-Point Verkabelung LBus 2 ☐ Multi-Point ☒ Point-to-Point	Leser 1 bis Leser 2 Leser 3 bis Leser 4	Jeweils 1 Leser pro Schnittstelle Max. 4 Leser	1	1 bis 2 1 bis 2
Verkabelung LBus 1 ☒ Multi-Point ☐ Point-to-Point Verkabelung LBus 2 ☒ Multi-Point ☐ Point-to-Point	Leser 1 bis Leser 2 Leser 3 bis Leser 4	Max. 8 Leser auf die Leserschnitt- stellen verteilt	---	1 bis 4 1 bis 4

Die tatsächlich mögliche Anzahl an Lesern wird durch die vorhandenen Leserlizenzen bestimmt.

11.4 Verkabelungsmöglichkeiten beim INTUS ACM40e mit Wiegand-Modul

Verkabelung LBus1 /LBus2	INTUS ACM40e Leserschnitt- stelle	Leser pro Schnittstelle	Leser HW-Adresse	
			einfache	feste
Verkabelung LBus 1 ☐ Multi-Point ☒ Point-to-Point Verkabelung LBus 2 ☐ Multi-Point ☒ Point-to-Point	Wiegand 1 bis 2 Wiegand 3 bis 4	Max. 4 Leser auf die Leserschnitt- stellen verteilt	---	---
	Leser 1 bis 2 Wiegand 1 bis 4	Max. 6 Leser auf die Leserschnitt- stellen verteilt	1 ---	1 bis 2 ---
	Wiegand 1 bis 4 Leser 1 bis 2	Max. 6 Leser auf die Leserschnitt- stellen verteilt	--- 1	--- 1 bis 2

11.5 Verkabelungsmöglichkeiten beim INTUS ACM80e

Verkabelung LBus1 /LBus2	INTUS ACM80e Leserschnitt- stelle	Leser pro Schnittstelle	Leser HW-Adresse	
			einfache	feste
Verkabelung LBus 1 ☐ Multi-Point Verkabelung LBus 2 ☒ Point-to-Point ☒ Multi-Point ☐ Point-to-Point ☐ Point-to-Point	Leser 1 bis Leser 8 -----	Jeweils 1 Leser pro Schnittstelle Max. 8 Leser	1	1 bis 8
Verkabelung LBus 1 ☐ Multi-Point Verkabelung LBus 2 ☒ Point-to-Point ☐ Multi-Point ☐ Point-to-Point ☒ Point-to-Point	Leser 1 bis Leser 4 Leser 5 bis Leser 8	Jeweils 1 Leser pro Schnittstelle Max. 8 Leser	1	1 bis 4 1 bis 4
Verkabelung LBus 1 ☒ Multi-Point Verkabelung LBus 2 ☐ Point-to-Poi ☒ Multi-Point ☐ Point-to-Point ☐ Point-to-Point	Leser 1 bis Leser 4 Leser 5 bis Leser 8	Max. 16 Leser auf die Leserschnitt- stellen verteilt	---	1 bis 8 1 bis 8

INTUS ACM80e mit zusätzlicher LBus2 Schnittstelle (Option)

Verkabelung LBus1/LBus2



Wählen Sie: Point-to-Point für die Schnittstellen Leser1 bis Leser8 / MultiPoint für die optionale LBus2-Schnittstelle.

11.6 Point-to-Point-Verkabelung des INTUS ACM80e

HW-Adresse der Leser*

Einfache Adressierung aktiviert: Leser HW-Adresse 1

Feste Leser HW-Adresse: LBus1 1 - 8;

LBus1+LBus2 1 - 4 + 1 - 4

TCL Adresse der Leser

LBus1: 1 - 8

LBus1 + LBus2: 1 - 4 + 9 - 12

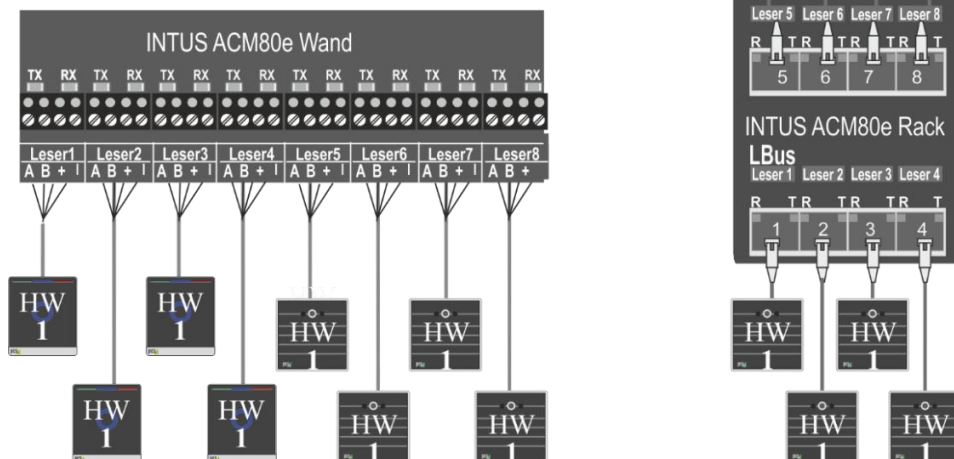


Abbildung 11-2: Point-to-Point-Verkabelung des INTUS ACM80e

Die tatsächlich mögliche Anzahl an Lesern wird durch die vorhandenen Leserlizenzen bestimmt.

11.7 MultiPoint-Verkabelung des INTUS ACM80e

Wie die Leser auf die Leser-Schnittstellen bzw. Steckplätze verteilt werden, hängt von den individuellen Umständen der Installation ab.

Die HW-Adresse der Leser* wird im Bereich 1 - 8 individuell festgelegt.

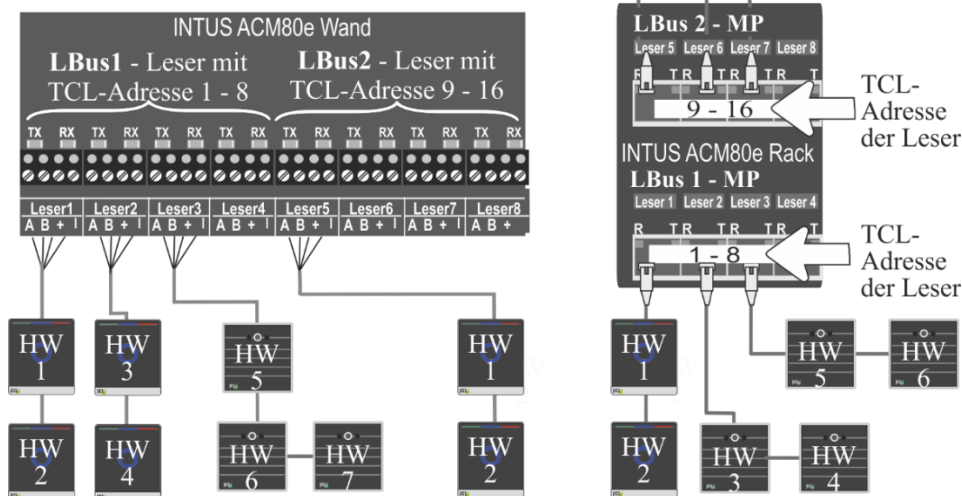


Abbildung 11-3: MultiPoint-Verkabelung des INTUS ACM80e



* Die HW(Hardware)-Adresse muss bei jedem Leser eingestellt werden. Informationen hierzu finden Sie im Installationshandbuch des Lesers.

11.8 Leser konfigurieren



Kanal A | Kanal B | Kanal C | IP-Konfiguration | Firewall | Interner Leser | **LBus** | TCL-Parameter

LBus (0 Leser konfiguriert, 16 Leser möglich)

LBus 1
LBus 2

1. Schritt:
LBus wählen
Verkabelung festlegen

Verkabelung LBus 1

☐ Multi-Point
☒ Point-to-Point

Verkabelung LBus 2

☒ Multi-Point
☐ Point-to-Point

LBus (0 Leser konfiguriert, 16 Leser möglich)

LBus 1
LBus 2

2. Schritt:
LBus1 oder *LBus2* auswählen

3. Schritt:
Lesertyp festlegen

LBus 1

Lesertyp:

☐ nicht konfiguriert
☒ INTUS 700/6xx/5x0/4x0/1600/1500/350H
☐ INTUS 300H/340H
☐ INTUS 300L/300M
☐ INTUS 300ro/315ro

☒ einfache Adressierung

Schlüssel erzeugen

Point-to-Point empfohlene Einstellung

LBus (0 Leser konfiguriert, 16 Leser möglich)

LBus 1
LBus 2

4. Schritt:
Leserschnittstelle auswählen

LBus 1/Leser 1

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
1	1	nicht konfiguriert	☐

nicht konfiguriert
Modus A 2x16 Zeichen Display, INTUS 1500, INTUS 610moto
Modus B Voreinstellung
Modus C erweiterte Tastaturfunktionalität, INTUS 1600-II

5. Schritt:
Betriebsart für den angeschlossenen Leser festlegen

LBus (1 Leser konfiguriert, 16 Leser möglich)

LBus 1
LBus 2

Der Leser ist konfiguriert

Abbildung 11-4: Leser konfigurieren



Bei den Terminals INTUS 5200/5320/5500/5540/5600 entfällt der 1. Schritt, da für LBus1 und LBus2 nur MultiPoint-Verkabelung möglich ist.

11.9 Lesertyp / einfache Adressierung

Mit der Einstellung des Lesertyps wird die Kommunikation am LBus festgelegt, aber noch kein Leser konfiguriert.



Gültig für folgende Leser:
 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
 empfohlene Einstellung



Abbildung 11-5: Lesertyp / einfache Adressierung

* Beim INTUS 350H bzw. INTUS 640H ist die Einstellung des Leser-Typs davon abhängig, ob LBus-Protokoll oder 340H-Protokoll am Leser konfiguriert ist.

Folgende Einstellung ist erforderlich:

- LBus-Protokoll „Leser-Typ: INTUS 700/6xx/.../350H“
- 340H-Protokoll „Leser-Typ: INTUS 300H/340H“

Siehe auch INTUS 350H bzw. INTUS 640H Installationsanleitung.

Bei gleicher „Lesertyp“-Einstellung der Leser ist ein Mischbetrieb möglich. Bitte beachten Sie bei Mischbetrieb die maximale LBus-Länge!

Einfache Adressierung aktiviert, nur INTUS ACM

Bei Point-to-Point-Verkabelung sollte einfache Adressierung aktiviert werden. So kann es zu keinem Konflikt der Leseradresse (1) und der Leser-Kennzeichnung bzw. TCL-Adresse im Zutrittsserver kommen.

Jeder externe Leser erhält die HW-Adresse1, die in der Regel voreingestellt ist. Die Einstellung sollte dennoch überprüft werden.

11.10 Betriebsart



Für die Konfiguration der Leser ist die Angabe der richtigen Betriebsart unbedingt erforderlich (nicht für Wiegand bzw. INTUS Flex (OSDP)).

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



LBus 1/Leser 1

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
1	1	nicht konfiguriert	☐

nicht konfiguriert

Modus A 2x16 Zeichen Display, INTUS 1500, INTUS 610moto

Modus B Voreinstellung

Modus C erweiterte Tastaturfunktionalität, INTUS 1600-II

Display-Formatierung

Leser	Modus A	Modus B	Modus C
	2 x 16 Zeichen	2 x 20 Zeichen	2 x 20 Zeichen + erweiterte Tastatur-Funktionalität
INTUS 700, 600/615/620, 500IP/520IP, 400/420, 350H, 640H, 600FP, 800FP	-	✓	-
INTUS 1600-II	-	✓	✓
INTUS 1500, 610Moto	✓	-	-
INTUS 1600	✓	✓	-
INTUS PS Controller	-	✓	-

INTUS 300H, INTUS 340H, INTUS 350H/ 640H (mit 340H-Protokoll)

LBus 1/Leser 1

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
1	1	nicht konfiguriert	☐

nicht konfiguriert

ID/SN ID, wenn vorhanden, sonst Seriennummer

SN+ID Seriennummer und ID, wenn vorhanden

SN Seriennummer

ID Identitätsnummer (ID)

SN bzw. ID werden ausschließlich gelesen

INTUS 300L, 300M

Die Einstellung „Standard-Modus“ sollte nur nach Rücksprache mit dem PCS Support verändert werden.

11.11 Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser

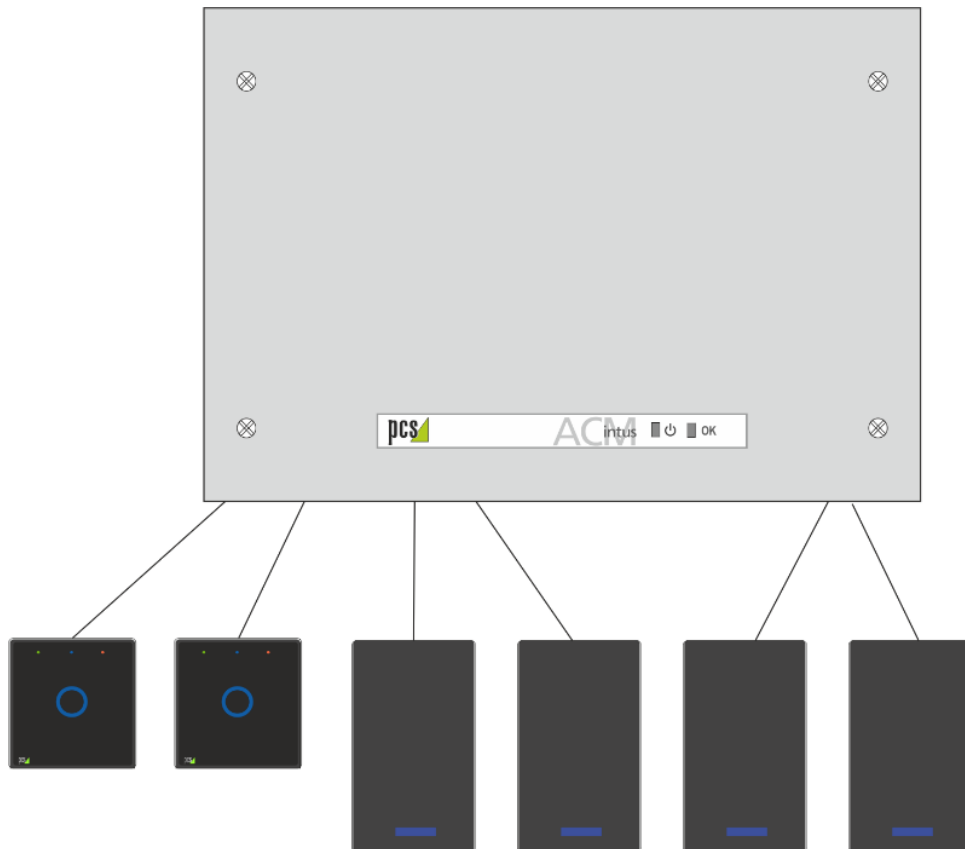


Abbildung 11-6: Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser

Einstellung Verkabelung PP/PP

Verkabelung LBus 1
☐ Multi-Point
☒ Point-to-Point

Verkabelung LBus 2
☐ Multi-Point
☒ Point-to-Point

Einstellung LBus 1

LBus 1

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☐ Wiegand

☐ OSDP

☒ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Einstellung LBus 2

LBus 2

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ Wiegand

☐ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Konfiguration der Leser an "Wiegand 1"

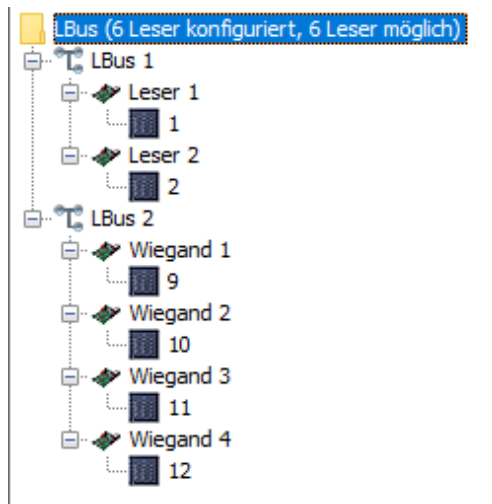
LBus 2/Wiegand 1

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	Standard-Modus	☐

nicht konfiguriert

Standard-Modus Wiegand

Resultat in der Baumansicht



11.12 Beispiel ACM40e mit 16Flex-Lizenz¹ - 16 funkverbundene INTUS Flex-Endgeräte

Sternverkabelung (Konfiguration MP/MP):

- Ein INTUS Flex Gateway ist an "Leser 1"-Schnittstelle angeschlossen.
- Ein INTUS Flex Gateway ist an "Leser 3"-Schnittstelle angeschlossen.

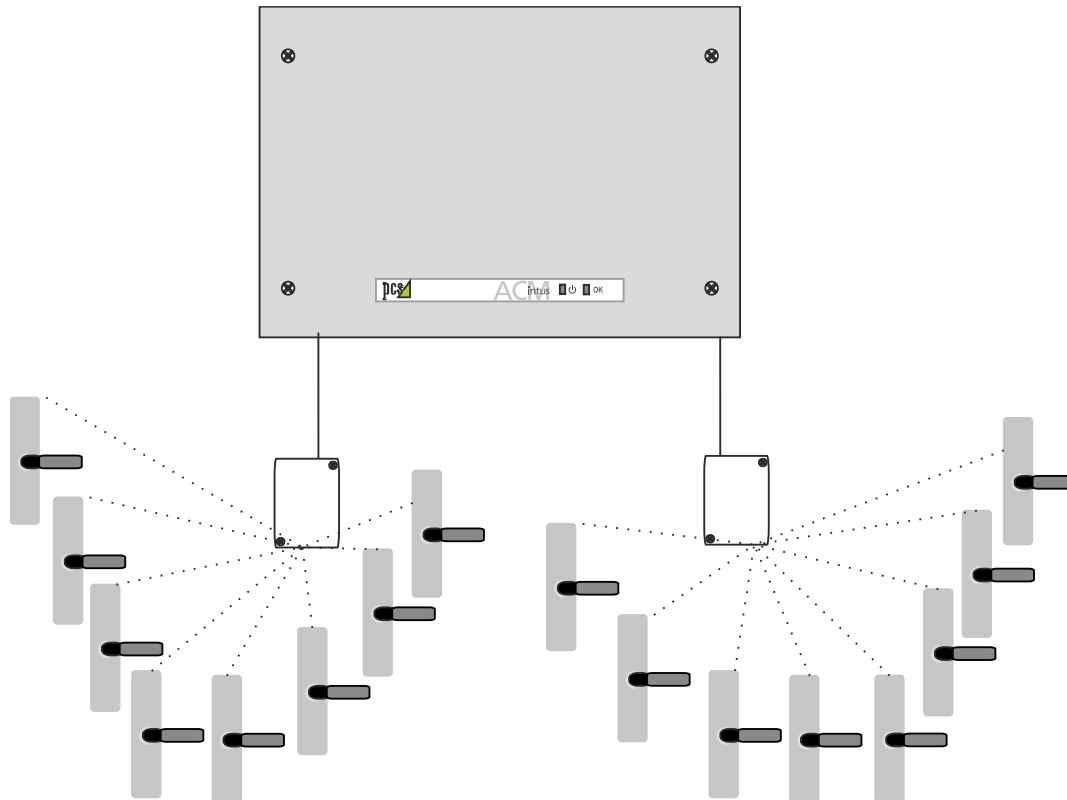


Abbildung 11-7: Beispiel ACM40e mit 16 INTUS Flex Endgeräten

Einstellung Verkabelung MP / MP

Das Bild zeigt die Konfigurationssoftware zur Einstellung der Verkabelung für LBus 1 und LBus 2. Für beide Buses ist die Option 'Multi-Point' ausgewählt.

Verkabelung LBus 1

- ☒ Multi-Point
- ☐ Point-to-Point

Verkabelung LBus 2

- ☒ Multi-Point
- ☐ Point-to-Point

¹ Bei Verwendung der 16Flex-Lizenz generell MP/MP auswählen

Einstellung LBus 1 / OSDP

LBus 1

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Einstellung LBus 2 / OSDP

LBus 2

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

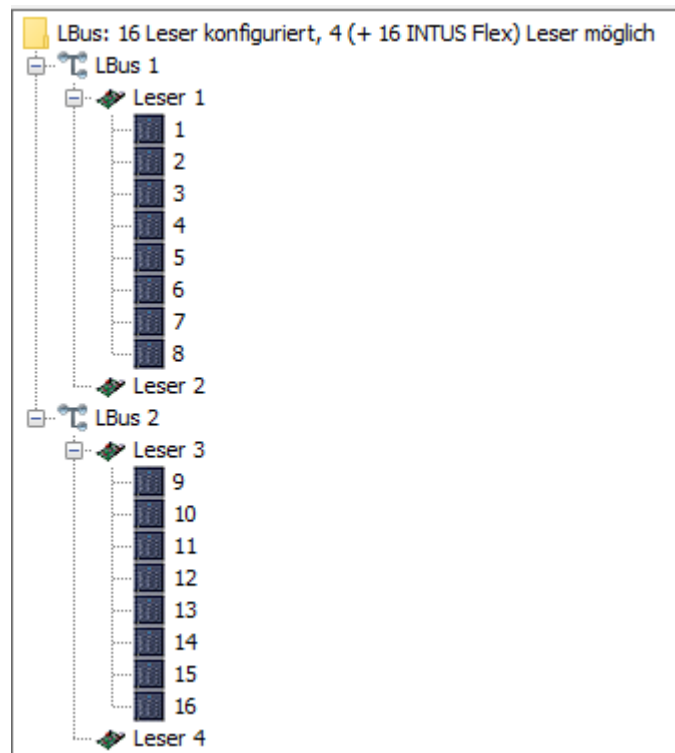
Konfiguration der Leser an "Leser 1"

LBus 1/Leser 1			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
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	☒

Konfiguration der Leser an "Leser 3"

LBus 2/Leser 3			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
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	☒

Resultat in der Baumansicht



11.13 Beispiel: ACM40e mit 16Flex-Lizenz² - Mischbetrieb mit sternförmig angeschlossenen INTUS Lesern

- LBus1: 2 INTUS Leser, sternförmige Verdrahtung. "Leser 1" und "Leser 2".
- LBus2: 2 INTUS Flex Gateways, 8 funkverbundene INTUS Flex Endgeräte. Busverdrahtung.
- Erstes INTUS Flex Gateway an "Leser 3". TCL-Adressen 9, 10, 11 und 12.
- Zweites INTUS Flex Gateway an "Leser 4": TCL-Adressen 13, 14, 15 und 16.



Es muss MP/MP eingestellt werden. Damit ist keine "Einfache Adressierung" an LBus1 möglich (diese ist nur bei PP möglich).

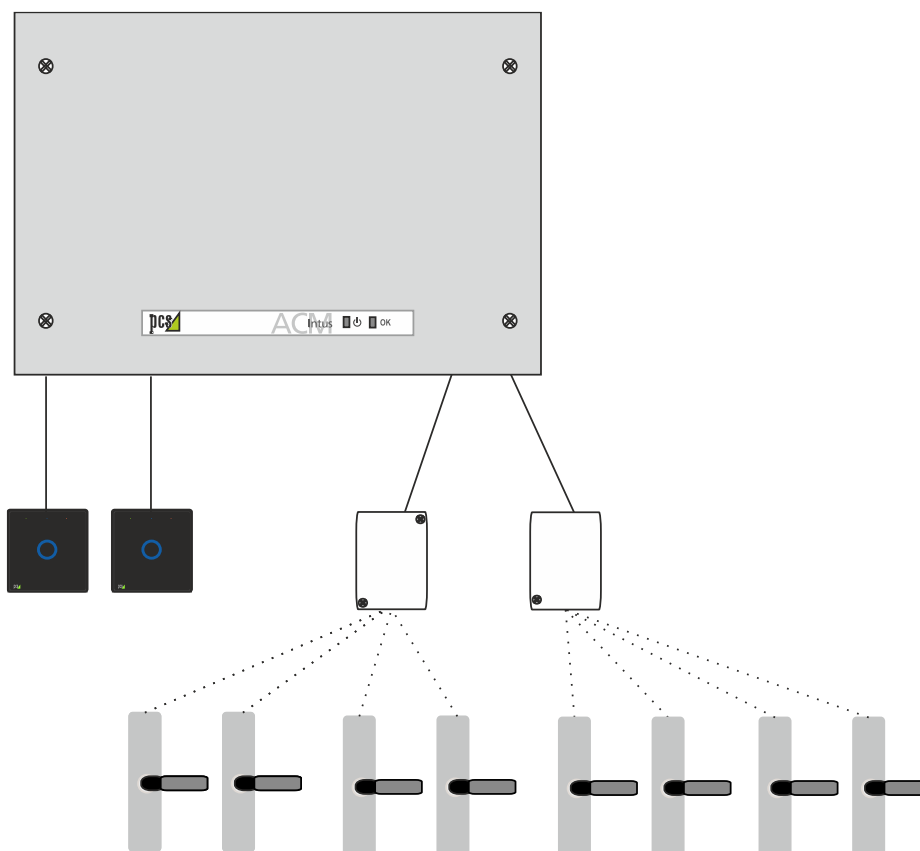


Abbildung 11-8: ACM40e, 2 Leser, 8 INTUS Flex Endgeräte

² Bei Verwendung der 16Flex-Lizenz generell MP/MP auswählen

Einstellung Verkabelung MP / MP

Verkabelung LBus 1

☒ Multi-Point

☐ Point-to-Point

Verkabelung LBus 2

☒ Multi-Point

☐ Point-to-Point

Einstellung LBus 1 / OSDP

LBus 1

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☐ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Einstellung LBus 2 / OSDP

LBus 2

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Konfiguration der Leser an "Leser 1"

LBus 1/Leser 1			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
1	1	Modus B	☒
3	3	nicht konfiguriert	☐
4	4	nicht konfiguriert	☐

Konfiguration der Leser an "Leser 2"

LBus 1/Leser 2			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
2	2	Modus B	☒
3	3	nicht konfiguriert	☐
4	4	nicht konfiguriert	☐

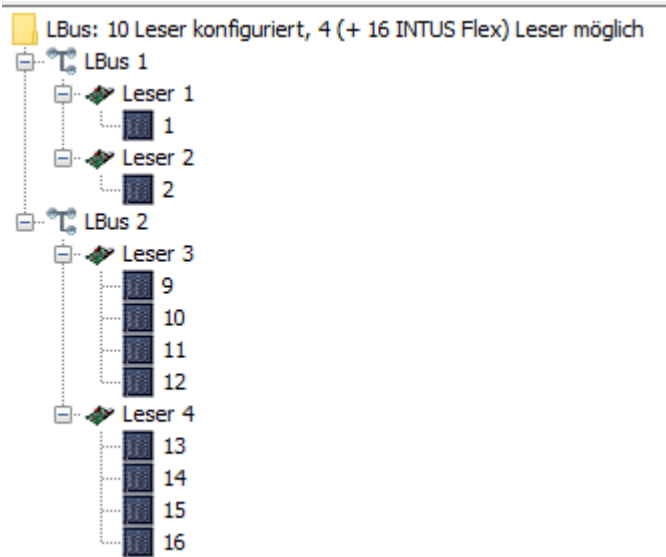
Konfiguration der Leser an "Leser 3"

LBus 2/Leser 3			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	INTUS Flex	☒
10	2	INTUS Flex	☒
11	3	INTUS Flex	☒
12	4	INTUS Flex	☒

Konfiguration der Leser an "Leser 4"

LBus 2/Leser 4			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
13	5	INTUS Flex	☒
14	6	INTUS Flex	☒
15	7	INTUS Flex	☒
16	8	INTUS Flex	☒

Resultat in der Baumansicht



11.14 Beispiel: ACM40e mit 16Flex-Lizenz³ - Mischbetrieb mit busverdrahteten INTUS Lesern

- LBus1: 4 INTUS Leser, alle 4 an "Leser 1". Busverdrahtung.
- LBus2: 2 INTUS Flex Gateways, 8 funkverbundene INTUS Flex Endgeräte. Busverdrahtung.
- Erstes INTUS Flex Gateway an "Leser 3". TCL-Adressen 9 und 10.
- Zweites INTUS Flex Gateway an "Leser 3": TCL-Adressen 11 und 12.
- Drittes INTUS Flex Gateway an "Leser 4": TCL-Adressen 13 und 14.
- Viertes INTUS Flex Gateway an "Leser 4": TCL-Adressen 15 und 16.

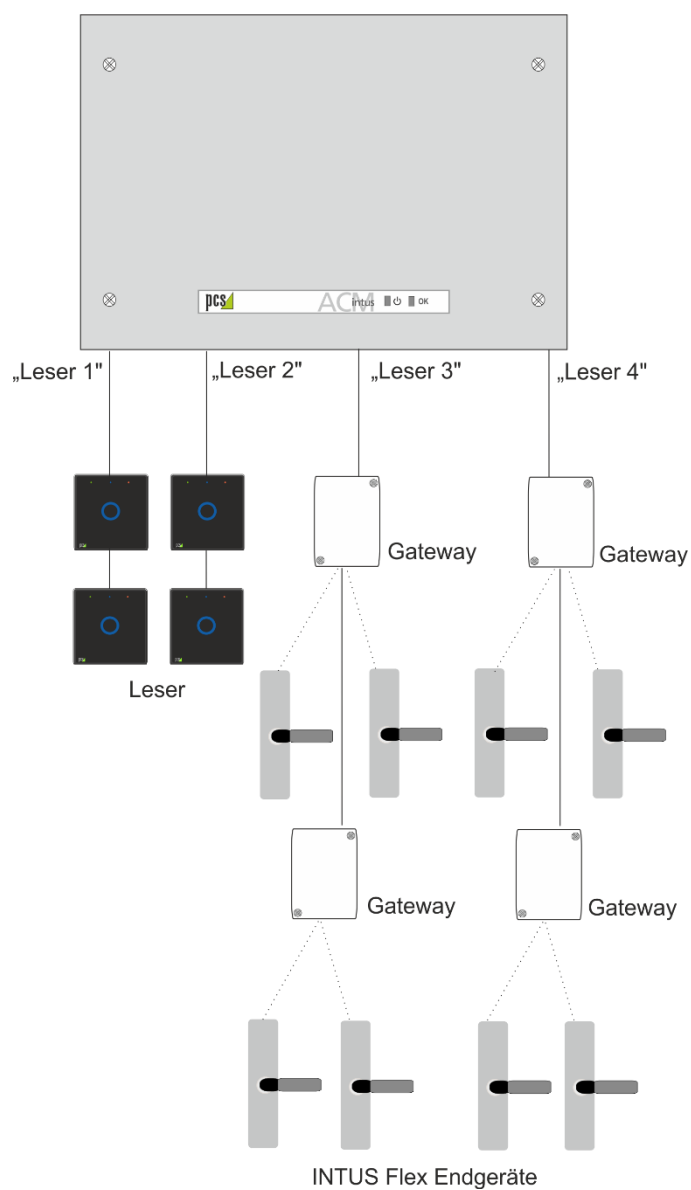


Abbildung 11-9: ACM40e, 4 Leser, 8 INTUS Flex Endgeräte

³ Bei Verwendung der 16Flex-Lizenz generell MP/MP auswählen

Einstellung Verkabelung MP / MP

Verkabelung LBus 1

☒ Multi-Point

☐ Point-to-Point

Verkabelung LBus 2

☒ Multi-Point

☐ Point-to-Point

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

LBus 1

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☐ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Einstellung LBus 2 / OSDP

LBus 2

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Konfiguration der Leser an "Leser 1"

LBus 1/Leser 1			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
1	1	Modus B	☒
2	2	Modus B	☒

Konfiguration der Leser an "Leser 2"

LBus 1/Leser 2			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
3	3	Modus B	☒
4	4	Modus B	☒

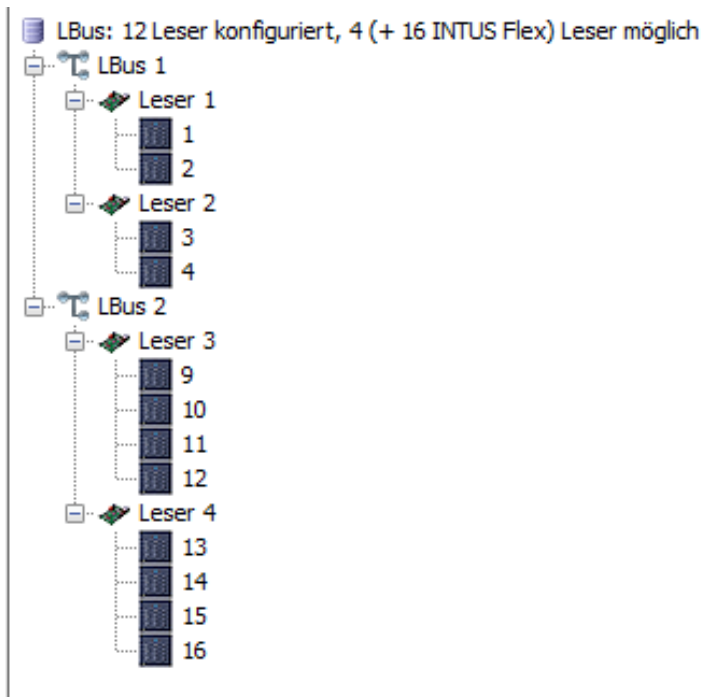
Konfiguration der Leser an "Leser 3"

LBus 2/Leser 3			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	INTUS Flex	☒
10	2	INTUS Flex	☒
11	3	INTUS Flex	☒
12	4	INTUS Flex	☒

Konfiguration der Leser an "Leser 4"

LBus 2/Leser 4			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
13	5	INTUS Flex	☒
14	6	INTUS Flex	☒
15	7	INTUS Flex	☒
16	8	INTUS Flex	☒

Resultat in der Baumansicht



11.15 Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten

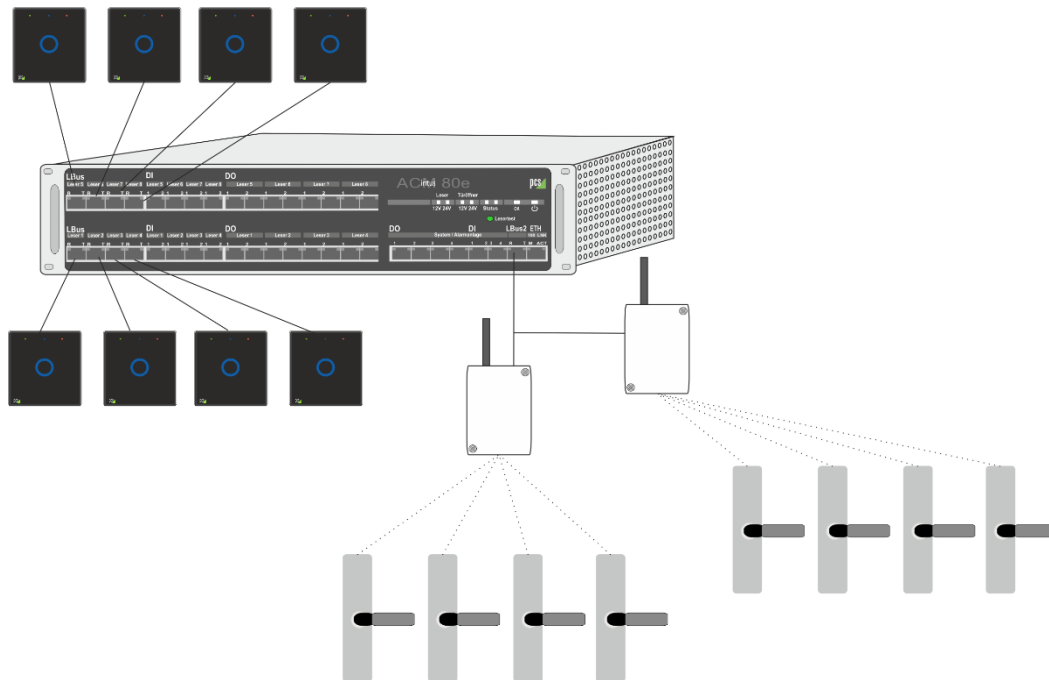


Abbildung 11-10: Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten

Einstellung Verkabelung PP/MP

Verkabelung LBus 1

☐ Multi-Point

☒ Point-to-Point

Verkabelung LBus 2

☒ Multi-Point

☐ Point-to-Point

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

LBus 1

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☐ OSDP

☒ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

Einstellung LBus 2 / OSDP

LBus 2

Lesertyp:

☐ nicht konfiguriert

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

☐ INTUS 300H/340H

☐ INTUS 300L/300M

☐ INTUS 300ro/315ro

☒ OSDP

☐ einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

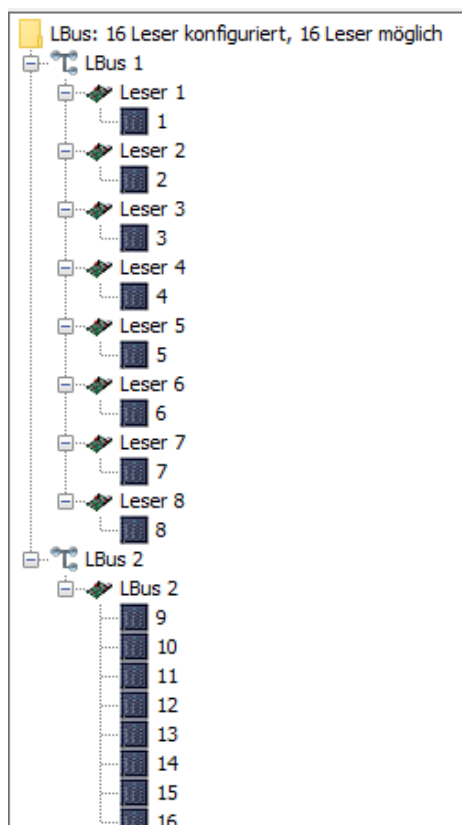
Konfiguration an LBus 1 fehlt

Konfiguration der Leser an "LBus 2"

LBus 2/LBus 2			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	nicht konfiguriert	☐
10	2	nicht konfiguriert	
11	3	INTUS Flex	☒

LBus 2/LBus 2			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
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	☒

Resultat in der Baumansicht



11.16 Beispiel: ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2

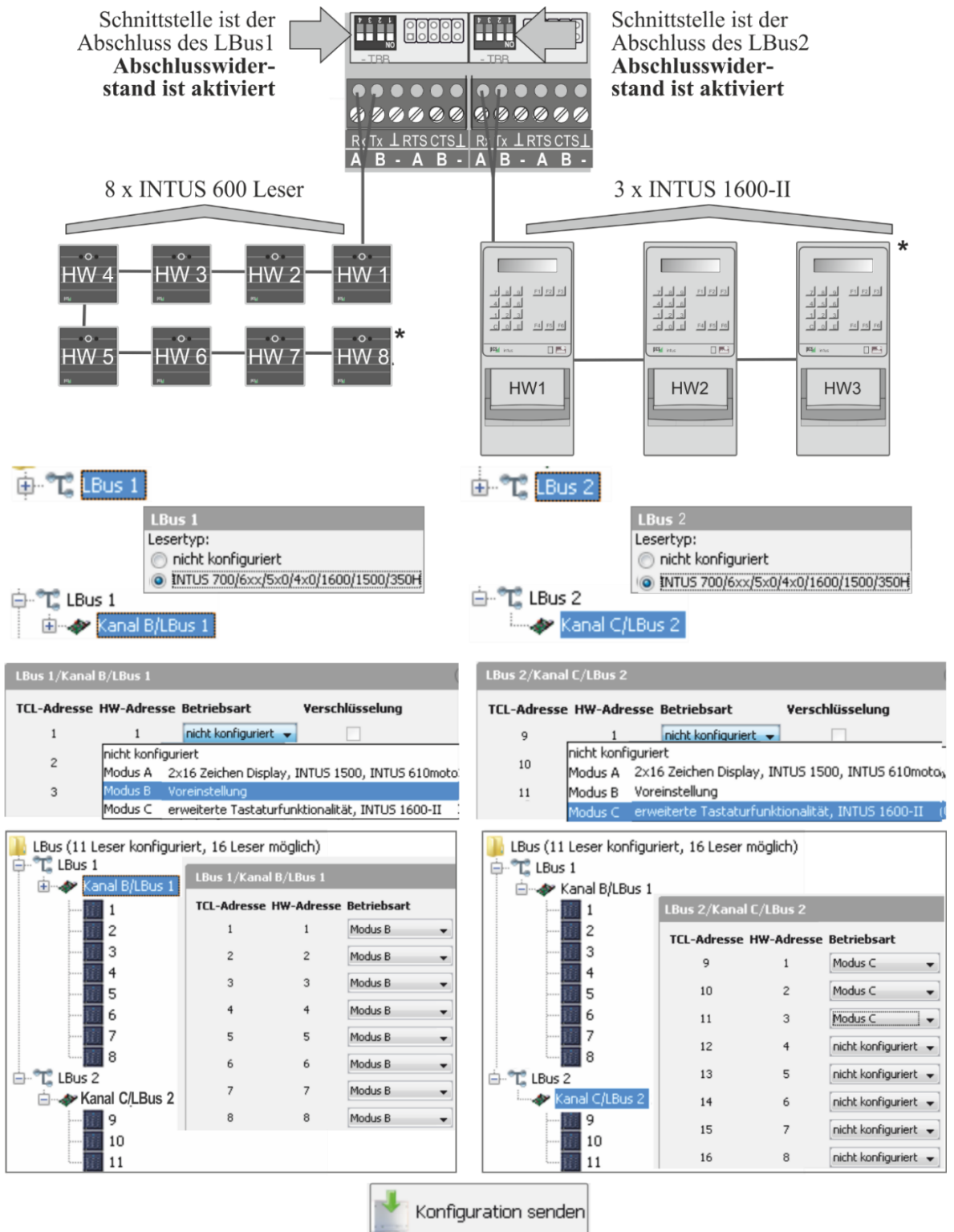


Abbildung 11-11: Beispiel - ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2



Der letzte Leser ist der Abschluss von LBus1 bzw. LBus2:
Abschlusswiderstand aktivieren!

* Die Adresse (HW) muss bei jedem Leser eingestellt werden. Informationen hierzu finden Sie in der Installationsanleitung des Lesers.

11.17 LBus AES-Verschlüsselung

Berechtigungsstufe 3

Es ist möglich, die Kommunikation zwischen einem LBus-Leser und dem Terminal mit AES-Verschlüsselung zu betreiben. Dies gilt nicht für den Leser-Typ Wiegand. Bezüglich OSDP und INTUS Flex beachten Sie die Hinweise in 11.17.8.

11.17.1 Voraussetzungen

- Die AES-Verschlüsselung kann nur verwendet werden, wenn die Geräte-Firmware dies unterstützt.
- Ab Geräte-Firmware 1.07 steht diese Funktion zur Verfügung.
- Außerdem muss die Leser-Firmware die AES-Verschlüsselung unterstützen.

11.17.2 Aktivierung der AES-Verschlüsselung

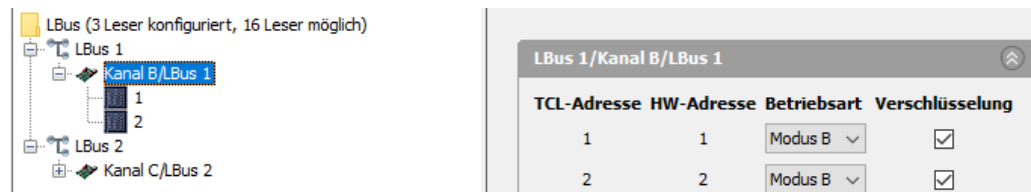


Abbildung 11-12: Aktivierung der AES-Verschlüsselung

- Automatische Aktivierung: Beim Aufbau der Kommunikation fragt das Terminal beim Leser an, ob dieser die AES-Verschlüsselung unterstützt.
- Unterstützt der Leser die AES-Verschlüsselung, wird sie automatisch aktiviert, selbst wenn die Option "Verschlüsselung" bei diesem Leser nicht gesetzt ist
- Durch Setzen der Option "Verschlüsselung" bei einem Leser kann erzwungen werden, dass die Kommunikation verschlüsselt erfolgt (mit AES-Verschlüsselung bzw. PCS-proprietär – siehe Kapitel 11.18).
 - Wenn ein Leser sowohl AES-Verschlüsselung als auch PCS-proprietäre Verschlüsselung unterstützt, wählt das Terminal stets die AES-Verschlüsselung.
- Ist diese Option gesetzt und ein Leser unterstützt keine Verschlüsselung, deaktiviert die Geräte-Firmware die Kommunikation mit dem Leser, d.h. der Leser ist inaktiv ("KO") und kann nicht für Lesungen verwendet werden.



11.17.3 Konfiguration der AES-Schlüssel



Allgemeine LBus Einstellungen

Kundenschlüssel für AES-Verschlüsselung: (nicht konfiguriert)

Noch kein Kundenschlüssel konfiguriert

☐ Schlüssel anzeigen

☒ beibehalten ☐ ändern

☐ AES-Verschlüsselung nur mit Kundenschlüssel

Abbildung 11-13: Konfiguration der AES-Schlüssel

- Standardmäßig verwendet die Geräte-Firmware den sogenannten "Geräteschlüssel" für die AES-Verschlüsselung mit einem Leser.
- Sie können per INTUS RemoteConf auch einen selbst gewählten "Kundenschlüssel" mit INTUS RemoteConf in das Terminal und in die angeschlossenen Leser laden.

11.17.4 Kundenschlüssel konfigurieren



Allgemeine LBus Einstellungen

Kundenschlüssel für AES-Verschlüsselung: ●●●●●●●●●●●●●●●●●●●●

Noch kein Kundenschlüssel konfiguriert

☐ Schlüssel anzeigen

☐ beibehalten ☒ ändern

☐ AES-Verschlüsselung nur mit Kundenschlüssel

Abbildung 11-14: Kundenschlüssel konfigurieren

- Für AES-Verschlüsselung wurde in INTUS RemoteConf V1.05.00 ein neuer Bereich "Allgemeine LBus-Einstellungen" eingeführt.
- Sie können einen eigenen Kundenschlüssel anlegen und per INTUS RemoteConf in das Terminal laden.
- Im Anschluss kann der Kundenschlüssel per LBus-Aktion "LBus-Schlüssel an Leser übertragen" an die angeschlossenen Leser übertragen werden (siehe Kapitel 17).

11.17.5 Option AES-Verschlüsselung nur mit Kundenschlüssel

- Es gibt eine Checkbox für die Option "AES-Verschlüsselung nur mit Kundenschlüssel".
- Wenn diese Checkbox nicht aktiviert ist: Ist in einem Leser der Kundenschlüssel nicht hinterlegt, wird vom Terminal der Geräteschlüssel zur Kommunikation verwendet.
- Ist diese Option aktiviert, deaktiviert die Geräte-Firmware die Kommunikation mit dem Leser, d.h. der Leser ist inaktiv ("KO") und kann nicht für Lesungen verwendet werden. Es ist aber möglich, den Kundenschlüssel per LBus-Aktion "LBus-Schlüssel an Leser übertragen" (siehe Kapitel 17) nachzuladen.

11.17.6 Kundenschlüssel ändern



Allgemeine LBus Einstellungen

Kundenschlüssel für AES-Verschlüsselung:

☐ Schlüssel anzeigen

☐ beibehalten ☒ ändern

☐ AES-Verschlüsselung nur mit Kundenschlüssel

Abbildung 11-15: Kundenschlüssel ändern

- Der Kundenschlüssel kann jederzeit wieder mit INTUS RemoteConf geändert werden.
- Das Terminal merkt sich beim Ändern des Kundenschlüssels den letzten vorherigen Kundenschlüssel (sogenannter "alter Kundenschlüssel").
- Im Anschluss kann der neue Kundenschlüssel per LBus-Aktion "LBus-Schlüssel an Leser übertragen" an die angeschlossenen Leser übertragen werden. (siehe Kapitel 17).
- Der "alte Kundenschlüssel" wird vom Terminal automatisch gelöscht, sobald alle angeschlossenen Leser den neuen Kundenschlüssel verwenden.

11.17.7 Kundenschlüssel entfernen



Abbildung 11-16: Kundenschlüssel entfernen

- Der konfigurierte Kundenschlüssel kann wieder aus dem Terminal/ACM entfernt werden, in dem der leere Schlüssel 00000000000000000000000000000000 (32 Mal 0) per INTUS RemoteConf konfiguriert wird.
- Per LBus-Aktion "LBus-Schlüssel an Leser übertragen" (siehe Kapitel 17) kann dieser leere Kundenschlüssel wieder an die Leser übertragen werden.
- Damit wird der vorhandene Kundenschlüssel auch in den Lesern entfernt.

11.17.8 AES-Verschlüsselung bei OSDP

Die Umsetzung der AES-Verschlüsselung für OSDP-Leser im Terminal unterscheidet sich leicht von der Umsetzung für allgemeine LBus-Leser, die in den vorigen Abschnitten beschrieben wurde:

- Die AES-Verschlüsselung wird vom Terminal nicht automatisch (Kapitel 11.17.2) aktiviert, sondern muss für jeden Leser explizit aktiviert werden.
- Da es bei OSDP keinen separaten "Geräteschlüssel" gibt, wird vom Terminal der Schlüssel verwendet, der als "Kundenschlüssel" in INTUS RemoteConf gesetzt wird.
- Daher hat die Einstellung "AES-Verschlüsselung nur mit Kundenschlüssel" (Kapitel 11.17.5) bei OSDP-Lesern keine Relevanz.
- Je nach Einstellung des OSDP-Lesers kann es sein, dass eine unverschlüsselte Verbindung oder ein Laden des Schlüssels per LBus-Aktion (siehe Kapitel 17) vom Leser nicht akzeptiert wird.

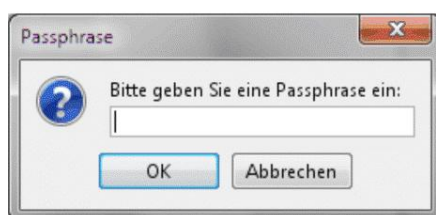
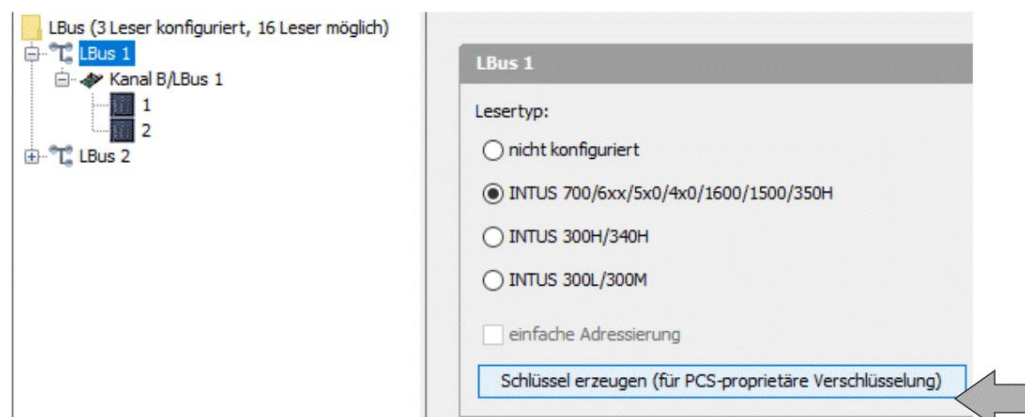
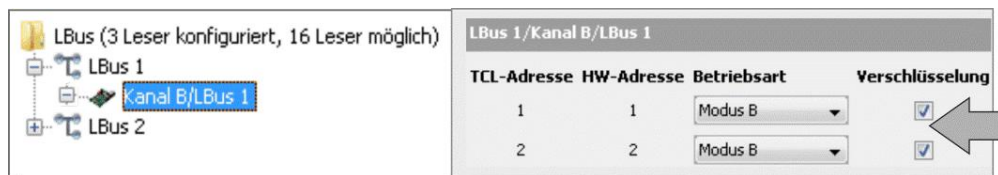
11.18 LBus-Verschlüsselung (PCS-proprietär)

Berechtigungsstufe 3

Es ist möglich, die Kommunikation zwischen einem externen Leser und dem Terminal zu verschlüsseln. Der Schlüssel muss immer eine feste Länge haben. Zur Vereinfachung wird mittels Eingabe einer beliebigen „Passphrase“, die maximal 512 Zeichen haben darf, der Schlüssel vom System automatisch korrekt erzeugt.

Derzeit wird dies unterstützt vom:

- INTUS 700/600/620 und INTUS 640H
- INTUS 400/420, INTUS 500/520 ab Firmware Version 1.08,
- INTUS 350H ab Firmware Version 1.01
- INTUS 1600-II



Eine Verschlüsselung (Passphrase) mit max 512 Zeichen kann eingegeben werden.

Abbildung 11-17: LBus-Verschlüsselung



Nur wenn Terminal und Leser die gleichen Schlüssel haben, ist eine verschlüsselte Kommunikation möglich, daher muss der Schlüssel (Passphrase) in jeden Leser geladen werden.

Sofern es die Firmware des Terminals unterstützt, ist es anschließend möglich, die im Terminal hinterlegten LBus-Schlüssel in die angeschlossenen Leser zu laden. Siehe dazu Kapitel 17.

12 Internen Leser einstellen

Berechtigungsstufe 2 / 3

Gilt nicht für den INTUS ACM



Eine Änderung der Voreinstellung ist in der Regel nur bei Anschluss eines Barcode-Lesers erforderlich.

Ist ein Barcode-Leser angeschlossen, so muss dieser als „zusätzlicher Barcode-Leser“ aktiviert werden.



Abbildung 12-1: Internen Leser einstellen

Lesertyp: Seriell-Standard

Leser-Modus	Erläuterung
Standard	Legic® oder Mifare® oder Hitag® Leser mit serieller Anbindung
DNCIN	freie serielle Leserschnittstelle
Standard + zusätzlicher Barcode-Leser	1x Abstandsleser + 1x Strichcode-Leser

Lesertyp "Takt-Daten" (INTUS 5320)

Leser-Modus	Erläuterung
Omron - Codekennung X	Leser mit Omron Emulation; TCL Codekennung „X“
Omron - Codekennung Y	Leser mit Omron Emulation; TCL Codekennung „Y“
Omron - Codekennung Z	Leser mit Omron Emulation; TCL Codekennung „Z“
Barcode (Wand Emulation)	Strichcode Leser

13 TCL Parameter einstellen

Berechtigungsstufe 2 / 3



Abbildung 13-1: TCL Parameter einstellen

13.1 Einstellungen



Tabellenfeld

Die Voreinstellung der Größe des Tabellenfeldes (TF-Feld) beträgt 49152 Byte (48 kByte).

Notpuffer

Die Voreinstellung ist eine Notpuffergröße (\$4 Ringpuffer) von 49152 Byte (48 kByte).



Tabellenfeld und Notpuffer müssen zusammen in den vorhandenen SRAM Ausbau passen. Wenn die Summe der Werte zu groß gewählt wird, werden beide Betriebsparameter auf die Voreinstellungen von 49152 Byte reduziert. Überprüfen Sie deshalb nach einem Reset, ob die Änderungen akzeptiert wurden.

Quittungszeit

Die logische Quittungszeit legt die Zeit fest, innerhalb der ein Datensatz aus dem Notpuffer vom Rechner quittiert werden muss, und kann zwischen 2 und 230 Sekunden eingestellt werden. Der voreingestellte Wert ist eine Quittungszeit von 26 Sekunden. Die Quittungszeit wird im TCL System zur Steuerung des MONOUT-Prozesses über das P3-Feld benutzt.

Notpuffersätze mit Satznummer

Mit dem Häkchen im Auswahlkasten wird festgelegt, dass den Datensätzen aus dem Notpuffer eine Satznummer automatisch hinzugefügt wird, mit Satznummer: "nein" wird keine Satznummer vorangestellt.

Weitere Angaben zum Aufbau der Datensätze aus dem Notpuffer sind in P20+22,1 und im P10-Feld abgelegt (siehe TCL Programmierhandbuch).

Default TCL-Programm bei Kaltstart laden

Wenn das Häkchen im Auswahlkasten (Voreinstellung) gelöscht wird, kann verhindert werden, dass das Default-Programm bei einem Kaltstart bzw. Eiskaltstart ausgeführt wird.

Damit wird dann auch die Ladeanforderung '77' nicht an den Leitrechner geschickt. Die Voreinstellung sollte normalerweise nicht verändert werden.

Größe BMI-Feld (Byte)

Die Größe der B-, M- und I-Felder kann von 88 Byte (Voreinstellung) auf 115 Byte verändert werden, wenn die Leser Datensätze von mehr als 80 Byte zurückliefern. Die Voreinstellung sollte normalerweise nicht verändert werden.

Label-Anzahl

Die Anzahl der möglichen Sprungziele in einem TCL Programm kann zwischen 512 und 4352 eingestellt werden. Voreinstellung: 1024.

Jedes Sprungziel belegt 4 Bytes SRAM Speicher. Wenn nicht so viele Sprungziele benötigt werden, sollte der Wert nicht zu groß eingestellt werden, da der Speicher für TF-Feld, Notpuffer und TCL Programmspeicher (DL) nicht genutzt werden kann.

Zeichensatz

Der voreingestellte Zeichensatz ISO 646 – Deutschland kann geändert werden.

13.2 Erweiterte Benutzerschnittstelle

Es kann ein Bereich definiert werden, der Zusatzinformationen für INTUS Graph enthalten kann. Dieser Bereich wird INTUS Graph von TCL zur Verfügung gestellt.

In der Regel wird diese Einstellung bereits über das TCL Programm vorgenommen.

13.3 INTUS Sound

Berechtigungsstufe 1 / 2 / 3

Es ist möglich, die Lautstärke für das Soundmodul (Option) einzustellen.

14 Hardware



Kanal A	Kanal B	Kanal C	IP-Konfiguration	Firewall	Interner Leser	LBus	TCL-Parameter	Hardware
Display								
Display-Kontrast:		21						
2x40 Zeichen Display-Emulation:		Nicht verfügbar						
Backlight-Saver		aktiviert						
Magic-Eye								
Helligkeit blau:		9						
Hupe								
Standard-Frequenz [Hz]:		2300						
☐ Akustische Rückmeldung bei Funktionstastendruck ☐ Akustische Rückmeldung bei Tastendruck (außer Funktionstasten) ☒ Hupensteuerung aus dem TCL-Programm								

Abbildung 14-1: Hardware-Einstellungen

14.1 Display

Display-Kontrast

Der Kontrast des Displays des INTUS 3150, 3155ro, 5500 und 5320 wird bei PCS optimal eingestellt. Durch ungünstige äußere Einflüsse kann eine Nachregulierung notwendig werden.



Die Voreinstellung ist in der Regel 21, die maximale Kontraststärke beträgt 64.

Backlight-Saver

Ist die Backlight-Saver Funktion aktiviert, wird das Backlight nach 1 Stunde Inaktivität dunkler geschaltet (INTUS 5320).

14.2 Magic-Eye (nur INTUS 5320)



Helligkeit blau: Hier können Sie die Helligkeit der blauen Magic-Eye-LED regeln. Wertebereich 0-15, Default 9.

Beim INTUS 5320 ist die Helligkeit in 3 Stufen regelbar: Aus (Wert 0), normal (Werte 1 bis 9) und hoch (Werte 10 bis 15).

14.3 Hupe



Die Hupen Frequenz kann im Bereich von 300 bis 6000Hz eingestellt werden.

15 Login – Wartungsgruppe und Passwörter ändern



Abbildung 15-1: Login – Wartungsgruppe und Passwörter ändern



Sobald die Wartungsgruppe oder das Passwort geändert und gesendet wurden, ist die Anzeige "⚠️ Sicherheitseinstellung befindet sich auf dokumentiertem Standardwert" ausgeblendet. Diese Warnung ist ein Hinweis, dass durch geänderte Passwörter und Wartungsgruppen das Terminal vor unerlaubten Zugriffen besser abgesichert ist.

15.1 Wartungsgruppe

Berechtigungsstufe 3

Es ist möglich, eine Wartungsgruppe festzulegen, um das Terminal nur einer begrenzten Netzteilnehmergruppe zugänglich zu machen.



Der Wertebereich ist 0 – 65535.

Voreinstellung: Das Terminal gehört zur Wartungsgruppe 0.



Notieren Sie auf jeden Fall die Wartungsgruppe.

15.2 Passwort der Berechtigungsstufe ändern

Die Änderung eines Passworts ist abhängig von der Berechtigungsstufe.

In Berechtigungsstufe 3 kann das Passwort für jede Berechtigungsstufe geändert werden.



Notieren Sie auf jeden Fall eine Änderung des Passwortes.

16 Zeit

Berechtigungsstufe 2 / 3



Kanal A	Kanal B	Kanal C	IP-Konfiguration	Firewall	Interner Leser	LBus	TCL-Parameter	Hardware	Login	Zeit
---------	---------	---------	------------------	----------	----------------	------	---------------	----------	-------	-------------

NTP-Client

☐ NTP-Server aus DHCP-Antwort verwenden

NTP-Server 1:

NTP-Server 2:

Abweichung zur UTC-Zeit am Standort

☒ Manuelle Einstellung

Offset [Minuten]:

Zeitumstellung

☐ automatisch

☐ immer Sommerzeit

☒ immer Normalzeit

☐ TZ-Daten aus DHCP-Antwort verwenden

POSIX TZ-String:

Abbildung 16-1: Zeiteinstellungen

16.1 NTP Client

Das Terminal unterstützt nun optional die Synchronisation von Datum/Uhrzeit über NTP (Network Time Protocol). Standardmäßig ist die NTP-Zeitsynchronisation aus.



NTP-Server 1 bzw. NTP-Sever 2: Es können eine IP-Adresse oder ein Hostname angegeben werden. NTP-Zeitsynchronisation ist aktiviert, wenn die Option "aus DHCP" aktiviert ist und/oder bei NTP-Server 1 bzw. NTP-Server 2 ein Wert gesetzt ist.

Aus allen konfigurierten Zeitservern (über DHCP oder INTUS RemoteConf) wird automatisch der am besten geeignete Server für die Synchronisation ausgewählt.



NTP verwendet immer UTC-Zeit. Es wird deshalb empfohlen, die Abweichung zur UTC-Zeit und die Zeitumstellung passend zu konfigurieren.

16.2 UTC offset - Abweichung zur UTC Zeit

UTC (UTC – Weltzeit) wird als Basis verwendet.



Für die Abweichung zwischen Ortszeit und UTC werden Richtung (östlich bzw. westlich) und Minuten eingegeben.

Diese Angabe bezieht sich auf die Winterzeit. Ein positiver Wert bedeutet dabei westlich von UTC, ein negativer Wert (Vorzeichen '-') östlich von UTC.

Beispiel:

Ortszeit Deutschland: derzeit eine 1 Stunde östlich von UTC. Es muss der Wert "-60" als Abweichung eingetragen werden.

16.3 Sommer/Winterzeitumschaltung



Soll die Sommer/Winterzeitumschaltung automatisch durch das Terminal erfolgen, so müssen Sommerzeitanfang und -ende im POSIX TZ Format angegeben werden.

Das POSIX TZ-Format Mm.w.d/h spezifiziert den Umschaltzeitpunkt als Tag d der Woche w im Monat m zur Stunde h. Der Tag d muss zwischen 0 (Sonntag) und 6 (Samstag) liegen.

Die Woche w muss zwischen 1 und 5 liegen; Woche 1 ist die erste Woche, in der der Wochentag d auftaucht und Woche 5 wählt die letzte Woche, in der der Wochentag d vorkommt. Der Monat m darf Werte zwischen 1 und 12 annehmen, die Stunde h Werte zwischen 0 und 23.

Derzeit gilt für Zentraleuropa:

Sommerzeitanfang: **M3.5.0/02** (letzter Sonntag im März um 2 Uhr)

Winterzeitanfang: **M10.5.0/03** (letzter Sonntag im Oktober um 3 Uhr)

Der komplette POSIX TZ-String für Zentraleuropa lautet somit:

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

17 LBus-Aktionen

Berechtigungsstufe 2 / 3

17.1 Überblick

Mit dieser Funktion ist es möglich, das Terminal bzw. den ACM bestimmte Aktionen für den internen Leser bzw. für die an den LBus angeschlossenen Leser durchführen zu lassen. Es können auch mehrere Terminals ausgewählt werden, bevor die Schaltfläche "LBus Aktionen" gedrückt wird. In diesem Fall wird die LBus-Aktion parallel an alle ausgewählten Terminals gesendet und die Aktion ausgeführt.



Wird eine LBus-Aktion an mehreren Terminals ausgeführt, werden Leser, die nicht an einem Terminal konfiguriert sind, ausgelassen und nicht als Fehler angezeigt.

Ist die Schaltfläche "LBus-Aktionen" inaktiv, so unterstützt die Geräte-Firmware die Ausführung von LBus-Aktionen nicht.



Ablauf:

- 1 Klicken Sie auf die Schaltfläche "LBus-Aktionen", um zu beginnen.
- 2 Wählen Sie eine der 4 Aktionen oder eine Aktionsfolge aus mehreren Aktionen aus, die dann nacheinander auf ausgewählten Terminals ausgeführt werden.

Die Aktion "Leserspezifische Einstellungen konfigurieren" kann nicht in eine Aktionsfolge aufgenommen werden.



"Leserspezifische Einstellungen konfigurieren" kann nicht selektiert werden, wenn mehr als ein Terminal ausgewählt ist.

- 3 Klicken Sie auf „Weiter“:

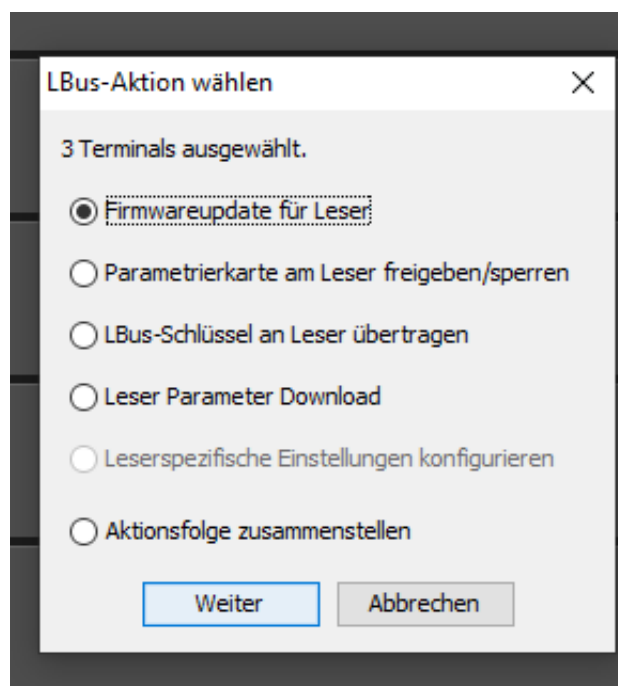


Abbildung 17-1: LBus-Aktionen wählen

- 4 Im darauffolgenden Schritt wählen Sie die Leser aus, für die die Aktion(en) ausgeführt wird/werden. Je nach Aktion müssen noch weitere Einstellungen vorgenommen werden. Siehe Folgekapitel.
- 5 Nach Drücken auf "Start" wird die Aktion für jeden ausgewählten Leser durchgeführt. Während das Terminal die LBus-Aktion ausführt, wird in INTUS RemoteConf eine Statusübersicht angezeigt.
- 6 Ist die Aktion abgeschlossen, wird nochmals eine Gesamtübersicht angezeigt.

17.2 Aktion "Firmwareupdate für Leser"

Unter Umständen kann es notwendig sein, ein Update der Firmware der am Terminal angeschlossenen Leser durchzuführen.

Eine Datei mit der Leserfirmware wird Ihnen vom PCS Support individuell zur Verfügung gestellt.



- 1 Wählen Sie über "IRFW-Datei auswählen..." eine IRFW-Datei aus.
- 2 Wählen Sie die Leser aus, für die das Firmwareupdate ausgeführt werden soll.



Nach einem Update der Leserfirmware von Version 4.x bzw. 5.x auf Version 6.x ist anschließend der Leser immer neu zu parametrieren. Dies erfolgt durch eine VX-Leserparametrierkarte, oder es kann das Laden über INTUS RemoteConf mit Hilfe einer IRPA-Datei erfolgen. Siehe Kapitel 17.5 und 17.7.

17.3 Aktion "Parametrierkarte am Leser freigeben/sperrern"

Hiermit ist es möglich, an einem Leser die Funktion „Parametrierkarte freigeben oder sperren“ einzurichten (Details hierzu im Handbuch „Leserparametrierung mit der Parametrierkarte“, Bestellnummer D3000-21). Damit ist eine nachträgliche Erweiterung oder Änderung der Leserparametrierung vor Ort möglich. Die Parametrierkarte erhalten Sie von der PCS.



- 1 Wählen Sie, ob freigegeben oder gesperrt werden soll.
- 2 Wählen Sie die Leser aus, für die das Freigeben bzw. Sperren der Parametrierkarte ausgeführt werden soll.

17.4 Aktion "LBus-Schlüssel an Leser übertragen"

Mit Hilfe dieser Aktion ist es möglich, die im Terminal hinterlegten Schlüssel für die LBus-Verschlüsselung an die Leser zu übertragen. Siehe auch Kapitel 11.17 und 11.18.



Wählen Sie die angeschlossenen Leser aus, für die der Schlüsseltransfer durchgeführt werden soll.



Die Übertragung des Schlüssels ist nur bei der Inbetriebnahme oder nach Änderung des Schlüssels erforderlich.

17.5 Aktion "Leser Parameter Download"

Unter Umständen kann es notwendig sein, die an ein Terminal angeschlossenen Leser mit INTUS RemoteConf zu parametrieren.

Statt der Parametrierung mit Parametrierkarte kann auch ein Leser Parameter Download verwendet werden. Für diese Aktion ist die Geräte-Firmware Version 1.10.00 oder höher notwendig.

Der PCS Support stellt Ihnen eine IRPA-Datei für den Leser Parameter Download zur Verfügung. Diese Datei enthält die Parameter (z. B. VXD) für die INTUS Leser.

Weiterhin erhalten Sie vom PCS Support das individuelle IRPA-Datei-Passwort für diese Datei.



- 1 Wählen Sie diese Datei über "IRPA-Datei auswählen" in INTUS RemoteConf aus und geben Sie das dazugehörige IRPA-Datei-Passwort in das Feld "IRPA-Passwort für Datei" ein.

VXD00-001.02.irpa IRPA-Datei auswählen...

IRPA-Datei-Passwort: ●●●●●●●●●●●●●●

☐ Passwort anzeigen

Start Abbrechen

- 2 Wählen Sie die zu parametrierenden Leser aus.

Das Terminal entschlüsselt die Daten in der IRPA-Datei mit Hilfe des eingegebenen IRPA-Datei-Passwortes und lädt daraufhin die entschlüsselten Parameter-Daten in die ausgewählten Leser.



Nach erfolgreichem Download der Parameter ist die Funktion der Parametrierkarte in diesen Lesern automatisch gesperrt. Sie kann jederzeit bei Bedarf über die LBus Aktion "Parametrierkarte" (Kapitel 17.3) wieder freigeschaltet werden.

17.6 Aktion "Leserspezifische Einstellungen konfigurieren"

Über diesen Dialog können Sie weitere Einstellungen für die angeschlossenen Leser vornehmen.

Für jeden angeschlossenen Leser gibt es einen Tab. Die Einstellungen können pro Leser separat eingegeben werden. Über die Schaltfläche "Konfiguration senden" werden die Einstellungen an das Terminal/den ACM geschickt.

The screenshot shows a configuration window for 'Leser 1' (Reader 1). The window has a tabbed interface with 'Leser 1' selected. The settings are organized into several sections, each with a title bar and an expand/collapse arrow:

- Allgemeine Aktionen** (General Actions):
 - ☐ Verwaltung leaserspezifischer Einstellungen deaktivieren
 - ☐ Leserspezifische Einstellungen auf Werkseinstellungen zurücksetzen
- Leserkennzeichnung** (Reader Identification):
 - Anzeigename: ?
 - Verwendung: ?
- Mobile Access**:
 - Betriebsmodus: ?
 - Wake-Up Empfindlichkeit: ?
 - BLE Reichweite [Min. RSSI, dBm]: ?
 - Rückmeldung: ?
- Apple Wallet**:
 - Authentifizierungsmodus: ?
- Sabotagekontakt**:
 - Empfindlichkeit:
- Frequenz**:
 - Frequenz Hupe:
 - Frequenz Tastenton:
- Helligkeit**:
 - Helligkeit Tastaturbeleuchtung:

Abbildung 17-2: Leserspezifische Einstellungen konfigurieren

17.6.1 Allgemeine Aktionen

Lesereinstellungen, die in RemoteConf vorgenommen werden, werden auf ACMs und Terminals gespeichert. Wird ein angeschlossener Leser getauscht, werden die gespeicherten Werte vom ACM/Terminal in den neuen Leser geladen. Ist dies nicht gewünscht, können Sie über das Kontrollkästchen **"Verwaltung leserspezifischer Einstellungen deaktivieren"** das Laden von Einstellungen auf den neuen Leser unterbinden.



- 1 Markieren Sie hierzu das Kontrollkästchen "Verwaltung leserspezifischer Einstellungen deaktivieren" und klicken Sie auf "Konfiguration senden". Die Einstellungen im ACM/Terminal werden gelöscht.
- 2 Stecken Sie den auszutauschenden Leser ab und den neuen an.
- 3 Nehmen Sie die Markierung des Kontrollkästchens wieder heraus, so dass der ACM die Einstellungen des neuen Lesers laden und speichern kann.



Wenn ein Leser getauscht werden soll, die Einstellungen aber beibehalten werden sollen, darf dieses Kontrollkästchen nicht markiert werden.

Über das Kontrollkästchen **"Leserspezifische Einstellungen auf Werkseinstellungen zurücksetzen"** können Sie alle über diesen Dialog vorgenommenen Einstellungen rückgängig machen.

17.6.2 Einstellungen von montageortspezifischen Parametern

Über die Bereiche **"Leser, Mobile Access, Apple Wallet, Sabotagekontakt, Frequenz, Helligkeit"** können montageortspezifischen Parameter für den jeweiligen Leser vorgenommen werden. Bewegen Sie die Maus über eines der Info-Symbole, um Informationen zur jeweiligen Einstellung zu erhalten.

17.7 Aktionsfolge zusammenstellen

Zur Arbeitserleichterung können Sie mehrere Aktionen zusammenstellen. So müssen Sie nicht am Rechner warten und aufpassen, bis z. B. ein Firmware Update abgeschlossen ist, um dann nochmals den Parameter Download als Aktion zu starten. Die angelegten Aktionen werden von allen Terminals nacheinander ausgeführt.

Zunächst ist die Liste der Aktionen leer. Sie kann über die Schaltfläche "Aktion hinzufügen" Schritt für Schritt erweitert werden.

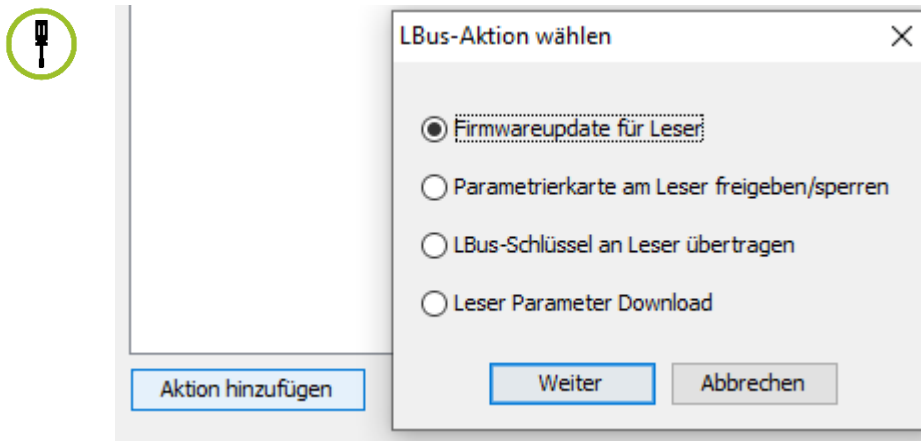


Abbildung 17-3: LBus-Aktionsfolge zusammenstellen

Jede Aktion wird von jedem Terminal nacheinander ausgeführt. Ist eine Aktion für alle beteiligten Leser beendet, wird vom Terminal die nächste Aktion gestartet.

Die Liste der Aktionen kann bis zu 99 Aktionen enthalten. Für jede Aktion können die beteiligten Leser individuell ausgewählt werden.

Tritt an einem Leser während einer Aktion ein Fehler auf, werden die darauffolgenden Aktionen für diesen Leser nicht mehr ausgeführt

Beispiel 1:

Es wird für Leser 1-8 zuerst ein Firmware-Update durchgeführt, dann werden die Parameter geladen:

Aktionsfolge zusammenstellen

Aktion	Detail	Leser
1 - Firmwareupdate	INTUS_Leser_Firmware_V6.12.irfw	1-8
2 - Parameter Download	VXD00-999.00.irpa	1-8

Beispiel 2:

Die Folge wurde im Vergleich zu Beispiel 1 so abgeändert, dass zuerst Leser 1-4 und danach erst Leser 5-8 behandelt werden:

Aktionsfolge zusammenstellen

Aktion	Detail	Leser
1 - Firmwareupdate	INTUS_Leser_Firmware_V6.12.irfw	1-4
2 - Parameter Download	VXD00-999.00.irpa	1-4
3 - Firmwareupdate	INTUS_Leser_Firmware_V6.12.irfw	5-8
4 - Parameter Download	VXD00-999.00.irpa	5-8

18 Serviceaktionen für INTUS Flex Air

Berechtigungsstufen 2 / 3



Nachfolgend werden folgende Serviceaktionen für INTUS Flex Air beschrieben:

- Das Ändern der Basisadresse des INTUS Flex Gateways
- Das Koppeln von INTUS Flex Geräten an einen INTUS Flex Gateway
- Das Entfernen von INTUS Flex Geräten an einem INTUS Flex Gateway
- Das Aktivieren des Servicemodus eines INTUS Flex Gateways

Ansicht der aktuellen Flex Konfiguration

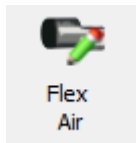


Abbildung 18-1: Flex Air

Über die Schaltfläche "Flex Air" gelangen Sie auf die vollständige Ansicht für die Flex Konfiguration. In dieser Ansicht wird die LBus Konfiguration des ACMs angezeigt, ergänzt um die aktuell angeschlossenen Gateways und um die an den Gateways gekoppelten Flex Geräten.

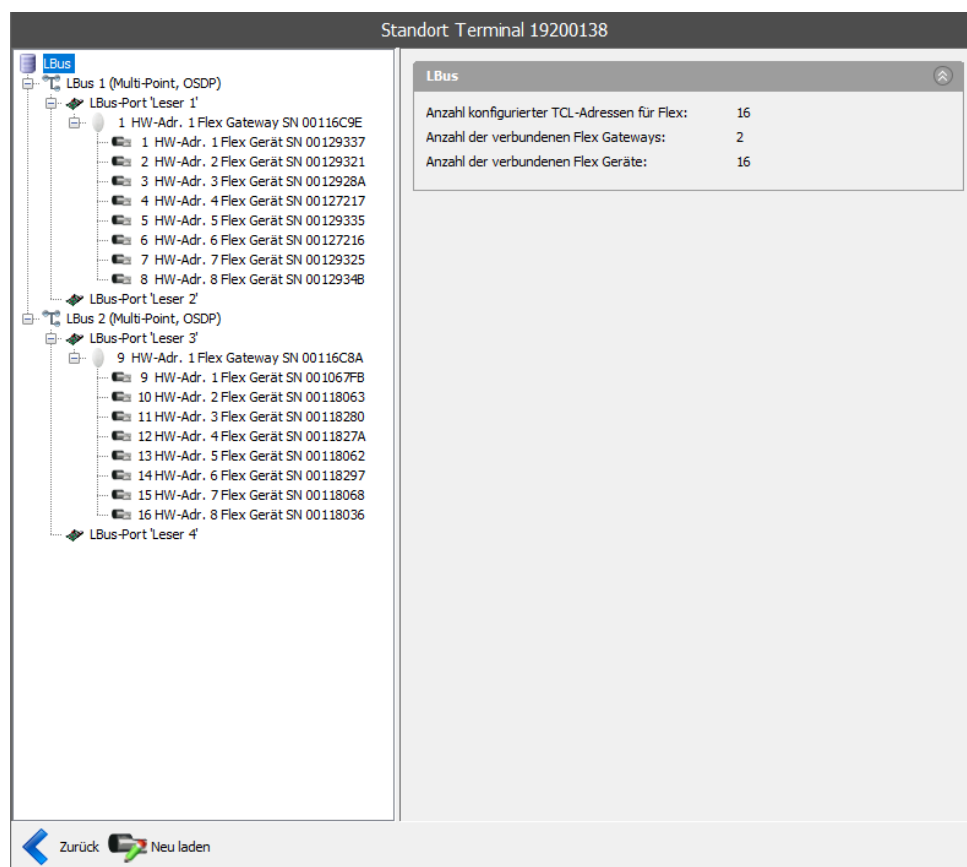


Abbildung 18-2: Ansicht für Flex Konfiguration

In diesem Beispiel wird ein ACM40e mit 16 Flex Lesern an zwei Gateways konfiguriert. Hier sind die zwei Gateways am ACM angeschlossen und werden damit angezeigt. Mit RemoteConf wurden bereits 16 Geräte an die Gateways gekoppelt.

Ändern der Basisadresse

Um die Basisadresse zu ändern, müssen alle Flex-Geräte entkoppelt sein. Die Änderung der Basisadresse ist normalerweise nur erforderlich, wenn Sie das Gateway zum ersten Mal konfigurieren.

Um den Vorgang zu starten, wählen Sie ein Gateway aus und wählen Sie dann die Option "Basisadresse ändern".

Stellen Sie sicher, dass keine Geräte mit einem Gateway verbunden sind, da der Vorgang sonst nicht fortgesetzt werden kann und eine Fehlermeldung angezeigt wird.

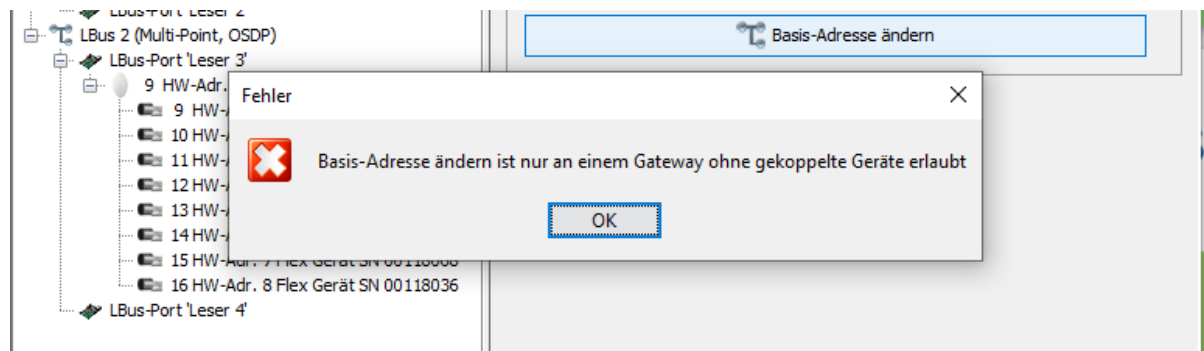


Abbildung 18-3: Fehlermeldung - Ändern der Basisadresse

Stellen Sie bei einem Betrieb mehrerer Gateways an einem LBus-Port sicher, dass diese auf unterschiedliche Basisadressen konfiguriert sind, da sonst nicht alle Gateways adressierbar sind und somit nicht angezeigt werden können.

Entfernen von INTUS Flex Geräten von einem INTUS Flex Gateway

Um Flex-Geräte von einem Gateway zu entfernen, wählen Sie ein Flex-Gerät aus und wählen Sie die Option "Flex Gerät von Gateway entfernen".

Für alle Flex-Geräte wird in der Gesamtansicht ein Zylinder-Symbol verwendet.

In Abbildung 18-4: Gerät von Gateway entfernen wurde das dritte Flex-Gerät (Adresse 11) ausgewählt und nach Bestätigen der Flex Aktion kann der Vorgang zum Entfernen des Gerätes abgeschlossen werden.

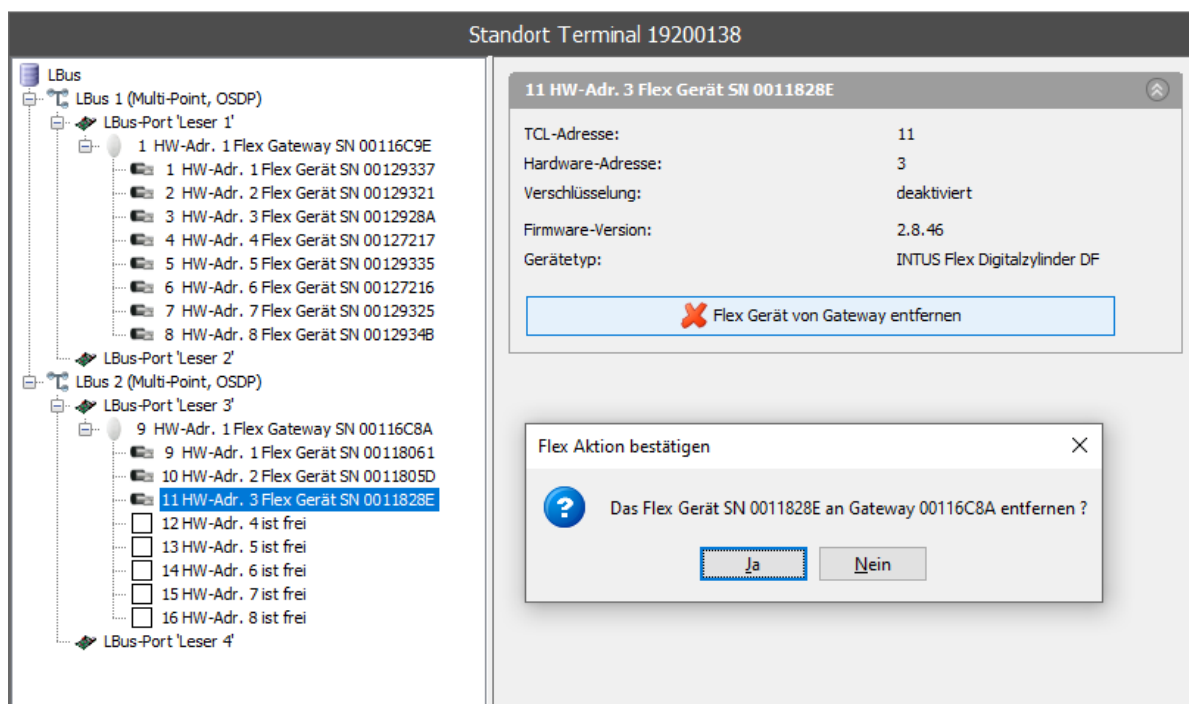


Abbildung 18-4: Gerät von Gateway entfernen

Hinzufügen von INTUS Flex Geräten an einem INTUS Flex Gateway

Um Flex-Geräte an einem Gateway zu koppeln, wählen Sie eine freie Adresse aus (weißes Rechteck) und wählen Sie die Option "Flex Gerät koppeln".

Bevor Sie die Flex Aktion bestätigen, um den Vorgang abzuschließen, halten Sie zuvor die Service-Karte an das Flex-Gerät.

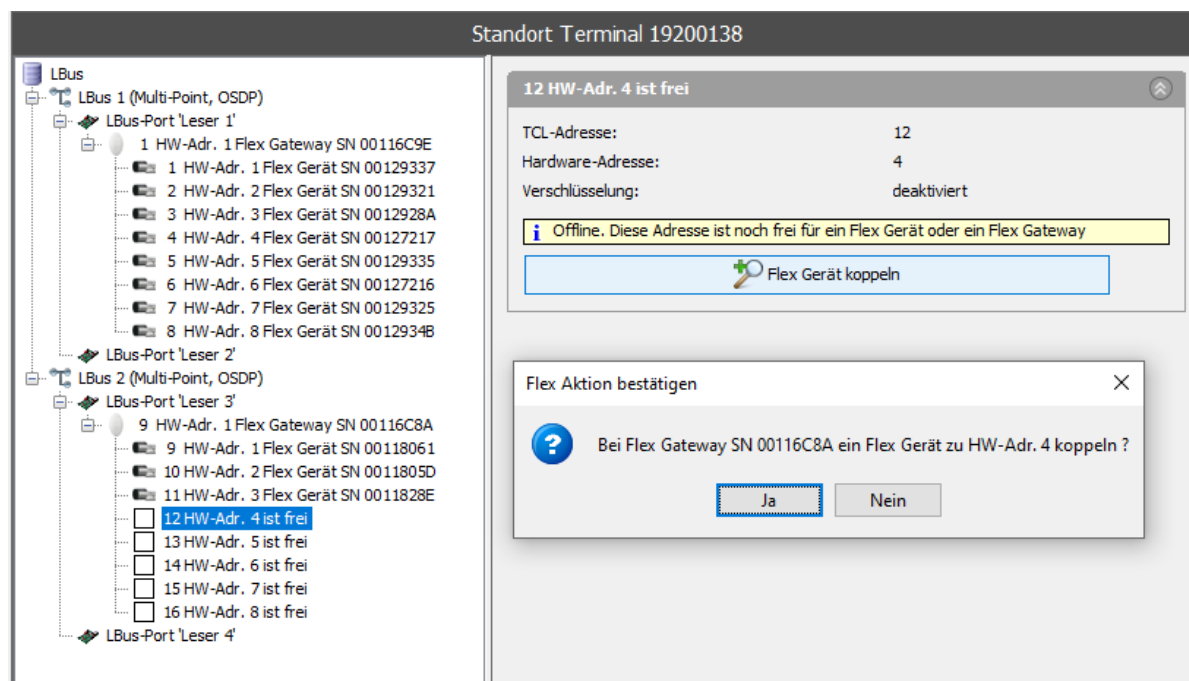


Abbildung 18-5: Gerät an Gateway koppeln

Ändern der Basisadresse

Im folgenden Beispiel ist ein Gateway am LBus 2 mit der HW-Adresse 9 angeschlossen. Es sind keine Flex-Geräte gekoppelt. Um die Basisadresse zu ändern, wählen Sie eine freie Adresse aus. In diesem Beispiel in Abbildung 18-6 wird die freie Adresse 13 ausgewählt.

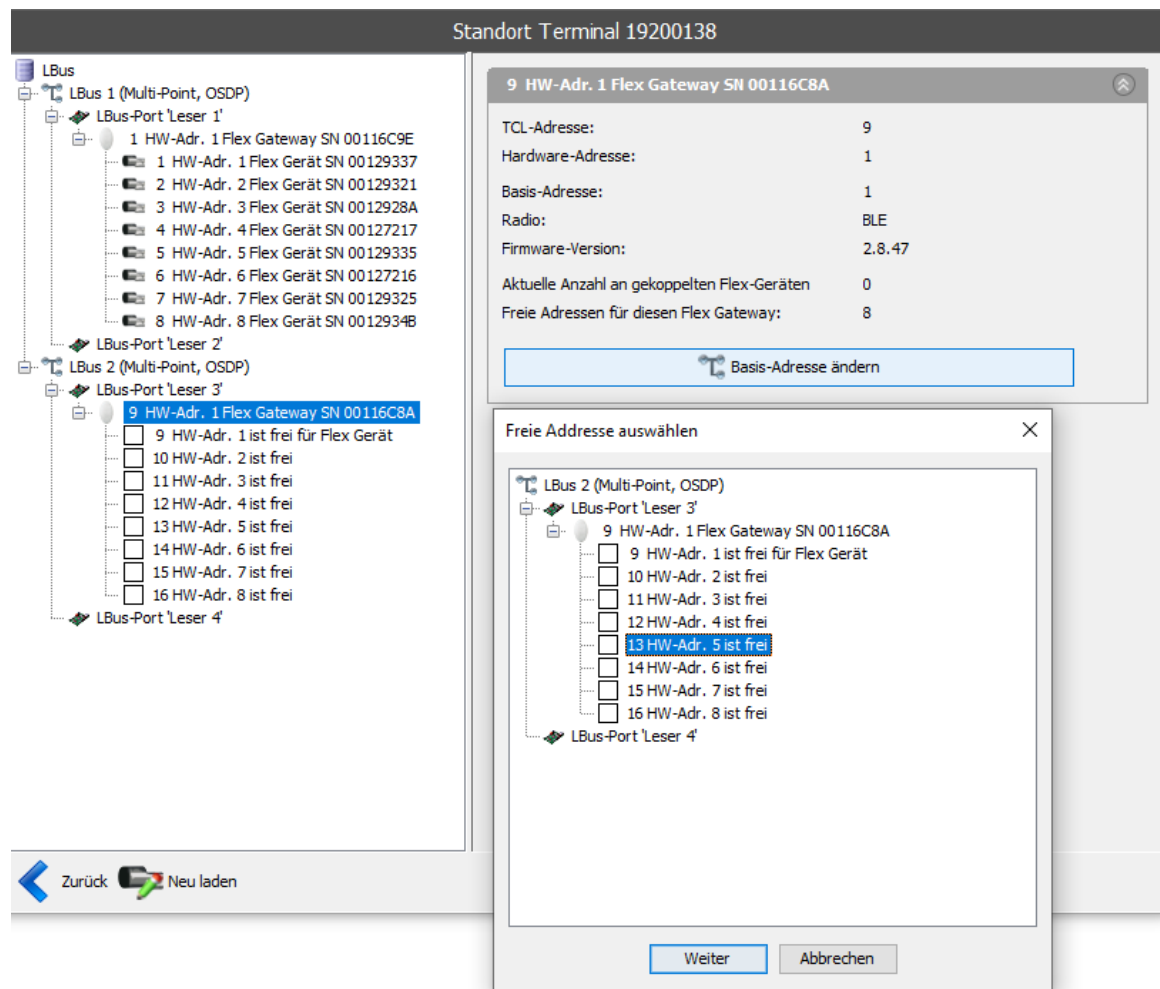


Abbildung 18-6: Freie Adresse auswählen

Ändern der Basisadresse mit Wechsel des LBus-Port

Für dieses Beispiel wurde die LBus-Konfiguration angepasst. LBus2 ist nun in vier Leser bei Port 3 und in vier Leser bei Port 4 aufgeteilt.

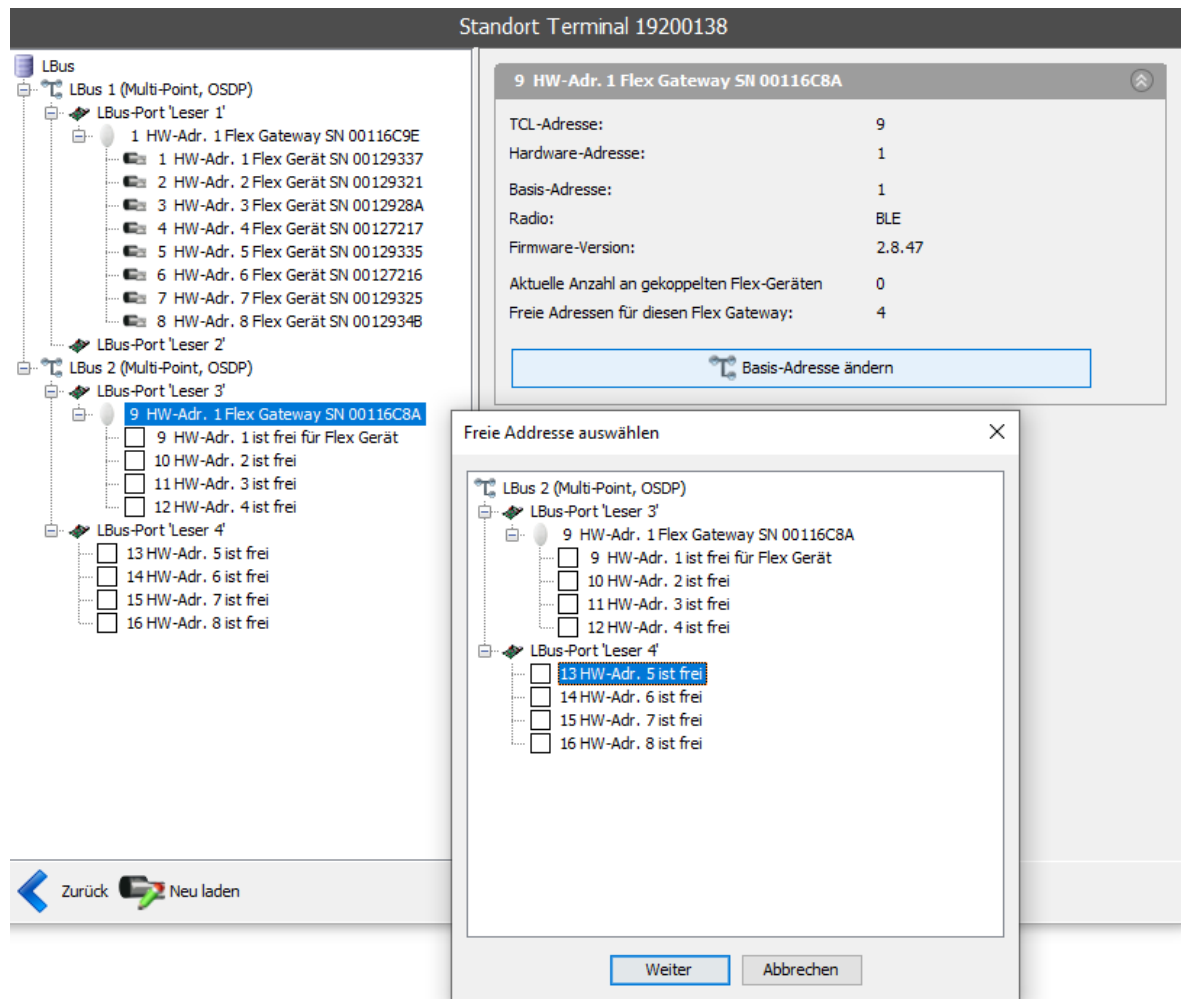


Abbildung 18-7: LBus Konfiguration

Um das Gateway von Adresse 9 (Port 3) auf Adresse 13 (Port 4) zu ändern, gehen Sie wie folgt vor:

- Wählen Sie die entsprechende Konfiguration aus, wie in Abbildung 18-6 dargestellt und klicken Sie auf "Weiter", um fortzufahren.
- Es wird ein Hinweis angezeigt, dass das Gateway auch an den anderen Port angeschlossen werden muss, wenn die Änderungen vorgenommen werden und bestätigen Sie den Vorgang durch Drücken von "Ja".

Nachdem Sie diese Schritte befolgt haben, ist das Gateway mit Adresse 9 erfolgreich auf Port 3 (Adresse 13) geändert. Sie können nun später ein anderes Gateway an Adresse 9 anschließen, falls gewünscht.

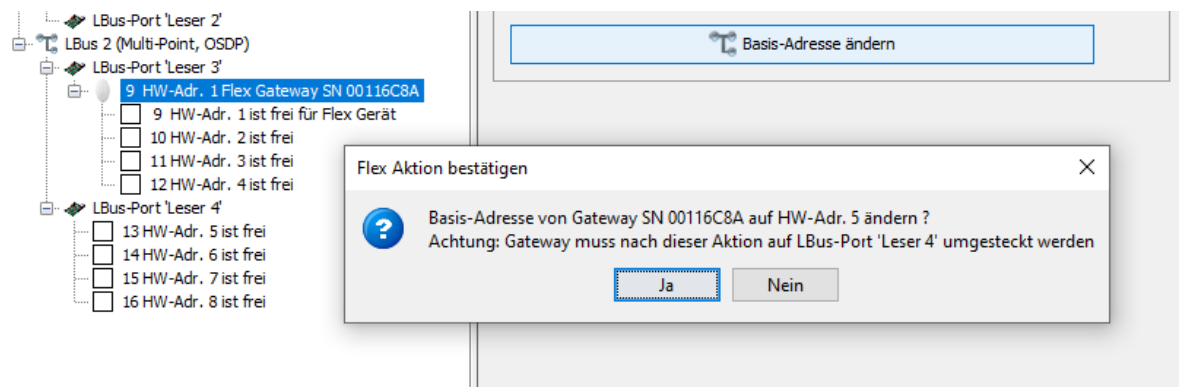


Abbildung 18-8: Hinweis Gateway umstecken

Das Gateway wurde nun auf Adresse 13 (HW Adresse 5) umkonfiguriert, allerdings noch nicht am ACM umgesteckt. Dadurch ist es nicht sichtbar (offline).

Sobald das Gateway umgesteckt wird, ist es sichtbar und der Vorgang ist abgeschlossen.

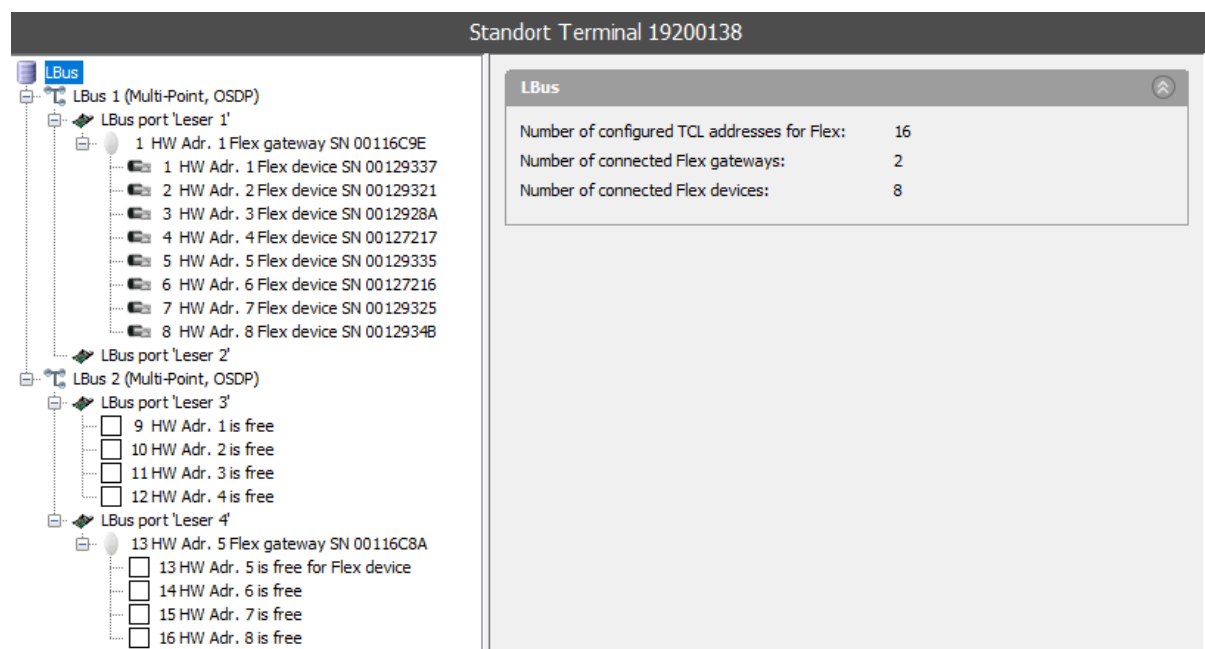


Abbildung 18-9: Basisadresse geändert

Aktivieren des Servicemodus eines INTUS Flex Gateway

Um den Servicemodus eines INTUS Flex Gateways zu aktivieren, wählen Sie das Gateway aus und wählen Sie anschließend die Option "Servicemodus aktivieren".

Der Flex Gateway wird in den Servicemodus versetzt. Details zum Servicemodus finden Sie im INTUS Flex Gateway Handbuch (D3800-615).

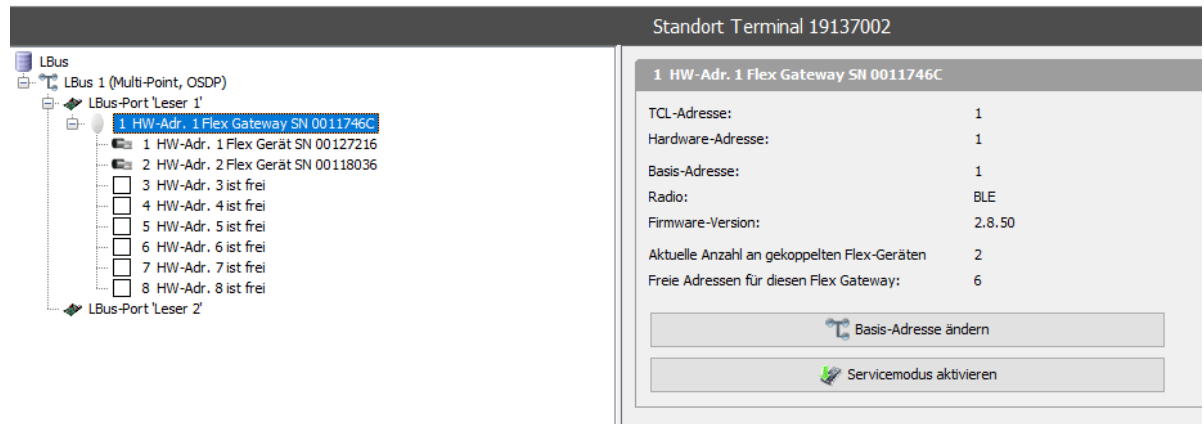


Abbildung 18-10: Servicemodus aktivieren

19 Reset

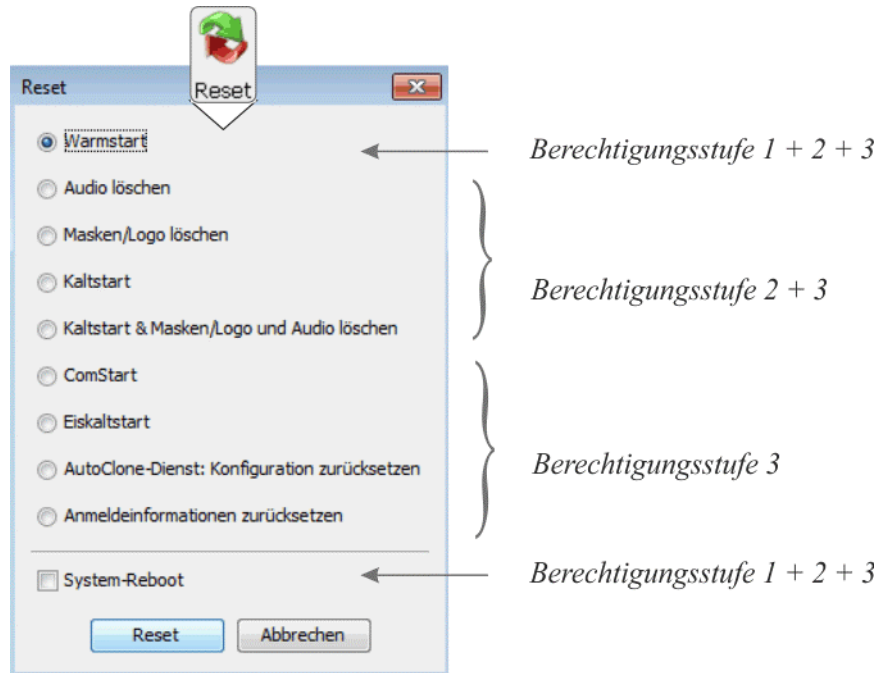


Abbildung 19-1: Reset

	Warmstart	Kaltstart	ComStart	Eiskaltstart
TCL Applikation Variablen Notpuffer	Bleiben gültig	Werden gelöscht	Werden gelöscht	Werden gelöscht
TCL Parameter	Bleiben gültig	Bleiben gültig		
TCP/IP Parameter	Bleiben gültig	Bleiben gültig	Bleiben gültig	
Audio Masken Logo	Bleiben gültig	Bleiben gültig	Werden gelöscht	
Default Programm	Geladen, wenn keine TCL Applikation vorhanden ist	Geladen	Geladen	Geladen



Wenn ein entscheidender Systemparameter verändert wird, z. B. die Größe des Tabellenfelds oder des Notpuffers, wird automatisch ein Kaltstart ausgeführt.

Mit Hilfe des Eiskaltstarts ist es möglich, das Terminal in einen definierten Zustand zu versetzen, wenn es sich fehlerhaft verhält.

AutoClone-Dienst

Diese Möglichkeit ist nur gegeben, wenn die Software INTUS COM eingesetzt wird.

Anmeldeinformationen zurücksetzen

Die Konfiguration von WLAN, IEEE 802.1X und HTTPS Client wird zurückgesetzt.

Dazu gehören Zertifikate, Benutzernamen und Passwörter.

Dies kann z. B. dazu verwendet werden, interne Information vom Gerät zu löschen, bevor es zum PCS Support gesendet wird.

Die Anmeldeinformationen werden bei einem Eiskaltstart ebenfalls gelöscht.

20 Logo laden



Berechtigungsstufe 2 / 3

Gültig für den INTUS 5200 & INTUS 5205.

Gültig für den INTUS 5600, sofern die geladenen Masken es erlauben.



Abbildung 20-1: Logo laden

Folgende Voraussetzungen müssen erfüllt sein, dass ein Logo in die rechte, obere Seite des Displays geladen werden kann:



Größe des Logos beim INTUS 5200 & INTUS 5205

Bei den TPI-Standardmasken (VIG 10-001) zu TPI 3.7.



Breite bis zu 70 Pixel

das Datumsfeld am Display wird ohne Einschränkung angezeigt

Breite bis zu 100 Pixel

das Datumsfeld am Display wird teilweise überschrieben,
nur verkürzte Wochentage werden angezeigt

Größe des Logos beim INTUS 5600

Ist abhängig vom Maskenlayout.

Datenformat des Logos

Dateityp:

21 Serielle Schnittstelle



In Ausnahmefällen wird für eine serielle Schnittstelle das Protokoll TTY oder BSC benötigt, es kann über Kanal A/B/C/D eingestellt werden.

21.1 Basiseinstellungen TTY/BSC

Baudrate

Einstellbare Baudraten sind abhängig vom Gerätetyp. Mögliche Baudraten:

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

Datenformat

Einstellbare Datenformate sind abhängig vom Gerätetyp. Daten-Bits: 8 / 7

Parität: none = Kein Paritäts-Bit, even = gerade Parität, odd = ungerade Parität.

Puffergröße

Empfangspuffer (byte) / Sendepuffer (byte).

21.2 TTY-Protokoll

Mit TTY wird ein Zeichenstrom-Modus ausgewählt, bei dem man die Art der Flusskontrolle einstellen kann. Der TTY Zeichenstrom-Modus enthält folgende Unterebenen:

Hardware-Flusskontrolle: Die Auswahl gibt an, ob das Terminal beim Senden das XON/XOFF Protokoll (None) befolgen soll. Das XON/XOFF Protokoll wird nicht benutzt, wenn RTS/CTS Handshake aktiviert wird.

Senden

Enthält folgende Parameter, die das Verhalten beim Senden eines Zeichens bzw. der Handshakes steuern:

Software-Flusskontrolle (XON/XOFF) aktivieren: Terminal befolgt beim Senden das XON/XOFF Protokoll.

Verarb. auswählen: Mit dieser Auswahl werden die folgenden Einstellungen aktiviert:

CR to EOL: Die Auswahl gibt an, ob das Satzendezeichen CR ("0D") in andere Zeichen umgesetzt wird.

EOL: Es können zwei Satzendezeichen ausgewählt werden, die separat mit hexadezimalen Werten eingestellt werden müssen. Wird beim zweiten Zeichen der Wert 00 gewählt, wird CR nur in ein Satzendezeichen umgesetzt.

Empfang

Enthält folgende Parameter, die das Verhalten beim Empfang eines Zeichens bzw. der Handshakes steuern:

Software-Flusskontrolle (XON/XOFF) aktivieren: Terminal befolgt beim Empfang das XON/XOFF Protokoll.

Verarb. auswählen: Die empfangenen Zeichen sollen verarbeitet werden.

Ignor. EOL aktivieren: Es wird der Eintrag des Zeilenendezeichens in den Empfangspuffer unterdrückt.

EOL 1: Auswahl des ersten von zwei möglichen Satzendezeichen des Leitrechners. Dieses wird mit einem hexadezimalen Wert eingestellt.

Zeichen unterdrücken aktivieren: Bestimmte Zeichen, die etwa aufgrund der im Leitrechner verwendeten Zeilenenden oder Zeichensätze sich in TCL störend auswirken, werden unterdrückt.

EOL to CR aktivieren: Das Satzende des Leitrechners, das unter EOL 1 und EOL 2 einstellbar ist, wird in ein TCL Satzendezeichen CR ("0D") umgesetzt.

EOL 2: Erlaubt die Einstellung eines zweiten Satzendezeichens in hexadezimaler Form. Wenn hier der Wert 00 eingestellt wird, wird nur ein Satzendezeichen erwartet und in CR umgesetzt.

Löschzeichen: Dieser Parameter ermöglicht das Einstellen eines Zeichens in hexadezimaler Form, das ein vorangehendes löschen kann. Dies ist nur im interaktiven Betrieb mit dem Terminal sinnvoll und sollte in allen anderen Fällen auf FF gestellt werden.

EOF / Counter: Der einstellbare hexadezimale Zeichenwert gibt die Anzahl der Zeichen an, auf die mit der unter EOL 1 einstellbaren Verzögerung gewartet wird, bevor sie weitergegeben werden.

Die Voreinstellung unterbindet das Verarbeiten von empfangenen Zeichen, stellt EOF/Counter auf 50 (hexadezimal) sowie EOL 1 auf 01 (100 ms) ein und ermöglicht eine empfangsseitige Datenflusskontrolle über das XON/XOFF-Protokoll.

21.3 BSC-Protokoll

BSC ist ein paketorientiertes Protokoll, das eine gesicherte Datenübertragung unterstützt. Wenn das BSC-Protokoll für eine serielle Schnittstelle ausgewählt wird, wird der BSC-Treiber in seiner Slave-Form aktiviert.

Gruppenkennung/ Geräteerkennung: Adresse zwischen @ und Z

Poll Timeout (s): Zeit in Sekunden (dezimal), die zwischen zwei an das Gerät adressierte Poll-Aktivitäten vergehen darf, ohne dass das BSC-Protokoll einen Offline-Zustand an das TCL-System meldet (das daraufhin das PO-Flag setzt). Diese Zeit muss nach Ausfall der Partyline verstreichen, bis der Offline-Zustand erkannt wird.

Daten Timeout (ms): Zeitspanne, die vom Empfang des ersten Zeichens eines Datenblocks bis zum Empfang des letzten Zeichens dieses Blocks verstreichen darf.

Sendeverzögerung (ms): Erlaubt die Einstellung einer Sendepause in Millisekunden, in der nach Empfang eines Protokoll-Telegramms Ruhe herrschen soll.

Quittungs-Timeout (ms): Stellt die Zeitspanne ein, in der nach Aussenden eines Protokoll-Telegramms eine Antwort von der Gegenstation erwartet wird.

Anzahl Füllzeichen: Anzahl der Füllzeichen, die einem Protokoll-Telegramm angehängt werden; Werte zwischen 0 und 9.

Mindestens 1 Füllzeichen wird bei einer Zweidraht-Partyline wegen der dabei notwendigen Sende-Empfangsumschaltung benötigt. Sollten bei komplexeren Partyline-Strukturen Zwischenstationen (Bridges oder Router) vorhanden sein, können weitere, angehängte Füllzeichen notwendig werden.

Die Empfangsstation darf sich nicht darauf verlassen, dass sie die Füllzeichen empfangen kann bzw. dass nicht aus Treiber- bzw. Leitungsgründen eventuell sogar zusätzliche Füllzeichen angehängt werden.

Weiterhin sollte die Empfangsstation Füllzeichen mit den hexadezimalen Kodierungen 7F und FF gleichwertig verarbeiten können. Die Sendeverzögerung (siehe oben) sollte immer so eingestellt werden, dass neben den eingestellten Füllzeichen ein weiteres Füllzeichen toleriert werden kann. Wenn der BSC-Treiber feststellt, dass Einstellungen nicht sinnvoll sind, werden diese automatisch korrigiert.

Um zu überprüfen, ob die Einstellung nach einem Reset so wie eingestellt übernommen wurde, sollte ein zweites Reset mit Hilfe Reset: "Ja" durchgeführt werden. Danach kann die Einstellung im Setup überprüft werden.

EOL: Das Satzendezeichen kann ausgewählt werden. Voreinstellung: 00

22 Firewall-Einstellungen im Netzwerk

Beim Betrieb von INTUS Terminals im Netzwerk können die Verbindungen zum Terminal in drei Kategorien aufgeteilt werden:

- Normaler Betrieb (Download von Stammdaten, ggfs. Upload von Buchungsdaten)
- Statusabfragen (insbesondere HTML-Statusseite)
- Wartung (Konfigurationsänderungen, Firmware Update)

Dabei werden unterschiedliche TCP/UDP-Verbindungen benötigt, die nachfolgend dokumentiert sind.

Darüber hinaus werden ggfs. noch die üblichen Ports für DHCP, DHCPv6, Ping (ICMP, ICMPv6) benötigt.

Bei TCP-Verbindungen ist nur die Richtung des Verbindungsaufbaus angegeben; es wird davon ausgegangen, dass die weiteren Datenpakete, aufgrund der bestehenden Verbindung, akzeptiert werden (stateful firewall).

Der Datenport ist konfigurierbar, neben der Richtung des Verbindungsaufbaus (Standard = passiv) ist auch die Portnummer (Standard = 3001) einstellbar.

Verbindungsaufbau	Protokoll	Quellport	Zielpport	Anmerkung
Host → Terminal	TCP	*2)	<wie konfiguriert>*4)	Verbindungsaufbau „passiv“ oder „passiv/RAS“
Terminal → Host	TCP	*3)	<wie konfiguriert>*4)	Verbindungsaufbau „aktiv“
PCStatusabfrage → Terminal	TCP	*2)	80	
PCWartung ↔ Terminal	UDP	57005	57005	
	UDP	48879	57005	
PCWartung → Terminal	TCP	*2)	3121	

1) Nur bei Terminals, die IPv6 unterstützen

2) Wird durch das Betriebssystem gewählt; unter Umständen eingegrenzt, je nach eingesetzter Software

3) Wird vom Terminal frei gewählt

4) Konfiguration > Kanal A > TCP-Einstellungen > Port

23 Fehlerdiagnose

23.1 Leser-Aktionstest

Mit diesem Test kann die Hardware des Geräts und der angeschlossenen, externen Leser auf Funktionalität (Gut-/Fehllesungen) überprüft werden.

23.1.1 INTUS 3xxx und 5xxx

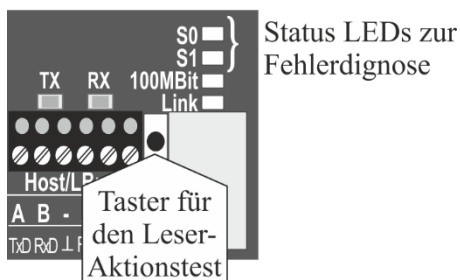
Für diese Geräte kann ein Leser-Aktionstest direkt am Gerät im lokalen Setup über „Test>Leser-Aktion“ durchgeführt werden, siehe auch Handbuch „Lokaler Setup“.

23.1.2 INTUS 5540

Für den INTUS 5540 finden Sie unter dem in Kapitel 1.2 genannten Download-Link ein Programm zum Testen der angeschlossenen Leser.

23.1.3 INTUS ACM80e

INTUS ACM80e Wand
Taster&LEDs innerhalb des Geräts



INTUS ACM80e Rack
Taster&LEDs an der Vorderfront

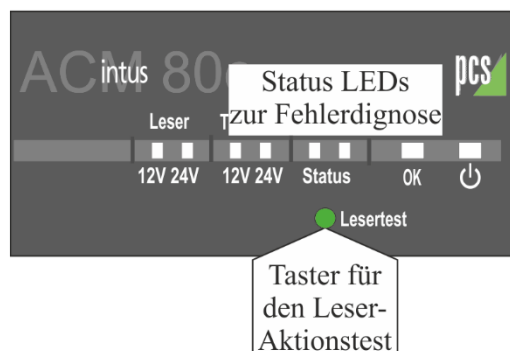


Abbildung 23-1: Leser-Aktionstest ACM80e

Leser-Aktionstest starten

INTUS ACM80e von der Stromversorgung trennen. An die Stromversorgung anschließen und sofort Taster „Lesertest“ drücken und gedrückt halten, bis zwei kurze Signaltöne ertönen.

Nach kurzer Zeit blinken die Status LEDs. Das Gerät ist im Leser-Aktionstest.

Alle vorhandenen Leser werden freigeschaltet; jede Lesung wird angezeigt:

- **Gutlesung:** Die beim Leser befindlichen Relais und die entsprechenden Relais im INTUS ACM80e werden für drei Sekunden aktiviert. Eine Gutlesung wird zusätzlich durch Hupen und das Aufleuchten der grünen Leuchtdiode signalisiert.
- **Fehllesung:** Am jeweiligen Leser wird die rote Leuchtdiode und die Hupe aktiviert.

Leser-Aktionstest beenden

INTUS ACM von der Stromversorgung trennen und wieder anschließen.

23.1.4 INTUS ACM40e

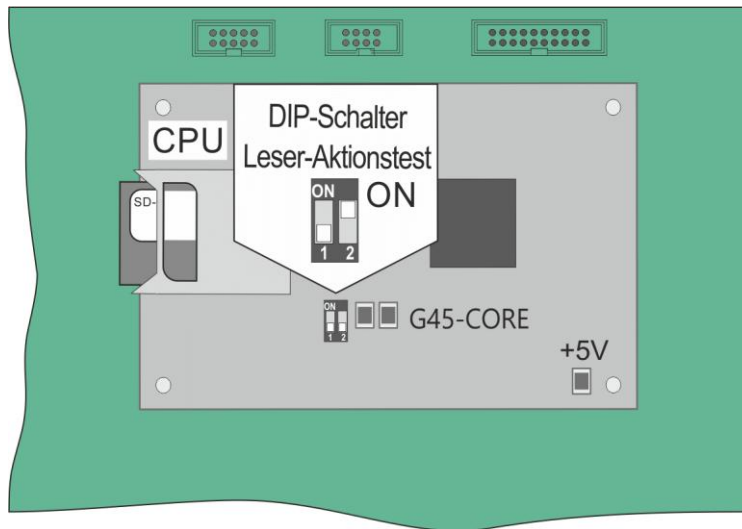


Abbildung 23-2: Leser-Aktionstest ACM40e



Leser-Aktionstest starten

INTUS ACM40e von der Stromversorgung trennen. Den rechten DIP-Schalter (2) auf der CPU auf ON stellen und das Gerät einschalten.

Warten Sie, bis das Gerät hochgefahren ist. Das Gerät ist im Leser-Aktionstest-Modus.

Alle vorhandenen Leser werden freigeschaltet; jede Lesung wird angezeigt:

- **Gutlesung:** Die beim Leser befindlichen Relais und die entsprechenden Relais im INTUS ACM40e werden für drei Sekunden aktiviert. Eine Gutlesung wird zusätzlich durch Hupen und das Aufleuchten der grünen Leuchtdiode signalisiert.
- **Fehllesung:** Am jeweiligen Leser wird die rote Leuchtdiode und die Hupe aktiviert.

Leser-Aktionstest beenden

INTUS ACM40e ausschalten, von der Stromversorgung trennen und den DIP-Schalter wieder auf OFF stellen.

23.2 Automatische Selbsttests

Nach dem Einschalten der Netzversorgung oder nach einem Reset führt das Terminal einen automatischen Selbsttest und eine Initialisierung durch.

Dabei kann es vorkommen, dass das System feststellt, dass Systemressourcen nicht ausreichen oder andere schwerwiegende Fehler aufgetreten sind.

Der Systemfehler wird angezeigt:

- Bei allen Terminals über die Hupe, diese ertönt jedoch nur, wenn der Deckel des Terminals mit dem Grundgerät verbunden ist.
- Beim INTUS ACM über die Status LEDs + Hupe.
- S0 - Status LED leuchtet, S1 - Status LED blinkt und die Hupe ertönt gleichzeitig, Position der Status LEDs siehe obenstehende Abbildung.
- Beim INTUS 5500 und INTUS 5320 wird im Display bei der Initialisierung zusätzlich folgende Meldung ausgegeben:

SYSTEM ERROR: X

SYSTEM ERROR:	Status LED blinkt, Hupe tönt	Ursache und Behebung
G	7x	Geräte-Firmware und Textdatei INTUS.TXT , mit den sprachlich abhängigen Meldungs- und Setuptexten, passen nicht zusammen. Firmware-Update mit INTUS RemoteSetup durchführen.
H	8x	Die Verbindung zum Leitrechner konnte nicht geöffnet werden. Behebung: Versuch eines Eiskaltstarts. Hat das keinen Erfolg, liegt ein Hardware-Problem vor, das repariert werden muss.
I	9x	Die Hardware-Konfiguration konnte nicht aus dem EEPROM geladen werden. Behebung: Der Zutrittskontrollmanager muss mit der Produktions- und Wartungssoftware neu produziert werden. Wenn das keinen Erfolg hat, liegt vermutlich ein Hardware-Fehler vor.
J	10x	Es wurden mehr Software-Timer angefordert als angelegt sind. Interner Software-Fehler, der nicht vorkommen sollte.
K	11x	Eine interne Speicheranforderung zur Anlage einer Tabelle im DRAM konnte nicht erfüllt werden. Die Ursache kann in einer zu großen Puffervorgabe für die seriellen Kanäle liegen. Behebung: Eiskaltstart und Neukonfiguration. Wenn das keinen Erfolg hat, liegt vermutlich ein Hardware-Fehler vor.
L	12x	Ein Software-Modul konnte sich nicht für eine De-Initialisierung eintragen. Interner Software-Fehler, der nicht vorkommen sollte.
M	13x	Speichermangel beim Anlegen einer Realzeitkomponente. Behebung wie unter 11x blinken/tönen.
N	14x	Speichermangel beim Anlegen eines Ringpuffers. Behebung wie unter 11x blinken/tönen.

O	15x	Fehler in der SRAM-Verwaltung. Interner Fehler, der nicht vorkommen sollte.
P	16x	Fehler in der SRAM-Verwaltung. Interner Fehler, der nicht vorkommen sollte.
Q	17x	Speichermangel beim Anlegen eines Realzeitprozesses. Behebung wie unter 11x blinken/tönen.
R	18x	Notpuffer-Konfiguration zu groß. Dieser Fehler sollte weitgehend vermieden werden durch die automatische Neukonfiguration, die die Notpuffergröße auf die Voreinstellung von 48kB reduziert. Behebung: Eiskaltstart mit Neukonfiguration, wobei Notpuffer und Tabellenfeld so konfiguriert werden sollten, dass mindestens 30 kB für den Download- Bereich, DL, übrigbleiben.



Bei Systemfehlern ist, im Gegensatz zu den Abbrüchen wegen defekter Hardware, INTUS RemoteConf weiterhin benutzbar.

So können Konfigurationsfehler im Reset durch einen Eiskaltstart behoben werden, siehe Kapitel 19.

23.3 Fehlerdiagnose über Log-Dateien



Die Log-Dateien werden gespeichert unter:

- %AppData%\INTUS\RemoteConf

Wenn RemoteConf0.log 512 KB überschreitet, wird RemoteConf0.log in RemoteConf1.log umbenannt und eine neue RemoteConf0.log angelegt ("logfile rotation").

Wird ein zweites INTUS RemoteConf gestartet, heißt dessen Logdatei RemoteConf0.log.1.

Bis zu 4 Dateien können angelegt werden:

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

Alle gerätespezifischen Einträge in der Log-Datei beginnen mit der Seriennummer des Geräts.

23.4 Erfolgreiche Fehlerdiagnose

Falls eine Fehlerdiagnose nicht möglich ist, wenden Sie sich bitte an den PCS Support:

E-Mail: support@pcs.com

In diesem Fall werden folgende Informationen benötigt:

- Genaue Fehlerbeschreibung
- Firmware-Versionsnummer und eingestellte Parameter des Geräts, beides finden Sie auf der Statusseite in INTUS RemoteConf.

24 Tabellen für die Parameter

Die folgenden Tabellen führen die wichtigsten einstellbaren Parameter mit ihren Voreinstellungen auf. Notieren Sie alle Änderungen und Einstellungen in den Tabellen, um sie bei Support-Anfragen parat zu haben.

IP-Konfiguration - Netzwerkanschluss

Parameter		Voreinstellung	Änderung
Standort		Standort Terminal <seriennummer>	
Kontakt		Ansprechpartner	
DHCP-Hostname		intus-<seriennummer>	
Hostschnittstelle		LAN	
IPv4		DHCP	
<i>IPv4 ohne DHCP</i>	IPv4 Adresse	192.168.042.127	
	IPv4 Netzmaske	255.255.255.000	
	IPv4 Gateway	0 . 0 . 0 . 0	
IPv6		RADV	
<i>IPv6 Manuelle Einstellung</i>	IPv6 Adresse	*2001:0000:0000:0000: 0000:0000:0000:0000	
	IPv6 Präfix	64	
<i>IPv6 DHCP</i>	IPv6-Gateway	RADV	
	IPv6-Gateway Adresse	*2001:0000:0000:0000: 0000:0000:0000:0000	
ETH-Link		Auto Negotiation	
IEEE 802.1X		Nicht aktiviert	

Kanal A - Host Kommunikation TCP

Parameter		Voreinstellung	Änderung
Verbindungsaufbau		Passiv	
Port-Nummer		3001	
Verbindungs- aufbau: aktiv	IPv4 oder IPv6 Adresse	0 . 0 . 0 . 0 oder *0000:0000:0000:0000: 0000:0000:0000:0000	

** Angezeigt wird 2001.:

TCL-Parameter

Parameter	Voreinstellung	Änderung
Tabellenfeld (Byte)	49152	
Notpuffer (Byte)	49152	
Quittungszeit (S)	26	
Notpuffer-Sätze mit Satznummer	Nein	
Default TCL-Programm bei Kaltstart laden	Ja	
Größe BMI-Feld (Byte)	88	
Label-Anzahl	1024	
Zeichensatz	ISO646-DE	

Tabellen für Sicherheitseinstellungen*Kanal A - Zugang zur Hostschnittstelle*

Parameter	Voreinstellung	Änderung
Verschlüsselung <i>Berechtigungsstufe 3</i>	deaktiviert	
Login		
Passwort für einfachen Zugriff <i>Berechtigungsstufe 2/3</i>	deaktiviert	
Passwort für administrativen Zugriff <i>Berechtigungsstufe 2/3</i>	deaktiviert	
Sendedatensatz Format		
Routingbytes <i>Berechtigungsstufe 2/3</i>	deaktiviert	
Satznummernzeichen für Login-Meldungen <i>Berechtigungsstufe 2/3</i>	deaktiviert	

Firewall IPv4

Netzadresse	Netzmaske	Daten	Wartung	Status
. . .	. . .			
. . .	. . .			
. . .	. . .			
. . .	. . .			
. . .	. . .			

Firewall IPv6

Netzadresse	Präfix	Daten	Wartung	Status

Wartungsgruppe & Passwort ändern / LBus Schlüssel

Parameter		Voreinstellung	Änderung
Login	Wartungsgruppe Berechtigungsstufe 3	0	
	Passwort Berechtigungsstufe 1	111111	
	Passwort Berechtigungsstufe 2	14789632	
	Passwort Berechtigungsstufe 3	14589632	
LBus 1	Schlüssel Berechtigungsstufe 3	ohne	
LBus 2	Schlüssel Berechtigungsstufe 3	ohne	

25 Lizenzbestimmungen der freien Software

Die Geräte-Firmware der PCS Terminals enthält unter anderem freie Software, die lizenziert ist.

Diese freie Software wurde von Dritten entwickelt und ist urheberrechtlich geschützt. Sie finden die Lizenztexte in der englischen Original-Fassung in INTUS RemoteConf.

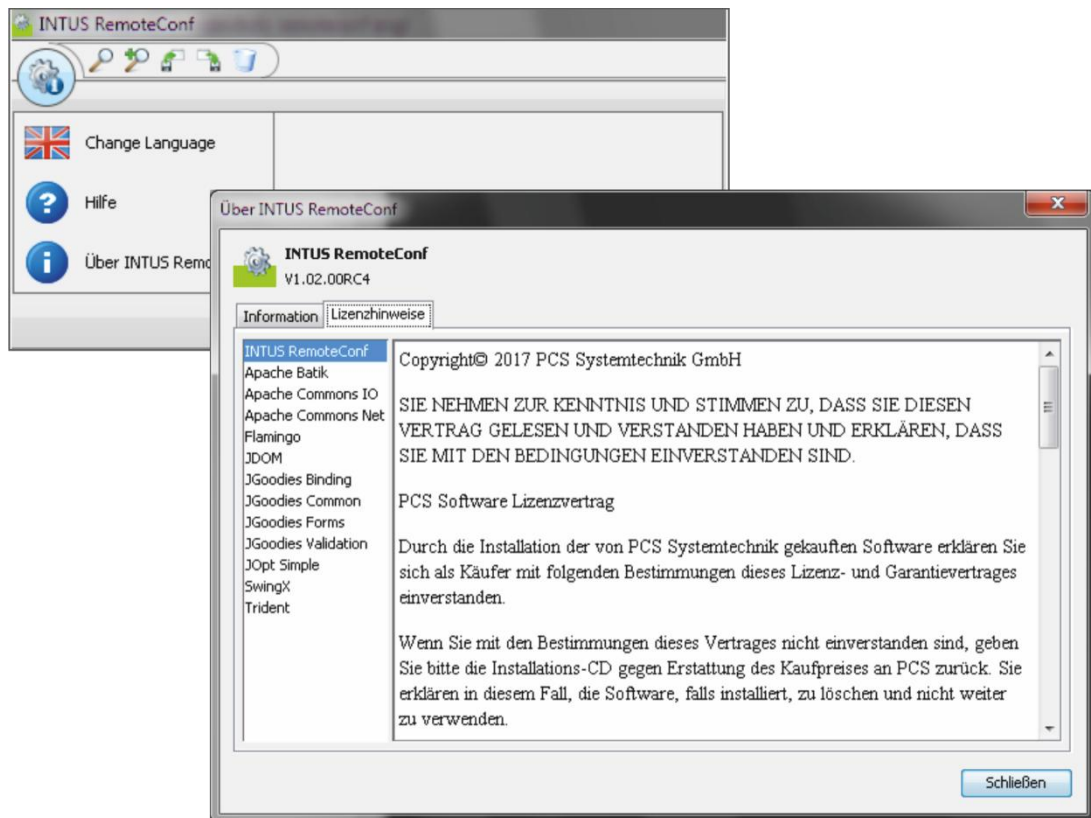


Abbildung 25-1: Lizenzbestimmungen

Die freie Software wird unentgeltlich überlassen. Sie sind berechtigt, diese freie Software gemäß den oben genannten Lizenzbedingungen zu nutzen. Bei Widersprüchen dieser Lizenzbedingungen zu den für die Software geltenden Lizenzbestimmungen der PCS Systemtechnik GmbH gehen für die freie Software die oben genannten Lizenzbestimmungen vor.

Sie haben keine Mängelhaftungsansprüche gegen die PCS Systemtechnik GmbH, wenn die freie Software Schutzrechte Dritter verletzt.

PCS Systemtechnik GmbH bietet an, auf Anfragen und gegen eine Gebühr, die die tatsächlichen Vertriebskosten nicht übersteigt, eine vollständige computerlesbare Kopie des entsprechenden Quellcodes auf einem für den elektronischen Datenaustausch üblichen Medium zu liefern oder verfügbar zu machen. Dieses Angebot gilt innerhalb eines Zeitraums von 3 Jahren nach dem Kauf dieses Produkts. Den Quellcode erhalten Sie beim PCS Support oder unter www.pcs.com/services/download.

26 Abbildungsverzeichnis

Abbildung 4-1: Anbindung PC/Terminal	22
Abbildung 4-2: Schaltflächen in RemoteConf.....	24
Abbildung 4-3: IP-Konfiguration	25
Abbildung 4-4: Terminalliste ordnen.....	26
Abbildung 4-5: PC-Firewall.....	26
Abbildung 4-6: Info-Schaltfläche	26
Abbildung 4-7: Lizenz freischalten	27
Abbildung 5-1: Einstieg in die Konfiguration.....	32
Abbildung 6-1: Einloggen	33
Abbildung 7-1: Übersicht Konfiguration.....	34
Abbildung 7-2: Konfiguration beenden	36
Abbildung 8-1: Netzanschluss konfigurieren	37
Abbildung 8-2: WLAN.....	39
Abbildung 8-3: IEEE 802.1X/WPA2-Enterprise	41
Abbildung 8-4: Mobilfunk.....	43
Abbildung 9-1: Kanal A - Nicht konfiguriert	44
Abbildung 9-2: HTTPS Client Einstellungen.....	46
Abbildung 10-1: Firewall Beispiel-Konfiguration	49
Abbildung 10-2: Status nicht freigegeben	49
Abbildung 11-1: Verkabelung beim INTUS 5200/5320/5500/5540/5600	52
Abbildung 11-2: Point-to-Point-Verkabelung des INTUS ACM80e.....	55
Abbildung 11-3: MultiPoint-Verkabelung des INTUS ACM80e.....	55
Abbildung 11-4: Leser konfigurieren	56
Abbildung 11-5: Lesertyp / einfache Adressierung.....	57
Abbildung 11-6: Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser	59
Abbildung 11-7: Beispiel ACM40e mit 16 INTUS Flex Endgeräten	62
Abbildung 11-8: ACM40e, 2 Leser, 8 INTUS Flex Endgeräte	66
Abbildung 11-9: ACM40e, 4 Leser, 8 INTUS Flex Endgeräte	70
Abbildung 11-10: Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten.....	74
Abbildung 11-11: Beispiel - ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2.....	77
Abbildung 11-12: Aktivierung der AES-Verschlüsselung.....	78
Abbildung 11-13: Konfiguration der AES-Schlüssel	79
Abbildung 11-14: Kundenschlüssel konfigurieren	79
Abbildung 11-15: Kundenschlüssel ändern	80
Abbildung 11-16: Kundenschlüssel entfernen	81
Abbildung 11-17: LBus-Verschlüsselung	82
Abbildung 12-1: Internen Leser einstellen.....	83
Abbildung 13-1: TCL Parameter einstellen	84
Abbildung 14-1: Hardware-Einstellungen.....	86
Abbildung 15-1: Login – Wartungsgruppe und Passwörter ändern.....	87
Abbildung 16-1: Zeiteinstellungen	89
Abbildung 17-1: LBus-Aktionen wählen	91
Abbildung 17-2: Leserspezifische Einstellungen konfigurieren	94

Abbildung 17-3: LBus-Aktionsfolge zusammenstellen	96
Abbildung 18-1: Flex Air	98
Abbildung 18-2: Ansicht für Flex Konfiguration	98
Abbildung 18-3: Fehlermeldung - Ändern der Basisadresse	99
Abbildung 18-4: Gerät von Gateway entfernen	100
Abbildung 18-5: Gerät an Gateway koppeln	100
Abbildung 18-6: Freie Adresse auswählen	101
Abbildung 18-7: LBus Konfiguration	102
Abbildung 18-8: Hinweis Gateway umstecken	103
Abbildung 18-9: Basisadresse geändert	103
Abbildung 18-10: Servicemodus aktivieren	104
Abbildung 19-1: Reset	105
Abbildung 20-1: Logo laden	107
Abbildung 23-1: Leser-Aktionstest ACM80e	112
Abbildung 23-2: Leser-Aktionstest ACM40e	113
Abbildung 25-1: Lizenzbestimmungen	120

27 Index

- Berechtigungsstufen 16
- Blau markiert 25
- BSC-Protokoll 106
- Datenport 108
- Datenübertragung: Datensatz 82
- Display: Kontrast 84
- DNS-Server 36
- EEPROM 111
- Eiskaltstart 102
- Fehler: Fehlerbeschreibung 113
- Fehlerdiagnose 112
- Firewall 46
- Firmware 111
- Freie Software 117
- Handbücher 9
- Hostname 36
- HTTPS Client 44
- Hupe 84
- INTUS Graph 83
- IP Setup 25
- IP-Konfiguration: Netzmaske 36
- IPv4 36
- IPv6 37
- Java 22
- Kaltstart 102
- Kanal A: Port-Nummer 43;
Verbindungs Aufbau 42
- Konfiguration 32
- LBus 48; Beispiel 75
- Leser 109; Fehllistung 110
- Lizenzbestimmungen 117
- Logo 104
- Modus 56
- Netzwerkanschluss 35
- Parameter 114
- Partner-Kit: INTUS.TXT 111
- Partyline 107
- Passwort 85
- PC Firewall 26
- PCS-Hotline 17
- Schaltflächen 24
- Sommerzeit 88
- Sound 83
- SRAM 112
- Symbole 8
- TCL: Default-Programm 83;
Ladeanforderung 83; Notpuffer
82
- TCL Programmierhandbuch 9
- TCL-Parameter 82
- Terminalliste 25
- TTY-Protokoll 105
- UTC 88
- Wartungsgruppe 85
- Winterzeit 88
- Zeichensatz 83

Haben Sie noch Fragen?

Rufen Sie uns an.

PCS-Hotline: +49 (0)89/68004 – 666

Email: support@pcs.com

Dieses Handbuch soll so hilfreich wie möglich sein. Wenn Sie Anregungen zur Optimierung haben, lassen Sie es uns bitte wissen. Wir bedanken uns schon jetzt für Ihre Mühe.

Ihre 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

