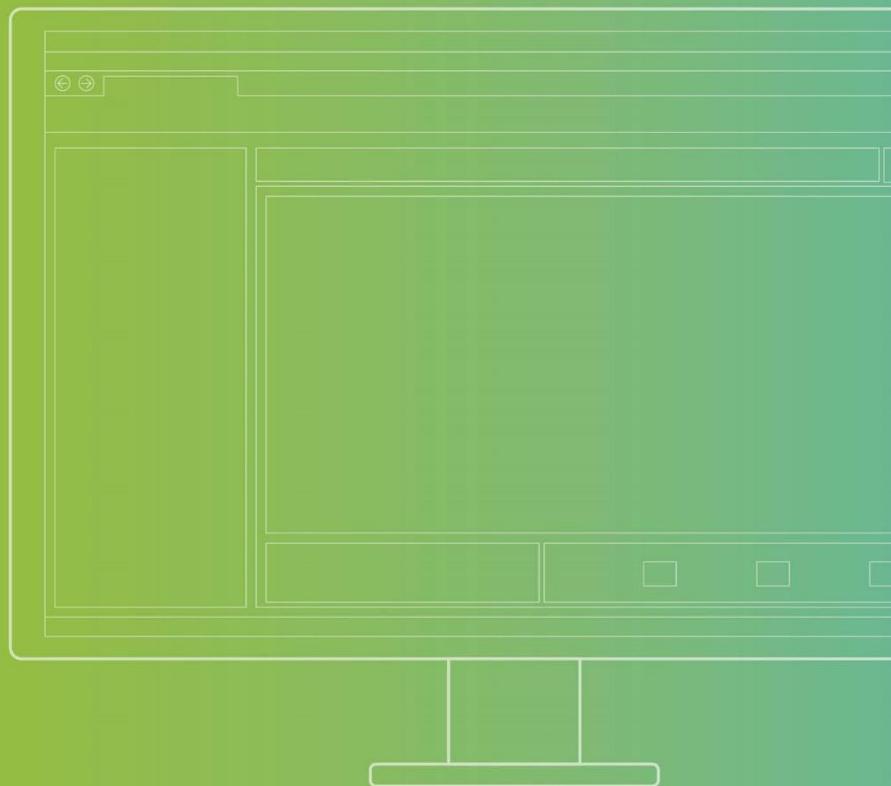


MANUAL



INTUS RemoteConf

Konfiguration und Betrieb

D5000-001.11

INTUS RemoteConf

Konfiguration und Betrieb

Stand 02/2023

Bestell-Nr. D5000-001.11

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 - 562E-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.

©2023 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
4 Einstieg in INTUS RemoteConf	17
4.1 Installation von INTUS RemoteConf auf dem PC	17
4.1.1 Installation auf PCs mit Microsoft Windows-Betriebssystemen	17
4.1.2 Ausführen von INTUS RemoteConf auf anderen Betriebssystemen	18
4.2 Schaltflächen von INTUS RemoteConf	19
4.3 Terminal zur Terminalliste hinzufügen	20
4.4 Terminalliste neu ordnen	21
4.5 PC-Firewall	21
4.6 Info-Schaltfläche	21
4.7 Gleichzeitiges Ausführen von Aktionen an mehreren Terminals	22
5 Einstieg in die Konfiguration	23
6 Login – Einloggen ins Terminal	24
6.1 Berechtigungsstufen	24
6.2 Vorgehen	24
7 Konfiguration	25
7.1 Übersicht	25
7.2 Konfiguration als Datei speichern	25
7.3 Konfiguration beenden	26
8 Netzwerkanschluss (IP) konfigurieren	27
8.1 WLAN	29

8.2	IEEE 802.1X/WPA2-Enterprise.....	30
8.3	Mobilfunk.....	31
9	Kanal A - Host Kommunikation einstellen	32
9.1	TCP-Einstellungen	32
9.2	HTTPS Client Einstellungen.....	34
9.3	Sicherheitseinstellungen	35
10	Firewall konfigurieren	36
11	LBus konfigurieren	37
11.1	Maximal mögliche Anzahl der Leser	37
11.2	Verkabelung beim INTUS 5200/5320/5500/5540/5600.....	38
11.3	Verkabelungsmöglichkeiten beim INTUS ACM40e	39
11.4	Verkabelungsmöglichkeiten beim INTUS ACM40e mit Wiegand-Modul	39
11.5	Verkabelungsmöglichkeiten beim INTUS ACM80e	40
11.6	Point-to-Point-Verkabelung des INTUS ACM80e.....	41
11.7	Multi-Point-Verkabelung des INTUS ACM80e	41
11.8	Leser konfigurieren	42
11.9	Lesertyp / einfache Adressierung.....	43
11.10	Betriebsart.....	44
11.11	Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser.....	45
11.12	Beispiel - ACM40e mit 2 INTUS 700/6xx/350H Lesern und 4 INTUS Flex Endgeräten	47
11.13	Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten	50
11.14	Beispiel - ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2	53
11.15	LBus AES-Verschlüsselung	54
11.15.1	Voraussetzungen.....	54
11.15.2	Aktivierung der AES-Verschlüsselung	54
11.15.3	Konfiguration der AES-Schlüssel.....	55
11.15.4	Kundenschlüssel konfigurieren	55
11.15.5	Option AES-Verschlüsselung nur mit Kundenschlüssel.....	56
11.15.6	Kundenschlüssel ändern.....	56
11.15.7	Kundenschlüssel entfernen.....	57
11.15.8	AES-Verschlüsselung bei OSDP	57
11.16	LBus-Verschlüsselung (PCS-proprietär)	58
12	Internen Leser einstellen.....	59
13	TCL Parameter einstellen	60

13.1	Einstellungen	60
13.2	Erweiterte Benutzerschnittstelle	61
13.3	INTUS Sound.....	61
14	Hardware	62
14.1	Display	62
14.2	Magic-Eye (nur INTUS 5320).....	62
14.3	Hupe	62
15	Login – Wartungsgruppe und Passwörter ändern.....	63
15.1	Wartungsgruppe	63
15.2	Passwort der Berechtigungsstufe ändern	63
16	Zeit.....	64
16.1	NTP Client.....	64
16.2	UTC offset - Abweichung zur UTC Zeit.....	65
16.3	Sommer/Winterzeitumschaltung	65
17	LBus-Aktionen.....	66
17.1	Überblick	66
17.2	Aktion "Firmwareupdate für Leser"	67
17.3	Aktion "Parametrierkarte am Leser freigeben/sperren"	67
17.4	Aktion "LBus-Schlüssel an Leser übertragen"	67
17.5	Aktion "Leser Parameter Download"	68
17.6	Aktion "Leserspezifische Einstellungen konfigurieren".....	69
17.6.1	Allgemeine Aktionen	69
17.6.2	Einstellungen von montageortspezifischen Parametern	70
17.7	Aktionsfolge zusammenstellen.....	70
18	Reset	72
19	Logo laden	74
20	Serielle Schnittstelle.....	75
20.1	Basiseinstellungen TTY/BSC	75
20.2	TTY-Protokoll	75
20.3	BSC-Protokoll	76
21	Firewall-Einstellungen im Netzwerk	78
22	Fehlerdiagnose	79
22.1	Leser-Aktionstest	79
22.1.1	INTUS 3xxx und 5xxx	79
22.1.2	INTUS 5540	79

22.1.3	INTUS ACM80e	79
22.1.4	INTUS ACM40e	80
22.2	Automatische Selbsttests	80
22.3	Fehlerdiagnose über Log-Dateien	82
22.4	Erfolglose Fehlerdiagnose	83
23	Tabellen für die Parameter	84
24	Lizenzbestimmungen der freien Software	87
25	Abbildungsverzeichnis	88
26	Index	90



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 unterwiesenen 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 V1.10.0.



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.

1.1 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 3100/3150/34x0/5300/5320/5500/ACM40/ACM40e/80e*
(*ab Firmware 1.6) 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 Maskenfreischaltung 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 á 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 Multi-Point	◆ / ◇ / ◇
LBus2 Modul für bis zu 8 weitere Zutrittsleser (Multi-Point)	◇
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 Ringkerntrofo, 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



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

Hierfür finden Sie Tabellen in Kapitel 23.

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**

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.

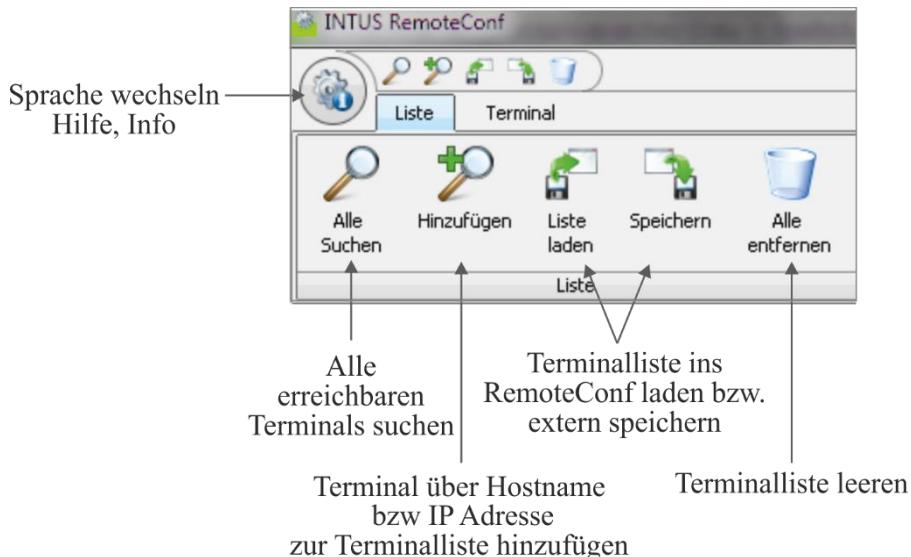


Sie müssen daher selbst eine Java-Laufzeitumgebung (JRE) Ihrer Wahl auf dem PC installieren, damit INTUS RemoteConf gestartet werden kann.

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:

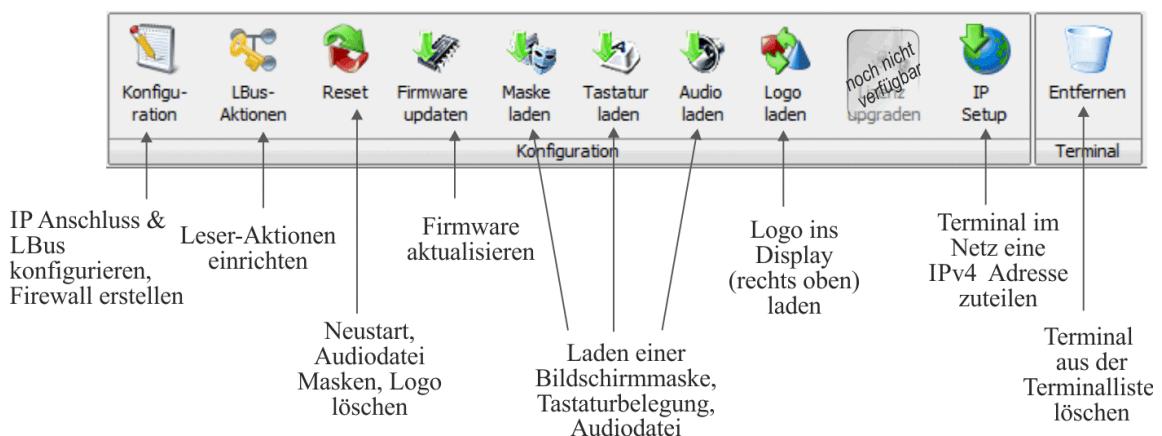
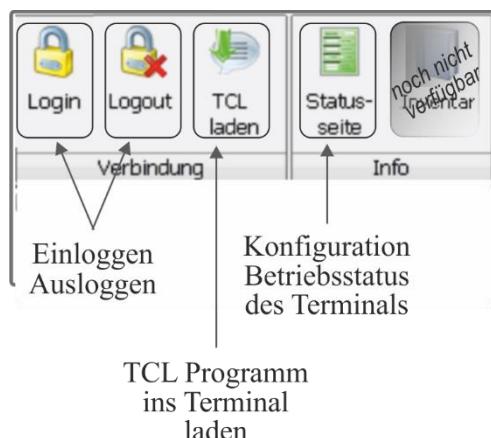


Abbildung 4-2: Schaltflächen in RemoteConf

4.3 Terminal zur Terminalliste hinzufügen

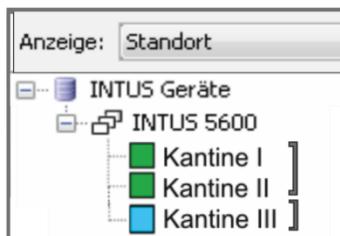


oder



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

Alle erreichbaren Terminals werden angezeigt



Grüne markierte Terminals sind erreichbar
 und können konfiguriert werden.
Blau markierte Terminals sind für die
 Konfiguration nicht ausreichend erreichbar.

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

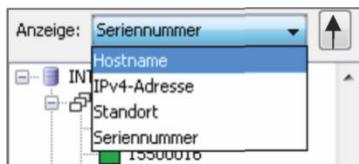
Gateway, auf 0.0.0.0 setzen, um vorhandene
 Einträge im Terminal zu löschen

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:

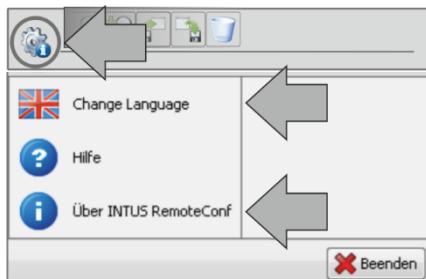


„Zugriff zulassen“ anklicken.

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
Lizenzzvereinbarungen

Abbildung 4-6: Info-Schaltfläche

4.7 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.

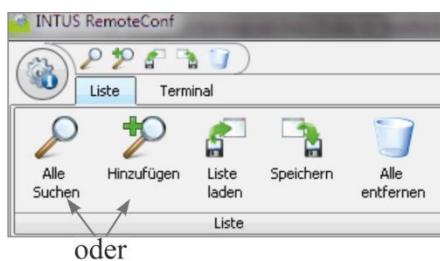
Die folgende Tabelle gibt eine Übersicht:

Schaltfläche	Aktionen an mehreren ausgewählten Terminals möglich
Login	ja
Logout	ja
TCL laden	nein
Statusseite	nein
Inventar	Die Funktion steht derzeit noch gar nicht zur Verfügung. Die Schaltfläche ist immer deaktiviert.
Konfiguration	nein
LBus-Aktionen	ja
Reset	ja
Firmware updaten	ja
Maske laden	ja
Tastatur laden	ja
Audio laden	ja
Logo laden	ja
Lizenz upgraden	Die Funktion steht derzeit noch nicht zur Verfügung. Die Schaltfläche ist immer ausgegraut.
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.

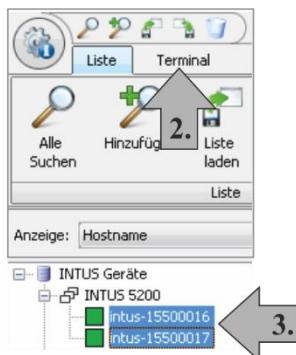
5 Einstieg in die Konfiguration



1. Schritt

Terminalliste aufrufen bzw.
Terminal zur Terminalliste
hinzufügen

oder



2. Schritt

Zum Register „Terminal“ wechseln

3. Schritt

Ein oder mehrere Terminals
in der Terminalliste auswählen



5. Schritt

Aktion auswählen



Abbildung 5-1: Einstieg in die Konfiguration

6 Login – Einloggen ins Terminal

6.1 Berechtigungsstufen

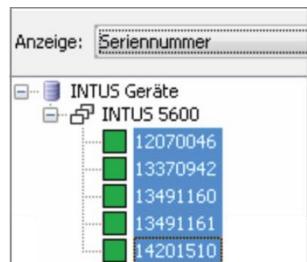
Aus Sicherheitsgründen gibt es drei Berechtigungsstufen, die über Passwörter zugänglich sind.

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“ können die Passwörter der Berechtigungsstufen geändert werden.

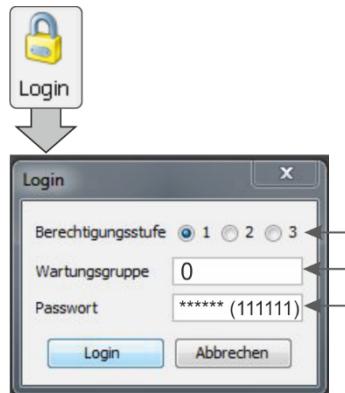
6.2 Vorgehen



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.

7 Konfiguration

7.1 Übersicht

Nach dem Login ist die Konfiguration freigegeben.

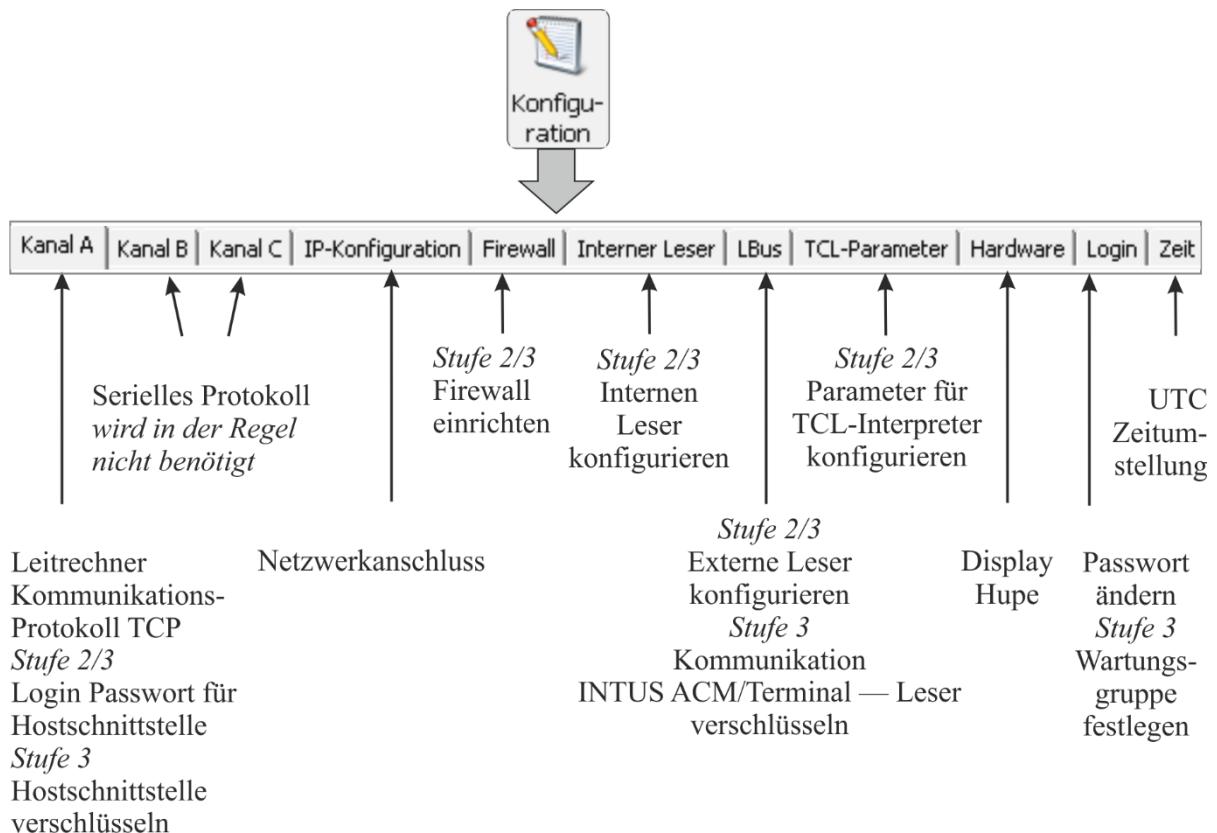


Abbildung 7-1: Übersicht Konfiguration



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.

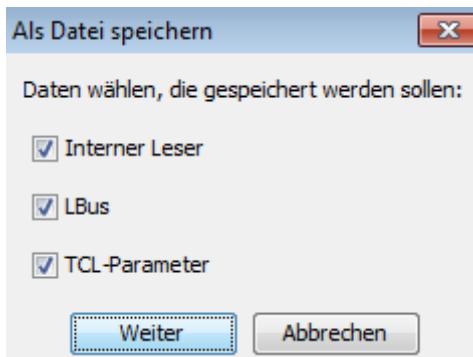


Die Schlüssel zur LBus-Verschlüsselung sind aus Sicherheitsgründen nicht Teil der in der Datei gespeicherten LBus-Konfiguration und müssen jeweils neu vergeben werden.

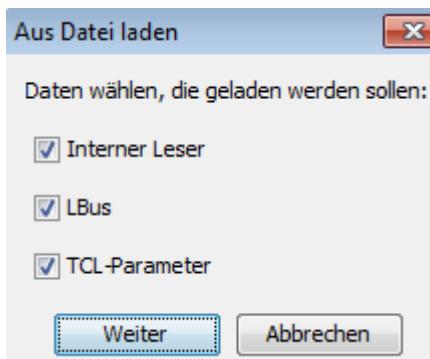
- 1 Klicken Sie auf die Schaltfläche „Als Datei speichern“, um Teile der Konfiguration zu speichern:



- 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:	::	
DNS-Server 2:	::	Gegebenenfalls DNS-Server angeben

IPv4

<input checked="" type="checkbox"/> Aktiviert	<input checked="" type="checkbox"/> 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

<input checked="" type="checkbox"/> Aktiviert	Voreinstellung IPv6 „RADV“ Das Gerät generiert eine IPv6 Adresse. In Verbindung mit IPv4 „DHCP“ sind weitere Einstellungen nicht erforderlich.	
Modus:		RADV ▾
IPv6-Adresse:		2001::
IPv6-Gateway:		<input checked="" type="checkbox"/> Gateway aus RADV
		::

Ethernet

Eth-Link:	Auto Negotiation ▾	Voreinstellung Gegebenenfalls IEEE 802.1X auswählen
IEEE 802.1X:	<input type="checkbox"/> 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 nur 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.

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.

The screenshot shows the 'IP-Optionen' configuration screen. Under the 'WLAN' tab, the following fields are visible:

- Regulierungsbereich: World (Note: 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.

** 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:

- 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



Es sollte vermieden werden, mit INTUS RemoteConf gleichzeitig über WLAN- und Ethernet-Schnittstelle auf das Terminal zuzugreifen.

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:	<input type="button" value="..."/>
Anonyme Identität:	<input type="checkbox"/>
CA-Zertifikat:	(nicht konfiguriert)
Innere Authentifizierung:	<input checked="" type="radio"/> <input type="checkbox"/> <input type="button" value="..."/>
Benutzername:	<input type="text"/>
Passwort:	<input type="password"/> (nicht konfiguriert)
Client-Zertifikat:	(nicht konfiguriert) <input checked="" type="radio"/> <input type="radio"/> beibehalten <input type="radio"/> ändern
Privater Schlüssel:	(nicht konfiguriert) <input checked="" type="radio"/> <input type="radio"/>
Passwort privater Schlüssel:	(nicht konfiguriert) <input type="checkbox"/> Passwort anzeigen <input checked="" type="radio"/> <input type="radio"/> beibehalten <input type="radio"/> löschen <input type="radio"/> ändern

Abbildung 8-3: 8.2 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 18.

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 interface for 'Mobilfunk'. It has a header bar with the title 'Mobilfunk'. Below it are four input fields: 'APN:' with a long empty text box, 'Benutzername:' with a long empty text box, 'Passwort:' with a long empty text box, and 'PIN:' with a long empty text box.

Abbildung 8-4: Mobilfunk

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

9 Kanal A - Host Kommunikation einstellen



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

Kommunikationsprotokoll

Nicht konfiguriert TCP **Voreinstellung** TTY

TCP-Einstellungen

Verbindungsaufbau: **passiv** **Voreinstellung** Port: 3001

IPv4/IPv6-Adresse: ::

Sicherheitseinstellungen

Verschlüsselung: deaktiviert TCL **Voreinstellung**

Schlüssel erzeugen

Login: deaktiviert MONOUT **Voreinstellung**

Passwort für einfachen Zugriff:

Passwort anzeigen

Passwort für administrativen Zugriff:

Passwort anzeigen

Sendedatensatz-Format: Routingbytes:

Satznummernzeichen für Login-Meldungen: *

Abbildung 9-1: 9 Kanal A - Host Kommunikation einstellen

Kommunikationsprotokoll mit dem Leitrechner (Host): TCP



Ein serielles Protokoll (BSC oder TTY) wird in der Regel nicht benötigt, alle Einstellung sind in Kapitel 20 beschrieben.

9.1 TCP-Einstellungen

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 solange, 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 TCP 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 abgebaute 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.

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 Verbindungsauflauf 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:ffff:c0a8:2a7f oder ::ffff:c0a8:2a7f

9.2 HTTPS Client Einstellungen

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: 9. 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.

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

9.3 Sicherheitseinstellungen

Verschlüsselung der Hostschnittstelle

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.

Nähtere 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 unterschiedlichen Dienste Daten, Wartung und Status für Netzwerkteilnehmer freigegeben werden.

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.

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 are tabs for Kanal A, Kanal B, Kanal C, IP-Konfiguration, Firewall (which is selected), Interner Leser, LBus, TCL-Parameter, and Hardware. On the left, there's a green circular icon with a wrench and screwdriver. The main area has two sections: 'IPv4-Netzadresse' and 'IPv6-Adresse'. Under 'IPv4-Netzadresse', five IP addresses are listed: 192.169.167.0, 192.169.10.33, 0.0.0.0, 0.0.0.0, and 0.0.0.0. To the right of these are their corresponding subnet masks: 255.255.255.0, 255.255.255.255, 0.0.0.0, 0.0.0.0, and 0.0.0.0. Below each subnet mask is a row of three checkboxes labeled 'Wartung', 'Daten', and 'Status'. The first row has all three checked. The second row has 'Wartung' and 'Daten' checked. The third row has none checked. The fourth and fifth rows also have none checked. Under 'IPv6-Adresse', there are five entries, each consisting of a colon-separated address followed by a slash and the prefix length 64. To the right of these are three columns: 'Wartung', 'Daten', and 'Status', each with an empty checkbox.

Abbildung 10-1: Firewall konfigurieren

11 LBus konfigurieren

Berechtigungsstufe 2 / 3

- Ein LBus ist die Schnittstelle zum Anschluss von externen Lesern.
- Bei der LBus-Konfiguration werden die verfügbaren LBus-Schnittstellen mit der entsprechenden Platinenbeschriftung angezeigt.
- Zur Verbesserung der Lesbarkeit wird nachfolgend der Begriff „Leser“ verwendet, auch wenn es sich um ein Subterminal handelt.
- **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
- **Multi-Point (MP)**: Werden mehrere Leser als Reihe an eine LBus-Schnittstelle angeschlossen, wird dies bei PCS Multi-Point (MP) genannt.



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

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

11.1 Maximal mögliche Anzahl der Leser

Gerät	Anzahl der Leser		
	LBus 1	LBus 2	Bemerkung
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	4	4	Standard 2 Leser Option 4 Leser Mit ACM40e Wiegand-Modul: + 4 Wiegand Leser Mit 4Flex-Lizenz: + 4 INTUS Flex Leser *

* Mit einem ACM40e in der Grundausstattung, also ohne 4Flex-Lizenz, können keine INTUS Flex Leser betrieben werden.

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

Verkabelung LBus1/LBus2

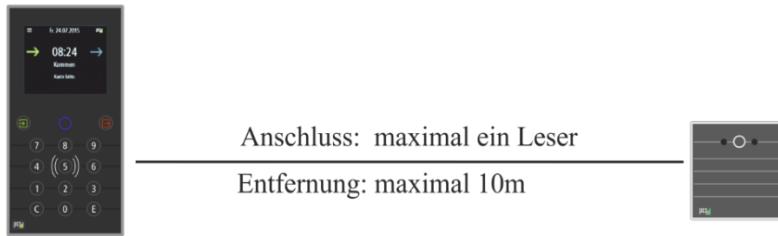


Nur die Einstellung Multi-Point / Multi-Point ist für nicht-ACM-Geräte möglich:

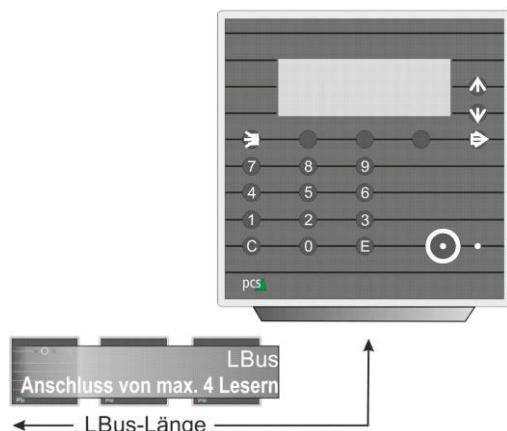
INTUS 5500/5540/5600 jeweils max. 8 Leser pro Schnittstelle (Option)

INTUS 5200 ein Leser pro Schnittstelle (Option)

INTUS 5200



INTUS 5320



INTUS 5500/5540/5600

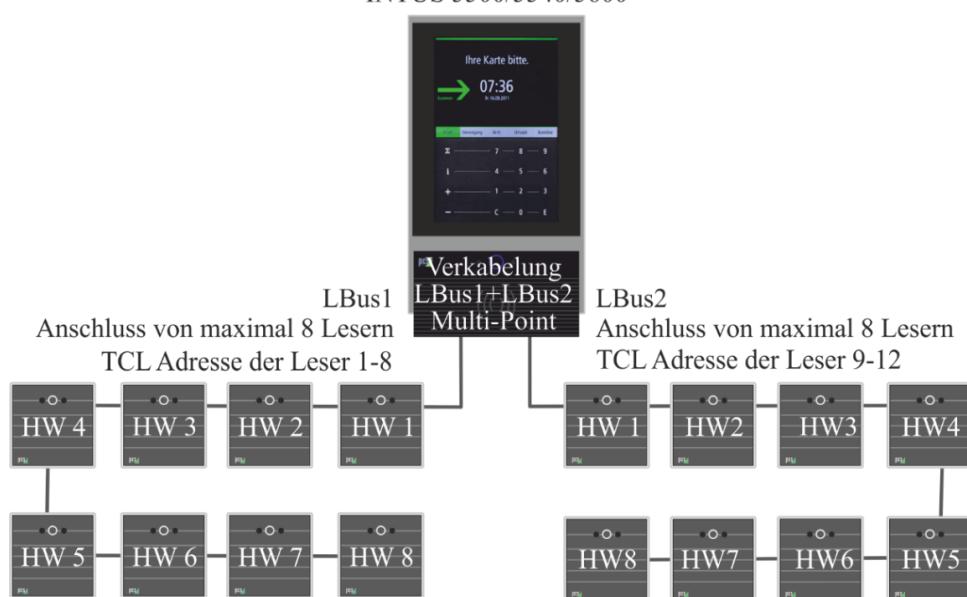


Abbildung 11-1: Verkabelung beim INTUS 5200/5320/5500/5540/5600



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 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input type="radio"/> Point-to-Point	Leser 1 bis Leser 4 -----	Jeweils 1 Leser pro Schnittstelle Max. 4 Leser	1	1 bis 4
Verkabelung LBus 1 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input checked="" type="radio"/> 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 <input checked="" type="radio"/> Multi-Point Verkabelung LBus 2 <input type="radio"/> Point-to-Poi <input type="radio"/> Multi-Point <input type="radio"/> 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

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 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input checked="" type="radio"/> Point-to-Point	Wiegand 1 bis 2 Wiegand 3 bis 4	Max. 4 Leser auf die Leserschnitt- stellen verteilt	---	---
Verkabelung LBus 1 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input checked="" type="radio"/> Point-to-Point	Leser 1 bis 2 Wiegand 1 bis 4	Max. 6 Leser auf die Leserschnitt- stellen verteilt	1 ---	1 bis 2 ---
Verkabelung LBus 1 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input checked="" type="radio"/> Point-to-Point	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 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input type="radio"/> Point-to-Point	Leser 1 bis Leser 8 -----	Jeweils 1 Leser pro Schnittstelle Max. 8 Leser	1	1 bis 8
Verkabelung LBus 1 <input type="radio"/> Multi-Point Verkabelung LBus 2 <input checked="" type="radio"/> Point-to-Point <input type="radio"/> Multi-Point <input type="radio"/> 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 <input checked="" type="radio"/> Multi-Point Verkabelung LBus 2 <input type="radio"/> Point-to-Poi <input type="radio"/> Multi-Point <input type="radio"/> 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 / Multi-Point 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

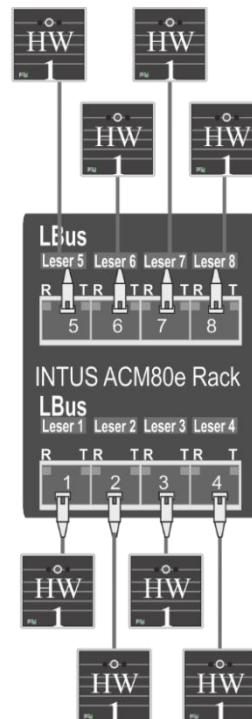


Abbildung 11-2: Point-to-Point-Verkabelung des INTUS ACM80e

11.7 Multi-Point-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.

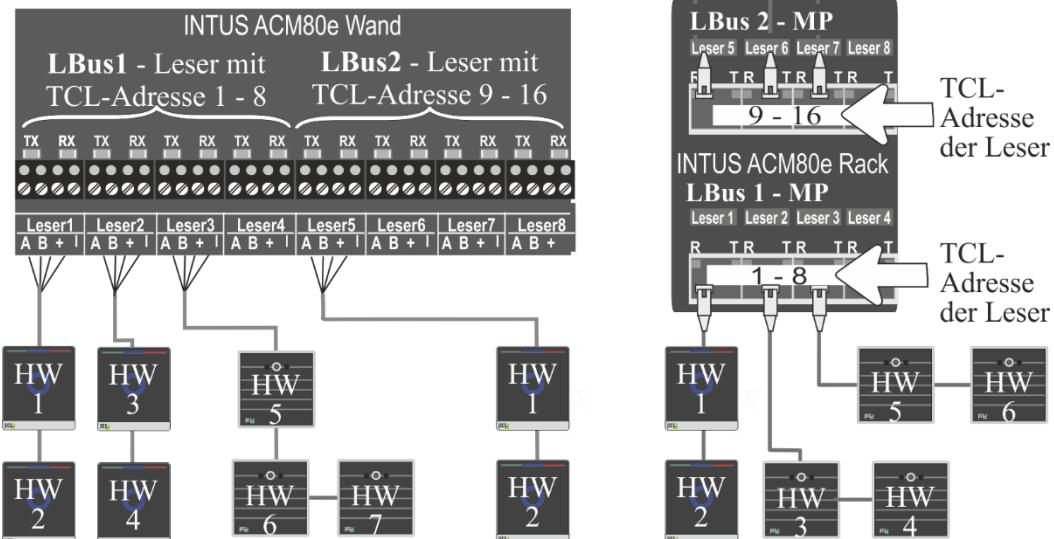


Abbildung 11-3: Multi-Point-Verkabelung des INTUS ACM80e

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



11.8 Leser konfigurieren



1. Schritt:
LBus wählen
Verkabelung festlegen

2. Schritt:
LBus1 oder LBus2 auswählen

3. Schritt:
Lesertyp festlegen

Point-to-Point empfohlene Einstellung

4. Schritt:
Leserschnittstelle auswählen

5. Schritt:
Betriebsart für den angeschlossen Leser festlegen

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 Multi-Point-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



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)

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 ▾	<input type="checkbox"/>
		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 ▾	<input type="checkbox"/>
		nicht konfiguriert	
SN bzw. ID werden ausschließlich gelesen	ID/SN	ID, wenn vorhanden, sonst Seriennummer	
	SN+ID	Seriennummer und ID, wenn vorhanden	
	SN	Seriennummer	
	ID	Identitätsnummer (ID)	

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

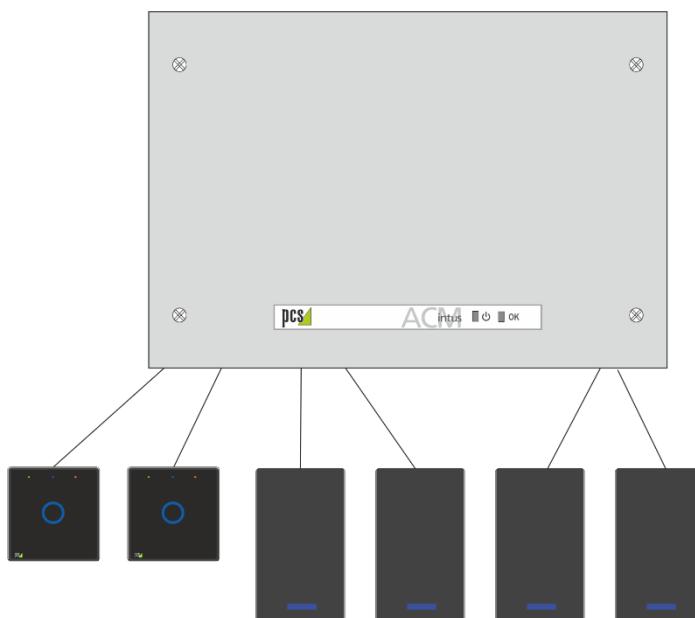


Abbildung 11-6: Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser

The screenshot shows the configuration interface for the ACM40e module. It includes two sections for LBus 1 and LBus 2, and a detailed configuration section for LBus 1.

Verkabelung LBus 1:

- Multi-Point
- Point-to-Point

Verkabelung LBus 2:

- Multi-Point
- Point-to-Point

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

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)

LBus 2/Wiegand 1

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	Standard-Modus	<input type="checkbox"/>
		nicht konfiguriert	
		Standard-Modus	Wiegand

Bus (6 Leser konfiguriert, 6 Leser möglich)

- └─ LBus 1
 - └─ Leser 1
 - └─ 1
 - └─ Leser 2
 - └─ 2
- └─ LBus 2
 - └─ Wiegand 1
 - └─ 9
 - └─ Wiegand 2
 - └─ 10
 - └─ Wiegand 3
 - └─ 11
 - └─ Wiegand 4
 - └─ 12

11.12 Beispiel - ACM40e mit 2 INTUS 700/6xx/350H Lesern und 4 INTUS Flex Endgeräten

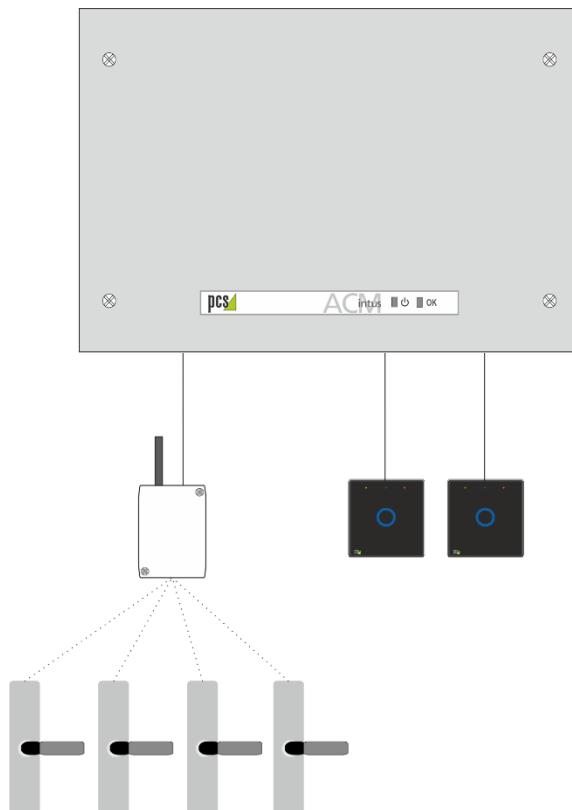
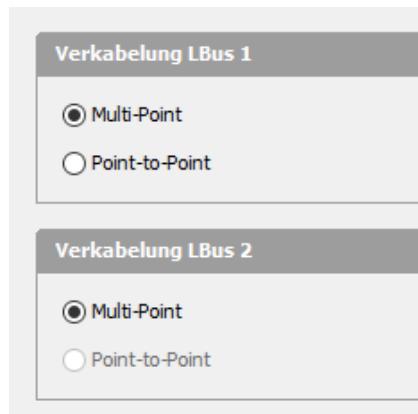


Abbildung 11-7: Beispiel - ACM40e mit 2 INTUS 700/6xx/350H Lesern und 4 INTUS Flex Endgeräten



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

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

LBus 1/Leser 1

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
1	1	Modus B	<input checked="" type="checkbox"/>

LBus 1/Leser 2

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
2	2	Modus B	<input checked="" type="checkbox"/>

LBus 2/Leser 3

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	nicht konfiguriert	<input type="checkbox"/>
10	2	INTUS Flex	nur OSDP INTUS Flex
11	3	Modus A	<input type="checkbox"/>

LBus 2/Leser 3

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	INTUS Flex	<input checked="" type="checkbox"/>
10	2	INTUS Flex	<input checked="" type="checkbox"/>

LBus 2/Leser 4

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
11	3	INTUS Flex	<input checked="" type="checkbox"/>
12	4	INTUS Flex	<input checked="" type="checkbox"/>

LBus: 6 Leser konfiguriert, 2 (+ 4 INTUS Flex) Leser möglich

```
graph TD; Root[LBus: 6 Leser konfiguriert, 2 (+ 4 INTUS Flex) Leser möglich] --> LBus1[LBus 1]; Root --> LBus2[LBus 2]; LBus1 --> Leser1[Leser 1]; LBus1 --> Leser2[Leser 2]; LBus2 --> Leser3[Leser 3]; LBus2 --> Leser4[Leser 4]; Leser1 --> Node1[1]; Leser2 --> Node2[2]; Leser3 --> Node9[9]; Leser3 --> Node10[10]; Leser4 --> Node11[11]; Leser4 --> Node12[12]
```

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

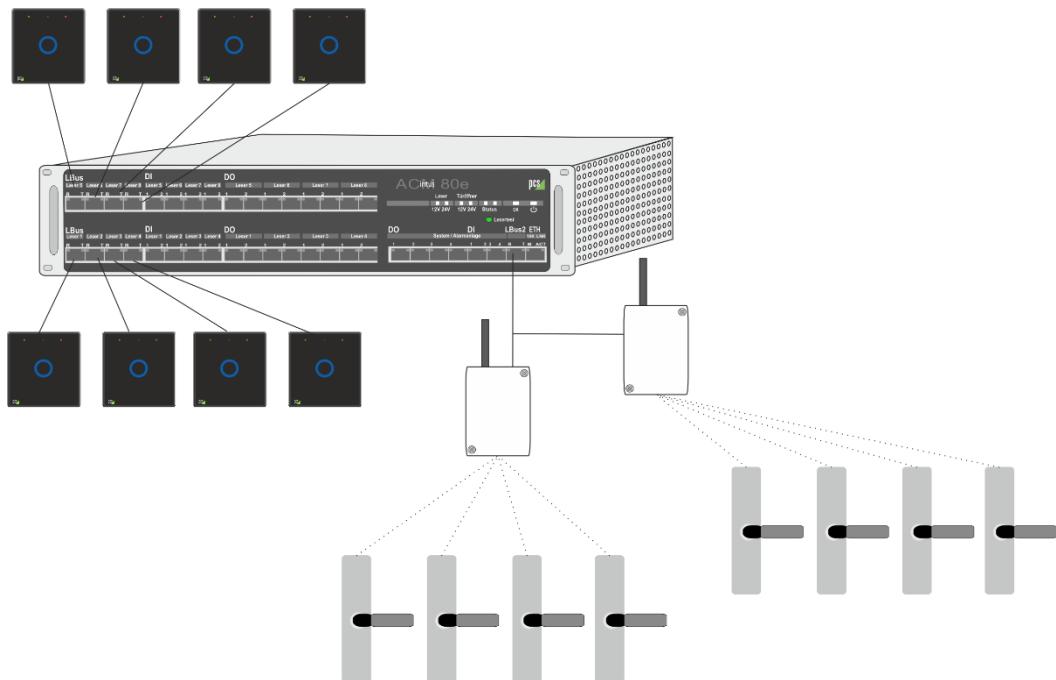
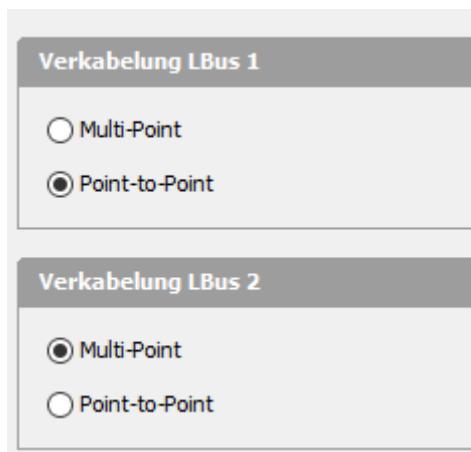


Abbildung 11-8: Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten



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)

LBus 2

Lesertyp:

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

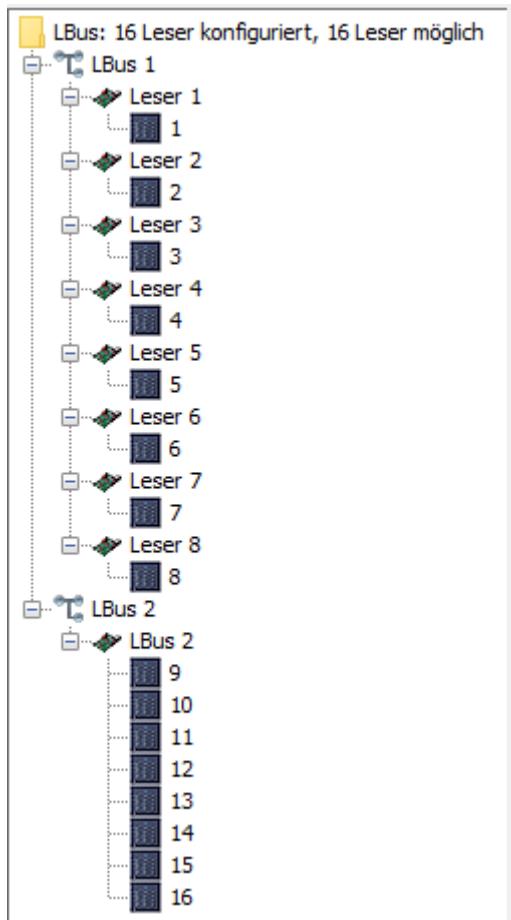
einfache Adressierung

Schlüssel erzeugen (für PCS-proprietäre Verschlüsselung)

LBus 2/LBus 2

TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	nicht konfiguriert	<input type="checkbox"/>
10	2	nicht konfiguriert	
11	3	Standard-Modus INTUS Flex	alle OSDP Leser außer INTUS Flex nur OSDP INTUS Flex

LBus 2/LBus 2			
TCL-Adresse	HW-Adresse	Betriebsart	Verschlüsselung
9	1	INTUS Flex	<input checked="" type="checkbox"/>
10	2	INTUS Flex	<input checked="" type="checkbox"/>
11	3	INTUS Flex	<input checked="" type="checkbox"/>
12	4	INTUS Flex	<input checked="" type="checkbox"/>
13	5	INTUS Flex	<input checked="" type="checkbox"/>
14	6	INTUS Flex	<input checked="" type="checkbox"/>
15	7	INTUS Flex	<input checked="" type="checkbox"/>
16	8	INTUS Flex	<input checked="" type="checkbox"/>



11.14 Beispiel - ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2

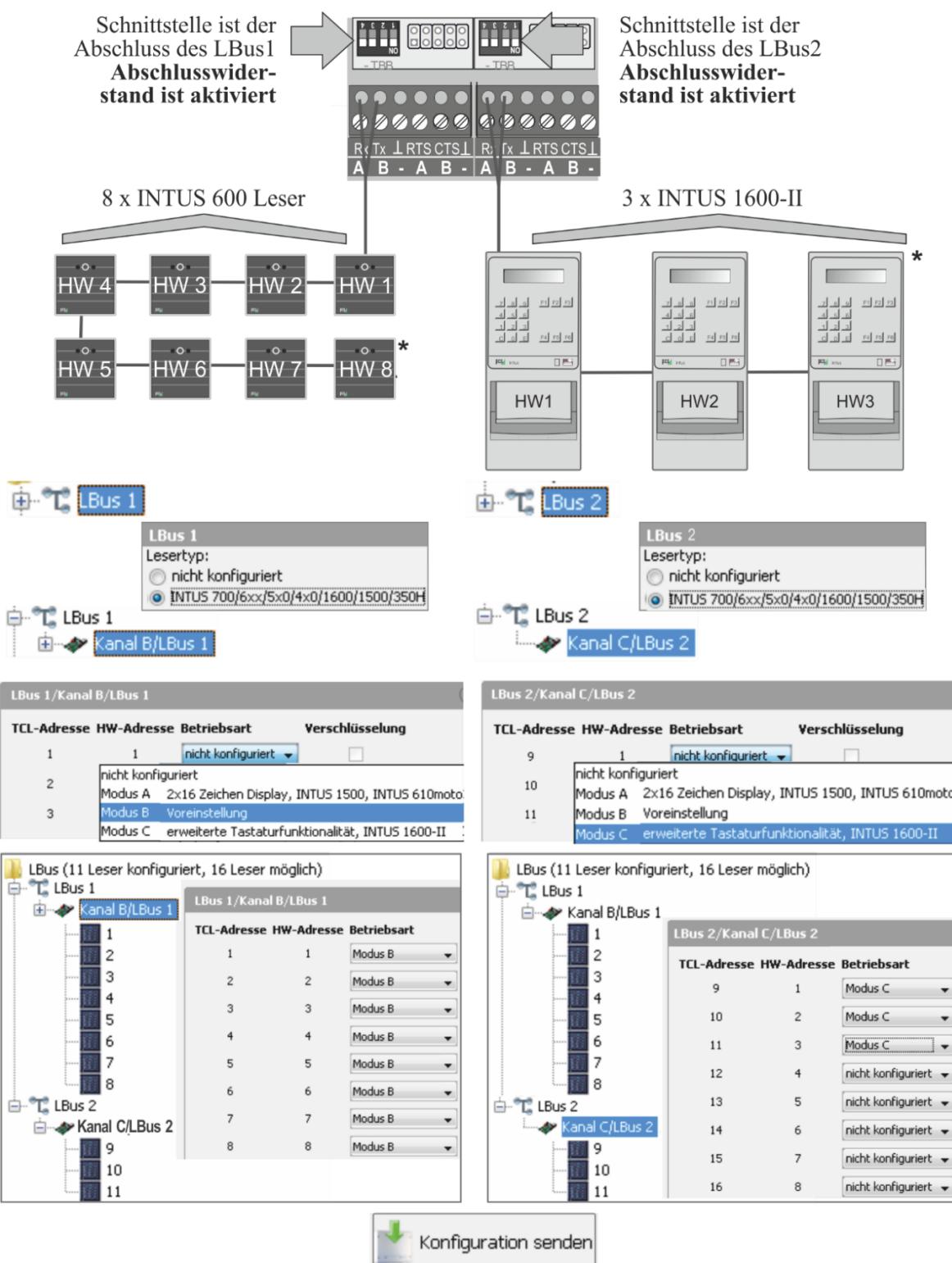


Abbildung 11-9: Beispiel - ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2



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.

11.15 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. Bezuglich OSDP und INTUS Flex beachten Sie die Hinweise in 11.15.8.

11.15.1 Vorraussetzungen

- 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.

11.15.2 Aktivierung der AES-Verschlüsselung



Abbildung 11-10: 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 0).
 - 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.



11.15.3 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 11-11: 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.

11.15.4 Kundenschlüssel konfigurieren



Allgemeine LBus Einstellungen

Kundenschlüssel für AES-Verschlüsselung: **••••••••••••••••••••••••••••••••**

⚠️ Noch kein Kundenschlüssel konfiguriert

Schlüssel anzeigen

beibehalten ändern

AES-Verschlüsselung nur mit Kundenschlüssel

Abbildung 11-12: 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).

11.15.5 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.

11.15.6 Kundenschlüssel ändern



Allgemeine LBus Einstellungen

Kundenschlüssel für AES-Verschlüsselung:

Schlüssel anzeigen

beibehalten ändern

AES-Verschlüsselung nur mit Kundenschlüssel

Abbildung 11-13: 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.

11.15.7 Kundenschlüssel entfernen



Allgemeine LBus Einstellungen

Kundenschlüssel für AES-Verschlüsselung:

Schlüssel anzeigen

beibehalten ändern

AES-Verschlüsselung nur mit Kundenschlüssel

Abbildung 11-14: 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.

11.15.8 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 11.15.2) 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 0) 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.

11.16 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

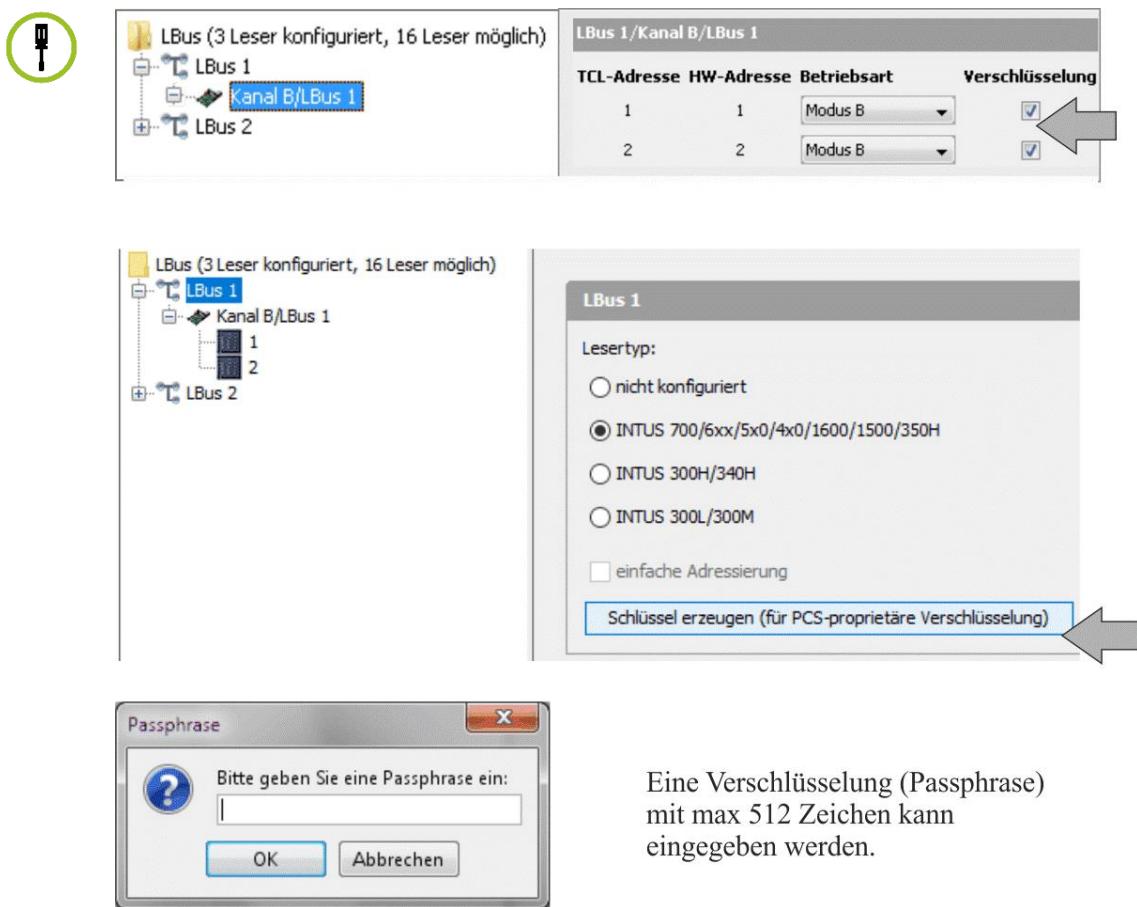


Abbildung 11-15: LBus-Verschlüsselung



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.

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

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.



Kanal A	Kanal B	Kanal C	IP-Konfiguration	Firewall	Interner Leser	LBus	TCL-Parameter	Hardware
Lesertyp: Seriell-Standard Modus: Standard Standard DNCIN <input checked="" type="checkbox"/> zusätzlicher Barcode-Leser								

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



The screenshot shows the 'TCL-Parameter' configuration screen with the 'Voreinstellung' tab selected. It includes three main sections:

- Einstellungen:** Contains fields for Tabellenfeld [Byte] (49152), Notpuffer-Sätze mit Satznummer (unchecked), Label-Anzahl (1024), Notpuffer [Byte] (49152), Default TCL-Programm bei Kaltstart laden (checked), Quittungszeit [s] (26), Größe BMI-Feld [byte] (radio buttons for 88 and 115), and Zeichensatz (ISO646-DE).
- Erweiterte Benutzerschnittstelle:** Contains fields for TCL Binding: Tabellenfeld, Startoffset (0), and Länge des zu synchronisierenden Bereichs (0).
- INTUS Sound:** Contains a field for Lautstärke [%] (70).

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)

Hupenansteuerung 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



The screenshot shows a 'Login' configuration page with several input fields and warning messages. At the top, there are tabs for Kanal A, Kanal B, Kanal C, IP-Konfiguration, Firewall, Interner Leser, LBus, TCL-Parameter, Hardware, and Login. The 'Login' tab is active. Below the tabs, there's a 'Login' section with a warning icon. It contains fields for 'Wartungsgruppe' (Maintenance Group) and three sets of password fields (Berechtigungsstufe 1-3) with their respective 'Wiederholung' (Repeat) fields. Each field has a yellow warning message below it stating: 'Sicherheitseinstellung befindet sich auf dokumentiertem Standardwert!' (Security setting is at documented standard value!).

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-Server 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 (Stand 2020) 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 (2021) 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“.

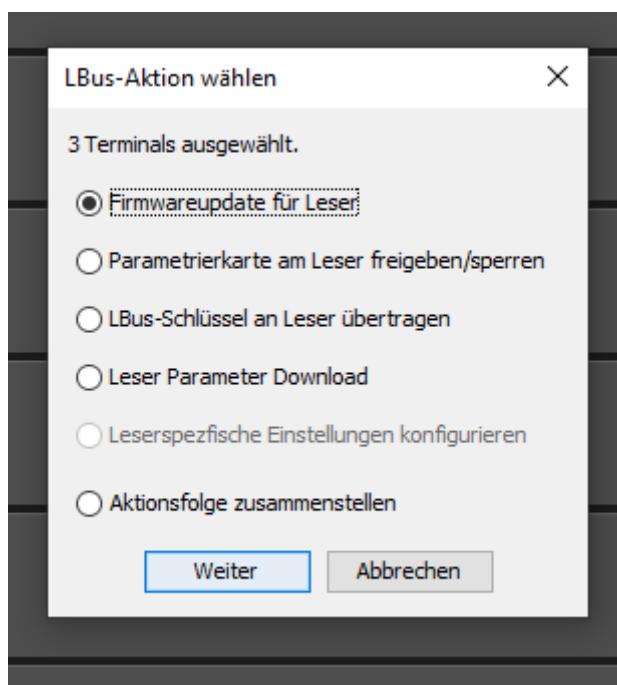


Abbildung 17-1: LBus-Aktionen wählen

- 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 0 und 0.

17.3 Aktion "Parametrierkarte am Leser freigeben/sperren"

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 Freigen 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 11.15 und 11.16.



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"

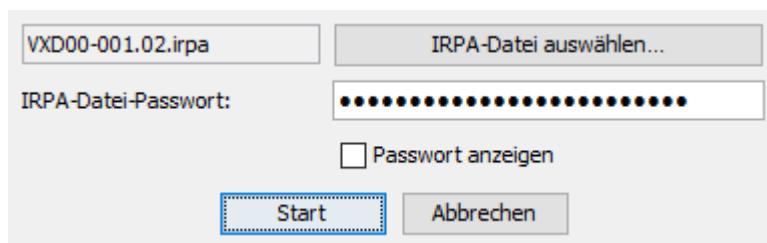
Unter Umständen kann es notwendig sein, die an ein Terminal angeschlossenen Leser mit INTUS RemoteConf zu parametrieren.

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-Datei-Passwort für Datei" ein.



- 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.

i 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.

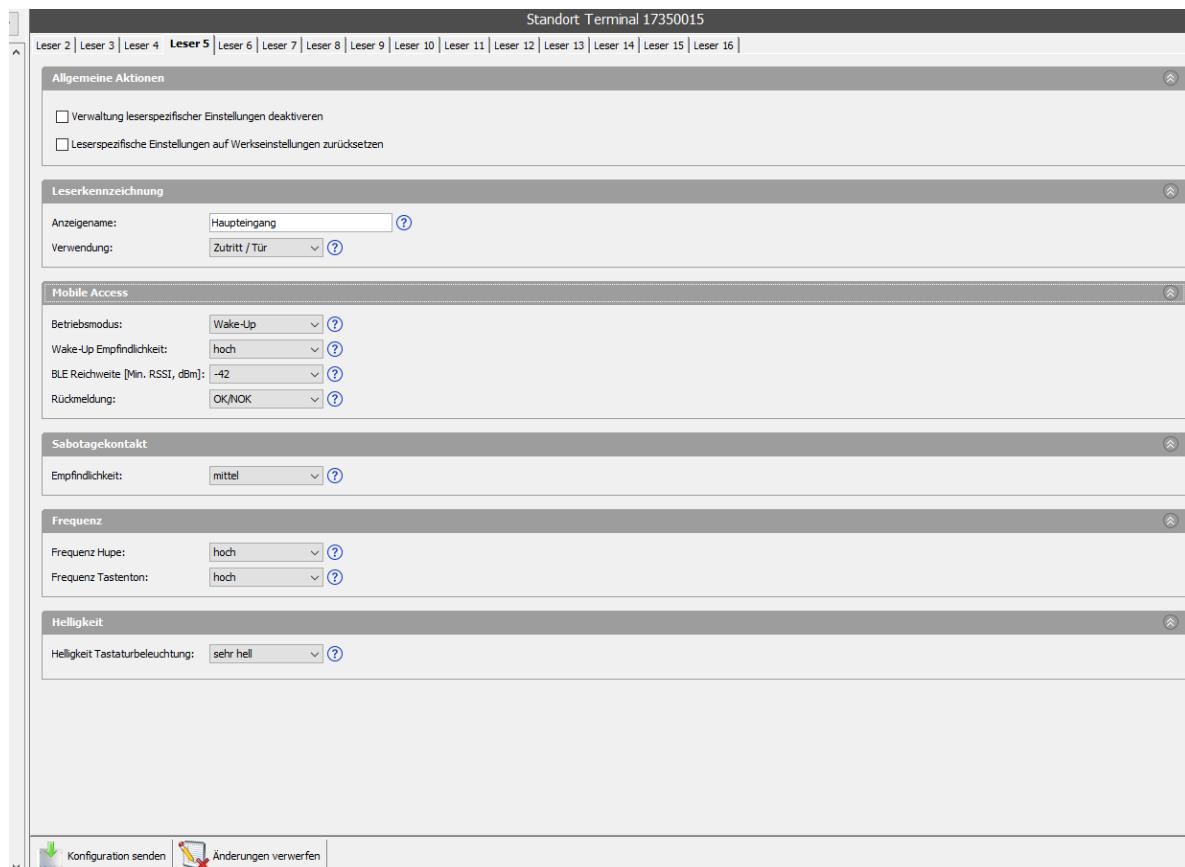


Abbildung 17-2: Leserspezifische Einstellungen konfigurieren

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, 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.

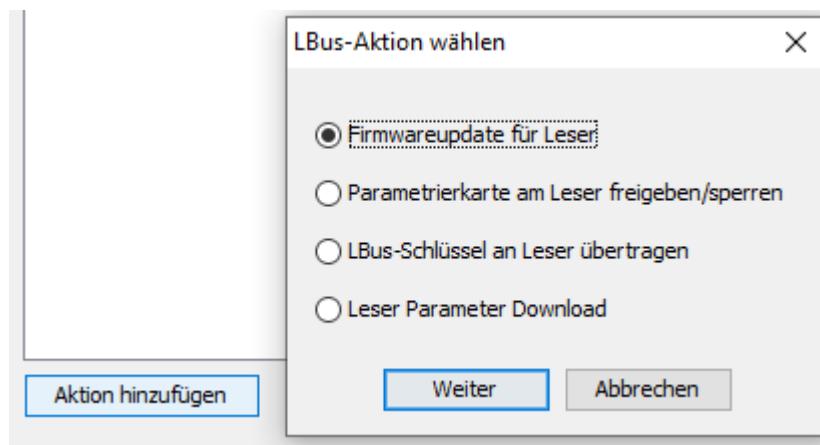


Abbildung 17-3: LBus-Aktionsfolge zusammenstellen

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 Reset

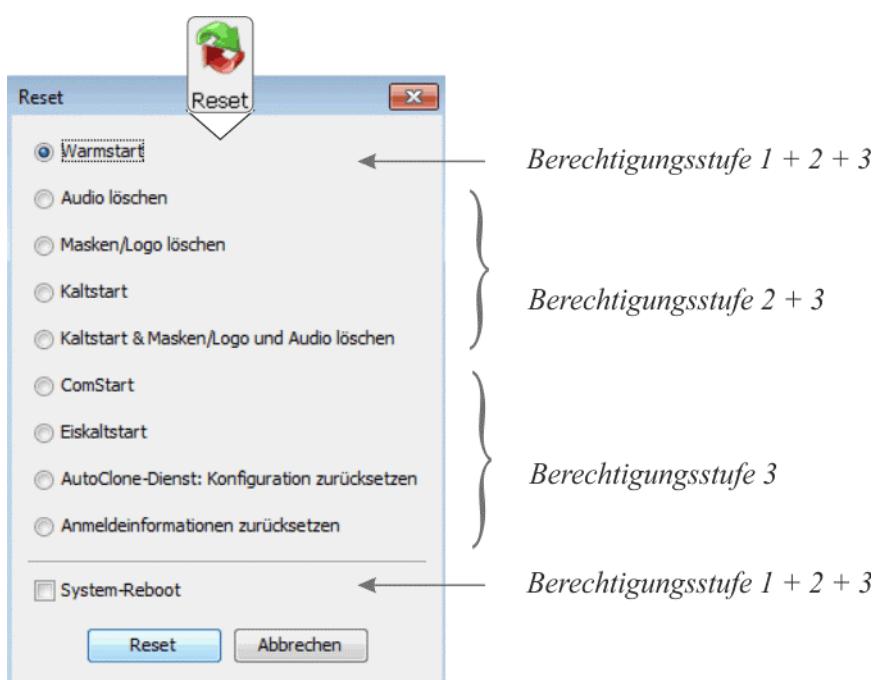


Abbildung 18-1: Reset

	Warmstart	Kaltstart	ComStart	Eiskaltstart
TCL Applikation Variablen Notpuffer	Bleiben gültig	Werden gelöscht	Werden gelöscht	
TCL Parameter	Bleiben gültig	Bleiben gültig		Werden gelöscht
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.

19 Logo laden



Berechtigungsstufe 2 / 3

Gültig für den INTUS 5200 & INTUS 5205.

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



Abbildung 19-1: 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: **PNG - Portierbare Netzwerk-Grafik**

20 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.

20.1 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).

20.2 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 folgenden 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.

Loeschzeichen: 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.

20.3 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/ Gerätekennung: 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 verstrecken, 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 verstrecken 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

21 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, DHCPv60F, 1Ping (ICMP, ICMPv61) 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	Zielport	Anmerkung
Host → Terminal	TCP	*2)	<wie konfiguriert> ^{*4)}	Verbindungs- aufbau „passiv“ oder „passiv/RAS“
Terminal → Host	TCP	*3)	<wie konfiguriert> ^{*4)}	Verbindungs- aufbau „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 Betriebssystem gewählt; unter Umständen eingegrenzt, je nach eingesetzter Software

³ Wird vom Terminal frei gewählt

⁴ Konfiguration > Kanal A > TCP-Einstellungen > Port

22 Fehlerdiagnose

22.1 Leser-Aktionstest

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

22.1.1 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“.

22.1.2 INTUS 5540

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

22.1.3 INTUS ACM80e

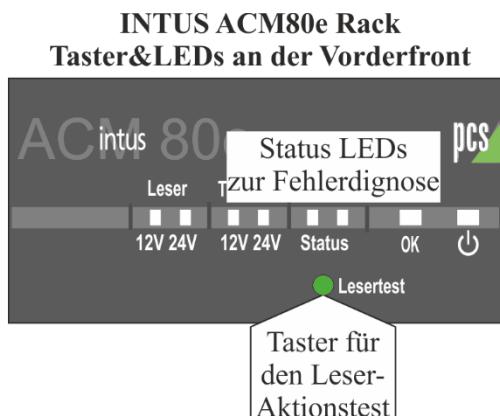
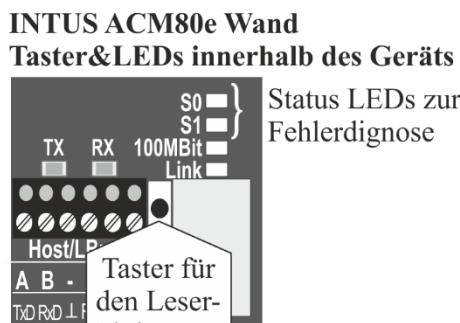


Abbildung 22-1:Leser-Aktionstest ACM80e

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.

22.1.4 INTUS ACM40e

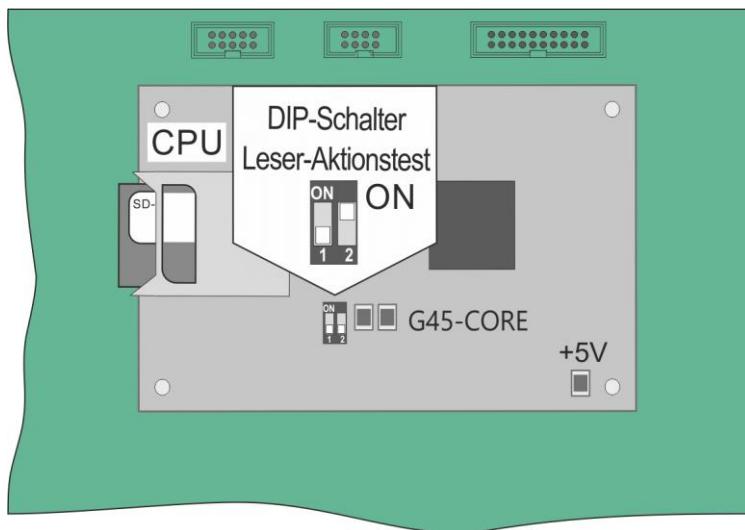


Abbildung 22-2: Leser-Aktionstest ACM40e



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.

22.2 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 anzeigt:

- 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	Speichermando 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 18.

22.3 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.

22.4 Erfolgslose 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.

23 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	ISO6464-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	

24 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.

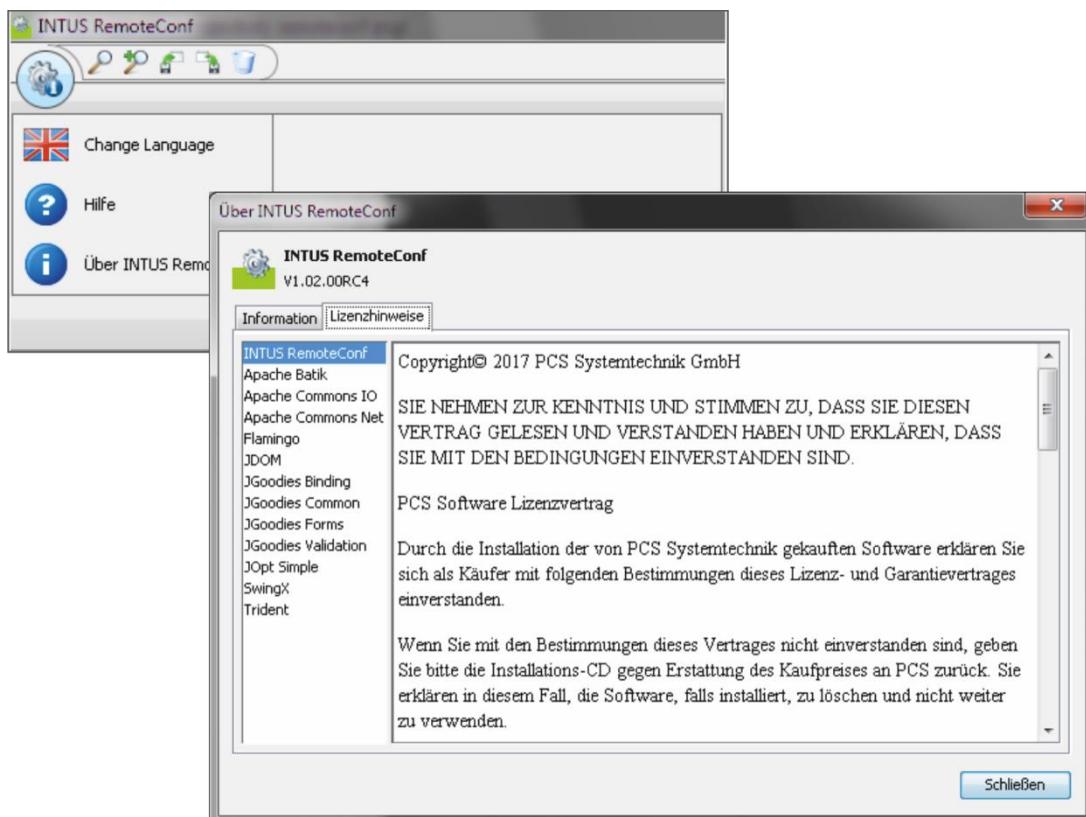


Abbildung 24-1: Lizenzbestimmungen

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.

25 Abbildungsverzeichnis

Abbildung 4-1: Anbindung PC/Terminal	17
Abbildung 4-2: Schaltflächen in RemoteConf.....	19
Abbildung 4-3: IP-Konfiguration	20
Abbildung 4-4: Terminaliste ordnen.....	21
Abbildung 4-5: PC-Firewall.....	21
Abbildung 4-6: Info-Schaltfläche	21
Abbildung 5-1: Einstieg in die Konfiguration.....	23
Abbildung 6-1: Einloggen	24
Abbildung 7-1: Übersicht Konfiguration.....	25
Abbildung 7-2: Konfiguration beenden	26
Abbildung 8-1: Netzanschluss konfigurieren	27
Abbildung 8-2: WLAN.....	29
Abbildung 8-3: 8.2 IEEE 802.1X/WPA2-Enterprise	30
Abbildung 8-4: Mobilfunk.....	31
Abbildung 9-1: 9 Kanal A - Host Kommunikation einstellen	32
Abbildung 9-2: 9. HTTPS Client Einstellungen.....	34
Abbildung 10-1: Firewall konfigurieren	36
Abbildung 11-1: Verkabelung beim INTUS 5200/5320/5500/5540/5600	38
Abbildung 11-2: Point-to-Point-Verkabelung des INTUS ACM80e	41
Abbildung 11-3: Multi-Point-Verkabelung des INTUS ACM80e	41
Abbildung 11-4: Leser konfigurieren	42
Abbildung 11-5: Lesertyp / einfache Adressierung.....	43
Abbildung 11-6: Beispiel ACM40e Wiegand Modul: 2 LBus Leser, 4 Wiegand Leser	45
Abbildung 11-7: Beispiel - ACM40e mit 2 INTUS 700/6xx/350H Lesern und 4 INTUS Flex Endgeräten.....	47
Abbildung 11-8: Beispiel ACM80e mit 8 INTUS 700/6xx/350H Lesern und 8 INTUS Flex Endgeräten.....	50
Abbildung 11-9: Beispiel - ein INTUS 5500/ 5540/ 5600 mit LBus1 & LBus2.....	53
Abbildung 11-10: Aktivierung der AES-Verschlüsselung.....	54
Abbildung 11-11: Konfiguration der AES-Schlüssel	55
Abbildung 11-12: Kundenschlüssel konfigurieren	55
Abbildung 11-13: Kundenschlüssel ändern.....	56
Abbildung 11-14: Kundenschlüssel entfernen	57
Abbildung 11-15: LBus-Verschlüsselung	58
Abbildung 12-1: Internen Leser einstellen.....	59
Abbildung 13-1: TCL Parameter einstellen	60
Abbildung 14-1: Hardware-Einstellungen.....	62
Abbildung 15-1: Login – Wartungsgruppe und Passwörter ändern	63
Abbildung 16-1: Zeiteinstellungen	64
Abbildung 17-1: LBus-Aktionen wählen	66
Abbildung 17-2: Leserspezifische Einstellungen konfigurieren	69
Abbildung 17-3: LBus-Aktionsfolge zusammenstellen	70
Abbildung 18-1: Reset.....	72
Abbildung 19-1: Logo laden	74

Abbildung 22-1:Leser-Aktionstest ACM80e	79
Abbildung 22-2: Leser-Aktionstest ACM40e	80
Abbildung 24-1: Lizenzbestimmungen	87

26 Index

- Berechtigungsstufen 16
- Blau markiert 20
- BSC-Protokoll 76
- Datenport 78
- Datenübertragung: Datensatz 60
- Display: Kontrast 62
- DNS-Server 28
- EEPROM 81
- Eiskaltstart 72
- Fehler: Fehlerbeschreibung 83
- Fehlerdiagnose 82
- Firewall 36
- Firmware 81
- Freie Software 87
- Handbücher 9
- Host Kommunikation 32
- Hostname 28
- HTTPS Client 34
- Hupe 62
- INTUS 300ro 37
- INTUS Graph 61
- IP Setup 20
- IP-Konfiguration: Netzmaske 28
- IPv4 28
- IPv6 28
- Java 17
- Kaltstart 72
- Kanal A: Port-Nummer 33;
Verbindungsaufbau 32
- Konfiguration 25
- LBus 37; Beispiel 53
- Leser 79; Fehllesung 80
- Lizenzbestimmungen 87
- Logo 74
- Modus 44
- Netzwerkanschluss 27
- Parameter 84
- Partner-Kit: INTUS.TXT 81
- Partyline 77
- Passwort 63
- PC Firewall 21
- PCS-Hotline 16
- Schaltflächen 19
- Sicherheits-Einstellungen 86
- Sommerzeit 65
- Sound 61
- SRAM 82
- Symbole 8
- TCL: Default-Programm 61;
Ladeanforderung 61; Notpuffer
60
- TCL Programmierhandbuch 9
- TCL-Parameter 60
- Terminalliste 20
- TTY-Protokoll 75
- UTC 65
- Wartungsgruppe 63
- Winterzeit 65
- Zeichensatz 61

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

pcs