

Manual INTUS

INTUS COM Terminal Management System

Anwenderhandbuch V3.6.0

D3000-430.25



Warn- und Hinweiszeichen



Dieses Zeichen warnt Sie vor Gefahren für Gesundheit und Leben (z.B. vor einem möglichen Kontakt mit der Netzspannung). Den Text neben diesem Zeichen sollten Sie darum in jedem Fall lesen und beachten!



Dieses Zeichen warnt Sie vor Gefahren, die zu Schäden des Geräts oder des Systems führen können (Fehlfunktion, Datenverlust, Materialbeschädigung oder ähnliches können).



Auf diese Weise hervorgehobener Text fordert Sie zum Handeln auf.



Dieses Zeichen weist Sie auf Informationen hin, die Ihnen dem Umgang mit dem Produkt oder dem Handbuch erleichtern können.

INTUS COM Terminal Management System

Anwenderhandbuch V3.6.0

Stand 04 / 2022

Bestell-Nr. D3000-430.25

PCS Systemtechnik GmbH

Pfälzer-Wald-Str. 36, D-81539 München, Tel. 089/68004-0

Homepage: www.pcs.com

Technische Kundenunterstützung

Telefon: 089/68004-666

Fax: 089/68004-410

Email: intuscom@pcs.com

Die Vervielfältigung 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.

INTUS ist ein eingetragenes Warenzeichen der PCS Systemtechnik GmbH.

Copyright 2022 by PCS Systemtechnik GmbH

Inhaltsverzeichnis

Warn- und Hinweiszeichen	2
1 Einleitung	11
1.1 Notwendige Vorkenntnisse.....	11
1.2 Weitere Handbücher	11
1.3 Systemarchitektur	12
1.3.1 INTUS COM Client und Admin-Server.....	12
1.3.2 Terminal-Handler.....	13
1.3.3 Der AutoClone Dienst.....	13
1.3.4 Konzentrator.....	13
1.3.5 Die Kommunikations-Server.....	13
1.3.6 Das Video-Interface	13
1.3.7 Der PS-Distributor	14
2 Windows Installation	15
2.1 INTUS Software installieren	15
2.1.1 Testinstallation.....	15
2.1.2 Benutzerdefinierte Installation.....	16
2.1.3 Datenbank-Schnittstelle	18
2.1.3.1 Demo-Datenbank installieren	18
2.1.3.2 Benutzerdefinierte Installation der Datenbank-Schnittstelle	18
2.1.4 Lizenzkostenfreie Java 11 Laufzeitumgebung (OpenJDK).....	23
2.1.5 INTUS COM HTTPS-Server installieren.....	23
2.1.5.1 Java Dienst	23
2.1.5.2 Server Zertifikat.....	23
2.2 INTUS COM aktualisieren.....	24
2.2.1 Update der INTUS Software Programme.....	25
2.2.2 Update der INTUS COM Datenbank-Schnittstelle.....	25
2.2.3 Update der TPI Komponenten	26
2.3 INTUS COM Serverkomponenten einrichten und starten.....	27
2.3.1 HTTPS-Server einrichten	27
2.3.1.1 HTTPS-Terminal konfigurieren.....	27
2.3.1.2 Generieren des Keystores und der Zertifikate	28
2.3.1.3 Änderung der Passwörter für den Keystore und das Zertifikat.....	35
2.3.2 Batch-Dateien	35
2.3.3 Kommandozeilenoptionen.....	35
2.3.4 Installieren als Windows Systemdienst (Service).....	35
2.3.5 Secure-Dateien.....	37
2.3.6 Portnummer des Admin-Servers ändern	37
2.4 INTUS COM Client starten.....	38
2.4.1 Speichereinstellung ändern.....	39
2.4.2 Verbindungsfehler.....	39
2.4.3 Verbindungstimeout.....	39
2.4.4 Lizenz eingeben	39
2.5 INTUS COM Installation sichern	40
3 INTUS COM Client Benutzeroberfläche	41
3.1 Hauptfenster des INTUS COM Clients.....	42
3.2 Fenstertypen	43

3.2.1	Verwaltungseinheiten-Fenster.....	43
3.2.2	Benutzer-Rollen-Berechtigungen-Fenster.....	44
3.2.3	Komponenten-Fenster.....	47
3.2.4	Videokomponenten-Fenster.....	50
3.2.5	PS-Distribution-Fenster.....	51
3.2.6	AutoClone-Fenster.....	52
3.2.7	Offlineanlagen-Fenster.....	52
3.2.8	K&S-Fenster.....	53
3.2.9	Suche/Fehler-Fenster.....	55
3.2.10	Meldungs-Fenster	57
3.2.11	Lageplan-Fenster	59
3.3	Bedienung.....	61
3.3.1	Menüleiste	61
3.3.1.1	Datei	61
3.3.1.2	Rollen	61
3.3.1.3	Neu.....	61
3.3.1.4	Bearbeiten.....	61
3.3.1.5	Ansicht	61
3.3.1.6	Steuerung.....	62
3.3.1.7	Werkzeuge.....	62
3.3.1.8	Fenster.....	63
3.3.1.9	Hilfe	63
3.3.2	Werkzeugleiste (Toolbar).....	63
3.3.3	Anzeige- und Änderungsmodus.....	65
3.3.3.1	Anzeigemodus	65
3.3.3.2	Änderungsmodus	65
3.3.4	Hinzufügen eines neuen Objekts	66
3.3.5	Ändern der Konfiguration eines Objekts.....	66
3.3.6	Löschen eines oder mehrerer Objekte	67
3.3.7	Kopieren und Einfügen	67
3.4	Weitere Funktionen.....	68
3.4.1	Terminal-Reset	68
3.4.2	Manueller Download aus Datei/Datenbank/Blocklist	69
3.4.3	Zeitversetzten Download planen.....	69
3.4.4	Neuladen der Fingerprint-Templates	70
3.4.5	Neuladen der PS-Templates	70
3.4.6	Terminal-Statusseite anfordern.....	70
3.4.7	Batteriezustand abfragen	70
3.4.8	AutoClone Passwort zurücksetzen.....	71
3.4.9	AutoClone Download starten	71
3.4.10	Email Benachrichtigung bei Alarmen	71
3.4.11	Netzwerk Terminalsuche.....	72
3.4.12	Uhrzeit stellen.....	74
3.4.13	Dialog mit Terminal.....	75
3.4.14	Einzeltüröffnung	75
3.4.15	Dauertüröffnung	75
3.4.16	Dauertüröffnung beenden.....	76
3.4.17	Export der Offline Terminal Konfiguration	76
3.4.18	Import der Offline Terminal Konfigurationsergebnisse	77
4	INTUS COM in Betrieb nehmen	79
4.1	Schrittweise Inbetriebnahme eines Terminalsystems.....	79
4.2	Verschlüsselung	80

4.3	Test der Terminalverbindung	80
4.3.1	TCP/IP.....	80
4.3.2	HTTPS.....	80
4.4	Berechtigungsverwaltung in INTUS COM	81
4.4.1	Verwaltungseinheiten.....	81
4.4.2	Benutzer	81
4.4.3	Rollen.....	81
4.4.4	Berechtigung.....	81
4.4.5	Benutzer-Rolle-Zuordnung.....	82
4.4.6	Berechtigung-Rolle-Zuordnung.....	82
4.4.7	Spezieller Adminstrator-Benutzer, -Rolle und –Berechtigung.....	82
4.5	Gemeinsame Parameter.....	83
4.5.1	Verwaltungseinheit	83
4.5.2	Seriennummer.....	83
4.5.3	Gemeinsame Parameter der INTUS COM Server	84
4.5.3.1	Rechnername oder IP-Adresse.....	84
4.5.3.2	Serviceport und Datenport.....	84
4.5.3.3	Server-ID.....	84
4.5.3.4	Messagelevel	84
4.6	Terminal Management System konfigurieren	85
4.6.1	Registerblatt Einstellungen.....	85
4.6.2	Registerblatt Lizenz	87
4.7	Verwaltungseinheit konfigurieren.....	88
4.8	Terminal-Handler konfigurieren.....	90
4.8.1	Registerblatt Grundeinstellungen.....	90
4.8.2	Registerblatt Upload	93
4.8.3	Registerblatt Download	95
4.8.4	Registerblatt Biometrie	98
4.8.5	Registerblatt SeeTec LPR.....	100
4.9	Konzentrator konfigurieren	102
4.9.1	Registerblatt Grundeinstellungen.....	102
4.9.2	Registerblatt Verschlüsselung	103
4.10	TCP-Server konfigurieren	104
4.10.1	Registerblatt Grundeinstellungen.....	105
4.10.2	Registerblatt Verschlüsselung	106
4.10.3	Terminalkommunikation über RAS-Verbindungen.....	107
4.10.4	TCP-Server ohne INTUS COM Client konfigurieren.....	107
4.11	HTTPS-Server konfigurieren.....	109
4.11.1	Registerblatt Grundeinstellungen.....	110
4.11.2	Konfiguration des Zertifikatsupdates	110
4.11.2.1	Allgemeines	111
4.11.2.2	Vorbereitung der Keystores.....	111
4.11.2.3	Manuelles Einstellen des neuen Keystores.....	111
4.11.2.4	Einstellen des neuen Keystores.....	111
4.11.2.5	Ablauf des Zertifikatsupdates	112
4.11.2.6	Besonderheiten beim Zertifikatsupdate über INTUS RemoteConf	114
4.12	INTUS 3000/3450 Server konfigurieren	114
4.12.1	Registerblatt Grundeinstellungen.....	116
4.13	INTUS Terminal/ACM konfigurieren	117
4.13.1	Netzwerkterminals aus csv-Datei importieren.....	117

4.13.2	Registerblatt Grundeinstellungen.....	119
4.13.3	Registerblatt Dateien.....	125
4.13.4	Registerblatt TPI.....	127
4.13.5	Registerblatt TCL.....	129
4.13.6	Registerblatt AutoClone	131
4.13.7	Registerblatt FP	132
4.14	Subterminals konfigurieren	134
4.14.1	Registerblatt Grundeinstellungen.....	135
4.14.2	Registerblatt TPI.....	137
4.15	Türüberwachung konfigurieren	138
4.16	Benutzer anlegen.....	140
4.17	Rolle konfigurieren	141
4.18	Berechtigung konfigurieren.....	142
4.18.1	Registerblatt Grundeinstellungen.....	144
4.18.2	Registerblatt Berechtigungen.....	145
4.19	Benutzer-Rolle-Zuordnung konfigurieren.....	148
4.20	Berechtigung-Rolle-Zuordnung konfigurieren	149
4.21	Video-Interface anlegen und konfigurieren.....	150
4.21.1	Registerblatt Grundeinstellungen.....	151
4.21.2	Registerblatt Videobildanforderung	152
4.22	Videoquelle konfigurieren.....	153
4.22.1	Registerblatt Grundeinstellungen.....	154
4.23	Kamera konfigurieren	155
4.24	Kamera-Leser-Zuordnung konfigurieren	158
4.25	PS-Distributor konfigurieren	159
4.25.1	Registerblatt Grundeinstellungen.....	159
4.25.2	Registerblatt Verschlüsselung	161
4.26	AutoClone Dienst konfigurieren.....	162
4.26.1	Registerblatt Grundeinstellungen.....	162
4.27	EMail-Einstellung konfigurieren	164
4.28	Offlineanlage konfigurieren	165
4.29	Offlineterminal konfigurieren.....	167
4.30	Blocklist konfigurieren.....	169
5	Fehlersuche und Fehlerbehebung.....	173
5.1	Verbindungsfehler.....	173
5.1.1	Allgemeine TCP/IP Verbindungsfehler	175
5.1.2	Verbindungsfehler in INTUS COM	176
5.2	Betriebsfehler.....	177
5.2.1	Betriebsfehler einer Serverkomponente	177
5.2.2	Betriebsfehler eines Terminals	178
5.2.3	Buchungssatzverlust.....	180
5.2.4	Email-Benachrichtigung.....	180
5.3	Log-Dateien	180
5.4	Sonstige Probleme	181

5.4.1	Passwort vergessen	181
6	INTUS COM Applikationsschnittstellen.....	183
6.1	Dateischnittstelle.....	184
6.1.1	Die statische Dateischnittstelle	185
6.1.1.1	Download	185
6.1.1.2	Dateiübergabe zwischen Applikation und INTUS COM	186
6.1.1.3	Satzformat	187
6.1.1.4	Ladeanforderungen	187
6.1.2	Die dynamische Dateischnittstelle	188
6.1.2.1	Upload	188
6.1.2.2	Download	188
6.1.2.3	Dateiübergabe zwischen Terminal-Handler und Applikation	189
6.1.2.4	Satzformat	190
6.2	Socket-Schnittstelle.....	191
6.2.1	Datenport der Socket-Schnittstelle.....	191
6.2.2	Satzformat	191
6.3	Datensätze in Datei- und Socket-Schnittstelle.....	192
6.3.1	Satzformate (Syntax).....	192
6.3.2	Satzarten (Semantik).....	192
6.3.2.1	Download	193
6.3.2.2	Upload.....	194
6.3.2.3	Syntax der INTUS COM Meldungsformate für Status-, Fehler- und Alarmmeldungen	195
6.3.2.4	Verwendung der Meldungsformate.....	198
6.3.2.5	Filtern von Datensätzen beim Upload.....	199
6.4	Datenbank-Schnittstelle	200
6.4.1	Tabellenübersicht.....	201
6.4.1.1	Datentypen.....	203
6.4.2	Download-Tabellen.....	203
6.4.2.1	Tabellendownload - Grundversorgung.....	204
6.4.2.2	INTUSCOM_TIMESTAMP - Grundversorgung durch die Applikation.....	204
6.4.2.3	INTUSCOM_MASTER_RECORDS - Stammdaten	206
6.4.2.4	INTUSCOM_OSO_CARD_DATA_IDS - OSO-Kartendaten-IDs	209
6.4.2.5	INTUSCOM_PROFILES - Profile	210
6.4.2.6	INTUSCOM_FUNCTION_PROFILES – Zeitliche Funktionsumschaltung	214
6.4.2.7	INTUSCOM_SPECIAL_DAYS Sondertage	215
6.4.2.8	INTUSCOM_AUTHORITY_GROUPS Berechtigungsgruppen.....	215
6.4.2.9	INTUSCOM_FUNCTION_STEP_VALUES Funktionsschrittwerte	215
6.4.2.10	INTUSCOM_CARD_DATA Kartendaten.....	216
6.4.3	Upload-Tabellen	219
6.4.3.1	INTUSCOM_UPLOAD_BOOKINGS - Buchungssätze	220
6.4.3.2	INTUSCOM_UPLOAD_OTHER - Alarme und Meldungen.....	221
6.4.4	INTUSCOM_TERMINALS Terminal-Konfiguration.....	221
6.4.5	Die Fingerprint-Schnittstelle	222
6.4.5.1	Begriffsdefinitionen	223
6.4.5.2	Bereitstellen von Templates-IDs.....	224
6.4.5.3	INTUSCOM_TH_TEMPLATES - Verteilung der Templates	226
6.4.5.4	INTUS_FP_APP_TEMPLATES - Bereitstellen von Templates	227
6.4.6	Die PS-Schnittstelle (PalmSecure).....	228
6.4.6.1	Begriffsdefinitionen	228
6.4.6.2	Bereitstellen von Templates-IDs.....	228
6.4.6.3	INTUS_PS_TEMPLATES - Verteilung der Templates.....	229
6.4.7	Die Videoschnittstelle	229

6.4.7.1	INTUSCOM_VIDEO_IMAGES	230
6.4.7.2	INTUSCOM_VIDEO_PROFILES	231
6.4.7.3	Systemarchitektur	233
6.4.7.4	Arbeitsweise	233
6.4.7.5	Beispiel Videoüberwachung mit globaler Ereigniseinstellung	233
6.4.7.6	Einstellungen in SeeTec	236
6.4.7.7	Verwendung der Videoprofile	238
6.4.8	LPR-Interface (Kennzeichenerkennungsschnittstelle)	238
6.4.8.1	INTUSCOM_LICENSE_PLATES	239
6.4.8.2	INTUS_LP_PROFILES	240
6.4.8.3	Systemarchitektur	241
6.4.8.4	Beispiel Kennzeichenerkennung mit Schrankensteuerung	243
6.5	Tabellenbasierte Dateischnittstelle (csv-Dateischnittstelle)	244
6.5.1	Dateiübergabe	244
6.5.2	Felder für die Übergabe von Stammsätzen	245
6.5.3	Felder für die Übergabe von Zutrittsprofilen	246
6.5.4	Felder für die Übergaben von Buchungsprofilen	247
6.5.5	Felder für die Übergaben von Türprofilen	249
6.5.6	Felder für die Übergabe von Profilen zur zeitlichen Funktionsteuerung	250
6.5.7	Felder für die Übergabe von Templates-IDs	250
6.5.8	Felder für die Übergabe von Kennzeichen	251
6.5.9	Felder für die Übergabe von Kennzeichenprofilen	252
6.6	INTUS COM Konfigurationsdatei	254
7	INTUS COM Konzept	257
7.1	Einsatz von INTUS COM ohne TPI	257
7.1.1	Anforderungen an das TCL-Programm	257
7.2	Die Kommunikation zwischen den INTUS COM Komponenten	260
7.2.1	Admin-Server	260
7.2.2	Der Datenport	260
7.2.3	Der Serviceport	260
7.2.4	Der Admin-Datenport	261
7.2.5	Portadressen	261
A.	Anhang	262
A.1.	Änderungsindex	262
A.1.1.	Änderungsindex 3.6.0	262
A.1.2.	Änderungsindex 3.5.0	262
A.1.3.	Änderungsindex 3.4.1	263
A.1.4.	Änderungsindex 3.4.0	263
A.1.5.	Änderungsindex 3.3.0	263
A.1.6.	Änderungsindex 3.2.0	265
A.1.7.	Änderungsindex 3.1.2	265
A.1.8.	Änderungsindex 3.1.0	265
A.1.9.	Änderungsindex 3.0.0	266
A.1.10.	Änderungsindex 2.10.0	266
A.1.11.	Änderungsindex 2.9.0	266
A.1.12.	Änderungsindex 2.8.0	266
A.1.13.	Änderungsindex 2.7.0	268
A.2.	Lizenzbestimmungen	270
A.1.1.	Lizenzbestimmungen der verwendeten Freien Software	270
A.1.2.	The OpenSSL Toolkit License	270
A.1.3.	ISB/BSC License	272

A.3.	Tabellen und Verzeichnisse.....	273
A.1.4.	Tabellenverzeichnis	273
A.1.5.	Verzeichnis der Beispiele	273
A.1.6.	Abbildungsverzeichnis.....	274
A.1.7.	Stichwortverzeichnis.....	276
A.4.	Probleme mit diesem Handbuch?	279
	Rufen Sie uns an.....	279

1 Einleitung

Das INTUS COM Terminal Management System ist ein modulares Programmpaket, das aus mehreren Komponenten besteht und für Windows (Windows 2008 Server R2, Windows 7, Windows 2012 Server R2, Windows 8 und 8.1, Windows 10) verfügbar ist. Einzelne Komponenten können optional eingesetzt werden.

Es übernimmt für die Rechnerapplikation (Zeiterfassung, Zutrittskontrolle, BDE) die Kommunikation und die Administration von INTUS-Geräten – Terminals, Zutrittskontrollmanagern und Zutrittslesern. Unterstützt sind die aktuellen INTUS Modelle – INTUS 5200, 5205, 5320, 5540, 5600, ACM40e, ACM80e und daran angeschlossene INTUS Zutrittsleser – und auch abgekündigte Modelle – siehe aktuelles White Paper „INTUS COM Einsatzbedingungen“. INTUS COM entlastet so die Applikation von Details der Anbindung der Terminals.

Die Kommunikationskomponenten (Server) ermöglichen die Kommunikation mit INTUS Terminals über das TCP/IP- und HTTPS-Protokoll.

Die Serverkomponenten (Admin-Server, Terminal-Handler, AutoClone) übernehmen Betriebsfunktionen (Dateidownload, Uhrzeitsynchronisation, Quittungsmechanismus). Darüber hinaus bietet die Clientkomponente (INTUS COM Client) Funktionen zur Betriebsstatusanzeige und -überwachung sowie manuelle Eingriffsmöglichkeiten in das laufende System.



INTUS COM ist auf den Einsatz mit INTUS Geräten ausgestattet mit der Gerätesoftware INTUS TPI-TASC) optimiert. Werden in den Terminals andere TCL-Programme eingesetzt, kann nicht die gesamte Funktionalität von INTUS COM genutzt werden.

Über das INTUSCOM Video-Interface können Kameras angeschlossen am Videomanagementsystem Cayuga genutzt werden, um Videobilder für bestimmte Ereignisse an INTUS Terminals zu erhalten.

Der INTUS COM Client verwendet eine Mehrfenstertechnik, in der die Informationen optimal an die jeweilige Bildschirmgröße angepasst werden können. Es gibt „Lageplan“-Fenster, in denen die Terminals auf Grundstücks-, Gebäude- oder Etagenplänen übersichtlich angeordnet und gruppiert werden können.

1.1 Notwendige Vorkenntnisse

Dieses Handbuch wendet sich zum einen an den Betreiber einer INTUS COM Installation (Kapitel 2-5). Für diesen Teil werden Kenntnisse des jeweils eingesetzten Betriebssystems und deren Bedieneroberfläche und von PZE bzw. Zutrittssystemen vorausgesetzt.

In der Regel sind spezielle Kenntnisse der INTUS Terminals nicht erforderlich, aber hilfreich.

Der zweite Teil (Kapitel 6-8) liefert Informationen für Software-Entwickler, die das Interface zwischen einer Rechnerapplikation und INTUS COM implementieren.

1.2 Weitere Handbücher

Außer dem vorliegenden INTUS COM Betriebshandbuch sind noch folgende Handbücher erhältlich:

INTUS TPI 4.0 Benutzerhandbuch

(Bestellnummer D3400-020)

Dieses Handbuch beschreibt das Terminal Parametrier Interface (TPI) des (optionalen) TCL-Programms INTUS TPI-TASC.

TPI ist eine Schnittstelle zur Parametrierung der INTUS Geräte, die alle Anforderungen an Zeiterfassung, Zutrittskontrolle und einfache Betriebsdatenerfassung erfüllt.

INTUSEnroll 3.2 Benutzerhandbuch

(Bestellnummer D3000.442.06)

Dieses Handbuch beschreibt das Einlernprogramm INTUSEnroll für INTUS PS Terminals und Fingerprintleser.

INTUS RemoteConf

(Bestellnummer D5000-001.02)

Dieses Handbuch beschreibt die Konfiguration von Terminals mit dem Programm INTUS RemoteConf.

1.3 Systemarchitektur

INTUS COM bildet eine Kommunikationsschicht zwischen der INTUS Terminalhardware und der Rechner-Applikation.

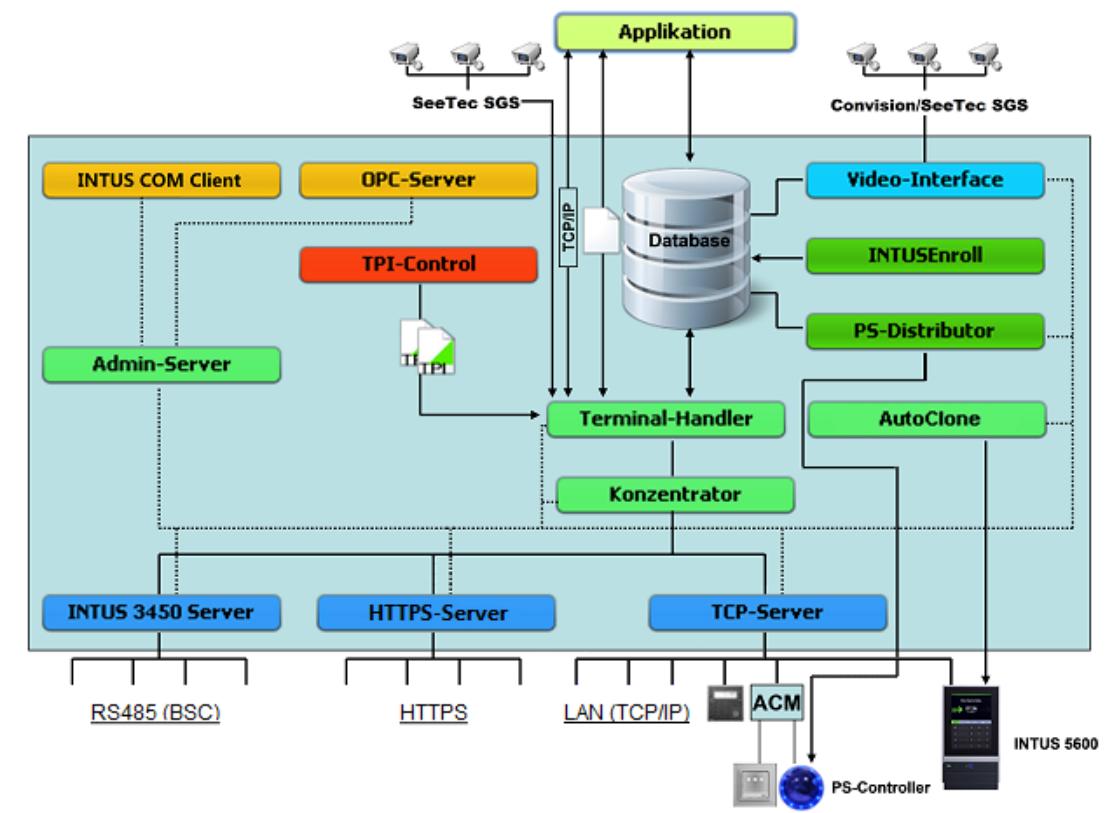


Abbildung 1.1 – INTUS COM Systemarchitektur

1.3.1 INTUS COM Client und Admin-Server

Der INTUS COM Client ist die Benutzerschnittstelle von INTUS COM. Er ermöglicht die Konfiguration der INTUS COM Serverkomponenten und der angeschlossenen Terminals, sowie der Betriebsstatusüberwachung der Terminals.

Der INTUS COM Client kann auf mehreren Rechnern installiert sein und auch mehrfach gestartet werden.

Der Admin-Server ist die Schnittstelle zwischen den verschiedenen Instanzen des INTUS COM Client und den Server-Komponenten. Er konfiguriert die anderen Komponenten. Weiterhin reagiert er auf bestimmte Ereignisse und sammelt Statusinformationen, die dann im INTUS COM Client angezeigt werden können.

Der Admin-Server ist ein Serverprozess und hat keine eigene Bedieneroberfläche.

1.3.2 Terminal-Handler

Der Terminal-Handler kann der Applikation verschiedene Routinefunktionen bei der Kommunikation mit den Terminals abnehmen (z. B. Dateidownload, Uhrzeitsynchronisation usw.).

Er stellt der Rechnerapplikation wahlweise eine TCP/IP-Schnittstelle (Socket-Schnittstelle), eine Dateischnittstelle oder eine Datenbankschnittstelle zur Verfügung, die auch gemischt eingesetzt werden können (siehe Kapitel 6).

Der Terminal-Handler ist ein Serverprozess und hat keine eigene Bedieneroberfläche. Der Terminal-Handler setzt auf dem Konzentrator auf.

1.3.3 Der AutoClone Dienst

Der AutoClone Dienst wird für den Download der Dateien

- INTUS Graph Masken (*.igma)
- INTUS Audio Archiv (*.iaa)
- INTUS Graph Tastatur (*.qml)

auf INTUS 5600 Terminals verwendet. Dabei kann der Download manuell über den INTUS COM Client angestossen werden oder vom INTUS 5600 Terminal selbst angefordert werden.

1.3.4 Konzentrator

Der Konzentrator führt die Datenströme von und zu den Servern zu einem Datenstrom zusammen. Er ist erforderlich, wenn mehr als ein Kommunikations-Server oder der Terminal-Handler eingesetzt werden.

1.3.5 Die Kommunikations-Server

Jedes Terminal wird je nach Kommunikationsart (TCP/IP, HTTPS, RS485) mit einen Kommunikations-Server verbunden. Die Kommunikations-Server sind Serverprozesse und haben keine eigene Bedieneroberfläche

Der TCP-Server übernimmt die Kommunikation mit allen Terminals, die über TCP/IP angeschlossen sind.

Der HTTPS-Server übernimmt die Kommunikation mit allen Terminals, die über HTTPS angegebunden sind.

Mit INTUS 3000/3450 Serverterminals können weitere INTUS Terminals über RS485 angebunden werden.

Die Server arbeiten als Protokollwandler und als Demultiplexer/Multiplexer.

Zum Konzentrator (bzw. Applikation) stellt jeder Server einen TCP/IP-Datenport für alle Terminals zur Verfügung (Demultiplexer/Multiplexer, siehe Kapitel 6.2).

Mit den Terminals kommuniziert er über das von den Terminals benötigte Protokoll (BSC, HTTPS oder TCP, Protokollwandler).

1.3.6 Das Video-Interface

Das Video-Interface lädt auf Anforderung, Bilddaten via HTTP direkt von einer Videoquelle. Als Videoquelle wird unterstützt:

- Cayuga angebunden über SGS (SeeTec Gateway Service)

Die Bilddaten werden in der Datenbankschnittstelle der Applikation zur Verfügung gestellt. Das Video-Interface ist ein Serverprozess und hat keine eigene Bedieneroberfläche. Die Konfiguration erfolgt durch den Admin-Server über den INTUS COM Client.



Der Einsatz des INTUSCOM Video-Interface setzt die Verwendung der Datenbankschnittstelle voraus.

1.3.7 Der PS-Distributor

Der PS-Distributor verteilt PS-Templates, die durch das Einlernprogramm INTUSEnroll in der Datenbankschnittstelle bereitgestellt werden, auf die angeschlossenen PS-Controller. Der PS-Distributor ist ein Serverprozess und hat keine eigene Bedieneroberfläche. Die Konfiguration erfolgt durch den Admin-Server über den INTUS COM Client.



Der Einsatz des INTUSCOM PS-Distributor setzt die Verwendung der Datenbankschnittstelle voraus.

2 Windows Installation

2.1 INTUS Software installieren

Sie erhalten INTUS COM im Rahmen der INTUS Software Distribution per Download. In dieser Distribution ist auch die komplette Dokumentation (auch dieses Handbuch) zu INTUS COM und TPI im pdf-Dateiformat enthalten. Nach dem Download entpacken Sie bitte das ZIP-Archiv. Rufen Sie dann bitte `INTUS_Software_Setup_1.7.0.exe` im Verzeichnis `distr\windows\Setup` auf und folgen den Anweisungen. Für die Installation benötigen Sie Administrator-Rechte.

Sie können den Setup mehrfach nacheinander aufrufen, um einzelne Komponenten nachzuinstallieren oder um den INTUS COM Client auf verschiedenen Rechnern zu installieren.

INTUS COM und „User Access Control“ (UAC)

Auf neueren Windows-Varianten (2008/2012/2016/2019/2022 Server und Windows 7/8/10/11), wird der Windows Benutzer durch die "User Access Control" (UAC) daran gehindert, Dateien im Ordner "Program Files" bzw. „Program Files (x86)“ zu verändern. Um Probleme mit der UAC zu umgehen, müssen Sie entweder

- die INTUS COM Programme und Batchdateien mit Administratorrechten ausführen.
- oder dem Windows-Benutzer Schreibrechte auf das Installationsverzeichnis geben.

2.1.1 Testinstallation

Wählen Sie Testinstallation, wenn Sie INTUS COM und TPI testen wollen. Es werden dann alle erforderlichen Komponenten inkl. TPI Demo-Konfigurationen für alle PCS Terminal-Typen auf einem Rechner installiert. Es wird außerdem automatisch eine **3-monatige Testlizenz** vergeben.

Bei der Testinstallation werden die Server nicht als Windows-Dienste installiert. Wenn Sie eine dieser Komponenten testen wollen, verwenden Sie anschließend die „benutzerdefinierte Installation“ und selektieren Sie nur diese Komponente.

2.1.2 Benutzerdefinierte Installation

Wählen Sie die Benutzerdefinierte Installation, wenn Sie ein Produktivsystem installieren wollen. Sie können dann folgende Installationsoptionen selektieren.

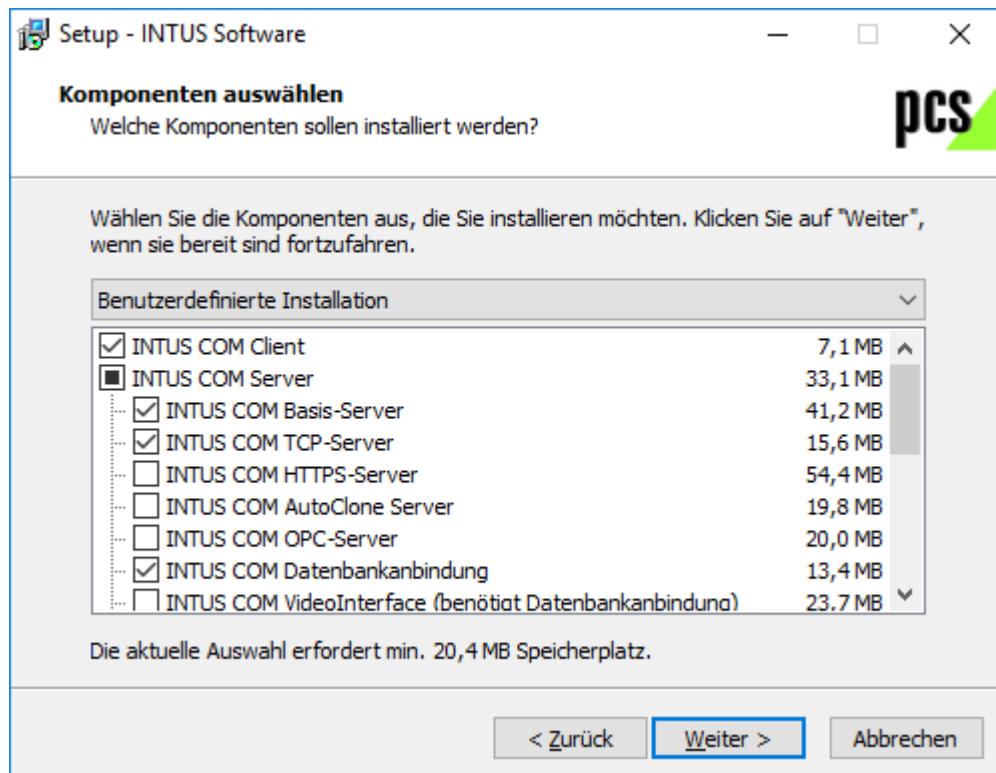


Abbildung 2.1 - INTUS COM installieren

INTUS COM besteht aus mehreren Komponenten (Server), die nach dem Client-Server Prinzip untereinander und mit den Terminals kommunizieren. Die Komponenten können deshalb auf mehreren Rechnern im System verteilt installiert werden. Rufen Sie den benutzerdefinierten Setup auf jedem dieser Rechner auf und selektieren Sie nur die jeweils benötigten Komponenten. Beachten Sie dabei die folgenden Installationshinweise zu den einzelnen Komponenten.

INTUS COM Client

Der INTUS COM Client kann auf mehreren Rechnern installiert werden, von denen INTUS COM administriert bzw. überwacht werden soll.

INTUS COM Basis-Server

Terminal-Handler, Admin-Server, Konzentrator, PS-Distributor und AutoClone dürfen nur einmal systemweit installiert werden. Es wird empfohlen, diese Komponenten und den TCP-Server zusammen auf einem zentralen Server-Rechner zu installieren.



Hinweise

- Zur Installation der Basis-Server ist ein gültiger Lizenz-Schlüssel erforderlich.
- PCS empfiehlt, die Basis-Server „als Service“ zu installieren. Sie werden dann bei jedem Systemstart automatisch gestartet.

TCP-Server

Dieser INTUS COM Kommunikations-Server kann mehrfach und auf mehreren Rechnern installiert werden. Auf einem Rechner darf der Server aber nur einmal installiert werden. Es ist ausreichend, den TCP-Server nur einmal im System (zusammen mit den Basisservern) zu installieren, wenn weniger als 500 Terminals angeschlossen werden sollen. Falls Sie 500 oder mehr Terminals anschließen möchten, konsultieren Sie bitte die PCS Projektabteilung, um von der Erfahrung der PCS zu profitieren und Unterstützung hinsichtlich der Fragestellung zu erhalten, ob ein TCP-Server in Ihrem Fall ausreicht.

HTTPS-Server

Dieser INTUS COM Kommunikations-Server kann mehrfach und auf mehreren Rechnern installiert werden. Es ist ausreichend, den HTTPS-Server nur einmal im System zu installieren, wenn weniger als 100 Terminals angeschlossen werden sollen.

AutoClone Server

Der AutoClone Server kann nur genau einmal in einer INTUS COM Konfiguration vorkommen. Der AutoClone Server wird für Terminals mit grafischer Oberfläche benötigt z.B: INTUS 5600.

INTUS COM OPC-Server

Der INTUS COM OPC-Server kann mehrfach und auf mehreren Rechnern installiert werden. Der INTUS COM OPC-Server stellt eine OPC Schnittstelle z.B: für Leitstandssysteme bereit um Statusinformationen der angeschlossenen INTUS Terminals anzuzeigen.

INTUS COM Datenbankanbindung

Installieren Sie die Datenbankanbindung nur, wenn Sie die INTUS COM Datenbank-Schnittstelle benötigen. Ein Fehler während der DB-Tabelleninstallation wird in der Datei `<Installationspfad>\log\<yyyy-MM-dd-hh-mm-Setup-1.7.0>\setup.log` aufgezeichnet.

Führen Sie bitte zuerst die in 2.1.3 beschriebenen Arbeiten durch, bevor Sie diese Installationskomponente wählen.

INTUS COM VideoInterface, PS-Distributor

Das INTUS COM VideoInterface und der PS-Distributor können genau einmal in einer INTUS COM Konfiguration vorkommen. Die Verwendung des INTUS COM VideoInterface oder des PS-Distributors setzt die INTUS COM Datenbankschnittstelle voraus. Für die Verbindung zur INTUS COM Datenbank wird eine ODBC-Datenquelle benötigt.

INTUS PS Setup

Das Programm INTUS PS Setup wird zur Suche und Konfiguration von PS-Controllern im Netzwerk verwendet.

INTUS RemoteConf

Das Program INTUS RemoteConf wird zur Suche und Konfiguration von INTUS Terminals im Netzwerk verwendet.

TPI Komponenten

Wenn Sie INTUS 3000, INTUS 5300, 5600 Terminals, ACM, ACM4, ACM8, ACM40 mit TPI einsetzen, müssen Sie die Komponente TPI-tasc zusammen mit den Basis-Servern auf einem Rechner installieren.

In der Regel ist eine Installation von TPI-Control nicht erforderlich. Sie benötigen für TPI-Control eine eigene Lizenz.

INTUS Enroll

Die Einlernsoftware INTUS Enroll kann mehrfach und auf mehreren Rechnern installiert werden. Die Verwendung von INTUS Enroll setzt die INTUS COM Datenbankschnittstelle voraus. INTUS Enroll benötigt dazu eine ODBC-Datenquelle um sich mit der INTUS COM Datenbank zu verbinden.



Auf Windows Systemen wird zwischen 32Bit und 64Bit Datenquellen unterschieden. INTUS Enroll benötigt auf einem 64Bit Windows eine 64Bit Datenquelle. Die INTUS COM Server verwenden immer eine 32Bit Datenquelle.

2.1.3 Datenbank-Schnittstelle

Damit der INTUS COM Setup die für die DB-Schnittstelle benötigten Tabellen über ODBC anlegen und folgende Dienste darauf zugreifen können:

- Terminal-Handler
- Video-Interface
- PS-Distributor

Dazu müssen Sie entweder die Demo-Datenbank bei der Installation auswählen, oder zuerst eine Datenbank anlegen, einen Benutzer definieren, der Schreibrechte in der Datenbank hat, und bei der Installation die benutzerdefinierte Einrichtung der DB-Schnittstelle durchführen.

Die genaue Funktionsweise der DB-Schnittstelle und die Beschreibung aller verwendeten Tabellen ist in Kapitel 6.4 enthalten.



Fehler, die während der Tabellen-Installation auftreten, werden in der Datei <Installationspfad>\log\<yyyy-mm-dd-hh-mm-Setup-1.7.0>\setup.log registriert.

2.1.3.1 Demo-Datenbank installieren

Um die Demo-Datenbank zu verwenden, wählen Sie die Komponente „INTUSCOM Datenbankanbindung“ aus, und stellen Sie auf der Seite „zusätzlichen Aufgaben“ die Option „Automatisch (MS-Access Demo-Datenbank)“ ein.

2.1.3.2 Benutzerdefinierte Installation der Datenbank-Schnittstelle

Für die benutzerdefinierte Installation der DB-Schnittstelle sollten Sie folgendermassen vorgehen.

Datenbank anlegen

Legen Sie zuerst eine Datenbank in Ihrem Datenbanksystem an. Im Folgenden wird als Datenbankname **INTUSCOM-DB** verwendet.

Benutzer anlegen

Legen Sie danach einen Benutzer an und geben Sie ihm Rechte, Tabellen anzulegen und zu schreiben. Im Folgenden wird als Benutzername **intuscom** und als Benutzerpasswort **pcs** verwendet.

ODBC-Datenquelle einrichten

Als nächstes muss auf dem Rechner, auf dem die INTUS COM Server installiert werden, ein Datenbanktreiber installiert und eine ODBC-Datenquelle eingerichtet werden. Dies können Sie entweder direkt durch Aufruf von **Systemsteuerung / (Verwaltung) / Datenquellen (ODBC)** tun oder während des INTUS Software Setups.

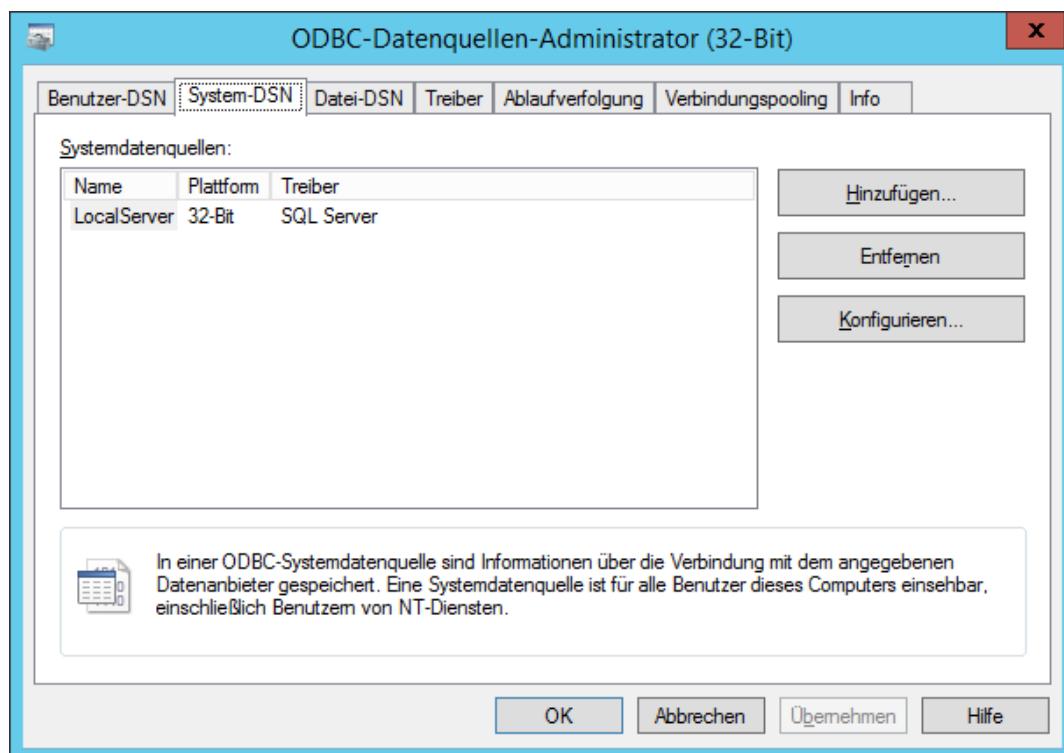


Abbildung 2.2 - Eintrag einer ODBC-Datenquelle in der Systemsteuerung

Wählen Sie im Registerblatt **System-DSN** **Hinzufügen** und tragen beim Datenquellennamen **INTUScom-DB** ein, wie das folgende Bild für eine MS Access-DB zeigt

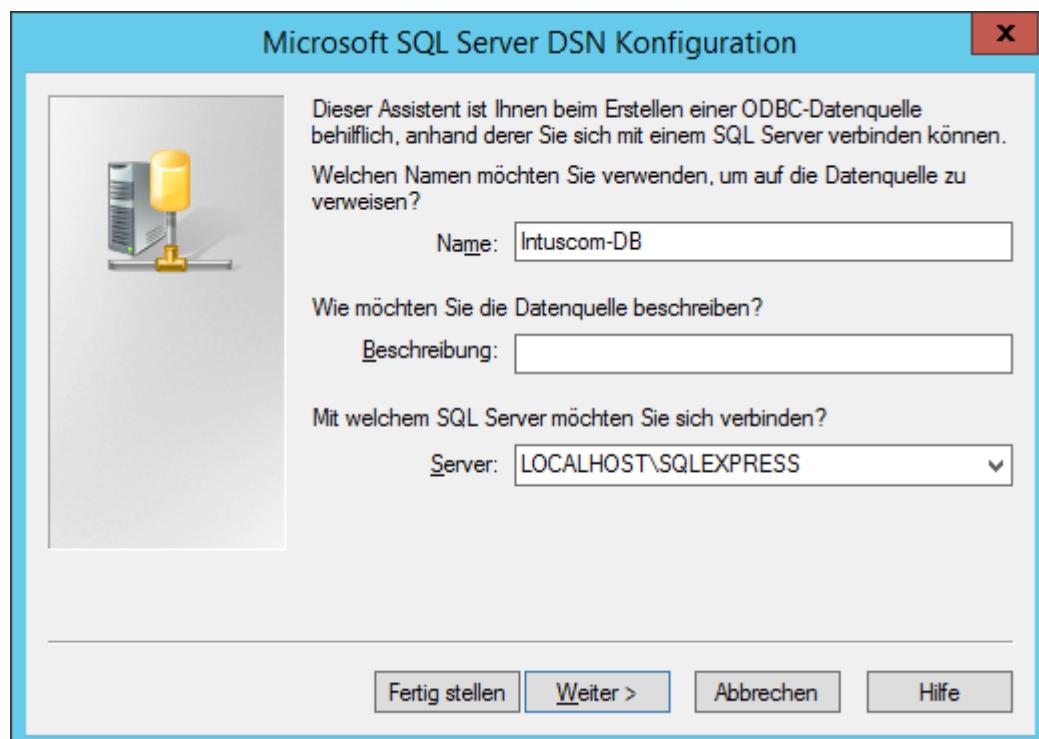


Abbildung 2.3 - Anlegen einer ODBC-Systemdatenquelle



Wird die Installation auf einer 64Bit Version von Windows durchgeführt, muss das Programm Windows\SysWow64\odbcad32.exe verwendet werden um die ODBC Datenquelle anzulegen.

Wenn Sie eine Microsoft SQL Server Datenbank verwenden, wählen Sie als nächstes „Mit SQL-Server Authentifizierung ...“

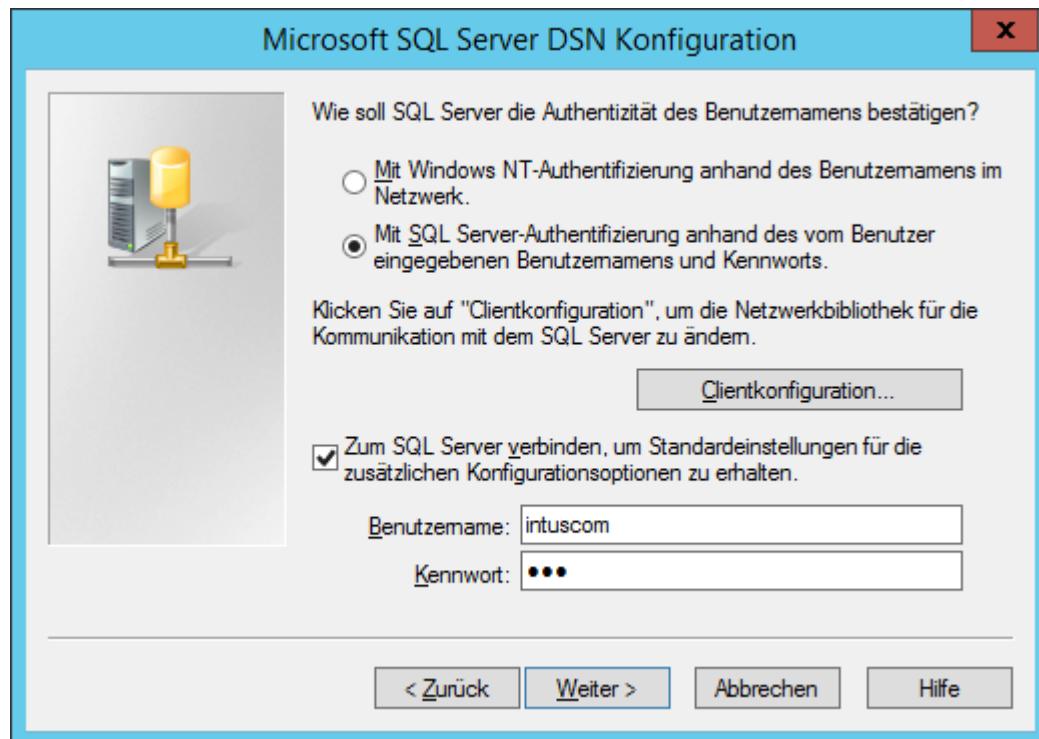


Abbildung 2.4 - Konfiguration des SQL-Server ODBC Treibers

INTUS COM Tabellen anlegen

Um die INTUS COM Tabellen anzulegen, wählen Sie während der Installation die Komponente

„INTUS COM Datenbankanbindung“ aus.

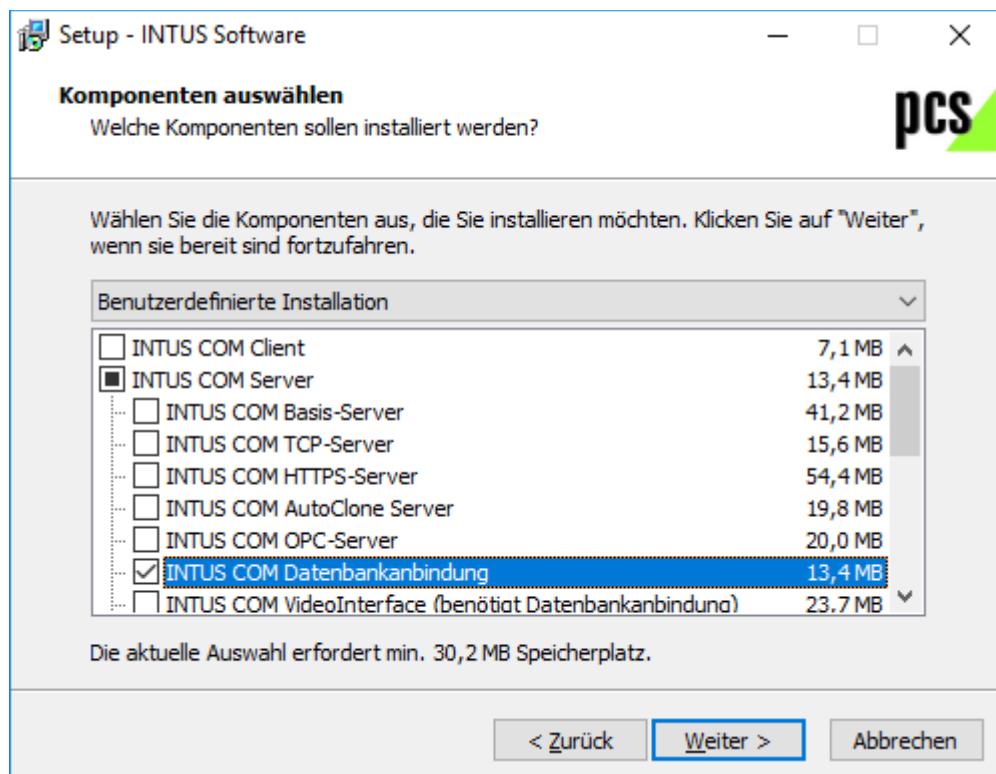


Abbildung 2.5 - INTUS COM Datenbankanbindung installieren

Auf der Setupseite „Zusätzliche Aufgaben auswählen“, kann dann die Option „INTUS COM DB-Tabellen installieren“ ausgewählt werden.

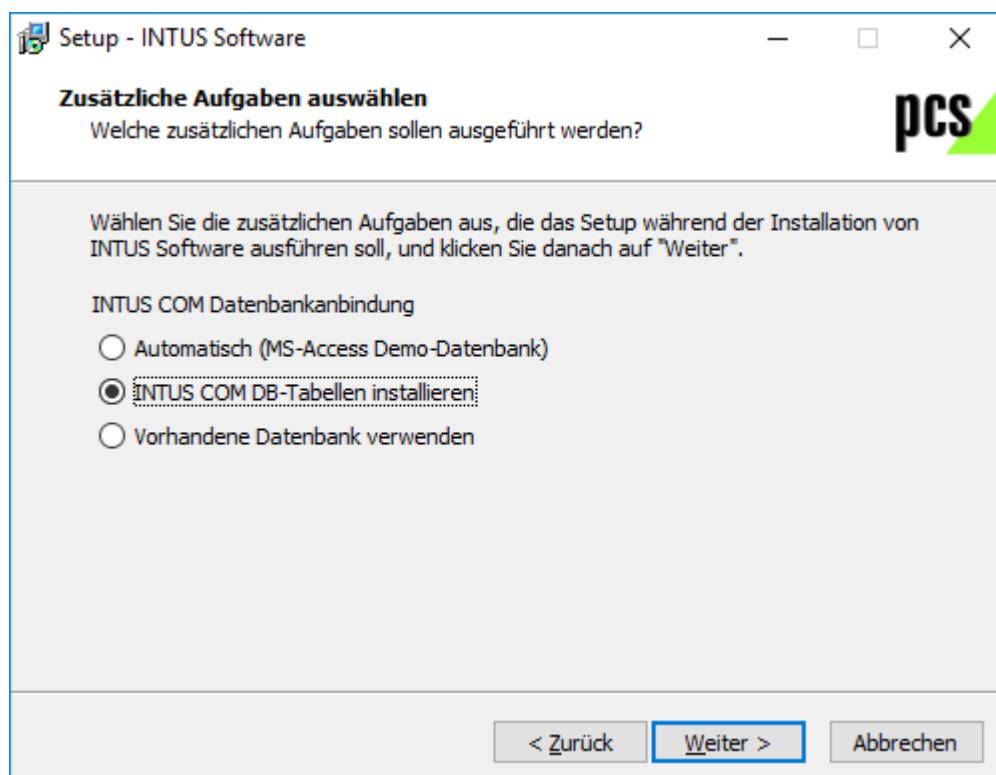


Abbildung 2.6 - INTUS COM DB-Tabellen installieren

Auf einer der folgenden Seiten werden dann die Verbindungseinstellungen für die ODBC Datenquelle abgefragt.

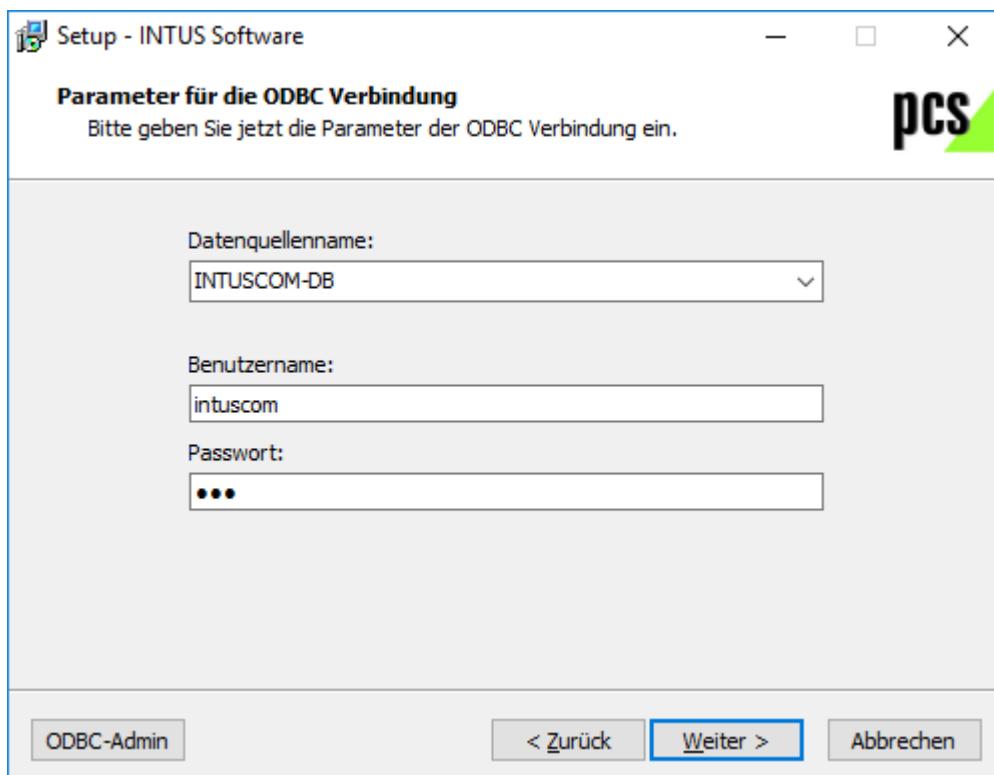


Abbildung 2.7 - ODBC Verbindungseinstellungen für INTUS COM

Danach wird durch eine Sicherheitsabfrage sichergestellt, dass die Tabelleninstallation nicht irrtümlich durchgeführt wird.



Eine nochmalige Installation der Datenbanktabellen versetzt die Datenbankschnittstelle in den Anfangszustand. D.h.: Alle Daten die seit der erstmaligen Installation in der Datenbankschnittstelle abgelegt wurden, gehen bei einer nochmaligen Installation der Datenbanktabellen verloren!

Datenbankzugriff mit ODBC

Während der Installation einer Komponente, die die Datenbankschnittstelle verwendet (z.B.: Video-Interface), werden auch die Verbindungsparameter Datenquellename, Benutzername und das Passwort durch das Installationsprogramm vom Benutzer abgefragt. Diese Verbindungsparameter werden als Standardeinstellung für diese Komponenten verwendet.

Sie können diese Einstellungen manuell ändern, indem Sie den Eintrag in der Registry

```
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS Systemtechnik\INTUSCOM\  
"DSN"="DSN=INTUSCOM-DB;UID=intuscom;PWD=pcs"
```

entsprechend ändern.

2.1.4 Lizenzkostenfreie Java 11 Laufzeitumgebung (OpenJDK)

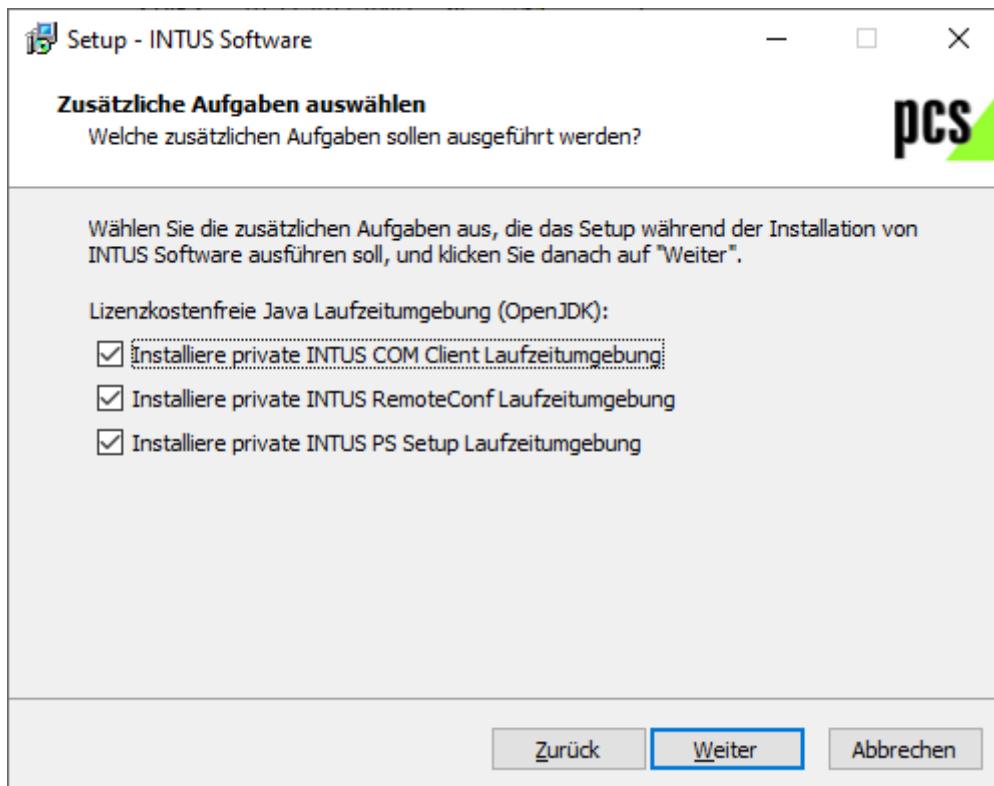


Abbildung 2.8 – Lizenzkostenfreie Laufzeitumgebung installieren

Die folgenden Programme benötigen eine Java Laufzeitumgebung:

- INTUS COM Client
- INTUS RemoteConf
- INTUS PS Setup

Mit dieser Option wird eine lizenzkostenfreie und für das Programm angepasste Laufzeitumgebung im jeweiligen Programmverzeichnis installiert. Ohne diese Option muss eine Java 8/9/10 oder 11 Laufzeitumgebung auf dem Zielrechner vorhanden sein.

2.1.5 INTUS COM HTTPS-Server installieren

2.1.5.1 Java Dienst

Der INTUS COM HTTPS-Server ist ein Java Programm. Um unter Windows als Dienst installiert und betrieben werden zu können wird ein sogenannter „Service Wrapper“ eingesetzt.

Der Wrapper für den INTUS COM HTTPS-Server wird durch den Setup unter „c:\Program Files (x86)\PCS-Systemtechnik\Intuscom\bin\https_server\yajsw“ installiert.

Weitere Informationen zu diesem Service Wrapper finden Sie unter <http://yajsw.sourceforge.net/>.

2.1.5.2 Server Zertifikat

Der INTUS COM HTTPS-Server benötigt einen Keystore mit einem Server-Zertifikat im Verzeichnis „Intuscom\cert“. Damit ein INTUS HTTPS-Terminal mit dem INTUS COM HTTPS-Server eine Verbindung aufnehmen kann muss das passende CA-Zertifikat mit INTUS RemoteConf auf das Terminal geladen werden.

Wurde der INTUS COM HTTPS-Server zur Installation ausgewählt, so können durch das Installationsprogramm die benötigten Zertifikate automatisch erstellt werden.

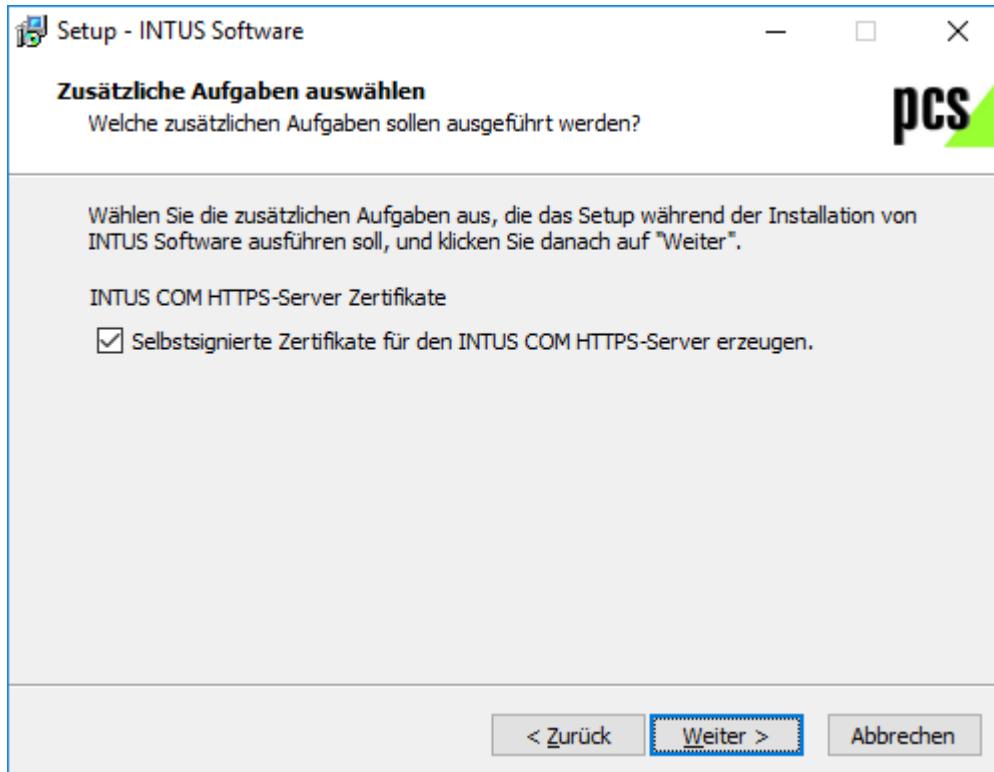


Abbildung 2.9 – INTUS COM HTTPS-Server Zertifikate

Durch die Auswahl „Selbstsignierte Zertifikate für den INTUS COM HTTPS-Server erzeugen“, wird im Verzeichnis „intuscom\cert“ ein KeyStore „PCSHhttpsStore.jks“ mit dem Server-Zertifikat und ein selbstsigniertes CA-Zertifikat „ca.pem“ durch den Setup erzeugt.

2.2 INTUS COM aktualisieren

Um eine vorhandene INTUS Software Installation zu aktualisieren, starten Sie bitte das Aktualisierungsprogramm „INTUS_Software_update_1.7.0.exe“ auf der Installations-CD und folgen den Anweisungen. Dieses Programm befindet sich auf der Installations-CD im Verzeichnis „\windows\update“. Für die Aktualisierung einer INTUS Software Installation benötigen Sie Administrator-Rechte.

Das Aktualisierungsprogramm erkennt automatisch die Version der installierten INTUS Software Programme und der Datenbankschnittstelle.

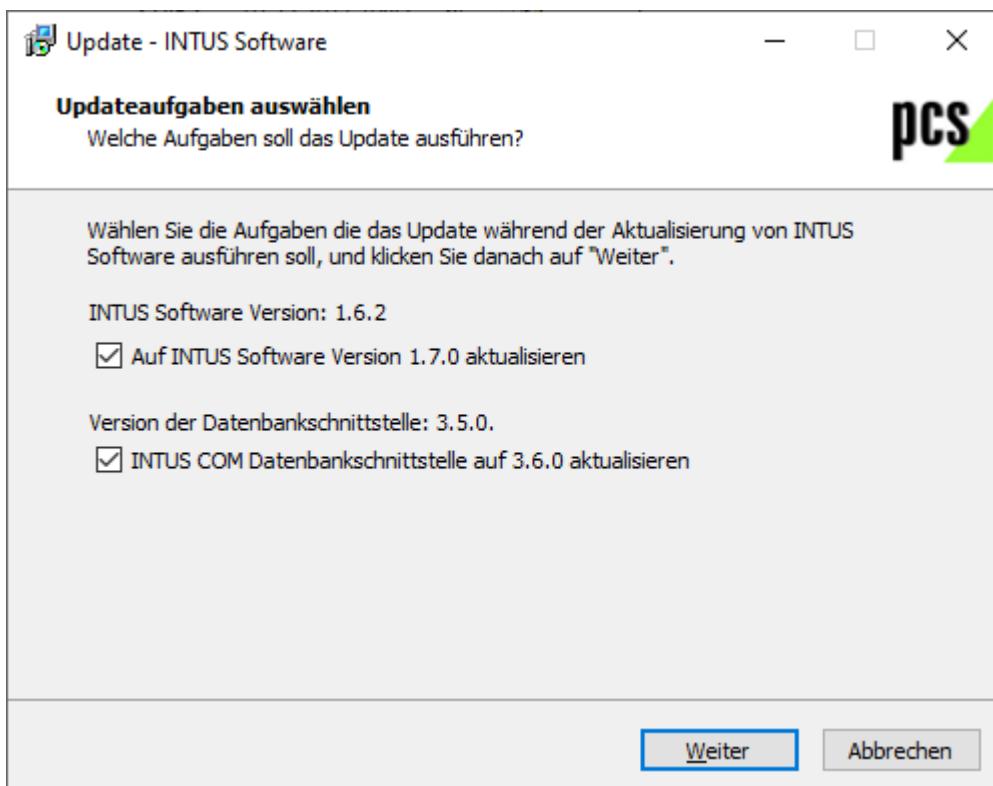


Abbildung 2.10 - Auswahl der Updatekomponenten

Die Aktualisierung der INTUS Software Programmversionen und der Datenbankschnittstelle können unabhängig voneinander durchgeführt werden.

Zusätzlich bietet das Update die Installation einer lizenzkostenfreien Java Laufzeitumgebung für die installierten Java Programme an, wenn diese installiert sind.

 Das Aktualisierungsprogramm „update.exe“ ist nur für die Aktualisierung einer INTUS COM/INTUS Software Installation ab Version 2.2.0. Bevor Sie eine ältere Installation aktualisieren können, müssen Sie die INTUS COM Installation mindestens auf die Version 2.2.0 bringen. Im Verzeichnis \Windows\Update\ finden Sie die dazu benötigten Aktualisierungsprogramme. Dazu starten Sie im Verzeichnis \Windows\Update\2.2.0\ das Programm setup.exe und wählen „Update Installation“. Um die Datenbankschnittstelle auf 2.2.0 zu aktualisieren verwenden Sie das Programm updateDb.exe im selben Verzeichnis.

2.2.1 Update der INTUS Software Programme

 Um die INTUS Software Installation auf den Stand 1.7.0 zu bringen, starten Sie die Datei „update.exe“, wählen „Auf INTUS Software Version 1.7.0 aktualisieren“ und folgen den Anweisungen.

Führen Sie das Update auf allen Rechnern aus, auf denen Sie INTUS Software Komponenten installiert haben. Ihre alte Installation wird in einem Verzeichnis INTUSCOM_yymmdd_hhMMss gesichert und eine Aktualisierung der vorhandenen Komponenten wird durchgeführt. Installationsspezifische Dateien wie Konfigurationsdateien, Parametrierdateien (siehe 2.2.3), etc. werden bei einer Aktualisierung nicht verändert.

2.2.2 Update der INTUS COM Datenbank-Schnittstelle

 Um die INTUS COM Datenbankschnittstelle auf den Stand 3.6.0 zu bringen, starten Sie die Datei „update.exe“, wählen „INTUS COM Datenbankschnittstelle auf 3.6.0 aktualisieren“ und folgen den Anweisungen.

Da in INTUS COM Versionen vor der Version 2.2.0 die Datenbankschnittstelle nicht automatisch aktualisiert wurde, kann es vorkommen, dass der Versionsstand der Datenbank-Schnittstelle

vom Versionsstand der Software abweicht. In diesem Fall muss die Datenbankschnittstelle vor dem Update auf den Versionsstand 2.2.0 gebracht werden. Das Aktualisierungsprogramm erkennt diesen Fall und bringt eine entsprechende Fehlermeldung. Brechen Sie das Update an dieser Stelle ab und führen Sie zuerst das Programm „updateDb.exe“ im Verzeichnis \Windows\Update\2.2.0 aus. Danach starten Sie das Update neu.



Bei der Aktualisierung wird die Datenbank-Schnittstelle auf den Stand wie in Kapitel 6.4 beschrieben, gebracht. Abweichungen von diesem Standard werden bei der Aktualisierung nicht berücksichtigt und gehen verloren. Eine Ausnahme ist die Spalte `TIMEID_NO`. In Version 2.0.0 wurde die Feldlänge der Spalte `TIMEID_NO` von 8 auf 10 Zeichen und in Version 2.8.0 von 10 auf 20 Zeichen erweitert. Um mit den alten Versionen kompatibel zu bleiben, wird die Länge dieser Spalte bei der Aktualisierung nicht verändert.

Zunächst werden alle Tabellen der Schnittstelle geprüft und mit dem Standard (siehe Kapitel 6.4) verglichen. Bei einer Abweichung vom Standard in einer Tabelle, wird diese umbenannt in `<Tabellen-Prefix><Zeitstempel><Tabellenname>`. Der Zeitstempel hat das Format „YYYY-MM-DD-HH-MM“ und bezeichnet den Zeitpunkt, an dem die Aktualisierung der Datenbank-Schnittstelle gestartet wurde. Nach dem Umbenennen wird die Tabelle entsprechend dem Standard angelegt und eventuell vorhandene Datensätze werden von der umbenannten Tabelle kopiert. Nach der Aktualisierung werden die Datenbanktabellen nochmals geprüft, um sicherzustellen dass die Aktualisierung erfolgreich war.

Das Update legt im log-Verzeichnis einen Ordner „`<Zeitstempel>-Update-<Version>`“ an. In diesem Ordner wird die Log-Datei des Aktualisierungsprogramms angelegt. Bei einer Aktualisierung der Datenbankschnittstelle werden in dem oben genannten Verzeichnis auch die, bei der Aktualisierung Verwendeten SQL-Skripte und resultierenden Log-Dateien, abgelegt.

2.2.3 Update der TPI Komponenten

TPI besteht aus den Komponenten

- TPI-TASC V4.03
- TPI Parameterdateien (`*_72.tpi`, `*_73.tpi`)
- TPI-Control V4.0.2
- TPI Referenzhandbuch V4.0

Durch das Update werden die TPI Parameterdateien und TPI-TASC im Verzeichnis `\work\TPI-TASC` nicht aktualisiert! Dadurch wird gewährleistet, dass das Terminal-System nach der Update-Installation voll funktionsfähig bleibt.

Durch die Update-Installation werden nur das TPI-Handbuch ersetzt und unter den TPI-Control und TPI-TASC Verzeichnissen ein Unterverzeichnis „4.0.0“ erstellt. In diesem Unterverzeichnis werden die aktuellen Programmversionen abgelegt.

Um auf die neue Version 4.0.0 umzustellen, müssen alle benötigten TPI Parameterdateien mit der neuen Version von TPI-Control angepasst werden. Dies ist aber nur dann nötig und wird nur dann empfohlen, wenn Funktionen genutzt werden sollen, die in der neuen Version enthalten sind.



2.3 INTUS COM Serverkomponenten einrichten und starten

Wenn Sie die INTUS COM Server auf verschiedenen Rechner installiert haben, müssen Sie zuerst die Secure-Dateien manuell anpassen (siehe 2.3.5).

2.3.1 HTTPS-Server einrichten

Für die gesicherte Kommunikation zwischen INTUS COM HTTPS-Server und den INTUS Terminals müssen im INTUS COM HTTPS-Server und in den Terminals, die über den INTUS COM HTTPS-Server angebunden werden Zertifikate eingestellt werden. Alle an einem INTUS COM HTTPS-Server angebundenen Terminals müssen dabei das gleiche CA-Zertifikat verwenden.

2.3.1.1 Übersicht

Die Terminals können entweder direkt über HTTPS, oder über einen Proxy an den HTTPS-Server angebunden werden. Wird ein Proxy verwendet, so kann zwischen Proxy und HTTPS-Server auch einfaches HTTP verwendet werden.

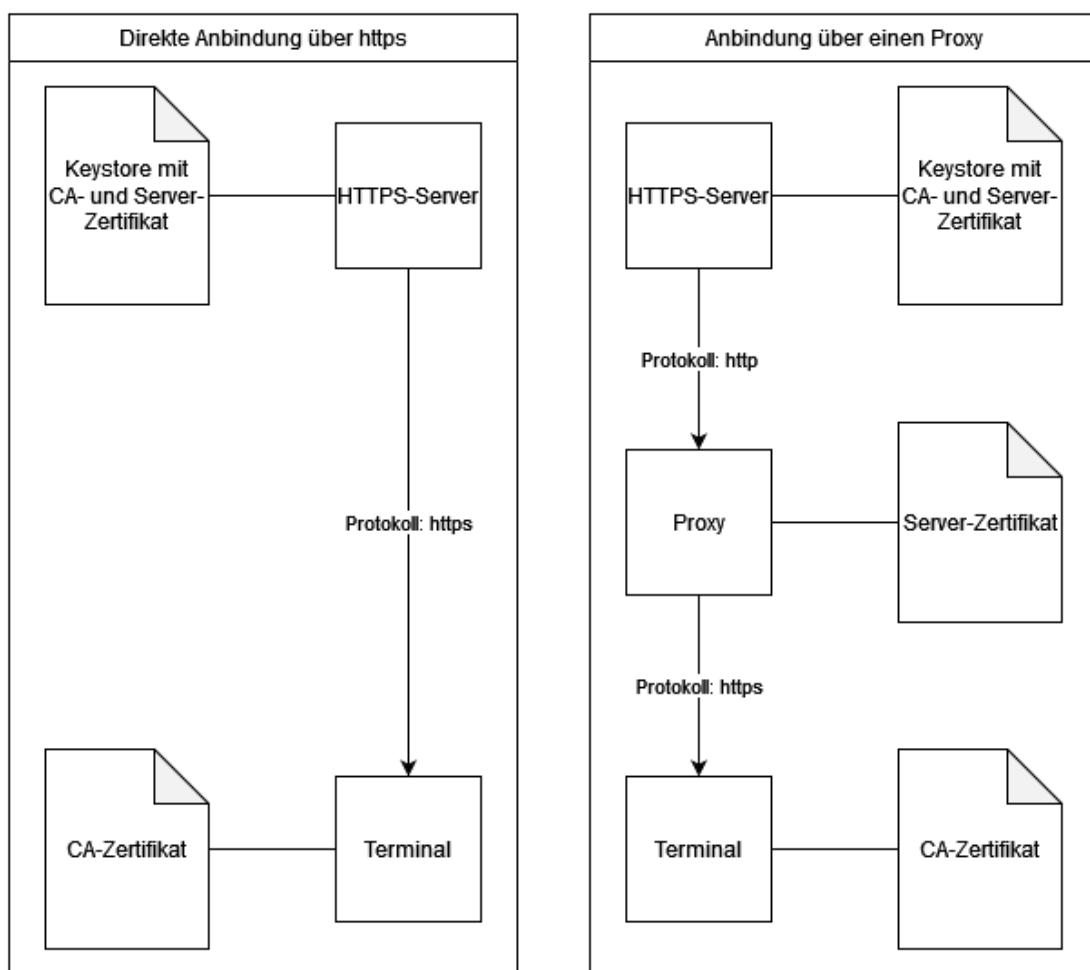


Abbildung 2.11 Vergleich HTTPS-Server mit und ohne Proxy

2.3.1.2 HTTPS-Terminal konfigurieren

Für die Terminals müssen folgende Einstellungen in INTUS RemoteConf getroffen werden:

- **Hostname:** Hostname oder IP-Adresse des HTTPS-Servers.
- **Port:** Im HTTPS-Server eingestellter HTTPS-Port.
- **Verzeichnis:** Dieser Wert wird nur intern vom HTTPS-Server verwendet und muss immer auf „htcl“ gesetzt werden.
- **Benutzername:** Dieser Wert wird vom INTUS COM HTTPS-Server momentan nicht verwendet und muss nicht konfiguriert werden.

- **Passwort:** Dieses Passwort authentifiziert das Terminal gegenüber dem HTTPS-Server. Es muss mit dem für dieses Terminal in INTUS COM eingestellten Passwort übereinstimmen.
- **CA-Zertifikat:** Das CA-Zertifikat, das mit dem selben CA-Schlüssel erstellt wurde, mit dem das Server-Zertifikat signiert wurde

Weitere Informationen zum Einstellen dieser Parameter sind im Handbuch „INTUS RemoteConf - Konfiguration und Betrieb“ zu finden.

2.3.1.3 Verwendung eines Proxys

Bei Verwendung eines Proxys kann für die Verbindung zwischen Proxy und HTTPS-Server einfaches HTTP verwendet werden (Aufbau siehe 2.3.1.1).

Damit die Terminals mit dem Proxy kommunizieren können, muss im Proxy ein mit dem CA-Zertifikat des Terminals signiertes Server-Zertifikat hinterlegt werden. Die Kommunikation zwischen Proxy und HTTPS-Server kann dann über http laufen.

Es ist aber zu beachten, dass im HTTPS-Server trotzdem ein Keystore mit CA- und Server-Zertifikat konfiguriert werden muss, da neben der Anbindung über HTTP und den Proxy auch eine direkte Anbindung über HTTPS unterstützt wird. Der Keystore wird außerdem für das automatische Update des CA-Zertifikats benötigt (siehe 4.11.2).

2.3.1.4 Generieren des Keystores

Das Programm „KeyStoreGen.exe“ kann verwendet werden, um den KeyStore PCSHtt-
psStore.jks für den INTUS COM HTTPS-Server zu erzeugen. Des Weiteren kann das CA-Zertifikat für die INTUS HTTPS-Terminals generiert und in eine Datei exportiert werden.

Das Programm „KeyStoreGen.exe“ befindet sich im Verzeichnis „C:\Program Files
(x86)\PCS-Systemtechnik\Intuscom\cert\“.

Keystore mit vorhandenen Zertifikaten erstellen

Das Programm „KeyStoreGen.exe“ kann verwendet werden, um einen Keystore aus bereits vorhandenen Zertifikaten zu erstellen. Dazu müssen folgende Dateien vorhanden sein:

- Server-Zertifikat im pfx-Format
- CA-Zertifikat im pem-Format

Diese Dateien können im Programm „KeyStoreGen.exe“ angegeben werden. Das Tool generiert dann aus diesen Dateien einen Keystore.

Wählen Sie hierzu die Option „Server-Zertifikat und CA in neuen Keystore importieren“ aus.

2.3 - INTUS COM Serverkomponenten einrichten und starten

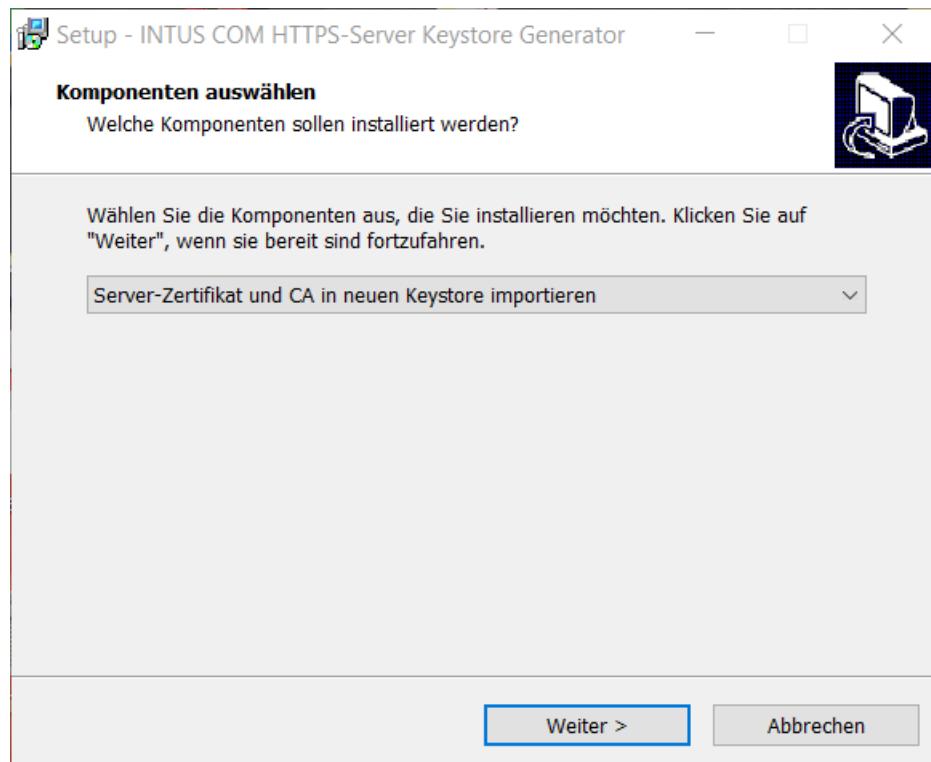


Abbildung 2.12 - Zertifikate importieren

Ist im HTTPS-Server noch kein Keystore hinterlegt, so kann der Keystore über die Option „Konfiguriere den aktuellen Keystore“ automatisch hinterlegt werden. Ist bereits ein Keystore hinterlegt, so kann über die Option „Konfiguriere den Update-Keystore“ ein Keystore für das automatische Zertifikatsupdate (siehe 4.11.2) hinterlegt werden.

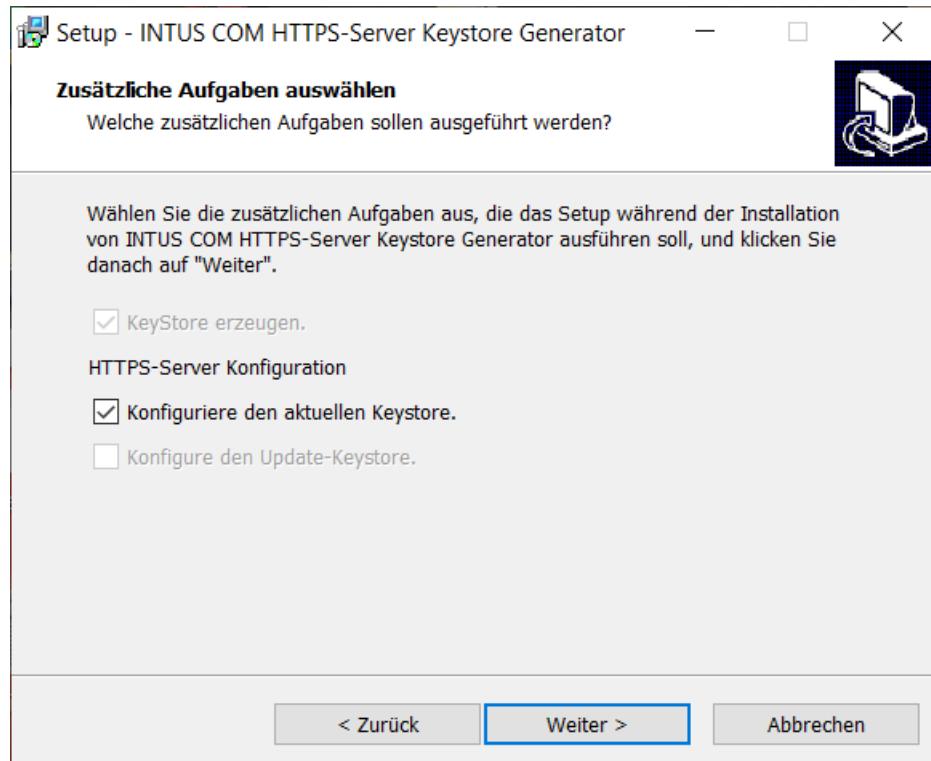


Abbildung 2.13 - Zusätzliche Aufgaben konfigurieren

Wählen Sie für den Export das Verzeichnis „C:\Program Files (x86)\PCS-Systemtechnik\Intuscom\certs“ aus.

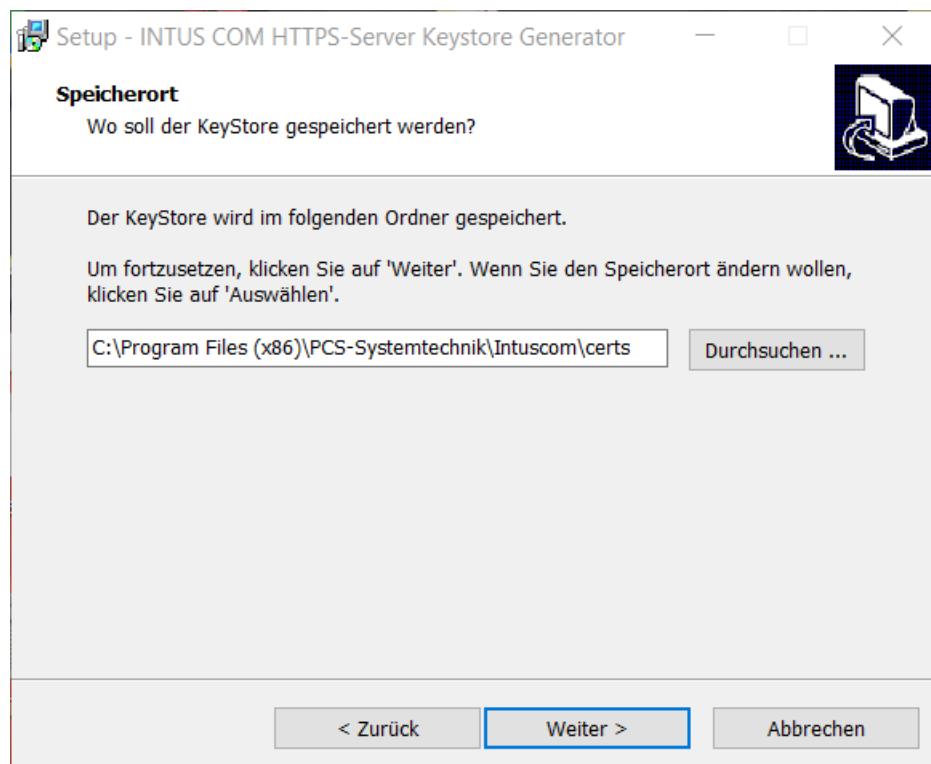


Abbildung 2.14 - Speicherort des Keystores

Im folgenden Dialog können Sie Name und Passwort des Keystores festlegen.

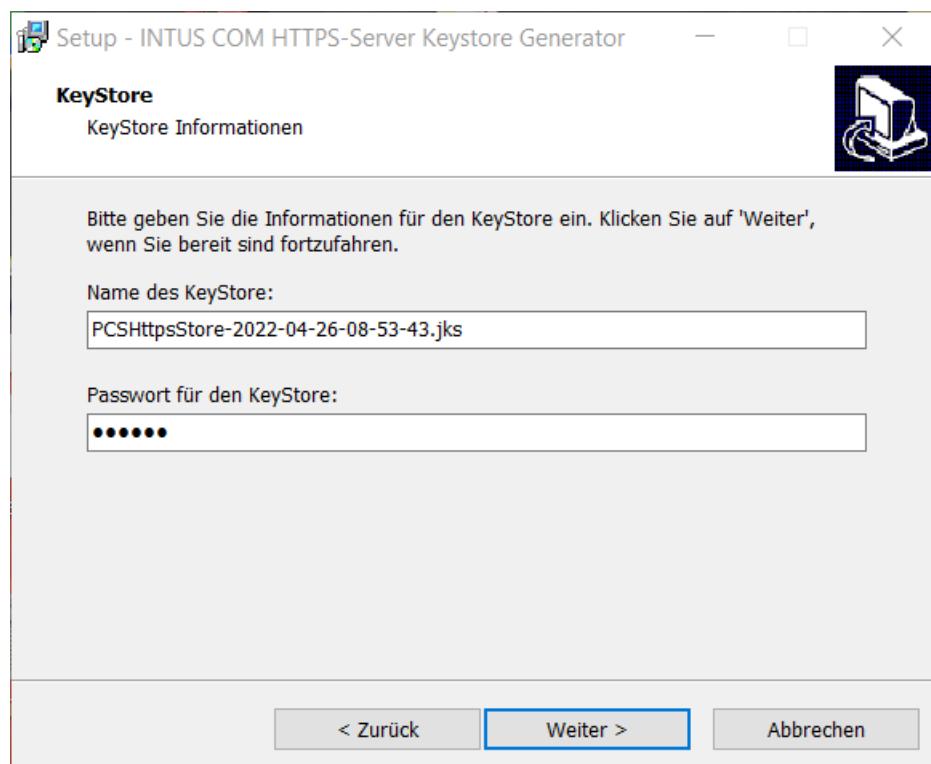


Abbildung 2.15 – Erstellen des Keystores

2.3 - INTUS COM Serverkomponenten einrichten und starten

Nun können Sie die Zertifikate auswählen, die in den Keystore importiert werden sollen.

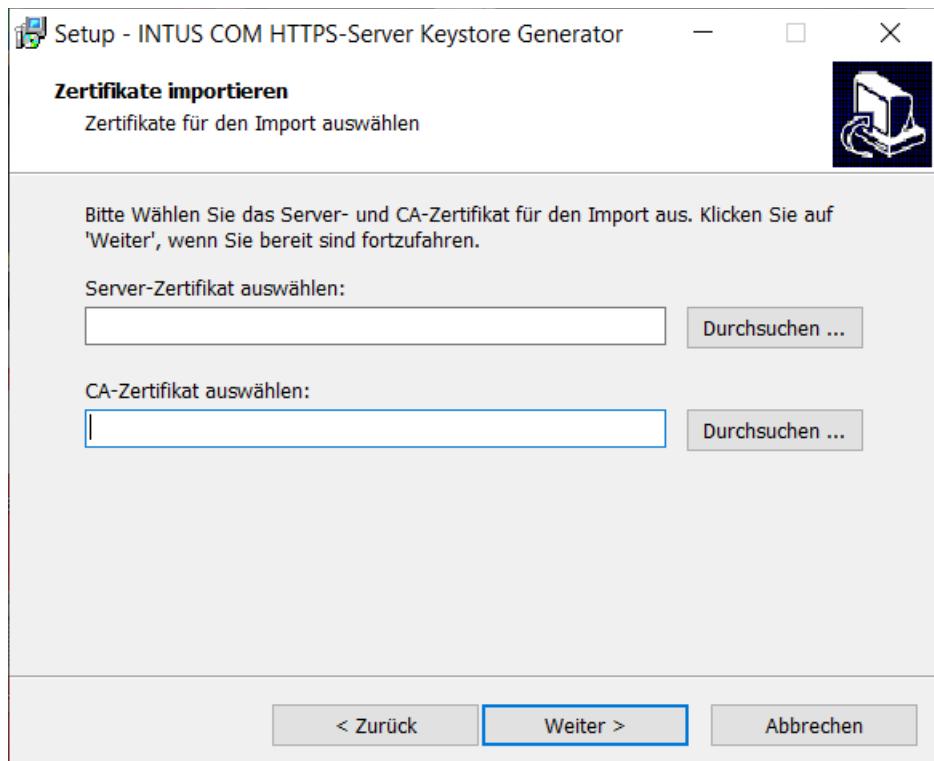


Abbildung 2.16 - Auswahl der Zertifikate

Geben Sie nun das Passwort für die PFX-Datei an.

Das Passwort der PFX-Datei muss mit dem Passwort des privaten Schlüssels des Server-Zertifikats übereinstimmen.

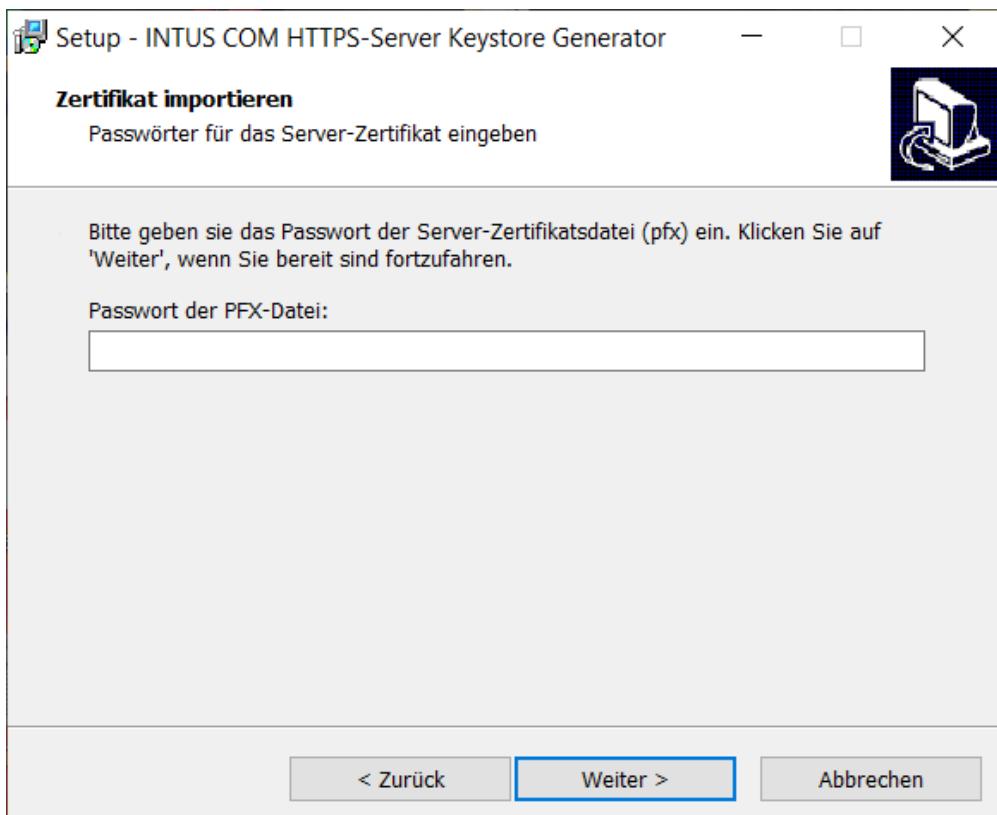


Abbildung 2.17 - Angeben der Passwörter

Durch Betätigen der Schaltfläche „Keystore erzeugen“ wird der KeyStore mit den angegebenen Zertifikaten erzeugt.

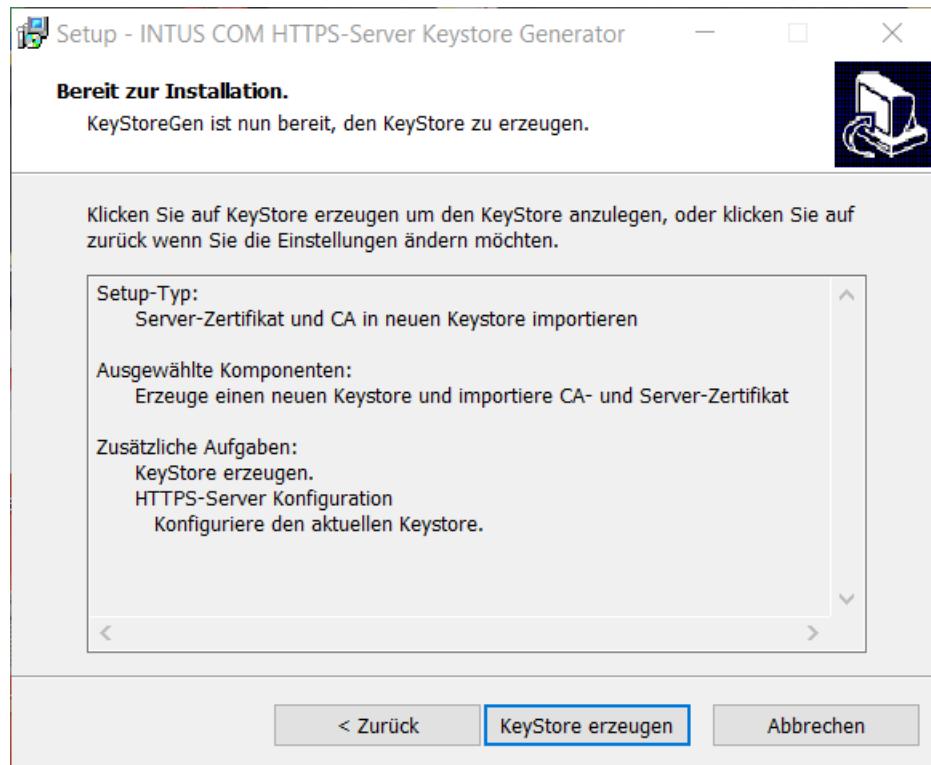


Abbildung 2.18 - Generieren des Keystores

Selbstsignierte Zertifikate

Das Programm „KeyStoreGen.exe“ kann verwendet werden, um einen Keystore mit selbstsignierten Zertifikaten zu erstellen. Wählen Sie hierzu die Option „Keystore für den INTUS COM HTTPS-Server erstellen“.

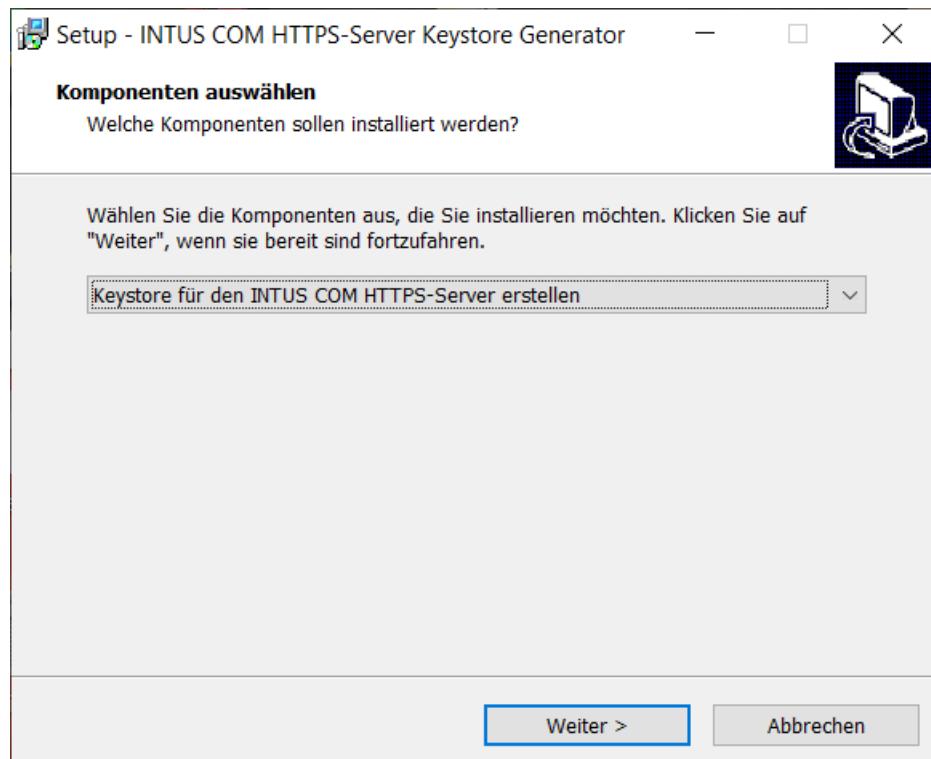


Abbildung 2.19 – Keystore mit selbsignierten Zertifikaten erstellen

2.3 - INTUS COM Serverkomponenten einrichten und starten

Wählen Sie die Aufgaben „KeyStore exportieren“ und „CA-Zertifikat in eine Datei exportieren“ aus.

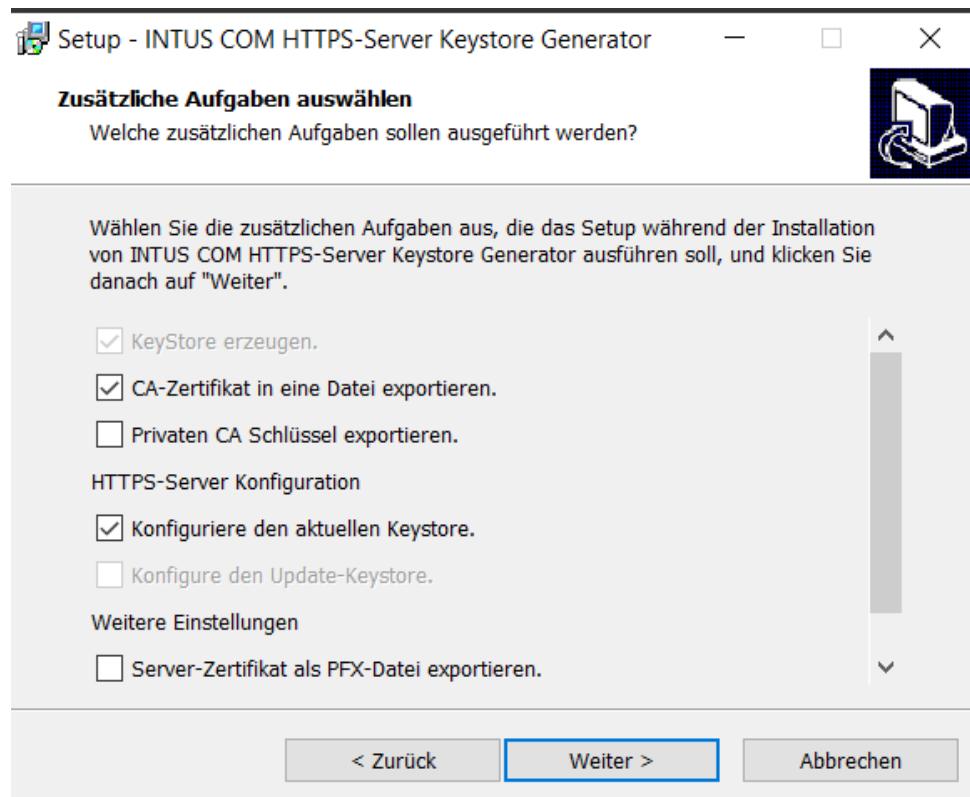


Abbildung 2.20 – KeyStoreGen – Exportdateien festlegen

Wählen Sie für den Export das Verzeichnis „C:\Program Files (x86)\PCS-Systemtechnik\Intuscom\certs“ aus.

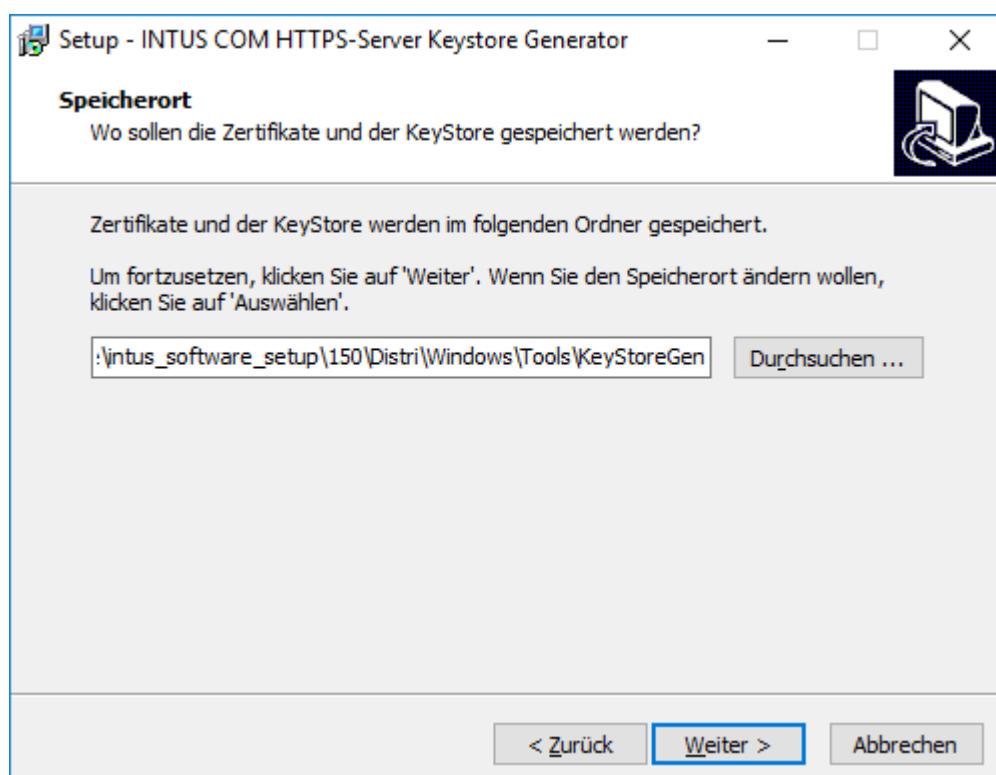


Abbildung 2.21 – KeyStoreGen – Exportpfad festlegen

Tragen Sie für das Feld „Allgemeiner Name (CN)“ den Hostnamen oder der IP-Adresse des Zielrechners ein. Das Programm KeyStoreGen.exe belegt dieses Feld mit dem Hostnamen des Rechners, auf dem das Programm gestartet wurde.

Die weiteren Eingabefelder können Sie auf den Defaulteinstellungen belassen. Auch die Folgeseiten können Sie unverändert lassen.

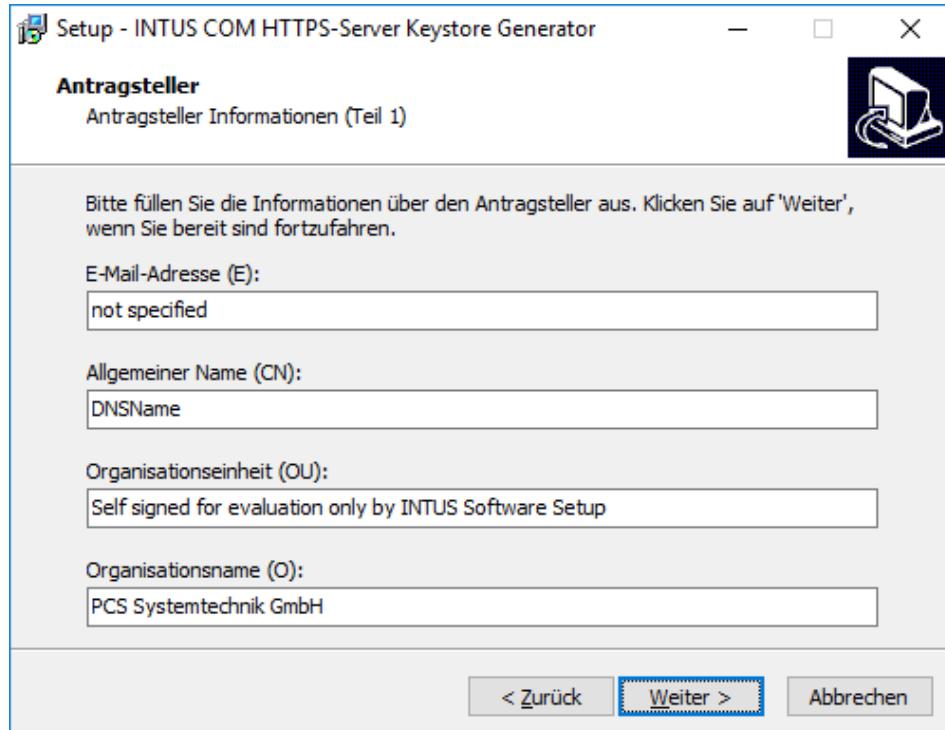


Abbildung 2.22 – KeyStoreGen – Antragsteller Informationen

Durch Betätigen der Schaltfläche „Keystore erzeugen“ wird der KeyStore „PCSHtt-
psStore.jks“ und das CA-Zertifikat erzeugt in das ausgewählte Verzeichnis exportiert.

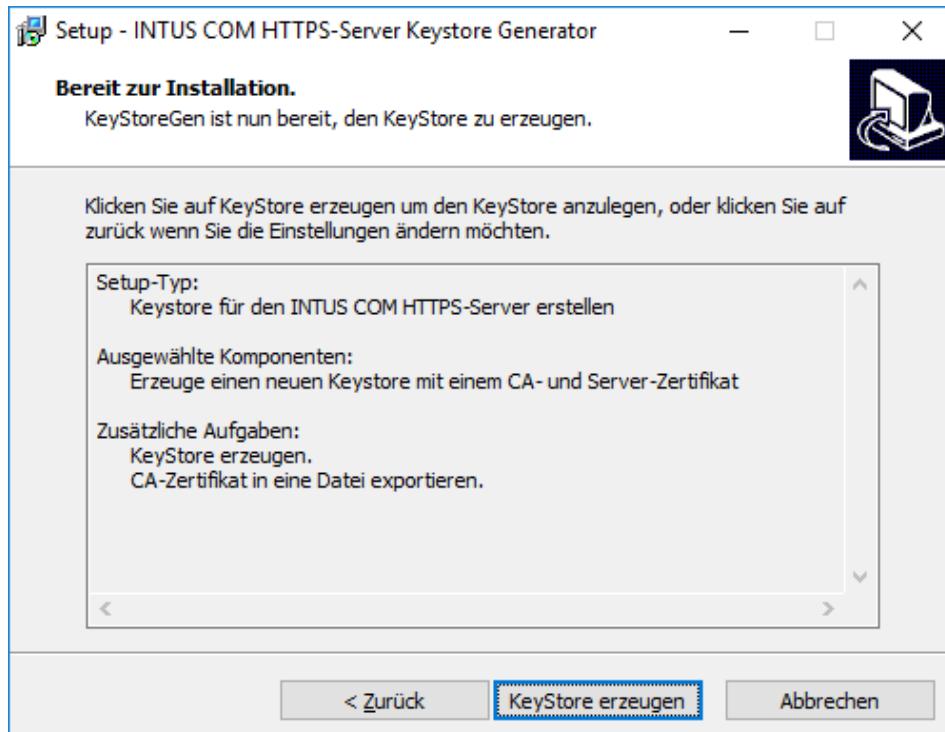


Abbildung 2.23 – KeyStoreGen – Ausführen

2.3.1.5 Änderung der Passwörter für den Keystore und das Zertifikat

Dieser Schritt ist nur notwendig, wenn ein Keystore durch einen neuen ersetzt werden soll, für den neue Passwörter gesetzt wurden.

Bevor Änderungen an der Datei „https_server.properties“ vorgenommen werden, sollte der HTTPS-Server beendet werden. Sonst kann es dazu kommen, dass die manuellen Änderungen wieder überschrieben werden. Außerdem werden Änderungen an dieser Datei erst nach einem Neustart des HTTPS-Servers übernommen.

Um das entsprechende Passwort zu ändern, muss das neue Passwort für „newKeyPassword“, bzw. „newKeystorePassword“ im Klartext in der Datei „https_server.properties“ angegeben werden. Der HTTPS-Server wird das Passwort beim nächsten Start verschlüsseln, unter „currentKeyPassword“, bzw. „currentKeystorePassword“ abspeichern und das Klartext-Passwort automatisch aus der Datei löschen. Sind unter „newKeyPassword“, bzw. „newKeystorePassword“ keine Werte eingetragen, so werden die verschlüsselten Passwörter verwendet.

2.3.2 Batch-Dateien

Zum Starten und Beenden der Basisserver liegen vier Batch-Dateien

- intuscom_start.bat
- intuscom_stop.bat
- intuscom_start_services.bat
- intuscom_stop_services.bat

im Installationsverzeichnis und es wird ein Link ins Start-Menü eingetragen. Sie können sie so über Start/Programme/INTUSCOM aufrufen.

2.3.3 Kommandozeilenoptionen

Sie können die Server auch einzeln mit den entsprechenden Kommandozeilenoptionen starten. Admin-Server, Terminal-Handler, Konzentrator, HTTPS-Server und TCP-Server sind Konsolenprogramme ohne grafische Oberfläche. Sie befinden sich im Unterverzeichnis \intuscom\bin der INTUS Software Installation.

Für den Aufruf von der Kommandozeile gibt es folgende Optionen:

- ? Anzeige der Kommandozeilenoptionen
- b im Hintergrund starten (unter Windows wird der Systemdienst gestartet)
- f im Vordergrund starten
- k laufenden Prozess beenden
- v Log-Meldungen auch auf den Bildschirm ausgeben (Verwenden Sie diese Option zusammen mit der Option -f)

2.3.4 Installieren als Windows Systemdienst (Service)

Unter

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows 10
- Windows 11

können Sie alle Serverkomponenten als Systemdienste installieren. Dazu gibt es folgende Kommandozeilenoptionen:

- install als Systemdienst installieren
- remove Systemdienst deinstallieren

2.3.5 Secure-Dateien

Um die Sicherheit zu erhöhen, schränken Terminal-Handler, Konzentrator, TCP-Server, HTTPS-Server, AutoClone, der PS-Distributor und das Video-Interface den Zugriff auf ihre Serviceports und sofern vorhanden auch ihres Datenports ein. Es werden nur Verbindungen von bestimmten IP-Adressen oder Netzwerken zugelassen. Verbindungen von unzulässigen IP-Adressen werden sofort wieder getrennt.

Die zulässigen IP-Adressen und Netzwerke müssen Sie in den Secure-Dateien angeben. Die Secure-Dateien befinden sich im Unterverzeichnis `\intuscom\conf` der INTUS Software Installation.

Programm	Secure-Datei für Datenport(s)	Secure-Datei für Serviceport
Terminal-Handler	<code>th_secure.cfg</code>	<code>th_conf_secure.cfg</code>
Konzentrator	<code>con_secure.cfg</code>	<code>con_conf_secure.cfg</code>
TCP-Server	<code>tcp_secure.cfg</code>	<code>tcp_conf_secure.cfg</code>
Video-Interface		<code>video_conf_secure.cfg</code>
PS-Distributor		<code>ps_conf_secure.cfg</code>
AutoClone		<code>autoclone_conf_secure.cfg</code>
HTTPS-Server	<code>https_secure.cfg</code>	<code>https_conf_secure.cfg</code>

Tabelle 2.1 – Secure-Dateien

Wenn Sie die Server auf einem Windows Rechner bereits als Systemdienst (Service) installiert haben, müssen Sie vorher den Systemdienst stoppen.

Secure-Dateien sind Textdateien.

Beispiel 2.1 - Secure-Datei

```
# Dies ist ein Kommentar.  
# Folgende Einträge erlauben Verbindungen von  
127.0.0.1      # dem lokalen Rechner (IPV4)  
::1            # dem lokalen Rechner (IPV6)  
134.98.135.105 # dem Rechner 134.98.135.105  
2001:1234:5678:9abc:ef01:2345:6789:abcd      # dem Rechner 2001:1234:...  
134.98.135. # allen Rechnern im Netz 134.98.135.*  
134.98.    # allen Rechnern im Netz 134.98.*.*  
134.    # allen Rechnern im Netz 134.*.*.*  
ALL     # allen Rechnern
```

2.3.6 Portnummer des Admin-Servers ändern

Der INTUS COM Client versucht eine Verbindung zum Admin-Server über Port 13050 aufzubauen. Wenn dieser Port durch eine Fremdapplikation belegt ist, muss eine andere freie Portnummer verwendet werden, z.B. 13055. Dazu müssen Sie zuerst den Admin-Server stoppen und dann mit einem Editor in der Datei `\intuscom\conf\admin-server.ini` in der Sektion `[settings.00001]` den Eintrag `port=13055` vornehmen. Anschließend kann der Server wieder gestartet werden.

2.4 INTUS COM Client starten

Starten Sie den INTUS COM Client über **Start/Programme/INTUSCOM/INTUSCOM-client**. Sie erhalten folgenden Login-Dialog:

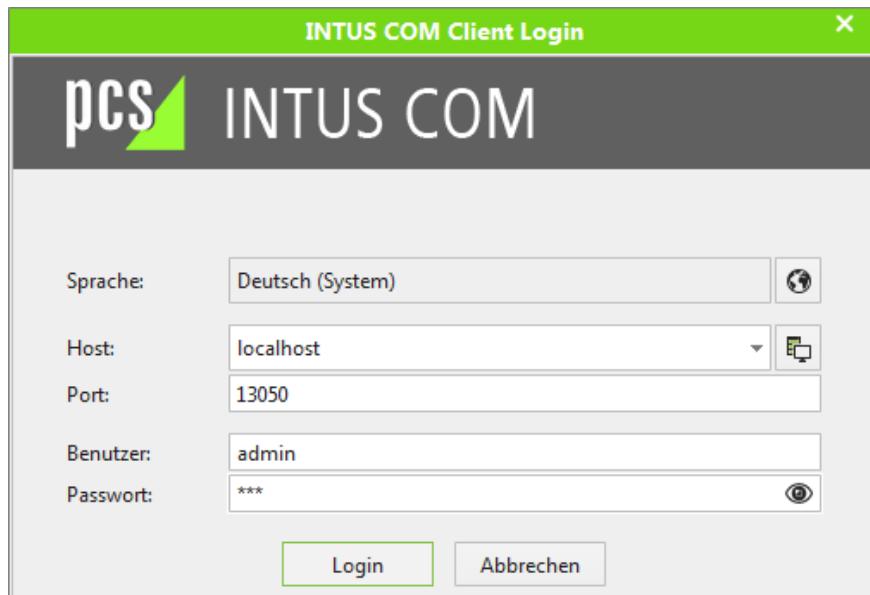


Abbildung 2.24 - Anmelden mit Benutzer und Passwort

Um die Sprache des INTUS COM Client zu ändern, betätigen Sie die Schaltfläche rechts neben der angezeigten Sprache und wählen Sie die gewünschte Sprache im Sprachdialog aus. Daraufhin wird der INTUS COM Client beendet. Beim nächsten Start des INTUS COM Client wird die ausgewählte Sprache verwendet.

Wenn der INTUS COM Client auf demselben Rechner installiert ist wie die Server, tragen Sie für **Host** den Wert **localhost** ein., ansonsten die IP-Adresse oder den Namen des Rechners, auf dem die INTUS COM Server installiert sind.

Port ist der Socket-Port, über den der INTUS COM Client mit dem Admin-Server kommuniziert (Voreinstellung: 13050). Er sollte nur geändert werden (siehe 2.3.6), wenn ein Port-Konflikt auftritt (siehe 2.4.2).

Außerdem müssen Sie sich mit Benutzername und Passwort anmelden. Wenn noch keine weiteren Benutzer angelegt wurden, kennt INTUS COM nur den Benutzer **admin**. Das Passwort für diesen Benutzer ist am Anfang auf **pcs** eingestellt.

Nachdem Sie die Schaltfläche OK gedrückt haben, erhalten Sie das Hauptfenster des INTUS COM Clients (siehe 3.1). Wenn Sie noch keine Benutzer-Lizenz eingetragen haben, werden Sie dazu aufgefordert (siehe 2.4.4). Wenn die Verbindung zum Admin-Server nicht hergestellt werden kann, erhalten Sie einen Verbindungsfehler (siehe 2.4.2).

Nach dem ersten Anmelden sollten Sie aus Sicherheitsgründen zunächst das Passwort ändern. Wählen Sie dazu im Menü unter **Bearbeiten** den Punkt **Eigenes Passwort...**

2.4.1 Speichereinstellung ändern

Dem INTUS COM Client steht $\frac{1}{4}$ des installierten RAM Speichers zur Verfügung. In einigen Situationen kann der Speicherbedarf des INTUS COM Clients größer sein (z.B: Wenn im Meldungsfester sehr viele Meldungen angezeigt werden sollen). Um dem INTUS COM Client mehr Speicher zur Verfügung zu stellen, starten Sie den INTUS COM Client mit den folgenden Parametern:

```
javaw.exe -mx2G -jar "<Pfad>\intuscom_client.jar"
```

So gestartet, werden dem INTUS COM Client 2GByte zur Verfügung gestellt, sofern auf dem Rechner ausreichend Speicher installiert ist.

2.4.2 Verbindungsfehler

Wenn Sie im Anmeldefenster des INTUS COM Clients einen Verbindungsfehler erhalten, liegt das daran, dass der INTUS COM Client den Admin-Server nicht erreichen kann.

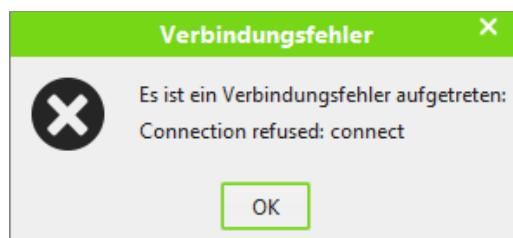


Abbildung 2.25 - Fehlerdialog für Verbindungsfehler

Dies kann drei Ursachen haben:

1. Der Admin-Server ist nicht gestartet. Überprüfen Sie, ob der Admin-Server Prozess läuft, bzw. ob der Systemdienst gestartet wurde.
2. Der Eintrag in **Host** ist fehlerhaft. Wenn der Admin-Server auf einem anderen Rechner läuft als der INTUS COM Client, dann muss hier der Name oder die IP-Adresse des Rechners eingetragen werden, auf dem der Admin-Server läuft.
3. Der Eintrag in **Port** ist fehlerhaft oder der verwendete **Port** ist durch eine Fremdapplikation belegt. Wenn der Admin-Server auf einem anderen **Port** auf Verbindungen wartet, dann muss hier der richtige **Port** eingetragen sein.

2.4.3 Verbindungstimeout

Ist die Portnummer 13050 durch eine Fremdapplikation belegt, kommt es zu einem Verbindungstimeout. In diesem Fall müssen Sie im Admin-Server eine andere Portnummer einstellen (siehe 2.3.6).

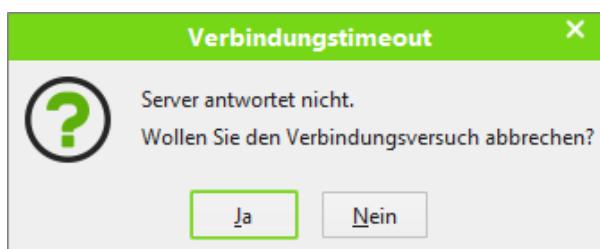


Abbildung 2.26 - Verbindungstimeout

2.4.4 Lizenzeingabe

 Wenn Sie eine Lizenz erworben haben, ist der Lizenzstring auf dem CD-Cover aufgedruckt.

Nach der ersten Installation legt INTUS COM automatisch eine auf 3 Monate begrenzte Testlizenz an. Die Testlizenz ist bis zum Ende des angezeigten Monats gültig. Nach Ablauf dieser

Frist findet keine Kommunikation mehr zwischen den Terminals und dem INTUS COM statt. Die Testlizenz ist auf fünf Terminals limitiert (Haupt- und Subterminals, z.B. fünf INTUS 5300 oder ein ACM40 mit vier I600).

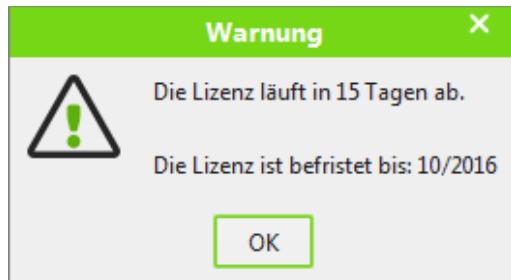


Abbildung 2.27 - Warndialog für befristete Lizenz

Nach der Warnung werden Sie aufgefordert eine gültige Lizenz einzugeben. Geben Sie den String hier ein. Sie können auch direkt OK drücken und die Lizenz später im Menü Hilfe/Über/Lizenz eingeben.



Abbildung 2.28 - Lizenzdialog

Informationen zur Lizenz sehen Sie auch in der Statuszeile am unteren Rand des Hauptfens-ters.

2.5 INTUS COM Installation sichern

Folgende Dateien und Verzeichnisse von INTUS COM sind zu sichern, um die Installation nach einem Rechnerabsturz oder Plattencrash wieder herstellen zu können:

1. Das INTUS COM Arbeitsverzeichnis mit allen Unterverzeichnissen (üblicherweise das Verzeichnis <INTUS COM Installationsverzeichnis>\work, siehe Kapitel 4.8.1)
2. Die INTUS COM Konfigurationsdatei
<INTUS COM Installationsverzeichnis>\conf\admin_server.ini

3 INTUS COM Client Benutzeroberfläche

In diesem Kapitel ist die Benutzeroberfläche des INTUS COM Clients beschrieben. Hier können zum einen fast alle Einstellungen von INTUS COM vorgenommen werden. Zum anderen werden hier der Verbindungs- und Betriebsstatus der INTUS COM Komponenten und der angeschlossenen Terminals, aufgetretene Fehler und Ereignisse angezeigt.

Machen Sie sich in diesem Kapitel mit der Oberfläche und der Bedienung des INTUS COM Clients vertraut. Welche Einstellungen erforderlich sind, um ein Terminalsystem in Betrieb zu nehmen (d.h. die INTUS COM Server und die Terminals zu konfigurieren) ist im nachfolgenden Kapitel 4 beschrieben.



Die Online-Hilfe zum INTUS COM Client kann durch Drücken der Taste F1 aus jedem Fenster aufgerufen werden.

3.1 Hauptfenster des INTUS COM Clients

Das Hauptfenster des INTUS COM Clients besteht aus einer Menüleiste, einer Werkzeugeleiste (Toolbar, siehe 3.3.1), einem Anzeigebereich und einer Statuszeile.

Im Anzeigebereich können verschiedene interne Fenster (siehe Kapitel 3.2) mit unterschiedlichen Informationen gleichzeitig angezeigt werden. Einzelheiten zum Arbeiten mit den Fenstern, zum Anlegen und Löschen von Objekten finden Sie im Kapitel 3.3. Die Fenster können im Anzeigebereich in Abhängigkeit der Bildschirmgröße und der jeweils gewünschten Information ergonomisch frei angeordnet werden. Das Layout und die Anordnung der internen Fenster wird benutzerspezifisch beim Beenden des INTUS COM Clients in der Datei `%user%\intuscom\intuscom_monitor.properties` gespeichert, sodass dasselbe Layout beim erneuten Starten des INTUS COM Clients wieder hergestellt wird.

Das folgende Bild zeigt die Grundanordnung der Fenster beim erstmaligen Starten des INTUS COM Clients. Diese Anzeige kann jederzeit auch über das Menü **Fenster/Defaultlayout** wiederhergestellt werden.

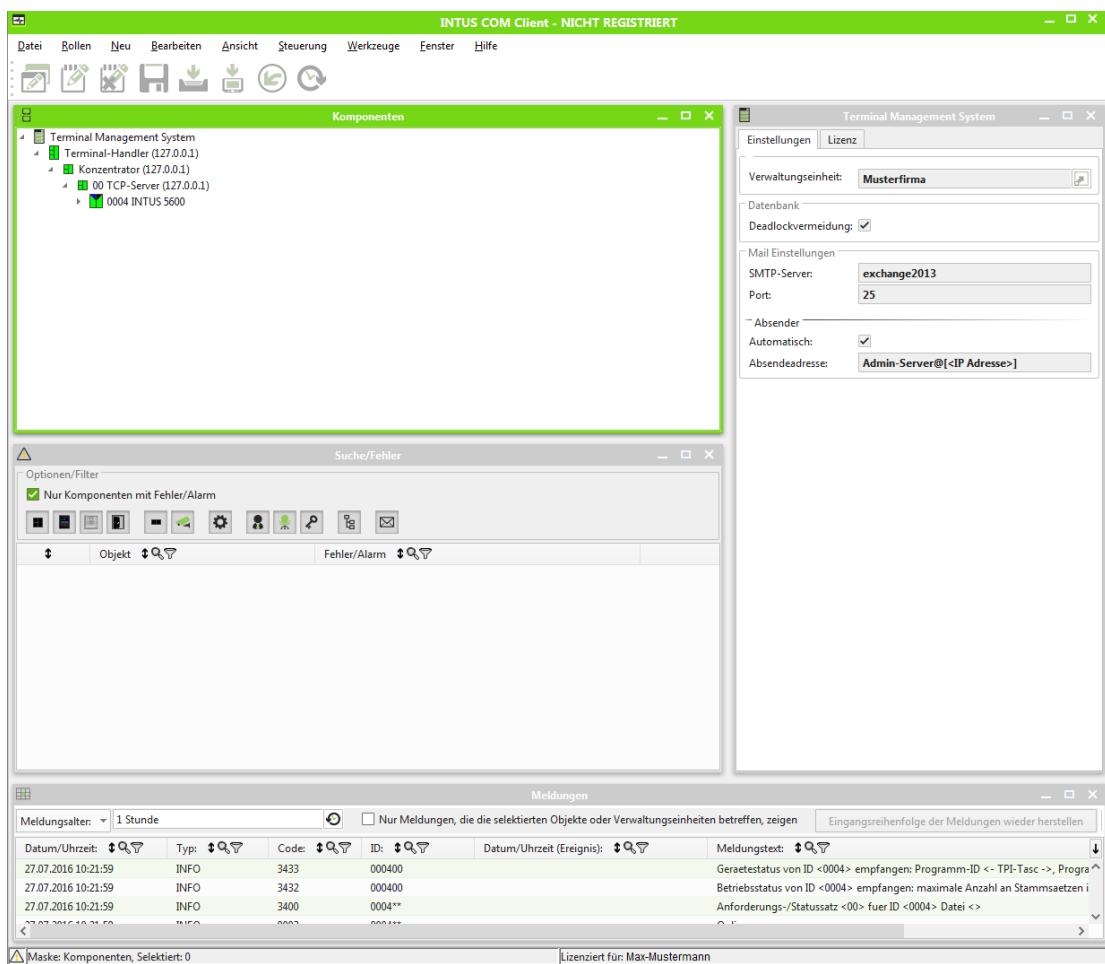


Abbildung 3.1 - Hauptfenster des INTUS COM Client

3.2 Fenstertypen

3.2.1 Verwaltungseinheiten-Fenster

Eine Verwaltungseinheit entspricht einem organisatorischen Teilbereich. Damit kann z.B. ein geografischer Standort, ein Werk, ein Gebäude, eine Etage o.ä. abgebildet werden, indem die Terminals den entsprechenden Verwaltungseinheiten zugeordnet werden. Dies ist insbesondere bei größeren Installationen wünschenswert, da man hier die Übersicht über die Standorte der Terminals im Komponenten-Fenster sehr schnell verliert.

Außer der einmalig verhandenen Wurzelverwaltungseinheit ist jede Verwaltungseinheit einer übergeordneten Verwaltungseinheit zugeordnet und für jede Verwaltungseinheit können beliebig viele untergeordnete Verwaltungseinheiten eingerichtet werden.

Das Fenster **Verwaltungseinheiten** zeigt die Hierarchie der Verwaltungseinheiten sowie die den Verwaltungseinheiten zugeordneten Objekte in einem Baum. INTUS COM gibt weder die Anzahl noch die Bedeutung der einzelnen Ebenen vor.

Objekte folgender Objekttypen werden genau einer Verwaltungseinheit zugeordnet und im Verwaltungsbaum unterhalb dieser dargestellt:

- Terminal Management System
- Terminal-Handler
- Konzentrator
- TCP-Server
- HTTPS-Server
- INTUS 3000/3450 Server
- Video-Interface
- Videoserver
- SeeTec Gateway Service
- PS-Distributor
- AutoClone-Server
- INTUS Terminal/ACM
- Subterminal
- Tür
- Kamera
- Offlineterminal
- Offlineanlage
- Blockllist
- EMail-Einstellung
- Benutzer
- Rolle
- Berechtigung

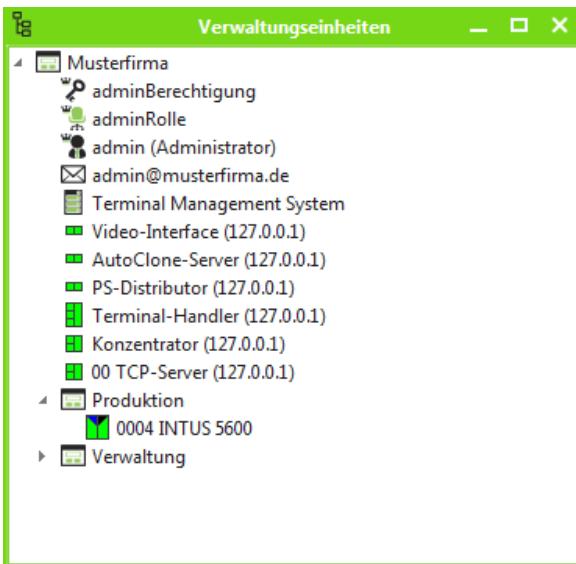


Abbildung 3.2 - Fenster "Verwaltungseinheiten"

Arbeiten mit dem Fenster

Wenn Sie eine Verwaltungseinheit mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration) im aktiven K&S-Fenster angezeigt. Die Konfiguration einer einzelnen Verwaltungseinheit erfolgt im K&S-Fenster (siehe 4.7).

Das Fenster **Verwaltungseinheiten** ist in der Grundeinstellung nicht geöffnet. Wenn das Fenster geschlossen ist, können Sie es im Menü **Fenster** mit dem Punkt **Verwaltungseinheiten** öffnen. Es kann nur ein Verwaltungseinheiten-Fenster geöffnet sein.

Das Verwaltungseinheiten-Fenster hat keinen Änderungsmodus (siehe 3.3.3.2).

Im Kontextmenü einer selektierten Verwaltungseinheit können untergeordnete Verwaltungseinheiten und Objekte der Objekttypen, die einer Verwaltungseinheit zugeordnet werden, hinzugefügt werden.

Es können nur Verwaltungseinheiten entfernt werden, denen keine weiteren Verwaltungseinheiten untergeordnet und keine Objekte zugeordnet sind. Wenn einer Verwaltungseinheit Objekte zugeordnet sind, die nicht entfernt werden können (z.B. AdminBenutzer, AdminRolle, AdminBerechtigung), dann kann diese Verwaltungseinheit auch nicht entfernt werden. Ansonsten erfolgt vor dem Löschen einer Verwaltungseinheit ggf. eine Abfrage, ob alle ihr untergeordneten Verwaltungseinheiten und zugeordneten Objekte gelöscht werden sollen.

3.2.2 Benutzer-Rollen-Berechtigungen-Fenster

INTUS COM Benutzer müssen sich mit Loginname und Passwort anmelden. Abhängig von den Rechten des angemeldeten Benutzers

- werden Komponenten und andere Objekte in den verschiedenen Fenstern dargestellt oder ausgeblendet
- können Operationen auf Komponenten und anderen Objekten zugelassen oder gesperrt werden

Eine Rolle bildet eine Funktion oder Zuständigkeit eines oder mehrerer Benutzer ab. Um Verwechslungen auszuschliessen, sind identische Namen für zwei Rollen nicht zulässig.

In Berechtigungen werden Rechte konfiguriert. Die konfigurierten Rechte können nur auf Objekte, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, angewandt werden.

Durch Berechtigung-Rolle-Zuordnungen erhält eine Rolle verschiedene Rechte auf Objekte einer Verwaltungseinheit (und ggf. untergeordneten Verwaltungseinheiten), die von Benutzern, die der Rolle durch Benutzer-Rolle-Zuordnungen zugeordnet sind, angewandt werden können.

Das Benutzer-Rollen-Berechtigungen-Fenster zeigt die konfigurierten Benutzer, Rollen, Berechtigungen und deren Zuordnungen in drei Bäumen nebeneinander.

Solange noch keine weiteren Benutzer angelegt wurden, kennt INTUS COM nur den Administrator-Benutzer **admin**. Das Passwort für diesen Benutzer ist am Anfang auf **pcs** eingestellt. Der Loginname dieses Benutzer kann nicht verändert werden. Weiter kann dieser Benutzer nicht gelöscht, aber gesperrt werden. Die Krone im Icon  kennzeichnet diesen Benutzer.

Solange noch keine weitere Rolle angelegt wurde, kennt INTUS COM nur die Administrator-Rolle, deren Name beliebig geändert werden kann. Die Administrator-Rolle kann nicht gelöscht werden. Die Krone im Icon  kennzeichnet diese Rolle.

Solange noch keine weitere Berechtigung angelegt wurde, kennt INTUS COM nur die Administrator-Berechtigung, deren Name beliebig geändert werden kann. Die Administrator-Berechtigung ist immer der Wurzelverwaltungseinheit zugewiesen und kann nicht gelöscht werden. Die Rechte der Administrator-Berechtigung können nicht verändert werden, es sind immer alle Rechte vorhanden. Aufgrund der nicht änderbaren Zuordnung zur Wurzelverwaltungseinheit berechtigt die Administrator-Berechtigung somit den vollständigen Zugriff auf alle im INTUS COM Terminal Management System vorhandenen Komponenten und anderen Objekten.

Die Krone im Icon  kennzeichnet diese Berechtigung.

Der Administrator-Benutzer und die Administrator-Berechtigung sind immer (nicht veränderbar) der Administrator-Rolle zugeordnet. Damit hat der Administrator-Benutzer immer alle Rechte für den vollständigen Zugriff auf alle im INTUS COM Terminal Management System vorhandenen Komponenten und andere Objekte.

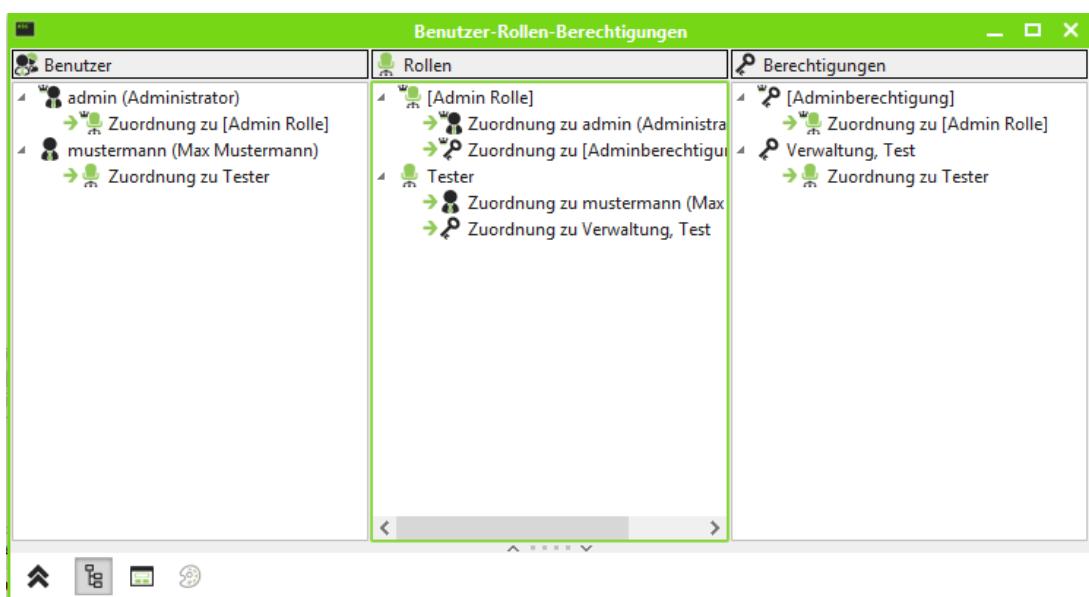


Abbildung 3.3 - Fenster "Benutzer-Rollen-Berechtigungen"

Arbeiten mit dem Fenster

Wenn Sie einen Benutzer, eine Rolle, eine Berechtigung oder eine Zuordnung mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration) im aktiven K&S-Fenster angezeigt. Die Konfiguration eines einzelnen Benutzers, einer einzelnen Rolle, einer einzelnen Berechtigung und einer einzelnen Zuordnung erfolgt im K&S-Fenster (siehe 4.16, 4.17, 4.18, 4.19 und 4.20).

Das Fenster **Benutzer-Rollen-Berechtigungen** ist in der Grundeinstellung nicht geöffnet. Um es zu öffnen, wählen Sie im Menü **Fenster** den Punkt **Benutzer-Rollen-Berechtigungen**. Es kann nur ein Benutzer-Rollen-Berechtigungen-Fenster geöffnet sein.

Im Kontextmenü im Benutzerbereich des Benutzer-Rollen-Berechtigungen-Fensters können **INTUS COM Benutzer** hinzugefügt werden.

Im Kontextmenü im Rollenbereich des Benutzer-Rollen-Berechtigungen-Fensters können **INTUS COM Rollen** hinzugefügt werden.

Im Kontextmenü im Berechtigungsbereich des Benutzer-Rollen-Berechtigungen-Fensters können **INTUS COM Berechtigungen** hinzugefügt werden.

Im Kontextmenü eines selektierten Benutzers können Benutzer-Rolle-Zuordnungen hinzugefügt werden.

Im Kontextmenü einer selektierten Rolle können Benutzer-Rolle-Zuordnungen und Berechtigung-Rolle-Zuordnungen hinzugefügt werden.

Im Kontextmenü einer selektierten Berechtigung können Berechtigung-Rolle-Zuordnungen hinzugefügt werden.

Wenn ein Benutzer den INTUS COM Client gestartet und mit dem INTUS COM Admin-Server verbunden ist, dann können Sie, entsprechende Rechte vorausgesetzt, diese Verbindung im Kontextmenü des selektierten Benutzers mit **Benutzer abmelden ...** trennen.

Das Benutzer-Rollen-Berechtigungen-Fenster hat keinen Änderungsmodus (siehe 3.3.3.2).

Erweiterte Darstellung

Die erweiterte Darstellung, einschaltbar durch Mausklick auf , zeigt unter den Bäumen grafisch die Beziehungen eines/einer im Baum selektierte(n) Benutzers/Rolle/Berechtigung/Zuordnung:

- Ist ein Benutzer selektiert, so werden dieser Benutzer, die ihm zugeordneten Rollen und die diesen Rollen zugewiesenen Berechtigungen gezeigt.
- Ist eine Rolle selektiert, so werden diese Rolle und die der Rolle zugeordneten Benutzer und Berechtigungen gezeigt.
- Ist eine Berechtigung selektiert, so werden diese Berechtigung, die ihr zugeordneten Rollen und die diesen Rollen zugeordneten Benutzer gezeigt.
- Ist eine Berechtigung-Rolle-Zuordnung selektiert, so werden die Berechtigung, die Rolle und die der Rolle zugeordneten Benutzer gezeigt.
- Ist eine Benutzer-Rolle-Zuordnung selektiert, so werden der Benutzer, die Rolle und die der Rolle zugeordneten Berechtigungen gezeigt.

In der erweiterten Darstellung kann die Hierarchie der Verwaltungseinheiten durch Mausklick auf  eingeblendet bzw. ausgeblendet werden. Dabei gibt es die Möglichkeit, alle Verwaltungseinheiten oder nur die, denen die gezeigten Benutzer, Rollen und Berechtigungen zugeordnet sind, darzustellen (Schaltfläche ). Die Farbwahl für die verschiedenen Ebenen der Verwaltungseinheiten kann dem eigenen Vorstellungen und Vorlieben angepasst werden (Schaltfläche ).

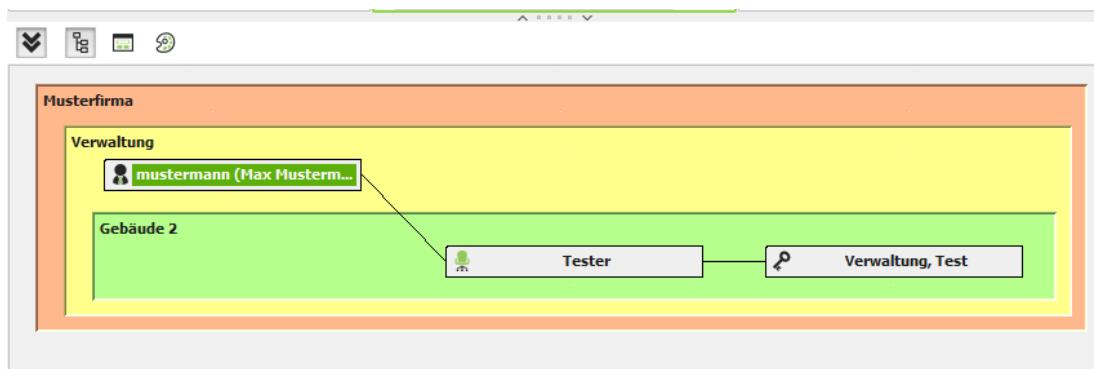


Abbildung 3.4 - Fenster "Benutzer-Rollen-Berechtigungen, erweiterte Darstellung"

3.2.3 Komponenten-Fenster

Im Komponenten-Fenster werden fast alle konfigurierten Hard- und Softwarekomponenten (INTUS Terminals und INTUS COM Server, ausser Videokomponenten, dem PS-Distributor und dem AutoClone Dienst) und ihre Abhängigkeiten voneinander in Form eines Strukturaumes, ähnlich einem Verzeichnisbaum dargestellt.

Außerdem werden der Betriebs- und Verbindungsstatus jeder Komponente farblich gekennzeichnet. Eine Alarmmeldung von einem Terminal wird durch ein Ausrufezeichen neben dem Icon des Terminals angezeigt..

Anhand dieser Struktur ist ersichtlich, wie der Datenfluss (z. B. von Stammdaten und Buchungsdaten) durch INTUS COM verläuft. Eine Buchung wird zum Beispiel vom Terminal zunächst an den Server (TCP-Server, HTTPS-Server oder INTUS 3000/3450 Server) gesendet, an den das Terminal angeschlossen ist. Der Server sendet die Buchung zum Konzentrator weiter und der Konzentrator schließlich zum Terminal-Handler. Dieser speichert die Buchung in einer Datei, Datenbank oder gibt sie direkt über TCP/IP an die Applikation weiter (je nach Konfiguration).



Abbildung 3.5 - Fenster "Komponenten"

Arbeiten mit dem Fenster

Wenn Sie eine Komponente mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration und Status) im aktiven K&S-Fenster (siehe 3.2.8) angezeigt.

Das Fenster **Komponenten** ist im Standardlayout geöffnet. Wenn das Fenster geschlossen ist, können Sie es im Menü **Fenster** mit dem Punkt **Komponenten** öffnen. Es kann nur ein Komponenten-Fenster geöffnet sein.

Im Kontextmenü können neue Komponenten angelegt oder vorhandene gelöscht werden. Außerdem kann der Strukturaum auf- und zugeklappt werden.

Die Komponenten-Fenster hat keinen Änderungsmodus (siehe 3.3.3.2).

Verbindungsstatus

Links im Symbol ist der Verbindungsstatus dargestellt. Beim Verbindungsstatus haben die Farben folgende Bedeutung:

	Grün	online
	Rot	offline (d.h. Verbindungsfehler)
	Schwarz	deaktiviert oder unbekannt
	Blau	nicht verbunden (zeitlich gewollte Trennung) bzw. Verbindung wird gerade hergestellt

Bei den Serverkomponenten ist der Verbindungsstatus normalerweise zweigeteilt:

- Oben: zeigt den Status des Datenports an.
- Unten: zeigt den Status des Serviceports an.

Beim Terminal-Handler ist der Verbindungsstatus dreigeteilt:

- Oben: zeigt den Status des Admin-Datenports an.
- Mitte: zeigt den Status des Datenports an.
- Unten: zeigt den Status des Serviceports an.

Beim INTUS 3000/3450 Server ist der Verbindungsstatus dreigeteilt, wenn die zweite Partyline aktiviert ist:

- Oben: zeigt den Status des zweiten Datenports (Line 1) an.
- Mitte: zeigt den Status des ersten Datenports (Line 0) an.
- Unten: zeigt den Status des Serviceports an.

Bei Sublesern mit Wiegandschnittstelle wird der Verbindungsstatus diagonal zweigeteilt dargestellt, um anzuzeigen, dass bei diesem Lesertyp nur der Verbindungsstatus zur Wiegand-Schnittstelle ermittelt werden kann. Die untere rechte Hälfte des Verbindungsstatus ist immer Schwarz.

Bei Terminals die AutoClone unterstützen wird ein Teil des Verbindungsstatus verwendet um den AutoClone-Verbindungsstatus darzustellen.

Betriebsstatus

Rechts im Symbol ist der Betriebsstatus dargestellt. Beim Betriebsstatus haben die Farben folgende Bedeutung:

	Grün	Terminal bzw. der Server ist betriebsbereit
	Rot	Es liegt eine Fehlersituation vor
	Schwarz	Der Status ist unbekannt
	Blau	Download / Kommunikation – Das Terminal ist noch nicht vollständig geladen bzw. es findet gerade eine Kommunikation mit der Serverkomponente statt.

Bei Terminals die AutoClone unterstützen wird ein Teil des Betriebstatus verwendet um den AutoClone-Betriebsstatus darzustellen.

PS-Controller Status

Subleser mit dem Lesertyp IPS_ und IPSf (INTUS PS) werden als PS-Controller bezeichnet. Bei PS-Controllern werden, zusätzlich zu dem normalen Subterminal Status, der Verbindungs- und Betriebsstatus aus der Sicht des PS-Distributors im Symbol dargestellt. Für die Darstellung eines PS-Controller wird ein Kreis verwendet, um eine Verwechslung mit den Serverkomponenten zu vermeiden.



Die obere Hälfte stellt den Status aus Sicht des PS-Distributors, die untere Hälfte stellt den normalen Subterminalstatus dar. Die Bedeutung der Farben, die zur Darstellung des Status aus Sicht des PS-Distributors verwendet werden, entspricht der Bedeutung der Farben für die Darstellung des Subterminalstatus.

Zusätzliche Status Terminal/Subterminal

Wird dieses Symbol neben einem Terminal oder Subterminal angezeigt, so wurde von diesem Gerät ein Alarmsatz gesendet (Stiller Alarm, Leser offline, usw.).

Dieses Symbol zeigt an, das an dem Gerät der Sabotagekontakt offen ist. D.h.: Das Gehäuse wurde geöffnet.

Türstatus

Das Türsymbol im Komponentenfenster dient der Türstatusüberwachung. Die Türüberwachung muss in der Parametrierung des Terminals bzw. Subterminals berücksichtigt werden.



Türen an INTUS 3000 Hauptterminals und Subterminals werden von INTUS COM nur unterstützt, wenn auf dem Hauptterminal TPI-TASC (mindestens Version 2.51) läuft.

Bei einem Türsymbol zeigt ein hellgrüner Rahmen den Dauertüroffenstatus an

- Tür geschlossen
- Tür geschlossen + Tür daueroffen
- Tür berechtigt offen
- Tür berechtigt offen + Tür daueroffen
- Tür unberechtigt offen
- Automatisches Senden des Türstatus abgeschaltet.
- Tür zulange auf
- Tür offen. Berechtigt oder unberechtigt kann nicht festgestellt werden. (z.B. Die Tür ist offen, während das Terminal hochgefahren wird)
- Tür offen + Tür daueroffen. Berechtigt oder unberechtigt kann nicht festgestellt werden (z.B. Die Tür ist offen, während das Terminal hochgefahren wird.)
- Türstatus unbekannt. (z.B.: Leser ist offline)

3.2.4 Videokomponenten-Fenster

Im Videokomponenten-Fenster werden alle konfigurierten Videoquellen (Convision Videoserver oder SeeTec Gateway Service), Kameras und Kamera-Leser-Zuordnungen und ihre Abhängigkeiten voneinander in Form eines Strukturaumes dargestellt. Videokomponenten wie INTUS COM Videointerface, VideoServer oder SeeTec Gateway Service und Kameras können über das Videokomponenten-Fenster angelegt werden.

Außerdem werden der Betriebs- und Verbindungsstatus der Videokomponenten farblich gekennzeichnet.



Abbildung 3.6 - Fenster "Videokomponenten"

Arbeiten mit dem Fenster

Wenn Sie eine Komponente mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration und Status) im aktiven K&S-Fenster (siehe 3.2.8) angezeigt.

Das Fenster **Videokomponenten** ist in der Grundeinstellung nicht geöffnet. Wenn das Fenster geschlossen ist, können Sie es im Menü **Fenster** mit dem Punkt **Videokomponenten** öffnen. Es kann nur ein Videokomponenten-Fenster geöffnet sein.

Im Kontextmenü können neue Komponenten angelegt oder vorhandene gelöscht werden. Außerdem kann der Strukturaum auf- und zugeklappt werden.

Das Videokomponenten-Fenster hat keinen Änderungsmodus (siehe 3.3.3.2).

Der Verbindungs- und Betriebsstatus des INTUSCOM Video-Interface und des Convision Videoserver bzw. des SeeTec Gateway Service werden analog zum Komponentenfenster dargestellt.

Verbindungsstatus

Links im Symbol ist der Verbindungsstatus dargestellt. Beim Verbindungsstatus haben die Farben folgende Bedeutung:

- | | |
|-----------|--|
| ■ Grün | online |
| ■ Rot | offline (d.h. Verbindungsfehler) |
| ■ Schwarz | deaktiviert oder unbekannt |
| ■ Blau | nicht verbunden (gewollte Trennung) bzw. Verbindung wird gerade hergestellt. |



Die Verbindung zu einem Videoserver wird nur aufgebaut, um Videobilder zu laden.

Betriebsstatus

Rechts im Symbol ist der Betriebsstatus dargestellt. Beim Betriebsstatus haben die Farben folgende Bedeutung:

- | | |
|--------|----------------|
| ■ Grün | Betriebsbereit |
|--------|----------------|

- Rot Es liegt eine Fehlersituation vor
- Schwarz Der Status ist unbekannt
- Blau Download / Kommunikation

3.2.5 PS-Distribution-Fenster

Im Fenster PS-Distribution werden alle konfigurierten PS-Controller angezeigt, für die die Templateverteilung aktiviert ist. Die PS-Controller werden alle unterhalb der PS-Distributor Komponente angezeigt.

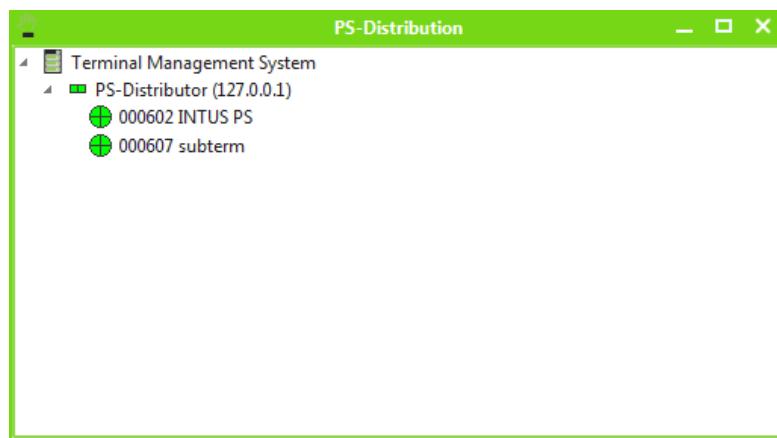


Abbildung 3.7 - Fenster "PS-Distribution"

Arbeiten mit dem Fenster

Wenn Sie eine Komponente mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration und Status) im aktiven K&S-Fenster (siehe 3.2.8) angezeigt.

Das Fenster **PS-Distribution** ist in der Grundeinstellung nicht geöffnet. Wenn das Fenster geschlossen ist, können Sie es im Menü **Fenster** mit dem Punkt **PS-Distribution** öffnen. Es kann nur ein Fenster „PS-Distribution“ geöffnet sein.

Das Fenster PS-Distribution hat keinen Änderungsmodus (siehe 3.3.3.2).

Der Verbindungs- und Betriebsstatus des INTUSCOM PS-Distributor und der PS-Controller werden analog zum Komponentenfenster dargestellt.

3.2.6 AutoClone-Fenster

Im Fenster AutoClone werden alle INTUS Terminals angezeigt, in deren Konfiguration der Parameter "AutoClone-Server" auf den AutoClone-Server verweist. Diese Terminals werden alle unterhalb des AutoClone Dienstes angezeigt.

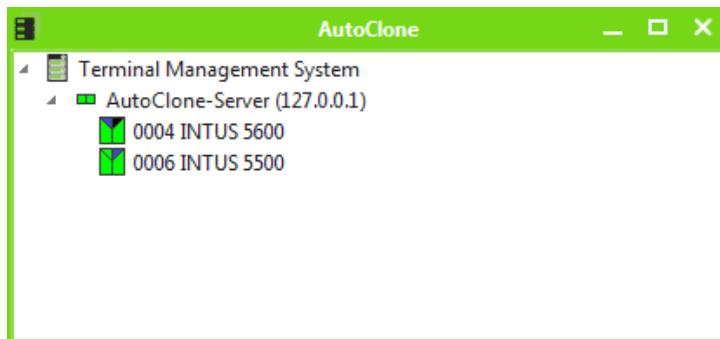


Abbildung 3.8 - Fenster "AutoClone"

Arbeiten mit dem Fenster

Wenn Sie eine Komponente mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration und Status) im aktiven K&S-Fenster (siehe 3.2.8) angezeigt.

Das Fenster AutoClone ist in der Grundeinstellung nicht geöffnet. Wenn das Fenster geschlossen ist, können Sie es im Menü Fenster mit dem Punkt AutoClone öffnen. Es kann nur ein Fenster "AutoClone" geöffnet sein.

Das Fenster AutoClone hat keinen Änderungsmodus (siehe 3.3.3.2).

Der Verbindungs- und Betriebsstatus des INTUSCOM AutoClone und der AuoClone Terminals werden analog zum Komponentenfenster dargestellt.

3.2.7 Offlineanlagen-Fenster

Das Offlineanlagen-Fenster dient der Anzeige von Offlineanlagen mit den ihnen zugeordneten Geräten sowie der Blocklist.

Die Anzeige erfolgt in einer Baumstruktur.

Offlineterminals erscheinen jeweils unter der Offlineanlage, der sie zugeordnet sind.

Terminals/ACMs, die einer Offlineanlage zugeordnet sind, erscheinen auch jeweils unter ihrer Offlineanlage.

Die Blocklist erscheint auf derselben Ebene wie Offlineanlagen. (Die Blocklist gilt Offlineanlagen-übergreifend.)

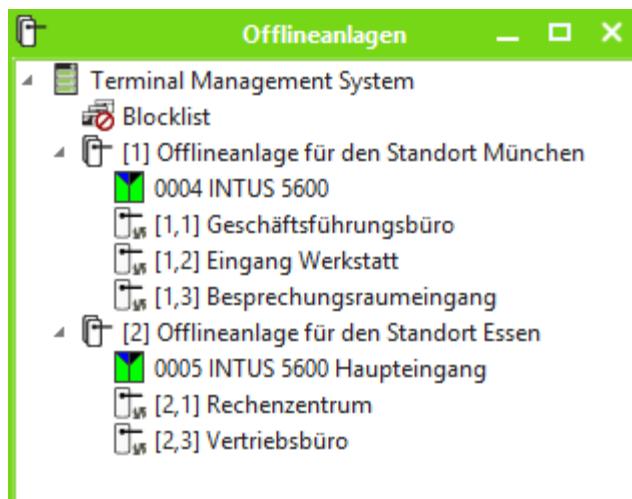


Abbildung 3.9 - Fenster "Offlineanlagen"

Arbeiten mit dem Fenster

Wenn Sie eines der dargestellten Objekte mit der Maus selektieren, dann werden die Detail-Informationen (Konfiguration und Status) im aktiven K&S-Fenster (siehe 3.2.8) angezeigt.

Das Fenster Offlineanlagen ist in der Grundeinstellung nicht geöffnet. Wenn das Fenster geschlossen ist, können Sie es im Menü Fenster mit dem Punkt Offlineanlagen öffnen. Es kann nur ein Offlineanlagen-Fenster geöffnet sein.

Das Offlineanlagen-Fenster hat keinen Änderungsmodus (siehe 3.3.3.2).

Konfigurationsstatus

Das kleine Icon neben dem Icon eines Offlineterminals bedeutet, dass der Konfigurationsstatus des Offlineterminals nicht mit der Konfiguration übereinstimmt. Dies kann darauf hinweisen, dass ein oder mehrere konfigurierte Werte noch nicht in die Offlineterminal-Hardware übertragen wurden oder dass das Konfigurationsergebnis (Configuration Result) einer solchen Übertragung noch nicht importiert wurde.

Wenn Sie herausfinden möchten, welche Parameterwerte nicht zusammenpassen, wählen Sie bitte das Offlineterminal aus und lassen es in einem K&S-Fenster anzeigen. Im K&S-Fenster werden die Parameter, deren Werte nicht zusammenpassen, mit dem Icon markiert.

Informationen dazu, wie Konfigurationsergebnisse importiert und Konfigurationsstatus aktualisiert werden, können Sie unter 3.4.18 finden.

3.2.8 K&S-Fenster

Im Fenster **Konfiguration und Status (K&S-Fenster)** erhalten Sie nähere Informationen zu dem jeweils selektierten Objekt. Die angezeigte Maske ist abhängig vom selektierten Objekt und ist jeweils bei dem Objekt beschrieben:

- Verwaltungseinheit, siehe 4.7
- Terminal Management System, siehe 4.6
- Terminal-Handler, siehe 4.8
- Konzentrator, siehe 4.9
- TCP-Server, siehe 4.10
- HTTPS-Server, siehe 4.11
- INTUS 3000/3450 Server, siehe 4.12
- Video-Interface, siehe 4.21
- Convision Videoserver, siehe 4.22
- Cayuga SGS (SeeTec Gateway Service)
- PS-Distributor, siehe 4.25

- AutoClone-Server, siehe 4.26
- INTUS Terminal/ACM, siehe 4.13
- Subterminal, siehe 4.14
- Tür, siehe 4.15
- Kamera, siehe 4.23
- Kamera-Leser-Zuordnung, siehe 4.24
- Email-Einstellung, siehe 4.27 und 3.4.10
- Benutzer, siehe 4.16
- Rolle, siehe 4.17
- Berechtigung, siehe 4.18
- Benutzer-Rolle-Zuordnung, siehe 4.19
- Berechtigung-Rolle-Zuordnung, siehe 4.20
- Offlineanlage, siehe 4.284.20
- Offlineterminal, siehe 4.29
- Blocklist, siehe 4.30

Die verfügbaren Konfigurations- und Statusdaten werden dann je nach selektierter Komponente auf verschiedenen Registerkarten in dem K&S-Fenster angezeigt.:

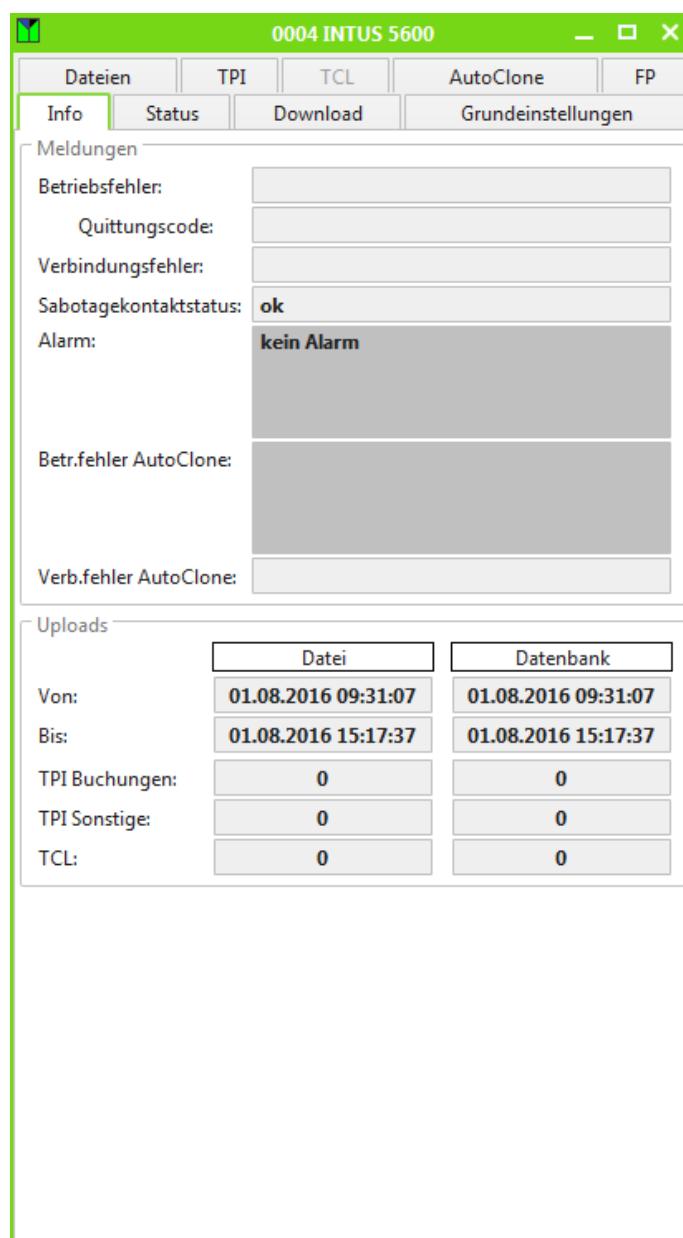


Abbildung 3.10 - K&S Fenster

Arbeiten mit dem Fenster

Das Fenster Konfiguration und Status (K&S-Fenster) ist in der Grundeinstellung geöffnet. Um ein K&S-Fenster zu öffnen, wählen Sie im Menü Fenster den Punkt neues Konfigurations-/Statusfenster. Die Größe eines K&S-Fenster ist änderbar, es gibt allerdings eine vorgegebene Mindestgröße, die nicht unterschritten werden kann.

Es können mehrere K&S-Fenster gleichzeitig geöffnet sein. Das Fenster, welches den Fokus hat, ist das aktive Fenster. Wenn sie in einem anderen Fenster eine Komponente selektieren, dann werden die Detailinformationen zu dieser Komponenten in diesem Fenster dargestellt.

Um die Konfiguration eines Objekts ändern zu können, müssen Sie das K&S-Fenster in den Änderungsmodus versetzen (siehe 3.3.2). Im Änderungsmodus reagiert das K&S-Fenster nicht auf die Auswahl in anderen Fenstern (z.B. Komponenten).

3.2.9 Suche/Fehler-Fenster

Das Fenster Suche/Fehler zeigt die Objekte des Verwaltungsbäums (siehe 3.2.1) und ggf. deren Fehlerzustand in einer Liste. Diese Liste wird dynamisch aktualisiert. Die Spaltenköpfe können zum Sortieren der Objekte verwendet werden. Alle Spalten mit Text können nach Zeichenketten durchsucht werden.

Ist das Häkchen „Nur Komponenten mit Fehler/Alarm“ gesetzt, sind alle Objekte, die nicht in einem Fehlerzustand sind, ausgeblendet. Auf diese Weise können ausgefallene Komponenten schnell erkannt werden. Wenn keine gezielte Suche nach Objekten durchgeführt wird, ist es sinnvoll, dieses Fenster mit dieser Einstellung dauerhaft geöffnet zu lassen.

Objekte eines Typs, deren zugehöriger ToggleButton nicht gedrückt ist, sind ebenfalls ausgeblendet.

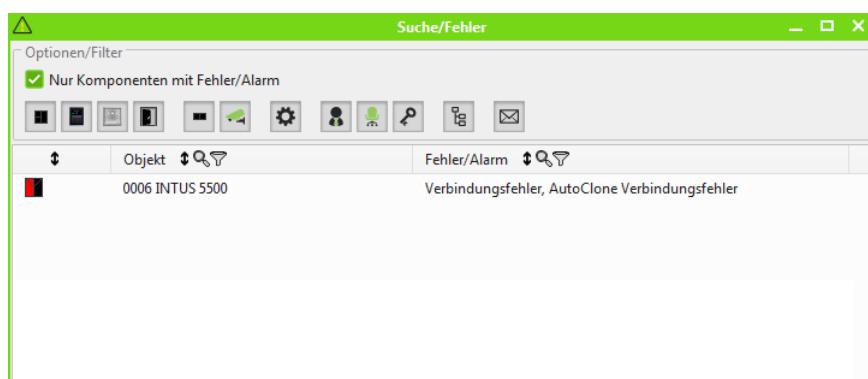


Abbildung 3.11 - Fenster "Fehler"

Arbeiten mit dem Fenster

Das Suche/Fehler-Fenster ist in der Grundeinstellung geöffnet. Um es zu öffnen, wählen Sie im Menü Fenster den Punkt Suche/Fehler. Es kann nur ein Suche/Fehler-Fenster geöffnet sein.

 Wenn das Suche/Fehler-Fenster nicht geöffnet ist und es tritt ein Fehlerzustand bei einer Komponente ein, so wird in der Statuszeile die Schaltfläche  eingeblendet um auf den Fehlerzustand hinzuweisen. Über diese Schaltfläche wird das Suche/Fehler-Fenster geöffnet.

Wenn Sie eine Komponente oder ein anderes Objekt mit der Maus in dem Fenster selektieren, dann werden die Detail-Informationen (Konfiguration und Status) im aktiven K&S-Fenster (siehe 3.2.4) angezeigt.

Detaillierte Fehlerinformationen finden Sie auch im Meldungs-Fenster (3.2.10).

Das Suche/Fehler-Fenster hat keinen Änderungsmodus.

3.2.10 Meldungs-Fenster

Meldungen werden von den Terminals oder den Serverkomponenten erzeugt, wenn bestimmte Ereignisse eintreten oder bestimmte Vorgänge gestartet oder beendet werden, insbesondere auch in Fehlersituationen. Meldungen machen den zeitlichen Ablauf bestimmter Vorgänge sichtbar, z. B. das Laden eines Terminals mit Daten aus verschiedenen Dateien.



Die Anzahl der Meldungen beeinflusst die Performance und den Speicherverbrauch des INTUS COM Clients. Eine zu hohe Einstellung kann abhängig von der Leistung des Rechners zu einem Performanceeinbruch führen. Die Anzahl der vom Client gehaltenen Meldungen ist abhängig von der Einstellung für das Meldungsalter oder den Zeitraum, für den Meldungen angezeigt werden sollen (siehe Filter).

Meldungen						
Meldungsalter:	2 Tage	Typ:	INFO, WARN, ERROR	Code:	ID:	Meldungstext:
Datum/Uhrzeit:	↓ ↗	Typ:	↓ ↗	Code:	↓ ↗	Datum/Uhrzeit (Ereignis): ↓ ↗
02.08.2016 11:41:30		INFO		0002		0004**
02.08.2016 11:41:18		ERROR		3643		0004**
02.08.2016 11:41:18		INFO		3433		000400
02.08.2016 11:41:18		INFO		3432		000400
02.08.2016 11:41:18		INFO		3400		0004**
02.08.2016 11:41:18		INFO		3400		0004**
02.08.2016 11:41:18		INFO		0003		0004**
02.08.2016 11:41:16		ERROR		0001		0004**
02.08.2016 11:40:15		INFO		0002		0004**
02.08.2016 11:40:04		ERROR		3643		0004**
02.08.2016 11:40:04		INFO		3433		000400
02.08.2016 11:40:03		INFO		3432		000400

Abbildung 3.12 - Fenster "Meldungen"

Die einzelnen Felder haben folgenden Inhalt:

Feld	Bedeutung
Datum/Uhrzeit	Zeitpunkt, zu dem das Ereignis eingetreten ist
Typ	INFO, WARN oder ERROR
Code	Interner Meldungscode
ID	Server-, Terminal- und Subterminal-ID des/der Terminals/Subterminals/Tür, auf welche(s) sich die Meldung bezieht
Meldungstext	Meldungstext, Inhalt der Meldung

Tabelle 3.1 – Meldungsanzeige im INTUS COM Client

Sortierung

Das Meldungs-Fenster verwendet zur Anzeige der Meldungen eine Tabelle.

Die Spaltenköpfe können zum Sortieren der Meldungen verwendet werden. Durch Mausklick auf / / im Spaltenkopf kann die Sortierung je nach Spaltenkopf geändert werden. Durch mehrfachen Mausklick wird die Sortierrichtung zwischen aufsteigend und absteigend gewechselt.

Außerdem können die Meldungen in der Reihenfolge, wie sie beim Terminal Management System eingetroffen sind, angezeigt werden (Schaltfläche „Eingangsreihenfolge der Meldungen wieder herstellen“).

Neue Meldungen werden entsprechend der aktuellen Sortierung eingefügt.

Filter

Der Zeitraum, für den die beim Admin-Server eingegangene Meldungen zum INTUS COM Client weitergeleitet werden, ist entweder durch

- Zeitraum (angegeben durch Beginn- und Ende-Datum/Uhrzeit)

oder

- Meldungsalter (angegeben durch eine Zeitspanne)

eingestellt. Bei der Einstellung durch ein Meldungsalter werden neue Meldungen dem Meldungs-Fenster dynamisch hinzugefügt. Alte Meldungen, die das Meldungsalter überschritten haben, werden dynamisch aus dem Meldungs-Fenster entfernt.

Ist das Häkchen „Nur Meldungen, die die selektierten Objekte oder Verwaltungseinheiten betreffen, zeigen“ gesetzt, werden alle Meldungen, die keinem aktuell selektiertem Objekt zugeordnet werden können, ausgeblendet.

Export

Die angezeigten Meldungen können als kommagetrennte Liste in eine Datei exportiert werden (*.csv-Datei).

Um die Meldungen aus dem Meldungs-Fenster zu exportieren, gibt es zwei Möglichkeiten:

1. Wählen Sie bei aktiviertem Meldungs-Fenster im Menü Datei den Punkt Daten exportieren.
2. Wählen Sie bei aktiviertem Meldungs-Fenster in der Werkzeugleiste die Schaltfläche  Daten exportieren.

Suche

Alle Tabellenspalten können durch Mausklick auf  nach Zeichenketten durchsucht werden.

Das Meldungs-Fenster ist in der Grundeinstellung geöffnet. Um das Meldungs-Fenster zu öffnen, wählen Sie im Menü Fenster den Punkt Meldungen. Es kann nur ein Meldungs-Fenster geöffnet sein.

Das Meldungs-Fenster hat keinen Änderungsmodus.

3.2.11 Lageplan-Fenster

Jeder Verwaltungseinheit (siehe 3.2.1) ist ein Lageplan zugeordnet, dessen Hintergrundbild im K&S-Fenster der Verwaltungseinheit (siehe 4.7) konfiguriert wird. Die verwendeten Hintergrundbilder müssen im jpg-Format in dem Unterverzeichnis `\maps` des INTUS COM Installationsverzeichnisses liegen. Ein sinnvolles Hintergrundbild wäre z.B. ein Gebäude-Grundriss.

Im Lageplan-Fenster können die Hardware-Komponenten, die der Verwaltungseinheit zugewiesen sind, auf dem Hintergrundbild nach Installationsorten angeordnet werden.

Folgende Hardware-Komponenten sind auf Lageplänen sichtbar:

- INTUS Terminal / ACM Zutrittsmanager
- Subterminals
- INTUS 3000/3450 Server
- Türen
- Convision Videoserver
- Kameras

In einem Lageplanfenster werden die Hardware-Komponenten als Icons vor der Hintergrundgrafik dargestellt. Die Icons können vom Benutzer nicht geändert werden. Die Icons verwenden die selbe Farbkodierung für den Betriebs- und Verbindungsstatus, wie die Symbole im Komponenten-Fenster (siehe 3.2.3). Eine Alarmmeldung eines Terminals wird nicht wie im Komponenten-Fenster durch ein Ausrufezeichen, sondern durch Blinken des Icons angezeigt.

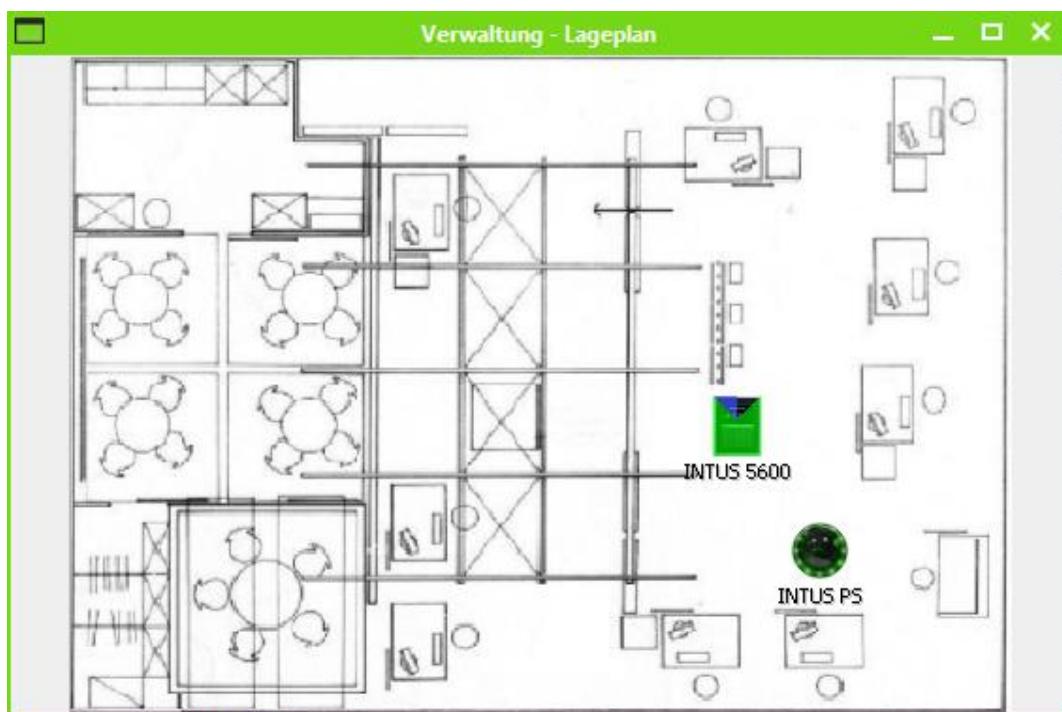


Abbildung 3.13 - Fenster "Lageplan"

Arbeiten mit dem Fenster

Lageplan-Fenster sind in der Grundeinstellung nicht geöffnet. Um ein neues Lageplan-Fenster zu öffnen, wählen Sie im Menü **Fenster** den Punkt **neues Lageplanfenster**. In der Titelzeile eines Lageplan-Fensters wird der Name der zugehörigen Verwaltungseinheit angezeigt.

Es können mehrere Lageplanfenster im Anzeigebereich des INTUS COM Client geöffnet werden. Dadurch können z.B. Terminals in mehreren Etagen angezeigt werden.

Die Größe des Lageplanfensters kann vom Anwender verändert werden. Die Hintergrundgrafik wird entsprechend der Fenstergröße skaliert. Dabei bleibt das Verhältnis von Breite und

Höhe gewahrt. Die Größe der Icons und der Beschriftung wird nicht skaliert, wohl aber deren Position.

Anzeigemodus

Im Anzeigemodus erlaubt das Lageplanfenster die Selektion von Hardware-Komponenten. Die Selektion mehrerer Geräte ist möglich.

Änderungsmodus

Im Änderungsmodus können die Positionen der Terminals und Subterminals mit der Maus verschoben werden („Drag and Drop“). Anders als beim K&S-Fenster gilt der Änderungsmodus für alle geöffneten Lageplanfenster gleichzeitig. Damit ist es möglich, ein Terminal per Drag and Drop von einem Lageplan in den anderen zu verschieben. Dies entspricht der Zuordnung des Terminals zu einer anderen Verwaltungseinheit.

Zum Einstellen und Verlassen des Änderungsmodus siehe 3.3.3.2.

Türstatus

Die Türsymbole im Lageplanfenster haben folgende Bedeutung:

-  Tür geschlossen
-  Tür geschlossen + Tür daueroffen
-  Tür berechtigt offen
-  Tür berechtigt offen + Tür daueroffen
-  Tür unberechtigt offen
-  Automatisches Senden des Türstatus abgeschaltet.
-  Tür zulange auf
-  Tür offen. Berechtigt oder unberechtigt kann nicht festgestellt werden. (z.B. Die Tür ist offen während das Terminal hochgefahren wird.)
-  Tür offen + Tür daueroffen. Berechtigt oder unberechtigt kann nicht festgestellt werden. (z.B. Die Tür ist offen, während das Terminal hochgefahren wird.)
-  Türstatus unbekannt. (z.B.: Leser ist offline)



Für den Türstatus wird TPI-TASC Version 2.51 oder neuer benötigt.

Zur Konfiguration von Türen siehe 4.15

3.3 Bedienung

Im INTUS COM Client gibt es in der Regel drei Möglichkeiten, eine Operation durchzuführen: über die Menüleiste, über die Werkzeugleiste oder das Kontextmenü eines selektierten Objekt bzw. eines Fensters.



Bitte beachten Sie, dass einzelne Menüpunkte und Schaltflächen der Werkzeugleiste deaktiviert sind, wenn sie im jeweiligen Kontext nicht zugelassen sind oder der angemeldete Benutzer nicht über die erforderliche Berechtigung verfügt.

3.3.1 Menüleiste

3.3.1.1 Datei

Neues Fenster	Öffnet ein weiteres INTUS COM Client Hauptfenster für den selben Benutzer.
Daten exportieren	siehe 3.2.10
verbindung trennen	Trennt die Verbindung zum Admin-Server, um eine neue Sitzung (z.B. unter einem anderen Benutzernamen) zu starten
Beenden	Beendet den INTUS COM Client.

3.3.1.2 Rollen

Für jede dem angemeldeten Benutzer zugewiesene Rolle gibt es einen Menüpunkt, mit dem die jeweilige Rolle aktiviert oder deaktiviert werden kann.

3.3.1.3 Neu

Alle Menüpunkte in diesem Menü dienen dazu ein neues Objekt anzulegen, siehe 3.3.4

3.3.1.4 Bearbeiten

Ausschneiden...	Das oder die markierten Objekte ausschneiden, siehe 3.3.7.
Kopieren	Das oder die markierten Objekte kopieren, siehe 3.3.7.
Einfügen...	Das oder die markierten Objekte einfügen, siehe 3.3.7.
Löschen...	Das oder die markierten Objekte löschen, siehe 3.3.6.
Änderungsmodus	Den Änderungsmodus für die selektierte Komponente aktivieren, siehe 3.3.3.2.
Änderungen verwerfen	Änderungsmodus ohne Speichern der Änderungen verlassen, siehe 3.3.3.2.
Änderungen speichern	Änderungen speichern und Änderungsmodus verlassen, siehe 3.3.3.2.
Aktivieren...	Aktiviert die markierten Komponenten,
Deaktivieren...	Deaktiviert die markierten Komponenten.
Eigenes Passwort...	Öffnet Dialog zum Ändern des Passworts.
Lizenz...	Zeigt Dialog zum Ändern der Lizenz.

3.3.1.5 Ansicht

Werkzeugleiste	Es kann die Symbolgröße für die Toolbar eingestellt werden.
Baum vollständig aufklappen	Klappt den Strukturbau in Fenstern mit Baumdarstellung vollständig auf (zeigt alle Objekte an)
Baum vollständig zu klappen	Klappt den Strukturbau in Fenstern mit Baumdarstellung vollständig zu (nur die Komponenten der obersten Ebenen werden angezeigt)

3.3.1.6 Steuerung

Serviceport neu verbinden...	Die Verbindung des Admin-Servers zum Serviceport wird getrennt und neu hergestellt.
Testmodus ein...	Der Testmodus bewirkt beim Konzentrator und TCP-Server, dass diese nach unten hin Verbindungen aufbauen, auch wenn sie nach oben (in Richtung Applikation) keine Verbindung haben. Der Testmodus wird automatisch abgeschaltet, wenn die Verbindung am Serviceport verloren geht.
Testmodus aus...	
AutoClone Download starten...	Öffnet einen Dialog zur Auswahl und Durchführung eines AutoClone Downloads.
Download starten...	Startet einen Download in ein Terminal
Download stoppen...	Beendet bzw. unterbricht einen laufenden Download in ein Terminal
Download planen...	Öffnet einen Dialog um einen zeitversetzten Download für das markierte Terminal zu planen.
Geplanten Download entfernen...	Entfernt den geplanten Download des markierten Terminal.
Reset...	Löst ein Terminal-Reset aus, siehe 3.4.1
FP-Templates neu laden...	Startet den Download von Fingerprint-Templates in ein Haupt- bzw. Subterminal
PS-Templates neu laden...	Startet den Download von PS-Templates auf einen PS-Controller (Subterminal mit Subterminaltyp INTUS PS)
Batteriezustand abfragen...	Fragt den Batteriezustand ab, siehe 3.4.7
AutoClone Status zurücksetzen...	Setzt den AutoClone Status, einschließlich des Passwortes, für das ausgewählte Terminal im AutoClone Dienst auf Standardwerte zurück.
Uhrzeit stellen...	Synchronisiert die Uhrzeit, siehe 3.4.12
Dialog mit Terminal...	Öffnet den Terminaldialog, siehe 3.4.13
Statusseite anfordern...	Fordert die Terminal-Statusseite des markierten Terminals an und zeigt sie in einem Dialogfenster an.
 Die Terminal-Statusseite kann nur für INTUS Terminals/ACM, die an einem INTUS COM TCP-Server konfiguriert sind, angefordert werden.	
Einzeltüröffnung...	Sendet einen Steuersatz an die markierten Terminals, um eine Einzeltüröffnung auszulösen.
Dauertüröffnung...	Sendet einen Steuersatz an die markierten Terminals, um eine Dauertüröffnung auszulösen.
Dauertüröffnung beenden...	Sendet einen Steuersatz an die markierten Terminals, um eine bestehende Dauertüröffnung zu beenden.
Benutzer abmelden...	Meldet den markierten Benutzer vom System ab.

3.3.1.7 Werkzeuge

Netzwerk Terminalsuche...	Öffnet den Dialog zur Suche nach INTUS Terminals in einem TCP/IP Netzwerk, siehe 3.4.11
Terminalimport...	Öffnet den Dialog zum Import von Netzwerk-Terminals über csv-Datei, siehe 4.13.1

Export der Offline Terminal Konfiguration...
Import der Offline Terminal Konfigurationsergebnisse...

Öffnet den Dialog zum Export von Offlineterminal-Konfigurationsdaten in eine XML-Datei; siehe 3.4.17
 Öffnet den Dialog zum Import von Offlineterminal-Konfigurationsergebnissen aus einer XML-Datei; siehe 3.4.18

3.3.1.8 Fenster

Defaultlayout	Stellt die Standard Fensteranordnung wieder her, siehe 3.1
Neues Konfigurations-/Statusfenster	Öffnet ein (weiteres) K&S-Fenster, siehe 3.2.8
Neues Lageplanfenster	Öffnet ein (weiteres) Lageplan-Fenster, siehe 3.2.11
Komponenten	Öffnet das Komponenten-Fenster, siehe 3.2.3 Fehler! Verweisquelle konnte nicht gefunden werden.
verwaltungseinheiten	Öffnet das Verwaltungseinheiten-Fenster, siehe 3.2.1.
Videokomponenten	Öffnet das Fenster Videokomponenten, siehe 3.2.4.
Suche/Fehler	Öffnet das Suche/Fehler-Fenster, siehe 3.2.9.
Meldungen	Öffnet das Meldungs-Fenster, siehe 3.2.10.
PS-Distribution	Öffnet das PS-Distribution-Fenster, siehe 3.2.5.
AutoClone	Öffnet das AutoClone-Fenster, siehe 3.2.6.
Benutzer-Rollen-Berechtigungen	Öffnet das Benutzer-Rollen-Berechtigungen-Fenster, siehe 3.2.2

3.3.1.9 Hilfe

Inhalt	Gibt das Inhaltsverzeichnis der Online-Hilfe aus.
Hilfe	Gibt kontextbezogene Online-Hilfe aus.
Über...	Zeigt die INTUS COM Version und Lizenz an.

3.3.2 Werkzeugeiste (Toolbar)

Im Hauptfenster ist eine Werkzeugeiste (Toolbar) mit folgenden Schaltflächen vorhanden. Die Schaltflächen sind nur dann aktiv, wenn ein Fenster aktiv ist, in dem die Funktion zur Verfügung steht.



Fenster im Änderungsmodus in den Vordergrund (siehe 3.3.3.2)



Fenster in den Änderungsmodus schalten (siehe 3.3.3.2)



Änderungsmodus beenden und Änderungen verwerfen (siehe 3.3.3.2)



Änderungsmodus beenden und Änderungen speichern (siehe 3.3.3.2)



Meldungen aus dem Meldungs-Fenster als kommagetrennte Liste in eine *.csv-Datei exportieren (siehe 3.2.10).



Download-Dialog für selektiertes Terminal aufrufen (siehe 3.4.2)



Reset-Dialog für selektiertes Terminal aufrufen (siehe 3.4.1)



Uhrzeit in selektiertem Terminal synchronisieren (siehe 3.4.12).

3.3.3 Anzeige- und Änderungsmodus

Fenster können sich im Anzeigemodus oder im Änderungsmodus befinden. Es kann sich jeweils nur ein K&S-Fenster im Änderungsmodus befinden.

3.3.3.1 Anzeigemodus

Normalerweise befinden sich alle Fenster des INTUS COM Clients im Anzeigemodus.

Der Anzeigemodus dient der Statusüberwachung der Komponenten des INTUS COM. Im Anzeigemodus können über das Kontextmenü Operationen (z.B. einen Reset für ein Terminal auslösen) auf die Komponenten angewendet werden.

Änderungen an der Konfiguration einer Komponente sind jedoch nicht möglich. Dazu muss in den Änderungsmodus gewechselt werden.

3.3.3.2 Änderungsmodus

Im Änderungsmodus kann die Konfiguration eines Objektes oder eines Lageplans geändert werden. Er ist nur in K&S-Fenstern (siehe 3.2.8) und Lageplan-Fenstern (siehe 3.2.11) verfügbar.

Im Änderungsmodus können keine Operationen (z.B. ein Reset an einem Terminal) auf Komponenten angewendet werden.

Änderungsmodus aktivieren

- Wählen Sie im Menü Bearbeiten den Punkt Änderungsmodus.
- Betätigen Sie die Schaltfläche  in der Werkzeugeiste.
- Wählen Sie im Kontextmenü des K&S-Fenster den Punkt Änderungsmodus.



Sie können nicht in den Änderungsmodus eines Fensters wechseln, so lange sich noch ein anderes Fenster im Änderungsmodus befindet. Alle entsprechenden Menüpunkte und Schaltflächen sind deaktiviert.

Sie müssen zuerst den Änderungsmodus in diesem anderen Fenster explizit beenden. Wenn es von anderen Fenstern verdeckt sein sollte, können Sie es mit der Schaltfläche  in der Werkzeugeiste in den Vordergrund holen.

Wenn der INTUS COM Client auf mehreren Rechnern gleichzeitig gestartet ist und ein anderer Benutzer ein Fenster im Änderungsmodus geöffnet hat, können Sie nicht in den Änderungsmodus wechseln. Sie erhalten dann folgende Meldung:

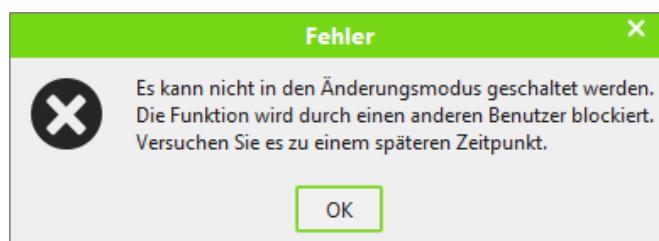


Abbildung 3.14 - Fehlermeldung "Änderungsmodus nicht verfügbar"

Änderungsmodus verlassen

- Wählen Sie im Menü Bearbeiten den Punkt Änderungen verwerfen oder Änderungen speichern.
- Betätigen Sie die Schaltfläche  (Verwerfen) oder  (Speichern) in der Werkzeugeiste.
- Wählen Sie im Kontextmenü des K&S-Fenster den Punkt Änderungen verwerfen oder Änderungen speichern.

Wie Änderungen durchgeführt werden

Sind die Änderungen zulässig, werden sie vom Admin-Server übernommen und zentral gespeichert. Das K&S-Fenster wird in den Anzeigemodus zurückversetzt, und die Änderungen erscheinen in der Anzeige. Der Admin-Server sendet die Konfigurationsänderung über den Serviceport an die betroffenen Komponenten.



Wenn eine Komponente deaktiviert oder offline ist, kann der Admin-Server die Konfigurationsänderung an diese Komponente nicht übertragen. Er holt dies nach, sobald die Voraussetzungen dafür erfüllt sind.

Dies gilt nicht für die Änderung der Port-Nummer. Dazu muss diese Komponente online sein. Änderungen an den Setup-Einstellungen für ein TCL-Terminal werden nicht sofort wirksam auch wenn Terminal-Handler und Terminal online sind, sondern sie gelangen erst im Zuge des nächsten TCL Programmdownloads durch den Terminal-Handler auf das Terminal.

Die Einstellung der TCP/IP-Parameter im INTUS Terminal/ACM oder INTUS 3000/3450 Server wird nicht vom Admin-Server zwischengespeichert. Sie können nur online erfolgen.

3.3.4 Hinzufügen eines neuen Objekts

Ein neues Objekt kann nur im Änderungsmodus (siehe 3.3.3.2) hinzugefügt werden.

Um eine neuen Objekt in die Konfiguration aufzunehmen, verfahren Sie folgendermaßen:

1. Wählen Sie im Menü **Neu** den Typ der neuen Komponente. (Alternativ dazu können Sie auch im Kontextmenü der übergeordneten Komponente (also z. B. zum Anlegen eines Terminals im Kontextmenü des Servers) **Neu** und den Typ der neuen Komponente wählen.) Im aktiven K&S-Fenster erscheint die Konfiguration für das neue Objekt (wenn kein K&S-Fenster vorhanden ist, wird automatisch eines geöffnet).
2. Ändern Sie die Einstellungen des Objekts im K&S-Fenster. (Die Konfigurationsmöglichkeiten der einzelnen Objekte sind in eigenen Abschnitten dieser Dokumentation beschrieben.)
3. Speichern Sie die Änderungen. Wenn die Änderungen zulässig sind, wird das K&S-Fenster wieder in den Anzeigemodus zurückversetzt. Ansonsten erscheint eine Fehlermeldung.

3.3.5 Ändern der Konfiguration eines Objekts

Die Konfiguration eines Objekt kann nur im Änderungsmodus (siehe 3.3.3.2) durchgeführt werden.

Die Konfiguration für ein Objekt kann folgendermaßen geändert werden:

1. Wählen Sie das Objekt in einem Fenster (z.B.: Komponenten). Das Objekt wird jetzt im aktiven K&S-Fenster angezeigt.
2. Setzen Sie den Fokus auf das K&S-Fenster und wählen Sie im Menü **Bearbeiten** den Punkt **Änderungsmodus** (Alternativ dazu können Sie auch den Punkt **Konfigurieren** im Kontextmenü wählen). Daraufhin wird das K&S-Fenster in den Änderungsmodus versetzt.
3. Ändern Sie die Einstellungen im K&S-Fenster. (Die Konfigurationsmöglichkeiten der einzelnen Objekte sind in eigenen Abschnitten dieser Dokumentation beschrieben.)
4. Speichern Sie die Änderungen beim Beenden des Änderungsmodus. Wenn die Änderungen zulässig sind, wird das K&S-Fenster wieder in den Anzeigemodus zurückversetzt. Ansonsten erscheint eine Fehlermeldung.

3.3.6 Löschen eines oder mehrerer Objekte

Zum Löschen eines oder mehrerer Objekte darf sich kein Fenster im Änderungsmodus (siehe 3.3.3.2) befinden.

Wenn Sie Objekte löschen möchten, verfahren Sie folgendermaßen:

1. Wählen Sie das oder die Objekte die Sie löschen möchten in einem Fenster (z.B: Komponenten) aus. Beachten Sie, dass immer nur gleichartige Objekte (z.B: Terminals) gleichzeitig ausgewählt werden können.
2. Wählen Sie im Menü **Bearbeiten** den Punkt „**Löschen ...**“ (Alternativ dazu können Sie auch den Punkt „**Löschen ...**“ im Kontextmenü wählen.)
3. Die zu löschenenden Objekte werden in dem folgenden Dialog aufgelistet. Bestätigen Sie das Löschen des oder der Objekte im angezeigten Dialog.

Terminal-Management-System, Terminal-Handler, Konzentrator, Wurzelverwaltungseinheit, Admin-Benutzer, AdminRolle, AdminBerechtigung, AdminBenutzer-Admin-Rolle-Zuordnung und AdminBerechtigung-Admin-Rolle-Zuordnung können nicht gelöscht werden.



Beachten Sie, dass Objekte die von dem zu löschenenden Objekt abhängen (z.B: Terminals an einem Server oder Subterminals an einem Terminal) ebenfalls gelöscht werden. Die Liste der zu löschenenden Objekte im Bestätigungsdialog zeigt diese untergeordneten Objekte ebenfalls an.

3.3.7 Kopieren und Einfügen

Zum Kopieren und Einfügen von Objekten darf sich kein Fenster im Änderungsmodus (siehe 3.3.3.2) befinden.

Die Menüpunkte **Kopieren** und **Einfügen...** (im Menü unter **Bearbeiten** oder im Kontextmenü) können den Arbeitsaufwand für die Konfiguration neuer Terminals und Subterminals oder anderen Objekt-Typen entscheidend verringern.

1. Selektieren Sie das zu kopierende Objekt und wählen Sie **Kopieren**.
2. Wählen Sie das Objekt, unter dem Sie das kopierte Objekt einfügen möchten.
3. Wählen Sie **Einfügen**. Das aktive K&S-Fenster wechselt in den Änderungsmodus und zeigt jetzt das eingefügte Objekt.
4. Prüfen Sie die Einstellungen im K&S-Fenster. Einige objekt-spezifische Angaben müssen normalerweise geändert werden.
5. Speichern Sie die Änderungen beim Beenden des Änderungsmodus.

Einige Objekt-Typen (Terminal-Management-System, Terminal-Handler, Konzentrator, Wurzelverwaltungseinheit, AdminBenutzer, AdminRolle, AdminBerechtigung, AdminBenutzer-Admin-Rolle-Zuordnung, AdminBerechtigung-Admin-Rolle-Zuordnung) lassen sich nicht kopieren.

3.4 Weitere Funktionen

3.4.1 Terminal-Reset

Um einen Reset (Warmstart, Kaltstart oder Neustart) an einem oder mehreren Terminals auszulösen, wählen Sie zuerst das oder die Terminals in einem Fenster (z.B.: Komponenten). Um einen Reset auszulösen, gibt es drei Möglichkeiten:

1. Wählen Sie im Menü **Steuerung** den Punkt **Reset**.
2. Betätigen Sie die Schaltfläche  in der Werkzeugeiste.
3. Wählen Sie im Kontextmenü den Punkt **Reset**.

Es erscheint ein Dialog, in welchem die ausgewählten Terminals aufgelistet werden und Sie die Art des durchzuführenden Reset auswählen können.

Einige Resettypen erlauben die Auswahl zusätzlicher Parameter, welche sind:

- **Masken löschen**
Ist dieser Parameter ausgewählt, werden bei Terminals die die INTUS Graph Benutzeroberfläche unterstützen, die INTUS Graph Masken gelöscht.
- **System-Reboot erzwingen**
Nicht alle Resettypen benötigen einen System-Reboot. Mit diesem Parameter kann ein System-Reboot erzwungen werden.

Auswählbare Resettypen sind:

- **Warmstart mittels TCL-Kommando**
Es soll ein Warmstart ausgelöst werden. Bei einem Warmstart bleiben das Terminal-Programm, die von ihm verwendeten Tabellen und insbesondere auch der Inhalt des Notpuffers (die gepufferten Buchungen) erhalten. Es wird ein entsprechendes TCL-Kommando an das Terminal geschickt.
Verfügbare Parameter sind "Masken löschen" und "System-Reboot" erzwingen.
- **Kaltstart mittels TCL-Kommando**
Es soll ein Kaltstart ausgelöst werden. Bei einem Kaltstart gehen Terminal-Programm, Tabellen und insbesondere auch der Inhalt des Notpuffers verloren. Es wird ein TCL-Kommando an das Terminal geschickt, um den Reset auszulösen.
Verfügbare Parameter sind "Masken löschen" und "System-Reboot" erzwingen.
- **Neustart mittels TCL-Kommando**
Es soll ein Neustart ausgelöst werden. Bei einem Neustart gehen Terminal-Programm, Tabellen und insbesondere auch der Inhalt des Notpuffers verloren. Um den Reset auszulösen, wird ein TCL-Kommando an das Terminal geschickt.
Verfügbare Parameter sind "Masken löschen" und "System-Reboot" erzwingen.
- **Comstart mittels TCL-Kommando**
Dieser Resettyp verhält sich wie der Eis-Kaltstart (s.u.) , allerdings bleiben die Netzwerkinstellungen erhalten.
Verfügbare Parameter sind "System-Reboot" erzwingen. Das Löschen der INTUS Graph Masken ist in diesem Resettyp implizit enthalten.
- **Eis-Kaltstart mittels TCL-Kommando (NUR FÜR EXPERTEN)**
Bei einem Eiskaltstart wird der gesamte Speicher (TCL Programm, Tabellen und gepufferte Buchungssätze) gelöscht. Außerdem werden die Setup-Parameter auf Werksvoreinstellungen zurückgesetzt. Ein Eiskaltstart sollte nur von geschultem Personal als letztes Mittel zur Fehlerbehebung eingesetzt werden.
Verfügbare Parameter sind "System-Reboot" erzwingen. Das Löschen der INTUS Graph Masken ist in diesem Resettyp implizit enthalten.

- **Warmstart mittels TCL/TPI-Kommando**
Es soll ein Warmstart ausgelöst werden. Bei einem Warmstart bleiben das Terminal-Programm, die von ihm verwendeten Tabellen und insbesondere auch der Inhalt des Notpuffers (die gepufferten Buchungen) erhalten. Wenn das Terminal als TPI-Terminal konfiguriert ist, wird ein entsprechender TPI-Satz an das Terminal geschickt, um den Reset auszulösen. Ist das Terminal dagegen als TCL-Terminal konfiguriert, wird ein entsprechendes TCL-Kommando an das Terminal geschickt.
Keine zusätzlichen Parameter verfügbar.
- **Kaltstart mittels TCL/TPI-Kommando**
Es soll ein Kaltstart ausgelöst werden. Bei einem Kaltstart gehen Terminal-Programm, Tabellen und insbesondere auch der Inhalt des Notpuffers verloren. Je nachdem, ob das Terminal als TPI- oder TCL-Terminal konfiguriert ist, wird ein entsprechender TPI-Satz oder ein TCL-Kommando an das Terminal geschickt, um den Reset auszulösen.
Keine zusätzlichen Parameter verfügbar.
- **Warten bis alle Offlinebuchungen transferiert wurden, dann Kaltstart mittels TCL/TPI-Kommando**
Es soll ein Kaltstart ausgelöst werden. Jedoch soll vorher gewartet werden, bis der Notpuffer geleert ist, damit keine Buchungen verloren gehen. Dazu schickt der Terminal-Handler in regelmäßigen Abständen Statusabfragen. Sobald gemeldet wird, dass der Notpuffer leer ist, wird der Kaltstart ausgelöst. Trotz der Abfrage kann es sein, dass noch einzelne Buchungen verloren gehen, die gerade zu dieser Zeit gemacht werden. Das Risiko ist jedoch deutlich geringer, als bei einem Kaltstart ohne vorherige Abfrage.
Keine zusätzlichen Parameter verfügbar.



Für das Auslösen eines Resets ist der Terminal-Handler zuständig. Das oder die Terminals müssen im Terminal-Handler aktiviert sein.

3.4.2 Manueller Download aus Datei/Datenbank/Blocklist

Um einen Download manuell zu starten, wählen Sie bitte ein oder mehrere Terminals in einem Fenster aus (z.B.: Komponenten). Um einen Download für die ausgewählten Terminals zu starten gibt es drei Möglichkeiten:

1. Wählen Sie im Menü **Steuerung** den Punkt **Download**.
2. Betätigen Sie die Schaltfläche in der Werkzeugleiste.
3. Wählen Sie im Kontextmenü den Punkt **Download**.

Es erscheint ein Dialog, in dem die Downloadtypen (68-77) aufgelistet sind. Wählen Sie den gewünschten Download aus, und klicken Sie auf **Ok**.



Im Falle des Parameterdownloads (73) werden auch die Parameterdateien der Subterminals mit geladen (soweit welche konfiguriert sind).

3.4.3 Zeitversetzten Download planen

Um einen zeitversetzten Download zu planen, wählen Sie bitte ein oder mehrere Terminals in einem Fenster aus (z.B.: Komponenten). Um einen Download für die ausgewählten Terminals zu planen gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü **Steuerung** den Punkt **Download planen**.
2. Wählen Sie im Kontextmenü den Punkt **Download planen**.

Es erscheint ein Dialog, in dem die Downloadtypen (68-77) aufgelistet sind und ein Eingabefeld für den Ausführungszeitpunkt. Wählen Sie den gewünschten Download aus und geben Sie einen Ausführungszeitpunkt ein und klicken **Ok**.

Im Falle des Parameterdownloads (73) werden auch die Parameterdateien der Subterminals mit geladen (soweit welche konfiguriert sind).



Der Ausführungszeitpunkt muss in der Zukunft liegen.

3.4.4 Neuladen der Fingerprint-Templates

Um das Neuladen der Fingerprint-Templates auf ein Fingerprint-Terminal manuell zu starten, wählen Sie bitte ein oder mehrere Haupt- oder Subterminals in einem Fenster aus (z.B.: Komponenten). Um den Download der Templates zu starten gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü **Steuerung** den Punkt **FP-Templates neu laden**.
2. Wählen Sie im Kontextmenü den Punkt **FP-Templates neu laden**.

Bestätigen Sie im daraufhin erscheinenden Dialog das Neuladen der FP-Templates.



Beim Neuladen der FP-Templates werden zunächst alle Templates aus dem Fingerprint-Terminal gelöscht und dann neu geladen. In der Zeit, bis alle Templates auf das Fingerprint-Terminal geladen sind, kann es zu Fehlerrückweisungen kommen.

3.4.5 Neuladen der PS-Templates

Um das Neuladen der PS-Templates auf einen PS-Controller manuell zu starten, wählen Sie bitte ein oder mehrere PS-Controller in einem Fenster aus (z.B.: Komponenten). Um den Download der Templates zu starten gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü **Steuerung** den Punkt **PS-Templates neu laden**.
2. Wählen Sie im Kontextmenü den Punkt **PS-Templates neu laden**.

Bestätigen Sie im daraufhin erscheinenden Dialog das Neuladen der PS-Templates.



3.4.6 Terminal-Statusseite anfordern

Um die Statusseite eines Terminals abzufragen, wählen Sie bitte das Terminal in einem Fenster aus (z.B.: Komponenten). Um die Statusseite anzuzeigen gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü unter **Steuerung** den Punkt **Statusseite anfordern**.
2. Wählen Sie im Kontextmenü den Punkt **Statusseite anfordern**.



Die Terminal-Statusseite kann nur für INTUS Terminals/ACM, die an einem INTUS COM TCP-Server konfiguriert sind, angefordert werden.

3.4.7 Batteriezustand abfragen

Um den Ladezustand der Batterie eines Terminals abzufragen, wählen Sie bitte das Terminal in einem Fenster aus (z.B.: Komponenten). Um den Batteriezustand abzufragen gibt es drei Möglichkeiten:

1. Wählen Sie im Menü unter **Steuerung** den Punkt **Batteriezustand abfragen**.
2. Betätigen Sie die Schaltfläche auf dem Register Status des K&S-Fenster für das Terminal.
3. Wählen Sie im Kontextmenü den Punkt **Batteriezustand abfragen**.

Bestätigen Sie im daraufhin erscheinenden Dialog das Abfragen des Batteriezustandes. Es wird eine Abfrage an das Terminal geschickt. Die Antwort des Terminals sehen Sie im K&S-Fenster des Terminals auf dem Register Status unter **Batteriestatus**.

3.4.8 AutoClone Passwort zurücksetzen

Um den AutoClone Status eines Terminals zurückzusetzen, wählen Sie bitte das Terminal in einem Fenster aus (z.B.: Komponenten) und wählen Sie dann

1. im Menü unter **Steuerung** den Punkt **AutoClone Status zurücksetzen**.
2. im Kontextmenü den Punkt **AutoClone Status zurücksetzen**.

Bestätigen Sie im daraufhin erscheinenden Dialog das Zurücksetzen des AutoClone Status.

Achtung:

Das Zurücksetzen des AutoClone Status bezieht sich nur auf die Einstellungen im AutoClone-Dienst. Die Einstellungen im Terminal werden dadurch nicht geändert. Um die Einstellungen im Terminal zu ändern, verwenden Sie bitte INTUS RemoteConf.

3.4.9 AutoClone Download starten

Um einen AutoClone-Download manuell zu starten, wählen Sie bitte ein oder mehrere Terminals in einem Fenster aus (z.B.: Komponenten). Um einen AutoClone-Download für die ausgewählten Terminals zu starten gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü **Steuerung** den Punkt **AutoClone Download starten**.
2. Wählen Sie im Kontextmenü den Punkt **AutoClone Download starten**.

Es erscheint ein Dialog, in dem die Downloadtypen

- INTUS Graph Masken (*.igma)
- INTUS Audio Archiv (*.iaa)
- INTUS Graph Tastatur (*.qml)

auswählbar sind.

Wählen Sie die gewünschten Downloads aus, und klicken Sie auf **Ok**.

3.4.10 Email Benachrichtigung bei Alarmen

INTUS COM kann auf einen TPI Alarm-/Ereignisdatensatz mit dem Senden von E-Mails reagieren. Es können mehrere Empfängeradressen im System eingerichtet werden.

Damit Benachrichtigungen an eine E-Mail-Adresse gesendet werden, muss ein Objekt vom Typ EMail-Einstellung (siehe 4.27) für diese E-Mail-Adresse vorliegen. Dieses bestimmt die auslösenden Alarne/Ereignisse und durch die Zuordnung zu einer Verwaltungseinheit auch die Komponenten, dessen Alarne/Ereignisse das Senden einer E-Mail an diese E-Mail-Adresse auslösen.

Soll für alle Komponenten bei einem Alarm/Ereignis eine E-Mail-Benachrichtigung an eine bestimmte E-Mail-Adresse gesendet werden, so muss der zugehörigen EMail-Einstellung die Wurzelverwaltungseinheit zugewiesen werden.

Für Hinweise zum Hinzufügen einer Email-Einstellung, siehe 3.3.4 und 4.27.

Eine E-Mail wird somit immer dann gesendet, wenn ein auslösender/s Alarm/Ereignis von einer Komponente ausgeht, die der gleichen (oder einer untergeordneten) Verwaltungseinheit zugewiesen ist wie die EMail-Einstellung.

Auf diese Weise können für verschiedene Verwaltungseinheiten bzw. den den Verwaltungseinheiten zugeordneten Komponenten und/oder verschiedene Alarne/Ereignisse jeweils unterschiedliche Empfängeradressen konfiguriert werden.

3.4.11 Netzwerk Terminalsuche

Die Netzwerk Terminalsuche ermöglicht es, die im LAN vorhandenen Terminals zu ermitteln. Um die Netzwerk Terminalsuche zu öffnen gibt es drei Möglichkeiten:

1. Wählen Sie im Menü Werkzeuge den Punkt Netzwerk Terminalsuche
2. Betätigen Sie die Schaltfläche während der Konfiguration eines INTUS 3000/3450 Server.
3. Betätigen Sie die Schaltfläche während der Konfiguration eines INTUS Terminals/ACM.

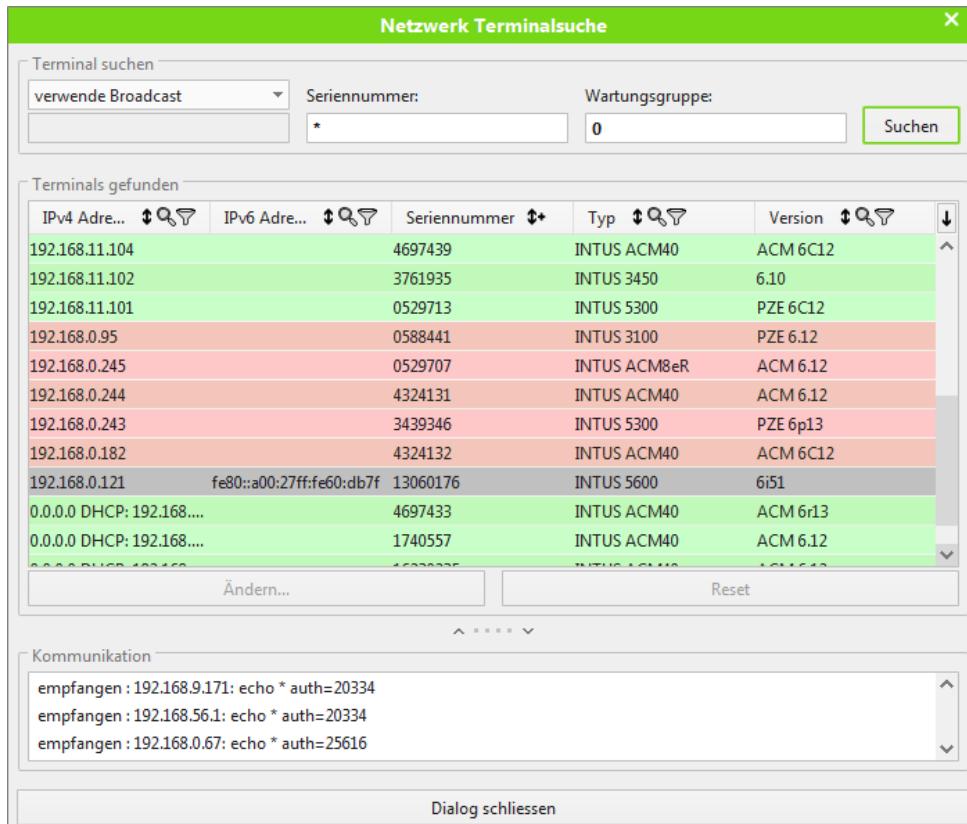


Abbildung 3.15 - Netzwerk Terminalsuche

Die im Netz vorhandenen Terminals können mit der Schaltfläche **Suchen** ermittelt werden.

Die Netzwerk Terminalsuche mit Broadcast kann nur funktionieren, wenn im LAN Broadcasts nicht gefiltert werden.

 Die Suche nach IPv6-Adressen ist in der **Netzwerk Terminalsuche** nicht möglich.

 Mit der Schaltfläche **OK** werden Seriennummer, Adresse und Port des ausgewählten Terminals in die Konfiguration des Terminals übernommen, wenn der Dialog von einem K&S-Fenster aus aufgerufen wurde.

Die Wartungsgruppe wird verwendet, um unautorisierte Änderungen an den Netzwerkparametern zu verhindern. Terminals die sich nicht in der eingestellten Wartungsgruppe befinden, werden in der Tabelle rot hinterlegt. Die Netzwerkparameter dieser Terminals können zwar

angezeigt, aber nicht geändert werden. Auch ist die Schaltfläche **Reset** für diese Terminals deaktiviert.

Befindet sich ein Terminal in der Tabelle in der eingestellten Wartungsgruppe, so wird die entsprechende Zeile grün hinterlegt. Die Netzwerkparameter dieser Terminals können geändert werden.

Über die Schaltfläche **Ändern..** wird ein weiterer Dialog geöffnet, der es ermöglicht die Netzwerkparameter des Terminals zu ändern. Der Dialog zum Ändern der Netzwerkparameter sieht folgendermaßen aus:

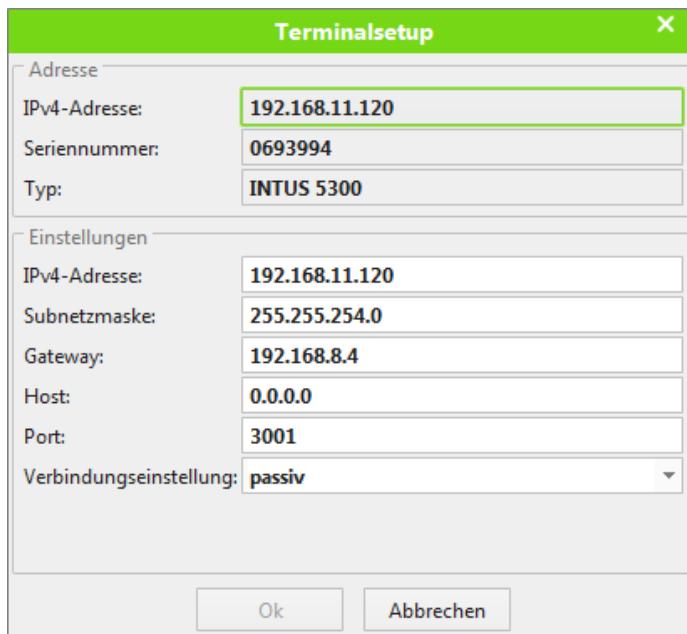


Abbildung 3.16 - Terminalsetup

Bei Betätigung der Schaltfläche **Ok**, wird das Kommando zum Ändern der Parameter an das Terminal gesendet.



Damit die geänderten Parameter wirksam werden, muss anschließend ein Reset mit der **Reset**-Schaltfläche ausgelöst werden.

Geräte mit einer IPV6-Adresse werden von der Netzwerk Terminalsuche nicht unterstützt.

Grau hinterlegte Terminals reagieren auf die neue 'locate' Anweisung und werden mit anderen Kommandos konfiguriert. Diese neuen Kommandos unterstützen weder Host, Port oder die Auswahl des Verbindungsaufbau (aktiv/passiv).

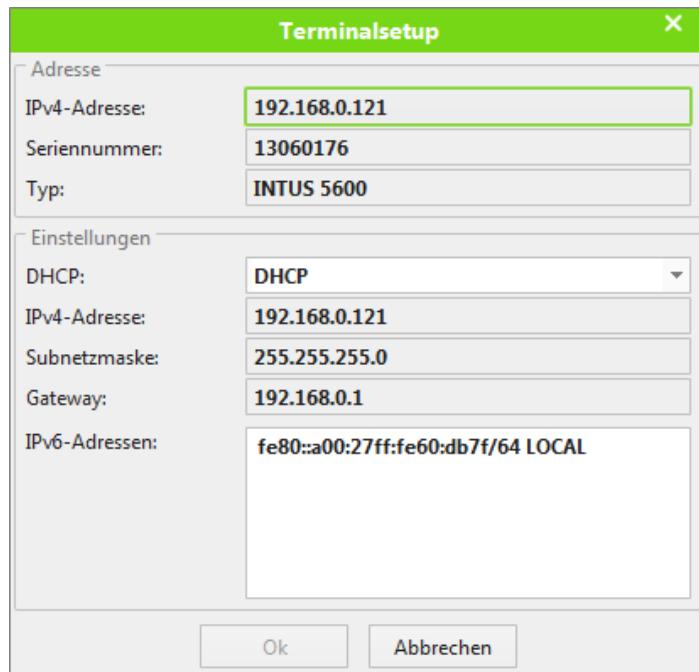


Abbildung 3.17 - Terminalsetup

Ob das Terminal DHCP verwenden soll, kann über das erste Auswahlfeld im Rahmen Einstellungen eingestellt werden. Auswählbar sind:

- **DHCP**
IPv4-Adresse, Subnetzmaske und Gateway sind nicht editierbar. Diese Einstellungen werden von einem DHCP Server bezogen.
- **Manuell**
IPv4-Adresse, Subnetzmaske und Gateway sind editierbar. Diese Einstellungen müssen manuell eingestellt werden.

Die Liste IPv6-Adressen kann nicht editiert werden und dient nur informativen zwecken.

3.4.12 Uhrzeit stellen

Um die Uhrzeit eines Terminals mit der des Terminal-Handler zu synchronisieren (**Zeiteinstellung**, siehe 4.13.2), wählen Sie bitte ein oder mehrere Terminals in einem Fenster aus (z.B.: Komponenten). Es gibt drei Möglichkeiten, die Uhrzeit zu synchronisieren:

1. Wählen Sie im Menü **Steuerung** den Punkt **Uhrzeit stellen**.
2. Betätigen Sie die Schaltfläche in der Werkzeugleiste.
3. Wählen Sie im Kontextmenü den Punkt **Uhrzeit stellen**.

Bestätigen Sie im daraufhin erscheinenden Dialog das Stellen der Uhrzeit.

3.4.13 Dialog mit Terminal

INTUS COM bietet die Möglichkeit, über einen Dialog mit dem Terminal zu kommunizieren. Damit sind Abfragen und Tests durch TCL-Kommandos oder auch TPI-Sätze für fortgeschrittene Anwender möglich (siehe 6.3.2.1).

Um diesen Dialog zu starten, wählen Sie das Terminal in einem Fenster aus (z.B.: Komponenten) und wählen Sie im Menü **Steuerung** oder im Kontextmenü den Punkt **Dialog mit Terminal**.

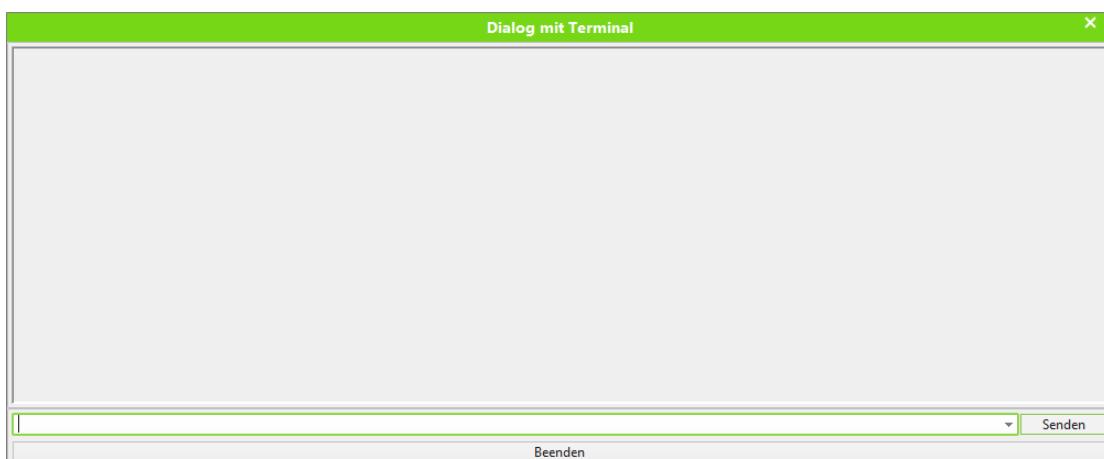


Abbildung 3.18 – Dialog mit Terminal



Solange dieser Dialog geöffnet ist, werden alle Datensätze des Terminals an diesen Dialog umgeleitet und nicht an die Applikation gesendet oder vom Terminal-Handler verarbeitet. In umgekehrter Richtung werden auch nur noch Datensätze, die über diesen Dialog gesendet werden, an das Terminal weitergeleitet.

In der Eingabezeile neben der Schaltfläche **Senden** können beliebige TCL-Kommandos bzw. TPI-Sätze eingegeben und an das Terminal gesendet werden. Über die Cursortasten können vorher gemachte Eingaben wieder herangeholt werden.

3.4.14 Einzeltüröffnung

Um für eine Tür eine Einzeltüröffnung auszulösen, wählen Sie bitte die Tür in einem Fenster aus (z. B. Komponenten). Um die Einzeltüröffnung durchzuführen gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü unter Steuerung den Punkt Einzeltüröffnung.
2. Wählen Sie im Kontextmenü den Punkt Einzeltüröffnung.

Bestätigen Sie im daraufhin erscheinenden Dialog die Einzeltüröffnung. Es wird ein Steuersatz an das Terminal/ACM gesendet an dem die Tür konfiguriert ist, um die Einzeltüröffnung an der gewählten Tür durchzuführen.

3.4.15 Dauertüröffnung

Um für eine Tür eine Dauertüröffnung auszulösen, wählen Sie bitte die Tür in einem Fenster aus (z. B. Komponenten). Um die Dauertüröffnung durchzuführen gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü unter Steuerung den Punkt Dauertüröffnung.
2. Wählen Sie im Kontextmenü den Punkt Dauertüröffnung.

Im daraufhin erscheinenden Dialog wählen Sie im Rahmen Kommando aus, ob Sie eine permanente Dauertüröffnung, oder eine zeitlich begrenzte Dauertüröffnung durchführen möchten. Im Falle einer zeitlich begrenzten Dauertüröffnung können Sie im darunterliegenden Eingabefeld die Dauer der Türöffnung im Bereich von 1 bis 150 Minuten einstellen.

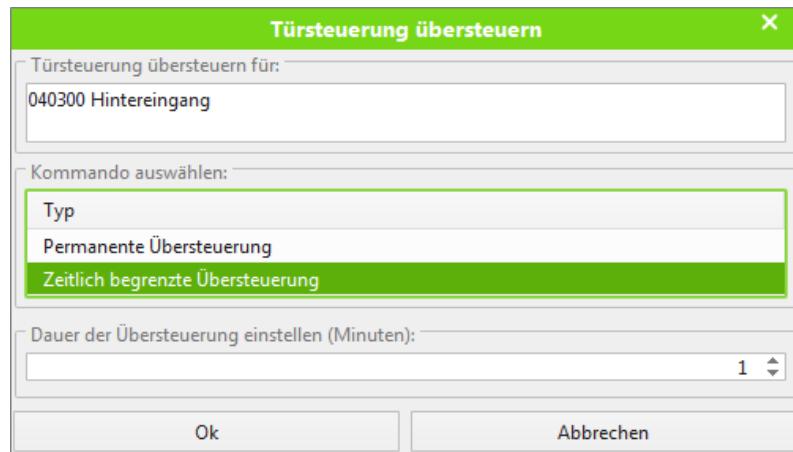


Abbildung 3.19 – Dauertüröffnung

Bestätigen Sie den Dialog um die Dauertüröffnung mit den getroffenen Einstellungen durchzuführen. Es wird ein Steuersatz an das Terminal/ACM gesendet an dem die Tür konfiguriert ist, um die Dauertüröffnung an der gewählten Tür durchzuführen.

3.4.16 Dauertüröffnung beenden

Um für eine Tür eine Dauertüröffnung zu beenden, wählen Sie bitte die Tür in einem Fenster aus (z. B. Komponenten). Um die Dauertüröffnung zu beenden gibt es zwei Möglichkeiten:

1. Wählen Sie im Menü unter Steuerung den Punkt Dauertüröffnung beenden.
2. Wählen Sie im Kontextmenü den Punkt Dauertüröffnung beenden.

Bestätigen Sie im daraufhin erscheinenden Dialog das Beenden der Dauertüröffnung. Es wird ein Steuersatz an das Terminal/ACM gesendet an dem die Tür konfiguriert ist, um die Dauertüröffnung an der gewählten Tür zu beenden.

3.4.17 Export der Offline Terminal Konfiguration

Zum Zwecke des Transfers von Informationen über Offlineterminals an ein Konfigurations-Tool (Configuration-Tool) kann INTUS COM Offlineterminals, die gemäß dem OSS Standard Offline arbeiten, in eine XML-Datei exportieren.

Wenn Sie Offlineterminals exportieren möchten, wählen Sie bitte im Menü **werkzeuge/Export der Offline Terminal Konfiguration...** Dadurch wird ein Dialog geöffnet, in dem Sie den zu exportierenden Inhalt wählen können.



Abbildung 3.20 – Offlineterminals in Datei exportieren

Für Offlineterminals von unterschiedlichen Herstellern werden typischerweise unterschiedliche Konfigurations-Tools eingesetzt. Deshalb sollten nur Offlineterminals desselben Herstellers in dieselbe Datei exportiert werden. Bitte wählen Sie oben im Dialog den passenden Hersteller.

In der Exportdatei wird zwischen neuen Offlineterminals und geänderten Offlineterminals unterschieden. INTUS COM wertet den Status der Offlineterminals aus und weist jedem der Offlineterminals automatisch eine der Kategorien „neu“, „geändert“ oder „nicht exportieren“ zu.

Mit der Checkbox „Nur neu oder geändert“ können Sie steuern, ob die darunterliegende Tabelle Offlineterminals aller drei Kategorien oder nur Offlineterminals der Kategorien „neu“ und „geändert“ enthalten soll.

Aus verschiedenen Gründen kann es sein, dass die Kategorie, die einem Offlineterminal automatisch zugewiesen wurde, nicht die Kategorie ist, die Sie benötigen. Deshalb können Sie die Kategorie ändern. Eine Möglichkeit ist, dazu die Checkboxen in den Spalten „Neu“ und „Geändert“ zu verwenden. Alternativ dazu können Sie ein oder mehrere Offlineterminals auswählen und anschließend die Schaltfläche „Bearbeiten“ klicken. Dadurch wird ein Dialog geöffnet, in dem Sie die Kategorie der ausgewählten Offlineterminals einstellen können. (Egal für welche Vorgehensweise Sie sich entscheiden, falls Sie Offlineterminals vermissen, kann es eventuell helfen, den Haken bei „Nur neu oder geändert“ herauszunehmen, um Offlineterminals mit der Kategorie „nicht exportieren“ zu sehen.)

Wenn die Kategorien richtig eingestellt sind, klicken Sie bitte die Schaltfläche „Exportieren“. Dadurch wird ein Dialog geöffnet, in dem Sie für die Exportdatei das Verzeichnis wählen, den Dateinamen eingeben und die Exportdatei speichern können.

3.4.18 Import der Offline Terminal Konfigurationsergebnisse

Für Offlineterminals, die gemäß dem OSS Standard Offline arbeiten, kann INTUS COM einen Konfigurationsstatus führen. Dieser gibt an, mit welchen Konfigurationsdaten die Offlineterminal-Hardware aus Sicht von INTUS COM konfiguriert ist.

Um diesen Konfigurationsstatus zu aktualisieren, kann INTUS COM Konfigurationsergebnisse importieren, die von einem Konfigurations-Tool (Configuration-Tool) in einer XML-Datei bereitgestellt werden.

Wenn Sie Konfigurationsergebnisse für Offlineterminals importieren möchten, wählen Sie bitte im Menü **Werkzeuge/Import der offline Terminal Konfigurationsergebnisse...**. Dadurch wird ein Dialog geöffnet.

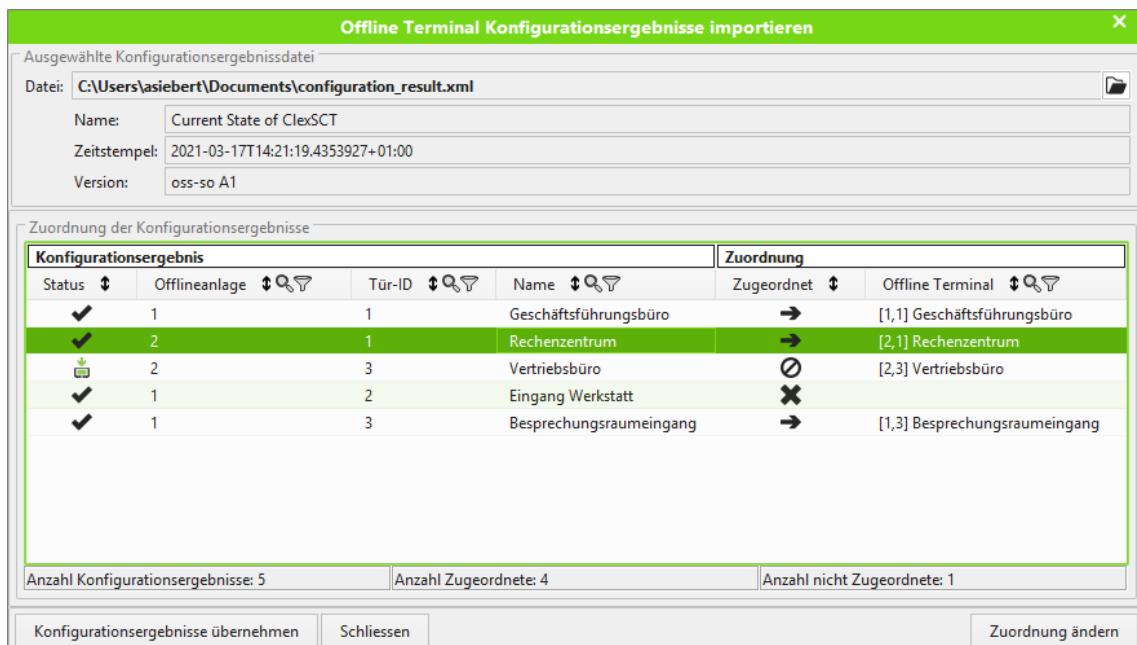


Abbildung 3.21 – Offlineterminal-Konfigurationsergebnisse importieren

Klicken Sie bitte oben rechts im Dialog auf die Schaltfläche . Es wird ein weiterer Dialog geöffnet, in dem Sie die Importdatei auswählen und öffnen können. Nach dem Öffnen der Importdatei, versucht der INTUS COM Client die aus der Importdatei gelesenen Konfigurationsergebnisse den ihm vorliegenden Offlineterminals zuzuordnen. Dies erfolgt anhand von Offlineanlagen-IDs (Site-IDs) und Tür-IDs (Door-IDs).

Einige Informationen aus der Importdatei sowie gegebenenfalls erfolgte Zuordnungen zu Offlineterminals werden dann in dem ersten Dialog angezeigt.

Informationen zur Bedeutung der Icons in den Spalten „Status“ und „Zugeordnet“ können Sie per Tooltip erhalten, indem Sie jeweils mit dem Mauszeiger auf das Icon zeigen.

Für Konfigurationsergebnisse, die einem Offlineterminal zugeordnet sind, ist die Spalte „Offline Terminal“ entsprechend belegt.

Für importierbare Konfigurationsergebnisse besteht die Möglichkeit, die Zuordnung zu bearbeiten, soweit dies nicht an der Nichtverfügbarkeit von Offlineterminals scheitert. Wenn Sie die Zuordnung bearbeiten möchten, wählen Sie bitte das Konfigurationsergebnis in der Tabelle aus und betätigen sie anschließend die Schaltfläche „Zuordnung ändern“. Dadurch wird ein Dialog geöffnet, mit dem Sie festlegen können, welchem der verfügbaren Offlineterminals das Konfigurationsergebnis zugeordnet sein soll oder dass das Konfigurationsergebnis keinem Offlineterminal zugeordnet sein soll.

Um die zugeordneten importierbaren Konfigurationsergebnisse zu importieren, betätigen Sie bitte die Schaltfläche „Konfigurationsergebnisse übernehmen“.

4 INTUS COM in Betrieb nehmen

In diesem Kapitel wird im Detail beschrieben, wie die INTUS COM Komponenten und die angeschlossenen Terminals und Subterminals zu konfigurieren und in Betrieb zu nehmen sind.

Alle Einstellungen werden über den INTUS COM Client vorgenommen. Machen Sie sich bitte zuerst mit der Bedieneroberfläche vertraut (siehe Kapitel 3). Wie Sie den INTUS COM Client starten, ist in Abschnitt 2.4 beschrieben.

4.1 Schrittweise Inbetriebnahme eines Terminalsystems

Um eine INTUS COM Installation einschließlich der angeschlossenen INTUS Terminals in Betrieb zu nehmen, gehen Sie wie folgt vor:

- Schließen Sie die INTUS Terminals an und testen Sie die Verbindung (siehe die jeweilige Installationsanleitung des Terminals und Abschnitt 4.3).
- Installieren Sie die benötigten INTUS COM Server und den INTUS COM Client auf dem/den Rechnern, aber starten Sie sie noch nicht (siehe 2.1).
- Wenn die INTUS COM Server und die Applikation auf verschiedenen Rechnern installiert sind, passen Sie die `secure.cfg` Dateien im Verzeichnis `\conf` an (siehe 2.3.5)
- Jetzt können Sie die INTUS COM Server (siehe 2.3) und den INTUS COM Client starten (siehe 2.4).
- Legen Sie einen neuen Benutzer mit Passwort an (siehe 3.2.2)
- Konfigurieren Sie den Terminal-Handler wie in 4.8 beschrieben
- Legen Sie den oder die benötigten Kommunikation-Server unter dem Konzentrator an und konfigurieren Sie sie (TCP-Server, siehe 4.10, HTTPS-Server, siehe 4.11).

Jeder Server benötigt eine eindeutige Server-ID.

- Legen Sie die (Haupt-) Terminals (INTUS Terminal/ACM) unter dem jeweiligen Server an und konfigurieren Sie sie (siehe 4.13).

Jedes Terminal an einem Server benötigt eine eindeutige Terminal-ID

- Subterminals an INTUS Terminal/ACM anlegen und konfigurieren (siehe 4.14)

Jedes Subterminal an einem Hauptterminal benötigt eine eindeutige Subterminal-ID.

Probleme bei der Inbetriebnahme

Treten Probleme bei der Inbetriebnahme auf, versuchen Sie die Ursache mit Hilfe der Hinweise im Kapitel 5 zu finden.

4.2 Verschlüsselung

Ab TCL Version 5.50 kann der Datenaustausch zwischen TCP-Server/INTUS Server und INTUS Terminal/ACM verschlüsselt werden.

Die Einstellung des Schlüssels am Konzentrator oder einem TCP-Server erfolgt im Registerblatt „Verschlüsselung“ (siehe 4.9.2 bzw. 4.10.2). Sie müssen dazu eine beliebige Zeichenkette ("pass phrase") eingeben, aus der das Programm den eigentlichen Schlüssel berechnet.

Die Verschlüsselung kann für jedes INTUS Terminal/ACM und jeden INTUS 3000/3450 Server einzeln auf dem Registerblatt „Grundeinstellungen“ ein- bzw. ausgeschaltet werden (siehe 4.12.1 bzw. 4.13.2). In der Voreinstellung ist die Verschlüsselung deaktiviert.

Die Einstellung des Schlüssels an einem INTUS Terminal, einem INTUS ACM Zutrittskontrollmanager oder einem INTUS 3000/3450 Server erfolgt nicht in INTUS COM sondern über das Programm INTUS RemoteSetup (oder ACM8Setup).

In allen INTUS Terminal/ACM, die mit einem TCP-Server verbunden sind und die Verschlüsselung verwenden, muss derselbe Schlüssel wie im TCP-Server eingestellt werden. Ebenso muss in allen INTUS 3000/3450 Servern derselbe Schlüssel eingestellt werden wie im Konzentrator.

4.3 Test der Terminalverbindung

4.3.1 TCP/IP

INTUS Terminal mit TCP/IP LAN-Anschluss haben eine eigene IP-Adresse und Datenportnummer, über die sie mit dem TCP-Server kommunizieren.

- Sie können die Leitungsverbindung zum Terminal mit dem ping-Kommando testen. Wenn das Terminal nicht antwortet, liegt ein Verkabelungsproblem vor (oder der Echo-Request wird von dazwischen geschalteten Routern gefiltert):
`ping <IP-Adresse des Terminals>`
- Wenn Sie die IP-Adresse von INTUS Terminal/ACM in einem Webbrowser eingeben, erhalten Sie die Web-Statusanzeige von dem Terminal.
- Sie können die Datenkommunikation zum Terminal mit einer Telnet-Verbindung testen:
`telnet <IP-Adresse des Terminals> <Portnummer des Terminals>`
Wenn sich die Telnetverbindung fehlerfrei herstellen lässt, liegt kein Kommunikationsproblem zum Terminal vor.

4.3.2 HTTPS

Bei Verbindungsproblemen zwischen HTTPS-Server und einem über diesen angebundenen Terminal können Sie folgende Tests bzw. Prüfungen durchführen:

- Stellen Sie fest, ob das Terminal über das Netzwerk erreichbar ist.
- Überprüfen Sie, ob das Terminal korrekt über den INTUS COM Client konfiguriert wurde. Dabei ist vor allem darauf zu achten, dass die korrekte Seriennummer und das korrekte Passwort eingestellt wurden.
- Überprüfen Sie, ob die korrekten Zertifikate verwendet wurden.
- Überprüfen Sie den Gültigkeitszeitraum der Zertifikate.
- Überprüfen Sie die Datumseinstellungen des Terminals. Bei einer falschen Datumseinstellung kann unter Umständen das Terminal das Zertifikat als ungültig ansehen.
- Prüfen Sie die Firewalleinstellungen. Der HTTPS-Server muss eingehende Verbindungen auf dem Port für die HTTPS-Terminals (Standardport=10443) akzeptieren können.

4.4 Berechtigungsverwaltung in INTUS COM

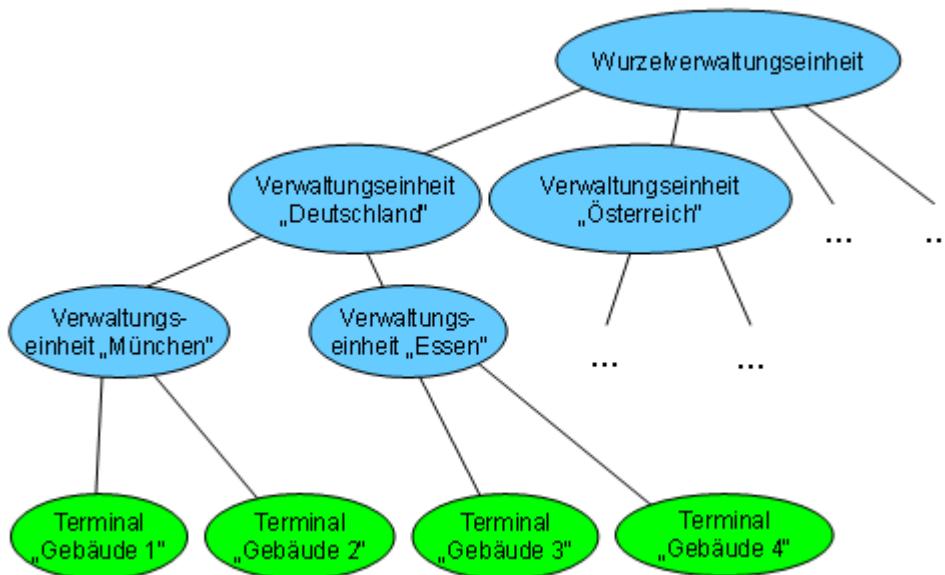
4.4.1 Verwaltungseinheiten

Mit Ausnahme von Objekten, die lediglich der Verknüpfung anderer Objekte dienen oder nicht explizit über den INTUS COM Client konfiguriert werden können, sind alle Objekte in einer Verwaltungseinheit und somit im Verwaltungsbaum enthalten. Ihre Position im Verwaltungsbaum spiegelt ihre administrative Zugehörigkeit zu Verwaltungseinheiten wieder.

Im Lageplanfenster wird auf die Darstellung von Objekten, die keine Hardwarekomponenten repräsentieren, verzichtet.

Alle Objekte, die sich im Verwaltungsbaum direkt oder indirekt unter einer Verwaltungseinheit befinden, gelten als zu dieser Verwaltungseinheit zugehörig.

Im folgenden Beispiel gehört das Terminal „Gebäude 2“ zu den Verwaltungseinheiten „München“ und „Deutschland“ sowie zur Wurzelverwaltungseinheit.



4.4.2 Benutzer

Benutzer werden in INTUS COM durch Benutzerobjekte repräsentiert. Die Berechtigungen eines Benutzers werden nicht im Benutzerobjekt sondern durch Zuordnung von Rollen zu dem Benutzer festgelegt. Einem Benutzer können mehreren Rollen zugeordnet werden. Die Zuordnung eines Benutzers zu einer Rolle wird durch ein Zuordnungs-Objekt repräsentiert (siehe 4.4.5 Benutzer-Rolle-Zuordnung).

Benutzer einschließlich des Administratorbenutzers können gesperrt werden. Gesperrte Benutzer können sich nicht an INTUS COM anmelden.

4.4.3 Rollen

Eine Rolle ist die Abbildung einer Funktion bzw. Zuständigkeit von Benutzern. Der Name einer Rolle muss in INTUS COM eindeutig sein. Einer Rolle können Benutzer und Berechtigungen über Zuordnungsobjekte zugeordnet werden (siehe 4.4.5 Benutzer-Rolle-Zuordnung und 4.4.6 Berechtigung-Rolle-Zuordnung).

4.4.4 Berechtigung

Eine Berechtigung bezieht sich immer auf die zugeordnete Verwaltungseinheit. Eine Berechtigung in INTUS COM definiert Rechte auf der Verwaltungseinheit und darin enthaltenen Objekten (z.B: Lesern/Terminals/Diensten). Berechtigungen werden Rollen zugeordnet.

4.4.5 Benutzer-Rolle-Zuordnung

Für die Zuordnung von Rollen zu Benutzern werden Benutzer-Rolle-Zuordnungsobjekte verwendet. Ein solches Benutzer-Rolle-Zuordnungsobjekt enthält eine Rolle und einen Benutzer, dem die Rolle zugeordnet ist.

4.4.6 Berechtigung-Rolle-Zuordnung

Für die Zuordnung von Rollen zu Berechtigungen werden Berechtigung-Rolle-Zuordnungsobjekte verwendet. Ein solches Berechtigung-Rolle-Zuordnungsobjekt enthält eine Rolle und eine Berechtigung, die der Rolle zugeordnet ist.

4.4.7 Spezieller Adminstrator-Benutzer, -Rolle und –Berechtigung

Der Administratorbenutzer besitzt bestimmte Mindestrechte, die ihm außer durch seine Sperrung nicht entzogen werden können.

Letzteres wird mit Hilfe einer speziellen Administratorrolle und einer speziellen Administratortberechtigung umgesetzt, die ebenfalls nicht gelöscht werden können. Der Administratorbenutzer und die Administratortberechtigung sind immer dieser Administratorrolle zugeordnet.

Die Administratortberechtigung enthält immer bestimmte Mindestrechte die sich auf den Wurzellageplan beziehen. Auf diese Weise wird eine Mindestberechtigung für den Administratorbenutzer sichergestellt, soweit er nicht gesperrt ist.

Die Administratorrolle kann auch an andere Benutzer als den Administratorbenutzer vergeben werden. Ebenso kann die Administratortberechtigung auch an andere Rollen als die Administratorrolle vergeben werden.

Wenn der Administratorbenutzer gesperrt wurde und es keinen Benutzer mehr gibt, der diese Sperrung wieder aufheben kann, so kann die Sperrung des Administratorbenutzers durch eine Änderung der Datei admin_server.ini im INTUS COM Konfigurationsverzeichnis „conf“ wieder entsperrt werden. Um den Administratorbenutzer zu entsperren, beenden Sie den INTUS COM Admin-Server Dienst, ändern unter dem Schlüssel [admin-user.00001] den Wert des Parameter „active“ von „0“ auf „1“ in der Datei „admin_server.ini“ und starten danach den INTUS COM Admin-Server Dienst wieder.



4.5 Gemeinsame Parameter

4.5.1 Verwaltungseinheit

Eine Verwaltungseinheit entspricht einem organisatorischen Teilbereich. Damit kann z.B. ein geografischer Standort, ein Werk, ein Gebäude, eine Etage o.ä. abgebildet werden.

Außer der einmalig vorhandenen Wurzelverwaltungseinheit hat jede Verwaltungseinheit eine übergeordnete Verwaltungseinheit und jede Verwaltungseinheit kann beliebig viele untergeordnete Verwaltungseinheiten haben.

Folgende Objekttypen werden im jeweiligen K&S-Fenster genau einer Verwaltungseinheit zugeordnet:

- Terminal Management System
- Terminal-Handler
- Konzentrator
- TCP-Server
- HTTPS-Server
- INTUS 3000/3450 Server
- Video-Interface
- Videoserver
- SeeTec Gateway Service
- PS-Distributor
- AutoClone-Server
- INTUS Terminal/ACM
- Subterminal
- Tür
- Kamera
- EMail-Einstellung
- Benutzer
- Rolle
- Berechtigung

Drücken Sie die Schaltfläche  zum Konfigurieren einer Verwaltungseinheit für ein Objekt (Zuordnung eines Objektes zu einer Verwaltungseinheit) im jeweiligen K&S-Fenster. Es öffnet sich ein Konfigurationsdialog welcher die Hierarchie der Verwaltungseinheiten, für die der angemeldete Benutzer leseberechtigt ist, in einem Baum zeigt. Wählen Sie einen Eintrag und bestätigen Sie mit der Schaltfläche ok.

Bei der Auswahl der Verwaltungseinheit spielt es keine Rolle, wo sich die Verwaltungseinheit in der Hierarchie der Verwaltungseinheiten befindet. Miteinander verschaltete Hardware-Komponenten (Terminals, Subterminals, Türen, ...) können unterschiedlichen Verwaltungseinheiten zugewiesen werden.

Alle Objekte, die sich in der Verwaltungseinheiten-Hierarchie direkt oder indirekt unter einer Verwaltungseinheit befinden, gelten als zu dieser Verwaltungseinheit zugehörig. Die Wurzelverwaltungseinheit umfasst alle untergeordneten Verwaltungseinheiten und deren Objekte, entweder direkt oder indirekt.

4.5.2 Seriennummer

Allen INTUS 3000/3450 Servern und INTUS Terminal/ACMs kann eine Seriennummer zugeordnet werden. Die Seriennummer darf leer bleiben. Wenn die Seriennummer nicht leer ist, dann darf der gleiche Wert nicht als Seriennummer eines anderen Gerätes eingestellt sein.

Bei Terminals, die über HTTPS-Server angebunden sind, dient die Seriennummer der Identifikation des Geräts.

Übliche Seriennummern bestehen aus 8 Ziffern.

4.5.3 Gemeinsame Parameter der INTUS COM Server

4.5.3.1 Rechnername oder IP-Adresse

Jedem INTUS COM Server ist die IP-Adresse des Rechners zugeordnet, auf dem sie installiert sind. Wenn der Server auf demselben Rechner installiert ist, wie der Admin-Server (Normalfall), kann auch localhost, ::1 oder 127.0.0.1 (Voreinstellung) eingetragen werden. Im anderen Fall die IP-Adresse des Rechners.



Geben Sie IPV4-Adressen nicht mit führender Null ein!
(Beispiel: 192.168.11.11 statt 192.168.011.011)

Wenn ein DNS-Server vorhanden ist, kann alternativ auch der jeweilige DNS-Name angegeben werden

Wenn Terminals mit aktiverter DHCP-Option eingesetzt werden, dann sollte nicht die IP-Adresse sondern der DHCP-Name des Terminals eingetragen werden. Dieser ist in den Terminals fest eingestellt und kann nicht geändert werden: **intus-<seriennummer>**.

Vorhandene Terminals mit IPV4 Adresse können mit dem Menüpunkt Werkzeuge/Netzwerk Terminalsuche (siehe 3.4.11) im Netz gesucht und die Netzwerkparameter geändert werden.

4.5.3.2 Serviceport und Datenport

Jedem INTUS COM Server ist mindestens eine Portnummer für den Serviceport zugeordnet. Der Serviceport dient nur zur Kommunikation der Server untereinander. Einige INTUS COM Server verfügen auch über einen Datenport, über den Datensätze von und zu den Terminals übertragen werden.

Für INTUS 3000/3450 Server und TCP-Server kann immer nur die Nummer des Serviceports geändert werden. Die Portnummer des Datenports, sofern vorhanden, liegt immer um eins höher.

Für HTTPS-Server können alle Portnummern unabhängig voneinander geändert werden.

Die Voreinstellung der jeweiligen Port-Nummern sollte nur geändert werden, wenn ein Konflikt mit anderen Programmen auftritt, die dieselbe Port-Nummer verwenden. (nähere Informationen finden Sie in 7.2)

4.5.3.3 Server-ID

Jeder Server im INTUS COM wird über zweistellige, alphanumerische Server-ID identifiziert. Diese ID muss eindeutig sein.

4.5.3.4 Messagelevel

Jeder INTUS COM Server protokolliert bestimmte Ereignisse in Abhängigkeit vom eingestellten Messagelevel in einer Log-Datei. Er kann erhöht werden, wenn zusätzliche Meldungen benötigt werden (siehe 5.3). Im Normalbetrieb sollte Level 2 eingestellt sein (Voreinstellung).

4.6 Terminal Management System konfigurieren

Die Konfiguration des Terminal Management System erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für das Terminal Management System wie in 3.3.3.2 beschrieben. Die Konfiguration des Terminal Management System ist auf mehrere Registerblätter verteilt.

4.6.1 Registerblatt Einstellungen

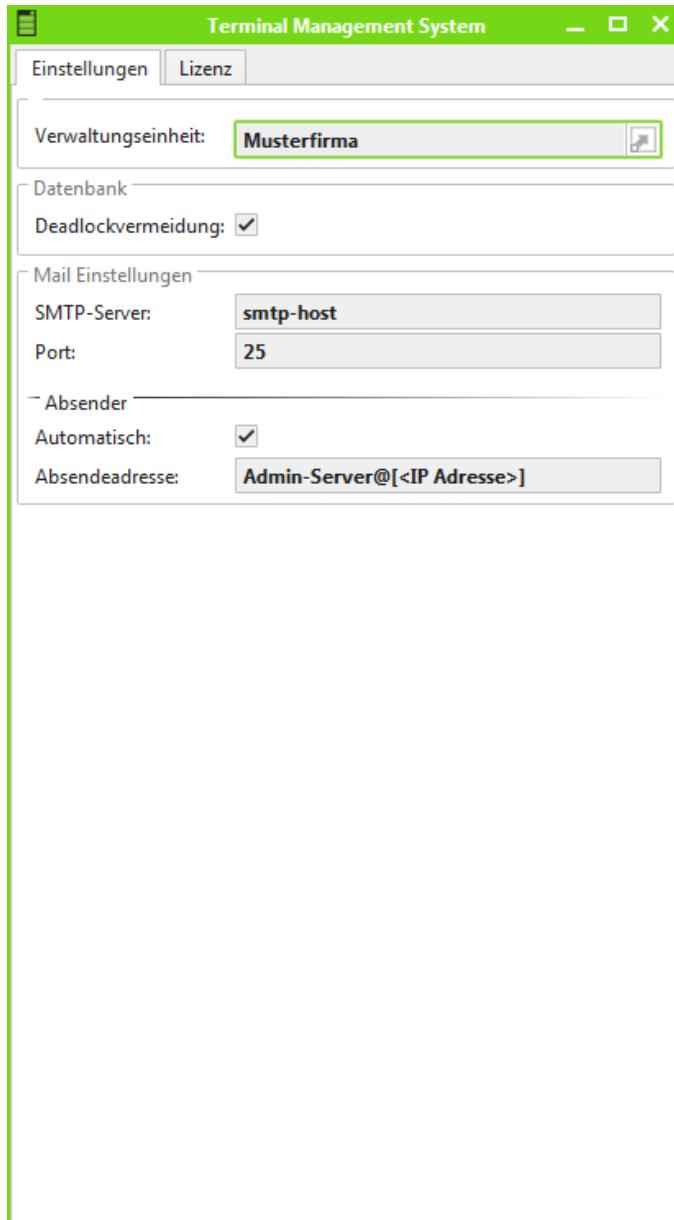


Abbildung 4.1 – Terminal Management System, Einstellungen

Verwaltungseinheit

Siehe 4.5.1.

Datenbank

Deadlockvermeidung verwenden

Ist diese Option ausgewählt, verwenden die INTUS COM Dienste bei Datenbankzugriffen die Prozedur INTUSCOM_LOCK_PROCEDURE zur Deadlockvermeidung.

Die Prozedur INTUSCOM_LOCK_PROCEDURE wird nur für die folgenden Datenbanktypen automatisch durch das Installationprogramm erzeugt:



- Microsoft SQL Server
- Oracle

Mail Einstellungen

SMTP-Server

Rechnername oder IP-Adresse, unter der der SMTP-Server vom Admin-Server angesprochen werden kann.

Port

Der Port des SMTP-Servers (Standard ist 25)

Absender

- Automatisch
Ist dieses Feld ausgewählt, wird automatisch eine Absendeadresse für E-Mail-Benachrichtigungen generiert.
Format: **Admin-Server@[IP-Adresse]** (z.B: Admin-Server@192.168.10.11).
- Absendeadresse
Ist das Feld 'Automatisch' nicht ausgewählt, kann hier eine Absendeadresse für E-Mail-Benachrichtigungen eingegeben werden.

4.6.2 Registerblatt Lizenz

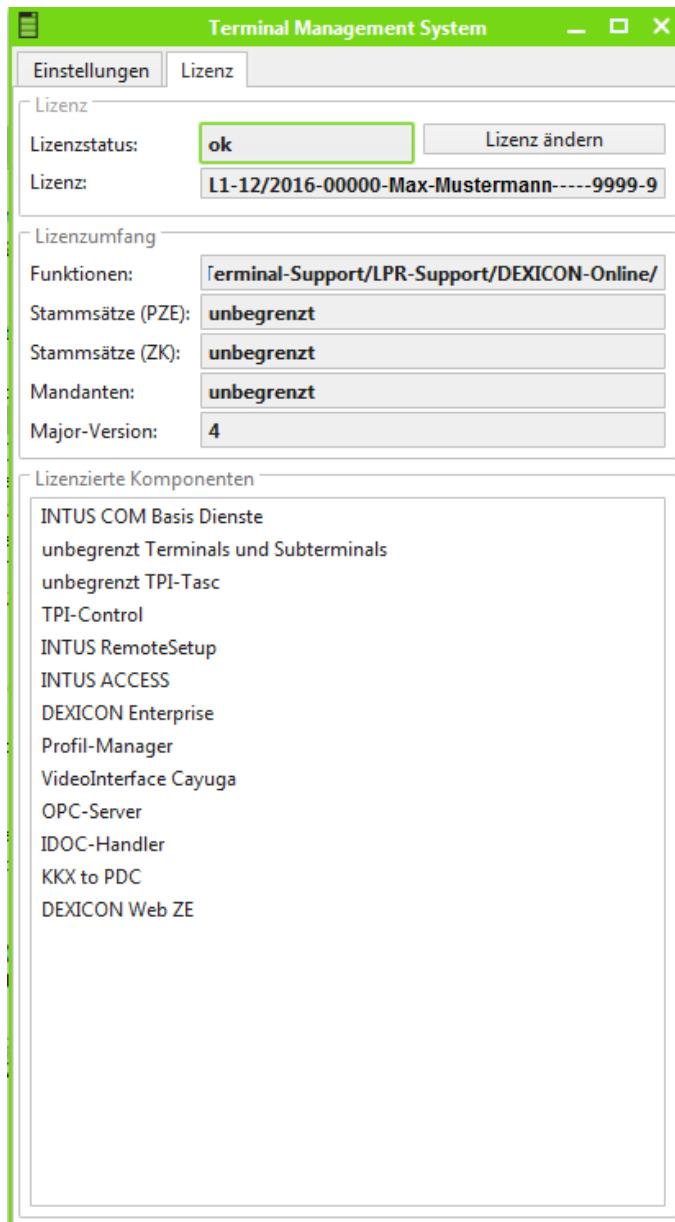


Abbildung 4.2 – Terminal Management System, Lizenz

Lizenz

Zeigt die aktuell verwendete Lizenz an.

Die Schaltfläche zum Ändern der Lizenz ist abweichend vom sonstigen Verhalten nur im Anzeigemodus aktiv.

Lizenzumfang

Zeigt den Lizenzumfang der aktuell verwendeten Lizenz an. Dieser wird durch die Lizenz bestimmt und kann nur über die Eingabe eines anderen Lizenzstrings verändert werden.

Lizenzierte Komponenten

Listet die lizenzierten Komponenten der aktuell verwendeten Lizenz auf. Diese werden durch die Lizenz bestimmt und können nur über die Eingabe eines anderen Lizenzstrings verändert werden.

4.7 Verwaltungseinheit konfigurieren

Die Konfiguration einer Verwaltungseinheit erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für die Verwaltungseinheit wie in 3.3.3.2 beschrieben.

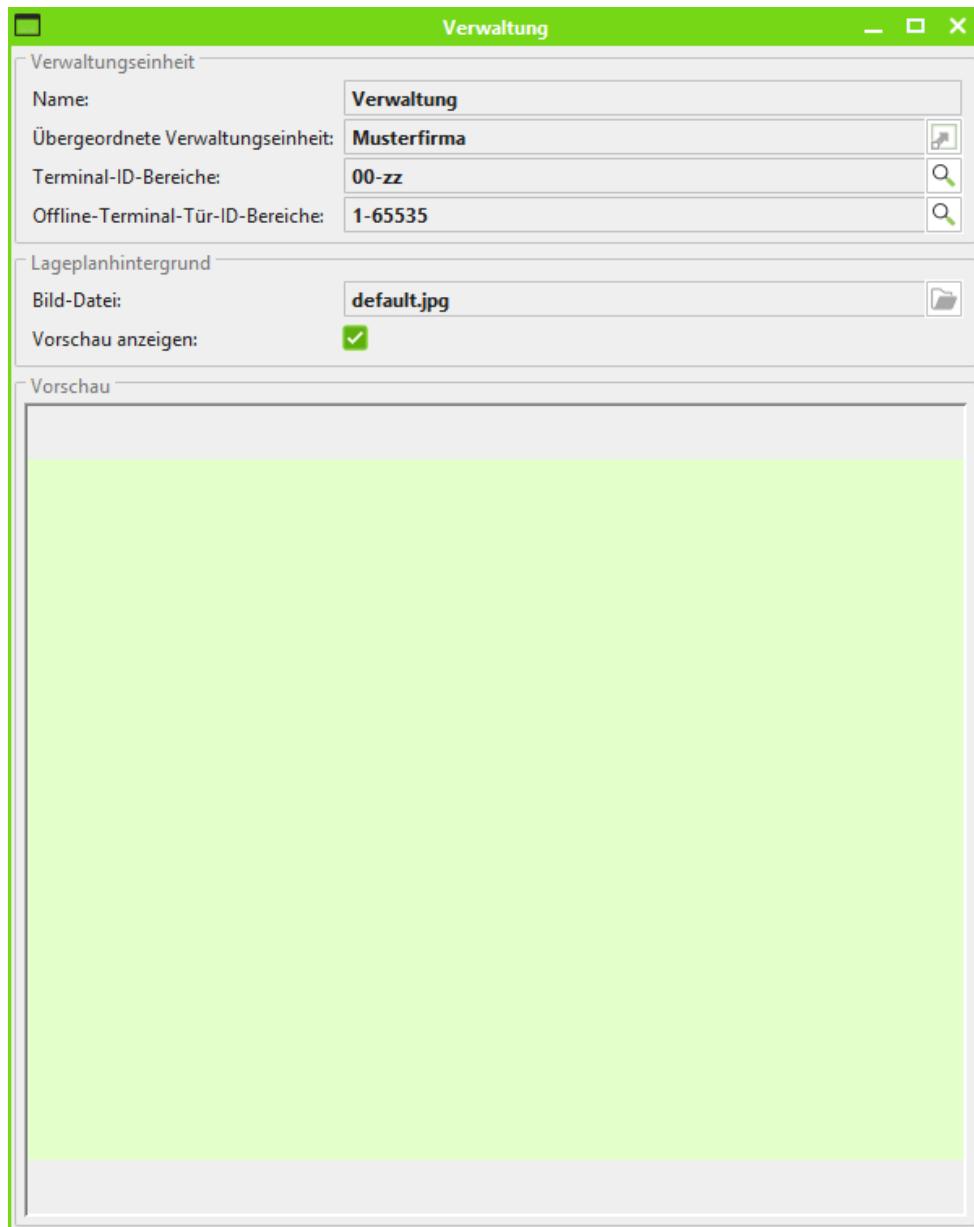


Abbildung 4.3 – Verwaltungseinheit, Grundeinstellungen

Verwaltungseinheit

Name

Anzeigetext zur Identifizierung der Verwaltungseinheit.

Übergeordnete Verwaltungseinheit

Siehe 4.5.1.

Terminal-ID-Bereiche

Ein über einen TCP-Server angebundenes INTUS Terminal/ACM kann einer Verwaltungseinheit nur zugeordnet werden, wenn dessen Terminal-ID in einem für die Verwaltungseinheit zulässigen Terminal-ID-Bereich liegt.

Die zulässigen Terminal-ID-Bereiche (bis zu 10) einer Verwaltungseinheit ergeben sich aus den Terminal-ID-Bereichen der übergeordneten Verwaltungseinheit sowie ggf. weiteren Einschränkungen, die hier eingegeben werden können.

Ausnahme: Der Terminal-ID-Bereich der Wurzelverwaltungseinheit enthält alle zulässigen Terminal-IDs ('00'-'zz') und kann nicht eingeschränkt werden.

Offline-Terminal-Tür-ID-Bereiche

Ein Offlineterminal, das gemäß dem OSS Standard Offline arbeitet, kann einer Verwaltungseinheit nur zugeordnet werden, wenn dessen Tür-ID (Door-ID) in einem für die Verwaltungseinheit zulässigen Tür-ID-Bereich liegt.

Die zulässigen Tür-ID-Bereiche (bis zu 10) einer Verwaltungseinheit ergeben sich aus den Tür-ID-Bereichen der übergeordneten Verwaltungseinheit sowie ggf. weiteren Einschränkungen, die hier angegeben werden können.

Ausnahme: Der Tür-ID-Bereich der Wurzelverwaltungseinheit enthält alle zulässigen Tür-IDs (1-65535) und kann nicht eingeschränkt werden.

Lageplanhintergrund

Bild-Datei

Hier kann ein Hintergrundbild für den Lageplan dieser Verwaltungseinheit angegeben werden (siehe 3.2.11). Zulässige Formate sind Jpeg und Gif-Bilder.

Vorschau anzeigen

Ist dieser Punkt selektiert, so wird das gewählte Hintergrundbild im darunterliegenden Rahmen als Vorschau angezeigt.

4.8 Terminal-Handler konfigurieren

Die Konfiguration des Terminal-Handlers erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für den Terminal-Handler wie in 3.3.3.2 beschrieben. Die Konfiguration des Terminal-Handlers ist auf mehrere Registerblätter verteilt.

4.8.1 Registerblatt Grundeinstellungen

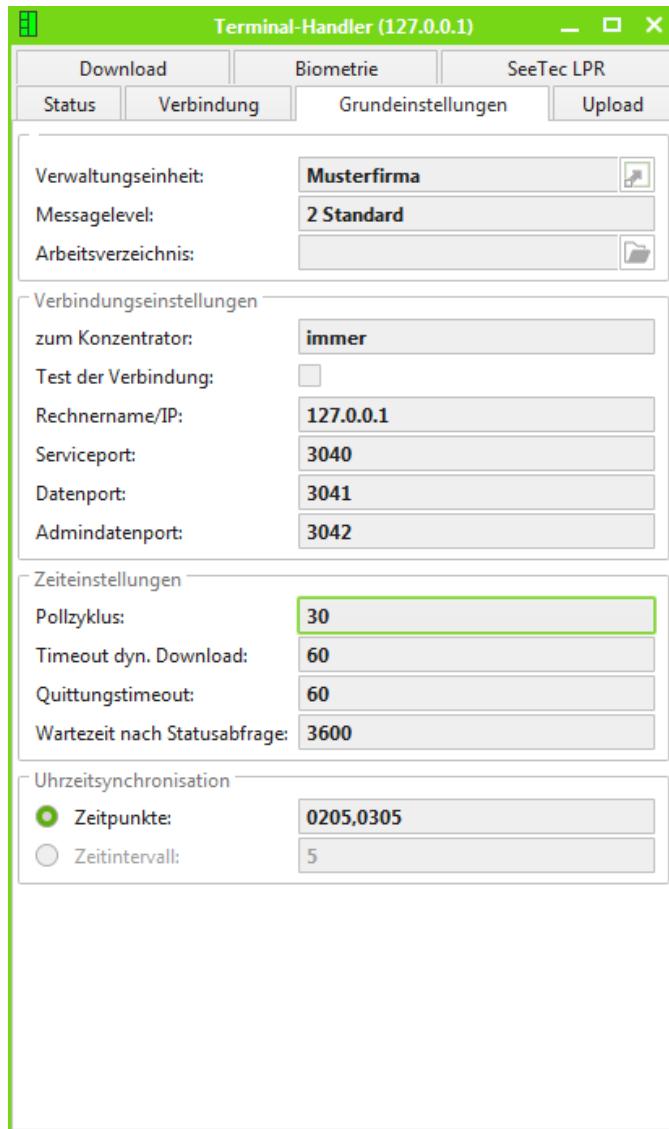


Abbildung 4.4 - Terminal-Handler, Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Arbeitsverzeichnis

Dieses Verzeichnis ist das Arbeitsverzeichnis für die TPI Parameterdateien der Terminals und der statischen und dynamischen INTUS COM Datei-Schnittstelle (siehe 6.1).

PCS empfiehlt, hier das Verzeichnis `work\` einzutragen.

Als Verzeichnisname kann ein UNC Pfadname eingegeben werden.



Die Dateien sind in diesem Verzeichnis oder einem Unterverzeichnis bereitzustellen. Sie werden in den Konfigurationsdialogen der Terminals und Subterminals konfiguriert. Eine Datei kann beliebig vielen Terminals zugeordnet werden.

Verbindungseinstellungen

zum Konzentrator

Bezüglich der Verbindung des Terminal-Handlers zum Konzentrator gibt es zwei Modi:

1. **bei Verbindung mit Applikation:** Wenn die Applikation die TCP/IP-Schnittstelle verwendet, kann sich der Terminal-Handler so wie Konzentrator und TCP-Server verhalten, nämlich dass er die Verbindung nach unten nur dann aufbaut, wenn er nach oben (zur Applikation) eine Verbindung hat.
2. **immer:** (Voreinstellung) Soll der Terminal-Handler dagegen auch ohne Verbindung zur Applikation arbeiten, dann muss eingestellt werden, dass er die Verbindung nach unten (zum Konzentrator) immer aufbaut. Dies ist insbesondere dann nötig, wenn nicht die TCP/IP-Schnittstelle, sondern nur die Dateischnittstelle verwendet wird.

Test der Verbindung

Weiterhin kann eingestellt werden, dass der Terminal-Handler im Abstand von ca. einer Minute leere Datensätze an die Terminals (die online sind) sendet. Dadurch können (unter Windows) Unterbrechungen der Verbindung früher erkannt werden (nach ca. 3 Minuten). Bei Verwendung dieser Option im Zusammenhang mit `dialup`- oder `auto`-Terminals am TCP-Server ist Vorsicht geboten. Wenn der Timeout (im TCP-Server) zu groß eingestellt ist, kann es vorkommen, dass die Verbindung nicht wieder getrennt wird.

Rechnername/IP, Serviceport, Datenport, Admin-Datenport

Siehe 4.5.3.

Zeiteinstellungen

Pollzyklus (in s)

Es kann angegeben werden, in welchen Abständen die Datei- bzw. Datenbankschnittstelle gepolt wird. Jeweils nach der angegebenen Zeit wird nachgeschaut, ob neue Daten für den Download bereitstehen oder ob neue Daten für den Upload bereitgestellt werden können.

Timeout dyn. Download

Für den dynamischen Download aus Datei ist ein Timeout anzugeben, nach dem alle dynamischen Sätze für ein Terminal gelöscht werden, wenn keine Übertragung der Sätze möglich ist (z. B. weil das Terminal nicht betriebsbereit ist). Dadurch wird das massenweise Ansammeln nicht übertragbarer Datensätze verhindert.

Quittungstimeout

Für die Zeitspanne, die auf eine Quittung vom Terminal gewartet wird, ist ein Timeout in Sekunden anzugeben.

Wartezeit nach Statusabfrage

Hier ist die Zeitspanne in Sekunden einzutragen, die nach einer Statusabfrage gewartet wird, bevor „`I...SR,77`“ gesendet wird.

Uhrzeitsynchronisation

Die Uhrzeitsynchronisation kann entweder zu einem oder mehreren, fest eingestellten Zeitpunkten, oder in einem regelmäßigen Intervall erfolgen.

Diese Angaben sind nur für Terminals wirksam, für die die Einstellung der Uhrzeit durch den Terminal-Handler aktiviert ist.

Zeitpunkte

Die Zeitpunkte für die Uhrzeitsynchronisation sind im Format **hhmm** anzugeben und mit Kommas zu trennen. (Es dürfen keine Leerzeichen vor oder nach dem Komma stehen.)

Zeitintervall

Das Zeitintervall für die Uhrzeitsynchronisation ist in Minuten anzugeben. Erlaubt sind Werte zwischen 1 und 999 Minuten.

4.8.2 Registerblatt Upload

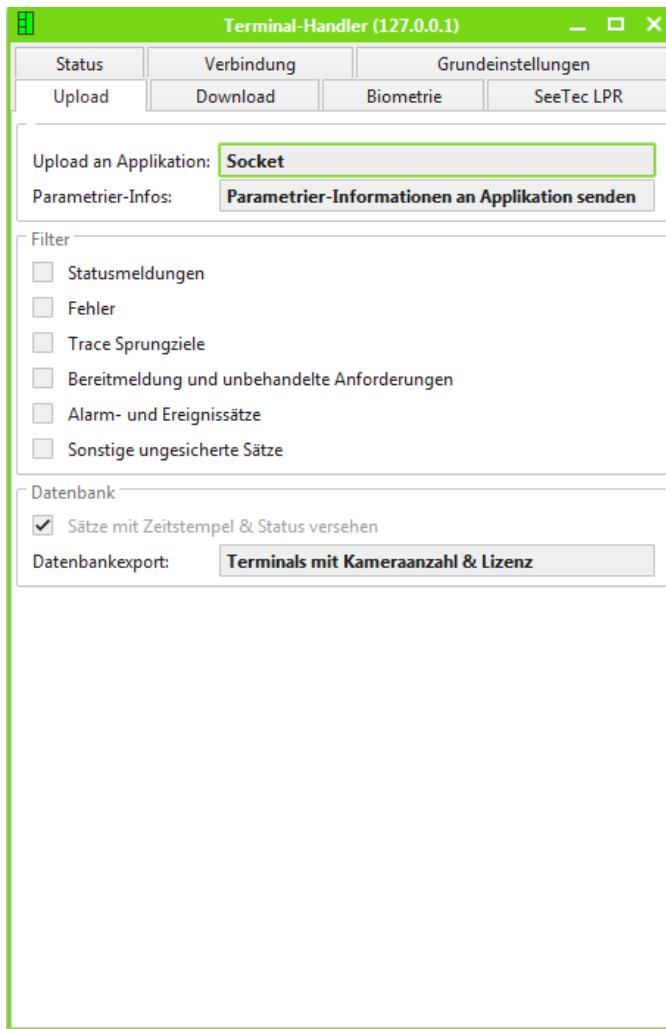


Abbildung 4.5 - Terminal-Handler, Upload

Upload an Applikation

Es kann eingestellt werden, über welche Schnittstellen die Datensätze (die nicht herausgefiltert werden) an die Applikation übergeben werden.

- **Socket** – Die Sätze, die nicht herausgefiltert wurden, werden über die Socket-Schnittstelle übergeben. Die Quittierung gesicherter Sätze erfolgt durch die Applikation. Wenn die Socket-Verbindung nicht besteht, gehen ungesicherte Sätze verloren.
- **nur gesicherte Sätze in Datei** – Alle gesicherten Sätze, die nicht herausgefiltert wurden, werden in die Dateischnittstelle geschrieben und vom Terminal-Handler quittiert. (Gesicherte Sätze sind Notpuffersätze mit Satznummer, wobei die Formate bei TCL und TPI unterschiedlich definiert sind.) Alle ungesicherten Sätze, die nicht herausgefiltert wurden, werden über die Socket-Schnittstelle übergeben. Wenn die Socket-Verbindung nicht besteht, gehen sie verloren.
- **alle in Datei** – Alle Sätze, die nicht herausgefiltert wurden, werden in die Dateischnittstelle geschrieben. Gesicherte Sätze werden vom Terminal-Handler quittiert.
- **gesicherte in Datenbank** – Alle gesicherten TPI-Sätze, die nicht herausgefiltert wurden, werden in die Datenbank geschrieben und vom Terminal-Handler quittiert. Alle anderen Sätze, die nicht herausgefiltert wurden, werden über die Socket-Schnittstelle übergeben. Wenn die Socket-Verbindung nicht besteht, gehen ungesicherte Sätze verloren.

Parametrier-Infos

Hier kann eingestellt werden, ob der INTUS COM Terminal-Handler Parametrierinformationen der Terminals über die Socket-Schnittstelle an eine Applikation weitergeben soll.

- **Parametrier-Informationen an Applikation senden**

Informationen über die Parametrierung der Terminals werden über die Socket-Schnittstelle gesendet.

- **Parametrier-Informationen nicht senden**

Es werden keine Parametrier-Informationen über die Socket-Schnittstelle gesendet.

Filter

Der Terminal-Handler kann Datensätze an der Applikationsschnittstelle filtern. Dies ist dann sinnvoll bzw. notwendig, wenn die Applikation bestimmte Satzarten nicht verarbeiten kann. Die konfigurierbaren Filter gelten unabhängig von der konfigurierten Applikationsschnittstelle (Socket-, Datei- oder Datenbankschnittstelle).

Statusmeldungen

INTUS COM Statusmeldungen (unabhängig davon, ob das Terminal bekannt ist)

Fehler

Fehlermeldungen vom Terminal (MONIN, INTERP, DE).

Trace Sprungziele

Trace-Sprungziele vom Terminal.

Bereitmeldungen und unbehandelte Anforderungen

Anforderungen, auf die der Terminal-Handler einen Download startet, werden gefiltert. Für andere Anforderungen und die Bereitmeldung ist die Filterung konfigurierbar.

Alarm- und Ereignissätze

TPI-Satzart IA

Sonstige ungesicherte Sätze

Datenbank

Sätze mit Zeitstempel & Status versehen

Diese Option bewirkt, dass beim Upload in die Datenbank zu jedem Datensatz ein Zeitstempel mit dem Upload-Zeitpunkt und ein Gültigkeitsstatus gespeichert werden.

Datenbankexport

Es kann eingestellt werden, ob und welche Konfigurationsdaten in die Datenbank exportiert werden.

- **kein Export** – Es werden keine Konfigurationsdaten in die Datenbank exportiert.
- **Terminals & Lizenz** – Die Terminal-Konfiguration wird in die Datenbank exportiert.
- **Terminals mit Kameraanzahl & Lizenz** – Wie „Terminals & Lizenz“. Zusätzlich wird die Anzahl der konfigurierten Kameras pro Terminal exportiert. Diese Option setzt die Datenbankschnittstelle ab der Version 2.8.0 voraus.

4.8.3 Registerblatt Download

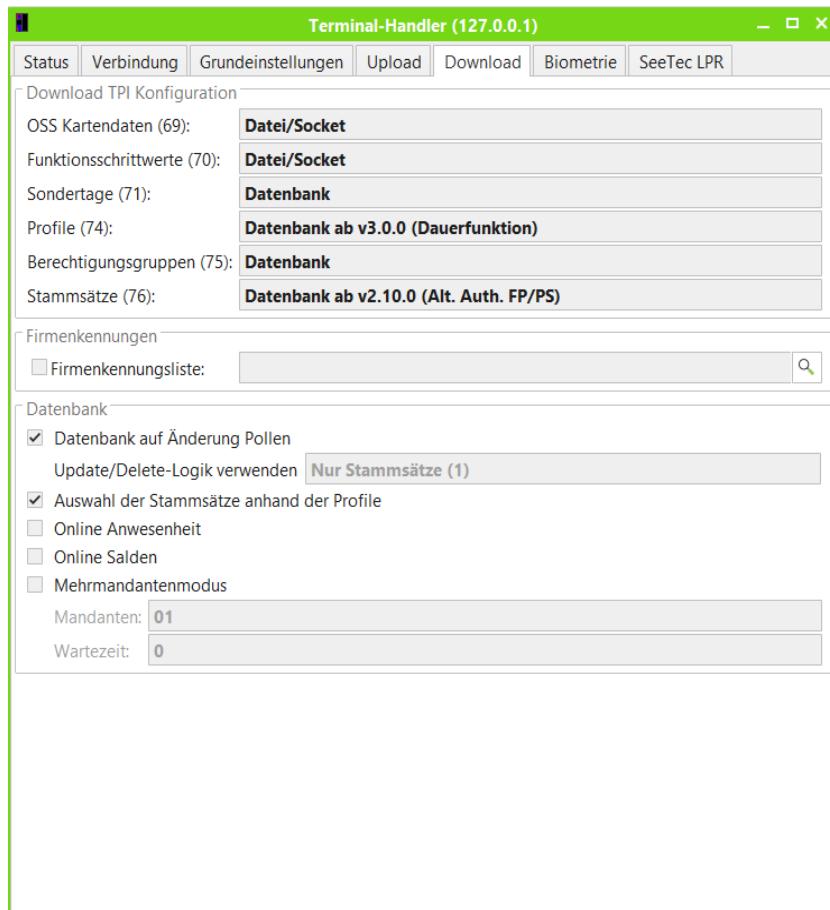


Abbildung 4.6 - Terminal-Handler, Download

Download TPI Konfiguration

OSS Kartendaten (69)

Hier kann die Quelle für die Kartendaten eingestellt werden.

Kartendaten werden für das Schreiben von Berechtigungen für Offlineterminals, die den OSS Standard Offline verwenden, benötigt.

Auswählbar sind:

- Datei/Socket
- Datenbank

Funktionsschrittwerke (70)

Hier kann die Quelle für die Funktionsschrittwerke eingestellt werden. Auswählbar sind:

- Datei / Socket
- Datenbank

Sondertage (71)

Hier kann die Quelle für die Sondertage (neues Sondertagsformat seit INTUS COM 2.0.0) eingestellt werden. Auswählbar sind:

- Datei / Socket
- Datenbank

Profile (74)

Hier kann die Quelle für die Profile eingestellt werden. Auswählbar sind:

- **Datei/Socket**
- **CSV-Dateischnittstelle**
Mit dieser Einstellung werden Profile aus einer csv-Datei in die Datenbank importiert und verwendet.
- **Datenbank bis v1.5.0 (altes Sondertagsformat)**
Mit dieser Einstellung werden Sondertage mit der Parameterdatei (Download 73) auf die Terminals geladen.
- **Datenbank ab v2.0.0**
Mit dieser Einstellung werden die Sondertage mit der Sondertagsdatei bzw. aus der Sondertagstabelle der Datenbankschnittstelle (Download 71) auf die Terminals geladen.
- **Datenbank ab v2.4.0 (befristete Profile)**
Mit dieser Einstellung können Profile zeitlich begrenzt werden. Das veranlasst den Terminal-Handler beim Download eines Profiles, das Profil gegen das aktuelle Datum zu prüfen, bevor es auf das Terminal geladen wird.
- **Datenbank ab v2.10.0 (Funktionsumschaltung)**
Mit dieser Einstellung können die Profile für die zeitliche Funktionsumschaltung verwendet werden.
- **Datenbank ab v3.0.0 (Dauerfunktion)**
Mit dieser Einstellung können Dauerfunktion und der Profilgesteuerten alternativen Authentifizierung verwendet werden.

Berechtigungsgruppen (75)

Hier kann die Quelle für die Berechtigungsgruppen eingestellt werden. Auswählbar sind:

- Datei/Socket
- Datenbank

Stammsätze (76)

Hier kann die Quelle für die Stammsätze eingestellt werden. Auswählbar sind:

- Datei/Socket
- CSV-Dateischnittstelle
Stammsätze werden von einer csv-Datei gelesen und in die Datenbank importiert.
- Datenbank
- Datenbank ab 2.10.0 (Alt. Auth. FP/PS)
Mit dieser Einstellung kann bei der alternativen Authentifizierung die Biometrieart (Fingerprint, PalmSecure) unterschieden werden.
- Datenbank ab v3.3.0 (Gesperrte Sätze)
Wird die Unterscheidung zwischen gesperrten und nicht vorhandenen Stammsätzen in der Parametrierung eines Terminals nicht unterstützt, so werden gesperrte Stammsätze behandelt als wären sie nicht vorhanden.

Firmenkennungen**Firmenkennungsliste**

Hier kann eine Liste von bis zu 20 Firmenkennungen eingetragen werden. Bei aktiviertem Kontrollfeld werden diese Firmenkennungen anstelle der Firmenkennungen aus den Parameterdateien verwendet.

Datenbank

Datenbank auf Änderung Pollen

Diese Option ermöglicht den automatischen Download aus der Datenbank über das Setzen von Zeitstempeln.

Update/Delete-Logik verwenden

Die Update/Delete-Logik ermöglicht den Download einzelner Update/Delete-Sätze (für Stammdaten und OSO-Kartendaten-IDs=). Diese Option ist nur verfügbar, wenn auch die Option **Datenbank auf Änderungen pollen** aktiviert ist.

Auswahl der Stammsätze anhand der Profile

Diese Option ermöglicht es, die auf ein Terminal zu ladenden Stammsätze anhand der Profile zu selektieren, so dass nicht alle Stammsätze auf alle Terminals geladen werden müssen.

Online Anwesenheit

Wenn diese Option eingeschaltet ist, antwortet der Terminal-Handler auf TPI Online-Anfragen, die einen Anwesenheitsstatus "K" oder "G" enthalten, indem er eine positive oder negative Antwort (Online Rückmeldung R1,R2) sendet (soweit der Stammsatz für die betreffende Ausweisnummer in der Datenbank gefunden wird und sein Anwesenheitsstatus nicht null ist). Außerdem werden der ATTENDANCE_STATUS und zugehörige Felder im Stammsatz geändert, wenn Buchungen in die Datenbank gespeichert werden. Diese Option ist nur relevant, wenn der Download von Stammsätzen aus der Datenbank eingeschaltet ist.

Online Salden

Wenn diese Option eingeschaltet ist, antwortet der Terminal-Handler auf TPI Online-Anfragen der Satzart "SA", indem er die Salden (Online Rückmeldung R4) sendet (soweit der Stammsatz für die betreffende Ausweisnummer in der Datenbank gefunden wird). Diese Option ist nur relevant, wenn der Download von Stammsätzen aus der Datenbank eingeschaltet ist.

Mehrmandantenmodus / Mandanten

Der Mehrmandantenmodus kann nur verwendet werden, wenn der Download der Stammdaten aus der Datenbank erfolgt. Mit Mandant ist ein System (eine Anwendung) gemeint, die Stammdaten bereitstellt. Jedem Mandant ist eine 2 oder 10-stellige alphanumerische Kennung zugeordnet. Im Mehrmandantenmodus werden nur die Stammdaten der konfigurierten Mandanten auf das Terminal geladen. Beim Upload von Buchungen in die Datenbank, wird der Mandant dann anhand der Stammdatentabelle bestimmt und mit in die Buchungstabelle eingetragen. Wenn der Mandant nicht bestimmt werden kann, werden Leerzeichen eingetragen.

10-stellige und 2-stellige Mandantenkennungen können nicht gleichzeitig verwendet werden.

Wartezeit

Wenn der Mehrmandantenmodus verwendet wird, kann eine Wartezeit angegeben werden. Diese Zeit wird nach einer Änderung des Zeitstempels für die Stammdaten-Grundversorgung gewartet. Erst wenn sich der Zeitstempel innerhalb dieser Zeit nicht mehr ändert, wird die Grundversorgung gestartet. (Auf diese Weise können unnötige mehrfache Grundversorgungen vermieden werden, die entstehen würden, wenn die einzelnen Mandanten nacheinander den Zeitstempel aktualisieren.)



4.8.4 Registerblatt Biometrie

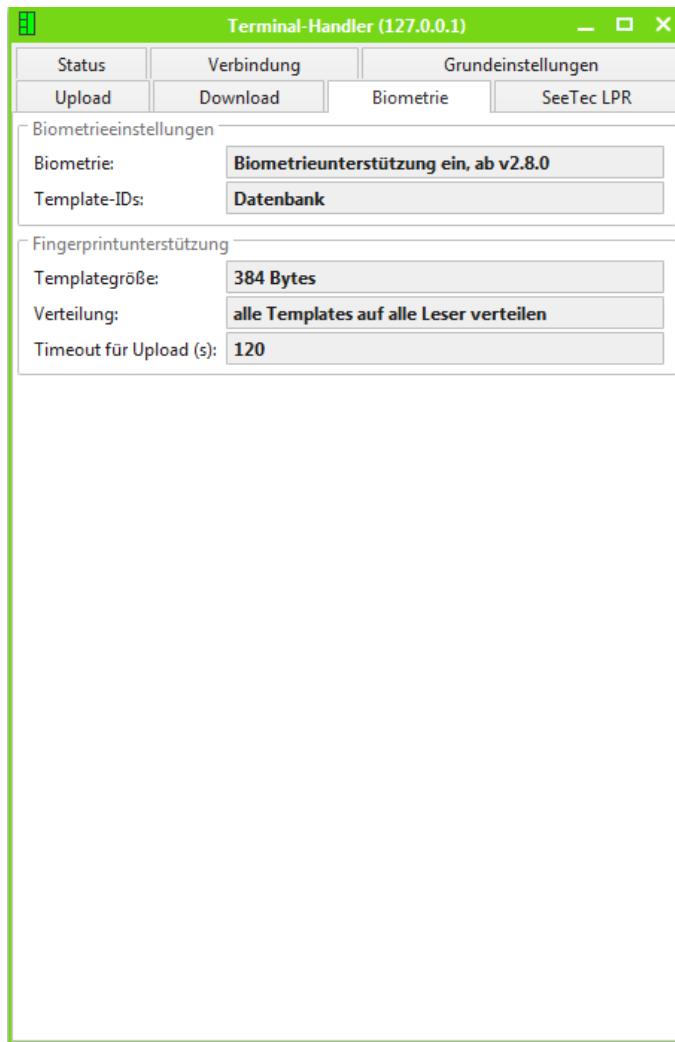


Abbildung 4.7 - Terminal-Handler, Biometrie

Biometrieeinstellungen

Biometrie

Durch diesen globalen Parameter wird die Template-Verwaltung durch den Terminal-Handler eingeschaltet.

- **Keine Biometrieunterstützung** – Die Biomtrieunterstützung durch den Terminal-Handler ist deaktiviert.
- **Biometrieunterstützung ein, bis v2.7.2**– Die Biomtrieunterstützung durch den Terminal-Handler ist aktiv. Die Templatequalität wird ignoriert.
- **Biomtrieunterstützung mit Templatequalität** – Die Biometrieunterstützung mit Templatequalität durch den Terminal-Handler ist aktiv. Diese Option benötigt die Datenbankschnittstelle in einer Version ab 2.8.0.

Templates-IDs

Durch diesen Parameter wird die Quelle der Template-IDs eingestellt (siehe 6.4.6.2). Zur Auswahl steht

- Datenbank
- csv-Datei

Fingerprintunterstützung

Template-Größe

Gibt die Anzahl der Bytes für die binäre Darstellung eines Templates an. Folgende Werte sind auswählbar:

- 256
- 384

Verteilung

Für die Verteilung von Templates auf die Leser, für die der Template-Download eingeschaltet ist, gibt es folgende Einstellmöglichkeiten:

- Alle Templates auf alle Leser verteilen
- Templates anhand der Stammsätze und Profile verteilen

Durch die Einstellung „Templates anhand der Stammsätze & Profile verteilen“ werden beim Download der FP-Templates die Datenbanktabellen INTUSCOM_MASTER_RECORDS und INTUSCOM_PROFILES zur Auswahl der FP-Templates herangezogen.

Timeout für Upload

Gibt an, wie viele Sekunden nach einer Uploadanforderung die vollständige Antwort vom Terminal vorliegen soll.

4.8.5 Registerblatt SeeTec LPR

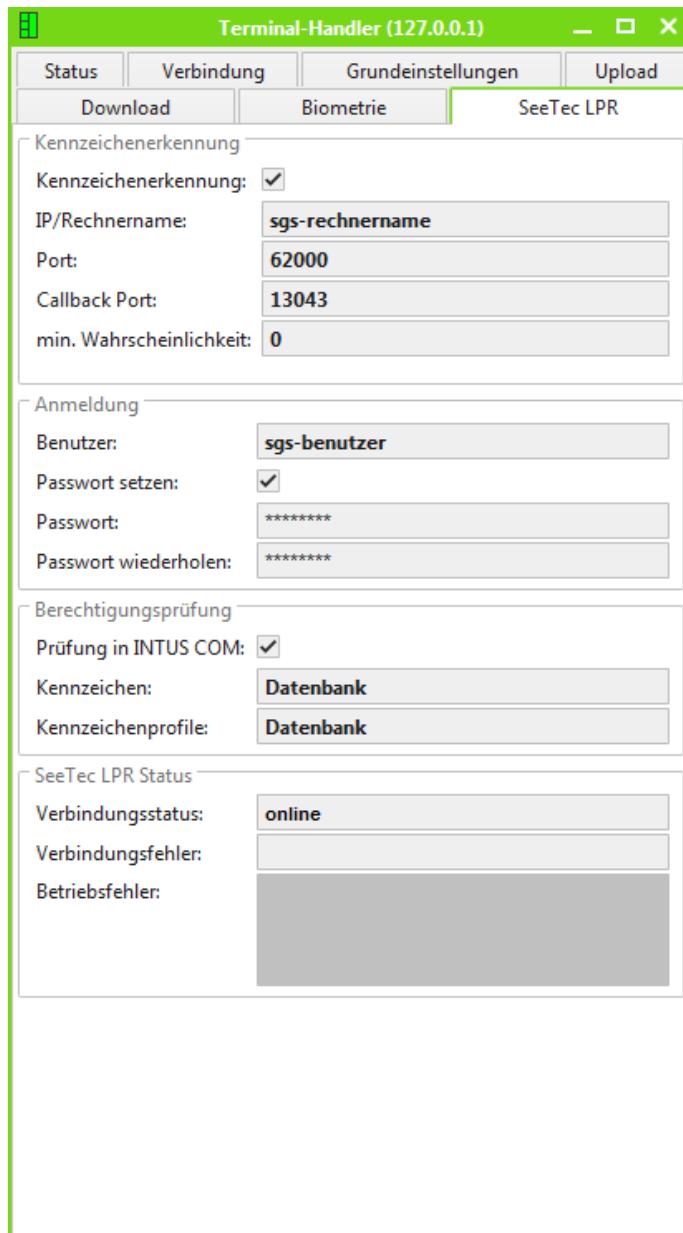


Abbildung 4.8 – Terminal-Handler, SeeTec LPR

Kennzeichenerkennung

Kennzeichenerkennung

Durch diesen globalen Parameter wird die Kennzeichenerkennungs-Unterstützung in INTUS COM aktiviert.

IP/Rechnername

Rechnername oder IP-Adresse des SeeTec Gateway Service.

Port

Port, auf dem der SeeTec Gateway Service auf Verbindungen wartet (Standardport 62000).

Callback Port

Port auf dem INTUS COM auf Callbacks des SeeTec Gateway Service wartet (Standardport 13043).

Min. Wahrscheinlichkeit

Der SeeTec Gateway Service liefert zu jedem erkannten Kennzeichen einen Wahrscheinlichkeitswert. Die mindest Wahrscheinlichkeit bestimmt ab wann ein Kennzeichen von INTUS COM als erkannt angesehen wird.

Anmeldung

Benutzer

Benutzername, mit dem sich INTUS COM am SeeTec Gateway Service anmeldet.

Passwort setzen

Ist diese Option gesetzt, werden die Passwort-Eingabefelder aktiviert. Beim Speichern wird das eingegebene Passwort übernommen.

Passwort

Hier muss das Passwort für den SeeTec Gateway Service Benutzer eingegeben werden.

Passwort wiederholen

Hier muss das Passwort für den SeeTec Gateway Service Benutzer ein zweites mal eingegeben werden.

Berechtigungsprüfung

Prüfung in INTUS COM

Mit dieser Option wird die Berechtigungsprüfung für erkannte Kennzeichen in INTUS COM aktiviert.

Kennzeichen

Durch diesen Parameter wird die Quelle der Kennzeichen eingestellt. Zur Auswahl steht

- Datenbank
- CSV-Datei

Kennzeichenprofile

Durch diesen Parameter wird die Quelle der Kennzeichenprofile eingestellt. Zur Auswahl steht

- Datenbank
- CSV-Datei

4.9 Konzentrator konfigurieren

Die Konfiguration des Konzentrator erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für den Konzentrator wie in 3.3.3.2 beschrieben.

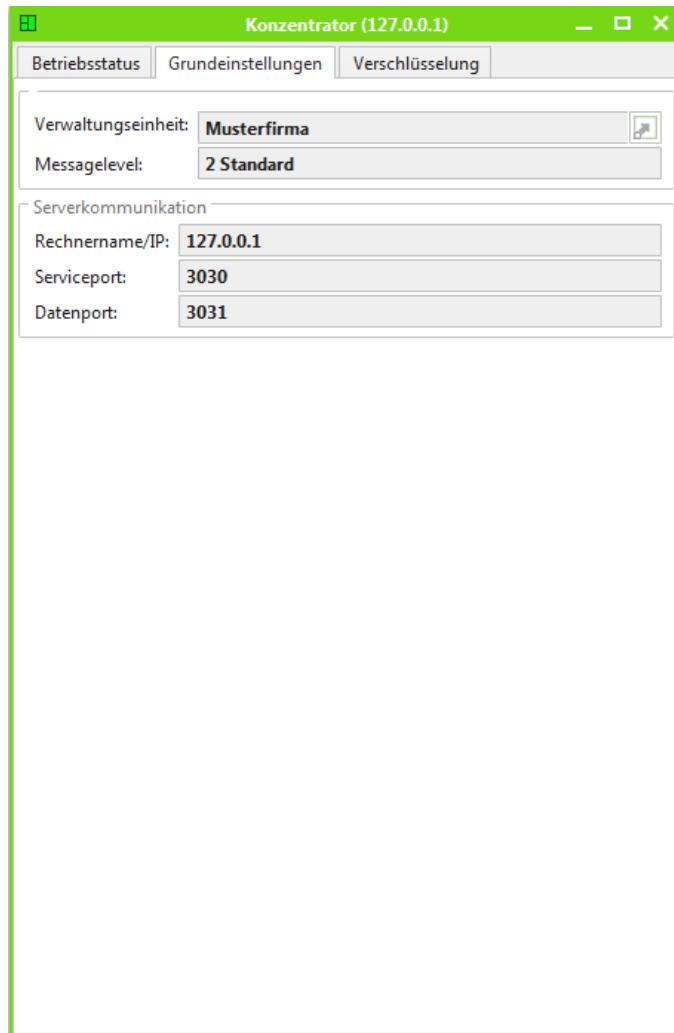


Abbildung 4.9 - Konzentrator, Grundeinstellungen

4.9.1 Registerblatt Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Serverkommunikation

Rechnername/IP, Serviceport, Datenport

Siehe 4.5.3.

4.9.2 Registerblatt Verschlüsselung

An dieser Stelle kann der Schlüssel gesetzt werden, den der Konzentrator verwendet, um mit INTUS 3000/3450 Server verschlüsselt zu kommunizieren.

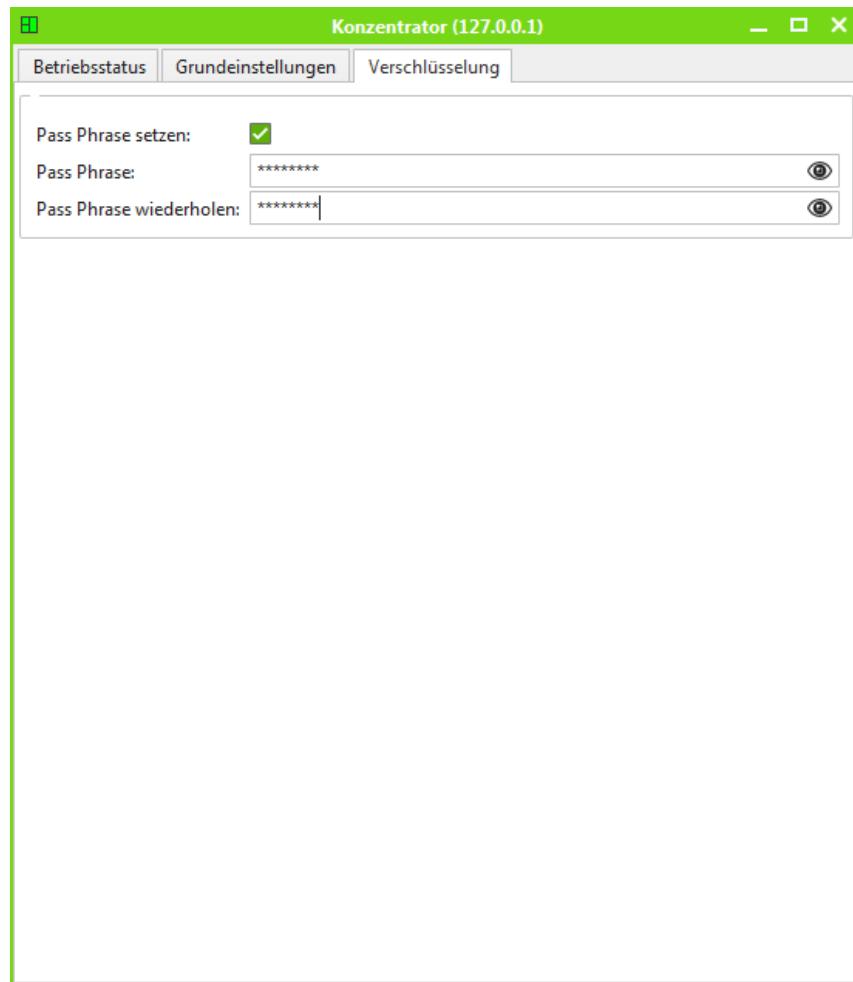


Abbildung 4.10 - Konzentrator, Verschlüsselung

Pass Phrase setzen

Hier kann eingestellt werden, dass der Schlüssel für die verschlüsselte Kommunikation geändert werden soll.

Pass Phrase

Hier kann die neue Pass Phrase eingegeben werden.

Pass Phrase wiederholen

Hier muss die neue Pass Phrase zur Bestätigung wiederholt werden.

4.10 TCP-Server konfigurieren

Die Konfiguration des TCP-Server erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für den TCP-Server wie in 3.3.3.2 beschrieben.



Abbildung 4.11 - TCP-Server, Grundeinstellungen

4.10.1 Registerblatt Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Server aktiviert

Hier kann eingestellt werden, ob der TCP-Server aktiviert oder deaktiviert ist.

Serverkommunikation

Rechnername/IP, Serviceport, Datenport, Server-ID

Siehe 4.5.3.

Konzentrator

Konzentrator mit dem der TCP-Server verbunden ist.

Timeout

Der Timeout gibt die Zeit an, nach der die Verbindung zu einem Terminal im Modus „dialup“ oder „auto“ getrennt wird, wenn keine Daten mehr übertragen werden (siehe 4.10.3).

Wenn Sie den Terminal-Handler leere Datensätze senden lassen (siehe 4.8), sollten Sie diesen Parameter nicht zu groß einstellen. Sonst wird die Verbindung wegen dieser leeren Sätze nicht wieder getrennt. Auch Lebendmeldungen vom Terminal sind zu berücksichtigen, falls solche verwendet werden.

Verbindung zu Terminals

Überwachung

Hier kann die Überwachung der Verbindung zum Terminal mittels Keepalive-Paketen ein- bzw. ausgeschaltet werden. Durch die Überwachung mit Keepalive-Paketen wird ein Verbindungsproblem schneller erkannt.

Wartezeit

Hier kann die Wartezeit bis das erste Keepalive-Paket nach dem Verbindungsauftbau gesendet wird eingestellt werden.

4.10.2 Registerblatt Verschlüsselung

An dieser Stelle kann der Schlüssel gesetzt werden, den der TCP-Server verwendet um mit Terminals verschlüsselt zu kommunizieren.

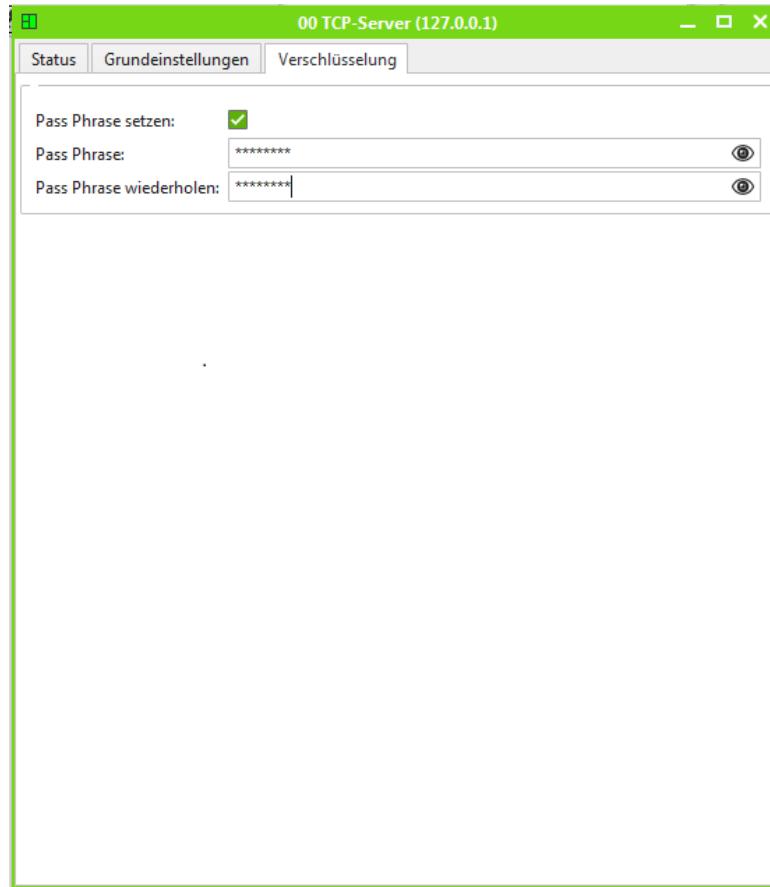


Abbildung 4.12 - TCP-Server, Verschlüsselung

Pass Phrase setzen

Hier kann eingestellt werden, dass der Schlüssel für die verschlüsselte Kommunikation geändert werden soll.

Pass Phrase

Hier kann die neue Pass Phrase eingegeben werden.

Pass Phrase wiederholen

Hier muss die neue Pass Phrase zur Bestätigung wiederholt werden.

4.10.3 Terminalkommunikation über RAS-Verbindungen

Der TCP-Server unterstützt 3 Modi für den Verbindungsaufbau zu einem Terminal. Die Einstellung erfolgt für jedes am TCP-Server angeschlossenen Terminal getrennt (siehe 4.13.2).

1. direct

Die Verbindung wird immer aufgebaut, wenn der TCP-Server eine Verbindung an seinem Applikationsport hat. (Wenn der Konzentrator eingesetzt wird, heißt das, wenn der TCP-Server eine Verbindung zum Konzentrator hat.)

2. dialup

Die Verbindung wird nur zu bestimmten Zeitpunkten aufgebaut.

3. auto

Die Verbindung wird zu bestimmten Zeiten aufgebaut. Zusätzlich wird die Verbindung aufgebaut, wenn Daten für ein Terminal anhängig sind.

Bei den Modi „dialup“ und „auto“ werden die Verbindungen wieder abgebaut, sobald über eine bestimmte Zeitdauer keine Daten mehr über die Verbindung gehen. Diese Zeitdauer (Timeout) kann im TCP-Server konfiguriert werden.

4.10.4 TCP-Server ohne INTUS COM Client konfigurieren



Wenn der TCP-Server in Verbindung mit anderen INTUS COM Komponenten eingesetzt wird, muss er über den INTUS COM Client konfiguriert werden.

Wenn der TCP-Server eigenständig eingesetzt wird, müssen folgende Konfigurationsdaten in der Datei `tcp_server.ini` eingetragen werden:

[TCP-Server]

Schlüssel	Beispiel	Beschreibung
Messagelevel	Messagelevel=2	Der Messagelevel des Prozesses (0 – 7)
ServerID	ServerID=00	2 Byte Server ID. Allen Paketen die nach oben gesendet werden wird diese ID vorangestellt. Ist dieser Parameter nicht konfiguriert (ServerID=) bzw. fehlt dieser Parameter in der Datei <code>tcp_server.ini</code> , so wird als Server-ID zwei Leerzeichen verwendet um einen Kompatibilitätsmodus zum INTUS 3000/3450 Server zu erreichen.
Port	Port=3020	Der Port, mit dem der TCP-Server angesprochen wird (Serviceport). Ist hier nichts eingetragen wird der Standardport 3020 verwendet. Als Datenport wird automatisch <Serviceport>+1 verwendet. Standard=3021.
Timeout	Timeout=60	Timeout in Sekunden Ist ein Terminal als dialup oder auto konfiguriert, so wird nach Ablauf der eingestellten hier Sekunden ohne Datentransfer vom oder zum Terminal, die Verbindung getrennt.
StatusMsgs	StatusMsgs=1	Senden von Statusmeldungen. 0: keine Statusmeldungen (kompatibel zum INTUS 3000/3450 Server). 1: Statusmeldungen werden gesendet.
License		INTUS COM Lizenz
KeepAlive-Enabled	KeepAlive-Enabled=1	Legt fest, ob die Verbindungen zu den Terminals mittels Keepalive-Paketen überwacht werden soll.

KeepAliveIdleTime	KeepAliveIdleTime=5	0: keine Überwachung mit Keepalive-Paketen 1: Verbindungen zu den Terminals werden überwacht (default). Zeitdauer in Sekunden, die vor Senden von Keepalive-Paketen an Terminals gewartet werden soll (5 - 600).
-------------------	---------------------	--

[Terminals]

In der Sektion Terminals werden die logischen Adressen der Terminals verwaltet, der Schlüssel hierfür ist von 1 aufsteigend durchnummertiert.

1=01
2=aa
3=09
4=..

Danach folgen die Terminalerträge, für jede Terminal-ID eine eigene Sektion.

[01]
[02]
...

Schlüssel	Beispiel	Beschreibung
Active	Active=1	Legt fest, ob das Terminal im TCP-Server aktiv ist. 0: deaktiviert 1: aktiv (Standard)
Encryption	Encryption=0	Legt fest, ob für dieses Terminal die Kommunikation verschlüsselt wird. 0: keine Verschlüsselung 1: Verschlüsselung wird verwendet
HostAddress	HostAddress=192.168.11.11 HostAddress=INTUS01	IP Adresse des Terminals oder DNS Name.
Port	Port=3001	Portadresse des Terminals (Standard=3001)
Mode	Mode=direct	Art der Verbindung. direct: Verbindung zum Terminal wird immer aufgenommen. dialup: Verbindung wird nur zu festen Zeiten aufgenommen. auto: Verbindung wird bei Bedarf hergestellt.
Location	Location=INTUS 3100	Standort des Terminals (Optional)
Dialup	Dialup=*-*-00 (jede volle Stunde Dialup=-00-00,*-03-00,*-06-00,*-09-00,... (alle 3 Stunden)	Kommagetrennte Liste der Zeiten, zu denen eine Verbindung zum Terminal aufgenommen wird. d-hh-mm d: Wochentag (0=Sonntag, 1= Montag, 2=... hh: Stunden

mm: Minuten

4.11 HTTPS-Server konfigurieren

Die Konfiguration des HTTPS-Server erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für den HTTPS-Server wie in 3.3.3.2 beschrieben.



Bei Änderungen an den Portnummern schließt der HTTPS-Server alle seine Verbindungen und liest seine Konfigurationsdateien neu ein. Danach baut der HTTPS-Server alle Verbindungen wieder auf.

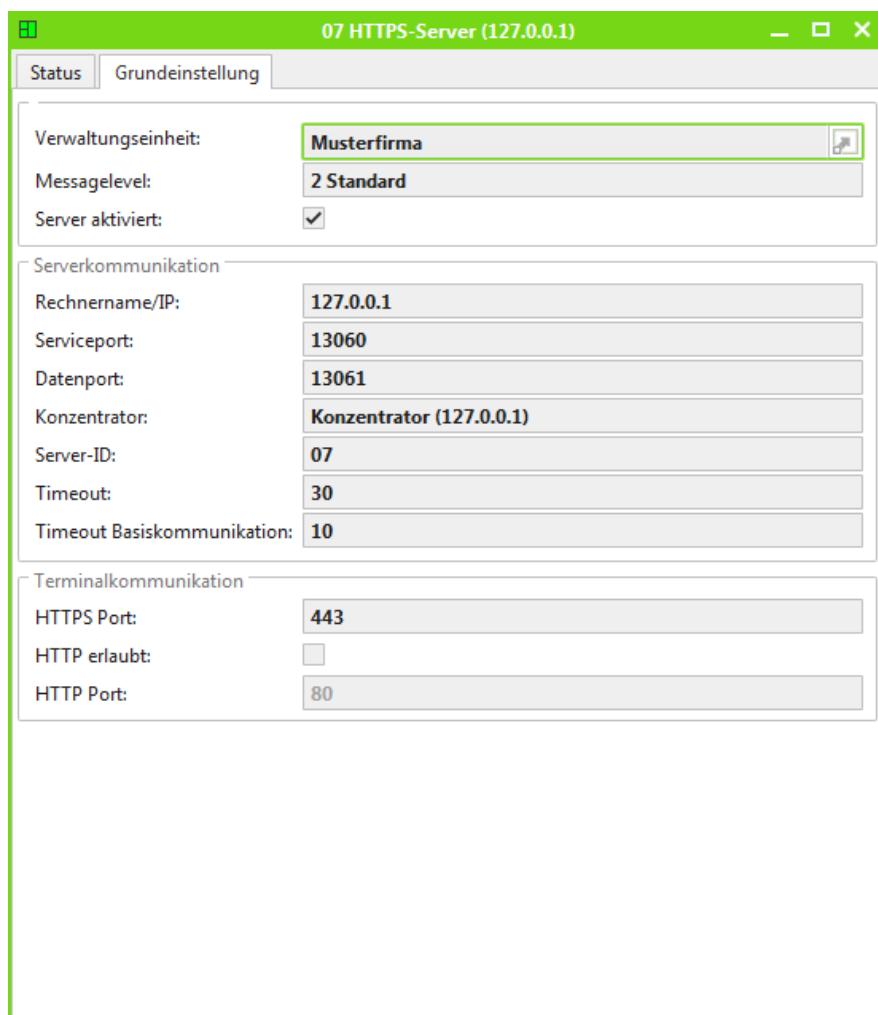


Abbildung 4.13 - HTTPS-Server, Grundeinstellungen

4.11.1 Registerblatt Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Server aktiviert

Hier kann eingestellt werden, ob der HTTPS-Server aktiviert oder deaktiviert ist.

Serverkommunikation

Rechnername/IP, Serviceport, Datenport, Server-ID

Siehe 4.5.3.

Konzentrator

Konzentrator mit dem der HTTPS-Server verbunden ist.

Timeout

Der Timeout gibt die Zeit in Sekunden an, nach welcher der HTTPS-Server Änderungsabfragen des Admin-Servers über seinen Serviceport beantworten soll, falls keine Änderungen vorliegen. Wenn oder sobald Änderungen vorliegen, soll der HTTPS-Server diese sofort beantworten.

Timeout Basiskommunikation

Zeitbeschränkung in Sekunden für ein Request-Zyklus bei der Kommunikation zwischen Admin-Server und HTTPS-Server. Wird die konfigurierte Zeit überschritten, so setzt der Admin-Server den Betriebsstatus Serviceport des HTTPS-Servers sowie alle vom HTTPS-Server empfangene Daten zurück.

Terminalkommunikation

HTTPS Port

Der HTTPS-Port wird für die HTTPS-Kommunikation dieses HTTPS-Servers mit den verbundenen Terminals verwendet.



Nach einer Änderung des HTTPS Port Parameter ist ein Neustart des HTTPS-Servers erforderlich. Der Neustart wird seit Version 1.0.4 des HTTPS-Servers automatisch durchgeführt.

HTTP erlaubt

Hier kann eingestellt werden, ob der HTTPS-Server unverschlüsseltes HTTP für die Kommunikation mit den verbundenen Terminals verwenden darf.

HTTP Port

Falls der HTTPS-Server unverschlüsseltes HTTP für die Kommunikation mit den verbundenen Terminals verwenden darf, wird der HTTP-Port für die HTTP-Kommunikation dieses HTTPS-Servers verwendet.



Nach einer Änderung des dieses Parameters ist ein Neustart des HTTPS-Servers erforderlich. Der Neustart wird seit Version 1.0.4 des HTTPS-Servers automatisch durchgeführt.

4.11.2 Konfiguration des Zertifikatsupdates

Die Konfiguration des Zertifikatsupdates für die über den HTTPS-Server angeschlossenen Terminals erfolgt nicht über den INTUS COM Client, sondern direkt über die Konfigurationsdatei des HTTPS-Servers ([https_server.properties](https://server.properties)). Diese Datei liegt im Arbeitsverzeichnis von INTUS COM im Verzeichnis /conf.

4.11.2.1 Allgemeines

Beim Zertifikatsupdate wird der aktuell verwendete Keystore ausgetauscht.

Damit das Update über den HTTPS-Server funktioniert, muss weiterhin der alte Keystore konfiguriert sein. Zusätzlich muss auch ein weiterer Keystore mit den neuen Zertifikaten konfiguriert werden.

Das Umschalten auf den neuen Keystore wird nach dem erfolgreichen Update der Zertifikate automatisch durchgeführt.

4.11.2.2 Vorbereitung der Keystores

Für das Zertifikatsupdate muss der aktuell verwendete Keystore das aktuelle CA-Zertifikat unter dem Alias „root“ enthalten. Ist dies nicht der Fall, so muss das CA-Zertifikat in den Keystore importiert werden. Zu diesem Zweck kann z.B. der „keytool“-Befehl verwendet werden:

```
keytool -importcert -file <ca.pem> -keystore <CurrentKeystore>.jks  
-alias "root"
```

Auch der neue Keystore muss neben dem Server-Zertifikat das neue CA-Zertifikat unter dem Alias „root“ enthalten.



Es wird empfohlen die Keystores über das mitgelieferte Tool „KeyStoreGen.exe“ zu generieren (siehe 4.11.2.4). In den Default Einstellungen wird das CA-Zertifikat unter dem Alias „root“ im Keystore gespeichert.

Um herauszufinden, ob das CA-Zertifikat korrekt im Keystore hinterlegt ist, kann folgender Befehl verwendet werden:

```
keytool -v -list -keystore <Keystore>.jks
```

4.11.2.3 Manuelles Einstellen des neuen Keystores

Der neue Keystore muss in der Datei https_server.properties eingetragen werden. Dazu müssen folgende Properties gesetzt werden:

- **certificateUpdate.KeyStore**: der neue Keystore
- **certificateUpdate.alias**: Alias, unter dem das Server-Zertifikat im neuen Keystore abgelegt ist
- **certificateUpdate.newKeyStorePassword**: Passwort für den Keystore
- **certificateUpdate.newKeyPassword**: Passwort für das Server-Zertifikat

Die Passwörter werden beim nächsten Start des HTTPS-Servers verschlüsselt und als „certificateUpdate.currentKeyStorePassword“ bzw. „certificateUpdate.currentKeyPassword“ gespeichert. Die Passwörter im Klartext werden dann gelöscht.

Damit der HTTPS-Server die neuen Werte übernimmt, muss er neu gestartet werden.

4.11.2.4 Einstellen des neuen Keystores über KeyStoreGen.exe

Die in Kapitel 4.11.2.3 beschriebenen Einstellungen können über das Tool „KeyStoreGen.exe“ automatisch gesetzt werden. Dazu muss die Option „Konfiguriere den Update-KeyStore“ gewählt werden.

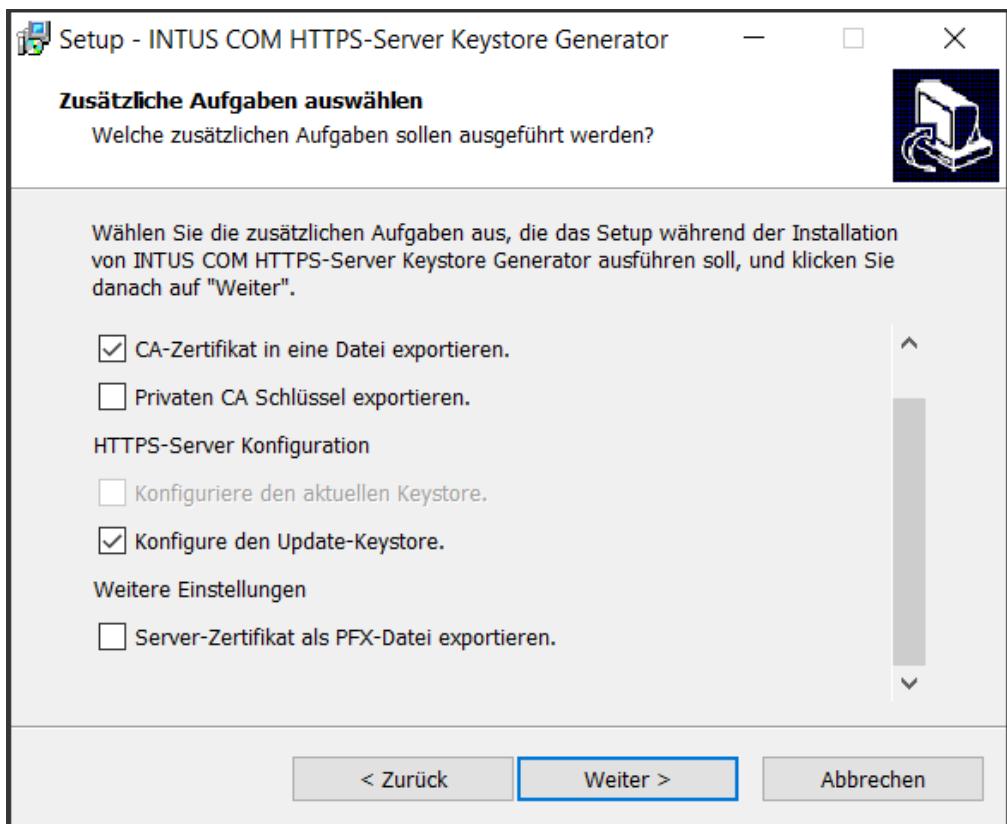


Abbildung 4.14 Konfigurieren des CA-Zertifikat Updates über den Keystore Generator

Diese Option generiert entweder einen neuen Keystore oder importiert bereits vorhandene Zertifikate (siehe 2.3.1.4). Danach werden die Einstellungen für den HTTPS-Server automatisch gesetzt. Der HTTPS-Server muss danach jedoch manuell neu gestartet werden, damit dieser die neuen Einstellungen übernimmt.



Ist bereits ein Keystore unter **certificateUpdate.KeyStore** eingetragen, so kann über das Tool kein weiterer Update-Keystore konfiguriert werden. Dadurch sollen unsaubere Stände verhindert werden.

4.11.2.5 Ablauf des Zertifikatsupdates

Nach dem Neustart des HTTPS-Servers wird für jedes über den HTTPS-Server angebundene Terminal der Zertifikatsdownload ausgelöst. Dazu muss über INTUS RemoteConf für das Terminal die Option „Online-Update“ aktiviert werden.

Vor dem Download wird aus den CA-Zertifikaten des alten und des neuen Keystores eine Zertifikatsdatei (ca.pem) generiert. Diese Datei enthält beide CA-Zertifikate. Sollte bereits eine Datei mit diesem Namen im Verzeichnis /certs vorhanden sein, wird überprüft, ob diese zu den eingestellten Keystores passt. Ist dies der Fall, wird die vorhandene Datei verwendet. Sonst wird die vorhandene Datei vor dem Erstellen der neuen Zertifikatsdatei gesichert.

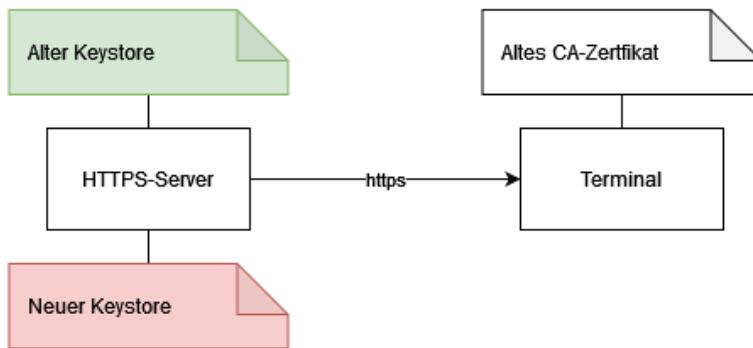


Abbildung 4.15 HTTPS-Server mit altem und neuem Keystore (grün = aktiv, rot = inaktiv)

Diese Datei wird dann auf alle Terminals heruntergeladen, die das neue Zertifikat noch nicht erhalten haben. War der Download erfolgreich, so wird in der Datei `https_terminals.json` für das Terminal der MD5-Hash der Zertifikatsdatei und das Ablaufdatum des Zertifikats gespeichert. Über diese Werte kann überprüft werden, welches Zertifikat verwendet wird.

Um einen Mischbetrieb aus Terminals mit dem alten und dem neuen Zertifikat zu erlauben, wird der HTTPS-Server weiterhin das alte Server-Zertifikat verwenden. Da das Terminal in der Zertifikatsdatei sowohl das alte als auch das neue CA-Zertifikat erhalten hat, kann es das zum Server-Zertifikat passende CA-Zertifikat verwenden.

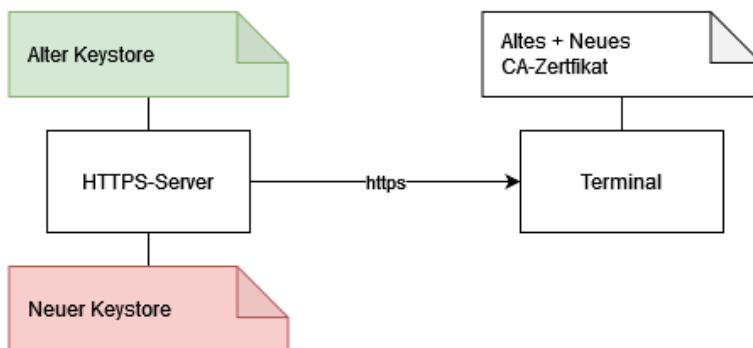


Abbildung 4.16 Das Terminal verwendet beide CA-Zertifikate. Der Server verwendet den alten Keystore (→ Mischbetrieb möglich)

Haben alle Terminals das neue Zertifikat erhalten oder ist das alte Zertifikat abgelaufen, startet sich der HTTPS-Server automatisch neu. Dabei werden die eingestellten Werte für das Zertifikatsupdate als produktive Werte für den HTTPS-Server übernommen. Die Terminals bauen nun ihre Verbindung mit den neuen Zertifikaten auf.

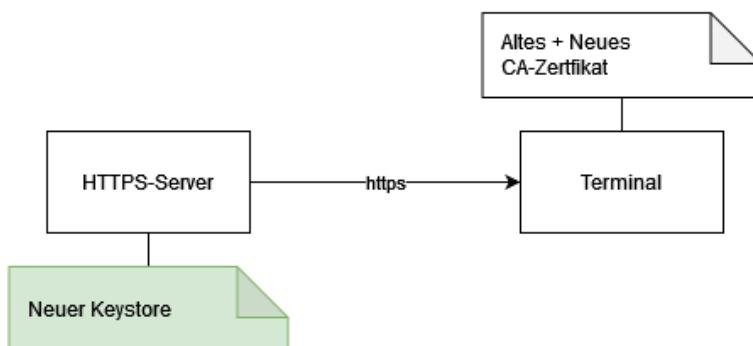


Abbildung 4.17 Das Terminal verwendet beide CA-Zertifikate. Der Server verwendet bereits den neuen Keystore

Um das alte CA-Zertifikat aus dem Terminal zu löschen wird nach dem Umschalten auf den neuen Keystore ein weiterer Download durchgeführt. Bei diesem Download wird nur das neue CA-Zertifikat heruntergeladen. Dadurch wird im Terminal das alte CA-Zertifikat gelöscht.

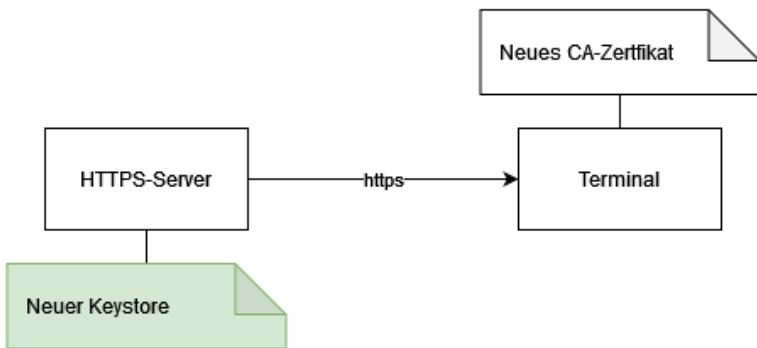


Abbildung 4.18 Das Terminal verwendet nur das neue CA-Zertifikat. Der Server verwendet den neuen Keystore



Es ist zu beachten, dass für deaktivierte Terminals und Terminals im Status „offline“ kein Zertifikatsupdate durchgeführt wird. Sind solche Terminals vorhanden, wird der HTTPS-Server weiterhin das alte Zertifikat verwenden, bis dieses abläuft.



Es wird empfohlen den alten Keystore aufzuheben. Dadurch kann im Falle eines Problems beim Zertifikatsupdate wieder auf den alten Keystore gewechselt werden.

4.11.2.6 Besonderheiten beim Zertifikatsupdate über INTUS RemoteConf

Wird für ein Terminal die Zertifikatsdatei über INTUS RemoteConf eingestellt, so wird trotzdem bei der nächsten Zertifikatsupdateanfrage an den HTTPS-Server (10 Minuten nach Systemboot, dann alle 23 bis 24 Stunden) ein Zertifikatsdownload durchgeführt. Damit wird sichergestellt, dass das CA-Zertifikat des Terminals genau dem im Keystore hinterlegten CA-Zertifikat entspricht. Dies geschieht auch, wenn kein neuer Keystore vorhanden ist.

Ist die Zertifikatsdatei „ca.pem“ im Verzeichnis /certs vorhanden, so wird ein Backup dieser Datei erstellt. Dann wird aus dem CA-Zertifikat des aktuellen Keystores eine neue Zertifikatsdatei namens „ca.pem“ erstellt. Diese wird dann an das Terminal gesendet.

Ist ein neuer Keystore vorhanden, so wird ein normaler Zertifikatsdownload (siehe 4.11.2.5) durchgeführt.

4.11.2.7 Besonderheiten bei Verwendung eines Proxys

Bei Verwendung eines Proxys ist zu beachten, dass die Terminals nach dem Download zum Löschen des alten CA-Zertifikats im Terminal keine Verbindung mehr mit dem Proxy aufbauen können, bis im Proxy das Server-Zertifikat umgestellt wurde.

4.12 INTUS 3000/3450 Server konfigurieren

Der INTUS 3000/3450 Server ist ein Server-Terminal der INTUS Serie. An ihn können INTUS Terminals an zwei RS485-Partylines angeschlossen werden.

Die Konfiguration des INTUS 3000/3450 Server erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für den INTUS 3000/3450 Server wie in 3.3.3.2 beschrieben.

4.12 - INTUS 3000/3450 Server konfigurieren

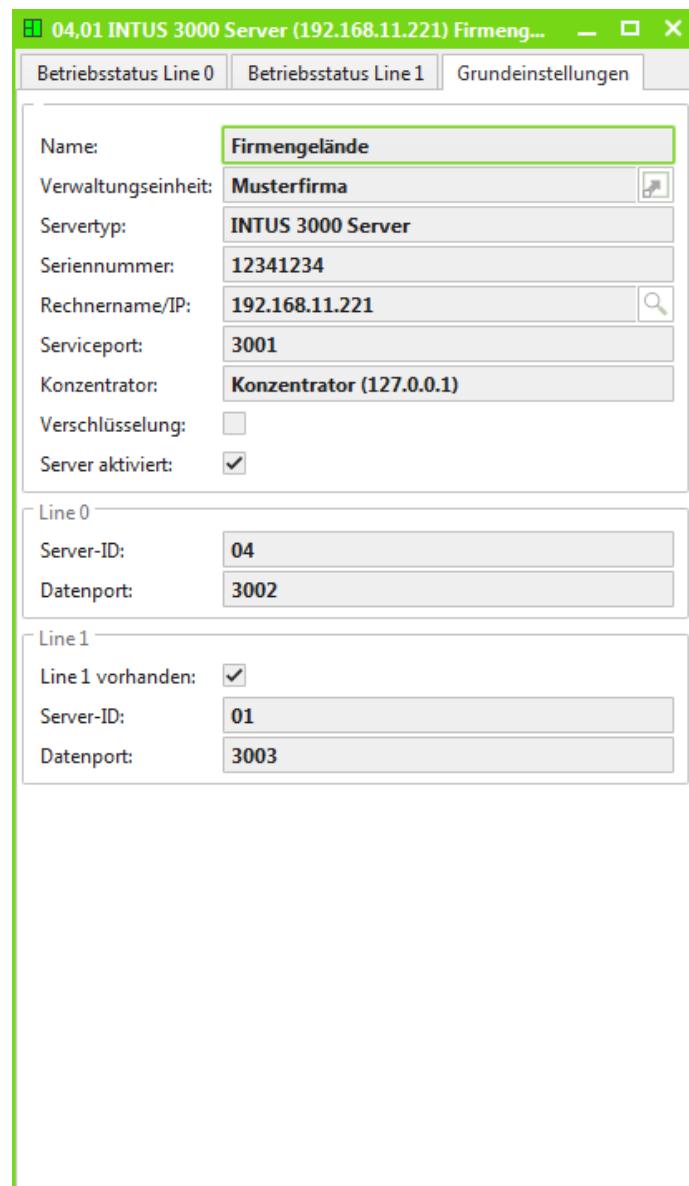


Abbildung 4.19 - INTUS 3000/3450 Server, Grundeinstellungen

4.12.1 Registerblatt Grundeinstellungen

Name

Anzeigetext zur Identifizierung eines INTUS 3000/3450 Servers in der Benutzeroberfläche.

Verwaltungseinheit

Siehe 4.5.1.

Seriennummer

Siehe 4.5.2 .

Rechnername/IP, Serviceport

Siehe 4.5.3.

Verschlüsselung

Siehe 4.2

Server aktiviert

Hier kann eingestellt werden, ob der INTUS 3000/3450 Server aktiviert oder deaktiviert ist.

Line 0

Server-ID, Datenport

Einstellungen für die erste Partyline. Siehe Abschnitt 4.3.

Line 1

Line 1 vorhanden

Hier kann eingestellt werden, ob der INTUS 3000/3450 Server über eine zweite Partyline verfügt.

Server-ID, Datenport

Einstellungen für die zweite Partyline. Siehe Abschnitt 4.3.

4.13 INTUS Terminal/ACM konfigurieren

Die Konfiguration eines INTUS Terminal/ACM erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für ein INTUS Terminal/ACM wie in 3.3.3.2 beschrieben. Die Konfiguration eines Terminals ist auf mehrere Registerblätter auf dem K&S-Fenster verteilt.

4.13.1 Netzwerkterminals aus csv-Datei importieren

Um die Konfiguration einer größeren Anzahl von Terminals zu erleichtern, besteht die Möglichkeit, INTUS Terminal/ACM, die über TCP/IP angeschlossen werden sollen, mit ihren Konfigurationsdaten in einer csv-Datei aufzulisten, und diese Datei automatisch zu importieren.

 Wenn Sie die Importdatei mit Excel erstellen, formatieren Sie bitte alle Felder als Text. Sonst kann es passieren, dass führende Nullen nicht gespeichert werden und dadurch später Fehler auftreten.

In der ersten Zeile müssen die Spaltennamen eingetragen sein. In jeder weiteren Zeile stehen die entsprechenden Werte für ein zu importierendes Terminal.

Spaltenname	Erforderlichkeit	Beschreibung
serial-number	immer erforderlich	Seriennummer
ip	immer erforderlich	IP-Adresse
terminal-id	immer erforderlich	2-stellige Terminal-ID
server-id	erforderlich, wenn mehrere TCP-Server vorhanden sind	2-stellige Server-ID
gateway	optional	Gateway IP-Adresse
mask	optional	IP-Subnetzmaske
port	optional	Portnummer
location	optional	Standorttext
encryption	optional	Verschlüsselung ein/aus
maintenance-group	optional	Wartungsgruppe (numerisch) des Terminals
file77	optional	Dateiname TCL-Programm
file72	optional	Dateiname Systemkonfiguration
file73	optional	Dateiname Parameter
file69	optional	Dateiname Kartendaten
file70	optional	Dateiname Funktionsschrittwerte
file71	optional	Dateiname Sondertage
file74	optional	Dateiname Profile
file75	optional	Dateiname Berechtigungsgruppen
file76	optional	Dateiname Stammdaten

Import durchführen

 Um Terminals zu importieren, wählen Sie den Menüpunkt **Werkzeuge / Terminalimport....** und selektieren Sie Ihre Importdatei, die auf dem Rechner liegen muss, auf dem der INTUS COM Client gestartet wurde. Damit wird der Import gestartet und der Import-Dialog angezeigt.

Damit die Terminals importiert werden können, müssen sie vom *Admin-Server* aus über UDP mit einem Broadcast erreichbar sein.

Der Import-Dialog dient der Anzeige des Fortschrittes sowie eventuell auftretender Fehler und Warnungen. Im oberen Teil sehen Sie eine Zusammenfassung des Importstatus. Im mittleren Teil sehen Sie den Status eines jeden aus der Importdatei gelesenen Terminals. Im unteren Teil werden die wichtigsten Einzelschritte sowie Fehler- und Warnmeldungen angezeigt.

Der Import kann insgesamt ein paar Minuten dauern.

Nach dem Einlesen der Importdatei wird für jedes zu importierende Terminal überprüft, ob dieses Terminal schon in der Konfiguration vorhanden ist, d. h. ob bereits ein Terminal mit der selben Server- und Terminal-ID konfiguriert ist. Bereits vorhandene Terminals werden nicht mehr verändert. Die noch nicht konfigurierten Terminals werden per UDP gesucht. Wenn nötig werden per UDP folgende weitere Aktionen durchgeführt:

- Ändern der IP-Einstellungen
- Reset
- Prüfung, ob die Geräte mit den gewünschten Einstellungen hoch gelaufen sind

Zum Schluss werden alle gefundenen neuen Terminals, sofern für sie keine Probleme oder Fehler aufgetreten sind, in die Konfiguration des INTUS COM aufgenommen. Sie werden dabei im Terminal-Handler deaktiviert angelegt (aber im TCP-Server aktiviert). Sie können die Terminals dann später bei Bedarf voll aktivieren.

Nach Beendigung des Imports können Sie den Import-Dialog schließen.

4.13.2 Registerblatt Grundeinstellungen

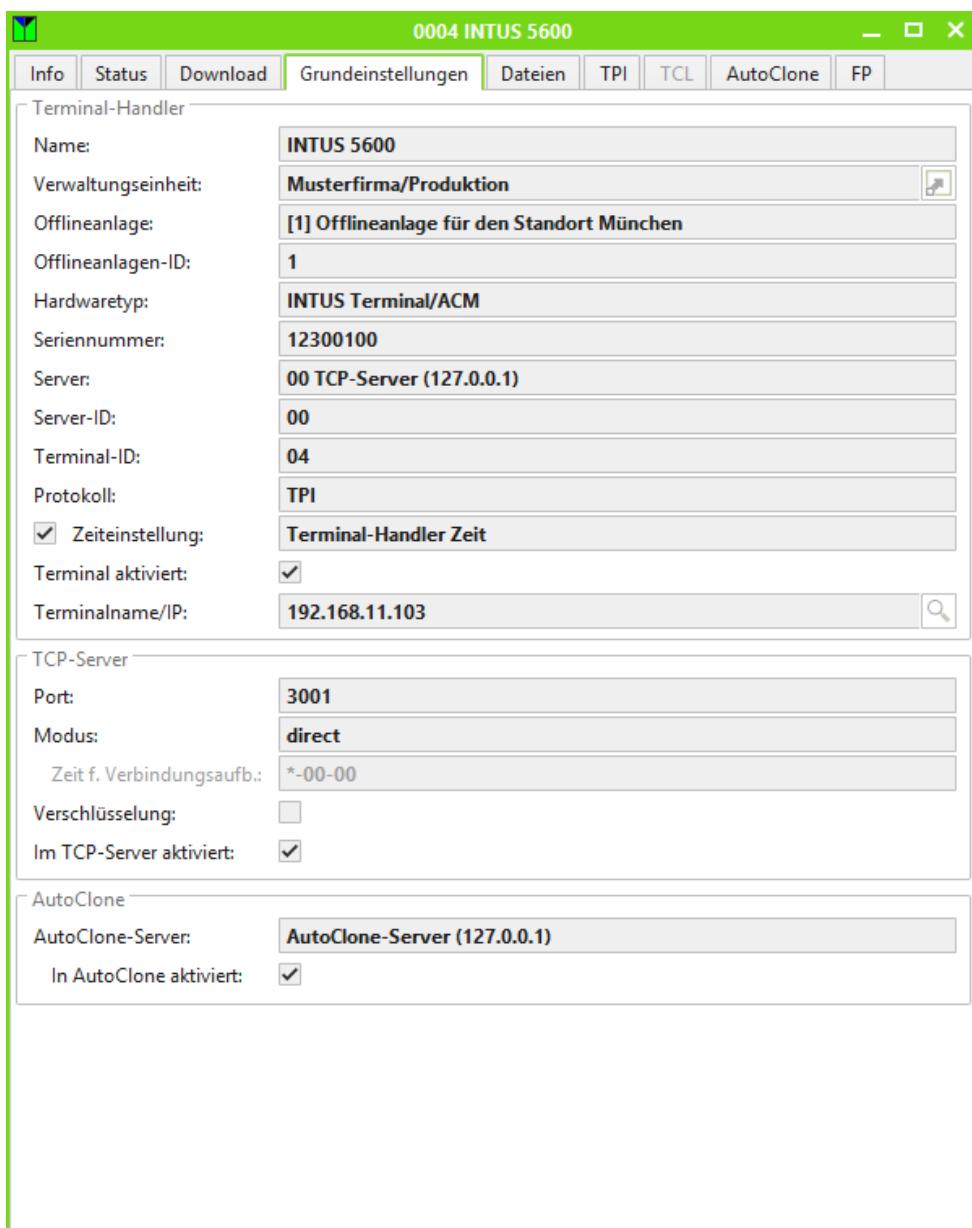


Abbildung 4.20 - INTUS Terminal/ACM, Grundeinstellungen

Terminal-Handler

Name

Anzeigetext zur Identifizierung eines Terminals in der Benutzeroberfläche

Verwaltungseinheit

Siehe 4.5.1.

Offlineanlage

Hier kann das Terminal bzw. der ACM einer Offlineanlage zugeordnet werden.

Die Angabe einer Offlineanlage ist erforderlich, wenn aus der Datenbank Berechtigungsdaten gemäß dem OSS Standard Offline auf das Terminal bzw. den ACM geladen werden sollen. In diesem Fall wird die Offlineanlagen-ID (Site-ID) verwendet, um die zu ladenden Daten auszuwählen.

Offlineanlagen-ID

Der Wert der Offlineanlagen-ID (Site-ID) des Terminals/ACMs kann nicht direkt konfiguriert werden. Er wird, soweit das Terminal bzw. der ACM einer Offlineanlage zugeordnet ist, von dieser Offlineanlage übernommen.

Seriennummer

Siehe 4.5.2 .

Server

Hier muss der Server selektiert werden, mit dem das Terminal kommunizieren soll.

Server-ID

Nach dem Speichern der Konfiguration wird hier die ID des Servers, mit dem das Terminal kommuniziert angezeigt.

Terminal-ID

Die zweistellige Terminal-ID identifiziert ein Terminal eindeutig an einem Server. Beim TCP-Server und beim HTTPS-Server darf die ID alphanumerisch sein, beim INTUS 3000 Server ist sie numerisch.

Protokoll

Bei einem INTUS Terminal/ACM ist TPI zu wählen, wenn das TCL-Programm TPI-tasc oder ein anderes an TPI angepasstes TCL-Programm eingesetzt werden soll, ansonsten TCL

Bei Verwendung von TPI kann auf der Registerkarte „TPI“ eingestellt werden, ob der Terminal-Handler beim Download das gesicherte Protokoll (mit Satznummer) verwenden soll.

Zeiteinstellung

Die Checkbox muss aktiviert sein, wenn der Terminal-Handler die Uhrzeit im Terminal synchronisieren soll. Die Uhrzeit wird gesendet:

- regelmäßig zu bestimmten konfigurierbaren Zeitpunkten (siehe Konfiguration des Terminal-Handler)
- nach manuellem Auslösen der Uhrzeitsynchronisation
- nachdem das Terminal offline war
- nach bestimmten Konfigurationsänderungen

Terminal-Handler Zeit

Die Uhrzeit im Terminal wird mit der lokalen Zeit des Rechners, auf dem der Terminal-Handler läuft, synchronisiert.

UTC-Zeitsynchronisation

Durch die UTC-Zeitsynchronisation können INTUS Terminals/ACMs, die in verschiedenen Zeitzonen installiert sind, zentral durch INTUS COM synchronisiert werden. Außerdem schalten diese Terminals **selbstständig** (also auch wenn sie offline sind) zwischen Sommer- und Winterzeit um. Zeitzonen ohne Sommerzeit werden ebenfalls unterstützt.

Die Zeitzonen müssen in einer Zeitzonendatei definiert werden. Dadurch kann jedem Terminal über den INTUS COM Client die Zeitzone zugeordnet werden, in der es installiert ist.

Zeitzonendatei

Die Zeitzonen müssen mit einem Texteditor in der Datei `time_zones.ini` im Verzeichnis `\conf` definiert werden. Wenn die Datei fehlt, verwendet INTUS COM keine Zeitzonen.



Es wird eine vordefinierte Datei mit ausgeliefert. Wenn der Inhalt der Zeitzonendatei verändert wird, müssen Admin-Server und Terminal-Handler gestoppt und neu gestartet werden.

Diese Datei hat das Windows ini-Dateiformat. Jede Sektion der Datei `time_zones.ini` entspricht einer Zeitzone. Eine Zeitzone im INTUS COM beinhaltet:

- einen kurzen einzeiligen Text zur Anzeige im INTUS COM Client
- eine Zeitdifferenz (Zeitabweichung) zwischen der UTC-Zeit und der Winterzeit der Zeitzone
- Angaben zu Sommer- und Winterzeitbeginn i. A. für mehrere Jahre

Im folgenden Beispiel sind 2 Zeitzonen definiert:

```
[time-zone.00001]
text=Zeitzone 1 (GMT+01:00)
has-daylight-saving-time=1
time-difference=-0060
2012=032500200,102800300
2013=033100200,102700300
2014=033000200,102600300
2015=033100200,102700300
```

```
[time-zone.00002]
text=Zeitzone 2
has-daylight-saving-time=1
time-difference=+0000
2012=032500200,102800300
2013=033100200,102700300
2014=033000200,102600300
2015=033100200,102700300
```

```
[time-zone.00003]
text=Zeitzone 3
has-daylight-saving-time=0
time-difference=+0120
```

Der Sektionsname besteht aus der Zeichenkette `time-zone` einem Punkt und einer eindeutigen 5-stelligen Nummer.

Der Parameter `text` enthält einen kurzen einzeiligen Text für die Anzeige im INTUS COM Client.

Der Parameter `time-difference` enthält die Zeitdifferenz zur UTC-Zeit in Minuten, immer eine 4-stellige Zahl mit Vorzeichen im Bereich [-0720,+0720]. Für mitteleuropäische Zeit ist -0060 anzugeben

 **Das Vorzeichen muss umgekehrt wie bei Windows angegeben werden.**

Der Parameter `has-daylight-saving-time` bestimmt ob in dieser Zeitzone die Sommerzeitumschaltung verwendet werden soll. Gültige Werte sind:

- **0** - keine Sommerzeitumschaltung
- **1** - die Zeitzone verwendet die Sommerzeitumschaltung.

Wird dieser Parameter nicht angegeben, wird eine Zeitzone mit Sommerzeitumschaltung angenommen.

Weiterhin sind jeweils unter der 4-stelligen Jahreszahl Sommer- und Winterzeitbeginn anzugeben, wenn die Zeitzone eine Sommerzeit hat. Dies kann für mehrere Jahre geschehen.

Das Format für die Angabe von Sommer- und Winterzeitbeginn ist:

<Jahr>=<Sommerzeitbeginn>,<Winterzeitbeginn>

genauer:

yyyy=MMddwHHmm,MMddwHHmm.

yyyy – Jahr 4-stellig

MM – Monat 2-stellig

dd – Tag des Monats 2-stellig

w – Wochentag einstellig (0 = Sonntag bis 6 = Samstag)

HH – Stunde 2-stellig

mm – Minute 2-stellig

Sommer- und Winterzeitbeginn werden in der lokalen Zeit (des Terminal-Handlers) angegeben, nicht in der UTC-Zeit. Im Terminal wird die **Minute nicht ausgewertet**. Deswegen wird intern immer auf die volle Stunde abgerundet.

Für eine Zeitzone ohne Sommerzeitumschaltung, darf keine Umschaltzeitpunkte enthalten.

Einstellen der Zeitzonen

Voreingestellt ist immer die "lokale Uhrzeit des Terminal-Handlers". In diesem Fall erfolgt die Uhrzeitsynchronisation wie bisher durch die lokale Uhrzeit des Server-Rechners, auf dem der Terminal-Server installiert ist. Sommer- und Winterzeitbeginn werden nicht in die Terminals geladen.



Zeitzonen können nur für INTUS Terminal/ACM mit **TCL ab Version 5.01** verwendet werden.

Statt der lokalen Uhrzeit wird bei Verwendung einer Zeitzone in den Terminals die UTC-Zeit eingestellt sowie alle Parameter die für die Berechnung der lokalen Uhrzeit aus der UTC-Zeit benötigt werden geladen. Das sind:

- Zeitdifferenz zwischen Winterzeit und UTC-Zeit
- Sommer- und Winterzeitbeginn des aktuellen Jahres, falls in diese Zeitzone eine Sommerzeit hat.

Darüber hinaus wird die automatische Sommer-Winter-Zeitumschaltung aktiviert oder die Winterzeit fest eingestellt. Als Nebeneffekt wird das Uhrzeit-Trennzeichen auf Doppelpunkt „::“ gestellt.

Terminal aktiviert

Die Checkbox muss aktiviert sein, wenn der Terminal-Handler Aktionen (Uhrzeit stellen, Download, usw.) für das Terminal ausführen soll.

Terminalname/IP

Diese Einstellung wird nur für über TCP-Server angebundene Terminals angezeigt.

IP-Adresse bzw. DNS-Name des Terminals.

Über die Schaltfläche in diesem Eingabefeld, kann der Dialog für die **Netzwerk Terminalsuche** aufgerufen werden, siehe 3.4.11.

Anbindung über HTTPS-Server

HTTPS-Server	
Authentifizierung:	
Passwort setzen:	<input type="checkbox"/>
Passwort:	<input type="text"/>
Passwort wiederholen:	<input type="text"/>
Im HTTPS-Server aktiviert:	<input checked="" type="checkbox"/>

Abbildung 4.21 - Terminaleinstellungen für HTTPS-Server

Authentifizierung

Der Aufbau der Verbindung zwischen Terminal und HTTPS-Server wird durch das Terminal gestartet. Dabei authentifiziert es sich per HTTP Basic Authentication. Der HTTPS-Server akzeptiert nur dann den Verbindungsaufbau, wenn das vom Terminal gesendete Passwort dem hier eingestelltem entspricht.

Die Übertragung des Passworts vom INTUS COM Client zum Admin-Server bzw. weiter zum HTTPS-Server erfolgt verschlüsselt durch einen Hash-Algorithmus.

Passwort setzen

Hier kann eingestellt werden, dass das Passwort, auf das der HTTPS-Server prüft, geändert werden soll.

Passwort

Hier kann das neue Passwort eingegeben werden.

Passwort wiederholen

Hier muss das neue Passwort zur Bestätigung wiederholt werden.

Im HTTPS-Server aktiviert

Nur wenn diese Checkbox aktiviert ist, akzeptiert der HTTPS-Server einen Verbindungsaufbau vom Terminal.

Anbindung über INTUS 3000/3450 Server

INTUS 3000 Server	
Anbindung:	Line 1

Abbildung 4.22 - Terminaleinstellungen für INTUS 3000 Server

Anbindung

Ein INTUS 3000/3450 Server unterstützt zwei RS485-Partylines. Deshalb muss die Partyline angegeben werden, an der das Terminal angeschlossen ist.

Anbindung über TCP-Server

TCP-Server	
Port:	3001
Modus:	direct
Zeit f. Verbindungsaufb.:	*-00-00
Verschlüsselung:	<input type="checkbox"/>
Im TCP-Server aktiviert:	<input checked="" type="checkbox"/>

Abbildung 4.23 - Terminaleinstellungen für TCP-Server

Port

Portnummer des Terminals (normalerweise 3001)

Modus

An einem TCP-Server stehen drei Anschlussmodi zur Verfügung:

- **direct** – Die Verbindung zum Terminal soll immer bestehen (lokales Netzwerk).
- **dialup** – Die Verbindung zum Terminal wird zu bestimmten Zeitpunkten (z.B. über ISDN-Router) aufgebaut und, wenn keine Daten mehr zu übertragen sind, wieder abgebaut.
- **auto** – Dieser Modus funktioniert ähnlich wie der Modus **dialup**, jedoch wird die Verbindung zusätzlich immer dann aufgebaut, wenn Daten an das Terminal zu übertragen sind.

Zeit f. Verbindungsaufb.

Für die Modi **dialup** und **auto** können die Zeiten für den Verbindungsauftakt angegeben werden. Eine Zeitangabe hat folgendes Format: **d-hh-mm**

d – Wochentag (0=Sonntag bis 6=Samstag) oder * für jeden Tag

hh – Stunde (00 – 23) oder * für jede Stunde

mm – Minute (00 – 59) oder * für jede Minute

z. B. jede volle Stunde: ***-*-00**

Bei mehreren Angaben sind diese durch Komma zu trennen z. B. täglich um Mitternacht und freitags um 18.30 Uhr: ***-00-00,5-18-30**

Verschlüsselung

Siehe 4.2

Im TCP-Server aktiviert

Die Checkbox muss aktiviert werden, wenn der TCP-Server eine Verbindung zu dem Terminal aufbauen soll.

AutoClone

AutoClone wird nur für Terminals, die an einem TCP-Server konfiguriert sind unterstützt.

AutoClone-Server

Die Auswahl des AutoClone-Servers aktiviert die INTUS COM AutoClone Unterstützung für dieses Terminal.

In AutoClone aktiviert

Ist diese CheckBox aktiviert, übernimmt der INTUS COM AutoClone Dienst den Download der INTUS Graph Masken, des INTUS Audio Archiv und der INTUS Graph Tastatur.

4.13.3 Registerblatt Dateien

Auf diesem Registerblatt wird festgelegt, ob und welche statischen Downloaddateien der Terminal-Handler ins Terminal laden soll

Falls im Terminal-Handler ein Download aus der Datenbank konfiguriert ist, sind diese Einstellungen deaktiviert. (Siehe 4.8.3)

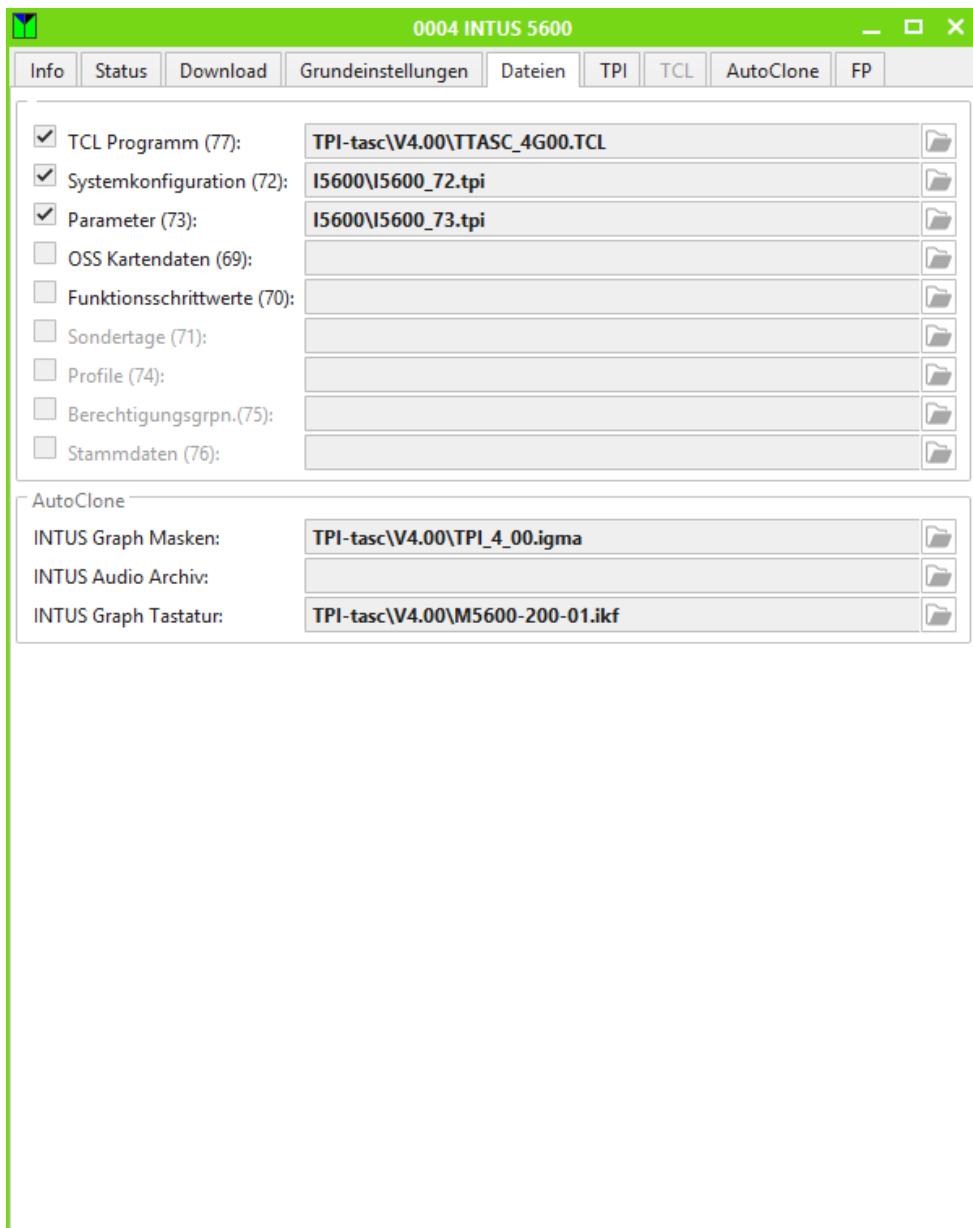


Abbildung 4.24 - INTUS Terminal/ACM, Dateien

Für jede Ladeanforderung (siehe TPI-Handbuch) kann eingestellt werden, ob der Terminal-Handler diese verarbeiten soll (Checkbox aktiviert), oder sie an die Applikation weiterleiten soll (Checkbox deaktiviert).

Wenn der Terminal-Handler die Anforderung verarbeiten soll, ist der Dateiname (optional mit relativem Pfad) anzugeben. (Das Basisverzeichnis, auf das sich der relative Pfad bezieht, wird bei der Konfiguration des Terminal-Handler eingestellt, siehe 4.8.1).

AutoClone

Für INTUS Terminals die die AutoClone Funktion unterstützen und an einem INTUS COM TCP-Server konfiguriert sind können hier die Dateien für die AutoClone Downloads konfiguriert

werden. Die Eingabefelder im Rahmen AutoClone sind nur aktiviert wenn auf dem Reiter "Grundeinstellungen" die Funktion "verwendet AutoClone" aktiviert ist.

Die Dateinamen können über Tastatur eingegeben werden, oder über einen Dialog, der mit der jeweiligen  Schaltfläche gestartet wird:

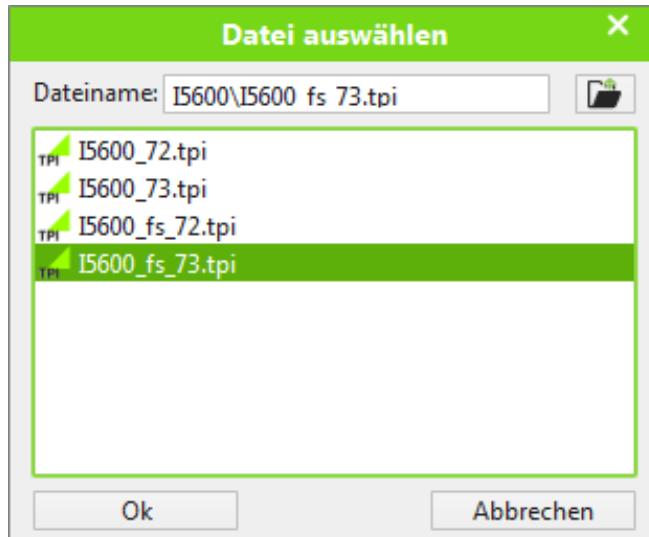


Abbildung 4.25 - Dateiauswahldialog des INTUS COM Client

4.13.4 Registerblatt TPI

Das Registerblatt TPI ist nur aktiviert, wenn im Registerblatt Grundeinstellungen als Protokoll für dieses Terminal TPI ausgewählt wurde.

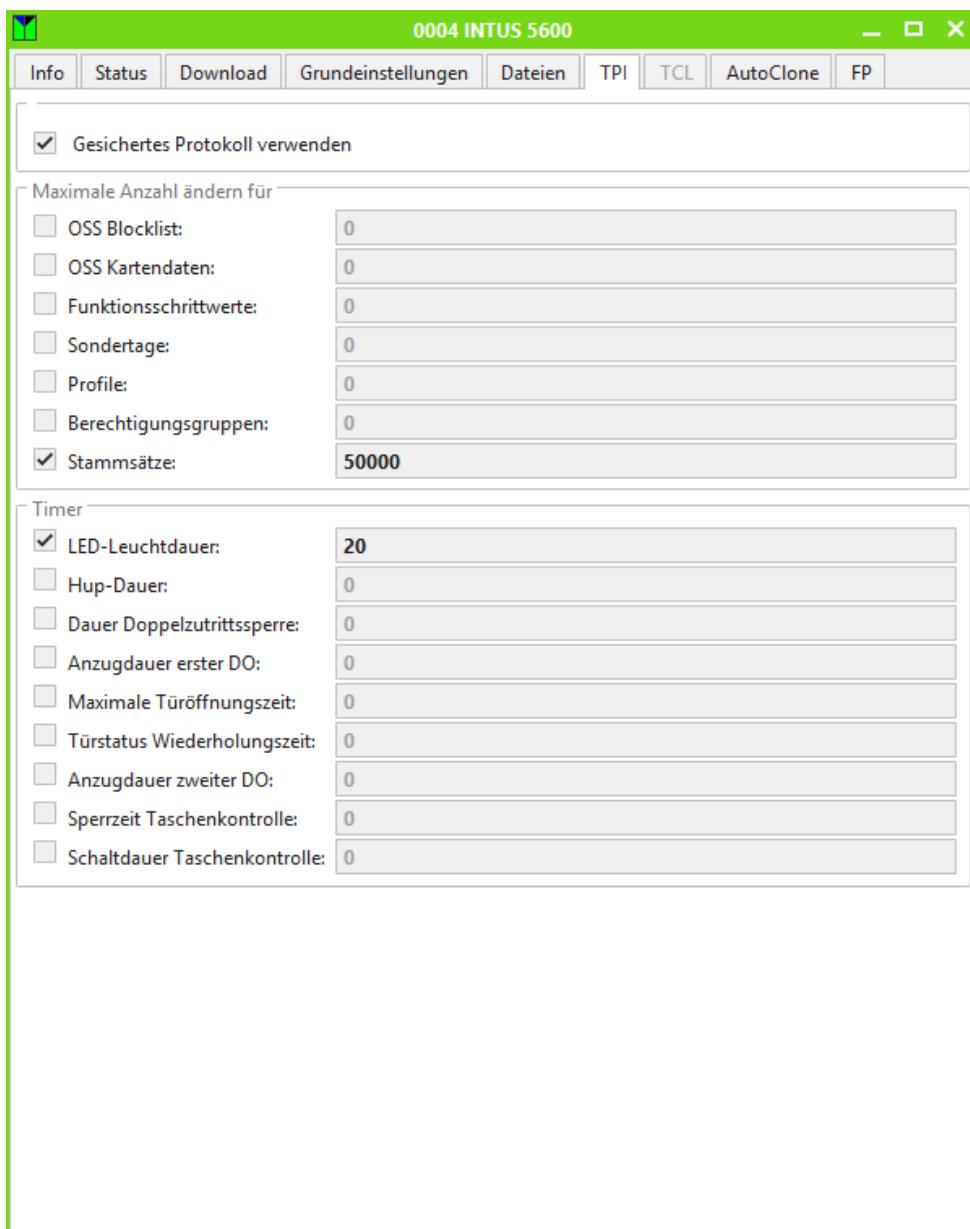


Abbildung 4.26 - INTUS Terminal/ACM, TPI

Gesichertes Protokoll verwenden

Hier kann eingestellt werden, ob der Terminal-Handler beim Download das gesicherte Protokoll (mit Satznummer) verwenden soll.

Maximale Anzahl ändern für

Für jedes Terminal mit TPI Protokoll können die Einstellungen aus der TPI Systemparameterdatei _72.tpi der Parameter maximale Anzahl für:

- OSO-Blocklist
- OSO-Kartendaten
- Funktionsschrittwerke
- Sondertage
- Profile

- Berechtigungsgruppen
- Stammsätze

individuell übersteuert werden.

Damit die übersteuerte Einstellung wirksam wird, ist ein Systemparameterdownload (72) notwendig. Dieser muss manuell angestoßen werden.

Der Systemparameterdownload (72) kann zu einer Speicher-Reorganisation mit Kaltstart des Terminal/ACMs führen.



ACHTUNG: Durch den Kaltstart geht der Inhalt des Notpuffers im Terminal/ACM verloren, es kann also zu Datenverlusten kommen! Außerdem müssen TPI-tasc, Parametrierung und sämtliche Tabellen erneut geladen werden. Abhängig von den zu ladenden Datenmengen ist das Terminal eine längere Zeit (mehrere Minuten bis zu Stunden) nicht betriebsbereit. Beachten Sie ggf. die möglichen Auswirkungen für die Wahl des Zeitpunktes, an dem Sie die übersteuerten Einstellungen wirksam schalten.

Timer

Für jedes Terminal mit TPI Protokoll können die Einstellungen aus der TPI Systemparametrierdateien für einige Timer übersteuert werden. Übersteuerbare Timer sind:

- LED-Leuchtdauer
- Hup-Dauer
- Dauer der Doppelzutrittssperre
- Anzugdauer des ersten DO
- Maximale Türöffnungszeit
- Türstatus Wiederholungszeit
- Anzugdauer des zweiten DO
- Sperrzeit für die Taschenkontrolle
- Schaltdauer der Taschenkontrolle

4.13.5 Registerblatt TCL

Die Konfiguration in diesem Registerblatt bezieht sich auf Einstellungen, die der Terminal-Handler direkt im Setup eines INTUS Terminal/ACM vornimmt, wenn im Registerblatt **Grundeinstellungen** als Protokoll für dieses Terminal **TCL** ausgewählt wurde..

Der Terminal-Handler überprüft die Einstellungen jeweils bevor er einen Download des TCL-Programms beginnt. Sind die Einstellungen im Setup des INTUS Terminal/ACM korrekt, wird der Download ausgeführt. Weichen die Einstellungen ab, werden sie geändert, und es wird ein Reset ausgelöst.

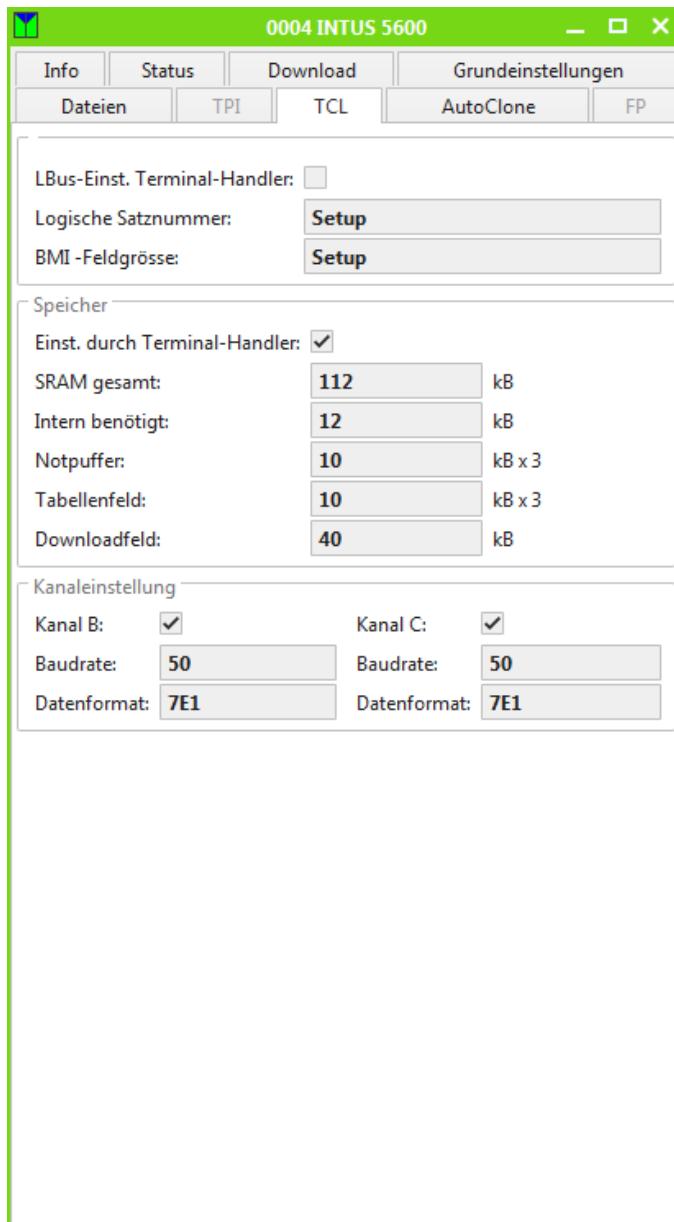


Abbildung 4.27 - INTUS Terminal/ACM, TCL

LBus Einst. Terminal-Handler

Wenn diese Option aktiviert ist, nimmt der Terminal-Handler LBus-Einstellungen im Setup des Terminals vor.

Logische Satznummer

Auswählbar für die Satznummer sind 'Setup' (unverändert), 'Satznummer ein' und 'Satznummer aus'.

Hinweis: Bei Verwendung des Uploads in Datei werden Satznummern benötigt, damit die Notpuffersätze als solche erkannt werden und Quittungen gesendet werden.

BMI-Feldgröße

Auswählbar für die Feldgröße sind 'Setup' (unverändert), '115 Bytes' und '88 Bytes'.

Speicher

Der Terminal-Handler kann die Speicheraufteilung zwischen Notpuffer, Tabellenfeld und Downloadfeld vornehmen.

Der gesamte SRAM wird in KByte angegeben, die Anteile von Notpuffer und Tabellenfeld in Einheiten von 3 KByte. Der intern benötigte SRAM ist durch das Laufzeitsystem des Terminals fest vorgegeben. Die anderen Werte werden berechnet.

Einst. durch Terminal-Handler

Wenn diese Option aktiviert ist, nimmt der Terminal-Handler die SRAM-Speicheraufteilung im Setup des Terminals vor.

SRAM gesamt

Größe des SRAM-Speichers im Terminal.

Der Terminal-Handler überprüft, ob der angegebene Gesamtspeicher mit dem tatsächlich vorhandenen Speicher übereinstimmt.

Intern benötigt

Intern benötigter Speicher (nur Anzeige).

Notpuffer

Größe des Notpuffers.

Tabellenfeld

Größe des Tabellenfeldes.

Downloadfeld

Größe des Downloadfeldes (nur Anzeige).

Kanaleinstellungen

Bei den Kanälen B und C kann man die Baudrate und das Datenformat einstellen. Das Protokoll (TTY) ist nicht über TCL einstellbar und muss ggf. direkt am Gerät im Setup eingestellt werden. Der Terminal-Handler überprüft jedoch, ob als Protokoll TTY eingestellt ist.

Kanal B/C

Optional übernimmt der Terminal-Handler bei TCL-Terminals das Einstellen der Baudrate und des Datenformats für seriell angeschlossene Geräte. Er überprüft dann auch, dass TTY als Protokoll für den betreffenden Kanal eingestellt ist.

Baudrate

Hier kann die Baudrate für den Kanal (B/C) eingestellt werden.

Datenformat

Hier kann das Datenformat für den Kanal (B/C) eingestellt werden.

4.13.6 Registerblatt AutoClone

Das Registerblatt AutoClone ist nur aktiv, wenn im Register Grundeinstellungen das Auswahlfeld AutoClone aktiviert ist, um die AutoClone-Funktionalität für dieses Terminal zu verwenden.

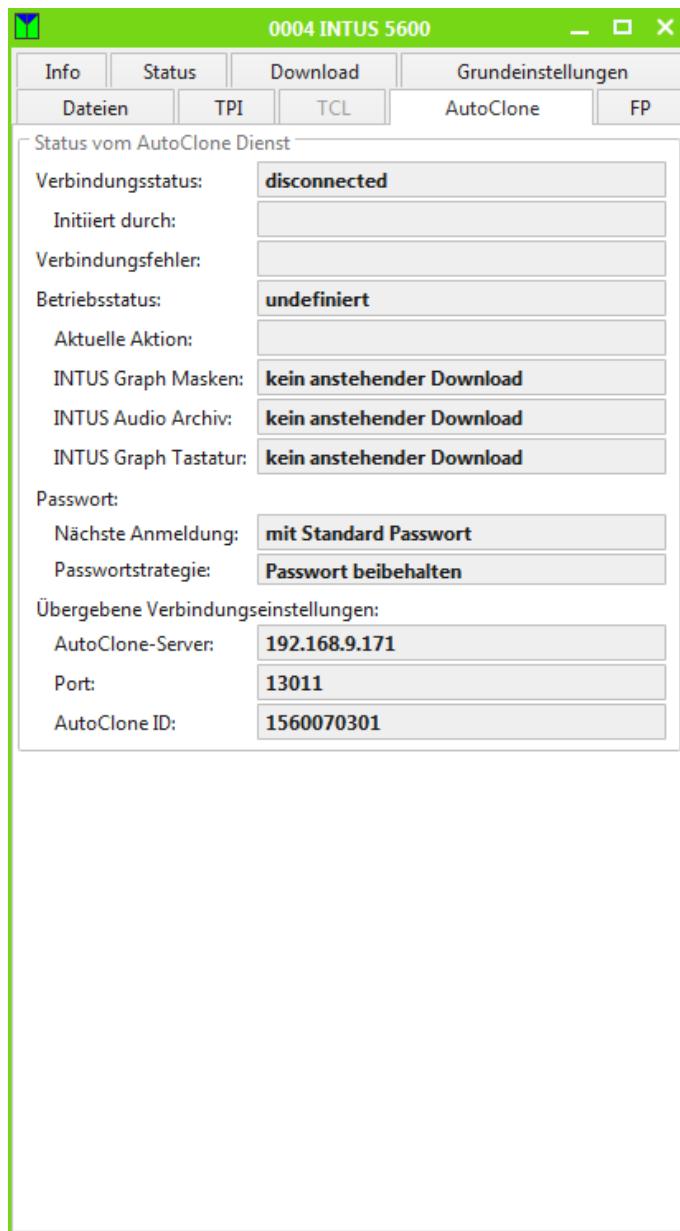


Abbildung 4.28 - INTUS Terminal/ACM, AutoClone

Passwort

Nächste Anmeldung

Hier wird angezeigt, welches Passwort der AutoClone Dienst, bei der nächsten Anmeldung am Terminal verwenden wird.

Passwortstrategie

Für das AutoClone Passwort können zwei Einstellungen verwendet werden

- Passwort beibehalten
- Terminalspezifisches Passwort verwenden

Ist "Passwort beibehalten" ausgewählt, so wird für die Kommunikation mit dem AutoClone Terminal keine Passwortänderung durchgeführt.

Die Einstellung "Terminalspezifisches Passwort verwenden" bewirkt, dass bei der Kontakt- aufnahme zu dem AutoClone-Terminal ein Terminalspezifisches Passwort in der Terminal- konfiguration eingestellt wird, wenn vorher das Standardpasswort (z.B: Auslieferungszustand) eingestellt war. Dadurch wird die Sicherheit der Kommunikation erhöht.

4.13.7 Registerblatt FP

Das Registerblatt FP ist nur aktiviert, wenn im Registerblatt Grundeinstellungen als Protokoll für dieses Terminal TPI ausgewählt wurde. Des Weiteren muss im Terminal-Handler der globale Parameter **Biometrie Unterstützung** aktiviert sein.

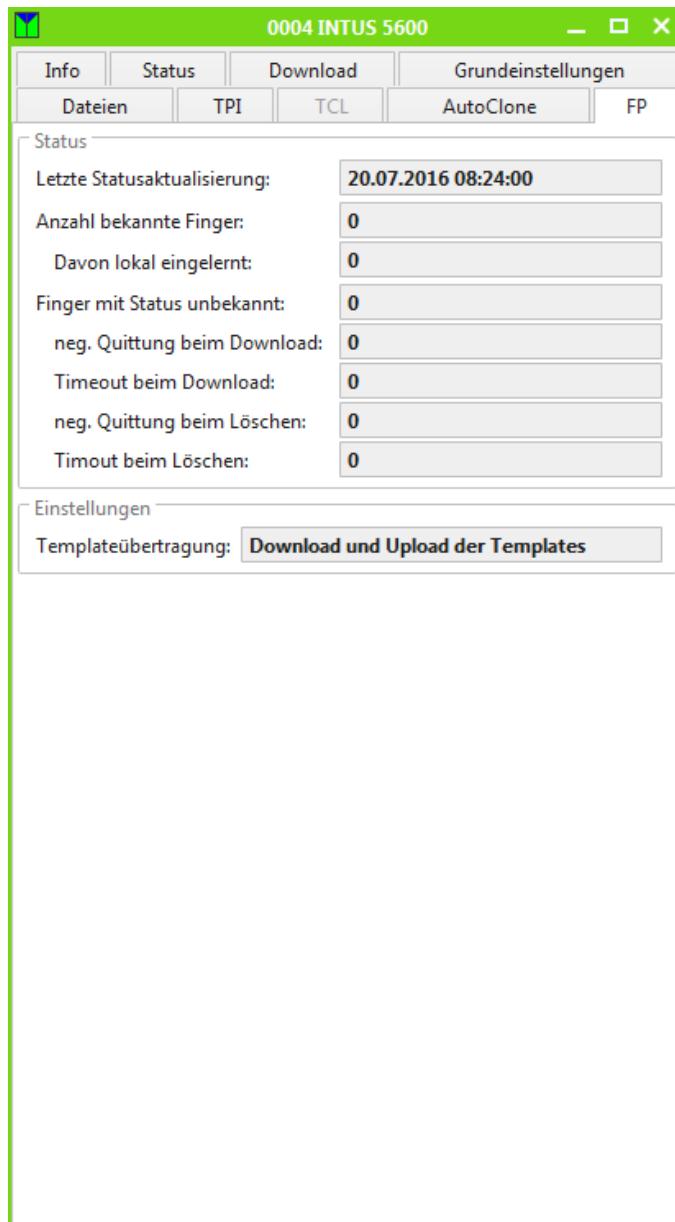


Abbildung 4.29 - INTUS Terminal/ACM, FP

Einstellungen

Template-Übertragung

Für die Template-Übertragung gibt es drei mögliche Einstellungen

- keine Template-Übertragung
- Download der Templates
- Download und Upload der Templates

keine Template-Übertragung deaktiviert die Template-Übertragung für dieses Terminal (Standardeinstellung). Einlernereignisse vom Terminal werden an die Socket-Schnittstelle übergeben.

Die Einstellung **Download der Templates** aktiviert die Template-Übertragung auf das Gerät und die Statusführung über die auf diesem Terminal befindlichen Templates. Einlernereignisse vom Terminal werden folgendermassen behandelt:

Templates-ID unbekannt	Es wird ein Löschsatz für die unbekannte Templates-ID an das Terminal geschickt.
Templates-ID bekannt	Einlernereignis wird ignoriert. Das geänderte Template verbleibt bis zum nächsten Template-Download auf dem Terminal.

Durch die Einstellung **Download und Upload der Templates** werden die an diesem Terminal eingelernten Templates auch auf andere Terminals verteilt.



Um Sicherheitsprobleme zu vermeiden, sollte der Upload von Templates nur für wenige Terminals aktiviert sein.

4.14 Subterminals konfigurieren

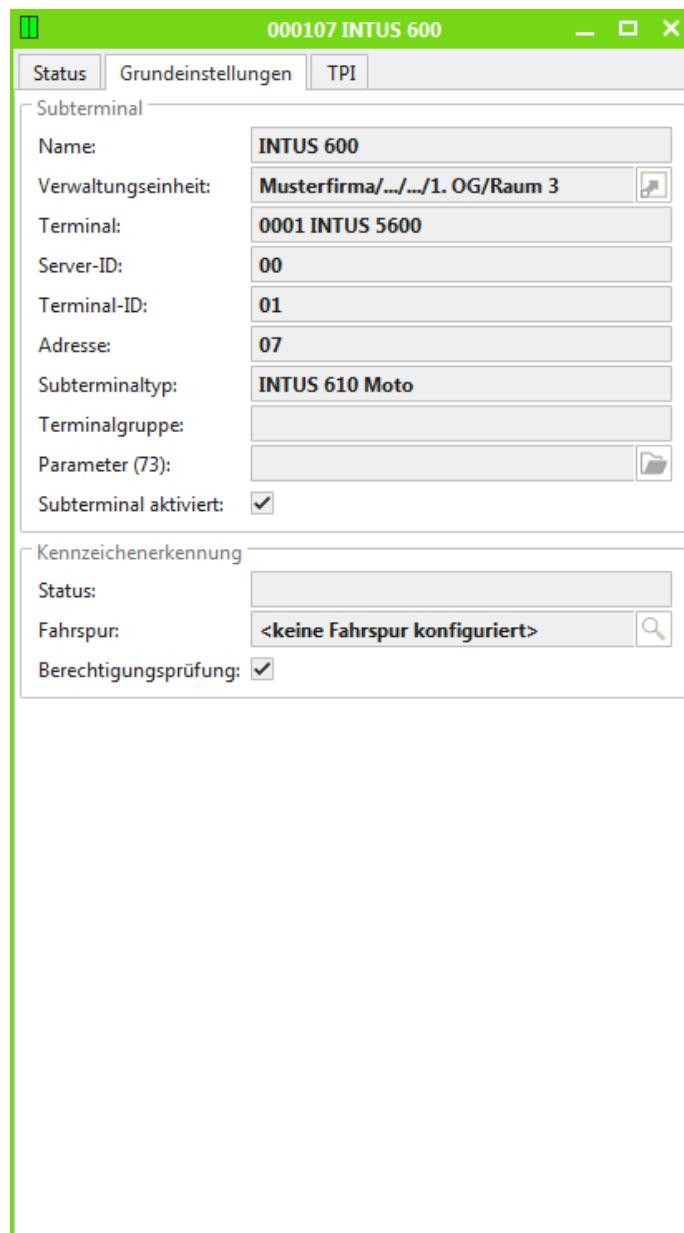


Abbildung 4.30 - Subterminal, Grundeinstellungen

4.14.1 Registerblatt Grundeinstellungen

Subterminal

Name

Der Name dient zur Unterscheidung der einzelnen Subterminals aus Sicht des Benutzers.

Verwaltungseinheit

Siehe 4.5.1.

Terminal

Für ein Subterminal ist das Terminal anzugeben, an welches das Subterminal angeschlossen ist. Dabei können nur INTUS Terminal/ACM gewählt werden.

Server-ID

Nach dem Speichern der Konfiguration wird hier die ID des Servers, mit dem das Terminal dieses Subterminals kommuniziert, angezeigt.

Terminal-ID

Nach dem Speichern der Konfiguration wird hier die ID des Terminals dieses Subterminals angezeigt.

Adresse

Für die Anbindung des Subterminals ist außerdem die Adresse am LBus auszuwählen:

- 01 bis 08 für den ersten LBus
- 09 bis 16 für den zweiten LBus

Subterminaltyp

Der Subterminal-Typ betrifft bei Verwendung von TPI den SK2 Satz. Der Terminal-Handler benötigt diese Angabe, um das Subterminal ggf. in den SK2 Satz einzutragen bzw. eine Konsistenzprüfung durchzuführen. Beachten Sie, dass verschiedene Subterminaltypen nicht beliebig an einem LBus gemischt werden können.

Parameter (73)

Die Parameterdatei ist optional. Wenn sie vorhanden ist, wird sie beim Download mit eingebunden. (Voraussetzung dafür ist, dass der Terminal-Handler den Parameterdownload durchführt, und nicht die Applikation.) Wenn keine eigene Parameterdatei für das Subterminal verwendet werden soll, ist das Feld einfach leer zu lassen.

Über die Schaltfläche kann (wie bei der Konfiguration des Terminals) ein Dialog zur Auswahl der Datei geöffnet werden.

Subterminal aktiviert

Das Subterminal kann vorübergehend deaktiviert werden. Dann wird es nicht in das Setup bzw. den SK2 Satz eingetragen und die Parameterdatei des Subterminals wird nicht mit geladen.

Kennzeichenerkennung

Fahrspur

Über den Auswahlbutton kann hier eine Fahrspur ausgewählt werden. Um eine Fahrspur auswählen zu können, muss im INTUS COM Terminal-Handler die Verbindung zur SeeTec Kennzeichenerkennung (LPR) konfiguriert und aktiviert sein.

Berechtigungsprüfung

Mit dieser Option wird die Berechtigungsprüfung für Kennzeichen in INTUS COM für dieses Terminal aktiviert. Ist die Berechtigungsprüfung im INTUS COM Terminal-Handler nicht konfiguriert wird eine Warnmeldung angezeigt, wenn diese Option für das Terminal aktiviert ist.

PS-Controller

Für Subterminals des Typs „INTUS PS/INTUS 16PS mit/ohne Tastatur“ (PS-Controller) wird ein Rahmen mit weiteren Einstellungen eingeblendet:

PS-Controller	
PS-Distributor:	PS-Distributor (127.0.0.1)
DNS name/IP:	192.168.11.94
Port:	3101
Verschlüsselung:	<input type="checkbox"/>

Abbildung 4.31 – Subterminal, Grundeinstellungen PS Controller

PS-Distributor

Der PS-Distributor stellt die Verbindung zum PS-Controller nur her, wenn die Referenz zum PS-Distributor gesetzt ist.

DNS-Name/IP

IP-Adresse bzw. DNS-Name des PS-Controller.

Port

Portnummer des Terminals (normalerweise 3101)

Verschlüsselung

Bei aktivierter Verschlüsselung erfolgt die Kommunikation mit dem PS-Distributor verschlüsselt.

Fingerprint

Für Subterminals des Typs „INTUS FP/INTUS 1600 Fingerprint“ und „INTUS 600FP“ (Fingerprint) wird ein Rahmen mit weiteren Einstellungen eingeblendet:

Fingerprint	
Templateübertragung:	Download und Upload der Templates

Abbildung 4.32 - Subterminal, Grundeinstellungen Fingerprint

Template-Übertragung

Für die Template-Übertragung gibt es drei mögliche Einstellungen

- keine Template-Übertragung
- Download der Templates
- Download und Upload der Templates

keine Template-Übertragung deaktiviert die Template-Übertragung für dieses Subterminal (Standardeinstellung). Einlernereignisse vom Subterminal werden an die Socket-Schnittstelle übergeben.

Die Einstellung **Download der Templates** aktiviert die Template-Übertragung auf das Gerät und die Statusführung über die auf diesem Subterminal befindlichen Templates. Einlernereignisse vom Subterminal werden folgendermassen behandelt:

Templates-ID unbekannt	Es wird ein Löschsatz für die unbekannte Templates-ID an das Subterminal geschickt.
Templates-ID bekannt	Einlernereignis wird ignoriert. Das geänderte Template verbleibt bis zum nächsten Template-Download auf dem Subterminal.

Durch die Einstellung **Download und Upload der Templates** werden die an diesem Subterminal eingelernten Templates auch auf andere Subterminals verteilt.



Um Sicherheitsprobleme zu vermeiden, sollte der Upload von Templates nur für wenige Terminals aktiviert sein.

4.14.2 Registerblatt TPI

Timer

Für jedes Subterminal verbunden mit einem Terminal mit TPI Protokoll können die Einstellungen aus der TPI Systemparametrierdateien für einige Timer übersteuert werden (siehe 4.13.4). Übersteuerbare Timer sind:

- LED-Leuchtdauer
- Hup-Dauer
- Dauer der Doppelzutrittssperre
- Anzugdauer des ersten DO
- Maximale Türöffnungszeit
- Türstatus Wiederholungszeit
- Anzugdauer des zweiten DO
- Sperrzeit für die Taschenkontrolle
- Schaltdauer der Taschenkontrolle

Damit die übersteuerten Timer wirksam werden, ist ein Parameterdownload (73) notwendig. Dieser muss manuell angestoßen werden.

Durch die Übersteuerung kann sich die Anzahl der Terminalgruppen (siehe TPI-Handbuch Kap. 1.5) oder die Zuordnung von Subterminals zu Terminalgruppen im zugehörigen Terminal/ACM ändern. In diesem Fall ist vor dem Parameterdownload (73) zusätzlich ein Systemparameterdownload (72) erforderlich. Wenn versucht wird, den Download (73) zu starten, obwohl vorher der Download (72) erforderlich ist, wird dies durch den Fehlerstatus des Hauptterminals signalisiert.

Der Systemparameterdownload (72) muss ggf. ebenfalls manuell angestoßen werden. Der Systemparameterdownload (72) kann zu einer Speicher-Reorganisation mit Kaltstart im zugehörigen Terminal/ACM führen.



ACHTUNG: Durch den Kaltstart geht der Inhalt des Notpuffers verloren, es kann also zu Datenverlusten kommen! Außerdem müssen TPI-tasc, Parametrierung und sämtliche Tabellen erneut geladen werden. Abhängig von den zu ladenden Datenmengen ist das Terminal eine längere Zeit (mehrere Minuten bis zu Stunden) nicht betriebsbereit. Beachten Sie ggf. die möglichen Auswirkungen für die Wahl des Zeitpunktes, an dem Sie die übersteuerten Timer wirksam schalten.

4.15 Türüberwachung konfigurieren

In INTUS COM können Türen überwacht werden, die an INTUS Terminals/ACM oder Subterminals konfiguriert sind. Die Türüberwachung wird in TPI-tasc ab Version 2.51 unterstützt und muss in der TPI-Parametrierung aktiviert werden.

Um eine Tür zu überwachen, muss ein Türobject an Haupt- oder Subterminals über das Menü oder das Kontextmenü **Neu/Tür** angelegt werden. Das folgende K&S Fenster wird angezeigt:

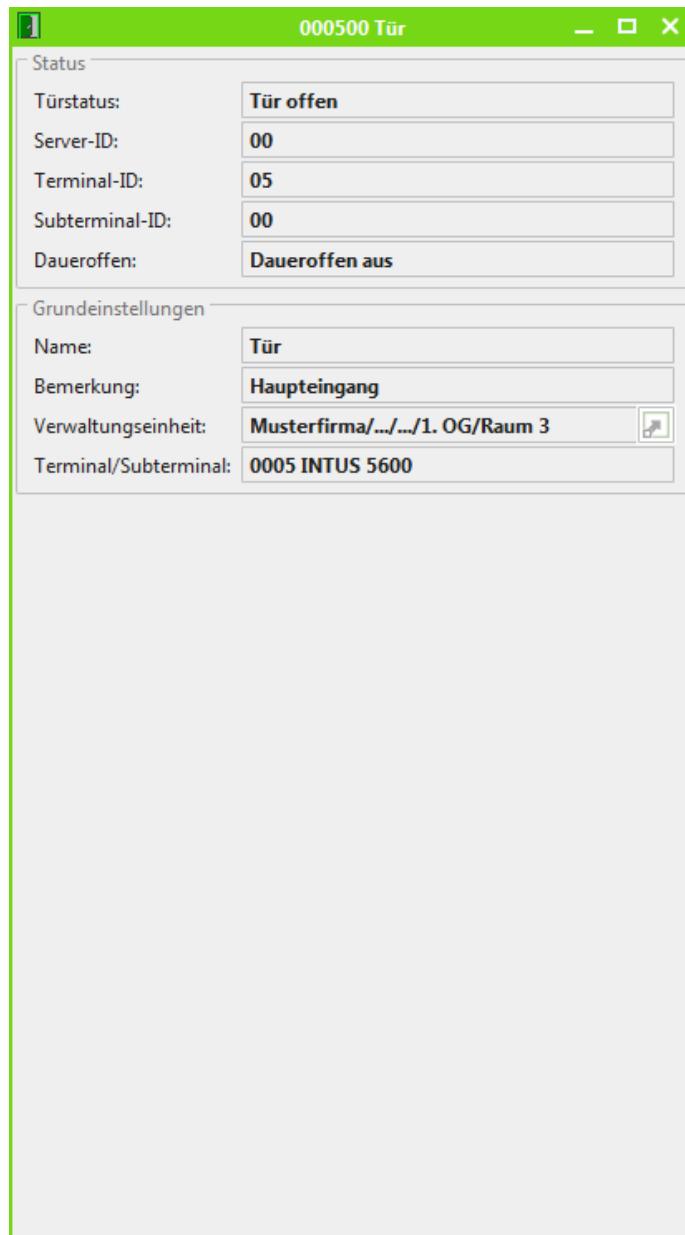


Abbildung 4.33 - Tür, Grundeinstellungen

Grundeinstellungen

Name

Hier kann ein Text zur Kennzeichnung der jeweiligen Tür eingegeben werden.

Bemerkung

Hier kann eine Bemerkung für diese Tür hinterlegt werden.

Verwaltungseinheit

Siehe 4.5.1.

Terminal/Subterminal

Wählen Sie hier das Terminal oder Subterminal aus, an dem die Tür angeschlossen ist.

4.16 Benutzer anlegen

Der INTUS COM Client kann nur mit Benutzernamen und Passwort gestartet werden. Bei der ersten Anmeldung kennt INTUS COM nur den Benutzer **admin** mit dem Passwort **pcs**.

Sie können weitere Benutzer entweder über das Menü **Neu/Benutzer ...** oder im Kontextmenü des Benutzer-Rollen-Berechtigungen-Fensters (siehe 3.2.2) anlegen. Das folgende K&S Fenster (siehe 3.2.8) wird angezeigt:

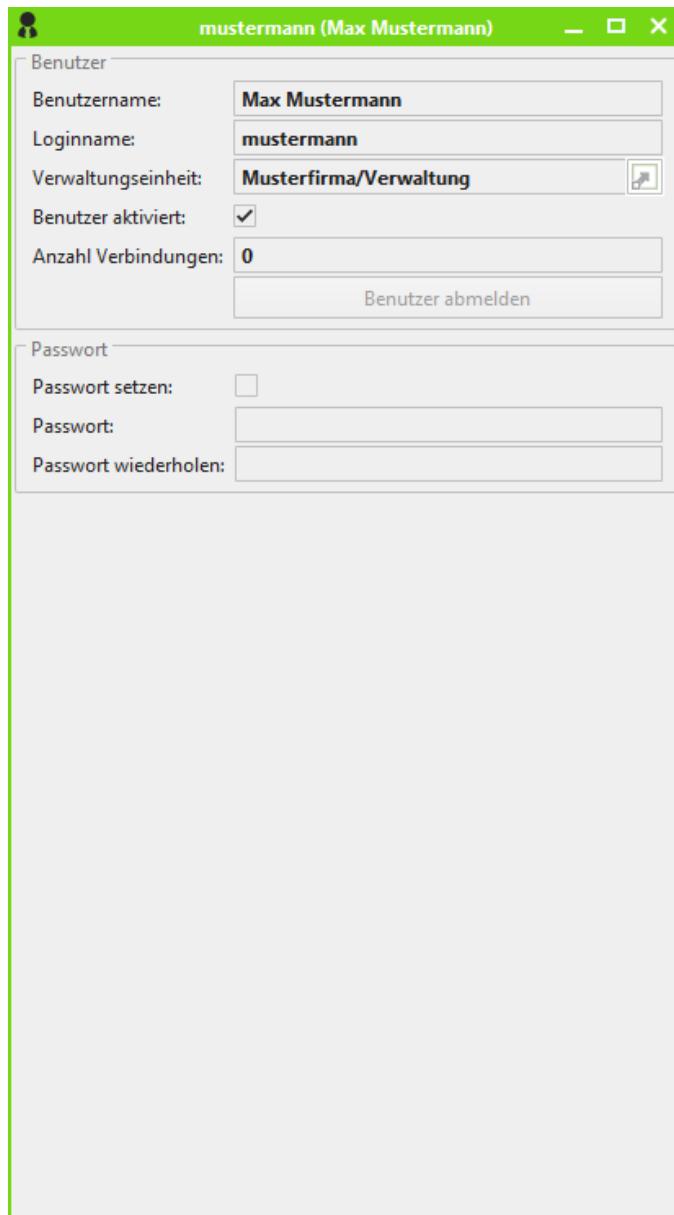


Abbildung 4.34 - Benutzer, Grundeinstellungen

Benutzer

Benutzername

Hier kann der Name des Benutzers eingetragen werden.

Loginname

Dies ist der Name, mit dem sich der Benutzer am Admin-Server anmeldet.



Der Loginname muss eindeutig sein!

Der Loginname des AdminBenutzer (**admin**) kann nicht geändert werden.

Verwaltungseinheit

Siehe 4.5.1.

Benutzer aktiviert

Nur aktivierte Benutzer können sich anmelden. Wird ein Benutzer deaktiviert (gesperrt), so werden bestehende Sitzungen sofort beendet.

Anzahl Verbindungen

Hier wird angezeigt, wie oft der Benutzer zur Zeit angemeldet ist.

Benutzer abmelden

Über diese Schaltfläche werden alle aktiven Sitzungen des gewählten Benutzers beendet.

Passwort

Passwort setzen

Wenn diese Checkbox selektiert ist, kann hier das Passwort eingestellt werden.

Passwort

Hier kann das Passwort des Benutzers gesetzt werden.

Passwort wiederholen

Geben Sie hier das Passwort aus Sicherheitsgründen ein zweites Mal ein.

4.17 Rolle konfigurieren

Eine Rolle bildet eine Funktion oder Zuständigkeit eines oder mehrerer Benutzer in INTUS COM ab.

Durch Berechtigung-Rolle-Zuordnungen erhält eine Rolle verschiedene Rechte auf Objekte einer Verwaltungseinheit (und ggf. untergeordneten Verwaltungseinheiten), die von Benutzern, die der Rolle durch Benutzer-Rolle-Zuordnungen zugeordnet sind, angewandt werden können.

Bei der ersten Anmeldung kennt INTUS COM nur die nicht löschenbare AdminRolle.

Sie können weitere Rollen entweder über das Menü **Neu/Rolle ...** oder im Kontextmenü des Benutzer-Rollen-Berechtigungen-Fensters (siehe 3.2.2) anlegen. Das folgende K&S Fenster (siehe 3.2.8) wird angezeigt:

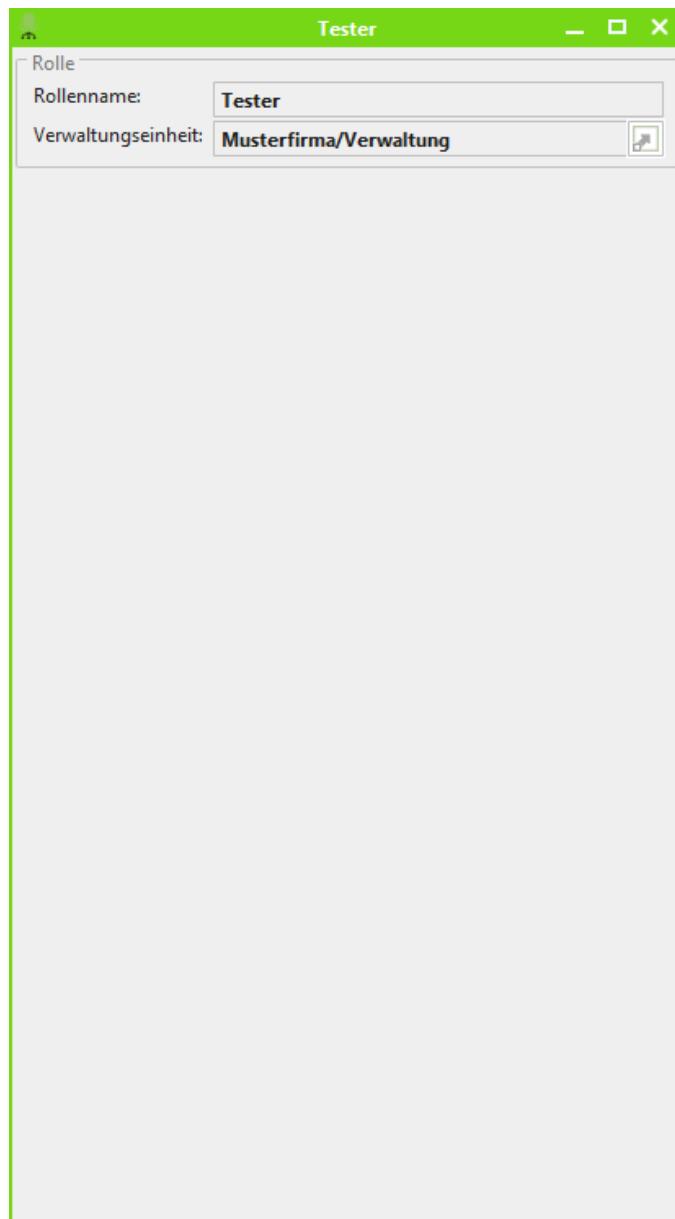


Abbildung 4.35 - Rolle, Grundeinstellungen

Rollenname

Der Rollenname dient dazu, die Rollen aus Anwendersicht voneinander zu unterscheiden.



Um Verwechslungen auszuschliessen, sind identische Namen für zwei Rollen nicht zulässig!

Verwaltungseinheit

Siehe 4.5.1.

4.18 Berechtigung konfigurieren

In Berechtigungen werden Rechte konfiguriert. Die konfigurierten Rechte können nur auf Objekte, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, angewandt werden.

Eine Berechtigung kann durch Berechtigung-Rolle-Zuordnungen einer Rolle zugeordnet werden. Benutzer, die ebenfalls dieser Rolle durch Benutzer-Rolle-Zuordnung zugeordnet sind, können die in der Berechtigung konfigurierten Rechte anwenden.

Bei der ersten Anmeldung kennt INTUS COM nur die nicht löschenbare AdminBerechtigung, welche immer alle Rechte auf alle Objekte enthält.

Sie können weitere Berechtigungen entweder über das Menü Neu/Berechtigung ... oder im Kontextmenü des Benutzer-Rollen-Berechtigungen-Fensters (siehe 3.2.2) anlegen. Das folgende K&S Fenster (siehe 3.2.8) wird angezeigt:

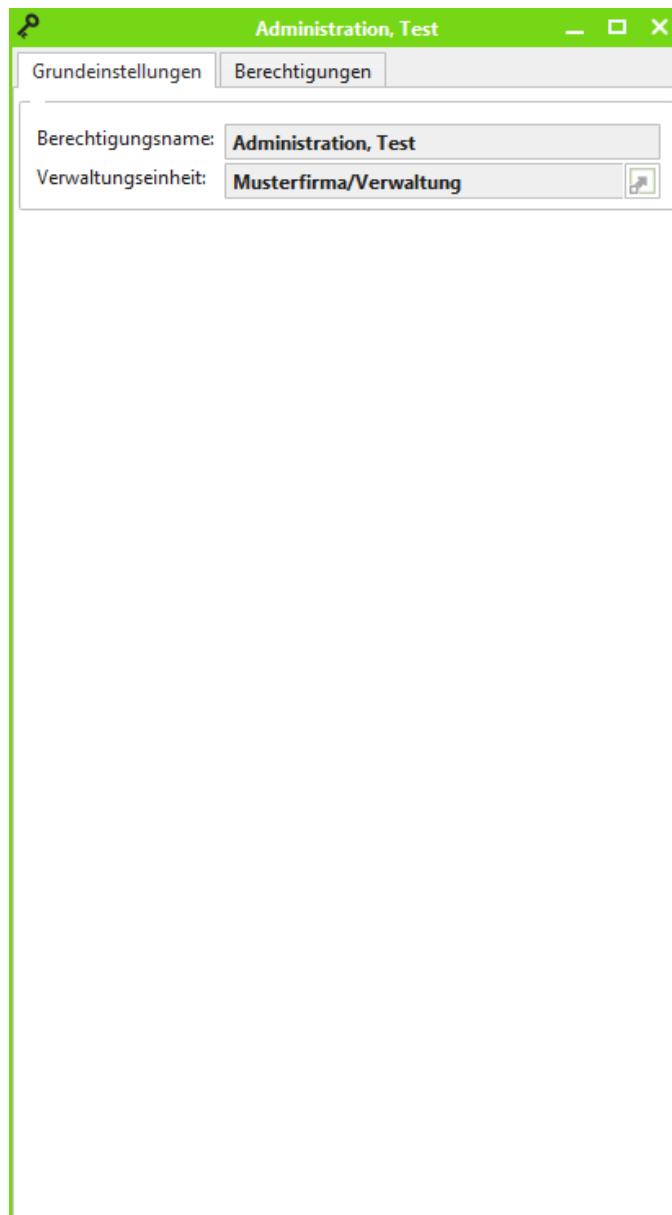


Abbildung 4.36 - Berechtigung, Grundeinstellungen

4.18.1 Registerblatt Grundeinstellungen

Berechtigungsname

Der Name, der nicht eindeutig sein muss, kann dem Anwender helfen, die Berechtigungen voneinander zu unterscheiden.

Verwaltungseinheit

Siehe 4.5.1.

4.18.2 Registerblatt Berechtigungen

Durch das Vorhandensein einer Berechtigung werden implizit

- das Leserecht für Hardware und Hardware-Verknüpfungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind
- das Leserecht für Offlineanlagen und Offlineblocklist, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind
- das Leserecht für Dienste und dienstbezogene Einstellungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind
- das Leserecht für die Verwaltungseinheit, der die Berechtigung zugewiesen ist, und ggf. deren untergeordnete Verwaltungseinheiten

gewährt.

Bei der AdminBerechtigung sind alle weiteren Rechte ebenfalls implizit gesetzt. Bei anderen Berechtigungen müssen weitere Rechte explizit gesetzt werden.

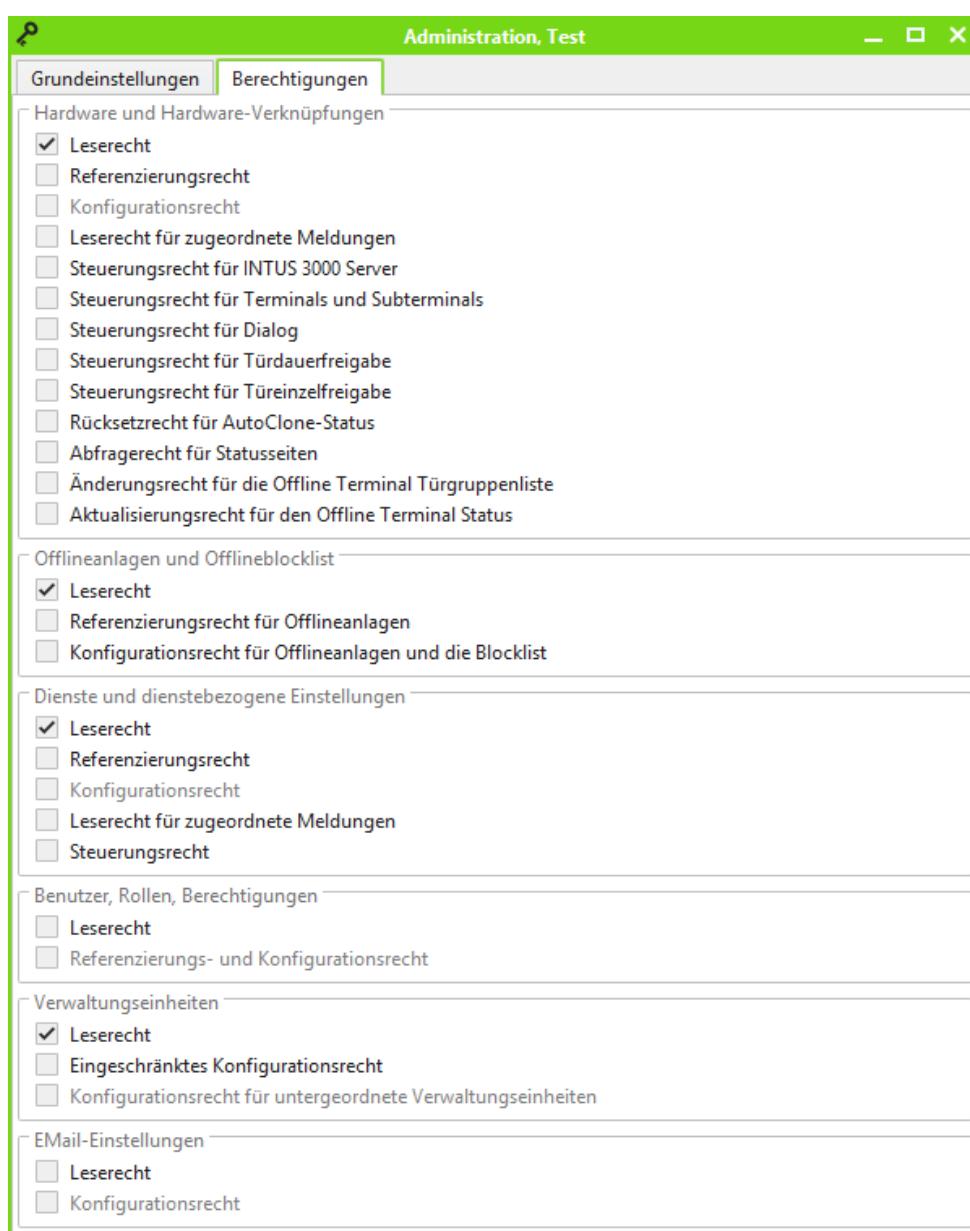


Abbildung 4.37 - Berechtigung, Berechtigungen

Hardware und Hardware-Verknüpfungen**Referenzierungsrecht**

Ermöglicht, dass bei der Konfiguration von Objekten auf Hardware, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, verwiesen werden darf.

Konfigurationsrecht

Ermöglicht das Anlegen, Konfigurieren und Löschen von Hardware und Hardware-Verknüpfungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Voraussetzung für die Vergabe dieses Rechts: Referenzierungsrecht für Hardware und Hardware-Verknüpfungen

Leserecht für zugeordnete Meldungen

Ermöglicht das Lesen von Meldungen für Hardware-Objekte, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Steuerungsrecht für INTUS 3000 Server

Ermöglicht es, den Serviceport für INTUS 3000 Server, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, neu zu verbinden.

Steuerungsrecht für Terminals und Subterminals

Ermöglicht es für INTUS 3000 Terminal/ACMs bzw. Subterminals, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind,

- einen AutoClone Download zu starten
- einen Download zu planen/starten/stoppen
- FP-Templates neu zu laden
- PS-Templates neu zu laden
- den Batterie-Zustand abzufragen
- die Uhrzeit zu stellen

Steuerungsrecht für Dialog

Ermöglicht es, einen Dialog mit INTUS 3000 Terminal/ACMs, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, zu starten.

Steuerungsrecht für Türdauerfreigabe

Ermöglicht es, für Türen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, eine Dauertüröffnung durchzuführen

Steuerungsrecht für Türeinzelfreigabe

Ermöglicht es, für Türen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, eine Einzeltüröffnung durchzuführen

Rücksetzrecht für AutoClone-Status

Ermöglicht es, den AutoClone Status von AutoClone Terminals, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, zurückzusetzen. Dabei wird das Passwort und die AutoClone-ID zurückgesetzt.

Abfragerecht für Statusseiten

Ermöglicht es, HTML-Statusseiten von INTUS 3000 Terminal/ACMs, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, anzuzeigen.

Änderungsrecht für die Offline Terminal Türgruppenliste

Ermöglicht das Bearbeiten und Ändern der Liste der Türgruppen-IDs von Offlineterminals, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind.

Voraussetzung für die Vergabe dieses Rechts: Konfigurationsrecht für Hardware und Hardware-Verknüpfungen

Aktualisierungsrecht für den Offline Terminal Status

Ermöglicht das Aktualisieren des Status von Offlineterminals, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind. Dieses Recht wird im Rahmen der Funktionalität „Import der Offline Terminal Konfigurationsergebnisse“ benötigt.

Offlineanlagen und Offlineblocklist

Referenzierungsrecht für Offlineanlagen

Ermöglicht, dass bei der Konfiguration von Objekten auf Offlineanlagen verwiesen werden darf, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind.

Konfigurationsrecht für Offlineanlagen und die Blocklist

Ermöglicht das Anlegen, Ändern und Löschen von Offlineanlagen und Blocklist, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie die Berechtigung zugewiesen sind.

Voraussetzung für die Vergabe dieses Rechts: Referenzierungsrecht für Offlineanlagen

Dienste und dienstebbezogene Einstellungen

Referenzierungsrecht

Ermöglicht, dass bei der Konfiguration von Objekten auf Dienste, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind, verwiesen werden darf.

Konfigurationsrecht

Ermöglicht das Anlegen, Konfigurieren und Löschen von Diensten, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Voraussetzung für die Vergabe dieses Rechts: Referenzierungsrecht für Dienste und dienstebbezogene Einstellungen

Leserecht für zugeordnete Meldungen

Ermöglicht das Lesen von Meldungen für Dienste, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Steuerungsrecht

Ermöglicht es für Dienste, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind,

- den Serviceport neu zu verbinden
- den Testmodus zu starten

Benutzer, Rollen, Berechtigungen

Leserecht

Ermöglicht das Lesen von Benutern, Rollen, Berechtigungen und ihren Verknüpfungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Referenzierungs- und Konfigurationsrecht

Ermöglicht das Anlegen, Konfigurieren und Löschen von Benutern, Rollen, Berechtigungen und ihren Verknüpfungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Voraussetzung für die Vergabe dieses Rechts: Leserecht für Benutzer, Rollen, Berechtigungen

Verwaltungseinheiten

Eingeschränktes Konfigurationsrecht

Ermöglicht es, das Hintergrundbild der Verwaltungseinheit, der die Berechtigung zugewiesen ist oder einer untergeordneten Verwaltungseinheit zu ändern.

Konfigurationsrecht für untergeordnete Verwaltungseinheiten

Ermöglicht das Anlegen, Konfigurieren und Löschen von Verwaltungseinheiten, die der Verwaltungseinheit, der die Berechtigung zugewiesen ist, untergeordnet sind.

Voraussetzung für die Vergabe dieses Rechts: Leserecht für Benutzer, Rollen, Berechtigungen, Leserecht für EMail-Einstellungen

EMail-Einstellungen

Leserecht

Ermöglicht das Lesen von EMail-Einstellungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Konfigurationsrecht

Ermöglicht das Anlegen, Konfigurieren und Löschen von EMail-Einstellungen, die der gleichen (oder einer untergeordneten) Verwaltungseinheit wie der Berechtigung zugewiesen sind.

Voraussetzung für die Vergabe dieses Rechts: Leserecht für EMail-Einstellungen

4.19 Benutzer-Rolle-Zuordnung konfigurieren

Eine Benutzer-Rolle-Zuordnung bezeichnet ein INTUS COM internes Verknüpfungsobjekt, das einem Benutzer eine Rolle zuweist. Dadurch erhält der Benutzer alle mit der Rolle verknüpften Rechte (siehe 4.18 und 4.20).

Bei der ersten Anmeldung kennt INTUS COM nur die nicht löschenbare AdminBenutzer-Admin-Rolle-Zuordnung, welche dem AdminBenutzer die AdminRolle zuweist.

Sie können weitere Benutzer-Rolle-Zuordnungen entweder über das Menü **Neu/Benutzer-Rolle-Zuordnung ...** oder im Kontextmenü des Benutzer-Rollen-Berechtigungen-Fensters (siehe 3.2.2) anlegen. Das folgende K&S Fenster (siehe 3.2.8) wird angezeigt:

4.20 - Berechtigung-Rolle-Zuordnung konfigurieren

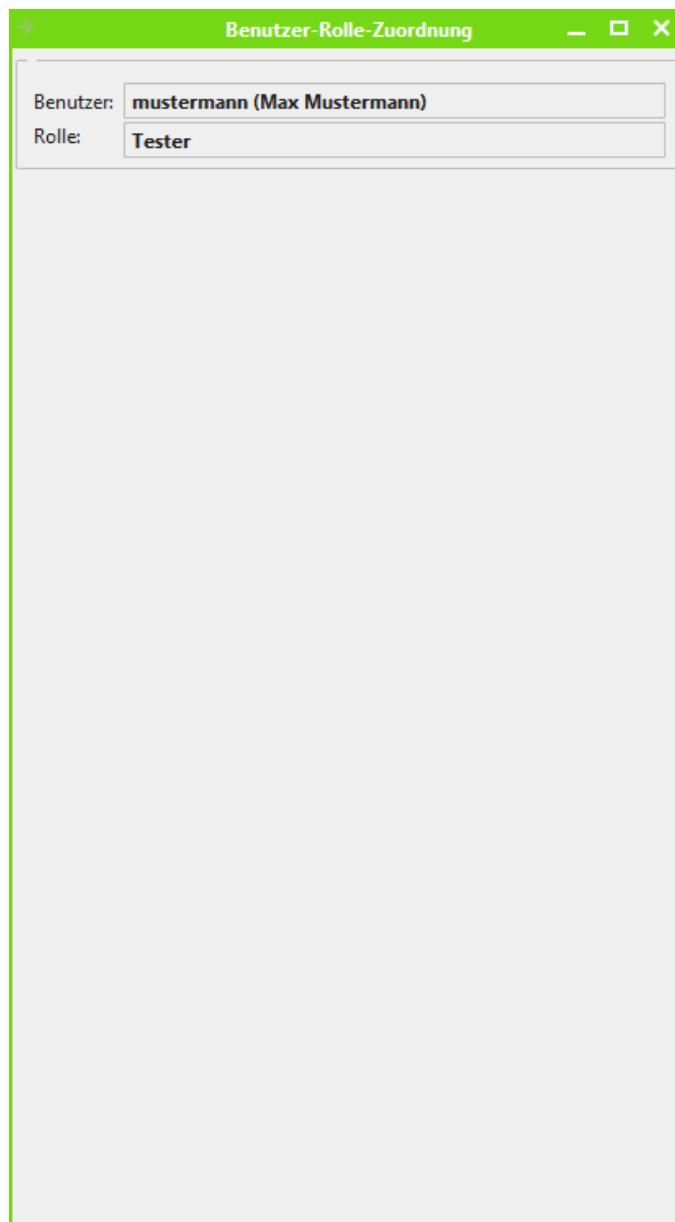


Abbildung 4.38 - Benutzer-Rolle-Zuordnung

Benutzer

Hier kann der Benutzer für diese Benutzer-Rolle-Zuordnung ausgewählt werden.

Rolle

Hier kann die Rolle für diese Benutzer-Rolle-Zuordnung ausgewählt werden.

4.20 Berechtigung-Rolle-Zuordnung konfigurieren

Eine Berechtigung-Rolle-Zuordnung bezeichnet ein INTUS COM internes Verknüpfungsobjekt, das einer Rolle eine Berechtigung zuordnet. Dadurch erhalten Benutzer, die der Rolle zugewiesen sind, alle Rechte dieser Berechtigung (siehe 4.18 und 0).

Bei der ersten Anmeldung kennt INTUS COM nur die nicht löschenbare AdminBerechtigung-AdminRolle-Zuordnung, welche die AdminBerechtigung der AdminRolle zuweist.

Sie können weitere Berechtigung-Rolle-Zuordnungen entweder über das Menü Neu/Berechtigung-Rolle-Zuordnung ... oder im Kontextmenü des Benutzer-Rollen-Berechtigungen-Fensters (siehe 3.2.2) anlegen. Das folgende K&S Fenster (siehe 3.2.8) wird angezeigt:

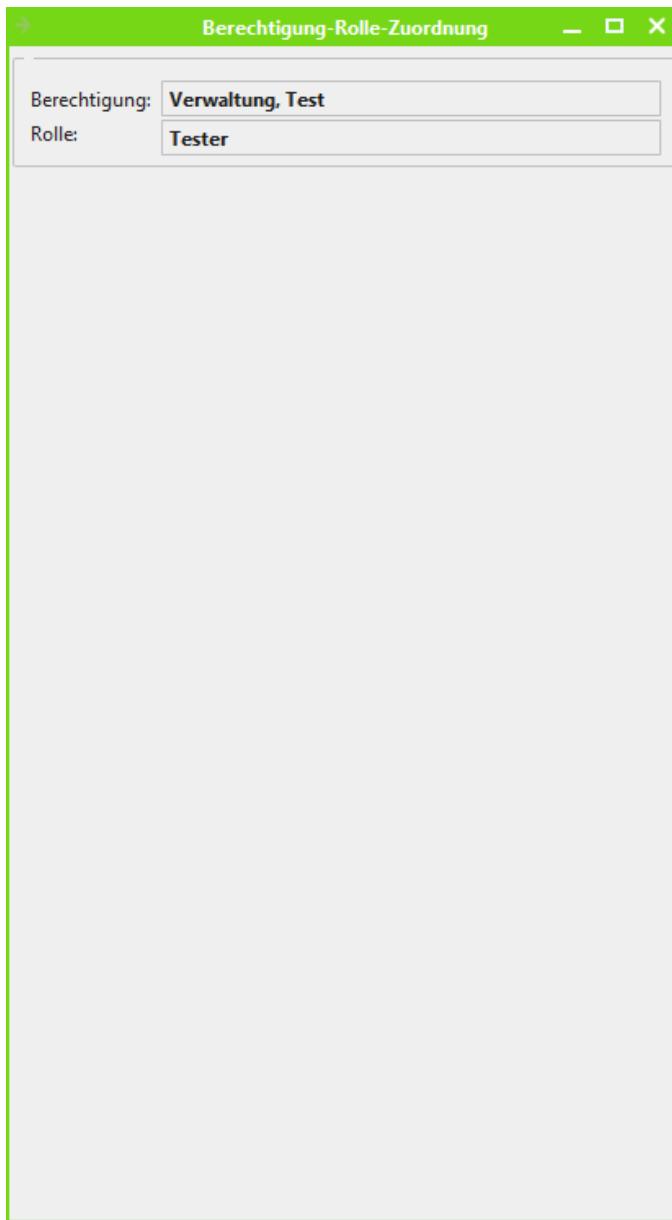


Abbildung 4.39 - Berechtigung-Rolle-Zuordnung

Berechtigung

Hier kann die Berechtigung für diese Berechtigung-Rolle-Zuordnung ausgewählt werden.

Rolle

Hier kann die Rolle für diese Berechtigung-Rolle-Zuordnung ausgewählt werden.

4.21 Video-Interface anlegen und konfigurieren

Das Video-Interface kann über das Menü **Neu / Video-Interface...** angelegt werden. Alternativ dazu öffnen Sie mit **Fenster / Videokomponenten** das Videokomponentenfenster und wählen Sie im Kontextmenü der ersten Komponente **Terminal Management System** den Punkt **Neu/Video-Interface...** aus.

Das Video-Interface kann nur genau einmal für eine INTUS COM Installation angelegt werden. Die Konfiguration des Video-Interface erfolgt in einem K&S-Fenster (siehe 3.2.8).

4.21.1 Registerblatt Grundeinstellungen

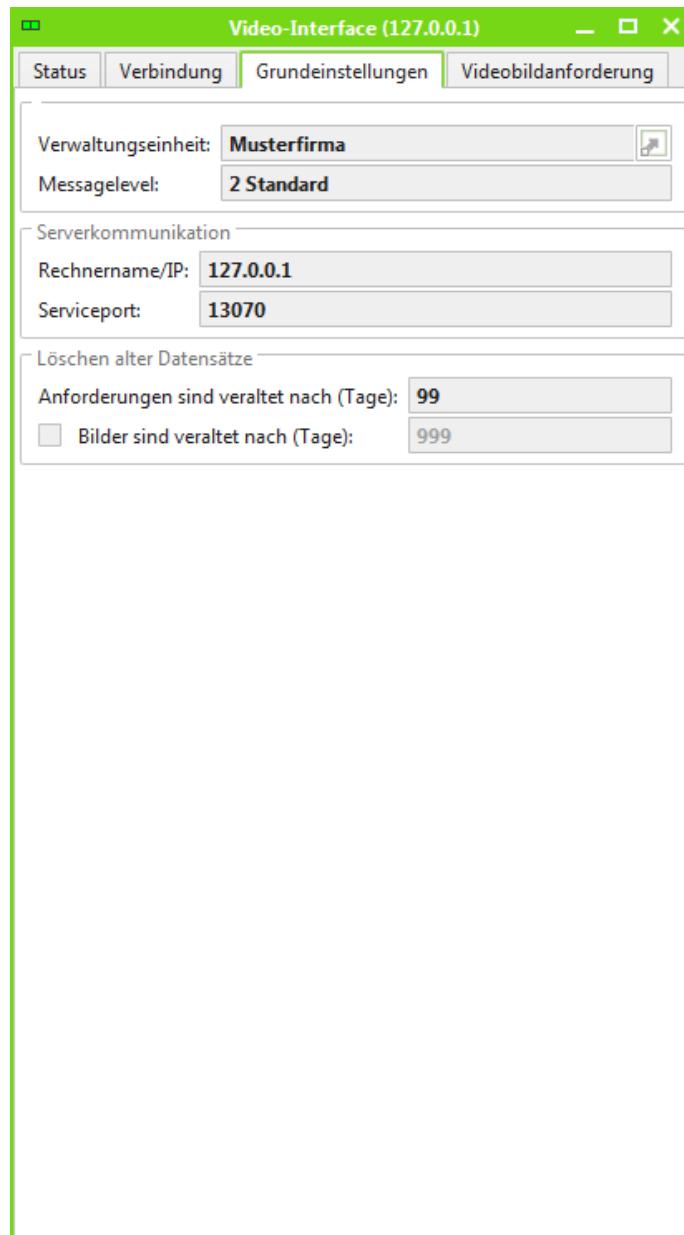


Abbildung 4.40 - Video-Interface, Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Rechnername/IP, Port

Siehe 4.5.3.

Anforderungen sind veraltet nach (Tage)

Dieser Parameter gibt die Anzahl der Tage an, nach denen eine Videobildanforderung durch das Video-Interface als veraltet angesehen wird. Veraltete Videobildanforderungen werden durch das Video-Interface aus der Tabelle INTUSCOM_VIDEO_REQUESTS entfernt. Einstellbar sind von 1 bis 99 Tage.

Bilder sind veraltet nach (Tage)

Dieser Parameter gibt die Anzahl der Tage an, nach denen ein Videobild durch das Video-Interface als veraltet angesehen wird. Ist dieser Parameter aktiviert, so werden veraltete Videobilder durch das Video-Interface aus der Tabelle INTUSCOM_VIDEO_IMAGES entfernt. Einstellbar sind von 1 bis 999 Tage.

4.21.2 Registerblatt Videobildanforderung

An dieser Stelle wird eingestellt wieviele und für welche Ereignisse, Videobilder von den konfigurierten Videoquellen geladen werden sollen.

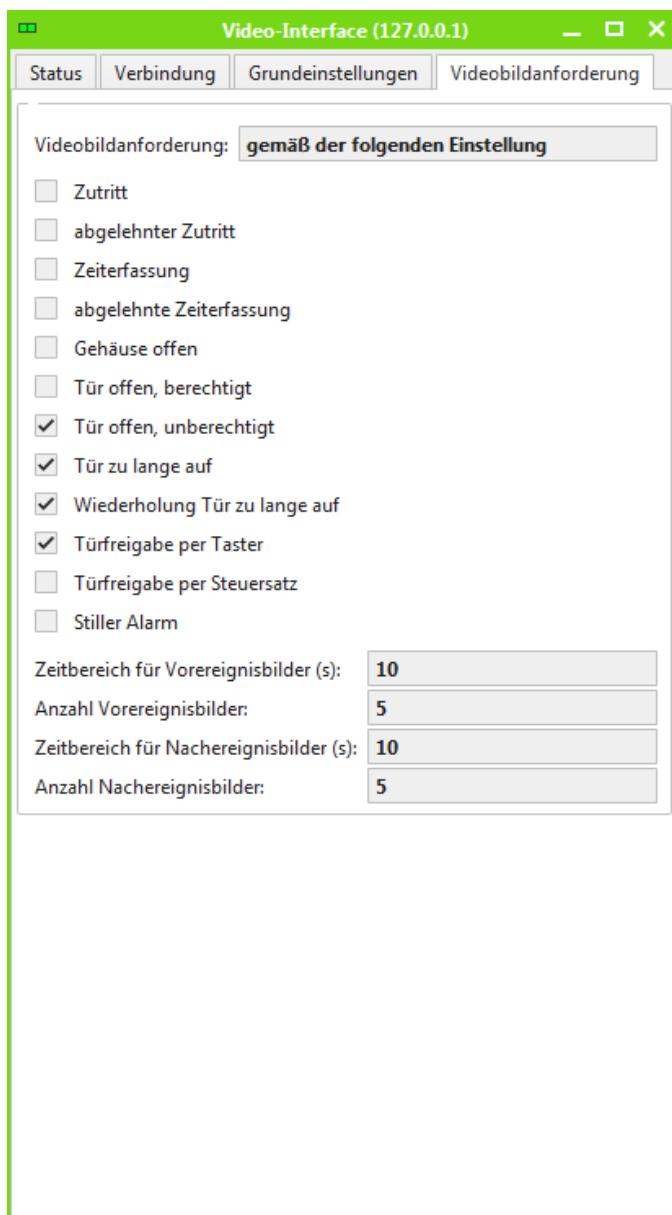


Abbildung 4.41 - Video-Interface, Videobildanforderung

Videobildanforderung

Es kann eingestellt werden, ob Videobildanforderungen durch eine globale Einstellung für alle Leser, oder über Videoprofile gesteuert werden.

- **gemäß der folgenden Einstellung** – Diese Einstellung bewirkt, dass Videobildanforderungen für alle Leser die mit mindestens einer Kamera verknüpft sind, gemäß den ausgewählten Ereignissen erzeugt werden.

- **Steuerung über Videoprofile** – Diese Einstellung bewirkt, dass die Erzeugung von Videobildanforderungen durch die Videoprofile in der Tabelle INTUSCOM_VIDEO_PROFILES gesteuert wird.

Zeitbereich für Vor-/Nachereignisbilder

Dieser Parameter bezeichnet den Zeitbereich für die Vor- bzw. Nachereignisbilder. Einstellbar sind von 0 bis 99 Sekunden.

Anzahl Vor-/Nachereignisbilder

Dieser Parameter bezeichnet die Anzahl der gewünschten Vor- bzw. Nachereignisbilder. Einstellbar sind von 0 bis 99 Bilder.

4.22 Videoquelle konfigurieren

Eine Videoquelle in INTUS COM können entweder Convision Videoserver oder SeeTec Gateway Service sein. Videoquellen halten Videobilder für einen bestimmten Zeitraum vor.

Abhängig von der INTUS COM Lizenz können entweder Convision Videoserver oder SeeTec Gateway Service angelegt werden.

Die Konfiguration einer Videoquelle erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für den Convision Videoserver bzw. SeeTec Application Gateway wie in 3.3.3.2 beschrieben.

4.22.1 Registerblatt Grundeinstellungen

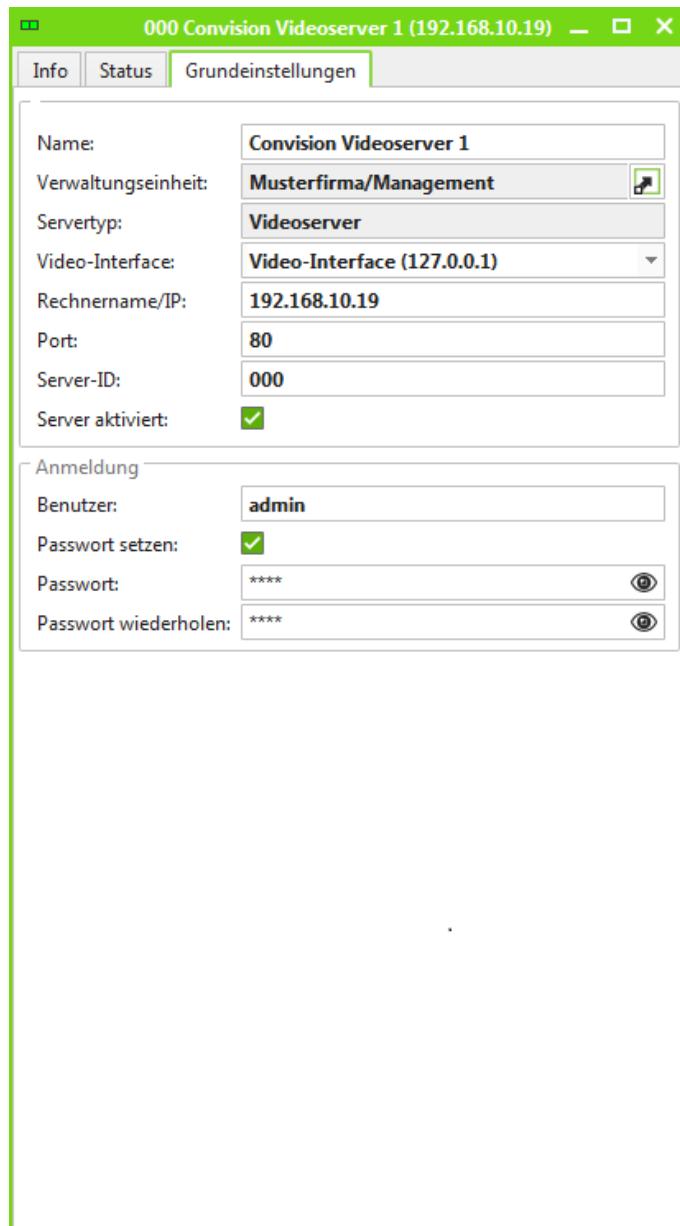


Abbildung 4.42 - VideoServer, Grundeinstellungen

Name

Anzeigetext zur Identifizierung einer Videoquelle in der Benutzeroberfläche.

Verwaltungseinheit

Siehe 4.5.1.

Video-Interface

Referenz auf Video-Interface.

Rechnername/IP

Siehe 0

Port

Port 80 ist der Standardport für einen Convision Videoserver.

Port 62000 ist der Standardport für ein SeeTec Gateway Service.

Server-ID

Hier kann die dreistellige Server-ID des Videoquelle eingestellt werden.

Server aktiviert

Hier kann eingestellt werden, ob der Videoquelle aktiviert oder deaktiviert ist.

Anmeldung

Benutzername

Benutzername für die Anmeldung am Videoquelle.

Passwort setzen

Hier kann eingestellt werden, dass das Passwort geändert werden soll.

Passwort

Hier kann das neue Passwort eingegeben werden.

Passwort wiederholen

Hier muss die neue Passwort aus Sicherheitsgründen wiederholt werden.

4.23 Kamera konfigurieren

Eine Kamera bezeichnet in INTUS COM eine Netzwerkkamera oder Analogkamera, die an Cayuga angeschlossen ist und über den SeeTec Gateway Service (ab Cayuga S100) erreichbar ist.

Die Konfiguration einer Kamera erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für die Kamera wie in 3.3.3.2 beschrieben.

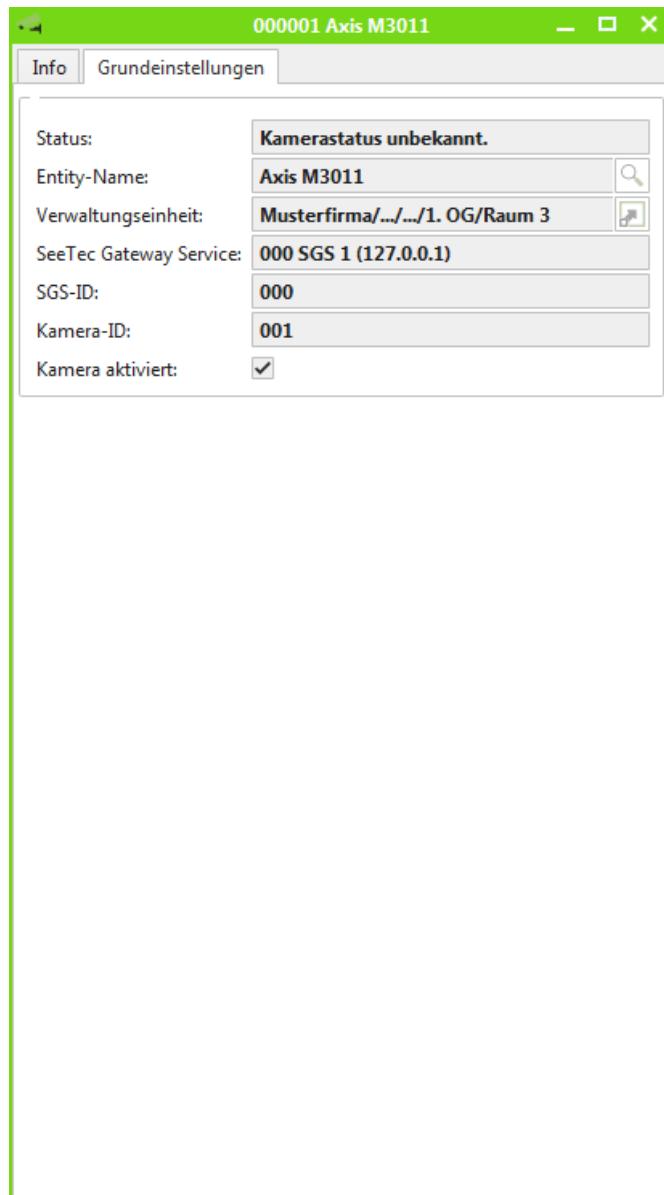


Abbildung 4.43 - Kamera an SeeTec Gateway Service, Grundeinstellungen

Status

Zeigt an, ob die konfigurierte Kamera im konfigurierten SeeTec Gateway Service bekannt ist. Diese Anzeige ist auch abhängig vom Verbindungs- und Betriebsstatus des SAG.

- **Kamera ok**
Entity-Name der Kamera ist im SAG bekannt.
- **Kamera unbekannt**
Entity-Name der Kamera ist im SAG nicht bekannt. Prüfen Sie die Kamerakonfiguration in SeeTec.
- **Kamerastatus unbekannt**
Der Entity-Name kann zur Zeit nicht verifiziert werden. Entweder liegt am SeeTec Gateway Service ein Verbindungs- oder Betriebsfehler vor, oder das SAG ist in INTUS COM deaktiviert.

Entity-Name

Der Entity-Name wird in SeeTec festgelegt. Die Schaltfläche rechts öffnet einen Dialog mit einer Auswahl der in SeeTec konfigurierten Kameras.

Verwaltungseinheit

Siehe 4.5.1.

SeeTec Gateway Service

Hier kann das SeeTec Gateway Service ausgewählt werden, an dem die Kamera angeschlossen ist. Es werden nur die SAG zur Auswahl angeboten, die bereits in INTUS COM konfiguriert sind.

SGS-ID

Nach dem Speichern der Konfiguration wird hier die ID des SeeTec Gateway Services, an dem die Kamera angeschlossen ist, angezeigt.

Kamera-ID

Hier kann die dreistellige Kamera-ID der Kamera eingestellt werden.

Kamera aktiviert

Hier kann eingestellt werden, ob die Kamera aktiviert oder deaktiviert ist.

4.24 Kamera-Leser-Zuordnung konfigurieren

Eine Kamera-Leser-Zuordnung bezeichnet ein INTUS COM internes Verknüpfungsobjekt, das innerhalb von INTUS COM eine Zuordnung von Lesereignissen zu einer bestimmten Kamera ermöglicht.

Die Konfiguration einer Kamera-Leser-Zuordnung erfolgt in einem K&S-Fenster (siehe 3.2.8). Aktivieren Sie den Änderungsmodus für die Kamera-Leser-Zuordnung wie in 3.3.3.2 beschrieben.

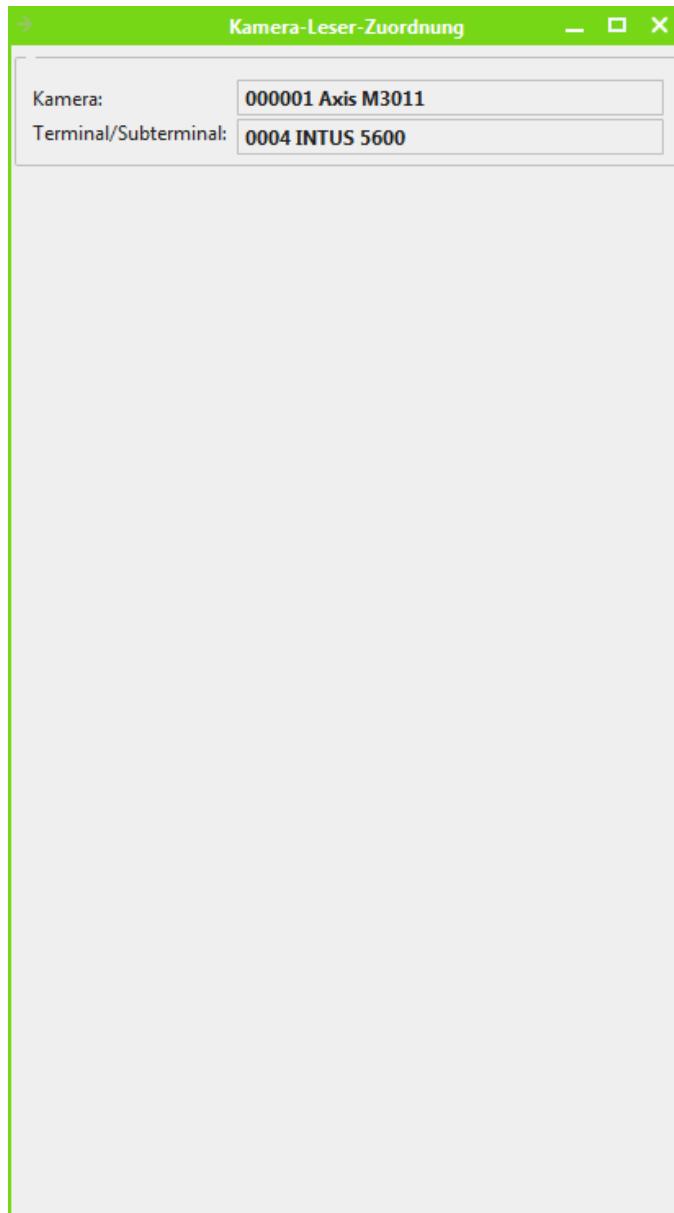


Abbildung 4.44 - Kamera-Leser-Zuordnung

Kamera

Hier kann die Kamera für diese Kamera-Leser-Zuordnung ausgewählt werden.

Terminal/Subterminal

Hier kann ein Terminal oder Subterminal für diese Kamera-Leser-Zuordnung ausgewählt werden.

4.25 PS-Distributor konfigurieren

Der PS-Distributor kann über das Menü Neu / PS-Distributor... angelegt werden. Alternativ dazu öffnen Sie mit Fenster / PS-Distribution das Fenster PS-Distribution und wählen Sie im Kontextmenü der ersten Komponente Terminal Management System den Punkt Neu / PS-Distributor... aus.

Der PS-Distributor kann nur genau einmal für eine INTUS COM Installation angelegt werden. Die Konfiguration des PS-Distributor erfolgt in einem K&S-Fenster (siehe 3.2.8).

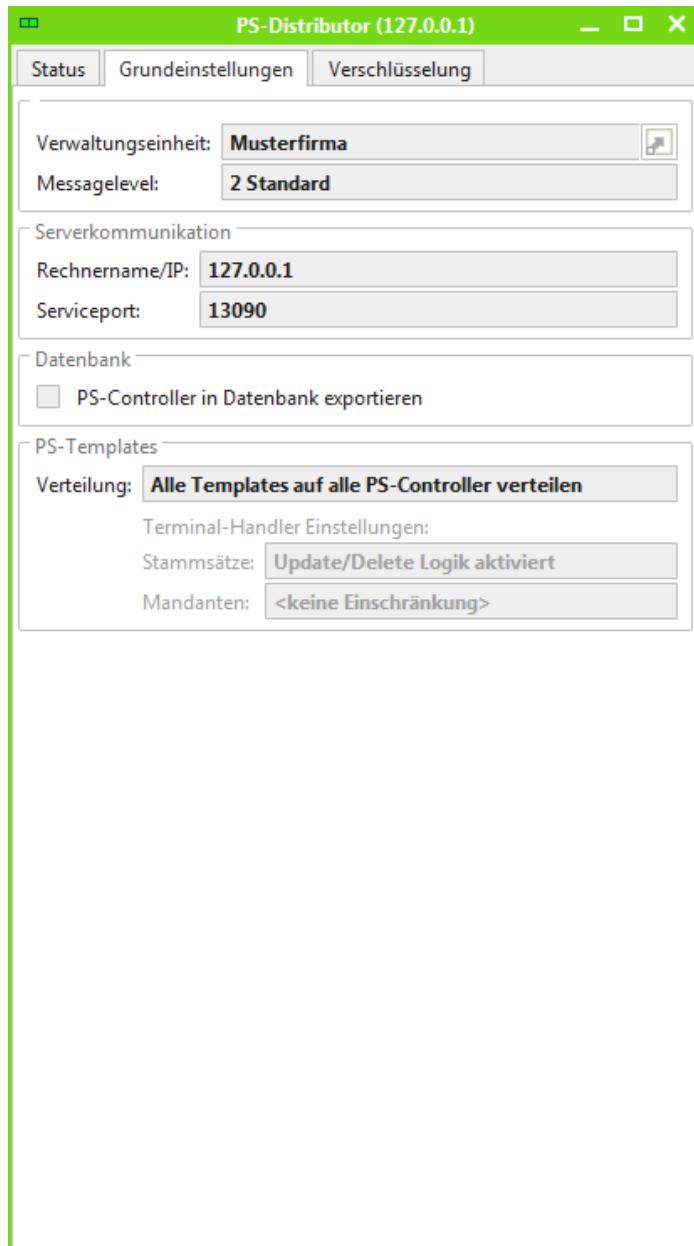


Abbildung 4.45 - PS-Distributor, Grundeinstellungen

4.25.1 Registerblatt Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Rechnername/IP, Serviceport

Siehe 4.5.3.

PS-Controller in die Datenbank exportieren

Dieser Parameter weist den INTUS COM PS-Distributor an, die Einstellungen der konfigurierten PS-Controller in die Datenbank (Tabelle: `INTUS_PS_READERS`) zu exportieren.

Verteilung

Dieser Parameter legt fest, wie die PS-Templates auf die PS-Controller verteilt werden. Für die PS-Templateverteilung gibt es zwei mögliche Einstellungen:

- Alle Templates auf alle PS-Controller verteilen
- Templates anhand der Stammsätze & Profile verteilen.

Durch die Einstellung „Templates anhand der Stammsätze & Profile verteilen“ werden beim Download der PS-Templates die Datenbanktabellen `INTUSCOM_MASTER_RECORDS` und `INTUSCOM_PROFILES` zur Auswahl der Templates für einen PS-Controller herangezogen. Die Verteilung der Templates anhand der Stammsätze und Profile ist abhängig von den folgenden Einstellungen im Terminal-Handler:

- Update/Delete Logik für Stammsätze
- Mehrmandantenmodus

4.25.2 Registerblatt Verschlüsselung

An dieser Stelle kann der Schlüssel gesetzt werden, den der PS-Distributor verwendet, um mit PS-Controllern verschlüsselt zu kommunizieren.

Die Einstellung der Pass Phrase an einem Subterminal erfolgt nicht durch INTUS COM, sondern muss über das Programm INTUS PS Setup eingegeben werden!

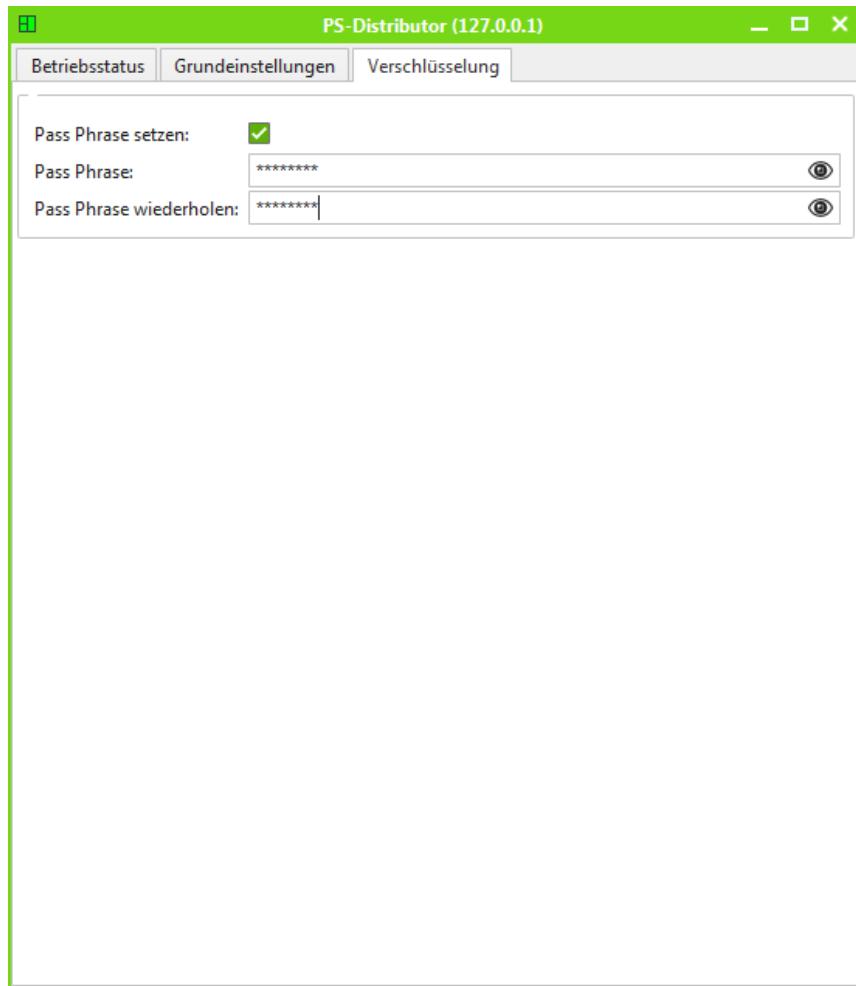


Abbildung 4.46 - PS-Distributor, Verschlüsselung

Pass Phrase setzen

Hier kann eingestellt werden, dass der Schlüssel für die verschlüsselte Kommunikation geändert werden soll.

Pass Phrase

Hier kann die neue Pass Phrase eingegeben werden.

Pass Phrase wiederholen

Hier muss die neue Pass Phrase zur Bestätigung wiederholt werden.

4.26 AutoClone Dienst konfigurieren

Der AutoClone Dienst kann über das Menü Neu / AutoClone Server... angelegt werden. Alternativ dazu öffnen Sie mit Fenster / AutoClone das Fenster AutoClone und wählen Sie im Kontextmenü der ersten Komponente Terminal Management System den Punkt Neu / AutoClone Server... aus.

Der AutoClone Dienst kann nur genau einmal für eine INTUS COM Installation angelegt werden. Die Konfiguration des AutoClone Dienst erfolgt in einem K&S-Fenster (siehe 3.2.8).

4.26.1 Registerblatt Grundeinstellungen

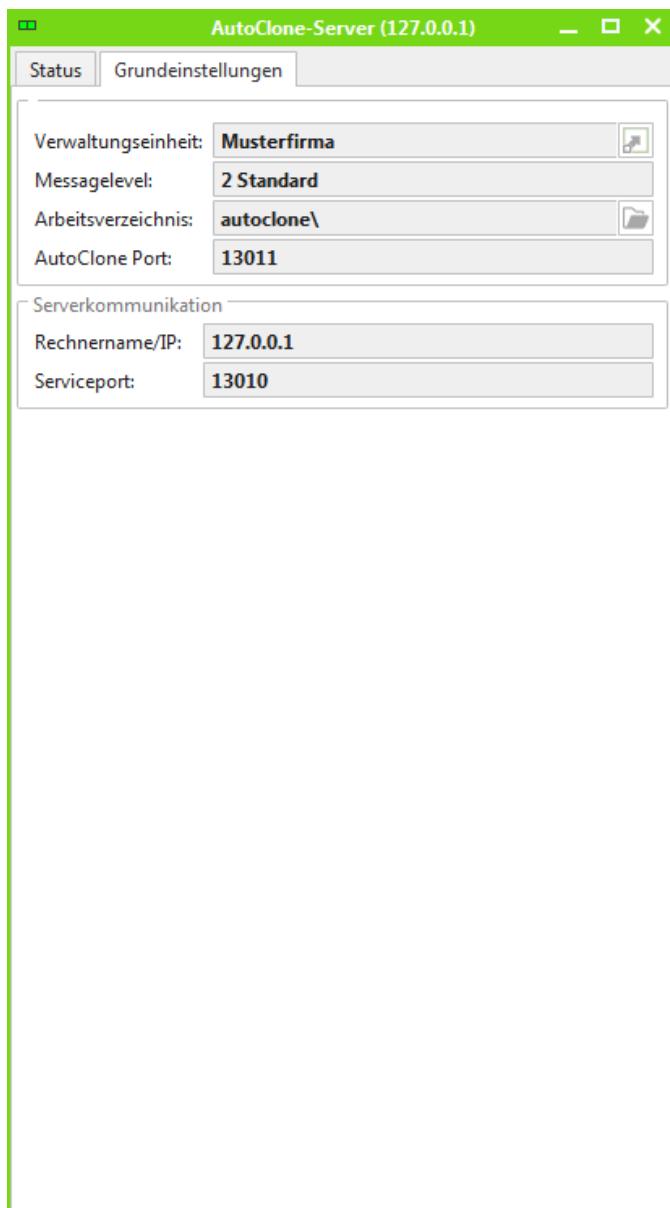


Abbildung 4.47 - AutoClone Dienst, Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Messagelevel

Siehe 4.5.3.4.

Arbeitsverzeichnis

Arbeitsverzeichnis des AutoClone Dienst.

AutoClone Port

Port, auf dem AutoClone Dienst auf Verbindungen von AutoClone-fähigen Terminals wartet.

Serverkommunikation

Rechnername/IP, Serviceport

Siehe 4.5.3.

4.27 EMail-Einstellung konfigurieren

Sie können eine EMail-Einstellung, die für jede Email-Adresse, die im Falle eines TPI Alarms oder Ereignis benachrichtigt werden soll, erforderlich ist, entweder über das Menü Neu/EMail-Einstellung ... oder im Kontextmenü des Verwaltungseinheiten-Fensters (siehe 3.2.1) anlegen. Das folgende K&S Fenster (siehe 3.2.8) wird angezeigt:

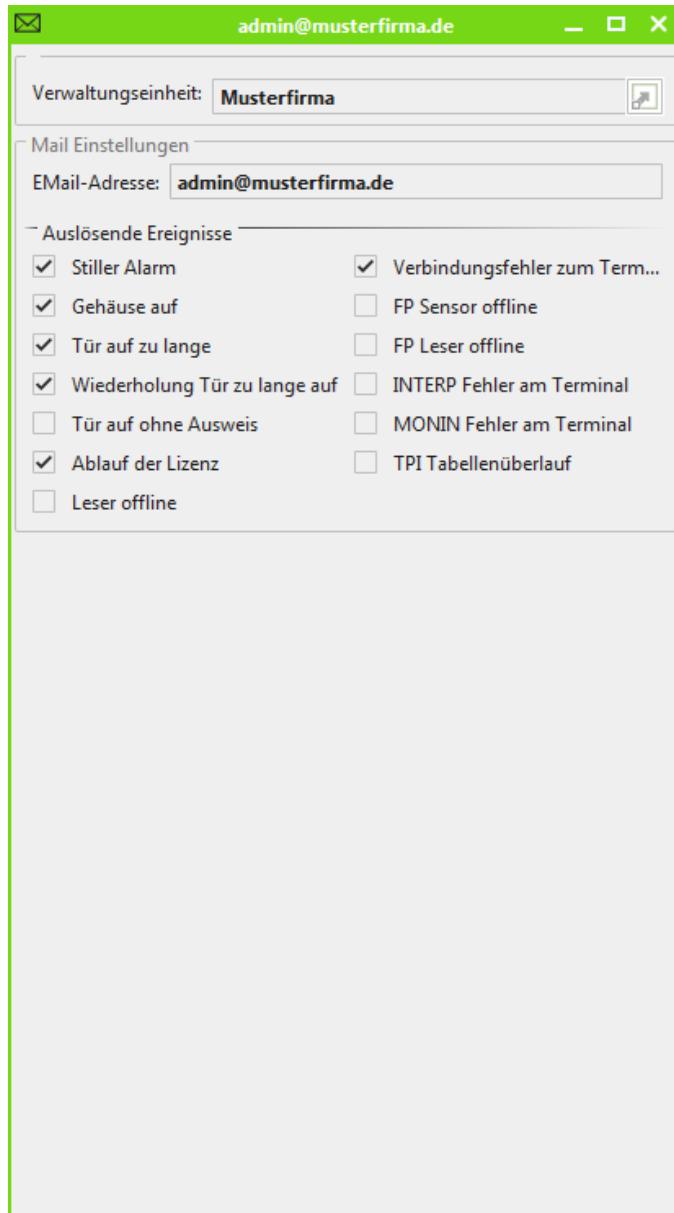


Abbildung 4.48 – Email-Einstellung, Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Eine E-Mail wird immer dann gesendet, wenn ein auslösender/s Alarm/Ereignis von einer Komponente ausgeht, die dieser (oder einer untergeordneten) Verwaltungseinheit zugewiesen ist.

Mail Einstellungen

EMail-Adresse

Adresse, an die die Email geschickt wird.

Auslösende Ereignisse

Hier kann festgelegt werden, auf welche Ereignisse eine Mail gesendet werden soll.

4.28 Offlineanlage konfigurieren

Eine Offlineanlage wird benötigt, um in INTUS COM Offlineterminals verwalten zu können, die gemäß dem OSS Standard Offline arbeiten. Jedes dieser Offlineterminals ist genau einer Offlineanlage zugeordnet.

INTUS COM bietet die Möglichkeit, mit mehreren Offlineanlagen zu arbeiten. Jede Offlineanlage muss eine eindeutige Offlineanlagen-ID haben. Diese Offlineanlagen-ID wird auch als Site-ID bezeichnet.

Wenn Sie eine neue Offlineanlage anlegen möchten, wählen Sie bitte im Menü den Punkt Neu/Offlineanlage... aus.

The screenshot shows a configuration window titled '[1] Offlineanlage für den Standort München'. The window is divided into sections:

- Grundeinstellungen**:
 - Name: Offlineanlage für den Standort München
 - Verwaltungseinheit: [Wurzelverwaltungseinheit]
 - Offlineanlagen-ID: 1
 - Spezielle Türgruppennummern:
- Voreinstellungen für Berechtigungsdaten**:
 - Berechtigungsdaten-Gültigkeit: Berechtigung endet mit Stammsatzgültigkeit
 - Gültigkeitsende Tag: 1
 - Gültigkeitsende Uhrzeit: 20:00
 - Gültigkeitsvortrags-Uhrzeit: 12:00

Abbildung 4.49 – Offlineanlage

Grundeinstellungen

Name

Der Name kann dem Anwender helfen, Offlineanlagen voneinander zu unterscheiden.

Verwaltungseinheit

Siehe 4.5.1.

Offlineanlagen-ID

Die Offlineanlagen-ID wird auch als Site-ID bezeichnet. Sie muss über alle Offlineanlagen eines INTUS COM Systems hinweg eindeutig sein.

Erlaubt sind Werte im Bereich 1 – 65535.

Bei der Inbetriebnahme von Offlineterminals wird unter Anderem die Offlineanlagen-ID (Site-ID) in der Offlineterminal-Hardware eingestellt. Deshalb ist es empfehlenswert, die Offlineanlagen-ID nicht mehr zu ändern, nachdem für die Offlineanlage bereits Offlineterminals in Betrieb genommen wurden.

Spezielle Türgruppennummern

Die Türgruppennummern 65533, 65534 und 65535 sind für Demontagekarten, Batteriewechselkarten bzw. Servicekey-Karten für INTUS Flex Offlineterminals reserviert.

Durch Einschalten der Option „Spezielle Türgruppennummern“ können diese speziellen Türgruppennummern Offlineterminals als normale Türgruppennummern zugewiesen werden.

Es wird empfohlen, diese Option ausgeschaltet zu lassen.

Voreinstellungen für Berechtigungsdaten

Diese Werte haben in INTUS COM keine besonderen Auswirkungen. Sie können durch die Applikation über das INTUSCOM Client-Interface abgefragt und für das Erzeugen von Kartendaten verwendet werden.

Berechtigungsdaten-Gültigkeit

Bei der Berechtigungsdaten-Gültigkeit handelt es sich um eine Voreinstellung zum Einfluss des Stammsatz-Gültigkeitsendes auf das Gültigkeitsende der Offline-Berechtigungen.

Folgendes ist zu beachten:

Wenn der Gültigkeitsvortrag im Terminal verwendet wird, und durch die Stammsatzgültigkeit begrenzt werden soll, müssen in TPI die Stammsatzfelder Gültigkeitsendedatum und –uhrzeit parametriert sein.

Wenn in TPI das Stammsatzfeld Gültigkeitsendedatum aber nicht das Stammsatzfeld Gültigkeitsendeuhrzeit parametriert ist, kann die Einstellmöglichkeit „Berechtigung kann die Uhrzeit der Stammsatzgültigkeit überschreiten“ verwendet werden.

Gültigkeitsende Tag, Gültigkeitsende Uhrzeit und Gültigkeitsvortrags-Uhrzeit

Bei dem Gültigkeitsende Tag, der Gültigkeitsende Uhrzeit und der Gültigkeitsvortrags-Uhrzeit handelt es sich um Voreinstellungen.

Die Gültigkeitsende Uhrzeit gibt die Uhrzeit an, zu der die Offline-Berechtigung enden soll.

Der Gültigkeitsende Tag gibt den Tag, an dem die Offline-Berechtigung enden soll, relativ zum Basistag des Gültigkeitsvortrags an.

Dieser Basistag ist entweder der Tag der Schreibbuchung (mit der die Offline-Berechtigung auf den Ausweis geschrieben wird) oder der Vortag der Schreibbuchung. Dies hängt davon ab, ob die Uhrzeit der Schreibbuchung vor der Gültigkeitsvortrags-Uhrzeit liegt.

Beispiel 4.1 – Gültigkeitsvortrag

Um das Beispiel einfach zu halten, wird davon ausgegangen, dass das Stammsatzgültigkeitsende nicht berücksichtigt werden muss.

Folgende Einstellungen werden verwendet:

Gültigkeitsende Tag: 1

Gültigkeitsende Uhrzeit: 20:00

Gültigkeitsvortrags-Uhrzeit: 12:00

Eine Schreibbuchung erfolgt am 01.04.2021 um 09:00 Uhr. Die Uhrzeit der Schreibbuchung liegt vor der Gültigkeitsvortrags-Uhrzeit von 12:00 Uhr. Deshalb wird der Vortag der Schreibbuchung, der 31.03.2021, als Basistag genommen. Der Gültigkeitsende Tag soll 1 Tag nach dem Basistag sein. Das ist der 01.04.2021. Die geschriebene Offline-Berechtigung endet also am 01.04.2021 um 20:00 Uhr.

Eine zweite Schreibbuchung erfolgt am 01.04.2021 um 14:00 Uhr. Die Uhrzeit der Schreibbuchung liegt nach der Gültigkeitsvortrags-Uhrzeit von 12:00 Uhr. Deshalb wird der Tag der Schreibbuchung, der 01.04.2021, als Basistag genommen. Der Gültigkeitsende Tag soll 1 Tag nach dem Basistag sein. Das ist der 02.04.2021. Die geschriebene Offline-Berechtigung endet also am 02.04.2021 um 20:00 Uhr.

4.29 Offlineterminal konfigurieren

INTUS COM unterstützt Offlineterminals die gemäß dem OSS Standard Offline arbeiten.

Um Offlineterminals konfigurieren zu können, muss bereits eine Offlineanlage konfiguriert sein.

Wenn Sie ein neues Offlineterminal anlegen möchten, wählen Sie bitte im Menü den Punkt **Neu/offline Terminal...** aus.

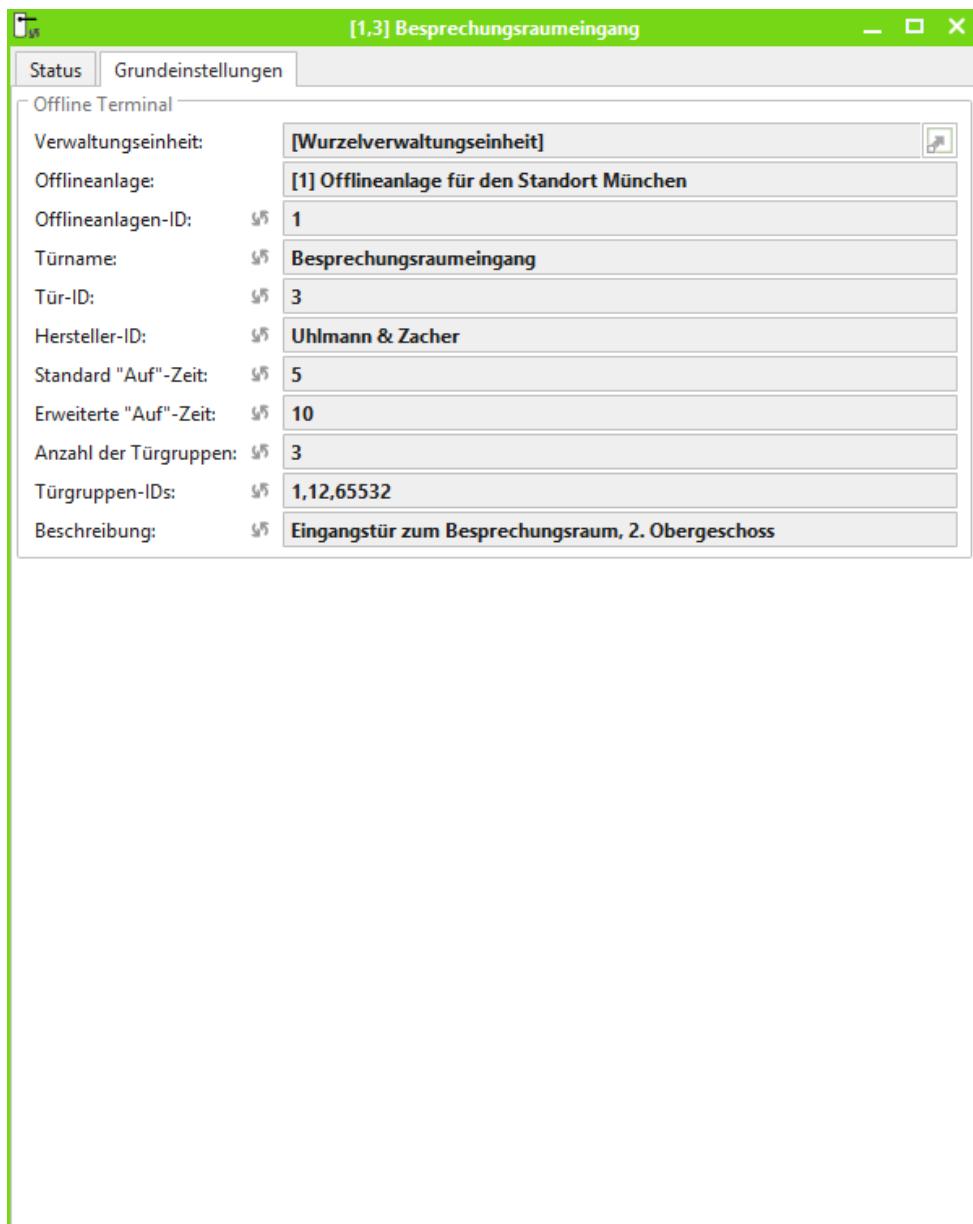


Abbildung 4.50 – Offlineterminal

Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Offlineanlage

Das ist die Offlineanlage, der das Offlineterminal zugeordnet ist.

Offlineanlagen-ID

Der Wert der Offlineanlagen-ID (Site-ID) des Offlineterminal kann nicht direkt konfiguriert werden. Er wird von der Offlineanlage übernommen, der das Offlineterminal zugeordnet ist.

Türname

Der Türname kann dem Anwender helfen, Offlineanterminals voneinander zu unterscheiden.

Tür-ID

Die Tür-ID wird auch als Door-ID bezeichnet. Die Tür-ID muss über alle Türen hinweg, die derselben Offlineanlage zugeordnet sind, eindeutig sein.

Erlaubt sind Werte im Bereich 1 – 65535.

Bei der Inbetriebnahme von Offlineterminals wird unter Anderem die Tür-ID (Door-ID) in der Offlineterminal-Hardware eingestellt. Die Kombination von Offlineanlagen-ID (Site-ID) und Tür-ID (Door-ID) identifiziert ein Offlineterminal im Kontext des OSS Standard Offline. Deshalb ist es empfehlenswert, die Tür-ID nicht mehr zu ändern, nachdem das Offlineterminal in Betrieb genommen wurde.

Hersteller-ID

Wenn der Hersteller des Offlineterminals in der von INTUS COM angebotenen Auswahlliste enthalten ist, sollte der passende Hersteller eingestellt werden.

Ansonsten sollte dieser Parameter leer gelassen werden.

Standard „Auf“-Zeit

Dies ist die Zeit in Sekunden, für die die Tür freigegeben werden soll, nachdem ein berechtigter Ausweis akzeptiert wurde, der die Türfreigabe mit Standardfreigabezeit („Default unlock time“) erlaubt.

Erweiterte „Auf“-Zeit

Dies ist die Zeit in Sekunden, für die die Tür freigegeben werden soll, nachdem ein berechtigter Ausweis akzeptiert wurde, der die Türfreigabe mit erweiterter Freigabezeit („Extended unlock time“) erlaubt.

Anzahl der Türgruppen

Die Anzahl der Türgruppen wird anhand der Liste der Türgruppen-IDs berechnet.

Türgruppen-IDs

Dieser Parameter gibt an, zu welchen Türgruppen das Offlineterminal gehören soll. Er enthält die Türgruppen-IDs (Door-Group-IDs) dieser Türgruppen in einer kommagetrennten Liste.

Türgruppen-IDs müssen im Bereich 1 – 65535 liegen. Die Türgruppennummern 65533, 65534 und 65535, die für Demontagekarten, Batteriewechselkarten bzw. Servicekey-Karten für INTUS Flex Offlineterminals reserviert sind, können jedoch nur dann angegeben werden, wenn bei der Offlineanlage (der das Offlineterminal zugeordnet ist) die Option „Spezielle Türgruppennummern“ eingeschaltet ist. Davon wird abgeraten.

Für das Bearbeiten der Liste der Türgruppen-IDs ist zusätzlich zum „Konfigurationsrecht für Hardware und Hardwareverknüpfungen“ das spezielle „Änderungsrecht für die Offline Terminal Türgruppenliste“ erforderlich.

Beschreibung

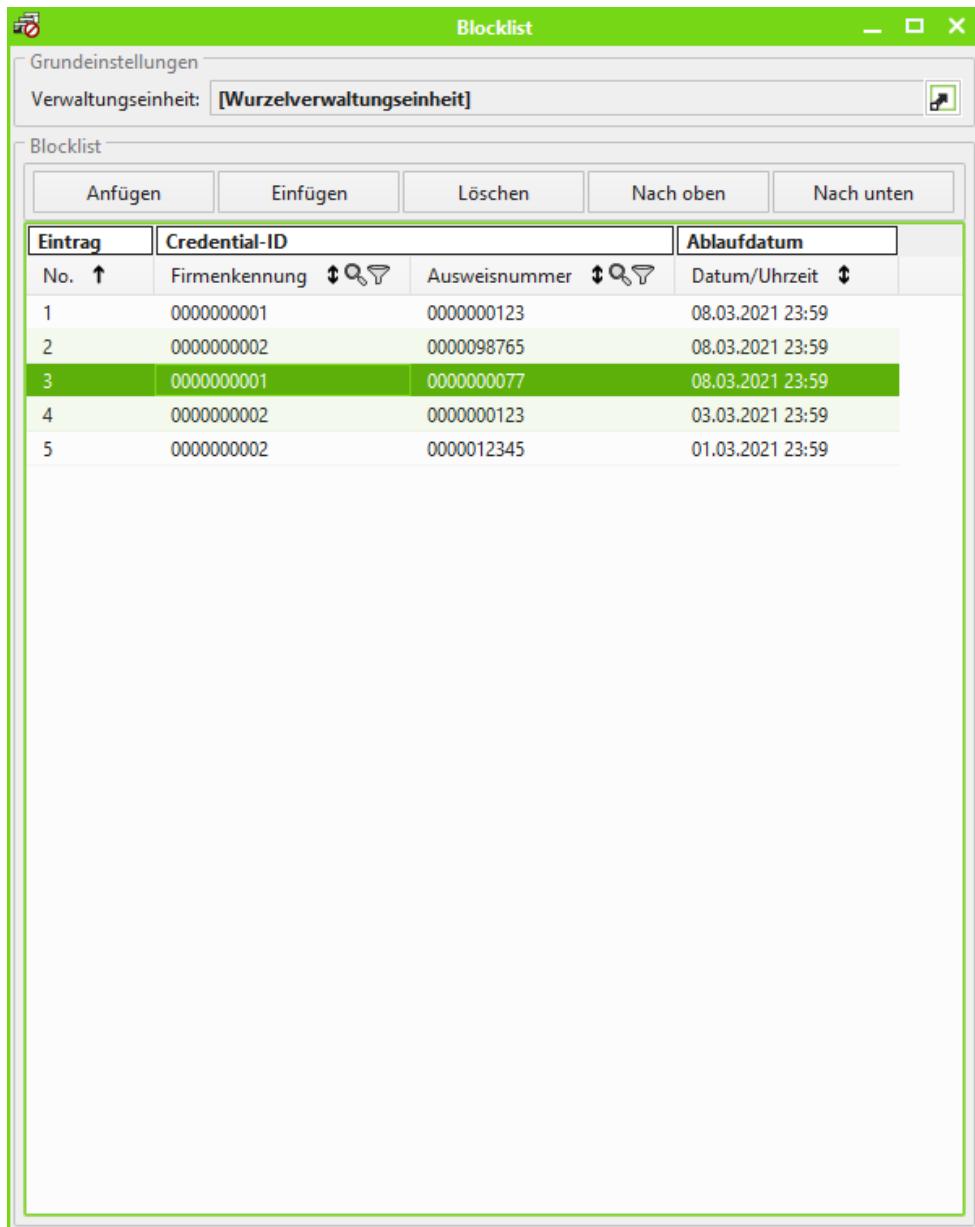
Dieser Parameter kann für zusätzliche Informationen zu dem Offlineterminal verwendet werden.

4.30 Blocklist konfigurieren

INTUS COM ermöglicht das Verwalten einer Blocklist. Diese dient dem Sperren von Ausweisen an Offlineterminals, die gemäß dem OSS Standard Offline arbeiten.

In einem INTUS COM System kann es nur eine Blocklist geben. Die Blocklist gilt für alle Offlineanlagen des INTUS COM Systems.

Wenn Sie die Blocklist anlegen möchten, wählen Sie bitte im Menü den Punkt **Neu/Blocklist...** aus.

*Abbildung 4.51 – Blocklist*

Prinzipielle Funktionsweise

Die Blocklist kann auf online angebundene TPI-Berechtigungsterminals geladen werden, die im Kontext des OSS Standard Offline als sogenannte Updater arbeiten.

Wenn das TPI-Berechtigungsterminal die Berechtigung auf einem Ausweis aktualisiert und auf dem Ausweis Speicherplatz für die Blocklist vorgesehen ist, dann aktualisiert das TPI-Berechtigungsterminal zusätzlich auch die Blocklist auf dem Ausweis. Falls der Speicherplatz auf dem Ausweis nicht für die gesamte Blocklist ausreicht, dann werden die Blocklisteinträge für den Ausweis vom Anfang der Blocklist genommen.

Bei einem Zutritt an einem Offlineterminal kann das Offlineterminal die Blocklisteinträge von dem Ausweis lesen und in seinen internen Blocklistspeicher übernehmen. Es sei darauf hingewiesen dass es passieren kann, dass das Offlineterminal wegen eines vollen Blocklistspeichers Blocklisteinträge nicht übernimmt.

Bei jedem Zutrittsversuch prüft das Offlineterminal anhand seiner internen Blocklist, ob der verwendete Ausweis gesperrt ist und lehnt ggf. den Zutritt ab.

Jeder Blocklisteintrag enthält einen Ablaufzeitpunkt. Wenn der Ablaufzeitpunkt erreicht ist, kann das Offlineterminal den Blocklisteintrag selbstständig aus seiner internen Blocklist entfernen und den vorher von dem Blocklisteintrag belegten Speicher freigeben. Der Ablaufzeitpunkt sollte normalerweise so gewählt werden, dass er nicht vor dem Gültigkeitsende der auf dem Ausweis stehenden Berechtigungen liegt.

Grundeinstellungen

Verwaltungseinheit

Siehe 4.5.1.

Blocklist

Die Blocklist kann maximal 255 Blocklisteinträge haben.

Die Blocklisteinträge werden in einer Tabelle dargestellt.

Mit dem Button „Anfügen“ kann ein Blocklisteintrag am Ende der Blocklist angefügt werden.

Mit dem Button „Einfügen“ kann ein Blocklisteintrag an einer ausgewählten Position in die Blocklist eingefügt werden.

Mit dem Button „Löschen“ kann ein ausgewählter Blocklisteintrag aus der Blocklist entfernt werden.

Mit den Buttons „Nach oben“ und „Nach unten“ kann die Reihenfolge von Blocklisteinträgen geändert werden.

Eintrag – No.

Diese Nummer gibt die Position des Blocklisteintrags an. Wenn die Blocklist mehr Einträge hat, als auf den Ausweis passen, werden die Einträge mit den niedrigsten Nummern auf den Ausweis übernommen.

Die Position von Blocklisteinträgen kann über die Buttons „Nach oben“ und „Nach unten“ verändert werden.

Credential-ID – Firmenkennung und Ausweisnummer

Gemäß dem OSS Standard Offline werden Ausweise über ihre jeweilige Credential-ID identifiziert.

PCS unterteilt die Credential-ID in die beiden gleich großen Teifelder Firmenkennung und Ausweisnummer.

PCS hat als Standard vorgesehen, dass auf dem Ausweis die Teifelder Firmenkennung und Ausweisnummer jeweils als gepackte BCD-Zahl mit 10 Ziffern kodiert werden. In diesem Fall sind Firmenkennung und Ausweisnummer in der Blocklist dezimal anzugeben.

Um auch mit anderen Kodierungen umgehen zu können, können in der Blocklist für Firmenkennung und Ausweisnummer auch hexadezimale Werte angegeben werden..

Ablaufdatum – Datum und Uhrzeit

Hier wird der Zeitpunkt angegeben, ab dem die Offlineterminals den Blocklisteintrag aus ihrer internen Blocklist löschen können.

Der Zeitpunkt sollte so gewählt werden, dass dann die auf dem Ausweis vorhandene Berechtigung abgelaufen ist. (Wenn die Berechtigung abgelaufen ist, dann ist mit dem Ausweis auch ohne Blocklisteintrag der Zutritt nicht mehr möglich.)

Der Zeitpunkt sollte aber auch nicht unverhältnismäßig weit in der Zukunft liegen, da sonst die Gefahr steigt, dass für neue Blocklisteinträge kein Speicherplatz in den Offlineterminals vorhanden ist.

5 Fehlersuche und Fehlerbehebung

INTUS COM bietet eine Reihe von Möglichkeiten, auftretende Probleme zu analysieren und zu beheben. Sollte ein Problem auftreten, versuchen Sie bitte anhand der in diesem Kapitel aufgeführten Hinweise, die Ursache zu klären.

Wenn Sie den Fehler auch mit den Hinweisen in diesem Kapitel nicht beheben konnten, wenden Sie sich bitte per Email an intuscom@pcs.de oder an die Service-Hotline 089/68004-666. Bitte geben Sie eine möglichst detaillierte Fehlerbeschreibung. Bitte packen Sie folgende Dateien (im zip-Format) und senden Sie sie in Ihrer Mail mit: die Log-Datei des Terminal-Handlers (Aufzeichnung des Fehlers auf Messagelevel 5), die Datei conf/admin_server.ini und die Parameter-Dateien `work*` der betroffenen Terminals.

Wenn der Verbindungsstatus keine Verbindung zu einer Komponente anzeigt (siehe 3.2.3), lesen Sie in 5.1 nach.

Wenn der Betriebsstatusstatus einer Komponente einen Fehler anzeigt (siehe 3.2.3), lesen Sie in 5.2 nach.

Wenn der Fehler nicht mit dem INTUS COM Client gefunden werden kann, sehen Sie in den [Log-Dateien](#) nach.

Wenn die Informationen in der Log-Datei unzureichend sind, erhöhen Sie den [Messagelevel](#) der Komponente und reproduzieren Sie den Fehler.

5.1 Verbindungsfehler

Verbindungsfehler erkennen Sie daran, dass im Komponentenbaum der Verbindungsstatus (linker Teil im Status-Icon) einer Komponente **rot** angezeigt wird, siehe 3.2.3. Die Fehlermeldung sehen Sie entweder

- im Fehler-Fenster,
- im K&S-Fenster,
- im Meldungs-Fenster oder
- in der Log-Datei der übergeordneten Serverkomponente (bei Verbindungsfehler zum Terminal in der Datei `tcp_server.log`)

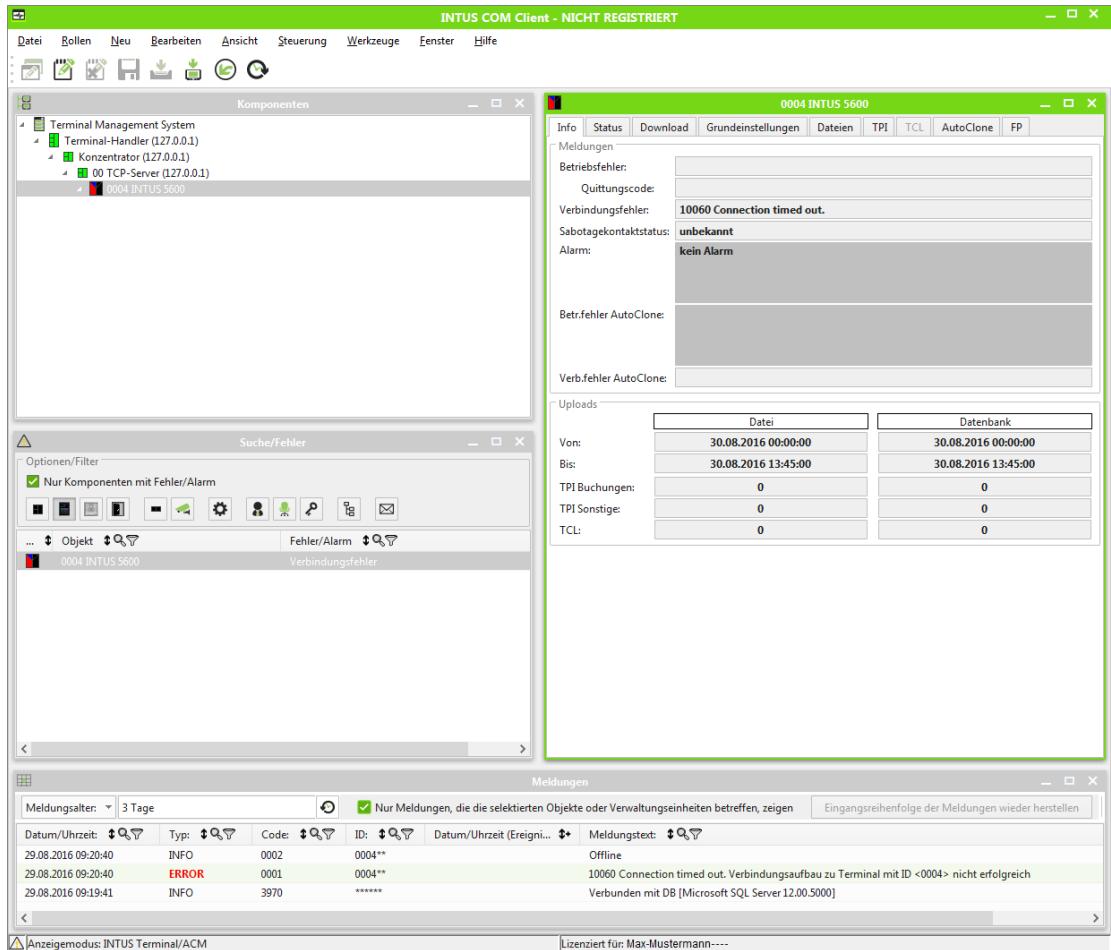


Abbildung 5.1 – Verbindungsfehler

Wie Sie einen Verbindungsfehler bei der Anmeldung im INTUS COM Client beheben, ist in Kapitel 2.4.2 beschrieben.

5.1.1 Allgemeine TCP/IP Verbindungsfehler

Die INTUS COM Server kommunizieren untereinander und mit den Terminals über das standardisierte TCP/IP Protokoll. Das TCP/IP Protokoll kennt folgende allgemeine Verbindungsfehler:

Fehlermeldung	Fehlerursache	Fehlerbehebung
Host not found	Der angegebenen DNS-Name einer Komponente ist dem DNS-Server nicht bekannt.	DNS-Name überprüfen und korrigieren.
No route to host	Die angegebene IP-Adresse ist dem Gateway / Router nicht bekannt	IP-Adresse überprüfen und korrigieren.
Connection timed out	Die angesprochene Komponente ist nicht vorhanden / eingeschaltet	<ul style="list-style-type: none"> • Terminal einschalten • IP-Adresse überprüfen • Kabel überprüfen
Connection refused	Die angesprochene Komponente lässt auf dem angegebenen Port keine Verbindung zu. 1. IP-Adresse fehlerhaft 2. Portnummer fehlerhaft 3. Port wird von einer anderen Applikation bereits belegt 4. die Verbindungseinstellung des Terminals ist active 5. Das Terminal ist nicht für TCP/IP Verbindungen eingestellt	1. IP-Adresse überprüfen und korrigieren. 2. Portnummer überprüfen und korrigieren. 3. Prüfen ob Verbindungsstatus auf Terminalstatusseite „online“. Andere Applikation beenden. 4. Verbindungseinstellung des Terminals auf passive setzen, siehe 3.4.11 und 0 5. Terminal Parameter „Prozedur“ für den Kanal A auf TCP/IP setzen.
Reset by peer	1. Kabelproblem 2. Router-Problem	1. Kabel überprüfen 2. Router-Konfiguration überprüfen

Tabelle 5.1 – Allgemeine TCP/IP Verbindungsfehler

5.1.2 Verbindungsfehler in INTUS COM

Fehler	Fehlerbehebung
Verbindungsfehler zum Serviceport einer Serverkomponente (z.B.: TCP-Server).	<p>Stellen Sie sicher, dass die Komponente überhaupt läuft.</p> <p>Stellen Sie sicher, dass der konfigurierte Hostname (oder die IP) richtig ist. Die Port-Nummer wird sowohl von der Komponente, als auch vom Admin-Server gespeichert. Beide Werte müssen übereinstimmen. Wenn Sie die Port-Nummer über den INTUS COM Client geändert haben, während die Komponente nicht mit dem Admin-Server verbunden war, gehen Sie noch einmal auf den alten Port zurück.</p> <p>Prüfen Sie, ob der Port bereits von einem anderen Programm verwendet wird.</p>
Verbindungsfehler zum Datenport einer Serverkomponente (z.B.: TCP-Server)	<p>Stellen Sie sicher, dass beide an der Verbindung beteiligten Komponenten (Client und Server) den Betriebsstatus bereit (grün) haben.</p> <p>Prüfen Sie, ob der Port bereits von einem anderen Programm verwendet wird.</p> <p>Bleibt der Verbindungsstatus blau, prüfen Sie, ob beim Terminal-Handler Parameter „Verbindungseinstellung / zum Konzentrator:“ „immer“ eingestellt ist.</p>
Verbindungsfehler zu einem Terminal, das über den TCP-Server angeschlossen ist	<p>Prüfen Sie, ob der TCP-Server im Betriebsstatus bereit (grün) ist.</p> <p>Stellen Sie sicher, dass das Terminal läuft.</p> <p>Stellen Sie sicher, dass der konfigurierte Hostname (oder die IP) richtig ist (Host not found ausschließen).</p> <p>Stellen Sie sicher, dass der konfigurierte Port mit dem im Terminal-Setup eingestellten Port übereinstimmt.</p> <p>Jedes Terminal erlaubt nur eine einzige Verbindung zu seinem Datenport. Prüfen Sie, dass kein anderes Programm den Port blockiert.</p> <p>Testen Sie die Verbindung, wie in 4.3.1 beschrieben.</p> <p>Wird die Verschlüsselung eingesetzt (siehe 4.2), stellen Sie sicher, dass auf dem Terminal und dem verwendeten TCP-Server der selbe Schlüssel verwendet wird.</p> <p>Wird eine Verbindung zwar aufgebaut, aber nach wenigen Sekunden wieder abgebrochen, verwenden Sie möglicherweise ein älteres Terminal das eine 10BaseT Verbindung benötigt. Deaktivieren Sie "Auto negotiation" im Router und stellen die Verbindung auf 10BaseT fest ein.</p> <p>Bleibt der Verbindungsstatus blau, prüfen Sie, ob beim Terminal-Handler Parameter „Verbindungseinstellung / zum Konzentrator:“ „immer“ eingestellt ist.</p>

5.2 Betriebsfehler

Bei einem Betriebsfehler (fehlerhafte Parametrierung eines Terminals) wird der Betriebsstatus einer Komponente (rechter Teil in dem Status-Icon) **rot** angezeigt, siehe 3.2.3. Die dazugehörige Fehlermeldung sehen Sie

- im Fehler-Fenster,
- im K&S-Fenster,
- im Meldungs-Fenster oder
- in der Log-Datei der übergeordneten Serverkomponente (bei Verbindungsfehler zum Terminal in der Datei `tcp_server.log` siehe 5.1)

5.2.1 Betriebsfehler einer Serverkomponente

In der Statusanzeige finden Sie das Serviceport-Kommando bei dem der Fehler aufgetreten ist. Wenn der Fehler beim Setzen eines Konfigurationsparameters aufgetreten ist, sollten Sie die Konfiguration entsprechend ändern. Solange der Fehlerzustand angezeigt wird, findet keine Kommunikation mit dem Serviceport statt. Es ist notwendig, dass Sie den Serviceport neu verbinden (im Menü unter **Steuerung**). Erst dann wird der Fehler zurückgesetzt.

5.2.2 Betriebsfehler eines Terminals

Im Terminalstatus können Sie erkennen, ob der Fehler während des Downloads oder erst nachdem das Terminal betriebsbereit (d. h. vollständig geladen) war, aufgetreten ist. Im Falle des Downloads wird die Fehlerursache über die Download-Nummer (70-77) weiter eingegrenzt. Folgende Fehler können auftreten:

Fehler	Fehlerbehebung
Fehler beim Öffnen der Datei	Der Terminal-Handler konnte die Datei nicht öffnen. Stellen Sie in der Konfiguration des Terminal-Handlers das Verzeichnis richtig ein. Stellen Sie in der Konfiguration des Terminals die Datei (ggf. mit Unterverzeichnissen) relativ zu dem beim Terminal-Handler konfigurierten Verzeichnis richtig ein. Starten Sie den Download manuell (Menü Steuerung).
Fehler beim Prüfen des Terminal-Setup	Wenn der Terminal-Handler die Speicheraufteilung eines Terminals einstellt, prüft er den Gesamtspeicher des Terminals. Wenn er Baudrate und Datenformat einer seriellen Schnittstelle einstellt, prüft er, dass als Protokoll TTY eingestellt ist. In der Meldungsanzeige oder in der Log-Datei können Sie nähere Informationen zu dem Fehler finden. Ändern Sie ggf. den im INTUS COM konfigurierten Wert für den SRAM des Terminals bzw. stellen Sie im Terminal-Setup für die entsprechende Schnittstelle TTY ein. (Leider kann diese Einstellung nicht von INTUS COM vorgenommen werden.) Führen Sie einen Reset des Terminals durch.
DE	Der Fehler DE wird vom Terminal gesendet, wenn das TCL-Programm nicht in das DL-Feld passt. Ändern Sie die Speicheraufteilung im Terminal-Setup und führen Sie einen Neustart durch. Bei TCL-Terminals (ohne TPI-tasc) kann alternativ dazu die Speicheraufteilung in INTUS COM konfiguriert werden. Diese wird dann vor jedem TCL Programm-Download (77) überprüft und ggf. eingestellt.
MONIN	Dieser Fehler wird vom Terminal gesendet. Er bedeutet, dass das Terminal einen ungültigen Datensatz empfangen hat. Überprüfen Sie den Inhalt der entsprechenden Downloaddatei bzw. die von der Applikation gesendeten Datensätze. Um nähere Informationen zu erhalten, erhöhen Sie den Messagelevel (z. B. Messagelevel des Terminal-Handlers auf 5 setzen) und reproduzieren Sie den Fehler. Dann sehen Sie in der Log-Datei die gesendeten und empfangenen Datensätze. Führen Sie nach Behebung des Fehlers am besten einen Kaltstart oder Neustart des Terminals durch.
INTERP	Dieser Fehler wird vom Terminal gesendet, wenn bei der Abarbeitung des TCL-Programms ein Fehler auftritt. Zur Behebung des Fehlers verfahren Sie ähnlich wie bei einem MONIN-Fehler. Zum Debuggen des TCL-Programms kann auch der Menüpunkt Dialog mit Terminal (im Menü Steuerung) verwendet werden. Wird TPI-tasc als TCL-Programm eingesetzt, liegt die Fehlerursache möglicherweise darin, dass die geladenen Parameterdateien für eine neuere Version von TPI-tasc erstellt wurden.

Negative Quittung(en) empfangen	Das Terminal sendet negative Quittungen, wenn es einen TPI-Satz nicht verarbeiten kann. Verfahren Sie ähnlich wie bei MONIN-Fehlern.
Keine Quittung bei gesichertem Download	Prüfen Sie (z. B. über den Dialog mit Terminal im Menü Steuerung), ob das Terminal überhaupt reagiert. Es könnte ein Verbindungsproblem vorliegen, das auf TCP/IP-Ebene noch nicht erkannt ist. Stellen Sie sicher, dass TPI-tasc komplett geladen ist. Verfahren Sie ansonsten ähnlich wie bei MONIN-Fehlern.
Der SK2 Satz ist inkonsistent zur INTUS COM Konfiguration	Sie haben im SK2-Satz andere Subterminals parametriert, als in INTUS COM konfiguriert sind. Ändern Sie die inkorrekte Einstellung. Beachten Sie, dass in INTUS COM deaktivierte Subterminals als nicht vorhanden angesehen werden. Starten Sie anschließend den Download 72 manuell (Menü Steuerung).
SK2 Satz kann nicht erzeugt werden	Sie haben in INTUS COM Subterminals konfiguriert. Diese sind jedoch nicht im SK2-Satz eingetragen. Der Terminal-Handler versucht deshalb, die Subterminals beim Download in den SK2-Satz einzutragen. Dazu benötigt er jedoch die numerische Terminalgruppe jedes Subterminals. Er versucht die Terminalgruppe jeweils aus der Parameterdatei des Subterminals zu ermitteln. Es könnte sein, dass für ein Subterminal keine Parameterdatei konfiguriert ist oder die Datei nicht geöffnet werden kann oder der Inhalt der Datei fehlerhaft ist. Sehen Sie in der Meldungsanzeige nach, ob ein Fehler beim Öffnen einer Datei aufgetreten ist. Starten Sie nach Behebung der Fehlerursache den Download 72 manuell (Menü Steuerung).
Datenbank nicht verbunden	Stellen Sie sicher, dass die Datenbank läuft und der Registry-Eintrag bzw. die Umgebungsvariable DSN korrekt ist. Starten Sie den Download danach manuell (Menü Steuerung).

5.2.3 Buchungssatzverlust

- Messagelevel des Terminal-Handlers auf 5 setzen und Log-Dateien auswerten.
- Zwei konkurrierende INTUS COM Installationen. Symptome:
 1. Terminal ist nach einem Reset offline (connection refused).
 2. Der Terminal Statuswert „Recv. not connect“ ist > „10“

5.2.4 Email-Benachrichtigung

Wenn der Admin-Server keine Emails versendet und die Fehlermeldung

`<smtp-server>: <[IP-Adresse], [Port]>: Funktion <connect> nicht erfolgreich
(in ClientManager::testSocketSet) : WSA Error 10061: Connection refused.`

in der Log-Datei des Admin-Server erscheint, kann es daran liegen, dass der Verbindungsversuch von INTUS COM auf Port 25 durch eine Firewall oder einen Virenschanner geblockt wird.

Um diesen Fehler zu vermeiden, muss sichergestellt sein, dass der eingestellte SMTP-Port (Standard Portnummer 25) für INTUS COM nicht durch eine Firewall oder einen Virenschanner blockiert ist.

5.3 Log-Dateien

Jeder INTUS COM Server protokolliert bestimmte Ereignisse in Abhängigkeit vom eingestellten [Messagelevel](#). Die Log-Dateien finden Sie im Unterverzeichnis `log` Ihrer INTUS COM Installation.

Eine Log-Datei ist eine Datei in einem Text-Format und kann in einem normalen Texteditor angezeigt werden. Eine Zeile enthält mehrere Felder die durch Semikolon getrennt sind.

1. Datum/Uhrzeit (yyyy-MM-dd HH:mm:ss)
2. Meldungstyp
3. Meldungscode
4. Server-ID +Terminal-ID
5. Prozess-ID
6. Kommunikationsrichtung
7. IP-Adresse, Port
8. Meldungstext

Der Meldungstyp kann folgende Werte annehmen:

- FATAL – fataler Fehler, der zum Programmabbruch führt
- ERROR – es ist ein Fehler aufgetreten, der behoben werden sollte
- WARN – Warnung, es ist ein ungewöhnliches Ereignis eingetreten
- INFO – die Meldung bezieht sich auf ein gewöhnliches Ereignis im Programm
- DEBUG – die Meldung dient nur der Fehlersuche

5.4 Sonstige Probleme

5.4.1 Passwort vergessen

Der Benutzer **admin** kann das Passwort eines anderen Benutzers auf einen neuen Wert setzen.

Wenn das Passwort für den Benutzer **admin** vergessen wurde, gehen Sie folgendermaßen vor:

1. Beenden Sie den Admin-Server.
2. Öffnen Sie die Datei **admin_server.ini** mit einem Texteditor.
3. Suchen Sie die Zeile **login-name=admin**. Die Sektion, in der diese Zeile steht, enthält auch das Passwort für den Benutzer **admin**.
4. Löschen Sie in derselben Sektion die Zeile **pass=...**. Dann wird für den Benutzer **admin** wieder das Defaultpasswort verwendet.
5. Starten Sie den Admin-Server und den INTUS COM Client.
6. Melden Sie sich mit dem Namen **admin** und dem Default-Passwort **pcs** an.
7. Ändern Sie Ihr Passwort.

6 INTUS COM Applikationsschnittstellen

INTUS COM stellt drei Schnittstellen zur Applikation zur Verfügung, die teilweise auch kombiniert eingesetzt werden können:

- TCP/IP Socket-Schnittstelle

Die TCP/IP Socket-Schnittstelle ist die flexible, effiziente, onlinefähige Schnittstelle zur Kommunikation zwischen Applikation und Terminals.

- Dateischnittstelle

Bei der Dateischnittstelle erfolgt der Datenaustausch zwischen Applikation und Terminals über Sende- und Empfangsdateien. Sie ist für Online-Verbindungen zwischen Applikation und Terminals nicht geeignet.

- Datenbankschnittstelle

Bei der Datenbankschnittstelle erfolgt der Datenaustausch zwischen Applikation und Terminals über (vordefinierte) Tabellen in einer ODBC-Datenbank. In den Terminals muss TPI ab 2.0 eingesetzt werden.

Empfehlungen für Einsatzszenarien

Die drei Schnittstellenvarianten können entweder einzeln oder auch kombiniert für Up- und Download eingesetzt werden. Folgende Kombinationen sind zu empfehlen:

- Statische Datei-Schnittstelle für Download und dynamische für Upload

Dies ist der einfachste Fall, für Zutrittskontrolle gut geeignet. Keine Online-Verarbeitung möglich. Für Zutrittskontrolle mit Profilen nur bedingt zu empfehlen.

- Statische Datei-Schnittstelle für Download und Socket-Schnittstelle für Upload

Hier ist auch Online-Verarbeitung (z.B. Salden- oder BDE-Rückmeldung) möglich.

- Datenbank-Schnittstelle für Up- und Download

Diese Schnittstelle ist mit dem geringsten Programmieraufwand realisierbar, wenn von vorneherein eine unterstützte Datenbank und TPI zum Einsatz kommt. Sie ist auch bei Zutrittskontrolle mit Profilen zu empfehlen. Keine Online-Verarbeitung möglich.

- Datenbank-Schnittstelle für Up- und Download, Socket-Schnittstelle für Online-Anfragen

Kombiniert Datenbank mit Online-Verarbeitung

6.1 Dateischnittstelle

Die Dateischnittstelle von INTUS COM bietet eine besonders einfache Möglichkeit, Daten zwischen Rechnerapplikation und Terminal auszutauschen – über Textdateien.

Für die Dateischnittstelle in INTUS COM wird der Terminal-Handler (TH) benötigt. Die Dateien müssen in dem Arbeitsverzeichnis (oder Unterverzeichnis) des Terminal-Handlers liegen. Dieses Verzeichnis wird im Konfigurationsdialog des Terminal-Handlers eingestellt.

Damit ein INTUS-Terminal sinnvoll eingesetzt werden kann, muss es mit verschiedenen Daten geladen werden. Beispiele hierfür sind das TCL-Programm, eine TPI-Parametrierung sowie Stammdaten.

Auf der anderen Seite erzeugt das Terminal auch Daten, z. B. Buchungen, die von einer Applikation verarbeitet werden sollen.



Die Dateien **upload.dat** und **download.dat** im Arbeitsverzeichnis des Terminal-Handlers haben eine spezielle Funktion (siehe 6.1.2) und dürfen nicht für andere Zwecke verwendet werden. Alle Dateien in diesem Verzeichnis, die mit dem Präfix **th_** beginnen, sind für interne Zwecke reserviert. Das Löschen solcher Dateien kann zu Datenverlust führen. Dateien, die auf **.th** enden haben ebenfalls eine spezielle Bedeutung (siehe 6.1.1.2).

Die Dateischnittstelle besteht aus zwei Teilen:

- der **Statischen Dateischnittstelle**

Die statische Dateischnittstelle dient dem Download der Betriebsdaten (Stammsätze, Profile, usw.) in die Terminals. Die Datensätze werden von der Applikation in separaten Dateien, den "statischen Downloaddateien" bereitgestellt. Ihr Inhalt ist über längere Zeit gültig und sie bleiben erhalten, nachdem sie ans Terminal gesendet wurden. So können sie bei Bedarf (z.B. nach Terminalausfall) vom Terminal-Handler automatisch wieder in das Terminal geladen werden. Wenn sich eine Datei geändert hat, erkennt dies der Terminal-Handler und sendet sie automatisch an alle Terminals, die dieser Datei zugeordnet sind.

- der **Dynamischen Dateischnittstelle**

Die dynamische Dateischnittstelle ermöglicht sowohl den Download als auch den Upload von Datensätzen. Die Datensätze werden in dieser Schnittstelle jeweils von der einen Seite bereitgestellt und von der anderen übernommen. Es werden im laufenden Betrieb immer wieder neue Datensätze in diese Schnittstelle gestellt, übernommene Datensätze werden aus der Schnittstelle gelöscht. Deswegen heißt diese Schnittstelle dynamisch.



Verwenden Sie die statische Dateischnittstelle zum Laden der Daten in die Terminals und die dynamische Dateischnittstelle zum Verarbeiten der Datensätze von den Terminals.

6.1.1 Die statische Dateischnittstelle

Die statische Dateischnittstelle wird **nur für den Download** in die Terminals verwendet.

Statischen Downloaddateien sind ASCII-Textdateien, die pro Zeile einen Datensatz enthalten. Sie werden satzweise vom Terminal-Handler an die im INTUS COM Client zugeordneten Terminals gesendet. Es gibt folgende statische Downloaddateien:

Inhalt der Datei	TPI Ladeanforderung
TCL-Programm (TCL-Terminal)	77
TPI-Systemkonfiguration	72
Kartendaten	69
TPI-Parameter	73
Funktionsschrittwerte	70
Sondertage	71
Profile	74
Berechtigungsgruppen	75
Stammdaten	76

Tabelle 6.1 – Statische Downloaddateien; TPI-Ladeanforderungen

Betriebsdatendateien

Die Dateien "Kartendaten", "Funktionsschrittwerte", "Sondertage", "Stammdaten", "Profile" und "Berechtigungsgruppen" sind Betriebsdaten, die von der Applikation zur Verfügung gestellt werden und regelmäßig aktualisiert werden müssen.

6.1.1.1 Download

Für jedes Terminal kann einzeln konfiguriert werden, welche Dateien für den statischen Download verwendet werden sollen (siehe 4.13.3). Die Terminals können unterschiedliche Dateien verwenden, es können aber auch mehrere Terminals dieselbe Datei verwenden. Bei der Konfiguration der Dateien sind folgende Einschränkungen zu beachten:

- Der Pfad der Dateien muss relativ zum TH-Arbeitsverzeichnis angegeben werden.
- Es dürfen keine Sonderzeichen oder Leerzeichen in den Dateinamen vorkommen.
- Die Dateinamen dürfen nicht auf „.th“ enden

Der Download wird entweder

- manuell im INTUS COM Client gestartet (siehe 3.4.2)
- durch Ladeanforderung vom Terminal ausgelöst (nur TPI-Terminals; siehe 6.1.1.4)
- durch Änderung (Aktualisierung) der Datei ausgelöst (siehe 6.1.1.2)

Nur TPI-Terminals generieren Ladeanforderungen ungleich "77". Für den Einsatz von INTUS Terminals ohne TPI mit INTUS COM finden Sie nähere Hinweise im Abschnitt 7.1 .

Bei Änderung (Aktualisierung) der Dateien 69 bis 71 und 73 bis 76 wird automatisch ein Download gestartet. Wenn das Terminal nicht bereit ist, wird vorher gewartet und der Download verzögert gestartet. Beim Parameterdownload (73) reicht die Aktualisierung einer der Parameterdateien (Subterminals können eigene Parameterdateien besitzen) um den Download zu starten.

Bei Aktualisierung der Dateien 72 oder 77 wird kein automatischer Download gestartet, da dies leicht zu Datenverlust auf dem Terminal führen könnte (denn es könnte ein Kaltstart erfolgen).



6.1.1.2 Dateiübergabe zwischen Applikation und INTUS COM

Damit die statischen Downloaddateien im laufenden Betrieb durch die Applikation aktualisiert werden können, gibt es zu jeder statischen Downloaddatei eine Übergabedatei. Übergabedateien haben die zusätzliche Endung `.th` (z. B. ist `76.tpi.th` die Übergabedatei zu `76.tpi`).

Der Übergabemechanismus funktioniert folgendermaßen:

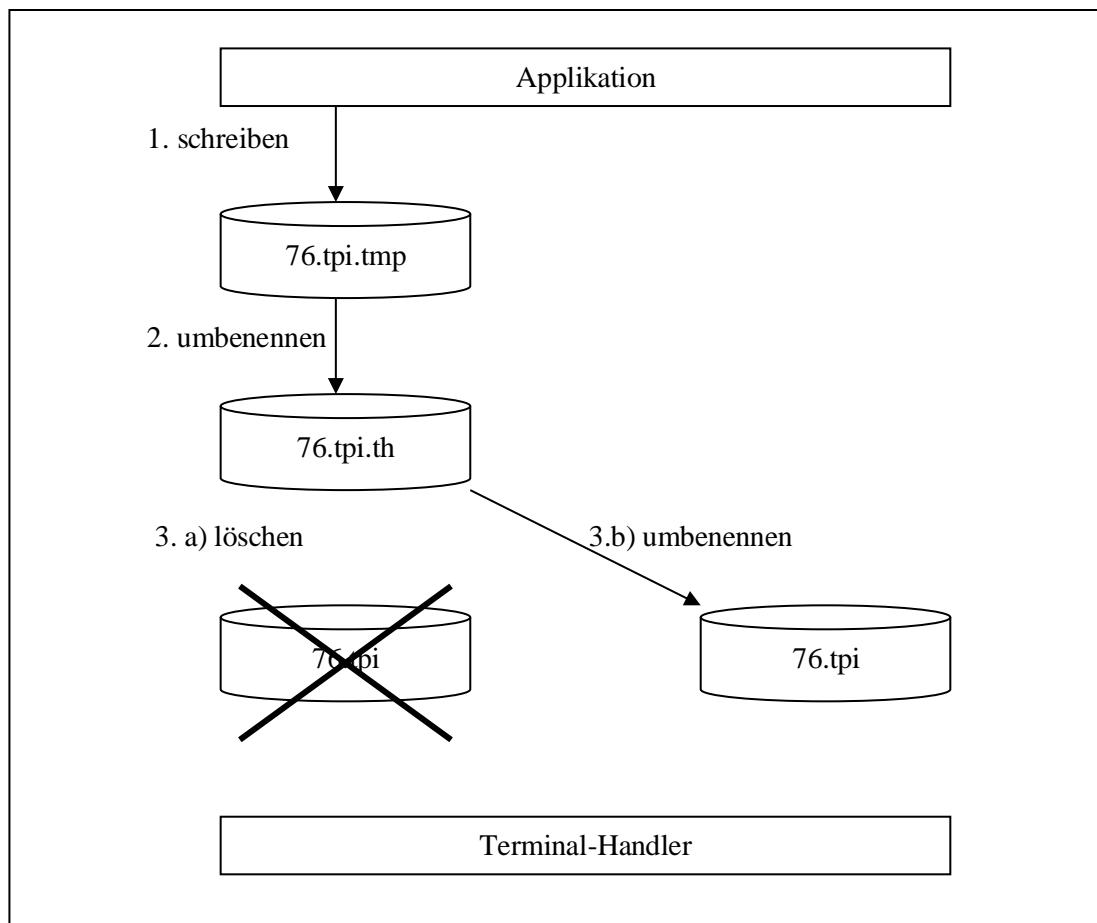


Abbildung 6.1 – Übergabemechanismus der statischen Dateischnittstelle

1. Die Applikation schreibt die neuen Daten in eine temporäre Datei (z. B. „76.tpi.tmp“).
2. Die Applikation erzeugt durch Umbenennen dieser temporären Datei die Übergabedatei (z. B. „76.tpi.th“). Davor muss die Applikation ggf. warten, bis die Übergabedatei nicht mehr existiert. Die Übergabedatei darf nicht nachträglich von der Applikation verändert oder gelöscht werden.
3. Der Terminal-Handler löscht die Downloaddatei und benennt die Übergabedatei in die Downloaddatei (z. B. „76.tpi“) um. Dabei stellt er sicher, dass das Löschen und Umbenennen mit laufenden Downloads synchronisiert wird. Ggf. wartet er, bis ein laufender Download beendet ist.

Der Terminal-Handler prüft regelmäßig, ob Übergabedateien vorhanden sind. Das Zeitintervall für das Prüfen der Dateischnittstelle durch den Terminal-Handler kann konfiguriert werden.

6.1.1.3 Satzformat

Bei der Verwendung der statischen Dateischnittstelle werden die Datensätze ohne Terminaladressen (Nettodatensätze; siehe 6.3.2.1) in die Dateien geschrieben. Der Terminal-Handler erhält die Adressen der zu ladenden Terminals über die Zuordnung der Dateien in der Terminalkonfiguration.

Neben Datensätzen für das Terminal kann eine Datei auch Kommentarzeilen enthalten. Diese beginnen mit einem * und werden vom Terminal-Handler herausgefiltert.

TPI-Datensätze

Die Satznummer eines TPI-Satzes muss in der Downloaddatei immer mit **** belegt sein, bei gesicherten Download wird die Satznummer immer vom Terminal-Handler mit der laufenden Satznummer überschrieben.

6.1.1.4 Ladeanforderungen

Der Download der statischen Downloaddateien kann auch durch Ladeanforderung vom Terminal ausgelöst werden.

Anforderungssätze, für deren Bearbeitung der Terminal-Handler nicht konfiguriert ist, werden an die Applikationsschnittstelle geschickt (soweit sie nicht gefiltert werden).

TCL-Terminals

Die Ladeanforderung 77 senden alle TCL-basierten Terminals. Die Datei, die der Ladeanforderung 77 zugeordnet ist, enthält das TCL-Programm.



Bestehende TCL-Programme können so erweitert werden, dass sie auch die anderen Ladeanforderungen unterstützen (siehe 7.1)

TPI-Terminals

TPI-Terminals (INTUS 3000 mit TPI-tasc) unterstützen auch die anderen Ladeanforderungen. Die anderen Dateien enthalten TPI-Sätze bzw. (wenn kein TPI zum Einsatz kommt) sonstige terminalprogrammabhängige Sätze.

TPI Parameterdateien für Subterminals

Es gibt keine eigene Ladeanforderung für Parameterdateien von Subterminals. Sie werden auf die Ladeanforderung 73 immer zusammen mit der Parameterdatei des Hauptterminals geladen. Wenn eine Parameterdatei bei mehreren Subterminals angegeben ist, wird sie nur einmal ans Terminal gesendet (Konzept der Terminalgruppe im TPI).

6.1.2 Die dynamische Dateischnittstelle

Die dynamische Dateischnittstelle dient in erster Linie dem Upload von Buchungen. Sie kann aber darüber hinaus in Sonderfällen auch für den Download eingesetzt werden, z. B. zum Löschen oder Aktualisieren einzelner Stammsätze.

Die dynamische Dateischnittstelle verwendet die ASCII Textdateien `upload.dat` und `download.dat` im Arbeitsverzeichnis des Terminal-Handlers.

6.1.2.1 Upload

Für den Upload stellt der Terminal-Handler die Datei `upload.dat` in der Schnittstelle bereit. Die Applikation übernimmt die darin enthaltenen Daten (liest die Datei ein) und entfernt (löscht) anschließend die Datei aus der Schnittstelle (s.u.).

Welche Satzarten in der Datei `upload.dat` gespeichert werden, ist konfigurierbar (siehe 6.3.2.5)

Gesicherte Datensätze

Gesicherte Datensätze vom Terminal müssen quittiert werden. Wenn die Dateischnittstelle für den Upload verwendet wird, werden sie automatisch vom Terminal-Handler quittiert.

Der Terminal-Handler sorgt dafür, dass Satzverdopplungen vermieden werden. Wenn ein gesicherter Satz empfangen wird, wird verglichen, ob der unmittelbar vorher vom selben Terminal empfangene gesicherte Satz dieselbe Satznummer hatte. Wenn das der Fall ist, wird der Satz nicht noch einmal übergeben. (Eine solche Situation kann vorkommen, wenn das Terminal die Quittung nicht oder nicht rechtzeitig erhalten hat und deswegen den Satz wiederholt.)



Damit dieser Mechanismus funktioniert, muss in den TCL-Terminals im `Setup:TCL:Log.Satznummer:ja` eingestellt sein. Dies kann auch in der INTUS COM Terminal-Konfiguration parametriert werden. TPI-Terminals stellen dies automatisch ein.

Da die Satznummer des letzten gesicherten Satzes nicht persistent gespeichert wird, funktioniert dieser Mechanismus nicht, wenn der Terminal-Handler zwischenzeitlich beendet und neu gestartet wurde. Datenverdopplung ist also nicht hundertprozentig auszuschließen.

6.1.2.2 Download

Für den Download stellt die Applikation die Datei `download.dat` bereit. Der Terminal-Handler übernimmt die Datei und entfernt sie anschließend aus der Schnittstelle.

Die dynamische Dateischnittstelle arbeitet TH-intern als persistenter FIFO-Speicher für jedes Terminal, der die an das Terminal zu sendenden Datensätze enthält. Neue Datensätze werden aus der Dateischnittstelle (d. h. aus der dynamischen Downloaddatei) hinten angefügt, während die, an die Terminals übertragenen Datensätze vom entfernt werden.



Übernommene Datensätze, die keinem Terminal zugeordnet werden können (deren ID unbekannt ist), werden gelöscht

Datensätze aus der dynamischen Downloaddatei werden erst gesendet, nachdem das Terminal betriebsbereit ist. Die statischen Downloaddateien haben Vorrang. Die Verwendung der dynamischen Downloaddatei für die Grundversorgung der Terminals wird **nicht** empfohlen.

Die Übertragung der Datensätze erfolgt bei TPI-Terminals je nach Konfiguration des Terminals auch gesichert.



Wenn ein Datensatz nach einer bestimmten Zeit nach seiner Übernahme noch nicht übertragen werden konnte, dann werden alle bis dahin übernommenen Datensätze gelöscht, die für das betreffende Terminal bestimmt sind. Dadurch soll verhindert werden, dass zu viele Daten auflaufen, wenn das Terminal offline oder nicht betriebsbereit ist. Die Zeit, nach der die Datensätze gelöscht werden, kann beim Terminal-Handler konfiguriert werden.

6.1.2.3 Dateiübergabe zwischen Terminal-Handler und Applikation

Der Übergabemechanismus ist für Up- und Download symmetrisch. Die Synchronisation erfolgt dadurch, dass die bereitstellende Seite in eine lokale temporäre Datei schreibt und sie in die Übergabedatei umbenennt, sobald diese von der lesenden Seite gelöscht wurde. Dadurch wird verhindert, dass die übernehmende Seite aus der Datei liest und sie löscht, während die bereitstellende Seite noch in die Datei schreibt.

Upload

Die Buchungen werden vom Terminal-Handler in einer temporären Datei `th_output.dat` gesammelt (1). Im konfigurierten Zeitintervall prüft der TH, ob die Datei „`upload.dat`“ noch existiert. Wenn das nicht der Fall ist, dann stellt der Terminal-Handler die Daten durch Umbenennen in die Datei `upload.dat` bereit (2). Treffen weitere Buchungen ein, so werden diese wieder in `th_output.dat` gesammelt. Sie können erst wieder bereitgestellt werden, nachdem die Applikation die alte `upload.dat` eingelesen (3) und gelöscht (4) hat.

 Aus diesem Grund muss die Applikation die Datei `upload.dat` zweimal hintereinander einlesen, um alle aktuellen Buchungsdaten zu erhalten.

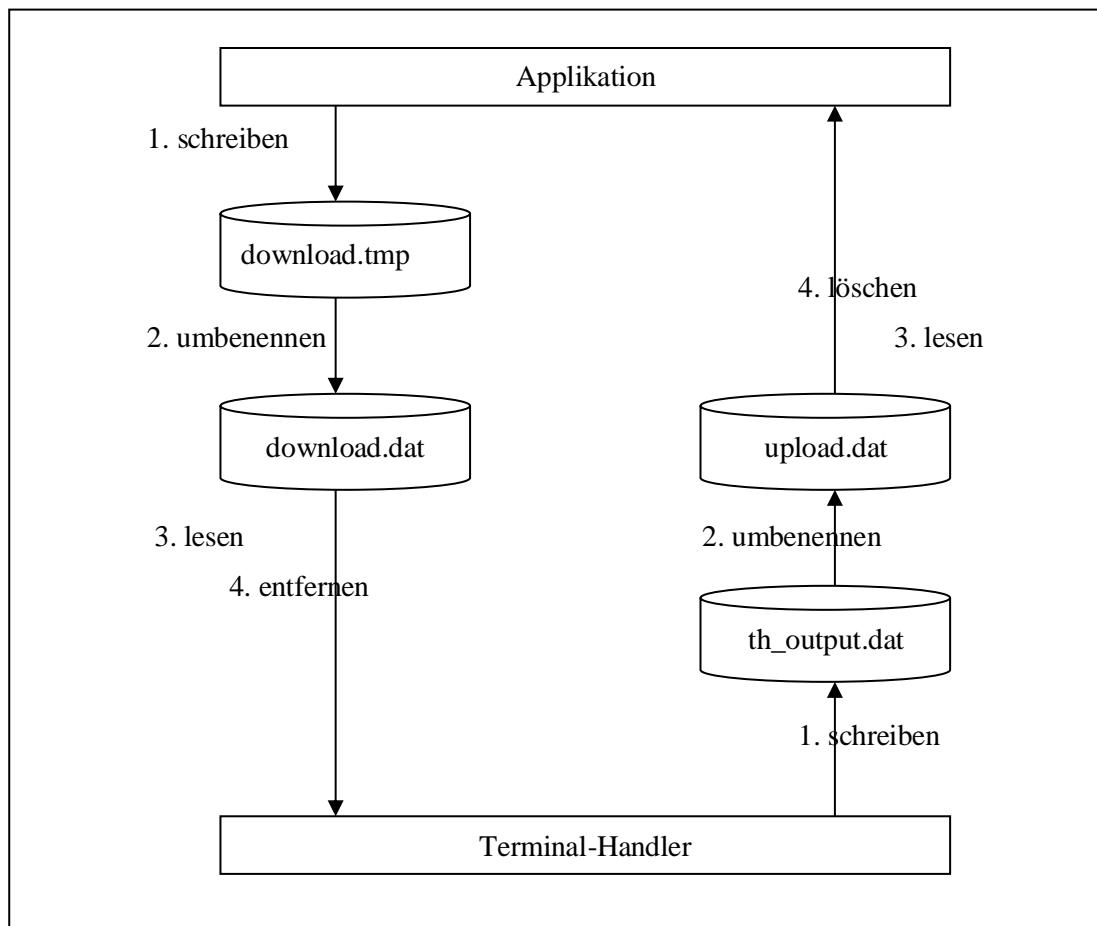


Abbildung 6.2 – Übergabemechanismus der dynamischen Dateischnittstelle

Download

Für den Download wird derselbe Mechanismus verwendet, wie für den Upload. Wenn die Applikation Daten für den dynamischen Download bereitstellen will, muss sie diese zunächst in eine andere Datei (z. B. `download.tmp`) schreiben (1). Anschließend benennt die Applikation diese Datei in `download.dat` um (2). Vor dem Umbenennen muss noch geprüft werden, ob bereits eine `download.dat` existiert. Wenn das der Fall ist, muss vor dem Umbenennen

noch gewartet werden, bis der Terminal-Handler die existierende `download.dat` übernommen und aus der Schnittstelle entfernt hat.

Der Terminal-Handler prüft in regelmäßigen Abständen, ob die Datei `download.dat` existiert. Wenn das der Fall ist, wird die Datei übernommen (3) und entfernt (4). Das Zeitintervall für das Prüfen der Dateischnittstelle durch den Terminal-Handler kann konfiguriert werden.

6.1.2.4 Satzformat

Die Uploaddatei `upload.dat` und die Downloaddatei `download.dat` sind ASCII Textdateien, die pro Zeile einen Datensatz enthalten.

Upload

Alle Datensätze von den Terminals (Nettodatensätze, siehe 6.3) werden vom Terminal-Handler in der Datei `upload.dat` an die Applikation übergeben. Damit die Applikation erkennen kann, von welchem Terminal sie den Satz erhalten hat, werden die Nettodatensätze in einen INTUS COM Frame gepackt, der die Terminaladresse enthält:

<Server-ID><Terminal-ID><Nettodatensatz>[<CR>]<LF>

<Server-ID> = 00..zz wie im INTUS COM Client konfiguriert
<Terminal-ID> = 00..zz, wie im INTUS COM Client konfiguriert

Download

Für den Download stellt die Applikation die Datei `download.dat` bereit. Im Gegensatz zur statischen Datei-Schnittstelle muss jeder Datensatz die Terminaladresse enthalten, damit der Terminal-Handler weiß, an welches Terminal der Satz gesendet werden soll. D.h. die Nettodatensätze (siehe 6.3) müssen von der Applikation in einen INTUS COM-Frame gepackt werden.

Dieser Frame dient ausschließlich der Adressierung der Datensätze innerhalb von INTUS COM. Er wird von den INTUS COM Kommunikationsservern (z.B.: TCP-Server, HTTPS-Server) wieder entfernt, bevor der Nettodatensatz an das Terminal gesendet wird.

6.2 Socket-Schnittstelle

INTUS Terminals und INTUS COM verwenden zur Kommunikation über LAN TCP/IP-Sockets. Dies ist eine genormte Schnittstelle, die auf allen Betriebssystemplattformen verfügbar ist. Informationen und Beispiele zur Programmierung der Socket-Schnittstelle finden Sie z.B. unter www.sockets.com.



Auf der INTUS COM CD im Verzeichnis `\Demo\c-demo` ist eine kleines Beispielprogramm (inkl. Quellcode) in C enthalten, das Buchungssätze von den Terminals entgegennimmt, quittiert und auf `stdout` (Standardausgabe) ausgibt.

Konfiguration des Terminal-Handlers

Bevor die Socket-Schnittstelle durch die Applikation verwendet werden kann, muss der Terminal-Handler entsprechend für Upload und/oder Download konfiguriert werden, siehe 4.8.

6.2.1 Datenport der Socket-Schnittstelle

Die Kommunikation der Applikation mit den Terminals über TCP/IP-Sockets ist sehr einfach. Der Terminal-Handler stellt der Applikation einen Datenport für alle Terminals zur Verfügung (Voreinstellung: 3041, siehe 4.8.1), zu dem die Applikation die Verbindung aufbauen muss. Der Datenaustausch erfolgt dann in beide Richtungen über folgendes Satzformat.

6.2.2 Satzformat

Download

Jeder Datensatz, den die Applikation über die Socket-Schnittstelle sendet, muss die Terminaladresse enthalten, damit INTUS COM weiß, an welches Terminal der Satz gesendet werden soll. Deshalb müssen die Nettodatensätze (siehe 6.3) von der Applikation in einen INTUS COM Frame gepackt werden:

<Server-ID><Terminal-ID><Nettodatensatz><CR>

<Server-ID> = 00..zz wie im INTUS COM Client konfiguriert
<Terminal-ID> = 00..zz, wie im INTUS COM Client konfiguriert

Dieser Frame dient ausschließlich der Adressierung der Datensätze innerhalb von INTUS COM. Er wird von den INTUS COM Kommunikationsservern (z.B.: TCP-Server, HTTPS-Server) wieder entfernt, bevor der Nettodatensatz an das Terminal gesendet wird.

Upload

Alle Datensätze, die die Applikation über die Socket-Schnittstelle empfängt, müssen die Terminaladresse enthalten, damit die Applikation erkennen kann, von welchem Terminal sie den Satz erhalten hat. Deshalb werden alle Nettodatensätze (siehe 6.3) von den INTUS COM Kommunikationsservern (z.B.: TCP-Server, HTTPS-Server) in einen INTUS COM Frame gepackt.

Checksumme (CR)

Die Checksumme wird durch zeichenweise Addition modulo 256 berechnet (z.B. 0x51) und in 2 Bytes ASCII-Hex (0x3531) angehängt. Die Checksumme ist über den gesamten TPI-Datensatz zu bilden. z.B:

0494!**Y00000123456000000000471100*000
13:25 88.00 +1:12 0.03120081219000000--51

6.3 Datensätze in Datei- und Socket-Schnittstelle

6.3.1 Satzformate (Syntax)

Nettodatensätze

Nettodatensätze sind die Datensätze, die **direkt von und zu den Terminals** gesendet werden. Sie enthalten keine Terminaladressen.

INTUS COM Frame

<Server-ID><Terminal-ID><Nettodatensatz><CR>

<Server-ID> = 00..zz wie im INTUS COM Client konfiguriert
<Terminal-ID> = 00..zz, wie im INTUS COM Client konfiguriert

Alle Nettodatensätze, die an die Terminals gesendet werden, müssen in Abhängigkeit der verwendeten Applikationsschnittstelle entweder von der Applikation oder vom Terminal-Handler in einen INTUS COM Frame eingepackt werden:

INTUS COM Applikationsschnittstelle	Instanz
statischer Datei-Schnittstelle (siehe 6.1.1)	durch Terminal-Handler
dynamische Datei-Schnittstelle (siehe 6.1.2)	durch Applikation
Socket-Schnittstelle (siehe 6.2)	durch Applikation

Alle Nettodatensätze die von den Terminals empfangen werden, werden von den INTUS COM Kommunikationsservern (z.B. TCP-Server, HTTPS-Server) in einen INTUS COM Frame gepackt, damit der Terminal-Handler und die Applikation erkennen kann, von welchem Terminal der Satz empfangen wurde.

6.3.2 Satzarten (Semantik)

Es gibt im wesentlichen vier unterschiedliche Satzarten, die von INTUS COM zwischen Applikation und den Terminals übertragen werden.

TPI Datensätze

Der wichtigste Satztyp bei Verwendung von Terminals mit TPI (INTUS 3000/ACM mit TPI-tasc) sind die TPI Datensätze.

Diese sind im TPI Benutzerhandbuch (Bestellnummer D3400-020) in den Kapiteln 4 (Datensätze vom Terminal) und 5 (Datensätze vom Rechner) beschrieben.

TCL Anwendungsdatensätze

Wenn statt TPI-tasc ein anderes TCL Programm in den Terminals eingesetzt wird, dann hängt der Satzaufbau der Anwendungsdatensätze (z.B. Stammdaten, Buchungssätze) von diesem Programm ab.

TCL Betriebssystemmeldungen

Neben den Datensätzen, die durch das eingesetzte TCL Anwendungsprogramm (z.B. TPI-tasc) gesendet werden, kann auch das TCL Betriebssystem der Terminals Datensätze senden.

INTUS COM Statusmeldungen

Die INTUS COM Server erzeugen in bestimmten Situationen Statusmeldungen.

6.3.2.1 Download

(Netto-) Datensätze über Datei- oder Socket-Schnittstelle (Details, siehe TPI Handbuch)

Satzart	Beispiel
TPI Stammdaten	J*****!**Y000001234560000000000000000*00012:00 13:00 14:00 15:00 **
TPI Profile	J*****!00PZ00106001200JJJJJJ0---N-JNNJNNNNNNJNNNNNN**
TPI Sondertage	J*****!**L0011226**
TPI Berechtigungsgruppen	
TPI Funktionsschrittwerthe	J*****!00S1VOR04Viet.-Frühlingsrolle**
TPI Satzquittungen	J*****!00Q 8217B6

(Netto-) Datensätze auch manuell über **Dialog mit Terminal** (siehe 3.4.13)

Satzart	Beispiel	Kommentar
TPI Systemstatus anfordern	J*****!00T5**	
TPI Betriebsstatus anfordern	J*****!00T6**	
TPI Terminalstatus anfordern	J*****!00T7**	
TPI Türstatus anfordern	J*****!00TA**	
TPI Stammsatz Upload	J*****!00Y8***	
TPI Profilsatz Upload	J*****!00P8***	
TPI Online-Antwort: Stille Quittung	J*****R00R0*****	auf Online-Anfragesatz
TPI Online-Antwort: berechtigt	J*****R00R1***berechtigt ***	auf Online-Anfragesatz
TPI Online-Antwort: nicht berechtigt	J*****R00R2***nicht berechtigt ***	
TCL Sende Uhrzeit	ISR,UR:	
TCL positive Satzquittung	Q0001	Satznummer aus Buchungssatz
TCL negative Satzquittung	S	
TCL Warmstart Reset	R	

6.3.2.2 Upload

Satzart	Filter	Beispiel	Kommentar
TPI Statusmeldung betriebsbereit	[<input type="checkbox"/>]	J****!00T 0000A7	
TPI Ladeanforderungsmeldung	[<input type="checkbox"/>]	J****!00T 7400B2	
TPI Satzquittungen	[<input type="checkbox"/>]	J****!00Q 008217**	
TPI Buchungssatz	-	J2498[02Z0014501****000003312009022415415900EE	
TPI Online-Anfragesätze	-		immer über Socket-Schnittstelle
TPI Alarm und Ereignissätze	<input type="checkbox"/>		
TPI Notpuffer-Leer Satz	(<input type="checkbox"/>)		
sonstige ungesicherte Sätze	<input type="checkbox"/>		
INTUS COM Statusmeldungen	<input type="checkbox"/>	0003165FTH00200902181613163400Anforderungs-/Statussatz <77> fuer ID <0003> Datei <"TPITASC\ttasc290.tcl">	Syntax, siehe 6.3.2.3
INTUS COM Offline-Meldungen	<input type="checkbox"/>	0003163F0000200902181612210002offline	Syntax, siehe 6.3.2.3
INTUS COM Online-Meldungen	<input type="checkbox"/>	0003160F0000200902181613160003online	Syntax, siehe 6.3.2.3
TCL Fehlermeldungen	<input type="checkbox"/>	MONIN:401:0007:1146:001:016	Download-Fehler
TCL Fehlermeldungen	<input type="checkbox"/>	INTERP:401:0001:1146:001:016	Programmfehler
TCL Fehlermeldungen	<input type="checkbox"/>	DE	Programmspeicherüberlauf
TCL Trace-Sprungziele	<input type="checkbox"/>		Debug-Meldung

siehe 6.3.2.4

() nur bei Datei-Schnittstelle

[] gefiltert, wenn vom Terminal-Handler verarbeitet

6.3.2.3 Syntax der INTUS COM Meldungsformate für Status-, Fehler- und Alarmmeldungen

Im Datenstrom des INTUS COM werden nicht nur Buchungen sondern auch Status- und Fehlermeldungen in Richtung Applikation übertragen. INTUS COM definiert drei Formate (Meldungsformat 1, 2 und ein Kurzformat) für Statusmeldungen. Das Meldungsformat 0 wird ab Version 3.3 nicht mehr verwendet.

Meldungsformat '1' und '2'

Offset	Länge	Bezeichnung	Erläuterung
0	2	Server-ID	Server-ID der Komponente, auf die sich die Meldung bezieht, oder '***' für alle Server-IDs, oder zwei Leerzeichen, wenn die Komponente keine Server-ID hat.
2	2	Terminal-ID	Terminal-ID der Komponente, auf die sich die Meldung bezieht, oder '***' für alle Terminal-IDs, oder zwei Leerzeichen, wenn die Komponente keine Terminal-ID hat. Wenn im Feld Server-ID zwei Leerzeichen angegeben sind, sind hier ebenfalls zwei Leerzeichen eingetragen. Wenn im Feld Server-ID '***' eingetragen ist, wird hier ebenfalls '***' eingetragen.
4	4	Meldungskennzeichen	160F - online. 163F - offline. 165F - sonstige Meldungen.
8	2	Sender-ID	Wenn im Feld Senderebene "TS" steht, ist hier die Server-ID eingetragen. Ansonsten ist hier eine Kopie des Wertes aus dem Feld Senderebene eingetragen.
10	1	Satzformat	1 – Satzformat für die Meldungsanzeige (Meldungsformat '1') 2 - Satzformat für die Datenübertragung (Meldungsformat '2')
11	1	Meldungsart	0 - INFO 1 - WARN 2 – ERROR
12	8	Datum	Datum im Format JJJJMMTT
20	6	Uhrzeit	Uhrzeit im Format hhmmss
26	4	Meldungscode	In INTUS COM eindeutiger Code
30	2	Subterminal-ID	Subterminal-ID der Komponente, auf die sich die Meldung bezieht, oder '***' für alle Subterminal-IDs, oder zwei Leerzeichen, wenn die Komponente keine subterminal-ID hat. Wenn im Feld Terminal-ID zwei Leerzeichen angegeben sind, sind hier ebenfalls zwei Leerzeichen eingetragen. Wenn im Feld Terminal-ID '***' steht, so ist hier ebenfalls '***' eingetragen.
32	2	Senderebene	Klasse des Objekts, das die Meldung erzeugt hat: TA - Admin-Server

			TH - Terminal-Handler TK - Konzentrator TS - Server TE – Terminal
34	2	Bezugsebene	Klasse des Objekts bzw. der Objekte, auf das bzw. die sich die Meldung bezieht: TA - Admin-Server TH - Terminal-Handler TK - Konzentrator TS - Server TE - Haupt- und/oder Subterminal TU – Tür
36	8	Ereignisdatum	Ereignisdatum im Format JJJJMMTT oder Leerzeichen.
44	6	Ereignisuhrzeit	Ereignisuhrzeit im Format hhmmss oder Leerzeichen.
50	0-450	Meldungstext	ASCII-Text <ul style="list-style-type: none"> • bei Meldungsformat '1': Text für Anzeige in Benutzerschnittstelle • bei Meldungsformat '2': Text für die INTUS COM interne maschinelle Auswertung

Tabelle 6.2 – INTUS COM Meldungsformat für Status, Fehler und Alarmmeldungen, Meldungsformat '1' und '2'

Die Länge einer solchen Meldung beträgt 50 bis 500 Byte.

Kurzformat für Meldungen

Neben diesen Formaten existiert noch ein Kurzformat, bei dem alle Felder ab Offset 8 entfallen (wie bei Meldungen des INTUS 3000/3450 Server).

Die Meldungen werden INTUS COM intern zur Statusüberwachung verwendet. Sie können aber auch für die Applikation interessant sein.

Wenn die Applikation keine Statusmeldungen verarbeiten kann, dann können sie vom INTUS COM herausgefiltert werden.

6.3.2.4 Verwendung der Meldungsformate

Fehler- und Alarmmeldungen

Fehler- und Alarmmeldungen werden im Meldungsformat '0' gesendet.

Online-/Offline Meldungen

Über diese Meldungen lässt sich der Verbindungsstatus der Terminals überwachen.

<xx><yy>160F... und

<xx><yy>163F...

Online-/Offline Meldungen können auch im Kurzformat gesendet werden.

Informationen zum Verbindzustand der Terminals

Um der Applikation Daten zum Verbindzustand von Terminals bereitzustellen, werden 165F-Statusmeldungen im Meldungsformt '2' mit Meldungscode 3517 verwendet. Die im Meldungstext übergebenen Daten haben das folgende Format

Offset	Länge	Beschreibung
0	1	Flag, ob der Verbindzustand des Terminals aus Sicht des Terminal-Handlers bekannt ist 0 - Verbindzustand im Terminal-Handler unbekannt 1 - Verbindzustand im Terminal-Handler bekannt.
1	1	Gültig, wenn der Verbindzustand des Terminals im Terminal-Handler bekannt ist. Flag, ob das Terminal aus Sicht des Terminal-Handlers verbunden ist 0 - nicht verbunden 1 - verbunden
2	variabel	reserviert.

Tabelle 6.3 – Informationen zum Verbindzustand

Parametrierinformationen an Applikation

Um der Applikation Daten zum Aufbau von TPI-Sätzen bereitzustellen, werden Parametrierungsinformationen über die INTUS COM Socket-Schnittstelle an die Applikation übergeben. Dazu werden 165F-Statusmeldungen mit Meldungscode 3515 verwendet.

Die zu übergebenen Parameterdaten werden im Meldungstext in Form von TPI-Sätzen übergeben. Meldungen mit Parametrierungsinformationen sind am Meldungscode '2' erkennbar. INTUS COM sendet auf diese Weise pro im Terminal-Handler aktiviertem TPI-Terminal jeweils

- einen SK1-Satz,
- einen AB1-Satz und
- einen AB2-Satz

Informationen zur Uhrzeitsynchronisation

Für Informationen zur Uhrzeitsynchronisation verwendet INTUS COM 165F-Statusmeldungen mit Meldungscode 3516. Der Datenteil der Meldungen zur Uhrzeitsynchronisation haben folgenden Aufbau

Offset	Länge	Beschreibung
0	1	Flag, ob Uhrzeitsynchronisation für das Terminal eingeschaltet 0 - Uhrzeitsynchronisation ausgeschaltet 1 - Uhrzeitsynchronisation eingeschaltet
1	1	Gültig, wenn Uhrzeitsynchronisation für das Terminal eingeschaltet ist: Flag, ob eine Zeitzone für das Terminal konfiguriert ist 0 - keine Zeitzone konfiguriert (lokale Terminal-Handler-Zeit) 1 - Zeitzone konfiguriert
2	1	Gültig, wenn Uhrzeitsynchronisation und Zeitzone für das Terminal eingeschaltet und konfiguriert ist. Flag, ob die Zeitzone bekannt ist 0 - Zeitzone unbekannt (d.h. nicht in der Datei "time_zones.ini" enthalten) 1 - Zeitzone bekannt (d.h. in Datei "time_zones.ini" enthalten).
3	5	Gültig, wenn Uhrzeitsynchronisation und Zeitzone für das Terminal eingeschaltet und konfiguriert und bekannt ist. Zeitdifferenz zu UTC in Minuten Offset 0: 1 Byte Vorzeichen ('-'=östlich,'+'=westlich) Offset 1: 4 ASCII-Ziffern
8	variabel	reserviert.

Tabelle 6.4 – Format für Informationen zur Uhrzeitsynchronisation

6.3.2.5 Filtern von Datensätzen beim Upload

Der Terminal-Handler kann Datensätze filtern (siehe 4.8.2). Dadurch kann erreicht werden, dass die Applikation nur die Sätze erhält, die für sie von Bedeutung sind. Die herausgefilterten Sätze werden nicht an die Applikation weitergegeben. Die Filter gelten unabhängig von der verwendeten Schnittstelle (Socket-Schnittstelle und/oder Dateischnittstelle).

Folgende Satzarten werden optional gefiltert: siehe Tabelle 6.3.2.2

Folgende Satzarten werden immer gefiltert:

- Anforderungs-/Statussätze (einschließlich Bereitmeldung), auf die der Terminal-Handler einen Download startet
- TPI Quittungen, wenn der Terminal-Handler auf eine Quittung (für einen von ihm gesendeten Satz) wartet.

Folgende Satzarten werden nicht gefiltert:

- Buchungssätze
- TPI Online-Anfragesätze
- Sätze unbekannter Terminals (außer INTUS COM Statusmeldungen)
- Sätze von im Terminal-Handler deaktivierten Terminals

6.4 Datenbank-Schnittstelle

Die Datenbankschnittstelle ermöglicht die Kommunikation zwischen Applikation und INTUS COM über vordefinierte Tabellen in einer Datenbank. Die Kommunikation zwischen Terminal-Handler (TH) und Datenbank erfolgt über ODBC. Die Datenbankschnittstelle ermöglicht z.B.:

- den Download von Stammsätzen, Profilen und Berechtigungsgruppen
- den Upload von Buchungen und Alarmen

Die Datenbankschnittstelle verbirgt mehr TPI-Funktionalität vor der Applikation, als die Datenschnittstelle oder die Socket-Schnittstelle.

Unterstützte Datenbanken

Folgende Datenbanken wurden mit INTUS COM getestet:

Datenbank	Datenbankversion	ODBC Treiberversion
Oracle 11g (32Bit version)	11.02.0020	10.01.00.07
Oracle 12g	12.01.0010	10.01.00.07
Microsoft SQL Server 2005	09.00.3042	2005.90.5000.00
Microsoft SQL Server 2008	10.00.4000	2007.100.4000.00
Microsoft SQL Server 2012	11.00.2100	2011.110.2100.60
Microsoft SQL Server 2014	12.00.1524	2011.110.2100.60
Microsoft Access	04.00.0000	6.01.7601.17632

Tabelle 6.5 – Getestete Datenbanken

Installieren und Konfigurieren der DB-Schnittstelle

Wie die Datenbank-Schnittstelle eingerichtet und installiert wird, ist in Kapitel 2.1 beschrieben.

Erforderliche Einstellungen im INTUS COM Client

Damit der Terminal-Handler die Tabellen einer Datenbank als Schnittstelle zur Applikation verwendet, müssen Sie die entsprechende Funktion in der Terminal-Handler Konfiguration mit dem INTUS COM Client konfigurieren (siehe 4.8). Aktivieren Sie nur die Funktionen, für die alle benötigten Tabellen und Felder angelegt sind.

Zum Erzeugen bzw. Interpretieren der TPI-Datensätze greift der Terminal-Handler auch auf die TPI-Parameterdateien (Systemkonfiguration (72) und Parametrierung (73)) der Terminals zu; speziell:

- die Länge der Ausweisnummer (SK1-Satz)
- der Buchungssatzaufbau (AB1-Satz)
- der Stammsatzaufbau (AB2-Satz)

Deadlockvermeidung

Der gleichzeitige Datenbankzugriff von INTUS COM und der Applikation kann zu Datenbank-deadlocks führen.

Um solche Deadlocks zu vermeiden, kann die Datenbankprozedur INTUSCOM_LOCK PROCEDURE verwendet werden. Die Datenbankprozedur INTUSCOM_LOCK PROCEDURE wird bei der Installation der Datenbanktabellen, für Oracle und Microsoft SQL Server, angelegt

Um die Deadlockvermeidung zu verwenden, muss die Applikation die Datenbankprozedur INTUSCOM_LOCK PROCEDURE am Beginn jeder kritischen Datenbanktransaktion ausführen. In INTUS COM muss die Verwendung der INTUSCOM_LOCK PROCEDURE über „Terminal Management System/Deadlockvermeidung verwenden“ aktiviert werden (siehe 4.6.1).

6.4.1 Tabellenübersicht

Name der Tabelle	Zugriff durch INTUS COM	Inhalt
Download (siehe 6.4.2)		
INTUSCOM_TIMESTAMPS	lesend/schreibend	Zeitstempel für Grundversorgung
INTUSCOM_MASTER_RECORDS	lesend/schreibend	TPI Stammdaten
INTUSCOM_OSO_CARD_DATA_IDS	lesend	OSO-Kartendaten-IDs
INTUSCOM_PROFILES	lesend/schreibend	TPI Profile
INTUSCOM_FUNCTION_PROFILES	lesend/schreibend	TPI Profile (zeitliche Funktionsumschaltung)
INTUSCOM_SPECIAL_DAYS	lesend	TPI Sondertage
INTUSCOM_AUTHORISATION_GROUPS	lesend	TPI Berechtigungsgruppen
INTUSCOM_FUNCTION_STEP_VALUES	lesend	Funktionsschrittwerte
INTUSCOM_CARD_DATA	lesend	TPI Kartendaten für das Schreiben von Berechtigungen gemäß OSS Standard Offline
Upload (siehe 6.4.3)		
INTUSCOM_UPLOAD_BOOKINGS	schreibend	TPI Buchungen
INTUSCOM_UPLOAD_OTHER	schreibend	sonstige Upload-Sätze (z. B. Alarmsätze)
Applikations-Tabellen		
INTUSCOM_TERMINALS (siehe 6.4.4)	schreibend	Terminal-Konfiguration
INTUSCOM_VIDEO_IMAGES	schreibend	Tabelle für das INTUS COM VideoInterface.
INTUS_PS_READERS	schreibend	PS-Leser Konfiguration
Biometrie (siehe 6.4.5ff)		
INTUS_FP_TEMPLATES_IDS	lesend/schreibend	Templates-IDs für Fingerprint & PS
INTUSCOM_TH_TEMPLATES	lesend/schreibend	Fingerprint-Templates
INTUS_FP_APP_TEMPLATES	lesend	Fingerprint-Templates von Einlernstation
INTUS_PS_TEMPLATES	lesend	PS-Templates von Einlernstation
Videodokumentation		
INTUSCOM_VIDEO_PROFILES	lesend	Videoprofile für das INTUS COM Video-Interface
Kennzeichenerkennung		
INTUSCOM_LP_PROFILES	lesend	Kennzeichenprofile
INTUSCOM_LICENSE_PLATES	lesend	Kennzeichen Stammdaten
Intern		
INTUSCOM_PROFILE_NAMES	lesend/schreibend	wird INTUS COM intern verwendet
INTUSCOM_POLL	lesend/schreibend	TH-interne Zeitstempel für Pollen

INTUSCOM_LOG	schreibend	wird INTUS COM intern verwendet
INTUSCOM_PARAMETERS	lesend/schreibend	wird INTUS COM intern verwendet
INTUSCOM_TEMPLATE_STATUS	lesend/schreibend	wird INTUS COM intern verwendet
INTUSCOM_VIDEO_REQUESTS	lesend/schreibend	wird INTUS COM intern verwendet
INTUSCOM_LOCK_TABLE	schreibend	wird INTUS COM intern verwendet

Tabelle 6.6 – Übersicht Datenbank-Tabellen

6.4.1.1 Datentypen

INTUS COM verwendet als Datentyp der Tabellenfelder ausschließlich Zeichenketten (Strings), Zeitstempel und Binary Large Objects (BLOBs). Die Tabellenfelder werden bei der Installation mit einer Default-Länge angelegt.

Zeichenketten

Die Feldlänge eines Stringfeldes in der Tabelle muss größer oder gleich der Länge des entsprechenden Feldes in der TPI Parametrierung sein.



Die Applikation muss beim Eintragen der Datensätze in die Download-Tabellen sicherstellen, dass die Stringlänge der in der Tabelle definierten Feldlänge entspricht (d.h. den String evtl. rechtsbündig mit Blanks, bzw. linksbündig mit Nullen auffüllen).

Zeitstempel

Neben den Stringfeldern werden noch Zeitstempel verwendet. Zeitstempel geben an, wann bestimmte Daten zuletzt geändert wurden. Durch Pollen der Zeitstempel kann eine Änderung erkannt und automatisch ein Download gestartet werden.

Mit Zeitstempel ist je nach Datenbank folgender Datentyp gemeint:

Datenbank	Typ für Zeitstempel
Oracle	date
MS SQL Server	datetime
MS Access	datetime

Tabelle 6.7 – Datentyp für Zeitstempel

Binary Large Objects

Des Weiteren werden zur Angabe von Binärdaten noch Binary Large Objects (BLOBs) verwendet.

Mit BLOB ist je nach Datenbank folgender Datentyp gemeint:

Datenbank	Typ für Binary Large Object (BLOB)
Oracle	BLOB
MS SQL Server	IMAGE
MS Access	OLEOBJECT

Tabelle 6.8 – Datentyp für Binary Large Object (BLOB)

6.4.2 Download-Tabellen

Die Datenbankschnittstelle ermöglicht den Download von

- Stammdaten
- Profilen
- Sondertagen
- Berechtigungsgruppen
- Funktionsschrittwerten
- Kartendaten

Jeder dieser 6 Datenarten ist eine Tabelle in der Datenbank zugeordnet:

Anforderungs-Nummer	Daten	Tabellen
69	Kartendaten	INTUSCOM_CARD_DATA
70	Funktionsschrittwerte	INTUSCOM_FUNCTION_STEP_VALUES
71	Sondertage	INTUSCOM_SPECIAL_DAYS
74	Profile	INTUSCOM_PROFILES und INTUSCOM_FUNCTION_PROFILES
75	Berechtigungsgruppen	INTUSCOM_AUTHORISATION_GROUPS
76	Stammdaten	INTUSCOM_MASTER_RECORDS

Tabelle 6.9 – Datenbanktabellen für den Download

6.4.2.1 Tabellendownload - Grundversorgung

Bei einer Grundversorgung (Download) werden alle relevanten Stammsätze, Profile, Berechtigungsgruppen usw. komplett neu auf das Terminal geladen. Während des Ladevorgangs bleiben die Terminals voll funktionsfähig. Die vorher im Terminal befindlichen Sätze der jeweiligen Satzart werden gelöscht.

Eine Grundversorgung (Download) aus der Datenbank kann auf 3 Arten gestartet werden:

- manuell im INTUS COM Client (siehe 3.4.2)
- durch Ladeanforderung vom Terminal; die Terminals senden nur dann eine Ladeanforderung, wenn sie entsprechend konfiguriert sind
- durch die Applikation über einen Zeitstempel in der Tabelle INTUSCOM_TIMESTAMPS

Erforderliche Einstellungen im INTUS COM Client

Für jede der 6 Datenarten muss im Register Download getrennt konfiguriert werden, ob der Download aus der Datenbank erfolgen soll (siehe 4.8). Wenn ja, muss die zugeordnete Tabelle in der Datenbank durch die Applikation mit Daten gefüllt werden.

Erforderliche Einstellungen in TPI

Damit die Tabellen fehlerfrei ins Terminal geladen werden können, muss für jede der Tabellen die maximale Satzanzahl mit TPI-Control in der Systemparameterdatei (72) definiert werden.

6.4.2.2 INTUSCOM_TIMESTAMPS - Grundversorgung durch die Applikation

Um eine Grundversorgung einer Download-Tabelle auszulösen, muss die Applikation das Feld TIME_STAMP in der Tabelle INTUSCOM_TIMESTAMPS für die entsprechende Tabelle aktualisieren.

Der Terminal-Handler prüft das Feld TIME_STAMP, indem er es mit dem internen Zeitstempeln in der Tabelle INTUSCOM_POLL vergleicht. Erkennt er, dass der Zeitstempel neu ist startet er daraufhin den Download.

Die Tabelle INTUSCOM_TIMESTAMPS hat folgenden Aufbau:

Feld	Typ	Beschreibung
TABLE_ID	char(2)	Anforderungsnummer: 69 – Kartendaten 70 – Funktionsschrittwerte 71 – Sondertage 74 – Profile 75 – Berechtigungsgruppen 76 – Stammsätze TI – Biometrie Templates-IDs (siehe 6.4.5.2) PS – PalmSecure Templates (siehe 6.4.6.3) FP – Reserviert für INTUS Enroll
TIME_STAMP	Zeitstempel	Zeitpunkt, zu dem die Applikation die letzte Grundversorgung der entsprechenden Tabelle bereitgestellt hat

Tabelle 6.10 – Die Tabelle INTUSCOM_TIMESTAMPS

Das Feld Anforderungsnummer ist das Schlüsselfeld.

Erforderliche Einstellungen im INTUS COM Client

Damit eine Grundversorgung über Zeitstempel ausgelöst wird, muss im Register Download die Checkbox Datenbank auf Änderungen pollen aktiviert werden (siehe 4.8.3).

6.4.2.3 INTUSCOM_MASTER_RECORDS - Stammdaten

Die Applikation muss die Stammdaten in der Tabelle `INTUSCOM_MASTER_RECORDS` bereitstellen. Für jeden Ausweis (Feld `TIMEID_NO`) darf nur ein Datensatz vorhanden sein.



Die Stammdaten für Fingerprint müssen in der Tabelle `INTUS_FP_TEMPLATES_IDS` bereitgestellt werden.

Nach Bereitstellung bzw. Änderung der Tabelle kann die Applikation einen Download (Grundversorgung) dieser Tabelle über die Synchronisationstabelle `INTUSCOM_TIMESTAMPS` auslösen (siehe 6.4.2.2).

Erforderliche Einstellungen im INTUS COM Client

- Im Terminal-Handler im Registerblatt Download muss in der Combobox Stammsätze (76) der Wert `Datenbank` ausgewählt werden, siehe 4.8.3

Erforderliche Einstellungen in TPI

- Der Stammsatzaufbau (d.h. welche Felder in welcher Reihenfolge verwendet werden sollen) muss in TPI-Control in dem TPI-Parametersatz AB2 festgelegt werden. Normalerweise kann die Voreinstellung verwendet werden. Der Terminal-Handler interpretiert den AB2-Satz, um die Stammdatensätze für den Download zu generieren (siehe auch TPI Handbuch Kap. 5.6.2).



Die Applikation muss nur die Felder in der Tabelle füllen, die auch in der Stammsatzdefinition verwendet werden.

- Damit die Tabelle fehlerfrei ins Terminal geladen werden kann, muss die maximale Stammsatzanzahl mit TPI-Control in der Systemparameterdatei (72) eingestellt werden.

Die Stammdatentabelle `INTUSCOM_MASTER_RECORDS` hat folgenden Aufbau:

Feld	Typ	TPI-Feldtyp	Beschreibung
<code>CLIENT</code>	char(10)	--	Mandant
<code>TIMEID_NO</code>	char(20)	01	Kartennummer (Ausweis-ID)
<code>ACCESS_PROFILE_NO</code>	char(3)	02	Zutrittsprofilnummer
<code>BOOKING_PROFILE_NO</code>	char(3)	03	Buchungsprofilnummer
<code>AUTHORISATION_GROUP</code>	char(3)	04	Berechtigungsgruppe
<code>PIN_CODE</code>	char(6)	05	Pincode
<code>ENCRYPTED_PIN_CODE</code>	char(64)	28	Verschlüsselter Pincode
<code>ATTENDANCE_STATUS</code>	char(1)	06	Anwesenheitsstatus K/G/*
<code>MAIL_NO</code>	char(2)	07	Mailboxtextnummer
<code>MAIL_COUNTER</code>	char(1)	08	Mailboxtext-Counter
<code>INFO_FIELD_1</code>	char(13)	14	Saldo 1
<code>INFO_FIELD_2</code>	char(13)	14	Saldo 2
<code>INFO_FIELD_3</code>	char(13)	14	Saldo 3
<code>INFO_FIELD_4</code>	char(13)	14	Saldo 4
<code>INFO_FIELD_5</code>	char(13)	14	Saldo 5
<code>INFO_FIELD_6</code>	char(13)	14	Saldo 6
<code>INFO_FIELD_7</code>	char(13)	14	Saldo 7
<code>INFO_FIELD_8</code>	char(13)	14	Saldo 8
<code>INFO_FIELD_9</code>	char(13)	14	Saldo 9

Feld	Typ	TPI-Feldtyp	Beschreibung	
INFO_FIELD_10	char(13)	14	Saldo 10	
ROOM_NO	char(3)	09	nach Raumnummer	
FROM_DATE	char(8)	10	JJJJMMTT Von-Gültigkeitsdatum	
TO_DATE	char(8)	11	JJJJMMTT Bis-Gültigkeitsdatum	
FROM_TIME	char(4)	12	hhmm Von-Gültigkeitsuhrzeit	
TO_TIME	char(4)	13	hhmm Bis-Gültigkeitsuhrzeit	
CARD_DATA	char(400)	17 oder 21	Berechtigungsdaten für Schreibterminal, von hinten mit Leerzeichen aufgefüllt	
CARD_DATA_CONFIG	char(17)	18	Konfigurationsdaten für Schreibterminal	
TEMPLATES_ID	char(8)	19	Templates-ID (Biometrie)	
ALTERNATIVE_AUTH	char(1)	20	1/0 alternative Authentifizierung (bis v2.8.0) 2: Zeitsteuerung durch Profile	
ALTERNATIVE_AUTH_FP	char(1)	20	1/0 alternative Authentifizierung Finger-print (ab 2.10.0)	
ALTERNATIVE_AUTH_PS	char(1)	20	1/0 alternative Authentifizierung PalmSecure (ab 2.10.0)	
NAME_FIELD	char(40)	22	Namensfeld	
COUNTRY_AND_LANGUAGE	char(7)	23	Länder-Sprachcode	
RECORD_DISABLED	char(1)	24	Stammsatz (Ausweis) gesperrt	
RETENTION_CONTROL	char(1)	25	Ausweiseinzug	
RETENTION_FROM_DATE	char(1)	26	Karenzzeit-Datum für Ausweiseinzug	
RETENTION_FROM_TIME	char(1)	27	Karenzzeit-Uhrzeit für Ausweiseinzug	
STATUS	char(1)	--	Update/Delete- Status: v - gültiger Datensatz u - aktualisierter Datensatz (gültig) d - zu löschernder Datensatz (ungültig)	
TIME_STAMP	Zeitstempel	--	Zeitstempel für Update/Delete	
ATT_BOOKING_DATE	char(8)	--	Datum	... aus der Buchung, die zuletzt den Anwesenheitsstatus gesetzt hat
ATT_BOOKING_TIME	char(6)	--	Uhrzeit	
ATT_SERVER_ID	char(2)	--	Server ID	
ATT_TERMINAL_ID	char(2)	--	Terminal ID	
ATT_SUB_TERMINAL_ID	char(2)	--	Subterminal ID	
ATT_RECORD_TYPE	char(2)	--	Satzart	

Tabelle 6.11 – Die Stammdatentabelle INTUSCOM_MASTER_RECORDS

In dieser Tabelle sind die Felder **CLIENT** und **TIMEID_NO** zusammen der eindeutige Schlüssel.

Das Feld **CLIENT** wird nur für den Mehrmandantenmodus benötigt (siehe 4.8.3), wenn er nicht verwendet wird, sollte die Applikation das Feld mit **0000000001** belegen.

Für alle Felder mit einem Eintrag in der Spalte **TPI-Feldtyp** gibt es ein analoges Feld in den TPI-Stammdatensätzen Y0. Die Bedeutung und Verwendung der Felder ist im TPI-Handbuch beschrieben.

Update/Delete-Logik

Manchmal ist es erwünscht, einzelne Stammsätze hinzuzufügen, zu ändern oder zu löschen, ohne dass der Personalstamm komplett neu auf die Terminals geladen werden muss. Dies wird mit der Update/Delete-Logik ermöglicht.

Für die Update/Delete-Logik können folgende Einstellungen getroffen werden:

- 0: Keine Update/Delete-Logik aktiviert
- 1: Update/Delete-Logik nur für Stammsätze aktiviert (**INTUSCOM_MASTER_RECORDS**)
- 2: Update/Delete-Logik sowohl für Stammsätze als auch für OSO-Kartendaten-IDs (**INTUSCOM_MASTER_RECORDS** und **INTUSCOM_OSO_CARD_DATA_IDS**)

Für Wert 1 werden die Felder **STATUS** und **TIME_STAMP** in der Stammdatentabelle **INTUSCOM_MASTER_RECORDS** benötigt.

Für Wert 2 werden zusätzlich die Felder **STATUS** und **TIME_STAMP** in der OSO-Kartendatentabelle **INTUSCOM_OSO_CARD_DATA_IDS** benötigt.

Erforderliche Einstellungen für die Update/Delete-Logik

- Die Update/Delete-Logik erfordert, dass auf dem Register Download die Checkbox Datenbank auf Änderungen pollen aktiviert ist. Es werden dann die Tabellen **INTUSCOM_TIMESTAMPS** und **INTUSCOM_POLL** verwendet (siehe 4.8.3).
- Die Pollzeit des Terminal-Handlers wird im Register Grundeinstellungen im Parameter Pollzyklus eingestellt.

Ablauf des Downloads von Update- und Delete- Sätzen

Die Applikation gibt normalen Grundversorgungs-Stammsätzen den Status „v“.

Wenn die Applikation einen Datensatz außerhalb der Grundversorgung hinzufügt oder ändert, dann gibt sie ihm den Status „u“ und setzt seinen **TIME_STAMP** auf den aktuellen Zeitpunkt.

Wenn die Applikation einen Datensatz löschen will, setzt sie seinen Status auf „d“ und seinen **TIME_STAMP** auf den aktuellen Zeitpunkt.

Der Terminal-Handler pollt die Zeitstempel der Update/Delete-Sätze. Wenn ein solcher Satz neu ist, schickt der Terminal-Handler ihn als Y0-Satz bzw. Y1-Satz an die Terminals.



Die Update/Delete-Logik beeinflusst auch die Grundversorgung: Es werden bei einer Grundversorgung nur Sätze mit dem Status „v“ oder „u“ ans Terminal gesendet, jedoch keine Sätze mit dem Status „d“.

Stammsatzsperrre

Das Feld **RECORD_DISABLED** ermöglicht die Unterscheidung zwischen

- gesperrten Stammsätzen
- nicht vorhandenen Stammsätzen

Dadurch kann die TPI-tasc ggf. unterschiedlich reagieren, vorausgesetzt die TPI-Parametrierung unterstützt dieses.

Unterstützt die TPI-Parametrierung eines Terminals die Unterscheidung nicht, hängt die Behandlung gesperrter Datensätze von der Einstellung für den Stammsatz-Download ab (siehe 4.8.3).

Bei Nutzung des Feldes **RECORD_DISABLED** und Verwendung der Datenbank-Schnittstelle ist für den Stammsatz-Download die Einstellung „Datenbank ab v3.3.0 (Gesperrte Sätze)“ zu empfehlen.

Online-Anwesenheitsprüfung

TPI-Terminals können sogenannte Online-Anfragen senden, um den Anwesenheitsstatus (Kommt- / Geht- Status) terminalübergreifend vom Rechner überprüfen zu lassen.

Der Terminal-Handler vergleicht das Statusfeld mit dem Feld **ATTENDANCE_STATUS** und sendet einen entsprechenden Antwortsatz (R1- oder R2-Satz).

Das Terminal antwortet wiederum mit einem Buchungssatz, in dem das Fehlerbyte entsprechend gesetzt ist. Im Falle einer korrekten Buchung aktualisiert der Terminal-Handler das Feld **ATTENDANCE_STATUS**.

Erforderliche Einstellungen für die Online-Anwesenheitsprüfung

- Die mit ATT-Unterstrich beginnenden Felder werden für die Online Anwesenheitsprüfung benötigt. Ein Download der Stammdaten ins Terminal ist in diesem Fall nicht erforderlich.
- Im Register Download muss die Checkbox Online-Anfrage aktiviert sein.
- IN TPI müssen Kommt- / Geht- Online-Funktionen definiert sein, die das Feld **Kommt- / Geht- Status** (06) enthalten (siehe TPI Handbuch Kap. 2.2.3).

Online-Saldenrückmeldung

TPI-Terminals können auch Online-Anfragen zur Saldenanzeige senden. Die Applikation sollte die Saldenfelder **INFO_FIELD_1..** regelmäßig aktualisieren. Wenn der Terminal-Handler eine Online-Anfrage erhält, antwortet er mit einem R4-Antwortsatz mit den aktuellen Zeitsalden.

Erforderliche Einstellungen für die Online-Saldenrückmeldung

- Im Register Download muss die Checkbox Online Salden aktiviert sein. Ein Download der Stammdaten ins Terminal ist in diesem Fall nicht erforderlich.
- Länge und Anzahl der Saldenwerte müssen im AB2-Satz definiert sein. Der Terminal-Handler benötigt diese Werte um den Antwortsatz zu generieren
- In der TPI-Parametrierung muss eine Funktion für die Saldenanfrage mit Satzart **SA** definiert sein (siehe TPI Handbuch Kap. 2.2.3).

6.4.2.4 INTUSCOM_OSO_CARD_DATA_IDS - OSO-Kartendaten-IDs

Die OSO-Kartendaten-ID-Tabelle **INTUSCOM_OSO_CARD_DATA_IDS** dient der Angabe der OSO-Kartendaten-IDs zu den Stammdaten in der Tabelle **INTUSCOM_MASTER_RECORDS**.

Die Tabelle **INTUSCOM_OSO_CARD_DATA_IDS** hat folgenden Aufbau:

Feld	Typ	Beschreibung
CLIENT	char(10)	Mandant wie in INTUSCOM_MASTER_RECORDS
TIMEID_NO	char(20)	Kartennummer (Ausweis-ID) wie in INTUSCOM_MASTER_RECORDS
OSO_CARD_DATA_ID	char(3)	Wert für TPI-Stammsatzfeld mit Feldtyp 29 (OSO-Kartendaten-ID) alphanumerisch nur ASCII-Buchstaben/-Ziffern Der in OSO_CARD_DATA_ID angegebene Wert kann auf Datensätze mit der entsprechenden Kartendaten-ID und dem Kartendatentyp O in der Tabelle INTUSCOM_CARD_DATA verweisen.
STATUS	char(1)	Update/Delete- Status: v - gültiger Datensatz u - aktualisierter Datensatz (gültig) d - zu löschernder Datensatz (ungültig)
TIME_STAMP	Zeitstempel	Zeitstempel für Update/Delete

Tabelle 6.12 – Die Tabelle INTUSCOM_OSO_CARD_DATA_IDS

6.4.2.5 INTUSCOM_PROFILES - Profile

Wenn Buchungs- oder Zutrittsberechtigungen zeitlich und räumlich eingeschränkt werden soll, muss die Applikation Profilsätze (Buchungs- und Zutrittsprofile) in der Tabelle INTUSCOM_PROFILES bereitstellen.

Mit sogenannten Türöffnenprofilen für einzelne Türen können Türöffnungszeiten definiert werden.

Zusätzlich werden Profile in INTUS COM dazu verwendet, Stammdaten aus der INTUSCOM_MASTER_RECORDS Tabelle selektiv in einzelne Terminals zu laden (s.u.).

Nach Bereitstellung bzw. Änderung der Tabelle kann die Applikation einen Download (Grundversorgung) dieser Tabelle über die Synchronisationstabelle INTUSCOM_TIMESTAMPS auslösen (siehe 6.4.2.2).

Raum-Zeitmodell der INTUS COM Datenbank-Schnittstelle

Für jedes Terminal bzw. Leser können mehrere Profile (identifiziert durch die Profilnummer) und für jedes Profil können mehrere Profilsätze definiert werden. Ein Profilsatz definiert pro Terminal und Profilnummer einen Zeitraum für bestimmte Wochentage.



Dieses Modell entspricht nicht dem Modell von TPI, das auch in der Datei- und Socket-Schnittstelle verwendet wird. Die Umsetzung in TPI-Profilsätze erfolgt automatisch durch den Terminal-Handler, wenn die Applikation einen Download (Grundversorgung) dieser Tabelle über die Synchronisationstabelle INTUSCOM_TIMESTAMPS auslöst (siehe 6.4.2.2).

Zusätzlich können Gruppen von Sondertagen (z.B. Feiertagen) mit von Normaltagen abweichenden Rechten in der Tabelle INTUSCOM_SPECIAL_DAYS definiert werden.

Vorgehensweise zur Bereitstellung von Profilen

1. Definieren Sie **disjunkte** Gruppen von Mitarbeitern mit denselben Rechten
2. Ordnen Sie jeder dieser Mitarbeitergruppen eine eindeutige Zutritts- bzw. Buchungsprofilnummer zu
3. Legen Sie passende Profilsätze für alle Profilnummern und Terminals an

Erforderliche Einstellungen im INTUS COM Client

Im Terminal-Handler auf dem Registerblatt Download muss im Rahmen "Download TPI Konfiguration" die Einstellung für Profile (74) auf den entsprechende Wert gesetzt werden (siehe 4.8.3).

Erforderliche Einstellungen in TPI

Damit die Tabelle fehlerfrei ins Terminal geladen werden kann, muss die maximale Anzahl der Profilsätze mit TPI-Control in der Systemparameterdatei (72) eingestellt werden.

Die Profiltabelle **INTUSCOM_PROFILES** hat folgenden Aufbau:

Feld	Typ	Beschreibung
SERVER_ID	char(2)	Server ID
TERMINAL_ID	char(2)	Terminal ID
SUB_TERMINAL_ID	char(2)	Subterminal ID 00 bis 16 In der Datenbank wird das Profil für jedes Subterminal separat angegeben. Der Terminal-Handler erzeugt daraus die TPI-Darstellung.
PROFILE_TYPE	char(1)	Z – Zutrittsprofil B – Buchungsprofil T – Türprofil
PROFILE_NO	char(3)	Profil-ID
FROM_TIME	char(4)	hhmm Gültigkeit, Beginn-Zeit
TO_TIME	char(4)	hhmm Gültigkeit, Ende-Zeit
SUNDAY	char(1)	J/N Gültigkeit Sonntag
MONDAY	char(1)	J/N Gültigkeit Montag
TUESDAY	char(1)	J/N Gültigkeit Dienstag
WEDNESDAY	char(1)	J/N Gültigkeit Mittwoch
THURSDAY	char(1)	J/N Gültigkeit Donnerstag
FRIDAY	char(1)	J/N Gültigkeit Freitag
SATURDAY	char(1)	J/N Gültigkeit Samstag
SPECIAL_DAY_1	char(1)	J/N Sondertag-Kennung 1 (alt)
SPECIAL_DAY_2	char(1)	J/N Sondertag-Kennung 2 (alt)
SPECIAL_DAY_3	char(1)	J/N Sondertag-Kennung 3 (alt)
SD_FLAG	char(1)	Sondertagsflag: 0 - Profilsatz gültig an Normaltagen 1 - Profilsatz gültig an Sondertagen
SD_GROUP	char(2)	Sondertagsgruppe
PINCODE_FLAG	char(1)	J/N PINCODE erforderlich
BUFFER_AUTHORISE_D_BOOKINGS	char(1)	J/N berechtigte Buchungen puffern
SPECIAL_AUTHORIZATION	char(1)	J/N Sonderberechtigung
ALTERNATIVE_AUTH	char(1)	Alternative Authentifizierung im Zutrittsprofil für Biometrie de/aktivieren N – alternative Authentifizierung nicht erlaubt J – alternative Authentifizierung erlaubt.
TOGGLE	char(1)	Schalter für Dauerfunktion in Zutritts- und Steuerprofilsätzen. Für Zutrittsprofile gilt: 0 = die Person hat keine Berechtigung 1 = die Person hat Berechtigung zum Ein- und Ausschalten 2 = die Person hat Berechtigung nur zum Einschalten 3 = die Person hat Berechtigung nur zum Ausschalten Für Türprofile gilt: 1 = Ein- und Ausschaltprofil (wie bisher)

		2 = Einschaltprofil; es wird nur die Beginn-zeit PT+3,4 geprüft. Zu diesem Zeitpunkt werden die Türen freigeschaltet, sofern sie nicht durch eine EMA gesperrt sind. 3 = Ausschaltprofil; es wird nur die Ende-zeit PT+7,4 geprüft. Zu diesem Zeitpunkt wird die Freischaltung beendet, sofern sie nicht durch eine BMA freigeschaltet sind.
FROM_DATE	char(8)	Gültigkeitsbeginndatum (Datum des Tages vor dem der Datensatz ungültig ist) im Format YYYYMMDD oder '-----' für kein Gültigkeitsbeginndatum
TO_DATE	char(8)	Gültigkeitsendedatum (Datum des Tages, nach dem der Datensatz ungültig ist) im Format YYYYMMDD oder '-----' für kein Gültigkeitsendedatum

Tabelle 6.13 – Die Profiltabelle INTUSCOM_PROFILES

Das Feld PROFILE_NO ist der (nicht eindeutige) Index der Tabelle, d.h. es können mehrere Datensätze mit der selben PROFILE_NO vorliegen.

SERVER_ID, TERMINAL_ID und SUB_TERMINAL_ID adressieren das jeweilige Terminal (SUB_TERMINAL_ID =00) bzw. den Leser.

Das Feld PROFILE_TYPE bestimmt die Profilart: Zutrittsprofil (Z), Buchungsprofil (B), Türöffnenprofil (T).

Sondertagsprofilsätze

Über das Feld SD_FLAG kann für jeden Profilsatz definiert werden, ob er an normalen oder an Sondertagen gelten soll. Mit dem Feld SD_GROUP wird die Sondertagsgruppe definiert, für die das Profil im Fall SD_FLAG=1 gelten soll

Die Felder sind seit der Version INTUS COM 2.0.0 in der Profiltabelle enthalten und ersetzen die Felder SPECIAL_DAY_1, SPECIAL_DAY_2, SPECIAL_DAY_3.

Auswahl von Stammsätzen anhand der Profile

Bei größeren Installationen ist es oftmals aus Speichermangel in den Terminals nicht erwünscht, dass alle Stammdaten in alle Terminals geladen werden.

INTUS COM bietet die Möglichkeit, die auf ein Terminal zu ladenden Stammsätze anhand der Zutritts- und Buchungsprofile zu selektieren (zur Konfiguration dieser Funktion siehe 4.8.3). Für diese Funktion werden die Profiltabelle und die Felder ACCESS_PROFILE_NO und BOOKING_PROFILE_NO in der Stammdatentabelle benötigt.

Der Download eines Stammsatzes erfolgt nur, wenn er (mindestens) eine der folgenden Bedingungen erfüllt:

- die Buchungsprofilnummer ist „000“ oder
- die Zutrittsprofilnummer ist „000“ oder
- in der Profiltabelle ist für das Terminal mindestens ein Eintrag mit der Buchungsprofilnummer vorhanden oder
- in der Profiltabelle ist für das Terminal mindestens ein Eintrag mit der Zutrittsprofilnummer vorhanden

Befristete Profile

Der Terminal-Handler lädt dann nur die Profile in die Terminals, für die die Datumsbedingungen in den beiden Feldern FROM_DATE und TO_DATE erfüllt sind.

Mit FROM_DATE kann die Gültigkeit des Profileintrags ab einem bestimmten Datum festgelegt werden.

Mit `TO_DATE` kann die Gültigkeit des Profileintrags bis zu einem bestimmten Datum festgelegt werden.

Er überprüft jeweils um Mitternacht, ob sich die Bedingung geändert hat und lädt bzw. löscht die entsprechenden Profile. Damit kann man (z.B. zum Jahreswechsel) schon mal neue Profile vorbereiten, die dann um Mitternacht gegen die alten ausgetauscht werden.

Damit die beiden Felder durch den Terminal-Handler ausgewertet werden, muss im Terminal-Handler im Registerblatt Download für Profile (74) der Wert `Datenbank ab v2.4.0 (befristete Profile)` eingestellt werden.

Die beiden Datumsfelder sind seit der Version INTUS COM 2.4.0 in der Profiltabelle enthalten.

6.4.2.6 INTUSCOM_FUNCTION_PROFILES – Zeitliche Funktionsumschaltung

In dieser Tabelle können Profilsätze für die Funktions-Voreinstellung eines Terminals durch die Applikation hinterlegt werden.

Durch die Terminal-Handler Einstellung „Datenbank ab 2.10.0 (zeitliche Funktionsumschaltung)“ wird der Terminal-Handler angewiesen beim Profildownload (74) diese Tabelle hinzuziehen.

Die Profiltabelle `INTUSCOM_FUNCTION_PROFILES` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>SERVER_ID</code>	char(2)	Server ID
<code>TERMINAL_ID</code>	char(2)	Terminal ID
<code>SUB_TERMINAL_ID</code>	char(2)	Subterminal ID 00 bis 16 In der Datenbank wird das Profil für jedes Subterminal separat angegeben. Der Terminal-Handler erzeugt daraus die TPI-Darstellung.
<code>RECORD_TYPE</code>	char(2)	TPI Buchungsart
<code>FROM_TIME</code>	char(4)	hhmm Gültigkeit, Beginn-Zeit
<code>TO_TIME</code>	char(4)	hhmm Gültigkeit, Ende-Zeit
<code>SUNDAY</code>	char(1)	J/N Gültigkeit Sonntag
<code>MONDAY</code>	char(1)	J/N Gültigkeit Montag
<code>TUESDAY</code>	char(1)	J/N Gültigkeit Dienstag
<code>WEDNESDAY</code>	char(1)	J/N Gültigkeit Mittwoch
<code>THURSDAY</code>	char(1)	J/N Gültigkeit Donnerstag
<code>FRIDAY</code>	char(1)	J/N Gültigkeit Freitag
<code>SATURDAY</code>	char(1)	J/N Gültigkeit Samstag
<code>SD_FLAG</code>	char(1)	Sondertagsflag: 0 - Profilsatz gültig an Normaltagen 1 - Profilsatz gültig an Sondertagen
<code>SD_GROUP</code>	char(2)	Sondertagsgruppe
<code>FROM_DATE</code>	char(8)	Gültigkeitsbeginndatum (Datum des Tages vor dem der Datensatz ungültig ist) im Format YYYYMMDD oder '-----' für kein Gültigkeitsbeginndatum
<code>TO_DATE</code>	char(8)	Gültigkeitsendedatum (Datum des Tages, nach dem der Datensatz ungültig ist) im Format YYYYMMDD oder '-----' für kein Gültigkeitsendedatum

Tabelle 6.14 – Die Profiltabelle INTUSCOM_FUNCTION_PROFILES

6.4.2.7 INTUSCOM_SPECIAL_DAYS Sondertage

Die Sondertagstabelle `INTUSCOM_SPECIAL_DAYS` wird in Verbindung mit der Tabelle `INTUSCOM_PROFILES` zur Definition von Sondertagen für Sondertagsprofile verwendet. Sie hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>SD_GROUP</code>	char(2)	Sondertagsgruppe
<code>SD_DATE</code>	char(8)	JJJJMMTT Von-Sondertagsdatum

Tabelle 6.15 – Die Sondertagstabelle INTUSCOM_SPECIAL_DAYS

6.4.2.8 INTUSCOM_AUTHORISATION_GROUPS Berechtigungsgruppen

Die Tabelle der Berechtigungsgruppen `INTUSCOM_AUTHORISATION_GROUPS` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>AUTHORISATION_GROUP</code>	char(3)	Berechtigungsgruppe
<code>RECORD_TYPE</code>	char(2)	Satzart

Tabelle 6.16 – Die Tabelle INTUSCOM_AUTHORISATION_GROUPS

Die Datenbankfelder entsprechen direkt den TPI-Feldern im B1-Satz (siehe TPI Benutzerhandbuch, Kapitel 2.3.1.5).

6.4.2.9 INTUSCOM_FUNCTION_STEP_VALUES Funktionsschrittwerthe

Die Funktionsschrittwerthe-Tabelle `INTUSCOM_FUNCTION_STEP_VALUES` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>FUNCTION_STEP</code>	char(3)	Funktionsschritt
<code>TABLE_VALUE</code>	char(40)	Funktionsschrittwert
<code>DISPLAY_TEXT</code>	char(40)	Anzeigetext

Tabelle 6.17 – Die Tabelle INTUSCOM_FUNCTION_STEP_VALUES

Eine ausführliche Beschreibung zur Verwendung der Funktionsschrittwertetabelle finden sie im TPI-Handbuch, Kapitel 2.3.2.1

6.4.2.10 INTUSCOM_CARD_DATA Kartendaten

Die Kartendaten-Tabelle **INTUSCOM_CARD_DATA** dient der Angabe von Berechtigungen für Offlineterminals, die den OSS Standard Offline verwenden.

Diese Tabelle ist so ausgelegt, dass sie darüber hinaus auch Kartendaten enthalten könnte, die nicht dem OSS Standard Offline entsprechen. (Um solche Kartendaten schreiben zu können, müsste jedoch zumindest INTUS TPI-TASC erweitert werden.)

Die Kartendaten-Tabelle **INTUSCOM_CARD_DATA** hat folgenden Aufbau:

Feld	Typ	Beschreibung
SITE_ID	char(5)	Offlineanlagen-ID(Site-ID) fünfstellig numerisch Für Kartendatentyp O (OSS Standard Offline) muss die Site-ID einen Wert im Bereich 00001 bis 65535 haben. (Die Site-ID wird im Zusammenhang mit INTUS Flex auch als Project Code bezeichnet.)
CARD_DATA_TYPE	char(1)	Kartendatentyp O – Berechtigungsdaten für OSS Standard Offline andere Buchstaben – reserviert für mögliche zukünftige Erweiterungen Ziffern (0 – 9) – reserviert für kundenspezifische Zwecke
CARD_DATA_ID	char(3)	Kartendaten-ID dreistellig alphanumerisch nur ASCII-Buchstaben/-Ziffern darf nicht 000 sein Für Kartendatentyp O (OSS Standard Offline) kann auf Datensätze mit einem bestimmten Wert in CARD_DATA_ID verwiesen werden, indem dieser Wert im Feld OSO_CARD_DATA_ID der Tabelle INTUSCOM_OSO_CARD_DATA_IDS angegeben wird.
SUB_ID	char(3)	Sub-ID dreistellig alphanumerisch nur ASCII-Buchstaben/-Ziffern darf nicht 000 sein Datensätze, die nicht anhand der Felder SITE_ID, CARD_DATA_TYPE und CARD_DATA_ID unterscheidbar sind, müssen unterschiedliche Werte in SUB_ID haben.
FROM_DATE	char(8)	Gültigkeitsbeginn des Datensatzes
FROM_TIME	char(4)	Beide Felder entsprechend ihrer Länge mit 0 gefüllt bedeutet „keine Beschränkung“. Sonst sind in FROM_DATE ein Datum im Format YYYYMMDD und in FROM_TIME eine Uhrzeit im Format hhmm anzugeben.

TO_DATE	char(8)	Gültigkeitsende des Datensatzes
TO_TIME	char(4)	Beide Felder entsprechend ihrer Länge mit 9 gefüllt bedeutet „keine Beschränkung“. Sonst sind in TO_DATE ein Datum im Format YYYYMMDD und in TO_TIME eine Uhrzeit im Format hhmm anzugeben.
MAJOR_VERSION	char(2)	Majorversion des Formats der Kartendaten zweistellig hexadezimal, A-F als Großbuchstaben Stand Februar 2021 für OSS Standard Offline immer 01
MINOR_VERSION	char(2)	Minorversion des Formats der Kartendaten zweistellig hexadezimal, A-F als Großbuchstaben Stand Februar 2021 für OSS Standard Offline entweder 00 oder 01
CHANGE_INDEX	char(2)	Änderungsindex alphanumerisch nur ASCII-Buchstaben/-Ziffern Für Kartendatentyp O (OSS Standard Offline) kann dieser Wert im Buchungssatz der Schreibbuchung zurückgemeldet werden, damit die Applikation daran erkennen kann, welcher Änderungsstand der Berechtigungsdaten beim Schreiben verwendet wurde.
EXCEED_MR_VALIDITY	char(1)	Angabe, ob das Gültigkeitsende der Berechtigungsdaten das Gültigkeitsende des Stammsatzes überschreiten darf Für Kartendatentyp O (OSS Standard Offline): J – ja N – nein U – Uhrzeit ja, Datum nein Bei N und U muss, damit die Berechtigungen geschrieben werden können, in der TPI-Parametrierung das Stammsatzfeld für das Gültigkeitsendedatum und im Falle von N zusätzlich das Stammsatzfeld für die Gültigkeitsendehuhrzeit parametriert sein.
EARIEST_RENEWAL_DATE	char(8)	frühester Gültigkeitsvortragsbasistag Für Kartendatentyp O (OSS Standard Offline): 00000000 – Gültigkeitsvortrag ab sofort 99999999 – kein Gültigkeitsvortrag Datum im Format YYYYMMDD – gibt in Verbindung mit RENEWAL_TIME an, ab wann ein Gültigkeitsvortrag erfolgen kann

<code>RENEWAL_TIME</code>	char(4)	Gültigkeitsvortragsuhrzeit Für Kartendatentyp O (OSS Standard Offline): Uhrzeit im Format hhmm Vor dieser Uhrzeit gilt der Vortag als Basistag. Ab dieser Uhrzeit gilt der aktuelle Tag als Basis- tag.
<code>RELATIVE_VALIDITY_END_DAY</code>	char(3)	relativer Gültigkeitsendetag für den Gültigkeits- vortrag Für Kartendatentyp O (OSS Standard Offline): numerisch 000 - 999 000 – Basistag 001 – 1. Tag nach Basistag 002 – 2. Tag nach Basistag usw.
<code>RENEWAL_LIMIT_DATE</code>	char(8)	Gültigkeitsvortragslimit
<code>RENEWAL_LIMIT_TIME</code>	char(4)	Für Kartendatentyp O (OSS Standard Offline): Beide Felder entsprechend ihrer Länge mit 0 ge- füllt bedeutet „kein Gültigkeitsvortrag“. Beide Felder entsprechend ihrer Länge mit 9 ge- füllt bedeutet „keine Beschränkung“. Sonst sind für den Zeitpunkt, bis zu dem die Gültigkeit maximal vorgetragen werden soll, in <code>RENEWAL_LIMIT_DATE</code> ein Datum im Format YYYYMMDD und in <code>RENEWAL_LIMIT_TIME</code> eine Uhrzeit im Format hhmm anzugeben.
<code>CARD_DATA</code>	BLOB	Kartendaten als Binärdaten Für Kartendatentyp O (OSS Standard Offline): Der Inhalt des Feldes muss das Format haben, das für das OSS Standard Offline Data File für die verwendete Version (die in <code>MAJOR_VERSION</code> und <code>MINOR_VERSION</code> angegeben ist) definiert ist.
<code>CARD_DATA_EXT</code>	BLOB	zusätzliche Kartendaten als Binärdaten Für Kartendatentyp O (OSS Standard Offline): Bei dem Kartendatenformat 1.1 können im Feld <code>CARD_DATA_EXT</code> Daten in dem Format angege- ben werden, das für das OSS Standard Offline Customer-Extensions File für die eingesetzte Version definiert ist. Bei dem Kartendatenformat 1.0 oder, wenn keine Customer Extensions-Daten geschrieben werden sollen, muss <code>CARD_DATA_EXT</code> entweder NULL oder leer sein. (Das Kartendatenformat wird in <code>MAJOR_VERSION</code> und <code>MINOR_VERSION</code> angegeben.)

Tabelle 6.18 – Die Tabelle INTUSCOM_CARD_DATA

6.4.3 Upload-Tabellen

Die Datenbankschnittstelle ermöglicht den Upload von gesicherten TPI-Sätzen. Diese werden in Buchungen und sonstige Sätze (z. B. Alarm-/Ereignisdatensätze) unterschieden. Die Unterscheidung erfolgt anhand der TPI-Satzart.

Die Buchungen werden in die Tabelle `INTUSCOM_UPLOAD_BOOKINGS` gespeichert. Die sonstigen Sätze werden in die Tabelle `INTUSCOM_UPLOAD_OTHER` gespeichert.

Upload und Quittierung der Sätze

Jeder Satz, der in die Datenbank eingefügt werden soll, wird zunächst anhand der Satzart als Buchungssatz oder sonstiger Satz erkannt.

Bei Buchungssätzen wird der Datenanteil anhand der TPI-Parametrierung (SK1-Satz und AB1-Satz siehe TPI Benutzerhandbuch) in die einzelnen Felder zerlegt.

Anschließend wird der Satz in die entsprechende Datenbanktabelle eingefügt.

Optional wird außer den Feldern des empfangenen Datensatzes auch der Upload-Zeitpunkt in die Datenbank gestellt (siehe 4.8.2). Wenn diese Option eingeschaltet ist wird in beiden Tabellen (`INTUSCOM_UPLOAD_BOOKINGS` und `INTUSCOM_UPLOAD_OTHER`) das Feld `TIME_STAMP` und `STATUS` benötigt.

Nach dem Eintrag in die Datenbank wird der Satz vom Terminal-Handler quittiert.

Satzverdopplungen

Wie auch beim Upload in die Dateischnittstelle versucht der Terminal-Handler Satzverdopplungen zu vermeiden. Wenn ein gesicherter Satz empfangen wird, wird verglichen, ob der unmittelbar vorher vom selben Terminal empfangene gesicherte Satz dieselbe Satznummer hatte. Wenn das der Fall ist, wird der Satz nicht noch einmal an die Datenbank übergeben.

Da die Satznummer des letzten gesicherten Satzes nicht persistent gespeichert wird, funktioniert dieser Mechanismus nicht, wenn der Terminal-Handler zwischenzeitlich beendet und neu gestartet wurde. Datenverdopplung ist also nicht hundertprozentig auszuschließen.

6.4.3.1 INTUSCOM_UPLOAD_BOOKINGS - Buchungssätze

Die Buchungstabelle **INTUSCOM_UPLOAD_BOOKINGS** hat folgenden Aufbau:

Feld	Typ	TPI-Feld	Beschreibung
SERVER_ID	char(2)	--	Server-ID
TERMINAL_ID	char(2)	--	Terminal-ID
SUB_TERMINAL_ID	char(2)	<TA>	Subterminal ID 00 bis 16
RECORD_TYPE	char(2)	<SA>	Satzart
CLIENT	char(10)	--	Mandant
COMPANY_CODE	char(10)	01	Firmenkennung
TIMEID_NO	char(10)	02	Kartennummer (Ausweis-ID)
BOOKING_DATE	char(8)	03	Buchungsdatum
BOOKING_TIME	char(6)	04	Buchungszeit
ERROR_STATUS	char(1)	05	Fehlerkennung
ATTENDANCE_STATUS	char(1)	06	Anwesenheitsstatus (K/G-Status)
PIN_CODE	char(6)	07	Pin
EXTRA_DATA	char(200)	--	Zusatzdaten aus frei definierbaren Funktions-schrittwerten
FINGER_STATUS	char(1)	09	Fingerstatus aus dem Buchungssatz
FINGER_ID	char(1)	10	Finger-ID aus dem Buchungssatz
TEMPLATES_ID	char(8)	11	Templates-ID aus dem Buchungssatz
DAYLIGHT_SAVING_TIME	char(1)	12	Zeitzone des Terminals ist in Sommerzeit (1/0)
ONLINE_TRANSACTION_D ATA	char(4)	13	Online-Transaktionskennung aus dem Bu-chungssatz
RETENTION	char(1)	14	Ausweis wurde eingezogen (J/N)
TIME_DIFFERENCE	char(5)	15	UTC Zeitzonenabweichung der Winterzeit (min +/-xxxx)
STATUS	char(1)	--	Gültigkeitsstatus
TIME_STAMP	Zeitstem-pel	--	Datum und Zeit, zu der der Satz in die Daten-base geschrieben wurde

Tabelle 6.19 – Die Buchungstabelle INTUSCOM_UPLOAD_BOOKINGS

Für alle Felder mit einem Eintrag in der Spalte **TPI-Feldtyp** gibt es ein analoges Feld in den TPI-Buchungssätzen. Der Aufbau (Feldtypen und Feldreihenfolge) der TPI-Buchungssätze wird im TPI-Parametersatz AB1 festgelegt. Der Terminal-Handler verwendet zur Zerlegung der Buchungssätze die Felddefinitionen aus dem AB1-Satz (siehe auch TPI Handbuch Kap. 5.6.1).

SERVER_ID und **TERMINAL_ID** sind durch INTUS COM definiert.

SUB_TERMINAL_ID entspricht der Terminaladresse im TPI-Rahmen.

RECORD_TYPE entspricht der TPI-Buchungssatzart.

In das Feld **CLIENT** wird im Mehrmandantenmodus der Mandant eingetragen.

In das Feld **EXTRA_DATA** werden die Daten aus den benutzerdefinierten Funktionsschritten ein-getragen (siehe TPI-Handbuch, Kapitel 5.6.12.2).

In die Felder `TIME_STAMP` und `STATUS` werden vom Terminal-Handler optional der Zeitpunkt des Uploads und „v“ (valid) eingetragen.

6.4.3.2 INTUSCOM_UPLOAD_OTHER - Alarme und Meldungen

In diese Tabelle werden alle TPI Alarmsätze geschrieben (IA, ID, IF, IP, siehe TPI Handbuch). Die Tabelle `INTUSCOM_UPLOAD_OTHER` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>SERVER_ID</code>	char(2)	Server-ID
<code>TERMINAL_ID</code>	char(2)	Terminal-ID
<code>SUB_TERMINAL_ID</code>	char(2)	Subterminal-ID 00 bis 16
<code>RECORD_TYPE</code>	char(2)	Satzart
<code>DATA</code>	char(35)	Datenteil des Satzes
<code>STATUS</code>	char(1)	Gültigkeitsstatus
<code>TIME_STAMP</code>	Zeitstempel	Datum und Zeit, zu der der Satz in die Datenbank geschrieben wurde

Tabelle 6.20 – Die Tabelle INTUSCOM_UPLOAD_OTHER

`SERVER_ID` und `TERMINAL_ID` sind durch INTUS COM definiert.

`SUB_TERMINAL_ID` entspricht der Terminaladresse im TPI-Rahmen.

`RECORD_TYPE` entspricht der TPI-Satzart.

Das Feld `DATA` entspricht dem Datenanteil des TPI-Satzes.

In die Felder `TIME_STAMP` und `STATUS` werden optional der Zeitpunkt des Uploads und „v“ (valid) eingetragen.

6.4.4 INTUSCOM_TERMINALS Terminal-Konfiguration

Damit die Applikation Profile in die Datenbank stellen kann, benötigt sie i. A. Informationen über die Terminal-Konfiguration, d. h. welche Terminals existieren und welche IDs ihnen zugeordnet sind.

Diese Informationen können von INTUS COM in der Tabelle `INTUSCOM_TERMINALS` bereitgestellt werden (zur Konfiguration dieser Funktion siehe 4.8.2)

Die Tabelle `INTUSCOM_TERMINALS` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>SERVER_ID</code>	char(2)	Server-ID
<code>TERMINAL_ID</code>	char(2)	Terminal-ID
<code>SUB_TERMINAL_ID</code>	char(2)	Subterminal-ID 00 bis 16
<code>LOCATION</code>	char(100)	konfigurierter Standort
<code>HARDWARE_TYPE</code>	char(4)	Gerätetyp
<code>SOFTWARE_TYPE</code>	char(3)	TCL/TPI
<code>CAMERA_COUNT</code>	char(1)	Anzahl der konfigurierten Kameras

Tabelle 6.21 – Die Tabelle INTUSCOM_TERMINALS

6.4.5 Die Fingerprint-Schnittstelle

Die Fingerprint-Schnittstelle von INTUS COM setzt die Verwendung der INTUS COM Datenbankschnittstelle voraus. Es werden folgende Tabellen verwendet.

Tabelle	Funktion	Applikation	INTUS COM
INTUS_FP_TEMPLATES_IDS	Bereitstellung der Stammdaten (Templates-IDs) durch die Applikation	schreibend, lesend	schreibend,lesend
INTUSCOM_TH_TEMPLATES	Templates zur Verteilung an die Terminals	lesend	schreibend, lesend
INTUS_FP_APP_TEMPLATES	Bereitstellung von Templates durch Applikation oder Einlernstation	schreibend, lesend	lesend
INTUSCOM_TIMESTAMPS	Steuerung der Synchronisation zwischen Applikation und TH	schreibend, lesend	schreibend,lesend

Tabelle 6.22 - Fingerprint - Tabellen

Unterstützte Terminaltypen

Derzeit werden folgende Fingerprint-Terminals unterstützt:

- INTUS 3100-FP
- INTUS 5300-FP
- INTUS 600 FP
- INTUS-FP

In den Terminals muss TPI-Tasc FP eingesetzt werden. Weitere Informationen zu Fingerprint finden Sie im TPI-Benutzerhandbuch, Kapitel 2.6.

Erforderliche Einstellungen im INTUS COM Client

- Im Terminal-Handler im Registerblatt Download muss die FP-Unterstützung aktiviert werden, siehe 4.8.4
- Im Terminal-Handler im Registerblatt Upload ist bei Upload an Applikation der Wert **gesicherte in Datenbank** auszuwählen.
- Bei einem FP-Terminal ist im Registerblatt FP-Unterstützung die FP-Unterstützung zu aktivieren, siehe 4.13.7.

6.4.5.1 Begriffsdefinitionen

Template

Die vom Sensor erfassten und rechnerisch reduzierten Daten eines Fingerabdrucks.

Templates-ID

8stellige (Personen-)Nummer, mit der Templates eindeutig einer Person zugeordnet werden .

Finger-ID

Einstellige Nummer von 0 – 9. Bezeichnung für die Finger von links nach rechts, beginnend mit dem kleinen Finger der linken Hand.

- 0. = kleiner Finger, linke Hand
- 1. = Ringfinger, linke Hand
- 2. = Mittelfinger, linke Hand
- 3. = Zeigefinger, linke Hand
- 4. = linker Daumen
- 5. = rechter Daumen
- 6. = Zeigefinger, rechte Hand
- 7. = Mittelfinger, rechte Hand
- 8. = Ringfinger, rechte Hand
- 9. = kleiner Finger, rechte Hand

Fingerstatus

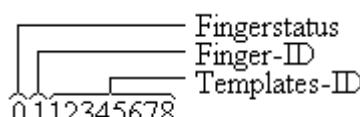
Einstelliger Status.

- 0 = Normalfinger
- 1 = Bedrohungsfinger
- 2 = Administratorfinger
- 3 = Administrator- und Bedrohungsfinger

User-ID

Eindeutige Nummer. Dezimal zusammengesetzt aus Fingerstatus, Finger-ID und Templates-ID.

Beispiel:



Fingerstatus = Normalfinger(0)
Finger-ID = Ringfinger, linke Hand (1)
Templates-ID = 12345678

6.4.5.2 Bereitstellen von Templates-IDs

Analog zu Ausweis-IDs bei Karten muss jeder Person, die sich per Fingerprint authentifizieren soll, eine eindeutige Templates-ID zugewiesen werden. Für die Vergabe von Templates-IDs ist die Applikation zuständig. Die Übergabe an INTUS COM erfolgt entweder direkt über die Tabelle INTUS_FP_TEMPLATE_IDS oder durch Bereitstellung einer Übergabedatei.

INTUS_FP_TEMPLATES_IDS - Datenbankschnittstelle

Die Tabelle INTUS_FP_TEMPLATES_IDS hat folgenden Aufbau:

Feld	Typ	Beschreibung
CLIENT	char(10)	Mandant
TEMPLATES_ID	char(8)	Templates-ID (numerisch)
SURNAME	nchar(40)	Familienname
FIRST_NAME	nchar(40)	Vorname
PERNO	char(20)	Personalnummer

Tabelle 6.23 – Die Tabelle INTUS FP TEMPLATES IDS

Um die Tabelle `INTUS_FP_TEMPLATES_IDS` als Übergabeschnittstelle zu verwenden muss auf dem Reiter **Biometrie** im Terminal-Handler als Schnittstelle **Datenbank** eingestellt sein.

Übergabedatei - Dateischnittstelle

Zur Übergabe der Templates-IDs durch die Applikation kann auch eine Übergabedatei verwendet werden. Um für die Übergabe der Templates-IDs die Dateischnittstelle zu verwenden, muss auf dem Reiter **Biometrie** im Terminal-Handler als Schnittstelle **Datei** eingestellt sein.

Beispiel Übergabedatei:

templates-id;surname;first-name;perno
00001234;Mustermann;Max;00000000000000000000000000000007
00001248;Mustermann;Hans;00000000000000000000000000000007

Bei der Übergabe der Datei ist folgendes zu beachten:

- Die Übergabedatei ist in dem Verzeichnis der Dateischnittstelle bereitzustellen.
 - Der Name der Übergabedatei muss **TI.csv** sein.
 - Die Übergabedatei ist von der Applikation stets durch Umbenennen bereitzustellen.
 - Die Übergabedatei wird nur für die Grundversorgung verwendet.
 - Die Übergabedatei wird nach der Übernahme durch INTUS COM aus der Schnittstelle entfernt.
 - Für die Übergabedatei ist das CSV-Format zu verwenden.
 - Zur Trennung der Felder in der Übergabedatei ist das Semikolon zu verwenden.
 - Die erste Zeile der Übergabedatei enthält die Feldnamen.

Soll ein Feldwert ein Semikolon oder Anführungszeichen enthalten, muss der Feldwert quoted werden.

Beispiel Quotieren von Sonderzeichen:

```
templates-id;surname;first-name;perno
00001234;“Dr.;Mustermann“;Max;00000000000000000000000000000007
00001248; ““Dr““;“Mustermann“““;Hans; 0000000000000000000000000000000753
```

Einlernen von Templates über die INTUS FP Einlernstation

Die INTUS FP Einlernstation liest diese Tabelle ein. Es können nur Finger für Personen eingelernt werden, deren Templates-ID in dieser Tabelle hinterlegt sind. Ab Version TPI 3.2 können Templates am Terminal nur eingelernt werden, wenn die Templates-ID in der Tabelle `INTUSCOM_MASTER_RECORDS` eingetragen ist.



Werden am Terminal Finger mit einer Templates-ID eingelernt, die nicht in der Tabelle `INTUS_FP_TEMPLATES_IDS` hinterlegt ist, werden diese vom Terminal-Handler wieder gelöscht!

Abläufe bei Datenänderung

Wenn die Applikation den Inhalt der Tabelle `INTUS_FP_TEMPLATES_IDS` geändert hat, muss sie den Zeitstempel für die `TABLE_ID TI` in der Tabelle `INTUSCOM_TIMESTAMPS` (siehe 6.4.2.2) aktualisieren, um INTUS COM darüber zu informieren.

Nachdem die Applikation neue Datensätze in diese Tabelle eingetragen hat, können Templates zu diesen neuen Templates-IDs eingelernt werden. Der Terminal-Handler trägt die neu eingelernten Templates in die Tabelle `INTUSCOM_TH_TEMPLATES` ein und lädt sie in die betroffenen Terminals.

Löscht die Applikation Datensätze aus dieser Tabelle, dann sendet der Terminal-Handler Löschsätze an alle betroffenen Terminals, um die zugehörigen Templates in den Terminals zu löschen. Anschließend werden auch alle zu dieser Templates-ID in der Tabelle `INTUSCOM_TH_TEMPLATES` gespeicherten Templates gelöscht.

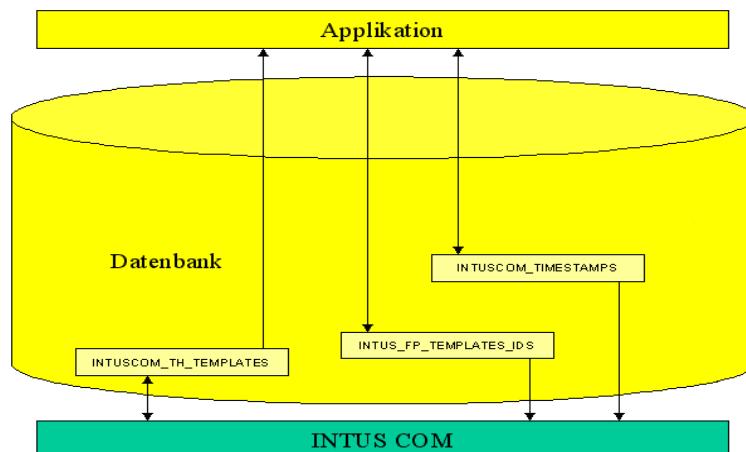


Abbildung 6.3 - Vergabe von Templates-IDs

6.4.5.3 INTUSCOM_TH_TEMPLATES - Verteilung der Templates

Die Tabelle `INTUSCOM_TH_TEMPLATES` enthält die Templates, die von INTUS COM auf die Terminals geladen werden. Sie werden vom Terminal-Handler entweder aus der Tabelle `INTUSCOM_FP_APP_TEMPLATES` übernommen oder durch ein Einlernereignis vom Terminal hochgeladen.



Der Terminal-Handler trägt nur Templates in diese Tabelle ein, wenn die Templates-ID in der Tabelle `INTUS_FP_TEMPLATES_IDS` definiert ist.

Die Tabelle `INTUSCOM_TH_TEMPLATES` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>FINGER_STATUS</code>	char(1)	Fingerstatus (0-3)
<code>FINGER_ID</code>	char(1)	Finger-ID (0-9)
<code>TEMPLATES_ID</code>	char(8)	Templates-ID, numerisch
<code>IMAGE_NO</code>	char(1)	Imagenummer
<code>TEMPLATE_DATA_1</code>	varchar(200)	Template-Daten
<code>TEMPLATE_DATA_2</code>	varchar(200)	hexadezimal dargestellt mit ASCII-Zeichen '0'-'9' und 'A'-'F'
<code>TEMPLATE_DATA_3</code>	varchar(200)	
<code>TEMPLATE_DATA_4</code>	varchar(200)	
<code>TEMPLATE_QUALITY</code>	char(3)	Qualität des Templates in % (000-100%)
<code>SERVER_ID</code>	char(2)	Server-ID, wenn an einem Terminal eingelernt, sonst --
<code>TERMINAL_ID</code>	char(2)	Terminal-ID, wenn an einem Terminal eingelernt, sonst --
<code>SUB_TERMINAL_ID</code>	char(2)	Subterminal-ID, wenn an einem Terminal eingelernt, sonst --
<code>SUPPLY_TIME_STAMP</code>	Zeitstempel	Datum und Zeit der Bereitstellung des Templates
<code>STATUS</code>	char(1)	,v' = valid ,i' = invalid
<code>TIME_STAMP</code>	Zeitstempel	Datum und Zeit, zu der der Satz in die Datenbank geschrieben wurde bzw. der letzten Aktualisierung

Tabelle 6.24 –Die Tabelle INTUSCOM_TH_TEMPLATES



Die Applikation darf nur lesend auf die Tabelle INTUSCOM_TH_TEMPLATES zugreifen.

Mit dieser Tabelle kann die Applikation z.B. Templates ermitteln die durch ein Einlernereignis von einem Terminal erzeugt wurden. Oder sie kann überprüfen, für welche Templates-IDs Templates existieren.

6.4.5.4 INTUS_FP_APP_TEMPLATES - Bereitstellen von Templates

Templates werden von der INTUS FP Einlernstation in der Tabelle `INTUS_FP_APP_TEMPLATES` bereitgestellt. Der Terminal-Handler übernimmt die Templates dann in die Tabelle `INTUSCOM_TH_TEMPLATES`.

Die Tabelle `INTUS_FP_APP_TEMPLATES` hat folgenden Aufbau:

Feld	Typ	Beschreibung
<code>FINGER_STATUS</code>	char(1)	Fingerstatus (0-3)
<code>FINGER_ID</code>	char(1)	Finger-ID (0-9)
<code>TEMPLATES_ID</code>	char(8)	Templates-ID, numerisch
<code>IMAGE_NO</code>	char(1)	numerisch
<code>TEMPLATE_DATA_1</code>	varchar(200)	Template-Daten
<code>TEMPLATE_DATA_2</code>	varchar(200)	hexadezimal dargestellt mit ASCII-Zeichen '0'-'9' und 'A'-'F'
<code>TEMPLATE_DATA_3</code>	varchar(200)	
<code>TEMPLATE_DATA_4</code>	varchar(200)	
<code>TEMPLATE_QUALITY</code>	char(3)	Qualität des Templates in % (000-100%)
<code>STATUS</code>	char(1)	,v' = valid ,i' = invalid
<code>TIME_STAMP</code>	Zeitstempel	Datum und Zeit, zu der der Satz in die Datenbank geschrieben wurde bzw. der letzten Aktualisierung

Tabelle 6.25 – Die Tabelle INTUS_FP_APP_TEMPLATES



Der eindeutige Schlüssel in dieser Tabelle sind die vier grau unterlegten Felder. Über jeden Satz wird dadurch ein Template eindeutig identifiziert. Für jeden Finger (USER-ID) können also mehrere Templates (Images) eingelernt werden, die durch das Feld `IMAGE_NO` indiziert sind.

Bereitstellung und Löschen von Templates

Neue Templates zu einer User-ID dürfen nur eingetragen werden, wenn die Templates-ID in der Tabelle `INTUS_FP_TEMPLATES_IDS` existiert. Dabei ist darauf zu achten, dass zu dieser User-ID

- der Bildindex `IMAGE_NO` lückenlos aufsteigend, beginnend bei '0', vergeben wird
- das Feld `STATUS` bei allen Sätzen den selben Wert hat
- das Feld `FINGER_STATUS` bei allen Sätzen den selben Wert hat; d. h. der Fingerstatus muss für jeden Finger eindeutig definiert sein.

Zu einer User-ID können nicht einzelne sondern nur alle Templates gelöscht werden:

Dazu müssen zuerst alle Datensätze einer User-ID bis auf den mit der `IMAGE_NO` '0' gelöscht werden. Dieser Datensatz muss dann mit dem Status `i` versehen und sein Wert für das Feld `TIME_STAMP` aktualisiert werden, um INTUS COM zu signalisieren, dass die Templates gelöscht werden sollen.

Die Einlernstation darf aus der Tabelle `INTUS_FP_APP_TEMPLATES` alle Datensätze löschen, die zu Templates-IDs gehören, die nicht (mehr) in der Tabelle `INTUS_FP_TEMPLATES_IDS` angegeben sind.

6.4.6 Die PS-Schnittstelle (PalmSecure)

Die PS-Schnittstelle von INTUS COM setzt den INTUSCOM PS-Distributor und die Verwendung der INTUS COM Datenbankschnittstelle voraus. Es werden folgende Tabellen verwendet.

Tabelle	Funktion	Applikation	INTUS COM
INTUS_FP_TEMPLATES_IDS	Bereitstellung der Stammdaten (Templates-IDs) durch die Applikation	schreibend, lesend	schreibend,lesend
INTUS_PS_TEMPLATES	Templates zur Verteilung an die PS-Controller	lesend	lesend
INTUSCOM_TIMESTAMPS	Steuerung der Synchronisation zwischen Applikation, Terminal-Handler und PS-Distributor	schreibend, lesend	schreibend,lesend
INTUS_PS_READERS	Bereitstellung von Informationen über die konfigurierten PS Leser	lesend	schreibend

Tabelle 6.26 – PS-Tabellen

Unterstützte Terminaltypen

Derzeit werden folgende PS-Geräte unterstützt:

- INTUS PS/INTUS 1600PS-II mit Tastatur
- INTUS PS/INTUS 1600PS-II ohne Tastatur

6.4.6.1 Begriffsdefinitionen

PS-Template

Die vom Sensor erfassten und rechnerisch reduzierten Daten eines Handvenenbildes.

Templates-ID

8stellige (Personen-)Nummer, mit der Templates eindeutig einer Person zugeordnet werden .

Palm-ID

Einstellige Nummer von 0 – 1. Bezeichnung für die Hand von links nach rechts, beginnend mit der linken Hand.

- 0 = linke Hand
1 = rechte Hand

Palmstatus

Einstelliger Status.

- 0 = Normalhand
1 = Bedrohungshand

PS-Controller

Steuereinheit für PS-Leseeinheit(en). Ein PS-Controller kann bis zu zwei Leseeinheiten mit Subterminaltyp „INTUS PS mit Tastatur“ oder „INTUS PS ohne Tastatur“ steuern. In INTUS COM werden die Steuereinheit und eine Leseeinheit über ein Subterminal abgebildet.

INTUSEnroll

Einlernprogramm für Handvenen-Templates (PS-Templates).

6.4.6.2 Bereitstellen von Templates-IDs

Die Bereitstellung der Templates-IDs für PS-Templates erfolgt analog zur Bereitstellung der Templates-IDs für Fingerprint-Templates (siehe 6.4.5.2).

6.4.6.3 INTUS_PS_TEMPLATES - Verteilung der Templates



Die Tabelle `INTUS_PS_TEMPLATES` enthält die Templates, die durch den INTUS COM PS-Distributor auf die PS-Controller geladen werden. Die Templates werden durch die Einlernsoftware INTUSEnroll in der Tabelle `INTUS_PS_TEMPLATES` bereitgestellt.

6.4.7 Die Videoschnittstelle

Die Anwenderschnittstelle zum INTUS COM VideoInterface setzt folgende Komponenten voraus:

- INTUS Terminals bzw. ACM
- INTUS COM Terminal Management System ab Version 2.8.0.
- INTUS COM Video-Interface (Die Verwendung des Video-Interface setzt eine geeignete INTUS COM Lizenz voraus.)
- Videoüberwachung mittels an Cayuga (SeeTec Gateway Service) angeschlossenen Kameras.

Das INTUS COM VideoInterface (im folgenden kurz als Video-Interface bezeichnet) ist eine Komponente von INTUS COM. Es integriert das Videoüberwachungssystem Cayuga in INTUS COM.

Die Videoüberwachungsschnittstelle von INTUS COM setzt die Verwendung der INTUS COM Datenbankschnittstelle voraus. Es werden folgende Tabellen verwendet:

Tabelle	Funktion	Applikation	INTUS COM
<code>INTUSCOM_VIDEO_PROFILES</code>	Bereitstellung der Videoprofile durch die Applikation	schreibend, lesend	lesend
<code>INTUSCOM_VIDEO_IMAGES</code>	Bereitstellung von Videobildern durch INTUS COM für die Applikation.	lesend	schreibend
<code>INTUSCOM_VIDEO_REQUESTS</code>	Wird INTUS COM intern verwendet		schreibend/lesend

Tabelle 6.27 – Videoüberwachung - Tabellen

6.4.7.1 INTUSCOM_VIDEO_IMAGES

Videobilder die durch die Videoüberwachung generiert wurden, werden der Applikation in der Tabelle INTUSCOM_VIDEO_IMAGES bereitgestellt.

Feld	Typ	Beschreibung
SERVER_ID	char(2)	Server-ID
TERMINAL_ID	char(2)	Terminal-ID
SUB_TERMINAL_ID	char(2)	Subterminal-ID (LBus-Adresse)
EVENT_DATE	char(8)	Datum des Ereignisses im Format yyyyymmdd
EVENT_TIME	char(6)	Uhrzeit des Ereignisses im Format hhmmss
EVENT_DAYLIGHT_SAVING_TIME	char(1)	Sommerzeitstatus des Ereignisses: 0: Winterzeit 1: Sommerzeit
EVENT_DATE_UTC	char(8)	Datum des Ereignisses in UTC-Zeit im Format yyyyymmdd
EVENT_TIME_UTC	char(6)	Uhrzeit des Ereignisses in UTC-Zeit im Format hhmmss
EVENT_CLASS	char(1)	Ereignisklasse: A: Alarmereignis (TPI-IA-Datensatz) B: Zeiterfassung Z: Zutritt
EVENT_TYPE	char(3)	Ereignistyp innerhalb der Ereignisklasse: Ereignisklasse A: 000: Gehäuse auf 004: Tür offen, berechtigt 006: Tür offen, unberechtigt 007: Tür zu lange auf 008: Wiederholung, Tür zu lange auf 00A: Stiller Alarm 00I: Türfreigabe durch Taster 00J: Türfreigabe durch Steuersatz Ereignisklassen B und Z: 000: erlaubte Buchung/Zutritt 001: abgelehnte Buchung/Zutritt
VIDEO_SERVER_ID	char(3)	Videoserver-ID
CAMERA_ID	char(3)	Kamera-ID
SEQUENCE_TYPE	char(1)	0: Vorereignisbild 1: Ereignisbild 2: Nachereignisbild
SEQUENCE_NO	char(2)	Nummer des Bildes innerhalb einer Sequenz
IMAGE_DATE	char(8)	Datum des Bildes im Format yyyyymmdd
IMAGE_TIME	char(6)	Uhrzeit des Bildes im Format hhmmss
IMAGE_DAYLIGHT_SAVING_TIME	char(1)	Sommerzeitstatus des Bildes: 0: Winterzeit 1: Sommerzeit
IMAGE_DATE_UTC	char(8)	Datum des Bildes in UTC-Zeit im Format yyyyymmdd
IMAGE_TIME_UTC	char(6)	Uhrzeit des Bildes in UTC-Zeit im Format hhmmss

Feld	Typ	Beschreibung
IMAGE_DATA	BLOB	Bildinformation im JPEG-Format
STATUS	char(1)	Gültigkeitsstatus (v: valid) Wird immer vom Video-Interface gesetzt
TIME_STAMP	Zeitstempel	Zeitpunkt, d.h. Datum und Uhrzeit, zu dem der Datensatz in die Datenbank gestellt oder zuletzt geändert wurde.

Tabelle 6.28 – Die Tabelle INTUSCOM_VIDEO_IMAGES

6.4.7.2 INTUSCOM_VIDEO_PROFILES

Durch die Verwendung von Videoprofilen können jedem einzelnen INTUS Terminal/ACM und Subterminal, dem Kameras in INTUS COM zugeordnet sind, Ereignisse zugeordnet werden, für die Videobilder erzeugt werden sollen. Videoprofile müssen durch die Applikation bereitgestellt werden.

Feld	Typ	Beschreibung
SERVER_ID	char(2)	Server-ID
TERMINAL_ID	char(2)	Terminal-ID
SUB_TERMINAL_ID	char(2)	Subterminal-ID (LBus-Adresse)
EVENT_CLASS	char(1)	Ereignisklasse: A: Alarmereignis (TPI-IA-Datensatz) B: Zeiterfassung Z: Zutritt
EVENT_TYPE	char(3)	Ereignistyp innerhalb der Ereignisklasse: Ereignisklasse A: 000: Gehäuse auf 004: Tür offen, berechtigt 006: Tür offen, unberechtigt 007: Tür zu lange auf 008: Wiederholung, Tür zu lange auf 00A: Stiller Alarm Ereignisklassen B und Z: 000: erlaubte Buchung/Zutritt 001: abgelehnte Buchung/Zutritt
PRE_EVENT_SECONDS	char(2)	Gewünschter Zeitbereich für Vorereignisbilder in Sekunden im Bereich von 00 bis 99.
PRE_EVENT_IMAGES	char(2)	Gewünschte Anzahl von Vorereignisbildern im Bereich von 00 bis 99.
POST_EVENT_SECONDS	char(2)	Gewünschter Zeitbereich für Nachereignisbilder in Sekunden im Bereich von 00 bis 99.
POST_EVENT_IMAGES	char(2)	Gewünschte Anzahl von Nachereignisbildern im Bereich von 00 bis 99.
FROM_TIME	char(4)	hhmm Gültigkeit, Beginn-Zeit
TO_TIME	char(4)	hhmm Gültigkeit, Ende-Zeit
SUNDAY	char(1)	J/N Gültigkeit Sonntag
MONDAY	char(1)	J/N Gültigkeit Montag
TUESDAY	char(1)	J/N Gültigkeit Dienstag

Feld	Typ	Beschreibung
WEDNESDAY	char(1)	J/N Gültigkeit Mittwoch
THURSDAY	char(1)	J/N Gültigkeit Donnerstag
FRIDAY	char(1)	J/N Gültigkeit Freitag
SATURDAY	char(1)	J/N Gültigkeit Samstag
SD_FLAG	char(1)	Sondertagsflag: 0 - Profilsatz gültig an Normaltagen 1 - Profilsatz gültig an Sondertagen
SD_GROUP	char(2)	Sondertagsgruppe
FROM_DATE	char(8)	Gültigkeitsbeginndatum (Datum des Tages vor dem der Datensatz ungültig ist) im Format YYYYMMDD oder '-----' für kein Gültigkeitsbeginndatum
TO_DATE	char(8)	Gültigkeitsendedatum (Datum des Tages, nach dem der Datensatz ungültig ist) im Format YYYYMMDD oder '-----' für kein Gültigkeitsendedatum

Tabelle 6.29 – Die Tabelle INTUSCOM_VIDEO_PROFILES

6.4.7.3 Systemarchitektur

Voraussetzung für den Einsatz von INTUS COM Video-Interface ist eine INTUS Terminal-Installation mit folgenden Komponenten

- INTUS Terminal/ACM
- INTUS COM Terminal Management System ab Version 2.8.0 mit Datenbank-Schnittstelle
- Videoüberwachung mittels Convision Videoservern oder SeeTec Gateway Service und den von diesen Videoservern / SAG unterstützten Kameras.

Das Video-Interface läuft als Dienst im Hintergrund und hat keine Bedienoberfläche. Für die Nutzung des Video-Interface ist eine Zusatzlizenz zur INTUS COM Lizenz erforderlich.

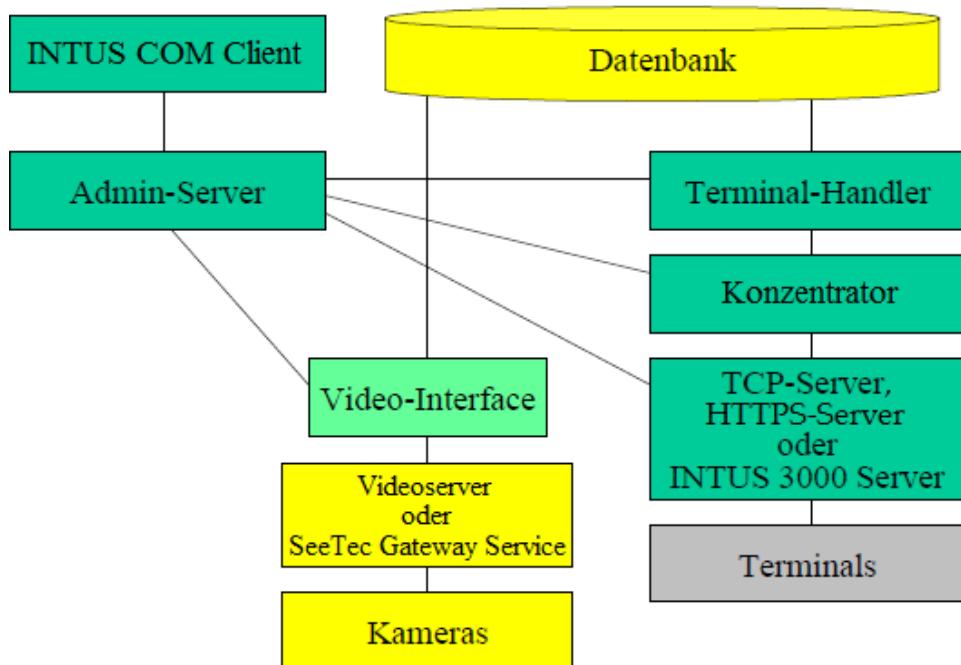


Abbildung 6.4 - Anbindung des INTUS COM Video-Interface

6.4.7.4 Arbeitsweise

Videobilder werden durch das Video-Interface in folgender Weise bereitgestellt:

1. Die Kamera sendet ständig Videobilder an den Videoserver/SeeTec zum Zwischenspeichern.
2. Das Terminal sendet einen Datensatz (zum Beispiel Zutrittsbuchung oder Alarmsatz)
3. Der Terminal-Handler bewertet den Datensatz, stellt aufgrund einer globale Einstellung oder über die Bewertung der Videoprofile fest, dass zu diesem Datensatz Videobilder angefordert werden sollen und stellt eine entsprechende Anforderung in die Tabelle INTUSCOM_VIDEO_REQUESTS.
4. Das Video-Interface erkennt die Anforderung und fordert daraufhin die Bilder über HTTP vom Videoserver/SeeTec an.
5. Der Videoserver/SeeTec sendet die angeforderten Bilder an das Video-Interface, das sie für die Applikation in der Tabelle INTUSCOM_VIDEO_IMAGES bereitstellt.

6.4.7.5 Beispiel Videoüberwachung mit globaler Ereigniseinstellung

Alternativ zu Convision Videoservern kann auch ein SeeTec Gateway Service verwendet werden. Welche Variante verwendet wird, wird durch die Lizenz festgelegt.

In der hier beschriebenen Konfiguration werden Videobilder, im Falle einer abgelehnten Bu-

chung am Terminal „intus-1“, vom Convision Videoserver „Videoserver-1“ durch das Video-Interface angefordert und in der Tabelle INTUSCOM_VIDEO_IMAGES bereitgestellt.

Vorbereitung

Einstellungen im Convision Videoserver

Um ein Kamera zu konfigurieren, melden Sie sich am Convision Videoserver mit Ihrem Benutzernamen und Passwort an.

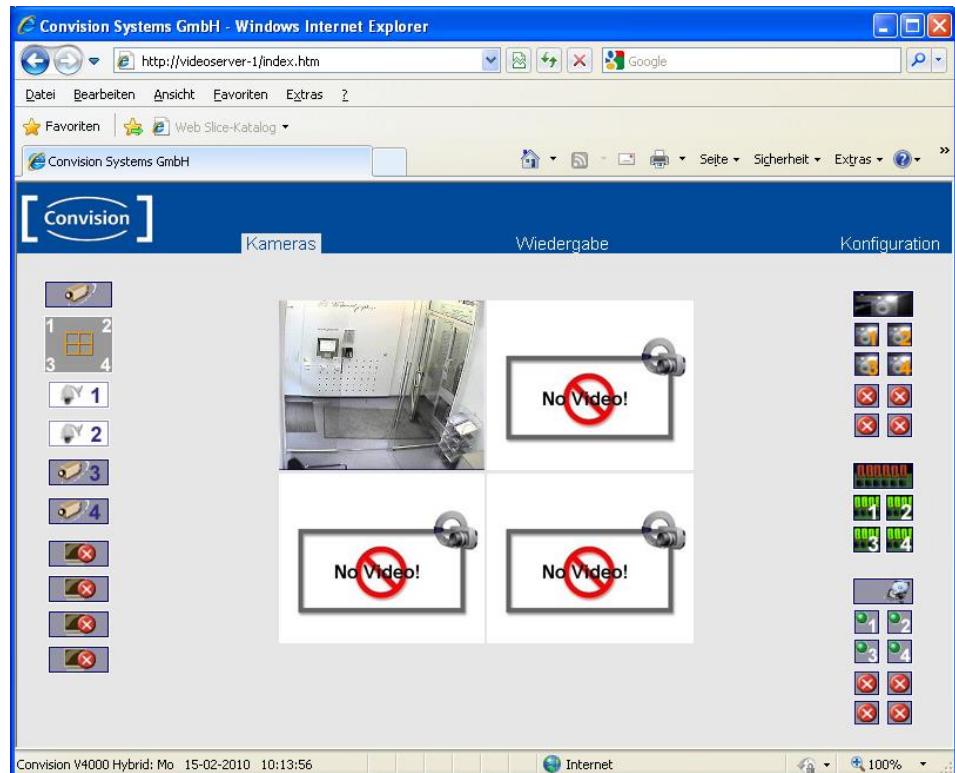


Abbildung 6.5 - Convision VideoServer, Startseite

Um die Videoüberwachung zu verwenden, muss mindestens eine Kamera im Videoserver konfiguriert sein.

Die Aufzeichnungsgeschwindigkeit des Videoservers muss hoch genug eingestellt sein, damit eine ausreichende Anzahl von Videobildern für das Video-Interface zur Verfügung stehen. Um die Aufzeichnungsgeschwindigkeit des Videoservers einzustellen, betätigen Sie die Schaltfläche Konfiguration (rechts oben). Auf der folgenden Seite wählen sie unter Aktionen die Option Aufnahme bei Ereignis beschleunigen um die Standardaufzeichnungsgeschwindigkeit einzustellen.

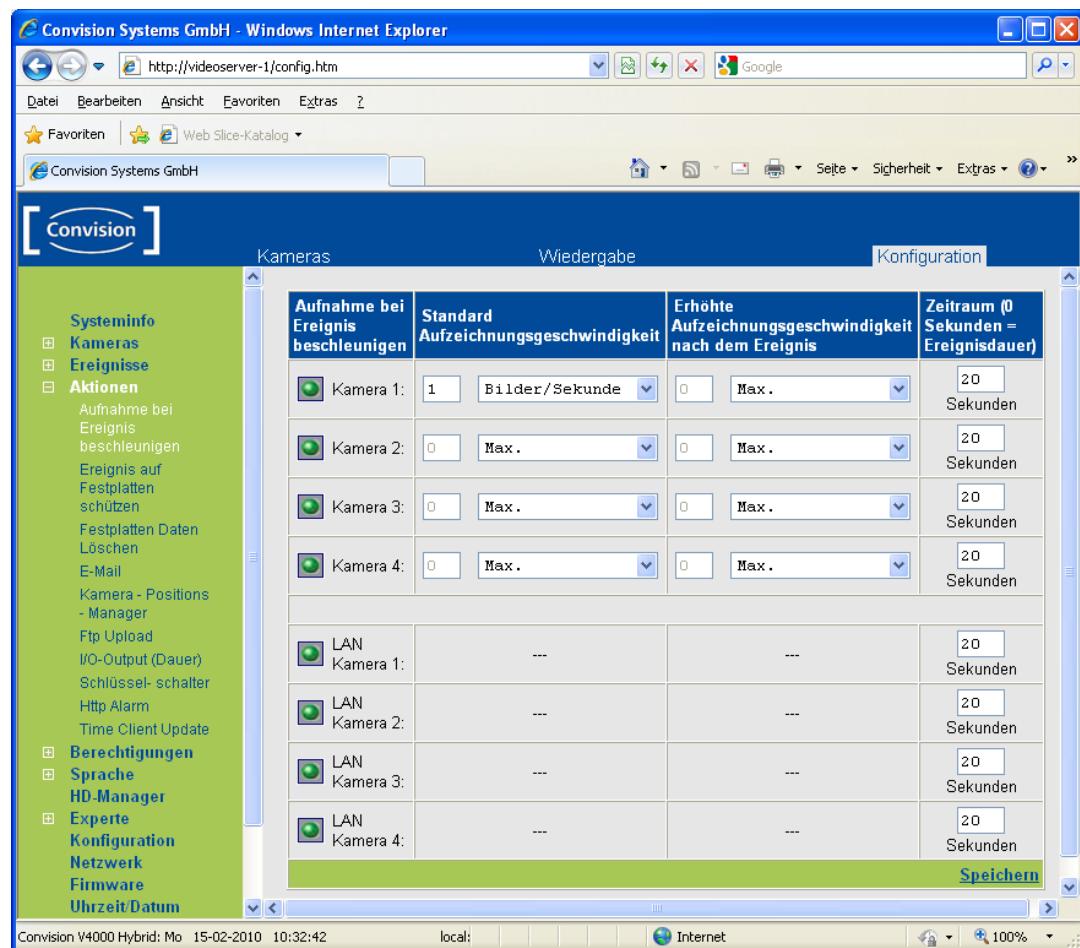


Abbildung 6.6 - Convision VideoServer, Aufnahmegeschwindigkeit einstellen

Um die Festplattenaufzeichnung zu starten wählen Sie im Konfigurationsmenü (links) die Option **HD-Manager** und wählen Sie auf der folgenden Seite **Aufnahme starten** aus.

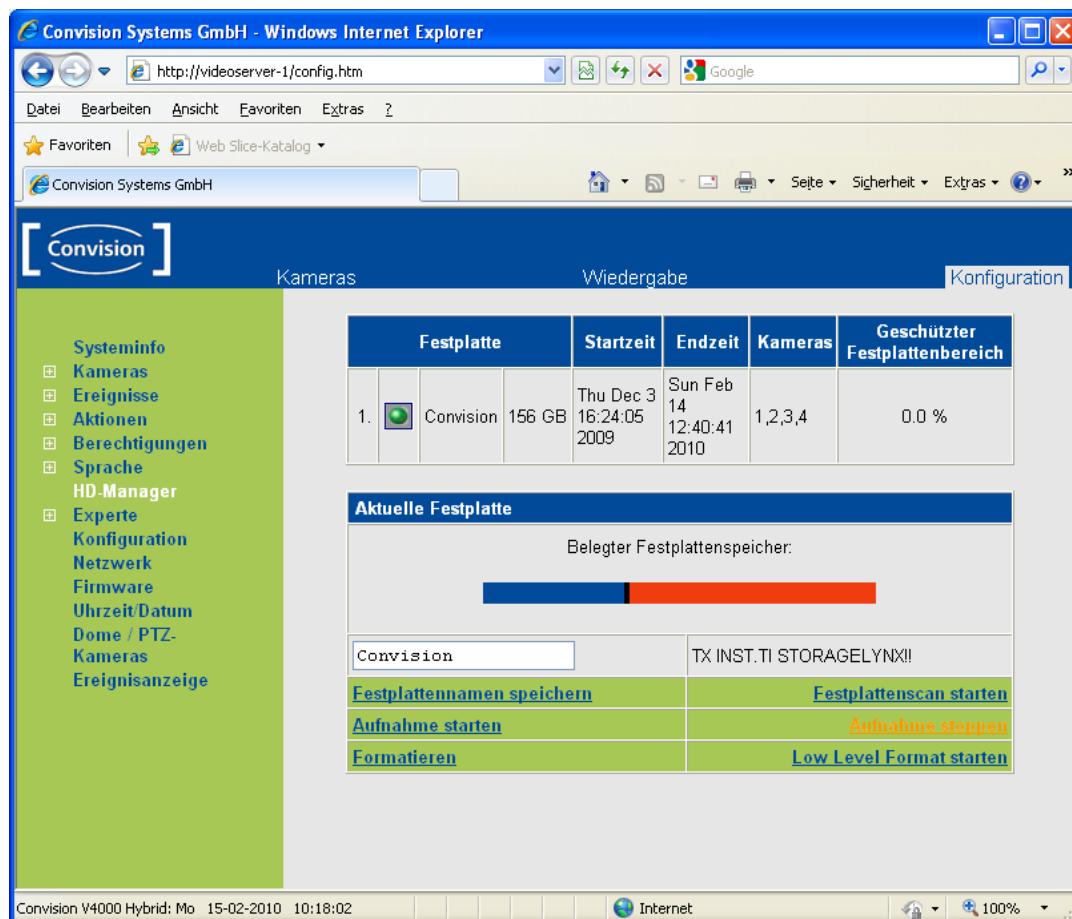


Abbildung 6.7 - Convision VideoServer, Aufnahme starten

6.4.7.6 Einstellungen in SeeTec



Alternativ zum SeeTec Gateway Service kann auch ein Convision Videoserver verwendet werden. Welche Variante verwendet wird, wird durch die Lizenz festgelegt.

Voraussetzungen

- SeeTec 5.3.9 Installation
- SeeTec Gateway Service

Starten Sie die SeeTec 5 Verwaltung über das Startmenü **Start->SeeTec->SeeTec Überwachung**. Wechseln Sie über das Menü **Datei** in den Kofigurationsmodus. Wählen Sie in der Administratorenicht **Hardware** aus. Auf der rechten Seite können Sie jetzt Videoquellen (z.B. IP-Kameras) hinzufügen und konfigurieren.



In INTUS COM können nur Kameras verwendet werden, die in SeeTec aktiviert sind und zu denen aktuell eine Vebindung besteht. Ist eine Kamera zwar in SeeTec aktiviert aber aktuell über das Netzwerk nicht erreichbar, wird dies in der SeeTec Überwachung mit einem Warnschild gekennzeichnet.

Auch wenn die Kamera aktiv ist und eine Verbindung besteht, kann es natürlich sein, dass keine Bilder vorhanden sind, z. B. wenn keine Standard- oder Alarmaufzeichnung für diese Kamera aktiviert ist.



Das SeeTec Gateway Service darf nicht in einer virtualisieren Umgebung (z.B. VMWare) installiert sein (siehe SeeTec Einsatzbedingungen).

Einstellungen im INTUS COM Client

Es muss zumindest ein INTUS Terminal angelegt und bereit sein. Die Zeiteinstellung des Terminals muss durch den Terminal-Handler mit einer Zeitzone aus der Konfigurationsdatei `time-zones.ini` erfolgen z.B: `utc-Zeitsynchronisation (MEZ)`.

Öffnen Sie über das Menü Fenster/Videokomponenten das Videokomponentenfenster.

Legen Sie über das Menü Neu/Video-Interface... das Video-Interface im INTUS COM Client an.

Stellen Sie auf dem Reiter Videobildanforderung in der K&S Maske des Video-Interface den Parameter Videobildanforderung auf gemäß der folgenden Einstellung und aktivieren sie das Auswahlfeld für abgelehnte Zeiterfassung.

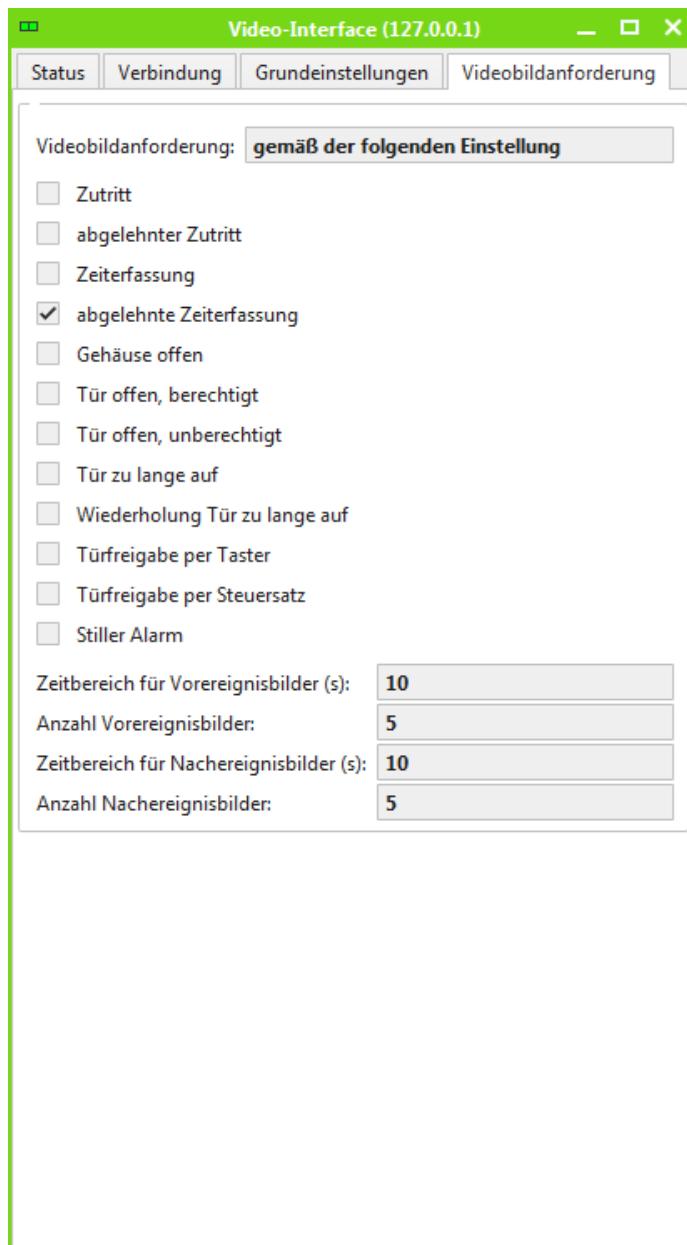


Abbildung 6.8 – Beispiel – Video-Interface Einstellungen

Legen Sie über das Menü Neu/videoserver... einen Videoserver bzw. ein SeeTec Gateway Service an.

Stellen Sie auf der K&S Maske des Videoserver/SeeTec Gateway Service die Adresse und die Anmelddaten des Videoserver/SeeTec Gateway Service ein.

Legen Sie über das Menü **Neu/Kamera...** eine Kamera an und stellen Sie als Server den gerade angelegten Videoserver ein. Die Kamera-ID muss der Konfiguration Ihres Videoservers entsprechen (Analogkamera 1 entspricht Kamera-ID A01).

Erstellen Sie über Menü **Neu/Kamera-Leser-Zuordnung...** eine Kamera-Leser-Zuordnung und stellen sie als Leser Ihr INTUS Terminal und als Kamera die gerade angelegte Kamera ein. Die Kamera-Leser-Zuordnung wird im Komponentenfenster unter dem Leser und im Videokomponentenfenster unter der Kamera angezeigt.

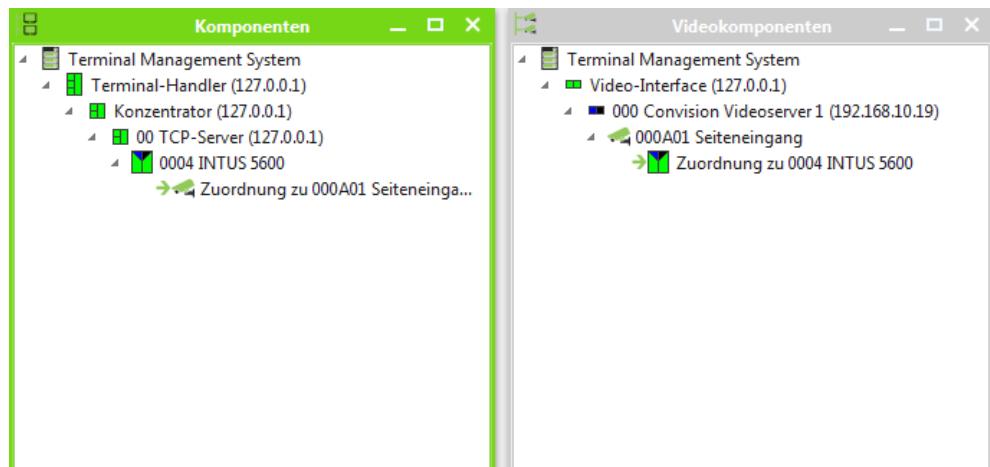


Abbildung 6.9 - Komponenten & Videokomponenten

6.4.7.7 Verwendung der Videoprofile

Videoprofile ermöglichen eine bessere Anpassung der Videoüberwachung als die globale Einstellung im vorangegangenen Beispiel. Mit Videoprofilen ist es zum Beispiel möglich, die Videoüberwachung auf einen bestimmten Zeitbereich zu beschränken, oder die auslösenden Ereignisse für jeden überwachten Leser getrennt zu konfigurieren. Videoprofile müssen durch die Applikation in der Tabelle INTUSCOM_VIDEO_PROFILES bereitgestellt werden (siehe 6.4.7.2).

6.4.8 LPR-Interface (Kennzeichenerkennungsschnittstelle)

Das INTUS COM LPR-Interface ermöglicht die Weiterverarbeitung von Kennzeichen, die durch die Cayuga Kennzeichenerkennung an INTUS COM übergeben werden. Aufgrund der erkannten Kennzeichen kann z.B. eine Schrankenöffnung durchgeführt werden.

Die Anwenderschnittstelle zum INTUS COM LPR-Interface setzt folgende Komponenten voraus:

3. Subleser bzw. Virtueller Leser an einem INTUS Terminal/ACM.
4. INTUS COM Terminal Management System ab Version 3.2.0.
5. Cayuga R14 und höher und Cayuga Kennzeichenerkennung.
6. Geeignete Kamera für die Kennzeichenerfassung.

Das LPR-Interface von INTUS COM setzt die Verwendung der INTUS COM Datenbankschnittstelle voraus. Es werden folgende Tabellen verwendet:

Tabelle	Funktion	Applikation	INTUS COM
INTUSCOM_LICENSE_PLATES	Bereitstellung von Kennzeichen für das INTUS COM LPR-Interface	schreibend, lesend	lesend
INTUS_LP_PROFILES	Bereitstellung von Kennzeichensprofilen für die räumlich/zeitliche Berechtigung	schreibend,lesend	lesend

6.4.8.1 INTUSCOM_LICENSE_PLATES

In der Tabelle INTUSCOM_LICENSE_PLATES werden die Kennzeichenstammdaten von der Applikation an INTUS COM übergeben. Die Felder COUNTRY_MODE,COUNTRY und LP_TEXT ergeben zusammen den eindeutigen Schlüssel.

Feld	Typ	Beschreibung
COUNTRY_MODE	char(1)	Modus für Landeskennung 0 – unvollständige Angabe 1 – vollständige Angabe
COUNTRY	char(3)	Landeskennung
LP_TEXT	char(20)	Kennzeichentext
LP_PROFILE_NO	char(3)	Kennzeichenprofil 000 – keine Kennzeichenprofilprüfung sonstiger Wert – Verweis auf Kennzeichenprofil
PERSON_ACCESS_CHECK	char(1)	Zusätzliche Personenberechtigungsprüfung 0 - nein 1 – ja 2 – profilabhängig
FROM_DATE	char(8)	Gültigkeitsbeginndatum im Format YYYYMMDD
FROM_TIME	char(4)	Gültigkeitsbeginnuhrzeit im Format hhmm
TO_DATE	char(8)	Gültigkeitsendedatum im Format YYYYMMDD
TO_TIME	char(4)	Gültigkeitsendeuhrzeit im Format hhmm

Modus für die Landeskennung (COUNTRY_MODE)

Der Modus für die Landeskennung legt fest, wie der als Landeskennung angegebene Wert auszuwerten ist.

Der Modus 0 bedeutet, dass der angegebene Wert nach Entfernung aller Leerzeichen an seinem Ende als unvollständiger Wert betrachtet wird. Dieser unvollständige Wert muss dann auf eine mit der Kennzeichenlesung gelieferten Landeskennung zutreffen, wenn diese mit dem unvollständigen Wert beginnt. Ein String mit der Länge 0 ist als unvollständiger Wert zulässig.

Der Modus 1 soll bedeuten, dass der angegebene Wert nach Entfernung aller Leerzeichen an seinem Ende als vollständiger Wert betrachtet wird. Dieser vollständige Wert muss dann auf eine mit der Kennzeichenlesung gelieferte Landeskennung zutreffen, wenn diese nach Entfernung aller Leerzeichen an ihrem Ende mit dem vollständigen Wert übereinstimmt. Ein String mit der Länge 0 ist als vollständiger Wert zulässig.

Die Beispiele in der folgenden Tabelle sollen die Bedeutung des Modus verdeutlichen:

Stammsatz Lesung vom SGS	Modus für Landeskennung	0	0	1	1	1
	Landeskennung		GER		GER	GER_OLEIMER
	Kennzeichentext	12345	12345	12345	12345	12345

Landeskennung	Kenn-zei-chen-text	Bedeutung		belie-bige Landes-ken-nung („ am Anfang)	Landes-ken-nung mit „GER“ am An-fang	keine bzw. leere Landes-ken-nung	Landes-ken-nung „GER“	Landes-kennung „GER_OLDTIMER“
		Bedeutung						
	12345	keine Landeskennung	zutref-fend	---	zutref-fend	---	---	---
GER	12345	<i>Landeskennung „GER“</i>	zutref-fend	zutref-fend	---	zutref-fend	---	---
GER_OLDTIMER	12345	<i>Landeskennung „GER_OLDTIMER“</i>	zutref-fend	zutref-fend	---	---	zutreffend	---
GER_SEASON	12345	<i>Landeskennung „GER_SEASON“</i>	zutref-fend	zutref-fend	---	---	---	---
AUT	12345	<i>Landeskennung „AUT“</i>	zutref-fend	---	---	---	---	---

6.4.8.2 INTUS_LP_PROFILES

In der Tabelle INTUS_LP_PROFILES werden die Kennzeichenprofile von der Applikation an INTUS COM übergeben.

Feld	Typ	Beschreibung
SERVER_ID	char(2)	Server-ID
TERMINAL_ID	char(2)	Terminal-ID
SUB_TERMINAL_ID	char(2)	Subterminal-ID
PROFILE_NO	char(3)	Kennzeichenprofilnummer ab 001
FROM_TIME	char(4)	Beginnahrzeit im Format hhmm
TO_TIME	char(4)	Endeuhrenzeit im Format hhmm
SUNDAY	char(1)	J/N Gültigkeitstag Sonntag
Monday	char(1)	J/N Gültigkeitstag Montag
TUESDAY	char(1)	J/N Gültigkeitstag Dienstag
WEDNESDAY	char(1)	J/N Gültigkeitstag Mittwoch
THURSDAY	char(1)	J/N Gültigkeitstag Donnerstag
FRIDAY	char(1)	J/N Gültigkeitstag Freitag
SATURDAY	char(1)	J/N Gültigkeitstag Samstag
SD_FLAG	char(1)	0/1 Sondertagsflag
SD_GROUP	char(2)	Sondertagsgruppe
PERSON_ACCESS_CHECK	char(1)	Zusätzliche Personenerichtigungsprüfung erfor-derlich 0 - nein 1 - ja
FROM_DATE	char(8)	Gültigkeitsbeginndatum im Format YYYYMMDD oder -----
TO_DATE	char(8)	Gültigkeitsendedatum im Format YYYYMMDD oder -----

6.4.8.3 Systemarchitektur

Voraussetzung für den Einsatz von INTUS COM LPR-Interface ist eine INTUS Terminal-Installation mit folgenden Komponenten

- Subleser an einem INTUS Terminal/ACM
- INTUS COM Terminal Management System ab Version 3.2.0 mit Datenbank-Schnittstelle
- SeeTec Cayuga R4 und SeeTec Kennzeichenerkennung und den von diesen unterstützten Kameras zur Kennzeichenerkennung.

Für die Nutzung des INTUS COM LPR-Interface ist eine Zusatzlizenz zur INTUS COM Lizenz erforderlich.

Das LPR-Interface ist in INTUS COM im Terminal-Handler realisiert. Als Gegensetze in SeeTec Cayuga R4 wird der SeeTec Gateway Service verwendet.

Für die Aufrufe an den SeeTec Gateway Service wird SSL/TLS eingesetzt. Für Rückrufe von SeeTec wird HTTP verwendet. Die Kommunikation zwischen INTUS COM und SeeTec sollte in einem geschützten Netzwerkbereich stattfinden.

Um über die Schnittstelle über Kennzeichenlesungen informiert zu werden, registriert sich der INTUS COM Terminal-Handler am SeeTec Gateway Service. Wird dann ein Kennzeichen in SeeTec gelesen, wird es dem INTUS COM Terminal-Handler übermittelt.

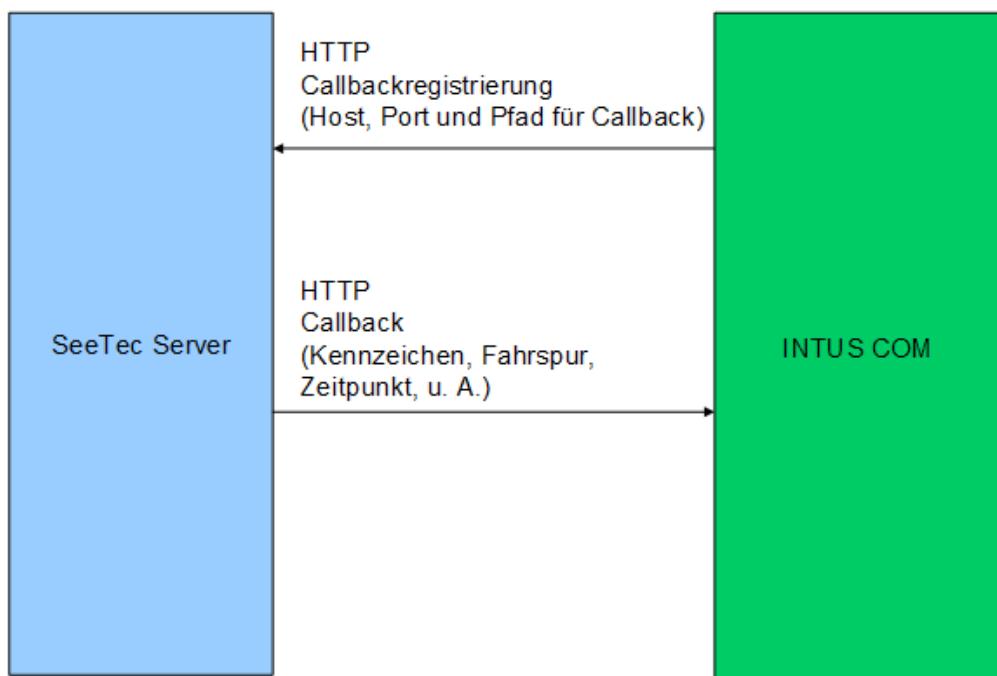


Abbildung 6.10 – LPR-Interface – Callbackregistrierung

Kennzeichen

Ein Kennzeichen wird über den Kennzeichentext oder über die Kombination von Landeskennung und Kennzeichentext repräsentiert. INTUS COM unterstützt beide Fälle. INTUS COM unterstützt jedoch nur Kennzeichentexte, die in Latin1 dargestellt werden können.

Fahrspur

In SeeTec erfolgt die Kennzeichenerkennung entlang einer sogenannten Fahrspur. In INTUS COM muss eine Fahrspur einem Subleser oder virtuellem Leser zugeordnet sein, um in INTUS COM verwendet werden zu können.

Berechtigungsprüfung

Eine Berechtigungsprüfung für ein übermitteltes Kennzeichen ist optional. Die Berechtigungsprüfung kann entweder in INTUS COM oder der Applikation durchgeführt werden, oder ganz entfallen.

Bereitstellung von Kennzeichen und Berechtigungen

Die Pflege der Kennzeichen für berechtigte Fahrzeuge, sowie deren zeitlichen und räumlichen Berechtigungen erfolgt in der Applikation und kann entweder über die Datenbankschnittstelle (INTUSCOM_LICENSE_PLATES, INTUS_LP_PROFILES) oder über CSV-Dateien (L1.csv, L2.csv) erfolgen.

Erkennung von Leerzeichen

In SeeTec kann eingestellt werden, ob Leerzeichen erkannt werden sollen. INTUS COM macht keine feste Vorgabe dazu. Aus Sicht von INTUS COM wird gefordert, dass im Projekt die Applikation und SeeTec sich hinsichtlich Leerzeichen in Kennzeichen einheitlich verhalten.

Wenn in SeeTec Leerzeichen erkannt werden, muss auch die Applikation die Leerzeichen in den berechtigten Kennzeichen angeben.

Wenn in SeeTec keine Leerzeichen erkannt werden, darf auch die Applikation keine Leerzeichen in den berechtigten Kennzeichen angeben.

Zeichensatz

INTUS COM macht keine Vorgabe zum Zeichensatz. Zu beachten ist die Einschränkung, dass nur Kennzeichen aus in Latin1 enthaltenen Zeichen unterstützt werden.

Ereignisgesteuerte Erkennung oder ständige Erkennung

In SeeTec kann eingestellt werden, ob für eine Fahrspur

- eine ereignisgesteuerte Erkennung oder
- eine ständige Erkennung

erfolgen soll.

Bei der ereignisgesteuerten Erkennung ist der Erkennungsvorgang durch ein Ereignis auszulösen. z. B. Die Kennzeichenerkennung wird gestartet wenn das Fahrzeug über eine Induktions schleife in der Fahrbahn erkannt wird.

Bei der ständigen Erkennung wird ständig eine Kennzeichenerkennung durchgeführt.

Für beide Fälle können in SeeTec weitere Parameter eingestellt werden.

INTUS COM macht keine Vorgabe, ob ereignisgesteuerte Erkennung oder ständige Erkennung zu verwenden ist oder wie die zugehörigen Parameter einzustellen sind.

6.4.8.4 Beispiel Kennzeichenerkennung mit Schrankensteuerung

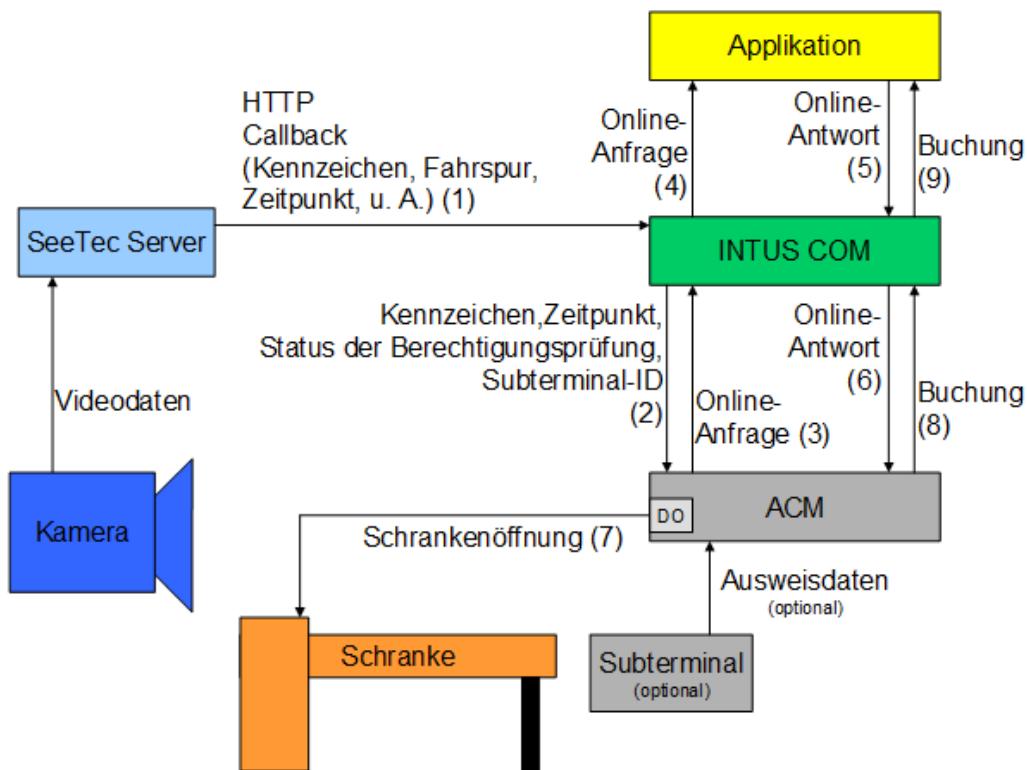


Abbildung 6.11 – Verarbeitungsablauf für gelesene Kennzeichen

1. INTUS COM nimmt ein erkanntes Kennzeichen über einen Callbackaufruf entgegen. Optional kann INTUS COM eine Berechtigungsprüfung für das erhaltene Kennzeichen durchführen. Das Ergebnis einer solchen Berechtigungsprüfung kann z.B. ergeben
 - a. dass das Kennzeichen nicht berechtigt ist
 - b. dass das Kennzeichen ohne zusätzliche Personenprüfung berechtigt ist oder
 - c. dass eine Personenprüfung zur Berechtigungsentscheidung benötigt wird.
2. INTUS COM schickt das Kennzeichen, den Zeitpunkt sowie das Ergebnis bzw. den Status der Berechtigungsprüfung aufbereitet an den ACM. Der ACM kann abhängig von der Parametrierung die gelieferten Daten mit dem vorläufigen Ergebnis einer Personenprüfung zusammenfassen.
3. Der ACM kann abhängig von der Parametrierung eine Online-Anfrage an INTUS COM senden.
4. Im Normalbetrieb wird diese Online-Anfrage an die Applikation weitergeleitet.
5. Antwort der Applikation auf eine Online-Anfrage
6. Antwort der Applikation wird von INTUS COM an den ACM weitergeleitet.
7. Abhängig vom Gesamtergebnis der Berechtigungsprüfung löst der ACM eine Schrankenöffnung aus oder nicht.
8. Optional wird ein Buchungssatz an INTUS COM gesendet.
9. Buchungssatz wird an Applikation übergeben.

6.5 Tabellenbasierte Dateischnittstelle (csv-Dateischnittstelle)

Die Verwendung der tabellenbasierten Dateischnittstelle setzt eine INTUS COM Datenbank der Version 3.1.0 voraus. Die Verwendung der tabellenbasierten Dateischnittstelle ist nur global im INTUS COM Terminal-Handler einstellbar.

Bei der tabellenbasierten Dateischnittstelle werden Daten über csv-Dateien an INTUS COM übergeben, und von INTUS COM in die Datenbank übernommen. Diese Schnittstelle ist nur für die Datenbanktabellen

- INTUS_FP_TEMPLATES_IDS
- INTUSCOM_MASTER_RECORDS
- INTUSCOM_PROFILES
- INTUSCOM_FUNCTION_PROFILES

verfügbar.

6.5.1 Dateiübergabe

Die Dateiübergabe erfolgt im Arbeitsverzeichnis des INTUS COM Terminal-Handler. Eine Übergabedatei muss von der Applikation stets durch Umbenennen bereitgestellt werden. Die Übergabedatei muss eine Grundversorgung enthalten. Eine Deltaversorgung über die tabellenbasierte Dateischnittstelle wird nicht unterstützt.

Wenn INTUS COM eine Übergabedatei bemerkt, übernimmt INTUS COM die enthaltenen Datensätze in die Datenbank. Nach Abschluss der Datenbanktransaktion benennt INTUS COM die Übergabedatei um, indem der Dateinamen um "_old" erweitert wird. Falls der daraus resultierende Dateiname bereits existiert, z.B. eine bereits übernommen Übergabedatei, wird diese Datei ersetzt.

Für die Dateiübergabe werden die folgenden Namen verwendet:

Daten	Tabelle	Übergabedatei	übernommene Übergabedatei
Stammsätze	INTUSCOM_MASTER_RECORDS	76.csv	76_old.csv
Zutrittsprofile	INTUSCOM_PROFILES	74Z.csv	74Z_old.csv
Buchungsprofile	INTUSCOM_PROFILES	74B.csv	74B_old.csv
Türprofile	INTUSCOM_PROFILES	74T.csv	74T_old.csv
Zeitliche Funktionssteuerung	INTUSCOM_FUNCTION_PROFILE S	74F.csv	74F_old.csv
Templates-IDs	INTUS_FP_TEMPLATES_IDS	TI.csv	TI_old.csv
Kennzeichenstammsätze	INTUSCOM_LICENSE_PLATES	L1.csv	L1_old.csv
Kennzeichenprofile	INTUSCOM_LP_PROFILES	L2.csv	L2_old.csv

6.5.2 Felder für die Übergabe von Stammsätzen

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung
client	Ja	Nein	Leer	10	Numerisch	Firmenkennung/Mandant
timeid-no	Ja	Ja	---	20	Numerisch	Ausweisnummer
access-profile-no	Nein	Nein	Leer	3	Numerisch	Zutrittsprofilnummer
booking-profile-no	Nein	Nein	Leer	3	Numerisch	Buchungsprofilnummer
authorisation-group	Nein	Nein	Leer	3	Numerisch	Berechtigungsgruppe
pin-code	Nein	Nein	Leer	6	Numerisch	Pincode
encrypted-pin-code	Nein	Nein	Leer	64	Text	Verschlüsselter Pincode
attendance-status	Nein	Nein	*	1	---	Anwesenheitsstatus
mail-no	Nein	Nein	Leer	2	Numerisch	Mailboxtextnummer
mail-counter	Nein	Nein	Leer	1	Numerisch	Mailboxtextzähler
info-field-1	Nein	Nein	Leer	13	Text	Saldo
info-field-2	Nein	Nein	Leer	13	Text	Saldo
info-field-3	Nein	Nein	Leer	13	Text	Saldo
info-field-4	Nein	Nein	Leer	13	Text	Saldo
info-field-5	Nein	Nein	Leer	13	Text	Saldo
info-field-6	Nein	Nein	Leer	13	Text	Saldo
info-field-7	Nein	Nein	Leer	13	Text	Saldo
info-field-8	Nein	Nein	Leer	13	Text	Saldo
info-field-9	Nein	Nein	Leer	13	Text	Saldo
info-field-10	Nein	Nein	Leer	13	Text	Saldo
room-no	Nein	Nein	Leer	3	Numerisch	Raumzonenummer
from-date	Nein	Nein	20000101	8	---	Datum Gültigkeitsbeginn im Format YYYYMMDD
to-date	Nein	Nein	21001231	8	---	Datum Gültigkeitsende im Format YYYYMMDD
from-time	Nein	Nein	0000	4	---	Uhrzeit Gültigkeitsbeginn im Format hhmm
to-time	Nein	Nein	2400	4	---	Uhrzeit Gültigkeitsende im Format hhmm
card-data	Nein	Nein	Leer	400	Text	Türterminalberechtigungsdaten
card-data-config	Nein	Nein	0197001010000----	17	---	Türterminalkonfiguration

templates-id	Nein	Nein	Leer	8	Numerisch	Templates-ID für Finger- print/PalmSecure
alternative-auth	Nein	Nein	Leer	1	Numerisch	Alternative Authentifizierung erlaubt ja/nein
alternative-auth-fp	Nein	Nein	Leer	1	Numerisch	Alternative Authentifizierung als Ersatz für Fingerprintken- nung erlaubt ja/nein
alternative-auth-ps	Nein	Nein	Leer	1	Numerisch	Alternative Authentifizierung als ersatz für Handvenenerken- nung erlauben ja/nein
name-field	Nein	Nein	Leer	40	Text	Namensfeld
country-and-language	Nein	Nein	DEU-deu	7	---	Länder-Sprachcode
record-disabled	Nein	Nein	N	1	---	Stammsatz (Ausweis) gesperrt ja/nein
retention-control	Nein	Nein	0	1	---	Ausweiseinzug 0-6
retention-from-date	Nein	Nein	20000101	8	---	Karenzzeit-Datum für Auswei- seinzug
retention-from-time	Nein	Nein	0000	4	---	Karenzzeit-Uhrzeit für Aus- weiseinzug

6.5.3 Felder für die Übergabe von Zutrittsprofilen

Feld-name	Schlüs- selfeld	Erfor- derlich	Default- wert	Länge	Füllmo- dus	Bemer- kung
server-id	Nein	Ja	---	2	---	Server-ID
terminal-id	Nein	Ja	---	2	---	Terminal-ID
sub-terminal-id	Nein	Ja	---	2	---	Subterminal-ID
profile-no	Nein	Ja	---	3	Numerisch	Profilnummer ab 001
from-time	Nein	Nein	0000	4	---	Beginnahrzeit im For- mat hhmm
to-time	Nein	Nein	2400	4	---	Endeuhrenzeit im Format hhmm
sunday	Nein	Nein	N	1	---	J/N Gültigkeitstag Sonntag
monday	Nein	Nein	N	1	---	J/N Gültigkeitstag Montag
tuesday	Nein	Nein	N	1	---	J/N Gültigkeitstag Dienstag
wednesday	Nein	Nein	N	1	---	J/N Gültigkeitstag Mitt- woch
thursday	Nein	Nein	N	1	---	J/N Gültigkeitstag Don- nerstag

6.5 - Tabellenbasierte Dateischnittstelle (csv-Dateischnittstelle)

friday	Nein	Nein	N	1	---	J/N Gültigkeitstag Freitag
saturday	Nein	Nein	N	1	---	J/N Gültigkeitstag Samstag
sd-flag	Nein	Nein	0	1	---	0/1 Sondertagsflag
sd-group	Nein	Nein	--	2	---	Sondertagsgruppe
pincode-flag	Nein	Nein	N	1	---	J/N Pincode erforderlich
buffer-authorised-bookings	Nein	Nein	N	1	---	J/N berechtigte Buchungen puffern
special-authorisation	Nein	Nein	N	1	---	J/N Sonderberechtigung
alternative-auth	Nein	Nein	N	1	---	J/N alternative Authentifizierung
toggle	Nein	Nein	0	1	---	0/1/2/3 Umschaltfunktion
from-date	Nein	Nein	-----	8	---	Gültigkeitsbeginndatum im Format YYYYMMDD oder -----
to-date	Nein	Nein	-----	8	---	Gültigkeitsendedatum im Format YYYYMMDD oder -----

6.5.4 Felder für die Übergaben von Buchungsprofilen

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung
server-id	Nein	Ja	---	2	---	Server-ID
terminal-id	Nein	Ja	---	2	---	Terminal-ID
sub-terminal-id	Nein	Ja	---	2	---	Subterminal-ID
profile-no	Nein	Ja	---	3	Numerisch	Profilnummer ab 001
from-time	Nein	Nein	0000	4	---	Beginnuzzeit im Format hhmm
to-time	Nein	Nein	2400	4	---	Endeuhzezeit im Format hhmm
sunday	Nein	Nein	N	1	---	J/N Gültigkeitstag Sonntag
monday	Nein	Nein	N	1	---	J/N Gültigkeitstag Montag

tuesday	Nein	Nein	N	1	---	J/N Gültigkeitstag Dienstag
wednesday	Nein	Nein	N	1	---	J/N Gültigkeitstag Mittwoch
thursday	Nein	Nein	N	1	---	J/N Gültigkeitstag Donnerstag
friday	Nein	Nein	N	1	---	J/N Gültigkeitstag Freitag
saturday	Nein	Nein	N	1	---	J/N Gültigkeitstag Samstag
sd-flag	Nein	Nein	0	1	---	0/1 Sondertagsflag
sd-group	Nein	Nein	--	2	---	Sondertagsgruppe
pincode-flag	Nein	Nein	N	1	---	J/N Pincode erforderlich
buffer-authorised-bookings	Nein	Nein	N	1	---	J/N berechtigte Buchungen puffern
special-authorisation	Nein	Nein	N	1	---	J/N Sonderberechtigung
alternative-auth	Nein	Nein	N	1	---	J/N alternative Authentifizierung
toggle	Nein	Nein	0	1	---	0/1/2/3 Umschaltfunktion
from-date	Nein	Nein	-----	8	---	Gültigkeitsbeginndatum im Format YYYYMMDD oder -----
to-date	Nein	Nein	-----	8	---	Gültigkeitsendedatum im Format YYYYMMDD oder -----

6.5.5 Felder für die Übergaben von Türprofilen

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung
server-id	Nein	Ja	---	2	---	Server-ID
terminal-id	Nein	Ja	---	2	---	Terminal-ID
sub-terminal-id	Nein	Ja	---	2	---	Subterminal-ID
from-time	Nein	Ja	---	4	---	Beginnurzeit im Format hhmm
to-time	Nein	Ja	---	4	---	Endeuhrenzeit im Format hhmm
sunday	Nein	Ja	---	1	---	J/N Gültigkeitstag Sonntag
monday	Nein	Ja	---	1	---	J/N Gültigkeitstag Montag
tuesday	Nein	Ja	---	1	---	J/N Gültigkeitstag Dienstag
wednesday	Nein	Ja	---	1	---	J/N Gültigkeitstag Mittwoch
thursday	Nein	Ja	---	1	---	J/N Gültigkeitstag Donnerstag
friday	Nein	Ja	---	1	---	J/N Gültigkeitstag Freitag
saturday	Nein	Ja	---	1	---	J/N Gültigkeitstag Samstag
sd-flag	Nein	Nein	0	1	---	0/1 Sondertagsflag
sd-group	Nein	Nein	--	2	---	Sondertagsgruppe
toggle	Nein	Nein	1	1	---	Umschaltfunktion
from-date	Nein	Nein	-----	8	---	Gültigkeitsbeginndatum im Format YYYYMMDD oder -----
to-date	Nein	Nein	-----	8	---	Gültigkeitsendedatum im Format YYYYMMDD oder -----

6.5.6 Felder für die Übergabe von Profilen zur zeitlichen Funktionsteuerung

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung
server-id	Nein	Ja	---	2	---	Server-ID
terminal-id	Nein	Ja	---	2	---	Terminal-ID
sub-terminal-id	Nein	Ja	---	2	---	Subterminal-ID
from-time	Nein	Ja	---	4	---	Beginnahrzeit im Format hhmm
to-time	Nein	Ja	---	4	---	Endeuhrenzeit im Format hhmm
sunday	Nein	Ja	---	1	---	J/N Gültigkeitstag Sonntag
monday	Nein	Ja	---	1	---	J/N Gültigkeitstag Montag
tuesday	Nein	Ja	---	1	---	J/N Gültigkeitstag Dienstag
wednesday	Nein	Ja	---	1	---	J/N Gültigkeitstag Mittwoch
thursday	Nein	Ja	---	1	---	J/N Gültigkeitstag Donnerstag
friday	Nein	Ja	---	1	---	J/N Gültigkeitstag Freitag
saturday	Nein	Ja	---	1	---	J/N Gültigkeitstag Samstag
sd-flag	Nein	Nein	0	1	---	0/1 Sondertagsflag
sd-group	Nein	Nein	--	2	---	Sondertagsgruppe
from-date	Nein	Nein	-----	8	---	Gültigkeitsbeginndatum im Format YYYYMMDD oder -----
to-date	Nein	Nein	-----	8	---	Gültigkeitsendedatum im Format YYYYMMDD oder -----

6.5.7 Felder für die Übergabe von Templates-IDs

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung

6.5 - Tabellenbasierte Dateischnittstelle (csv-Dateischnittstelle)

client	Nein	Nein	Leer	10	Numerisch	Mandant für IN-TUSEnroll
templates-id	Nein	Ja	---	8	Numerisch	Templates-ID
surname	Nein	Nein	Leer	40	Text	Nachname
first-name	Nein	Nein	Leer	40	Text	Vorname
pemo	Nein	Nein	leer	8	Numerisch	Personalnummer

6.5.8 Felder für die Übergabe von Kennzeichen

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung
country-mode	Ja- Bilden zusammen den eindeutigen Schlüssel	Nein	0	1	(entfällt)	Modus für Landeskennung: 0 – unvollständige Angabe 1 – vollständige Angabe
country-code		Nein	Leer	20	Text	Landeskennung
lp-text		Ja	Leer	20	Text	Kennzeichen
lp-profile-no	Nein	Nein	Leer	3	Numerisch	Kennzeichenprofil 000 – keine Kennzeichenprofilprüfung Sonstiger Wert – Verweis auf Kennzeichenprofil
person-access-check	Nein	Nein	0	1	entfällt	Bestimmt, ob eine zusätzliche Personenberechtigungsprüfung erfolgen soll 0 - nein 1 – ja 2 – profilabhängig
from-date	Nein	Nein	20000101	8	Entfällt	Gültigkeitsbeginndatum YYYYMMDD

from-time	Nein	Nein	0000	4	Entfällt	Gültigkeitsbeginnahrzeit hhmm
to-date	Nein	Nein	21001231	8	Entfällt	Gültigkeitsendeadatum YYYYMMDD
to-time	Nein	Nein	2400	4	Entfällt	Gültigkeitsendeahrzeit hhmm

6.5.9 Felder für die Übergabe von Kennzeichenprofilen

Feldname	Schlüsselfeld	Erforderlich	Defaultwert	Länge	Füllmodus	Bemerkung
server-id	Nein	Ja	Entfällt	2	Entfällt	Server-ID
terminal-id	Nein	Ja	Entfällt	2	Entfällt	Terminal-ID
sub-terminal-id	Nein	Ja	Entfällt	2	Entfällt	Subterminal-ID
profile-no	Nein	Ja	Entfällt	3	Numerisch	Kennzeichenprofilnummer ab 001
from-time	Nein	Ja	Entfällt	4	Entfällt	Beginnahrzeit im Format hhmm
to-time	Nein	Ja	Entfällt	4	Entfällt	Endeahrzeit im Format hhmm
sunday	Nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Sonntag
monday	Nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Montag
tuesday	nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Dienstag
wednesday	Nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Mittwoch
thursday	Nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Donnerstag
friday	Nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Freitag
saturday	Nein	Ja	Entfällt	1	Entfällt	J/N Gültigkeitstag Samstag
sd-flag	Nein	Nein	0	1	Entfällt	0/1 Sondertagsflag
sd-group	Nein	Nein	--	2	Entfällt	Sondertagsgruppe

6.5 - Tabellenbasierte Dateischnittstelle (csv-Dateischnittstelle)

person-access-check	Nein	Nein	0	1	Entfällt	Bestimmt, ob eine zusätzliche Personenberechtigungsprüfung erfolgen soll 0 – nein 1 – ja
from-date	Nein	Nein	-----	8	Entfällt	Gültigkeitsbeginndatum YYYYMMDD oder -----
to-date	Nein	Nein	-----	8	Entfällt	Gültigkeitsendendatum im Format YYYYMMDD oder -----

6.6 INTUS COM Konfigurationsdatei

INTUS COM legt die Terminalkonfiguration in einer XML-Datei ab. Über diese Datei kann die Applikation die Konfiguration, insbesondere die <Server-ID> und <Terminal-ID> der konfigurierten Server und Terminals einlesen.

Diese ist insbesondere für die Socket-Schnittstelle und die dynamische Dateischnittstelle relevant, da die Applikation hier die Terminaladresse (Server-ID, Terminal-ID) den Datensätzen voranstellen muss.

Die XML-Datei wird vom Admin-Server unter dem Namen `intuscom_conf.xml` im Verzeichnis `\conf` der INTUS COM Installation angelegt.

Die XML-Datei bildet den Baum der INTUS COM Komponenten (wie er im INTUS COM Client erscheint) ab. Dazu werden die XML-Tags ineinander verschachtelt. Z. B. ist das Subterminal im Terminal enthalten, dieses im Server, dieser im Konzentrator und dieser wiederum im Terminal-Handler. Verschiedene Parameter der Komponenten (z. B. Host und Port) werden als Tags angegeben, die den entsprechenden Parameterwert enthalten.

Beispiel 6.1 - INTUS COM Konfiguration in XML-Datei

```
<?xml version="1.0"?>
<intuscom>
  <terminal-handler>
    <host>127.0.0.1</host>
    <port>3040</port>
    <concentrator>
      <host>127.0.0.1</host>
      <port>3030</port>
      <TCP-Server>
        <host>127.0.0.1</host>
        <port>3020</port>
        <active>1</active>
        <id>00</id>
        <INTUS-3000-terminal>
          <host>INTUS02</host>
          <port>3000</port>
          <active>1</active>
          <id>05</id>
          <location>Eingang</location>
          <file72>i3300\72.tpi</file72>
          <file73>i3300\73.tpi</file73>
          <file76>i3300\76.tpi</file76>
          <file77>ttasc_205b.tcl</file77>
          <type>TPI</type>
          <sub-terminal>
            <active>1</active>
            <lbus-address>01</lbus-address>
            <location>Tuer 1</location>
            <sub-terminal-type>160f</sub-terminal-type>
            <file73>i3300\73_01.tpi</file73>
          </sub-terminal>
          <sub-terminal>
            <active>1</active>
            <lbus-address>02</lbus-address>
            <location>Tuer 2</location>
            <sub-terminal-type>162f</sub-terminal-type>
            <file73>i3300\73_01.tpi</file73>
          </sub-terminal>
        </INTUS-3000-terminal>
      </TCP-Server>
      <bsc-server>
        <host>127.0.0.1</host>
        <port>3001</port>
        <active>0</active>
        <id>43</id>
        <INTUS-1800-terminal>
```

```
<active>1</active>
<id>01</id>
<location>Kantine</location>
<file72>1800_tpi_1\72.tpi</file72>
<file73>1800_tpi_1\73.tpi</file73>
<file74>1800_tpi_1\74.tpi</file74>
<file75>1800_tpi_1\75.tpi</file75>
<file76>1800_tpi_1\76.tpi</file76>
</INTUS-1800-terminal>
</bsc-server>
<INTUS-3000-server>
<host>intserv01</host>
<port>3000</port>
<active>0</active>
<line1>
<id>10</id>
<INTUS-1800-terminal>
<active>1</active>
<id>01</id>
<location>???</location>
<file72>1800/72.tpi</file72>
<file73>1800/73.tpi</file73>
<file74>1800/74.tpi</file74>
<file75>1800/75.tpi</file75>
<file76>1800/76.tpi</file76>
</INTUS-1800-terminal>
</line1>
<line2>
<id>01</id>
<INTUS-3000-terminal>
<active>1</active>
<id>05</id>
<location>Eingang</location>
<file72>i3300\72.tpi</file72>
<file73>i3300\73.tpi</file73>
<file76>i3300\76.tpi</file76>
<file77>ttasc_202b.tcl</file77>
<type>TPI</type>
</INTUS-3000-terminal>
</line2>
</INTUS-3000-server>
</concentrator>
</terminal-handler>
</intuscom>
```


7 INTUS COM Konzept

7.1 Einsatz von INTUS COM ohne TPI

Sie können INTUS COM auch ohne TPI, d. h. mit einem anderen TCL-Programm einsetzen.

Dabei sind 2 Vorgehensweisen möglich:

1. Das Terminal wird im Terminal-Handler deaktiviert. Dann greift der Terminal-Handler nicht in die Kommunikation mit dem Terminal ein. In diesem Fall können Sie ein beliebiges Terminal-Programm einsetzen. Allerdings müssen Sie dann auf viele INTUS COM Funktionen wie Programm-Download, Buchungs-Upload in Datei (mit automatischer Quittierung), Uhrzeitsynchronisation, usw. verzichten.
2. Das Terminal wird als TCL-Terminal konfiguriert. Das TCL-Programm wird so angepasst, dass es mit dem Terminal-Handler zusammenarbeitet. Dann bietet Ihnen INTUS COM umfangreiche Funktionen wie Upload von Buchungen in Datei, Programm-Download, Stammdaten-Download, Uhrzeitsynchronisation usw.

Im folgenden sind die Anforderungen beschrieben, die im zweiten Fall an das TCL-Programm gemacht werden.

7.1.1 Anforderungen an das TCL-Programm

INTUS-Terminals senden automatisch die Ladeanforderung 77, wenn sie mit einem TCL-Programm geladen werden müssen. Sie fordern einen Programm-Download an.

Für TPI-Terminals wurde dieses Konzept dahingehend erweitert, dass auch andere Daten (Profile, Stammdaten usw.) vom Terminal angefordert werden können.

Wenn das Terminal komplett neu geladen wird, werden folgende Schritte durchlaufen:

1. Das Terminal fordert das TCL-Programm an. (Anforderung 77)
2. Der Terminal-Handler lädt das TCL-Programm auf das Terminal.
3. Das Terminal fordert die Systemkonfiguration an. (Anforderung 72)
4. Der Terminal-Handler lädt die Systemkonfiguration auf das Terminal.
5. Das Terminal fordert die Parameter an. (Anforderung 73)
6. Der Terminal-Handler lädt die Parameter auf das Terminal.
7. Das Terminal fordert die Funktionsschrittweite an (Anforderung 70)
8. Der Terminal-Handler lädt die Funktionsschrittweite auf das Terminal.
9. Das Terminal fordert die Sondertage an (Anforderung 71)
10. Der Terminal-Handler lädt die Sondertage auf das Terminal.
11. Das Terminal fordert die Profile an. (Anforderung 74)
12. Der Terminal-Handler lädt die Profile auf das Terminal.
13. Das Terminal fordert die Berechtigungsgruppen an. (Anforderung 75)
14. Der Terminal-Handler lädt die Berechtigungsgruppen auf das Terminal.
15. Das Terminal fordert die Stammdaten an. (Anforderung 76)
16. Der Terminal-Handler lädt die Stammdaten auf das Terminal.
17. Das Terminal ist jetzt vollständig geladen, es meldet dem Terminal-Handler, dass es betriebsbereit ist. (Bereit-Meldung 00)

Dabei können einzelne Anforderung auch entfallen. Wenn z. B. keine Profile benötigt werden, entfällt die entsprechende Anforderung. Einzig die abschließende Bereit-Meldung darf nicht entfallen.

Die Anforderungssätze sind für TCL-Terminals einfach zweistellige ASCII-Zahlen:

00 – betriebsbereit

72 bis 77 – Anforderung einer Downloaddatei

(Für TPI ist ein komplexerer Anforderungs-/Statussatz definiert.)

Das Terminal muss nach jedem Download einer statischen Downloaddatei von sich aus die nächste Anforderung oder die Bereit-Meldung schicken.

Außerdem muss das Terminal auf Anfrage entweder eine Anforderung oder eine Bereit-Meldung schicken. Diese Anfrage wird vom Terminal-Handler gesendet. Sie hat für TCL-Terminals folgendes Aussehen:

I@1023:

Der TCL-Interpreter führt also die Routine an Label 1023 aus. Diese Routine muss im TCL-Programm so implementiert sein, dass sie eine Ladeanforderung oder eine Bereit-Meldung sendet.

Die Forderung, dass nach einem Download aus einer statischen Downloaddatei das Terminal von sich aus eine Anforderung oder Bereit-Meldung schicken muss, kann dadurch erfüllt werden, dass die Downloaddatei als letzten Satz eine Statusanfrage enthält.

Nachfolgend ist ein Beispiel gegeben, das die Anforderungen des Terminal-Handler erfüllt. Im Beispiel werden nur ein TCL-Programm und eine Stammdaten-Datei verwendet.

Beispiel 7.1 - Beispiel für ein TCL-Programm mit Ladeanforderungen

```
IR,S:  
D! Beispielprogramm  
D! T,6 enthält die Anzahl der geladenen Stammsätze.  
D! TF enthält die Stammsätze.  
D! Ein Stammsatz besteht nur aus 4 Byte Ausweisnummer.  
D! In der Stammsatzdatei ist jedem Stammsatz ein J voranzustellen.  
D! Mindestens ein Stammsatz sollte enthalten sein.  
D! Am Ende der Stammdatendatei muss der Status gesendet werden.  
IK,'11',P20:  
IK,'000000',T,6:  
D#200:  
D! Hier steht der Hauptteil des Programms:  
DF,D,/D/, :  
DK,'Beispielprogramm für Terminal-Handler',D:  
DK,'KT      =' ,D[1]:K,KT,D[1]+11:A:  
DK,'UR      =' ,D[2]:K,UR,D[2]+11:A:  
DK,'Groesse NP=' ,D[3]:K,CV+5,ER+1:K,CV+107,ER,1:KW,258,ER,D[3]+11,1:  
DK,'Groesse TF=' ,D[4]:K,CV+6,ER+1:K,CV+108,ER,1:KW,258,ER,D[4]+11,1:  
D%300:  
D%400:  
DS:  
D! ----- :  
D! Karten einlesen und Buchungen senden :  
D#300:  
DE,(M,14-14Z,@310):  
D%:  
D#310:  
DPT,M+10,4,0,TF,(T,6),@320:  
DSE,M+10,4&' Stammsatz nicht gefunden':  
D@330:  
D#320:  
DSE,M+10,4&' Stammsatz gefunden':  
D#330:  
D%300:
```

```
DS:  
D! -----:  
D! Stammsätze empfangen :  
D#400:  
DRS,$7,4,@410:  
D%:  
D#410:  
DRD,$7,S:  
DP,EZ,<>'004',@420:  
DMU,(T,6),4:  
DK,S,TF+(ER,(EZ)),4:  
DI,T,6,0-999999:  
D#420:  
D%400:  
DS:  
D! -----:  
D! Sprungziel 0 erst hier, vermeidet Hochlaufen, wenn unvollständig:  
D#0:@200:  
D! -----:  
D! Statusabfrage ganz am Ende des Programms:  
D#1020:  
DP,T,'000000',@1021:  
D! wenn mindestens ein Stammsatz geladen -> bereit:  
DSR,'00':  
DS:  
D#1021:  
D! wenn kein Stammsatz geladen -> Anforderung Stammsätze:  
DSR,'76':  
DS:  
D#1023:@1020:  
D! -----:  
D! Programm starten und Status senden:  
I@0:  
I@1023:
```

Beispiel 7.2 - Beispiel für eine Stammdaten-Datei

```
J0001  
J0173  
I@1023:
```

7.2 Die Kommunikation zwischen den INTUS COM Komponenten

Die Kommunikation zwischen den INTUS COM Komponenten erfolgt über TCP/IP. Nur zwischen Server und Terminals kommt auch HTTPS oder BSC zum Einsatz.

Die einzelnen Komponenten stellen verschiedene Ports zur Kommunikation bereit.

7.2.1 Admin-Server

Zwischen dem INTUS COM Client und den anderen zu konfigurierenden Programmen, ist der Admin-Server geschaltet. Er verwaltet die Benutzer des INTUS COM, und deren Rechte. Jeder Benutzer, der über den INTUS COM Client auf das INTUS COM zugreifen will, muss sich mit seinem Benutzernamen und Passwort anmelden.

Der Admin-Server spielt im Hinblick auf die Konfiguration die zentrale Rolle in INTUS COM. Er speichert sämtliche Konfigurationsdaten, und konfiguriert mit diesen Daten die anderen Programme. So wird sichergestellt, dass die Konfigurationsdaten der anderen Programme untereinander konsistent sind.

7.2.2 Der Datenport

Der Datenport ist der Port einer INTUS COM Komponente, über den Datensätze gesendet und empfangen werden, die für ein Terminal bestimmt sind oder von einem Terminal erzeugt wurden.

Der Datenstrom von der Applikation zu den Terminals wird durch Konzentrator und Server aufgeteilt. Jeder Datensatz im Datenstrom wird nur an das Terminal weitergeleitet, für das er bestimmt ist. Dazu wird jedem Datensatz eine Server-ID und eine Terminal-ID vorangestellt. Ein Datensatz hat folgenden allgemeinen Aufbau:

<Server-ID><Terminal-ID><Daten><CR>

Feld	Erläuterung
Server-ID	zweistellige Server-ID
Terminal-ID	zweistellige Terminal-ID
Daten	der eigentliche Inhalt des Datensatzes
CR	ein Carriage-Return kennzeichnet das Ende des Datensatzes

Der Konzentrator teilt den Datenstrom anhand der Server-ID auf die einzelnen Server auf. Der Server teilt den Datenstrom anhand der Terminal-ID auf die einzelnen Terminals auf. Server- und Terminal-ID werden vom Server entfernt. D. h. das Terminal erhält nur die Daten und das CR.

In umgekehrter Richtung sendet das Terminal nur die eigentlichen Daten und das CR. Der Server setzt Server-ID und Terminal-ID davor. Damit haben die Sätze vom Terminal in Richtung Applikation denselben Aufbau, und die Applikation kann feststellen, von welchem Terminal der Satz stammt.

7.2.3 Der Serviceport

Der Serviceport ermöglicht die Steuerung und die Konfiguration einer Komponente durch den Admin-Server.

Der Serviceport ist immer der Basisport einer Komponente. Außer beim HTTPS-Server ist die Port-Nummer des Datenports stets um eins höher als die des Serviceports. Beim HTTPS-Server können die Port-Nummern unabhängig voneinander eingestellt werden.

Terminals besitzen keinen Serviceport.

7.2.4 Der Admin-Datenport

Der Terminal-Handler verwendet den Admin-Datenport um Datensätze (Alarmmeldungen usw.) an den Admin-Server zu senden.

7.2.5 Portadressen

Von	Nach	Protokoll	Port	Beschreibung
INTUS COM Client	Admin-Server	TCP	13050	Clientport
Admin-Server	Terminal-Handler	TCP	3040	Serviceport
Admin-Server	Terminal-Handler	TCP	3042	Admin-Datenport (Serviceport + 2)
Admin-Server	Terminal	UDP	57005	Terminalsuche und Konfiguration
Admin-Server	SMTP-Server	TCP	25	Alarm- und Ereignismails
Admin-Server	Concentrator	TCP	3030	Serviceport
Admin-Server	TCP-Server	TCP	3020	Serviceport
Admin-Server	HTTPS-Server	TCP	13060	Serviceport
Admin-Server	Video-Interface	TCP	13070	Serviceport
Admin-Server	PS-Distributor	TCP	13090	Serviceport
Admin-Server	AutoClone Dienst	TCP	13010	Serviceport
Admin-Server	INTUS 3000/3450 Server	TCP	3001	Serviceport
Admin-Server	Terminal	TCP	80	Statusseite
Application	Terminal-Handler	TCP	3041	Datenport (Service port + 1)
Tcp-Server	Terminal	TCP	3001	
Terminal	HTTPS-Server	HTTPS	10443	
Terminal über Protokollumsetzer	HTTPS-Server	HTTP	10080	
Remote setup	Terminal	UDP	57005	Terminalsuche und Konfiguration
Remote setup	Terminal	UDP	48879	PS-Controller-Suche und Konfiguration
Remote setup	Terminal	UDP	69	Tftp
Html-Browser	Terminal	TCP	80	Statusseite
Terminal-Handler	Concentrator	TCP	3031	Datenport
Concentrator	TCP-Server	TCP	3021	Datenport
Concentrator	HTTPS-Server	TCP	13061	Datenport
Concentrator	INTUS 3000/3450 Server	TCP	3002	Datenport (line 0)
Concentrator	INTUS 3000/3450 Server	TCP	3003	Datenport (line 1)
Video-Interface	Videoserver	TCP	80	HTTP Schnittstelle
Video-Interface	SeeTec Gateway Service	TCP	62000	SOAP Schnittstelle

PS-Distributor	PS-Controller	TCP	3101	Datenport
AutoClone Dienst	AutoClone Terminal	TCP	3121	Datenport
AutoClone Terminal	AutoClone Dienst	TCP	13011	Datenport

Tabelle 7.1 -- INTUS COM Standardports

A. Anhang

A.1. Änderungsindex

A.1.1. Änderungsindex 3.6.0

INTUS COM Dienste und INTUS COM Client	<ul style="list-style-type: none"> - neu bei Terminal-Handler: <ul style="list-style-type: none"> - Update/Delete Logik für OSO_CARD_DATA_IDS - neu bei HTTPS-Server: <ul style="list-style-type: none"> - Unterstützung des CA-Zertifikatsdownloads
Datenbank	<ul style="list-style-type: none"> - Neue Felder STATUS und TIMESTAMP für INTUSCOM_OSO_CARD_DATA_IDS

A.1.2. Änderungsindex 3.5.0

INTUS COM Dienste und INTUS COM Client	<ul style="list-style-type: none"> - neue Arten von Objekten: <ul style="list-style-type: none"> - Offlineanlage - Offline Terminal - Blocklist - neu bei Terminal/ACM: <ul style="list-style-type: none"> - Offlineanlage, Offlineanlagen-ID - Kartendatendatei (Datei 69) - Übersteuerung für maximale Anzahl Einträge in: <ul style="list-style-type: none"> - Kartendatentabelle - OSO-Blocklisttabelle - neu bei Terminal-Handler: <ul style="list-style-type: none"> - Datenquelle für Kartendaten - neu beim Terminalimport: <ul style="list-style-type: none"> - file69 – Dateiname für Kartendaten - neu bei Berechtigung: <ul style="list-style-type: none"> - Änderungsrecht für die Offline Terminal Türgruppenliste - Aktualisierungsrecht für den Offline Terminal Status - Referenzierungsrecht für Offlineanlagen - Konfigurationsrecht für Offlineanlagen und die Blocklist - neu bei Verwaltungseinheit: <ul style="list-style-type: none"> - Offline-Terminal-Tür-ID-Bereiche - Unterstützung für neue Subterminal-Typen hinzugefügt: <ul style="list-style-type: none"> - OSDP-Leser ohne Tastatur - OSDP-Leser mit Tastatur - neues Fenster „Offlineanlagen“ - neue Downloads 68 und 69 - neue Funktionalitäten: <ul style="list-style-type: none"> - Konfiguration von Offlineterminals exportieren - Konfigurationsergebnisse für Offlineterminals importieren
Datenbank	<ul style="list-style-type: none"> - neue Tabelle INTUSCOM_CARD_DATA - neue Tabelle INTUSCOM_OSO_CARD_DATA_IDS

Dateischnittstelle	- neue Datei 69 für Kartendaten
--------------------	---------------------------------

A.1.3. Änderungsindex 3.4.1

Änderungen	Beschreibung
INTUS COM Dienste und INTUS COM Client	<ul style="list-style-type: none"> - neue Einstellung „Timeout Basiskommunikation“ und neue Statusparameter im K&S-Fenster für HTTPS-Server - neue Einstellung „Verschlüsselung“ im K&S-Fenster für Subterminals - neuer Reiter „Verschlüsselung“ im K&S-Fenster für PS-Distributor - Unterstützung für neue Subterminal-Typ hinzugefügt: <ul style="list-style-type: none"> - INTUS 800FP - verbesserte Darstellung und verbessertes Verhalten im K&S-Fenster bei der Neuanlage eines Terminals sowie Subterminals

A.1.4. Änderungsindex 3.4.0

Änderungen	Beschreibung
INTUS COM Dienste und INTUS COM Client	<ul style="list-style-type: none"> - neuer Dienst HTTPS-Server - K&S-Fenster für HTTPS-Server hinzugefügt - K&S-Fenster des INTUS Terminal/ACMs für über HTTPS-Server angebundene Terminals angepasst - Konfigurationsparameter "Seriennummer" für INTUS Terminal/ACMs und INTUS 3000 Server hinzugefügt - Unterstützung für neue Subterminal-Typen hinzugefügt: <ul style="list-style-type: none"> - INTUS 700 - INTUS 700 Pincode - INTUS LBus I/O Box - Sonderleser - Spezialleser (BPA9 Protokoll) - INTUS XT-1 - INTUS XT-Mini - Passwort-Eingaben werden bei Mausklick auf ein Auge als Text angezeigt - Übernahme der Seriennummer aus der Netzwerkterminalsuche für über TCP-Server angebundene Terminals und INTUS 3000 Server hinzugefügt - Übernahme der Seriennummer aus der Import-Datei beim Terminalimport - Für über Intus3000-Server angebundene Terminals wird der nicht verwendete Parameter "Terminalname/IP" nicht mehr angezeigt

A.1.5. Änderungsindex 3.3.0

Änderungen	Beschreibung
INTUS COM Dienste und INTUS COM Client	<ul style="list-style-type: none"> - Umbenennung INTUSCOM-Monitor in INTUS COM Client - geändertes Look&Feel, Look&Feel nicht mehr änderbar - Umbenennung des Konfigurationsparameter „Standort“ in „Name“

	<ul style="list-style-type: none"> - neues Berechtigungskonzept: - Lagepläne werden zu Verwaltungseinheiten - Benutzer werden Verwaltungseinheiten zugordnet. - "Terminal Management System" wird einer Verwaltungseinheit zugeordnet. - Berechtigungen werden nicht mehr beim Benutzer eingestellt. - Berechtigungsobjekte zum Einstellen von Berechtigungen - Ein Berechtigungsobjekt bezieht sich stets auf eine Verwaltungseinheit. - detailliertere Unterscheidungen hinsichtlich erlaubter Operationen - Rollen - Zuordnungen von Berechtigungsobjekten zu Rollen - Zuordnungen von Benutzern zu Rollen - Benutzerliste durch Benutzer-Rollen-Berechtigungen-Fenster (mit erweiterter Darstellung) ersetzt - eigener Objekttyp für vordefinierten Administratorbenutzer, für uneingeschränkte Administrationsberechtigung, für Administratorrolle - feste Zuordnung des Administratorbenutzers zu Administratorrolle, feste Zuordnung der uneingeschränkten Administrationsberechtigung zu Administratorrolle - Benutzer können gesperrt werden. Anmeldeversuche gesperrter Benutzer werden abgelehnt und protokolliert. - Berechtigungsänderungen werden auch für bereits laufende Sessions wirksam. - Rollen können mit Gültigkeit für die laufende Session aktiviert und deaktiviert werden. - für Verwaltungseinheiten außer der Wurzelverwaltungseinheit können Terminal-ID-Bereiche eingestellt werden, die festlegen, welche Terminal-IDs unterhalb der Verwaltungseinheit für Terminals, die über TCP-Server angebunden werden, erlaubt sind. - diverse neue Konfigurationsparameter, z. B. Konzentrator (TCP-Server), Video-Interface (Videoserver, SeeTec Gateway Service), ... - diverse neue Statusparameter, z. B. Server-ID (Terminals, Subterminals, Türen), Terminal-ID (Subterminal, Türen), Subterminal-ID (Türen), Videoserver-ID (Kamera), ... - Meldungen werden Objekten zugeordnet - INTUS COM Client kann nicht mehr bestimmte Anzahl von Meldungen anfordern sondern Meldungen für einen bestimmten Zeitraum oder bis zu einem bestimmten Alter. - neues Konzept für Emailversand - Unterstützung für neuen Subterminaltyp "061M" für INTUS 610 Moto - Kommando zur Statusaktualisierung ersetzt durch automatische Statusaktualisierung - Kommando zu Uhrzeitsynchronisation bezieht sich nur noch auf selektierte Terminals - neuer Modus für den Stammdatendownload („Datenbank ab v3.3.0 (Gesperzte Sätze)“)
--	--

	<ul style="list-style-type: none"> - Suche/Fehler-Fenster ersetzt Fehler-Fenster - Anzeige aller (ausser Zuordnungsobjekte) Objekte - verschiedene Sortiermöglichkeiten - mögliche Filterung von Objekten verschiedener Typen - mögliche Filterung von Objekten ohne Fehler
Datenbank	<ul style="list-style-type: none"> - Tabelle INTUSCOM_MASTER_RECORDS erweitert
csv-Dateischnittstelle	<ul style="list-style-type: none"> - Felder für die Übergabe von Stammdaten erweitert
Meldungen	<ul style="list-style-type: none"> - Meldungen im Format 1 statt 0

A.1.6. Änderungsindex 3.2.0

Änderungen	Beschreibung
INTUS COM and Monitor	<ul style="list-style-type: none"> - Anzeige des Sabotagekontaktstatus. - Unterstützung für die SeeTec Kennzeichenerkennung - Datenbank-Deadlockvermeidung - Einstellen von Timer-Parametern - Einstellen von Firmenkennungen - Wechsel von SeeTec Application Gateway zu SeeTec Gateway Service - Modem-Server-Unterstützung entfernt.
Datenbank	<p>Neue Tabellen:</p> <p>INTUSCOM_LICENCE_PLATES INTUS_PS_PROFILES INTUSCOM_LOCK_TABLE</p> <p>Geänderte Tabellen:</p> <p>INTUSCOM_UPLOAD_BOOKINGS + RETENTION + TIME_DIFFERENCE</p> <p>Neue Prozeduren:</p> <p>INTUSCOM_LOCK PROCEDURE</p>

A.1.7. Änderungsindex 3.1.2

Änderungen	Beschreibung
INTUS COM Dienste und Monitor	<ul style="list-style-type: none"> - Netzwerkterminalsuche um Broadcast erweitert. - Fehlerbehebungen.
Linux	Linuxversion wird nicht mehr unterstützt.
Releasemedium	Releasemedium umbenannt von "INTUSCOM / TPI CD" in "INTUS Software CD"

A.1.8. Änderungsindex 3.1.0

Änderungen	Beschreibung
Datenbank	<ul style="list-style-type: none"> - Tabelle INTUSCOM_UPLOAD_BOOKINGS erweitert - Tabelle INTUS_FP_TEMPLATES_IDS erweitert.

AutoClone	Neuer INTUS COM Dienst: AutoClone
-----------	-----------------------------------

A.1.9. Änderungsindex 3.0.0

Änderungen	Beschreibung
Datenbank	- Tabelle INTUSCOM_MASTER_RECORDS erweitert - Tabelle INTUSCOM_VIDEO_IMAGES erweitert. - Tabelle INTUSCOM_VIDEO_REQUESTS erweitert. - Tabelle INTUSCOM_UPLOAD_BOOKINGS erweitert - Tabelle INTUSCOM_PROFILES erweitert.
VideoInterface	Unterstützung für SeeTec Gateway Service
Alle Dienste	Unterstützung für IPV6
BSC-Server	Wird nicht mehr unterstützt.
INTUS 1800 Terminal	Wird nicht mehr unterstützt

A.1.10. Änderungsindex 2.10.0

Änderungen	Beschreibung
PS-Distributor 1.0.1	Logmeldungen verbessert
Datenbank	- Neue Tabelle INTUSCOM_FUNCTION_PROFILES - Tabelle INTUSCOM_MASTER_RECORDS erweitert
Reset	Neuer Terminal-Reset-Typ "Com-start"
VideoInterface	Bei globaler Einstellung jetzt Videobild für Türöffnung durch Taster und Steuersatz einstellbar
INTUSEnroll 1.1.0	Unterstützung für Verifikation and Template on card

A.1.11. Änderungsindex 2.9.0

Änderungen	Beschreibung
PS-Distributor 1.0.0	Der PS-Distributor verteilt PS-Templates auf die angeschlossenen PS-Controller (Subterminals vom Typ INTUS PS)
Datenbank erweitert	Neue Tabelle INTUS_PS_TEMPLATES
Fehlende Menüpunkte ergänzt	Beschreibung der Menüpunkte für Einzel- und Dauertüröffnung hinzugefügt.
Fehler behoben	Übergabedatei für Templates-ID muss TI.csv heissen.

A.1.12. Änderungsindex 2.8.0

Änderungen Server	Beschreibung
INTUS COM Client Anmelde-dialog	Über den AnmeldeDialog kann jetzt die Anzeigesprache geändert werden.

Video-Interface 2.0.0	Das Video-Interface 2.0.0 wird jetzt über den INTUS COM Client und den Admin-Server konfiguriert.
Datenbank erweitert	<ul style="list-style-type: none"> - Geänderte Spalte TIMEID_NO char(20) - Neue Spalte: DAYLIGHT_SAVING_TIME char(1) in INTUSCOM_UPLOAD_BOOKINGS - Neue Spalte: CAMERA_COUNT char(1) in INTUSCOM_TERMINALS - Neue Spalten: EVENT_DAYLIGHT_SAVING_TIME char(1), VIDEO_SERVER_ID char(3), CAMERA_ID char(3), EVENT_CLASS char(1), EVENT_TYPE char(3), IMAGE_DAYLIGHT_SAVING_TIME char(1), IMAGE_DATE char(8), IMAGE_TIME char(6) in INTUSCOM_VIDEO_IMAGES - Neue Tabelle INTUSCOM_VIDEO_PROFILES - Neue Tabelle INTUSCOM_VIDEO_REQUESTS
Neues Fenster: Videokomponenten	Neues Fenster für Videokomponenten: <ul style="list-style-type: none"> - Video-Interface - Video-Server - Kamera - Kamera-Leser-Zuordnung
Verbesserung der Uhrzeitsynchronisation	Alternativ zu festen Zeitpunkten, kann jetzt auch ein Zeitintervall für die Zeitsynchronisation durch den Terminal-Handler eingestellt werden.
Downloads planen	Terminaldownloads können jetzt auch zu einem konfigurierbaren Zeitpunkt durchgeführt werden.
Terminalstatusseite anzeigen	Im INTUS COM Client kann jetzt die Statusseite eines Terminals angefordert und angezeigt werden.
Zeitzonenunterstützung erweitert	Unterstützung für Zeitzonen ohne Sommer-/Winterzeitumstellung.
Unterstützte Datenbanken	Die Verwendung eines unbekannte Datenbanktyp durch INTUS COM wird nicht mehr grundsätzlich abgelehnt. D.h: Es wird nur noch eine Warnung im Logfile ausgegeben.
TEMPLATE_QUALITY	Der Terminal-Handler unterstützt jetzt das Feld TEMPLATE_QUALITY
Neue Meldungen zu TPI-IA-Sätzen	T = Fehler FW-Flash Speicher U = Fehler Speichererweiterung V = Terminal im Notbetrieb W = Terminal im Onlinebetrieb X = Tür geschlossen nach unberechtigt Y = Türöffnungsalarm Z = Türöffnungsalarm Ende
Satznummer bei gesichertem Download	Terminal-Handler verwendet jetzt das Präfix ,T' für die Satznummer.
Türfreigabe über INTUS COM	Über den INTUS COM Client und den Admin-Server kann jetzt eine Einzel- / und Dauerfreigabe einer Tür geschaltet werden.

Fingerprintheinlernergeignissatz	Der TPI-IE-Satz (Fingerprintheinlernereignissatz) wird beim Upload in die Datenbank in die Tabelle INTUSCOM_UPLOAD_OTHER gestellt.
Unterstützung für den SD-Statussatz.	Der SD-Statussatz kennzeichnet das beenden des Fingerprint-Einlern/Löschenmodus am Terminal.

A.1.13. Änderungsindex 2.7.0

Änderungen Server	Beschreibung
Subterminals	Deaktivierte Subterminals werden jetzt auch in die Datenbank exportiert.
Quittungstimeout	Standardwert für den Quittungstimeout auf 60s erhöht. (siehe Kap.: 4.8.1)
Terminalinitialisierung	Beim Einstellen des Terminalsetups für TPI-Terminals wird die Grösse des Tabellenfeldes nicht mehr auf 16 * 3072 Bytes sondern auf 24 * 3072 Bytes eingestellt.
Socket-Schnittstelle	TPI-Sätze mit Satznummer "*****" und der Satzart „T0“ bis „T9“, „TA“, „TB“, „TO“ und „TT“ werden jetzt auch während eines Downloads (ausser bei Download „77“, „72“ und „73“) auf ein TPI-Terminal, über die Socket-Schnittstelle weitergeleitet.
Fehler bei Batteriestatusabfrage behoben	Der Alarmcode für "Akku nicht voll" wurde fälschlicherweise als "Akku leer" bzw. "accumulator battery empty" übersetzt.
Fehler bei Template-Download behoben	Bei ausgeschalteter Templateunterstützung, aber eingeschalteter Templateübertragung im Terminal-Handler, konnte es dazu kommen das Fingerprint-Löschenereignisse nicht quittiert und nicht in die Datenbank geschrieben wurden.
Neue Subterminaltypen	Unterstützung für Subterminaltypen INTUS 600, INTUS 600 Pincode und INTUS 600 FP.
Stammdatendownload erweitert	Unterstützung für Feldtyp 22 in TPI-AB2-Satz. (siehe TPI-Handbuch Kap.: 5.6.2).
Stammdatendownload erweitert	Unterstützung für TPI-Y2-Satz. (siehe TPI-Handbuch Kap.: 5.1.25)
Türterminal-Batteriestatus	Gesicherte TPI-Sätze mit Satzart IP werden als Meldungen zum Batteriezustand von Türterminals betrachtet und beim Upload in die Datenbank in die Datenbanktabelle INTUSCOM_UPLOAD_OTHER gestellt.
Meldungen	Neue Meldungen für Terminal-Setupprüfung und Terminal-Setupänderung bei Download „77“.
Quittingscodes	Spezifische Übersetzungen für TPI-Quittingscodes 27, 28, 30, 31 und 32 in Meldungen. (siehe TPI-Handbuch Kap.: 4.2)
Terminalstatus	Register „Info“ auf K&S Fenster „INTUS Terminal/ACM“ um Feld für den Quittingscode erweitert.
Fingerprint-Ereignisse	Fingerprint-Einlern- und Löschenereignisse wirken sich jetzt auch auf den Templatestatus aus, wenn für den Upload gesicherter TPI-Sätze die Datei- oder Socketschnittstelle im Terminal-Handler eingestellt ist.

Dateischnittstelle für Templates-IDs	Auswahl der Schnittstelle für Templates-IDs: 0: Datenbankschnittstelle (Standard) 1: CSV-Dateischnittstelle (siehe Kap.: 4.8.4)
INTUS COM Client Anmeldungstimeout	Gelingt der Verbindungsaufbau zum Admin-Server nicht innerhalb von 5 Sekunden, wird ein Dialog angezeigt, der den Abbruch des Verbindungsversuch ermöglicht.
Bezeichnung geändert	„INTUS 3000 Terminal“ in „INTUS Terminal/ACM“ umbenannt.
De/aktivieren von Subterminals	Neuer Dialog um auf den Download „72“ nach dem de/aktivieren eines Subterminals hinzuweisen.
Datenbank erweitert	Neue Spalte TEMPLATE_QUALITY char(3) in den Tabellen INTUS_FP_APP_TEMPLATES und INTUSCOM_TH_TEMPLATES.
Update geändert	Update der Datenbanktabellen kann jetzt getrennt vom Update der Programmdateien durchgeführt werden. (siehe Kap.: 2.2)
Datenbank erweitert	Neue Spalte NAME_FIELD char(40) in Tabelle INTUSCOM_MASTER_RECORDS.
Datenbank geändert	Spalte PIN_CODE in INTUSCOM_MASTER_RECORDS und INTUSCOM_UPLOAD_BOOKINGS jetzt als char(6) definiert.

A.2. Lizenzbestimmungen

A.1.1. Lizenzbestimmungen der verwendeten Freien Software

INTUS COM enthält freie Software. Diese freie Software wurde von Dritten entwickelt und ist urheberrechtlich geschützt.

Diese freie Software wird unentgeltlich überlassen.

Sie sind berechtigt, diese freie Software gemäß deren Lizenzbedingungen zu nutzen. Bei Widersprüchen dieser Lizenzbedingungen zu den für die Software geltenden Lizenzbestimmungen der PCS Systemtechnik GmbH gehen für die freie Software deren Lizenzbestimmungen vor.

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

A.1.2. The OpenSSL Toolkit License

INTUS COM enthält freie Software, die unter der The OpenSSL Toolkit License lizenziert ist. Die The OpenSSL Toolkit License wird mit diesem Produkt mitgeliefert. Zusätzlich können Sie die Lizenzbestimmungen aus dem Internet herunterladen. Die The OpenSSL Toolkit License finden Sie im Internet unter <http://www.openssl.org>.

Im folgenden finden Sie den Lizenztext in der englischen Original-Fassung:

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the
OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, SHA, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

A.1.3. ISB/BSC License

INTUS COM enthält die freie Software jBcrypt, die unter der ISB/BSD License lizenziert ist.

Im folgenden finden Sie den Lizenztext in der englischen Original-Fassung:

jBCrypt is subject to the following license:

Copyright (c) 2006 Damien Miller

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY
DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,
ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

A.3. Tabellen und Verzeichnisse

A.1.4. Tabellenverzeichnis

Tabelle 2.1 – Secure-Dateien.....	37
Tabelle 3.1 – Meldungsanzeige im INTUS COM Client	57
Tabelle 5.1 – Allgemeine TCP/IP Verbindungsfehler	175
Tabelle 6.1 – Statische Downloaddateien; TPI-Ladeanforderungen.....	185
Tabelle 6.2 – INTUS COM Meldungsformat für Status, Fehler und Alarmmeldungen, Meldungsformat '1' und '2'.....	197
Tabelle 6.3 – Informationen zum Verbindungszustand	198
Tabelle 6.4 – Format für Informationen zur Uhrzeitsynchronisation.....	199
Tabelle 6.5 – Getestete Datenbanken.....	200
Tabelle 6.6 – Übersicht Datenbank-Tabellen	202
Tabelle 6.7 – Datentyp für Zeitstempel.....	203
Tabelle 6.8 – Datentyp für BinaryLarge Object (BLOB).....	203
Tabelle 6.9 – Datenbanktabellen für den Download.....	204
Tabelle 6.10 – Die Tabelle INTUSCOM_TIMESTAMPS	205
Tabelle 6.11 – Die Stammdatentabelle INTUSCOM_MASTER_RECORDS.....	207
Tabelle 6.12 – Die Tabelle INTUSCOM_OSO_CARD_DATA_IDS	210
Tabelle 6.13 – Die Profiltabelle INTUSCOM_PROFILES.....	213
Tabelle 6.14 – Die Profiltabelle INTUSCOM_FUNCTION_PROFILES	214
Tabelle 6.15 – Die Sondertagstabelle INTUSCOM_SPECIAL_DAYS	215
Tabelle 6.16 – Die Tabelle INTUSCOM_AUTHORISATION_GROUPS	215
Tabelle 6.17 – Die Tabelle INTUSCOM_FUNCTION_STEP_VALUES	215
Tabelle 6.18 – Die Tabelle INTUSCOM_CARD_DATA	218
Tabelle 6.19 – Die Buchungstabellen INTUSCOM_UPLOAD_BOOKINGS	220
Tabelle 6.20 – Die Tabelle INTUSCOM_UPLOAD_OTHER	221
Tabelle 6.21 – Die Tabelle INTUSCOM_TERMINALS.....	221
Tabelle 6.22 - Fingerprint - Tabellen	222
Tabelle 6.23 – Die Tabelle INTUS_FP_TEMPLATES_IDS	224
Tabelle 6.24 –Die Tabelle INTUSCOM_TH_TEMPLATES	226
Tabelle 6.25 – Die Tabelle INTUS_FP_APP_TEMPLATES	227
Tabelle 6.26 – PS-Tabellen	228
Tabelle 6.27 – Videoüberwachung - Tabellen.....	229
Tabelle 6.28 – Die Tabelle INTUSCOM_VIDEO_IMAGES	231
Tabelle 6.29 – Die Tabelle INTUSCOM_VIDEO_PROFILES	232
Tabelle 7.1 - - INTUS COM Standardports	262

A.1.5. Verzeichnis der Beispiele

Beispiel 2.1 - Secure-Datei.....	37
Beispiel 4.1 – Gültigkeitsvortrag	166
Beispiel 6.1 - INTUS COM Konfiguration in XML-Datei	254
Beispiel 7.1 - Beispiel für ein TCL-Programm mit Ladeanforderungen.....	258
Beispiel 7.2 - Beispiel für eine Stammdaten-Datei	259

A.1.6. Abbildungsverzeichnis

Abbildung 1.1 – INTUS COM Systemarchitektur.....	12
Abbildung 2.1 - INTUS COM installieren	16
Abbildung 2.2 - Eintrag einer ODBC-Datenquelle in der Systemsteuerung	19
Abbildung 2.3 - Anlegen einer ODBC-Systemdatenquelle.....	19
Abbildung 2.4 - Konfiguration des SQL-Server ODBC Treibers.....	20
Abbildung 2.5 - INTUS COM Datenbankanbindung installieren.....	21
Abbildung 2.6 - INTUS COM DB-Tabellen installieren	21
Abbildung 2.7 - ODBC Verbindungseinstellungen für INTUS COM	22
Abbildung 2.8 – Lizenzkostenfreie Laufzeitumgebung installieren	23
Abbildung 2.9 – INTUS COM HTTPS-Server Zertifikate	24
Abbildung 2.10 - Auswahl der Updatekomponenten.....	25
Abbildung 2.11 – KeyStoreGen – Exportdateien festlegen.....	33
Abbildung 2.12 – KeyStoreGen – Exportpfad festlegen.....	33
Abbildung 2.13 – KeyStoreGen – Antragsteller Informationen	34
Abbildung 2.14 – KeyStoreGen – Ausführen.....	34
Abbildung 2.15 - Anmelden mit Benutzer und Passwort.....	38
Abbildung 2.16 - Fehlerdialog für Verbindungsfehler.....	39
Abbildung 2.17 - Verbindungstimeout.....	39
Abbildung 2.18 - Warndialog für befristete Lizenz	40
Abbildung 2.19 - Lizenzdialog	40
Abbildung 3.1 - Hauptfenster des INTUS COM Client	42
Abbildung 3.2 - Fenster "Verwaltungseinheiten"	44
Abbildung 3.3 - Fenster "Benutzer-Rollen-Berechtigungen"	45
Abbildung 3.4 - Fenster "Benutzer-Rollen-Berechtigungen, erweiterte Darstellung"	47
Abbildung 3.5 - Fenster "Komponenten"	47
Abbildung 3.6 - Fenster "Videokomponenten"	50
Abbildung 3.7 - Fenster "PS-Distribution"	51
Abbildung 3.8 - Fenster "AutoClone"	52
Abbildung 3.9 - Fenster "Offlineanlagen"	53
Abbildung 3.10 - K&S Fenster	55
Abbildung 3.11 - Fenster "Fehler"	55
Abbildung 3.12 - Fenster "Meldungen"	57
Abbildung 3.13 - Fenster "Lageplan"	59
Abbildung 3.14 - Fehlermeldung "Änderungsmodus nicht verfügbar"	65
Abbildung 3.15 - Netzwerk Terminalsuche	72
Abbildung 3.16 - Terminalsetup	73
Abbildung 3.17 - Terminalsetup	74
Abbildung 3.18 - Dialog mit Terminal	75
Abbildung 3.19 - Dauertüröffnung	76
Abbildung 3.20 – Offlineterminals in Datei exportieren	77
Abbildung 3.21 – Offlineterminal-Konfigurationsergebnisse importieren	78
Abbildung 4.1 – Terminal Management System, Einstellungen	85
Abbildung 4.2 – Terminal Management System, Lizenz	87
Abbildung 4.3 – Verwaltungseinheit, Grundeinstellungen	88
Abbildung 4.4 - Terminal-Handler, Grundeinstellungen	90
Abbildung 4.5 - Terminal-Handler, Upload	93
Abbildung 4.6 - Terminal-Handler, Download	95
Abbildung 4.7 - Terminal-Handler, Biometrie	98
Abbildung 4.8 – Terminal-Handler, SeeTec LPR	100
Abbildung 4.9 - Konzentrator, Grundeinstellungen	102
Abbildung 4.10 - Konzentrator, Verschlüsselung	103
Abbildung 4.11 - TCP-Server, Grundeinstellungen	104
Abbildung 4.12 - TCP-Server, Verschlüsselung	106
Abbildung 4.13 - HTTPS-Server, Grundeinstellungen	109

Abbildung 4.14 - INTUS 3000/3450 Server, Grundeinstellungen.....	115
Abbildung 4.15 - INTUS Terminal/ACM, Grundeinstellungen	119
Abbildung 4.16 - Terminaleinstellungen für HTTPS-Server	123
Abbildung 4.17 - Terminaleinstellungen für INTUS 3000 Server.....	123
Abbildung 4.18 - Terminaleinstellungen für TCP-Server.....	123
Abbildung 4.19 - INTUS Terminal/ACM, Dateien	125
Abbildung 4.20 - Dateiauswahl dialog des INTUS COM Client.....	126
Abbildung 4.21 - INTUS Terminal/ACM, TPI	127
Abbildung 4.22 - INTUS Terminal/ACM, TCL.....	129
Abbildung 4.23 - INTUS Terminal/ACM, AutoClone	131
Abbildung 4.24 - INTUS Terminal/ACM, FP.....	132
Abbildung 4.25 - Subterminal, Grundeinstellungen	134
Abbildung 4.26 – Subterminal, Grundeinstellungen PS Controller.....	136
Abbildung 4.27 - Subterminal, Grundeinstellungen Fingerprint	136
Abbildung 4.28 - Tür, Grundeinstellungen	138
Abbildung 4.29 - Benutzer, Grundeinstellungen	140
Abbildung 4.30 - Rolle, Grundeinstellungen.....	142
Abbildung 4.31 - Berechtigung, Grundeinstellungen	143
Abbildung 4.32 - Berechtigung, Berechtigungen	145
Abbildung 4.33 - Benutzer-Rolle-Zuordnung	149
Abbildung 4.34 - Berechtigung-Rolle-Zuordnung.....	150
Abbildung 4.35 - Video-Interface, Grundeinstellungen	151
Abbildung 4.36 - Video-Interface, Videobildanforderung	152
Abbildung 4.37 - VideoServer, Grundeinstellungen.....	154
Abbildung 4.38 - Kamera an SeeTec Gateway Service, Grundeinstellungen	156
Abbildung 4.39 - Kamera-Leser-Zuordnung	158
Abbildung 4.40 - PS-Distributor, Grundeinstellungen.....	159
Abbildung 4.41 - PS-Distributor, Verschlüsselung.....	161
Abbildung 4.42 - AutoClone Dienst, Grundeinstellungen	162
Abbildung 4.43 – Email-Einstellung, Grundeinstellungen.....	164
Abbildung 4.44 – Offlineanlage	165
Abbildung 4.45 – Offlineterminal.....	168
Abbildung 4.46 – Blocklist.....	170
Abbildung 5.1 – Verbindungsfehler.....	174
Abbildung 6.1 – Übergabemechanismus der statischen Dateischnittstelle	186
Abbildung 6.2 – Übergabemechanismus der dynamischen Dateischnittstelle	189
Abbildung 6.3 - Vergabe von Templates-IDs.....	225
Abbildung 6.4 - Anbindung des INTUS COM Video-Interface.....	233
Abbildung 6.5 - Convision VideoServer, Startseite.....	234
Abbildung 6.6 - Convision VideoServer, Aufnahmegeschwindigkeit einstellen	235
Abbildung 6.7 - Convision VideoServer, Aufnahme starten.....	236
Abbildung 6.8 – Beispiel – Video-Interface Einstellungen.....	237
Abbildung 6.9 - Komponenten & Videokomponenten	238
Abbildung 6.10 – LPR-Interface – Callbackregistrierung.....	241
Abbildung 6.11 – Verarbeitungsablauf für gelesene Kennzeichen.....	243

A.1.7. Stichwortverzeichnis

6	E
A	
<i>64Bit</i>	20
A	
<i>Aktualisierung .</i>	179
<i>Alarm</i>	
<i>Meldungen .</i>	43, 55, 189, 255
<i>Alarm .</i>	67, 90, 213
<i>Änderungsmodus .</i>	40, 42, 43, 46, 47, 48, 49, 51, 52, 54, 56, 57, 59, 61, 62, 63, 81, 84, 86, 98, 100, 105, 109, 112, 148, 150, 153
<i>Anschlussart</i>	
<i>dialup .</i>	87, 101, 103, 119
<i>Anzeigemodus .</i>	56, 61, 62
<i>Applikationsschnittstelle .</i>	90, 177, 181
<i>Arbeitsverzeichnis .</i>	36, 86, 178, 179, 182
B	
<i>Batterie</i>	
<i>Batteriestatus .</i>	66
<i>Batterie .</i>	66
<i>Benutzername .</i>	135
<i>Benutzerschnittstelle .</i>	12
<i>Berechtigungsgruppen .</i>	92, 112, 123, 179, 194, 195, 197, 198, 200, 209, 251
<i>Bereitmeldung .</i>	90, 193
<i>Bereitstellung von Templates</i>	221
<i>betriebsbereit .</i>	87, 172, 182, 251, 252
<i>Betriebsdatenerfassung .</i>	11, 177
<i>Betriebsstatus .</i>	37, 44, 46, 170, 171
<i>BLOB</i>	197
<i>Blocklist</i>	48, 122, 164, 165
<i>Buchungen</i>	
<i>Buchungsprofil .</i>	206
<i>Buchungssatz .</i>	213
<i>Buchungstabelle .</i>	93, 214
<i>Buchungen .</i>	43, 64, 65, 93, 178, 182, 183, 189, 194, 195, 201, 206, 213, 251, 252
D	
<i>Dateischnittstelle .</i>	13, 87, 89, 177, 178, 179, 180, 181, 182, 183, 184, 193, 194, 213, 248
<i>Datenbank</i>	
<i>MS Access .</i>	19, 197
<i>ODBC .</i>	18, 19, 177
<i>ODBC DSN .</i>	19, 22, 173
<i>Oracle .</i>	197
<i>SQL-Server .</i>	20
<i>Datenbankschnittstelle</i>	
<i>Update/Delete .</i>	93, 201, 202, 204
<i>Datenbankschnittstelle .</i>	13, 17, 18, 87, 90, 177, 194, 197, 213
<i>Datenübertragung</i>	
<i>Baudrate .</i>	125, 172
<i>Datenformat .</i>	125, 172
<i>Datensatz .</i>	90, 172, 179, 182, 184, 202, 254
<i>Datenverlust</i>	2
<i>Datenverlust .</i>	178, 179
<i>Kanal .</i>	125
<i>Door-ID</i>	74, 85, 163, 164
F	
<i>Einlernereignis</i>	220
<i>E-Mail .</i>	2, 67, 167
<i>Ereignis .</i>	53, 174
Fehler	
<i>Betriebsfehler .</i>	171, 172
<i>Fehlerbeschreibung .</i>	167
<i>Fehlermeldung .</i>	62, 90, 167, 169, 171, 189
<i>Fehlersuche .</i>	167, 174
<i>Finger-ID</i>	217, 222
<i>Fingerstatus</i>	217, 222
<i>FP</i>	94, 127
<i>FP Unterstützung</i>	127
<i>Funktionsschritte</i>	91, 179, 198, 209
G	
<i>Grundversorgung .</i>	93, 195, 198, 199, 202
H	
<i>Handbücher</i>	
<i>Benutzerhandbuch .</i>	11, 186, 209, 213
<i>Betriebshandbuch .</i>	11
<i>Handbücher .</i>	11
<i>HTTPS-Server</i>	105
I	
<i>Inbetriebnahme .</i>	75
<i>Installation</i>	
<i>Installationshinweise .</i>	16
<i>Secure-Dateien .</i>	27, 33
<i>Installation .</i>	11, 15, 16, 17, 18, 32, 33, 35, 36, 75, 174, 197, 248
<i>INTUS COM Server</i>	
<i>Datenport .</i>	13, 33, 80, 87, 98, 101, 106, 111, 170, 185, 254, 255
<i>Serviceport .</i>	33, 58, 62, 80, 87, 98, 101, 106, 111, 115, 149, 152, 171, 254
<i>INTUS Terminal</i>	
<i>INTUS 3000 - .</i>	13, 17, 44, 55, 62, 68, 75, 115, 118, 181, 186
<i>INTUS 3000 Server .</i>	13, 44, 68, 79, 109, 111, 118, 152, 191
K	
<i>Kartendaten</i>	91, 112, 122, 179, 195, 198, 210, 212
<i>Kommandozeilenoptionen .</i>	31, 32
<i>Konfigurationsdialog .</i>	178
<i>Konflikt .</i>	34, 80
<i>Kontextmenü .</i>	40, 42, 43, 46, 61, 62, 63, 64, 65, 66, 67, 70, 71, 135, 136, 138, 143, 144, 159
L	
<i>Ladeanforderung .</i>	120, 179, 181, 198, 251, 252
<i>Lageplan .</i>	11, 55, 56, 59, 61
<i>LBus .</i>	124, 130
<i>Lizenz</i>	
<i>Testlizenz .</i>	15, 35
<i>Lizenz .</i>	16, 17, 34, 35, 36, 57, 59
<i>Lizenzbestimmungen</i>	264
<i>Log-Datei .</i>	80, 167, 171, 172, 174

M

Messagelevel . 80, 86, 98, 101, 106, 146, 154, 157, 167, 172, 174
Multiplexer . 13

N

Name . 84, 111, 130, 133, 149, 151
Netzwerk
 DNS-Server . 80, 117, 131, 169
 Gateway . 112, 169
 Parameter . 69, 80
 Router . 119, 169
 Telnet . 76
Netzwerk . 58, 68, 80, 117, 119
Notpuffer . 125

O

odbcad32 . 20
Offlineanlage . 48, 114, 160, 161, 162, 163, 164
Offlineanlagen-ID . 74, 114, 115, 160, 161, 163, 164
Offlineterminal . 48, 49, 72, 73, 74, 85, 160, 162, 163, 164
Online-Hilfe . 37, 59
OSO-Kartendaten-IDs . 195, 203, 204
OSS Standard Offline . 72, 73, 85, 91, 114, 160, 162, 164, 165, 166

P

Parameterdatei . 130, 173
Partyline . 44, 109, 111, 118
Passwort . 34, 40, 41, 57, 75, 135, 175, 254
Personalstamm . 202
Personalzeiterfassung . 11
Pollzyklus . 87
Produktivsystem . 16
Profile . 92, 93, 112, 122, 179, 195, 198, 199, 207, 215, 251, 252
Profiltabelle . 204, 206, 207, 208
Protokoll
 Adress-Kennung . 93, 206
 Quittung . 87, 173, 182, 193
 Verbindungsauflaufbau . 103, 119

R

RAS-Verbindung . 103
Reset
 Kaltstart . 64, 65, 172, 179
 Warmstart . 64
Reset . 58, 59, 61, 64, 65, 69, 113, 124, 169, 172

S

Satzart . 90, 93, 198, 201, 207, 209, 213, 214, 215
Satzfilter . 90, 193
Satzformat . 181, 184, 185
Satznummer . 89, 115, 122, 124, 181, 182, 213
Schnittstellen
 RS485 . 13, 109, 118
Setup
 Einstellungen . 62
Site-ID . 74, 114, 115, 160, 161, 164
SMTP-Server . 82, 83
Socket-Schnittstelle . 13, 89, 177, 185, 193, 194, 248
Sonderberechtigung . 206
Sondertage . 198
Sondertage . 92, 122, 179, 195, 206
Sondertagstabelle . 209
SRAM . 125, 172
Stammdaten

Datensätze . 92, 93, 123, 182, 198, 199, 202, 207, 252, 253

Tabelle . 93, 200, 201, 202, 207

Stammdaten . 43, 93, 112, 178, 179, 195, 197, 198, 207, 251, 252, 253

Standort . 215

Status
 Statusanfrage . 252

Statusatz . 193, 252

Subterminal . 55, 75, 130, 173, 201, 206, 208, 214, 215, 248

Systemarchitektur . 12

Systemdienst (Service) . 32, 33, 35

Systemkonfiguration . 112, 179, 194, 251

T

TCL
 CV-Feld . 252

Ladeanforderung . 120, 179, 181, 198, 251, 252

TF-Feld . 125

TCL-Programm . 11, 62, 112, 115, 124, 172, 178, 179, 181, 251, 252

TCL-Terminal . 62, 65, 125, 172, 179, 181, 182, 251, 252

TCP/IP
 IP-Adresse . 33, 34, 35, 76, 80, 82, 112, 117, 131, 169

Port . 33, 34, 62, 68, 80, 82, 119, 169, 170, 248, 254

Port-Nummer . 62, 80, 170, 254

Template . 217, 222

Templatedownload . 95

Templategröße . 95

Templates . 220, 223

Templates-ID . 217, 222

Templateübertragung . 127, 131

Terminaladresse
 Server-ID . 75, 80, 101, 106, 111, 112, 214, 215, 218, 221, 248, 254

Subterminal-ID . 75, 215

Terminal-ID . 53, 75, 104, 112, 113, 115, 184, 185, 186, 214, 215, 218, 248, 254

Terminaladresse . 214, 215, 248

Terminalkonfiguration . 248

Terminalstatus . 172

Timeout . 87, 101, 103, 106

Timeout Basiskommunikation . 106

TPI
 Hauptterminal . 75

Subterminal . 55, 75, 130, 173, 201, 206, 208, 214, 215, 248

Terminalgruppe . 173, 181

TPI Onlineanfragen . 93

TPI-Control . 17

TPI-tasc . 11, 17, 45, 56, 115, 133, 172, 173, 181, 186

TPI-Terminal . 65, 179, 181, 182, 186, 251

Tür-ID . 74, 85, 163, 164

U

UDP/IP . 112, 113

Uhrzeit . 53, 58, 59, 70, 88, 115, 117, 201

Uhrzeitsynchronisation . 11, 13, 88, 115, 117, 251

UNC-Pfad . 86

User-ID . 217

V

Verbindungsfehler . 34, 35, 167, 168, 169, 171

Verbindungsstatus . 43, 44, 46, 55, 167, 192

Vergabe von Templates-IDs . 218

Verteilung von Templates . 95

<i>Verwaltungseinheit</i> .	39, 77, 79, 81, 84, 86, 98, 101, 106, 111, 114, 130, 133, 136, 137, 139, 146, 149, 152, 154, 157, 159, 161, 163, 166	
<i>Voreinstellung</i> .	22, 34, 80, 87, 185	
<i>Vorkenntnisse</i> .	11	
	W	
<i>Wartezeit</i> .	87, 93	
<i>Winterzeit</i> .	115, 116, 117	
<i>Wochentag</i> .	117, 119	
	X	
<i>XML</i> .	248	
	Z	
<i>ZDE</i> .	11	
<i>Zeit</i>		
<i>Einstellungen</i> .	87	
<i>GMT/UTC-Zeitabweichung</i> .	116	
<i>Uhrzeit</i> .	53, 58, 59, 70, 88, 115, 117, 201	
<i>UTC-Zeit</i> .	115, 116, 117	
<i>Zeitzone</i> .	115, 116, 117	
<i>Zeitintervall</i> .	180, 183, 184	
<i>Zeitstempel</i> .	90, 93, 195, 197, 198, 199, 201, 202, 204, 214, 215	
<i>Zutrittskontrolle</i> .	11, 177	
<i>Zutrittsprofil</i> .	206	

A.4. Probleme mit diesem Handbuch?

Haben Sie einen Fehler entdeckt, vermissen Sie Informationen oder verstehen Sie etwas nicht?

Haben Sie einen Verbesserungsvorschlag oder eine Idee für eine Ergänzung?

Wir bemühen uns, das Handbuch so hilfreich wie möglich zu machen. Trotzdem kann einmal etwas vergessen oder übersehen werden. Und weil Handbuch**benutzer** immer am besten wissen, was an einem Handbuch gut oder schlecht ist:

Rufen Sie uns an

und sagen Sie uns, was wir noch besser machen können. Wir bedanken uns schon jetzt für die kleine Mühe.

Ihre PCS Systemtechnik GmbH

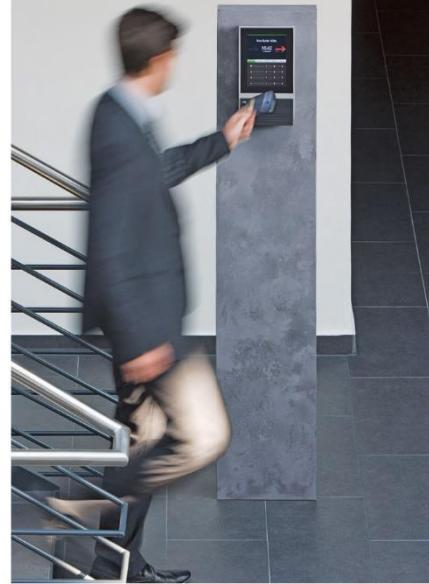
PCS-Hotline: 089 / 68004 - 666

Emails:

support@pcs.com

intuscom@pcs.com

HCS. The terminal people.®



PCS Systemtechnik GmbH

Pfälzer-Wald-Str. 36

81539 München

Fon +49-89-68004-0

intus@pcs.com

Ruhrallee 311

45136 Essen

Fon +49-201-89416-0

www.pcs.com

