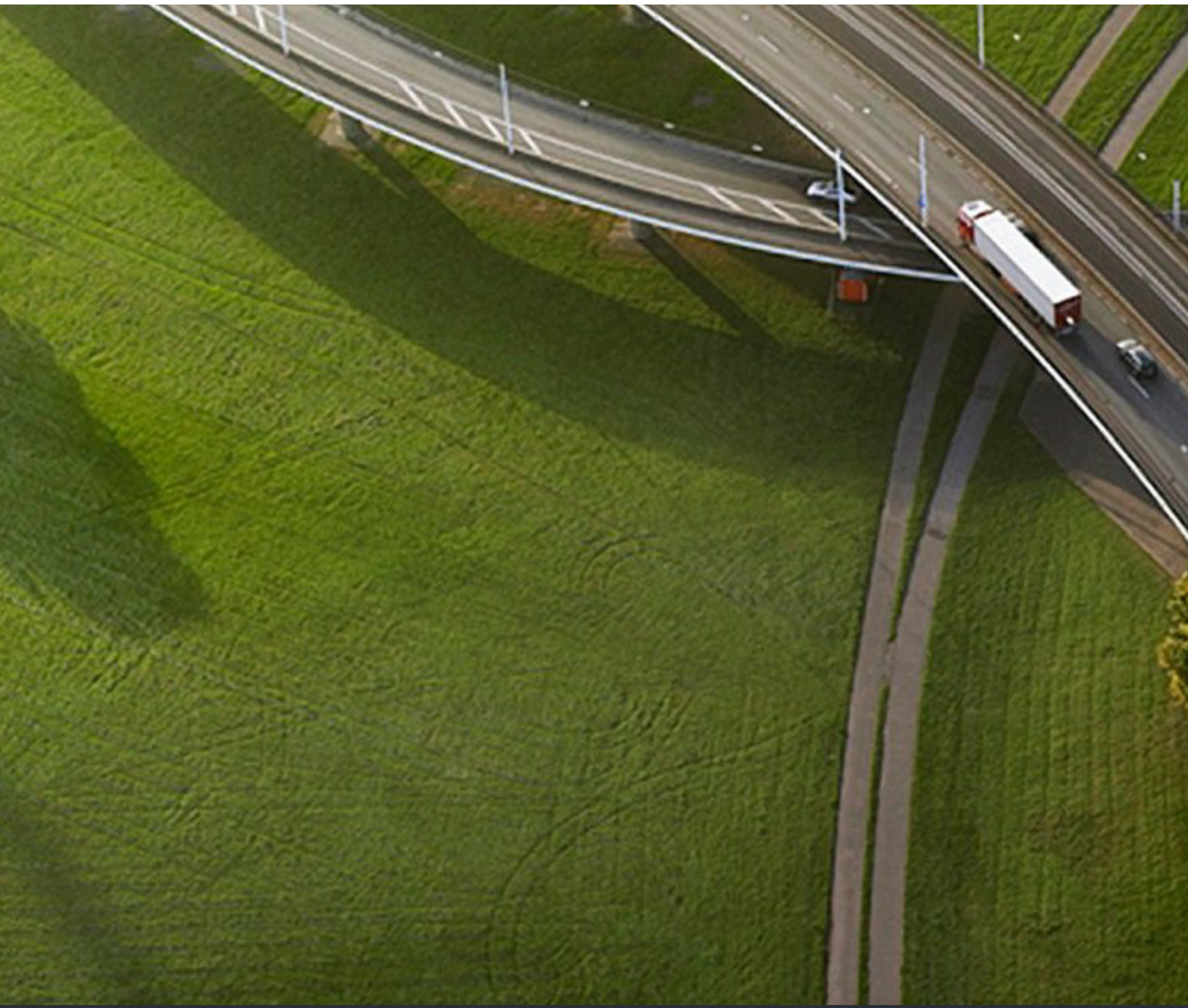
UNIFY Harmonize your enterprise



OpenScape Deployment Service V7

Administrations- und Installationsanleitung

P31003-S2370-M107-19-A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Reference No.: P31003-S2370-M107-19-A9

UNIFY Harmonize your enterprise

unify.com

Contents

1 Einführung 1-1
1.1 Zielgruppe 1-1
1.2 Verwendete Konventionen 1-1
1.3 Einschränkende Hinweise 1-2

2 Schnelleinstieg 2-1
2.1 DLS-Installation 2-2
2.1.1 Systemvoraussetzungen 2-2
2.1.2 Systemkapazitäten 2-5
2.1.3 Lizensierung 2-6
2.1.4 Installation der DLS-Software 2-8
2.2 Erstinbetriebnahme des DLS (Single Mode) 2-8
2.3 Erforderliche Workpoint-Firmware installieren 2-11
2.3.1 Software-Images automatisch anlegen 2-11
2.3.2 Auto Deployment 2-12
2.3.3 Manuelles Deployment 2-12
2.4 Auswahl häufig genutzer Funktionen 2-13
2.4.1 IP Devices scannen 2-13
2.4.2 Konfiguration von Parametern: Beispiel Tastenbelegung 2-13
2.4.3 Jobs 2-15
2.5 Einsatz der Mobility-Funktion 2-15
2.6 Security 2-17
2.6.1 Zertifikate 2-17

3 Konzept und Leistungsmerkmale 3-1
3.1 Übersicht 3-1
3.2 Komponenten des OpenScape Deployment Service 3-2
3.3 Grundsätzliches zur Bedienung 3-3
3.4 Einsatzgebiet 3-4
3.5 Übersicht der Software- und Datei-Typen 3-7
3.6 Die wichtigsten Leistungsmerkmale 3-10
3.6.1 Ausbaugrenzen und Einschränkungen 3-12
3.6.2 Verwendete Ports 3-12
3.7 Vom Deployment Service unterstützte Bereitstellungen 3-13
3.8 Mobility im DLS – Grundlagenwissen 3-14
3.8.1 Mobility-Begriffserklärungen 3-14
3.8.2 Mobility verwenden 3-14
3.8.3 Mobility ID 3-16

3.8.4 Mobility einrichten 3-16
3.8.5 Profil-Konzept im DLS 3-17
3.9 DLS-Systemüberwachung 3-19
3.9.1 Systemüberwachungstools - DLS RapidStat 3-19

4 Installation und Erstkonfiguration 4-1
4.1 Voraussetzungen 4-1
4.1.1 Allgemeine Voraussetzungen am Server 4-1
4.1.2 Generelle Voraussetzungen am Client-PC 4-2
4.1.3 Personelle Voraussetzungen 4-3
4.1.4 Verfügbarkeit des DLS 4-3
4.1.5 Infrastruktur bei Cluster-Betrieb 4-4
4.2 SQL-Server für entfernte Datenbank installieren 4-5
4.2.1 Microsoft SQL Server 2005 4-7
4.2.2 Microsoft SQL Server 2008 R2 4-11
4.2.3 SQL Native Client – bei Nutzung einer entfernten Datenbank 4-30
4.2.4 Ändern des Service-Passworts 4-32
4.3 Konfiguration des Network Load Balancer 4-32
4.3.1 Network Load Balancer für Windows Server 2003 4-32
4.3.2 Network Load Balancer für Windows Server 2008 4-40
4.3.3 Network Load Balancer für Windows Server 2008 R2 4-50
4.3.4 Network Konfiguration für Windows NLB 4-51
4.4 DCMP einrichten 4-52
4.4.1 DCMP installieren 4-52
4.4.2 DCMP konfigurieren 4-55
4.4.3 DLS für DCMP konfigurieren 4-57
4.4.4 Telefon für DCMP konfigurieren 4-58
4.4.5 DCMP testen 4-60
4.5 Installation des DLS 4-62
4.5.1 Single Node-Betrieb mit lokaler Datenbank 4-62
4.5.2 Single Node-Betrieb mit entfernter oder kundenspezifischer Datenbank 4-78
4.5.3 Multi-Node-Betrieb 4-83
4.6 Spiegelung der SQL-Datenbank aufsetzen 4-101
4.7 DLS-Datenbank-Wiederherstellung in einer Multi-Node-Umgebung 4-125
4.8 Upgrade von DLS-Multi-Node-Umgebungen 4-126
4.9 DLS starten 4-127
4.10 Erstkonfiguration 4-128
4.11 Starten des DLS-Clients 4-130
4.11.1 Aufruf des Clients 4-130
4.12 Installieren von Netzwerk-Komponenten 4-131
4.12.1 FTP Server 4-132

4.12.2 HTTPS-Server 4-134
4.12.3 Allgemeines zu DHCP 4-135
4.12.4 DHCP-Server in einer Windows-Umgebung 4-136
4.12.5 DHCP-Server in einer Linux/Unix-Umgebung 4-146
4.12.6 DNS-Server für DLS konfigurieren 4-148
4.12.7 DHCP Server mit Infoblox Appliance 4-149
4.13 Verwendung von pcAnywhere bei Fernzugriff auf den DLS 4-159
4.13.1 Allgemein 4-159
4.13.2 Einstellungen auf dem Host-Rechner 4-159
4.13.3 Einstellungen auf dem Remote-Rechner 4-160
4.13.4 Verschlüsselungsstufen 4-161
4.14 Deinstallation des OpenScape Deployment Service 4-162
4.14.1 Deinstallation des DLS 4-162
4.14.2 Deinstallation des SQL-Servers 4-162

5 Die DLS-Benutzeroberfläche 5-1
5.1 Starten und einloggen 5-1
5.2 Beenden 5-2
5.3 Aufruf der kontextsensitiven Hilfe-Funktion 5-3
5.4 Anwendungsoberfläche 5-3
5.4.1 Hauptmenü 5-4
5.4.2 Arbeitsbereich 5-6
5.4.3 Anzeigebereich 5-22
5.5 Suchfunktionalität 5-25

6 Administration 6-1
6.1 Account Management 6-2
6.1.1 Account Konfiguration 6-4
6.1.2 Policy Einstellungen 6-12
6.1.3 Rollen und Rechte 6-22
6.2 PKI 6-30
6.2.1 Plug-In Konfiguration 6-31
6.2.2 Connector Konfiguration 6-38
6.2.3 Interne CA;CA intern 6-49
6.2.4 Renewal 6-54
6.3 Server Konfiguration 6-56
6.3.1 Mandanten 6-57
6.3.2 Standort 6-63
6.3.3 P&P Einstellungen 6-78
6.3.4 FTP Server Konfiguration 6-82
6.3.5 HTTPS Server Konfiguration 6-91
6.3.6 HTTPS Client Konfiguration 6-104

6.3.7 Netzlaufwerk Konfiguration 6-108
6.3.8 Infrastruktur Policy 6-114
6.3.9 API Notifizierungen 6-118
6.3.10 XML Applikationen 6-120
6.3.11 Optionen 6-126
6.3.12 TLS Connector Konfiguration 6-129
6.4 Cluster Konfiguration 6-136
6.4.1 Deployment Server 6-137
6.4.2 Cluster Einstellungen 6-141
6.5 Protokoll-Daten 6-142
6.5.1 Aktivitäten- und Fehlerprotokoll 6-143
6.5.2 Audit- und Security Log Dateien 6-147
6.5.3 P&P Import Protokolle 6-151
6.5.4 Alarm Protokoll 6-152
6.5.5 Alarm List 6-154
6.6 Alarm Konfiguration 6-156
6.6.1 Register „Alarmklassen“ 6-159
6.6.2 Register „Signalisierung“ 6-161
6.6.3 Register „SNMP“ 6-162
6.6.4 Register „Kommando Datei“ 6-164
6.6.5 Register „Email“ 6-165
6.6.6 Register „Syslog“ 6-167
6.6.7 Register „Einstellungen“ 6-169
6.7 Backup / Restore 6-171
6.7.1 Register „Backup“ 6-175
6.7.2 Register „Restore“ 6-176
6.7.3 Register „Protokoll“ 6-178
6.8 File Server 6-180
6.9 Workpoint Interface Konfiguration 6-183
6.9.1 Register „Secure Modus“ 6-185
6.9.2 Register „DCMP“ 6-193
6.9.3 Register „HTTP-Proxy“ 6-196
6.10 Automatische SPE Konfiguration 6-197
6.10.1 Register „CA Administration“ 6-199
6.10.2 Register „Aussteller Administration“ 6-204
6.10.3 Register „Einstellungen“ 6-206
6.11 Automatische Zertifikatsverteilung 6-208
6.12 Automatische Archivierung 6-213

6.12.1 Register „Einstellungen“ 6-216
6.12.2 Register „zu archivierende IP Devices“ 6-218
6.12.3 Register „zu archivierende Mobile User“ 6-219
6.12.4 Register „Protokoll“ 6-220
6.13 Automatischer Upload Diagnose- und Security Log Dateien 6-222
6.13.1 Register „Protokoll“ 6-225
6.14 Trace Konfiguration 6-226
6.14.1 Register „Zusätzliche Einstellungen und Aktionen“ 6-232
6.14.2 Register „Wiederholungs-Filter“ 6-234
6.14.3 Register „Meldungs-Filter“ 6-236
6.14.4 Register „Filter-Test“ 6-237
6.14.5 Register „OSVTM Configuration“ (OSVTM-Konfiguration) 6-238
6.14.6 Register „Thread Überwachung“ 6-240
6.15 Server Lizenzen 6-241
6.15.1 Register „Lizenzstatus“ 6-244
6.15.2 Register „Betrieb mehrerer DLS Server“ 6-251

7 IP Devices 7-1
7.1 IP Phone Konfiguration 7-2
7.1.1 Gateway / Server 7-8
7.1.2 IP Routing 7-27
7.1.3 Ports 7-39
7.1.4 Features 7-46
7.1.5 Quality of Service 7-80
7.1.6 QoS Data Collection 7-90
7.1.7 Security Einstellungen 7-96
7.1.8 Telefonie 7-122
7.1.9 Small Remote Site Redundancy 7-124
7.1.10 Wahlparameter 7-127
7.1.11 Uhrzeit Einstellungen 7-133
7.1.12 Audio Einstellungen 7-137
7.1.13 SNMP Einstellungen 7-150
7.1.14 Applikationen 7-154
7.1.15 LDAP 7-167
7.1.16 Anwendereinstellungen 7-173
7.1.17 SIP Mobility 7-186
7.1.18 HFA Mobility 7-190
7.1.19 Keysets / Tastenbelegung 7-193
7.1.20 WLAN Einstellungen 7-212
7.1.21 Signaling and Payload Encryption (SPE) 7-224
7.1.22 IEEE 802.1x 7-232
7.1.23 Diagnose 7-245
7.1.24 Sonstiges 7-268
7.1.25 File Deployment 7-285
7.2 IP Client Konfiguration 7-289

7.2.1 CTI Konfiguration 7-293
7.2.2 Gateway / Server 7-307
7.2.3 Ports 7-332
7.2.4 Quality of Service 7-336
7.2.5 Telefonie 7-342
7.2.6 Small Remote Site Redundancy 7-345
7.2.7 Wahlparameter 7-347
7.2.8 Audio / Video Einstellungen 7-357
7.2.9 Verzeichnisse / Adressbücher 7-371
7.2.10 Sonstiges 7-382
7.2.11 Keysets / Tastenbelegung 7-389
7.2.12 Signaling and Payload Encryption (SPE) 7-401
7.2.13 Einwahlort 7-408
7.2.14 OpenScape 7-415
7.3 IP Gateway Konfiguration 7-419
7.3.1 QoS Data Collection 7-420
7.3.2 Security Einstellungen 7-429
7.3.3 Signaling and Payload Encryption (SPE) 7-434
7.3.4 IPSec / VPN 7-444
7.4 IP Device Interaktion 7-453
7.4.1 IP Device Daten lesen 7-454
7.4.2 IP Device zurücksetzen 7-460
7.4.3 IP Device Zertifikate sperren 7-464
7.4.4 IP Device Response Test 7-467
7.4.5 IP Devices pingen 7-471
7.4.6 IP Devices scannen 7-478
7.5 IP Device Verwaltung 7-490
7.5.1 Inventar Daten 7-491
7.5.2 Papierkorb 7-504
7.5.3 IP Infrastruktur 7-506
7.5.4 IP Device Konfiguration 7-509

8 Mobile User 8-1
8.1 SIP Mobile User Konfiguration 8-2
8.1.1 Gateway / Server 8-7
8.1.2 IP Routing 8-16
8.1.3 Features 8-18
8.1.4 Quality of Service 8-47
8.1.5 Security Einstellungen 8-49
8.1.6 Telefonie 8-53
8.1.7 Wahlparameter 8-55
8.1.8 Uhrzeit Einstellungen 8-60
8.1.9 Audio Einstellungen 8-62
8.1.10 Applikationen 8-66
8.1.11 LDAP 8-75

8.1.12 Anwendereinstellungen 8-78
8.1.13 SIP Mobility 8-91
8.1.14 Keysets / Tastenbelegung 8-95
8.1.15 Signaling and Payload Encryption (SPE) 8-114
8.1.16 Sonstiges 8-117
8.2 SIP Mobile User Interaktion 8-132
8.2.1 SIP Mobile User 8-137
8.2.2 Logon / Logoff 8-145
8.2.3 Automatisches Logoff 8-148
8.2.4 SIP User Tastenbelegung 8-149
8.2.5 Mobile User Response Test Einstellungen 8-153
8.3 User Daten Administration 8-157
8.3.1 Register „Statistik“ 8-159
8.4 Mobility Statistiken 8-161
8.4.1 Register „SIP Mobility“ 8-165
8.5 Mobility Statistiken Konfiguration 8-168

9 Gateways 9-1
9.1 Gateway Konfiguration 9-2
9.1.1 Register „Gateway Verbindung“ 9-7
9.2 QoS Data Collection 9-9
9.2.1 Register „Server Daten“ 9-13
9.2.2 Register „Report Einstellungen“ 9-15
9.2.3 Register „Schwellwerte“ 9-17

10 Software Deployment 10-1
10.1 Workpoint Deployment 10-2
10.1.1 Register „Software Deployment“ 10-7
10.1.2 Register „Datei Deployment“ 10-9
10.1.3 Register „Software Inventar“ 10-11
10.1.4 Register „LDAP Inventar“ 10-12
10.1.5 Register „Wartemusik Inventar“ 10-13
10.1.6 Register „INCA Inventar“ 10-14
10.1.7 Register „Java Midlet Inventar“ 10-15
10.1.8 Register „LOGO Datei Inventar“ 10-16
10.1.9 Register „System-/Rufton Inventar“ 10-17
10.1.10 Register „APM Inventar“ 10-18
10.1.11 Register „NETBOOT Inventar“ 10-19
10.2 Regeln bearbeiten 10-20

11 Element Manager 11-1
11.1 Element Manager Konfiguration 11-2
11.1.1 Register „OpenScape Voice“ 11-9
11.1.2 Register „OpenScape Voice Assistant“ 11-14
11.1.3 Register „OpenScape Voice Assistant V3.0“ 11-16
11.1.4 Register „HiPath 4000 Assistant“ 11-18

11.1.5 Register „HiPath 3000/5000“ 11-21
11.1.6 Register „OpenScape Office MX/LX“ 11-22
11.1.7 Register „OpenOffice EE“ 11-23
11.1.8 Register „HiPath DXWeb Pro“ 11-24
11.1.9 Register „Protokoll“. 11-25

12 Profil Management. 12-1
12.1 Geräteprofil 12-2
12.1.1 Register „Templates“ 12-6
12.1.2 Register „Unterstützte Geräte“ 12-7
12.1.3 Register „Mandanten“. 12-8
12.1.4 Register „Profile des übergeordneten Standortes“. 12-9
12.2 User Data Profile. 12-10
12.2.1 Register „Templates“ 12-13
12.2.2 Register „Mandanten“. 12-14
12.3 Template Übersicht. 12-15
12.3.1 Register „Template-Daten“. 12-19
12.3.2 Register „Profile“. 12-20
12.3.3 Register „Mandanten“. 12-22

13 XML Applikationen. 13-1
13.1 MakeCall 13-4
13.1.1 Register „Info“. 13-6
13.2 NewsService 13-7
13.2.1 Register „Info“. 13-8
13.3 NewsService Archiv 13-9
13.3.1 Register „Info“. 13-11
13.3.2 Register „IP Devices“ 13-12

14 Job Koordination 14-1
14.1 Job Kontrolle 14-2
14.1.1 Register „Basis Daten“ 14-8
14.1.2 Register „Deployment Daten“. 14-13
14.1.3 Register „Konfiguration Daten“. 14-16
14.1.4 Register „XML Applikationen Daten“ 14-18
14.2 Täglicher Status 14-19
14.2.1 Register „Statusinformation“. 14-22
14.3 Job Konfiguration 14-23
14.3.1 Register „IP Phones“ 14-27
14.3.2 Register „IP Clients“ 14-30
14.3.3 Register „IP Gateways“ 14-32
14.3.4 Register „Gateways“. 14-34

15 Bedienabläufe. 15-1
15.1 Erste Schritte: Ändern von IP Device-Parametern 15-2
15.2 Änderung der Element Manager-Konfiguration und Joberzeugung 15-4
15.3 Registrieren von Workpoint-Software und -Dateien 15-5

15.3.1 Automatische Registrierung 15-6
15.3.2 Verstehen der Lizenzinformationen bei IP Phone-Software 15-7
15.4 Templates bearbeiten 15-8
15.4.1 Template manuell anlegen 15-8
15.4.2 Template aus vorhandener Konfiguration erstellen. 15-9
15.4.3 Template laden 15-10
15.4.4 Weitere Funktionen 15-10
15.5 Autokonfiguration von Workpoints (Plug&Play) 15-11
15.5.1 Voraussetzungen 15-11
15.5.2 Plug&Play-Registrierung einrichten. 15-12
15.5.3 Registrierungsvorgang 15-14
15.6 Verteilen von Workpoint-Software 15-16
15.6.1 Manuelles Deployment 15-17
15.6.2 Automatisches Deployment. 15-20
15.7 Nutzen der Job-Koordination 15-22
15.7.1 Festlegen eines Jobs 15-23
15.7.2 Eigenschaften und Status von Jobs ansehen 15-24
15.8 Backup / Restore 15-25
15.8.1 Automatisierte Datensicherungen 15-25
15.8.2 Manuelle Datenbank-Manipulation 15-27
15.8.3 DLS-Wiederherstellungspunkt. 15-31
15.9 Backup & Restore auf OpenScape Voice und Linux Standalone-Installationen . . 15-32
15.9.1 Backup 15-32
15.9.2 Wiederherstellung (Restore) 15-35
15.9.3 Nach der Wiederherstellung 15-38
15.10 Automatische Wiederherstellung bei fehlerhaftem Upgrade 15-39
15.11 Import und Export von Plug&Play-Daten 15-40
15.11.1 Export von Plug&Play-Daten. 15-40
15.11.2 Import von Plug&Play-Daten 15-40
15.11.3 Plug&Play-Daten über OpenScape Desktop-Clients 15-40
15.11.4 Syntax der .csv-Dateien 15-43
15.12 Copy-Makro für P&P und Templates 15-61
15.12.1 Makrokommando Syntax. 15-61
15.12.2 Verfügbare <item name> 15-62
15.12.3 Verfügbare Zielfelder. 15-62

16 Administrations-Szenarien 16-1
16.1 Neuinstallation eines Workpoints bei HiPath 4000 16-2
16.2 Neuinstallation eines Workpoints bei HiPath 3000 16-3
16.3 Einrichten eines Gateways im DLS 16-4
16.3.1 Gateway hinzufügen 16-4
16.3.2 Angaben zur Freigabe (QDC und VoIP Security) 16-5
16.4 Konfigurieren von Zertifikaten in DLS 16-6
16.4.1 Erstellen einer neuen PKI 16-9
16.4.2 Verteilen des Signaling and Payload Encryption (SPE)-Zertifikats 16-13

16.4.3 Verteilen von neuen Web Based Management (WBM)-Zertifikaten an Telefone 16-14
16.4.4 Sicherer Modus für Telefone (Secure Modus) 16-15
16.4.5 Ersetzen der DLS-Web-Schnittstelle und der API-Zertifikate 16-17
16.4.6 SHA1-Konfiguration für AutoSPE 16-19
16.5 Austausch eines IP Devices 16-31
16.6 Austausch eines alten Workpoints (TDM) durch einen neuen (IP) 16-33
16.7 Austausch von HFA- durch SIP-Software und umgekehrt bei identischer Device ID 16-34
16.7.1 Austausch HFA- durch SIP-Software 16-34
16.7.2 Austausch SIP- durch HFA-Software 16-35
16.8 Einrichten eines IP Client 130 im DLS 16-36
16.8.1 Anlegen der Templates 16-36
16.8.2 Erstellung eines Profils aus den Templates 16-37
16.8.3 Einstellungen am optiClient 130 16-37
16.8.4 optiClient in Callcentern 16-39
16.9 Ändern der IP-Adresse und/oder Portnummer des DLS 16-40
16.10 Einsatz eines TAP mit DLS in einem Kundennetz ohne permanenten DLS 16-41
16.10.1 Installation und Erstkonfiguration des DLS auf dem TAP 16-41
16.10.2 Manipulation der DLS-Datenbank zur Verwendung des TAP bei verschiedenen Kunden 16-42
16.11 Steuern des DLS über die Programmschnittstelle (DlsAPI) 16-43
16.11.1 Web Service-Schnittstelle der DlsAPI 16-43
16.12 Security: Administration von Zertifikaten 16-45
16.12.1 WBM Server Zertifikat importieren 16-46
16.12.2 Phone bzw. RADIUS Zertifikat importieren 16-48
16.12.3 SPE CA Zertifikate 16-50
16.12.4 SPE CA Zertifikate für IP Client importieren 16-52
16.12.5 SPE Zertifikate und SPE CA Zertifikate für IP Gateway importieren 16-54
16.12.6 Zertifikat entfernen (am Beispiel IEEE 802.1x Phone) 16-56
16.12.7 IP Phone austauschen 16-57
16.13 Mobility:EinrichtenMobility:Administrieren 16-58
16.13.1 Mobility-Funktion auf dem Endgerät einrichten 16-58
16.13.2 Taste „Mobility“ einrichten 16-58
16.13.3 Mobile User:Profil 16-59
16.13.4 Mobile User erstellen 16-59
16.13.5 Home Phone einrichten 16-61
16.13.6 Mobile User anmelden (Forced Logon) 16-62
16.13.7 Mobile User abmelden (Forced Logoff) 16-62
16.13.8 Fehlersuche bei An- und Abmeldungsvorgängen 16-62
16.13.9 Voreinstellung für die Tastenbelegung bei Mobility-Telefonen 16-63
16.13.10 Datensicherung in einem .zip-Archiv 16-63
16.13.11 Mobile User Daten importieren 16-68
16.13.12 Mobility zwischen optiPoint und OpenStage 16-70

16.14 HFA Mobility an HiPath 3000 16-71
16.14.1 HiPath 3000 Konfiguration Voraussetzungen 16-71
16.14.2 DLS Konfiguration für netzwerkweite HFA Mobility 16-71
16.14.3 Bedienablauf 16-72
16.15 Datenstrukturen für DLS-eigene XML-Applikationen 16-73
16.15.1 Verzeichnisstruktur 16-73
16.15.2 Verzeichnisse bei Upgrade-Installationen 16-73
16.15.3 Dateiverzeichnisse bei Backup/Restore 16-74
16.16 Mandantenfähigkeit 16-75
16.16.1 Mandantenfähigkeit installieren /deinstallieren 16-75
16.16.2 Mandanten einrichten 16-76
16.16.3 Mandanten löschen 16-77
16.16.4 Mandantenfähigen Account einrichten 16-77
16.16.5 Mandantenfähige Alarm-Konfiguration 16-77
16.16.6 Serverzuweisungen 16-78
16.16.7 Mobile User 16-78
16.16.8 Mandantenfähiges Profil Management 16-78
16.16.9 Rufnummernband bei Mandantenfähigkeit 16-78
16.17 Migrationsszenarien 16-79
16.17.1 Von Onboard DLS bei Integrated Simplex V3R1/V6R1/V7 nach Windows DLS Single Node V7R1 16-79
16.17.2 Von Onboard DLS bei Integrated Simplex V3R1/V6R1/V7 nach Windows DLS Multi-Node V7R1 16-81
16.17.3 Von DLS Single Node V3R1/V6R1/V7 nach Windows DLS Multi-Node V7R1 16-82
16.17.4 DLS Multi-Node-Systeme mit Datenbankspiegelung bei Upgrade bzw. Migration des Betriebssystems 16-85

17 Anhang 17-1
17.1 Abkürzungen und Fachbegriffe 17-1

Contents

1 Einführung

Dieses Dokument beschreibt den OpenScape OpenScape Deployment Service V7 (DLS)-Client in der Version **V7 R1 (HI-DLS7.2xx)** und enthält Informationen zur Erstkonfiguration des DLS-Servers.

Dieses Handbuch ist auch als Online-Hilfe verfügbar. Sie können diese über die Benutzeroberfläche des DLS-Client aufrufen (siehe Abschnitt Abschnitt 5.3, “Aufruf der kontextsensitiven Hilfe-Funktion”).

HINWEIS: Eine Schnellstartanleitung finden Sie im gleichnamigen Kapitel 2.

1.1 Zielgruppe

Dieses Handbuch richtet sich an Administratoren, die den DLS-Server installieren und konfigurieren sowie an Benutzer, die mithilfe des DLS-Client Konfigurations- und Bereitstellungsaufgaben durchführen. Die Benutzer müssen Vorkenntnisse in puncto LAN-Administration und fundierte Kenntnisse in puncto IP Device-Konfiguration haben.

Weitere Informationen zu den Fähigkeiten, die ein DLS-Administrator besitzen muss, finden Sie unter Abschnitt 4.1.3, “Personelle Voraussetzungen”.

1.2 Verwendete Konventionen

Für die Darstellung von Informationen werden in diesem Handbuch die folgenden Konventionen verwendet:

Konvention	Beispiel
`Courier`	Eingabe und Ausgabe Beispiel: `LOCAL` als Dateiname eingeben
kursiv	Variable Beispiel: *Name* kann bis zu acht Zeichen lang sein
fett	Bezeichnet Elemente der Benutzeroberfläche Beispiel: Klicken Sie auf **OK** Wählen Sie **Schließen** im Menü **Datei**
fett	Besondere Hervorhebung Beispiel: Sie dürfen diesen Namen **nicht** löschen
Element	Elemente der Benutzeroberfläche mit zusätzlichen Informationen
`<Courier>`	Tastenkombinationen Beispiel: `<XTRG>+<ALT>+<ESC>`
>	Menüfolge Beispiel: **Datei** > **Ende**
HINWEIS:	Zusätzliche Informationen

Tabelle 1 Typografische Konventionen

Konvention	Beispiel
***WICHTIG*:**	Warnung in Bezug auf kritische Aspekte eines Prozesses

Tabelle 1 Typografische Konventionen

1.3 Einschränkende Hinweise

Einige der über DLS konfigurierbaren Einstellungen sind nur für bestimmte Endgeräte oder Firmware-Versionen verfügbar. In solchen Fällen wird jeweils ein entsprechender Hinweis angegeben.

2 Schnelleinstieg

Diese Kurzanleitung soll Administratoren in die Lage versetzen, ohne weiterführendes Hintergrundwissen, innerhalb kurzer Zeit den OpenScape Deployment Service V7 in Betrieb zu nehmen und einfache Konfigurationsmaßnahmen sowie den Anschluss neuer Telefone durchzuführen.

HINWEIS: Um dieses Kapitel möglichst kurz zu halten, wurde hier bewusst auf folgende Informationen verzichtet:
- Unterschiedliche Einsatzfälle
Hier wird nur beispielhaft ein Standard-Einsatzfall erläutert.
- Parameterbeschreibungen
Hier wird nur erklärt, was Sie tun sollen, nicht warum.
- Hintergrundinformationen
Hier sind nur die wichtigsten Informationen zusammengefasst.

Weiterführende Informationen finden Sie im restlichen Handbuch, insbesondere in den Kapiteln:
- Kapitel 3: Konzept und Leistungsmerkmalübersicht
- Kapitel 4: Installation des DLS und weiterer Software-Komponenten
- Kapitel 5: Allgemeine Informationen zur Benutzeroberfläche
- Kapitel 6 bis Kapitel 14: Informationen zu einzelnen Parametern
- Kapitel 15 und Kapitel 16: Praxisbeispiele mit Ablaufbeschreibungen.

Folgende Abläufe sind hier beschrieben:

- Abschnitt 2.1, “DLS-Installation”
- Abschnitt 2.2, “Erstinbetriebnahme des DLS (Single Mode)”
- Abschnitt 2.4, “Auswahl häufig genutzer Funktionen”
- Abschnitt 2.5, “Einsatz der Mobility-Funktion”
- Abschnitt 2.6, “Security”

2.1 DLS-Installation

2.1.1 Systemvoraussetzungen

- Hardware-Mindestanforderungen für den DLS-Client-PC:
  - Pentium 4-kompatible CPU mit 1,4 GHz
  - 2048 MB RAM (empfohlen >= 2048 MB)
  - 10-Mbit Ethernetkarte
  - JRE 1.7.x (Client); Browser: Beliebiger Browser mit Unterstützung für Java Plug-Ins, z. B. Internet Explorer, Firefox, Chrome, Opera, Safari

    HINWEIS: Internet Explorer muss bei großen Netzwerken über 512 MB verfügen, und zusätzlich über 1024 MB als Heapgröße für JRE.
    Bitte achten Sie darauf, dass für das Betriebssystem und die restlichen Applikationen noch genügend Arbeitsspeicher vorhanden ist.

    1. Gehen Sie im Windows-Startmenü zu **Start** > **Einstellungen** > **Systemsteuerung** und klicken Sie auf das **Java**-Symbol.
    2. Gehen Sie im Fenster **Java Control Panel** zum Register **Java** und klicken Sie auf die Schaltfläche **Ansicht**. Wählen Sie Ihre primäre (oder einzige) Java-Umgebung aus der Liste aus und doppelklicken Sie in die Zelle mit der Bezeichnung „Runtime-Parameter“.
    3. Geben Sie die anfänglichen und maximalen Heapgrößen ein und verwenden Sie dabei die im ersten Abschnitt oben angegebenen Parameter. Geben Sie als maximale Heapgröße 1024 MB an, indem Sie in das Feld Folgendes eintragen:
       -Xmx1024m
    4. Klicken Sie auf **OK**, um das Runtime-Umgebungs-Fenster zu schließen. Klicken Sie anschließend noch einmal auf OK, um das Fenster Java Control Panel zu schließen.

- Hardware-Mindestanforderungen für den Single-Node DLS-Server

	Standalone DLS
CPU	3,1 GHz CPU (Intel Xeon E3-1220, 4C/4T)
RAM	4 GB
Ethernet	100 MBit (1 GBit empfohlen)
Festplattenspeicher	80 GB

- Hardware-Mindestanforderungen für den DLS-Server bei einer Multi-Node-Bereitstellung

	Multi-Node DLS
CPU	Intel Xeon Quadprozessor > = 2,9 GHz
RAM	4 GB
Ethernet	100 MBit (1 GBit empfohlen)
Festplattenspeicher	300 GB

- Hardware-Mindestanforderungen für den DB-Server bei einer Multi-Node-Bereitstellung

	Datenbank-Server
CPU	Intel Xeon Quadprozessor > = 2,9 GHz
RAM	4 GB
Ethernet	100 MBit (1 GBit empfohlen)
Festplattenspeicher	80 GB

- Hardware-Mindestanforderungen für einen Witness-Server (Zeugenserver)

	Witness-Server
CPU	Intel Xeon Doppelkernprozessor mit 3 GHz
RAM	2 GB
Ethernet	100 MBit (1 GBit zwischen Servern)
Festplattenspeicher	10 GB

- Datenbank-Anforderungen
  - Der Einsatz von Microsoft® SQL Server™ 2008 Enterprise Edition ist möglich, erfordert jedoch 4 GB RAM. Die Datenbank muss vom Kunden bereitgestellt werden.
  - DLS ab V6R1 unterstützt Microsoft® SQL Server™ 2008 R2 Datacenter Edition

    HINWEIS: Für die Verwendung von Microsoft SQL 2008 R2 Enterprise oder Datacenter Edition sind entsprechende Microsoft-Lizenzen erforderlich. In der Regel empfiehlt sich die Verwendung von CPU-Lizenzen. Clientzugriffslizenzen (Client Access Licenses, CALs) sind ebenfalls möglich; hier wird für jedes unterstützte Gerät eine Geräte-Clientzugriffslizenz benötigt.
    Die Bereitstellung von Hardware- und Microsoft-Lizenzen im Rahmen einer DLS-Bestellung ist nicht möglich; diese Lizenzen müssen separat bestellt werden.

- Betriebssysteme für alle Bereitstellungen
  - Windows Server 2008 Enterprise Edition (64-Bit)
  - Windows Server 2008 Standard (64-Bit)
  - Windows Server 2008 R2 Standard und Enterprise Edition (64-Bit)
  - SUSE Linux Enterprise Edition (nur für die Integrated Simplex-Bereitstellung)

mit neuestem Service Pack und aktuellen Sicherheitspatches

Alle Betriebssysteme werden auch in der 64-Bit-Variante unterstützt.

Eine Linux Standalone-Bereitstellung ist derzeit nur im Rahmen einer OpenScape Voice-Bereitstellung möglich.

HINWEIS: Stellen Sie vor Durchführung einer Upgrade-Installation immer sicher, dass genügend freier Speicherplatz vorhanden ist.

WICHTIG: Bei Multi-Node-Installationen sollten die Netzwerkkartentreiber für die virtuelle IP-Adresse des Network Load Balancer (NLB) dynamische Änderungen der MAC-Adresse unterstützen, müssen also **Unicast** unterstützen.
Bei Verwendung von Unicast teilen sich alle Clusterhosts ein und dieselbe Unicast-MAC-Adresse. Der Network Load Balancer überschreibt die ursprüngliche MAC-Adresse des Clusteradapters mit der Unicast-MAC-Adresse, die allen Clusterhosts zugeordnet ist.
Weitere Informationen hierzu finden Sie in Abschnitt 4.3, “Konfiguration des Network Load Balancer”.

2.1.2 Systemkapazitäten

Die folgenden Tabellen zeigen die empfohlene maximale Anzahl von Endgeräten, die von einem Single-Node-DLS verwaltet werden können:

- Bei Verwendung von Microsoft SQL Server 2008 R2 Express Edition

Szenario	Max. Anzahl von:	Maximal
Nur HFA	HFA-Endgeräte	50.000
Nur SIP	SIP-Endgeräte	40.000
DLS Mobility	Mobile User	20.000
DLS Mobility	An- bzw. Abmeldungen von Mobile Usern pro Stunde (30 k Daten)	20.000
DlsAPI	DlsAPI-Sitzungen	100
Element Manager Synchronisation	Element Manager	100

- Bei Verwendung von Microsoft SQL Server 2008 R2 Enterprise Edition

Szenario	Max. Anzahl von:	Maximal
Nur HFA	HFA-Endgeräte + SIP-Endgeräte + Mobile User	100.000
Nur SIP		
DLS Mobility		
DLS Mobility	An- bzw. Abmeldungen von Mobile Usern pro Stunde (30 k Daten)	20.000
DlsAPI	DlsAPI-Sitzungen	100
Element Manager Synchronisation	Element Manager	100

- Bei Verwendung mit Microsoft SQL Server 2008 R2 Enterprise oder DataCenter Edition in einer Multi-Node-Bereitstellung mit zwei DLS-Knoten sowie synchroner Datenbankspiegelung und automatischem Failover (Redundanz-Szenario)

Szenario	Anzahl	Maximal
Anzahl der Knoten: 2		

Szenario	Anzahl	Maximal
DLS Mobility	An- bzw. Abmeldungen von Mobile Usern pro Stunde (30 k Daten)	20.000
Anzahl der Knoten: 3		
DLS Mobility	An- bzw. Abmeldungen von Mobile Usern pro Stunde (30 k Daten)	22.000
Anzahl der Knoten: 4		
DLS Mobility	An- bzw. Abmeldungen von Mobile Usern pro Stunde (30 k Daten)	24.000

HINWEIS: Zugrunde gelegt wird die Annahme, dass alle Anforderungen während des einstündigen Zeitfensters gleichmäßig eintreffen.
Beispiel: 20000/Stunde entspricht 330/Minute und 5,5/Sekunde.

HINWEIS: In Multi-Node-Umgebungen sind die tatsächlichen Systemkapazitäten abhängig von der verwendeten Serverhardware. Dies bedeutet, dass bei leistungsfähigerer Hardware höhere Zahlen möglich sind als die hier angegebenen.

2.1.3 Lizensierung

Für das Einrichten der Basis-Software sowie von Basis-Geräten, mobilen Benutzern (Mobile User) und PKI-Benutzern, das Nutzen von DLS-Knoten im Cluster, sowie der Datenbankspiegelung, der XML Push-Funktionalität und des Location Service (IP Infrastruktur) ist eine kostenpflichtige Lizensierung erforderlich. Alle weiteren Funktionen des DLS sind kostenfrei.

Die erforderlichen Lizenzen werden über das HiPath Lizenz-Management auf dem Lizenzagenten eingespielt. Die Angabe des Lizenzagenten erfolgt bei der Installation des DLS bzw. nachträglich unter **Administration** > **Server Lizenzen**.

Lizenzagent und -Management stehen auf dem C-SWS zum Download zur Verfügung.

Für Testinstallationen werden folgende Übergangslizenzen gewährt, bestehend aus:

- 1 Base Software Lizenz (30 Tage)
- 500 Basic Device Lizenzen (= registrierte IP Devices) (30 Tage)
- 10 Mobile User Lizenzen (30 Tage)

- 10 PKI User Lizenzen (30 Tage)
- 1 Location Service Lizenz (30 Tage)
- 1 Knoten Lizenz (30 Tage)
- 1 Datenbankspiegelung Lizenz (30 Tage)
- 1 XML Push Lizenz (30 Tage

Lizenzinstallation bei einer OpenScape Onboard-Installation

Bei einer Linux DLS-Bereitstellung in einer Integrated Simplex-Umgebung, bei der die DLS-Lizenzen in den CLA der OSV (intern) geladen werden, sind folgende Anweisungen zu beachten:

1. Kopieren Sie die DLS-Lizenzdatei in das Verzeichnis: `/opt/unisphere/srx3000/cla/import .`
2. Warten Sie einige Minuten, bis die Lizenz aktiviert ist.

   HINWEIS: Die Lizenzdatei wird kopiert nach: `/opt/unisphere/srx3000/cla/license`.
3. Überprüfen Sie abschließend, ob die Lizenzdatei in folgendem Verzeichnis vorhanden ist: `/opt/unisphere/srx3000/cla/license`.

2.1.4 Installation der DLS-Software

Die Installation geschieht in folgenden Schritten:

1. Laden Sie die DLS-Software vom SWS-Server herunter und entzippen Sie die heruntergeladene Datei.
2. Klicken Sie auf *setup.exe*.
3. Folgen Sie der Benutzerführung der Installationsroutine.

Die von DLS benötigten Komponenten wie Datenbank und Webserver werden installiert, falls noch nicht auf dem System vorhanden.

2.2 Erstinbetriebnahme des DLS (Single Mode)

1. Programmstart

Zum Starten des DLS-Client verwenden Sie die folgende URL-Syntax:

- **http://<IP des DLS-Servers>:18080/DeploymentService/** (Verbindung zum Windows-DLS über http)
- **https://<IP des DLS-Servers>:10443/DeploymentService/** (sichere Verbindung zum Windows-DLS über https)
- **https://<IP des DLS Servers>/DeploymentService/** (Linux / OSV integriert)
  [IP-Adresse des Servers]:18080/DeploymentService/ oder
  https://[IP-Adresse des Servers]:10443/DeploymentService/ (verschlüsselte Verbindung über Secure HTTP).

Wenn der Client auf demselben Computer (Windows) läuft wie der DLS-Server:

- **http://localhost:18080/DeploymentService/** (Standard)
  HINWEIS: <IP des DLS-Servers> ist die IP-Adresse des Windows-Servers. Bei Multi-Node-Konfigurationen ist dies die virtuelle IP-Adresse, die beim Cluster-Setup der Multi-Node-Konfiguration angegeben wird.

  Bei IPv6 ist die Angabe von eckigen Klammern erforderlich, z. B. **http://[2000.1..100]:18080/DeploymentService/**
  oder es wird dringend empfohlen, Hostnamen, DNS-Namen anzugeben, z. B.
  http://MyDlsServer:18080/DeploymentService/
  oder
  http://MyDlsServer.myDomain.com:18080/DeploymentService/

  HINWEIS: In der Sicherheitscheckliste des DLS wird die Verwendung von sicheren Zugriffsmethoden empfohlen.

2. Login

Loggen Sie sich mit dem Account „admin“ mit dem bei der Installation vergebenen Passwort ein.

Standardmäßig gelten für die Anmeldung am DLS folgende Vorgaben:

Account: **admin**

Passwort: **Asd123!.**

HINWEIS: Beachten Sie bei dem Passwort das groß geschriebene ‘S’, da bei Passwörtern zwischen Groß- und Kleinschreibung unterschieden wird.

3. Passwörter ändern / Accounts einrichten

Es ist empfohlen, für jeden DLS Administrator einen eigenen Account im DLS einzurichten. Dies kann nur mit dem Standard-Account „admin“ erfolgen. Wählen Sie hierzu in der Menüleiste **Administration > Account Management**. Klicken Sie auf **Suchen**. Wenn sie zur Ansicht **Tabelle** wechseln, erhalten Sie die Daten aller Accounts in tabellarischer Übersicht. Über **Neu** können Sie einen neuen Account anlegen.

4. Standort-Konfiguration

Mithilfe des Standorts können Sie Gruppen von Endgeräten definieren, die jeweils einen Bereich von IP-Adressen und/oder den Anschluss an bestimmte Anlagen gemeinsam haben. Nehmen Sie die Grundkonfiguration des Standorts wie folgt vor:

Legen Sie in **Administration** > **Server Konfiguration** > **Standort** > **Register „IP Bereiche“** den IP-Adressbereich für den Standort fest.

Tragen Sie in **Administration** > **Server Konfiguration** > **Standort** > **Register „Reg-Adressen“** die IP-Adressen oder Hostnamen der Anlagen (PBX/Gateway oder SIP Server) für den Standort ein.

Die weiteren Konfigurationsmöglichkeiten finden Sie unter **Administration** > **Server Konfiguration** > **Standort**.

Fall Sie keinen Standort definieren, bekommen alle standortabhängigen Parameter den Standort „Default Location“ zugewiesen.

5. FTP-Konfiguration

Um IP Phone-Software sowie andere Dateien auf die Endgeräte zu laden, ist ein FTP-Server erforderlich, der die Software-Images bereitstellt. Der DLS unterstützt die Konfiguration und Verwendung beliebig vieler FTP-Server. Um die Zugangsdaten zu einem FTP-Server einzugeben, gehen Sie auf **Administration > Server Konfiguration > FTP Server Konfiguration**. Mit der Aktionsschaltfläche **Neu** legen Sie einen neuen FTP-Server an.

Im Feld **Server ID** geben Sie einen Namen für den FTP-Server ein, den Sie für die Übertragung der IP Phone-Software verwenden wollen.

Geben Sie im Feld **Hostname** den Netzwerknamen bzw. die IP-Adresse des FTP-Servers ein.

Im Feld **SW Image Pfad** wird der Pfad zum Verzeichnis mit den Software-Imagedateien angegeben. Diese Pfadangabe versteht sich als relativ gegenüber dem Root-Verzeichnis der vom DLS benutzten FTP-Benutzerkennung. Befinden sich die Imagedateien direkt im Root-Verzeichnis, geben Sie als Pfad „./“ ein.

Im Feld **Benutzer** geben Sie die Benutzerkennung ein, mit dem sich der DLS am FTP-Server anmelden soll. Im Feld **Passwort** geben Sie das dazugehörige Passwort ein.

Über **Test** können Sie mit einem FTP-Verbindungstest die Richtigkeit der Einstellungen prüfen. Übernehmen Sie die Eingaben durch Klick auf **Sichern**.

Eine Beschreibung aller Felder und weitere Hinweise finden Sie im Abschnitt 6.3.4, “FTP Server Konfiguration”.

6. HTTPS-Konfiguration (für OpenStage-Endgeräte)

OpenStage-Telefone können zum Download von Dateien alternativ einen HTTPS-Server verwenden.

Im Feld **HTTPS-Server ID** geben Sie einen Namen für den HTTPS-Server ein, den Sie für die Übertragung von Dateien verwenden wollen.

Geben Sie im Feld **HTTPS-Server URL** den Netzwerknamen bzw. die IP-Adresse des HTTPS-Servers ein.

Eine Beschreibung aller Felder und weitere Hinweise finden Sie im Abschnitt 6.3.5, “HTTPS Server Konfiguration”.

7. Plug & Play/Autokonfiguration

Der DLS bietet die Möglichkeit, IP Devices vorzukonfigurieren, so dass diese sogleich nach dem Anschließen ans Netzwerk in Betrieb gehen können. Hierzu überträgt der DLS die erforderlichen Konfigurationsparameter zum IP Device. Für IP Devices (IP Phones, IP Clients, IP Gateways) gilt dies insbesondere für die rufnummern-abhängigen Daten zur Registrierung an der Telefonanlage. Um die erforderlichen Daten aus der Telefonanlage in die DLS-Datenbank zu übernehmen, muss der DLS die Zugangsdaten zur Anlage erhalten. Geben Sie diese auf **Element Manager** > **Element Manager Konfiguration** ein.

Mithilfe von Profilen können Sie Standardkonfigurationen für mehrere Geräte erstellen. Geräteprofile setzen sich aus Templates, d.h. den zusammengefassten Einstellungen einzelner Masken sowie Informationen über die vom jeweiligen Profil unterstützte Geräte und Gatekeeper sowie IP-Bereiche. Die Konfiguration erfolgt unter **Profil Management** > **Geräteprofil**.

Wollen Sie einzelne Parameter für ein bestimmtes Gerät einstellen, können Sie ein sog. virtuelles Gerät anlegen. Gehen Sie hierzu auf **IP Device Verwaltung** > **IP Device Konfiguration** und klicken Sie auf die Aktionsschaltfläche **Neu**. Das virtuelle Gerät erhält anstelle der Device ID einen Platzhalter, der mit „@“ beginnt, und IP-Adresse sowie E.164-Nummer sind auf 0 gesetzt. Damit ein physisches Gerät zugeordnet

werden kann, müssen entweder eine E.164-Nummer oder eine echte Device ID (in der Regel die MAC-Adresse) eingegeben werden. Das Symbol  neben dem Feld **Gerätetyp** zeigt an, dass sich das IP Device noch nicht beim DLS registriert hat. Ansonsten erfolgt die Konfiguration wie bei einem angeschlossenen, registrierten Gerät.

HINWEIS: Ein Endgerät wird über das Wertepaar Device ID und E.164 vom DLS erfasst. Bei sämtlichen Konfigurationsmasken befinden sich diese Angaben in der oberen Hälfte der Bedienoberfläche. Achten Sie darauf, dass hier die Daten des IP Devices stehen, das Sie konfigurieren wollen, damit die Konfigurationsdaten dem richtigen IP Device zugewiesen werden.

2.3 Erforderliche Workpoint-Firmware installieren

Wird ein Endgerät bei laufendem DLS erstmals angeschlossen, so erhält es automatisch die aktuellste verfügbare Software. Für die Hochrüstung bereits angeschlossener Endgeräte ist das Auto-Deployment zuständig. Voraussetzung ist ein laufender FTP-Server und eine korrekte FTP-Konfiguration im DLS (siehe Abschnitt 2.2, “FTP-Konfiguration”). Die Image-Dateien der Firmware müssen sich in dem Verzeichnis befinden, das bei der FTP-Konfiguration als **SW Image Pfad** angegeben wurde. Sie können auch in Unterverzeichnissen gruppiert sein.

2.3.1 Software-Images automatisch anlegen

Nachdem die Images auf dem FTP-Server liegen, kann der DLS diese automatisch registrieren. Dabei werden den Dateien Informationen u. a. über den passenden Gerätetyp, den Software-Typ (SIP oder HFA) und die Software-Version zugeordnet. Die automatische Registrierung können Sie anstoßen, indem Sie auf Software **Deployment** > **Software Images bearbeiten** gehen und dort auf **Automatisch Anlegen** klicken. Im daraufhin erscheinenden Dialogfenster klicken Sie auf **Start**.

2.3.2 Auto Deployment

Sobald ein neues Endgerät am DLS registriert wird, erfolgt ein Software Deployment nach zuvor festgelegten Regeln. Diese Regeln werden wie folgt erstellt:

1. Klicken Sie im Bereich **Software Deployment > Regeln bearbeiten** auf **Neu**.
2. Wählen Sie im Feld **Gerätetyp** den Typ des Endgeräts aus. Zu beachten ist, dass es für jeden Gerätetyp nur eine Regel geben kann.
3. Wählen Sie im Feld **SW Typ** den richtigen Software-Typ aus.
4. Wenn Sie möchten, dass ein Software-Deployment mit der neusten verfügbaren Software durchgeführt wird, aktivieren Sie **Deploy neueste Version**.

   Wenn Sie wollen, dass dann eine von Ihnen angegebene Software-Version installiert wird, wenn die zuvor installierte Software älter ist, aktivieren Sie **Deploy Service bei einem Upgrade** und wählen Sie im Feld **SW Image** das gewünschte Firmware-Image.

   Wollen Sie , dass dann eine von Ihnen angegebene Software-Version installiert wird, wenn die zuvor installierte Software neuer ist, aktivieren Sie **Deploy Service bei einem Downgrade** und wählen Sie im Feld **SW Image** das gewünschte Firmware-Image.

2.3.3 Manuelles Deployment

1. Gehen Sie auf **Software Deployment > Workpoint Deployment**. Wählen Sie in der oberen Hälfte der Benutzeroberfläche das Endgerät aus, auf dem Sie die Software installieren wollen. Klicken Sie auf **Deploy**.
2. Es erscheint ein Fenster mit einer Liste sämtlicher verfügbarer Software. Per Voreinstellung ist nur solche Software anwählbar, die zum Typ des aktuell ausgewählten Endgeräts passt. Wählen Sie nun die gewünschte Software an und klicken Sie auf **Deploy**.
3. Es öffnet sich ein Dialog, in dem Sie den Zeitpunkt des Deployments einstellen können. Die Checkboxen **Deployment erzwingen falls Gerät belegt ist** und Deployment **Einschränkungen überschreiben** sollten nicht angekreuzt werden. Ein Klick auf **OK** setzt das Deployment in Gang.

2.4 Auswahl häufig genutzer Funktionen

2.4.1 IP Devices scannen

Beim Scannen erfasst der DLS die Daten der IP Devices. Hierzu ist es nicht erforderlich, dass die IP Devices am DLS registriert sind.

1. Gehen Sie auf **IP Devices > IP Device Interaktion > IP Devices scannen**. Um einen Scan zu veranlassen, benötigen Sie ein Scanner-Objekt. Falls bereits eines erstellt wurde, können Sie es suchen, indem Sie auf **Suchen** klicken. Andernfalls müssen Sie ein Scanner-Objekt erzeugen. Klicken Sie hierzu auf **Neu**. Im **Register „IP Bereiche“** geben Sie im Feld **IP-Scanner** einen Namen für das Objekt ein, z. B. **Scanner 1**. Als nächstes geben Sie den Bereich von IP-Adressen ein, der gescannt werden soll. Klicken Sie hierzu auf das Symbol  . In die jetzt aktivierten Felder **IP Adresse von** und **IP-Adresse bis** geben Sie die entsprechenden Werte ein. Das Feld **Port** enthält als Voreinstellung 8085; dies ist der Default-Port für HTTP bei IP Phones. Wenn Sie nun auf **Sichern** klicken, ist das Scanner-Objekt einsatzbereit.

   HINWEIS: In der Standardeinstellung sendet der DLS an jede IP-Adresse des zu scannenden Bereichs einen ICMP-Ping. Falls im Netzwerk keine ICMP-Pings zugelassen sind, muss der Schalter **ICMP Pings zulassen** unter **IP Devices** > **IP Device Interaktion** > **IP Devices scannen** > **Register „Konfiguration“** deaktiviert sein.

2. Durch Klick auf die Schalftläche **IP Devices scannen** starten Sie den Scanvorgang.

Näheres zu diesem Thema erfahren Sie in Abschnitt 7.4.6, “IP Devices scannen”.

2.4.2 Konfiguration von Parametern: Beispiel Tastenbelegung

Die Konfiguration von Parametern an einzelnen IP Devices soll nun anhand der Tastenbelegung demonstriert werden. Es soll die Funktion und der Text einer Funktionstaste konfiguriert werden. Als Beispiel-Funktion dient der Mobility-Key, mit dem sich ein Benutzer als Mobile User am Telefon anmelden kann.

1. Gehen Sie auf **IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung**. Klicken Sie auf **Suche** und wählen Sie anschließend das Endgerät in der Ansicht **Tabelle**. Zu den Einstellungen im Register **Keysets** siehe Abschnitt 7.1.19.1, “Register „Keysets“”.

2. Um einen neuen Eintrag zu erzeugen, gehen Sie in das Register **Ziele** und klicken Sie auf das Symbol  . Es erscheint eine neue Tabellenzeile.

3. Da sich die Tastenfunktion **Mobility** in der 1. Ebene befindet, treffen Sie in der Spalte **Ebene** die Auswahl „1. Ebene“.

4. Wählen Sie nun in der Spalte **Tastennummer** die Taste aus, der die neue Funktion zugewiesen werden soll. Siehe hierzu Abschnitt 7.1.19.2, “Register „Ziele“”.

5. In der Spalte **Tastenfunktion** wählen Sie „Mobility“.

6. Schließlich können Sie noch in der letzten Spalte einen Tastentext eintragen. Dieser wird nur bei Modellen der optiPoint 420-Familie sichtbar, die über eine automatische Tastenbeschriftung verfügen.

Schließen Sie die Aktion durch **Sichern** ab.

2.4.3 Jobs

Alle Aktionen, die per DLS an IP Devices durchgeführt werden, wie beispielsweise das Konfigurieren der Tastenbelegung, werden vom DLS als Job verwaltet.

Mithilfe der Job-Kontrolle können Sie Informationen zu einzelnen Jobs ansehen, Jobs abbrechen, löschen oder erneut aktivieren. Gehen Sie hierzu auf **Job Koordination > Job Kontrolle**.

Grundsätzlich lassen sich Jobs sowohl sofort als auch zu einem bestimmten, vorgewählten Zeitpunkt starten. Um beispielsweise die in Abschnitt 2.4.2, “Konfiguration von Parametern: Beispiel Tastenbelegung” durchgeführte Aktion zu einer bestimmten Zeit durchzuführen, führen Sie alle Schritte bis auf das abschließende **Sichern** wie beschrieben aus. Tragen Sie dann in das rechts oben befindliche Feld **Job ID** eine frei vergebbare Job-ID ein und wählen Sie durch Klick auf das Symbol  neben dem Feld **Ausführungszeit** den Zeitpunkt, an dem die Aktion ausgeführt werden soll. Hiernach aktivieren Sie den Job durch **Sichern**.

Weitergehende Informationen zur Job-Koordination finden Sie in Abschnitt , “Job Koordination”.

2.5 Einsatz der Mobility-Funktion

Mit der Mobility-Funktion lassen sich Rufnummern alternativ zu Endgeräten bestimmten Personen zuteilen. Neben seiner Rufnummer kann der Benutzer persönliche Einstellungen, wie etwa die Tastenbelegung, vom einen zum anderen Endgerät mitnehmen. An einem dafür freigegebenen Endgerät muss er sich hierzu mit seiner Rufnummer und einem Passwort anmelden. Mit der Anmeldung werden die Rufnummer des Endgeräts und alle weitere Benutzerdaten durch die Daten des neuen Benutzers ausgetauscht. Nach der Abmeldung erhält das Endgerät seine ursprüngliche Rufnummer und Benutzerdaten wieder zurück.

Um die Mobility-Funktion benutzen zu können, muss ein Profil für einen Mobile User erstellt werden. Identifiziert wird dieses Profil durch eine Rufnummer und ein Passwort. Hierzu gibt es zwei Möglichkeiten: Erstellung durch Hinzufügen oder Erstellung durch Migrieren eines Basis-Profils. Letzteres wird im folgenden beschrieben.

1. Voraussetzung für die Nutzung der Mobility-Funktion ist die Freigabe eines Workpoints für die Anmeldung eines Mobile Users. Gehen Sie dazu auf **IP Devices > IP Phone Konfiguration > SIP Mobility** und aktivieren Sie im **Register „SIP Mobility“** die Option **„**Endgerät verfügbar für Mobile User**“**. Die Aktivierung dauert einige Sekunden und läuft im Hintergrund.
2. Gehen Sie auf **Mobile User > SIP Mobile User Interaktion > SIP Mobile User**. Wenn Sie nun im Feld **Anwender Typ** „Endgerät für Mobile User“ wählen und danach auf **Suchen** klicken, bekommen Sie in der Ansicht **Tabelle** eine Auflistung all derjenigen Endgeräte, die für einen Mobile User verfügbar sind.
3. Klicken Sie auf **Migration zu Mobile User**. Daraufhin erscheint ein Dialogfenster.
4. Geben Sie nun im Feld **Neue Basis E.164** für das aktuell ausgewählte Endgerät, dessen Basisprofil migriert werden soll, eine neue Basis-Rufnummer ein. Diese muss am SIP-Server registriert sein. Eine neue Basis-Nummer ist nötig, damit das Endgerät auch ohne angemeldete Mobile User einsatzbereit bleibt. Weiterhin muss für diese Basis-Rufnummer ein virtuelles Gerät existieren, das die erforderlichen Plug&Play-Daten zur Verfügung stellt (siehe Abschnitt 15.5.2.2, “Plug&Play-Daten anlegen”). Sobald die Migration erfolgt ist, wird die bisherige Basis-Rufnummer dem Mobile User zugeordnet. Die Rufnummer eines Mobile Users wird auch als Mobility ID bezeichnet.

5. In das Feld **Basis Mobile User Profil** muss ein neues Profil für den Basis User (die Basis-Rufnummer) eingetragen werden. Der Mobile User übernimmt die Daten und die Rufnummer des Endgeräts, wobei diese Daten automatisch sein neues individuelles Profil bilden. Sucht man nach Abschluss der Aktion nach dem Mobile User, wird im Feld Mobile User Profile die Rufnummer des Mobile Users angezeigt mit einem vorangestellten „@“. Dies ist ein Platzhalter für sein individuelles Profil.
6. Starten Sie die Migration über **Starte Migration**.
7. Geben Sie nun im Feld Mobile User Passwort ein neues Passwort für den Mobile User ein (das Default-Passwort ist „000000“). Bestätigen Sie abschließend mit **Sichern**.

2.6 Security

2.6.1 Zertifikate

Zertifikate ermöglichen eine sichere Authentisierung zwischen Server und Client. Sie können bei folgenden Server-Client-Konstellationen eingesetzt werden:

- WebServer Zertifikate für web-based Management (WBM in IP Phones/IP Gateways)
- Zertifikate für IEEE 802.1x/EAP-TLS Authentifizierung (nur IP Phones)
- TLS-basierte Signaling Encryption (alle Gerätetypen)
- zusätzliche Server Applikationen für IP Phones (z.B. LDAPS)

Mit dem DLS lässt sich der Einsatz von Zertifikaten administrieren.

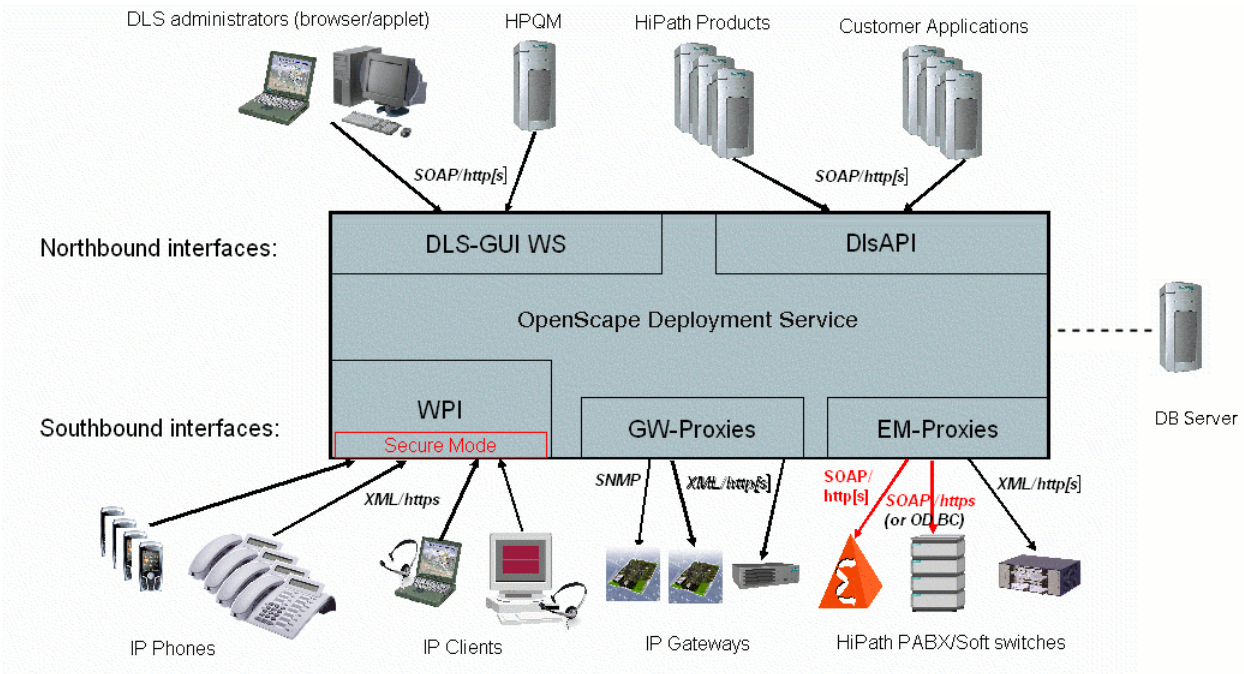
Siehe hierzu Abschnitt 16.12, “Security: Administration von Zertifikaten”.

3 Konzept und Leistungsmerkmale

3.1 Übersicht

Der OpenScape Deployment Service (DLS) ist eine OpenScape Management Anwendung zum Administrieren von IP Devices (IP Phones, IP Client-Installationen und IP Gateways) in HiPath- und nicht-HiPath-Netzwerken. Die Datenbank des DLS kann optional auf einen eigenen Server ausgelagert werden.

Die nachfolgende Übersicht zeigt mögliche Komponenten, die in einem Netzwerk zusammen mit dem DLS arbeiten können.



HINWEIS: Es wird empfohlen, einen DHCP-Server im DLS-Umfeld einzusetzen, um

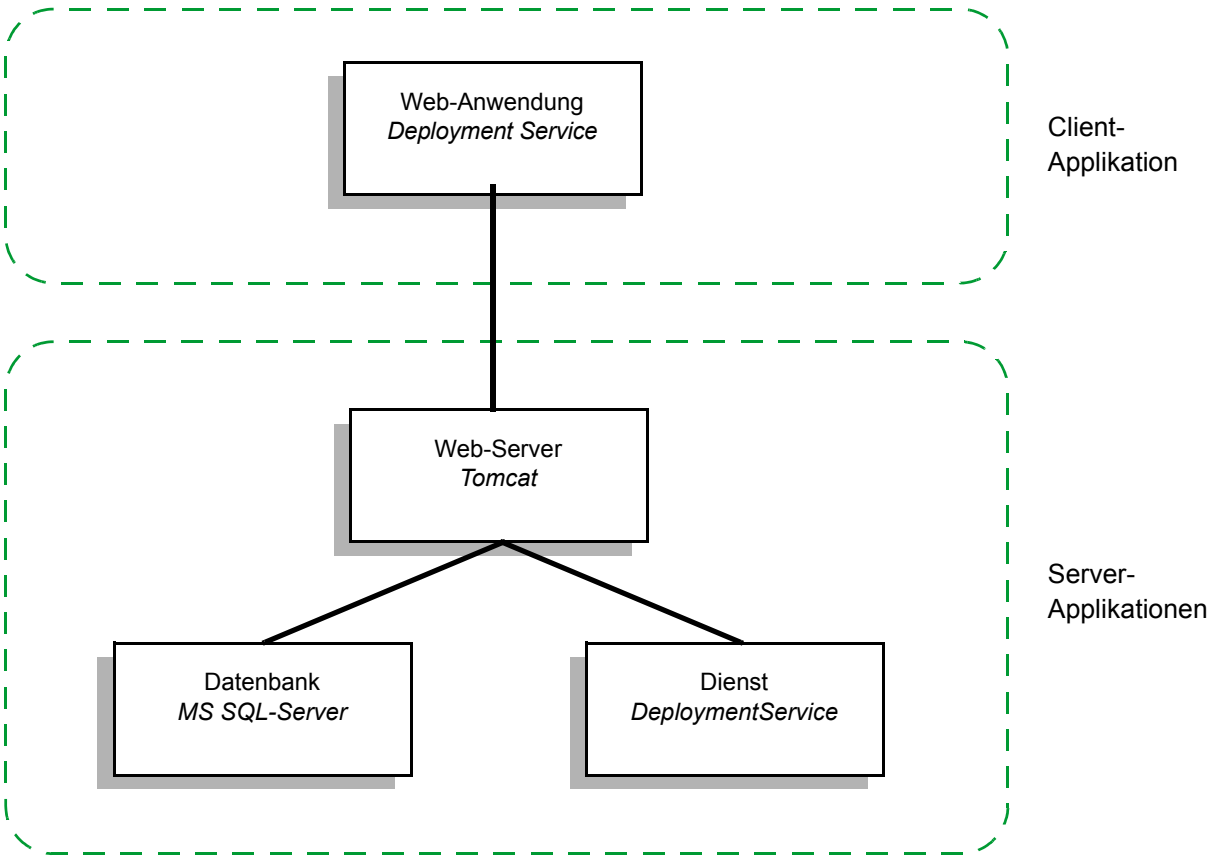
- Plug&Play zu unterstützen und
- die Authentizität des DLS-Servers sicherzustellen.

Der DHCP-Server sollte möglichst frühzeitig eingerichtet werden; wenn möglich noch vor der Installation der IP Devices.

Es ist nur ein DLS-Server pro DHCP-Domain beim Kunden erlaubt.

3.2 Komponenten des OpenScape Deployment Service

Die nachfolgende Übersicht zeigt die Komponenten, die beim Betrieb des OpenScape Deployment Service auf Server- und Client-Seite beteiligt sind.



Die Client-Applikationen können sowohl auf einem im IP-Netz erreichbaren Client-PC, als auch auf dem Server-PC selbst ausgeführt werden.

HINWEIS: Achten Sie beim getrennten Betrieb von Server und Client auf eine Synchronisation der Betriebssystem-Zeiten.

3.3 Grundsätzliches zur Bedienung

Um IP Devices mit dem DLS konfigurieren zu können, müssen nach der Neuinbetriebnahme des DLS zunächst alle IP Device-Daten „gesammelt“ werden. Das heißt, die Konfigurationsdaten in den IP Devices müssen zunächst in die Datenbank des DLS-Servers übernommen werden.
Dies geschieht dadurch, dass sich die IP Devices am DLS registrieren und diese Daten zum DLS übertragen.

Das Auslesen der IP Device-Daten erfolgt durch

- Scannen der IP Devices mittels DLS, siehe Abschnitt 7.4.6, “IP Devices scannen”
  (sinnvoll, wenn nach der DLS-Neuinbetriebnahme bereits eine Reihe von IP Devices in Betrieb sind)

  oder durch

- Einstecken des LAN-Steckers bzw. der Stromversorgung am IP Device
  (sinnvoll, wenn einzelne weitere IP Devices in Betrieb genommen werden).

Jede Aktion, die Sie mithilfe des DLS ausführen, sei es nun eine Aktualisierung der Workpoint-Software oder das Ändern von Konfigurationsdaten, wird im DLS protokolliert.

Sie werden dabei von der Job-Koordination unterstützt. Hierin können Sie zu jeder Aktion den Status ansehen und im Fehlerfall die Ursache erkennen. Siehe hierzu Abschnitt , “Job Koordination”.

3.4 Einsatzgebiet

HINWEIS: Zu den aktuell existierenden Unterstützungen/Einschränkungen lesen Sie bitte die Release Notes bzw. die Vertriebsfreigabe der tatsächlich eingesetzten Version.

Mit dem DLS können Sie die folgenden IP Devices administrieren:

IP Device	HFA Version	SIP Version
AC-Win 2Q IP	alle Versionen	alle Versionen
AC-Win MQ IP	alle Versionen	alle Versionen
HG1500		
HG3500		
HG3575		
HOOEE (HiPath OpenOffice EntryEdition)	alle Versionen	alle Versionen
HOOME (HiPath OpenOffice MediumEdition)	ab V1.0	ab V1.0
HP2K V2.0	ab V2.0	ab V2.0
optiClient 130	ab V5.0	ab V2.0
Unify OpenScape Desktop Client	alle Versionen	alle Versionen
optiPoint 400 economy	ab V5.0	-
optiPoint 400 standard	ab V5.0	-
optiPoint 410 entry	ab V5.0	ab V4.1
optiPoint 410 economy	ab V5.0	ab V4.1
optiPoint 410 economy plus	ab V5.0	ab V4.1
optiPoint 410 standard	ab V5.0	ab V4.1
optiPoint 410 advance	ab V5.0	ab V4.1
optiPoint 420 economy	ab V5.0	ab V4.1
optiPoint 420 economy plus	ab V5.0	ab V4.1
optiPoint 420 standard	ab V5.0	ab V4.1
optiPoint 420 advance	ab V5.0	ab V4.1
optiPoint 600 office	alle Versionen	-
optiPoint WL2 professional S	-	V1.0 (50/70)
optiPoint WL2 professional	V1.0 (50)	-
OpenStage 5	alle Versionen	alle Versionen
OpenStage 15	alle Versionen	alle Versionen
OpenStage 20E	alle Versionen	alle Versionen
OpenStage 20	alle Versionen	alle Versionen
OpenStage 40	alle Versionen	alle Versionen
OpenStage 60	alle Versionen	alle Versionen

Tabelle 2 Unterstützte IP Devices/Versionen

IP Device	HFA Version	SIP Version
OpenStage 80	alle Versionen	alle Versionen
OpenScape Desk Phone IP 35 G	alle Versionen	alle Versionen
OpenScape Desk Phone IP 55 G	alle Versionen	alle Versionen

Tabelle 2 Unterstützte IP Devices/Versionen

HINWEIS: Auf folgenden Gerätetypen ist die Mobility-Funktionalität ab SIP V6.0 verfügbar: optiPoint 410 economy, optiPoint 410 economy plus, optiPoint 410 standard, optiPoint 410 advance, optiPoint 420 economy, optiPoint 420 economy plus, optiPoint 420 standard, optiPoint 420 advance.

Auf folgenden Gerätetypen ist die Mobility-Funktionalität in allen Versionen verfügbar: OpenStage 20E, OpenStage 20, OpenStage 40, OpenStage 60, OpenStage 80.

Die Administration ist für unterschiedliche Kommunikationsplattformen möglich. Sowohl HiPath- als auch nicht-HiPath-Plattformen werden unterstützt:

Plattform	P&P Anbindung	Plug&Play	QDC Anbindung	QDC	SRTP Anbindung	SRTP
OpenOffice EE V1.0	stand-alone	nein	nein	nein	nein	nein
OpenScape Office MX/LX	stand-alone	nein	nein	nein	nein	nein
HiPath 3000/5000 <V5.0	stand-alone	nein	nein	nein	nein	nein
HiPath 3000/5000 V5.0	HG1500	ja	HG1500	ja	nein	nein
HiPath 3000/5000 V6.0	HG1500	ja	HG1500	ja	HG1500	ja
HiPath 3000/5000 V7.0	HG1500	ja	HG1500	ja	HG1500	ja
HiPath 4000 V1.0	Assistant	ja	nein	nein	nein	nein
HiPath 4000 V2.0	Assistant	ja	HG3530/50/70/75	ja	nein	nein
HiPath 4000 V3.0	Assistant	ja	HG3530/50/70/75	ja	HG3530/50	ja
HiPath 4000 V4.0 / V5	Assistant	ja	HG3500/75	ja	HG3500/75	ja
HiPath 4000 V6[1]	Assistant	ja	HG3500/75	ja	HG3500/75	ja
OpenScape Voice V3.1	SOAP I/F H8000	ja	nein	nein	nein	nein
OpenScape Voice V3.1	Assistant	ja	nein	nein	nein	nein
OpenScape Voice V4.0	SOAP I/F H8000	ja	nein	nein	nein	nein
OpenScape Voice V4.0	Assistant	ja	nein	nein	nein	nein
OpenScape Voice V4.1	Assistant	ja	nein	nein	nein	nein
HiPath DX V9	DX WebPro	ja	nein	nein	nein	nein
HiPath RG2700 V1.0	nicht relevant	nein	RG2700	ja	nein	nein

Tabelle 3 Unterstützte Kommunikationsplattformen

1 Parametereinstellungen für HiPath 4000 gelten auch für HiPath 4000 V6, soweit nicht anders vermerkt.

HINWEIS: Werden SIP IP Phones an den Plattformen HiPath 3000 und HiPath 4000 betrieben, so sind einige Leistungsmerkmale nicht verfügbar. Deaktivieren Sie diese am Workpoint, damit sie für den Benutzer nicht sichtbar bzw. auswählbar sind.

Siehe hierzu Abschnitt 7.1.4.4, “Register „Verfügbarkeit“”.

3.5 Übersicht der Software- und Datei-Typen

Die folgende Tabelle zeigt, wie der DLS in der Standardkonfiguration Dateiendungen und Dateitypen einander zuordnet.

HINWEIS: Der Administrator kann die Dateiendungen nach Wunsch ändern in der Datei `file_map.xml`, die sich unter `DeploymentService\Tomcat5\webapps\DeploymentService\WEB-INF\classes` befindet.
Um zur Standardkonfiguration zurückzukehren, kopieren Sie `default_file_map.xml` und benennen Sie es um in `file_map.xml`.

Objekttyp (Name im DLS)	Dateierweiterung	Beispiel	Inhalt
Software-Objekte			
Software Image	*.img	opera_bind.img	OpenStage-Firmware
Software Image	*.app	optiPoint410std-V5.0.0.app	DLS-kompatible optiPoint-Firmware („neues Format“)
Software Image (alt)	*.app	vxWorks.app	nicht kompatible optiPoint-Firmware („altes Format“)
Software Image	*.exe	setup.exe	PC-Softwareinstallation
Firmware (Netboot)	*.fli	vxWorks.fli	Software-Image für Übertragung via Netboot-Server
		netboot308.fli	Netboot-Firmware
Datei-Objekte			
LDAP Template	*.ldap	ldap_temp.ldap	LDAP-Template für optiPoint und OpenStage 40/60/80
	*.txt	ldap_template.txt	LDAP-Template für OpenStage 40/60/80

Tabelle 4 Unterstützte Software- und Datei-Typen

Music On Hold (Wartemusik)[1] [2]	*.moh	opti410.moh	Proprietäres Format für optiPoint und OpenStage.
	*.wav	music.wav	Audiodatei im WAV-Format für OpenStage. Empfohlene Spezifikationen: Audioformat: PCM Bitrate: 16 kB/sec Samplingrate: 8 kHz Quantisierung: 16 bit
	*.mp3	music.mp3	Audiodatei im mp3-Format für OpenStage 60/80.
	*.mid	music.mid	MIDI-Datei für OpenStage.
Screen Saver (Bildschirmschoner)[2]	*.jpg	screenPic1.jpg	Bilddatei für den Bildschirmschoner des OpenStage 60/80. Auflösung: OpenStage 60: 320x240 OpenStage 80: 640x480
	*.png	screenPic1.png	
INCA Firmware	*.h86	inca.h86	INCA-Firmware zum optiPoint 600 office
JAVA Midlet	*.jad	?	Java-Anwendung
-	*.jar[3]	?	Java-Archiv
Logo Datei[2]	?	?	
	*.jpg		Bilddatei für ein Logo auf dem OpenStage. Empfohlene Spezifikationen für OpenStage 60: Breite: 240 px Höhe: 70 px Auflösung: 70,55 dpi Empfohlene Spezifikationen für OpenStage 80: Breite: 480 px Höhe: 148 px Auflösung: 124,5 dpi
	*.png		
System- und Rufton[1] -	*.xml	?	System- und Klingeltöne
	*.wav	?	
	*.mp3	?	
	*.mid	?	
	*.app	bootrom.app	Boot-Lader zum optiPoint 600 office
-	?	?	Neue/andere Applikationen
-	?	?	DSM-Firmware
-	*.csv	?	Für ENB-Import/-Export
Dongle Keys	*.key	dongle.key	Dongle Keys für OpenStage Remote Test Tool

Tabelle 4 Unterstützte Software- und Datei-Typen

1 Nur für SIP-Variante.
2 Ruftondateien dürfen nicht größer als 1 MB, Screensaver- und Logo-Dateien nicht größer als 300 kB sein.
3 Nur in Verbindung mit einer *.jad-Datei.

Bei LDAP wird ein LDAP-Template auf dem Telefon bereitgestellt, über das das Telefon auf das Unternehmensverzeichnis zugreifen kann. Bei dem Template handelt es sich um eine einfache, kurze Liste von Attributen in Form einer Textdatei. Diese Datei wird von dem Telefon verwendet, um mit einem LDAP-Server zu kommunizieren (der sich normalerweise im DNS befindet) und um Verzeichnisabfragen durchzuführen (beispielsweise um einen Kontakt im Unternehmen zu suchen und seine Telefonnummer zu finden). Über das Template werden Telefone und LDAP-Server-Einträge einander zugeordnet. Welche Attribute im Template enthalten sind, hängt ab von den Menüelementen des Telefon-Unternehmensverzeichnisses und dem verwendeten LDAP-Typ (z. B. Microsoft 2008 R2 LDAP).

Nachstehend sehen Sie ein Beispiel-Template eines Microsoft 2008 R2 LDAP-Servers für OpenStage-Telefone und DPIPs.
Es enthält nützliche Informationen und erspart Ihnen bei der Ersteinrichtung von LDAP-Unternehmensverzeichnissen viel Zeit:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE=”CN=Users,DC=opera,DC=local”
ATTRIB01=”sn”
ATTRIB02=”givenName”
ATTRIB03=”telephoneNumber”
ATTRIB04=”otherTelephone”
ATTRIB05=”mobile”
ATTRIB06=”homePhone”
ATTRIB07=”company”
ATTRIB08=”department”
ATTRIB09=”l”
ATTRIB10=”title”
ATTRIB11=”mail”
EOF
```

HINWEIS: Der Administrator sollte für jedes LDAP-Verzeichnis die richtige Suchbasis (SEARCHBASE) eingeben. Diese entspricht einer Baumstruktur, innerhalb der der Kontakt im Verzeichnis gesucht wird. Die linke Spalte der nummerierten Attribute hängt ab von den Menüelementen des jeweiligen Telefons. Die Entsprechungen der Menüelemente (rechte Spalte) hängen ab vom Typ des LDAP-Servers.

3.6 Die wichtigsten Leistungsmerkmale

Sicherheit:

Der DLS bietet umfangreiche Funktionen, um eine hohe Sicherheit bei der VoIP-Kommunikation zu gewährleisten. Die wichtigsten Elemente im Überblick:

- Generieren und Verteilen von PSS innerhalb einer SRTP Security Domain (Identifizierung mittels Passwort).
- Import and Verteilung von individuellen Zertifikaten zur gesicherten Authentisierung.
  Siehe Abschnitt 16.12, “Security: Administration von Zertifikaten”.
- Sicherer Modus (Secure Mode) einrichtbar für die wechselseitge Authentifizierung von IP Device und DLS.
  Bereich: **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „DLS Verbindung“**.
- Minimale Länge von Benutzer-, Admin- und Screenlock-Passwort sowie für den SNMP Community-String einrichtbar.
  Bereich: **IP Devices** > **IP Phone Konfiguration** > **Security Einstellungen** > **Register „Passwörter“**.
- Möglichkeit der gezielten Deaktivierung von Workpoint-Services (z. B. WBM-Schnittstelle).
  Bereich: **IP Devices** > **IP Phone Konfiguration** > **Security Einstellungen** > **Register „Freigeschaltete Services (NW Stack)“**.

Mobility für SIP-IP Phones:

Mit dem DLS besitzen Sie ein Werkzeug, um SIP-IP Phones Mobility-fähig zu machen, Mobile User einzurichten und diese zu administrieren. Nutzen Sie die Möglichkeiten zur Migration bereits vorhandener Workpoints und den Einsatz von Mobile User Standards.

Grundlageninformationen zum Thema Mobility im DLS finden Sie im Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Software-Deployment:

Mit dem DLS können Sie komfortabel bei allen verfügbaren Workpoints oder bei einer festlegbaren Anzahl an Workpoints ein Software-Upgrade durchführen.

Siehe hierzu Abschnitt , “Software Deployment”.

Inventardaten-Management:

Der DLS ist die zentrale Inventardaten-Verwaltung. Die Inventardaten beschreiben die Hardware-Konfiguration bzw. Ausbauzustand des IP Devices, wie z. B. vorhandene Beistellgeräte oder Adapter.

Inventardaten können über die CSV-Schnittstelle exportiert werden.

Plug&Play-Funktion:

Der DLS unterstützt Plug&Play. Plug&Play bedeutet, dass das IP Phone ohne Benutzereingriff durch alleiniges Anstecken am Netz betriebsbereit ist. Das IP Device wird im Optimalfall automatisch mit der erforderlich Software und allen notwendigen Konfigurationsdaten versorgt und kann nach wenigen Minuten verwendet werden.

Siehe hierzu Abschnitt 15.5, “Autokonfiguration von Workpoints (Plug&Play)”.

Benutzeroberfläche:

Der DLS hat eine Java-unterstützte, web-basierte Benutzeroberfläche und läuft in einem Internet-Browser.

Konfigurations-Management:

Das Konfigurations-Management im DLS ist das zentrale Werkzeug zum Anzeigen und Administrieren von IP Device-Parametern in einer HiPath-Umgebung. Die Bedienung kann sowohl kundenseitig als auch vom Service per Fernadministration vorgenommen werden.

Zudem können IP Devices mit der Reset-Funktion neu gestartet werden.

Weitere Funktionen:

Folgende Basis-Funktionen werden unterstützt:

- Import/Export:

  Diese Funktion ist vor allen Dingen bei der Erstkonfiguration des DLS nützlich und kann auch im späteren Betrieb zum Sichern von Konfigurationsdaten verwendet werden.

  Durch das Ex- und Importieren kann eine DLS-Konfiguration komfortabel von einer DLS-Installation auf eine weitere übertragen werden.

- Zugangssicherheit:

  Der Zugang zum DLS ist passwortgeschützt.

- Error und Aktivitäts-Logging und Trace-Funktion.

- Unterstützung der Konfiguration von QDC-Features für HG3550 V2.0, HG1500, RG2700 und HiPath HG3530/70/75 (über SNMP-Proxy).
  Der SNMP-Proxy wird bei der Installation des DLS mit installiert und automatisch gestartet (läuft als Lokaler Service „DeploymentServiceSNMPProxy“).

3.6.1 Ausbaugrenzen und Einschränkungen

- Ein vollständiges Plug&Play im DLS kann nur dann genutzt werden, wenn im Netzwerk eine DHCP/DNS-Infrastruktur existiert und diese für die Zusammenarbeit mit dem DLS konfiguriert ist (siehe Abschnitt 15.5, “Autokonfiguration von Workpoints (Plug&Play)”).
- Pro DHCP-Domain kann nur ein DLS im Netzwerk installiert werden.
- Die Benutzeroberfläche des DLS ist in deutscher und englischer Sprache verfügbar.

3.6.2 Verwendete Ports

Eine Übersicht der vom DLS verwendeten Ports ist in der Sicherheitscheckliste des Planungshandbuchs zu finden.

3.7 Vom Deployment Service unterstützte Bereitstellungen

DLS-Bereitstellungen
Single Node mit entfernter Datenbank [1]
Multi-Node mit entfernter Datenbank und synchroner Spiegelung[2]
OpenScape Voice Entry (Integrated Simplex-Bereitstellung)[3]

Tabelle 5 DLS-Bereitstellungen

1 Der DCMP-Dienst kann optional entweder als Teil des DLS-Servers oder auf einem separaten Server installiert werden.
2 Der DCMP-Dienst kann optional entweder als Teil des DLS-Servers oder auf einem separaten Server installiert werden.
3 Der DLS-Dienst ist als Komponente in den OpenScape Voice Entry-Server integriert

3.8 Mobility im DLS – Grundlagenwissen

Mobility können Sie im DLS wie folgt nutzen (Begriffserklärungen siehe unten):

- Mobile User erstellen, aktualisieren und löschen.
- User-Profile für Mobile User erstellen.
- Parameter von Mobile Profileen ändern.
- Basic Profilee zu Mobile Profile migrieren.
- Mobile User anmelden, abmelden und Aktivitäten überwachen.
- Mobile User archivieren.

Weitere Informationen zur Bedienung finden Sie im Abschnitt 16.13, “Mobility:EinrichtenMobility:Administrieren”.

3.8.1 Mobility-Begriffserklärungen

In diesem Dokument werden zum Thema „Mobility“ folgende Begriffe häufig verwendet:

Begriff	Erklärung
Mobility Function	Ein Mobile User kann sich mit dieser Funktion an einem beliebigen Mobility Phone anmelden und dieses mit seinen eigenen Einstellungen benutzen.
Mobility Phone	Ein Telefon, das die Mobility Function unterstützt. Das bedeutet, ein Mobile User kann sich an diesem Telefon anmelden und dieses mit seinen eigenen Einstellungen benutzen.
Mobility ID	Rufnummer des Mobile Users. Mobility ID und Passwort dienen zur Authentifizierung bei der Anmeldung an einem Mobility Phone.
Basic User	Rufnummer und Benutzerdaten eines Mobility Phones, wenn kein Mobile User angemeldet ist.
Mobile User	Ein Benutzer, der sich an einem beliebigen Mobility Phone anmelden und dieses mit seinen eigenen Einstellungen benutzen kann.
User Data Profile	Hierbei handelt es sich um eine konfigurierbare Gesamt- oder Teilmenge an Anwenderdaten, abhängig vom Umfang der zugeordneten Templates. Die Parameter sind nicht gerätespezifisch.
Device Profile	Enthält Parameter eines Telefons, die unabhängig vom Benutzer zur Verfügung stehen. Diese Parameter sind ausschließlich gerätespezifisch (auf das Telefon bezogen).
Mobile User Archiv	Kann zur Sicherung von Mobile User-Daten angelegt werden.

Tabelle 6 Erklärungen der Begriffe zum Thema Mobility

3.8.2 Mobility verwenden

Mit Mobility hat ein dafür eingerichteter Benutzer die Möglichkeit, seine individuellen Einstellungen an jedem Telefon mit Mobility-Funktion zu nutzen. Zu den übertragbaren Parametern gehören beispielsweise benutzerspezifische Konfigurationen (z. B. Berechtigungen) und Einstellungen, die der Benutzer selbst am Telefon vorgenommen hat (z. B. Spracheinstellungen).

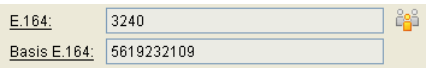
Zum Verwenden der Funktion drückt der Benutzer die Funktionstaste „Mobility“ an einem Mobility Phone oder verwendet das entsprechende Menü am Telefon und meldet sich als Mobile User mit seiner Rufnummer (Mobility ID) und seinem Benutzer-Passwort an.

Ein Mobile User kann nach erfolgreicher Anmeldung über dieses Mobility Phone Gespräche annehmen und selbst anrufen. Dabei ist er immer über seine persönliche Rufnummer erreichbar und abgehende Gespräche werden über diese Rufnummer geführt.

Das Abmelden kann vom Mobile User am Telefon selbst, von ihm per Fernzugriff mittels Web Based Management (WBM) oder mittels DLS („Forced Logoff“) erfolgen.

3.8.3 Mobility ID

Im DLS-Client im Bereich **IP Devices** > **IP Phone Konfiguration** werden diese beiden Rufnummern als **E.164** und **Basis E.164** angezeigt.



Die **E.164** ist die Rufnummer des Mobile Users (Mobility ID) und die **Basis E.164** die Rufnummer des Mobility Phones, wenn kein Mobile User angemeldet ist.
Das Smiley rechts neben der **E.164** signalisiert, dass zur Zeit ein Mobile User angemeldet ist.

3.8.4 Mobility einrichten

Das Einrichten der Mobility Function für ein Telefon ist ausschließlich mittels DLS möglich. Zum Einrichten muss das Telefon durch Aktivieren der Mobility-Funktion freigegeben werden.

HINWEIS: Mit der Funktion „Mobility“ kann nur eine Taste des Telefons selbst belegt werden, nicht die eines angeschlossenen optiPoint key module oder optiPoint self labeling key module.

Ein Mobile User kann auf zweierlei Weise erstellt werden:

- **Erstellen eines Mobile Users durch Hinzufügen**

  Ein neuer Mobile User wird erzeugt, indem eine neue Rufnummer zusammen mit einem Passwort vergeben wird. Die weiteren Parameter erhält der Mobile User aus einem User Data Profile. Wenn der Mobile User angemeldet ist, bleiben nur gerätespezifische Parameter im Telefon erhalten.

- **Erstellen eines Mobile Users durch Migrieren**

  Die bisherige Rufnummer des Telefons wird zur Mobility ID, und das Telefon erhält eine neue Basis-Nummer. Der Mobile User übernimmt die Parameter des Telefons. Die Migration macht dann Sinn, wenn z. B. ein bestehender Arbeitsplatz zu einem mobilen Arbeitsplatz umgestaltet wird. Der Benutzer ist dann, sofern er an einem Mobility Phone angemeldet ist, unter der bisher bekannten Rufnummer an seinem mobilen Arbeitsplatz weiter erreichbar.

Eine detaillierte Beschreibung zum Einrichten der Mobility Function für SIP-IP Phones finden Sie im Abschnitt 16.13, “Mobility:EinrichtenMobility:Administrieren”.

3.8.5 Profil-Konzept im DLS

HINWEIS: Siehe dazu auch die Erklärungen zu Profilen in Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

3.8.5.1 Unterschied zwischen Device Profile und User Data Profile

Zur Verdeutlichung, was den Unterschied zwischen Device Profile und User Data Profile ausmacht, nachfolgend Beispiele zu Parametern und die Profile, denen sie angehören.

Die Parameter im Beispiel werden im folgenden Bereich des DLS-Client angezeigt:
IP Devices > **IP Phone Konfiguration** > **Sonstiges** > **Register „Land & Sprache“**

Parameter	Profil	Erklärung
IP Adresse	Device Profile	Egal, welcher Benutzer das Telefon verwendet, die IP Adresse ist mit dem physikalischen Telefon verbunden und damit Teil des Device Profiles.
Tastenbelegung	User Data Profile	Die Tastenbelegung eines Telefons soll der Mobile User an jedem Mobility Phone nutzen können. Deshalb ist sie Teil des User Data Profiles.
QoS Parameter	Device Profile	QoS Parameter sind standortabhängig und ist damit Teil des Device Profiles.
Sprache	User Data Profile	Die einmal eingerichtete Sprache am Telefon soll für einen Mobile User an jedem Mobility Phone verfügbar sein und gehört deshalb zum User Data Profile.

Tabelle 7 Parameter-Beispiele mit Profil-Zugehörigkeit

Beim User Data Profile kann es sich um ein Basic Profile oder um ein Mobile Profile handeln, siehe Abschnitt 3.8.5.2, “Verfügbarkeit der Parameter-Konfiguration”.

3.8.5.2 Verfügbarkeit der Parameter-Konfiguration

Grundsätzlich sind im Bereich **IP Phone Konfiguration** immer die Parameter des Device Profiles änderbar. Device Profile Die Parameter des s sind nicht Bestandteil der Daten eines Mobile Users und sind deshalb im Bereich **SIP Mobile User Konfiguration** grundsätzlich nicht verfügbar.

Abhängig davon, ob an einem Telefon die Mobility Function verfügbar ist und, wenn ja, ob sich ein Mobile User angemeldet hat, sind unterschiedliche Konfigurationsmöglichkeiten im DLS-Client verfügbar.

Nachfolgend sind nur Basic Profile und Mobile Profile erwähnt, da das Device Profile im Bereich **IP Phone Konfiguration** immer und im Bereich **SIP Mobile User Konfiguration** nie verfügbar ist.

Zustand	**Parameter im Bereich: IP Phone Konfiguration**	**Parameter im Bereich: SIP Mobile User Konfiguration**
Kein Mobility Phone	Alle änderbar.	Nicht verfügbar.
Mobility Phone, Mobile User ist nicht angemeldet	Basic Profile: änderbar. Mobile Profile: nicht verfügbar.	Basic Profile: änderbar. Mobile Profile: änderbar. Beide Profile sind als zwei Objekte im DLS sichtbar.
Mobility Phone, Mobile User ist angemeldet	Basic Profile: nicht verfügbar. Mobile Profile: nur lesbar.	Basic Profile: änderbar (Änderungen werden erst nach dem Abmelden des Mobile User an das Telefon übertragen). Mobile Profile: änderbar.

Tabelle 8 Parameter-Verfügbarkeit im DLS

Beachten Sie bitte den Unterschied bei der Darstellung der Parameter im Bereich **IP Phone Konfiguration** und **SIP Mobile User Konfiguration**:

- Im Bereich **IP Phone Konfiguration** existiert *ein* Objekt (Ansicht **Objekt** oder eine Zeile in der Ansicht **Tabelle**) immer für ein physikalisches SIP-IP Phone (ob Mobility oder nicht).
- Im Bereich **SIP Mobile User Konfiguration** existieren zwei unterschiedliche Objekt-Typen:
  - Ein Objekt für das Mobility Phone und
  - ein Objekt für den Mobile User.

3.9 DLS-Systemüberwachung

Die DLS-Systemüberwachung stellt Informationen zum System bereit, die als Grundlage für Wartungsaktionen dienen. Hierbei handelt es sich insbesondere um automatische Alarme und Fehlermeldungen der Systemkomponenten.

3.9.1 Systemüberwachungstools - DLS RapidStat

Das Überwachungstool DLS RapidStat dient zur Durchführung von Diagnoseprüfungen auf DLS-Rechnern. Ein separates Tool, **traceDls**, dient zum Sammeln aller Log-, Trace- und sonstiger Dateien für die Fehlersuche und zu Archivierung bzw. Ablage in Verzeichnissen für den schnellen Abruf von Informationen.

DLS RapidStat ist ein Diagnose- und Informationserfassungs-Tool, das DLS-Administratoren dabei hilft, ein System für eine DLS-Installation bzw. ein DLS-Upgrade vorzubereiten und mögliche Probleme zu beheben. Der Name des Tools wurde in Anlehnung an das entsprechende Tool in OSV gewählt. Auch die Funktionsweise von DLS RapidStat wurde größtenteils an das OSV-Gegenstück angelehnt, damit OpenScape Voice-Benutzer sich möglichst schnell mit dem Tool vertraut machen können.

> ***HINWEIS:*** OSV RapidStat läuft nur unter Linux; **DLS RapidStat** läuft nur unter Windows. Zunkünftige Versionen werden je nach Bereitstellung sowohl unter Windows als auch unter Linux lauffähig sein.

RapidStat liefert Statusinformationen zum Systemzustand vor und nach geplanten Wartungsarbeiten wie zum Beispiel:

- Allgemeine Software-Upgrades
- Patching
- Systemwartungsreleases
- Hardware-Reparaturen
- Abrufen von Protokolldateien (Log File Retrieval, LFR) für Debugging- und Reparaturzwecke
- Andere durch Administratoren und/oder lokale Betriebsvorschriften vorgesehene Aktivitäten.

Dieses Programm macht eine manuelle Systemabfrage zur Feststellung des Systemstatus überflüssig und hilft damit, menschliche Fehler und Eskalationen zu vermeiden. Dies trägt zur Reduzierung von Wartungsaktivitäten und Vermeidung von möglichen Ausfällen in diesem Zusammenhang bei.

Bei Problemen mit dem DLS-Dienst kann RapidStat in zweierlei Hinsicht helfen:

- Es gibt dem Administrator die Möglichkeit, das Problem selbst zu diagnostizieren und zu beheben, oder
- Es liefert dem Support-Team wertvolle Informationen über das System und hilft ihm, mögliche Fehlerursachen zu identifizieren

3.9.1.1 RapidStat-Funktionen

RapidStat unterstützt die folgenden Funktionen:

1. Sammeln von Informationen

RapidStat sammelt nicht-DLS-spezifische Informationen über das Zielsystem:

- Hardware-Informationen
  - Marke/Modell des Rechners
  - CPU-Typ
  - CPU-Taktfrequenz
  - CPU-Auslastung (pro Kern)
  - Gesamtspeicher
  - Größe der Auslagerungsdatei
  - Auslagerungsspeicher
  - Speicherplatz
  - Physische Datenträger
  - Gesamter Speicherplatz
  - Belegter Speicherplatz
  - Netzwerkschnittstellen
- Betriebsystem
- Betriebssystemversion
- Bitlänge des Betriebssystems
- Datum und Uhrzeit
- .NET Framework & Version (falls auf Windows installiert)
- Java-Version
- Antivirusprüfung

  Überprüfen Sie, ob eine Antivirus-Software installiert ist. Falls ja, zeigt DLS RapidStat den Produktnamen der Software an.

2. DLS-spezifische Überprüfungen

DLS RapidStat führt verschiedene Überprüfungen durch, anhand derer der Systemadministrator erkennen kann, ob ein Dienst ordnungsgemäß und ohne Probleme ausgeführt wird. Diese Überprüfungen können in regelmäßigen Abständen durchgeführt werden, um mögliche Probleme schon im Vorfeld oder zumindest kurz nach Auftreten eines Fehlers zu erkennen:

- Installation
- Version
- Bereitstellungstyp
  - Single Node
  - Multi Node
  - Benutzerdefinierte Datenbank
- Dienststatus
  - Dienstregistrierung
  - Wird ausgeführt / Angehalten
  - Benutzerkennung, unter der der Dienst ausgeführt wird
  - Überprüfung und Erstellung eines Berichts über alle Dienste, die nicht benötigt werden oder nicht identifiziert werden können. Bericht mit Warnhinweis zu unerwartet ausgeführten Prozesse
- Prozessüberprüfung
  - Überprüfung und Erstellung eines Berichts über alle Prozesse, die nicht benötigt werden oder nicht identifiziert werden können. Bericht mit Warnhinweis zu unerwartet ausgeführten Prozesse
- Datenbankstatus
  - Wird ausgeführt / Angehalten
  - Verbindung zur Datenbank
  - Benutzerkennung, unter der der Dienst ausgeführt wird
  - Verfügbarkeit von DlsDB
- Wenn RapidStat im Rahmen eines DLS-Upgrades (beim Start des Installationsprogramms) ausgeführt wird, überprüfen Sie, ob das geplante Upgrade durchgeführt werden kann (Upgrade-Pfad überprüfen) und stellen Sie sicher, dass alle Migrationsskripte verfügbar sind.
- SNMP-Proxy
  - Überprüfen Sie, ob der Dienst ‘DeploymentServiceSNMPProxy’ ausgeführt wird. Fehler melden, wenn kein Zugriff möglich ist.

3. Vorbereitung des DLS-Server-Upgrades

Wenn ein DLS-Server-Upgrade ansteht, sollte DLS RapidStat vor Beginn des Upgrades ausgeführt werden, um erkennen zu können, ob das System in gutem Zustand ist. Hierdurch kann ein Fehlschlagen des Upgrades verhindert werden.
Die Offenheit des zugrunde liegenden Betriebssystems (Windows Server) und die Koexistenz der DLS-Software mit anderer Software auf ein und demselben Computer führen dazu, dass die Betriebsumgebung oft unerwartet verändert wird. DLS RapidStat trägt dazu bei, dass die Softwareumgebung stabil und berechenbar bleibt.

3.9.1.2 Verwendung von DLS RapidStat

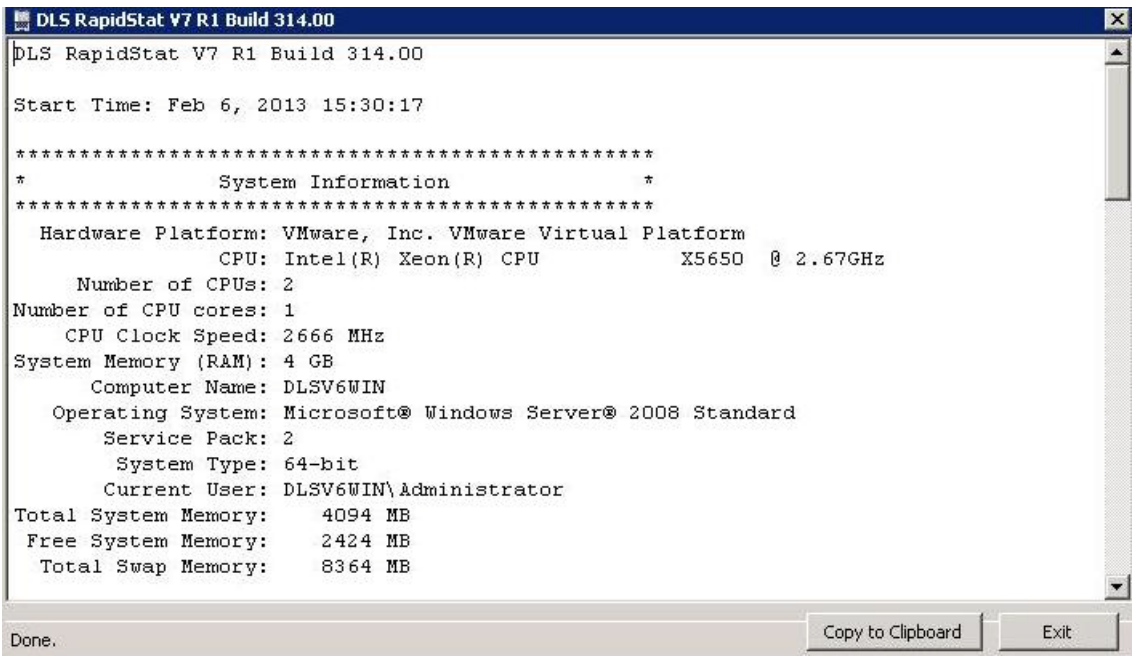
DLS RapidStat ist ein Windows-basiertes und in Java geschriebenes Befehlszeilentool, das im Standalone-Modus oder als Teil des NSIS-Installationsprogramms ausgeführt wird. Es wird bei der Installation von DLS automatisch mitinstalliert; manuelle Eingriffe sind nicht erforderlich.

Gehen Sie zu `C:<Program Files>\DeploymentService\tools` und führen Sie `DlsRapidStat.exe` aus.

Während seiner Ausführung führt DLS RapidStat verschiedene Überprüfungsläufe durch, arbeitet Checklisten ab und erstellt Berichte im OSV RapidStat-Format. Im Header des Berichts stehen unterschiedliche Informationen zum Betriebssystem und zur Hardware bzw. Software (wie z. B. Betriebssystemtyp/-versionen, CPU, Arbeitsspeicher, Speicherplatz etc.); im Anschluss daran folgen nacheinander die einzelnen DLS-spezifischen Überprüfungen. Am Ende des Berichts sollte eine Zusammenfassung mit gefundenen Warnungen oder Fehlern stehen.

Die Berichtergebnisse werden entweder in einem Befehlszeilenfenster angezeigt

oder in einem Textfenster mit zwei Schaltflächen:



- Copy to Clipboard (In Zwischenablage kopieren): kopiert den Ergebnistext in die Zwischenablage

- Exit (Beenden): beendet RapidStat und geht entweder zurück zum Installationsprogramm oder zum Betriebssystem, je nachdem wie RapidStat aufgerufen wurde

Bei jeder Ausführung speichert RapidStat einen Bericht und eine Protokolldatei im Verzeichnis des aktuellen Benutzers „`%LOCALAPPDATA%\DeploymentService\RapidStat`“. Der Dateiname enthält das Datum und die Uhrzeit der Ausführung und ist daher eindeutig.

Beispiel:

```
C:\Users\dlsuser\AppData\Local\DeploymentService\RapidStat\dls.20120919.160910.
rapidstat.report.txt
```

oder

```
C:\Users\dlsuser\AppData\Local\DeploymentService\RapidStat\dls.20120919.160910.
rapidstat.log.txt.
```

4 Installation und Erstkonfiguration

Für Installation und Betrieb des DLS gibt es mehrere Varianten:

- **Single Node-Betrieb mit lokaler Datenbank**: DLS-Server und DLS-Datenbank befinden sich auf demselben Rechner.
- **Single Node-Betrieb mit entfernter Datenbank**: Die DLS-Datenbank befindet sich auf einem eigenen Rechner.
- **Multi-Node-Betrieb (Cluster)**: Der DLS-Server läuft verteilt auf mehreren Rechnern. Die DLS-Datenbank befindet sich auf einem weiteren Rechner oder auf einem der DLS-Knotenrechner.

Beim Einsatz einer entfernten Datenbank besteht zudem die Möglichkeit, die Datenbank zu spiegeln (Modus für erhöhte Datensicherheit / Hochverfügbarkeit). Die Spiegelung kann synchron erfolgen, d. h. mit gleichzeitiger Aktualisierung von Haupt- und Spiegeldatenbank, oder asynchron. Bei der asynchronen Spiegelung wird die Aktualisierung der Spiegeldatenbank erst nach der Transaktion auf der Hauptdatenbank vorgenommen.

Die folgenden Kapitel sind in der Reihenfolge ihrer Relevanz für eine bestimmte Variante der DLS-Installation angeordnet.

Variante	Kapitel
Single Node mit lokaler Datenbank	• Abschnitt 4.5.1, “Single Node-Betrieb mit lokaler Datenbank”
Single Node mit entfernter Datenbank	• Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren” • Abschnitt 4.5.2, “Single Node-Betrieb mit entfernter oder kundenspezifischer Datenbank”
Multi-Node/Cluster	• Abschnitt 4.1.5, “Infrastruktur bei Cluster-Betrieb” • Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren” • Abschnitt 4.3, “Konfiguration des Network Load Balancer” • Abschnitt 4.5.3, “Multi-Node-Betrieb”
Erhöhte Datenbanksicherheit / Hochverfügbarkeit durch Datenbankspiegelung	• Abschnitt 4.6, “Spiegelung der SQL-Datenbank aufsetzen”

4.1 Voraussetzungen

4.1.1 Allgemeine Voraussetzungen am Server

Hinweise zur benötigten Hardware finden Sie unter Abschnitt 2.1.1, “Systemvoraussetzungen”.

Der DLS-Server läuft auf folgenden Betriebssystemen in der deutschen oder englischen Version:

- Windows Server 2008 Enterprise Edition (64-Bit)
- Windows Server 2008 Standard (64-Bit)

- Windows Server 2008 R2 Standard & Enterprise Edition (64-Bit)

mit neuestem Service Pack und aktuellen Sicherheitspatches

HINWEIS: Bei größeren Installationen und speziell bei Cluster-Betrieb ist generell ein Serverbetriebssystem erforderlich.

HINWEIS: Wenn Sie die SQL Express Edition installieren wollen, stellen Sie bitte sicher, dass das Datenbankverzeichnis nicht in einer Partition mit der Eigenschaft ‘komprimiert’ liegt.

HINWEIS: Um CPU-Auslastungsprobleme zu vermeiden, nehmen Sie folgende Einstellungen vor:

1. Klicken Sie auf **Control Panel (Systemsteuerung)** > **Power Options (Energieoptionen)**> **Change Advanced Power Settings (Erweiterte Energieeinstellungen ändern)**.
2. Wählen Sie die Option **High Performance (Höchstleistung)**.

Dies gilt nur für 64-Bit-Betriebssystemsvarianten ab Windows 2008.

Der DLS-Client läuft als Java-Applet in einem Webbrowser. Erforderlich sind:

- Java PlugIn
- Beliebiger Browser mit Unterstützung für Java Plug-ins, z. B. Internet Explorer, Firefox, Chrome, Opera, Safari

4.1.2 Generelle Voraussetzungen am Client-PC

Der PC, auf dem der DLS-Client läuft, sollte die folgenden Hardware-Eigenschaften aufweisen:

- Festplattenplatz: keine besonderen Anforderungen.
- CPU Pentium IV mit min. 1,4 GHz Taktfrequenz oder vergleichbar.
- Arbeitsspeicher min. 512 MB RAM.
- Netzwerkgerät mit 10 Mbit, 100 Mbit oder höher, oder Modem.
- Bildschirmauflösung: mindestens 1024 × 768 Pixel, mindestens 16 bit Farbtiefe.

4.1.3 Personelle Voraussetzungen

Remote Service Engineer (RSE):

- Fundiertes Wissen über LAN-Technologie IP-Netzwerke.
- Fundiertes Wissen zu den vom DLS unterstützten IP Devices (siehe Abschnitt 3.4).
- Bei Multi-Node (Cluster): fundiertes Wissen über Microsoft Betriebssysteme und MS SQL Server 2008/2008 R2.

Field Service Engineer (FSE)

- Fundiertes Wissen zu den vom DLS unterstützten IP Devices (siehe Abschnitt 3.4).
- Basiswissen über LAN-Technologie, IP-Netzwerke und die unterstützten Betriebssysteme.
- Bei Multi-Node (Cluster): fundiertes Wissen über Microsoft Betriebssysteme und MS SQL Server 2008/2008 R2.

4.1.4 Verfügbarkeit des DLS

Informationen zur Lizensierung des DLS bzw. von einzelnen Funktionalitäten des DLS finden Sie in Abschnitt 2.1.3, “Lizensierung”.

Für den Service stehen weitere Installationsmöglichkeiten zur Verfügung:

- Zur DLS-Installation beim Kunden (z. B. HiPath SPA Server) kann die Software vom BE1 mittels RCC bezogen werden.
- Die Installation beim Service kann wie folgt geschehen:
  - Im internationalen Markt kann zur Installation auf dem Service-Laptop ebenfalls der BE1 genutzt werden.

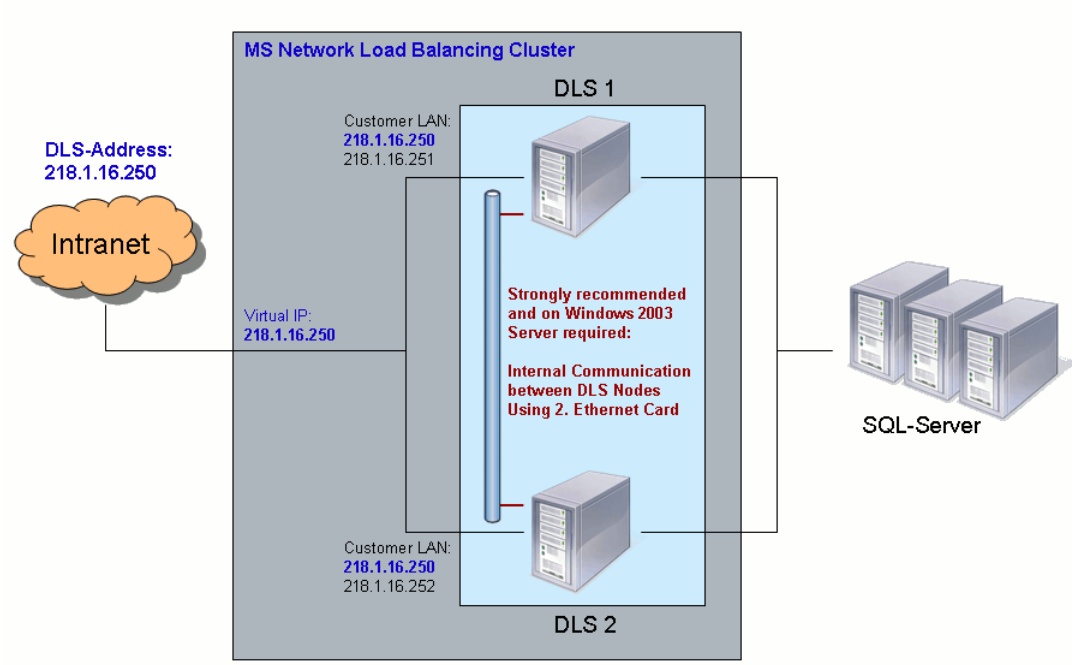
4.1.5 Infrastruktur bei Cluster-Betrieb

Ein DLS-Cluster besteht aus bis zu 4 DLS-Knoten und bis zu 3 SQL-Servern. DLS-Knoten und SQL-Server können zwar eine gemeinsame Hardware nützen, es wird aber empfohlen, separate Rechner zu verwenden. Aus Sicht der Endgeräte bilden die DLS-Knoten einen Cluster mit einer virtuellen IP-Adresse, die über den Windows Network Load Balancing Manager zur Verfügung gestellt wird. Der Network Load Balancer läuft auf allen DLS-Knoten als Service und leitet die Anfragen an die DLS-Knoten weiter. Für die Kommunikation zwischen den einzelnen DLS-Knoten benötigen alle DLS-Knoten eine zweite IP-Adresse und somit eine zusätzliche Netzwerk-Karte.

HINWEIS: Die über den NLB administrierten Knoten dürfen nicht über DHCP konfiguriert sein.

HINWEIS: Bei den für die SQL-Kommunikation (internes Netzwerk) an den einzelnen Knoten benötigten Netzwerkkarten sollte kein Standardgateway konfiguriert sein.

Die DLS-Datenbank läuft als entfernte Datenbank auf einem oder mehreren Rechnern, je nachdem, ob eine Spiegelung der Daten gewünscht ist. Der DLS nimmt dabei stets nur mit einen Rechner Verbindung auf. Es ist auch möglich, DLS-Server und Datenbankserver auf ein und demselben Rechner zu betreiben.



4.2 SQL-Server für entfernte Datenbank installieren

Eine einfache Möglichkeit, die Kapazität und Effizienz des DLS zu steigern, besteht darin, den Microsoft SQL Server 2008 Enterprise Edition einzusetzen. Damit lässt sich die bei der mit dem DLS mitgelieferten Version Microsoft SQL Server 2008 Express Edition anfallende Beschränkung der Dateigröße auf 4 GB vermeiden.

HINWEIS: Es wird empfohlen, den SQL-Server auf einem separaten Rechner zu installieren. Das Datenbankverzeichnis darf dabei nicht in einer Partion mit der Eigenschaft „komprimiert“ liegen.

HINWEIS: Die Kommunikation zwischen DLS-Knoten und SQL-Server findet im Klartext statt. Es müssen also geeignete Absicherungsmaßnahmen getroffen werden.

Für den DLS können sowohl Microsoft SQL Server 2005 als auch Microsoft SQL Server 2008/2008 R2 eingesetzt werden. Im Folgenden werden beide Versionen beschrieben.

Da die einzelnen SQL-Server für die Konfiguration der Datenbankspiegelung über FQDNs (Fully Qualified Domain Names) angesprochen werden, müssen zumindest für alle SQL-Server DNS-Namen zur Verfügung stehen. Voraussetzung dafür ist entweder ein DNS-Server (empfohlen) oder eine Namenszuweisung für alle beteiligten Rechner mithilfe von Windows-Arbeitsgruppen (Workgroups). Die Konfigurationsdateien, in denen IP-Adressen und Workgroup-Namen einander zugeordnet werden, finden Sie unter:

```
C:\Windows\system32\drivers\etc\hosts
```

Für die Datenbankspiegelung erwartet Microsoft SQL Server 2008 Enterprise Edition Namen in den Formaten:

`<IP address> <hostname>.<domain>` (DNS)

oder

`<IP address> <hostname>.<workgroup>` (Windows Workgroup)

Im Betriebssystem Windows 2008 R2 Server ist bereits ein DNS-Server enthalten; beachten Sie bitte die zugehörige Dokumentation.

HINWEIS: Achten Sie darauf, dass die Systemzeit auf allen Rechnern synchron ist. Bei Verwendung des in Windows 2008 Server enthaltenen DNS-Servers ist dies der Fall, denn hier wird die Systemzeit vorgegeben.

Die hier beschriebene Installation ist erforderlich, wenn die DLS-Datenbank auf einem eigenen Rechner betrieben werden soll. Für den Betrieb von DLS-Server und Datenbank auf einem gemeinsamen Rechner im Rahmen einer Single Node-Lösung ist keine gesonderte Installation nötig, denn dies wird von der DLS-Installationsroutine erledigt (siehe Installationsbeschreibung im DLS-Softwarepaket). Bei Multi Node-Lösungen ist auf jeden Fall eine separate Installation der Datenbank erforderlich, auch wenn Datenbank und DLS auf dem gleichen Rechner laufen sollen.

HINWEIS: Der für Multi Node-Lösungen benötigte Microsoft SQL Server 2008 Enterprise Edition ist nicht im DLS-Softwarepaket enthalten und muss daher separat erworben werden.

HINWEIS: Weitergehende Informationen zum Microsoft SQL Server finden Sie in:
Ray Rankins u. a. (1987): Microsoft SQL Server 2005 Unleashed. SAMS Verlag, ISBN: 0-672-32824-0; Ray Rankins u. a. (2009): Microsoft SQL Server 2008 Unleashed. SAMS Verlag, ISBN-10: 0672330563.

1. Account für DLS und Datenbank

   Alternative A: Lokaler Benutzer.

   Richten Sie auf dem Rechner, der die Datenbank beherbegen soll, ein lokales Administratorkonto ein, z. B. „dls“.

   Alternative B: Verwendung von Active Directory.

   Verwenden Sie ein bereits in Ihrem Active Directory existierendes Domain-Benutzerkonto oder erstellen Sie ein neues Benutzerkonto für den Zugang zur Datenbank.

   Alternativen A und B: Fügen Sie das Benutzerkonto der Gruppe der lokalen Administratoren zu.

   Bei einer Datenbank mit Spiegelung muss auf jedem Datenbankserver das gleiche Benutzerkonto verwendet werden.

Da während der Installation in der Master-Datenbank eine Stored Procedure eingerichtet werden muss, sollte dieser User während der Installation die Rolle „sysadmin“ haben. Nach der Installation kann die Rolle für den Server nach „public“ und die Rolle für die Datenbank nach „db_owner“ geändert werden. Eine Rolle für die Ausführung von Stored Procedures kann wie folgt erstellt und zugewiesen werden:

```
USE [DLSdb]
GO
CREATE USER [<user full name>] FOR LOGIN [<user full name>]
GO
CREATE ROLE db_executor
GO
GRANT EXECUTE TO db_executor
GO
EXEC sp_addrolemember 'db_executor', '<user full name>'
GO
```

`<user full name>` ist der gültige und vollständige Anmeldename des Benutzers.

Der vollständige Name hat folgende Struktur: wenn eine Domäne existiert, lautet der vollständige Name `<domain>\<user name>` ; ohne Domäne lautet er `<computer name>\<user name>`

Beispiel 1: Wenn eine Domäne mit dem Namen `'GLOBAL-AD.NET'` existiert und der Benutzer `'DLSUSER'` heisst (Groß-/Kleinschreibung spielt keine Rolle) lautet der vollständige Name des Benutzers: `GLOBAL-AD.NET\DLSUSER`

Beispiel 2: Wenn keine Domäne existiert, wird stattdessen der Computername verwendet. Heisst der Computername `'DLSDBPRINCIPAL'` und der Benutzer `'DLSUSER'`, dann lautet der vollständige Name des Benutzers:

```
DLSDBPRINCIPAL\DLSUSER
```

Ausführlichere Beispiele mit den oben genannten Namen:

```
CREATE USER [GLOBAL-AD.NET\DLSUSER] FOR LOGIN [GLOBAL-AD.NET\DLSUSER]
```

```
EXEC sp_addrolemember 'db_executor', 'GLOBAL-AD.NET\DLSUSER'
```

und

```
CREATE USER [DLSDBPRINCIPAL\DLSUSER] FOR LOGIN [DLSDBPRINCIPAL\DLSUSER]
EXEC sp_addrolemember 'db_executor', 'DLSDBPRINCIPAL\DLSUSER'
```

2. Datenverzeichnis

   Erstellen Sie auf dem Datenbankserver ein Verzeichnis für die Datenbank, z. B. `D:\DATA\DLSDB`. Dieses Verzeichnis wird später bei der DLS-Installation benötigt.

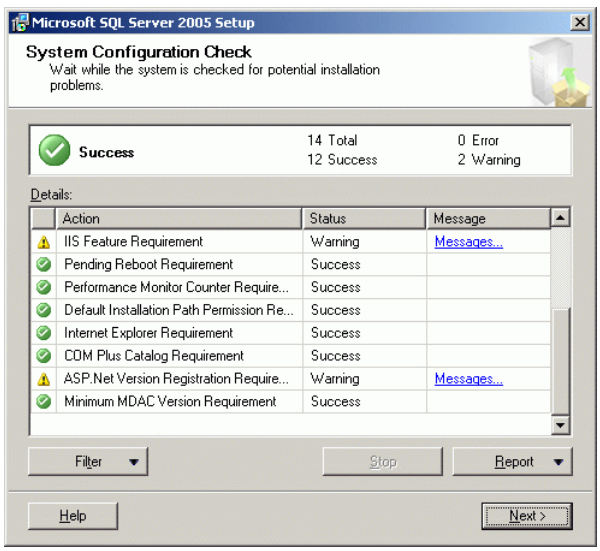
   Bei Spiegelung ist auf dem Haupt- und auf dem Spiegelserver jeweils das gleiche lokale Verzeichnis anzugeben.

   Die weiteren Installationsschritte werden für Microsoft SQL Server 2005 und Microsoft SQL Server 2008 R2 getrennt beschrieben.

4.2.1 Microsoft SQL Server 2005

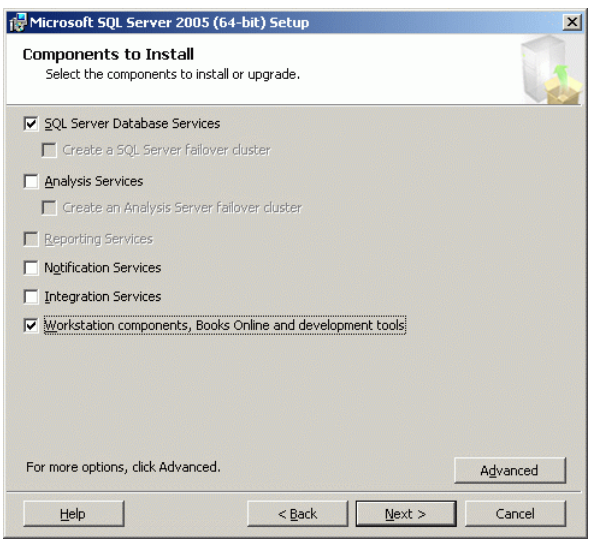
1. Öffnen Sie das Setup-Programm und klicken Sie auf **Next**.

2. Die Systemkonfiguration wird untersucht. Falls Sie Warnungen im Zusammenhang mit den Komponenten IIS (Internet Information Server) oder ASP.Net erhalten, können Sie diese ignorieren.



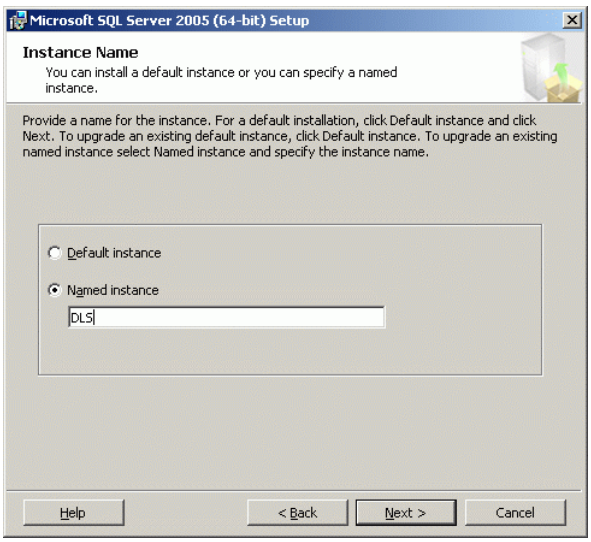
Klicken Sie auf **Next**.

3. Selektieren Sie die Komponenten **SQL Server Database Services** und **Workstation components...**. Letztere Komponente ermöglicht die Steuerung der Datenbank-Spiegelung per Benutzeroberfläche.



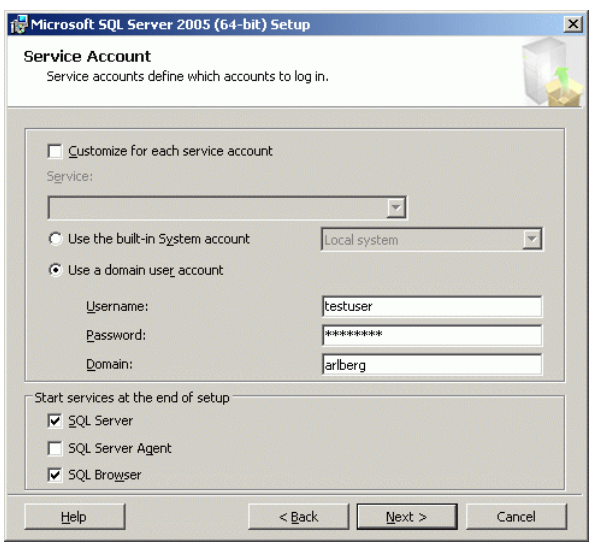
Klicken Sie auf **Next**.

4. Vergeben Sie einen Instanznamen, der für alle SQL-Server gleich ist, z. B. „DLS“.



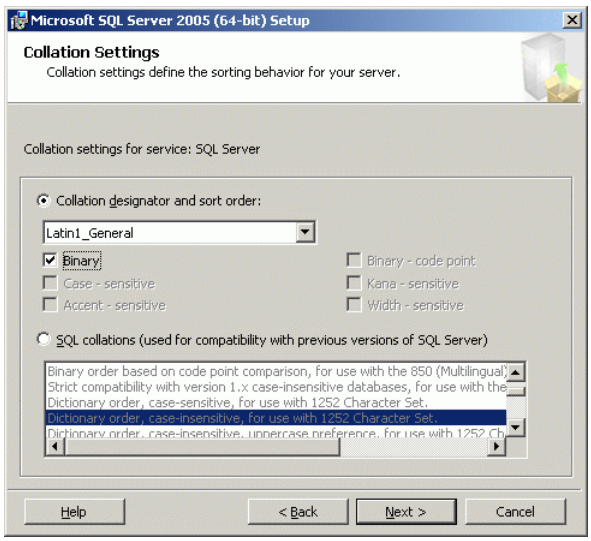
Klicken Sie auf **Next**.

5. Im Fenster **Service Account** wählen Sie die Option **Use a domain user account**. Geben Sie dann in den Feldern **Username** und **Password** die Daten desjenigen Benutzers ein, unter dem sich die DLS-Knoten mit der Datenbank verbinden. Dieser Benutzer muss zur Gruppe der Administratoren gehören. Im Feld **Domain** geben Sie die DNS-Domäne an, die demjenigen Subnetz zugewiesen ist, in dem sich die DLS-Knoten sowie der Datenbank-Server befinden. Unter **Start services at the end of setup** aktivieren Sie **SQL Server** und **SQL Browser**.



Klicken Sie auf **Next**.

6. Legen Sie die geeignete Einstellung des Sortierverhaltens fest. Aktivieren Sie hierzu die Option **Collation designator and sort order** und wählen Sie **Latin1_General**. Aktivieren Sie die Option **Binary** und klicken Sie auf **Next**.

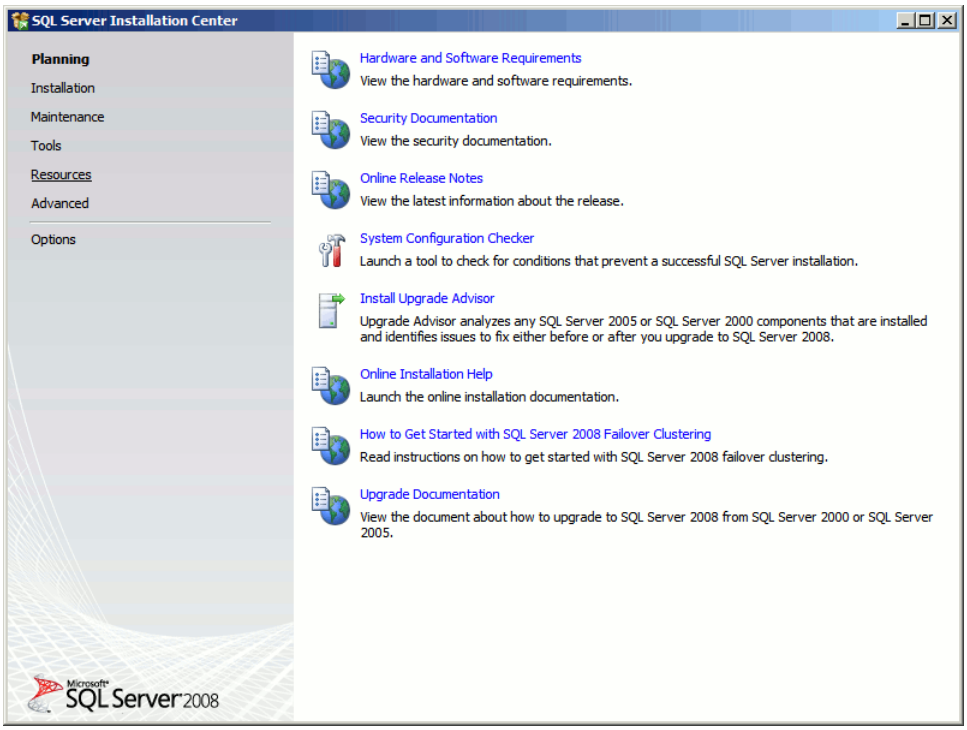


7. Die Installation des Microsoft SQL Server 2005 in der Grundversion ist abgeschlossen. Fahren Sie nun fort mit der Installation des Service Pack 1 für Microsoft SQL Server 2005. Starten Sie hierzu das Setup-Programm und folgen Sie den Anweisungen.

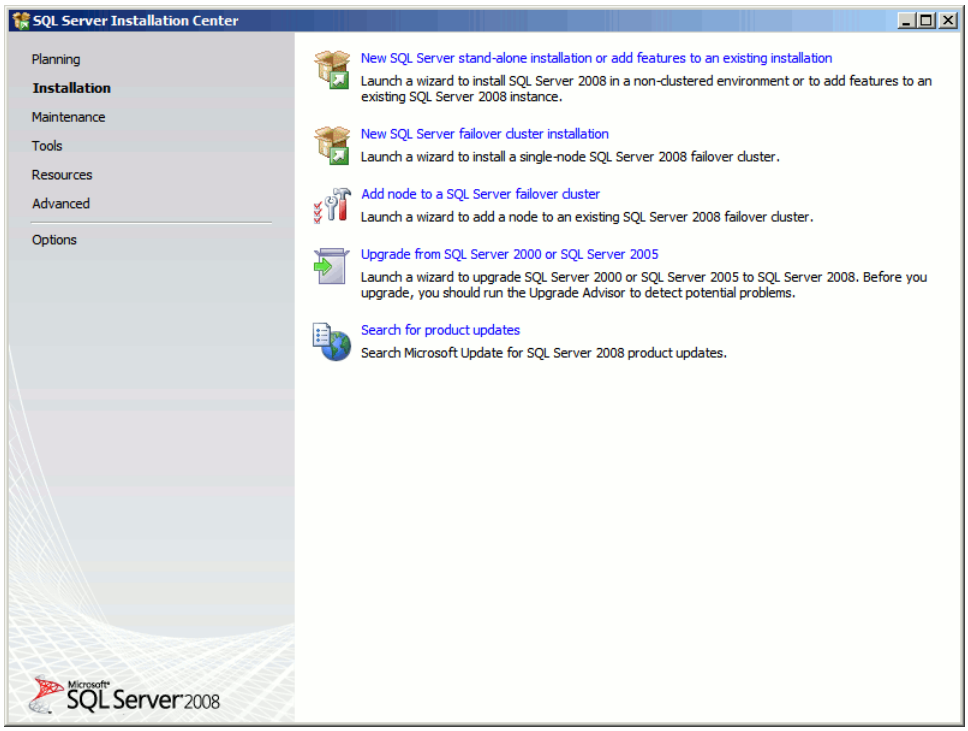
8. Es wird empfohlen, auch das Service Pack 2 für Microsoft SQL Server 2005 zu installieren. Starten Sie hierzu das Setup-Programm und folgen Sie den Anweisungen.

4.2.2 Microsoft SQL Server 2008 R2

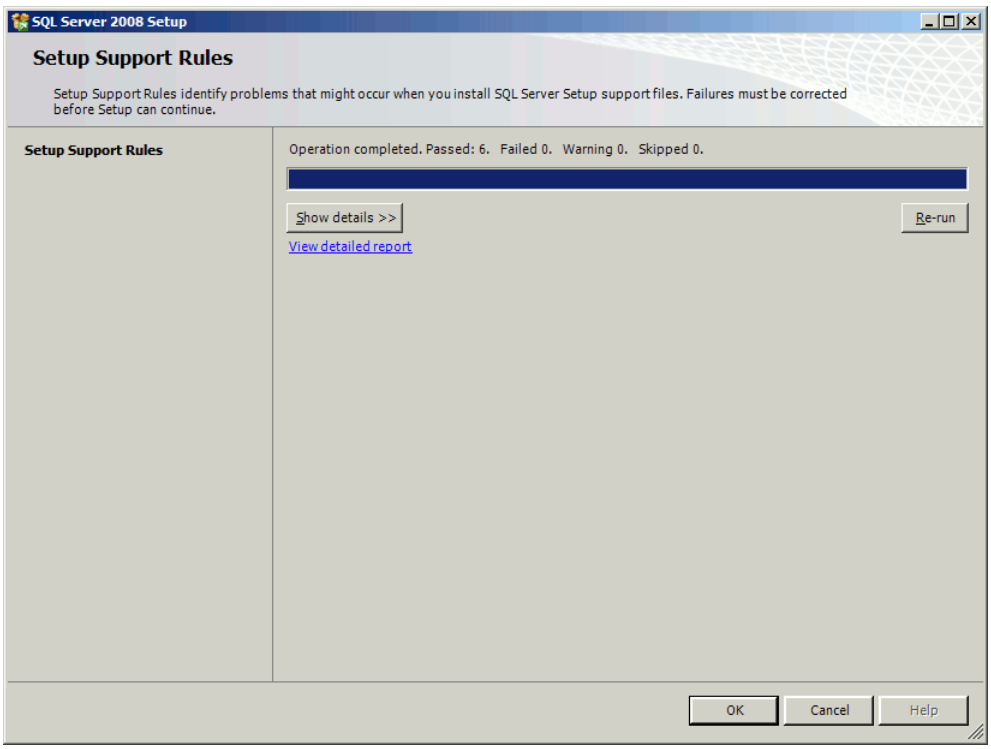
1. Öffnen Sie das Setup-Programm und wählen Sie **Installation**.



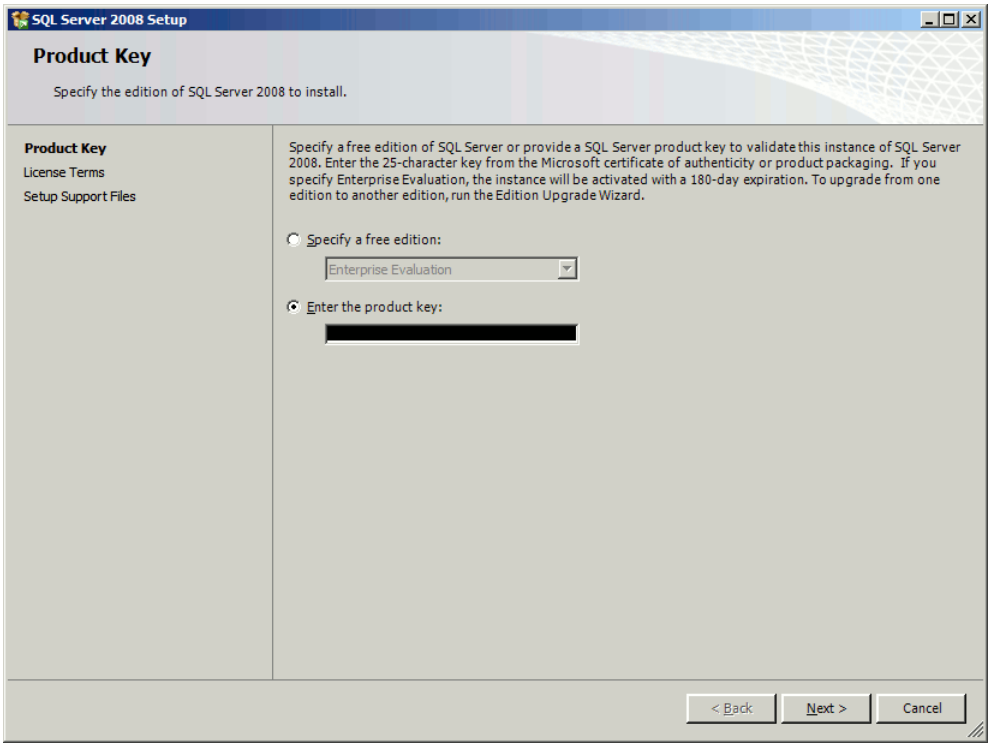
2. Wählen Sie **New Server stand alone installation or add features to an existing installation**.



3. Das Installationsprogramm überprüft die Installationsvoraussetzungen. War die Überprüfung erfolgreich, so klicken Sie **OK**.

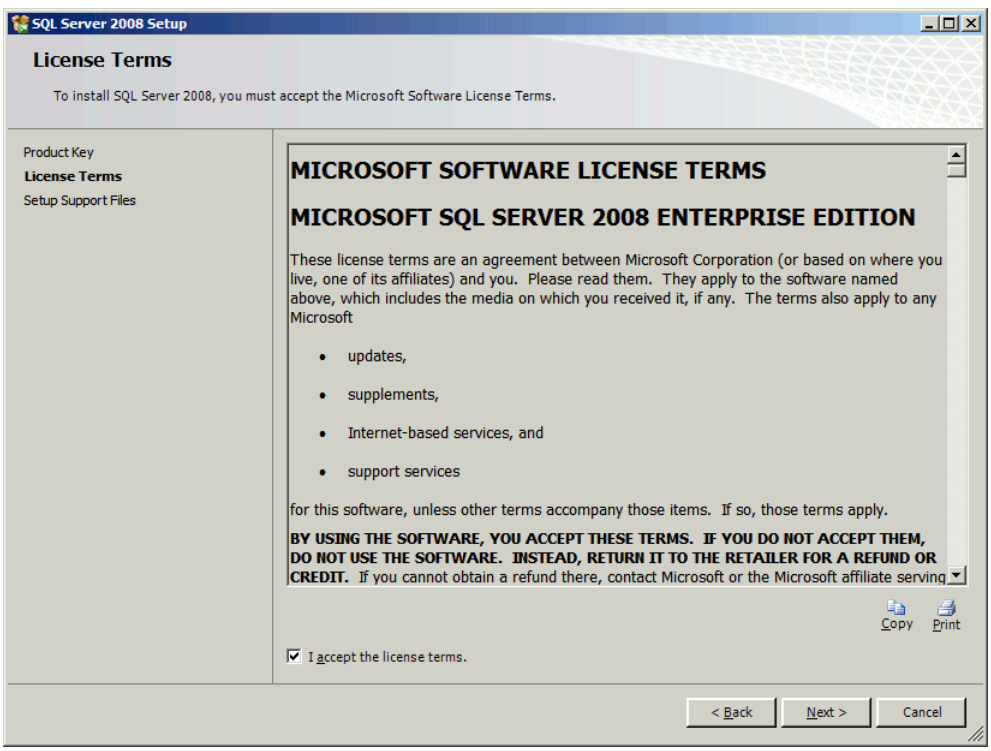


4. Geben Sie den Produktschlüssel ein.



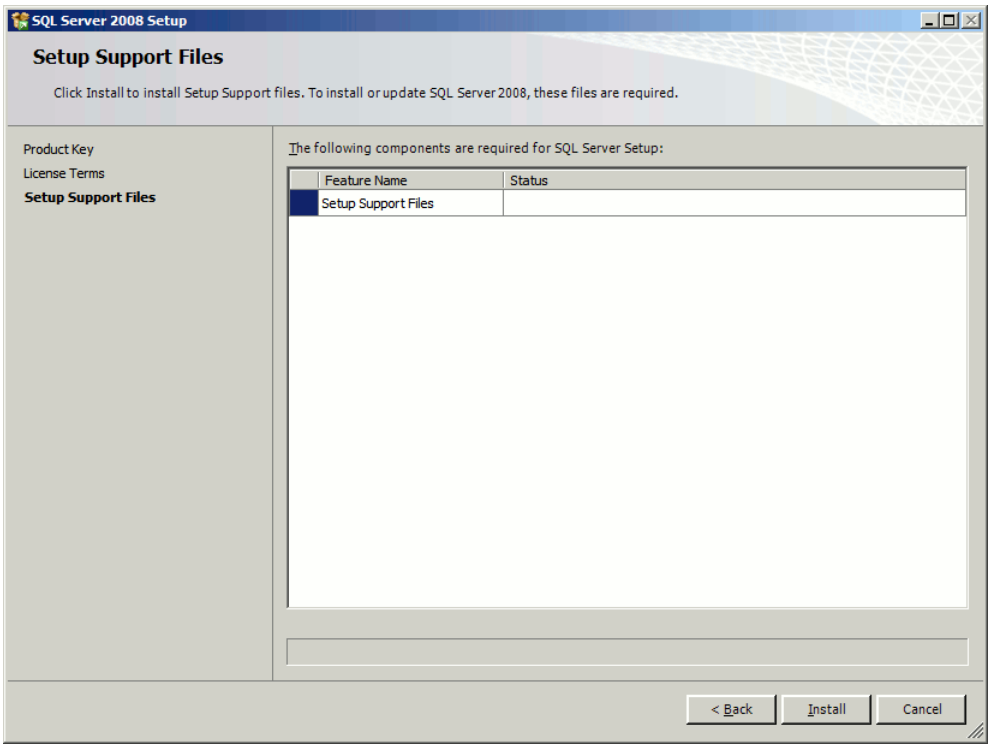
Klicken Sie auf **Next**.

5. Akzeptieren Sie die Lizenzbestimmungen.

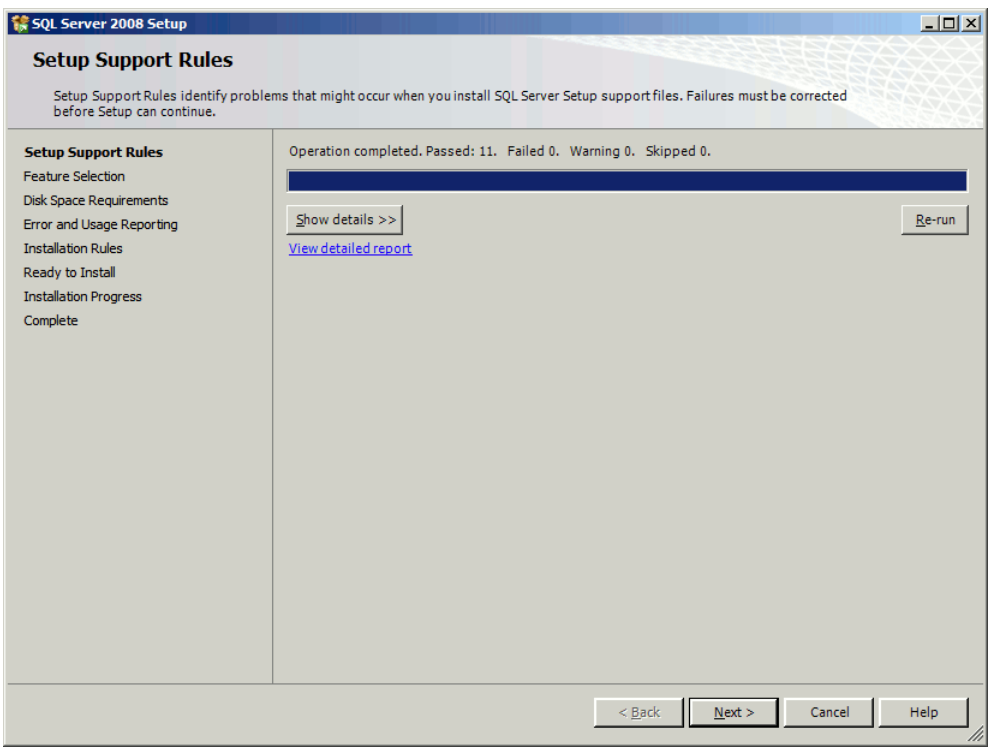


Klicken Sie auf **Next**.

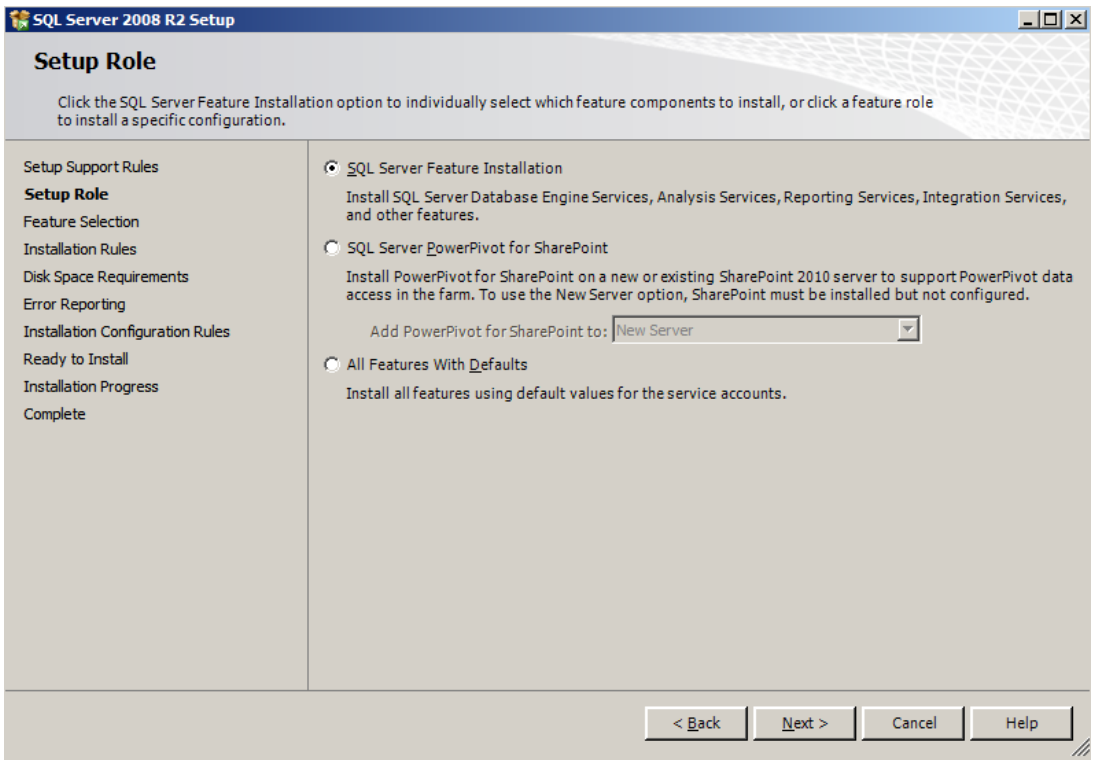
6. Bestätigen Sie mit **Install** die Installation der für das Setup benötigten Support-Dateien.



7. War die Installation der Setup-Dateien erfolgreich, so klicken Sie **Next**.

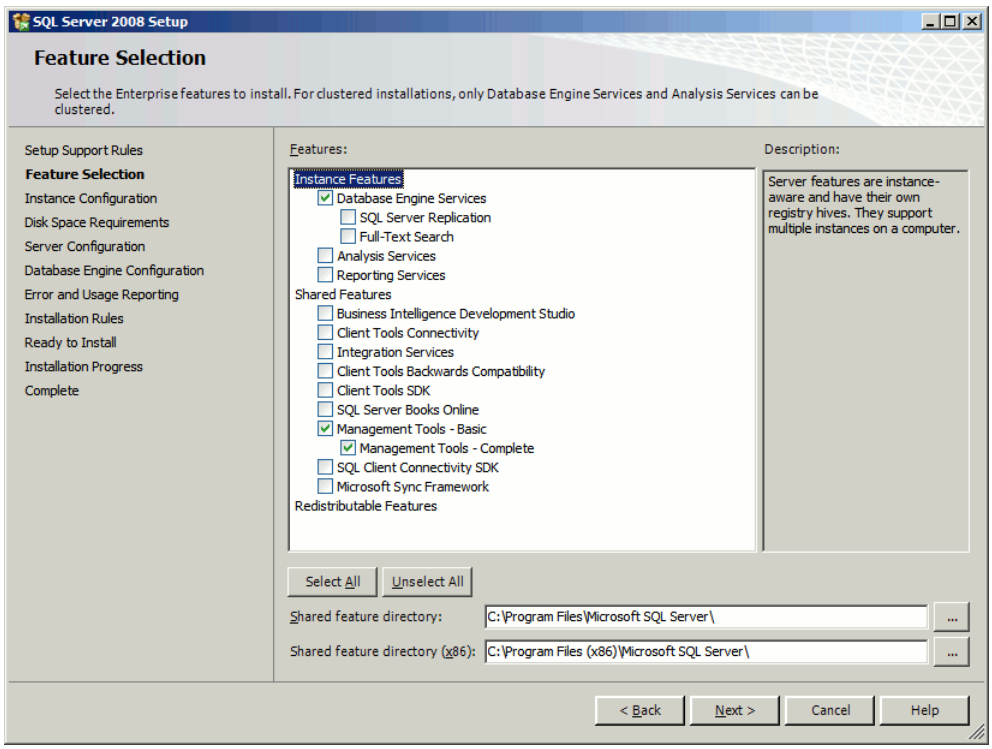


8. Wählen Sie die Option „SQL Server Feature Installation“ aus, um die zu installierenden SQL Server-Komponenten einzeln auswählen, oder klicken Sie auf eine Funktionsrolle, um eine bestimmte Konfiguration zu installieren.



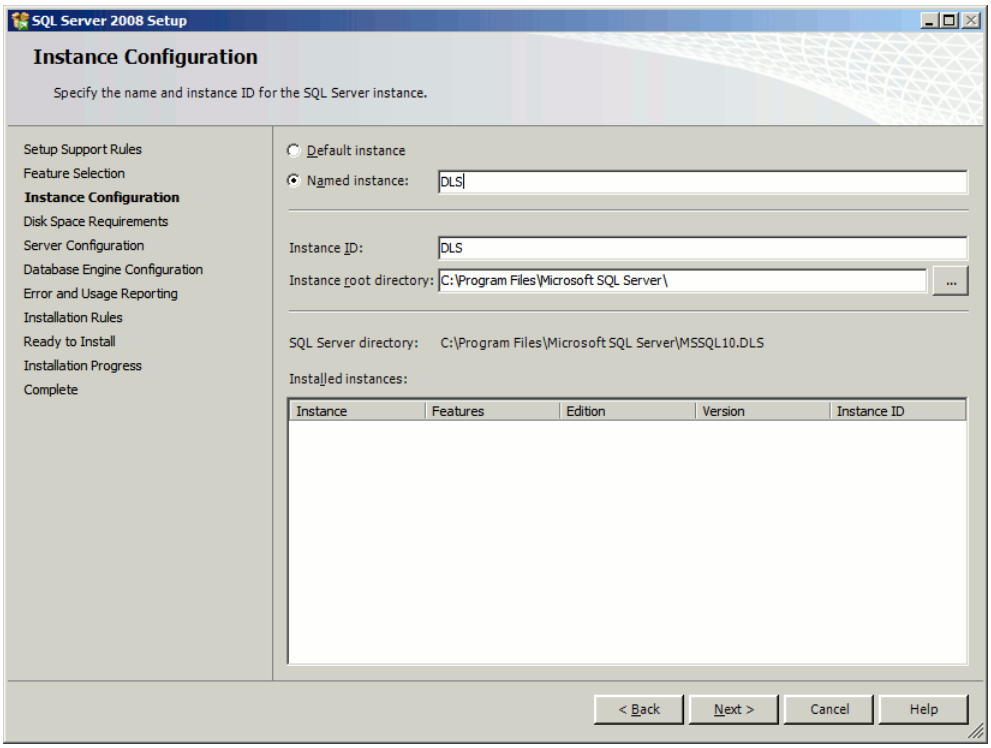
Klicken Sie auf **Next**.

9. Wählen Sie die folgenden Features zur Installation aus: **Database Engine Services**, **Management Tools – Basic**, **Management Tools – Complete**.



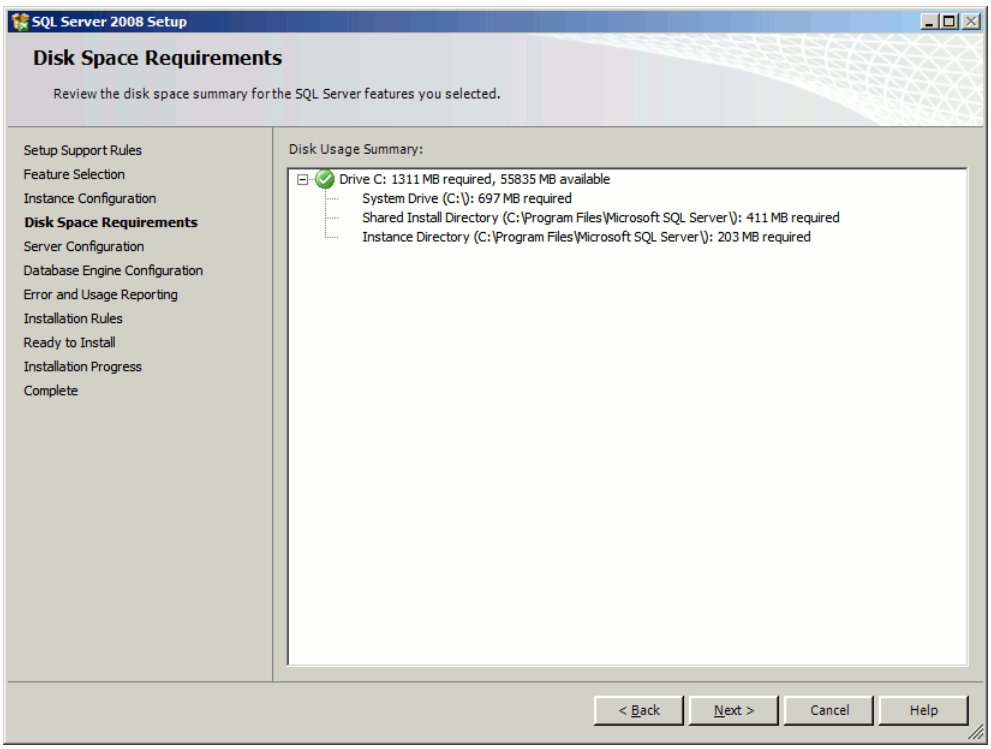
Klicken Sie auf **Next**.

10. Konfigurieren Sie nun die für den DLS verwendete Instanz des SQL-Servers. Wählen Sie hierzu **Named instance** aus und vergeben Sie einen Instanznamen, beispielsweise „DLS“. Unter **Instance root directory** geben Sie das Wurzelverzeichnis an.

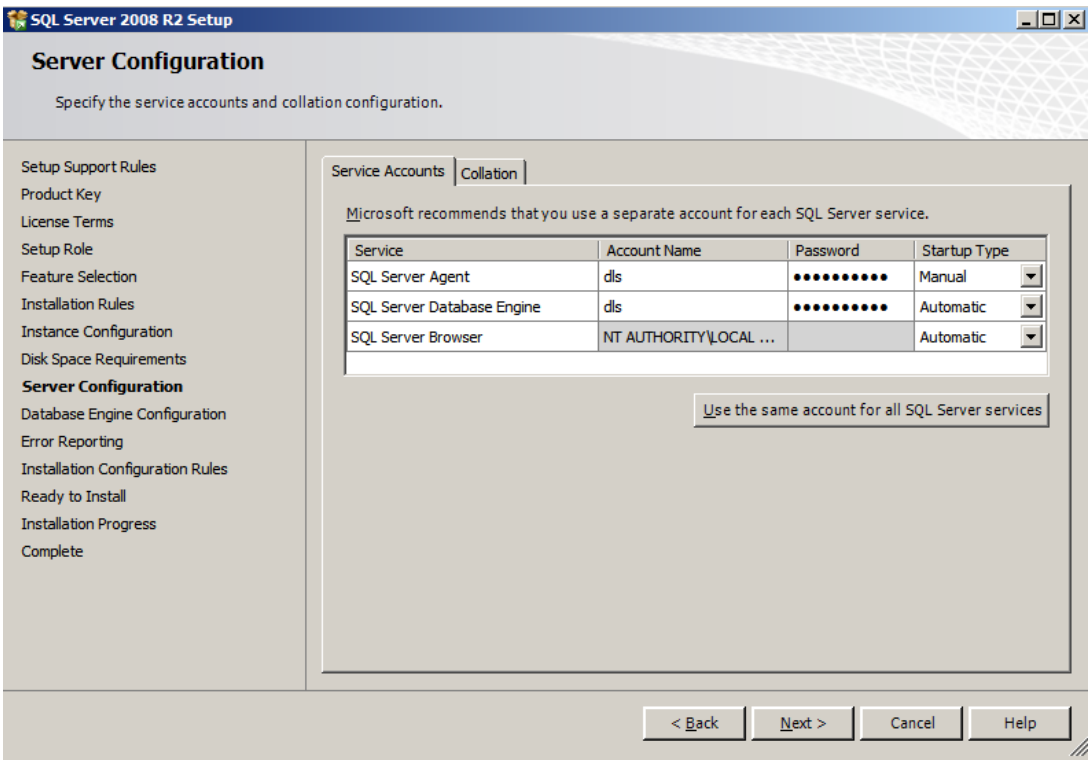


Klicken Sie auf **Next**.

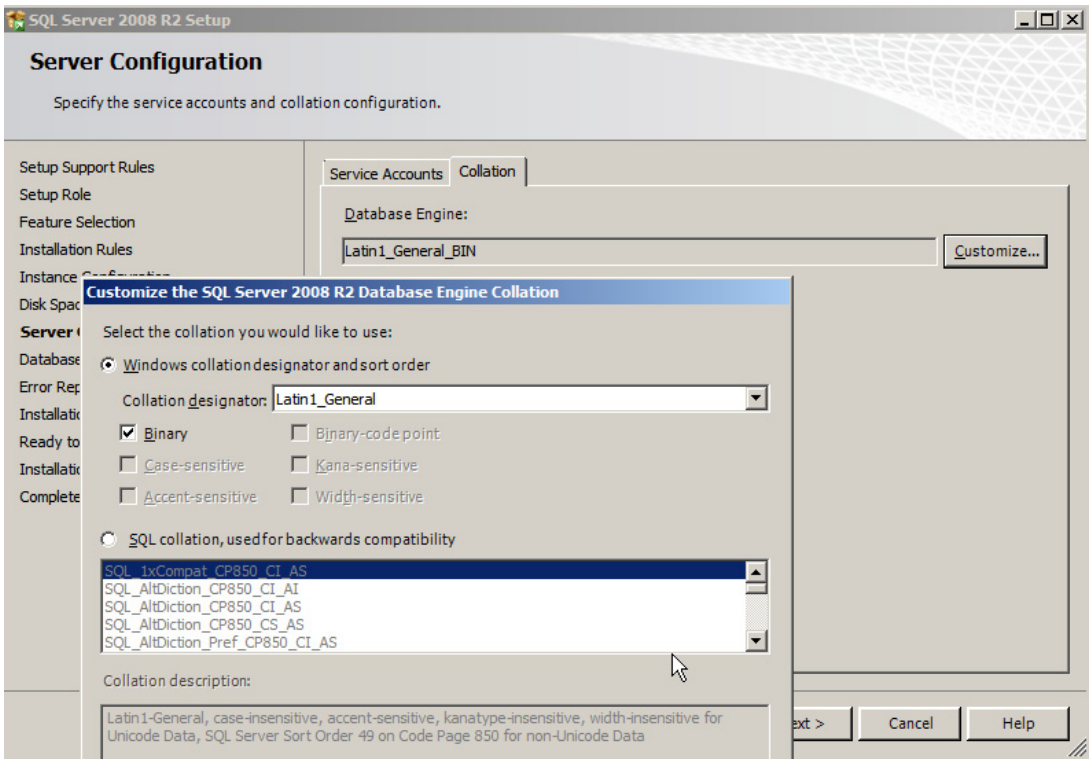
11. Der benötigte Speicherplatz auf der Festplatte wird angezeigt. Klicken Sie auf **Next**.



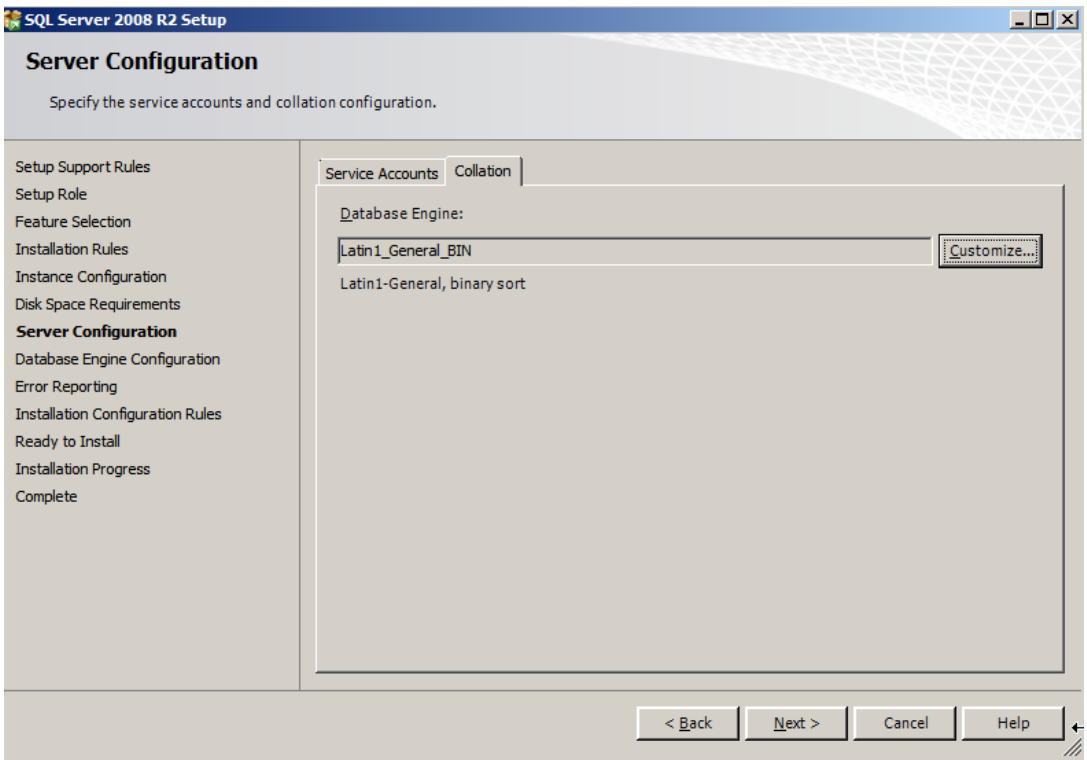
12. Im Karteireiter **Service Account** geben Sie für die Dienste **SQL Server Agent** und **SQL Server Database Engine** die Daten desjenigen Benutzers ein, unter dem sich die DLS-Knoten mit der Datenbank verbinden. Dieser Benutzer muss zur Gruppe der Administratoren gehören. Unter **Startup Type** wählen Sie für den **SQL Server Agent** „Manual“ und für die SQL Server Database Engine „Automatic“.



13. Legen Sie ein geeignetes Sortierverhalten fest. Klicken Sie für die **Database Engine** auf **Customize**.

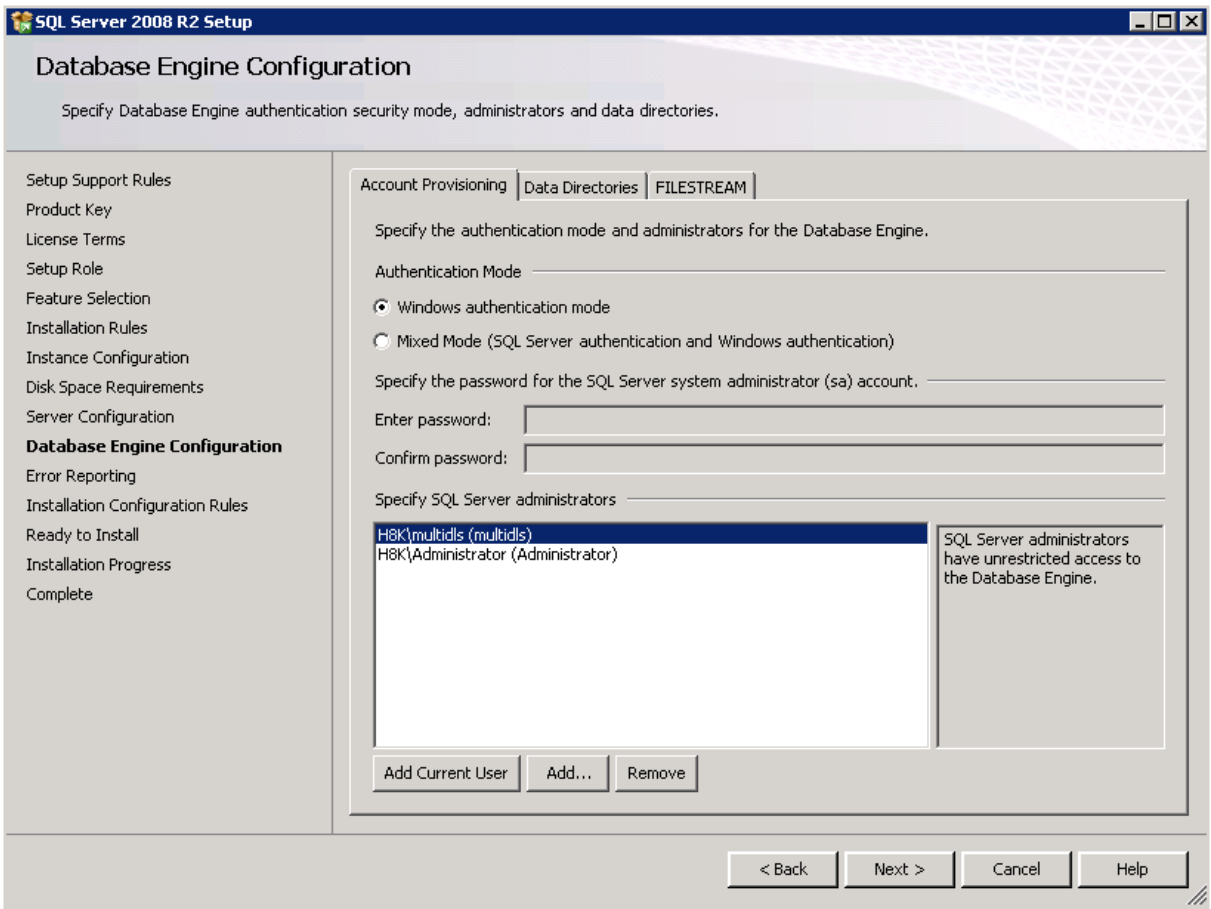


14. Für die Kollation selektieren Sie **Windows collation designator and sort order**. Unter **Collation designator** wählen Sie „Latin1_General_BIN“. Die Option **Binary** ist aktiviert.



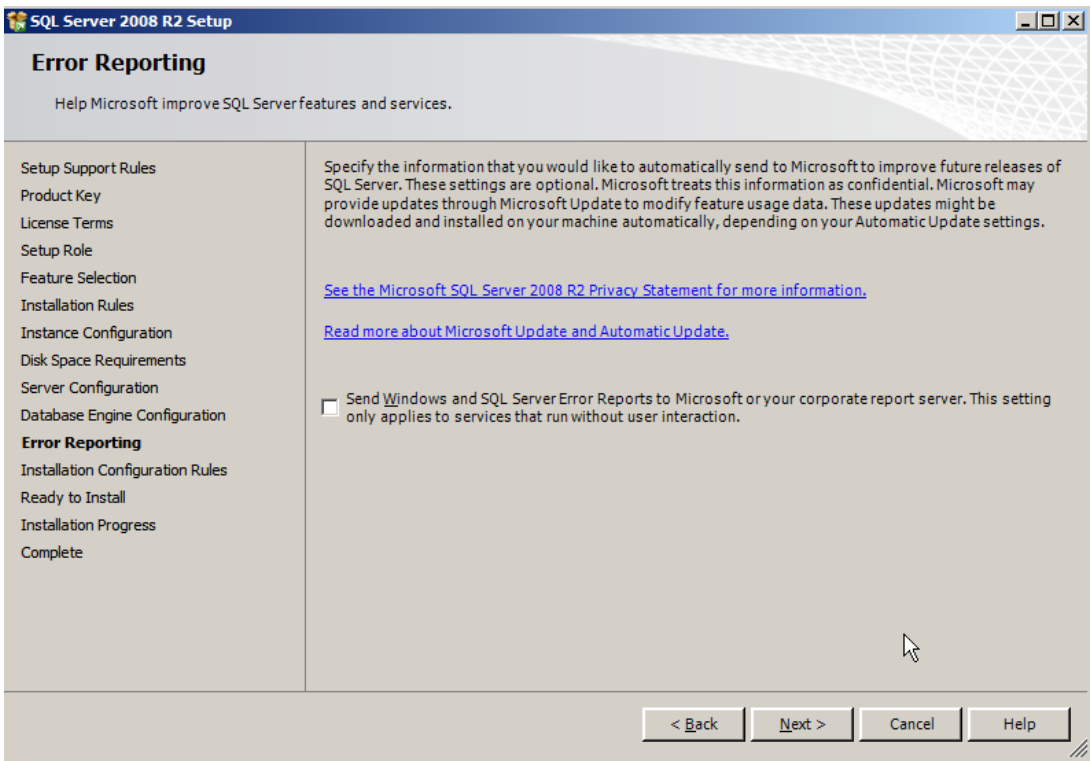
Bestätigen Sie mit **OK** und klicken Sie **Next**.

15. Im Karteireiter **Account Provisioning** unter **Authentication Mode** wählen Sie **Windows authentication mode**. Unter **Specify SQL Server administrators** fügen Sie mittels **Add...** den Administrator des Datenbank-Rechners hinzu sowie den Benutzeraccount, unter dem sich die DLS-Knoten mit der Datenbank verbinden.

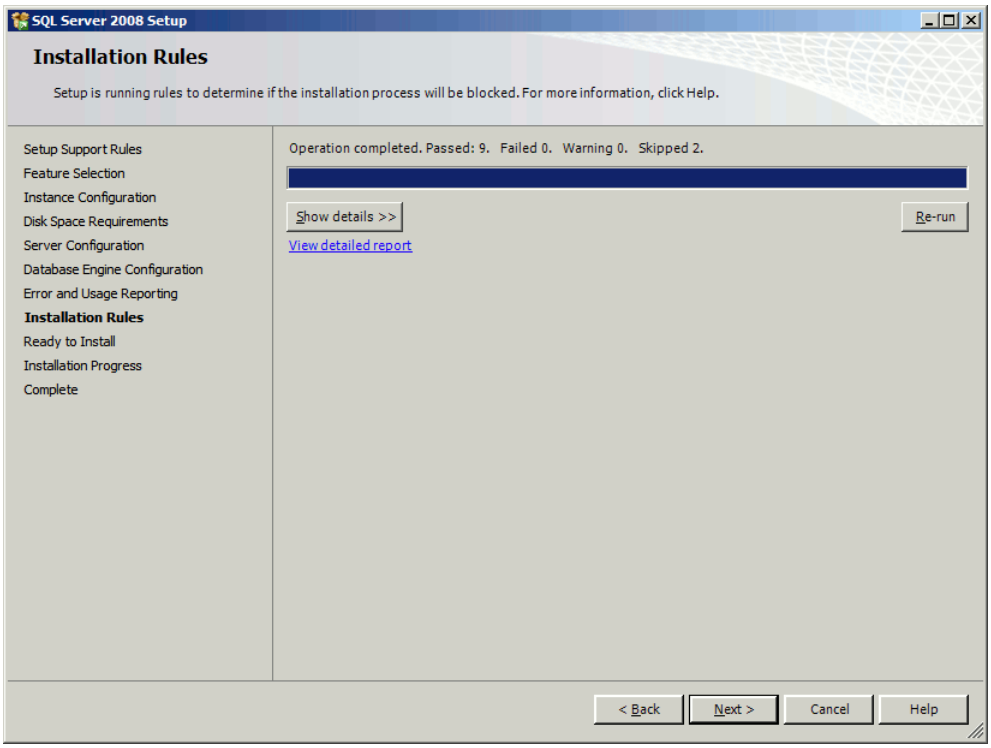


Klicken Sie auf **Next**.

16. Wenn Sie wünschen, aktivieren Sie die automatische Weitergabe von Informationen zum laufenden Betrieb des SQL-Servers an Microsoft.

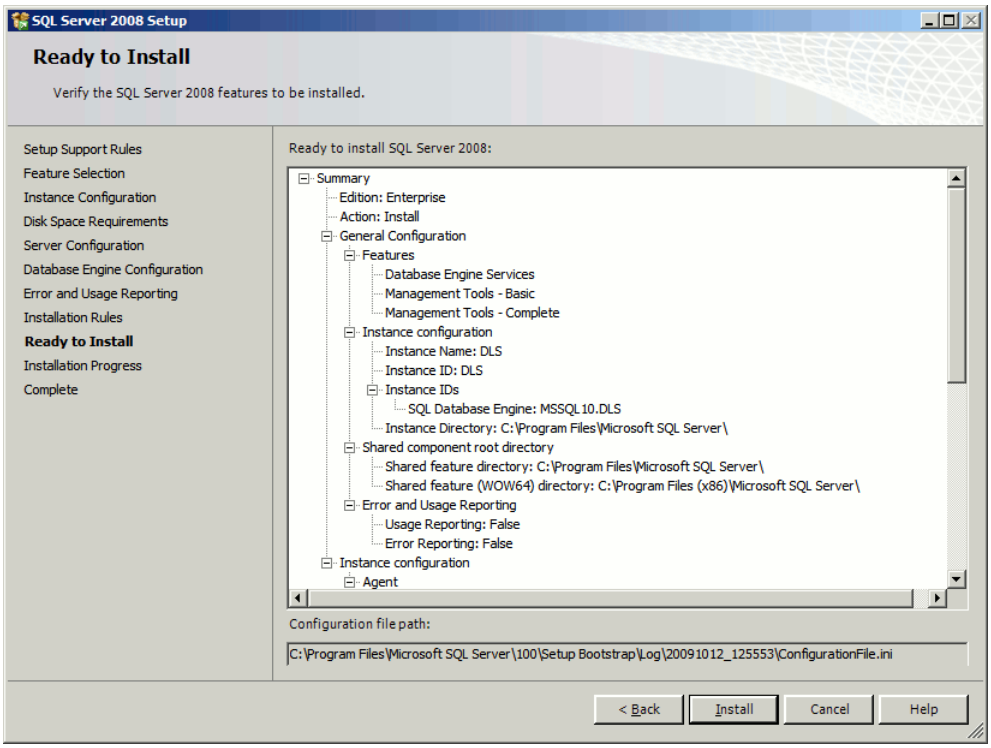


17. Das Installationsprogramm prüft, ob die Installation problemlos durchführbar ist.



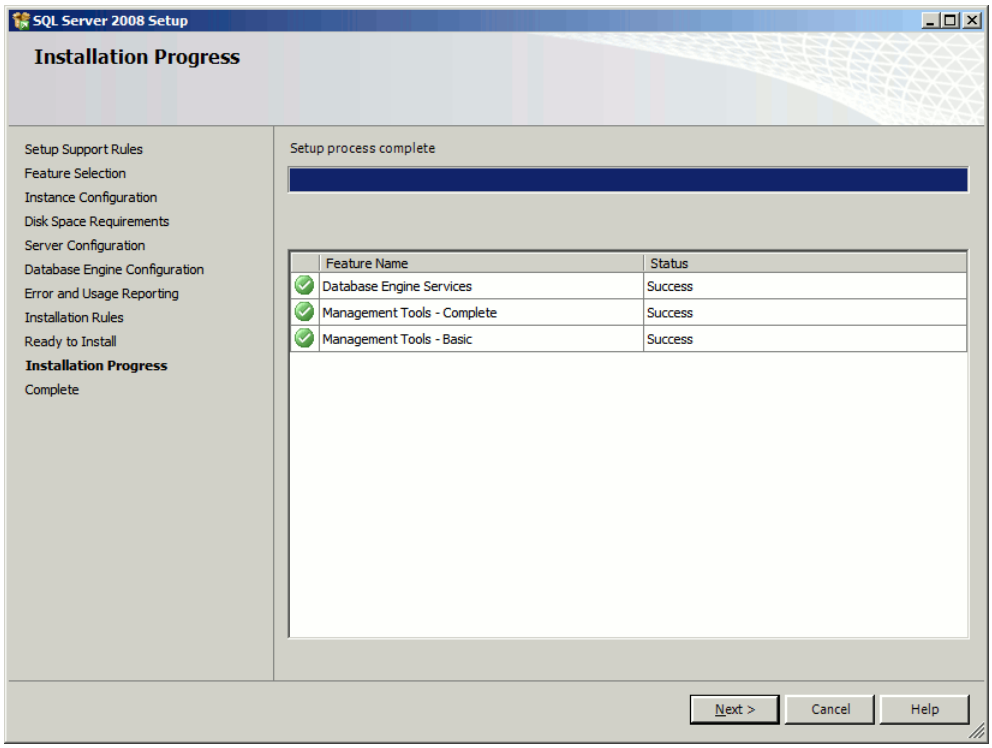
Wenn die Prüfung erfolgreich abgeschlossen ist, klicken Sie **Next**.

18. Die zur Installation vorgesehenen Komponenten und Konfigurationen werden angezeigt.

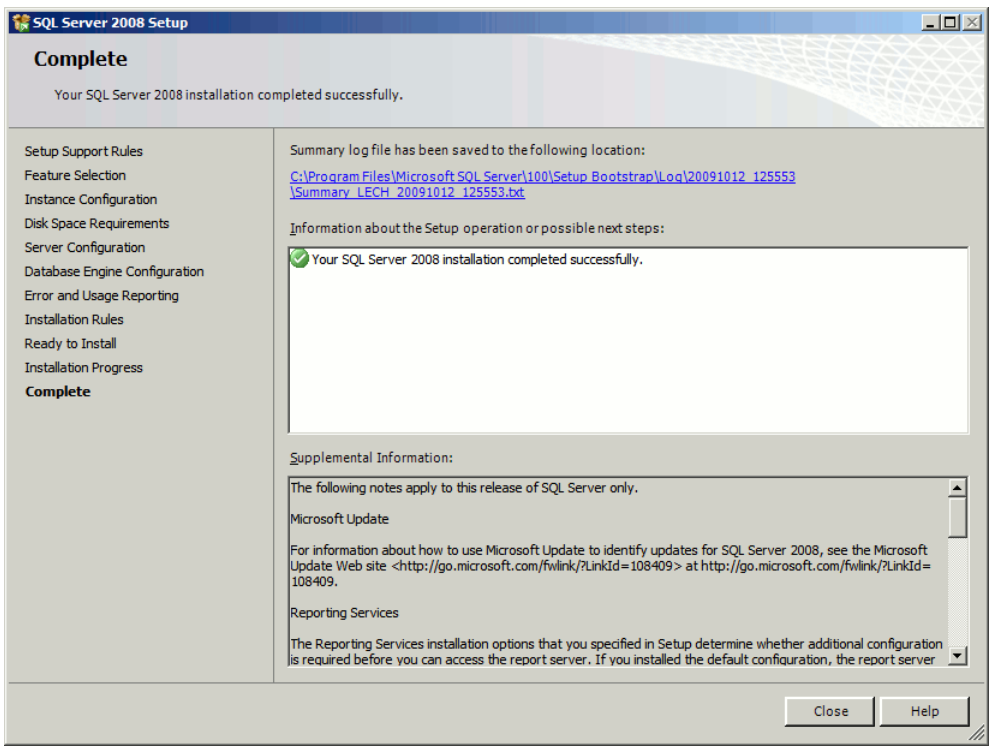


Wenn die Angaben dem Gewünschten entsprechen, klicken Sie **Next**.

19. Wenn die Installation erfolgreich verlaufen ist, klicken Sie **Next**.



20. Sie können jetzt das Installationsprogramm beenden, indem Sie **Close** klicken.



4.2.3 SQL Native Client – bei Nutzung einer entfernten Datenbank

Wenn der DLS mit einer entfernten Datenbank verwendet wird, muss der SQL Native Client installiert werden. Wenn noch kein SQL Native Client im System vorhanden ist, muss er vor der Installation von DLS installiert werden.

HINWEIS: Bitte achten Sie darauf, dass der SQL Native Client, der vor SQL installiert wurde, zu der zu installierenden SQL-Version passt.

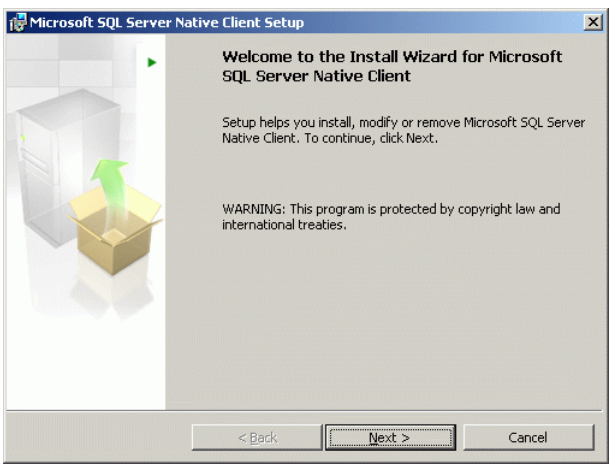
Es gibt zwei 2 DLS-Konfigurationen, bei denen eine entfernte Datenbank zum Einsatz kommt:

- Single Node mit entfernter Datenbank
- Multi-Node mit entfernter Datenbank

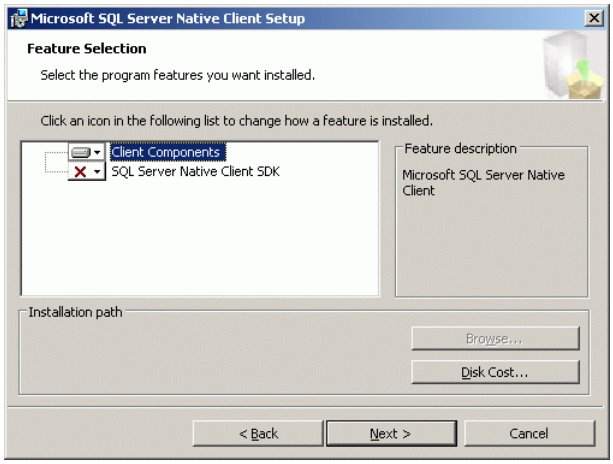
Für Konfigurationen mit mehreren Knoten muss der SQL Native Client auf jedem Knoten installiert sein.

Die Installation des Native Client muss einzeln ausgeführt werden. Der Native Client ist sowohl für 32-Bit als auch für 64-Bit-Betriebssysteme erforderlich. Der Native Client ist darüber hinaus auch dann erforderlich, wenn die Umgebung aus Domänen oder Arbeitsgruppen besteht.

1. Starten Sie das Setup-Programm.



2. Folgen Sie den Anweisungen der jeweiligen Fenster und klicken Sie **Next**. Im Fenster **Feature Selection** selektieren Sie **SQL Server Native Client SDK**.



3. Setzen Sie die Installation bis zum Abschluss fort.

Falls Probleme bei der DLS Neuinstallation auftreten, weil DLS und MSSQL zuvor über das gleiche System deinstalliert wurden, beachten Sie bitte das folgende:

1. Wenn MS SQL deinstalliert wurde, aber der DLS Installer meldet MS SQL vorhanden:
2. In Registry (regedit) löschen: `HKLM\Software\Microsoft\Microsoft SQL Server (HKEY_LOCAL_MACHINE)`
3. Kompletes Verzeichnis `\Microsoft SQL Server` in `\Program Files` Verzeichnis auf lokalem Laufwerk löschen
4. Rebooten (wichtig, da einige SQL Prozesse immer noch aktiv sein können)
5. Falls Fehler während der SQL Installation auftreten, Log-Datei **Detail_ComponentUpdate.txt** durchsuchen z.B.: `..\Microsoft SQL Server\100\Setup Bootstrap\Log\20110225_092344`) nach der Fehlermeldung „MsiGetProductInfo failed to retrieve ProductVersion for package“ in der eine GUID aufgeführt wird.

   Lösche den Registry-Eintrag wie folgt:

   Den ersten Teil der GUID `2243F21A-E132-44F7-BA13-024D0845C815` nehmen (`2243F21A`) und umdrehen (`A12F3422`). Dann innerhalb des Registry-Key danach suchen `HKCR\Installer\UpgradeCodes` (`HKEY_CLASSES_ROOT`).

4.2.4 Ändern des Service-Passworts

Sollte eine Änderung des Service-Passworts notwendig sein, gehen Sie in

```
<DLS-Installationsverzeichnis>\Tomcat5\webapps\DeploymentService\
database
```

und rufen Sie `dlsSetServicePW.bat <neues Passwort>` auf.

Anschließend ändern Sie auf jedem DLS-Knoten das Passwort für den Dienst ‘DeploymentService’.

4.3 Konfiguration des Network Load Balancer

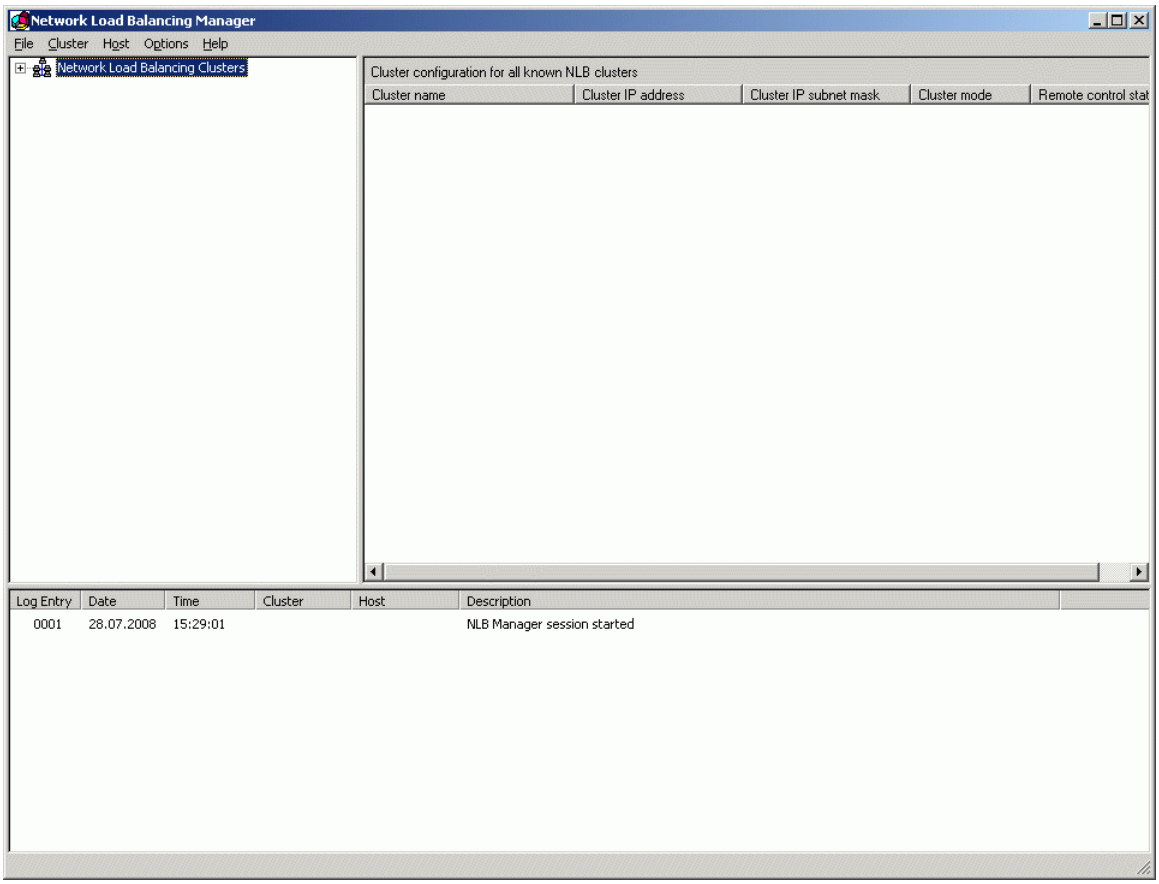
Für den Cluster-Betrieb ist ein Netzwerk-Load Balancer erforderlich. Im Folgenden wird jeweils der in Windows Server 2003/2008 enthaltene Network Load Balancer beschrieben.

> ***HINWEIS:*** Es wird dringend empfohlen, den Microsoft Network Load Balancer zu verwenden, da derzeit die volle Funktionalität nur durch den Netzwerklastenausgleich (NLB) von Microsoft unterstützt wird.

4.3.1 Network Load Balancer für Windows Server 2003

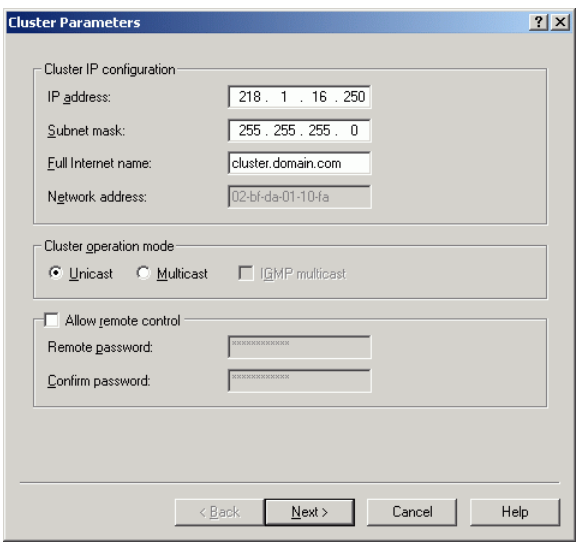
HINWEIS: Einzelne Konfigurationsschritte können bis zu etwa 1 Minute dauern. Warten Sie in solchen Fällen ab und machen Sie in der Zwischenzeit keine Eingaben.

1. Die Bezeichnungen für Menüs, Eingabefelder und Parameter sowie die Screenshots sind der englischsprachigen Version von Windows Server 2008 entnommen. Rufen Sie auf einem der Knotenrechner **Start** > **Administrative Tools** > **Network Load Balancer Manager** auf. Damit wird der Dienst auf allen Knotenrechnern aktiviert, was für den Cluster-Betrieb erforderlich ist.
2. Ein dreigeteiltes Konfigurationsfenster öffnet sich. Um einen neuen Cluster anzulegen, gehen Sie im Menü auf **Cluster** > **New** oder rufen Sie mit der rechten Maustaste das Kontextmenü auf und gehen Sie auf **New Cluster**.


Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
Cluster configuration for all known NLB clusters
Cluster name
Cluster IP address
Cluster IP subnet mask
Cluster mode
Remote control stat
Log Entry
Date
Time
Cluster
Host
Description
0001
28.07.2008
15:29:01
NLB Manager session started

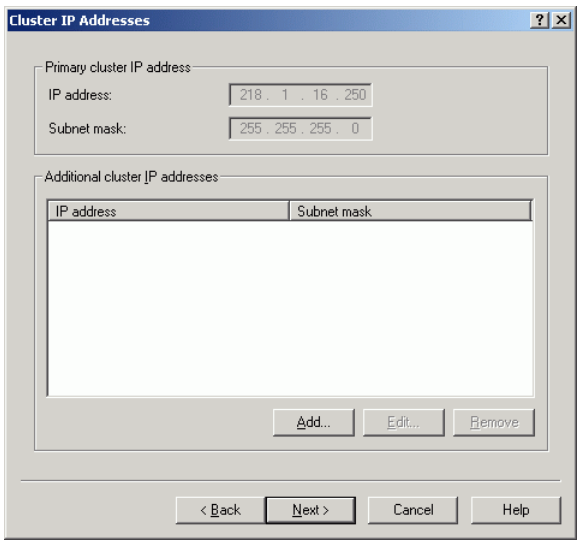
3. Im Fenster **Cluster Parameters** geben Sie die folgenden Parameter ein:

   - **IP address**: IP-Adresse, unter der der DLS-Cluster von außerhalb erreichbar ist („virtuelle IP-Adresse“).
   - **Subnet mask**: Subnetz-Maske für den Cluster.
   - **Full internet name**: DNS-Name, unter dem der DLS-Cluster von außerhalb erreichbar ist.
   - **Cluster operation mode**: Selektieren Sie **Unicast**. Mit dieser Einstellung bekommen alle Netzwerkschnittstellen im äußeren Netzwerk dieselbe MAC-Adresse zugewiesen. Die eingehenden Datenpakte werden damit zunächst von allen Knotenrechnern empfangen und dann vom Network Load Balancer gefiltert.
     HINWEIS: Wenn Sie versuchen, über den Network Load Balancing Manager eine Verbindung zu einem Network Load Balancing (NLB)-Cluster herzustellen, ist unter Umständen nur eine Verbindung zu einem Knoten möglich. Lesen Sie hierzu:
     http://support.microsoft.com/kb/898867
   - **Allow remote control**: Erlauben Sie die Fernsteuerung und geben Sie ein starkes Passwort an, um Missbrauch zu vermeiden. Dieses Passwort müssen Sie sich merken und später dem DLS mitteilen (siehe Abschnitt 4.5.3.1, “Erster Knoten”, Schritt 15).

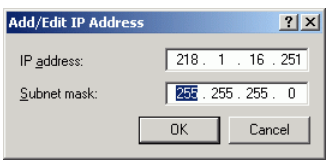


Klicken Sie auf **Next**.

4. Nun kann der neue Cluster mit IP-Adressen bevölkert werden. Klicken Sie hierzu im Fenster **Cluster IP Addresses** auf **Add**.

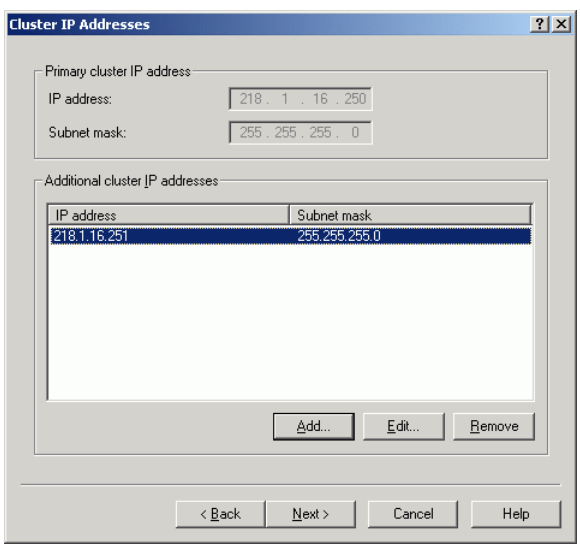


5. Es öffnet sich das Dialogfenster **Add/Edit IP Address**, in welchem Sie IP-Adresse und Subnetzmaske des ersten Knotenrechners angeben.

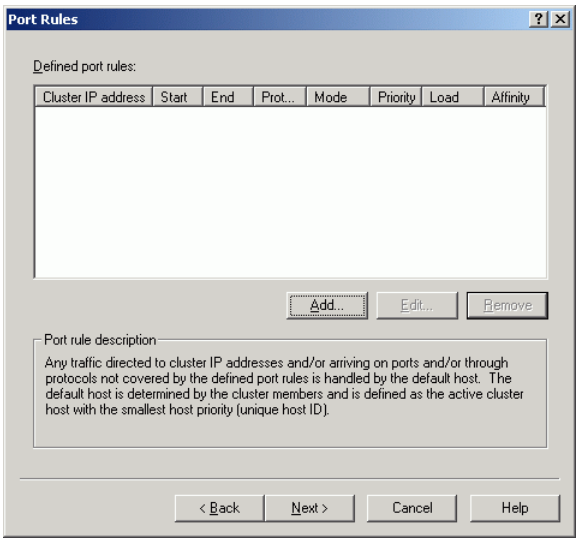


Klicken Sie anschließend auf **OK**.

6. Sie gelangen wieder in das Fenster **Cluster IP Adresses**. Der neu eingetragene Rechner erscheint nun unter **Additional cluster IP adresses**.



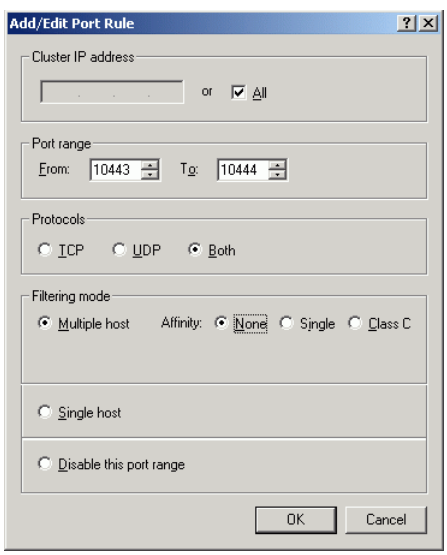
7. Klicken Sie auf **Next**. Im Fenster **Port Rules** legen Sie Regeln fest für all diejenigen Ports, über die der DLS-Cluster nach außen kommuniziert. Falls hier bereits Port-Regeln vorhanden sind, entfernen Sie diese mit **Remove**.



Klicken Sie auf **Add**.

8. Es öffnet sich das Fenster **Add/Edit Port Rule**. Machen Sie hier jeweils die Angaben für die verwendeten Ports bzw. Portbereiche. Unter **Cluster IP address** aktivieren Sie **All**, um die Regel allen IP-Adressen innerhalb des Clusters zuzuweisen. Wählen Sie unter **Affinity** die Option **None**. Bei dieser Einstellung ist es möglich, dass aufeinanderfolgende Anfragen von ein und derselben IP-Adresse jeweils durch verschiedene Knoten bearbeitet werden. Somit ist sichergestellt, dass die Lasten gleichmäßig verteilt werden.

   Das folgende Bildschirmfoto zeigt die Angaben für die Ports 10443 und 10444. (Funktion dieser Ports siehe Schritt 9).

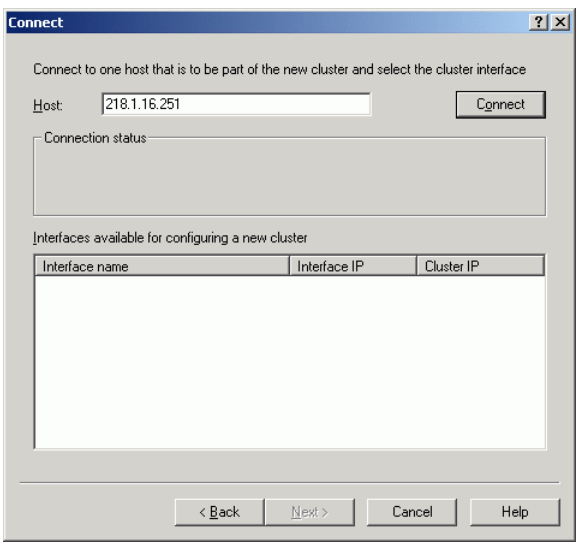


9. Geben Sie die Regeln für die restlichen Ports an, wie in Schritt 7 und 8 beschrieben. Im Folgenden sind die für den DLS elementaren Ports aufgelistet (eine vollständige Liste aller DLS-Ports finden Sie in der Sicherheitscheckliste des Planungshandbuchs):

   - 10443: Empfängt Daten von der grafischen Benutzeroberfläche, also vom Web-Browser, wenn HTTPS benutzt wird.
   - 10444: Empfängt Daten über HTTPS von der DlsAPI, dem Web Service-Interface des DLS.
   - 18080: Empfängt Daten von der grafischen Benutzeroberfläche, also vom Browser, wenn HTTP benutzt wird.
   - 18443: Empfängt Daten von den Endgeräten (HTTP und HTTPS).
   - 18444: Empfängt Daten von den Endgeräten bei sicherer Verbindung zwischen DLS und Endgerät (Secure Modus).

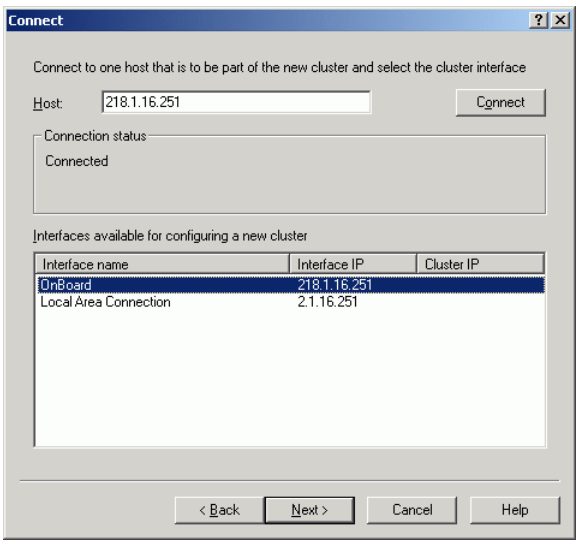
   Wenn Sie alle Port-Regeln eingetragen haben, klicken Sie **Next**.

10. Nun werden die einzelnen Knotenrechner zu einem Cluster verbunden. Im Fenster **Connect** geben Sie im Feld **Host** die IP-Adresse des ersten Knotenrechners ein.



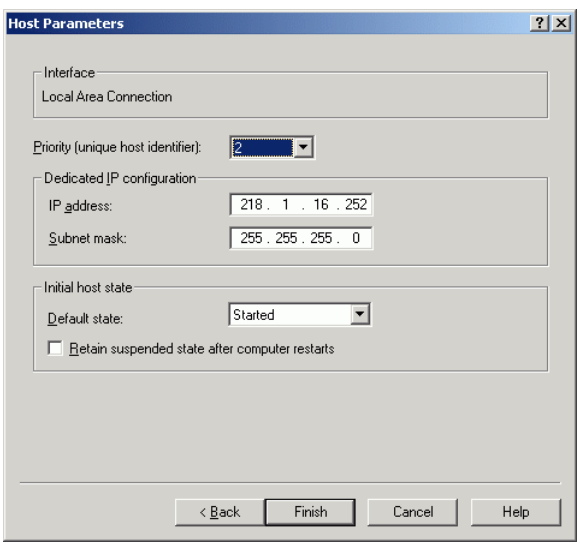
   Klicken Sie anschließend auf **Connect**.

11. Unter **Interfaces available for configuring a new cluster** finden Sie jetzt alle Netzwerkschnittstellen des neu hinzugefügten Rechners. Markieren Sie diejenige Netzwerkkarte, die sich im äußeren Netzwerk befindet, um in das Fenster **Host Parameters** zu gelangen.



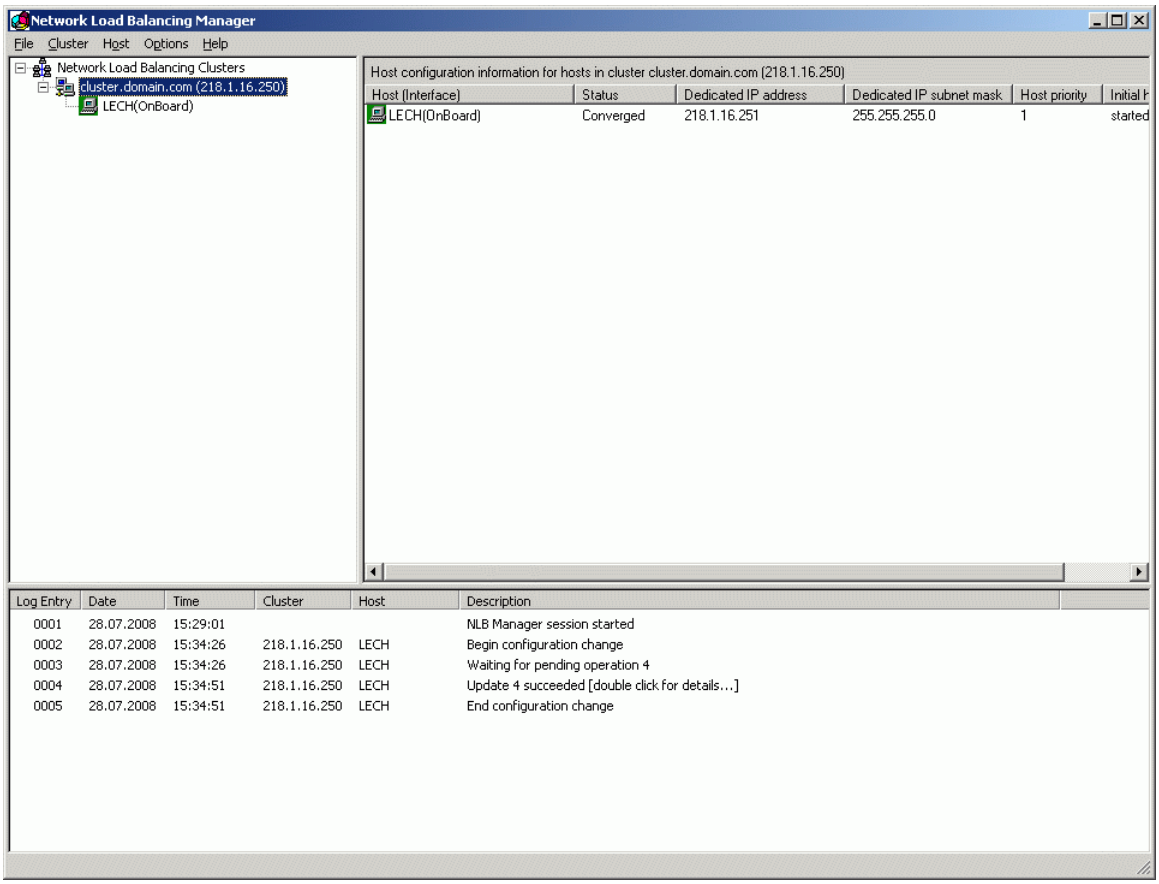
Klicken Sie anschließend auf **Next**.

12. Im Feld **Priority** wird ein vorgegebener Wert angezeigt, der eine reine Numerierung darstellt und keine Priorisierung impliziert. Das Feld **IP address** enthält die IP-Adresse der Netzwerkschnittstelle.



Wenn alle Werte stimmen, klicken Sie auf **Finish**. Das Hinzufügen des Knotens zum Cluster kann 1-2 Minuten dauern.

13. Sie gelangen in das Hauptfenster des **Network Load Balancing Manager**, wo der Cluster in seiner aktuellen Zusammensetzung angezeigt wird. Wenn das Einfügen des Knotenrechners erfolgreich war, ist der **Status** auf **Converged** gesetzt.



Gehen Sie auf **Add Host** im Menü **Cluster** oder rufen Sie mit der rechten Maustaste das Kontextmenü auf und gehen auf **Add Host to Cluster**, um einen weiteren Knotenrechner hinzuzufügen.

14. Gehen Sie für den nächsten sowie alle weiteren Knotenrechner vor wie in Schritt 10 bis 12 beschrieben.

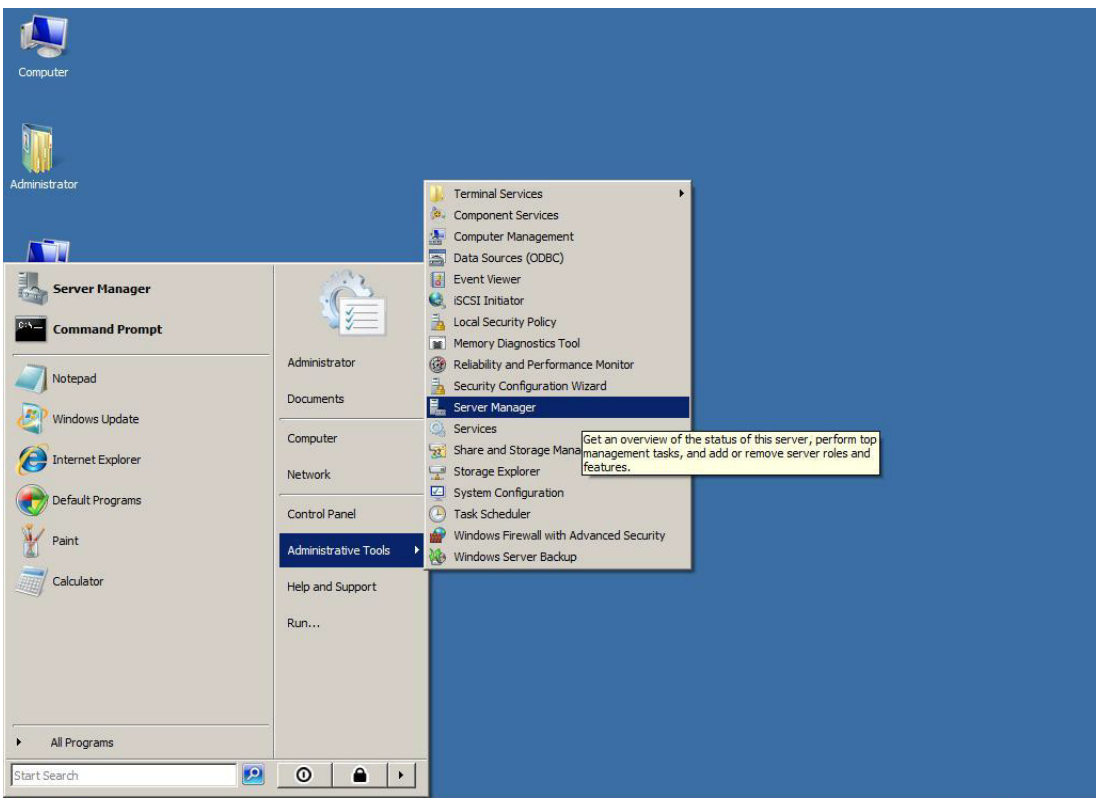
HINWEIS: Falls Sie nach dem Konfigurieren der Host-Parameter keine aktuelle Ansicht des Clusters erhalten, drücken Sie die Steuertaste F5 auf Ihrem Rechner. Falls Sie dann Fehlermeldungen erhalten, schließen Sie den NLB Manager, starten ihn neu und verbinden sich erneut mit dem Cluster. Falls weitere Probleme auftreten, konsultieren Sie bitte die einschlägige Dokumentation zum Microsoft Network Load Balancer.

4.3.2 Network Load Balancer für Windows Server 2008

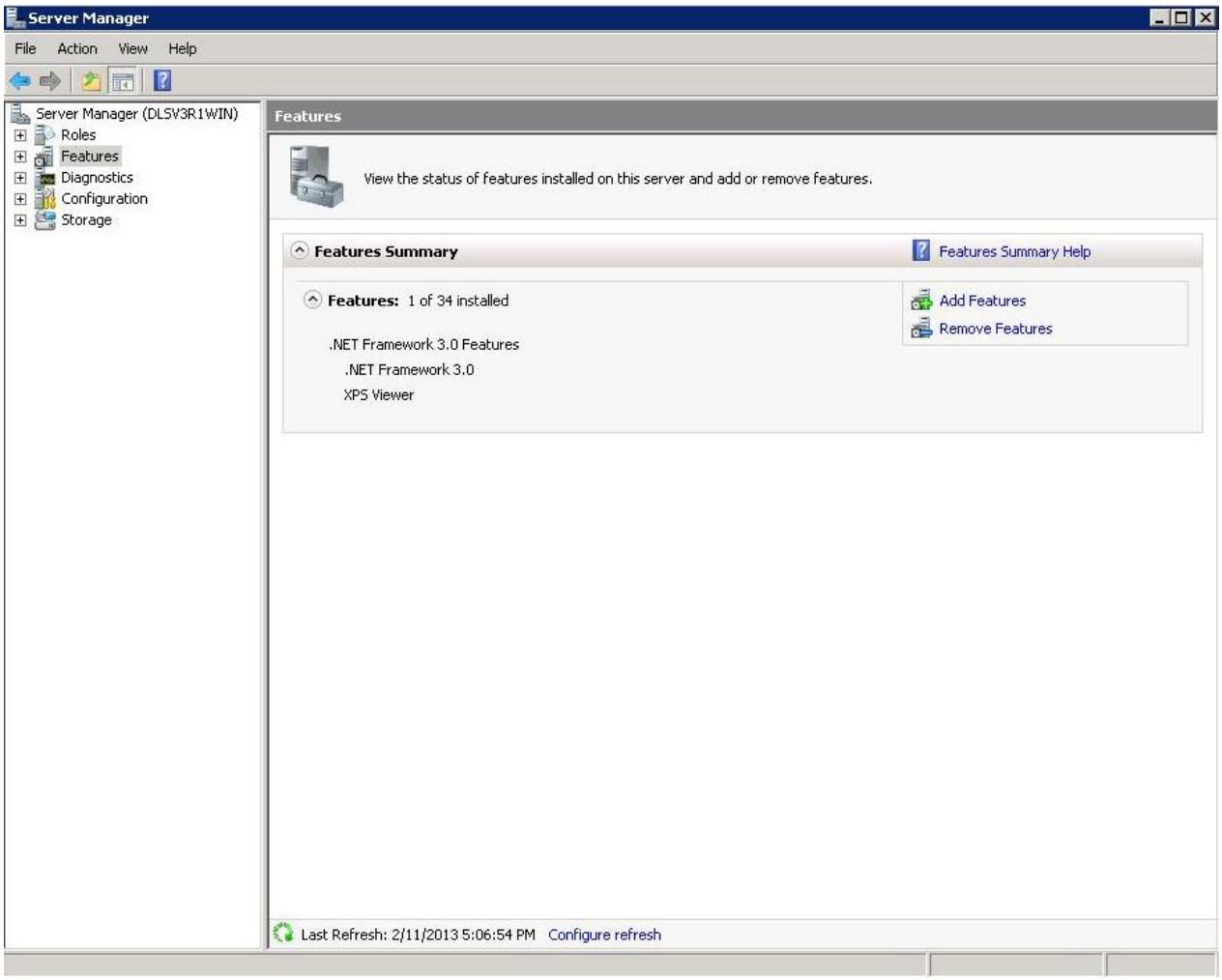
HINWEIS: Einzelne Konfigurationsschritte können bis zu etwa 1 Minute dauern. Warten Sie in solchen Fällen ab und machen Sie in der Zwischenzeit keine Eingaben.

Für den Fall, dass der Network Load Balancer nicht vom System vorinstalliert wird:

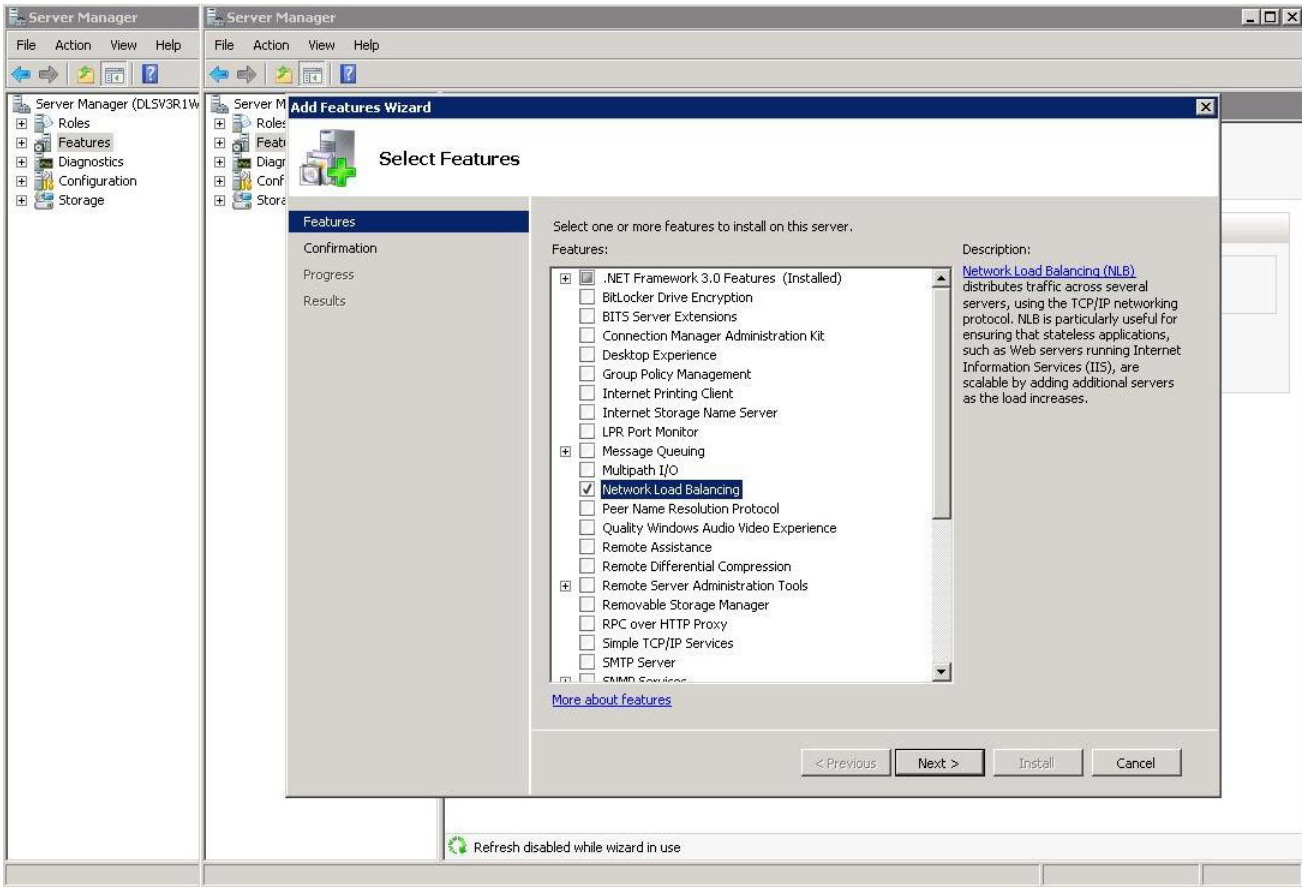
- Rufen Sie den **Server Manager** wie folgt über das Windows-Startmenü auf: **Start** > **Programs** > **Administrative Tools** > **Server Manager.**



- Klicken Sie im Fenster **Server Manager**, im Navigationsbaum links auf **Features**. Klicken Sie anschließend auf **Add Features**, um den Assistenten **Add Features** zu starten.



- Aktivieren Sie dann das Kontrollkästchen **Network Load Balancing**.



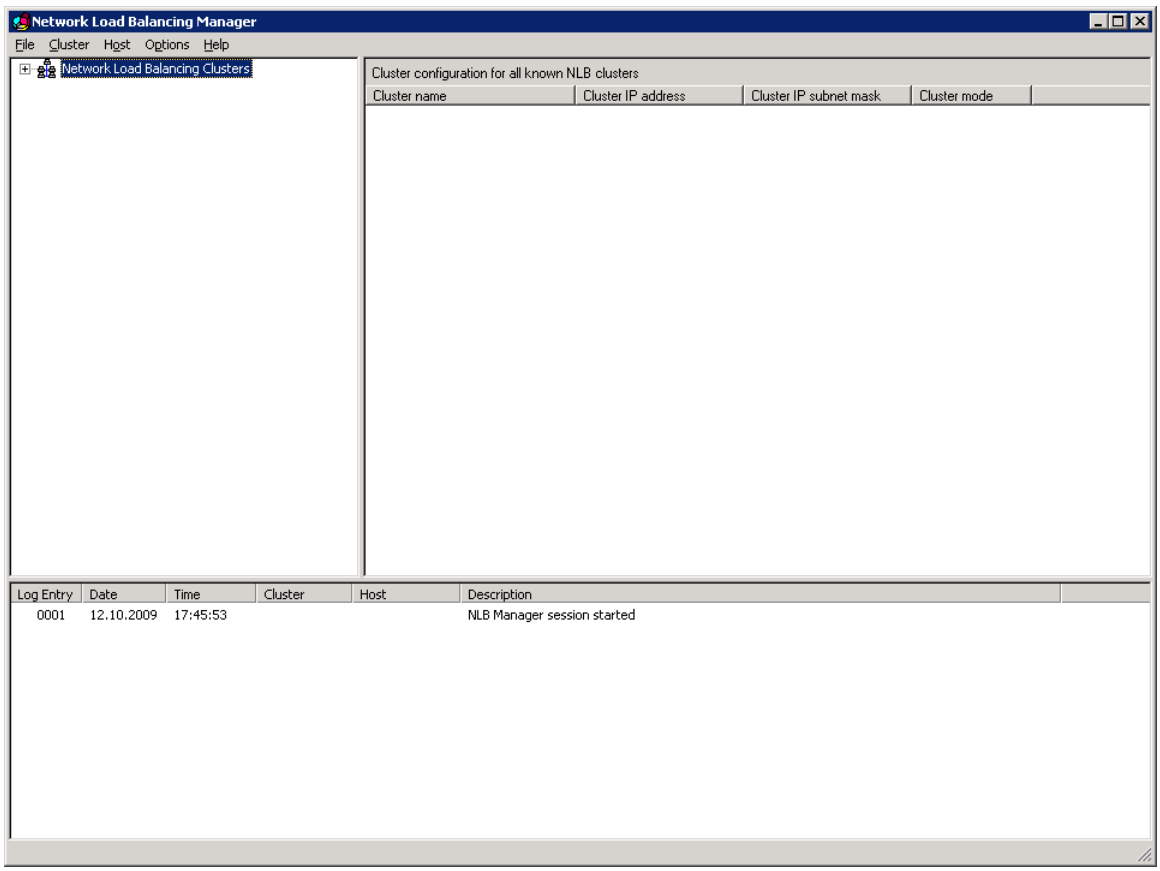
Klicken Sie auf **Next**.

- Warten Sie, bis die Installation abgeschlossen ist und der abschließende Dialog erscheint.
- Klicken Sie auf **Finish**. Die Installation ist abgeschlossen.

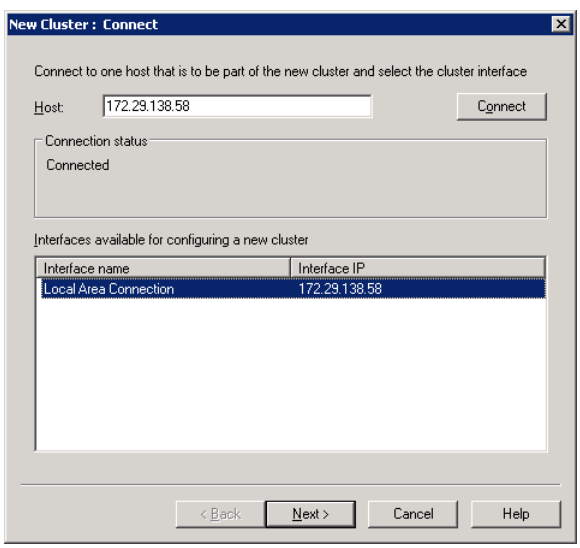
HINWEIS: Der Network Load Balancer sollte nun auf allen DLS-Knoten installiert/aktiviert sein.

Nachfolgend wird beschrieben, wie Sie den Network Load Balancer konfigurieren:

1. Die Bezeichnungen für Menüs, Eingabefelder und Parameter sowie die Screenshots sind der englischsprachigen Version von Windows Server 2008 entnommen. Rufen Sie auf einem der Knotenrechner **Start** > **Administrative Tools** > **Network Load Balancer Manager** auf. Damit wird der Dienst auf allen Knotenrechnern aktiviert, was für den Cluster-Betrieb erforderlich ist.
2. Ein dreigeteiltes Konfigurationsfenster öffnet sich. Um einen neuen Cluster anzulegen, gehen Sie im Menü auf **Cluster** > **New** oder rufen Sie mit der rechten Maustaste das Kontextmenü auf und gehen Sie auf **New Cluster**.

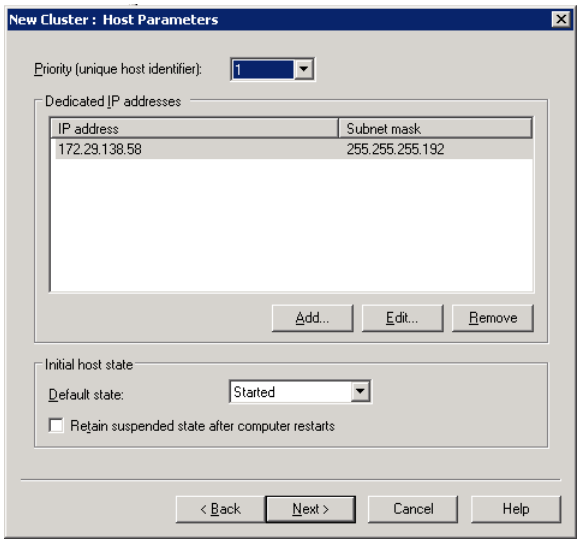


3. Im Fenster **New Cluster: Connect** geben Sie im Feld **Host** die IP-Adresse des ersten Knotenrechners ein.



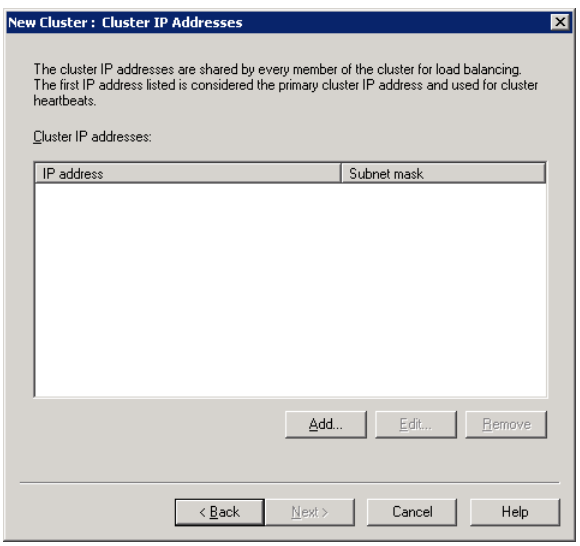
Klicken Sie anschließend auf **Connect**.

4. Sie befinden sich nun Fenster **New Cluster: Host Parameters**. Im Feld **Priority** wird ein vorgegebener Wert angezeigt, der eine reine Numerierung darstellt und keine Priorisierung impliziert. Das Feld IP address enthält die IP-Adresse der Netzwerkschnittstelle.

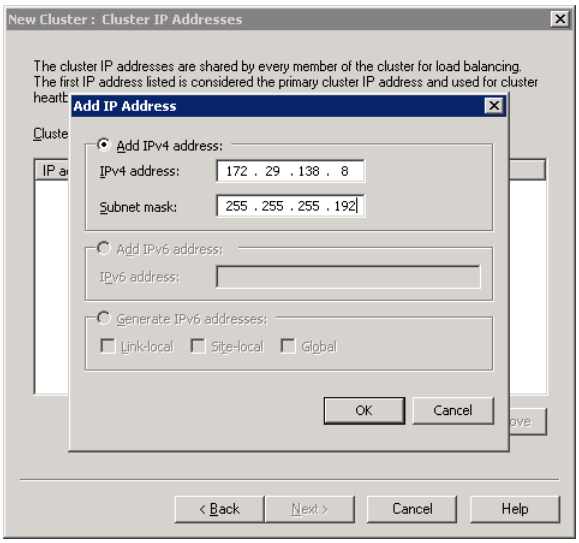


Wenn alle Werte stimmen, klicken Sie auf **Finish**. Das Hinzufügen des Knotens zum Cluster kann 1-2 Minuten dauern.

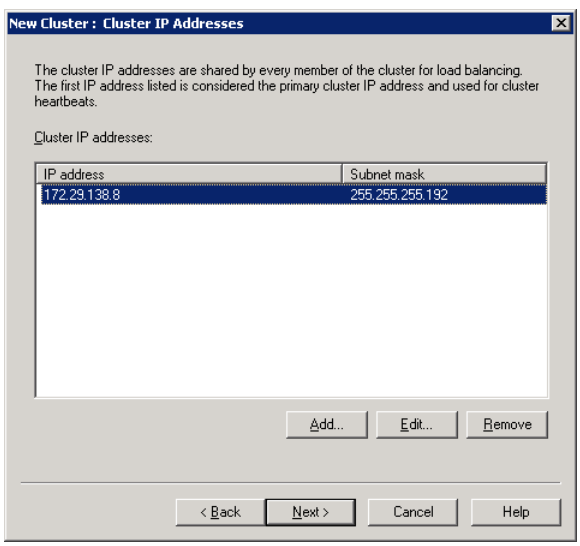
5. Im Fenster **New cluster: Cluster IP Addresses** werden die gemeinsamen Adressen des Clusters eingegeben. Klicken Sie auf **Add**.



6. Im Dialogfenster **Add IP Address** geben Sie in **IPv4 address** die IP-Adresse ein, unter der der Cluster erreichbar sein soll. Im Feld **Subnet mask** geben Sie die entsprechende Subnetzmaske ein.

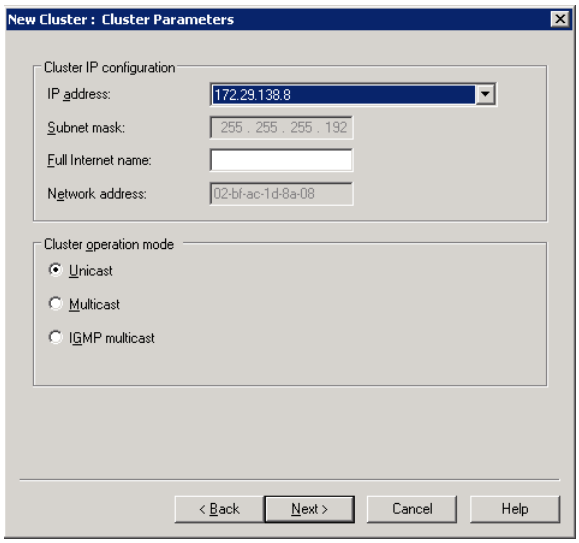


7. Im Fenster **New Cluster: Cluster IP Addresses** erscheint nun die Adresse des Clusters.



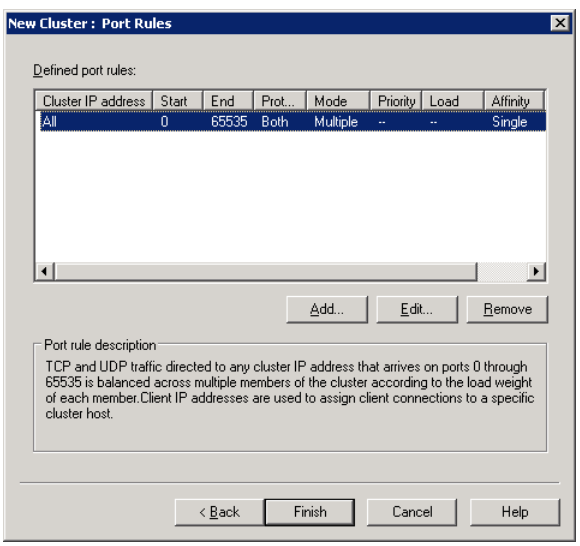
   Klicken Sie auf **Next**.

8. Sie befinden sich jetzt im Fenster **New Cluster: Cluster Parameters**. Soll der Cluster unter einem DNS-Namen erreichbar sein, geben Sie diesen in **Full Internet name** ein, z. B. `cluster.domain.com`. Im Feld **Cluster operation mode** wählen Sie **Unicast**. Mit dieser Einstellung bekommen alle Netzwerkschnittstellen im äußeren Netzwerk dieselbe MAC-Adresse zugewiesen. Die eingehenden Datenpakte werden damit zunächst von allen Knotenrechnern empfangen und dann vom Network Load Balancer gefiltert.



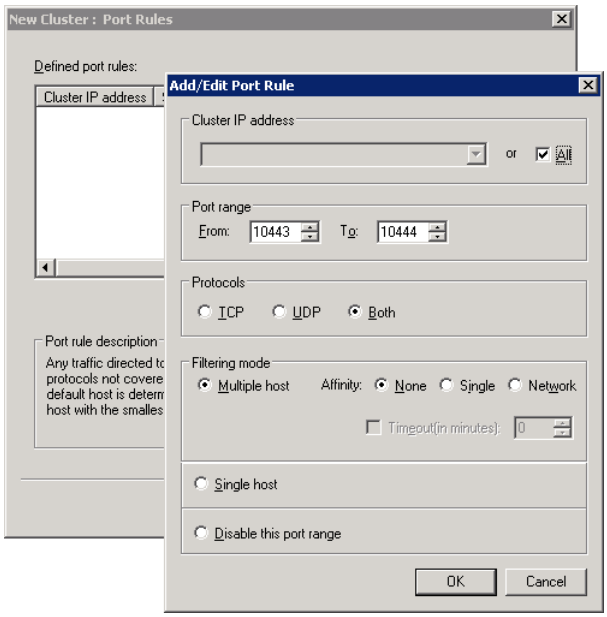
Klicken Sie auf **Next**.

9. Im Fenster **New Cluster: Port Rules** legen Sie Regeln fest für all diejenigen Ports, über die der DLS-Cluster nach außen kommuniziert. Falls hier bereits Port-Regeln vorhanden sind, entfernen Sie diese mit **Remove**.



Klicken Sie auf **Add**.

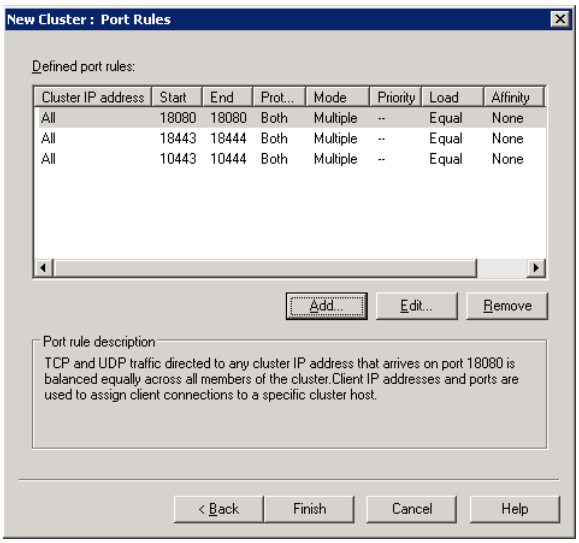
10. Es öffnet sich das Dialogfenster **Add/Edit Port Rule**. Machen Sie hier jeweils die Angaben für die verwendeten Ports bzw. Portbereiche. Unter **Cluster IP address** aktivieren Sie **All**, um die Regel allen IP-Adressen innerhalb des Clusters zuzuweisen. Wählen Sie unter **Affinity** die Option **None**. Bei dieser Einstellung ist es möglich, dass aufeinanderfolgende Anfragen von ein und derselben IP-Adresse jeweils durch verschiedene Knoten bearbeitet werden. Somit ist sichergestellt, dass die Lasten gleichmäßig verteilt werden. Das folgende Bildschirmfoto zeigt die Angaben für die Ports 10443 und 10444. Die Funktionen dieser Ports sind in Schritt 11 beschrieben.



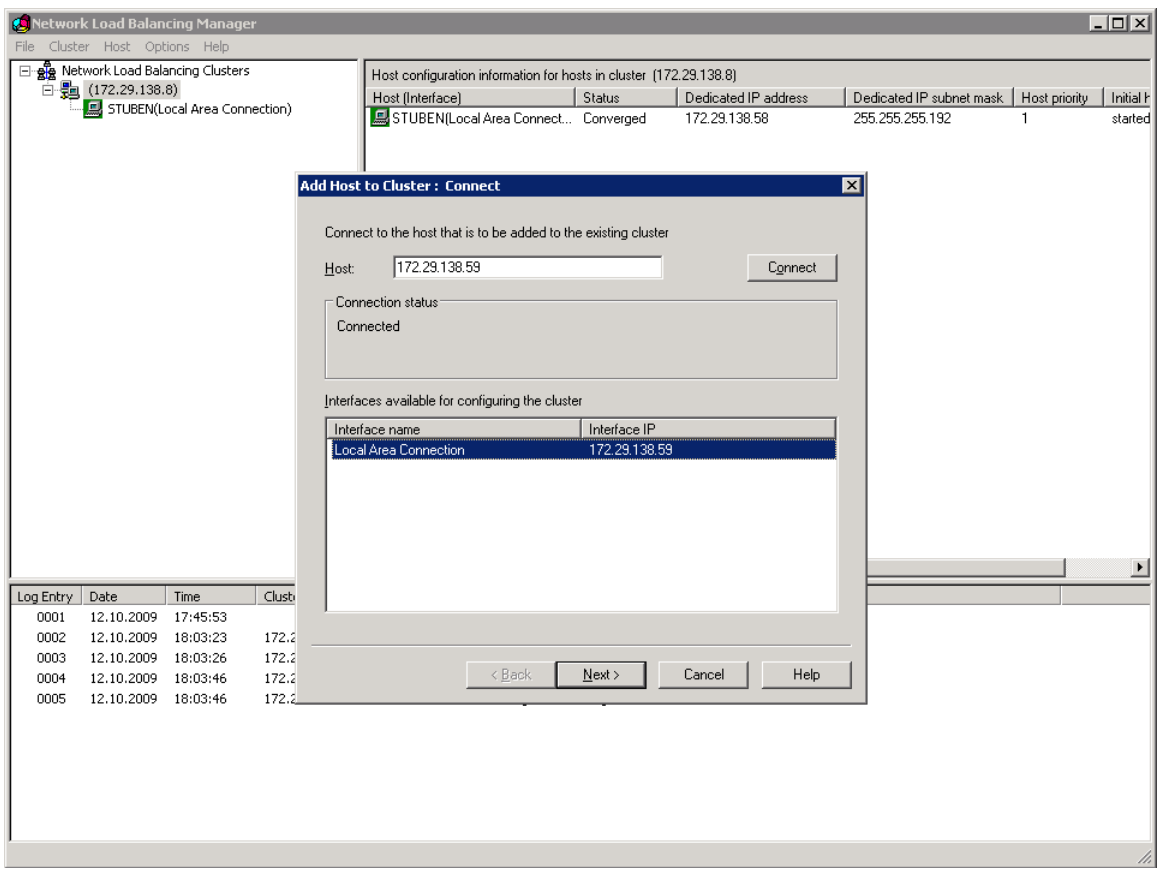
11. Geben Sie die Regeln für die restlichen Ports an, wie in Schritt 9 und 10 beschrieben. Im Folgenden sind die für den DLS elementaren Ports aufgelistet (eine vollständige Liste aller DLS-Ports finden Sie in der Sicherheitscheckliste des Planungshandbuchs):

    - 10443: Empfängt Daten von der grafischen Benutzeroberfläche, also vom Web-Browser, wenn HTTPS benutzt wird.
    - 10444: Empfängt Daten über HTTPS von der DlsAPI, dem Web Service-Interface des DLS.
    - 18080: Empfängt Daten von der grafischen Benutzeroberfläche, also vom Browser, wenn HTTP benutzt wird.
    - 18443: Empfängt Daten von den Endgeräten (HTTP und HTTPS).
    - 18444: Empfängt Daten von den Endgeräten bei sicherer Verbindung zwischen DLS und Endgerät (Secure Modus).

12. Wenn Sie alle Port-Regeln eingetragen haben, klicken Sie **Finish**.



13. Sie gelangen wieder in das Hauptfenster des Network Load Balancing Manager, wo der Cluster in seiner aktuellen Zusammensetzung angezeigt wird. Wenn das Einfügen des Knotenrechners erfolgreich war, ist der **Status** auf **Converged** gesetzt. Gehen Sie auf **Add Host** im Menü **Cluster** oder rufen Sie mit der rechten Maustaste das Kontextmenü auf und gehen auf **Add Host to Cluster**, um einen weiteren Knotenrechner hinzuzufügen.



14. Gehen Sie für den zweiten und ggf. alle weiteren Knotenrechner ebenso vor wie beim ersten Knotenrechner.

4.3.3 Network Load Balancer für Windows Server 2008 R2

Die in Abschnitt 4.3.2 durchgeführten Konfigurationsschritte gelten analog für Windows Server 2008 R2.

4.3.4 Network Konfiguration für Windows NLB

Allgemeine Information stehen zur Verfügung unter:
http://www.microsoftnow.com/2007/09/frequently-asked-questions-on-windows.html

Dieser Abschnitt beschreibt diejenigen Punkte, die besonders berücksichtigt werden müssen.

4.3.4.1 Wie sind Layer 2-Switche für die Zusammenarbeit mit Windows NLB einzurichten?

Stellen sie sicher, dass der Switch nicht die Cluster-MAC-Adresse mit einem konkreten Switch Port verbindet.

4.3.4.2 Wie sind Layer 3-Switche für die Zusammenarbeit mit Windows NLB einzurichten?

Layer 3-Switche müssen speziell für die Zusammenarbeit mit Windows NLB eingerichtet werden. Für die Hosts im Cluster muss ein VLAN eingerichtet werden; dieses VLAN muss im Layer 2-Modus arbeiten.

4.3.4.3 Was ist wegen der Fragmentierung der IP-Pakete zu tun?

Windows NLB hat Probleme bei der Verarbeitung von fragmentierten IP-Paketen; deshalb muss die Paketffragmentierung vermieden werden.

Besonders in dem Fall, dass Teile der Verbindung zwischen IP Phones und DLS über VPN-Kanäle führen, kann es zur Fragmentierung kommen. Dies kann vermieden werden, indem Raum für zusätzliche Bytes im VPN-Kanal geschaffen wird. Hierzu muss der TCP-Parameter „MSS“ (Maximum Segment Size; maximum TCP payload) auf einen Wert unterhalb des TCP-Maximums von 1460 gesetzt werden. Wird Cisco® -Zubehör verwendet, sollte das Merkmal „MSS adjust“ gesetzt werden. Beispiel: **ip tcp adjust-mss 1300**

4.4 DCMP einrichten

Um den DCMP (DLS-Contact-Me-Proxy) einzurichten, gehen Sie in den folgenden Schritten vor:

- DCMP installieren
- DCMP konfigurieren
- DLS für DCMP konfigurieren
- Telefon für DCMP konfigurieren
- DCMP testen

4.4.1 DCMP installieren

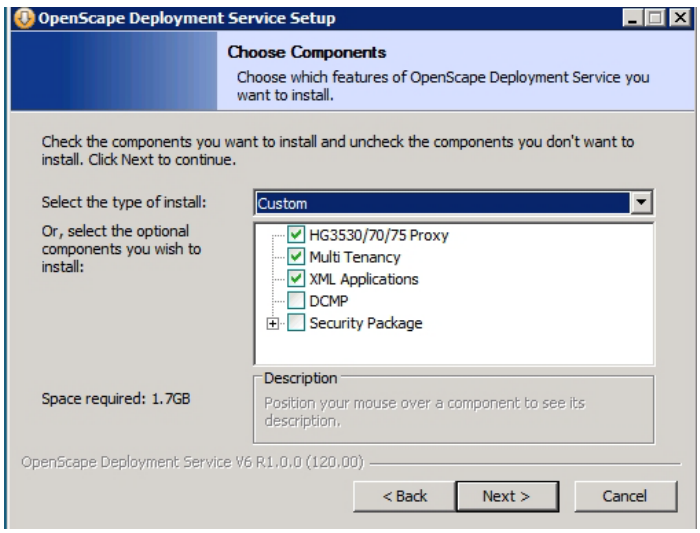
Stellen Sie zunächst sicher, dass der DCMP nicht bereits installiert ist. Hierzu gehen Sie mit einem Web-Browser auf
http://<IP Adresse des DLS-Rechners>:18080/dcmp. Falls Sie eine Fehlermeldung erhalten, müssen Sie den DCMP installieren. Der DCMP kann sowohl auf dem DLS-Rechner installiert werden als auch auf einem weiteren Rechner.

Gehen Sie im Installationsmedium in das Verzeichnis **dcmp** und starten den **dcmp-installer** mit einem Doppelklick.

> ***WICHTIG:*** Führen Sie die Datei „**dcmp-installer.exe**“ nicht auf einem Computer aus, auf dem der DLS bereits läuft. Der DCMP-Installer selbst fordert Sie hierzu auf und sollte daher vermieden werden.

4.4.1.1 Installation auf dem DLS-Rechner

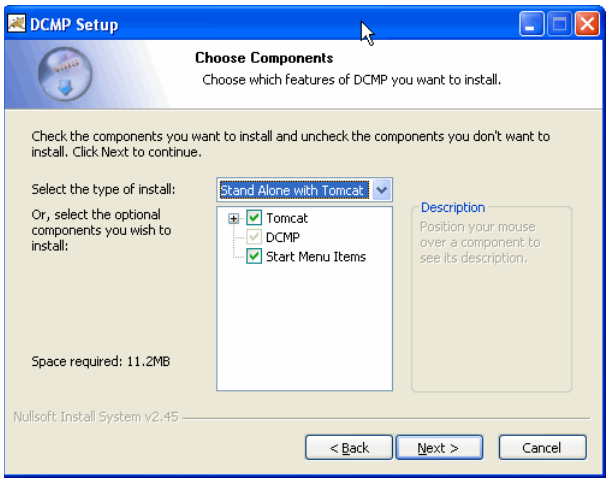
Wenn Sie DCMP und DLS auf demselben Rechner installieren wollen, wählen Sie die Option **DCMP**.



Folgen Sie den Anweisungen zur Installation.

4.4.1.2 Installation auf einem anderen Rechner

Für die Installation auf einem anderen Rechner wählen Sie die Optionen **DCMP** und **Service Startup**.

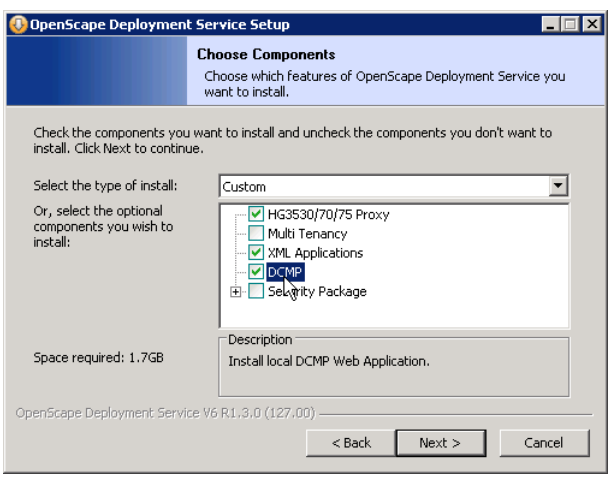


Während der Installation werden Sie nach dem Passwort für den DCMP gefragt.

4.4.1.3 Installation in einer Multi-Node-Umgebung

Bei einer Multi-Node-Umgebung mit 4 Knoten (maximal unterstützte Anzahl, siehe Abschnitt 4.1.5, “Infrastruktur bei Cluster-Betrieb”) ohne DCMP fahren Sie mit den folgenden Schritten fort:

1. Starten Sie den DLS-Installer über Knoten 1. DCMP kann im Laufe der Installation hinzugefügt werden, indem Sie die Option DCMP auswählen. Dadurch wird die Konfigurationsdatei für die Installation aktualisiert. Führen Sie eine DLS-„Upgrade“-Installation auf die selbe DLS-Load durch, die bereits auf einem System installiert ist; die zu installierenden Zusatzmodule werden Ihnen dann zur Auswahl angeboten.



2. Simulieren Sie ein DLS-Upgrade über Knoten 2, 3 und 4, damit die aktualisierte Installations-Konfigurationsdatei auf Knoten 1 erkannt wird und DCMP anschließend transparent über die verbleibenden Knoten installiert werden kann.

   HINWEIS: Sie müssen den Installer auf dem zweiten (und allen weiteren) Knoten erneut ausführen, um DCMP auch dort zu installieren. Dies ist nötig, da der Installer für die restlichen Knoten die aktualisierte Installations-Konfigurationsdatei in den allgemeinen Daten der jeweiligen Umgebung (die auf dem ersten Knoten liegen) zuerst „triggern“ muss, um DCMP transparent auf den restlichen Knoten installieren zu können.

3. Rufen Sie **http://<IP-Adresse>:18080/dcmp** auf, um sich am DCMP-Server anzumelden. Fahren Sie ggf. mit der DCMP-Cluster-Konfiguration fort (siehe Abschnitt 4.4.2, “DCMP konfigurieren”) und stellen Sie über die virtuelle IP-Adresse des DLS-Clusters eine Verbindung zum DCMP her. Fahren Sie ggf. mit der DCMP-Cluster-Konfiguration fort (und folgen Sie den Prompts der DLS-Benutzeroberfläche).

   Wenn der DCMP-Server bereit ist, kann der DLS für den DCMP-Betrieb konfiguriert werden.

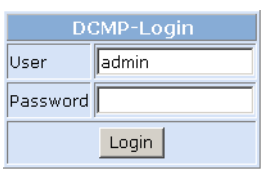
4. Unter **Administration** > **Workpoint Interface Konfiguration** > **Register „DCMP“** klicken Sie auf den Button **DCMP umschalten**, um den DCMP zu aktivieren. Eine Meldung weist darauf hin, dass die Verbindung zum DCMP-Server erfolgreich hergestellt wurde. (Siehe Abschnitt 4.4.3, “DLS für DCMP konfigurieren”)

5. Um zu überprüfen, dass der Job läuft, sehen Sie in **Job Koordination** > **Job Kontrolle** nach und klicken Sie die Aktionsschaltfläche **Suchen**. Dann klicken Sie auf den gesuchten Eintrag und wählen Sie die Ansicht „Objekt“. Im **Register „Basis Daten“** sehen Sie, dass der Job über DCMP gehandhabt wird.

6. Gehen Sie zu **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „DCMP“**. Der Schalter **DCMP aktiv** sollte markiert sein, und die Einstellungen sollten dieselben sein wie sie für diese IP-Adresse in **Administration** > **Workpoint Interface Konfiguration** > **Register „DCMP“** gemacht wurden.

4.4.2 DCMP konfigurieren

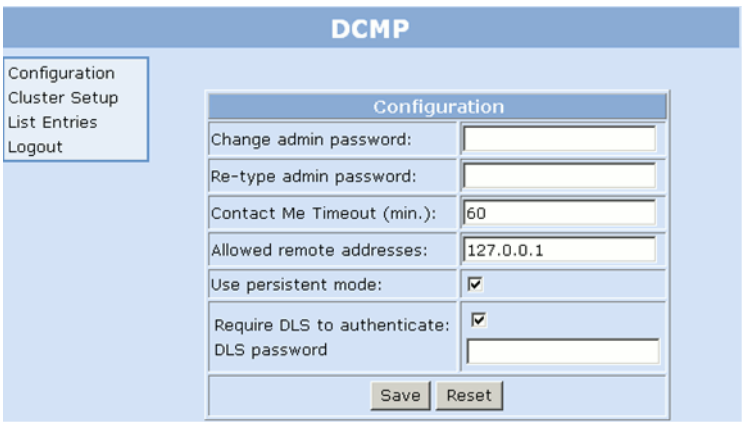
1. Gehen Sie mit einem Web-Browser auf **http://<IP Address>:18080/dcmp**, um sich am DCMP-Server anzumelden. Der Benutzername ist **admin**. Das Passwort ist identisch mit dem Admin-Passwort für den DLS, wenn der DCMP zusammen mit dem DLS installiert wurde. Falls der DCMP nachträglich installiert wurde, lautet das voreingestellte Passwort **Asd123!.**. Dies sollte nach der Installation geändert werden. Falls der DCMP auf einem eigenen Server installiert wurde, geben Sie das Passwort ein, das sie bei der Installation vergeben hatten.



2. Nach der Anmeldung öffnet sich das erste Konfigurationsfenster. Mit **Change admin password** und **Re-type admin password** können Sie das Passwort ändern, wenn gewünscht.

   Im Feld **Allowed remote addresses** geben Sie die Adressen der DLS-Server als kommaseparierte Liste ein, oder als einzelne Adresse, wenn es nur einen DLS-Server gibt. Wenn der DCMP auf dem DLS-Rechner installiert ist, so ist der Wert 127.0.0.1.

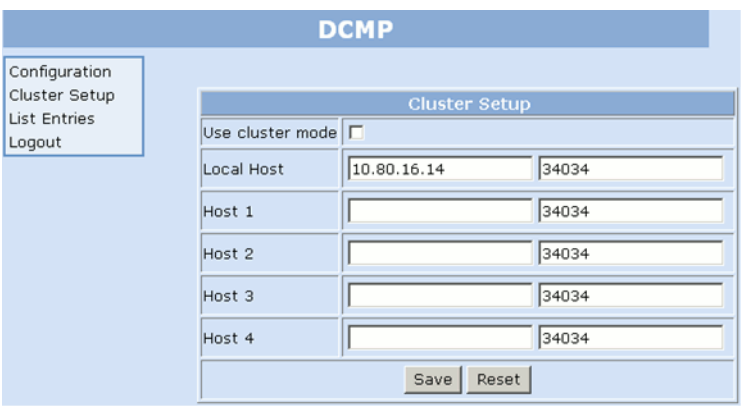
   Wenn **Require DLS to authenticate** aktiviert ist, muss der DLS sich authentifizieren, um mit dem DCMP zu kommunizieren. Im Feld **DLS password** muss das Passwort des DLS eingegeben werden, wenn diese Option genutzt wird.



3. Im Fenster **Cluster Setup** überprüfen bzw. konfigurieren Sie die korrekten Adressen und Ports für einen oder mehrere DLS-Rechner. Soll ein DLS-Cluster verwendet werden, aktivieren Sie **Use cluster mode**.

   Das Feld **Local Host** enthält die IP-Adresse des DCMP-Servers.

   Wenn der DLS als Cluster betrieben wird, müssen die IP-Adressen sämtlicher DLS-Rechner in **Host 1 ... 4** eingegeben werden.

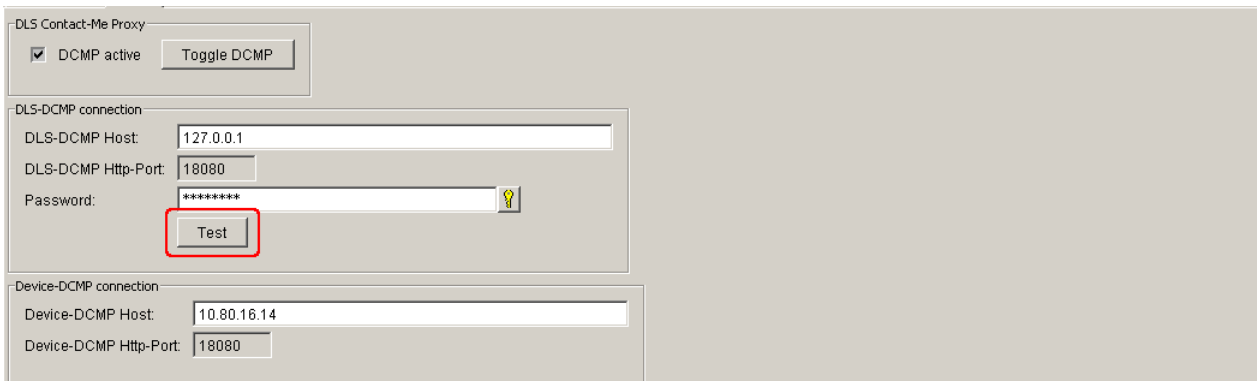


   Im Fenster **List Entries** können Sie alle Contact-Me-Nachrichten des DLS ansehen.

4.4.3 DLS für DCMP konfigurieren

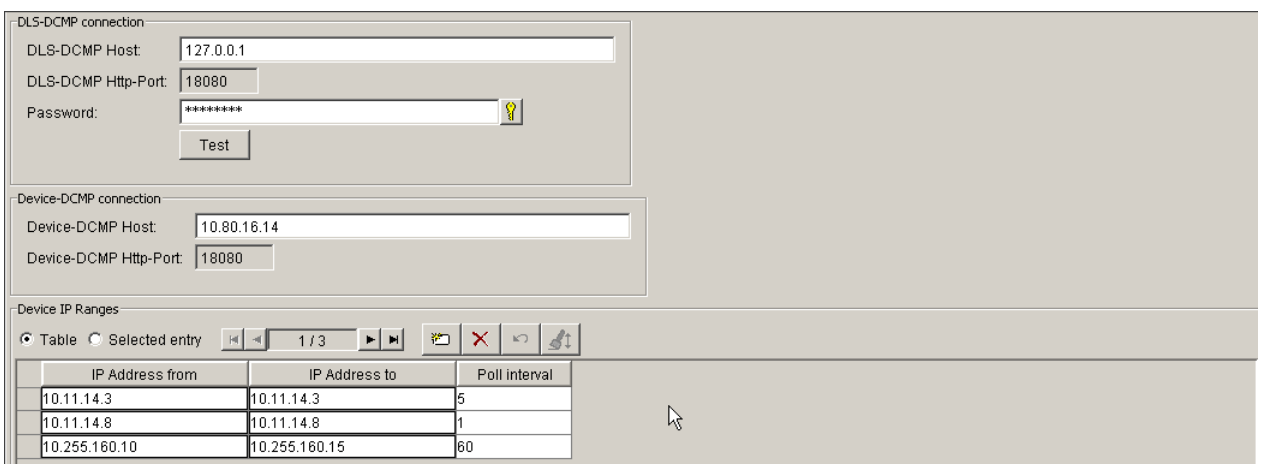
Wenn der DCMP-Server bereit ist, kann der DLS für den DCMP-Betrieb konfiguriert werden.

1. Unter **Administration** > **Workpoint Interface Konfiguration** > **Register „DCMP“** klicken Sie auf den Button **DCMP umschalten**, um den DCMP zu aktivieren.
2. Wenn der DCMP auf dem DLS-Recher läuft, wird die IP-Adresse des DCMP-Servers in **DLS-DCMP Host** angezeigt; andernfalls muss sie hier eingegeben werden.
3. Wenn Sie die Option **Require DLS to authenticate** in der DCMP-Konfiguration aktiviert haben (siehe Abschnitt 4.4.2, “DCMP konfigurieren”), müsen Sie im Feld **Passwort** das zuvor in der DCMP-Konfiguration definierte **DLS password** eingeben.
4. Um die Kommunikation zwischen DLS und DCMP zu testen, klicken Sie auf den Button **Test**.



Für Testzwecke kann ein sehr kurzes **Poll Intervall** gewählt werden; im Live-Betrieb sind längere Intervalle empfohlen.

5. Definieren Sie einen oder mehrere Device **IP Bereiche**. Jedes IP Device innerhalb der IP-Bereiche, die durch I**P Adresse von** und **IP Adresse bis** definiert sind, wird über den DCMP aktualisiert. Somit sendet der DLS immer dann, wenn eine Änderung an einem Telefon innerhalb einer der aufgelisteten IP-Bereiche vorgenommen wird, eine Nachricht an den DCMP mit der Aufforderung, den Contact-Me-Eintrag für dieses Telefon zu setzen.

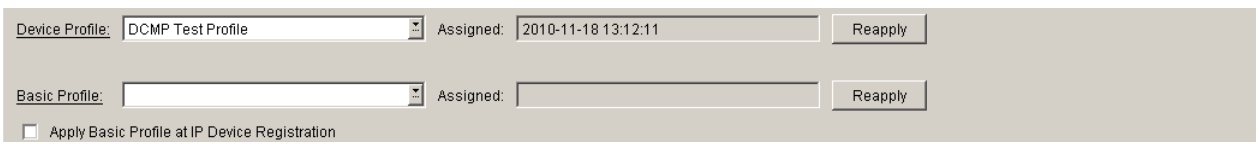


4.4.4 Telefon für DCMP konfigurieren

1. Das Telefon sollte so konfiguriert werden, dass es passive FTP-Transfer verwendet, damit es Software und andere Daten auch dann herunterladen kann, wenn es sich hinter einer NAT-Firewall befindet. Dies geschieht in **IP Devices** > **IP Phone Konfiguration** > **Sonstiges** > **Register „FTP Server“**. Da dieses Flag in einem bereits eingerichteten Gerät nicht geändert werden kann, empfiehlt es sich, ein Template für „DCMP Sonstiges“ zu erstellen und dieses Template im Profil für DCMP-Benutzer zu verwenden.

2. Gehen Sie zu **Profil Management** > **Geräteprofil** und erzeugen Sie ein Geräteprofil, in dem das neu erstellte „DCMP Sonstiges“-Template verwendet wird.

3. Gehen Sie zu **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration**. Verwenden Sie die Funktion **Suchen**, die Ansicht „Tabelle“ und die Ansicht „Objekt“, um die Rufnummer für das zu konfigurierende Telefon auszuwählen. Im **Register „Profil“** wählen Sie das zuvor erzeugte Profil und weisen es dem Telefon zu.



4.4.4.1 Home-User-Geräte für DLS / DCMP konfigurieren

DCMP wurde für Fälle entwickelt, in denen der DLS nicht mit Endgeräten kommunizieren kann.

Wenn der DLS mit Home/Office-User-Endgeräten kommuniziert, kann der DLS die IP-Adresse des Endgeräts sehen; diese IP-Adresse ist aber die dem Modem/Router des Benutzers zugewiesene öffentliche IP-Adresse. Wenn der DLS versucht, eine Konfigurationsänderung an diese IP-Adresse zu übermitteln, wird diese Änderung nie an das Gerät hinter dem Modem/Router übergeben, aber genau dort wird DHCP verwendet. Wenn DCMP aktiv ist und der IP-Bereich in die DCMP-Konfiguration aufgenommen wurde, gehen die in diesem IP-Bereich enthaltenen Telefone in den DCMP-Modus über.

1. Der DLS fordert eine Konfigurationsänderung von einem Telefon an, das sich im DCMP-Modus befindet
2. Diese Anforderung geht nicht direkt zum Gerät sondern zum DCMP.
3. Das Gerät kontaktiert den DCMP in konfigurierten Intervallen und wird darüber informiert, dass der DLS Änderungen für dieses Gerät hat.
4. Das Gerät nimmt Kontakt zum DLS auf, um die verfügbaren Änderungen anzufordern.

Um Home-User-Geräte verwalten zu können, muss der Rechner, der für den DLS und den DCMP verwendet wird, mit zwei Netzwerkschnittstellen ausgestattet sein. Einer der beiden wird die interne und der anderen die externe IP-Adresse zugewiesen. Hierzu werden zunächst zwei IP-Adressen eingerichtet: eine interne für Geräte im Intranet (172.x.x.x) und eine externe, bei der nur die benötigten Ports in der Firewall geöffnet werden.

In der Firewall werden folgende Ports geöffnet: der DLS-Port 18443, den Geräte standardmäßig verwenden, um mit DLS zu kommunizieren und der FTP-Port 21, der für Geräte-Firmware-Upgrades genutzt wird. (Die Kommunikation zwischen dem DLS-Server und dem DLS-Client erfolgt über Port 18080).

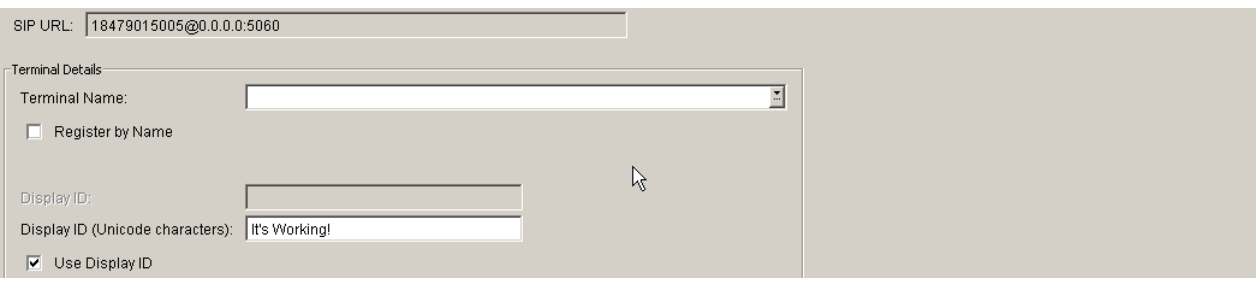
Bei der Konfiguration gilt folgende Reihenfolge:

- DCMP auf demselben Server wie den DLS installieren
- Die Konfiguration wie in der DLS-Dokumentation (Abschnitt 4.4, „Telefon für DCMP konfigurieren“) beschrieben abschließen
- Konfiguration der Netzwerk-Firewall für die benötigten Ports 18443, 18080 und 21 durchführen.

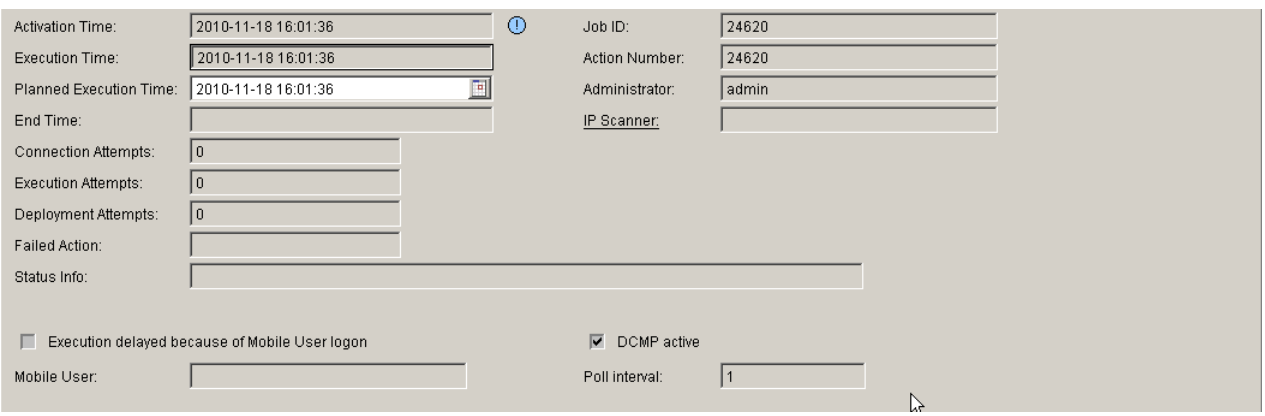
4.4.5 DCMP testen

1. Zunächst wählen Sie ein Telefon aus, dessen IP-Adresse sich innerhalb eines für DCMP konfigurierten IP-Bereichs befindet (siehe Abschnitt 4.4.3, “DLS für DCMP konfigurieren”) und führen Sie einen Factory Reset (Zurücksetzen auf Werkseinstellungen) durch.
2. Wenn das Telefon neu gestartet ist, geben Sie ihm die Rufnummer, der Sie zuvor das DCMP-Profil zugewiesen haben.
3. Gehen Sie auf **IP Devices**> **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „DCMP“**. Der Schalter **DCMP aktiv** sollte markiert sein, und die Einstellungen sollten dieselben sein wie sie für diese IP-Adresse in **Administration** > **Workpoint Interface Konfiguration** > **Register „DCMP“** gemacht wurden.

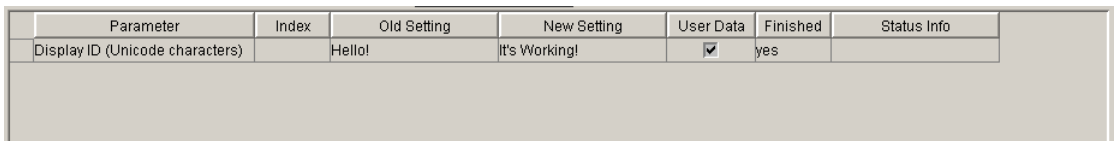
4. Um eine Konfigurationsänderung zu testen, ändern Sie den Display-Namen des Telefons. Gehen Sie zu **IP Devices** > **IP Phone Konfiguration** > **Gateway / Server** > **Register „SIP Terminaleinstellungen“**. Aktivieren Sie **Verwende Display ID** (oderr **Verwende Display ID (Unicode Zeichen)**), setzen Sie die **Display ID** beispielsweise auf „It’s Working!“. Speichern Sie die Änderungen im DLS.



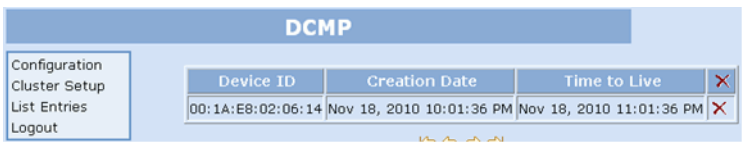
5. Um zu überprüfen, dass der Job läuft, sehen Sie in **Job Koordination** > **Job Kontrolle** nach und klicken Sie die Aktionsschaltfläche **Suchen**. Dann klicken Sie auf den gesuchten Eintrag und wählen Sie die Ansicht „Objekt“. Im **Register „Basis Daten“** sehen Sie, dass der Job über DCMP gehandhabt wird.



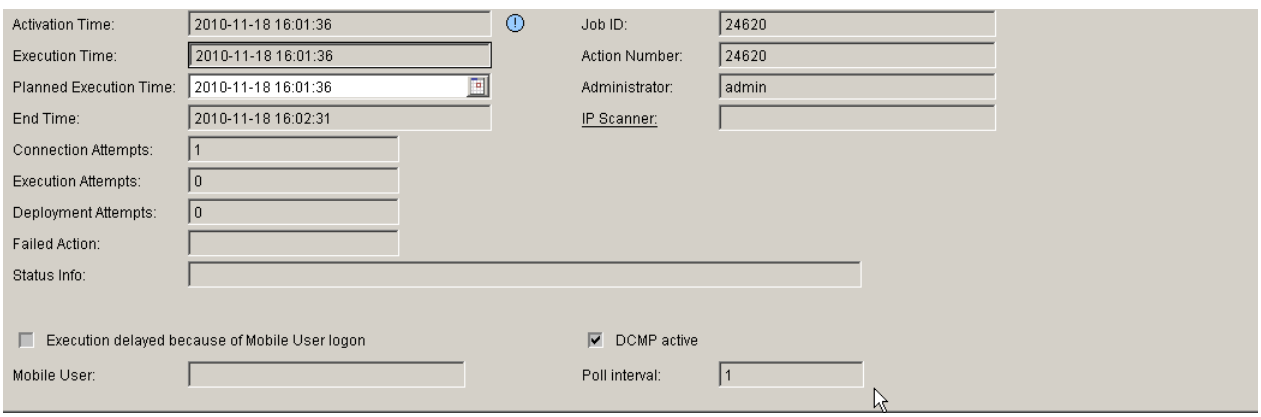
6. Im **Register „Konfiguration Daten“** sehen Sie die konkrete Änderung sehen, die angefordert wurde.



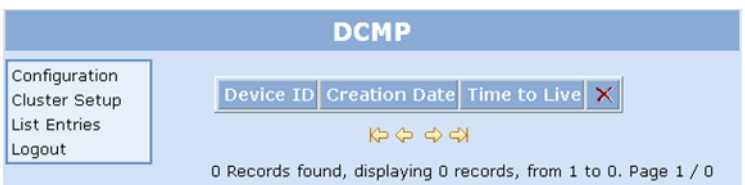
7. Auf der DCMP-Benutzeroberfläche klicken Sie auf das Menü **List Entries**. Sie sollten die Contact Me-Einstellung auf der Liste sehen. Die **Device ID** sollte die MAC-Adresse des Telefons sein.



8. Auf der DLS-Benutzeroberfläche sehen Sie unter **Job Koordination** > **Job Kontrolle** > **Register „Basis Daten“** eine „Endzeit“, sobald die Änderung durchgeführt worden ist.



9. Auf der DCMP-Benutzeroberfläche sehen Sie, dass der Contact Me-Eintrag entfernt wurde.



Der Test ist beendet.

4.5 Installation des DLS

4.5.1 Single Node-Betrieb mit lokaler Datenbank

Dies ist die Standard-Installation des DLS. Folgen Sie dabei den Anweisungen des Installationsassistenten. Bei Installation von DLS V7 wird als Standard-Datenbank MS SQL 2008 R2 verwendet. Hierfür müssen die folgenden Voraussetzungen erfüllt sein:

- Microsoft SQL Server 2008 R2 Express
- Microsoft .NET v3.51
- Microsoft Windows Installer 4.5

HINWEIS: Der Microsoft Windows Installer 4.5 ist bereits auf dem Microsoft SQL Server 2008 R2 installiert.

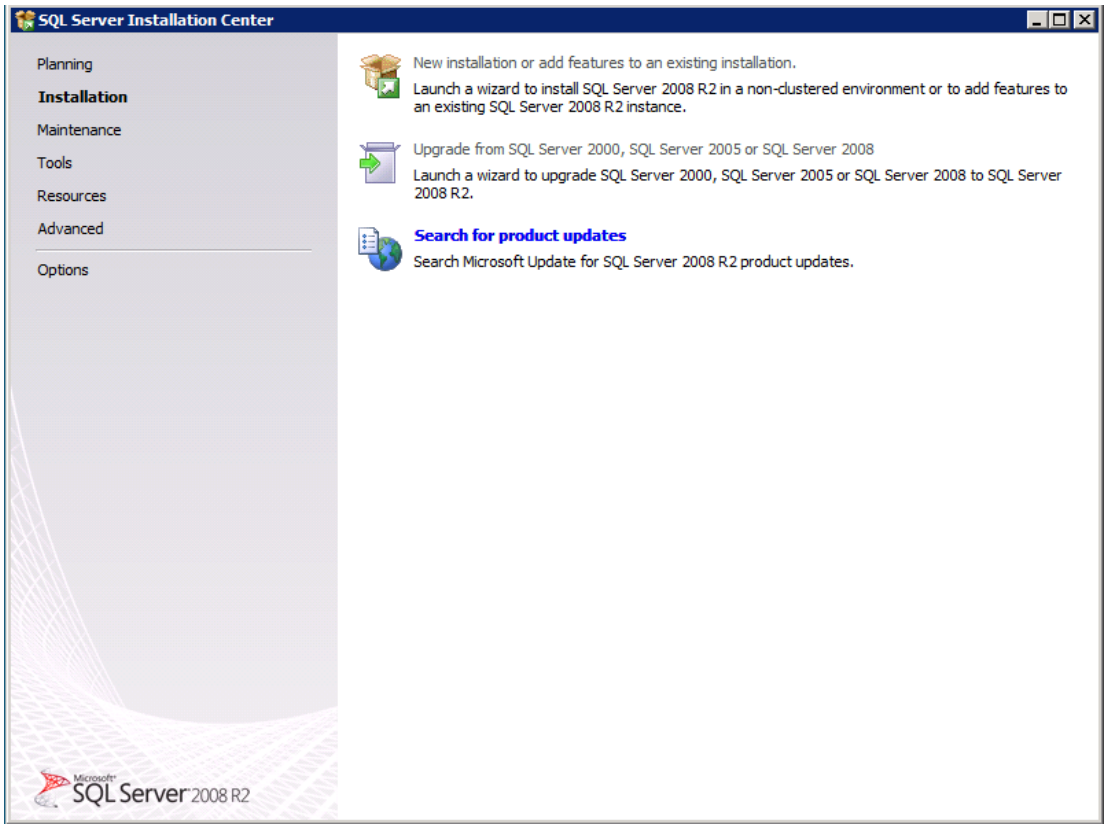
HINWEIS: Die neueste aktuell verfügbare Version von Microsoft SQL Server 2008 R2 (Service Pack 2) finden Sie hier:
http://www.microsoft.com/en-us/download/details.aspx?id=30437

4.5.1.1 Installation von SQL Server 2008 R2 Express Edition

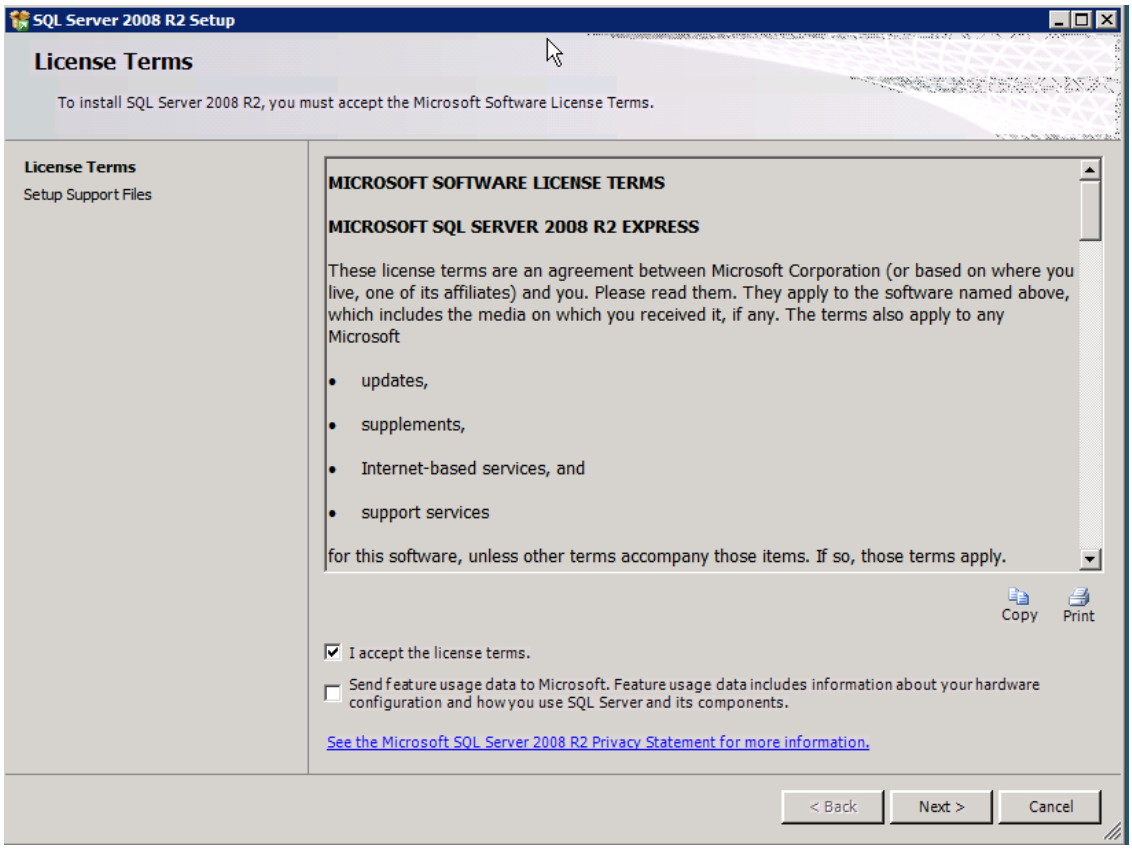
Es gibt zwei Möglichkeiten, um das Installationsprogramm für SQL Server 2008 R2 Express aufzurufen:

- **Manuelle Installation**

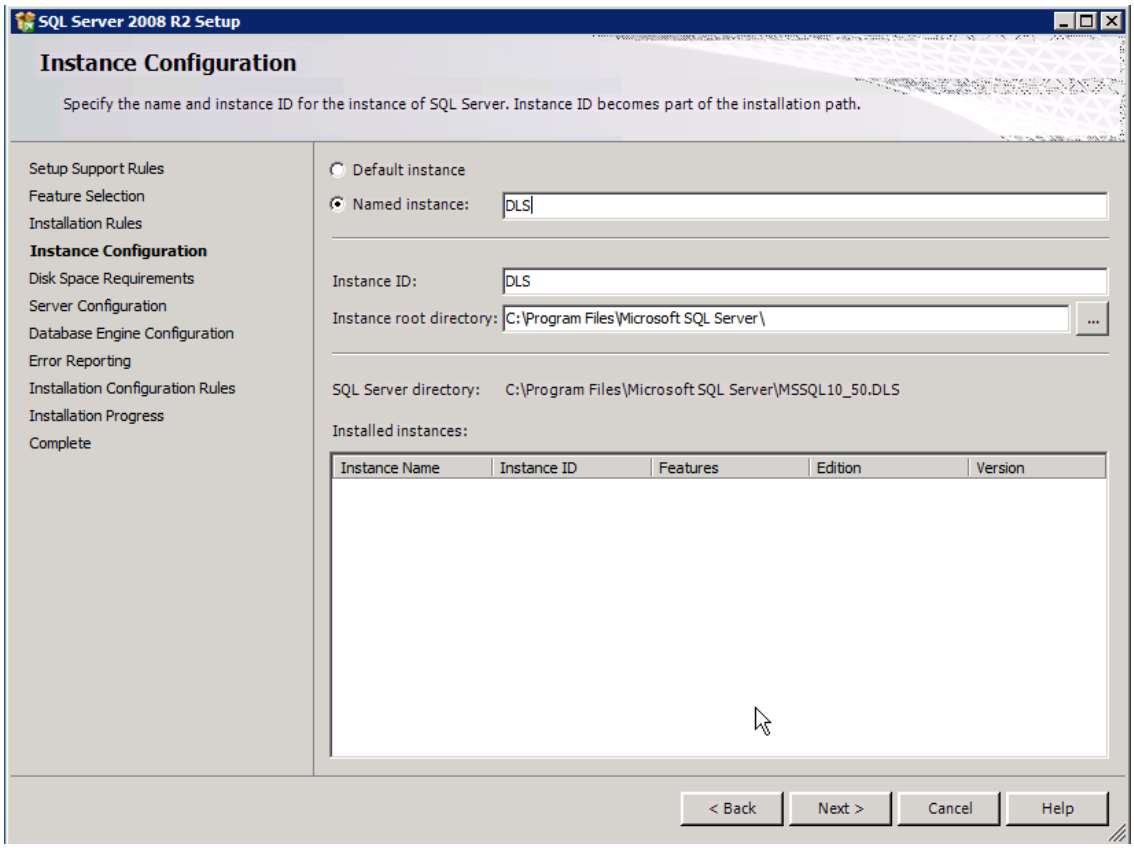
  1. Gehen Sie zur entsprechenden Microsoft-Webseite (http://www.microsoft.com/en-us/download/details.aspx?id=30438)
     und klicken Sie auf **Download**. Ein Popup-Fenster erscheint mit der Frage, ob Sie die Installation direkt ausführen möchten oder ob Sie sie auf Ihrem Computer speichern möchten. Klicken Sie auf **Run** (Ausführen).
  2. Das SQL Server-Installationscenter wird aufgerufen. Klicken Sie zunächst links im Menü auf **Installation** und dann oben im Bildschirm auf **New SQL Server stand-alone installation**, um den Installations-Assistenten zu starten.



3. Die Installationsroutine überprüft, ob Ihr Computer die erforderlichen Hardware- und Softwareanforderungen erfüllt, und in der Lage ist, Studio Express auszuführen. Wenn eine dieser Überprüfungen fehlschlägt, müssen Sie den Fehler beheben und dann auf **Re-run** (Erneut ausführen) klicken. Wenn die Überprüfungen erfolgreich waren, klicken Sie auf **OK**, um fortzufahren.
4. Klicken Sie auf **Next**.
5. Lesen Sie die Lizenzbedingungen (End User License Agreement, EULA). Markieren Sie das Kontrollkästchen „I accept the license terms“, um die Lizenzbedingungen zu akzeptieren und klicken Sie auf **Next.**

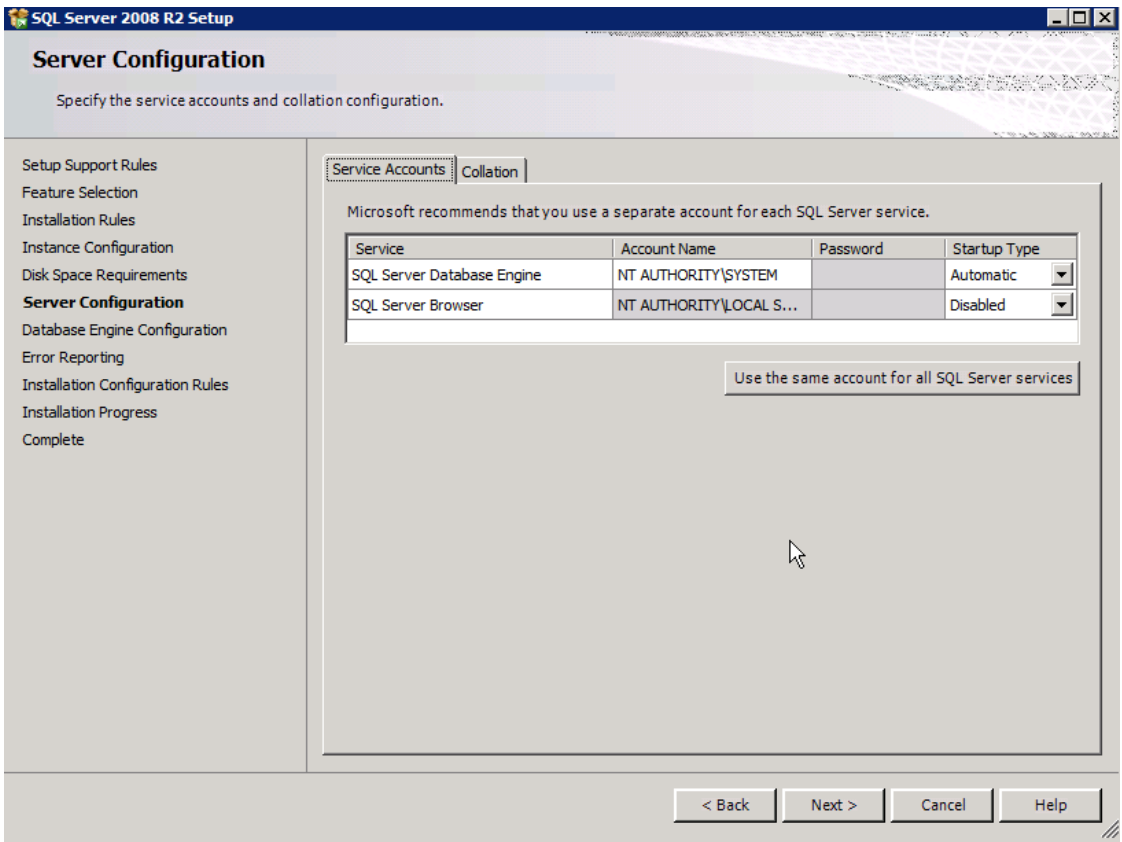


6. Installieren Sie die Setup-Unterstützungsdateien und führen sie die notwendigen Einstellungen durch. Klicken Sie auf **Install**, um die Installation zu starten.
7. Überprüfen Sie den Instanznamen.



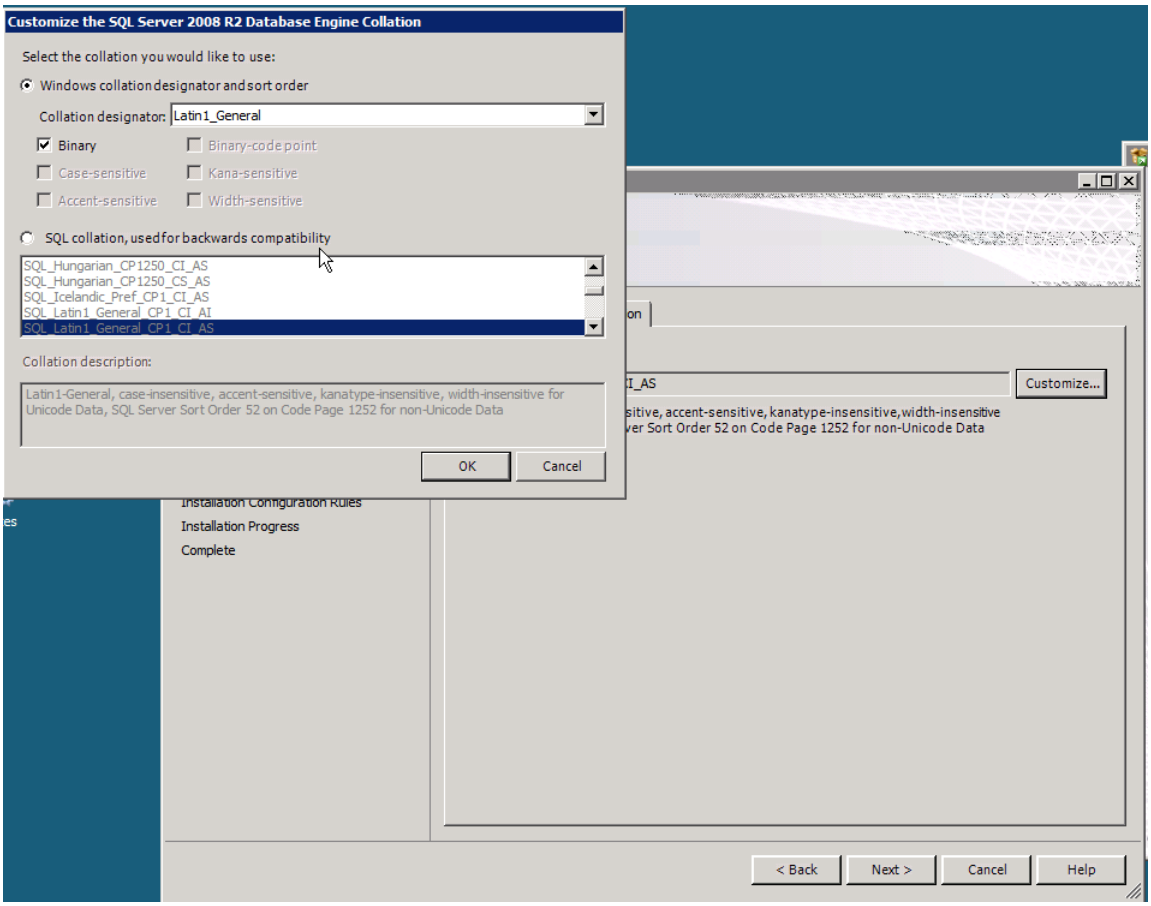
HINWEIS: Der Name der Instanz-ID (Instance ID) muss „DLS“ lauten.

8. Überprüfen Sie die Credentials, die für die zu erstellenden Dienste verwendet werden.



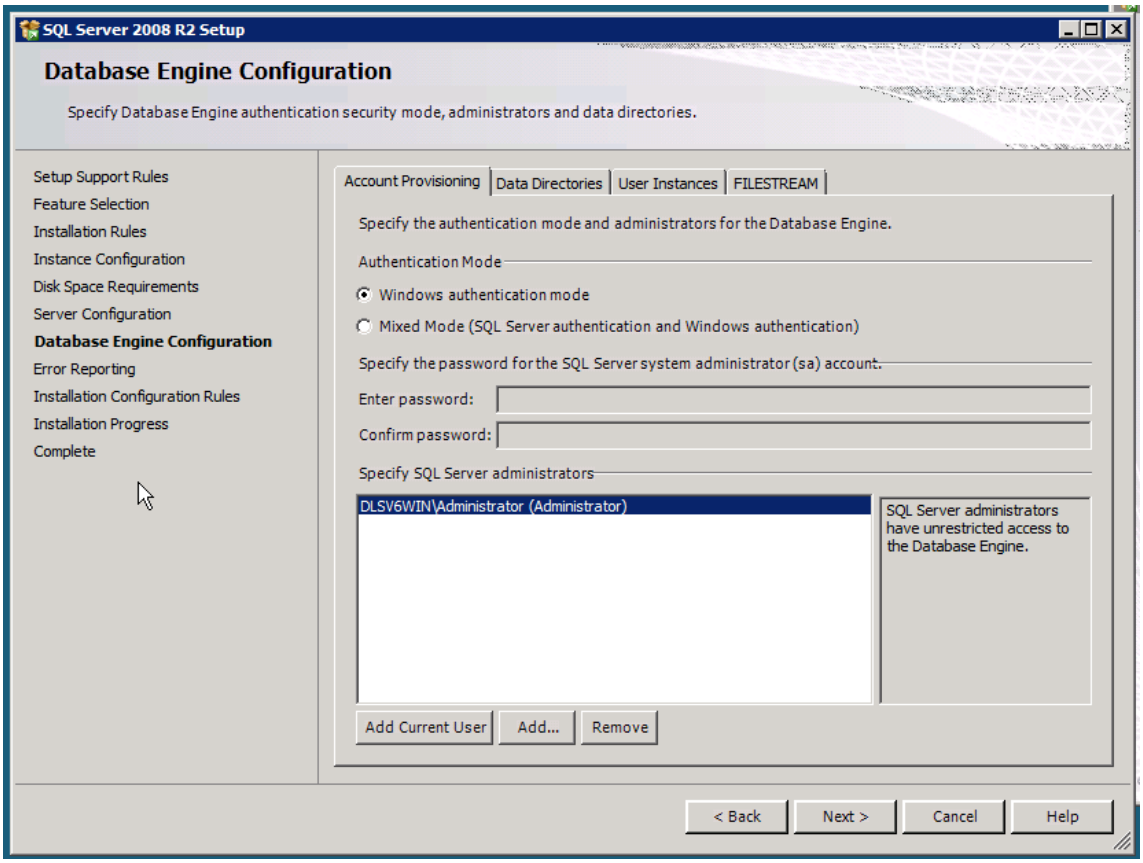
HINWEIS: Der Accountname muss NT_AUTHORITY\SYSTEM lauten.

9. Passen Sie die Sortierreihenfolge (Collation) für das SQL Server-Datenbankmodul an.

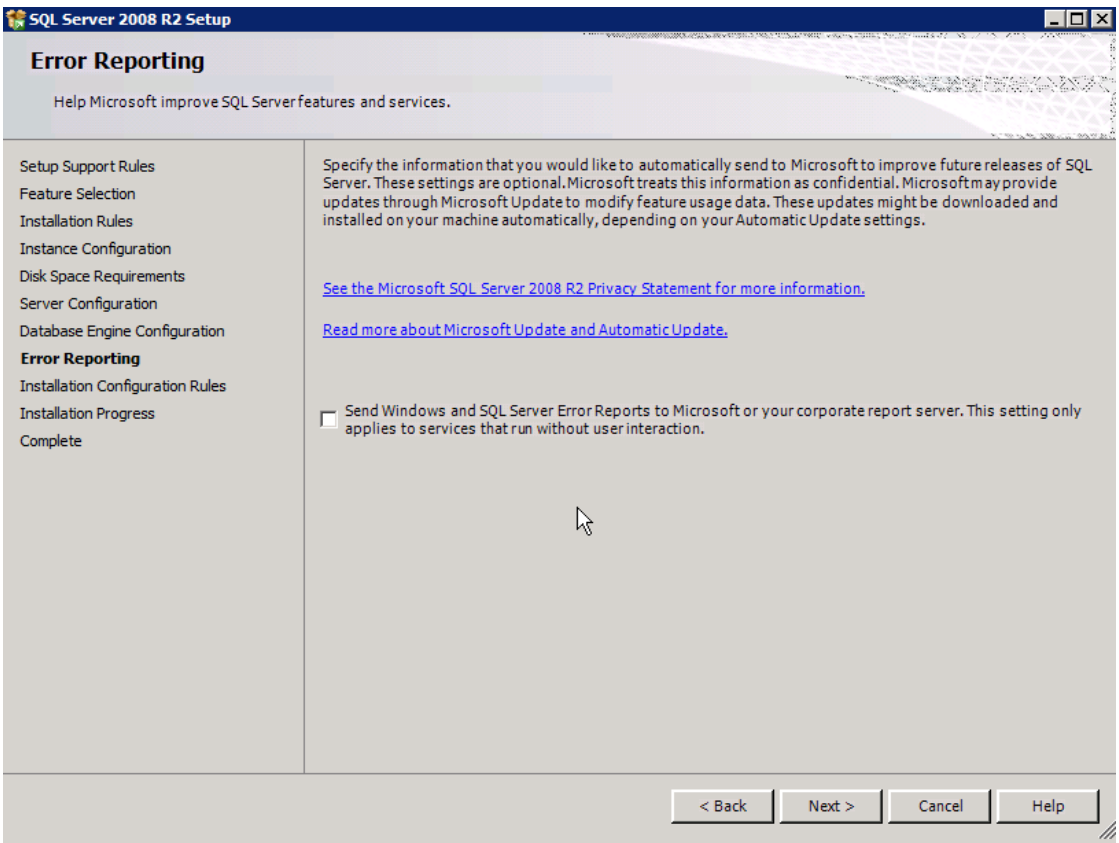


HINWEIS: Im Feld Sortierungskennzeichner (Collation designator) tragen Sie die Zeichenfolge „Latin1_General“ ein.

10. Überprüfen Sie die Einstellungen für den Authentifizierungsmodus (Authentication Mode) und die Administratoren, die zum Datenbankmodul hinzugefügt werden.



11. Überprüfen Sie die Einstellungen für die Fehlerberichterstattung (Error Reporting).

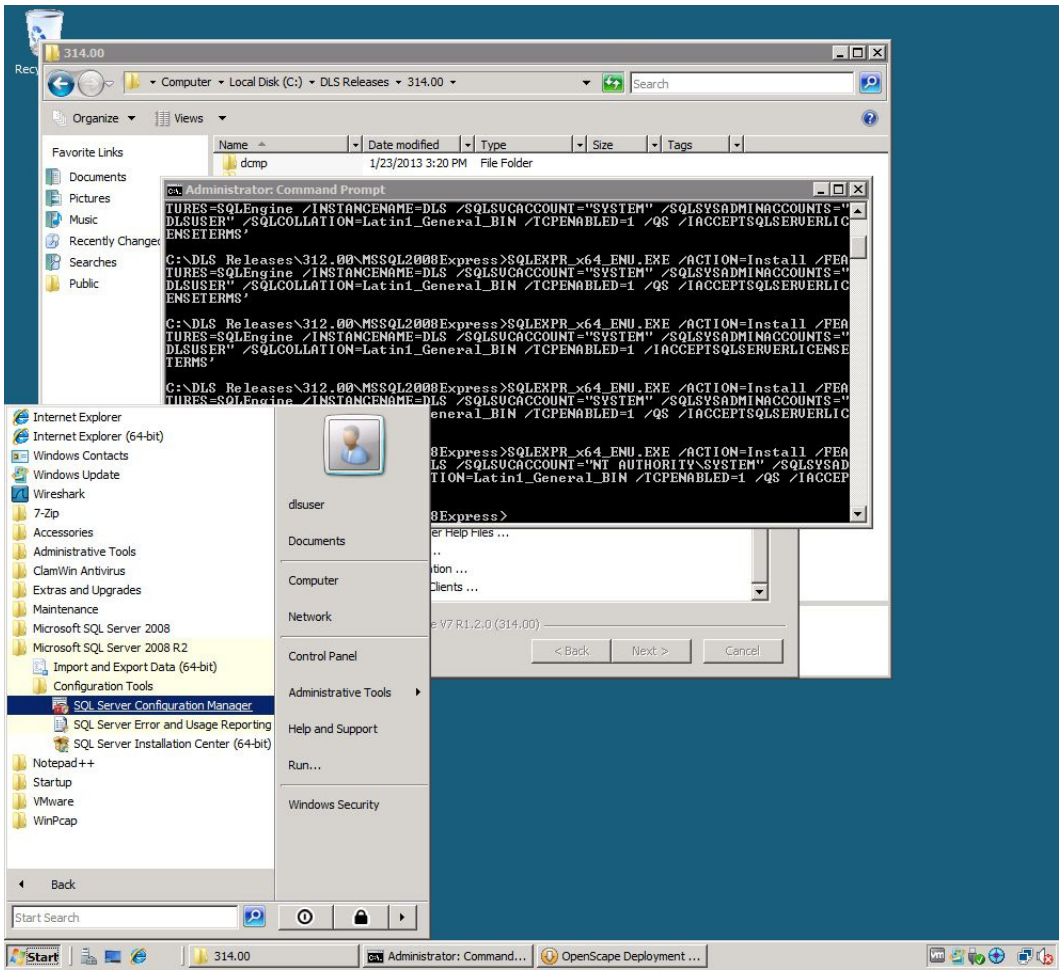


12. Klicken Sie nach Abschluss der Installationsroutine auf **Close**, um das Setup von SQL Server 2008 R2 Express Edition zu beenden.

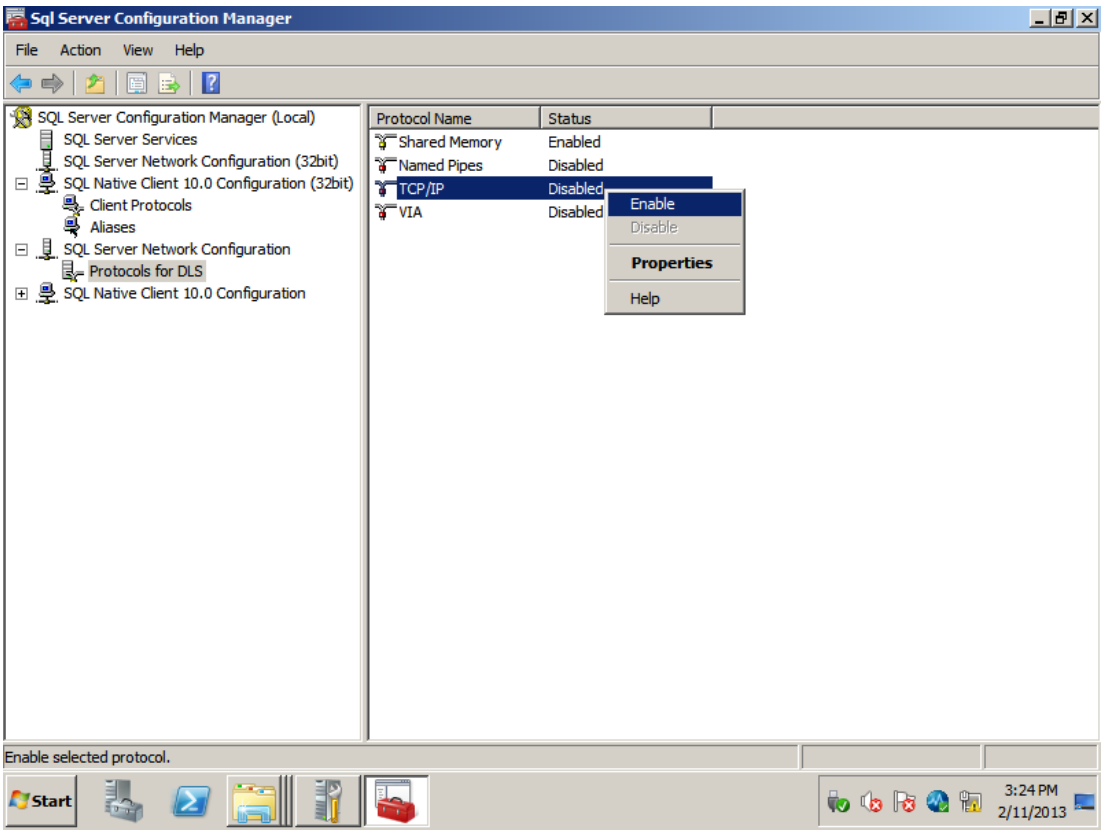
13. Aktivieren Sie für SQL Server Express die Kommunikation über TCP/IP.

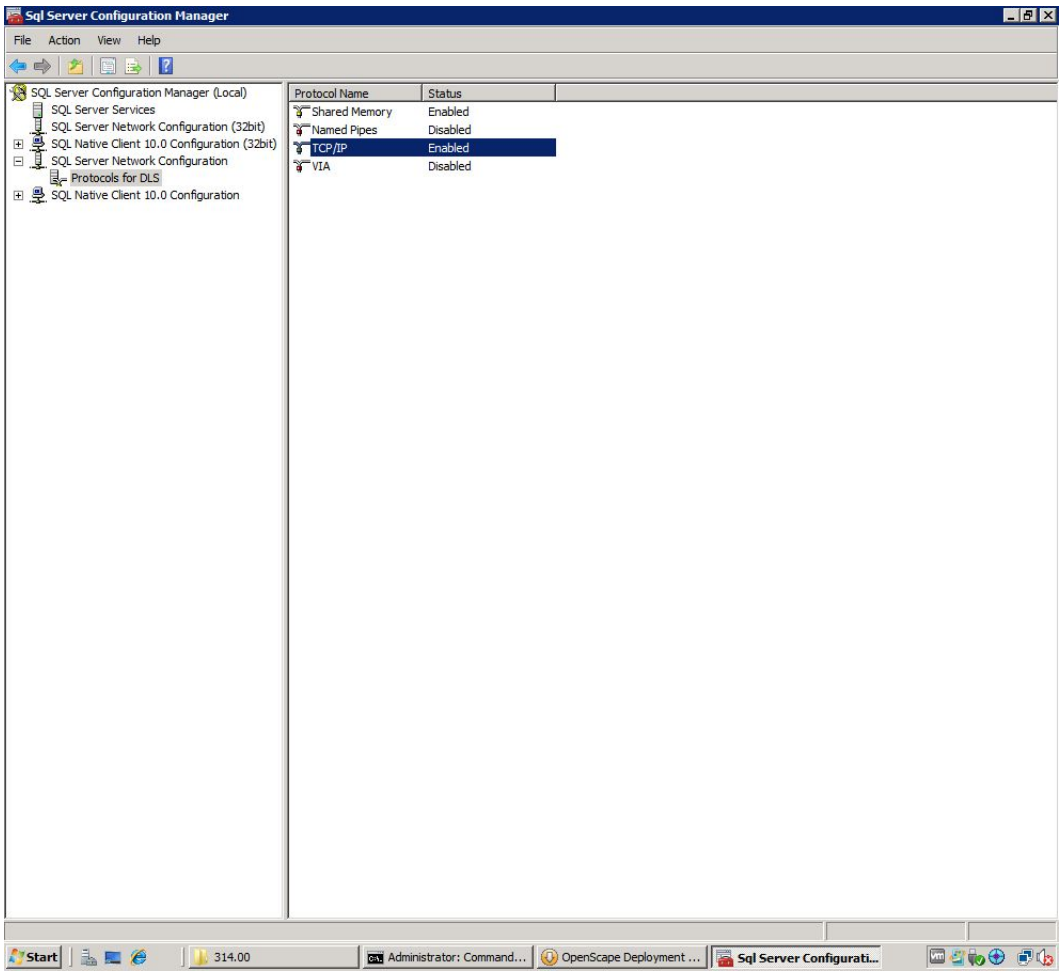
    Standardmäßig ist die SQL Server 2008 R2 Express-Datenbank so konfiguriert, dass keine Kommunikation über TCP/IP möglich ist. Erst nach Aktivierung des TCP/IP-Protokolls ist sichergestellt, dass die Datenbank ordnungsgemäß funktioniert.

    Klicken Sie im Startmenü auf **All Programs** > **Microsoft SQL Server 2008 R2**> **Configuration Tools** > **SQL Server Configuration Manager**.

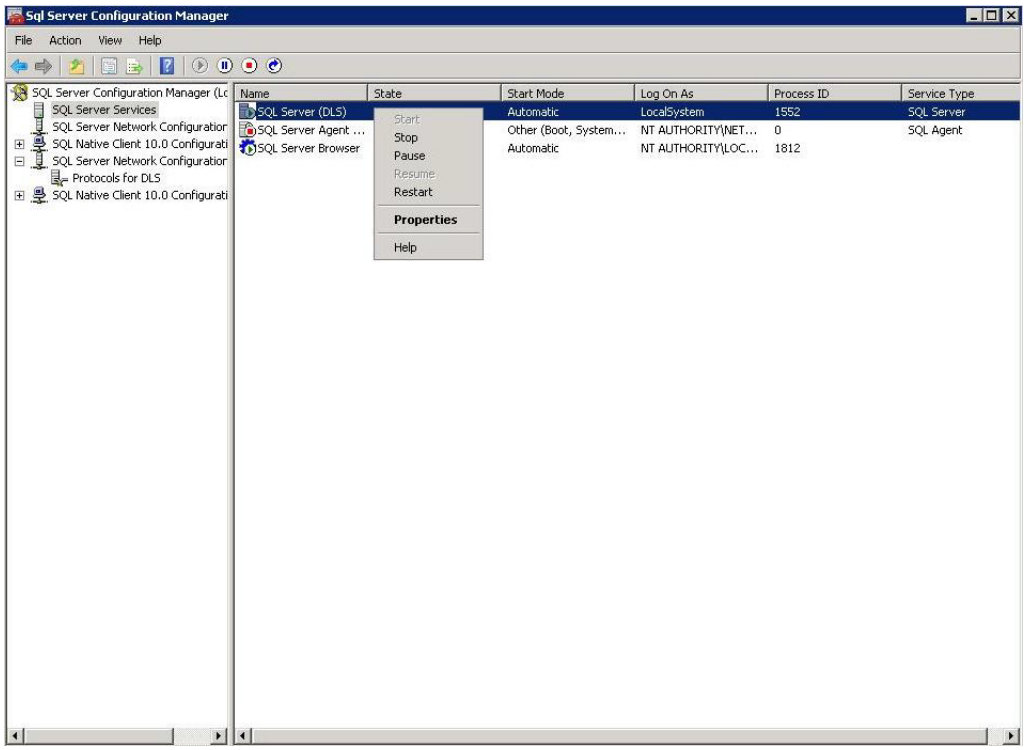


14. Erweitern Sie den Knoten **SQL Server Network Configuration** und wählen Sie anschließend den Eintrag **Protocols for DLS**.
    Klicken Sie mit der rechten Maustaste auf **TCP/IP** und klicken Sie auf **Enable**, um TCP/IP zu aktivieren.

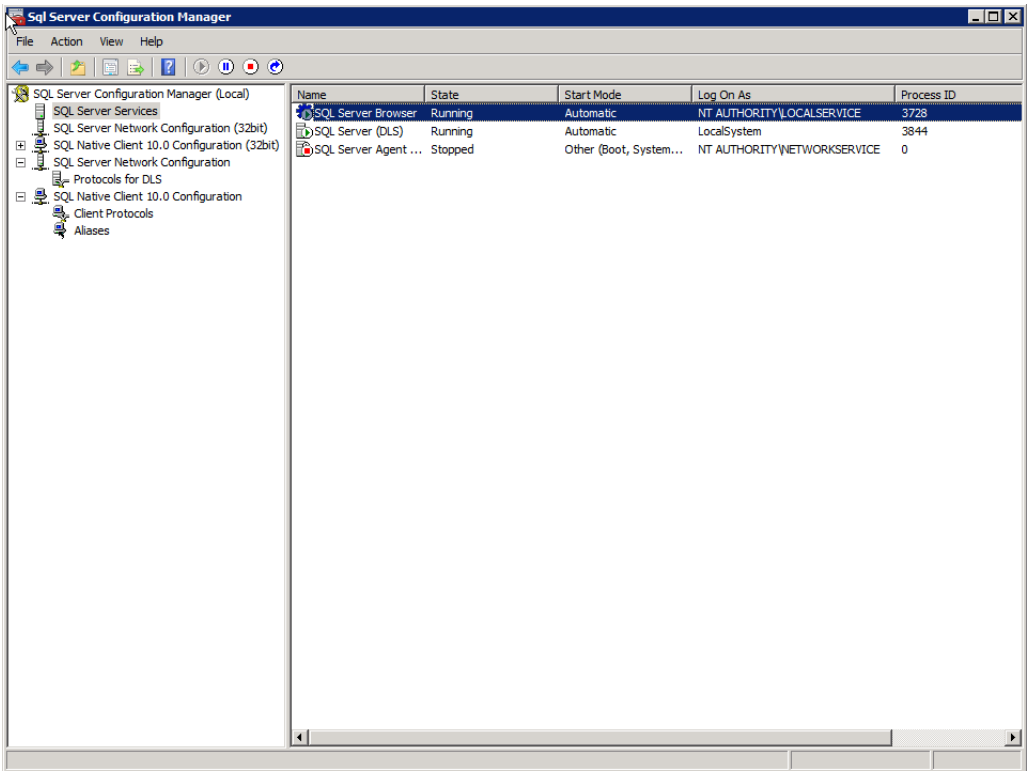

Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
Client Protocols
Aliases
SQL Server Network Configuration
Protocols for DLS
SQL Native Client 10.0 Configuration
Protocol Name
Status
Shared Memory
Enabled
Named Pipes
Disabled
TCP/IP
Disabled
VIA
Disabled
Enable
Disable
Properties
Help
Enable selected protocol.
Start
3:24 PM
2/11/2013



15. Wählen Sie im Navigationsbaum „SQL Server Services“. Klicken Sie mit der rechten Maustaste auf **SQL Server (SQL Instance Name= DLS)** und klicken Sie anschließend auf **Restart**.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Lc
SQL Server Services
SQL Server Network Configuratior
SQL Native Client 10.0 Configurati
SQL Server Network Configuration
Protocols for DLS
SQL Native Client 10.0 Configurati
Name
State
Start Mode
Log On As
Process ID
Service Type
SQL Server (DLS)
SQL Server Agent ...
SQL Server Browser
Automatic
LocalSystem
1552
SQL Server
Other (Boot, System...
NT AUTHORITY\NET...
0
SQL Agent
Automatic
NT AUTHORITY\LOC...
1812
Start
Stop
Pause
Resume
Restart
Properties
Help

16. Stellen Sie sicher, dass der SQL Server Browser-Dienst ordnungsgemäß ausgeführt wird. Klicken Sie mit der rechten Maustaste auf **SQL Browser** und wählen Sie die Einstellung **Automatic**. Klicken Sie auf **Restart**.



17. Die Installation ist abgeschlossen.

HINWEIS: Die SQL Server Express Edition wurde von Microsoft ausdrücklich so konfiguriert, weil diese SQL Server Edition normalerweise für den Heim- oder Einzelcomputereinsatz gedacht ist, also Szenarien, in denen das TCP/IP-Netzwerkprotokoll nicht unbedingt erforderlich ist. Beim DLS muss TCP/IP jedoch immer aktiviert sein; dies gilt auch dann, wenn der SQL-Server lokal installiert wird. Die Aktivierung des TCP/IP-Protokolls und die Konfiguration des SQL Browser-Dienstes sind nur bei der SQL Server Express Edition erforderlich. Bei höheren Editionen von SQL Server, wie sie z. B in Szenarien mit entfernter DLS-Datenbank und Multi-Node-Bereitstellungen zum Einsatz kommen, ist TCP/IP standardmäßig aktiviert.

Alternativ zur oben beschriebenen manuellen Installation gibt es auch die Möglichkeit der automatischen Installation. Hierzu gehen Sie wie folgt vor:

- **Automatische Installation**

1. Öffnen Sie die Eingabeaufforderung. Geben im Eingabefeld unter **Start** > **Run** die Zeichenfolge **cmd** ein und klicken Sie auf **OK**.
2. Geben Sie den Pfad zum Zielverzeichnis an, in dem sich das Installationsprogramm für Microsoft SQL Express befindet.

   z. B. `C:\MSSQL2008Express>`
3. Geben Sie den folgenden Befehl ein:

   ```
   <SQL_SERVER_INSTALLER> /ACTION=Install /FEATURES=SQLEngine /INSTANCENAME=DLS
   /SQLSVCACCOUNT="NT AUTHORITY\SYSTEM" /
   SQLSYSADMINACCOUNTS="<CURRENT_USER_ACCOUNT>" /SQLCOLLATION=Latin1_General_BIN
   /TCPENABLED=1 /QS /IACCEPTSQLSERVERLICENSETERMS
   ```

   Hierbei ist

   <SQL_SERVER_INSTALLER> die ausführbare Installationsdatei für den SQL Server

   z. B. `SQLEXPR_x64_ENU.EXE`: 64-Bit-Version von SQL Server 2008 R2 Express Edition

   <CURRENT_USER_ACCOUNT> ist das aktuelle Windows-Benutzerkonto, unter dem der DLS installiert wird. Wenn das Benutzerkonto ein Domänenkonto ist, müssen Sie zusätzlich auch die Domäne angeben (also <DOMAIN>\<USER_ACCOUNT> (Domänenbenutzer) oder <USER_ACCOUNT> (lokaler Benutzer)

   z. B. POSTM3\dlsuser (Domäne) oder dlsuser (lokal)

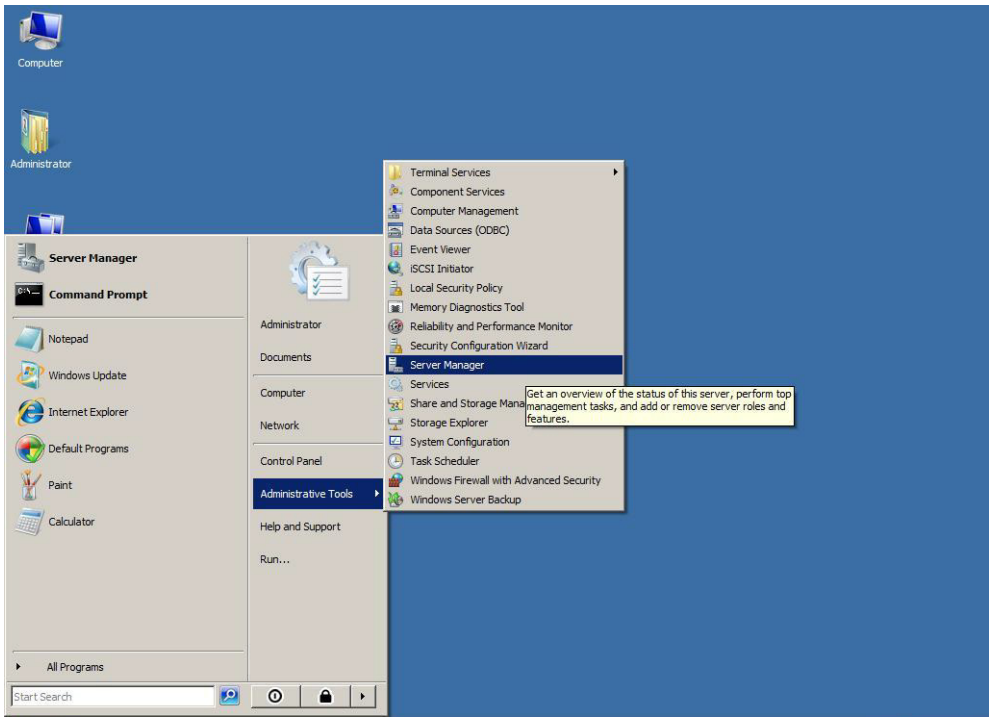
   SQLSYSADMINACCOUNTS ist das Windows-Konto, unter dem der SQL Server und der DLS installiert werden (Domäne oder lokal)

   HINWEIS: Geben Sie „`NT  AUTHORITY\SYSTEM`“ ein; achten Sie dabei auf das Leerzeichen zwischen „`NT`“ und „ `AUTHORITY`“.

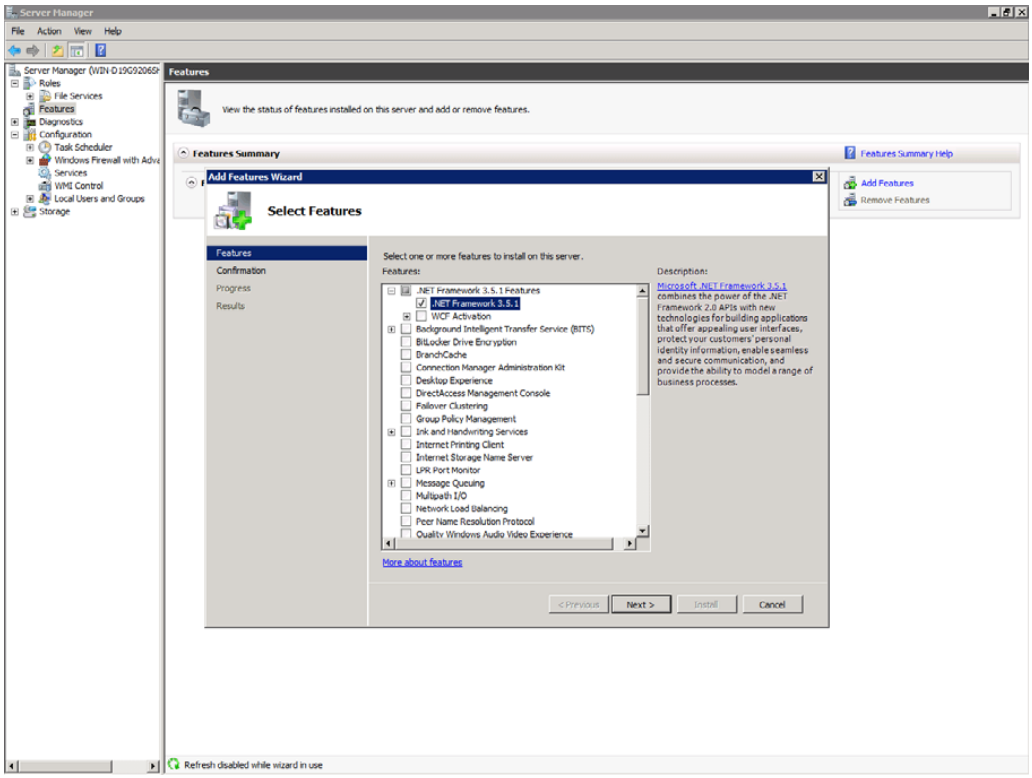
4.5.1.2 Microsoft .NET v3.51 installieren

Bei Microsoft SQL Server 2008 R2 kann .NET v3.51 nur über den Server Manager installiert werden.

1. Rufen Sie den **Server Manager** wie folgt über das Windows-Startmenü auf: **Start** > **Programs** > **Administrative Tools** > **Server Manager**



2. Klicken Sie im Fenster **Server Manager**, im Navigationsbaum links auf **Features**. Klicken Sie anschließend auf **Add New Feature**, um den Assistenten **Add Features** zu starten. Aktivieren Sie dann das Kontrollkästchen **.NET Framework 3.5.1**. Klicken Sie auf **Next.**



3. Warten Sie, bis die Installation abgeschlossen ist und der abschließende Dialog erscheint. Klicken Sie dort auf **Finish.**

4.5.1.3 DLS installieren

Folgen Sie hierzu dem im DLS-Softwarepaket enthaltenen Installationsassistenten.

WICHTIG: Installieren Sie einen Hotfix NICHT direkt. Installieren Sie immer zuerst die Basisversion des Hotfixes und führen Sie daran anschließend ein Upgrade auf den Hotfix durch. Die Basisversion von **V7 R1 314.05** lautet beispielsweise **V7 R1 314.00**.

4.5.2 Single Node-Betrieb mit entfernter oder kundenspezifischer Datenbank

Vor der Installation des DLS mit einer kundenspezifischen oder externen Datenbank muss zunächst der Microsoft SQL Server 2005/2008 Enterprise Edition installiert werden (siehe Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren”).

WICHTIG: Microsoft .NET v3.51 muss ebenfalls auf dem Server installiert werden, auf dem DLS installiert ist, damit RapidStat ordnungsgemäß funktioniert (siehe Abschnitt 4.5.1.2, “Microsoft .NET v3.51 installieren”).

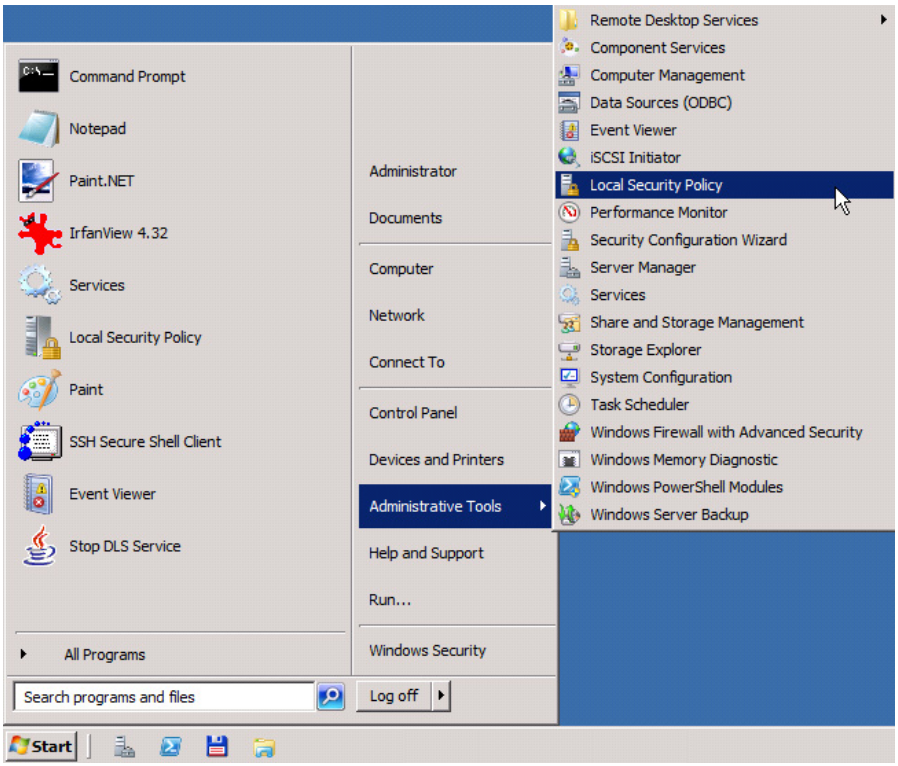
HINWEIS: Zu Beginn muss zuerst der SQL Native Client auf dem Computer installiert werden, auf dem die eigentliche DLS-Anwendung laufen soll, also auf dem DLS-Knoten (siehe Abschnitt 4.2.3, “SQL Native Client – bei Nutzung einer entfernten Datenbank”).

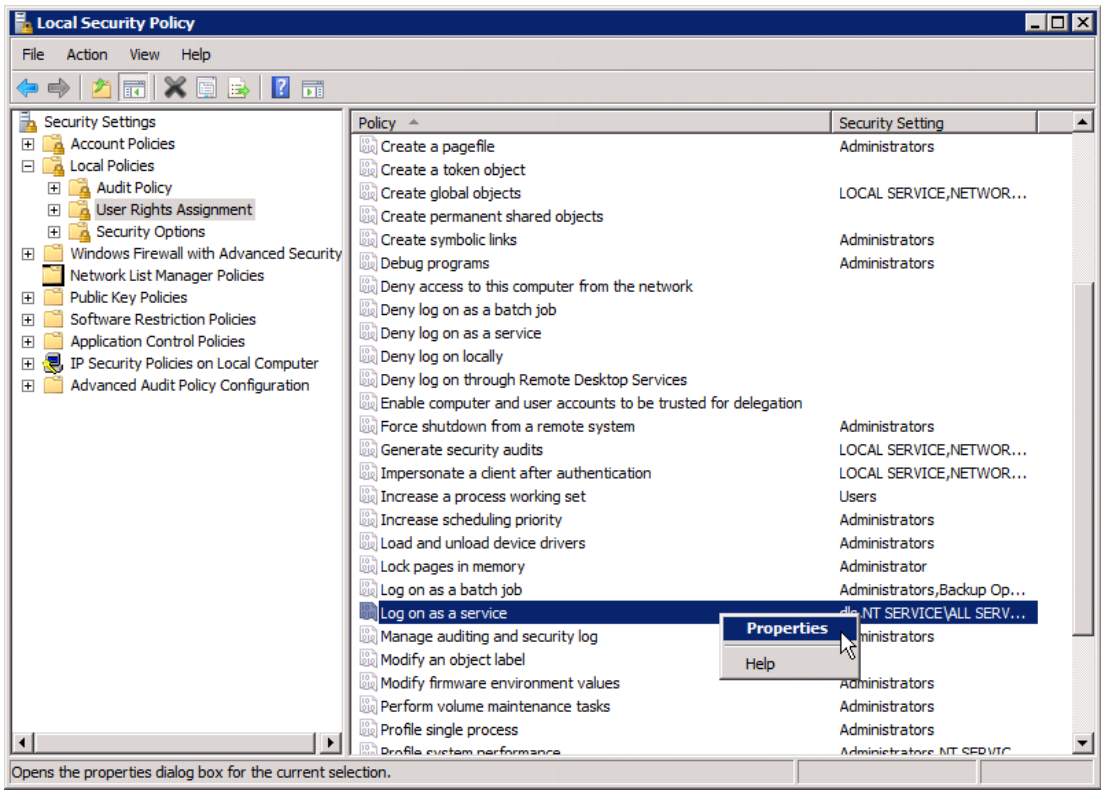
Bitte gehen Sie wie folgt vor:

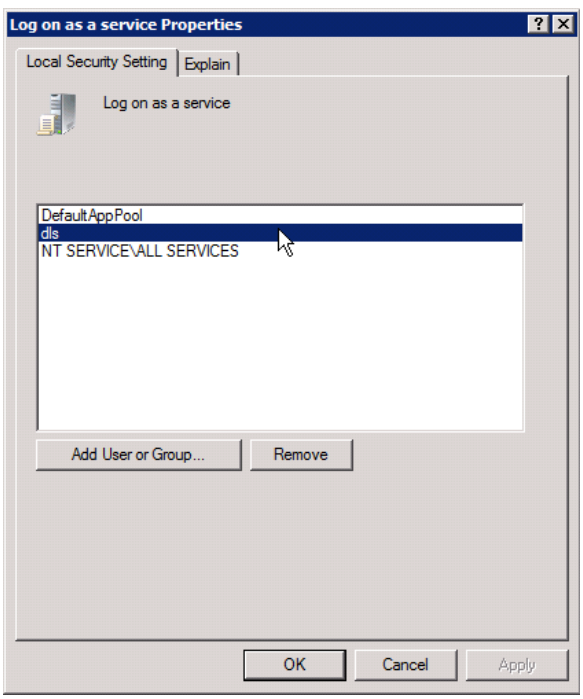
1. Wenn sich DLS-Server und Datenbankserver auf verschiedenen PCs befinden und auf dem Datenbankserver ein lokales Benutzerkonto verwendet wird, muss ein identisches Benutzerkonto auf dem DLS-Server eingerichtet werden. Fügen Sie am DLS-Rechner das für die Datenbank genutzte Benutzerkonto der Gruppe der lokalen Administratoren hinzu. Der Benutzer ‘dls’ sollte bereits beim Anlegen des Benutzers mit der Berechtigung ‘**Log on as a Service**‘ (Anmelden als Dienst) ausgestattet werden.

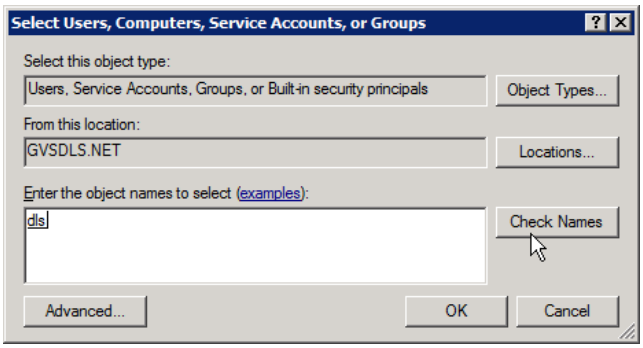
   Nachdem der ‘dls’-Benutzer entsprechend dem Verfahren für DLS-Konfigurationen mit entfernten Datenbanken mit Administratorrechten ausgestattet wurde, sollten Sie folgende Schritte ausführen:

   - Gehen Sie zu **Administrative Tools** > **Local Security Policy** > **Local Policies** > **User Rights Assignment** und fügen Sie den Benutzer ‘dls’ zur Richtlinie ‘**Log on as a service**‘ hinzu.


Command Prompt
Notepad
Paint.NET
IrfanView 4.32
Services
Local Security Policy
Paint
SSH Secure Shell Client
Event Viewer
Stop DLS Service
All Programs
Search programs and files
Administrator
Documents
Computer
Network
Connect To
Control Panel
Devices and Printers
Administrative Tools
Help and Support
Run...
Windows Security
Log off
Start
Remote Desktop Services
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
iSCSI Initiator
Local Security Policy
Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell Modules
Windows Server Backup


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Create a pagefile
Administrators
Create a token object
Create global objects
LOCAL SERVICE,NETWOR...
Create permanent shared objects
Create symbolic links
Administrators
Debug programs
Administrators
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop Services
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system
Administrators
Generate security audits
LOCAL SERVICE,NETWOR...
Impersonate a client after authentication
LOCAL SERVICE,NETWOR...
Increase a process working set
Users
Increase scheduling priority
Administrators
Load and unload device drivers
Administrators
Lock pages in memory
Administrator
Log on as a batch job
Administrators,Backup Op...
Log on as a service
Manage auditing and security log
Modify an object label
Modify firmware environment values
Administrators
Perform volume maintenance tasks
Administrators
Profile single process
Administrators
Properties
Help
Opens the properties dialog box for the current selection.

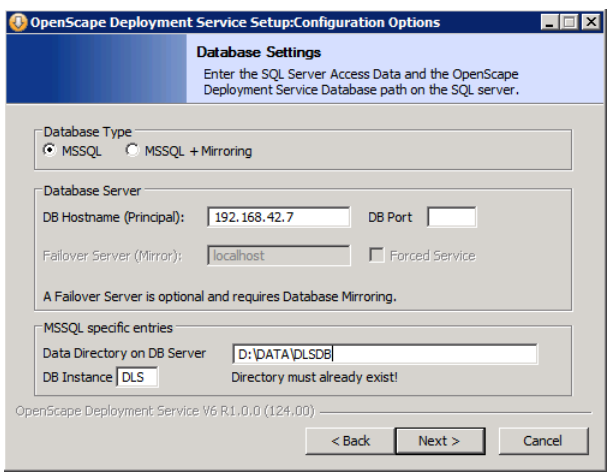

Log on as a service Properties
Local Security Setting
Explain
Log on as a service
DefaultAppPool
dls
NT SERVICE\ALL SERVICES
Add User or Group...
Remove
OK
Cancel
Apply



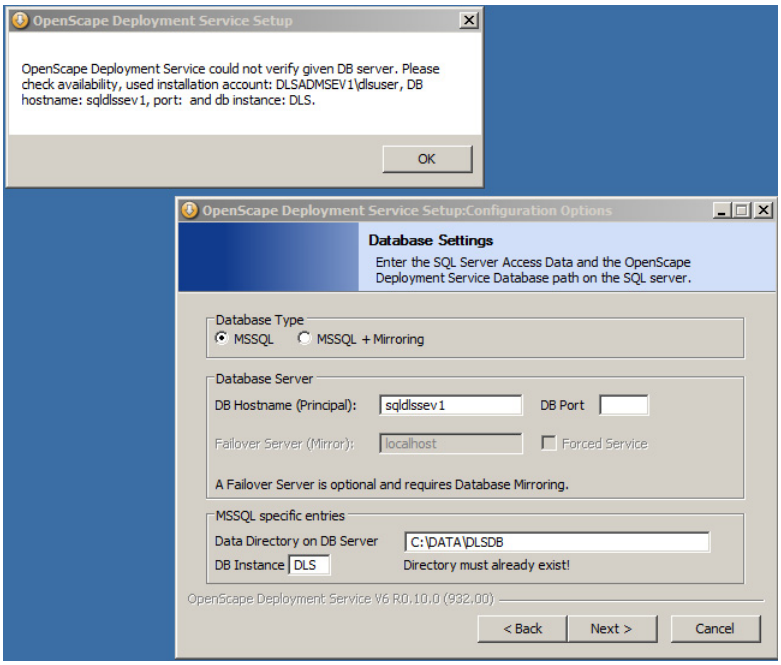
2. Melden Sie sich auf dem DLS-Server mit dem für die Datenbank verwendeten Benutzerkonto an und starten Sie das Setup-Programm. Alternativ können sie den Befehl `runas/user:<used account> <path to setup.exe>` verwenden, um die Installation zu starten.

3. Wählen Sie im Fenster **Konfiguration der Installation** im Feld **Datenbank Installationstyp** die Option **Verwende kundenspezifische oder entfernte Datenbank** aus.

4. Folgen Sie den Anweisungen zur Installation. Im Fenster **Konfiguration der Datenbank** unter **MSSQL spezifische Einstellungen** geben Sie das Datenbankverzeichnis ein, das Sie vor der Datenbankinstallation für die DLS-Daten erstellt haben, z. B. `D:\DATA\DLSDB`. Beachten sie, dass der Verzeichnispfad relativ zum Datenbankserver ist. Im Feld **DB Instanz** geben Sie „DLS“ ein. Klicken Sie auf **Next**.



Falls der SQL Native Client nicht auf dem DLS-Knotenrechner installiert ist, erscheint eine Fehlermeldung.



5. Unter **Benutzerkonto für Zugriff auf SQL-Server** geben Sie den Namen des oben genannten Benutzerkontos ein, z. B.
   `<local account>` („`dlsservice`“) oder
   `<domain name>\<sql account>` („`mydomain\dlsservice`“) oder
   `<sql account>@<domain url>` („`dlsservice@mydomain.com`“), sowie das dazugehörige Passwort.

6. Beenden Sie die Installation. Das Ergebnis können Sie überprüfen unter **Start** > **Einstellungen** > **Systemsteuerung** > **Verwaltung** > **Dienste: DeploymentService**.

4.5.3 Multi-Node-Betrieb

Das folgende Beispiel zeigt die Installation zweier DLS-Knoten mit gespiegelter SQL-Datenbank.

> ***HINWEIS:*** Sowohl die Erstinstallation als auch die Update-Installation darf nicht auf mehreren Knoten gleichzeitig vorgenommen werden, da die Knoten auf gemeinsame Dateien zugreifen. Installieren Sie also die Knoten nacheinander.

> ***WICHTIG:*** Microsoft .NET v3.51 muss ebenfalls auf dem Server installiert werden, auf dem DLS installiert ist, damit RapidStat ordnungsgemäß funktioniert (siehe Abschnitt 4.5.1.2, “Microsoft .NET v3.51 installieren”).

4.5.3.1 Erster Knoten

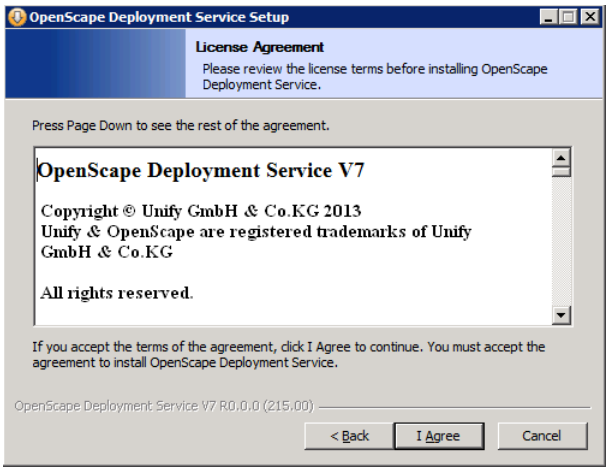
Melden Sie sich mit dem ‘dls’-Account, das zuvor bei der Remote-SQL-Installation des DLS-Zugangs erstellt wurde, am Knoten an.

> ***HINWEIS:*** Der SQL Native Client muss zuerst manuell installiert werden. Seine Version sollte mit der des installierten SQL-Remote-Servers übereinstimmen. Abwärtskompatibilität ist nicht unbedingt erforderlich. Die für die Abwärtskompatibilität notwendigen Dateien werden demzufolge von DLS nicht automatisch installiert. Wenn der SQL Native Client nicht installiert ist, wird unter Schritt 6 eine fehlerhafte Verbindung zum SQL-Server gemeldet.

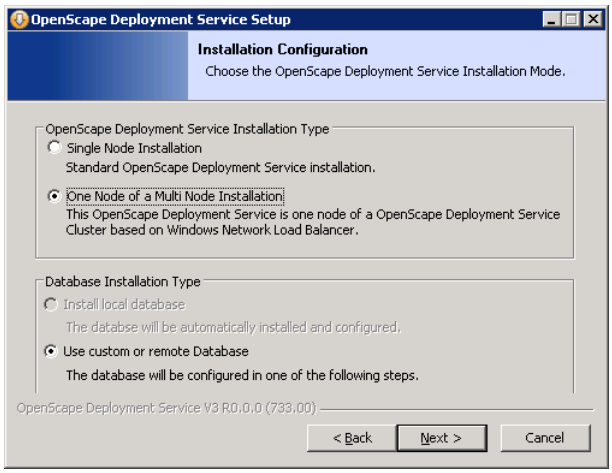
1. Starten Sie das Setup-Programm. Sie erhalten einen Begrüßungsbildschirm.

   Klicken Sie auf **Next**.

2. Klicken Sie **I Agree**, um die Lizenzvereinbarung zu akzeptieren.


OpenScape Deployment Service Setup
License Agreement
Please review the license terms before installing OpenScape Deployment Service.
Press Page Down to see the rest of the agreement.
OpenScape Deployment Service V7
Copyright © Unify GmbH & Co.KG 2013
Unify & OpenScape are registered trademarks of Unify GmbH & Co.KG
All rights reserved.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenScape Deployment Service.
OpenScape Deployment Service V7 R0.0.0 (215.00)
< Back
I Agree
Cancel

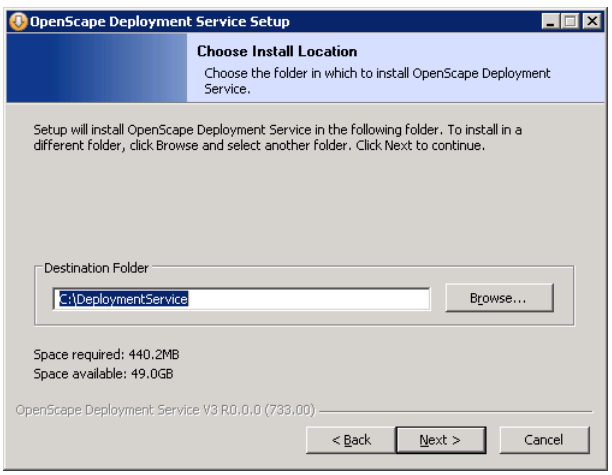
3. Im Fenster **Installation Configuration** wählen Sie unter **OpenScape Deployment Service Installation Type** die Option **One Node of a Multi Node Installation**.



Klicken Sie auf **Next**.

4. Im Fenster **Choose Install Location** wählen Sie das Zielverzeichnis, in dem der DLS installiert werden soll.

HINWEIS: Der Verzeichnispfad darf keine Leerzeichen enthalten, wie z. B. in „Program Files“.



Klicken Sie auf **Next**.

5. Im Fenster **Default Data Path** geben Sie den Pfad eines Verzeichnisses an, auf das alle Knoten Zugriff haben müssen. Hier werden Konfigurationsdaten gespeichert, die allen DLS-Knoten gemeinsam sind. Dieses Verzeichnis muss vorhanden sein und der DLS muss bereits für die Installation Schreibzugriff darauf haben. Die IP-Adresse muss die Adresse des 1. DLS-Knotens (aus Sicht des NLB-Clusters) sein.

   HINWEIS: Falls an dieser Stelle ein Hinweisfenster erscheint und mit der Frage, ob ein weiterer Knoten installiert werden soll, zusätzlich zu bereits vorhandenen Knoten, klicken Sie auf „Nein“. Das Hinweisfenster erscheint dann, wenn in dem angegebenen Verzeichnis von einer vorangegangenen DLS-Installation die Datei `common_dls.properties` vorhanden ist.

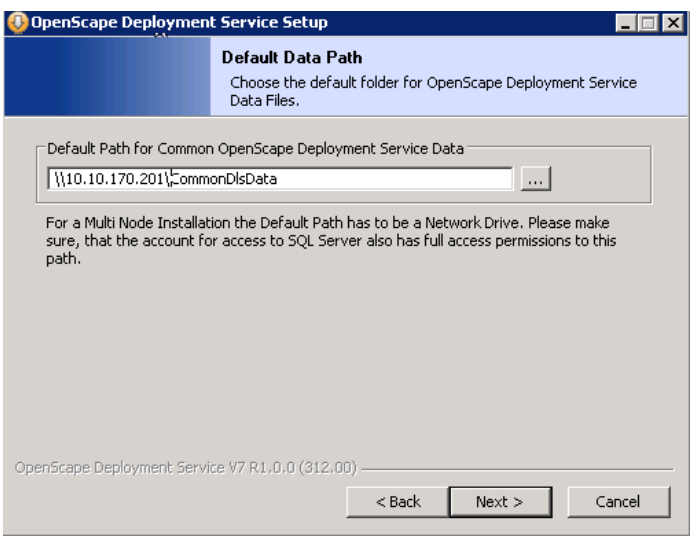
   HINWEIS: Um Backup/Restore-Probleme bei heruntergefahrenem bzw. nicht erreichbarem DLS Knoten 1 zu vermeiden, müssen Sie den Standardpfad für gemeinsame OpenScape Deployment Service-Daten auf den Pfad des Dateiservers ändern; dieser muss sich in der gleichen Domäne befinden wie der Rest der Multi-Node-Server, also
   `\\POSTM3-FileServer\MultinodeShare\CommonDlsData`

   oder

   `\\10.10.170.100\MultinodeShare\CommonDlsData`

   HINWEIS: Der Ordner CommonDLSData sollte auf dem Witness-Server liegen, sofern dieser vorhanden ist (bei synchroner Spiegelung). Wenn kein Witness-Server vorhanden ist, sollte der Ordner auf einem externen Server liegen, allerdings nicht auf dem Rechner, auf dem der CLA installiert ist. Sonstige Einstellungen können bei Multi-Node-Migrationsszenarien zu Problemen führen (siehe Abschnitt 16.17, “Migrationsszenarien”), bei denen mit minimalen Ausfallzeiten zu rechnen ist.

   WICHTIG: Das gemeinsame Datenverzeichnis sollte nicht verwendet werden, um Dateien zu speichern, die außerhalb des eigenen DLS-Knoten-Clusters fallen bzw. nicht für DLS-Verwaltungsaufgaben herangezogen werden; dies sind z. B. .csv/Archiv-Exporte, Profil-/Template-Exporte etc.



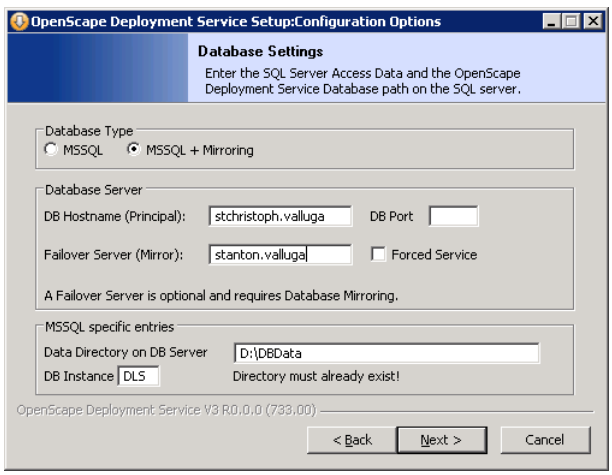
   Klicken Sie auf **Next**.

6. Im Fenster **Database Settings** machen Sie die erforderlichen Angaben zur Datenbank. Wenn Sie eine gespiegelte Datenbank für größte Ausfallsicherheit einsetzen wollen, wählen Sie unter **Database Type** die Option **MSSQL + Mirroring**. Unter **Database Server** geben Sie im Feld **DB Hostname (Principal)** den „Principal“-Datenbankserver an, und im Feld **Failover Server (Mirror)** den Ersatz-Datenbankserver, der einspringt, sobald der Principal ausfällt.

   Unter **MSSQL specific entries** geben Sie im Feld **Data Directory on DB Server** das Verzeichnis auf dem Datenbankserver an, in dem sich die DLS-Datenbank befindet. Dieses Verzeichnis muss bereits existieren. Es sollte vor der Installation des SQL-Servers angelegt worden sein (siehe Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren”, Schritt 2).

   HINWEIS: Es wird empfohlen, auf dem Mirror-Rechner den gleichen Verzeichnispfad zu benutzen wie auf dem Principal-Rechner.

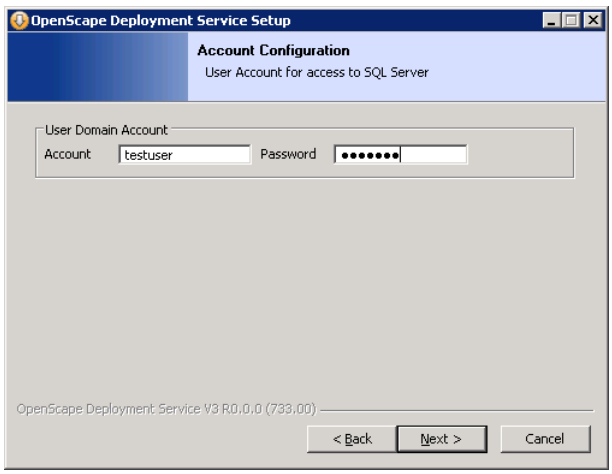
   Unter **DB Instance** geben Sie die Instanz ein, unter der die DLS-Datenbank laufen soll (siehe Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren”, Schritt 4 bzw. Abschnitt 4.2.2, “Microsoft SQL Server 2008 R2”, Schritt 9).



   Klicken Sie auf **Next**.

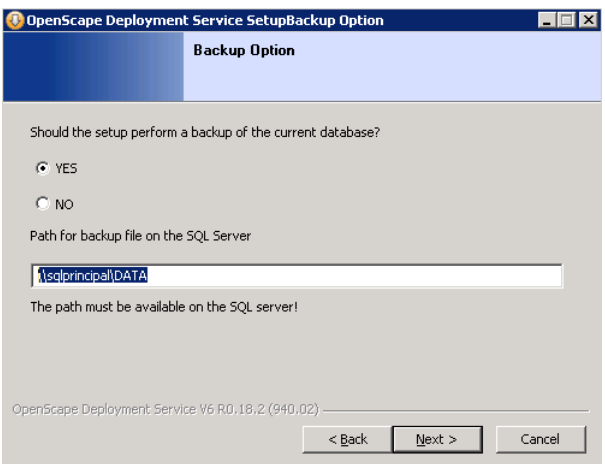
7. Im Fenster **Account Configuration** geben Sie in den Feldern **Account** und **Password** die Zugangsdaten des Benutzers ein, unter dem der DLS laufen soll. Der Benutzer muss zur Gruppe der Administratoren gehören und bereits existieren.

   HINWEIS: Wenn DLS in einer DNS-Umgebung installiert wird, müssen Sie den vollständigen Namen des FQDN-Accounts, also testuser@multinode.local or multimode.local\testuser, eingeben. Der normale „testuser“-Account ist kein Domänenbenutzer, sondern entspricht dem Benutzer eines lokalen Rechners (mit der Umgebung **Arbeitsgruppe**).



   Klicken Sie auf **Next**.

8. Im Fenster **Backup Option** wählen Sie „Yes“, wenn Sie Ihre Datenbank während der Installation bzw. des Upgrades sichern wollen.



   Das Datenbank-Backup kann folgendermaßen in lokale oder entfernte Datenbank-Bereitstellungen übernommen werden:

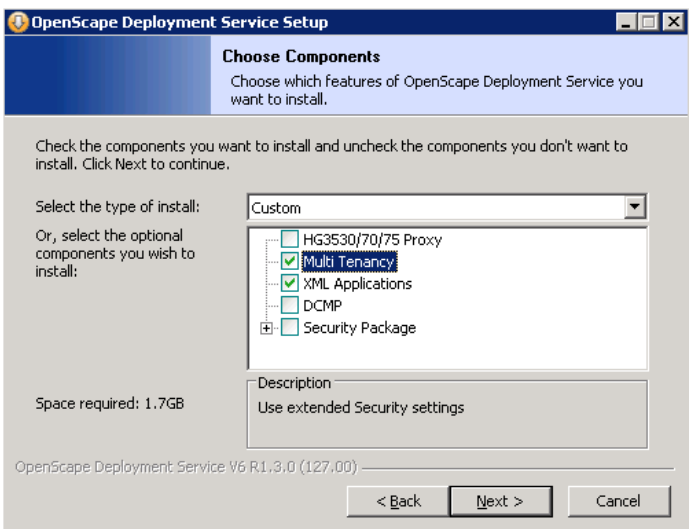
a) Über ein bereits existierendes lokales Datenbank-Verzeichnis auf dem Computer, auf dem die Datenbank installiert ist (z. B. `C:\DLSDB`). Dies kann der Rechner sein, auf dem neben SQL auch DLS installiert ist, oder bei Konfigurationen mit entfernten Datenbanken einer der SQL-Server (bei Datenspiegelung für das komplexeste Szenario).

b) Verwenden Sie ein existierendes und freigegebenes UNC-Verzeichnis am Remotestandort (z. B.`\\10.10.1.12\DBBACKUP` oder `\\CENTRALSERVER.COMPANU.NET\Backup` oder `\\MYSERVER\CommonDlsData\Backups` etc).

HINWEIS: Die Angabe von Netzlaufwerken (d. h. Remote-Standorten mit lokal zugewiesenem Laufwerkbuchstaben) ist nicht zulässig, weil Windows-Dienste nicht auf Netzlaufwerke zugreifen dürfen und DLS ein Dienst ist. Windows-Dienste können einzig und allein über einen UNC-Pfad auf Remote-Standorte zugreifen.

HINWEIS: Dabei muss für den Account, für den die SQL-Datenbank-Instanz erstellt wurde, Schreibzugriff auf den UNC-Pfad erteilt werden. DLS sorgt dafür, dass diese Anforderung erfüllt ist. Beim Exportieren der Datenbank besteht der SQL darüber hinaus jedoch darauf, dass der zugehörige Account auch auf Dateisystemebene über den Zielpfad als „vertrauenswürdig“ erkannt wird.

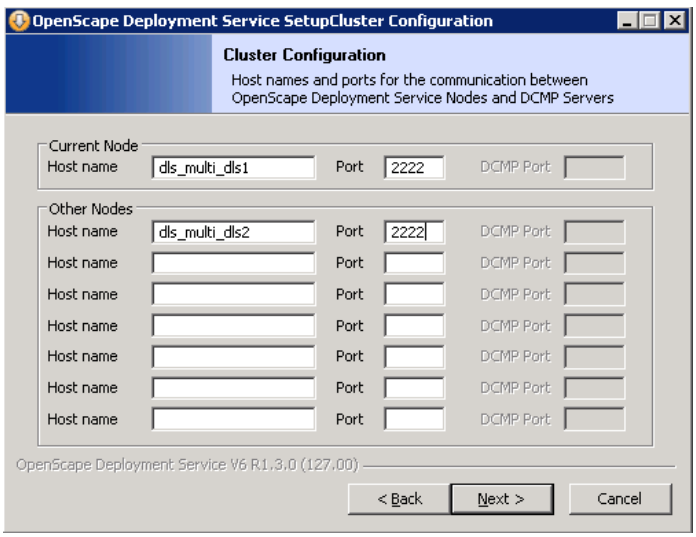
9. Wählen Sie nun im Fenster **Choose Components** die gewünschten DLS-Komponenten aus.



Klicken Sie auf **Next**.

10. Im Fenster **Cluster Configuration** sehen Sie unter **Current Node** den Knotenrechner, auf dem Sie gerade den DLS installieren. Unter **Other Nodes** geben Sie im Feld **Host Name** den Namen des jeweiligen Knotenrechners ein und im Feld **Port** den Port, den der auf diesem Rechner laufende DLS zur Kommunikation mit den anderen Knoten verwendet. Haben Sie in Schritt 8 den DCMP ausgewählt, müssen sie im Feld **DCMP-Port** den Port angeben, auf dem der DLS Daten vom DCMP empfängt.

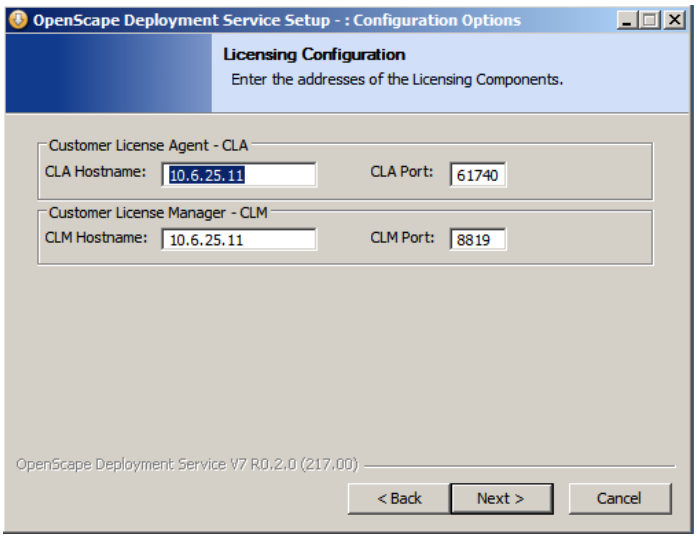
    HINWEIS: Bei einer Arbeitsgruppe oder einem DNS ohne FQDN wird stattdessen eine IP-Adresse hinzugefügt.



    Klicken Sie auf **Next**.

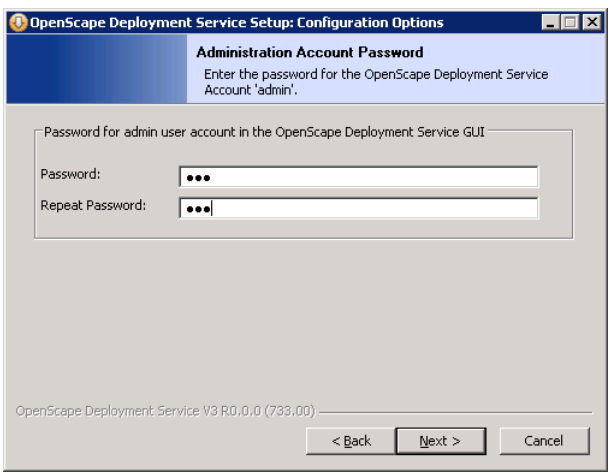
11. Im Feld **Licensing Configuration** machen Sie die zur Lizensierung nötigen Angaben. Unter **Customer License Agent – CLA** geben Sie im Feld **CLA Hostname** die IP-Adresse des CLA-Rechners ein, und im Feld **CLA Port** den dazugehörigen Port. Unter **Customer License Manager – CLM** geben Sie im Feld **CLM Hostname** die IP-Adresse des CLM-Rechners ein, und im Feld **CLM Port** den dazugehörigen Port.

    HINWEIS: Die Ordner CLA und CommonDLSData müssen sich auf auf unterschiedlichen Servern befinden. Andernfalls ist eine Spiegelung nicht möglich und es könnte bei Multi-Node-Migrationsszenarien zu Problemen kommen (siehe Abschnitt 16.17, “Migrationsszenarien”), bei denen mit minimalen Ausfallzeiten zu rechnen ist.



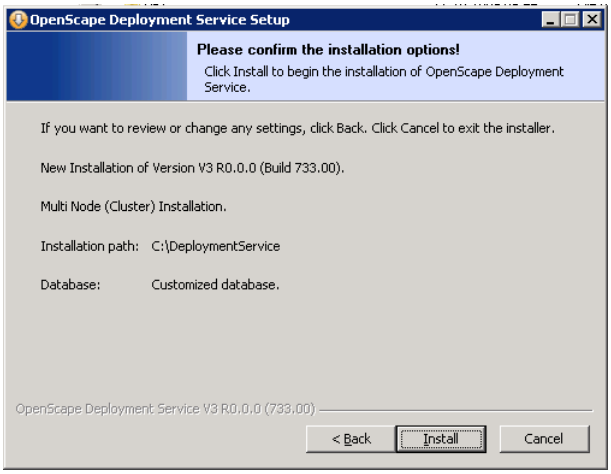
Klicken Sie auf **Next**.

12. Im Fenster **Administration Account Password** geben Sie in den Feldern **Password**/**Repeat Password** das Passwort für den DLS-Benutzer „admin“ ein.

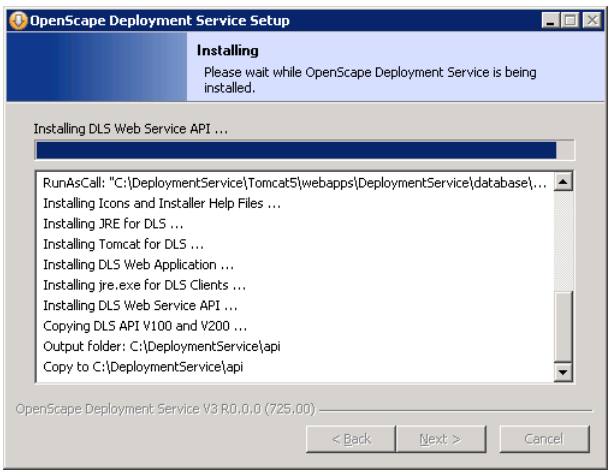


Klicken Sie auf **Next**.

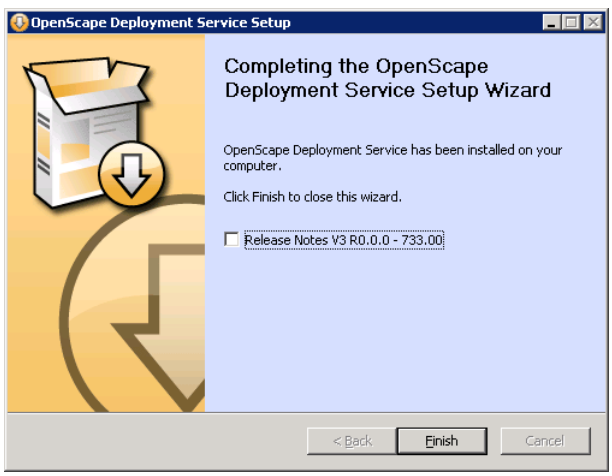
13. Im nächsten Fenster erhalten Sie eine kurzen Überblick über die Einstellungen zur Installation. Um die Installation zu starten, klicken Sie auf **Install**; um Einstellungen zu revidieren, klicken Sie auf **Back**.


OpenScape Deployment Service Setup
Please confirm the installation options!
Click Install to begin the installation of OpenScape Deployment Service.
If you want to review or change any settings, click Back. Click Cancel to exit the installer.
New Installation of Version V3 R0.0.0 (Build 733.00).
Multi Node (Cluster) Installation.
Installation path: C:\DeploymentService
Database: Customized database.
OpenScape Deployment Service V3 R0.0.0 (733.00)
< Back
Install
Cancel

14. Wenn Sie zuvor auf **Install** geklickt haben, erhalten Sie Meldungen über den Verlauf der Installation.



15. Die Installation ist abgeschlossen.



16.

HINWEIS: Gilt (nur) für Windows Server 2003. Überspringen Sie diesen Schritt, wenn Sie ein anderes Betriebssystem haben.

NLB Passwort eintragen:

Das bei der NLB-Administration (siehe Konfiguration des Network Load Balancer, Schritt 3) vergebene Passwort zur Fernsteuerung muss dem DLS mitgeteilt werden. Es ist lediglich unter Windows 2003 verfügbar.

Öffnen Sie dazu eine DOS-Box (Eingabeaufforderung). Als aktuelles Verzeichnis muss
`<DLS Installationspfad>\DeploymentService\Tomcat5\webapps\DeploymentService\database`
eingestellt sein. Setzen Sie hier das DOS Kommando ab:

```
dlsconfig set nlb_password <das von Ihnen vergebene Passwort>
```

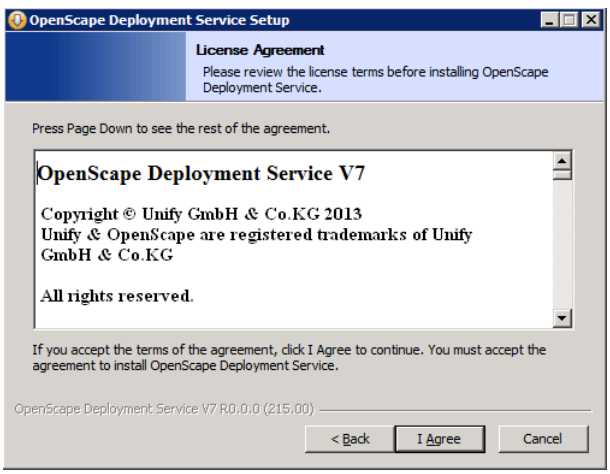
Um ein Passwort wieder zu löschen, geben Sie als neues Passwort einen Leerstring (“”) ein.

4.5.3.2 Zweiter und weitere Knoten

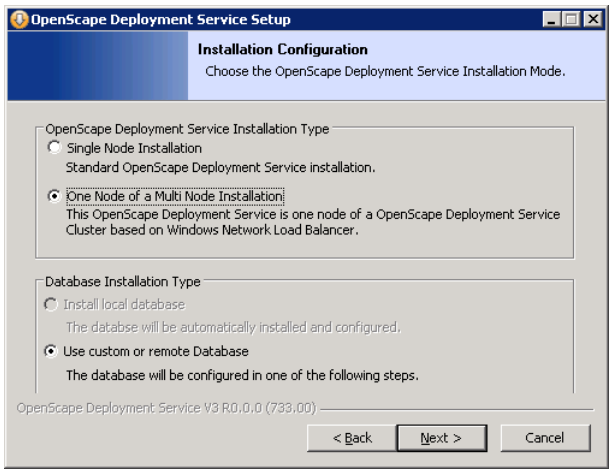
1. Starten Sie das Setup-Programm. Sie erhalten einen Begrüßungsbildschirm.

   Klicken Sie auf **Next**.

2. Klicken Sie **I Agree**, um die Lizenzvereinbarung zu akzeptieren.



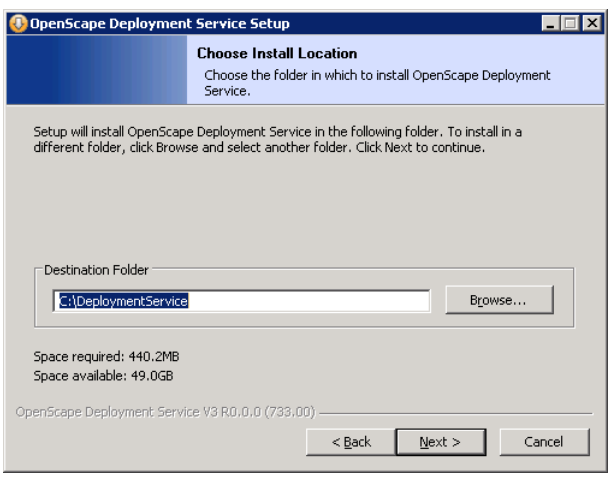
3. Im Fenster **Installation Configuration** wählen Sie unter **DLS Installation Type** die Option **One Node of a Multi-Node-Installation**.



Klicken Sie auf **Next**.

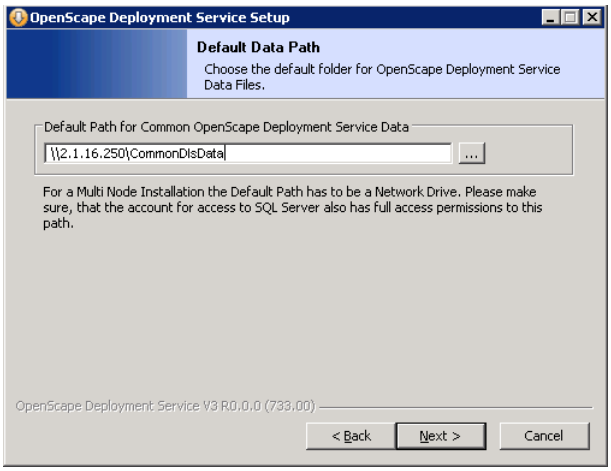
4. Im Fenster **Choose Install Location** wählen Sie das Zielverzeichnis, in dem der DLS installiert werden soll.

HINWEIS: Der Verzeichnispfad darf keine Leerzeichen enthalten, wie z. B. in „Program Files“.



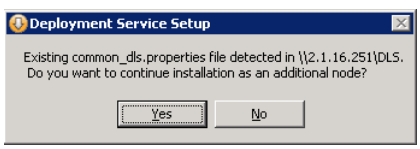
Klicken Sie auf **Next**.

5. Im Fenster **Default Data Path** geben Sie den Pfad des Verzeichnisses für gemeinsame Konfigurationsdaten des DLS an. Dieser wurde in Abschnitt 4.5.3.1, “Erster Knoten”, Schritt 5, festgelegt.



Klicken Sie auf **Next**.

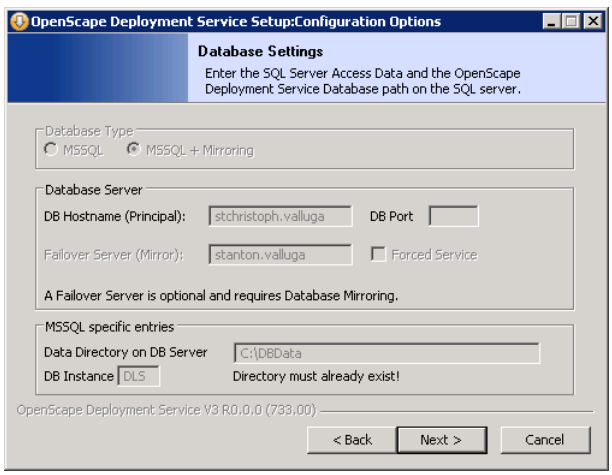
6. Da der erste DLS-Knoten bereits installiert ist und die Datei `common_dls.properties` im entsprechenden Verzeichnis abgelegt hat, erhalten Sie einen Hinweis:



Klicken Sie **Yes**.

7. Im Fenster **Database Settings** machen Sie die erforderlichen Angaben zur Datenbank. Wenn Sie eine gespiegelte Datenbank für größte Ausfallsicherheit einsetzen wollen, wählen Sie unter **Database type** die Option **MSSQL + Mirroring**.

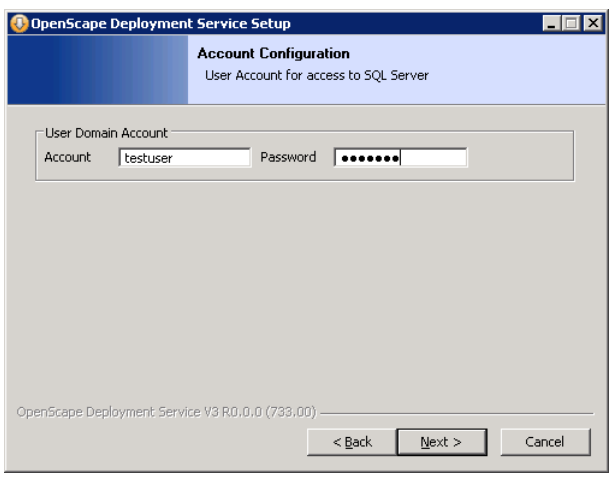
   Unter **MSSQL specific entries** geben Sie im Feld **Data Directory on Server** das Verzeichnis auf dem Datenbankserver an, in dem sich die DLS-Datenbank befindet. Dieses Verzeichnis muss bereits existieren. Unter DB Instance geben Sie die Instanz ein, unter der die DLS-Datenbank laufen soll (siehe Abschnitt 4.2.1, “Microsoft SQL Server 2005”, Schritt 4 bzw. Abschnitt 4.2.2, “Microsoft SQL Server 2008 R2”, Schritt 9).



   Klicken Sie auf **Next**.

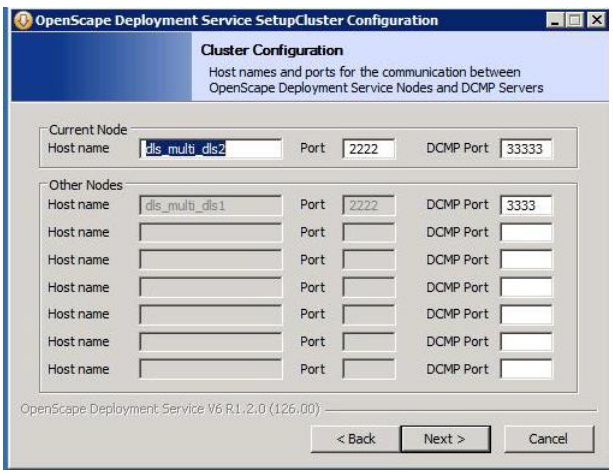
8. Im Fenster **Account Configuration** geben Sie in den Feldern **Account** und **Password** die Zugangsdaten des Benutzers ein, unter dem der DLS laufen soll. Der Benutzer muss zur Gruppe der Administratoren gehören und bereits existieren.

   HINWEIS: Wenn DLS in einer DNS-Umgebung installiert wird, müssen Sie den vollständigen Namen des FQDN-Accounts, also testuser@multinode.local or multimode.local\testuser, eingeben. Der normale „testuser“-Account ist kein Domänenbenutzer, sondern entspricht dem Benutzer eines lokalen Rechners (mit der Umgebung **Arbeitsgruppe**).



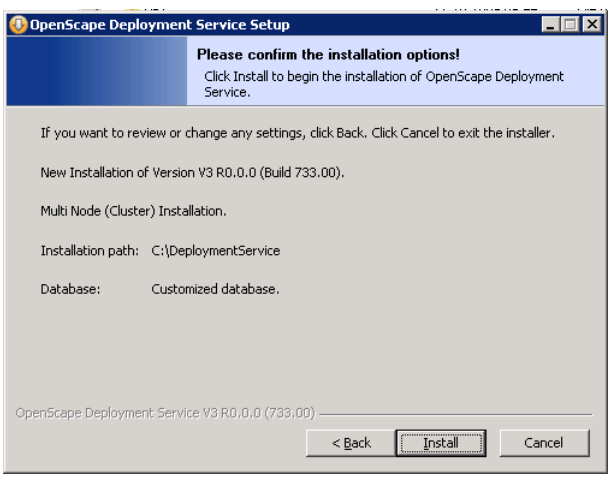
   Klicken Sie auf **Next**.

9. Im Fenster **Cluster Configuration** sehen Sie unter **Current Node** den Knotenrechner, auf dem Sie gerade den DLS installieren. Unter **Other Nodes** geben Sie im Feld **Host Name** jeweils den Namen des jeweiligen Knotenrechners ein und im Feld **Port** den Port, den der auf diesem Rechner laufende DLS zur Kommunikation mit den anderen Knoten verwendet. Haben Sie in Schritt 8 den DCMP ausgewählt, müssen sie im Feld **DCMP-Port** den Port angeben, auf dem der DLS Daten vom DCMP empfängt. Wurden die Daten bereits beim ersten Knoten eingegeben, können sie hier nochmals geprüft, geändert oder erweitert werden.

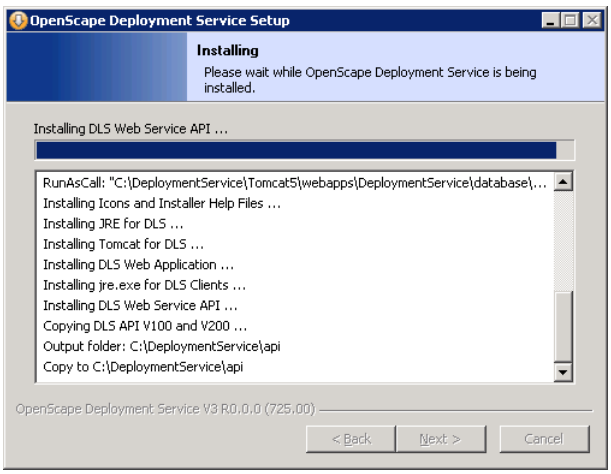


Klicken Sie auf **Next**.

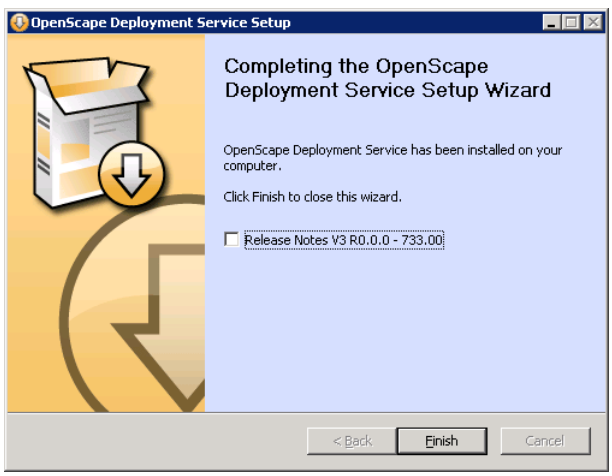
10. Im nächsten Fenster erhalten Sie eine kurzen Überblick über die Einstellungen zur Installation. Um die Installation zu starten, klicken Sie auf **Install**; um Einstellungen zu revidieren, klicken Sie auf **Back**.



11. Wenn Sie zuvor auf **Install** geklickt haben, erhalten Sie Meldungen über den Verlauf der Installation.



12. Die Installation ist abgeschlossen.



4.5.3.3 Neuinstallation der DLS Knoten bei vorhander Datenbank

Wenn man die DLS-Knoten neu installieren will (kein Upgrade), aber auf den SQL-Servern bereits eine DLS Datenbank vorhanden ist, muss man

- die DB-Spiegelung mit dem „MS SQL Management Studio“ auf dem SQL-Server Principal beenden,
- die DLS-Datenbank auf dem Principal und dem Mirror löschen,
- auf dem Principal und dem Mirror die vom DLS eingerichteten Stored Procedures entfernen.
- den 1. Knoten neu installieren und das letzte verfügbare Backup einspielen,
- alle weiteren Knoten installieren,
- wie beschrieben die Spiegelung einrichten (siehe Abschnitt 4.6, “Spiegelung der SQL-Datenbank aufsetzen”), wobei die SQL-Statements zum Einrichten der Endpoints nicht mehr notwendig sind.

4.6 Spiegelung der SQL-Datenbank aufsetzen

Um größte Ausfallsicherheit zu gewährleisten, können zwei separate Datenbankserver eingesetzt werden. Hierbei ist nur einer der Datenbankserver mit dem DLS (Single Node oder Cluster) verbunden, während auf dem anderen Server die Daten gespiegelt werden. Fällt der Hauptserver („Principal“) aus, übernimmt der zweite Server („Mirror“) dessen Funktion.

Für das Spiegeln der Datenbank werden zwei Modelle unterstützt:

- **Synchrone Spiegelung**: Ein dritter Server („Witness“) überwacht den Zustand des Hauptservers. Kommt es zum Ausfall des Principals, schaltet der Witness automatisch auf den Mirror um, der damit zum Principal wird. Der Witness kontrolliert zudem, ob alle Transaktionen auch auf dem Mirror vollendet werden. Dadurch wird sichergestellt, dass kein Datenverlust eintritt. Die Performanz wird dabei allerdings etwas geringer als bei der asynchronen Spiegelung.

  HINWEIS: Hochverfügbarkeit mit garantierter Sicherheit vor Datenverlust ist nur mit der synchronen Spiegelung möglich.

- **Asynchrone Spiegelung**: Es gibt keinen Witness, und die Umschaltung auf den Mirror-Server erfolgt durch „Forced Service“, d. h. durch den DLS.

Die folgenden Voraussetzungen müssen für die Datenbankspiegelung erfüllt sein:

- Auf allen für die Datenbankspiegelung benötigten Servern (Principal, Mirror und ggf. Witness) ist der Microsoft SQL Server 2005/2008 Enterprise Edition installiert, mit den Service Packs 1 und 2. Falls verfügbar, sollte auch SP3 installiert sein (siehe Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren”). Die Datenbanken können sowohl auf den DLS Knoten als auch auf eigenen Serverrechnern installiert sein.
- Microsoft SQL Server Management Studio muss installiert sein.
- Mindestens der erste DLS-Knoten ist installiert (siehe Abschnitt 4.5, “Installation des DLS”), da die Spiegelung nur für eine bereits installierte DLS-Datenbank eingeschaltet werden kann. Dies ist mit der Installation des ersten DLS-Knotens geschehen.
- Der Service **DeploymentService** ist auf allen beteiligten DLS-Knoten gestoppt.
- Für die Datenbank des DLS (DLSdb) ist das Recovery Model „Full“ eingestellt.
- Die Größe des Transaktions-Logs (TransactionLog) ist unbegrenzt.

HINWEIS: Da das Transaktions-Log beliebig groß werden kann, könnte es vorkommen, dass auf der Festplatte irgendwann so wenig Speicherplatz verfügbar ist, dass der SQL-Server und der DLS nicht mehr ordnungsgemäß funktionieren.

Planen Sie deshalb regelmäßige Sicherungen des Transaktions-Logs zusätzlich zu den Sicherungen der DLS-Daten. Dies bewirkt eine Reduktion des jeweils aktiven Transaktions-Logs. Das Transaktions-Log sollte zudem wesentlich häufiger gesichert werden als die eigentlichen Daten, um diese Datei immer möglichst klein zu halten.

Beim Datenbank-Backup werden entsprechende .trn-Dateien als Sicherungen der Transaktions-Logs angelegt. Dies stellt sicher, dass die Transaktions-Log-Datei „DLS-Log.LDF“ nicht unendlich anwächst.

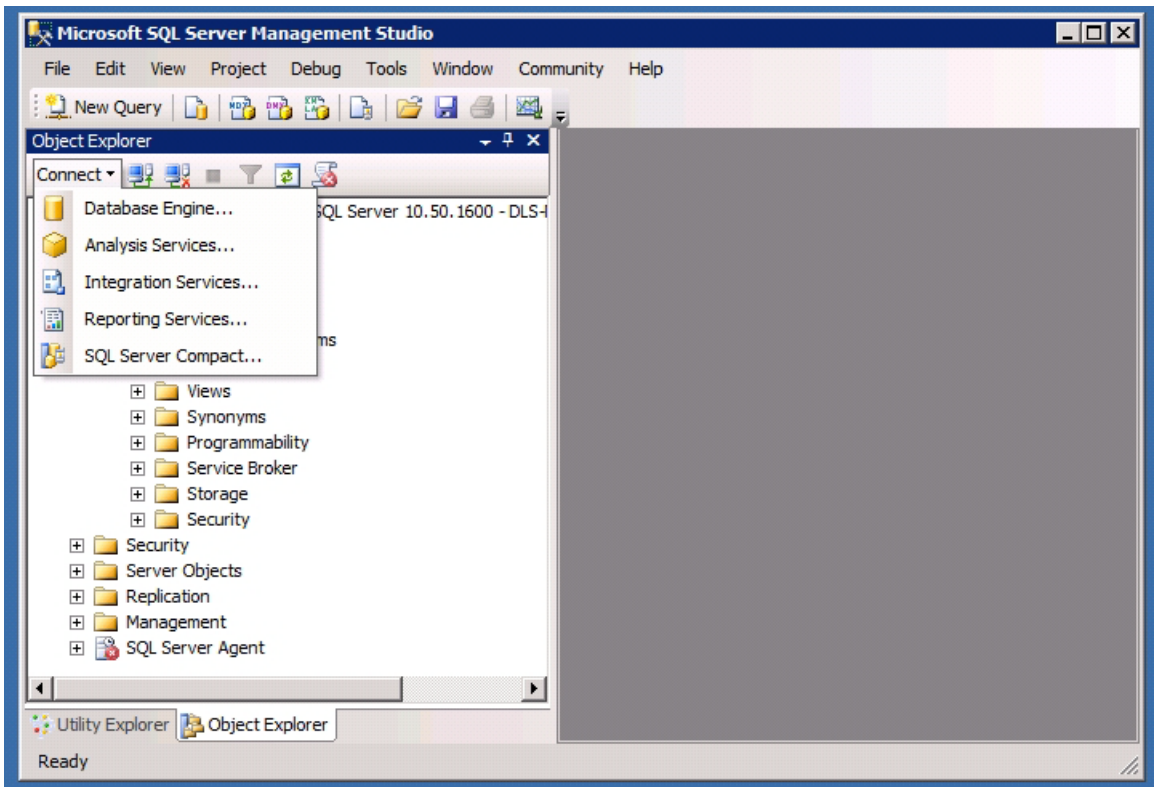
Das erste Anlegen einer .trn-Datei kann länger dauern, wenn eine sehr große „DLS-Log.LDF“-Datei verarbeitet werden muss.

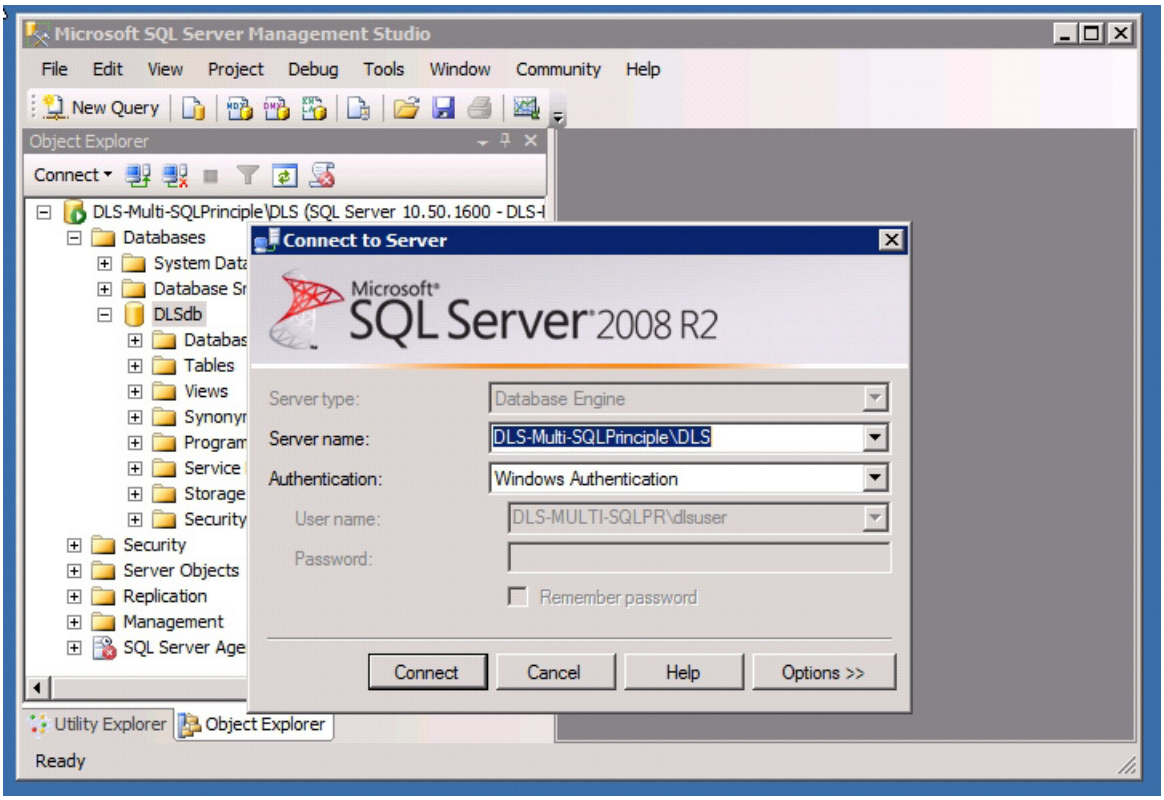
Bei der Wiederherstellung einer DLS-Datenbank ist keine entsprechende .trn-Datei nötig. Es wird jedoch empfohlen, für eventuelle Nachforschungen in Problemfällen die letzte Sicherung der Transaktions-Log-Datei aufzubewahren.

Die Installation des Microsoft SQL Server 2005/2008 Enterprise Edition ist beschrieben in Abschnitt 4.2, “SQL-Server für entfernte Datenbank installieren”. Nun folgt das Aufsetzen einer synchron gespiegelten SQL-Datenbank.

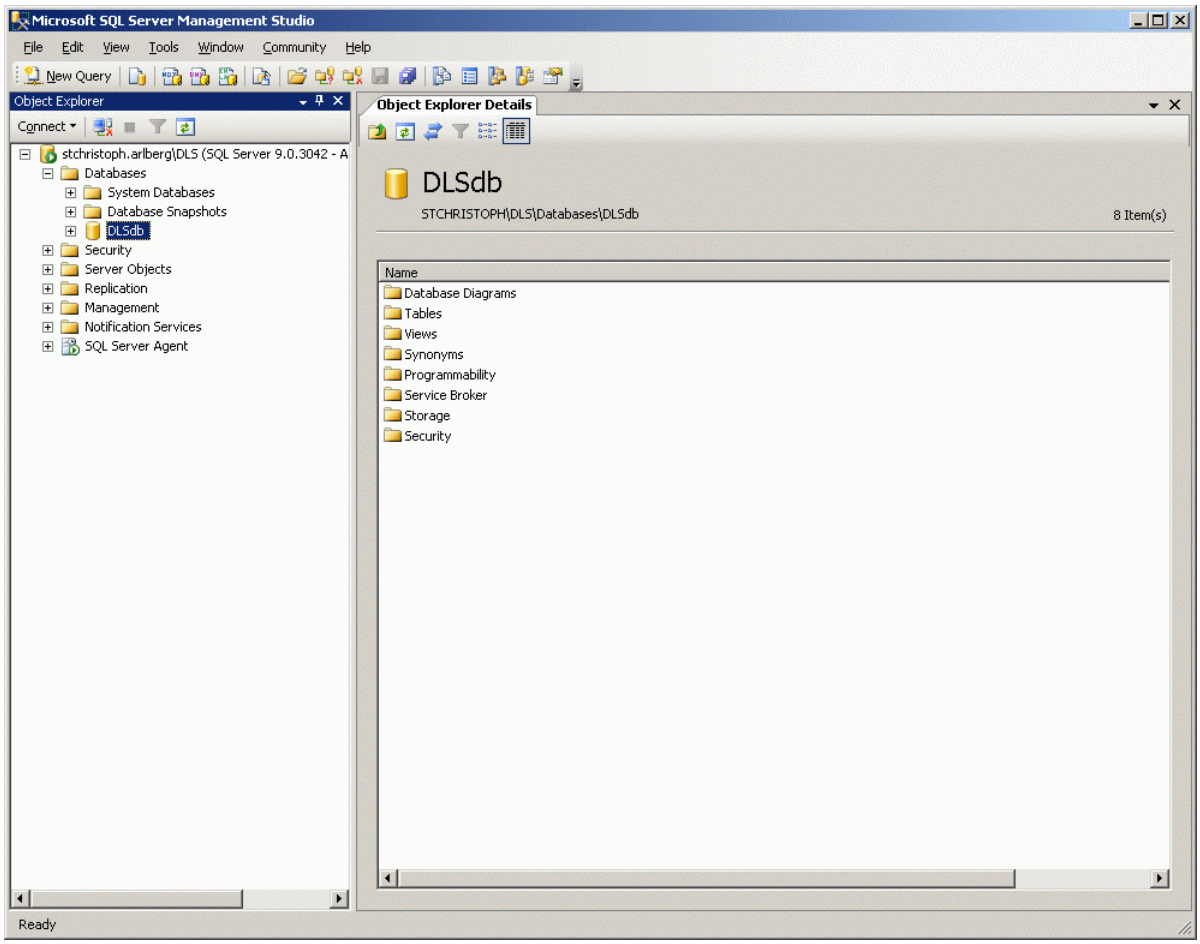
HINWEIS: Bei aktiver Datenbank-Spiegelung ist keine Wiederherstellung (Restore) eines Backups möglich.

1. Auf dem Rechner, der als Principal fungieren soll, gehen Sie auf **Start** > **Microsoft SQL Server 2005/2008** > **Microsoft SQL Server Management Studio**. Klicken Sie auf **Connect**. Wählen Sie wie nachstehend gezeigt den gewünschten **Datenbankeintrag** aus. Ein **Connect to Server**-Fenster wird angezeigt. Geben Sie abhängig vom vorherigen Setup den richtigen Servernamen ein. Klicken Sie abschließend auf **Connect**.

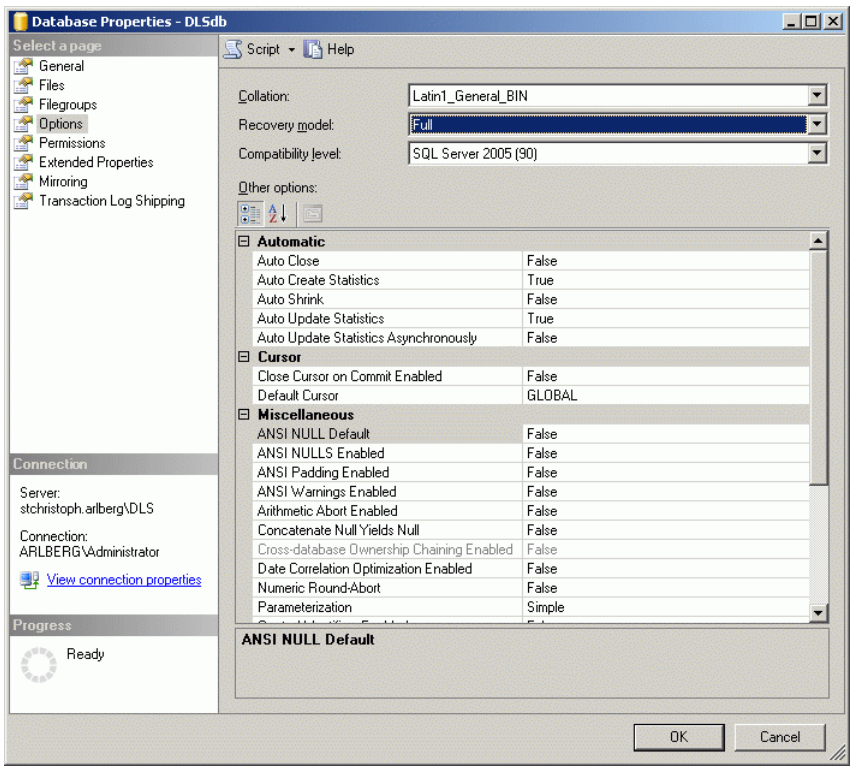




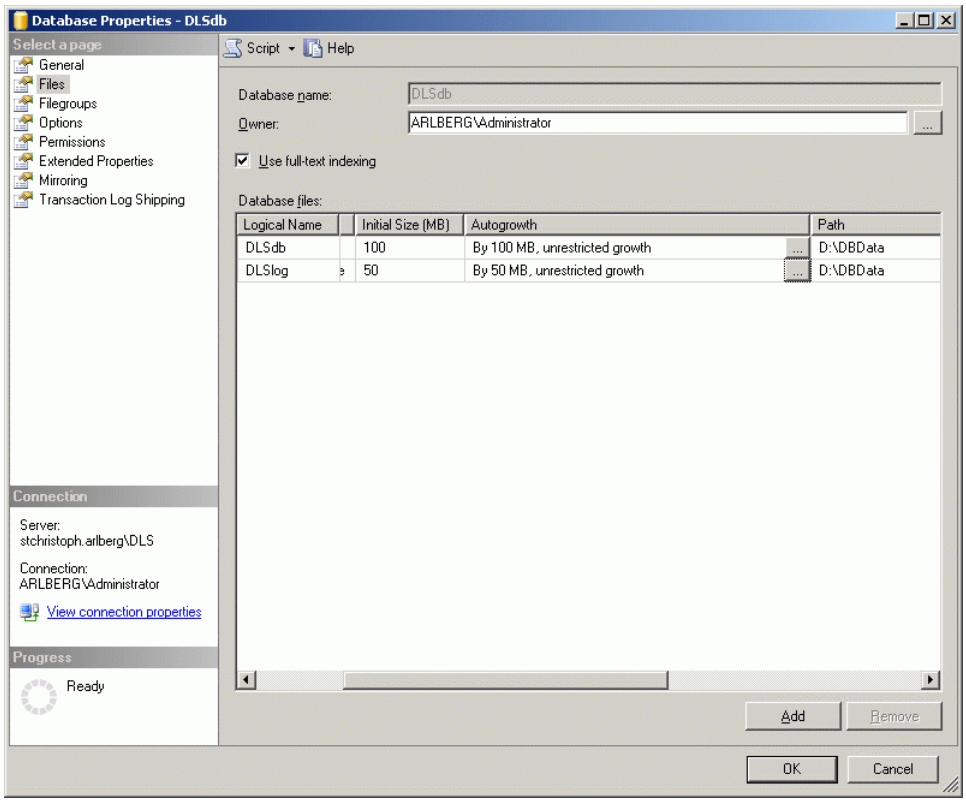
Sie erhalten eine Übersicht über die vorhandenen Datenbanken. Der Principal sollte der Datenbankrechner sein, der bei der Installation des DLS bereits angegeben wurde.


Microsoft SQL Server Management Studio
File Edit View Tools Window Community Help
New Query
Object Explorer
Connect
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
Object Explorer Details
DLSdb
STCHRISTOPH\DLS\Databases\DLSdb
8 Item(s)
Name
Database Diagrams
Tables
Views
Synonyms
Programmability
Service Broker
Storage
Security
Ready

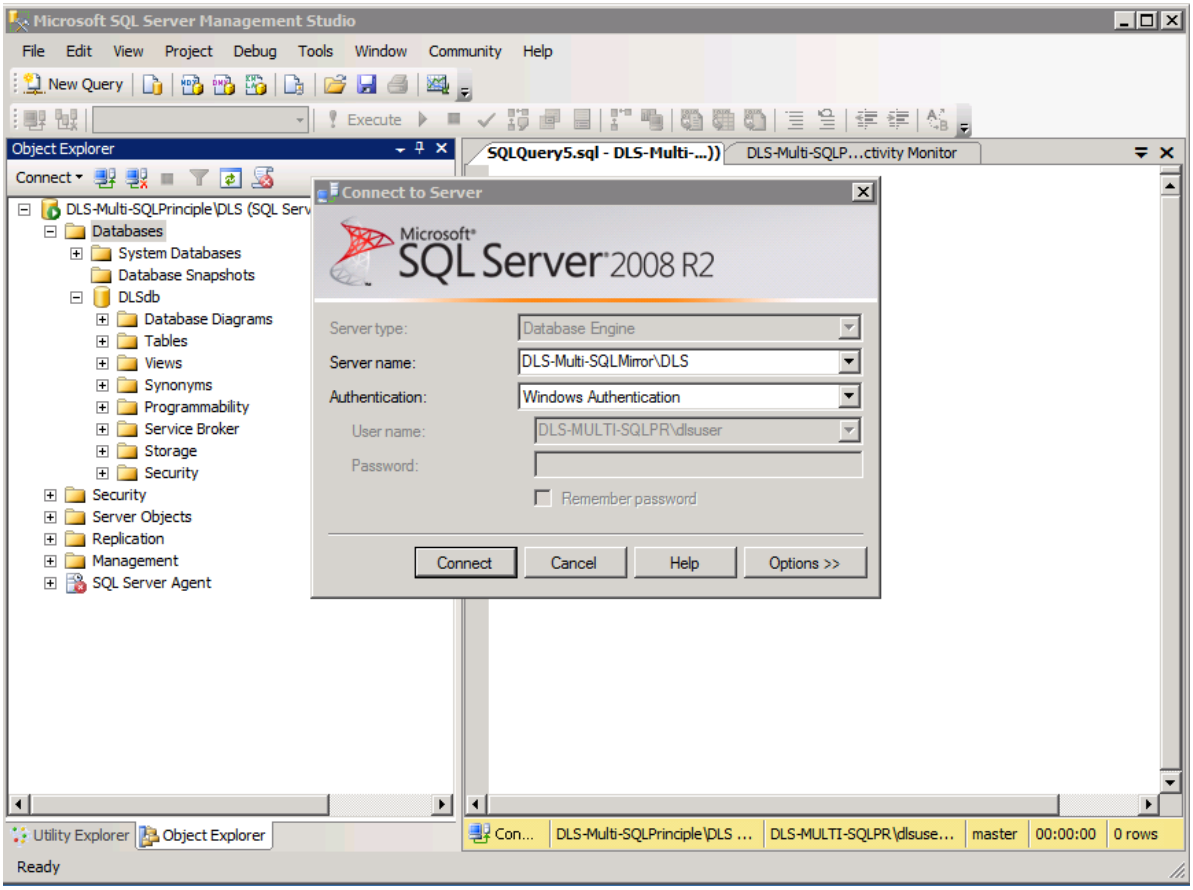
2. Gehen Sie auf den Baum auf der rechten Seite des MS SQL Server Management Studio und selektieren Sie den Eintrag **DLSdb**. Klicken Sie nun mit der rechten Maustaste auf **DLSdb** und wählen Sie im Kontextmenü **Properties**. Es öffnet sich das Fenster **Database Properties**. Im Untermenü **Options** wählen Sie unter **Recovery model** die Option **Full**.



3. Es wird empfohlen, im Untermenü **Files** eine unbeschränkte Dateigröße einzustellen, indem Sie für **DLSdb** und **DLSlog** die Option **unrestricted growth** wählen.

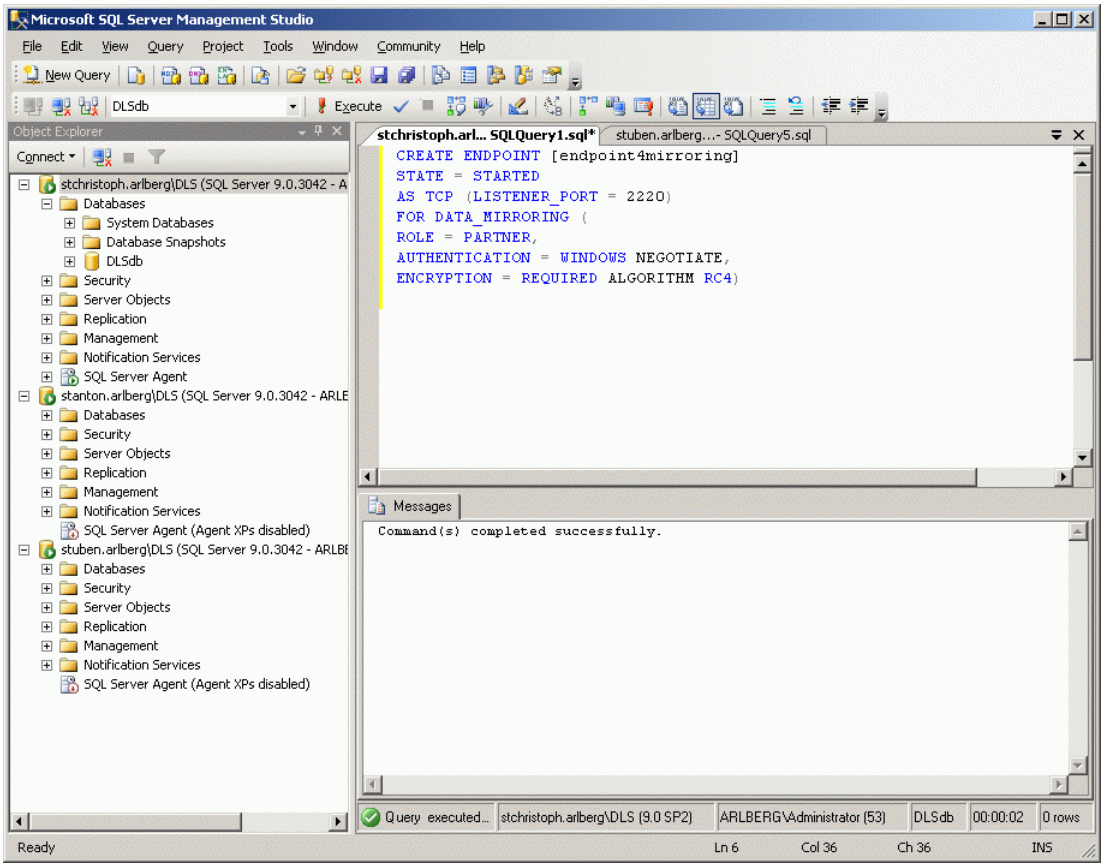


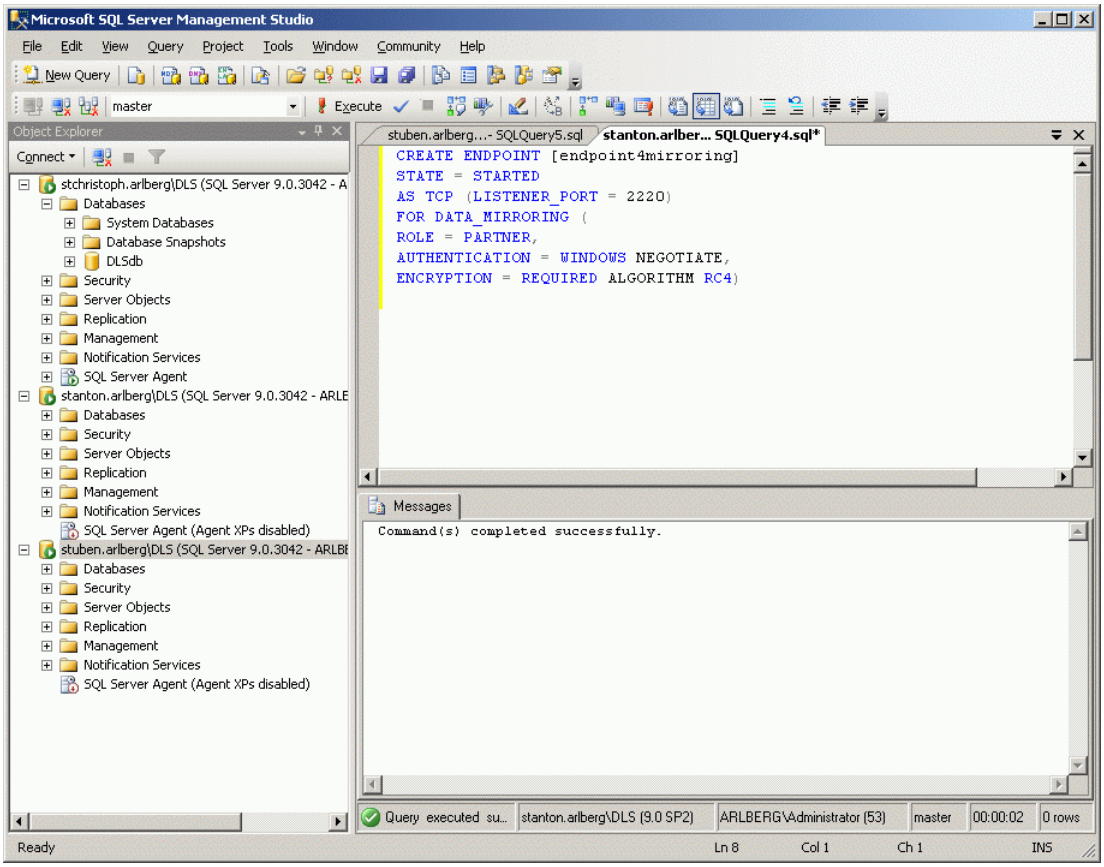
4. Geben Sie wie in Schritt 1 die Witness- und Mirror-Datenbanken an.



Legen Sie die beiden „Endpoints“ für die Datenbankspiegelung an, indem Sie auf dem Principal-Server und dem Mirror-Server die folgenden Kommandos ausführen:

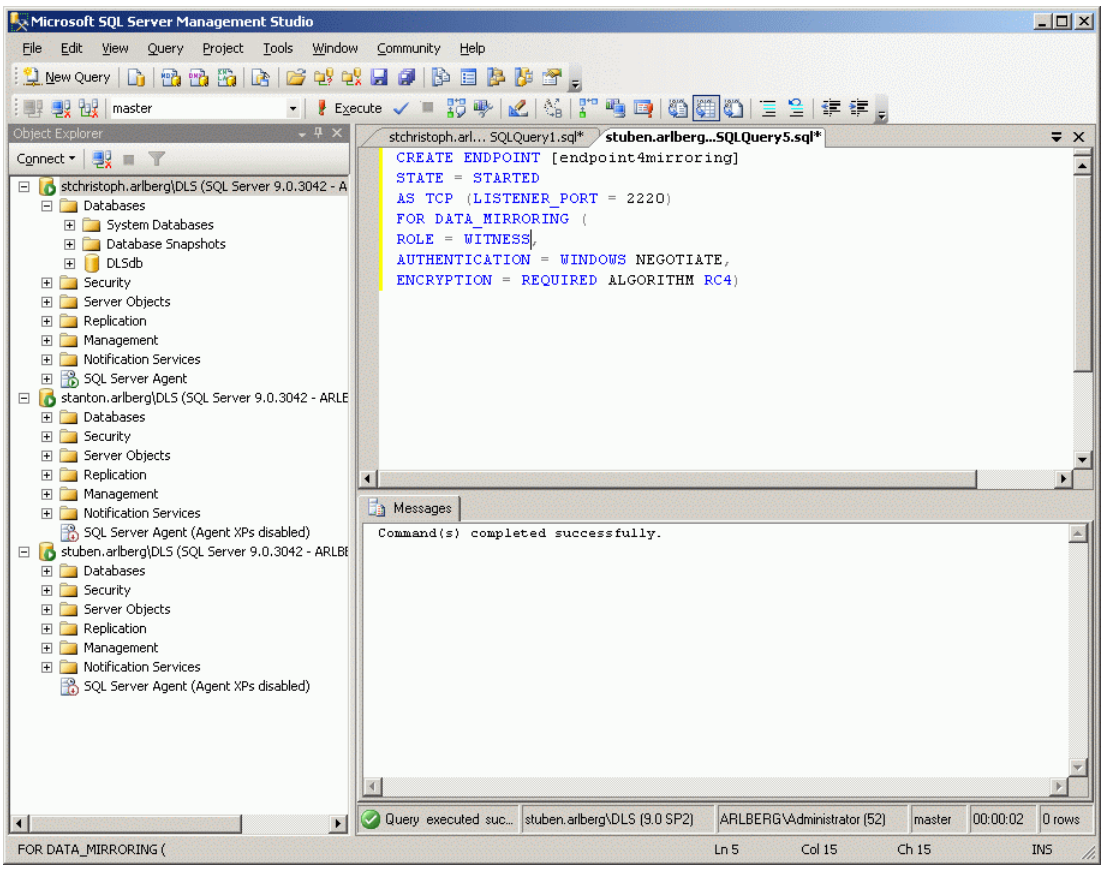
```
CREATE ENDPOINT [endpoint4mirroring]
   STATE = STARTED
   AS TCP (LISTENER_PORT = 2220, LISTENER_IP = ALL)
   FOR DATA_MIRRORING (
      ROLE = PARTNER,
      AUTHENTICATION = WINDOWS NEGOTIATE,
      ENCRYPTION = REQUIRED ALGORITHM RC4)
```


Microsoft SQL Server Management Studio
File Edit View Query Project Tools Window Community Help
New Query
DLSdb
Execute
Object Explorer
Connect
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
stanton.arlberg\DLS (SQL Server 9.0.3042 - ARLE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg\DLS (SQL Server 9.0.3042 - ARLBE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stchristoph.arl... SQLQuery1.sql*
stuben.arlberg...- SQLQuery5.sql
CREATE ENDPOINT [endpoint4mirroring]
STATE = STARTED
AS TCP (LISTENER_PORT = 2220)
FOR DATA_MIRRORING (
ROLE = PARTNER,
AUTHENTICATION = WINDOWS NEGOTIATE,
ENCRYPTION = REQUIRED ALGORITHM RC4)
Messages
Command(s) completed successfully.
Query executed...
stchristoph.arlberg\DLS (9.0 SP2)
ARLBERG\Administrator (53)
DLSdb
00:00:02
0 rows
Ready
Ln 6
Col 36
Ch 36
INS


Microsoft SQL Server Management Studio
File Edit View Query Project Tools Window Community Help
New Query
Execute
master
Object Explorer
Connect
stchristoph.arlberg\DLS (SQL Server 9.0.3042 - A
Databases
System Databases
Database Snapshots
DLSdb
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent
stanton.arlberg\DLS (SQL Server 9.0.3042 - ARLE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg\DLS (SQL Server 9.0.3042 - ARLBE
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)
stuben.arlberg...- SQLQuery5.sql
stanton.arlber... SQLQuery4.sql*
CREATE ENDPOINT [endpoint4mirroring]
STATE = STARTED
AS TCP (LISTENER_PORT = 2220)
FOR DATA_MIRRORING (
ROLE = PARTNER,
AUTHENTICATION = WINDOWS NEGOTIATE,
ENCRYPTION = REQUIRED ALGORITHM RC4)
Messages
Command(s) completed successfully.
Query executed su...
stanton.arlberg\DLS (9.0 SP2)
ARLBERG\Administrator (53)
master
00:00:02
0 rows
Ready
Ln 8
Col 1
Ch 1
INS

5. Legen Sie den Witness an, indem sie auf dem dafür vorgesehenen Rechner die folgenden Kommandos auführen:

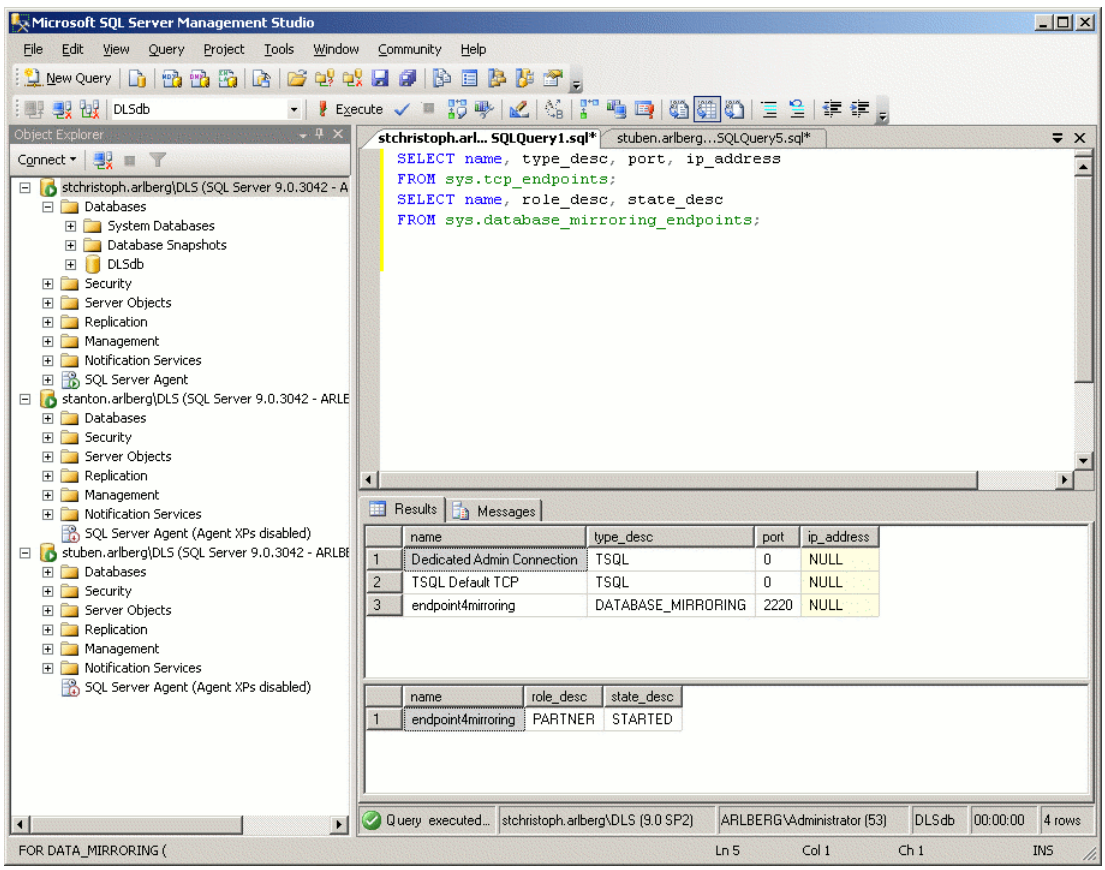
```
CREATE ENDPOINT [endpoint4mirroring]
   STATE = STARTED
   AS TCP (LISTENER_PORT = 2220, LISTENER_IP = ALL)
   FOR DATA_MIRRORING (
      ROLE = WITNESS,
      AUTHENTICATION = WINDOWS NEGOTIATE,
      ENCRYPTION = REQUIRED ALGORITHM RC4)
```



6. Sie können das Ergebnis ansehen, indem Sie auf allen drei Datenbankservern den folgenden Code ausführen:

```
SELECT name, type_desc, port, ip_address
   FROM sys.tcp_endpoints;
SELECT name, role_desc, state_desc
   FROM sys.database_mirroring_endpoints;
```

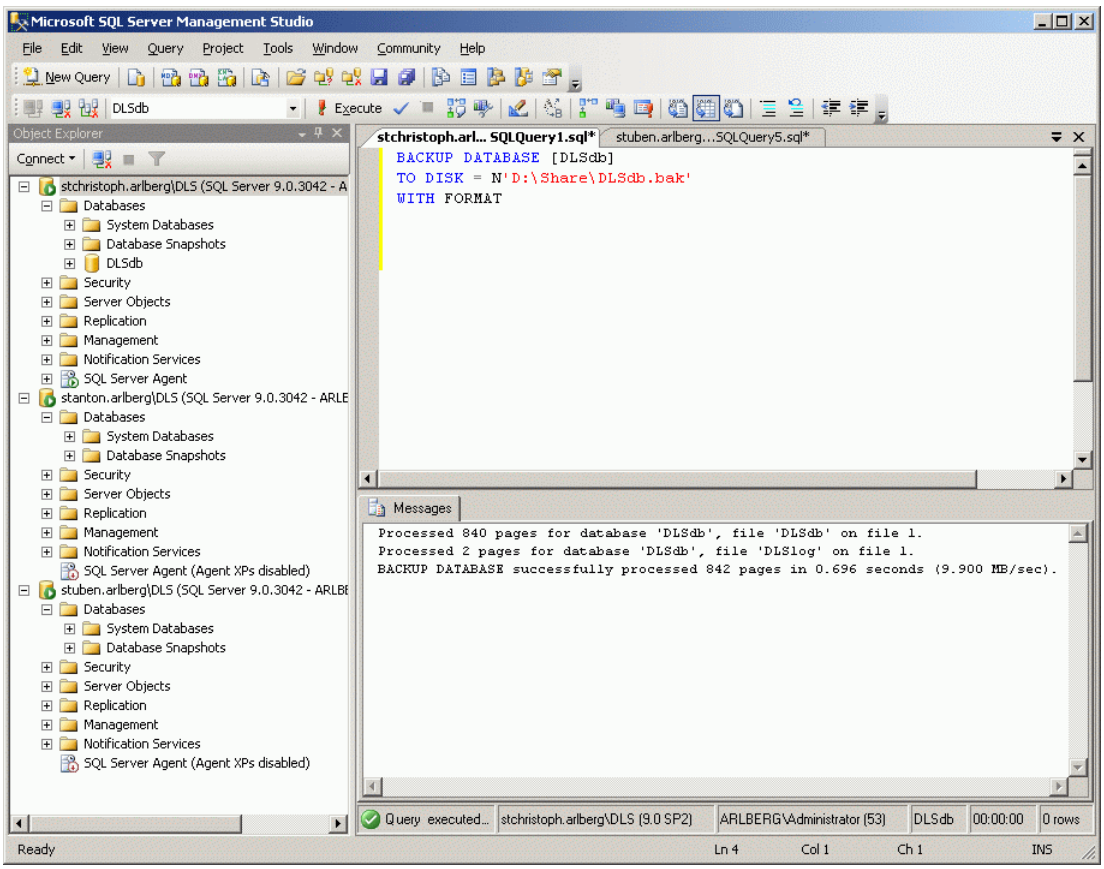
Der Screenshot zeigt beispielhaft die Ausgabe für den Principal.



7. Erstellen Sie nun eine Sicherung (Backup) der DLS-Datenbank auf dem Principal-Server:

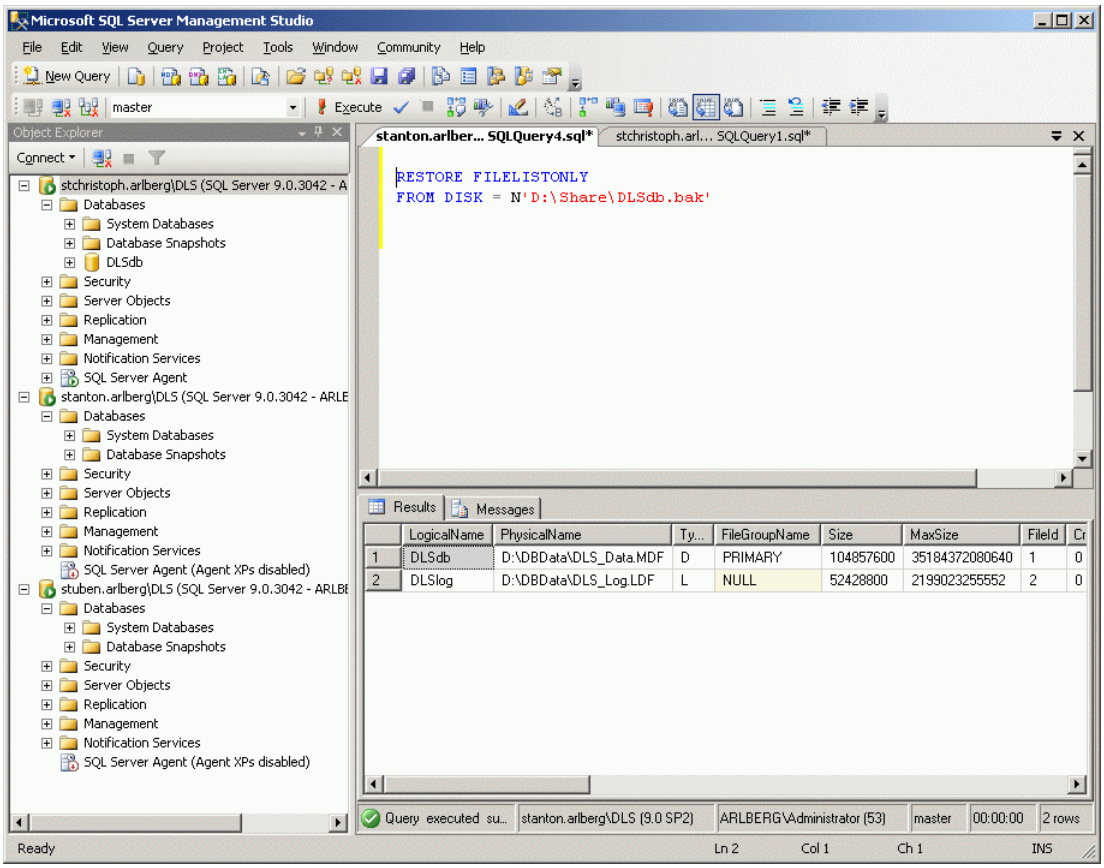
HINWEIS: Vor dem Ausführen der folgenden Abfrage müssen Sie sicherstellen, dass der Ordner ‘Share’ leer ist. Eine eventuell vorhandene Backup-Datei in diesem Ordner würde die Ausführung des Skripts verhindern.

```
BACKUP DATABASE [DLSdb]
   TO DISK = N’D:\Share\DLSdb.bak’
   WITH FORMAT
```



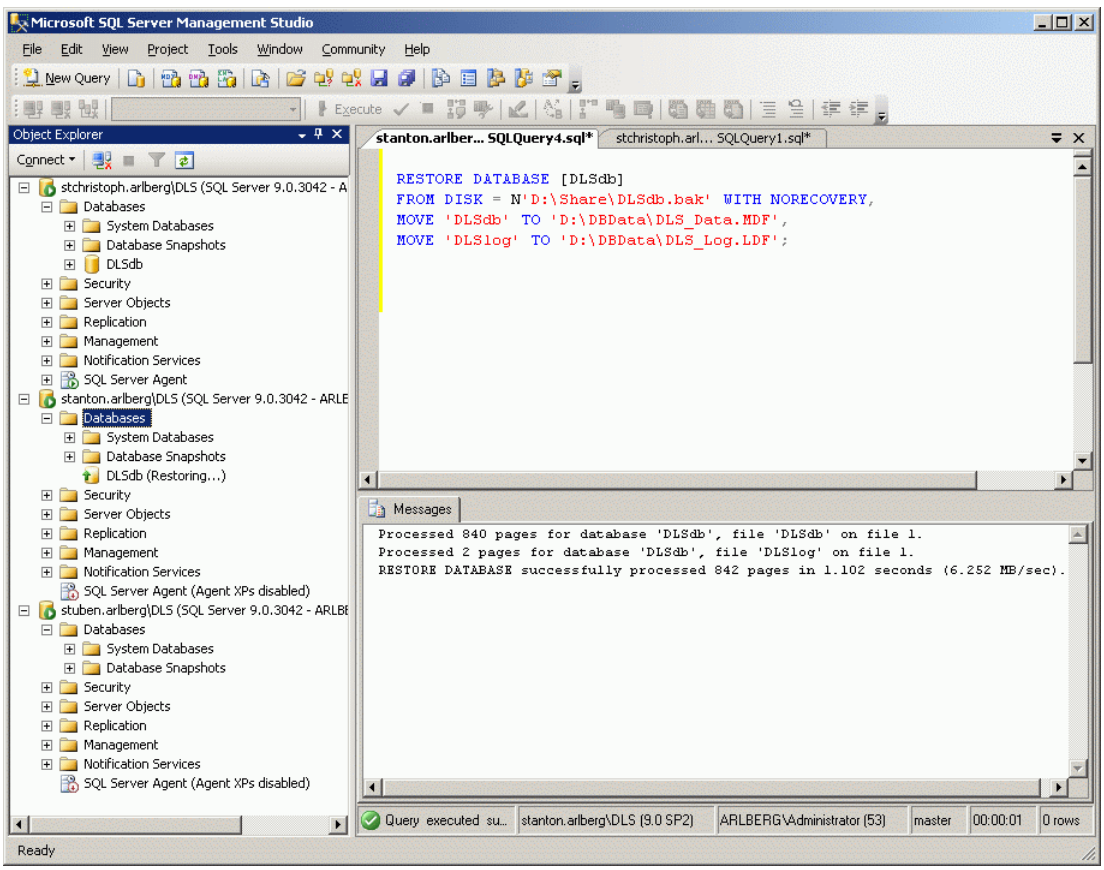
8. Um die Wiederherstellung der Datenbank auf dem Mirror-Server vorzubereiten, müssen Sie die logischen und physischen Namen der Backup-Dateien wissen. Geben Sie hierzu den folgenden Code ein:

```
RESTORE FILELISTONLY
   FROM DISK = N'\\<principal computer name>\share\DLSdb.bak'
```



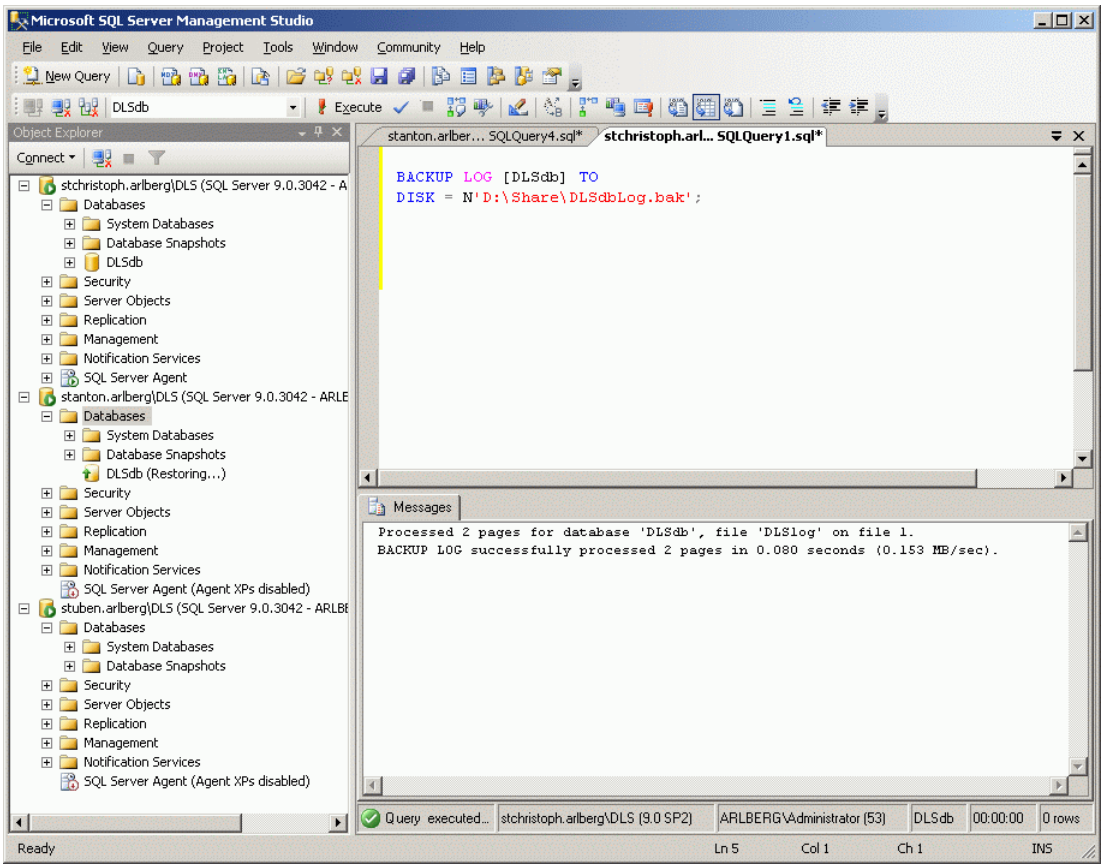
9. Mithilfe dieser Namen starten Sie nun die Wiederherstellung der Datenbank.

```
RESTORE DATABASE [DLSdb]
FROM DISK = N'\\<principal computer name>\share\DLSdb.bak' WITH NORECOVERY,
MOVE 'DLSdb' TO 'D:\DBData\DLS_Data.MDF',
MOVE 'DLSlog' TO 'D:\DBData\DLS_Log.LDF';
```



10. Auf dem Principal erstellen Sie ein Backup des initialen Transaktionsprotokolls.

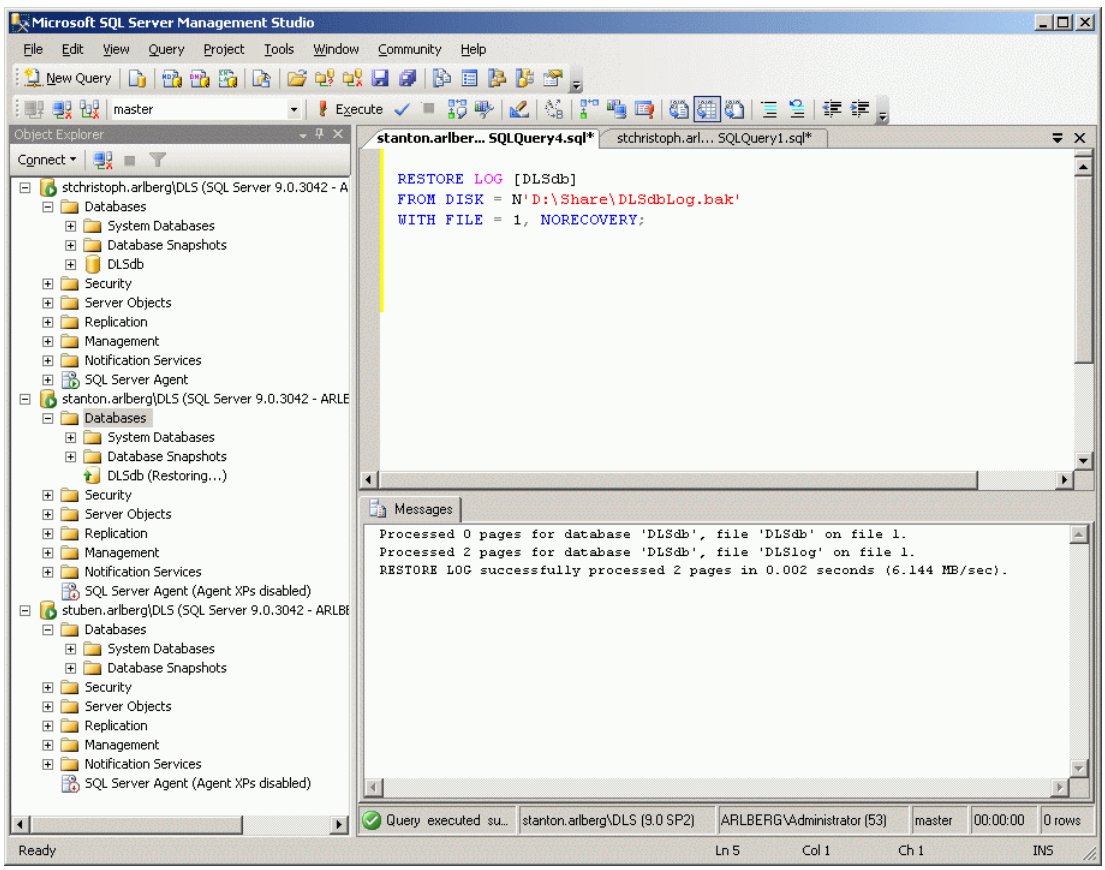
```
BACKUP LOG [DLSdb] TO
   DISK = N'D:\Share\DLSdbLog.bak';
```



Notieren Sie sich die Datei-ID im Meldungsfenster (im Beispiel: 1)

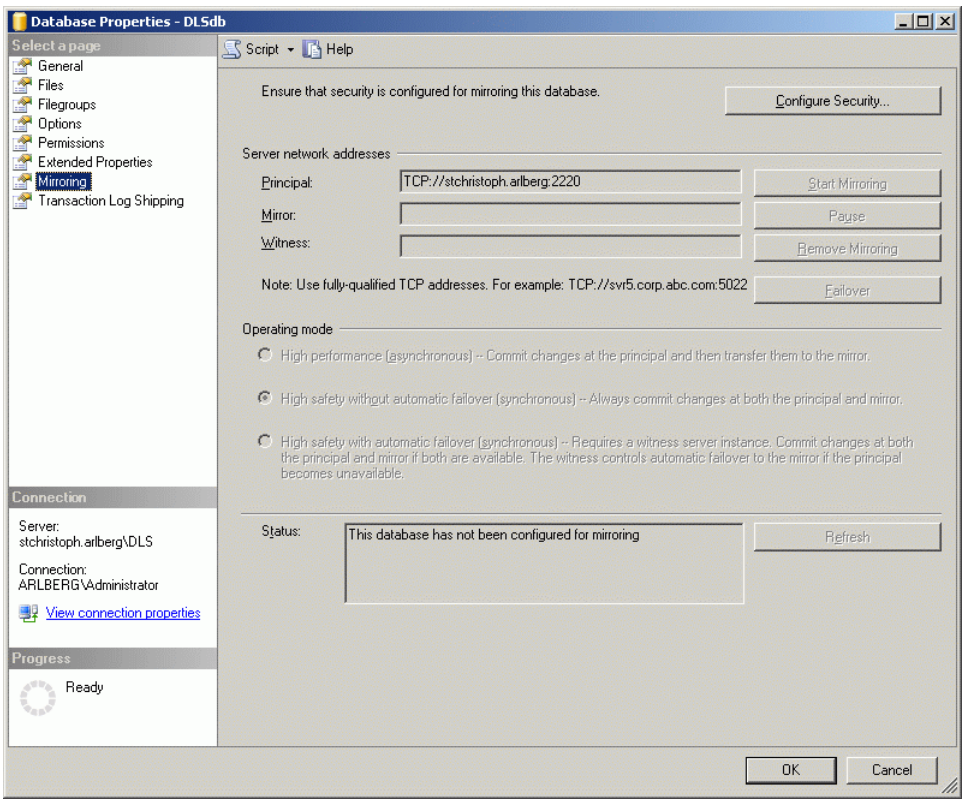
11. Nehmen Sie anschließend auf dem Mirror die Wiederherstellung des Transaktionsprotokolls vor. Die Datei-ID entnehmen Sie dem Meldungsfenster des vorangegangenen Backup-Vorgangs (siehe Schritt 10).

```
RESTORE LOG [DLSdb]
FROM DISK = N'\\<principal computer name>\share\DLSdbLOG.bak'
WITH FILE = 1, NORECOVERY;
```



12. Der DLS nutzt eigene Stored Procedures in der Master-Datenbank, die bei Backup und Restore der DLSdb nicht erfasst werden. Daher muss am Mirror das SQL-Skript `create_master_usp.sql` ausgeführt werden. Dieses Skript finden Sie in
`<DLS Installationsverzeichnis>\Tomcat5\webapps\DeploymentService\database\dbinstaller\mssql\DlsDb`

13. Um die Spiegelung zu starten, klicken Sie mit der rechten Maustaste auf die Datenbank **DLSdb**, gehen Sie auf das Untermenü **Tasks** und wählen dort **Mirror**.



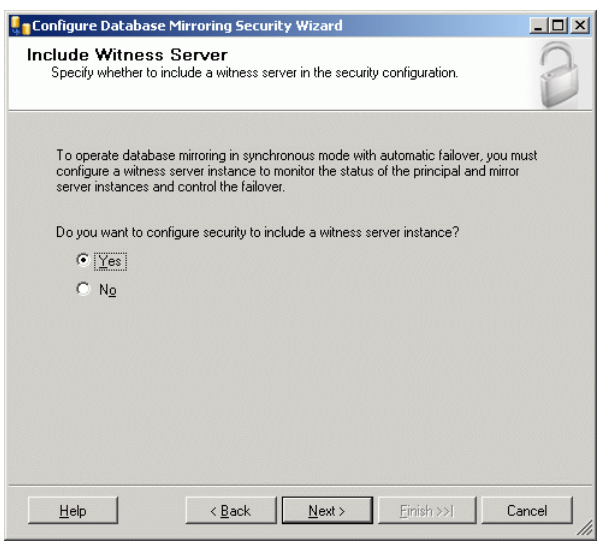
Klicken Sie auf **Configure Security...**.

WICHTIG: Wenn die Spiegelung deinstalliert wurde (z. B. infolge einer DB-Wiederherstellung oder eines DLS-Upgrades) und Sie möchten sie erneut installieren, müssen Sie sicherstellen, dass nur die DLS-Datenbank auf dem SQL-Spiegelserver (über SQL Management Studio) gelöscht wird. Wenn auf dem Spiegelserver noch eine ‘alte’ Datenbank existiert, schlägt die Spiegelung fehl.

14. Ein Wizard zur Konfiguration der Sicherheitseinstellungen für die Spiegelung öffnet sich.

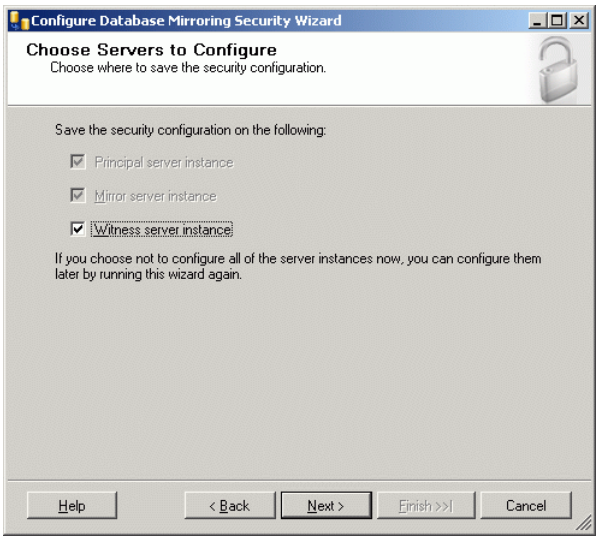
Klicken Sie auf **Next**.

15. Im Fenster **Include Witness Server** wählen Sie **Yes**.



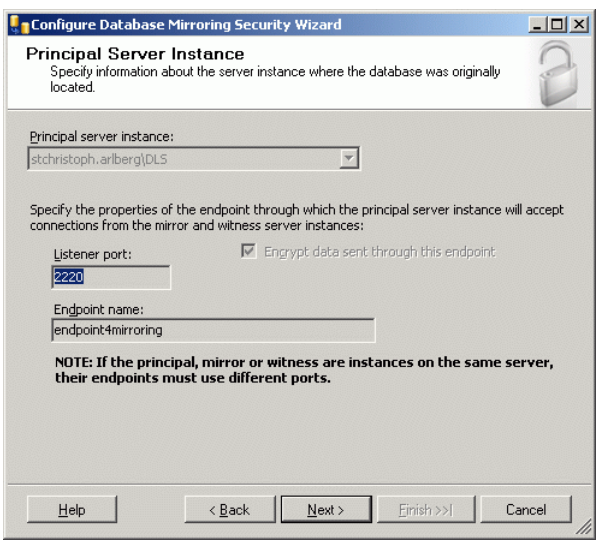
Klicken Sie auf **Next**.

16. Stellen Sie sicher, dass im Fenster **Choose Servers to Configure** die Option **Witness server instance** angewählt ist.



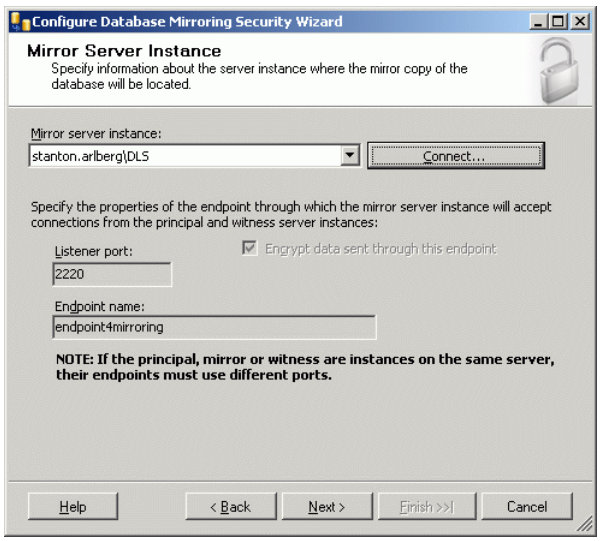
Klicken Sie auf **Next**.

17. Im Fenster **Principal Server Instance** überprüfen Sie die Einstellungen für den Principal-Server und ändern Sie gegebenenfalls. Wichtig ist insbesondere, dass der im Feld **Listener port** angegebene Port, der bei der Rollenvergabe (Schritte 4, 5) festgelegt wurde, nicht anderweitig vergeben ist.



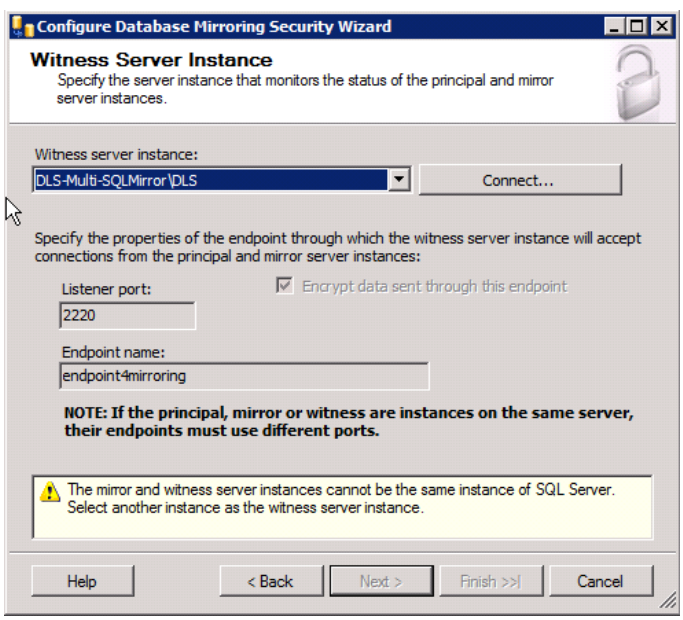
Klicken Sie auf **Next**.

18. Analog zum Principal-Server überprüfen Sie im Fenster **Mirror Server Instance** die Einstellungen für den Mirror-Server und ändern diese gegebenenfalls. Vor Änderung der Einstellungen muss sichergestellt sein, dass die Verbindung zum Mirror-Server steht. Klicken Sie auf Connect.



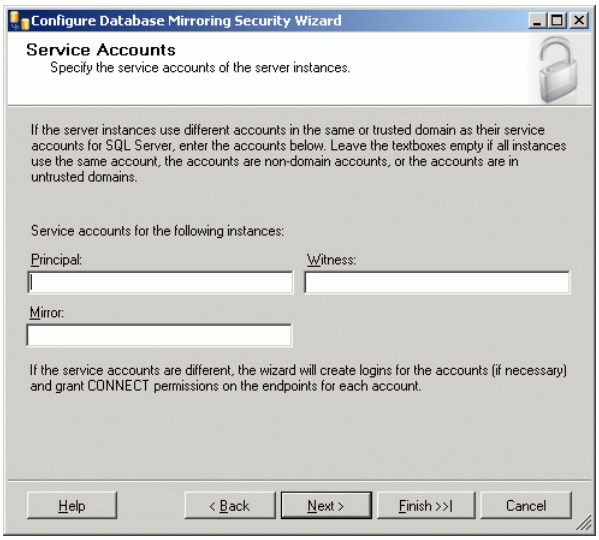
Klicken Sie auf **Next**.

19. Analog zum Principal-Server überprüfen Sie im Fenster **Mirror Server Instance** die Einstellungen für den Witness-Server und ändern diese gegebenenfalls. Vor Änderung der Einstellungen muss sichergestellt sein, dass die Verbindung zum Mirror-Server steht. Klicken Sie auf Connect.



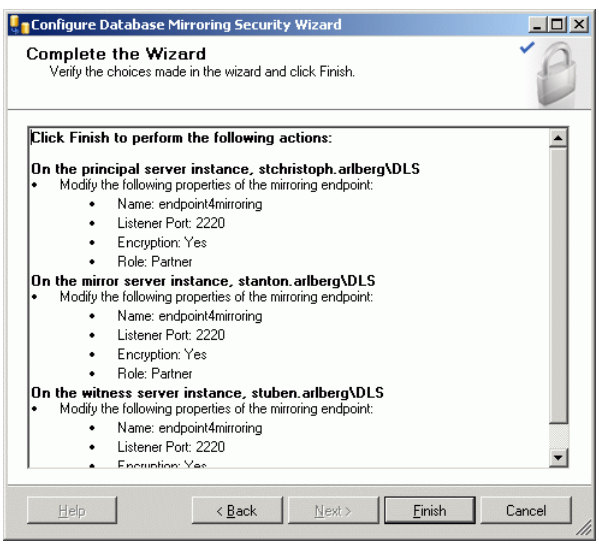
Klicken Sie auf **Next**.

20. Im Fenster **Service Accounts** müssen Sie nichts eintragen, da alle drei Serverinstanzen unter demselben Account laufen.



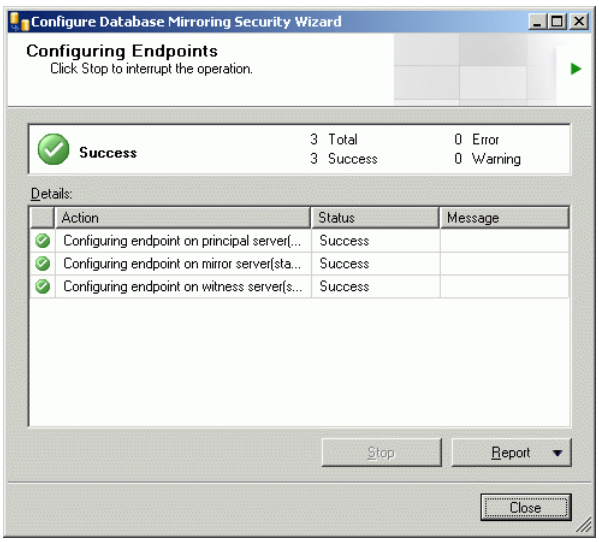
Klicken Sie auf **Next**.

21. Im Fenster **Complete the Wizard** können Sie die Einstellungen für die drei Serverinstanzen abschließend überprüfen.



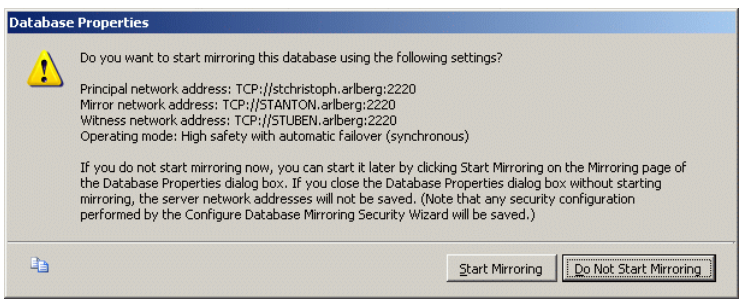
Klicken Sie auf **Finish**.

22. Das Fenster **Configuring Endpoints** gibt über den Fortschritt der Konfiguration Auskunft.



Wenn der Vorgang beendet ist, klicken Sie auf **Close**.

23. Starten Sie die Spiegelung mit **Start Mirroring**. Die gespiegelte SQL-Datenbank ist einsatzbereit.



24. Sie können die Datenbankspiegelung überwachen, indem Sie im Hauptfenster des Microsoft SQL Server Management Studio mit der rechten Maustaste auf **DLSdb** klicken und im Untermenü **Tasks** die Option **Launch Database Mirroring Monitor...** wählen.

    Des weiteren besteht die Möglichkeit, die Spiegelung während des laufenden Betriebs abzuschalten. Hierzu klicken Sie im Hauptfenster des Microsoft SQL Server Management Studio mit der rechten Maustaste auf **DLSdb**, wählen im Untermenü **Tasks** die Option **Mirroring** und klicken den Button **Remove Mirroring**.

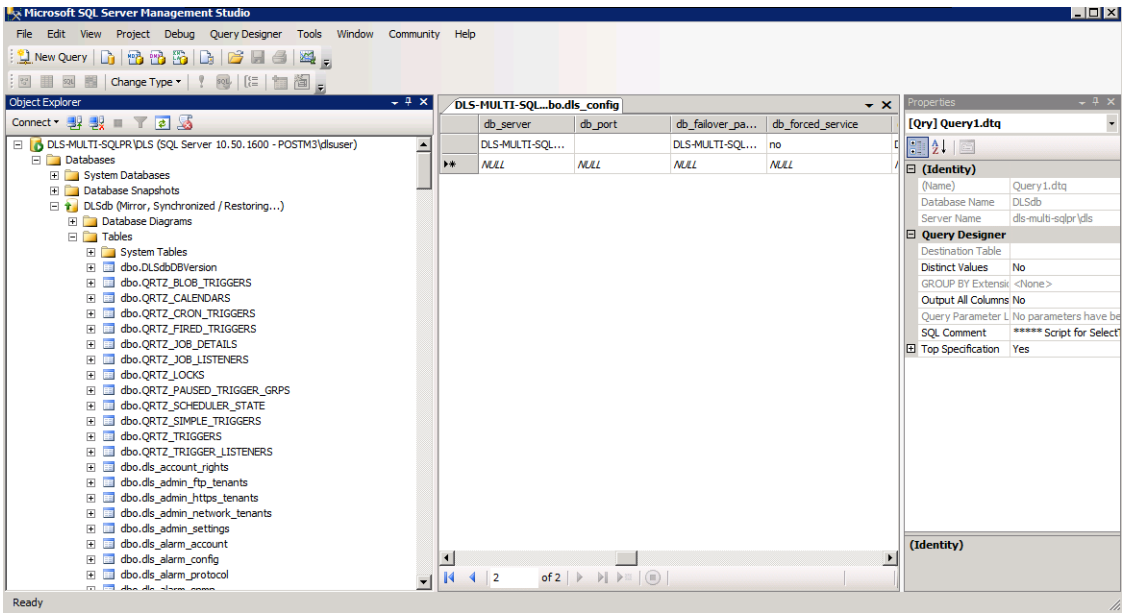
HINWEIS: Wenn die beiden Datenbank-Dateien (`DLSdb.bak`, `DLSdbLog.bak`) (nach dem Entfernen der Spiegelung) aus dem Ordner „\Share“ des Principal-Server gelöscht werden, ist eine Neukonfigurierung der Spiegelung nicht mehr möglich.

Beim **SQL Database Mirroring Setup** im **Asynchronous**-Modus sind folgende Schritte erforderlich:

4. Stoppen Sie die Spiegelung der MSSQL-Datenbank, indem Sie auf die Schaltfläche **Remove Mirroring** klicken.

5. Gehen Sie auf dem Principal-SQL-Server zu **Start** > **Microsoft SQL Server 2005/2008** > **Microsoft SQL Server Management Studio** > **Databases** >**DLSDbTables** > `dbo.dls_config`

   Öffnen Sie dieses Skript, gehen Sie zu db_forced_service und ändern Sie **No** auf **Yes** .



6. Starten Sie die Spiegelung ohne Zeuge (Witness), indem Sie mit der rechten Maustaste auf die Datenbank **DLSdb** klicken, navigieren Sie zum Untermenü **Tasks** und wählen Sie dort den Eintrag **Mirror** aus (befolgen Sie anschließend Schritt 13 und die darauf folgenden Schritte bis zum Ende der Installation).

Näheres zu weiteren Möglichkeiten finden Sie in der Dokumentation zum Microsoft SQL Server 2005 / 2008 Enterprise Edition.

4.7 DLS-Datenbank-Wiederherstellung in einer Multi-Node-Umgebung

Zum Wiederherstellen von Datenbank-Backups bei DLS-Multi-Node-Bereitstellungen gehen Sie folgendermaßen vor:

1. Entfernen Sie die Datenbankspiegelung (sofern vorhanden). Hierzu klicken Sie im Hauptfenster des Microsoft SQL Server Management Studio mit der rechten Maustaste auf **DLSdb**, wählen im Untermenü **Tasks** die Option **Mirroring** und klicken den Button **Remove Mirroring**.

   WICHTIG: Klicken Sie auf keinen Fall auf die Schaltfläche **Pause Mirroring**.

2. Stoppen Sie alle DLS-Knoten außer dem DLS-Knoten, auf dem der Wiederherstellungsvorgang läuft.

3. Stellen Sie das Datenbank-Backup wieder her (Restore).

   HINWEIS: Verwenden Sie für die Durchführung der Datenbank-Wiederherstellung die Adresse (IP / FQDN oder Hostname) des einzigen aktiven DLS-Knotens, da die virtuelle IP-Adresse oder der FQDN nicht richtig funktionieren.

4. Melden Sie sich am aktiven DLS-Knoten an (IP-Adresse oder Hostname) und starten Sie alle zuvor angehaltenen DLS-Knoten.

5. Konfigurieren Sie die Datenbankspiegelung wie in Abschnitt 4.6, “Spiegelung der SQL-Datenbank aufsetzen” beschrieben (falls eine Spiegelung vorhanden ist).

4.8 Upgrade von DLS-Multi-Node-Umgebungen

Beim Upgrade von DLS-Multi-Node-Bereitstellungen ist Folgendes zu beachten:

- Führen Sie immer zuerst eine Sicherung der DLS-Datenbank durch. Dann können Sie beim Auftreten von Fehlern gegebenenfalls auf einem früheren Stand der Datenbank aufsetzen.
- Führen Sie eine einfache Updateinstallation aller Knoten durch (wie im Rahmen regelmäßiger Single-Node-Upgrades erforderlich).
- Stellen Sie sicher, dass die Installation nicht gleichzeitig auf allen Knoten, sondern immer nacheinander auf jedem Knoten einzeln ausgeführt wird.
- Führen Sie während des Upgrades möglichst wenige Aktionen aus, die den Network Load Balancer, den bzw. die SQL-Server, Client-Verbindungen zum DLS und das Leistungsmerkmal Mobility beanspruchen.

HINWEIS: Bei diesem einfachen Upgrade-Szenario besteht keine Notwendigkeit, die Spiegelung anzuhalten und neu zu konfigurieren; darüber hinaus ist auch keine Wiederherstellung erforderlich.

4.9 DLS starten

Bevor Sie den DLS-Cluster starten, stellen Sie sicher, dass alle Rechner zeitsynchron laufen. Bei Verwendung des in Windows 2003 Server enthaltenen DNS-Servers ist dies der Fall, denn hier wird die Zeit vorgegeben. Sollten Sie mit einer Workgroup anstelle dieses DNS-Servers arbeiten, müssen Sie die Zeitsynchronität mit anderen Mitteln garantieren.

1. Starten Sie den DLS jeweils auf den einzelnen Knoten.
2. Starten Sie den Cluster mithilfe des Network Load Balancer Manager.

HINWEIS: Falls Sie einen DLS-Knoten herunterfahren wollen, etwa für Wartungszwecke, entfernen Sie den Rechner zuerst mithilfe des Network Load Balancer Manager aus dem Cluster. So ist sichergestellt, dass keine Anfragen mehr von dieser DLS-Instanz empfangen werden.

4.10 Erstkonfiguration

Für die Erstkonfiguration des DLS empfiehlt es sich, folgende Bereiche der Reihe nach zu konfigurieren:

1. **Passwort ändern / Account einrichten**

   Aufruf: Hauptmenü > Administration > Account Management > Account Konfiguration

   Falls erforderlich, ändern Sie das bei der Installation vergebene Admin-Passwort und richten Sie ggf. weitere Accounts ein.

   Eine Beschreibung der Felder finden Sie im Abschnitt 6.1, “Account Management”.

2. **FTP Server Konfiguration**

   Aufruf: Hauptmenü > Administration > Server Konfiguration > FTP Server Konfiguration

   Geben Sie die Daten für die Verbindung zu einem oder mehreren FTP-Servern ein.

   Die Verbindung zu einem FTP-Server ist für den Download von IP Phone-Software erforderlich.

   Eine Beschreibung der Felder und weitere Hinweise finden Sie im Abschnitt 6.3.4, “FTP Server Konfiguration”.

3. **HTTP Server Konfiguration**

   Aufruf: Hauptmenü > Administration > Server Konfiguration > HTTPS Server Konfiguration

   Geben Sie die Daten für die Verbindung zu einem oder mehreren HTTPS-Servern ein.

   OpenStage-Endgeräte können für den Download von IP Phone-Software einen HTTPS-Server alternativ zu einem FTP-Server verwenden.

   Eine Beschreibung der Felder und weitere Hinweise finden Sie im Abschnitt 6.3.5, “HTTPS Server Konfiguration”.

4. **Netzlaufwerk Konfiguration**

   Aufruf: Hauptmenü > Administration > Server Konfiguration > Netzlaufwerk Konfiguration

   Geben Sie die Daten für das Windows-Netzlaufwerk ein.

   Die Angaben zum Windows-Netzlaufwerk sind für den Download von IP Client-Software erforderlich.

   Eine Beschreibung der Felder und weitere Hinweise finden Sie im Abschnitt 6.3.7, “Netzlaufwerk Konfiguration”.

5. **Einstellungen (Protokollierung)**

   Aufruf: Hauptmenü > Administration > Protokoll-Daten > Aktivitäten- und Fehlerprotokoll ODER > P&P Import Protokolle

   Ändern Sie ggf. die Angaben, welche Ereignisse protokolliert werden und wie lange die Protokolldaten gespeichert werden sollen.

   Eine Beschreibung der Felder und weitere Hinweise finden Sie im Abschnitt 6.5, “Protokoll-Daten”.

6. **Import Templates**

   Aufruf: Hauptmenü > Profil Management > Template Übersicht > Register „Template-Daten“

   Sie haben die Möglichkeit, bereits vorhandene und in ZIP-Dateien gespeicherte DLS-Templates zu laden.

   Mehr zum Thema „Template“ finden Sie im Abschnitt 15.4, “Templates bearbeiten”.

7. **Element Manager**

   Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration

   Wählen Sie unter **Element Manager Typ** den Typ des zu konfigurierenden Element Managers aus. Die Konfigurationsmöglichkeiten finden Sie unter Abschnitt , “Element Manager”.

4.11 Starten des DLS-Clients

4.11.1 Aufruf des Clients

Bevor Sie den DLS starten, sollten Sie die Erstkonfiguration vorgenommen haben (siehe Abschnitt 4.10, “Erstkonfiguration”).

Rufen Sie den DLS-Client wie folgt auf:

- Am Server-Rechner:
  - Über das Windows-Startmenü **Start** > **Programme** > **Deployment Service** > **DeploymentService**.
  - Mittels Programmverknüpfung **DeploymentService** auf dem Desktop.
- Am Client-Rechner:
  - Über folgende URL im Web-Browser:
    http://[IP-Adresse]:18080/DeploymentService/
    oder
    https://[IP-Adresse]:10443/DeploymentService/ (für verschlüsselte Verbindung)

Informationen zur Bedienung des DLS-Clients finden Sie ab dem Kapitel 5.

4.12 Installieren von Netzwerk-Komponenten

Im Normalfall sind die hier beschriebenen Netzwerk-Komponenten bereits vorhanden. Falls eine oder mehrere Komponenten jedoch nachinstalliert werden müssen, finden Sie in diesem Kapitel die entsprechende Beschreibung dazu.

Folgende Komponenten sind beschrieben:

- FTP Server
- HTTPS-Server
- Allgemeines zu DHCP
- DHCP-Server in einer Windows-Umgebung
- DHCP-Server in einer Linux/Unix-Umgebung
- DNS-Server für DLS konfigurieren
- DHCP Server mit Infoblox Appliance

4.12.1 FTP Server

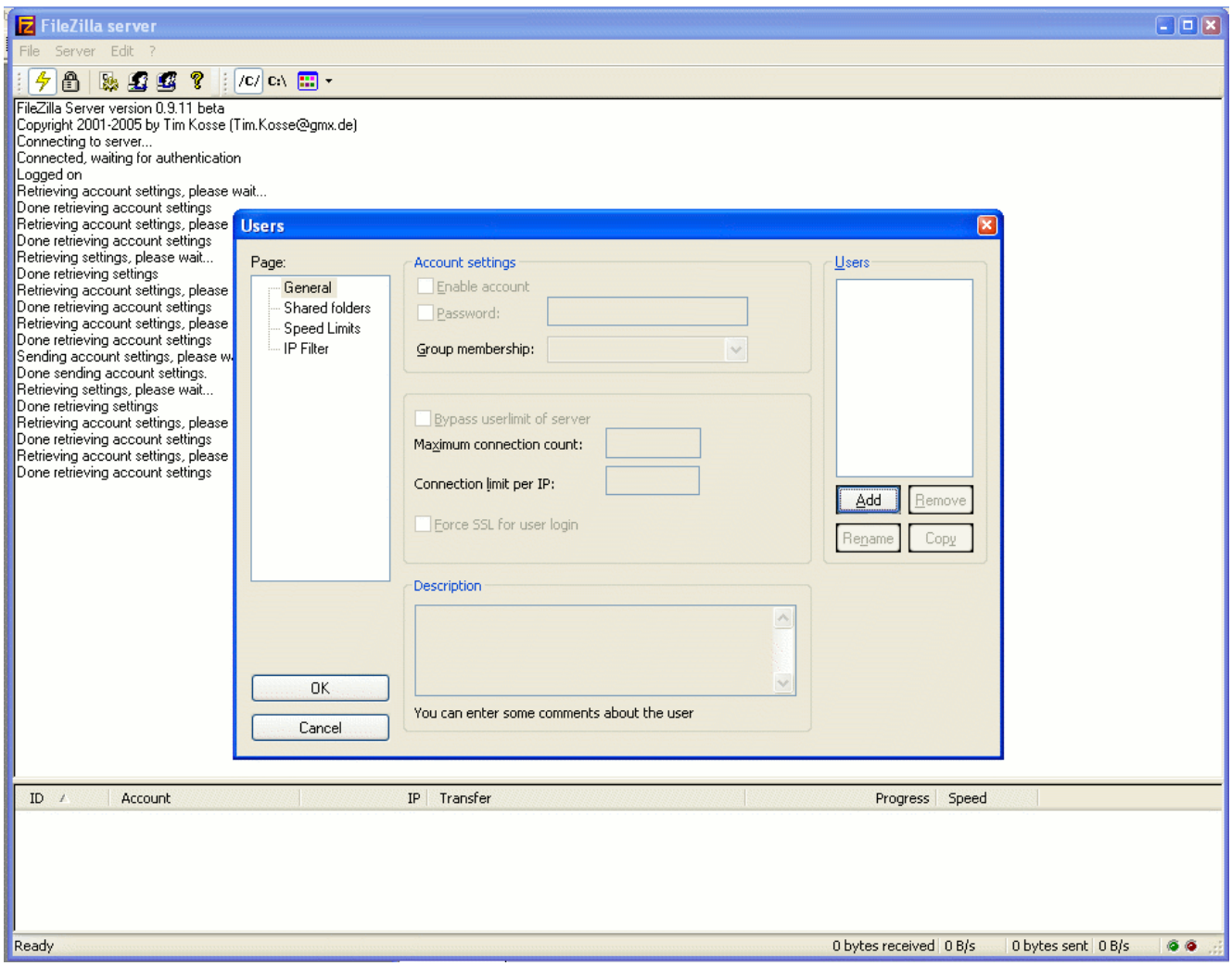
Nachfolgend ist beispielhaft das Einrichten des Server-Programms *FileZilla* beschrieben.

4.12.1.1 Installation und Konfiguration

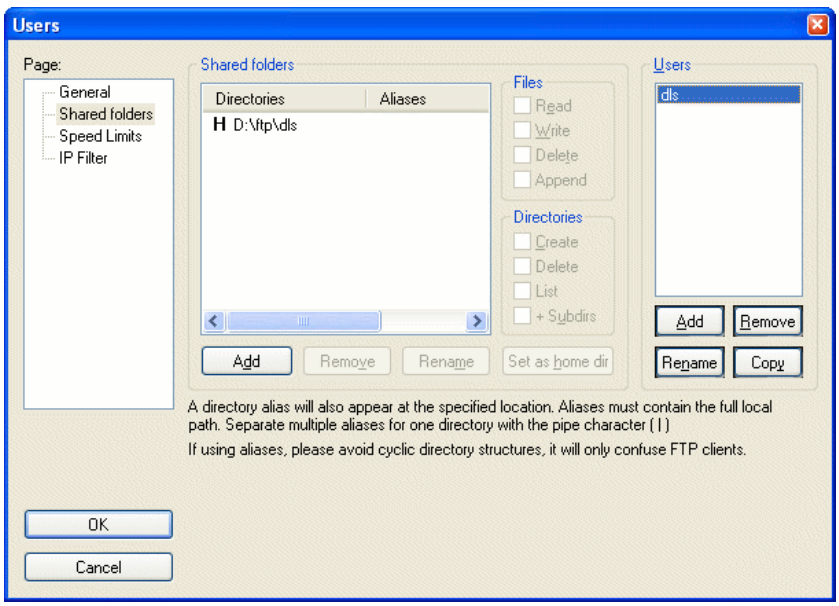
Installieren Sie die Software (im Beispiel *FileZilla Server*, downloadbar von http://sourceforge.net/projects/filezilla/).

Starten Sie das Server-Programm.

Richten Sie einen Benutzer ein. Öffnen Sie hierzu im Menü **Edit** > **Users**. Im Bereich **Page** muss **General** ausgewählt sein. Klicken Sie auf den Button **Add** unter dem linken Teil des Dialogfensters. Es öffnet sich ein Eingabefenster, in dem Sie den Benutzernamen eingeben. Die Option **Enable account** im Bereich **Account Settings** muss aktiviert sein. Soll der Benutzer ein Passwort erhalten, aktivieren Sie im selben Bereich die Option **Password** und geben Sie ein Passwort ein.



Um dem neu erstellten Benutzer ein Verzeichnis zuzuweisen, wählen Sie im Bereich **Page** den Eintrag **Shared Folders** aus und klicken Sie auf **Add**. Wählen Sie im sich nun öffnenden Fenster das Verzeichnis, in dem Sie die Software-Unterverzeichnisse ablegen wollen. Im Bereich **Files** muss die Option **Read** aktiviert sein, um dem DLS Lesezugriff zu ermöglichen.



Klicken Sie auf **OK**. Der FTP-Server steht nun zur Verfügung. Im Statusfenster des Servers werden die gerade aktuellen Verbindungen angezeigt.

4.12.2 HTTPS-Server

Die Endgeräte der OpenStage-Familie unterstützen den Download von Dateien über HTTPS. Um diese Möglichkeit zu nutzen, ist die Installation eines HTTPS-Servers erforderlich. Zur Installation konsultieren Sie bitte die Anweisungen zur jeweiligen Software.

4.12.3 Allgemeines zu DHCP

Die IP Phones verfügen über einen DHCP-Client, so dass die zu einem vollständigen Plug&Play benötigten Parameter per DHCP übermittelt werden können.

Neben den standardmäßigen Parametern IP-Adresse, Netzmaske und Default-Router sind folgende Optionen über DHCP konfigurierbar:

- IP Routing/Route 1 & 2 (Option 33)
- IP-Adresse des SNTP-Servers (Option 42)
- Zeitzonenverschiebung (Option 2)
- IP-Addressen des primären und sekundären DNS-Servers (Option 6)
- DNS Domain Name des Telefons (Option 15)
- IP-Adressen von SIP-Server und SIP-Registrar (Option 120)

Bei Unify IP Phones können in den Vendor-spezifischen Parametern die IP-Adresse des DLS sowie die VLAN-ID übermittelt werden.

Die VLAN ID-Zuweisung per DHCP arbeitet beim optiPoint 410/420 auf folgende Weise:

Wenn im Telefon die VLAN-Methode „DHCP“ eingestellt ist und QoS auf Layer 2 eingeschaltet ist, wird die VLAN ID von einem DHCP-Server zugewiesen. Dieser Vorgang umfasst zwei Schritte. Im ersten Schritt versucht das Telefon, über eine *discover*-Meldung mit der Herstellerklasse (*vendor class*) „OptiPoint“ eine IP-Adresse von einem DHCP-Server zu beziehen. Im zweiten Schritt sendet das Telefon eine getaggte *discover*-Meldung in dem VLAN, dessen ID es im ersten Schritt erhalten hat. Diesmal wird die Herstellerklasse „OptiIpPhone“ verwendet.

Steht die VLAN-Methode auf „manuell“, wird vom Telefon nur eine lease mit der Herstellerklasse „OptiIpPhone“ bezogen.

4.12.4 DHCP-Server in einer Windows-Umgebung

Das Betriebssystem Windows 2008 Server bzw. Windows 2003 Server beinhaltet die Komponente DHCP Server.

Dieser Abschnitt beschreibt das Einrichten und Konfigurieren eines neuen Windows 2008-DHCP-Servers in einer Windows 2008 Active Directory-Domäne. Der Windows 2008-DHCP-Dienst stellt Clients IP-Adressen sowie Informationen zu dem Standort des jeweiligen Standard-Gatekeepers, des DNS-Servers und des WINS-Servers zur Verfügung.

HINWEIS: Es wird empfohlen, einen DHCP-Server im DLS-Umfeld einzusetzen, um
- vollständiges Plug&Play zu unterstützen und
- die Authentizität des DLS-Servers sicherzustellen.

4.12.4.1 Installation

Sie können DHCP entweder während oder nach der ursprünglichen Installation von Windows 2008 Server oder Advanced Server installieren. Es ist jedoch ratsam, einen funktionierenden DNS-Server in der Umgebung zu konfigurieren. Damit ist es möglich, aktives DNS-Forwarding per DHCP durchzuführen.

Klicken Sie zum Überprüfen des DNS-Servers auf **Start**, klicken Sie auf **Ausführen**, geben Sie `cmd` ein, drücken Sie die <EINGABETASTE>, geben Sie ping [angezeigter Name des DNS-Servers] in Ihrer Umgebung ein und drücken Sie anschließend die <EINGABETASTE>. Bei einer nicht erfolgreichen Abfrage wird in der Antwort die Meldung „Unbekannter Host [DNS-Servername]“ angezeigt.

Gehen Sie folgendermaßen vor, um den DHCP-Dienst auf einem vorhandenen Windows 2008-Server zu installieren:

1. Wählen Sie aus dem Windows-Startmenü **Start** > **Einstellungen** > **Systemsteuerung**.
2. Doppelklicken Sie auf **Software**, und wählen Sie dann die Option **Windows-Komponenten hinzufügen/ entfernen**.
3. Klicken Sie im **Assistenten für Windows-Komponenten** im Feld **Komponenten** auf **Netzwerkdienste**, und klicken Sie dann auf **Details**.
4. Aktivieren Sie den Schalter **DHCP (Dynamic Host Configuration Protocol)**, wenn es nicht bereits aktiviert ist, und klicken Sie anschließend auf **OK**.
5. Klicken Sie im **Assistenten für Windows-Komponenten** auf **Weiter**, um das Windows 2008-Setupprogramm zu starten.
6. Legen Sie die Windows 2008 Advanced Server-CD-ROM in das CD-ROM-Laufwerk ein, wenn Sie dazu aufgefordert werden. Das Setup-Programm kopiert die Dateien für den DHCP-Server und das DHCP-Tool auf Ihren Computer.
7. Wenn die Ausführung des Setup abgeschlossen ist, klicken Sie auf **Fertig stellen**.

4.12.4.2 Allgemeine Konfiguration

Nach dem Installieren und Starten des DHCP-Dienstes müssen Sie einen Bereich erstellen (einen Bereich gültiger IP-Adressen, die für die Überlassung (Lease) an DHCP-Clients verfügbar sind). Jeder DHCP-Server in Ihrer Umgebung sollte über mindestens einen Bereich verfügen, der sich nicht mit einem anderen DHCP-Serverbereich in Ihrer Umgebung überschneidet.

Beim Installieren und Konfigurieren des DHCP-Dienstes auf einem Domänencontroller wird der Server normalerweise beim ersten Hinzufügen des Servers zur DHCP-Konsole autorisiert. Wenn Sie den DHCP-Dienst jedoch auf einem Mitgliedsserver oder einem eigenständigen Server installieren und konfigurieren, müssen Sie den DHCP-Server konfigurieren.

Gehen Sie folgendermaßen vor, um einen DHCP-Server zu autorisieren:

1. Wählen Sie aus dem Windows-Startmenü **Start** > **Programme** > **Verwaltung** > **DHCP**.

   HINWEIS: Sie müssen bei dem Server mit einem Konto angemeldet sein, das Mitglied der Gruppe „Organisationsadministratoren“ ist.

2. Wählen Sie im Menü der DHCP-Konsole den neuen DHCP-Server aus. Wenn sich in der unteren rechten Ecke des Serverobjekts ein roter Pfeil befindet, wurde der Server noch nicht autorisiert.

3. Klicken Sie mit der rechten Maustaste auf den Server, und klicken Sie anschließend auf **Autorisieren**.

4. Klicken Sie nach einigen Augenblicken erneut mit der rechten Maustaste auf den Server, und klicken Sie dann auf **Aktualisieren**. Der Server sollte jetzt einen grünen Pfeil in der unteren rechten Ecke anzeigen, der bedeutet, dass der Server autorisiert wurde.

Gehen Sie folgendermaßen vor, um einen neuen Bereich zu erstellen:

1. Wählen Sie aus dem Windows-Startmenü **Start** > **Programme** > **Verwaltung** > **DHCP**.

   HINWEIS: Wählen Sie in der Konsolenstruktur den DHCP-Server aus, auf dem der neue DHCP-Bereich erstellt werden soll.

2. Klicken Sie mit der rechten Maustaste auf den Server, und klicken Sie dann mit der linken Maustaste auf **Neuer Bereich**.

3. Klicken Sie im Bereichserstellungs-Assistenten auf **Weiter**, und geben Sie anschließend einen Namen und eine Beschreibung für den Bereich ein. Sie können einen beliebigen Namen wählen, der jedoch den Zweck des neuen Bereichs im Netzwerk deutlich erkennbar beschreiben sollte. Sie könnten zum Beispiel „Clientadressen im Verwaltungsgebäude“ eingeben.

4. Geben Sie den Adressbereich ein, der in diesem Bereich als Lease überlassen werden kann, z. B. eine IP-Startadresse von 192.168.100.1 bis zu einer Endadresse von 192.168.100.100. Da diese Adressen an Clients ausgegeben werden, sollte es sich ohne Ausnahme um gültige Adressen im Netzwerk handeln, die derzeit nicht in Gebrauch sind. Wenn Sie eine andere Subnetzmaske verwenden möchten, geben Sie die neue Subnetzmaske ein. Klicken Sie auf **Weiter**.

5. Geben Sie alle IP-Adressen ein, die vom eingegebenen Bereich ausgeschlossen werden sollen. Dazu zählen alle Adressen, die möglicherweise bereits verschiedenen Computern in Ihrer Organisation statisch zugewiesen wurden. Klicken Sie auf **Weiter**.

6. Geben Sie die Anzahl der Tage, Stunden und Minuten an, nach denen eine IP-Adresslease aus diesem Bereich abläuft. Dadurch wird die Zeitspanne bestimmt, für die ein Client eine geleaste Adresse halten kann, ohne sie erneuern zu müssen. Klicken Sie auf **Weiter**.
7. Wählen Sie **Ja, ich möchte diese Optionen jetzt konfigurieren**, und erweitern Sie dann den Assistenten um die Aufnahme von Einstellungen für die häufigsten DHCP-Optionen. Klicken Sie auf **Weiter**.
8. Geben Sie die IP-Adresse des Standard-Gatekeepers ein, der von den Clients, die eine IP-Adresse aus diesem Bereich erhalten, verwendet werden soll.
9. Klicken Sie auf **Hinzufügen**, um die Adresse des Standard-Gatekeepers in die Liste aufzunehmen, und klicken Sie dann auf **Weiter**.

   HINWEIS: Wenn im Netzwerk bereits DNS-Server vorhanden sind, geben Sie den Domänennamen Ihrer Organisation im Feld **Übergeordnete Domäne** ein. Geben Sie den Namen des DNS-Servers ein, und klicken Sie dann auf **Auflösen**, um sicherzustellen, dass der DHCP-Server eine Verbindung zu dem DNS-Server herstellen und dessen Adresse ermitteln kann. Klicken Sie anschließend auf **Hinzufügen**, um diesen Server in die Liste der DNS-Server aufzunehmen, die den DHCP-Clients zugeordnet sind. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **Ja, ich möchte diesen Bereich jetzt aktivieren**, um den Bereich zu aktivieren und Clients den Bezug von Leases vom Bereich zu ermöglichen.
11. Klicken Sie auf **Weiter** und auf **Fertig stellen**.

4.12.4.3 DHCP-Server für DLS konfigurieren

Der DHCP-Server sollte so konfiguriert sein, dass der Server bei einer IP-Adressanfrage von einem IP Device diesem neben der IP-Adresse und der Adresse von DNS und Default Router auch die IP-Adresse und Portnummer des DLS automatisch übermittelt. Nach diesem Vorgang kann das IP Device den DLS kontaktieren. Diese zusätzlichen Informationen können in Form von *Vendor Classes* vom DHCP-Server bereitgestellt werden.

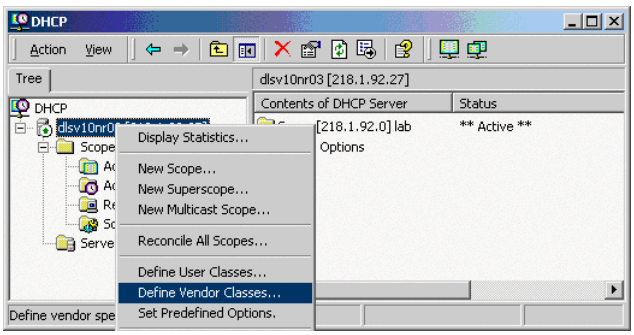
Diese Methode wird nachfolgend dargestellt:

Im nachfolgenden Beispiel wird erläutert, wie Sie eine neue Vendor-Klasse einrichten, ihr Eigenschaften zuordnen und ihren Bereich festlegen.

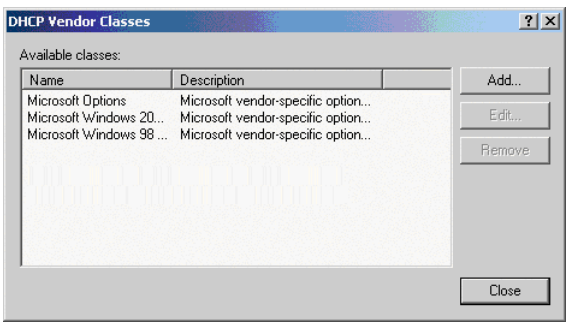
1. Wählen Sie aus dem Windows-Startmenü **Start** > **Programme** > **Verwaltung** > **DHCP**.

Neue Vendor Class einrichten

2. Klicken Sie mit der rechten Maustaste im Menü der DHCP-Konsole auf den betreffenden DHCP-Server und wählen Sie **Define Vendor Classes...** aus dem Kontextmenü.

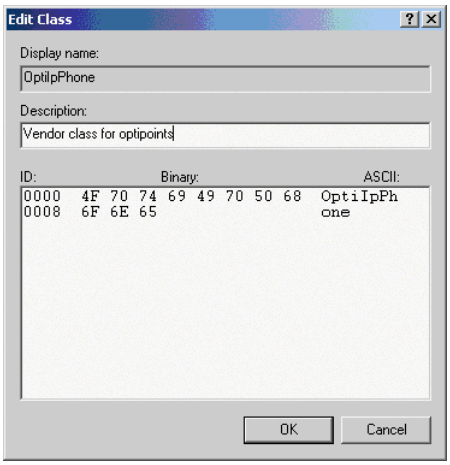


3. Ein Dialogfenster mit einer Liste der bereits verfügbaren Klassen erscheint.



Klicken Sie auf **Add...**, um eine neue Klasse hinzuzufügen.

4. Legen Sie eine neue *Vendor Class* mit dem Namen **OptiIpPhone** für IP Phones (bzw. **opticlient** für optiClients) fest und geben Sie eine Beschreibung zu dieser Klasse ein.

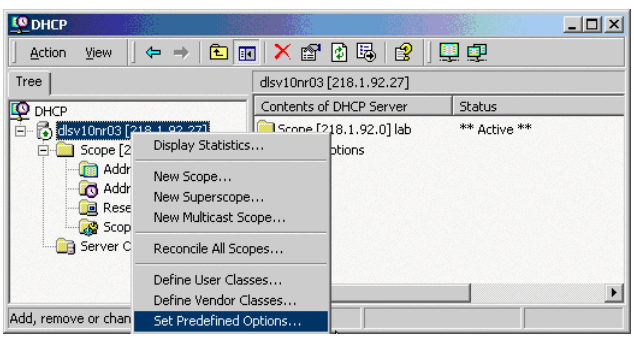


Klicken Sie auf **OK**, um die Änderungen zu übernehmen. In der Liste erscheint nun die neue Vendor Class.

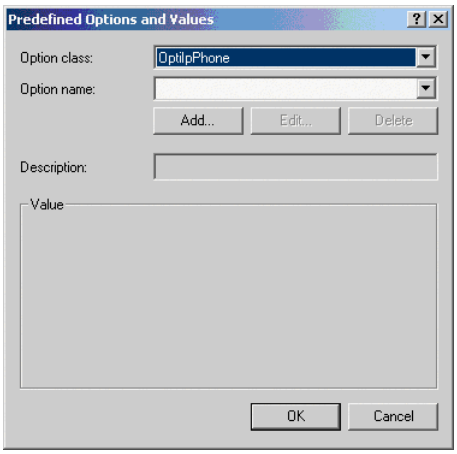
5. Schließen Sie das Fenster mit **Close**.

Eigenschaften zur neuen Vendor Class hinzufügen

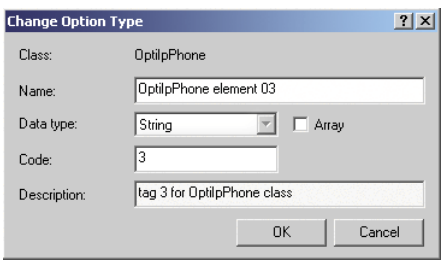
6. Klicken Sie mit der rechten Maustaste im Menü der DHCP-Konsole auf den betreffenden DHCP-Server und wählen **Set Predefined Options...** aus dem Kontextmenü.



7. Wählen Sie im Dialogfenster die zuvor definierte Klasse **OptiIpPhone** aus und klicken Sie auf **Add...**, um eine neue Option hinzuzufügen.



8. Tragen Sie die Daten zu der neuen Option ein.



Vergeben Sie einen Namen und wählen Sie im Feld **Data type** den Datenttyp je nach aktuell einzutragender Option:

- 01: **String**
- 02: **Long**
- 03: **String**
- 04: **String**

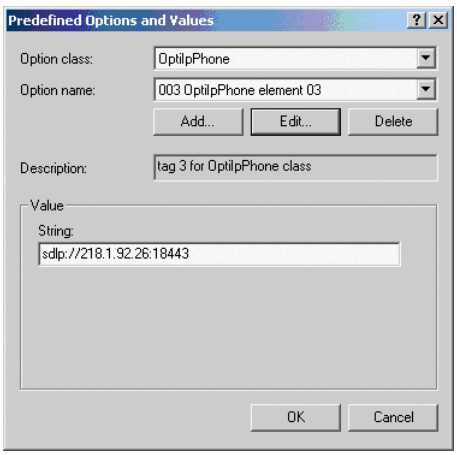
Tragen Sie die zur aktuellen Option gehörende Tag-Nummer im Feld **Code** ein:

- 01: **1**
- 02: **2**
- 03: **3**
- 04: **4**

Zusätzlich sollte eine Beschreibung für die jeweilige Option im Feld Description eingegeben werden.

Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

9. Geben Sie den Wert für diese Option ein.


Predefined Options and Values
Option class:
OptiIpPhone
Option name:
003 OptiIpPhone element 03
Add...
Edit...
Delete
Description:
tag 3 for OptiIpPhone class
Value
String:
sdlp://218.1.92.26:18443
OK
Cancel

Die Werte der beiden erforderlichen Optionen sind:

Option Name	Vendor	Wert
001 optiPoint Element 1	OptiIpPhone	Unify
003 optiPoint Element 3	OptiIpPhone	sdlp://[DLS IP-Adresse]:18443

Tabelle 9 DHCP Optionen und Werte

Statt der DLS IP-Adresse kann, wenn ein DNS-Server vorhanden ist, auch der Hostname des DLS als **004 optiPoint Element 4** eingetragen werden (im weiteren Verlauf der Beispielbeschreibung wird die DLS IP-Adresse eingetragen).

HINWEIS: Kommt ein VLAN zur Anwendung, ist die Angabe einer VLAN-ID als Tag 2 erforderlich.

10. Klicken Sie auf **OK** und wiederholen Sie die Schritte 7 bis 9 für jede weitere Option.

    HINWEIS: Für DHCP-Server auf einem Windows 2003 Server:
    .
    Bei Windows 2003 Server ist es auf Grund eines Fehlers nicht möglich, eine Option mit der ID 1 für eine selbstdefinierte Herstellerklasse über die DHCP-Konsole einzurichten. Dieser Eintrag muss stattdessen mittels Kommandozeile (DOS-Shell) mit dem Tool `netsh` vorgenommen werden.

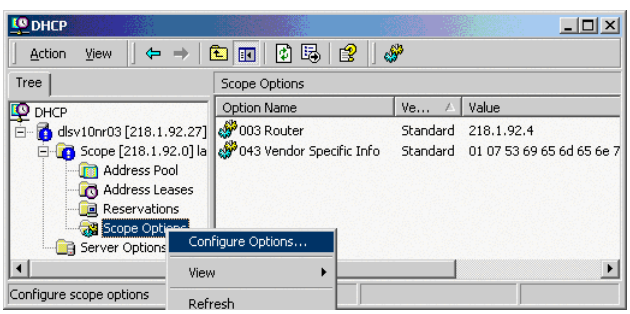
    Über das folgende Kommando können Sie die gewünschte Option ohne Fehlermeldung konfigurieren, so dass sie danach auch in der DHCP-Konsole zur Verfügung steht:

    ```
    netsh dhcp server add optiondef 1 "Optipoint element 001" STRING 0
    vendor=OptiIpPhone comment="Tag 001 für Optipoint"
    ```

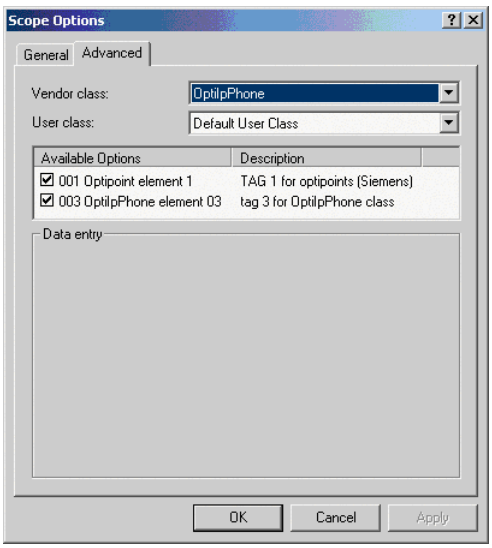
    Der Wert **Unify** für das optiPoint Element 1 kann dann wieder über die DHCP-Konsole zugewiesen werden.
    Eine Korrektur dieses Fehlers steht im SP2 für Windows 2003 Server zur Verfügung.

Bereich der neuen Vendor Class festlegen

11. Wählen Sie den betreffenden DHCP-Server und Bereich (**Scope**) und klicken Sie mit der rechten Maustaste auf **Scope Options**. Wählen Sie **Configure Options...** aus dem Kontextmenü.

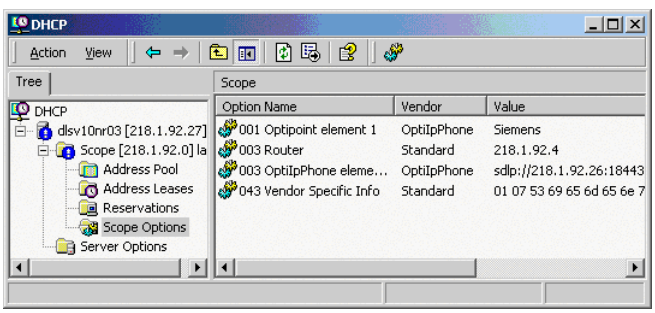


12. Wählen Sie das **Register** Advanced. Wählen Sie bei **Vendor Class** die zuvor festgelegt Klasse **OptiIpPhone** und bei **User Class** die Klasse **Default User Class**.



Aktivieren Sie die Checkboxen der Optionen, die Sie dem Bereich zuordnen möchten (im Beispiel **001** und **003**).

13. Die DHCP-Konsole zeigt nun die Informationen, die für die entsprechenden Workpoints übertragen werden.



Dabei werden die Informationen des Vendors **Standard** allen Clients übertragen, wohingegen die Informationen des Vendors **OptiIpPhone** an die Clients (IP Devices) dieser Vendor-Klasse übertragen werden.

4.12.4.4 Problembehandlung

Clients können keine IP-Adresse erhalten

Wenn ein DHCP-Client nicht über eine konfigurierte IP-Adresse verfügt, bedeutet dies normalerweise, dass der Client keine Verbindung zu einem DHCP-Server herstellen konnte. Dies liegt entweder an einem Netzwerkproblem oder daran, dass der DHCP-Server nicht verfügbar ist.

Wenn der DHCP-Server gestartet wurde und andere Clients gültige Adressen abrufen konnten, überprüfen Sie, ob der Client über eine gültige Netzwerkverbindung verfügt und alle zugehörigen Hardwaregeräte des Clients (einschließlich Kabel und Netzwerkkarten) ordnungsgemäß funktionieren.

Der DHCP-Server ist nicht verfügbar

Wenn ein DHCP-Server den Clients keine Adress-Leases zur Verfügung stellt, hat das häufig den Grund, dass der Start des DHCP-Dienstes fehlgeschlagen ist. Wenn dies der Fall ist, wurde der Server möglicherweise nicht für den Betrieb im Netzwerk autorisiert.

Wenn Sie den DHCP-Dienst zuvor starten konnten, er aber mittlerweile beendet wurde, verwenden Sie die Ereignisanzeige, um das Systemprotokoll auf Einträge zu überprüfen, die möglicherweise die Ursache erklären.

HINWEIS: Klicken Sie zum erneuten Starten des DHCP-Dienstes auf **Start**, klicken Sie auf **Ausführen**, geben Sie *cmd* ein, und drücken Sie dann die <EINGABETASTE>. Geben Sie *net start dhcpserver* ein, und drücken Sie anschließend die <EINGABETASTE>.

4.12.5 DHCP-Server in einer Linux/Unix-Umgebung

Dieser Abschnitt beschreibt die Konfiguration der herstellerspezifischen Optionen unter Linux/Unix zum Nutzen der Plug&Play-Funktionalität.

HINWEIS: Es wird empfohlen, einen DHCP-Server im DLS-Umfeld einzusetzen, um
- vollständiges Plug&Play zu unterstützen und
- die Authentizität des DLS-Servers sicherzustellen.

Die Einrichtung der herstellerspezifischen Optionen kann je nach verwendetem DHCP-Server von dem hier gezeigten Beispiel abweichen. Weitere Informationen finden Sie in den Hilfe-Seiten (man-pages) von Linux und Unix (z. B. dhcp-options und dhcpd.conf).

Die Konfiguration wird in der Datei /etc/dhcpd.conf vorgenommen. Diese Datei kann einfach mittels eines Texteditors bearbeitet werden. In der Regel befindet sich in dieser Datei bereits eine Beispielkonfiguration, die den eigenen Wünschen angepasst werden kann.
Vor jeder Veränderung der Konfigurationsdatei bitte eine Sicherungskopie anfertigen!

In folgender Konfiguration sind alle benötigten Parameter enthalten:

21

Zeile	Inhalt
1	`option domain-name-servers 192.168.3.2;`
2	`option broadcast-address 192.168.3.255;`
3	`option routers 192.168.3.2;`
4	`option subnet-mask 255.255.255.0;`
5	`option domain-name "DSLSUB3";`
6	`default-lease-time 864000;`
7	`max-lease-time 8640000;`
8	`ddns-update-style ad-hoc;`
9	
10	`class "OptiIpPhone" {`
11	`  option vendor-encapsulated-options`
12	`  01:07:53:69:65:6D:65:6E:73:`
13	`  03:19:73:64:6C:70:3A:2F:2F:31:39:32:2E:31:36:38:2E:33:2E:33:30:3A:31:38:34:34:33;`
14	`  match if substring (option vendor-class-identifier, 0, 11) = "OptiIpPhone";`
15	`}`
16	
17	`class "VLAN-discovery-OptiPoint" {`
18	`  option vendor-encapsulated-options`
19	`  01:07:53:69:65:6D:65:6E:73:`
20	`  02:04:00:00:00:0A;`
21	`  match if substring (option vendor-class-identifier, 0, 9) = "OptiPoint";`
22	`}`
23	`subnet 192.168.3.0 netmask 255.255.255.0 {`
24	`  range 192.168.3.100 192.168.3.254;`
25	`}`

Der Bereich von Zeile 10 bis 15 sorgt für die Übertragung der DLS-Adresse zum IP Device. In Zeile 12 und 13 befinden sich zwei hexadezimale Werte, die wie folgt aufgebaut sind:
Option – Länge – Wert.

Die erste der beiden Zeilen enthält den Wert „Siemens“ und die zweite enthält „sdlp://192.168.3.6:18443“ (die Adresse des DLS).

In Zeile 10 steht ein frei wählbarer Name, und in Zeile 14 wird festgelegt, für welche Herstellerklasse diese Konfiguration gültig ist.

Zeile 17 bis 21 enthalten die Zuweisung der VLAN ID. Die VLAN ID wird in Zeile 20 mit der Option 2, der Länge 4 und dem Wert als Hexadezimale Zahl (hier 0A = 10) übergeben. Anders als bei den anderen Optionen wird die dezimale VLAN ID in eine hexadezimale Zahl umgewandelt.

HINWEIS: Für die Umwandlung von ASCII-Zeichen in hexadezimale Werte siehe „ASCII-Tabelle (Standard)“ und „ASCII-Tabelle (Erweitert)“ auf Seite 17-2 bzw. auf Seite 17-3.

Nach der Änderung der Konfiguration muss der DHCP-Dienst neu gestartet werden. Dafür kann das Kommando `rcdhcpd restart` oder alternativ `etc/init.d/dhcp stop` und danach `/etc/init.d/dhcp start` verwendet werden. Für einen Syntax-Check kann man auch `rcdhcp check-syntax` über die Konsole eingeben.

Wenn die Konfiguration korrekt ist, sollten die Endgeräte sich nach einem Restart selbständig am DLS registrieren. Sollte dies nicht der Fall sein, können Sie mit einem sogenannten „Netzwerksniffer“, z. B. *Ethereal* (ab V 0.10.11), dem Fehler auf den Grund gehen.

4.12.6 DNS-Server für DLS konfigurieren

HINWEIS: Nachfolgend sind nur die Einstellungen beschrieben, die zur Konfiguration des DNS-Servers bzgl. DLS erforderlich sind. Zur allgemeinen Installation und Konfiguration lesen Sie bitte in der Dokumentation zum DNS-Server.

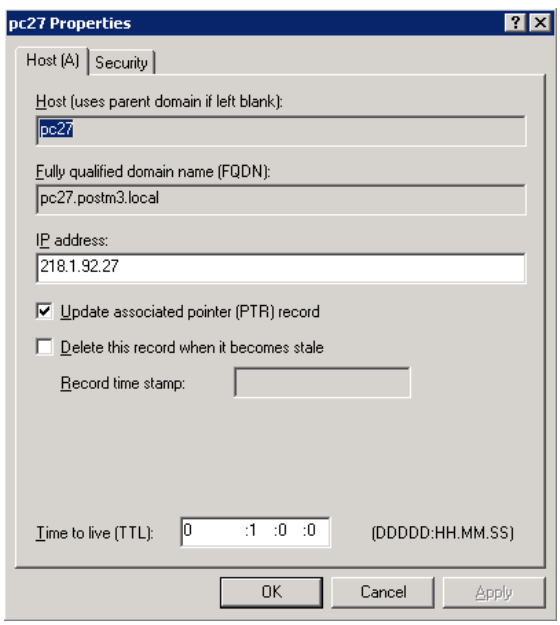
Um den DLS als Hostname eintragen zu können, muss ein DNS-Server entsprechend konfiguriert sein.

Beispiel:

IP-Adresse des DLS: 218.1.92.27

Gewünschter Hostname: sdlp://pc27.postm3.local:18443

Für dieses Beispiel muss folgender Eintrag im DNS-Server vorgenommen werden:



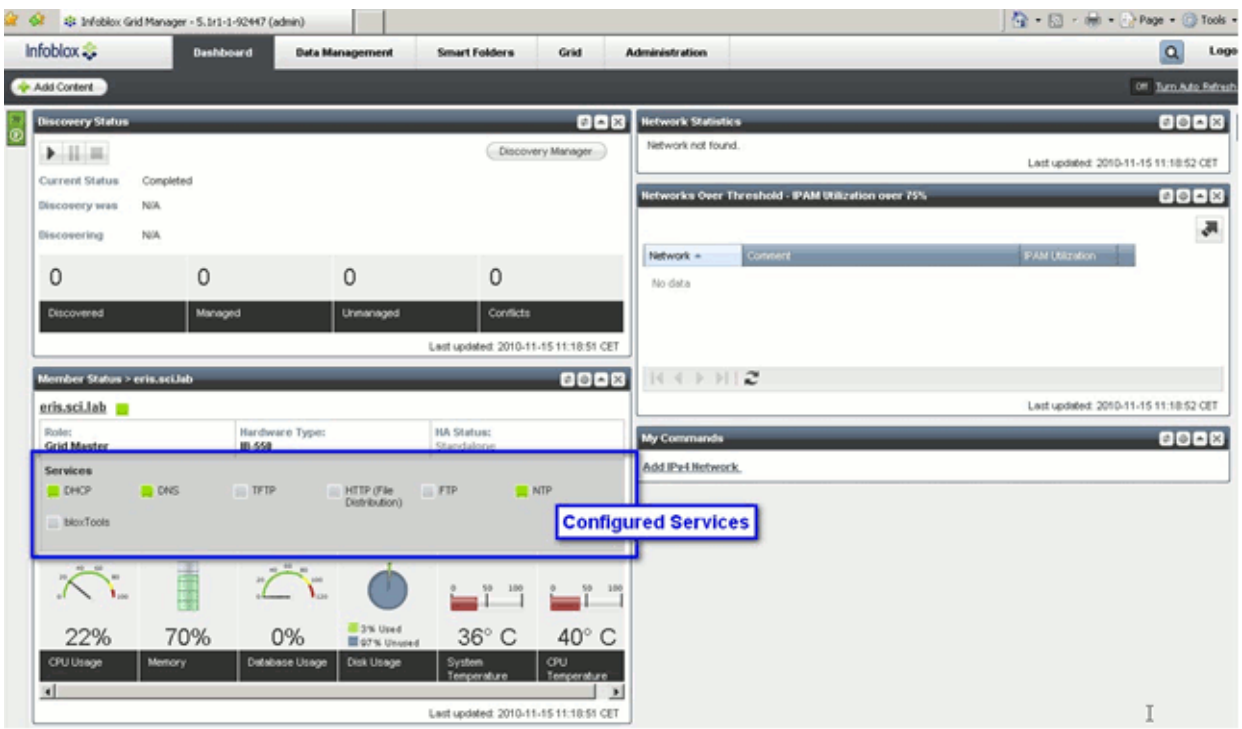
4.12.7 DHCP Server mit Infoblox Appliance

Alternativ zu einem herkömmlichen DHCP-Server unter Windows oder Unix kann der DHCP-Dienst von der Infoblox Appliance übernommen werden.

Zusätzlich kann die Infobox Appliance die folgenden grundlegenden Netzwerkdienste anbieten:

- DNS
- NTP
- FTP
- TFTP

Die folgende Abbildung zeigt die Kontrollübersicht derInfoblox 550, hier konfiguriert als DHCP-, DNS- und NTP-Server für eine OpenScape Voice-Umgebung:



4.12.7.1 Installation

Nachdem die Infoblox Appliance mit dem Netzwerk verkabelt ist (siehe beigefügte Installationsanleitung), können Sie das Gerät über das Ethernet-Netzwerk erreichen.

Die Administration und Konfiguration können Sie wahlweise mit einem Web-Browser über HTTPS vornehmen oder mit der Kommandozeile (CLI) über SSH. Wenn Sie SSH verwenden wollen, müssen Sie sich zuvor einmalig über HTTPS einloggen und den SSH-Zugang erlauben.

Diese Anleitung beschreibt die Administration über HTTPS; detaillierte Informationen zur Administration über die Kommandozeile finden Sie im „Infoblox CLI Guide“.

Zugang über HTTPS

Um sich anzumelden, gehen Sie wie folgt vor:

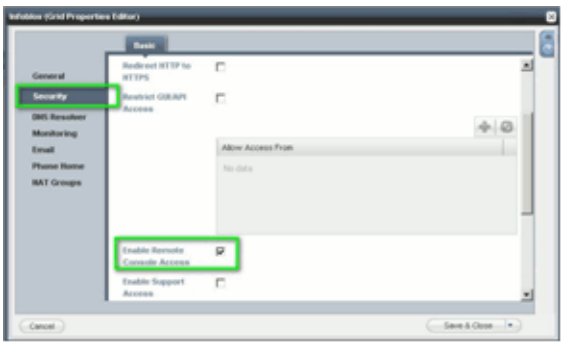
1. Öffnen Sie einen Web-Browser und geben Sie
   https://<IP-Addresse oder Hostname Ihrer Infoblox Appliance> ein.
2. Geben Sie Benutzername und Passwort ein.
   Der voreingestellte Benutzername ist „admin“, und das dazugehörige Passwort „infoblox“. Achten Sie darauf, das Passwort nach der ersten Anmeldung zu ändern.

Zugang für Kommandozeile über SSH

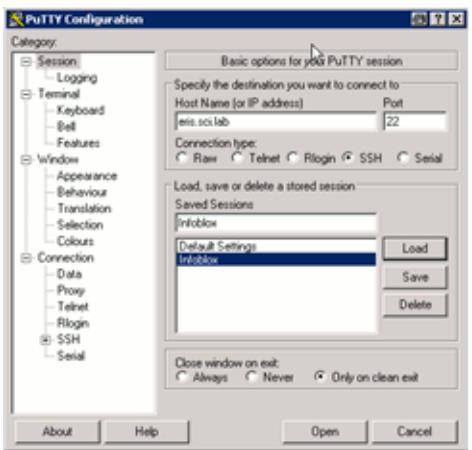
Um den Zugang für die Kommandozeile zu ermöglichen, müssen Sie über HTTPS angemeldet sein (siehe Zugang über HTTPS).

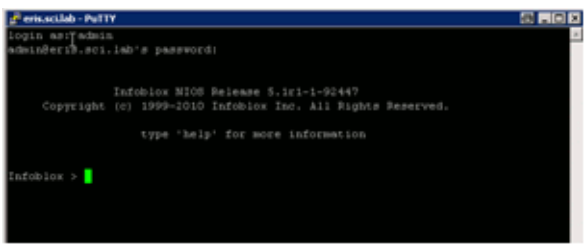
1. Wählen Sie **Grid** > **Grid Manager** und expandieren Sie die Werkzeugleiste (Toolbar). Im Menü **Edit** wählen Sie **Grid Properties**.

2. Der **Grid Properties Editor** öffnet sich. Im Register **Security** markieren Sie das Feld **Enable Remote Console Access**.



3. Nun können Sie Ihre Infoblox Appliance mittels Kommandozeile über SSH administrieren und konfigurieren. Hierfür kann jeder SSH v2 Client verwendet werden, beispielsweise PuTTY für Windows:





Grundkonfiguration

1. Öffnen Sie einen Web-Browser und stellen Sie eine HTTPS-Verbindung zur IP-Adresse des LAN1-Ports her. Um die voreingestellte IP-Adresse zu erreichen, geben Sie**https://<192.168.1.2>** ein.

   HINWEIS: Während der Anmeldung können verschiedene Zertifikatswarnungen erscheinen; sie können aber in dieser Phase der Konfiguration ignoriert werden. Um die Warnungen zu verhindern, ist ein neues selbst unterzeichnetes Zertifikat notwendig oder der Import eines Third Party-Zertifikats. Mehr Informationen zur Implementierung von Zertifikaten finden Sie in der Administrationsanleitung für Infoblox.

2. Melden Sie sich als „admin“ mit dem voreingestellten Passwort „infoblox“ an.
3. Lesen Sie die Lizenzvereinbarung durch und akzeptieren Sie diese.
4. Der **Grid Setup Wizard** erscheint. Wählen Sie **Configure a Grid Master** > **Next**.
5. Legen Sie die **grid properties** fest:

   - **Grid Name**
     Dieser Name (Text-String) wird vom Grid Master und den weiteren zum Grid-Netz hinzukommenden Teilnehmern verwendet, um sich beim Aufbau eines VPN-Tunnels gegenseitig zu authentifizieren. Der voreingestellte Name ist „Infoblox“.
   - **Shared Secret**
     Dieser Text-String wird beim Aufbau eines VPN-Tunnels vom Grid Master und den weiteren zum Grid-Netz hinzukommenden Teilnehmern als gemeinsames Geheimnis bei der gegenseitigen Authentifizierung verwendet.
   - **Show Password**
     Aktivieren Sie den Schalter, um das Passwort anzeigen zu lassen, oder deaktivieren Sie ihn, um das Passwort zu verbergen.
   - **Hostname**
     Geben Sie einen validen DNS-Hostnamen für die Infoblox Appliance an.
   - **Is the Grid Master an HA pair?**
     Wählen Sie **No**.

   Klicken Sie anschließend auf **Next**.

6. Konfigurieren Sie die Netzwerkeinstellungen.

   - **Host Name**
     Geben Sie einen validen DNS-Hostnamen für die Infoblox Appliance an.
   - **IP Address**
     Zeigt die IP-Adresse des LAN-Ports an.
   - **Subnet Mask**
     Zeigt die Subnetz-Maske des LAN-Ports an.
   - **Gateway**
     Zeigt die IP-Adresse des Gateways bzw. Routers für das Subnetz an, in dem sich der LAN-Port befindet.
   - **Port Settings**
     Wählen Sie aus der Liste die passenden Einstellungen für den Port aus.

   Klicken Sie anschließend auf **Next**.

7. Geben Sie ein neues Passwort ein. Das Passwort muss ein einzelner hexadezimaler String mit mindestens 4 Zeichen Länge sein.
   Klicken Sie anschließend auf **Next**.

8. Wählen Sie die Zeitzone für den Grid Master und geben Sie an, ob der Grid Master seine Zeit über einen NTP-Server synchronisieren soll.

   Wenn Sie NTP verwenden wollen, klicken Sie das **Add**-Symbol und geben Sie die IP-Adresse eines NTP-Servers ein. Sie können auch mehrere NTP-Server angeben.

   Wenn Sie NTP nicht verwenden wollen, stellen Sie Datum und Uhrzeit manuell ein.

   Klicken Sie anschließend auf **Next**.

9. Im letzten Fenster können Sie alle Einstellungen, die Sie mit dem Wizard gemacht haben, überprüfen.

   Klicken Sie auf **Finish**.

   Daraufhin erfolgt ein Neustart.

4.12.7.2 Konfiguration

Allgemeine DHCP-Konfiguration

Zuerst müssen Sie ein Netzwerk und einen Bereich von zu vergebenden IP-Adressen angeben.

HINWEIS: Für aktives DNS-Forwarding über DHCP muss ein funktionierender DNS-Server in Ihrem Netzwerk vorhanden sein. Dies können Sie mithilfe der folgenden Befehle auf der Kommandozeile überprüfen:

- Ermitteln Sie die IP-Adresse des DNS-Servers, der für Ihr Netzwerk konfiguriert wurde. Unter Windows geschieht das mit dem Befehl:
`ipconfig /all`

- Mit einem Ping können Sie überprüfen, ob dieser DNS-Server erreichbar ist:
`ping <IP-Adresse des DNS-Servers>`

- Mit nslookup und einer beliebigen IP-Adresse oder einem beliebigen Hostnamen können Sie feststellen, ob der DNS-Server korrekt funktioniert:
`nslookup 172.21.101.15` oder
`nslookup wsname.domain.net`

Netzwerk hinzufügen

1. Wählen Sie **Data Management** > **IPAM** und klicken Sie in der Werkzeugleiste unter **Add** auf **Add IPv4 Network**.

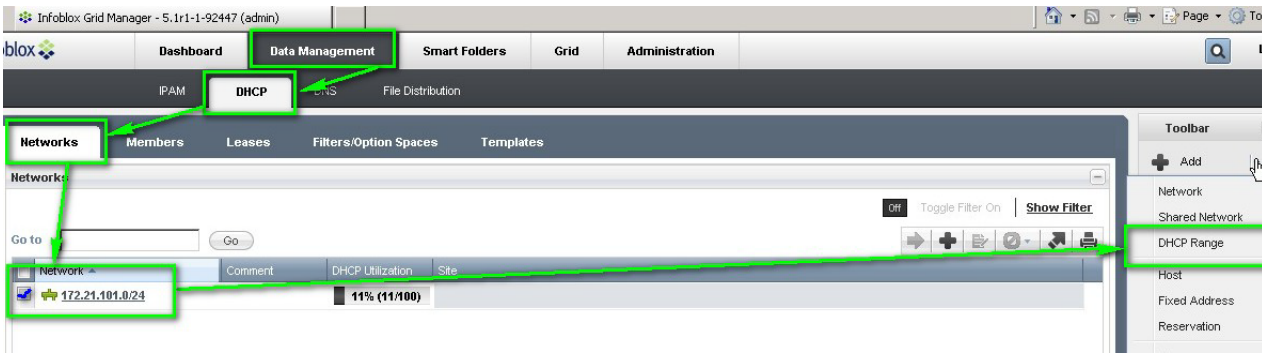
2. Im Wizard **Add Network** ergänzen Sie die folgenden Angaben:

   - **Adress:**
     Adresse des Netzwerks. Beispiel: **172.21.101.0**
   - **Netmask:**
     Wählen Sie mithilfe des Netmask-Reglers die Netzmaske **/24 (255.255.255.0)** .

3. Klicken Sie **Save&Close**.

DHCP-Bereich erzeugen

1. Wählen Sie unter **Data Management** > **DHCP** > **Networks** Ihr Netzwerk aus (z.B. 172.21.101.0), klicken Sie in der Werkzeugleiste auf **Add** und dann auf **DHCP Range**.



2. Im Wizard **Add Range** ergänzen Sie die folgenden Angaben:

   - **Start:**
     Anfang des Adressbereichs. Beispiel: **172.21.101.100**
   - **End:**
     Ende des Adressbereichs. Beispiel: **172.21.101.199**

3. Klicken Sie **Save&Close**.

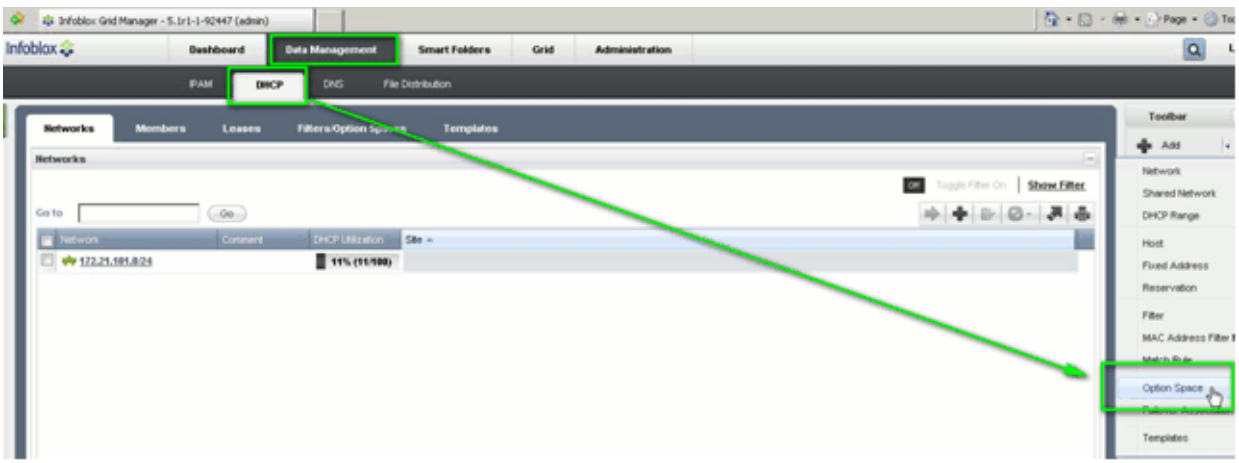
   HINWEIS: Bitte beachten Sie, dass jeder DHCP-Server in Ihrer Umgebung mindestens einen Bereich haben sollte, der sich nicht mit einem Bereich eines anderen DHCP-Servers in derselben Umgebung überlappt.

DHCP-Server für DLS konfigurieren

Für vollständiges Plug&Play muss der DHCP-Server dem Telefon während des Starts die IP-Adresse und Portnummer des DLS mitteilen. Daraufhin Das Telefon wird dann den DLS kontaktieren, um die erforderlichen Einstellungen zu erhalten.

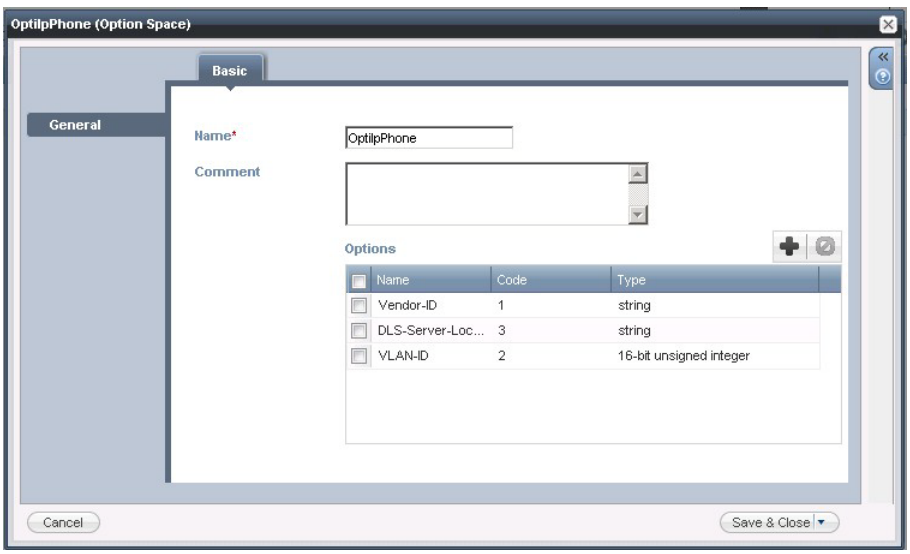
Infoblox übergibt die DLS-relevanten Informationen in Form von Vendor-spezifischen Optionen.

1. Gehen Sie auf **Data Management** > **DHCP** > **Filters/Option Spaces** und wählen Sie auf der rechten Seite **Add**.

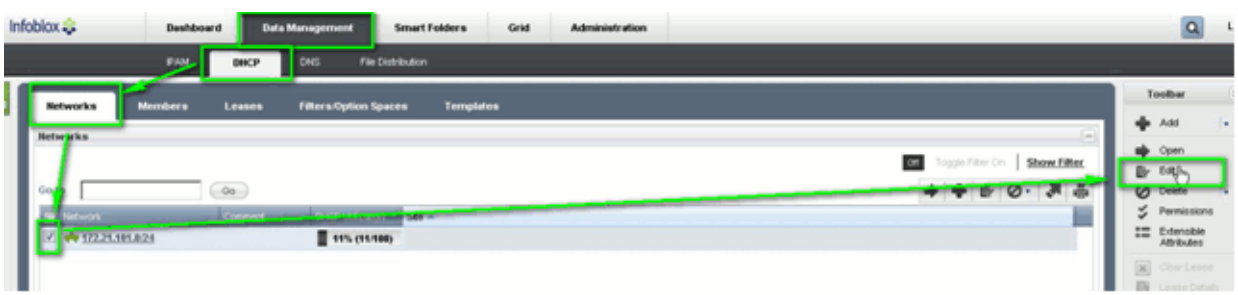


2. Spezifizieren Sie die DCHP-Optionen wie folgt:

   - Im Feld **Name** geben Sie „OptiIpPhone“ ein.
   - Fügen Sie eine neue Option hinzu mit den Eigenschaften **Name=**„Vendor-ID“, **Code=** „1“ und **Type=**„String“.
   - Fügen Sie eine weitere Option hinzu mit den Eigenschaften **Name=**„DLS-Server-Location“, **Code=**„1“ und **Type=**„String“.
   - Wenn ein Virtuelles LAN (VLAN) verwendet wird: Fügen Sie eine weitere Option hinzu mit den Eigenschaften
     Name=„VLAN-ID“, **Code=**„2“ und **Type=**„16-bit unsigned integer“.

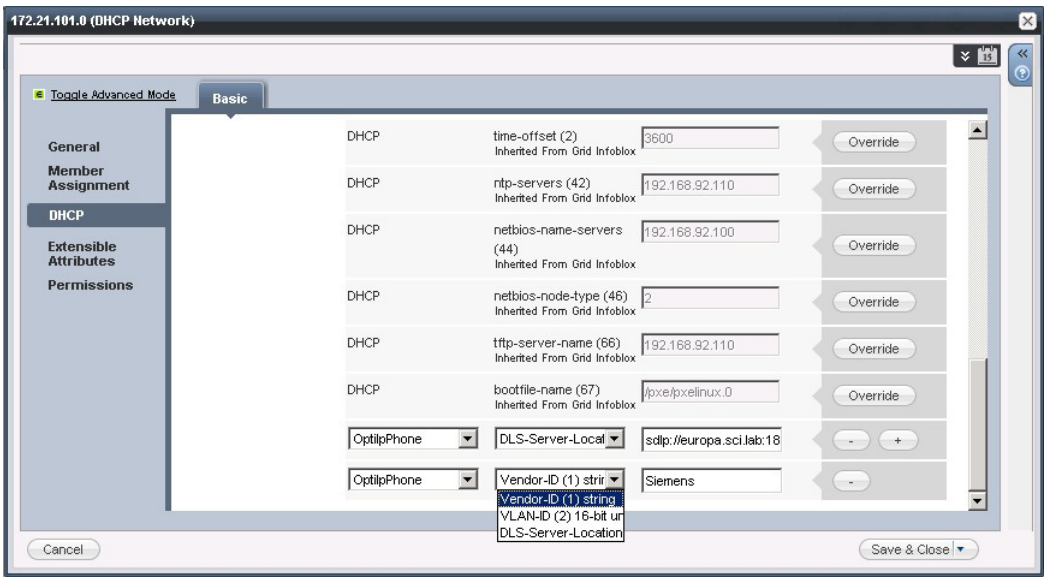


3. Gehen Sie auf **Data Management** > **DHCP** > **Networks**, wählen Sie Ihr Netzwerk aus (z.B. 172.21.101.0/24) und klicken Sie in der Werkzeugleiste auf **Edit**.

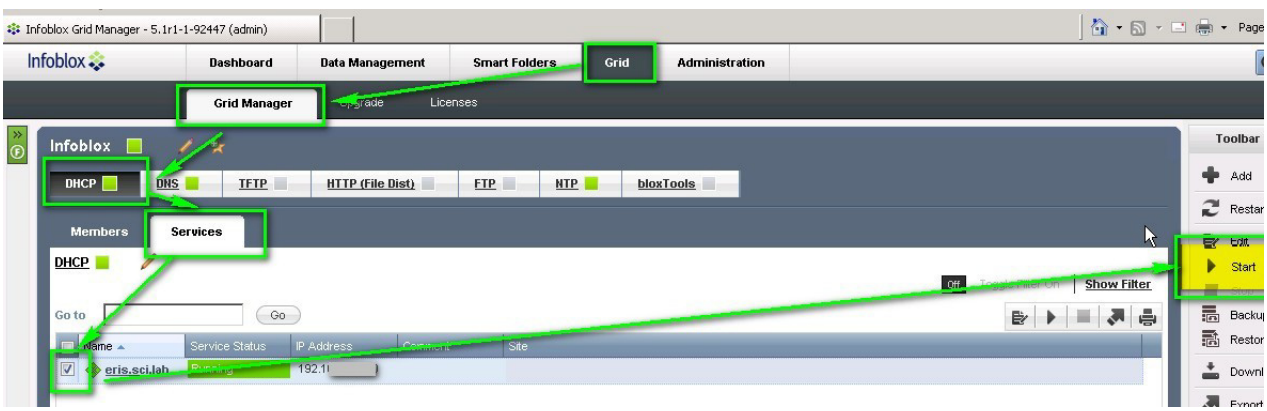


4. Gehen Sie auf **Basic** > **DHCP** und führen Sie die folgenden beschriebenden Aktionen durch.

   - Fügen Sie einen neuen Eintrag hinzu mit den Eigenschaften **space=**„OptiIpPhone“, **name=**„DLS-Server-Location“, **value=**„sdlp://<Name oder Hostname Ihres DLS-Servers>:18443“.
   - Fügen Sie einen neuen Eintrag hinzu mit den Eigenschaften **space=** „OptiIpPhone“, **name=** „Vendor ID (1) string“, **value=** „Unify“.
   - Wenn ein Virtuelles LAN (VLAN) verwendet wird, muss analog die VLAN ID spezifiziert werden.



5. Gehen Sie auf **Grid** > **Grid Manager** > **DHCP** > **Services**. Markieren Sie Ihr Netzwerk und klicken Sie den Play-Button. Der DHCP-Service startet.



4.13 Verwendung von pcAnywhere bei Fernzugriff auf den DLS

HINWEIS: Der Remotezugang von den Unify Service Centers (RCC) auf den DLS bei einem Kunden ist in der Service-Richtlinie des DLS beschrieben.

Für den Einsatz von pcAnywhere als Remote-Anbindung sind die nachfolgenden Hinweise zu beachten.

4.13.1 Allgemein

- Installieren Sie auf dem Hostrechner (der Rechner, der die pcAnywhere-Anrufe entgegennimmt) ein Betriebssystem mit 128 Bit Verschlüsselung.
- Nehmen Sie für den Hostrechner die im aktuellen Maßnahmenplan des Siemens CERT beschriebenen Einstellungen vor. Installieren Sie auf dem Hostrechner zumindest das aktuellste Service Pack.
- Installieren Sie auf dem Hostrechner die aktuellsten pcAnywhere-Patche.
- Ermöglichen Sie den Zugriff auf den Hostrechner für pcAnywhere-Nutzer nur über RLA oder ReLaX.
- Begrenzen Sie die Zugriffsrechte der Kennungen auf dem Hostrechner, die pcAnywhere nutzen dürfen.
- Setzen Sie restriktive NTFS-Rechte auf alle Verzeichnisse auf dem Hostrechner.
- Ändern Sie den Status- und den Datenport von pcAnywhere in der Registry sowohl auf dem Hostrechner als auch auf den Remote-Rechnern:
  Ändern Sie die Werte von **TCPIPDataPort** bzw. **TCPIPStatusPort** des Registry-Schlüssels **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System** von **5631** bzw. **5632** auf z. B. **6631** bzw. **6632**.

4.13.2 Einstellungen auf dem Host-Rechner

Nehmen Sie folgende Einstellungen unter **Hauptmenü** > **Datei** > **Programmoptionen** bei pcAnywhere vor:

- Aktivieren Sie die Protokollierung in der Windows NT-Ereignislogdatei durch **NT-Ereignislogbuch verwenden**.
- Um einen unbefugten Zugriff auf die Netzwerkrechte des Host-Benutzers zu verhindern, aktivieren Sie bei beiden Feldern die Option **Sicherheit** und hier den Punkt **Benutzer abmelden**.
- Wenn der Host-Rechner nach dem Neustart auf einen weiteren Anruf warten soll, aktivieren Sie die Option **Mit Windows starten**.
- Aktivieren Sie die Option **NT-Benutzerrechte**.
  So fügen Sie Remote-Benutzer hinzu und verwenden die Windows NT-Sicherheitsrechte: Wählen Sie einzelne Benutzer oder Gruppen in der Windows NT-Benutzerliste. Die Benutzer oder Gruppen auf dieser Liste werden vom Windows NT-Systemverwalter erstellt und gepflegt. Wenn Sie über Administratorrechte für Windows NT verfügen, können Sie auf die Schaltfläche **NT-Benutzer-Manager** klicken, um Benutzer hinzuzufügen oder zu löschen.

- Aktivieren Sie die Option **Verbindungsfehlversuche in Logbuch eintragen**. Damit werden die Fehlversuche in das pcAnywhere-Logbuch eingetragen.
- Aktivieren Sie die Option **Groß-/Kleinschreibung bei Kennwort**.
- Aktivieren Sie die Optionen **Anmeldeversuche pro Anruf begrenzen** und **Zeit für Anmeldung begrenzen**.
- Verwenden Sie **Datenverschlüsselung** während der Sitzungen. Wählen Sie mindestens die symmetrische Verschlüsselung.
- Aktivieren Sie die Option **Unterbrechung bei Inaktivität**.
- Objektschutz: Geben Sie ein Kennwort ein, um dieses Verbindungsobjekt vor unbefugter Nutzung zu schützen. Sie müssen das Kennwort erneut in dem Feld **Kennwortbestätigung** eingeben. Bei Kennwörtern zum Schutz von Objekten wird immer zwischen Groß- und Kleinbuchstaben unterschieden.
- Aktivieren Sie die Option **Erforderlich zur Anzeige der Eigenschaften**. Damit wird der Benutzer aufgefordert, ein Kennwort einzugeben, bevor er die Eigenschaften dieses Objekts einsehen kann.

4.13.3 Einstellungen auf dem Remote-Rechner

HINWEIS: Tragen Sie in das Feld **Zu steuernder Host-PC oder IP-Adresse** die IP-Adresse des Host-Rechners ein, den Sie mit pcAnywhere erreichen wollen. Wenn Sie hier keinen Eintrag vornehmen, wird auf dem angeschlossenen Netzsegment eine Suche nach pcAnywhere-Host-Rechner initiiert, was unnötige Netzlast verursacht und zu Problemen führen kann.

- Aktivieren Sie nicht die Option **Automatische Anmeldung beim Host bei Verbindung**. Die Speicherung dieser Informationen in pcAnywhere ist nicht sicher genug.
- Verwenden Sie **Datenverschlüsselung** während der Sitzungen. Wählen Sie mindestens die symmetrische Verschlüsselung.

4.13.4 Verschlüsselungsstufen

Öffentlicher Schlüssel

Diese Option bietet die höchste Sicherheitsstufe und wird verwendet, wenn eine Zertifizierungsstelle dem CSP[1] sowohl auf der Host- als auch auf der Remote-Seite öffentliche Schlüssel zur Verfügung stellt.

Symmetrisch

Diese Option stellt die nächst niedrigere Sicherheitsstufe dar und wird verwendet, wenn keine Zertifizierungsstelle sondern nur ein CSP vorhanden ist.

pcANYWHERE

Diese Option stellt eine Mindestverschlüsselung zur Verfügung und wird verwendet, wenn kein CSP verfügbar ist. Dies ist die einzige Verschlüsselungsstufe, die mit pcAnywhere 2.0, 5.0 und 7.x kompatibel ist.

1 Cryptographic Service Provider: Betriebssystemsoftware, die mit dem Microsoft CryptoAPI konforme Kryptografiedienste zur Verfügung stellt. Einfache CSPs sind im Lieferumfang von Windows NT 4.0 und im Microsoft Internet Explorer ab Version 3.0 enthalten.

4.14 Deinstallation des OpenScape Deployment Service

Bei einer Multi-Node-Installation werden die Daten erst gelöscht, wenn der letzte Knoten deinstalliert wird.

WICHTIG: Bei einer Deinstallation werden alle Daten der DLS-Datenbank ebenfalls gelöscht. Um einen Datenverlust zu vermeiden, erstellen Sie vor dem Deinstallieren ein Backup der Datenbank, siehe Abschnitt 15.8, “Backup / Restore”.

WICHTIG: Das Deinstallationsprogramm entfernt alle Rollback-Verzeichnisse außer dem Rollback-Datenbank-Backup für entfernte Datenbankbereitstellungen, da es das vom Benutzer während der Upgrade-Installation definierte Datenbank-Backup-Verzeichnis nicht kennt.

WICHTIG: Bei Bereitstellungen mit entfernten Datenbanken muss die Datenbank nach der Deinstallation vom Administrator manuell gelöscht werden.

4.14.1 Deinstallation des DLS

1. Wählen Sie im Windows-Startmenü **Einstellungen** > **Systemsteuerung** > **Software** und klicken Sie in der Liste der installierten Software auf den Eintrag **Deployment Service**.
2. Klicken Sie auf **Entfernen** und folgen Sie dem weiteren Ablauf.

Nach Abschluss der Deinstallation ist sowohl die DLS-Anwendung als auch der mitinstallierte Web-Server *Tomcat* vom Server-PC entfernt.

HINWEIS: Das bei der Installation des DLS angelegte Wurzelverzeichnis „DeploymentService“ wird bei der Deinstallation geleert, es muss aber manuell entfernt werden.

4.14.2 Deinstallation des SQL-Servers

Im Rahmen der Deinstallation des DLS erhalten Sie die Möglichkeit, auch den vorhandenen Microsoft SQL Server 2005/2008 zu deinstallieren, sofern es sich nicht um eine entfernte Datenbank handelt. Ansonsten können Sie den SQL-Server manuell entfernen:

1. Wählen Sie im Windows-Startmenü **Einstellungen** > **Systemsteuerung** > **Software** und klicken Sie in der Liste der installierten Software auf den Eintrag **Microsoft SQL Server 2005** oder **Microsoft SQL Server 2008**.
2. Klicken Sie auf **Entfernen** und folgen Sie dem weiteren Ablauf.

Nach Abschluss der Deinstallation ist die SQL-Datenbankanwendung vom Server-PC entfernt.

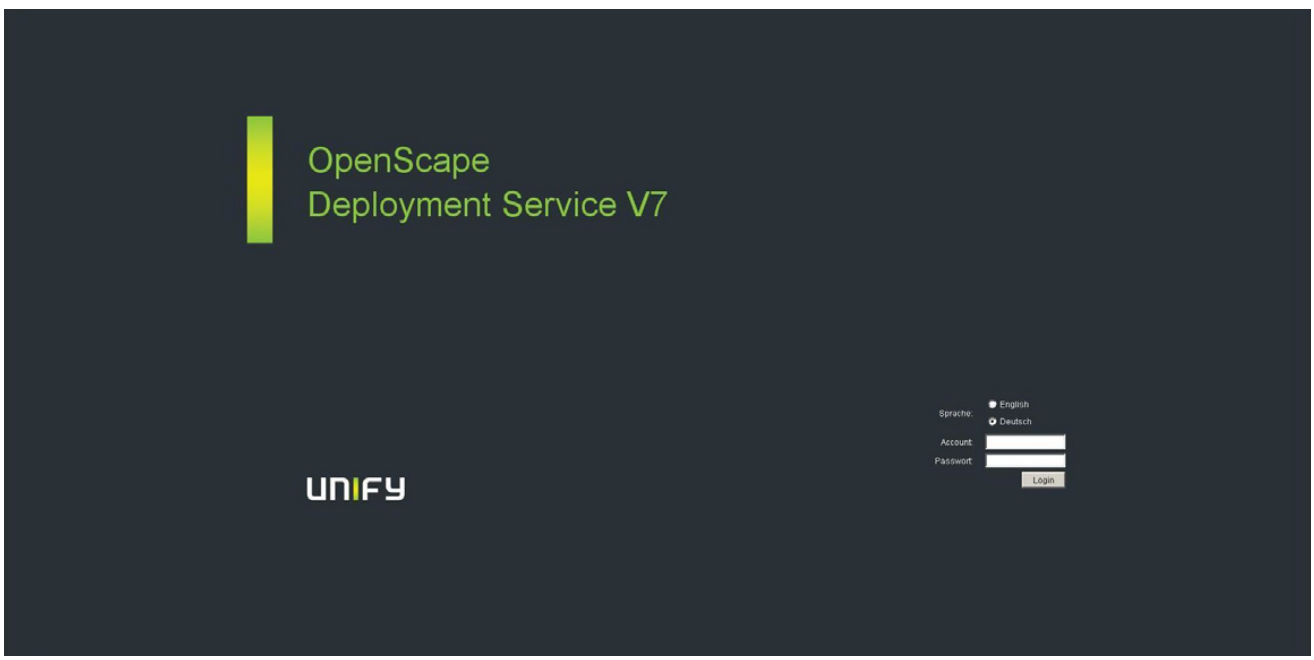
5 Die DLS-Benutzeroberfläche

5.1 Starten und einloggen

1. Geben Sie im Web-Browser eine der folgenden URLs ein:
   http:///[IP-Adresse]:18080/DeploymentService/
   oder
   https:///[IP-Adresse]:10443/DeploymentService/ (für verschlüsselte Verbindung)

   Geben Sie als [IP-Adresse] die IP-Adresse des Rechners ein, auf dem der Deployment Service läuft (DLS-Server).

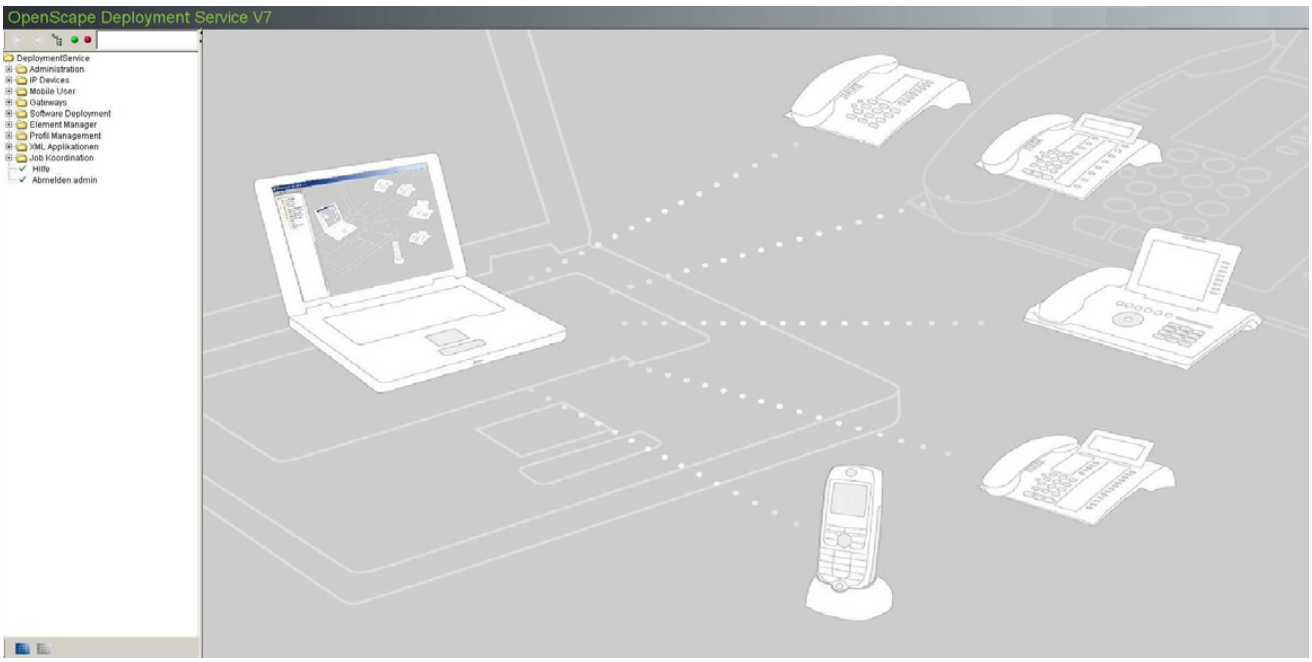
2. Das Login-Fenster wird angezeigt:



   Geben Sie bei **Account** „admin“ ein und bei **Passwort** das bei der Installation vergebene Passwort.

   Wählen Sie ggf. Ihre Sprache und bestätigen Sie mit **Login**.

3. Der Startbildschirm wird angezeigt:



HINWEIS: Die Kommunikation zwischen DLS-Server und **DLS-Client** wird mittels Portnummer **18080** oder **10443** (gesicherte Verbindung) hergestellt.
Beachten Sie, dass die Kommunikation zwischen DLS-Server und **IP Device** über die Ports **18443** (Default Modus) oder **18444** (Secure Modus) stattfindet.
Siehe dazu auch Abschnitt 7.5.4.4, “Register „DLS Verbindung“”.

5.2 Beenden

1. Wählen Sie im Hauptmenü (siehe Abschnitt 5.4.1) **Abmelden <account>**.
2. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Das Login-Fenster wird zum erneuten Einloggen wieder angezeigt.
3. Schließen Sie das Browser-Fenster.

5.3 Aufruf der kontextsensitiven Hilfe-Funktion

Zu jedem Thema der Oberfläche des DLS-Clients (Seite im Inhaltsbereich, siehe Abschnitt 5.4.2) kann diese Anleitung als Online-Hilfe aufgerufen werden. Wählen Sie dazu in der Menüleiste bei **Hilfe** den Eintrag **Maskenhilfe**.

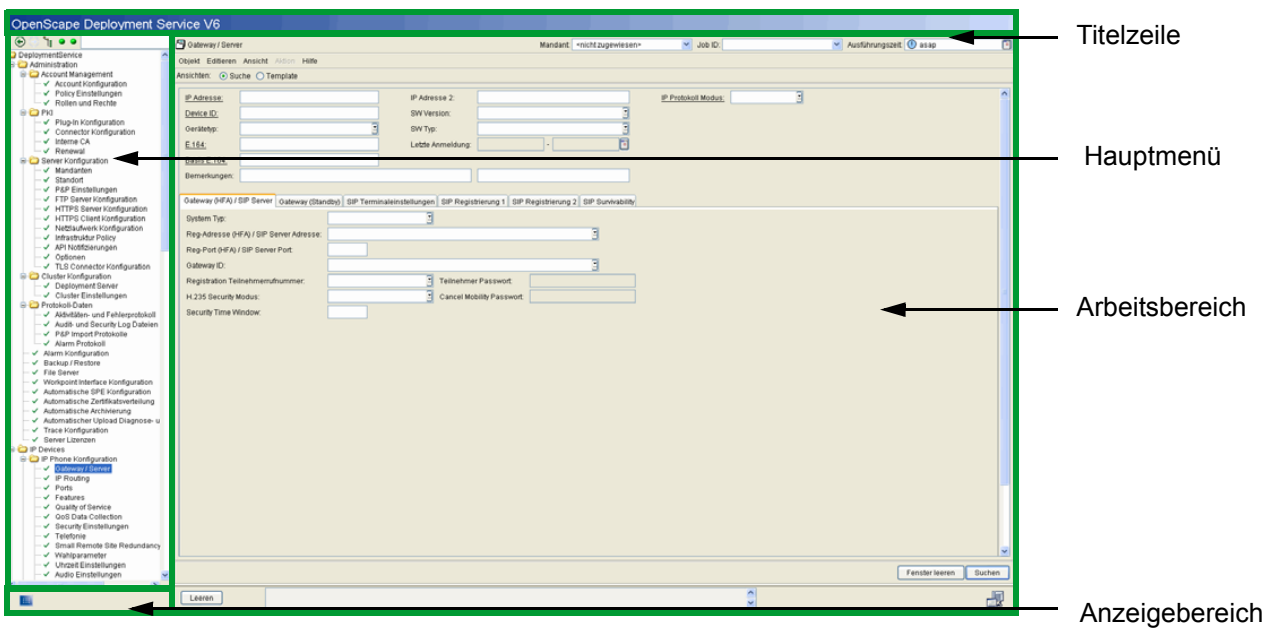
Für die lokale Version des DLS (OpenScape Deployment Service local) steht die Maskenhilfe nicht zur Verfügung. Es wird dann die allgemeine Hilfe aufgerufen.

Ohne ein spezielles Thema kann die Hilfe durch Klick auf **Help** im Hauptmenü (siehe Abschnitt 5.4.1) aufgerufen werden.

Die Hilfe wird in einem neuen Browser-Fenster angezeigt.

5.4 Anwendungsoberfläche

Die Anwendungsoberfläche besteht aus drei Teilen:

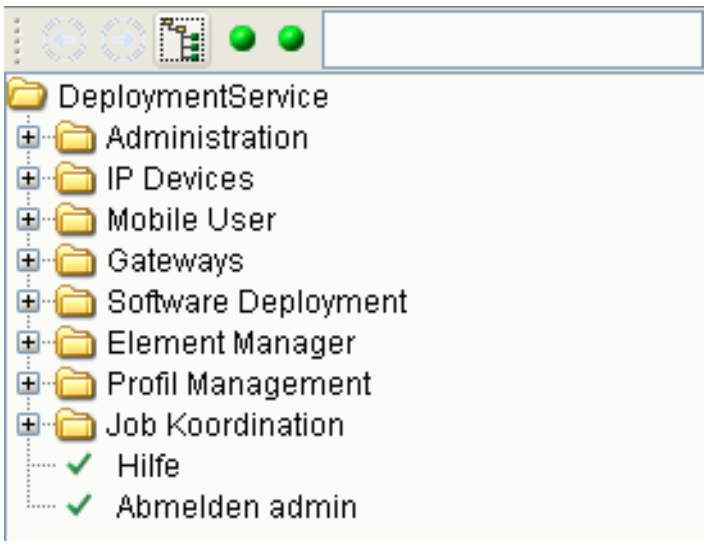


Die Position der Trennung zwischen Hauptmenü und Arbeitsbereich können Sie durch Klicken und Ziehen der Trennlinie ändern. Ein Klick auf eines der Pfeilsymbole im oberen Bereich der Trennlinie setzt die Trennung außerdem ganz nach rechts oder links, so dass der Arbeitsbereich oder das Hauptmenü ausgeblendet wird.

HINWEIS: Zum näheren Kennenlernen der Oberfläche können Sie auch den Bedienablauf in Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern” nutzen.

5.4.1 Hauptmenü

Der Aufbau dieses Handbuchs ist ab Kapitel 6, “Administration” größtenteils an die Struktur des Hauptmenüs angelehnt.



Das Hauptmenü enthält folgende Schaltflächen:

Mithilfe dieser Schaltflächen kann man zwischen bereits aufgerufenen Menüs navigieren. Die Zurück-Schaltfläche wird aktiv, sobald man ein Menü aufgerufen hat. Die Vor-Schaltfläche wird aktiv, sobald man einmal den Zurück-Button angeklickt hat.

Mit einem Klick auf diese Schaltfläche kann man alle Untermenüs auf- und zuklappen.

Die Statusanzeige für aktuelle Jobs wird bei jedem Serverzugriff aktualisiert, kann aber auch über ein PopUp-Menü angestoßen werden. Klicken Sie hierzu mit der rechten Maustaste auf das Anzeigefeld und wählen Sie im Popup-Menü **Status aktualisieren**. Soll ein bestimmter Job gezielt überwacht werden, empfiehlt es sich, die Statusanzeige zunächst per **Status zurücksetzen** in den Ausgangszustand zu versetzen. Mit **Jobs anzeigen** gelangen Sie in das Menü **Job Kontrolle** (); dort können Sie Details zu einzelnen Jobs sehen. Zeitgesteuerte Jobs werden erst dann in der Statusanzeige berücksichtigt, wenn sie gestartet sind.
Die Anzeige links informiert über laufende Jobs. Folgende Zustände sind möglich:
Es laufen keine Jobs.
Job läuft.
Die Anzeige rechts informiert über beendete und abgebrochene Jobs. Folgende Zustände sind möglich:
Jobs sind fehlerfrei durchgeführt worden.
Ein Job ist fehlgeschlagen. Wird der Job abgebrochen (siehe Abschnitt 14.1, “Job Kontrolle”), so wird die Anzeige wieder auf grün gesetzt.

Dieses Feld ermöglicht es dem Benutzer, Blätter von Baumeinträgen herauszufiltern, die der Suchzeichenfolge des DLS-Baum-Menüs entsprechen. Nur die gefilterten Blätter werden im Baum-Menü angezeigt.

Über das strukturierte Hauptmenü erreichen Sie alle Komponenten des DLS. Ein einfacher Klick auf das „+“ oder „-“ vor einem Verzeichnis-Symbol (oder Doppelklick auf den Verzeichnisnamen) öffnet oder schließt das Verzeichnis, ein Klick auf ein Inhalts-Symbol zeigt den Inhalt im Arbeitsbereich an.

Die Inhalts-Symbole können wie folgt aussehen:

- Verzeichnis mit weiteren Unterverzeichnissen und/oder Seiten.
- Seite im Normalzustand (Aktion fehlerfrei beendet oder noch nicht durchgeführt).
- Seite, in der momentan eine Aktion läuft (z. B. beim Scannen von IP Devices).
- Seite mit fehlerhaft beendeter Aktion.
- Seite wegen fehlender Account-Rechte gesperrt.

Zusätzlich enthält das Hauptmenü diese besonderen Funktionen:

- Hilfe

Öffnet die Online-Hilfe.

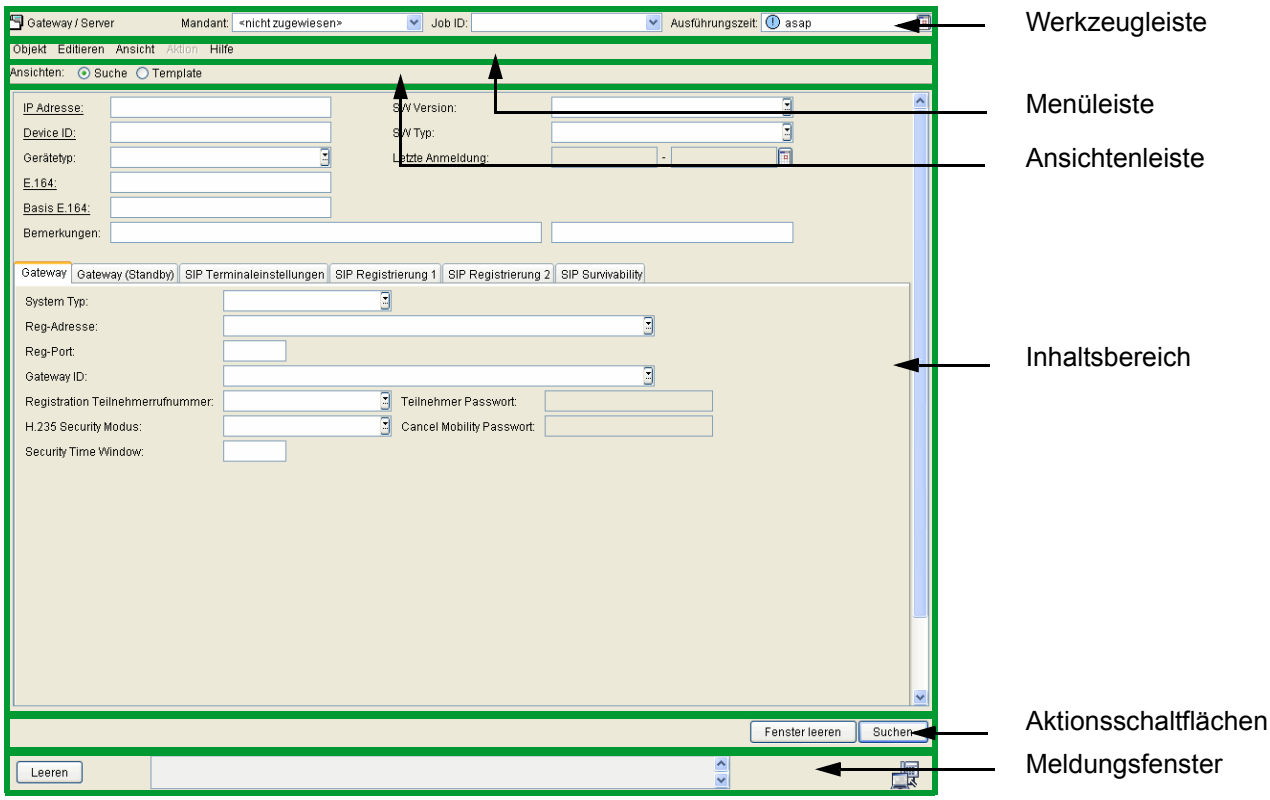
- Abmelden <account>

Abmelden des in <account> angezeigten Benutzers.

Weitere Symbole siehe Abschnitt 5.4.2.4, “Symbole neben Eingabefeldern”.

5.4.2 Arbeitsbereich

Rechts neben dem Hauptmenü befindet sich der Arbeitsbereich, der sich wie folgt gliedert:



5.4.2.1 Werkzeugleiste

Links wird angezeigt, welche Komponente aktuell aus dem Hauptmenü aufgerufen wurde.

Auf der rechten Seite werden die Elemente zu

- Mandanten
- Job ID
- Ausführungszeit

angezeigt.

Mandant

Es werden alle Mandanten angezeigt, die dem aktuellen Account zugeordnet sind. Für den Account 'admin' werden zusätzlich

- <alle> = alle Mandanten und
- <nicht zugewiesen> = Mandanten, die keinem Account zugewiesen sind,

angezeigt.

Job ID

Unter einem „Job" versteht man die Zusammenfassung von Deployment-Aktionen, die zu einem festgelegten Zeitpunkt ausgeführt werden.

HINWEIS: Die Umstellung von Sommerzeit auf Winterzeit (eine Stunde zurück) führt nicht zu einem erneuten Ausführen eines Jobs, der in dem dadurch verdoppelten Zeitintervall gestartet wurde. Allerdings wird bei der Umstellung von Winterzeit auf Sommerzeit (eine Stunde vor) ein Job, der in die dadurch übersprungene Zeit fällt, nicht ausgeführt.

Siehe hierzu auch die Oberflächenbeschreibung im Kapitel 14, "Job Koordination" und Ablaufbeschreibungen im Abschnitt 15.7, "Nutzen der Job-Koordination".

Ausführungszeit

Geben Sie die Ausführungszeit an. Standard ist „asap", d.h. der Job wird sofort ausgeführt. Durch Klicken auf das Kalendersymbol können Sie mithilfe eines separaten Kalender-Dialogfensters einen Zeitpunkt und Bedingungen für die Job-Ausführung festlegen.

5.4.2.2 Menüleiste

In der Menüleiste werden abhängig vom Inhaltsbereich unterschiedlich viele Einträge angezeigt.

HINWEIS: In vielen Fällen haben Sie verschiedene Möglichkeiten, um eine Funktion auszuführen. Beispielfunktion **Suche**: Mittels Menüleisteneintrag **Objekt**, über die gleichnamige Schaltfläche oder die Funktionstaste <F3>.

Die Menüleiste kann maximal folgende Einträge enthalten:

- **Objekt**
  - **Neu** (neuen Datensatz erstellen)
  - **Sichern** (Datensatz speichern, <F3>)
  - **Verwerfen** (Änderungen an einem Datensatz verwerfen)
  - **Löschen** (Datensatz löschen)
  - **Suche** (Datensatz suchen, <F3>)
  - **Kopieren** (Datensatz kopieren)
  - **Einfügen** (kopierten Datensatz einfügen)
- **Editieren**
  - **Verwerfen** (letzte Änderung in einer Seite des Inhaltsbereichs zurücknehmen)
  - **Fenster leeren** (alle Einträge einer Seite des Inhaltsbereichs löschen)
  - **Feld rückgängig** (letzte Änderung in einem Feld zurücknehmen)
  - **Ausschneiden** (markierten Inhalt ausschneiden)
  - **Kopieren** (markierten Inhalt kopieren)
  - **Einfügen** (markierten Inhalt einfügen)
  - **Auswahl aufheben** (Markierung entfernen)
  - **Alles markieren** (alle Objekte markieren)

- **Ansicht**
  - **Suche** (Suchansicht)
  - **Objekt** (Objektansicht)
  - **Tabelle** (Tabellenansicht)
  - **Neu** (Ansicht zum Neuanlegen)
  - **Template** (Vorlagenansicht)
  - **Gehe zu**
    - **Erstes Objekt** (zu erstem Datensatz springen)
    - **Vorheriges Objekt** (zu vorherigem Datensatz springen)
    - **Nächstes Objekt** (zu nächstem Datensatz springen)
    - **Letztes Objekt** (zu letztem Datensatz springen)
  - **verwandtes Objekt** (verwandte Objekte, <F4>)
  - **Auswahlliste** (Auswahlliste anzeigen, <F5>)
  - **Aktualisieren** (Ansicht aktualisieren)
- **Aktion**
  - **Job abbrechen** (laufenden Job abbrechen)
  - **Import Datei** (Job-Datei importieren)
  - **Export Datei** (Job-Datei exportieren)
  - **Template holen** (Template-Daten laden)
  - **Als Template sichern** (Template-Daten sichern)
  - **Template umbenennen** (Name eines gesicherten Templates ändern)
  - **Template löschen** (gesichertes Template löschen)
  - **In Template kopieren** (Daten in das Template kopieren)
  - **Template anwenden** (Template-Daten in aktuelle Ansicht übernehmen)
  - **Alle Templates generieren** (Für alle Objekte bzw. Masken des ausgewählten IP Device-Typs werden Templates generiert)
  - **Mobile User in Archiv speichern** (Daten des Mobile User in zip-Archiv speichern; siehe Abschnitt 16.13.10.2, “Mobile User:Daten speichern”)
  - **Mobile User aus Archiv laden** (Daten eines Mobile User aus zip-Archiv holen; siehe Abschnitt 16.13.10.3, “Mobile User-Daten laden”)

- **IP Device kopieren** (Daten eines IP Devices kopieren, siehe auch Abschnitt 16.5, “Austausch eines IP Devices”, Abschnitt 16.7, “Austausch von HFA- durch SIP-Software und umgekehrt bei identischer Device ID”, Abschnitt 16.12.7, “IP Phone austauschen”)
- **Ausgewählte IP Devices in Archiv speichern** (Daten eines ausgewählten IP Devices in zip-Archiv speichern)
- **IP Device aus Archiv laden** (Daten von IP Devices aus zip-Archiv holen)
- **Plug&Play simulieren** (Für ein ausgewähltes IP Device kann Plug&Play simuliert werden. Hierzu werden zunächst standortrelevante Daten eingegeben. Mit einem Klick auf **Plug&Play simulieren** kann dann kontrolliert werden, was an ein Telefon geschickt werden würde, das sich mit diesen Daten beim DLS anmeldet.)
- **Zertifikat importieren** (Importiert ein Zertifikat für das gewählte IP Device (nur in der Zertifikatsverwaltung verfügbar. Weitere Informationen siehe Abschnitt 16.12, “Security: Administration von Zertifikaten”.)
- **Zertifikat löschen** (Löscht ein Zertifikat für das gewählte IP Device; nur in der Zertifikatsverwaltung verfügbar. Weitere Informationen siehe Abschnitt 16.12, “Security: Administration von Zertifikaten”.)

- **Hilfe**
  - **Maskenhilfe** (kontextsensitive Hilfe zum DLS öffnen)
  - **Über...** (Information zum DLS)

5.4.2.3 Ansichtenleiste

Für manche Inhalte stehen mehrere Ansichten zur Verfügung.
Diese können Sie unterhalb der Menüleiste auswählen.

HINWEIS: Alle Optionen der Ansichtenleiste können Sie auch über das Menü **Ansicht** der Menüleiste aufrufen (siehe Abschnitt 5.4.2.2, “Menüleiste”).

Folgende Optionen stehen bei den Ansichten maximal zur Verfügung:

- **Suche**

  Zeigt im Inhaltsbereich eine Suchmaske zum Filtern einzelner IP Devices aus der Gesamtmenge der registrierten IP Devices. Siehe auch Abschnitt 5.5, “Suchfunktionalität”.

- **Objekt**

  Zeigt im Inhaltsbereich einen einzelnen Datensatz eines IP Devices an.

- **Tabelle**

  Zeigt im Inhaltsbereich alle verfügbaren Datensätze in einer Listenansicht an.

- **Neu**

  Legt einen neuen Datensatz an.

- **Template**

  Zeigt im Inhaltsbereich ein Template an, das abgespeichert und später zur Suche verwendet werden kann.

HINWEIS: Befinden Sie sich in der Ansicht **Suche**, können Sie alle Elemente ändern (z. B. in Feldern Werte eingeben oder Checkboxen aktivieren), um so Suchkriterien zu bestimmen oder Daten festzulegen.
In der Ansicht **Template** und **Neu** sind nur die in der DLS-Datenbank änder- und sicherbaren Daten editierbar, alle anderen Felder sind ausgegraut. Allgemeine Daten des Inhaltsbereiches können nicht als Template gesichert werden.
Werden Daten vorhandener IP Devices als Suchergebnis angezeigt (Ansicht **Objekt** oder **Tabelle**), sind in vielen Fällen einige Elemente nicht änderbar und werden ebenfalls ausgegraut dargestellt.

5.4.2.4 Inhaltsbereich

Hier werden Informationen angezeigt und Daten eingegeben oder ausgewählt.

HINWEIS: Bei der Parameterbeschreibung der Elemente im Inhaltsbereich (ab Abschnitt , “Administration”) wird, wenn erforderlich, zwischen den jeweils möglichen Ansichten unterschieden (siehe Abschnitt 5.4.2.3, “Ansichtenleiste”).
Hiervon ist abhängig, ob Elemente geändert oder nur angesehen werden können.

Register

Bei umfangreichen Inhalten, bei denen eine Gruppierung sinnvoll ist, können diese Inhalte mittels Registerblätter im Inhaltsbereich ausgewählt und angezeigt werden.

Klicken Sie auf das Register, dessen Inhalt Sie ansehen oder bearbeiten möchten. Informationen zu den Oberflächen aller Register finden Sie ab Kapitel 6, “Administration” bis Kapitel 14, “Job Koordination”.

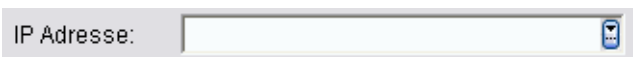
Die wichtigsten Bedienelemente

- **Textfeld**

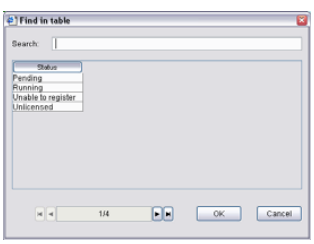
  

  Zur freien Anzeige und Eingabe von alphanumerischen Zeichen.

- **Auswahllistenfeld**

  Zur Auswahl eines Eintrags aus einer Liste und zur freien Eingabe.
  Wenn verfügbar, öffnet sich bei Klick auf die Listenschaltfläche rechts im Feld das Dialogfenster **Finde in Tabelle** mit mehreren Einträgen.

- **Auswahlfeld**

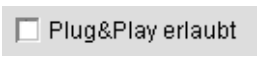
  

  Auf einen Wert klicken (z. B. `17`) und durch Klick auf die Pfeile den Wert vergrößern bzw. verkleinern.

- **Optionen**

Zur Auswahl einer von mehreren möglichen Optionen.

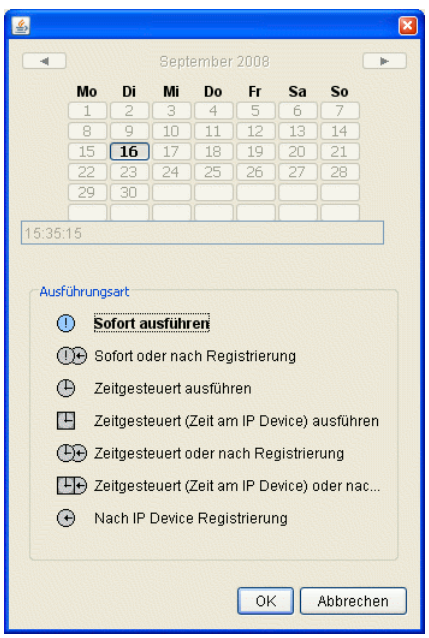
- **Checkbox**



Zur Aktivierung/Deaktivierung einer Eigenschaft. Für eine Checkbox in der Ansicht **Suche** gibt es auch den dritten Status „undefiniert“ (gerasterte Darstellung).

- **Zeitfeld mit Kalender-Schaltfläche und Ausführungsart**

Mit dieser Schaltfläche können Sie mithilfe eines separaten Kalender-Dialogfensters einen Zeitpunkt und Bedingungen für die Job-Ausführung festlegen.



Die folgenden Optionen stehen zur Verfügung:

- **Sofort ausführen**: Der Job wird sofort ausgeführt. Falls das IP Device nicht erreichbar ist, wird der Job abgebrochen.
- **Sofort oder nach Registrierung**: Der Job wird sofort ausgeführt. Falls das IP Device nicht erreichbar ist, wird der Job bei der Registrierung des IP Devices erneut gestartet.
- **Zeitgesteuert ausführen**: Der Job wird zu dem Zeitpunkt ausgeführt, der im Kalenderfeld angegeben ist.

- **Zeitgesteuert (Zeit am IP Device) ausführen**: Der Job wird zu dem Zeitpunkt ausgeführt, der im Kalenderfeld angegeben ist. Hier gilt jedoch nicht die Systemzeit des DLS-Servers, sondern die lokale Zeit im IP Device. Diese Option ist sinnvoll, wenn sich DLS-Server und IP Devices in verschiedenen Zeitzonen befinden.
- **Zeitgesteuert oder nach Registrierung**: Der Job wird zu dem Zeitpunkt ausgeführt, der im Kalenderfeld angegeben ist. Falls das IP Device nicht erreichbar ist, wird der Job bei der Registrierung des IP Devices erneut gestartet.
- **Zeitgesteuert (Zeit am IP Device) oder nach Registrierung**: Der Job wird zu dem Zeitpunkt ausgeführt, der im Kalenderfeld angegeben ist. Hier gilt jedoch nicht die Systemzeit des DLS-Servers, sondern die lokale Zeit im IP Device. Diese Option ist sinnvoll, wenn sich DLS-Server und IP Devices in verschiedenen Zeitzonen befinden. Falls das IP Device nicht erreichbar ist, wird der Job bei der Registrierung des IP Devices erneut gestartet.
- **Nach IP Device Registrierung**: Der Job wird ausgeführt, wenn sich das IP Device registriert hat.

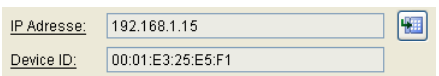
OK übernimmt die Werte in das Zeitfeld, **Abbrechen** schließt den Kalender ohne Datenübernahme.

- **Zeitfeld mit Kalender-Schaltfläche und Ausführungsart**

HINWEIS: Bitte beachten Sie, dass die Ausführung nicht neu berechnet wird, wenn das IP Device zwischenzeitlich in eine andere Zeitzone umgezogen wird.

- **WBM mit aktueller IP-Adresse öffnen**

  Durch Klick auf die Browser-Schaltfläche neben dem Feld **IP Adresse** wird das Web Based Management (WBM) des IP Devices mit dieser IP-Adresse in einem neuen Browser-Fenster geöffnet.



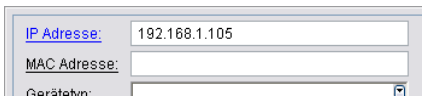
  Die Schaltfläche ist nur dann aktiv, wenn das Feld eine IP-Adresse enthält. Informationen zur Bedienung des WBMs finden Sie in der Administrationsanleitung zum IP Devices.

- **Weitere Symbolschaltflächen**

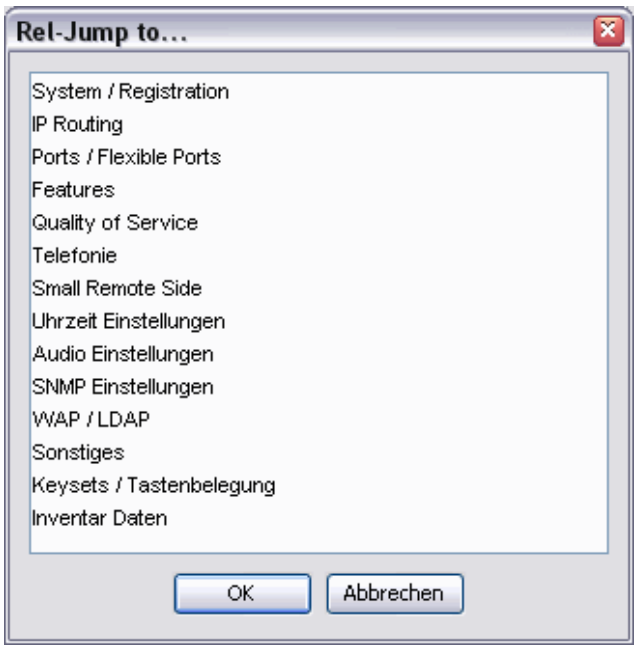
  Symbolschaltflächen (z. B. ) erscheinen innerhalb eines Objektes (z. B. für ein IP Phone), wenn pro Objekt mehrere Einträge vorhanden sind oder hinzugefügt werden können; siehe Abschnitt 5.4.2.4, “Mehrfachobjekte”.

- **Suche mit Parameter-Übernahme (Related Jump)**

  Durch eine Verlinkung in der Oberfläche kann komfortabel der eingetragene Wert bei verschiedenen Feldern (z. B. **IP Adresse** und **Device ID**) in weiteren Oberflächen unter **IP Devices** gesucht werden.



  Klicken Sie auf den unterstrichenen Link (wird beim Überfahren blau dargestellt).



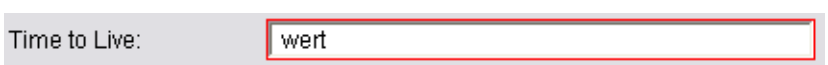
  Ein Dialogfenster mit einer Liste aller weiteren Themen zu **IP Devices** öffnet sich.
  Wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf **OK**. Die gewählte Oberfläche wird mit dem übertragenen Wert angezeigt und eine Suche automatisch durchgeführt.

Darstellung von Eingabefeldern

Elemente ohne direkte Eingabemöglichkeit werden ausgegraut dargestellt (siehe Textfeld bei Kalender-Schaltfläche). Ebenfalls ausgegraut werden Felder dargestellt, die in der aktuellen Konfiguration nicht relevant sind, z. B. ein SIP-Parameter bei einem HFA-IP Device.

Pflichtfelder werden schwarz umrahmt dargestellt.

Elemente, die einen ungültigen Wert enthalten, werden nach dem Verlassen des Feldes oder beim Ausführen einer Aktion rot umrahmt dargestellt.



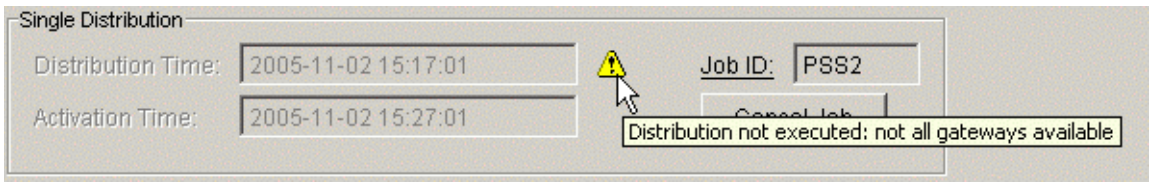
In diesem Fall korrigieren Sie den Wert und führen Sie die Aktion erneut durch.

Beim Überfahren von Elementen werden oftmals Hinweise am Mauszeiger, sogenannte „ToolTips“ angezeigt (Beispiel).

Letzte Anmeldung

Symbole neben Eingabefeldern

In bestimmten Situationen erscheinen neben einigen Eingabefeldern Symbole zur Information oder Warnung. Bei Überfahren des Symbols erscheint eine erklärende Meldung („ToolTip“). Beispiel:



Symbol	in Bereich Feld	Bedeutung
	IP Phone Konfiguration **IP Client Konfiguration** **Gerätetyp**	Die Authentisierung des IP Devices am DLS ist fehlgeschlagen. Die Ursache kann z. B. in einem unzureichenden Authentisierungsmodus liegen, siehe Abschnitt 7.5.4.4, “Register „DLS Verbindung“”.
	IP Phone Konfiguration **IP Client Konfiguration** **Device ID**	Die IP-Adresse ist von einem anderen Gerät belegt (IP-Adresskonflikt). Die Ursache liegt in vielen Fällen an einer Doppelbelegung durch den DHCP-Server.
	IP Phone Konfiguration **IP Client Konfiguration** **Gerätetyp**	Der angegebene Gerätetyp wird nicht unterstützt.
	Titelzeile **Alarme vorhanden**	Alarmhinweis für ausgewählte DLS-Benutzer. Weitere Informationen siehe Abschnitt 6.6, “Alarm Konfiguration”.
	IP Phone Konfiguration **E.164**	Das Telefon ist als Mobility Phone eingerichtet, es ist jedoch kein Mobile User angemeldet. Mehr zum Thema Mobility siehe Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.
	IP Phone Konfiguration **E.164**	Am IP Phone ist ein Mobile User angemeldet. Mehr zum Thema Mobility siehe Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.
	IP Phone Konfiguration **Gerätetyp**	Das aktuell konfigurierte Gerät ist noch nicht gesteckt, d. h. es ist ein virtuelles Gerät.
	IP Phone Konfiguration **IP Client Konfiguration** **IP Gateway Konfiguration** **Gerätetyp**	Das Gerät wurde über die API Schnittstelle gelöscht. Soll es weiterverwendet werden, kann es aus dem Papierkorb geholt werden, indem man **IP Device Daten Lesen** anstößt.

Tabelle 10 Hinweis- und Warnsymbole im Inhaltsbereich

Symbol	in Bereich Feld	Bedeutung
	**IP Phone Konfiguration** **IP Client Konfiguration** **Gerätetyp**	Das Synchronisierungs-Symbol, das nach einer Datenbank-Wiederherstellung auf allen physischen Geräten angezeigt wird (und angibt, dass die Geräte - wieder - in DLS registriert werden müssen), verschwindet auf angemeldeten Mobilgeräten erst nach Abmeldung, da die DLS-Datenbank und das Gerät erst dann miteinander synchronisiert werden. Diese Funktionsweise ist so gewünscht. Während ein Mobile User angemeldet ist, können die Daten des Basisgeräts nicht “gelesen” werden, da das Lesen der Daten über die aktive E.164-Nummer erfolgt. Durch Übermittlung der Status zwischen An- und Abmeldung können die Status der Pfeil-Symbole auch an der Benutzeroberfläche angezeigt werden.

Tabelle 10 Hinweis- und Warnsymbole im Inhaltsbereich

Ein Teil der Symbole wird auch in der Tabellenansicht in einer separaten Spalte angezeigt. Dadurch lassen sich IP Devices mit einer bestimmten Eigenschaft (z. B. Fehlermeldung) komfortabel sortieren und herausfiltern. Symbole werden ebenfalls im Hauptmenü (Abschnitt 5.4.1, “Hauptmenü”) und im Meldungsfenster (Abschnitt 5.4.2.6, “Meldungsfenster”) angezeigt.

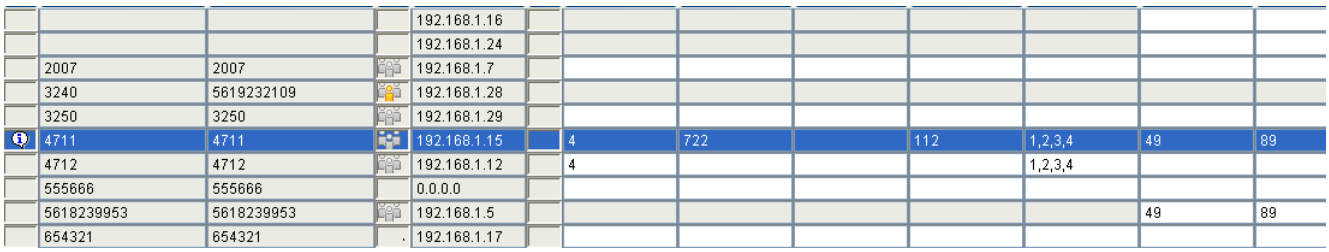
Mehrfachauswahl und Datenübernahme in der Tabellen-Ansicht

Wurden Änderungen im Bereich **IP Devices** vorgenommen, so können diese Änderungen auf weitere Geräte in der Suchauswahl übertragen werden.

HINWEIS: Stellen Sie sicher, dass bei der Nutzung des DLS-Client an einem PC mit dem Betriebssystem Windows XP das Farbschema „Blau (standard)“ beibehalten wird. Werden die Farbschemata „Olivgrün“ und „Silber“ verwendet, kann es zu Darstellungsproblemen von Listenanzeigen kommen.

Aufruf: „Eigenschaften von Anzeige“ > „Darstellung“ > „Farbschema“.

Wechseln Sie **vor** dem Sichern der Änderungen in die Ansicht **Tabelle**. Der Eintrag mit den geänderten Parametern wird dunkelblau dargestellt.

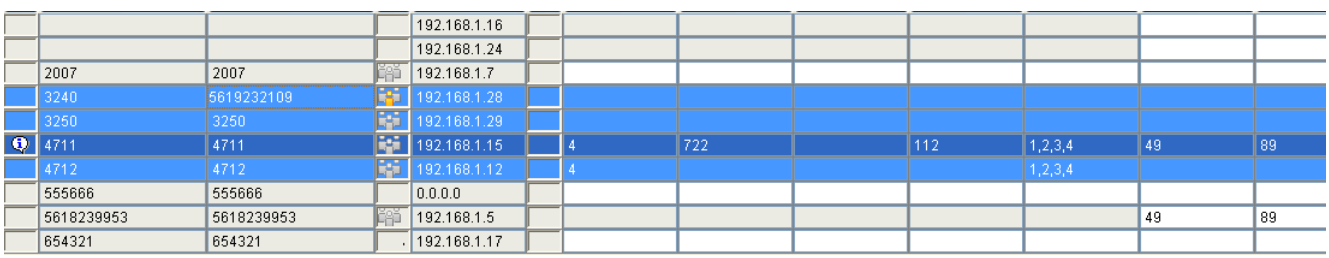


			192.168.1.16								
			192.168.1.24								
2007	2007		192.168.1.7								
3240	5619232109		192.168.1.28								
3250	3250		192.168.1.29								
4711	4711		192.168.1.15	4	722		112	1,2,3,4	49	89	
4712	4712		192.168.1.12	4				1,2,3,4			
555666	555666		0.0.0.0								
5618239953	5618239953		192.168.1.5						49	89	
654321	654321		192.168.1.17								

Wählen Sie weitere IP Devices aus, für die die Änderungen auch gelten sollen:

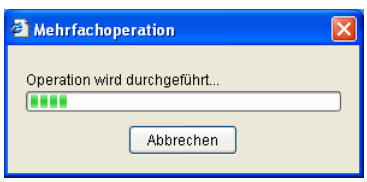
- Bei Klick mit gedrückter <UMSCHALT>-Taste werden alle Zeilen zwischen den beiden gewählten Zeilen markiert (einschl. der beiden Zeilen).
- Bei Klick mit gedrückter <STRG>-Taste können Sie einzelne Einträge zur Auswahl hinzufügen oder wegnehmen.
- Bei Auswahl von **Editieren** – **Alles markieren** aus der Menüleiste können Sie alle Einträge zur Auswahl hinzufügen.

Alle weiteren Einträge werden hellblau dargestellt.



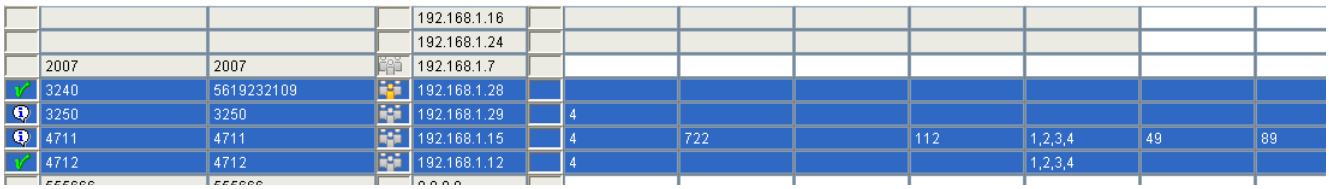
			192.168.1.16								
			192.168.1.24								
2007	2007		192.168.1.7								
3240	5619232109		192.168.1.28								
3250	3250		192.168.1.29								
4711	4711		192.168.1.15	4	722		112	1,2,3,4	49	89	
4712	4712		192.168.1.12	4				1,2,3,4			
555666	555666		0.0.0.0								
5618239953	5618239953		192.168.1.5						49	89	
654321	654321		192.168.1.17								

Klicken Sie auf Sichern, um die Daten zu übernehmen.



Durch Klick auf **Abbrechen** werden die Änderungen am aktuellen IP Device noch beendet, aber kein darüber hinaus keine weiteren Daten übernommen. Zum Fortsetzen starten Sie den gesamten Vorgang neu.

Nach erfolgreicher Datenübernahme wird für jeden betroffenen Eintrag ein grüner Haken angezeigt. Für diejenigen Einträge, bei denen der Job noch nicht abgeschlossen ist, erscheint ein Notiz-Symbol.



				192.168.1.16							
				192.168.1.24							
	2007	2007		192.168.1.7							
✓	3240	5619232109		192.168.1.28							
?	3250	3250		192.168.1.29	4						
?	4711	4711		192.168.1.15	4	722		112	1,2,3,4	49	89
✓	4712	4712		192.168.1.12	4				1,2,3,4		

Individuelle Anpassung der Tabellendarstellung

Der Benutzer kann die Tabellenansicht nach seinen Bedürfnissen einrichten. Diese Einstellungen werden benutzerspezifisch in der DLS-Datenbank gespeichert, so dass der DLS-Account auf jedem Client seine individuellen Einstellungen zur Verfügung hat.

Um die Reihenfolge der Tabellenspalten zu ändern, klicken Sie mit der linken Maustaste auf den Titel einer Spalte und ziehen Sie die Spalte an die gewünschte Stelle (Drag and Drop).

Um die Breite einer Spalte anzupassen, bewegen Sie den Mauszeiger an einen der Ränder des Spaltentitels. Sobald der Zeiger zu einem Doppelpfeil wird, drücken Sie die linke Maustaste und ziehen Sie den Rand an die gewünschte Stelle.

Außerdem können Sie festlegen, welche Spalten angezeigt werden und welche Spalten in ihrer Position fixiert sein sollen. Klicken Sie hierzu mit der rechten Maustaste auf den Spaltentitel. Es öffnet sich ein Kontextmenü, mit dessen Hilfe Sie die gewünschten Einstellungen vornehmen können.

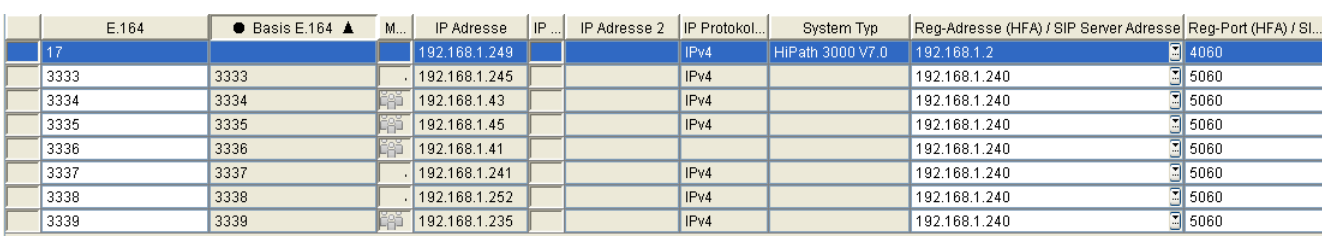
HINWEIS: Möglicherweise werden die individuellen Tabelleneinstellungen bei einem Update des DLS zurückgesetzt, falls durch das Update Objekte in der Datenbank geändert werden.

Sortierung über mehrere Spalten

Der Benutzer hat die Möglichkeit, mehr als eine Spalte für die Sortierung in der Tabellenansicht auszuwählen. Alle ausgewählten Spalten werden kombiniert.

Die erste ausgewählte Spalte wird als Hauptsortierspalte verwendet, alle weiteren ausgewählten Spalten werden Untersortierspalten.

Die Hauptspalte wird durch klicken mit der linken Maustaste in den Spaltenkopf ausgewählt. Alle folgenden Untersortierspalten werden durch gleichzeitiges Drücken der Umschalttaste (bzw. Hochstelltaste) und der linken Maustaste im Spaltenkopf ausgewählt. Die Hauptsortierspalte wird durch einen Punkt vor der Spaltenüberschrift markiert. Die Sortierreihenfolge (aufsteigend, absteigend) wird durch einen Pfeil nach oben oder nach unten rechts neben der Spaltenüberschrift markiert. Durch erneutes Klicken in den Spaltenkopf wird die Sortierreihenfolge umgekehrt.



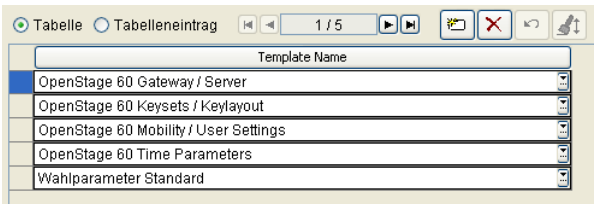
	E.164	● Basis E.164 ▲	M...	IP Adresse	IP ...	IP Adresse 2	IP Protokol...	System Typ	Reg-Adresse (HFA) / SIP Server Adresse	Reg-Port (HFA) / SI...
	17			192.168.1.249			IPv4	HiPath 3000 V7.0	192.168.1.2	4060
	3333	3333		192.168.1.245			IPv4		192.168.1.240	5060
	3334	3334		192.168.1.43			IPv4		192.168.1.240	5060
	3335	3335		192.168.1.45			IPv4		192.168.1.240	5060
	3336	3336		192.168.1.41					192.168.1.240	5060
	3337	3337		192.168.1.241			IPv4		192.168.1.240	5060
	3338	3338		192.168.1.252			IPv4		192.168.1.240	5060
	3339	3339		192.168.1.235			IPv4		192.168.1.240	5060

Die Auswahl von zusätzlichen Spalten als Untersortierspalten kann sinnvoll sein, wenn die Hauptsortierspalte mehrere gleiche Werte enthält.

Mehrere Spalten können nur in der Tabellenansicht von Objekten ausgewählt werden. Für Tabellen im Inhaltsbereich, die einem bestimmten Objekt zugeordnet sind, steht diese Funktion nicht zur Verfügung. Bei diesen Tabellen kann nur die Sortierreihenfolge geändert werden.

Mehrfachobjekte

Bei einigen Objekten können pro Objekt wiederum mehrere verschiedene Einträge erstellt und angezeigt werden, z. B. bei Profil Management > Geräteprofil > Register „Templates“.



Die Schaltflächen haben folgende Bedeutung:

Fügt einen neuen Eintrag hinzu.

Löscht alle markierten Einträge.

Macht letzte Änderungen an markierten Einträgen rückgängig und entfernt Markierung.

Übernimmt den Inhalt der aktuellen Zeile (Zeile mit Cursor) in alle markierten Einträge.

In der Spalte ganz links wird die aktuelle Zeile in dunklerem Grau markiert. Folgende Symbole sind möglich:

- * (Sternchen): Der Eintrag wurde geändert aber noch nicht gesichert.
- + (Plus): Der Eintrag wurde hinzugefügt aber noch nicht gesichert.
- - (Minus): Der Eintrag wurde gelöscht aber noch nicht gesichert.

In diesen Fällen kann mit die Änderung rückgängig gemacht werden. .

Zum Übernehmen von Daten einer Zeile in weitere Zeilen gilt Folgendes:

- Die Daten werden aus der aktuellen Zeile (Zeile mit Cursor) übernommen.
- Die Daten werden in allen markierten Zeilen übernommen.
- Bei Klick mit gedrückter <UMSCHALT>-Taste werden alle Zeilen zwischen den beiden gewählten Zeilen markiert (einschl. der beiden Zeilen).
- Bei Klick mit gedrückter <STRG>-Taste können Sie einzelne Zeilen zur Markierung hinzufügen oder wegnehmen.
- Bei Klick auf die Schaltfläche werden die Daten übernommen (alle geänderten Zeilen erhalten ein * (Sternchen) bis zur nächsten Sicherung).

5.4.2.5 Aktionsschaltflächen

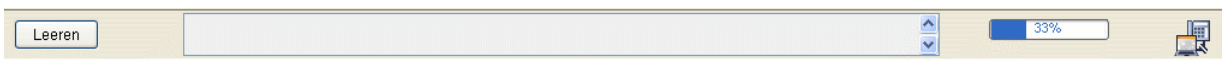
Abhängig vom Inhaltsbereich können Sie mit den Aktionsschaltflächen die erforderlichen Aktionen durchführen.

In der Ansicht **Objekt** und **Tabelle** wird eine Navigation zur Auswahl von Datensätzen angezeigt. Bei einer Einfachauswahl wird im linken Feld die Nummer des selektierten Datensatzes angezeigt und im rechten Fenster die Gesamtanzahl der Datensätze in der Tabelle. Bei einer Mehrfachauswahl wird im linken Feld die höchste Nummer der selektierten Datensätze angezeigt und im rechten Feld die Gesamtanzahl der Datensätze in der Tabelle, gefolgt von der Anzahl der selektierten Datensätze in Klammern.

Weitere Informationen zur Bedienung der DLS-Oberfläche finden Sie Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”.

5.4.2.6 Meldungsfenster

Nach dem Starten einer Aktion werden hier Status- und Fehlermeldungen ausgegeben sowie der Fortschritt der Durchführung angezeigt.



Meldungen werden durch Symbole kategorisiert:

 Eine Warnmeldung wird z. B. bei erfolgloser Suche angezeigt.

 Angezeigt wird eine Fehlermeldung, z. B. bei der Eingabe eines ungültigen Wertes.

Alle ausgegebenen Meldungen können Sie jederzeit mit **Leeren** löschen.

Bei bestimmten Aktionen, wie z. B. dem Scannen von IP Devices, wird auf der rechten Seite ein Fortschrittbalken angezeigt.

Die Größe des Meldungsfensters können Sie durch Klicken und Ziehen der Trennlinie zwischen Meldungsfenster und dem restlichen Arbeitsbereich ändern.

5.4.3 Anzeigebereich

Dieser Bereich informiert über die Auslastung jedes einzelnen Knotens im DLS-Cluster. In der dazugehörigen DLS-Maske wird der Name jedes Knotens und die Anzahl der Anfragen für jeden Knoten während der letzten Stunde angezeigt. Die Anzeige steht auch bei Single Node-Konfigurationen zur Verfügung; in diesem Fall ist sie unveränderlich, wobei die Anzahl der Anfragen ein wichtiger Hinweis in Überlastsituationen sein kann.

HINWEIS: Diese Funktion steht nur für den Administrator zur Verfügung.

Im Anzeigebereich werden für jeden Knoten des Clusters folgende Symbole verwendet:

 Server läuft mit voller Kapazität.

 Server läuft mit halber Kapazität. Das ist der Fall, wenn

- die Anzahl der Anfragen geringer ist als 50% der maximalen Anzahl und
- die Differenz zwischen der maximalen und der tatsächlichen Anzahl der Anfragen größer ist als 10.

 Server ist stillgelegt.

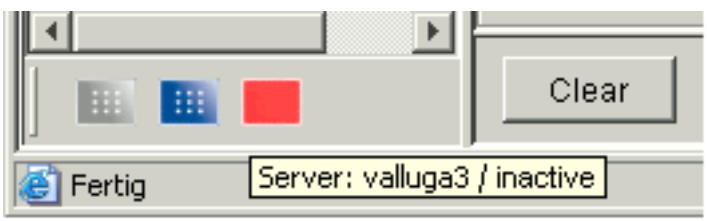
Zwei verschiedene Ansichten stehen zur Verfügung.

Basis-Ansicht

Die Basis-Ansicht (Standard) zeigt die Knoten des DLS Clusters als Serversymbole in der linken unteren Ecke an. Die Namen der DLS-Knoten und die Anzahl der Anfragen während der letzten Stunde werden als Tooltip angezeigt.

Dieses Beispiel zeigt einen mit „valluga2“ benannten Knoten, der mit voller Kapazität läuft und in der letzten Stunde 49 Anfragen erhalten hat:

In diesem Beispiel wurde der DLS-Knoten „valluga3“ in den Cluster integriert, ist aber zurzeit nicht in Betrieb:

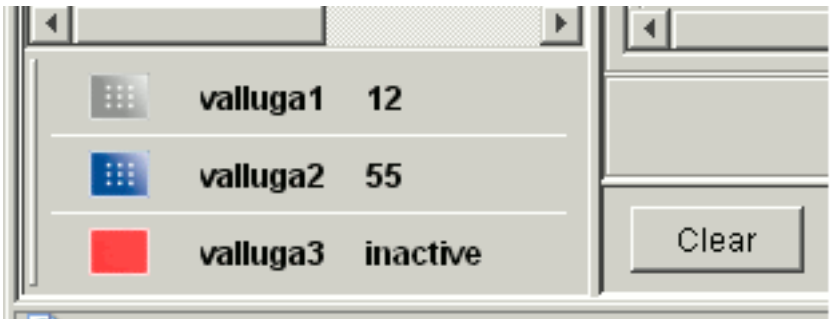


Erweiterte Ansicht

Um in die erweiterte Ansicht zu gelangen, klicken Sie mit der rechten Maustaste auf ein Serversymbol. Es öffnet sich das DLS Cluster-Menü, in welchem Sie **Ansicht wechseln** auswählen.

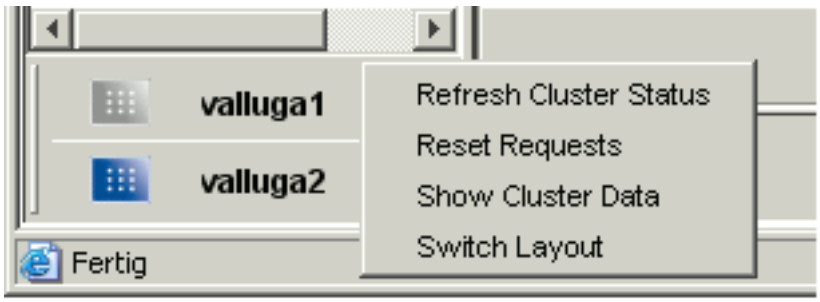
Die erweiterte Ansicht zeigt detaillierte Informationen wie die Namen der DLS-Knoten und die Anzahl der Anfragen an.

Im folgenden Beispiel läuft ein Knoten mit halber Kapazität, einer mit voller Kapazität, und ein Knoten ist außer Betrieb.



Cluster-Menü

Wenn Sie in der Basis-Ansicht oder der erweiterten Ansicht mit der rechten Maustaste auf ein Serversymbol klicken, erhalten Sie das DLS Cluster-Menü.



Hier stehen folgende Funktionen zur Verfügung:

- **Cluster Status aktualisieren**: Aktualisiert die Daten (Symbol, Anzahl der Anfragen) für alle Knoten.
- **Requests zurücksetzen**: Setzt für alle Knoten die Anzahl der Anfragen auf 0.
- **Cluster Daten anzeigen**: Leitet weiter zu **Administration** > **Cluster Konfiguration** > **Deployment Server**.
- **Ansicht wechseln**: Wechselt zwischen Basis-Ansicht und erweiterter Ansicht.

5.5 Suchfunktionalität

In der Ansicht **Suche** können Sie in allen Textlistenfeldern folgende „Jokerzeichen“ (=Wildcards) bzw. Sonderzeichen nutzen. Alle Felder werden intern durch ein logisches UND verknüpft. Wenn Sie z. B. einen Gerätetyp und einen IP-Adressbereich angeben, werden nur die IP Phones ausgewählt, die dem angegebenen Gerätetyp entsprechen und zum angegebenen IP-Adressbereich gehören. Bei der Suche innerhalb von Tabellen im Inhaltsbereich (Embedded Tables) werden alle Objekte gefunden, die mindestens dem Suchkriterium entsprechen. Diese Objekte werden nach der Suche vollständig angezeigt.

- * (Sternchen): Steht für ein oder mehrere beliebige Zeichen. Die Kombination mit ‚Jokern’ (=Wildcards) ist zulässig. So sind z. B. Teileingaben wie 192.168.* für einen IP-Adressbereich von 192.168.0.0 bis 192.168.255.255 möglich.
- ? (Fragezeichen): Steht für genau ein beliebiges Zeichen. Die Kombination mit ‚Jokern’ (=Wildcards) ist zulässig. Zum Beispiel: ab??c findet alle Sätze, bei denen das Feld 5 Zeichen lang ist, mit ab beginnt und mit c endet.
- ^ (Dach): Steht für leeres Feld. Es darf nicht mit „Jokern“ verwendet werden. Zum Beispiel: ^ findet Sätze mit einem leeren Feld, a^a findet Sätze, die die Zeichenkette „a^a“ enthalten.
- ! (Ausrufezeichen): Wenn es als erstes Zeichen einer Zeichenkette steht, wird die Suche verneint. So findet „!Suchtext“ alle Datensätze, in denen im betreffenden Feld etwas anderes als „Suchtext“ steht. Das Ausrufezeichen kann mit *, ? und | kombiniert werden. Soll ‚!’ als erstes Zeichen gesucht werden, so ist dieses durch ein vorangestelltes ‚\’ zu markieren. Die Kombination mit ‚Jokern’ (=Wildcards) ist zulässig. Zum Beispiel: !a* findet alle Sätze, in denen das Feld nicht mit a startet.
- < (kleiner): Wenn als erstes Zeichen einer Zeichenkette „<Suchtext“ steht, liefert die Suche nur Werte, die kleiner als „Suchtext“ sind. Soll ‚<’ als erstes Zeichen gesucht werden, so ist dieses durch ein vorangestelltes ‚\’ zu markieren. Die Kombination mit ‚Jokern’ (=Wildcards) ist zulässig. Zum Beispiel: <100 findet alle Sätze, in denen der Inhalt des Feldes kleiner 100 ist.
- > (größer): Wenn als erstes Zeichen einer Zeichenkette „>Suchtext“ steht, liefert die Suche nur Werte, die größer als „Suchtext“ sind. Soll ‚>’ als erstes Zeichen gesucht werden, so ist dieses durch ein vorangestelltes ‚\’ zu markieren. Die Kombination mit ‚Jokern’ (=Wildcards) ist zulässig. Zum Beispiel: >München findet alle Sätze, die größer München sind, das sind etwa Paris, Oslo, aber nicht Berlin, Athen.
- | (senkrechter Strich): Hierdurch können unterschiedliche Suchtexte voneinander getrennt und so für die ODER-Suche genutzt werden. Dabei werden alle Elemente, die aus „Suchtext1|Suchtext2|Suchtext3“ bestehen, gesucht. Die Kombination mit ‚Jokern’ (=Wildcards) ist nicht zulässig. Die ODER-Suche kann durch Voranstellen von ‚!’ verneint werden. Dabei werden alle Elemente gesucht, die nicht aus “Suchtext1|Suchtext2|Suchtext3” bestehen. Soll nach ‚|’ gesucht werden, so ist dieses durch ein vorangestelltes ‚\’ zu markieren. Zum Beispiel: abc|def|ghi findet alle Sätze, in denen das Feld abc ODER def ODER ghi enthält. !abc|def|ghi findet alle Sätze, in denen das Feld alles außer abc ODER def ODER ghi enthält.

6 Administration

Aufruf: Hauptmenü > Administration

Im Bereich **Administration** werden grundsätzliche Einstellungen zum Betrieb des DLS vorgenommen.

Dieses Menü besteht aus folgenden Untermenüs:

- Account Management
- PKI
- Server Konfiguration
- Cluster Konfiguration
- Protokoll-Daten
- Alarm Konfiguration
- Backup / Restore
- File Server
- Workpoint Interface Konfiguration
- Automatische SPE Konfiguration
- Automatische Zertifikatsverteilung
- Automatische Archivierung
- Automatischer Upload Diagnose- und Security Log Dateien
- Trace Konfiguration
- Server Lizenzen

6.1 Account Management

Dieser Bereich besteht aus folgenden Inhalten:

- Account Konfiguration
- Policy Einstellungen
- Rollen und Rechte

Bei Administration und Wartung ist es hilfreich, Aufträge auf mehrere Personen aufzuteilen. Diese können verschiedenen Accounts (Benutzerkennungen) erhalten. Aus Sicherheitsgründen ist es aber nicht erwünscht, dass jeder Account Zugang zu allen Bereichen des DLS erhält. Deshalb können die einzelnen Bereiche für jeden Account individuell erlaubt oder gesperrt werden.

Jeder Administrationsfunktion des DLS wird ein Zugangsrecht zugeordnet, und nur Accounts mit diesem Zugangsrecht wird erlaubt, die entsprechende Funktion aufzurufen. In Einzelfällen können mehrere Funktionen in einem Recht zusammengefasst sein, so ist auch mit dem Recht Jobs anzulegen das Recht verbunden, Jobs zu bearbeiten, d. h. den Job Status zu aktualisieren, den Job zurückzusetzen usw.

Es gibt keine Rechte, die einen Zugang explizit verweigern.

Der DLS bietet ein Rollen-Konzept an. Jede Rolle bündelt eine Anzahl von Rechten. Es können beliebig viele Rollen definiert werden, je nach Bedarf.

Einige wichtige Rollen sind vom System vorgegeben und können weder geändert noch gelöscht werden, nur der Beschreibungstext kann geändert werden. Diese System-Rollen dienen in erster Linie als Bausteine für selbstdefinierte Rollen. Nicht jede dieser System-Rollen ist für sich allein genommen sinnvoll verwendbar.

Jedem Account können nach Bedarf beliebig Rollen zugeordnet werden. Das Zugangsrecht des Account ist die Summe aller Rechte aller Rollen des Account.

Nach der Neuinstallation des DLS gibt es einen „admin“-Account, dem auf Basis von Systemrollen alle Rechte zugeordnet sind. Dieser Account selbst kann nicht gelöscht oder umbenannt werden, und die Systemrollen können ihm nicht entzogen werden.

Wenn der Benutzer sich nach erfolgter Installation zum ersten Mal mit dem Administratorkonto über den Assistant an der DLS-Benutzeroberfläche anmeldet, muss er das Standard-Passwort aus Sicherheitsgründen ändern. Dabei muss das Passwort auch im Assistant aktualisiert werden.

Bei einer Update-Installation eines DLS ohne Account Management zu einem DLS mit Account Management wird ein „admin“-Account mit allen systemdefinierten Rollen eingerichtet. Dieser Account besitzt somit alle Rechte. Allen anderen Accounts wird die INFO-Rolle zugeordnet, die es erlaubt alle Masken zu öffen und darin zu suchen, alle anderen Funktionen sind gesperrt. Weitere Rollen und Rechte müssen manuell hinzugefügt werden.

Bei zukünftigen Upgrade-Installationen des DLS werden neue Funktionen und neue Masken ausschließlich den Systemrollen zur Verfügung gestellt. Selbst definierte Rollen müssen von Hand mit den neu vorhandenen Rechten versehen werden. Daher wird empfohlen, eine neue Rechtekombination aus einer Kombination von Systemrollen und kleinen eigenen Rollen zu erzielen, anstatt durch Kopieren und Modifizieren einer Systemrolle.

Beispiel

Ziel: ein Account soll Edit-Rechte (außer Massenänderungen und Templateerstellung) ausschließlich bei Gateways haben.

- Variante A: Neue Rolle auf Basis einer leeren Rechtezuordnung definieren.
- Variante B: Neue Rolle mit EDIT_ONE als Basis definieren und in allen in Frage kommenden Masken (Gateway Konfiguration, QoS Data Collection) zusätzlich das ‚Suchen'-Recht setzen.
- Variante C: Neue Rolle definieren mit Suchen-Recht für alle Gateway-Masken (Gateway Konfiguration, QoS Data Collection) PLUS System-Rolle EDIT_ONE.

Nur in der Variante C erhält der Account automatisch das Recht, neu hinzugekommene Funktionen innerhalb der drei Gateway-Masken zu nutzen.

HINWEIS: Änderungen in aktuell verwendeten Rollen stehen erst nach dem nächsten Login zur Verfügung.

6.1.1 Account Konfiguration

Aufruf: Administration > Account Management > Account Konfiguration

Hier können Sie zusätzliche Accounts einrichten, Passwörter ändern, sowie einzelnen Accounts bestimmte Rollen zuweisen oder entziehen. Ist die Mandantenfähigkeit installiert worden, können einem Account ein oder mehrere Mandanten zugeordnet werden.

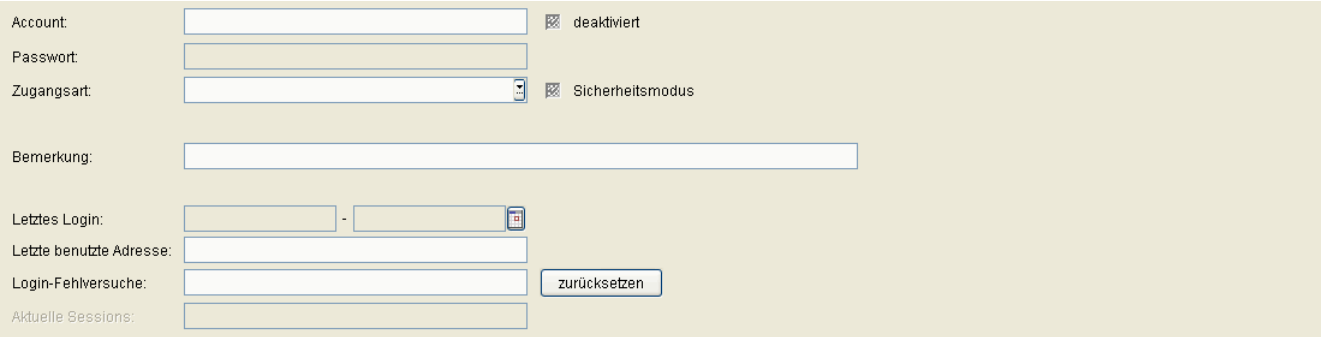
Nur solche Accounts, die das Recht zum Account-Management besitzen, können Änderungen an Accounts vornehmen, d. h. neue Accounts einrichten, ändern oder bestehende Accounts löschen.

Wenn die Mandantenfähigkeit genutzt wird, wird empfohlen, die Rolle Account Management nur an solche Accounts zu vergeben, die **alle** Mandanten bearbeiten dürfen. Hat der Account nicht Berechtigungen für alle Mandanten, kann er nicht alle angelegten Accounts sehen. Dadurch kann es vorkommen, dass der Benutzer dieses Accounts versucht, einen neuen Account mit einem bereits vorhandenden Namen anzulegen. In einem solchen Fall erscheint eine entsprechende Fehlermeldung, und der Account wird nicht angelegt.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Rollen“
- Register „Rechte“
- Register „Mandanten“
- Register „Windows Anwender“

Allgemeine Daten



Account:

Name des Accounts (Benutzerkontos).

deaktiviert

Dieser Schalter ist aktiviert, wenn dieser Account gesperrt ist.

Passwort:

Neues (geändertes) Passwort für diesen Account.

Das Passwort sollte mindestens sechs Zeichen lang und nicht trivial sein. Ungeeignet sind Einträge, die in Lexika oder Wörterbüchern zu finden sind. Ideal sind Kombinationen aus Zahlen, Sonderzeichen und Buchstaben, die jedoch keinen persönlichen Bezug haben.

Zugangsart:

Auswahl der erlaubten Schnittstellen zum DLS-Server.

Mögliche Optionen:

- **DLS-GUI**
  Der Zugriff auf den DLS-Server wird ausschließlich über die DLS-Benutzeroberfläche erlaubt.
- **DLS-API (Webservice Interface)**
  Der Zugriff auf den DLS-Server wird ausschließlich über die Programmierschnittstelle erlaubt.

HINWEIS: Zur Verwendung der Programmierschnittstelle des DLS (DLS-API) siehe Abschnitt 16.11, “Steuern des DLS über die Programmschnittstelle (DlsAPI)”.

Sicherheitsmodus

Ist dieser Schalter aktiviert, müssen bestimmte Konfigurationsänderungen, die zum Ausfall des IP Devices führen können, in einem zusätzlichen Dialogfenster bestätigt werden.

Bemerkung:

Feld für allgemeine Informationen.

Letztes Login

Zeigt Datum und Uhrzeit des letzten erfolgreichen Logins an.

Letzte benutzte Adresse

Adresse, von der der letzte (erfolgreiche oder gescheiterte) Loginversuch erfolgte.

Login-Fehlversuche

Anzahl der Fehlversuche seit dem letzten erfolgreichen Login.

zurücksetzen

Setzt die Anzahl der Login-Fehlversuche zurück, um den Account zu entsperren.

Aktuelle Sessions

Zeigt die Anzahl der aktuell genutzten Sessions an.

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen eingerichteten Accounts, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Legt einen neuen Account an.

Sichern

Sichert die eingegebenen/geänderten Daten.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Löschen

Löscht einen oder mehrere Accounts (Mehrfachauswahl in Tabellenansicht möglich. Der „admin“´-Account kann nicht gelöscht werden.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.1.1.1 Register „Rollen“

Aufruf: Administration > Account Management > Account Konfiguration > Register „Rollen“

Rolle

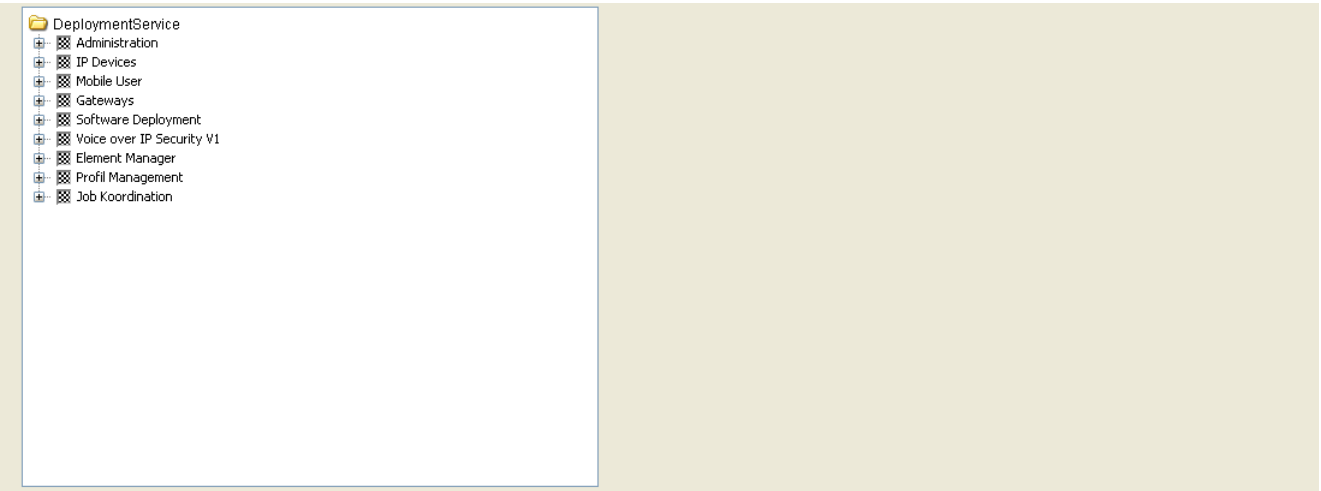
Name der Rolle, die diesem Account zugeordnet ist. Systemdefinierte Rollen können im „admin“-Account nicht gelöscht werden.

Beschreibung

Detaillierte Beschreibung der Rolle.

6.1.1.2 Register „Rechte“

Aufruf: Administration > Account Management > Account Konfiguration > Register „Rechte“

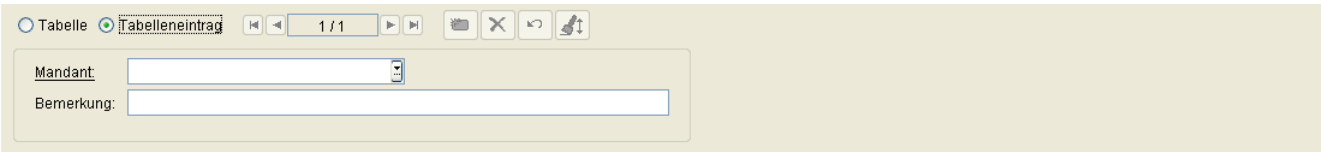


Hier wird die Summe der Rechte aus den verschiedenen zugewiesenen Rollen je Account angezeigt.

6.1.1.3 Register „Mandanten“

Aufruf: Administration > Account Management > Account Konfiguration > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.



Mandant

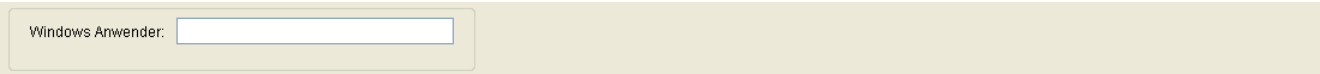
Name des Mandanten, der diesem Account zugeordnet ist.

Bemerkung

Bemerkung zum Mandanten.

6.1.1.4 Register „Windows Anwender“

Aufruf: Administration > Account Management > Account Konfiguration > Register „Windows Anwender“



Windows Anwender

Name des Windows Anwenders, der diesem DLS Account zugeordnet ist. Verschiedene Windows Anwender können dem gleichen DLS Account zugeordnet werden, ein Windows Anwender kann aber nur einem DLS Account zugeordnet werden.

6.1.2 Policy Einstellungen

Aufruf: Administration > Account Management > Policy Einstellungen

In diesem Bereich werden Richtlinien für die Passwörter der Benutzer (Accounts) des DLS festgelegt, wie beispielsweise Länge und Gehalt an Sonderzeichen.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Passwort Policy“
- Register „Login Policy“
- Register „Session Policy“

Allgemeine Daten

Zugangsart:

Die Passwort Policy gilt für die hier angezeigte Zugangsart. Um auf eine andere Zugangsart umzuschalten, verwenden Sie die Navigation im Bereich der Aktionsschaltflächen:

Mögliche Werte:

- **kein Zugang**
  Dieser Account ist gesperrt.
- **DLS-GUI**
  Der Zugang zum DLS-Server ist ausschließlich über die DLS-Benutzerschnittstelle erlaubt.
- **DLS-API (Webservice Interface**
)Der Zugang zum DLS-Server ist ausschließlich über die Programmierschnittstelle erlaubt.

HINWEIS: Zur Verwendung der Programmierschnittstelle des DLS (DLS-API) siehe Abschnitt 16.11, “Steuern des DLS über die Programmschnittstelle (DlsAPI)”.

Mögliche Aktionsschaltflächen

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Sichern

Sichert die eingegebenen/geänderten Daten.

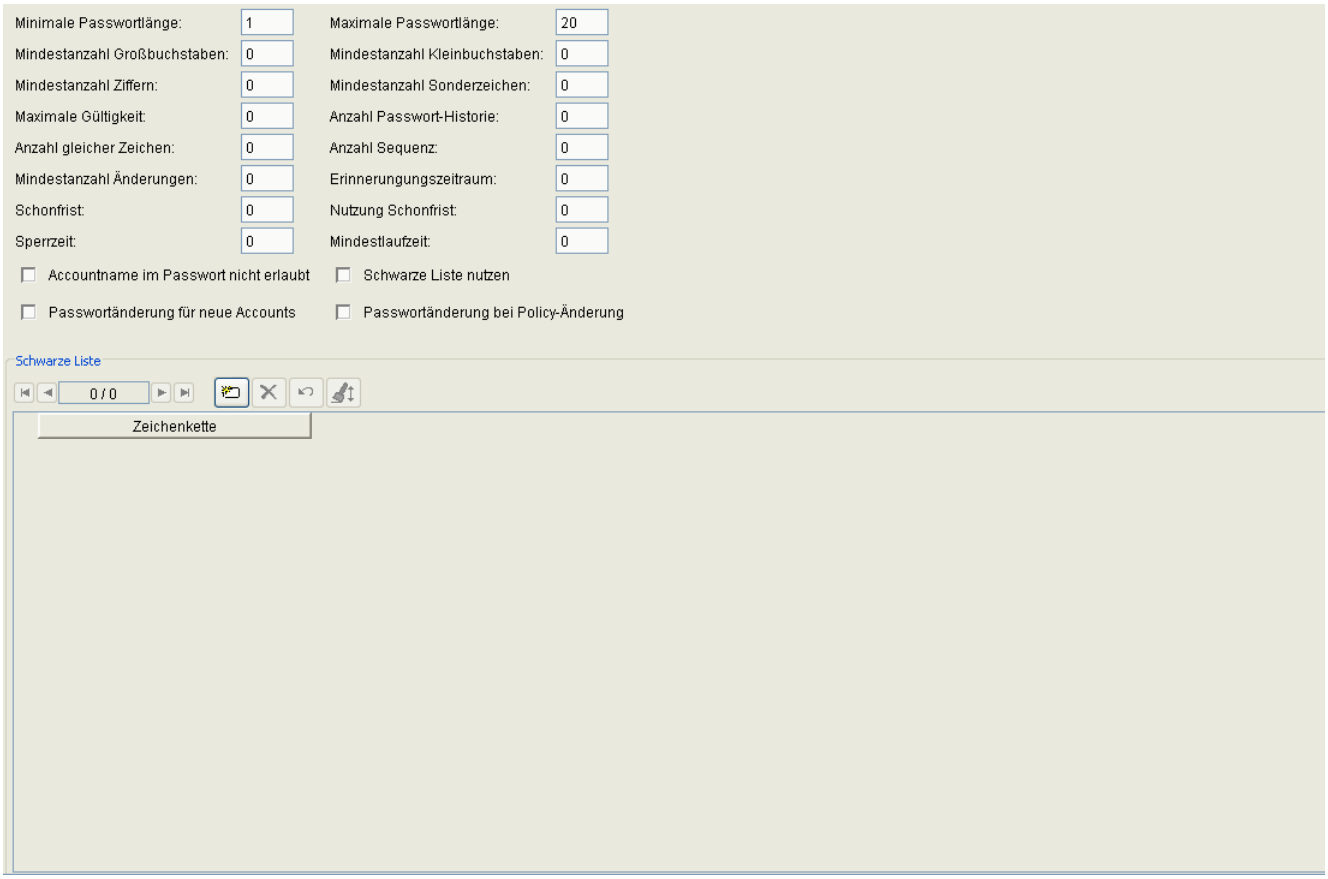
Aktualisieren

Aktualisiert den Inhalt dieser Maske aus der Datenbank.

6.1.2.1 Register „Passwort Policy“

Aufruf: Administration > Account Management > Policy Einstellungen > Register „Passwort Policy“

In diesem Bereich werden Richtlinien für die Passwörter der DLS-Benutzer (Accounts) des DLS festgelegt, etwa Länge und Gehalt an Sonderzeichen.



Minimale Passwortlänge

Minimale Länge des Passworts.

Wertebereich: **1** - **20**

Standard: **1**

Maximale Passwortlänge

Maximale Länge des Passworts.

Wertebereich: **1** - **20**

Standard: **20**

Mindestanzahl Großbuchstaben

Minimale Anzahl von Großbuchstaben im Passwort.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Kleinbuchstaben

Minimale Anzahl von Kleinbuchstaben im Passwort.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Ziffern

Minimale Anzahl von Ziffern im Passwort.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Sonderzeichen

Minimale Anzahl von Sonderzeichen im Passwort.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Maximale Gültigkeit

Maximale Gültigkeitsdauer des Passworts in Tagen. Der Wert muss größer sein als der für **Erinnerungszeitraum**.

Wertebereich: **0** - **180**

Standardwert: **0** (= Keine Prüfung)

Anzahl Passwort-Historie:

Anzahl der gespeicherten alten Passwörter, die nicht wiederverwendet werden können.

Wertebereich: **0** - **10**

Standardwert: **0** (= Keine Prüfung)

Anzahl gleicher Zeichen:

Erlaubte Anzahl aufeinanderfolgender gleicher Zeichen.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Anzahl Sequenz

Anzahl von aufeinander folgenden Zeichen mit auf- oder absteigendem Wert.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Änderungen

Mindestanzahl an Zeichen, die bei einer Passwortänderung geändert werden müssen.

Wertebereich: **0** - **20**

Erinnerungszeitraum

Zeitraum vor Ablauf eines Passwortes, innerhalb dessen die Nutzer daran erinnert werden, dass eine Passwortänderung fällig wird. Der Wert muss kleiner sein als der für **Maximale Gültigkeit**.

Wertebereich: **0** - **30**

Schonfrist

Frist in Tagen, innerhalb derer ein abgelaufenes Passwort weiter benutzt werden darf.

Wertebereich: **0** - **90**

Nutzung Schonfrist

Anzahl von Logins, bei denen ein abgelaufenes Passwort weiter benutzt werden darf

Wertebereich: **0** - **3**

Sperrzeit

Zeit in Tagen, in denen ein einmal benutztes Passwort nicht erneut vom selben Account genutzt werden darf.

Wertebereich: **0** - **180**

Standard **0** (= keine Prüfung)

Mindestlaufzeit

Zeit in Stunden, in der ein Passwort nicht erneut geändert werden darf

Wertebereich: **0** - **168**

Accountname im Passwort nicht erlaubt

Ist dieser Schalter gesetzt, so wird überprüft, ob der Accountname, weder in korrekter noch in umgekehrter Buchstabenfolge, Teil des Passworts ist. Ist das der Fall, so wird das Passwort nicht akzeptiert. Standard: keine Prüfung.

Schwarze Liste nutzen

Ist dieser Schalter gesetzt, wird das gewünschte Passwort gegen die Schwarze Liste überprüft (siehe **Zeichenkette**). Standard: keine Prüfung.

Passwortänderung für neue Accounts

Ist dieser Schalter gesetzt, muss beim ersten Logon eines neu eingerichteten Accounts das Passwort geändert werden.

Der betreffende GUI-Benutzer kann sich mit dem vordefinierten Passwort einloggen und wird dann über ein Meldungsfenster aufgefordert, das Passwort zu ändern. Bis dahin sind alle anderen Funktionen gesperrt.

Ein betreffender API-Benutzer kann sich zunächst nicht mehr einloggen. Hierzu muss ein GUI-Benutzer mit den entsprechenden Account Management-Rechten das Passwort des API-Accounts ändern. Standard: nicht gesetzt (keine Passwortänderung notwendig.

Passwortänderung bei Policy-Änderung

Ist dieser Schalter gesetzt, muss ein Passwort beim nächsten Logon geändert werden, falls es nicht mehr der aktuellen Passwort-Policy entspricht.

Der betreffende GUI-Benutzer kann sich mit dem alten Passwort einloggen und wird dann über ein Meldungsfenster aufgefordert, das Passwort zu ändern. Bis dahin sind alle anderen Funktionen gesperrt.

Ein betreffender API-Benutzer kann sich zunächst nicht mehr einloggen. Hierzu muss ein GUI-Benutzer mit den entsprechenden Account Management-Rechten das Passwort des API-Accounts ändern. Standard: gesetzt (Passwortänderung ist notwendig).

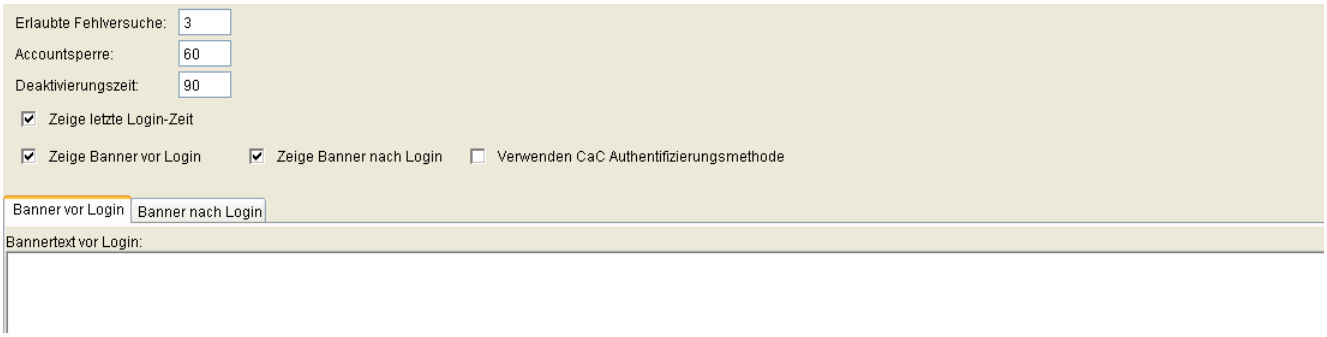
Schwarze Liste

Zeichenkette

Liste mit benutzerdefinierten Zeichenketten, die nicht in einem neu definierten Passwort vorkommen dürfen (Schwarze Liste). Die Prüfung unterscheidet nicht zwischen Klein- und Großbuchstaben.

6.1.2.2 Register „Login Policy“

Aufruf: Administration > Account Management > Policy Einstellungen > Register „Login Policy“



Erlaubte Fehlversuche

Erlaubte Anzahl aufeinanderfolgender Login-Fehlversuche. Wird diese Anzahl überschritten, so wird der Account für die in **Accountsperre** eingestellte Zeit gesperrt.

Wertebereich: **2** - **5**

Accountsperre

Wenn die erlaubte Anzahl von Fehlversuchen (**Erlaubte Fehlversuche**) überschritten ist, so wird Account für die hier eingestellte Zeit (in Sekunden) gesperrt.

Wertebereich: **0** - **300**

Deaktivierungszeit

Wenn ein Account für die hier angegebene Anzahl von Tagen nicht benutzt wurde, so wird er gesperrt.

Wertebereich: **0** - **180**

Zeige letzte Login-Zeit

Wenn aktiv, wird bei jedem erfolgreichen Login der Zeitpunkt des letzten Logins in einem eigenem Dialogfenster angezeigt.

Zeige Banner vor Login

Ist der Schalter aktiv, wird der Vor-Login-Bannertext nach dem Starten eines neuen DLS-Clients angezeigt.

Zeige Banner nach Login

Wenn aktiv, wird der Nach-Login-Bannertext nach jedem Login angezeigt.

Verwenden CaC Authentifizierungsmethode

Mit diesem Schalter wird die Authentifikation über Windows Anwendername und CaC PIN aktiviert. Standardmässig ist die Authenfikation über DLS Account und Passwort eingeschaltet. Die beiden Authentifikationsmethoden sollen an einem DLS nicht gleichzeitig aktiviert sein.

Bannertext vor Login

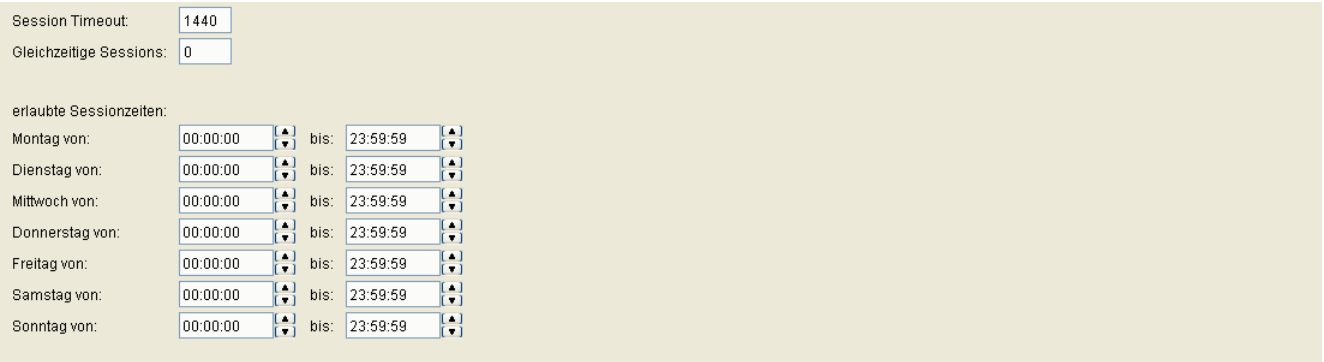
Text für das Vor-Login-Banner, der nach dem Starten eines neuen Clients gezeigt wird. Es wird empfohlen, den Text zweisprachig zu verfassen.

Bannertext nach Login

Text für das Nach-Login-Banner, der nach jedem Login gezeigt wird. Es wird empfohlen, den Text zweisprachig zu verfassen.

6.1.2.3 Register „Session Policy“

Aufruf: Administration > Account Management > Policy Einstellungen > Register „Session Policy“



Session Timeout

Bei Inaktivität werden Sessions nach dieser Zeit (in Minuten) geschlossen

Wertebereich: **5** - **999999**

Standardwert: **1440**

Gleichzeitige Sessions

Erlaubte Anzahl von Sessions eines Accounts zur gleichen Zeit.

(**0** = keine Grenze)

erlaubte Sessionzeiten

Außerhalb der hier definierten Sessionzeiten darf sich außer dem Administrator kein Account anmelden.

Montag... Sonntag von ... bis

Beginn und Ende der erlaubten Sessionzeit für jeden Tag.

6.1.3 Rollen und Rechte

Aufruf: Administration > Account Management > Rollen und Rechte

Hier können Sie Rollen mit den entsprechenden Rechten neu einrichten oder bestehende ändern. Systemdefinierte Rollen können weder geändert noch gelöscht werden.

Die folgenden Rollen sind vom System vorgegeben und können weder geändert noch gelöscht werden.

Rolle	Rechte	Gewichtung
ACCOUNT_MGM	Alle vorhandenen Rechte für den Bereich **Account Konfiguration**.	90
EDIT_BULK	Alle Editierrechte (neu, löschen und ändern) für alle Masken, außer für: • Rollen und Rechte • Account Konfiguration • alle Template-Aktivitäten Diese Rolle ist für den Standard-Administrator geeignet. In der Regel ist diese Rolle nicht eigenständig nutzbar, sondern muss mit einer anderen Rolle kombiniert werden oder dient als Basis für die Definition einer eigenen Rolle.	60
EDIT_GENERAL_ONE	Alle Editierrechte für nicht systembezogene Masken, ohne die Möglichkeit der Mehrfachänderung. Diese Rolle ist in der Regel nicht eigenständig nutzbar, sondern muss mit einer anderen Rolle kombiniert werden oder dient als Basis für die Definition einer eigenen Rolle.	20
EDIT_ONE	Wie EDIT_BULK, jedoch ohne die Möglichkeit zur Mehrfachauswahl.	40
EDIT_PKI	Alle Editierfunktionen für PKI-relvante Masken. Diese Rolle ist in der Regel nicht eigenständig nutzbar, sondern muss mit einer anderen Rolle kombiniert werden oder dient als Basis für die Definition einer eigenen Rolle.	98
EDIT_SYSTEM	Alle Editierrechte für systembezogene Masken (etwa Backup/Restore ohne Mehrfachauswahl), außer für: • **Rollen und Rechte** • **Account Konfiguration** Diese Rolle ist in der Regel nicht eigenständig nutzbar, sondern muss mit einer anderen Rolle kombiniert werden oder dient als Basis für die Definition einer eigenen Rolle.	30
INFO	Recht zum Anzeigen und Suchen von Daten in allen verfügbaren Masken, keine Editierberechtigung.	10
INFO_GENERAL	Recht zum Anzeigen und Suchen von Daten in allen nicht-systembezogenen Masken (etwa Backup/Restore), keine Editierberechtigung.	0
INFO_PKI	Recht zum Anzeigen und Suchen von PKI relevanten Masken, keine Editierberechtigung.	15
INFO_SYSTEM	Recht zum Anzeigen und Suchen von Daten in allen systembezogenen Masken, keine Editierberechtigung..	5
ROLE_MGM	Alle vorhandenen Rechte für den Bereich **Rollen und Rechte**.	99

Rolle	Rechte	Gewichtung
SECURITY_MGM	Recht zum Bearbeiten von Security-Einstellungen. Bei der Installation werden alle Security-relevanten Funktionen dieser Systemrolle zugeordnet; dies kann nicht verändert werden. Diese Rolle wird dem Account „admin“ zugeordnet. Jeder Account, dem beide Rollen ACCOUNT_MGM und SECURITY_MGM zugeordnet sind, kann die Rolle SECURITY_MGM anderen Accounts zuweisen. Accounts, die nur über eine dieser Rollen verfügen, können diese Zuweisung nicht vornehmen. Jeder Account, dem beide Rollen ROLE_MGM und SECURITY_MGM zugeordnet sind, kann Security-relevante Funktionen nicht-System-Rollen zuweisen. Accounts, die nur über eine der beiden erwähnten Rollen verfügen, können dies nicht. Security-relevante Funktionen werden nur dann in der Benutzeroberfläche angezeigt, wenn jeweils angemeldete Account das Recht hat, Security-relevante Funktionen auszuführen.	100
TEMPLATE_MGM	Recht zum Bearbeiten von Templates. Gilt in allen Bereichen, in denen Templates verfügbar sind. Diese Rolle ist in der Regel nicht eigenständig nutzbar, sondern muss mit einer anderen Rolle kombiniert werden oder dient als Basis für die Definition einer eigenen Rolle.	50

Um Rollen anlegen zu können, benötigen Sie einen Account, der die Rolle ROLE_MGM enthält. Sie können jeder neuen Rolle einen benutzerdefinierten Namen und eine beliebige Kombination aus Rechten zuweisen.

Sobald eine Rolle in der Maske **Rollen und Rechte** angezeigt wird, können Sie diese kopieren, indem Sie **Neu** klicken, unter **Rollenname** einen neuen Namen vergeben und anschließend auf **Sichern** klicken.

Um Rollen zu Accounts hinzuzufügen oder aus Accounts zu entfernen, benötigen Sie einen Account, der die Rolle ACCOUNT_MGM enthält.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Rechte“
- Register „Policy Einstellungen“

Allgemeine Daten

Rollenname

Name der Rolle, deren Rechte festgelegt werden sollen.

Vom System definierte Rolle

Zeigt an, ob es sich um eine vom System definierte Rolle handelt. Derartige Rollen können nicht geändert oder gelöscht werden.

Beschreibung:

Detaillierte Beschreibung der Rolle.

Wird nur in der Objekt-Darstellung angezeigt.

Gewichtung der Rolle

Die Rollen werden gewichtet. Wenn für wenigstens eine der Rollen, die einem Account zugeordnet sind, eigene Policy-Einstellungen gemacht wurden, werden die Policy-Einstellungen der Rolle mit der größten Gewichtung gültig und überschreiben die globalen Policy-Einstellungen dieses Accounts. Die Gewichtungen der system definierten Rollen sind in der Tabelle Rollen-Rechte oberhalb beschrieben. Diese Gewichtungen können nicht geändert werden.

Alle Gewichtungen von benutzerdefinierten Rollen können von Accounts mit der Rolle ROLE_MGM geändert werden. Die Standard-Gewichtung für benutzerdefinierte Rollen ist **0**.

Wird nur in der Tabellen-Darstellung angezeigt.

Wertebereich: **0** - **100**

System Policy anwenden

Wenn aktiviert, werden alle spezifischen Policy-Einstellung dieser Rolle ignoriert.

Wird nur in der Tabellen-Darstellung angezeigt.

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen eingerichteten Rechten, die den Suchkriterien entsprechen.

Bei der Suche nach Rechten haben die Checkboxen folgende Bedeutung:

 Suche nach aktivem Recht.

 Recht wird bei der Suche nicht berücksichtigt.

 Recht wird bei der Suche nicht berücksichtigt.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Legt einen neuen Account an.

Sichern

Sichert die eingegebenen/geänderten Daten.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Löschen

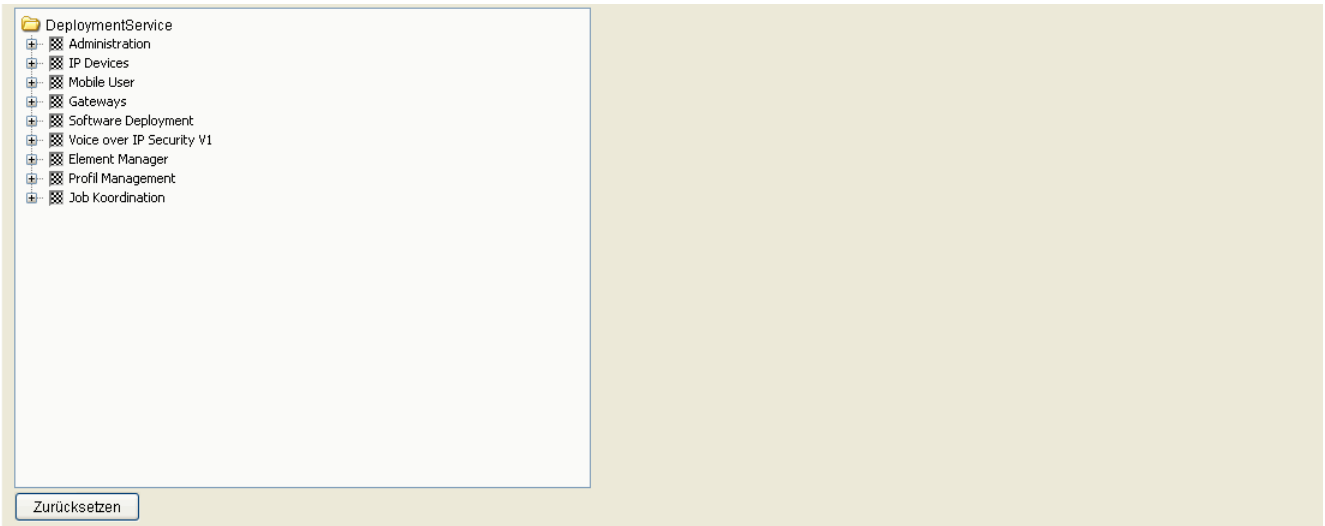
Löscht eines oder mehrere Rechte (Mehrfachauswahl in Tabellenansicht möglich).

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.1.3.1 Register „Rechte“

Aufruf: Administration > Account Management > Rollen und Rechte > Register „Rechte“



Rechte

Die Rechte können auf Funktionslevel vergeben werden.

Mögliche Optionen:

Bereich: Recht ist aktiv für diesen Bereich. Untermenü: Recht ist aktiv in allen Bereichen dieses Untermenüs.

Bereich: Recht ist nicht aktiv für diesen Bereich. Untermenü: Recht ist in keinem Bereichen dieses Untermenüs aktiv.

Untermenü: Recht ist in mindestens einem Bereich dieses Untermenüs aktiv.

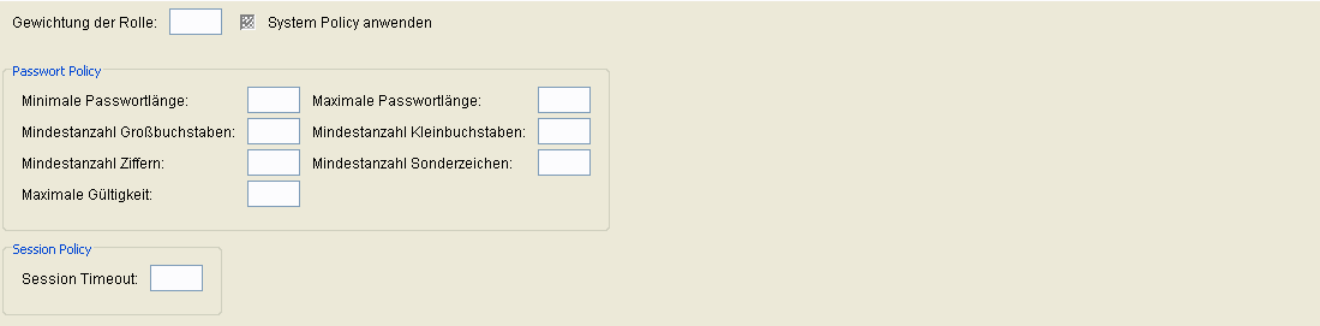
Recht ist undefiniert.

Zurücksetzen

Mit diesem Button können alle Felder auf nicht aktiv gesetzt werden.

6.1.3.2 Register „Policy Einstellungen“

Aufruf: Administration > Account Management > Rollen und Rechte > Register „Policy Einstellungen“



Gewichtung der Rolle

Je umfangreicher die Rechte der Rolle sind, desto höher sollte die Gewichtung sein. Die rollenabhängigen Einstellungen werden auf die Accounts übertragen.

Wertebereich: **1** - **100**

System Policy anwenden

Wenn aktiviert, werden globale System-Policy-Einstellungen anstatt rollenabhängiger Einstellungen verwendet.

Passwort Policy

Minimale Passwortlänge

Minimale Länge für ein Passwort.

Wertebereich: **1** - **20**

Standard: **1**

Maximale Passwortlänge

Maximale Länge für ein Passworts.

Wertebereich: **1** - **20**

Standard: **20**

Mindestanzahl Großbuchstaben

Minimale Anzahl von Großbuchstaben, die das Passwort enthalten muss.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Kleinbuchstaben

Minimale Anzahl von Kleinbuchstaben, die das Passwort enthalten muss.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Ziffern

Mindestanzahl Ziffern, die das Passwort enthalten muss.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Mindestanzahl Sonderzeichen

Mindestanzahl an Sonderzeichen, die das Passwort enthalten muss.

Wertebereich: **0** - **20**

Standardwert: **0** (= Keine Prüfung)

Maximale Gültigkeit

Maximale Gültigkeitsdauer des Passworts in Tagen.

Wertebereich: **0** - **180**

Standardwert: **0** (= Keine Prüfung)

Session Policy

Session Timeout

Die Sessions wird nach dieser Zeit der Inaktivität geschlossen (in Minuten). Ist der Wert 0, so erfolgt keine Prüfung.

Wertebereich: **5** - **999999**

Standard: **1440**

6.2 PKI

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Plug-In Konfiguration
- Connector Konfiguration
- Interne CA;CA intern
- Renewal

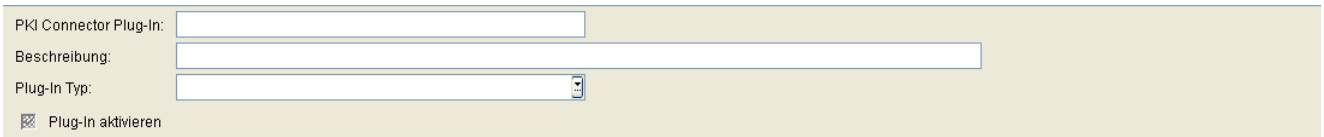
6.2.1 Plug-In Konfiguration

Aufruf: Administration > PKI > Plug-In Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Allgemeine Features“
- Register „Ausstellende Zertifizierungsstellen“
- Register „Plug-In Properties“

Allgemeine Daten



PKI Connector Plug-In

Name der PKI Connector Plug-In Konfiguration.

Beschreibung

Beschreibung der PKI Connector Plug-In Konfiguration.

Plug-In Typ

Auswahl des Plug-In-Moduls für diese Konfiguration.

Mögliche Werte:

- **DLS Internal Plug-In**
- **DLS Storage Plug-In 1.0**
- **MSCA Connector Plug-In 1.0**

Plug-In aktivieren

Aktiviert die hier ausgewählte Plug-In Konfiguration. Eine PKI Connector Lizenz ist erforderlich um eine externe PKI nutzen zu können.

Bevor die Plug-In-Konfiguration aktiviert werden kann, muss über die Aktionsschaltfläche **Synchronisieren** eine Synchronisation mit der PKI durchgeführt werden.

Mögliche Aktionsschaltflächen

Synchronisieren

Die Synchronisation mit der PKI muss durchgeführt werden, bevor das Plug-In aktiviert werden kann. Das Ergebnis der Synchronisation wird im Statusbalken angezeigt. Während der Synchronisation werden die Daten für das **Register „Allgemeine Features“** und das **Register „Ausstellende Zertifizierungsstellen“** aus der PKI gelesen und in die DLS-Datenbank geschrieben.

Suche

Sucht in der Datenbank nach eingerichteten PKI Plug-In-Konfigurationen, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Richtet neue PKI Plug-In Konfigurationen ein.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

Verwirft die eingetragenen Änderungen.

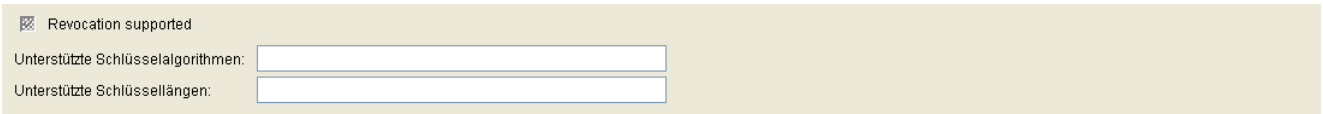
Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.2.1.1 Register „Allgemeine Features“

Aufruf: Administration > PKI > Plug-In Konfiguration > Register „Allgemeine Features“

Die hier angezeigten Daten wurden über die Funktion **Synchronisieren** aus der PKI gelesen und in die DLS-Datenbank geschrieben. Diese Daten können nicht geändert werden.



Revocation unterstützt

Zeigt an, ob diese Plug-In Konfiguration Revocation-Anfragen unterstützt.

Unterstützte Schlüsselalgorithmen

Unterstützte Schlüsselalgorithmen.

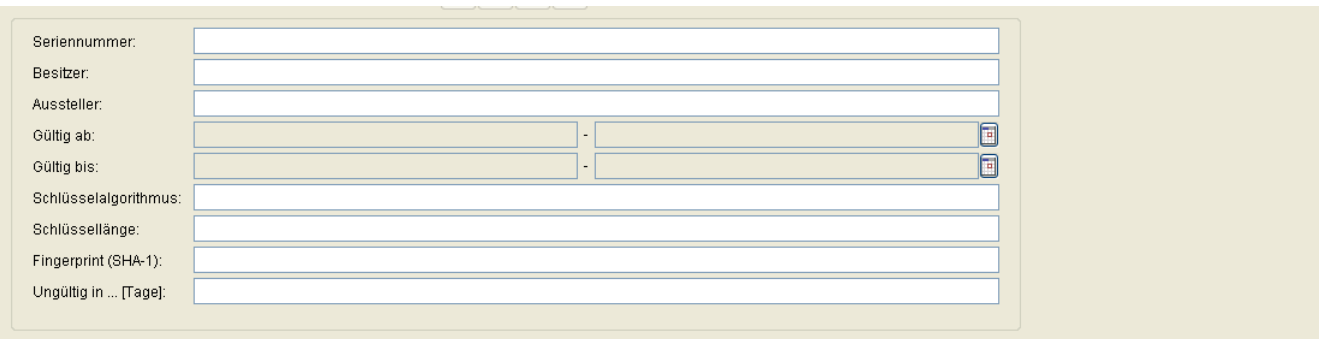
Unterstützte Schlüssellängen

Unterstützte Schlüssellängen.

6.2.1.2 Register „Ausstellende Zertifizierungsstellen“

Aufruf: Administration > PKI > Plug-In Konfiguration > Register „Ausstellende Zertifizierungsstellen“

Die hier angezeigten Daten wurden über die Funktion **Synchronisieren** aus der PKI gelesen und in die DLS-Datenbank geschrieben. Diese Daten können nicht geändert werden.



Seriennummer

Seriennummer des Zertifikats (nur Anzeige).

Besitzer

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Zertifikat (nur Anzeige).

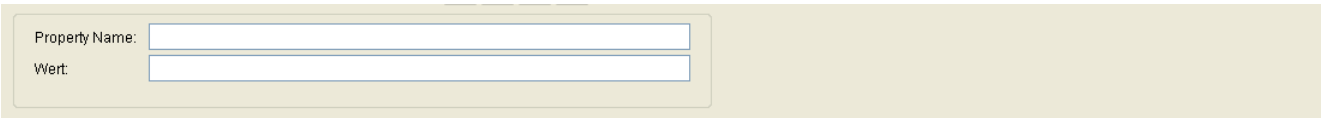
Ungültig in ... [Tage]:

Anzahl der verbleibenden Tage, bis das Zertifikat ungültig wird (nur Anzeige).

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

6.2.1.3 Register „Plug-In Properties“

Aufruf: Administration > PKI > Plug-In Konfiguration > Register „Plug-In Properties“



Property Name

Property Name.

Wert

Wert.

6.2.2 Connector Konfiguration

Aufruf: Administration > PKI > Connector Konfiguration

Eine Connector-Konfiguration dient dazu,

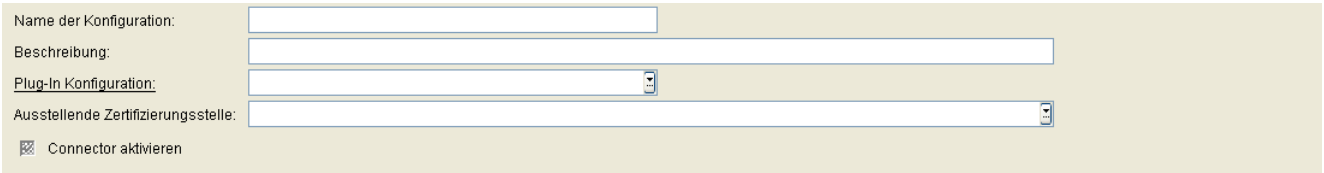
- Plug-In Konfigurationen zu definieren für den Zugriff zum externen PKI,
- eine ausstellende Zertifizierungsstelle auszuwählen, um Zertifikate anzufordern und die Verbindung zum Trust Anchor zu verifizieren,
- Parameter für die Zertifikatsanforderung einzustellen,
- das Trust Anchor-Zertifikat, das bei dieser Konfiguration auf den IP Devices eingespielt wird, zu definieren und importieren.

Eine Connector-Konfiguration kann einem bestimmten Zertifikatstyp (z.B. SPE, 802.1x, WBM usw.) zugewiesen werden oder als globale Konfiguration für alle oder einige Typen von einzuspielenden Zertifkaten verwendet werden.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Request Parameter“
- Register „Zertifikat Renewal“
- Register „Trust Anchor“
- Register „User Certificates“

Allgemeine Daten



Name der Konfiguration

Name der Konfiguration.

Beschreibung

Beschreibung.

Plug-In Konfiguration

Zugehörige Plug-In Konfiguration.

Ausstellende Zertifizierungsstelle

Name der ausstellenden Zertifizierungsstelle (Issuing CA Name).

Connector aktivieren

Bevor die Plug-In-Konfiguration aktiviert wird, muss eine Synchronisation mit der PKI erfolgen.

Mögliche Aktionsschaltflächen

Suche

Sucht in der Datenbank nach eingerichteten Internen CAs, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Richtet einen Datensatz im DLS für neue Interne CAs ein.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

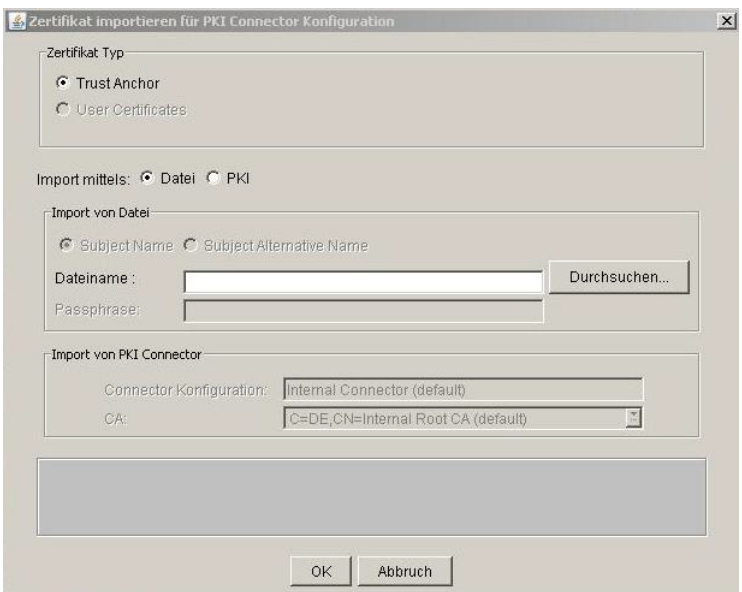
Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

Zertifikat importieren

Trust Anchor-Zertifikat oder User Certificate in DLS importieren. Die entsprechenden Einstellungen werden in einem Dialogfenster abgefragt.



Das Trust Anchor-Zertifikat wird verwendet, wenn von diesem Connector ein Server CA Zertifikat angefordert wird.

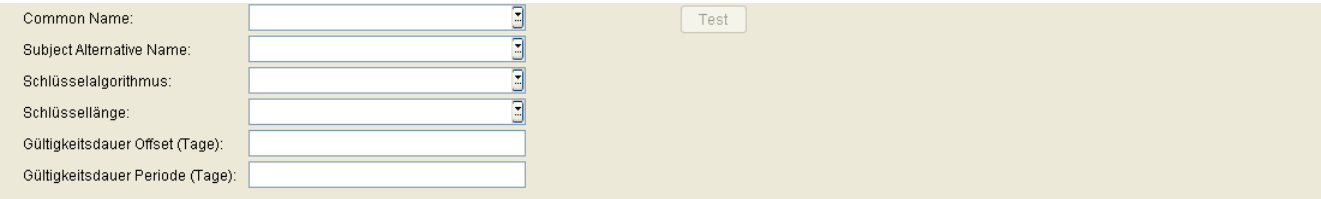
Beim Import von Benutzerzertifikaten (User Certificates) durch den Connector werden die folgenden Daten in der DLS-Datenbank gespeichert:

- Die PKI Connector-ID
- Die Zertifikat-ID. Dies ist der Subject Name (Antragstellername) oder der Subject Alternative Name (alternativer Antragstellername) des Zertifikats. Die Kombination von PKI Connector-ID und Zertifikat-ID muss eindeutig sein. Der Administrator legt beim Import fest, ob für die Zertifikat-ID der Subject Name oder der Subject Alternative Name verwendet wird.
- Der Ausstellername
- Das Zertifikat

Weitere Informationen zu CA-Zertifikaten finden Sie im Abschnitt 16.4, “Konfigurieren von Zertifikaten in DLS”.

6.2.2.1 Register „Request Parameter“

Aufruf: Administration > PKI > Connector Konfiguration > Register „Request Parameter“



Common Name

Common Name (Subject Name).

Mögliche Werte:

- **MAC Adresse**
- **DNS Name**
- **IP Adresse**

Subject Alternative Name

Subject Alternative Name.

Mögliche Werte:

- **None**
- **MAC Adresse**
- **DNS Name**
- **IP Adresse**

Schlüsselalgorithmus

Schlüsselalgorithmus.

Mögliche Werte:

- **DSA**
- **RSA**

Schlüssellänge

Schlüssellänge.

Mögliche Werte:

- **512**
- **1024**
- **2048**

Gültigkeitsdauer Offset (Tage)

Gültigkeitsdauer Offset in Tagen.

Gültigkeitsdauer Periode (Tage)

Gültigkeitsdauer Periode in Tagen.

Test

Testen der PKI Connector Konfiguration.

6.2.2.2 Register „Zertifikat Renewal“

Aufruf: Administration > PKI > Connector Konfiguration > Register „Zertifikat Renewal“

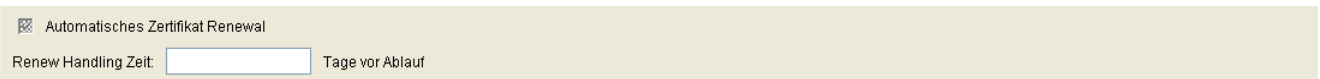
In diesem Register können Einstellungen zum Renewal dieser Connector Konfiguration gemacht werden.

Für den Fall, dass ein mit dieser Konfiguration angefordertes Zertifikat bald abläuft, kann eine automatische Erneuerung eingerichtet werden.
HINWEIS: Bei der Erneuerung eines Zertifikats wird grundätzlich immer ein neues Zertifikat angefordert. Die Verlängerung der Gültigkeitsdauer eines bereits ausgestellten Zertifikats wird nicht unterstützt. .

Die Connector-Konfiguration, die für die Beantragung und Bereitstellung des alten Zertifikats verwendet wurde, muss für dieses Gerät aber immer noch verfügbar sein. Ist dies nicht der Fall, fehlt die benötigte Zuordnung zwischen dem (bald ablaufenden) Zertifikat und den zum Anfordern und Bereitstellen eines neuen Zertifikats erforderlichen Konfigurationen.

In solchen Fällen wird ein Alarm ausgegeben und die Bereitstellung des Zertifikats muss, sofern es keine globale Konfiguration für die Zertifikatserneuerung gibt, manuell durchgeführt werden.

Diese Konfiguration kann auch von der globalen Erneuerungs-Konfiguration verwendet werden (siehe auch Abschnitt 6.2.4, “Renewal”).



Automatisches Zertifikat Renewal

Ist der Schalter aktiviert, so wird das Zertifikat automatisch erneuert. Sollte die automatische Erneuerung einen anderen Aussteller erfordern (CA mit längerer Laufzeit) oder sogar eine andere PKI, kann diese Konfiguration entsprechend geändert werden. Dies erfordert unter Umständen auch einen neuen Trust Anchor.

HINWEIS: Eine neue, über ihren Namen identifizierte Konfiguration hat keine Verbindung zu bereits zugewiesenen Zertifikaten und kann auch nicht für deren Erneuerung verwendet werden. In diesem Fall ist eine globale Erneuerungs-Konfiguration erforderlich (siehe auch Abschnitt 6.2.4, „Renewal“).

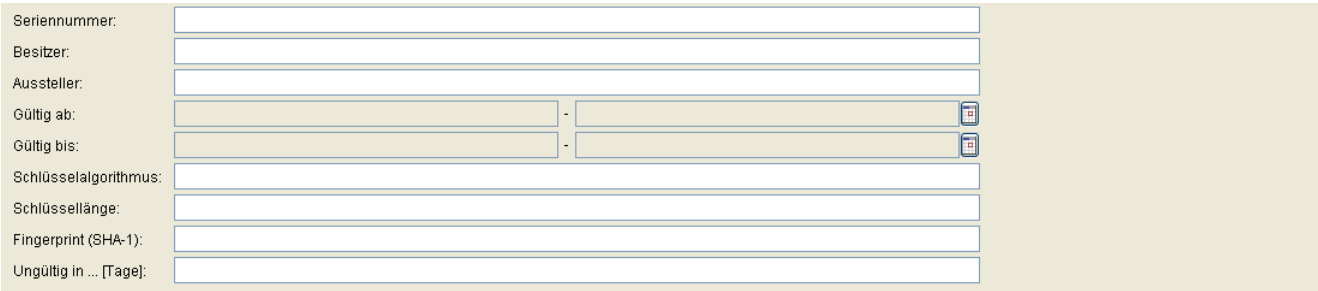
Renew Handling Zeit

Das Zeitintervall (in Tagen), mit dem die Erneuerung eines (mit dieser Konfiguration ausgestellten) Zertifikats vor dessen Ablauf geplant wird.

6.2.2.3 Register „Trust Anchor“

Aufruf: Administration > PKI > Connector Konfiguration > Register „Trust Anchor“

Für jede Konfiguration muss ein Trust Anchor eingerichtet werden. In den meisten Szenarien ist es die Root-CA selbst, es kann aber auch eine untergeordnete CA sein. Die Konfiguration kann nur gespeichert werden, wenn ein Trust Anchor eingetragen ist!



Seriennummer

Seriennummer des Zertifikats (nur Anzeige).

Besitzer

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Zertifikat (nur Anzeige).

Ungültig in ... [Tage]:

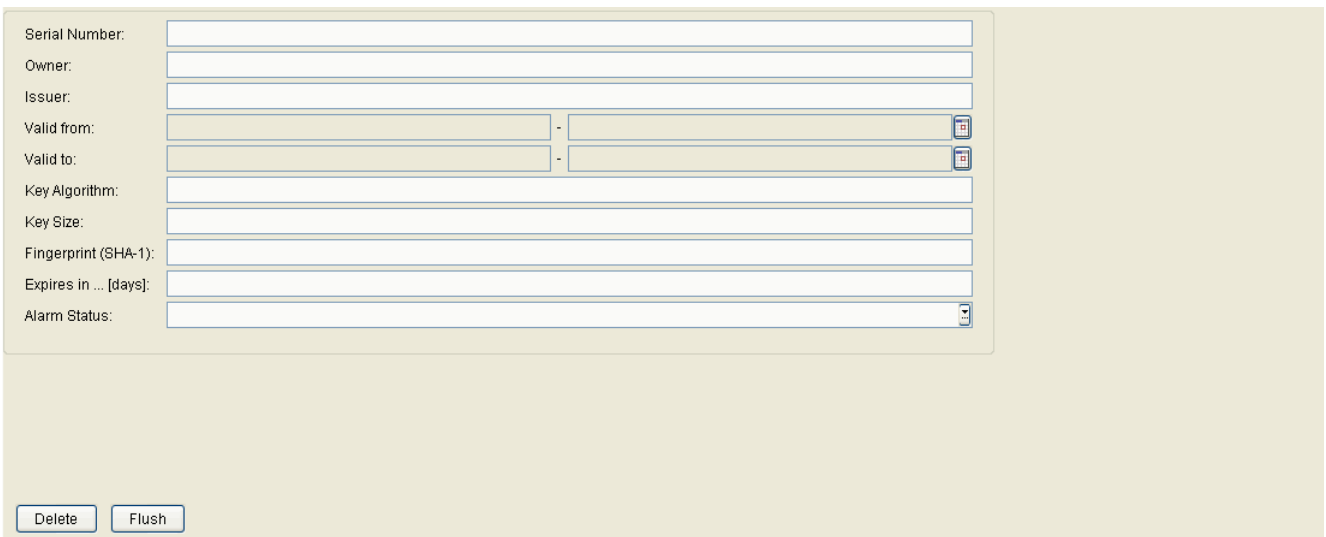
Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

6.2.2.4 Register „User Certificates“

Aufruf: Administration > PKI > Connector Konfiguration > Register „User Certificates“

Für jede Konfiguration muss ein User Certificate eingerichtet werden.



Seriennummer

Seriennummer des Zertifikats (nur Anzeige).

Besitzer

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des aktiven Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Zertifikat (nur Anzeige).

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarmstatus des Zertifikats (nur Anzeige).

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

Löschen

Löscht das User Certificate

Flush

Startet die Übertragung des User Certificates

6.2.3 Interne CA;CA intern

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Allgemeine Daten

CA Name

Name der CA.

Beschreibung

Beschreibung der CA.

Interne CA aktivieren

Schalter zum Aktivieren der internen CA. Hierfür muss eine CA angelegt worden sein, entweder durch **Import CA** oder über **Create CA**.

Mögliche Aktionsschaltflächen

Suche

Sucht in der Datenbank nach eingerichteten Internen CAs, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Richtet einen Datensatz im DLS für neue Interne CAs ein.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

Import CA

CA aus .zip-Datei importieren.

Export CA

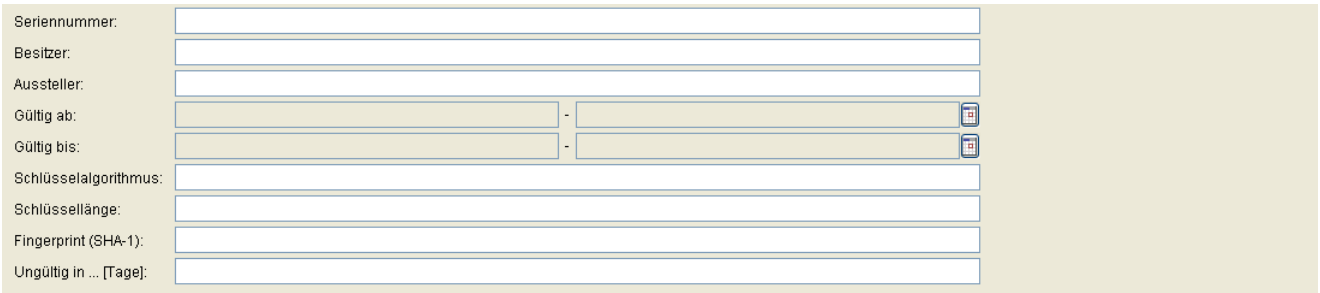
CA in .zip-Datei exportieren.

Create CA

CA aus Daten eines DLS-Datensatzes anlegen.

6.2.3.1 Register „Info“

Aufruf: Administration > PKI > Interne CA;CA intern > Register „Info“



Seriennummer

Seriennummer des Zertifikats (nur Anzeige).

Besitzer

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Zertifikat (nur Anzeige).

Ungültig in ... [Tage]:

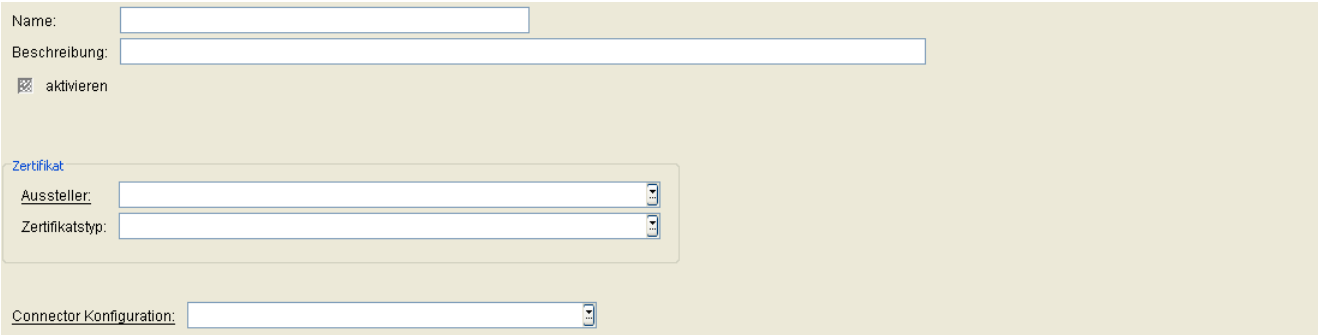
Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

6.2.4 Renewal

Aufruf: Administration > PKI > Renewal

Mit dieser Funktion können allgemeine Einstellungen zum Renewal für alle Zertifikate eines Typs gemacht werden.



Name

Name der Renewal-Konfiguration.

Beschreibung

Beschreibung der Renewal-Konfiguration.

aktivieren

Aktivieren der Renewal-Konfiguration. Aktivieren (deaktivieren) aller globalen Renewal-Einstellungen für das Zertifikat.

Zertifikat

Aussteller:

Aussteller des Zertifikats (muss übereinstimmen).

Zertifikatstyp

Typ des Zertifikats.

Mögliche Werte:

- **ALLE**

- **Phone Zertifikat**
- **WBM Server Zertifikat**
- **SPE Zertifikat**

Bei der Einstellung ALLE erfolgt kein Abgleich mit dem Zertifikatstyp.

Connector Konfiguration

Die bei Übereinstimmung von Aussteller und Zertifikatstyp zu verwendende Connector-Konfiguration.

Wenn Zertifikate sich dem Ende ihrer Gültigkeitsdauer nähern, kann automatisch eine Erneuerung beantragt werden. Da es verschiedene Connector-Konfigurationen und externe PKIs gibt, an die Erneuerungsanforderungen gesendet werden können, muss zunächst festgelegt werden, welche Konfiguration (und damit welches Plug-in und welche externe PKI) verwendet werden soll. Es kann auch sein, dass die Ursprungs-Konfiguration, die zur Erstellung des vorliegenden Zertifikats verwendet wurde, verloren gegangen ist oder nicht ermittelt werden kann.

In solchen Fällen wird eine globale Konfiguration benötigt, um ein Zertifikat über seinen Aussteller mit einer Connector-Konfiguration zu verknüpfen; über diese wird dann das neue Zertifikat angefordert und das alte Zertifikat ersetzt.

Dabei wird die Connector-Konfiguration in einer zuvor definierten Reihenfolge durchsucht:

1. die globale Zertifikatserneuerungs-Konfiguration verwenden, um nach eine Connector-Konfiguration zu suchen, die dem Aussteller und Zertifikatstyp entspricht, ansonsten
2. die ursprüngliche Konfiguration, die zum Anfordern des vorliegenden Zertifikats verwendet wurde, suchen und verwenden, ansonsten
3. einen Alarm ausgeben, da anhand der globalen Alarm-Einstellungen keine Erneuerungs-Konfiguration ermittelt werden kann

Die Überprüfung der verbleibenden Gültigkeitsdauer des Zertifikats erfolgt in den im Register „Alarm Konfiguration“ festgelegten Intervallen (siehe auch Abschnitt 6.6.7 Register „Einstellungen“).

HINWEIS: Diese Überprüfung muss einmal pro Tag ausgeführt werden

HINWEIS: Bei der Erneuerung eines Zertifikats wird grundätzlich immer ein neues Zertifikat angefordert. Die Verlängerung der Gültigkeitsdauer eines bereits ausgestellten Zertifikats wird nicht unterstützt.

6.3 Server Konfiguration

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Mandanten
- Standort
- P&P Einstellungen
- FTP Server Konfiguration
- HTTPS Server Konfiguration
- HTTPS Client Konfiguration
- Netzlaufwerk Konfiguration
- Infrastruktur Policy
- API Notifizierungen
- XML Applikationen
- Optionen
- TLS Connector Konfiguration

6.3.1 Mandanten

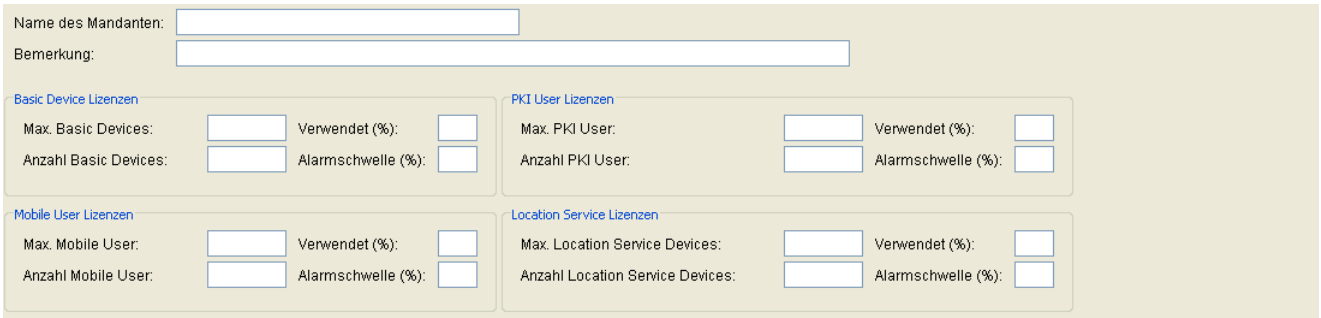
Aufruf: Hauptmenü > Administration > Server Konfiguration > Mandanten

HINWEIS: Dieser Bereich steht nur zur Verfügung, wenn Mandantenfähigkeit installiert wurde. (Siehe Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”)

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Standorte“

Allgemeine Daten



Name des Mandanten

Eindeutiger Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

Basic Device Lizenzen

Max. Basic Devices:

Maximale Anzahl erlaubter Basic Devices für diesen Mandanten.

Anzahl Basic Devices

Anzahl der registrierten IP Devices.

Verwendet (%)

Zeigt an, wieviel Prozent der vorhandenen Basic Device-Lizenzen bereits verwendet werden.

Alarmschwelle (%)

Legt fest, ab welchem Prozentsatz an verwendeten Basic Device-Lizenzen ein Lizenzalarm generiert werden soll.

Mobile User Lizenzen

Max. Mobile User

Maximal erlaubte Anzahl erlaubter Mobile User für diesen Mandanten.

Anzahl Mobile User

Anzahl der registrierten Mobile User.

Verwendet (%)

Zeigt an, wie viel Prozent der vorhandenen Mobile User-Lizenzen bereits verwendet werden.

Alarmschwelle (%)

Legt fest, ab welchem Prozentsatz an verwendeten Mobile User-Lizenzen ein Lizenzalarm generiert werden soll.

PKI User Lizenzen

Max. PKI User

Maximal Anzahl erlaubter IP Devices für diesen Mandanten, die über PKI Service versorgt werden können.

Anzahl PKI User

Anzahl der IP Devices, die mittels PKI Service versorgt werden.

Verwendet (%)

Prozentsatz an verwendeten Lizenzen.

Alarmschwelle (%)

Prozentsatz, bei dessen Überschreitung ein Lizenzalarm generiert wird.

Location Service Lizenzen

Max. Location Service Devices

Maximal erlaubte Anzahl von Location Service Devices für diesen Mandanten.

Anzahl Location Service Devices

Anzahl der IP Devices, die mittels des Location Service mit IP-Infrastrukturdaten versorgt werden.

Verwendet (%)

Zeigt an, wie viel Prozent der vorhandenen Lizenzen bereits verwendet werden.

Alarmschwelle (%)

Legt fest, ab welchem Prozentsatz an verwendeten Lizenzen ein Lizenzalarm generiert werden soll.

Mögliche Aktionsschaltflächen

Suchen

Durchsucht die Datenbank nach bereits konfigurierten Mandanten, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Erzeugt einen neuen Datensatz für einen Mandanten.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

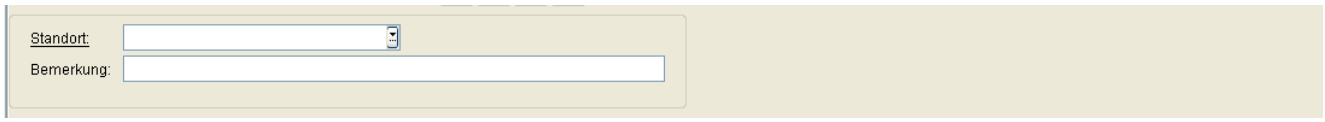
Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.3.1.1 Register „Standorte“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Mandanten > Register „Standorte“



Standort

Name des Standortes.

Bemerkung

Bemerkung zum Standort.

6.3.2 Standort

In diesem Bereich können Sie Standorte definieren, um Endgeräte zusammenzufassen, die gemeinsame Eigenschaften haben, wie z.B. IP-Adressen, Registrierungsadressen oder E.164-Rufnummernmuster.

IP-Adressbereiche für einen Standort werden unter **Administration** > **Server Konfiguration** > **Standort** > **Register „IP Bereiche“** eingerichtet.

IP-Adressen oder Hostnamen von Systemen (PBX/Gateway oder SIP Server) für einen Standort können unter **Administration** > **Server Konfiguration** > **Standort** > **Register „Reg-Adressen“** angegeben werden.

Weitere Einstellungsmöglichkeiten finden Sie in den anderen Registern unter **Administration** > **Server Konfiguration** > **Standort**.

Wird kein Standort definiert, so werden alle standortspezifischen Parameter in der **Default Location** festgelegt.

Um die Weiterverwendung bestehender Templates oder Geräteprofile zu ermöglichen, wenn Kundennetzwerke in Filialen aufgeteilt werden sollen, stehen hierarchische Standortdefinitionen zur Verfügung. Der übergeordnete Standort kann z.B. über Business Groups definiert und durch E.164-Muster in untergeordnete Standorte unterteilt werden. Solche Standardprofile, die für die untergeordneten Standorte definiert werden, erweitern bzw. überschreiben die Daten der Standardprofile des übergeordneten Standorts.

Zur Überprüfung einer Standort- bzw. Profil-Konfiguration steht dem Administrator die Möglichkeit zur Verfügung, Plug&Play mit standortspezifischen Daten für ein Gerät zu simulieren. Die ermittelten Parameterwerte werden temporär gespeichert und können über die Register unter **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** angezeigt werden.

Um ein Überlappen der Standorte zu verhindern, wurden die folgenden Einschränkungen festgelegt:

- Die Eigenschaft, die einen untergeordeneten Standort definiert, muss sich unterscheiden von der Eigenschaft, die den übergeordneten Standorts definiert. Falls also beispielsweise der übergeordnete Standort über ein E.164-Muster definiert worden ist, muss der untergeordnete Standort über eine andere Eigenschaft definiert werden.
- Pro Ebene ist nur die eine bestimmte Eigenschaft zur Definition von Standorten erlaubt. Beispiel: Alle übergeordneten Standorte sind über Registrierungs-Adressen definiert. Die untergeordneten Standorte eines bestimmten übergeordneten Standorts sind über Business Groups definiert, während die untergeordneten Standorte eines anderen übergeordneten Standorts über E.164-Muster definiert sind.
- Überlappende Definitionen von Standorten sind nicht zulässig.

Um einen untergeordneten Standort anzulegen, erzeugen Sie einen neuen Standort und weisen Sie diesem einen bereits existierenden Standort als übergeordneten Standort zu. Dieser darf nicht selbst als untergeordneter Standort fungieren.

Die Eigenschaften des übergeordneten Standorts sind in den untergeordneten Standorten sichtbar; es können nur Untermengen der Eigenschaften des übergeordneten Standorts eingerichtet werden. Die Einschränkungen für Software- und Zertifikat-Deployment (**Register „SW Deployment Einschränkungen“** und **Register „Zertifikatsverteilung Einschränkungen“**) in einem untergeordneten Standort hingegen sind jeweils unabhängig von den Einstellungen im übergeordneten Standort.

Automatische Jobs, die für einen übergeordneten Standort gestartet werden, betreffen alle Endgeräte, die sich an diesem Standort bzw. an diesem Standort untergeordneten Standorten befinden. Im Einzelnen gilt das Folgende:

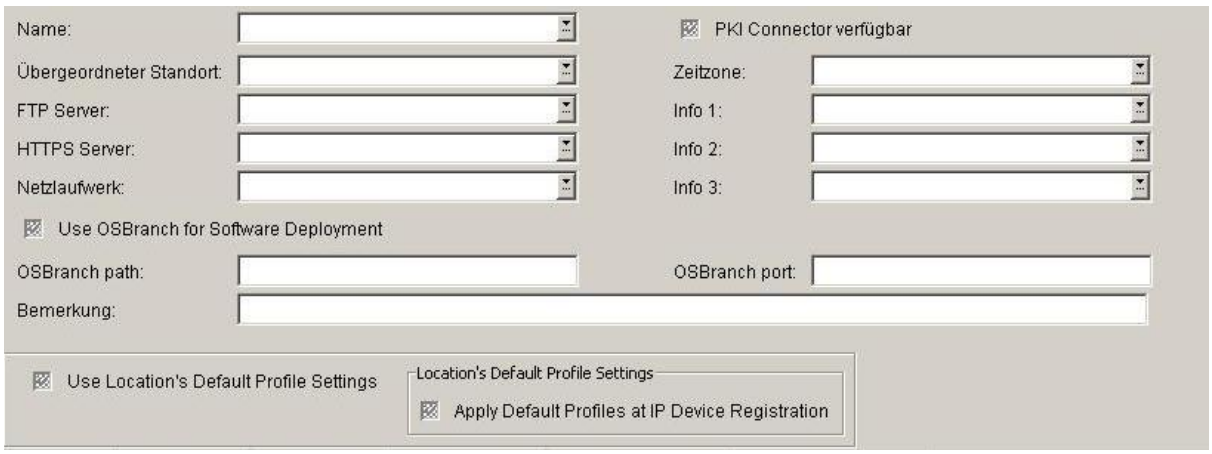
- Beim automatischen Software-Deployment haben Regeln in untergeordneten Standorten Vorrang vor Regeln in den jeweils übergeordneten Standorten.
- Beim automatischen Zertifikatsdeployment werden die angeforderten Zertifikate an alle IP Devices verteilt, sowohl an die der übergeordneten als auch an die aller untergeordneten Standorte.
- Bei der automatischen Archivierung werden alle IP Devices archiviert, sowohl die der übergeordneten als auch die aller untergeordneten Standorte.
- Beim automatischen Mobile User Logoff werden alle IP Devices abgemeldet, sowohl die der übergeordneten als auch die aller untergeordneten Standorte.
- Bei Plug&Play werden virtuelle Devices, die in einem Rufnummernband liegen, einem Standort entsprechend ihrer E.164 Nummer zugewiesen.
- Bei Plug&Play mit Mandantenfähigkeit werden virtuelle Devices, die in einem Rufnummernband liegen, einem Mandanten entsprechend ihrer E.164 Nummer zugewiesen.

Für einen Standort können ein FTP-Server, zeitliche Einschränkungen im Software-Deployment sowie eine Infrastruktur-Policy festgelegt werden.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „IP Bereiche“
- Register „Reg-Adressen“
- Register „E.164-Patterns“
- Register „Business Groups“
- Register „Infrastruktur Policies“
- Register „P&P Rufnummernband“
- Register „SW Deployment Einschränkungen“
- Register „Zertifikatsverteilung Einschränkungen“
- Register „Mandanten“

Allgemeine Daten



Name:

Name des Standorts.

Übergeordneter Standort

Name des diesem Standort übergeordneten Standorts, falls vorhanden.

FTP Server:

Zum Standort gehöriger FTP-Server.

HTTPS Server:

Zum Standort gehöriger HTTPS-Server.

Netzlaufwerk:

Zum Standort gehöriges Netzlaufwerk.

Use OSBranch for Software Deployment

Wenn dieses Kontrollkästchen aktiviert ist, wird OS Branch für die Softwarebereitstellung verwendet.

OSBranch path:

Pfad zum Verzeichnis mit den von OSBranch bereitgestellten Telefonsoftware-Images.

OSBranch port:

Port-Nummer für die Kommunikation mit OSBranch zur Softwarebereitstellung (Telefonsoftware-Images).

Bemerkung:

Frei formulierte Bemerkung zum Standort.

PKI Connector verfügbar

Der Schalter ist aktiviert, wenn ein PKI Connector für die IP Devices, die zu diesem Standort gehören, verfügbar ist.

Zeitzone:

Legt die Zeitzone des Standortes fest. Die möglichen Werte entnehmen Sie bitte der Auswahlliste.

Info 1:

Zusätzliche optionale Information zur Standortbeschreibung, z. B. Adressinformationen.

Info 2:

Zusätzliche optionale Information zur Standortbeschreibung, z. B. Adressinformationen.

Info 3:

Zusätzliche optionale Information zur Standortbeschreibung, z. B. Adressinformationen.

Location’s Default Profile Settings (Standard-Profileinstellungen des Standorts)

Use Location’s Default Profile Settings (Standard-Profileinstellungen des Standorts verwenden):

Wenn dieser Schalter aktiviert ist, wird die Einstellung „Default Profile anwenden bei IP Device Registrierung“ auf Standortebene aktiviert.

Dieser Schalter ist standardmäßig deaktiviert.

Default Profile anwenden bei IP Device Registrierung

Ist der Schalter aktiviert, werden bei jeder Registrierung die in **Profil Management** > **Geräteprofil** für einen bestimmten Standort definierten Default-Profile ermittelt und angewendet.

Dieser Schalter wird standardmäßig nicht verwendet.

> ***HINWEIS:*** Wenn der Schalter „Use Location’s Default Profile Settings“ nicht aktiviert ist, wird die Einstellung „Default Profile anwenden bei IP Device Registrierung“ nicht verwendet und steht daher nicht zur Verfügung (ist ausgegraut).
> Wenn der Schalter aktiviert ist, steht die Einstellung „Default Profile anwenden bei IP Device Registrierung“ zur Verfügung und kann konfiguriert werden.

Bemerkung:

Bemerkung

FTP Server:

Zum Standort gehöriger FTP-Server.

HTTPS Server:

Zum Standort gehöriger HTTPS-Server.

Netzlaufwerk:

Zum Standort gehöriges Netzlaufwerk.

Mögliche Aktionsschaltflächen

Suchen

Durchsucht die Datenbank nach bereits konfigurierten Standorten, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Erzeugt einen neuen Datensatz für einen Standort.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

Standort exportieren

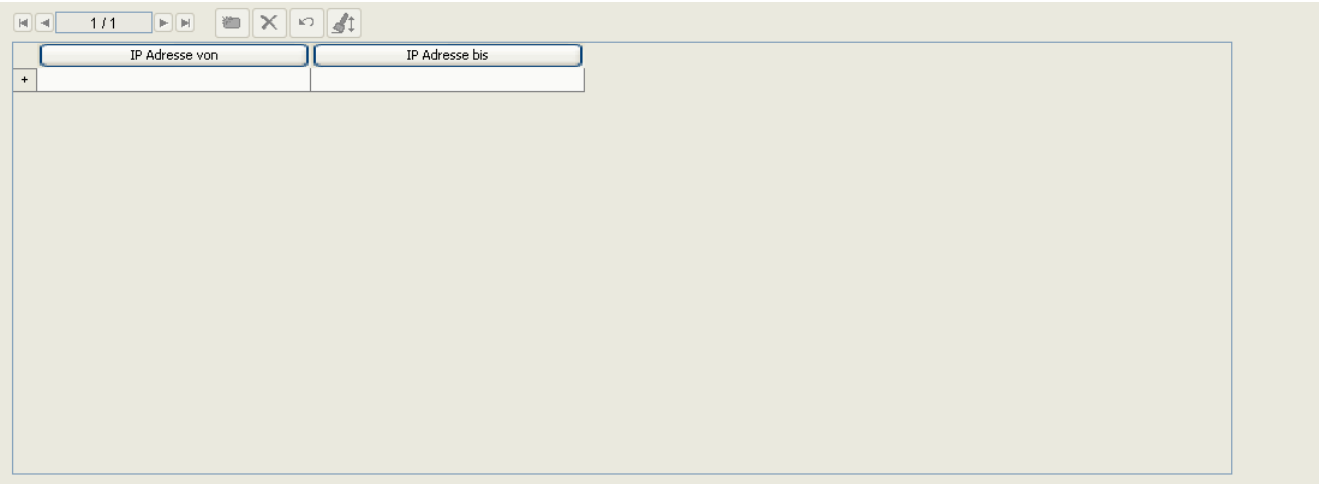
Die selektierten Standorte werden in eine Datei im .zip-Format exportiert.

Standort importieren

Standorte werden aus einer Datei im .zip-Format importiert.

6.3.2.1 Register „IP Bereiche“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „IP Bereiche“



IP Adresse von

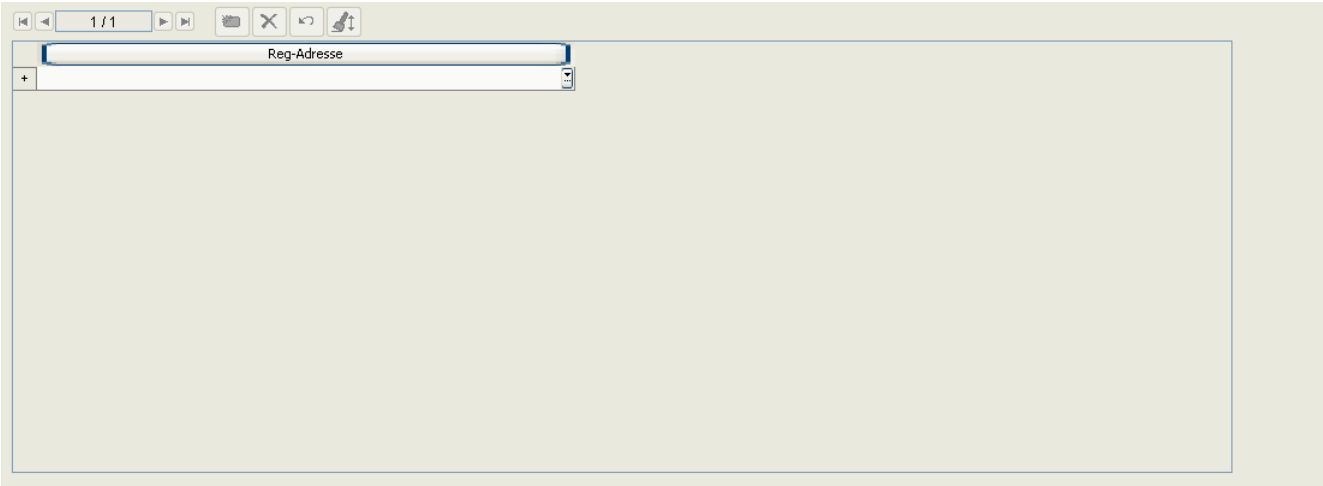
Untergrenze des zu diesem Standort gehörenden IP-Bereiches.

IP Adresse bis

Obergrenze des zu diesem Standort gehörenden IP-Bereiches.

6.3.2.2 Register „Reg-Adressen“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „Reg-Adressen“

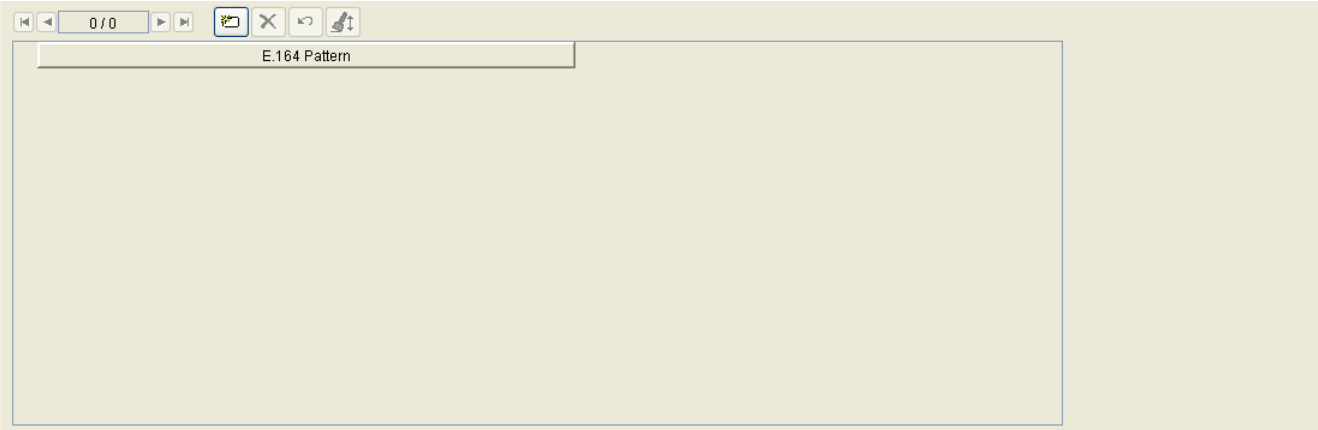


Reg-Adresse

IP Adressen oder Hostnamen der zu diesem Standort gehörenden PBX-/Gateway- oder SIP-Server.

6.3.2.3 Register „E.164-Patterns“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „E.164-Patterns“



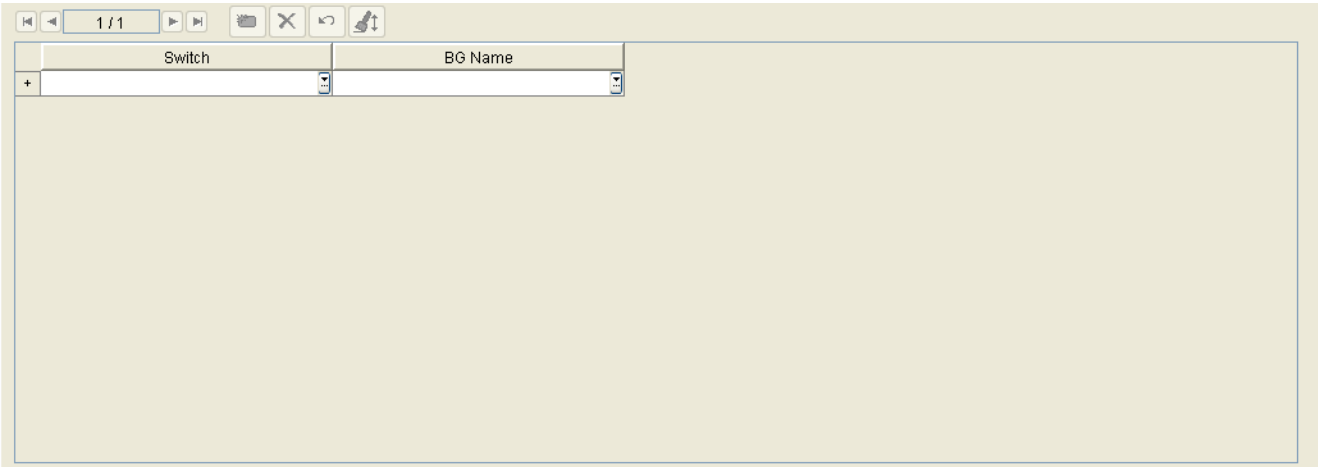
E.164 Pattern

Pattern von E.164 Nummern, die zu diesem Standort gehören. Es können reguläre Ausdrücke mit dem Symbol * gebildet werden.

Beispiel: **4989722***.

6.3.2.4 Register „Business Groups“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „Business Groups“



Switch

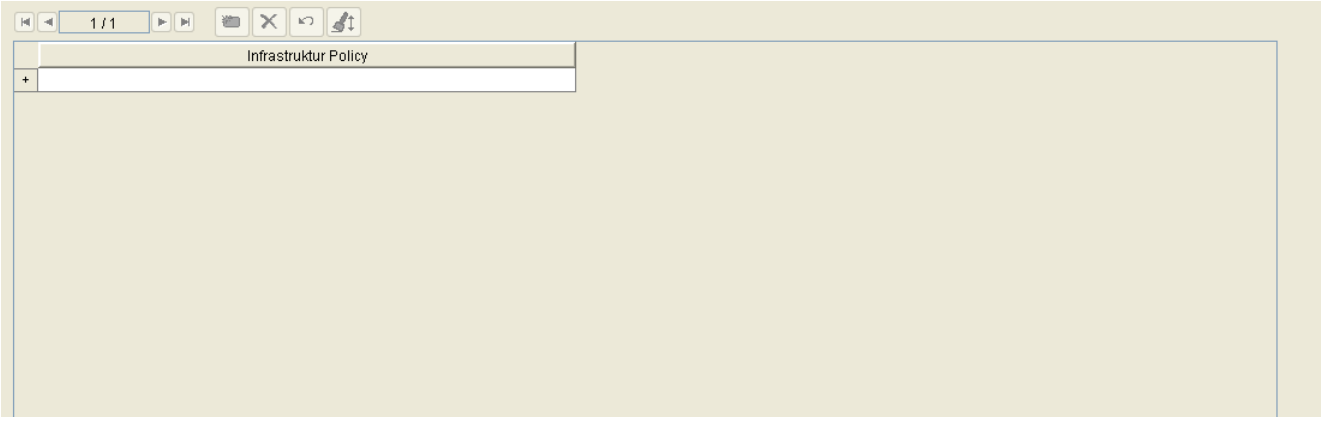
Name des Switches, an dem die Business Group eingerichtet ist.

BG Name

Name der Business Group.

6.3.2.5 Register „Infrastruktur Policies“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „Infrastruktur Policies“



Infrastruktur Policy

Der Standort wird berücksichtigt, wenn für ein Device die Infrastruktur-Policy via DLSAPI oder über die XML-Applikation „Location Services“ geändert wird.

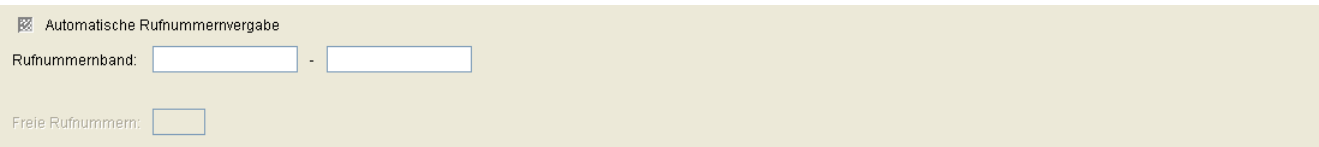
6.3.2.6 Register „P&P Rufnummernband“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „P&P Rufnummernband“

Hier können Sie die automatische Vergabe einer E.164 Nummer aus einem Rufnummernband während des Plug&Play konfigurieren.

Falls ein standortspezifisches Rufnummernband erforderlich ist, so muss dies während der Einrichtung des Standorts festgelegt werden. Das Rufnummernband für die „Default Location“ darf dann nicht aktiviert werden. Für die automatische Rufnummernvergabe muss ein Standort über IP Bereiche definiert sein, und er muss ein übergeordneter Standort sein. Dies ist erforderlich, da sonst für IP Phones, die sich ohne E.164-Nummer anmelden, kein Standort zugewiesen werden kann.

Weitergehende Informationen finden Sie in Abschnitt 15.5.2, “Plug&Play-Registrierung einrichten”.



Automatische Rufnummernvergabe

Ist der Schalter gesetzt, wird dem IP Device bei Plug&Play automatisch eine E.164-Nummer aus dem Rufnummernband zugewiesen.

Rufnummernband

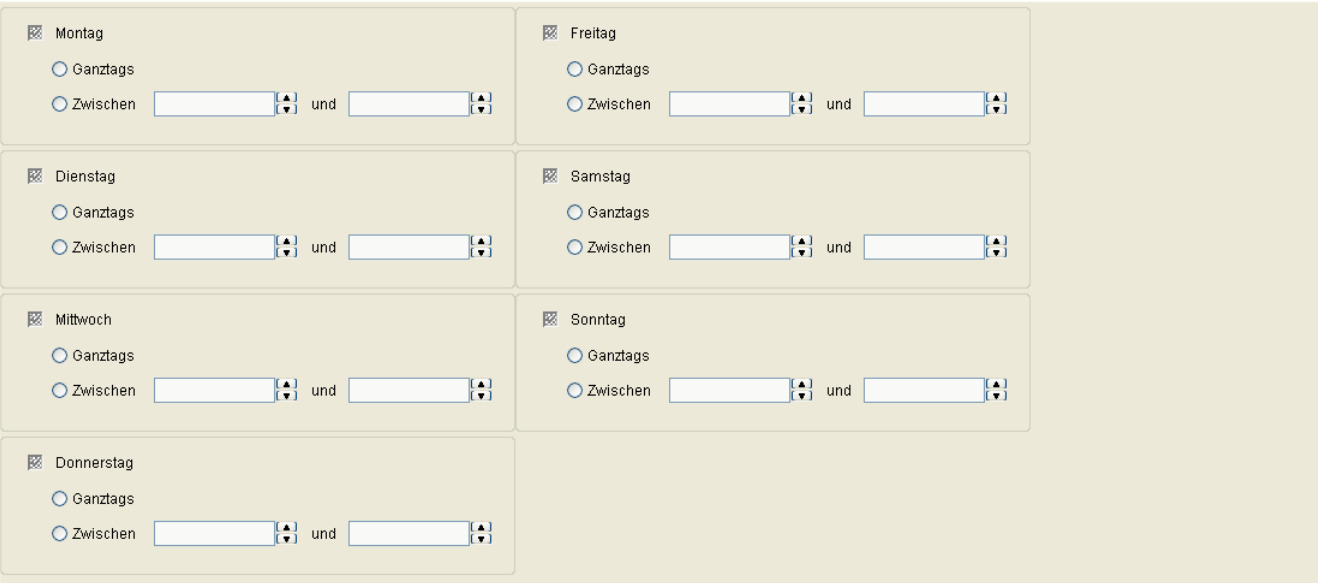
Bereich von aufeinanderfolgend vollständigen E.164-Rufnummern, der durch Eingabe der niedrigsten und der höchsten Rufnummer definiert wird.

Freie Rufnummern

Anzahl der noch nicht zugewiesenen E.164-Rufnummern aus dem Rufnummernband.

6.3.2.7 Register „SW Deployment Einschränkungen“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „SW Deployment Einschränkungen“



Montag ... Sonntag

Schalter zum Aktivieren der Wochentage, an denen keine bzw. nur ein eingeschränktes Software-Deployment durchgeführt werden soll.

Ganztags

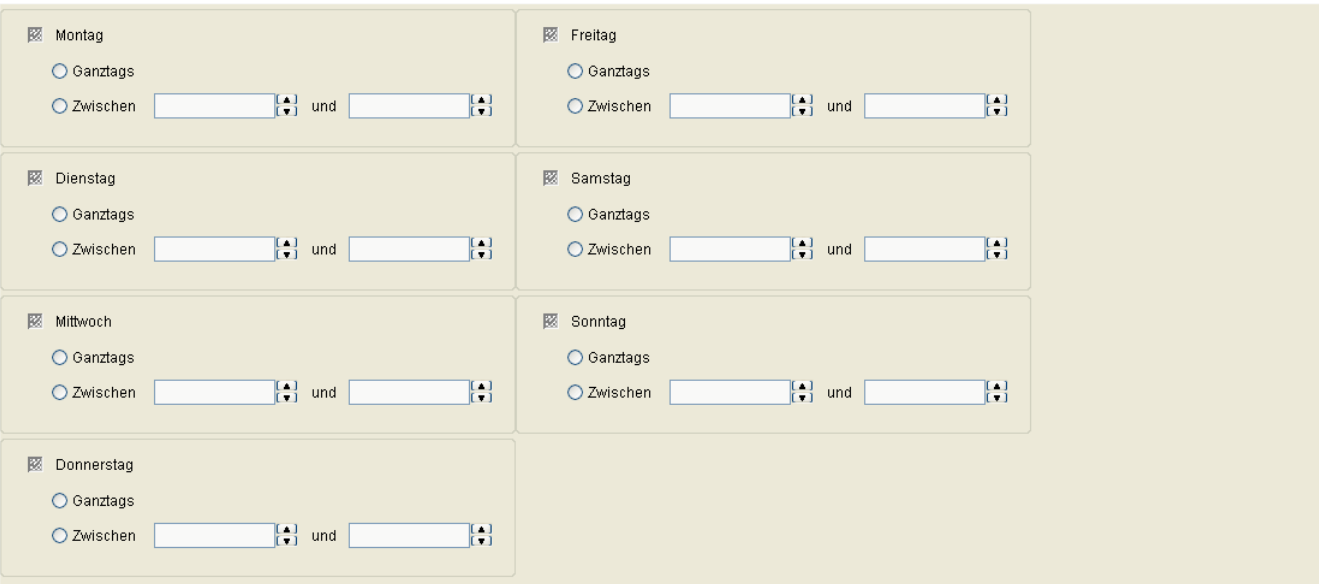
Schalter zum Aktivieren der Option, an dem jeweiligen Tag überhaupt keine Software-Verteilung zuzulassen.

Zwischen ... und ...

Schalter zum Aktivieren der Option, an dem jeweiligen Tag während eines Zeitbereiches keine Software-Verteilung zuzulassen. Es kann der Beginn und das Ende des Zeitbereiches festgelegt werden.

6.3.2.8 Register „Zertifikatsverteilung Einschränkungen“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „Zertifikatsverteilung Einschränkungen“

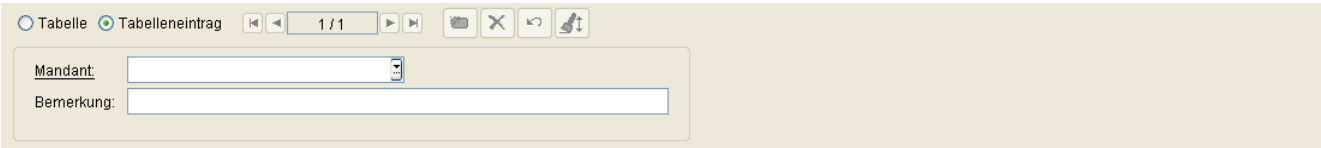


Parameterbeschreibungen siehe Abschnitt 6.3.2.7, “Register „SW Deployment Einschränkungen“”.

6.3.2.9 Register „Mandanten“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Standort > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.



Mandant

Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

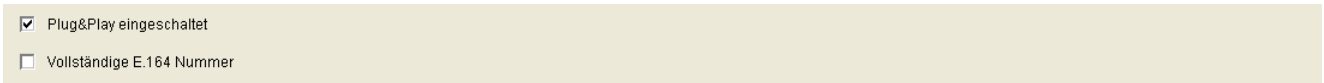
6.3.3 P&P Einstellungen

Aufruf: Hauptmenü > Administration > Server Konfiguration > P&P Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Standard Profil“
- Register „IP Client Mapping Konfiguration“

Allgemeine Daten



Plug&Play eingeschaltet

Wenn aktiviert, ist Plug&Play für alle Geräte eingeschaltet.

Vollständige E.164 Nummer

Ist dieser Schalter aktiviert, erwartet der DLS bei Plug&Play bzw. Autokonfiguration eines IP Devices dessen vollständige E.164-Rufnummer, um das entsprechende virtuelle Gerät zu finden.

Mögliche Aktionsschaltflächen

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Sichern

Sichert die Änderungen.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

6.3.3.1 Register „Standard Profil“

Aufruf: Hauptmenü > Administration > Server Konfiguration > P&P Einstellungen > Register „Standard Profil“

Legen Sie fest, wie die E.164-Nummer bei der Autokonfiguration verwendet werden soll.

Standard Profil eingerichtet

Dieser Schalter ist aktiviert, wenn das Standardprofil existiert.

Standard Profil anlegen

Erzeugt ein Standard-Profil für IP Phones und IP Clients. Dieses Profil enthält vordefinierte Templates.

HINWEIS: Bei der Zuweisung von Templates zu P&P-Profilen MUSS allen P&P-Profilen eine SW-Version zugewiesen sein, damit die entsprechenden Masken verfügbar sind.

HINWEIS: Beispiel: Unter **IP Devices** > **IP Phone Konfiguration** > **IP Routing**> -**Register „IPv6 Einstellungen“** ist „IPv4 / IPv6 Protokoll Modus“ nur dann verfügbar, wenn der Gerätetyp auf OpenStage eingestellt wurde und die SW Version V3 oder höher ist (siehe Abschnitt 7.1.2.2, “Register „IPv6 Einstellungen“”).

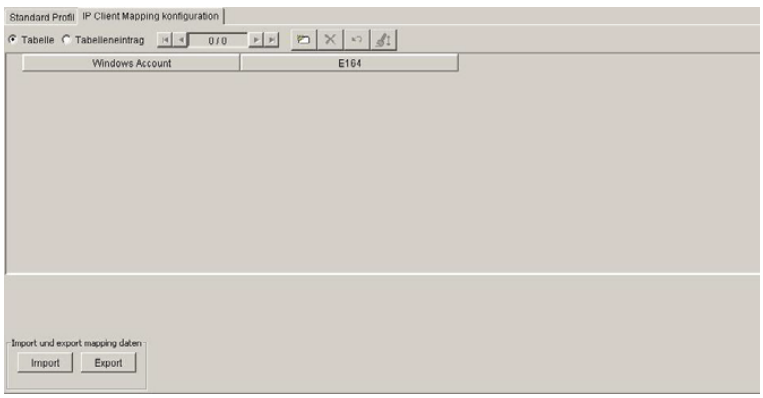
HINWEIS: Dies gilt auch für alle Masken, die nach SW Version gefiltert werden.

Standard Profil löschen

Entfernt das Standard-Profil.

6.3.3.2 Register „IP Client Mapping Konfiguration“

Aufruf: Hauptmenü > Administration > Server Konfiguration > P&P Einstellungen > Register „IP Client Mapping Konfiguration“



Windows-Account-Namen werden E.164-Rufnummern zugeordnet, um eine Verknüpfung zwischen Windows-Accounts und Rufnummern herzustellen. Die Konfiguration dieser Zuordnung im DLS sollte manuell über die DLS-Benutzeroberfläche erfolgen. Anschließend sollten die Mapping-Daten über CSV-Dateien importiert und exportiert werden, um DLS Plug & Play auszulösen.

Import und export mapping daten

Import

Die Mapping-Daten werden aus eine CSV-Datei importiert.

Export

Die Mapping-Daten werden in eine CSV-Datei exportiert.

6.3.4 FTP Server Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Mandanten“

Allgemeine Daten

Aufruf: Hauptmenü > Administration > Server Konfiguration > FTP Server Konfiguration.

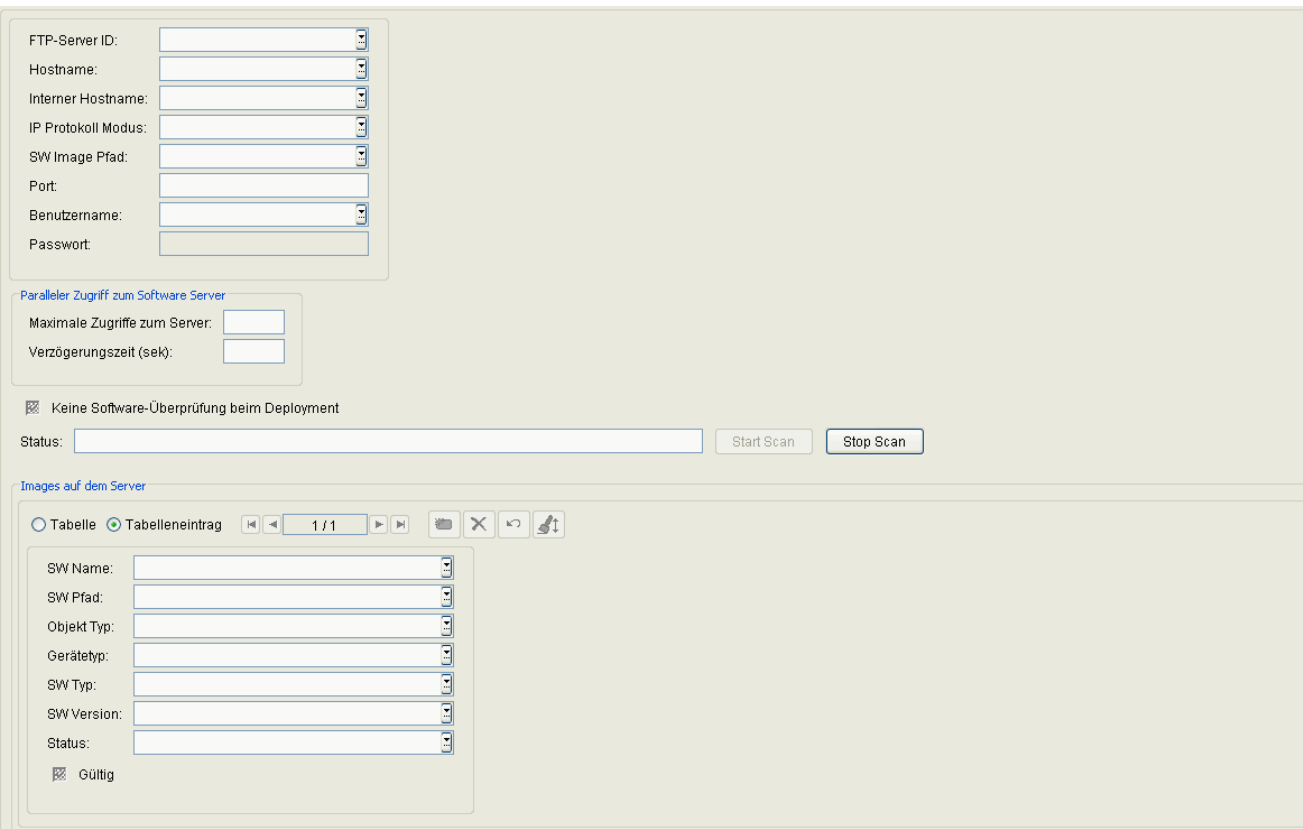
In diesem Bereich können Sie die Zugangsdaten eines oder mehrerer FTP-Server konfigurieren. In der Ansicht **Tabelle** sind alle über die **Suche** gefundenen FTP-Server aufgelistet. Außerdem können Sie alle auf dem FTP-Server vorhandenen Dateien, die für IP Devices relevant sind, per Scan in die DLS-Datenbank einlesen. Die Daten stehen dann für das Deployment zur Verfügung.

Für jede Datei auf dem FTP-Server wird pro Verwendungsmöglichkeit ein Objekt angelegt. So kann z. B. eine WAV-Datei sowohl als Klingelton als auch als Wartemusik (Music on Hold) verwendet werden. Für eine Datei „notify.wav“ würden also beispielsweise die beiden Objekte „notify.wav (OpenStage,RINGTONE)“ und „notify.wav (OpenStage,MOH)“ angelegt.

HINWEIS: Die Angaben hängen von der Konfiguration des jeweils verwendeten FTP-Servers ab. Weitere Informationen zur Konfiguration von FTP-Servern siehe Abschnitt 4.12.1, “FTP Server”.

Ein FTP-Server wird benötigt, um Daten wie beispielsweise Telefonsoftware-Images oder Wartemusik auf ein Endgerät zu laden. Zudem ist die Konfiguration mindestens eines FTP-Servers erforderlich, damit der DLS die verfügbaren Telefonsoftware-Images registrieren kann.

HINWEIS: Im Unterschied zu Software und Dateien für IP Phones, die auf einem FTP-Server vorliegen müssen, werden Software und Dateien für IP Clients auf einem Netz-Laufwerk bereitgestellt, wie unter **Netzlaufwerk Konfiguration** eingerichtet.



FTP-Server ID:

Eindeutiger Name, um den jeweils konfigurierten FTP-Server zu verwalten und anzusprechen.

Hostname:

Hostname oder IP-Adresse des FTP-Servers (von den IP Devices aus erreichbar).

Interner Hostname

Diese URL wird, falls angegeben, vom DLS für Scan und Software-Überprüfung verwendet.

Die Konfigurationsdateien, in denen IP-Adressen und Workgroup-Namen einander zugeordnet werden, finden Sie unter:

```
C:\Windows\system32\drivers\etc\hosts
```

Fügen Sie die IP-Adresse und den Namen des internen FTP-Server-Hosts zur Datei (Host) hinzu.

HINWEIS: Diese Änderungen muss auf allen Knoten einer Multi-Node-Umgebung durchgeführt werden.

IP Protokoll Modus

Vom FTP-Server unterstützte IP-Version.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

SW Image Pfad:

Pfad zum Software-Image, relativ zur Verzeichnis-Root des FTP-Servers. Wenn die Daten direkt im Verzeichnis-Root liegen, geben Sie „/“ („Slash“) ein.

Port:

Die Standard-Portnummer für FTP ist 21 und kann nicht geändert werden.

Benutzername:

Benutzername für den Lese-Zugriff auf dem FTP-Server. Der lesende Zugriff wird für den Zugriff der IP Devices auf die Software verwendet.

Passwort:

Passwort für den Lese-Zugriff auf dem FTP-Server. Diese Angabe ist optional.

Paralleler Zugriff zum Software Server

Maximale Zugriffe zum Server

Maximale Anzahl der gleichzeitig möglichen Zugriffe auf den jeweiligen Server. Dieser Wert entspricht der Anzahl der gleichzeitigen Verteilungsaktionen der Software (Software Deployment-Jobs) an die Geräte. Der Wert muss kleiner sein als die maximale Anzahl der gleichzeitigen Verbindungen, für die der FTP-Server konfiguriert ist

Wertebereich: **1 - 500**.

Standard: **10**.

Verzögerungszeit (sek):

Zeit zwischen zwei Verteilungsaufträgen. Der vorgegebene Wert sollte jedoch nur bei einer langsamen LAN-Infrastruktur (im speziellen bei einer nur mäßig schnellen Verbindung zum FTP-Server) erhöht werden.

Wertebereich: **1 - 3000** Sekunden.

Standard: **10**.

Keine Software-Überprüfung beim Deployment

Wenn der DLS den FTP Server nach Dateien durchsucht (Scan), überprüft er alle Telefonsoftware-Dateien. Dabei werden Header und Footer der Dateien überprüft. Ist der Schalter deaktiviert, so wird die Überprüfung wiederholt, bevor eine Software-Datei auf das Telefon gespielt wird. Ist er aktiviert, so entfällt diese Überprüfung.

Status:

Status der Server-Aktion.

Mögliche Werte:

- **scannen läuft**

- **Beendet**
- **scannen gestoppt**

Start Scan

Der FTP-Server wird nach Software- und Daten-Dateien durchsucht. Einträge zu Dateien, die nicht mehr auf dem Server zu Verfügung stehen, werden in der DLS-Datenbank gelöscht.

Stop Scan

Durchsuchen des FTP-Servers nach Software- und Daten-Dateien abbrechen.

Images auf dem Server

Wenn ein Scan durchgeführt worden ist, werden hier Informationen zu allen Software- und Daten-Dateien angezeigt, die beim Scan gefunden worden sind.

SW Name:

Name der Datei.

SW Pfad:

Verzeichnispfad und Dateiname

Objekt Typ:

Typ der Datei je nach Verwendungszweck auf dem Telefon.

Beispiele: **Software Image**, **Logo Datei**, **Bildschirmschoner**

Gerätetyp:

Gerätetyp, für den die Datei geeignet ist.

Beispiele: **optiPoint 410**, **OpenStage Hi**,**OpenStage Lo.**

HINWEIS: OpenStage 15 und OpenStage 40 werden gemeinhin unter der Bezeichnung ‘OpenStage Lo’ zusammengefasst.
OpenStage 15-Endgeräte gehören zur Gerätesoftwarekategorie ‘Lo’ und verwenden eine gemeinsame Firmware für OpenStage 15, OpenStage 20 und OpenStage 40.

HINWEIS: Bei der automatischen Bereitstellung von Software (SW) ermittelt DLS die passende Firmware basierend auf der Familienzugehörigkeit (Hi oder Lo) sowie der gewünschten SW-Version. Der DLS durchsucht die FTP-Liste, bis die erste verfügbare Firmware gefunden wird, die den angegebenen Kriterien entspricht und eine gültige Übereinstimmung wird angeboten. Der DLS stellt daraufhin die korrekte Firmware bereit (soweit OS15 und OS40 zur gleichen Familie gehören und die gleichen Firmware-Daten haben), auch wenn die angezeigten für das SW-Update verwendeten Dateinamen möglicherweise irreführend sind.
Bei der manuellen SW-Bereitstellung müssen Sie die zu installierende Firmware-Datei explizit auswählen.

SW Typ:

Typ der Telefon-Software.

Beispiele: **Unify SIP**, **Unify HFA**.

SW Version:

Version der Telefon-Software.

Status:

Status der Telefon-Software.

Beispiel: **version info missing**.

Gültig:

Ist aktiviert, wenn es sich um ein eine gültige Datei handelt.

Mögliche Aktionsschaltflächen

Suchen

Durchsucht die Datenbank nach bereits eingestellten FTP-Servern.

Fenster leeren

Löscht die eingegebenen Daten aus dem Fenster.

Sichern

Sichert die eingegebenen/geänderten Daten.

Verwerfen

Verwirft die vorgenommenen Änderungen.

Neu

Legt einen neuen FTP-Server an.

Löschen

Löscht den gerade in der Objektansicht befindlichen FTP-Server.

Test FTP Parameter

Testet die Verbindung zum aktuell konfigurierten FTP-Server. Das Ergebnis wird im Statusfenster angezeigt.

Aktualisieren

Aktualisiert die Feldinhalte aus der Datenbank.

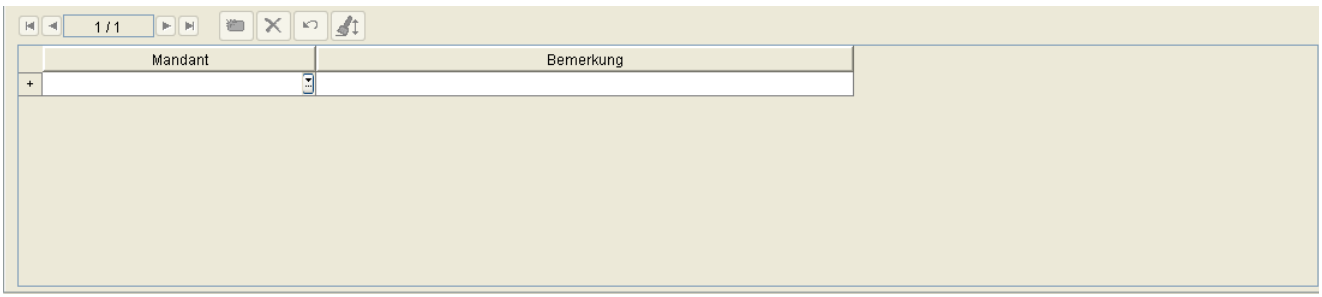
Alle Scannen

Alle eingerichteten FTP-Server werden nacheinander gescannt. Eine Fortschrittsanzeige zeigt den Status des Scans des aktuellen Servers an. Sie können diesen Scan wie auch die einzelnen Scans abbrechen, indem man **Stop Scan** drückt.

6.3.4.1 Register „Mandanten“

Aufruf: Hauptmenü > Administration > Server Konfiguration > FTP Server Konfiguration > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.



Mandant

Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

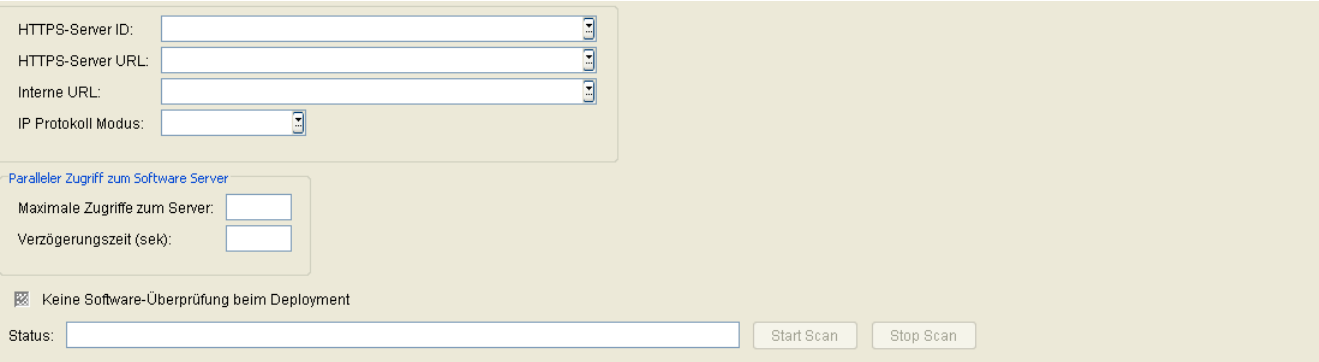
6.3.5 HTTPS Server Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Images auf dem Server“
- Register „HTTPS Server CA Zertifikate“
- Register „Trust Anchor“
- Register „Mandanten“

Allgemeine Daten

Aufruf: Hauptmenü > Administration > Server Konfiguration > HTTPS Server Konfiguration.



HINWEIS: HTTPS Server können nur für OpenStage Devices verwendet werden.

In diesem Bereich können Sie die Zugangsdaten für einen oder mehrere HTTPS-Server konfigurieren. In der Ansicht **Tabelle** sind alle über die Suche gefundenen HTTPS-Server aufgelistet.

Ein HTTPS-Server kann alternativ zu einem FTP-Server verwendet werden, um Daten wie etwa Wartemusik oder Telefonsoftware-Images auf ein OpenStage-Endgerät zu laden. Zudem ist die Konfiguration mindestens eines HTTPS-Servers erforderlich, damit der DLS die verfügbaren Telefonsoftware-Images registrieren kann.

HINWEIS: Die Angaben hängen von der Konfiguration des jeweils verwendeten HTTPS-Servers ab.

HINWEIS: Im Unterschied zur Software für IP Phones, die auf einem HTTPS -Server vorliegen muss, wird die Software für IP Clients auf einem Netz-Laufwerk bereitgestellt, wie unter Netzlaufwerk Konfiguration eingerichtet.

HTTPS-Server ID

Eindeutiger Name, um den jeweils konfigurierten HTTPS-Server zu verwalten und anzusprechen.

HTTPS-Server URL

URL des HTTPS-Servers. Diese muss von den IP Devices aus erreichbar sein.

Interner Hostname

Diese URL wird, falls angegeben, vom DLS für Scan und Software-Überprüfung verwendet.

Die Konfigurationsdateien, in denen IP-Adressen und Workgroup-Namen einander zugeordnet werden, finden Sie unter:

```
C:\Windows\system32\drivers\etc\hosts
```

Fügen Sie die IP-Adresse und den Namen des internen FTP-Server-Hosts zur Datei (Host) hinzu.

HINWEIS: Diese Änderungen muss auf allen Knoten einer Multi-Node-Umgebung durchgeführt werden.

IP Protokoll Modus

Vom HTTPS-Server unterstützte IP-Version.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Paralleler Zugriff zum Software Server

Maximale Zugriffe zum Server

Maximale Anzahl der gleichzeitig möglichen Zugriffe auf den jeweiligen Server. Dieser Wert entspricht der Anzahl der gleichzeitigen Verteilungsaktionen der Software (Software Deployment-Jobs) an die Geräte. Der Wert muss kleiner sein als die maximale Anzahl der gleichzeitigen Verbindungen, für die der HTTPS-Server konfiguriert ist

Wertebereich: **1 - 500**.

Standard: **10**.

Verzögerungszeit (in Sekunden)

Zeit zwischen zwei Verteilungsaufträgen. Der vorgegebene Wert sollte jedoch nur bei einer langsamen LAN-Infrastruktur (im speziellen bei einer nur mäßig schnellen Verbindung zum HTTPS-Server) erhöht werden.

Wertebereich: **1 - 3000** Sekunden.

Standard: **10**.

Keine Software-Überprüfung beim Deployment

Wenn der DLS den HTTPS Server nach Dateien durchsucht (Scan), überprüft er alle Telefonsoftware-Dateien. Dabei werden Header und Footer der Dateien überprüft. Ist der Schalter deaktiviert, so wird die Überprüfung wiederholt, bevor eine Software-Datei auf das Telefon gespielt wird. Ist er aktiviert, so entfällt diese Überprüfung.

Status:

Status der Server-Aktion.

Mögliche Werte:

- **scannen läuft**
- **Beendet**
- **scannen gestoppt**

Start Scan

Der HTTPS-Server wird nach Software- und Daten-Dateien durchsucht. Einträge zu Dateien, die nicht mehr auf dem Server zu Verfügung stehen, werden in der DLS-Datenbank gelöscht.

Stop Scan

Durchsuchen des HTTPS-Servers nach Software- und Daten-Dateien abbrechen.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Durchsucht die Datenbank nach bereits konfigurierten HTTPS-Servern.

Fenster leeren

Löscht die eingegebenen Daten aus dem Fenster.

Neu

Legt einen neuen HTTPS-Server an.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Test

Testet die Verbindung zum aktuell konfigurierten HTTPS-Server. Das Ergebnis wird im Statusfenster angezeigt.

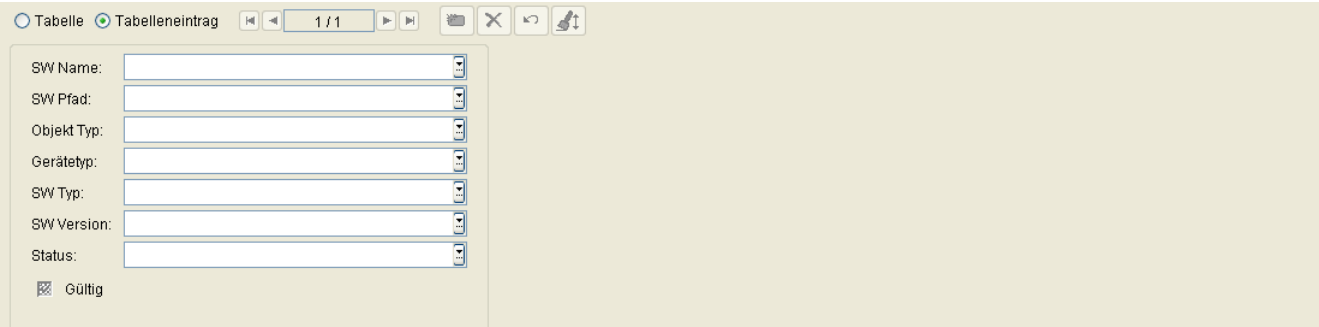
Alle Scannen

Alle eingerichteten HTTPS-Server werden nacheinander gescannt. Eine Fortschrittsanzeige zeigt den Status des Scans des aktuellen Servers an. Sie können diesen Scan wie auch die einzelnen Scans abbrechen, indem man **Stop Scan** drückt.

6.3.5.1 Register „Images auf dem Server“

Aufruf: Hauptmenü > Administration > Server Konfiguration > HTTPS Server Konfiguration > Register „Images auf dem Server“

Wenn ein Scan durchgeführt worden ist, werden hier Informationen zu allen Software- und Daten-Dateien angezeigt, die beim Scan gefunden worden sind.



SW Name:

Name der Datei.

SW Pfad:

Verzeichnispfad und Dateiname

Objekt Typ:

Typ der Datei je nach Verwendungszweck auf dem Telefon.

Beispiele: **Software Image**, **Logo Datei**, **Bildschirmschoner**

Gerätetyp:

Gerätetyp, für den die Datei geeignet ist.

Beispiele: **optiPoint 410**, **OpenStage Hi**.

SW Typ:

Typ der Telefon-Software.

Beispiele: **Unify SIP**, **Unify HFA**.

SW Version:

Version der Telefon-Software.

Status:

Status der Telefon-Software.

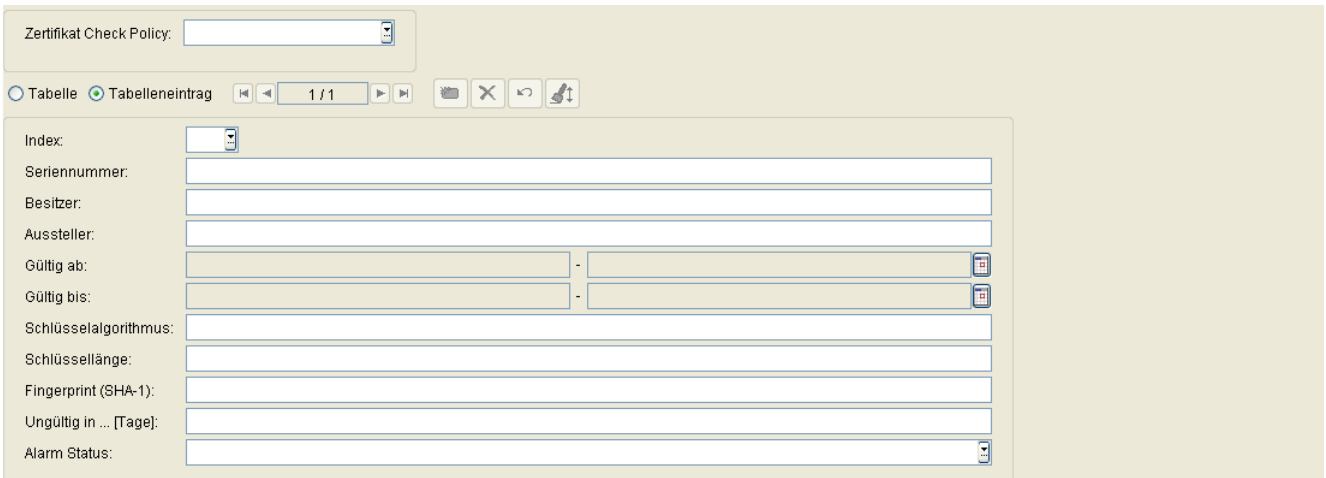
Beispiel: **version info missing**.

Gültig:

Ist aktiviert, wenn es sich um ein eine gültige Datei handelt.

6.3.5.2 Register „HTTPS Server CA Zertifikate“

Aufruf: Hauptmenü > Administration > Server Konfiguration > HTTPS Server Konfiguration > Register „HTTPS Server CA Zertifikate“



Zertifikat Check Policy

Legt fest, ob und wie das Zertifikat überprüft wird.

Mögliche Werte:

- **Keine**

  Keine Authentifizierung des Servers. Ungültige Zertifikate, die vom Server empfangen oder vorher vom IP Phone geladen wurden, werden ignoriert. HTTPS-Verbindungen werden immer ohne Authentifizierung aufgebaut.

- **Trusted**

  Die Zertifikate werden überprüft auf „abgelaufen“, „nicht gültig“, „signed by trusted CA“ und „zurückgerufen“. Dazu sind eine oder zwei Listen mit „trusted CAs“ erforderlich, wobei für „Trusted“ und „Voll“ dieselben Listen verwendet werden. „Trusted“ CAs können Root CAs, kurzzeitig angelegte CAs oder sogar das Server-Zertifikat selbst sein. Weitere Werte wie Besitzer, Aussteller etc. werden nicht überprüft. HTTPS-Verbindungen zum Server werden auch dann aufgebaut, wenn einige Werte des Zertifikates falsch sind.

- **Voll**

  Die Zertifikate werden überprüft auf „abgelaufen“, „nicht gültig“, „signed by trusted CA“ , „zurückgerufen“, passenden Besitzer etc. Dazu sind eine oder zwei Listen mit „trusted CAs“ erforderlich, wobei für „Trusted“ und „Voll“ dieselben Listen verwendet werden. „Trusted“ CAs können Root CAs, kurzzeitig angelegte CAs oder sogar das Server-Zertifikat selbst sein. HTTPS-Verbindungen zum Server werden nur für gültige und korrekte Zertifikate aufgebaut.

Index

Index des Zertifikats.

Seriennummer:

Seriennummer des Zertifikats (nur Anzeige).

Besitzer:

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) des Zertifikats (nur Anzeige).

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarmstatus des Zertifikats (nur Anzeige).

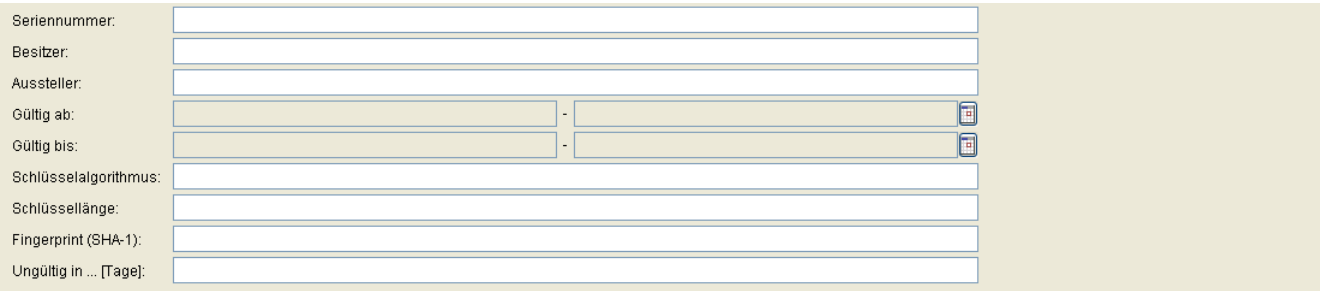
Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

6.3.5.3 Register „Trust Anchor“

Aufruf: Administration > Server Konfiguration> HTTPS Server Konfiguration > Register „Trust Anchor“

Für jede Konfiguration muss ein Trust Anchor eingerichtet werden. In den meisten Szenarien ist es die Root-CA selbst, es kann aber auch eine untergeordnete CA sein. Die Konfiguration kann nur gespeichert werden, wenn ein Trust Anchor eingetragen ist!



Seriennummer

Seriennummer des Zertifikats (nur Anzeige).

Besitzer

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Zertifikat (nur Anzeige).

Ungültig in ... [Tage]:

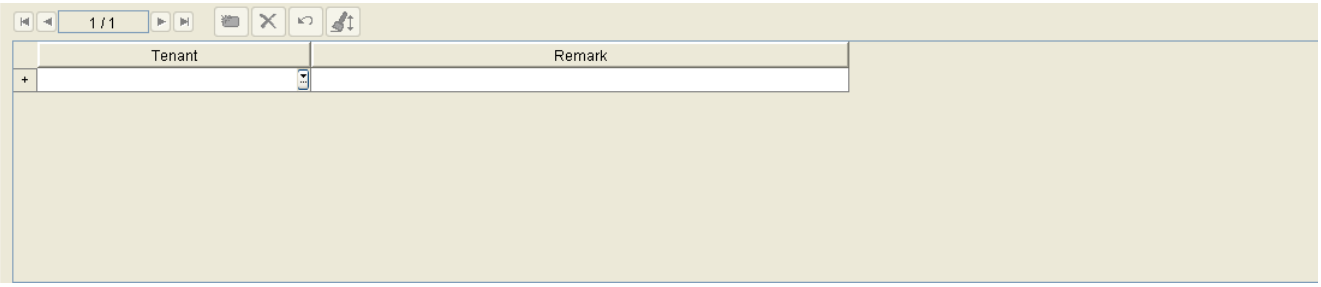
Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

6.3.5.4 Register „Mandanten“

Aufruf: Hauptmenü > Administration > Server Konfiguration > HTTPS Server Konfiguration > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.



Mandant

Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

6.3.6 HTTPS Client Konfiguration

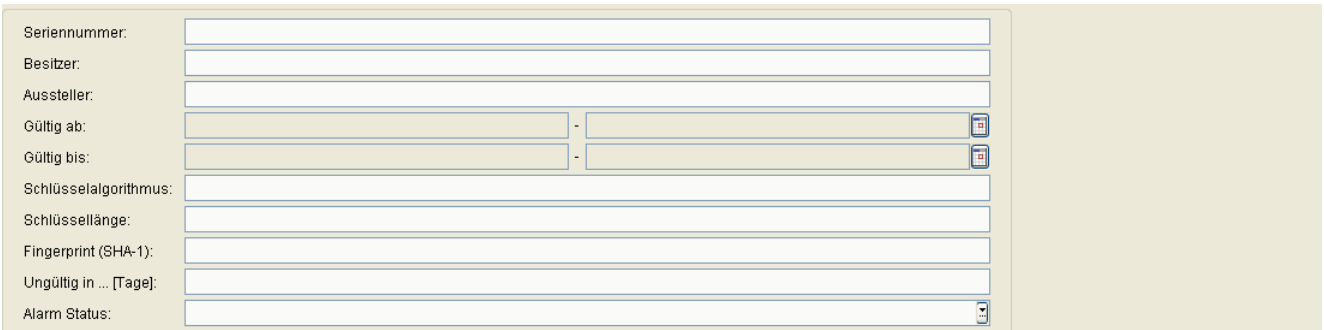
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen

Allgemeine Daten

Aufruf: Hauptmenü > Administration > Server Konfiguration > HTTPS Client Konfiguration.

In diesem Menüpunkt können Zertifikate der HTTPS Client Konfiguration importiert und angezeigt werden.



Seriennummer:

Seriennummer des Zertifikats (nur Anzeige).

Besitzer:

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus des Zertifikats (nur Anzeige).

Schlüssellänge

Schlüssellänge des Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) des Zertifikats (nur Anzeige).

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig (nur Anzeige).

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarmstatus des Zertifikats (nur Anzeige).

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Durchsucht die Datenbank nach bereits konfigurierten HTTPS-Servern.

Fenster leeren

Löscht die eingegebenen Daten aus dem Fenster.

Zertifikat importieren

HTTPS Client Zertifikat importieren.

Synchronize Keystore

Synchronisation des Keystore starten.

6.3.7 Netzlaufwerk Konfiguration

Aufruf: Hauptmenü > Administration > Server Konfiguration > Netzlaufwerk Konfiguration.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Mandanten“

Allgemeine Daten

In diesem Bereich können Sie eines oder mehrere Netzlaufwerke konfigurieren.

HINWEIS: Das Deployment über ein Netzlaufwerk steht in der onboard-Variante des DLS auf OpenScape Voice nicht zur Verfügung.

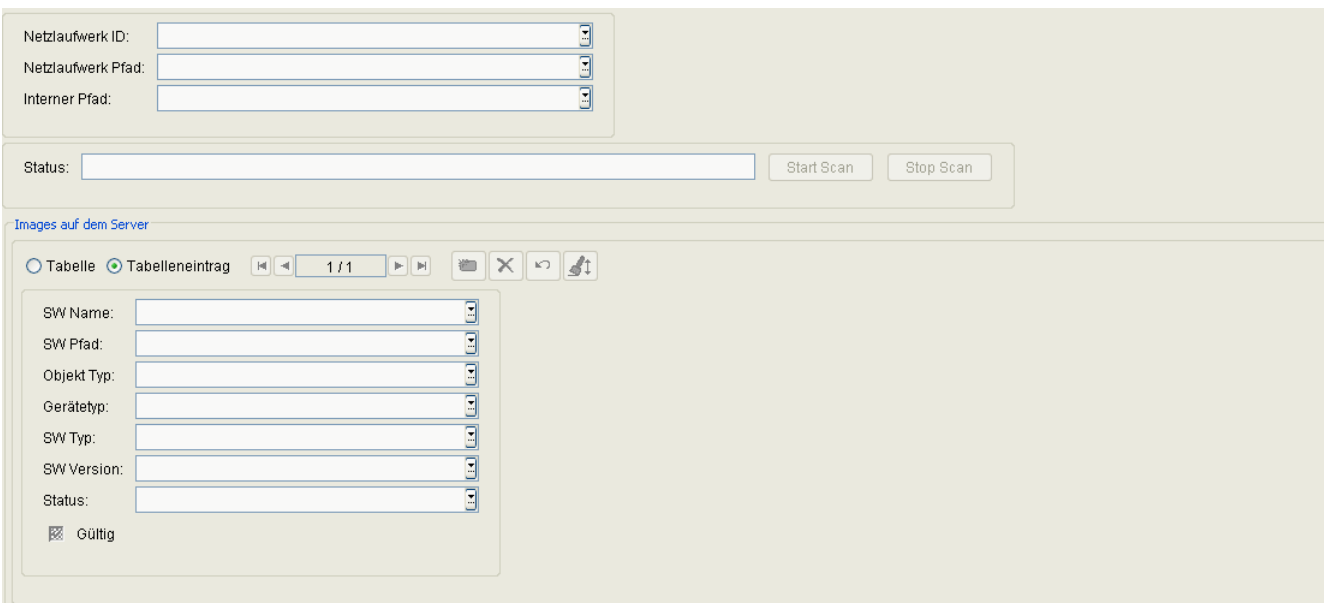
HINWEIS: Die Angaben hier sind nur für die Verteilung von Software für IP Clients erforderlich. Der Zugriff auf Software für IP Phones erfolgt mittels FTP/HTTPS; die Konfiguration der Server erfolgt im Bereich **FTP Server Konfiguration** oder **HTTPS Server Konfiguration**.

Die Berechtigungen für Zugriffe auf die Netzwerkfreigabe müssen auf *[DLS-Servername]\system* gesetzt werden, um dem DLS-Webserver, der im Standardfall als Dienst läuft, Zugriff zu gewähren.

Ist es nicht möglich, diese Berechtigungen zu erweitern, bzw. sind die Berechtigungen für die Zugriffe auf die Netzwerkfreigaben auf eine Benutzergruppe eingeschränkt, so ist darauf zu achten, dass der DLS in dem Benutzerkontext läuft, der auch in dieser Benutzergruppe enthalten ist bzw. der Zugriff auf diese Netzwerkfreigabe hat.

Der Benutzerkontext kann wie folgt geändert werden (Beispiel Windows XP):
Start > **Einstellungen** > **Systemsteuerung** > **Verwaltung** > **Dienste** > **DeploymentService** > [rechte Maustaste] **Eigenschaften** > Register **Anmelden**.

Geben Sie die erforderlichen Daten für das Windows-Netzlaufwerk ein.



Netzlaufwerk ID:

Eindeutiger Name, um das jeweils konfigurierte Netzlaufwerk anzusprechen (von den IP Clients aus erreichbar).

Netzlaufwerk Pfad:

Computername oder IP-Adresse des Rechners, auf dem das Laufwerk freigegeben ist, sowie Pfad des freigegebenen Verzeichnisses. Das Verzeichnis muss von den IP Clients aus erreichbar sein.

Interner Pfad

Falls angegeben, wird dieser Pfad vom DLS für den Scan verwendet.

Status:

Status der Server-Aktion.

Mögliche Werte:

- **scannen läuft**
- **Beendet**
- **scannen gestoppt**

Start Scan

Das Netzlaufwerk wird nach Software- und Daten-Dateien durchsucht. Einträge zu Dateien, die nicht mehr auf dem Server zu Verfügung stehen, werden in der DLS-Datenbank gelöscht.

Stop Scan

Durchsuchen des Netzlaufwerks nach Software- und Daten-Dateien abbrechen.

Images auf dem Server

Wenn ein Scan durchgeführt worden ist, werden hier Informationen zu allen Software- und Daten-Dateien angezeigt, die beim Scan gefunden worden sind.

SW Name:

Name der Datei.

SW Pfad:

Verzeichnispfad und Dateiname

Objekt Typ:

Typ der Datei je nach Verwendungszweck auf dem Telefon.

Beispiele: **Software Image**, **Logo Datei**, **Bildschirmschoner**

Gerätetyp:

Gerätetyp, für den die Datei geeignet ist.

Beispiele: **optiPoint 410**, **OpenStage Hi**.

SW Typ:

Typ der Telefon-Software.

Beispiele: **Unify SIP**, **Unify HFA**.

SW Version:

Version der Telefon-Software.

Status:

Status der Telefon-Software.

Beispiel: **version info missing**.

Gültig:

Ist aktiviert, wenn es sich um ein eine gültige Datei handelt.

Mögliche Aktionsschaltflächen

Sichern

Sichert die eingegebenen/geänderten Daten.

Verwerfen

Verwirft die vorgenommenen Änderungen.

Neu

Legt ein neues Netzlaufwerk an.

Löschen

Löscht den gerade in der Objektansicht befindlichen Netzlaufwerk-Pfad.

Aktualisieren

Aktualisiert die Feldinhalte aus der Datenbank.

Alle Scannen

Alle eingerichteten Netzlaufwerke werden nacheinander gescannt. Eine Fortschrittsanzeige zeigt den Status des Scans des aktuellen Netzlaufwerks an.

Sie können diesen Scan wie auch die einzelnen Scans abbrechen, indem man **Stop Scan** drückt.

6.3.7.1 Register „Mandanten“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Netzlaufwerk Konfiguration > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.

Mandant

Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

6.3.8 Infrastruktur Policy

Aufruf: Hauptmenü > Administration > Server Konfiguration > Infrastruktur Policy

In dieser Maske werden die Daten für die Zuordnung einer Infrastruktur-Policy nach Switch IP Adresse, Switch Port und Network Policy erfasst. Die Zuordnung folgt nach der Reihenfolge des Eintrags, d. h. der erste passende Eintrag führt zur Infrastruktur Policy.

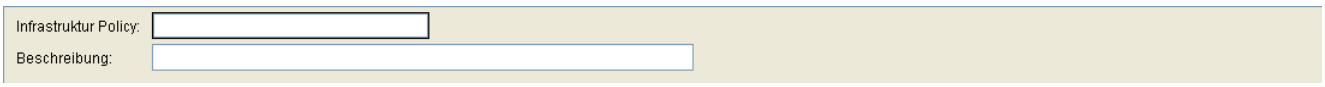
Für die für Zuordnung relevanten Werte können reguläre Ausdrücke verwendet werden. Ein leerer Wert wird als nicht relevant für die Zuordnung bewertet.

Um eine automatische Anpassung zu veranlassen, muss die Infrastruktur Policy einem Standort zugeordnet werden (siehe **Administration** > **Server Konfiguration** > **Standort** > **Register „Infrastruktur Policies“**).

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Infrastruktur Policies“
- Register „Infrastruktur Policy“

Allgemeine Daten



Infrastruktur Policy:

Name der Infrastruktur-Policy.

Beschreibung:

Beschreibung der Infrastruktur-Policy.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Durchsucht die Datenbank nach bereits konfigurierten IP-Infrastruktur-Policies.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht Suche können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Legt eine neue IP-Infrastruktur-Policy an.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

Verwirft die eingetragenen Änderungen.

Aktualisieren

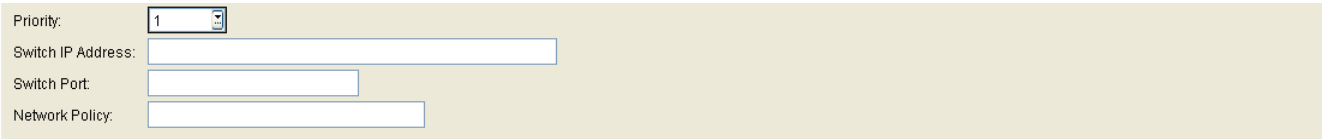
Aktualisiert das Fenster anhand der Datenbank.

Anwenden

IP-Infrastruktur-Tabelle wird auf schon registrierte IP Devices erneut angewandt.

6.3.8.1 Register „Infrastruktur Policy“

Aufruf: Hauptmenü > Administration > Server Konfiguration > Infrastruktur Policy > Register „Infrastruktur Policy“



Priorität:

Priorität, nach der die IP Policy abgearbeitet und zugeordnet wird.

Switch IP Adresse:

IP-Adresse des Switches, an dem das IP Phone steckt.

Reguläre Ausdrücke können verwendet werden.

Switch Port:

Portnummer des Switches, an dem das IP Phone steckt.

Reguläre Ausdrücke können verwendet werden.

Network Policy:

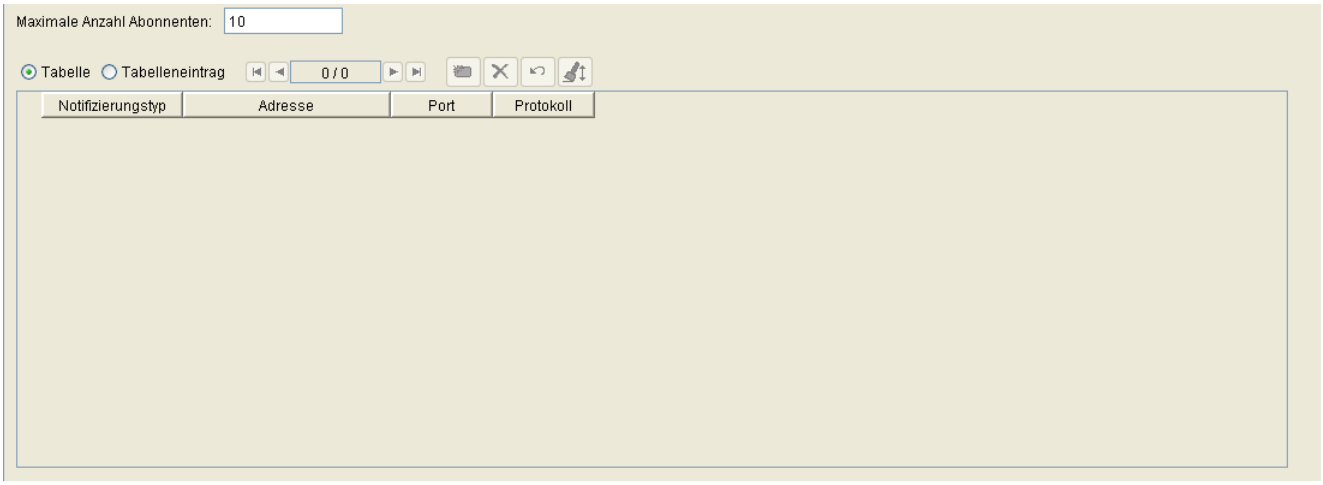
Dem IP Phone zugeordnete Netzwerk-Policy.

Reguläre Ausdrücke können verwendet werden.

6.3.9 API Notifizierungen

Aufruf: Hauptmenü > Administration > Server Konfiguration > API Notifizierungen

Diese Maske zeigt einen Überblick über die aktuellen Einwahlen zur API-Notifizierung. Der Benutzer kann die Anzahl der Einwahlen begrenzen und auch Einträge löschen.



Maximale Anzahl Abonnenten:

Der Versuch, Notifizierungen zu abonnieren schlägt fehl, wenn diese Zahl schon erreicht ist.

Notifizierungstyp

Art der Notifizierung.

Mögliche Werte:

- **inventoryInfo**
  Neue IP Phones und E.164 Änderungen werden notifiziert.
- **serverStart**
  Notifizierung bei DLS-Server Start.

Adresse

Ziel-IP-Adresse für die Notifizierung.

Port

Zielport für die Notifizierung.

Protokoll

Das für die Notifizierung zu verwendende Protokoll: UDP.

6.3.10 XML Applikationen

Aufruf: Hauptmenü > Administration > Server Konfiguration > XML Applikationen

Hier werden Einstellungen zu XML-Applikationen vorgenommen.

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Deployment Service“
- Register „Location Service“
- Register „News Service“
- Register „MakeCall“

Allgemeine Daten

XML Applikationen Passwort

Gemeinsames Passwort für alle passwortgeschützten XML-Applikationen.

DLS Adresse

IP-Adresse des DLS. Bei einer Multi-Node-Installation ist das die IP-Adresse des DLS-Clusters.

Trace Level

Trace Level für XML-Applikationen, die als eigenständige Web-Applikation laufen. Die Trace-Daten werden unter `<Installationsverzeichnis>\Tomcat5\webapps\XMLApplications\log\dlsXMLAppsLog.txt` abgelegt.

Mögliche Optionen:

- **ERROR**
- **INFO**
- **DEBUG**

Mögliche Aktionsschaltflächen

Verwerfen

Verwirft die eingetragenen Änderungen.

Sichern

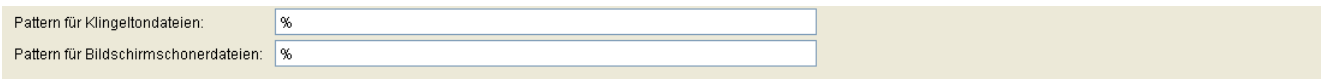
Sichert die Feldinhalte in der Datenbank.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.3.10.1 Register „Deployment Service“

Aufruf: Hauptmenü > Administration > Server Konfiguration > XML Applikationen > Register „Deployment Service“



Pattern für Klingelton Dateien

Muster für die teilqualifizierte Auswahl von Klingeltondateien, die auf dem FTP- oder HTTPS-Server verfügbar sind.

Beispiel: ***Unify*New*Devices***

Pattern für Bildschirmschoner

Muster für die teilqualifizierte Auswahl von Bildschirmschonerdateien, die auf dem FTP- oder HTTPS-Server verfügbar sind.

Beispiel: ***Unify*New*Devices***

6.3.10.2 Register „Location Service“

Aufruf: Hauptmenü > Administration > Server Konfiguration > XML Applikationen > Register „Location Service“

Authentifizierung

Auswahl des Passworts zum Ausführen dieser XML-Applikation.

Mögliche Optionen:

- **IP Device User Passwort**

  HINWEIS: Soll die Rufnummer des OpenStage-Endgerätes geändert werden, handelt es sich hierbei um das Passwort desjenigen virtuellen Geräts, dem die neue Rufnummer zugewiesen ist.

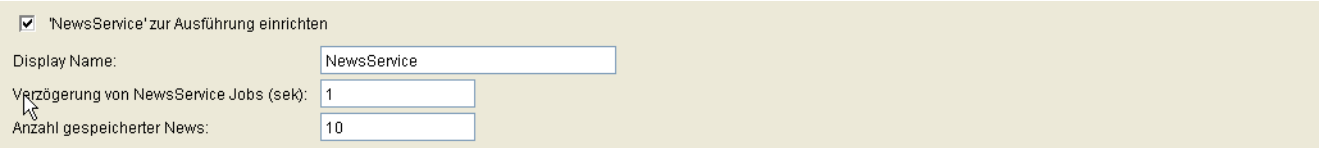
- **XML Applikationen Passwort**
- **IP Device User Passwort oder XML Applikationen Passwort**

Factory Reset Password

Passwort, um an OpenStage-Endgeräten einen Factory Reset durchführen zu können. Dabei werden die Werkseinstellungen wiederhergestellt.

6.3.10.3 Register „News Service“

Aufruf: Hauptmenü > Administration > Server Konfiguration > XML Applikationen > Register „News Service“



‘News Service’ zur Ausführung einrichten

Wenn aktiviert, wird die XML-Applikation ‘NewsService’ vor der ersten Ausführung eingerichtet, falls sie am Endgerät noch nicht konfiguriert ist.

Display Name:

Dieser Name wird für die XML-Applikation ‘NewsService’ am Display des Endgerätes angezeigt, wenn diese automatisch eingerichtet worden ist.

Verzögerung von News Service Jobs (sek)

Verzögerung von Jobs in Sekunden nach Massenänderungen (Bulk change). Dabei handelt es sich um die minimale Zeit zwischen dem Senden der gleichen Meldung an zwei verschiedene Endgeräte. Hinweise werden nicht verzögert.

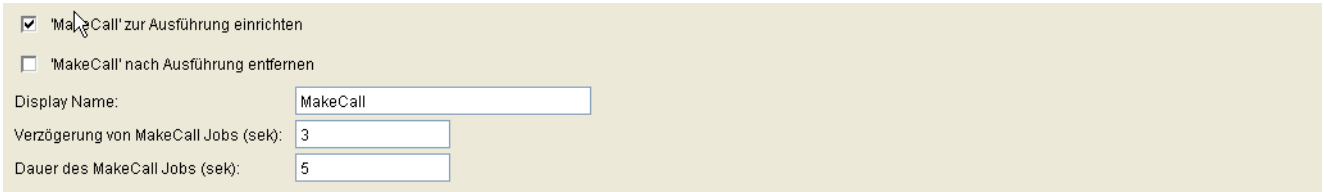
Wertebereich: **1** - **300**

Anzahl gespeicherte News

Anzahl der News, die mittels der XML-Applikation ‘NewsService’ bereits gesendet und gespeichert wurden. Die gespeicherten News können am Endgerät erneut gelesen werden. Sobald die Anzahl überschritten ist, wird die älteste Nachricht gelöscht.

6.3.10.4 Register „MakeCall“

Aufruf: Hauptmenü > Administration > Server Konfiguration > XML Applikationen > Register „MakeCall“



‘MakeCall’ zur Ausführung einrichten

Schalter zur Aktivierung der ersten Bereitstellung der MakeCall-Applikation.

Wenn aktiviert, wird die XML-Applikation ‘MakeCall’ vor der ersten Ausführung eingerichtet, falls sie am Endgerät noch nicht konfiguriert ist.

‘MakeCall’ nach Ausführung entfernen

Wenn aktiviert, wird die XML-Applikation ‘MakeCall’ vom Endgerät entfernt, nachdem sie ausgeführt worden ist.

Display Name:

Dieser Name wird für die XML-Applikation ‘MakeCall’ am Display des Endgerätes angezeigt, wenn diese automatisch eingerichtet worden ist.

Verzögerung von MakeCalls Jobs (sek)

Minimale Zeit in Sekunden zwischen dem Initiieren eines Anrufes von zwei verschiedene Endgeräten aus; wird für Massenänderungen (Bulk-Change) zu benötigt.

Wertebereich: **1** ... **500**

Dauer des MakeCall Jobs (sek)

Die Dauer entspricht der Summe der Zeit für das Initiieren des Anrufes und des Anrufes selbst in Sekunden.

6.3.11 Optionen

Aufruf: Hauptmenü > Administration > Server Konfiguration > Optionen

Suchen

Max. Anzahl Ergebnisse bei einer Suche

Maximale Anzahl der angezeigten Ergebnisse, wenn eine Suche ausgeführt wird.

HINWEIS: Der geänderte Wert wird erst nach Restart des DLS Client aktiv.

Max. Anzahl Ergebnisse in integrierten Tabellen

Maximale Anzahl der angezeigten Ergebnisse in integrierten Tabellen, wenn eine Suche ausgeführt wird.

HINWEIS: Der geänderte Wert wird erst nach Restart des DLS Client aktiv.

IP Device Papierkorb

IP Devices aus Papierkorb löschen nach Tagen

Anzahl der Tage bis zum vollständigen Löschen der zum Löschen markierten IP Devices aus der DLS-Datenbank.

Standardwert: 31 Tage

Wertebereich: **1** ... **365**

> ***HINWEIS:*** Wenn Sie den Parameter auf Null (0) setzen, wird der Wert beim nächsten Klick auf die Schaltfläche „Save (Speichern)“ oder bei Auswahl eines anderen Feldes auf den Standardwert geändert.

Nicht meldende IP Devices aus Papierkorb löschen

Anzahl der Tage bis zum vollständigen Löschen der sich nicht meldenden IP Devices aus der DLS-Datenbank.

Standardwert: 31 Tage

Wertebereich: **1** ... **365**

> ***HINWEIS:*** Wenn Sie den Parameter auf Null (0) setzen, wird der Wert beim nächsten Klick auf die Schaltfläche „Save (Speichern)“ oder bei Auswahl eines anderen Feldes auf den Standardwert geändert.

Mobile User Passwort Verfügbarkeit

Mobile User Passwort Verfügbarkeit in gemischten Netzen (Voreinstellung)

Ist dieser Schalter gesetzt und wird ein Mobile User Passwort an einem OpenStage Endgerät mit Software ab V3.0 geändert, so ist dieses Passwort auch an älteren Endgerätetypen oder Software-Versionen verfügbar. Ist der Schalter nicht gesetzt, kann es geschehen, dass das Mobile User Passwort bei älteren Endgerätetypen oder älteren Software-Versionen durch das Standardpasswort „000000“ ersetzt wird.

Nur für SIP-Phones verfügbar.

> ***WICHTIG:*** Diese Option wird bei der Erstanmeldung von Endgeräten am DLS als Standardwert verwendet.
> In Abschnitt 7.1.7.1, “Register „Passwörter“” wird die Aktivierung dieser Option für bestimmte IP-Telefone beschrieben (IP Phone Konfiguration).

> ***HINWEIS:*** Bei OpenStage V3 und höher wird das Passwort für Mobile User unter Verwendung von Hash-Werten übermittelt. Daher kann der DLS beim Klicken auf die Schaltfläche „Refresh (Aktualisieren)“ das Passwort nicht im Passwort-Feld anzeigen.
> Das Passwort ist nicht verloren gegangen; es ist in der grafischen Benutzeroberfläche von DLS nur nicht sichtbar.

Mögliche Aktionsschaltflächen

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Sichern

Sichert die Änderungen.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

6.3.12 TLS Connector Konfiguration

Aufruf: Hauptmenü > Administration > Server Konfiguration > TLS Connector Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Mögliche Aktionsschaltflächen
- Register „DLS Client GUI“
- Register „Truststore DLS Client GUI“
- Register „DLS API“
- Register „Truststore DLS API“

Mögliche Aktionsschaltflächen

Zertifikat importieren und aktivieren

Zertifikat importieren und aktivieren. Durch Klicken des Buttons wird ein Eingabefenster eingeblendet, in dem der Zertifikatstyp und die Importquelle ausgewählt werden.

Zertifikat entfernen

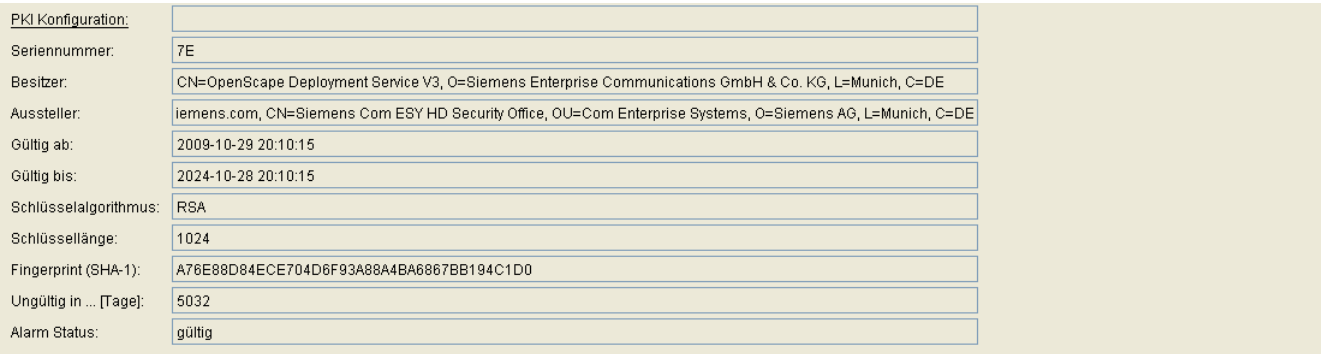
Zertifikat wird entfernt. Durch Klicken des Buttons wird ein Eingabefenster eingeblendet, in dem der Zertifikatstyp ausgewählt wird.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.3.12.1 Register „DLS Client GUI“

Aufruf: Hauptmenü > Administration > Server Konfiguration > TLS Connector Konfiguration > Register „DLS Client GUI“



Seriennummer:

Seriennummer des Zertifikats (nur Anzeige).

Besitzer:

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

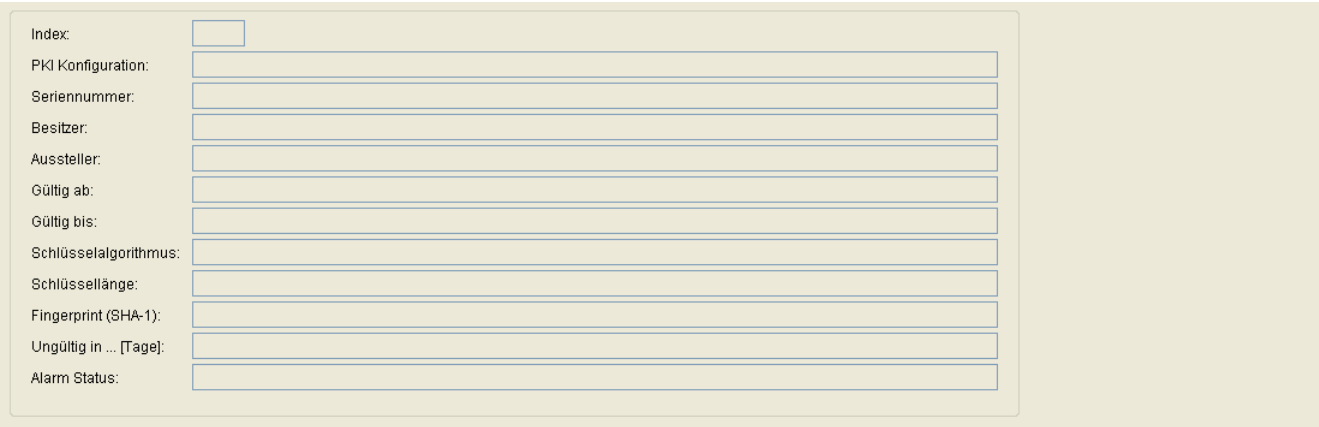
Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

6.3.12.2 Register „Truststore DLS Client GUI“

Aufruf: Hauptmenü > Administration > Server Konfiguration > TLS Connector Konfiguration > Register „Truststore DLS Client GUI“



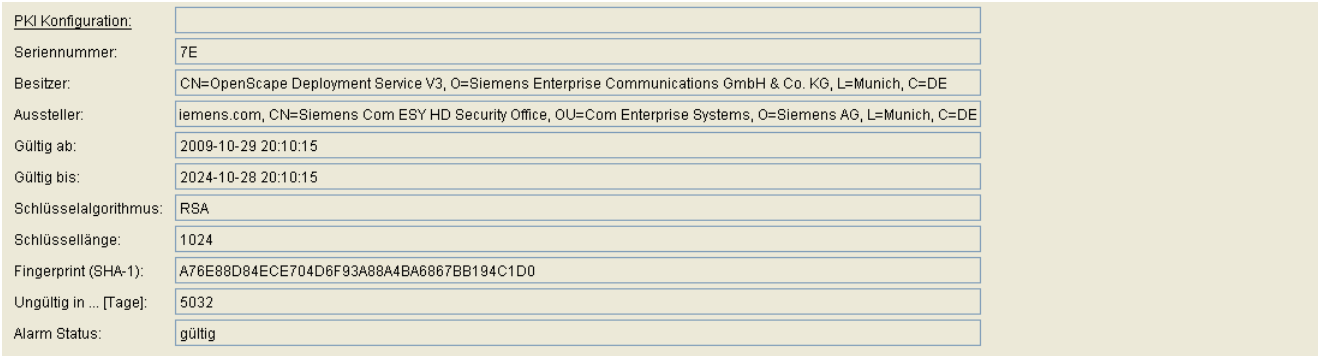
Index

Index des TLS Connectors.

Für die weiteren Parameter siehe Abschnitt 6.3.12.1, “Register „DLS Client GUI“”.

6.3.12.3 Register „DLS API“

Aufruf: Hauptmenü > Administration > Server Konfiguration > TLS Connector Konfiguration > Register „DLS API“

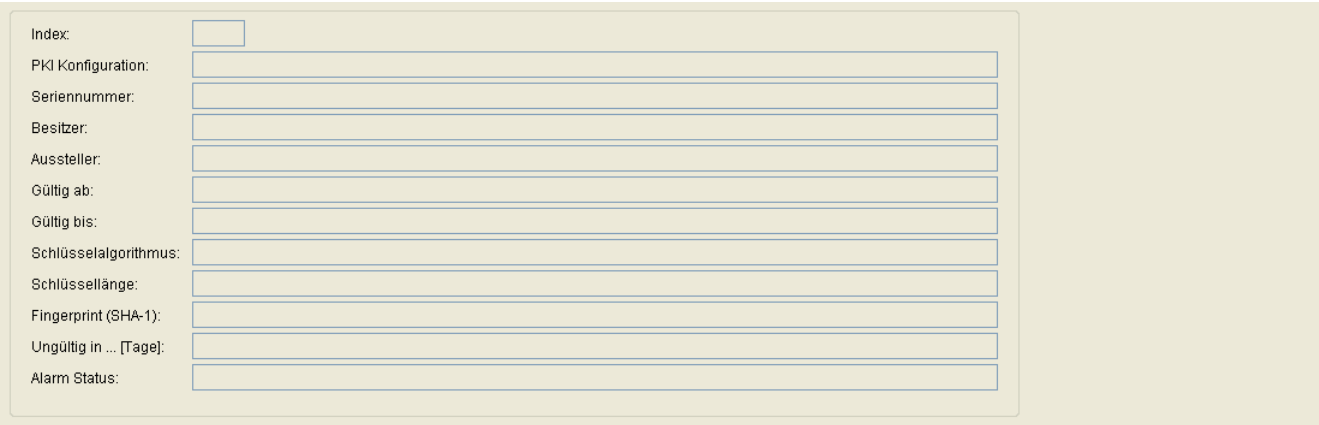


PKI Konfiguration:	
Seriennummer:	7E
Besitzer:	CN=OpenScape Deployment Service V3, O=Siemens Enterprise Communications GmbH & Co. KG, L=Munich, C=DE
Aussteller:	iemens.com, CN=Siemens Com ESY HD Security Office, OU=Com Enterprise Systems, O=Siemens AG, L=Munich, C=DE
Gültig ab:	2009-10-29 20:10:15
Gültig bis:	2024-10-28 20:10:15
Schlüsselalgorithmus:	RSA
Schlüssellänge:	1024
Fingerprint (SHA-1):	A76E88D84ECE704D6F93A88A4BA6867BB194C1D0
Ungültig in ... [Tage]:	5032
Alarm Status:	gültig

Für die weiteren Parameter siehe Abschnitt 6.3.12.1, “Register „DLS Client GUI“”.

6.3.12.4 Register „Truststore DLS API“

Aufruf: Hauptmenü > Administration > Server Konfiguration > TLS Connector Konfiguration > Register „Truststore DLS API“



Index

Index des TLS Connectors.

Für die weiteren Parameter siehe Abschnitt 6.3.12.1, “Register „DLS Client GUI“”.

6.4 Cluster Konfiguration

Aufruf: Hauptmenü > Administration > Cluster Konfiguration

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Deployment Server
- Cluster Einstellungen

6.4.1 Deployment Server

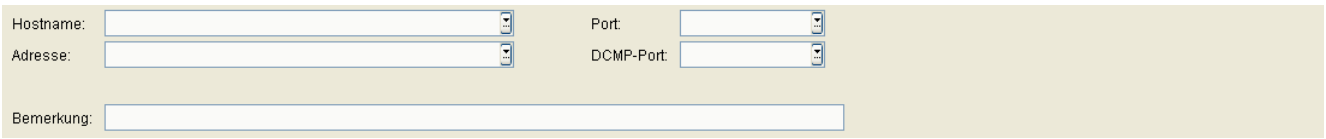
Aufruf: Hauptmenü > Administration > Cluster Konfiguration > Deployment Server

Dieser Bereich dient zur Überwachung und Steuerung der im Cluster installierten DLS-Server. Zudem kann der auf den einzelnen Servern laufende DLS gestoppt, gestartet oder neu gestartet werden. Voraussetzung ist, dass diese in der DLS-Datenbank als Knoten des Clusters registriert sind. Aktive Knoten registrieren sich im Abstand von 5 Minuten neu.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Allgemeine Daten



Hostname:

Name des Knotens im Cluster.

Adresse:

IP-Adresse, Domänenname oder Hostname des DLS.

Bemerkung:

Feld für allgemeine Informationen.

Port:

Portnummer des DLS.

DCMP-Port:

Portnummer des DCMP (DLS Communication Management Proxy).

Mögliche Aktionsschaltflächen

Suchen

Durchsucht die Datenbank nach bereits konfigurierten Servern, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

Deployment Service

Öffnet ein Dialogfenster zum Starten, Stoppen oder Neustarten des DLS auf den ausgewählten Knoten.

6.4.1.1 Register „Info“

Aufruf: Hauptmenü > Administration > Cluster Konfiguration > Deployment Server > Register „Info“

Letzte Registrierung

Datum der letzten Registrierung des Knotens am Cluster.

Status

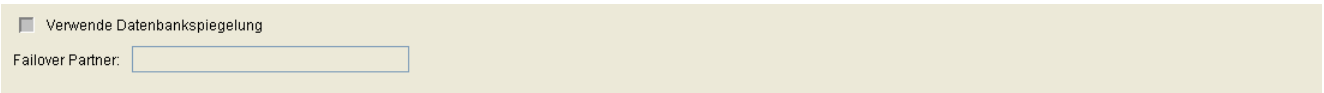
Status des Knotens im Cluster.

Mögliche Werte:

- **Aktiv**
  Der Knoten ist aktiv.
- **Inaktiv**
  Der Knoten hat sich entweder selbst inaktiv gemeldet oder wurde von anderen Knoten des Clusters als inaktiv erkannt.

6.4.2 Cluster Einstellungen

Aufruf: Hauptmenü > Administration > Cluster Konfiguration > Cluster Einstellungen



Verwende Datenbankspiegelung

Die Datenbankspiegelung kann eingeschaltet werden, was aber nur sinnvoll ist, wenn für die DLS Datenbank die MS SQL Server Datenbankspiegelung eingerichtet ist.

Failover Partner

IP Adresse der Spiegelinstanz für die DLS-Datenbank.

6.5 Protokoll-Daten

Aufruf: Hauptmenü > Administration > Protokoll-Daten

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Aktivitäten- und Fehlerprotokoll
- Audit- und Security Log Dateien
- P&P Import Protokolle
- Alarm Protokoll
- Alarm List

6.5.1 Aktivitäten- und Fehlerprotokoll

Aufruf: Hauptmenü > Administration > Server Konfiguration > Protokoll-Daten > Aktivitäten- und Fehlerprotokoll

Legen Sie fest, welche Ereignisse protokolliert werden und wie lange Ereignisse gespeichert werden sollen.

Sie können durch Auswahl von Filtern einen definierten Umfang von protokollierten Daten ansehen. Die gefilterten Daten werden in einem separaten Browser-Fenster angezeigt.

Dieser Bereich besteht aus folgenden Inhalten:

- Mögliche Aktionsschaltflächen
- Register „Konfiguration“
- Register „Protokoll“

Mögliche Aktionsschaltflächen

Sichern

Die Änderungen werden gesichert.

Verwerfen

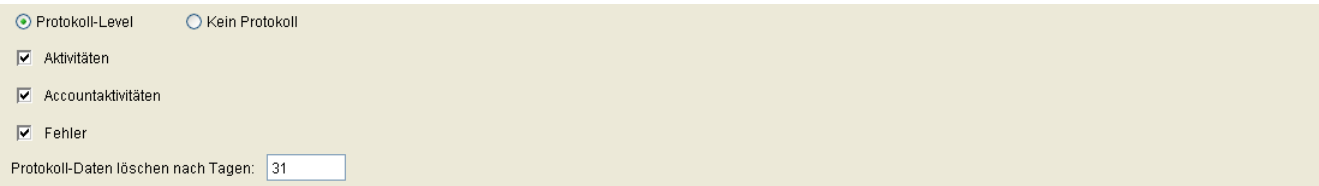
Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.5.1.1 Register „Konfiguration“

Aufruf: Hauptmenü > Administration > Protokoll-Daten > Aktivitäten- und Fehlerprotokoll > Register „Konfiguration“



Protokoll-Level

Schalter zum Aktivieren der Protokollierung.

Kein Protokoll

Schalter zum Deaktivieren der Protokollierung.

Aktivitäten

Im Aktivitäten-Protokoll werden alle Aktivitäten des DLS protokolliert.

Accountaktivitäten

Im Accountaktivitäten-Protokoll werden alle Aktivitäten des Accounts protokolliert.

Fehler

Das Fehler-Protokoll zeichnet fehlgeschlagene Aktionen und interne Fehler auf, wie z.B. Lizenzverletzungen oder SQL-Datenbankfehler.

Protokoll-Daten löschen nach Tagen:

Anzahl der Tage, die protokollierte Ereignisse gespeichert bleiben sollen, bevor sie automatisch gelöscht werden.

Wertebereich: 1 ... 365 Tage.

Standard: 31

6.5.1.2 Register „Protokoll“

Aufruf: Hauptmenü > Administration > Protokoll-Daten > Aktivitäten- und Fehlerprotokoll > Register „Protokoll“

Protokoll-Level

Aktivitäten

Im Aktivitäten-Protokoll werden alle Aktivitäten des DLS protokolliert.

Accountaktivitäten

Im Accountaktivitäten-Protokoll werden alle Aktivitäten des Accounts protokolliert.

Fehler

Das Fehler-Protokoll zeichnet fehlgeschlagene Aktionen und interne Fehler auf, wie z.B. Lizenzverletzungen oder SQL-Datenbankfehler.

Datum:

Zeitbereich, für den die Protokolldaten angezeigt werden sollen (Kalender siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

Protokoll

Ausgabe der Protokoll-Daten starten. Die gefilterten Daten werden in einem separaten Browser-Fenster angezeigt.

6.5.2 Audit- und Security Log Dateien

Diese Funktion wird abhängig von den Rollen und Rechten des Accounts in der Benutzeroberfläche angeboten.

Aufruf: Hauptmenü > Administration > Server Konfiguration > Protokoll-Daten > Audit- und Security Log Dateien

Dieser Bereich besteht aus folgenden Inhalten:

- Mögliche Aktionsschaltflächen
- Register „Konfiguration“
- Register „Protokoll“

Mögliche Aktionsschaltflächen

Verwerfen

Verwirft die eingetragenen Änderungen. Nicht anwendbar für das Register „Protokoll“.

Sichern

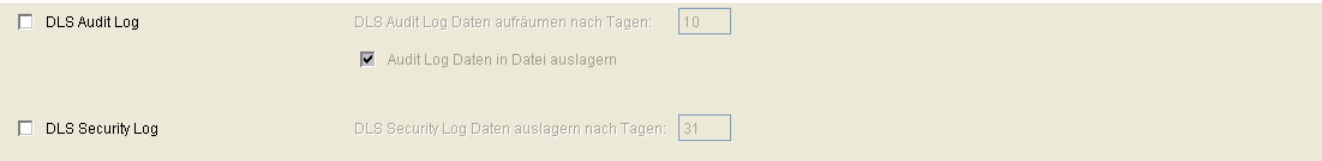
Die Änderungen werden gesichert. Nicht anwendbar für das Register „Protokoll“.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.5.2.1 Register „Konfiguration“

Aufruf: Hauptmenü > Administration > Protokoll-Daten > Audit- und Security Log Dateien > Register „Konfiguration“



DLS Audit Log

Wenn aktiv, werden alle Aktivitäten protokolliert, die durch einen Account angestoßen wurden.

DLS Audit Log Daten aufräumen nach Tagen

Anzahl der Tage bis zum automatischen Löschen bzw. Auslagern der Protokolldaten in eine Datei.

Wertebereich: **1** ... **365**

Audit Log Daten in Datei auslagern

Wenn aktiv, werden die Audit-Protokolldaten nach der in **Audit Log Daten aufräumen nach Tagen** eingestellten Zeit in eine Datei ausgelagert, andernfalls werden sie gelöscht.

DLS Security Log

Wenn aktiv, werden alle Security-relevanten Aktivitäten protokolliert.

DLS Security Log Daten auslagern nach Tagen

Anzahl der Tage bis zum automatischen Auslagern der Security-Protokolldaten in eine Datei

Wertebereich: **1** ... **365**

6.5.2.2 Register „Protokoll“

Aufruf: Hauptmenü > Administration > Protokoll-Daten > Audit- und Security Log Dateien > Register „Protokoll“

Datum

Protokolldaten, die im angegebenen Zeitraum angelegt wurden, werden ausgegeben.

Audit Log

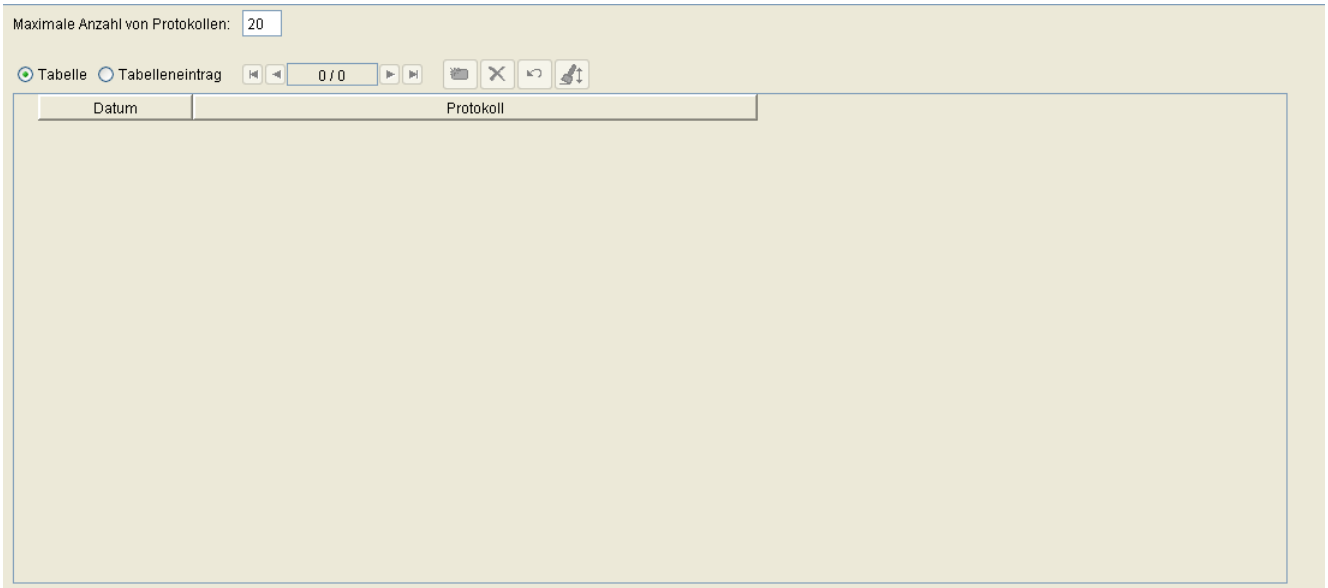
Über diesen Button wird die Ausgabe der DLS Audit Log-Daten gestartet.

Security Log

Über diesen Button wird die Ausgabe der DLS Security Log-Daten gestartet.

6.5.3 P&P Import Protokolle

Aufruf: Hauptmenü > Administration > Protokoll-Daten > P&P Import Protokolle



Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

> ***HINWEIS:*** Die Ansicht **Objekt** ist nur pro Mandant verfügbar. Daher werden bei der Option **ALL** auch keine Ergebnisse angezeigt.

Maximale Anzahl von Protokollen:

Maximale Anzahl von Protokollen, die beim Import von Plug&Play-Daten angelegt werden.

Wertebereich: **1** ... **40**.

Datum

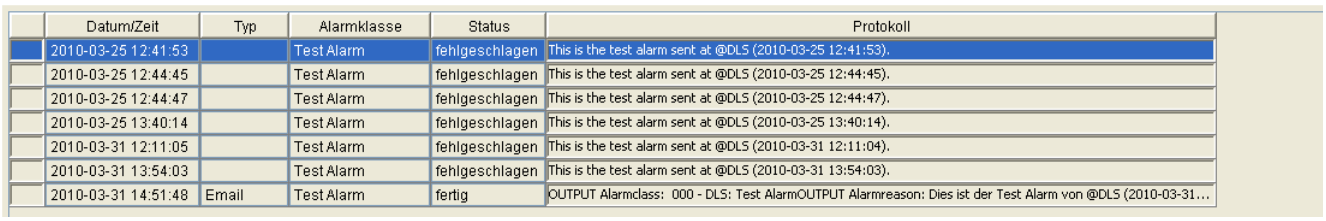
Zeitpunkt des Imports von P&P-Daten.

Protokoll

Protokoll des Imports von P&P Daten.

6.5.4 Alarm Protokoll

Aufruf: Hauptmenü > Administration > Protokoll-Daten > Alarm Protokoll



Datum/Zeit	Typ	Alarmklasse	Status	Protokoll
2010-03-25 12:41:53		Test Alarm	fehlgeschlagen	This is the test alarm sent at @DLS (2010-03-25 12:41:53).
2010-03-25 12:44:45		Test Alarm	fehlgeschlagen	This is the test alarm sent at @DLS (2010-03-25 12:44:45).
2010-03-25 12:44:47		Test Alarm	fehlgeschlagen	This is the test alarm sent at @DLS (2010-03-25 12:44:47).
2010-03-25 13:40:14		Test Alarm	fehlgeschlagen	This is the test alarm sent at @DLS (2010-03-25 13:40:14).
2010-03-31 12:11:05		Test Alarm	fehlgeschlagen	This is the test alarm sent at @DLS (2010-03-31 12:11:04).
2010-03-31 13:54:03		Test Alarm	fehlgeschlagen	This is the test alarm sent at @DLS (2010-03-31 13:54:03).
2010-03-31 14:51:48	Email	Test Alarm	fertig	OUTPUT Alarmclass: 000 - DLS: Test AlarmOUTPUT Alarmreason: Dies ist der Test Alarm von @DLS (2010-03-31…

Datum/Zeit

Datum und Uhrzeit, als die Aktion gestartet wurde.

Alarmklasse

Klasse des Alarms.

Typ

Alarmtyp.

Status

Status der Aktion.

Mögliche Optionen:

- **läuft**
- **offen**
- **fertig**
- **fehlgeschlagen**
- **Zeit überschritten**

Protokoll

Protokoll der Aktionsausführung.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.5.5 Alarm List

Aufruf: Hauptmenü > Administration > Protokoll-Daten > Alarm List

DLS zeigt eine Liste mit den in der DLS-Datenbank gespeicherten DLS-Alarmen an. Wenn eine Alarmbedingung auftritt (Protokollereignis), wird ein neuer Eintrag zur Datenbank hinzugefügt.

Datum/Zeit

Datum und Uhrzeit, als die Aktion gestartet wurde.

Alarmklasse

Klasse des Alarms.

Status

Status der Aktion.

Mögliche Optionen:

- **aktiv**

  Der Status bleibt aktiv, solange die Alarmbedingung existiert.

- **bestätigt**

  Der Status wird bestätigt, sobald die Alarmbedingung nicht mehr existiert.

Protokoll

Protokoll der Aktionsausführung.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Löschen

Wird verwendet, um einen Alarm aus der Liste zu löschen. DLS bestätigt den Alarm und entfernt ihn anschließend aus der Datenbank.

Alarm bestätigen

Wird verwendet, um den Status eines Alarms von „aktiv“ auf „bestätigt“ zu ändern.

Der DLS aktualisiert den Alarmstatus in der Datenbank und sendet einen Bestätigungs-Trap für diesen Alarm in den konfigurierten SNMP-Zielen.

Wenn ein Alarm mehr als einmal ausgelöst (und angezeigt wird) und Sie die Option „Alarm bestätigen“ verwenden, sollte der Alarmstatus in allen Zeilen von „aktiv“ auf „bestätigt“ wechseln.

Aktualisieren

Aktualisiert den Inhalt der Alarmliste.

6.6 Alarm Konfiguration

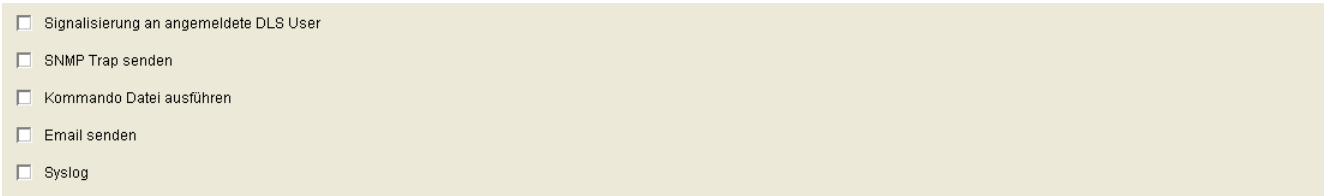
Aufruf: Hauptmenü > Administration > Alarm Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Alarmklassen“
- Register „Signalisierung“
- Register „SNMP“
- Register „Kommando Datei“
- Register „Email“
- Register „Syslog“
- Register „Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten



Signalisierung an angemeldete DLS User

Bei aktiviertem Schalter werden angemeldete Benutzer bei einem Alarm benachrichtigt, abhängig von den individuellen Einstellungen im Register „Alarmklassen“. Hierfür müssen die DLS-Benutzer im Register „Signalisierung“ für die Signalisierung ausgewählt werden. Die Alarm-Signalisierung wird in der Titelzeile des DLS-Fensters angezeigt.

SNMP Trap senden

Bei aktiviertem Schalter wird, abhängig von den individuellen Einstellungen im Register „SNMP“, ein SNMP-Trap zu dem im Register „Alarmklassen“ festgelegten SNMP-Empfänger versendet.

Kommando Datei ausführen

Bei aktiviertem Schalter wird, abhängig von den individuellen Einstellungen im Register „Kommando Datei“, die im Register „Alarmklassen“ festgelegte Kommando-Datei ausgeführt.

Email senden

Bei aktiviertem Schalter wird, abhängig von den individuellen Einstellungen im Register „Email“, eine Email mit den im Register „Alarmklassen“ festgelegten Daten versendet.

Syslog

Bei aktiviertem Schalter wird, abhängig von den individuellen Einstellungen im Register „Alarmklassen“, ein Eintrag in die Systemprotokolldatei gemacht.

Mögliche Aktionsschaltflächen

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

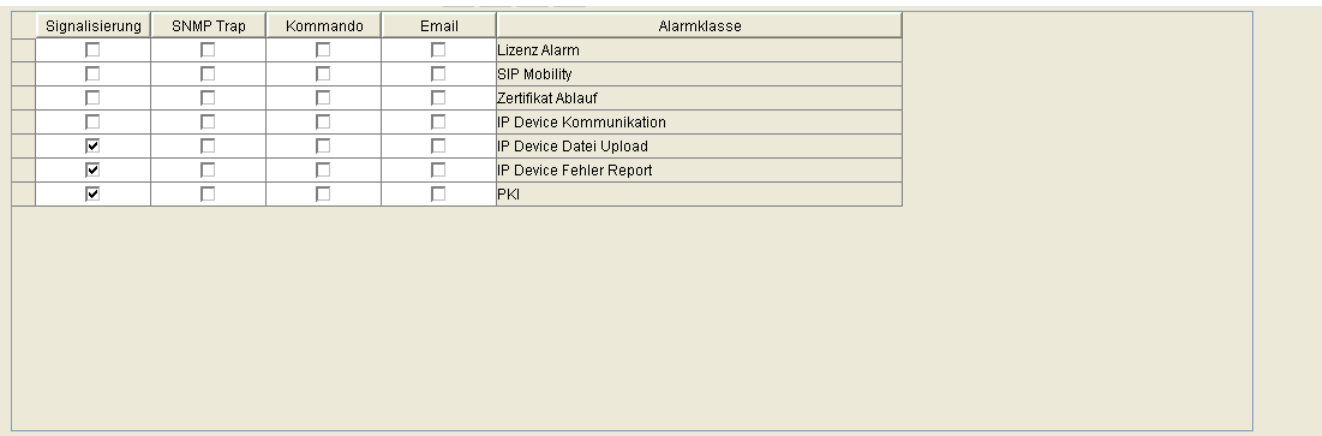
Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.6.1 Register „Alarmklassen“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „Alarmklassen“

Hier werden die Aktionen für spezifische Alarmklassen ausgewählt. Die Zusammensetzung dieser Liste hängt von den Start-Einstellungen des DLS ab und kann nicht modifiziert werden. Die möglichen Aktionen sind Signalisierung, Kommando Datei ausführen, Email senden und SNMP-Trap senden. Ob die Aktionen allerdings tatsächlich ausgeführt werden, hängt von den Schaltern unter **Allgemeine Daten** ab. Wenn z.B. **Email senden** unter **Allgemeine Daten** deaktiviert ist, werden die individuellen Einstellungen in der Tabelle der Alarmklassen nicht mehr berücksichtigt.



Index

Index für die auszulösende Alarm-Aktion (Signalisierung, Kommando Datei, SNMP Trap oder Email).

Signalisierung

Ist dieser Schalter und der Schalter **Signalisierung an angemeldete DLS User** im Bereich **Allgemeine Daten** aktiviert, werden die im Register „Signalisierung“ aufgelisteten DLS-Benutzer gemäß dieser Alarmklasse benachrichtigt.

SNMP Trap

Ist dieser Schalter sowie der Schalter **SNMP Trap senden** im Bereich **Allgemeine Daten** aktiviert, so wird der SNMP-Trap an den für diese Alarmklasse konfigurierten Empfänger geschickt.

Kommando Datei

Ist dieser Schalter sowie der Schalter **Kommando Datei ausführen** im Bereich **Allgemeine Daten** aktiviert, wird die konfigurierte Kommando-Datei für diese Alarmklasse ausgeführt.

Email

Bei aktiviertem Schalter wird, wenn **Email senden** im Bereich **Allgemeine Daten** aktiviert ist, die konfigurierte Email für diese Alarmklasse ausgeführt.

Alarmklasse

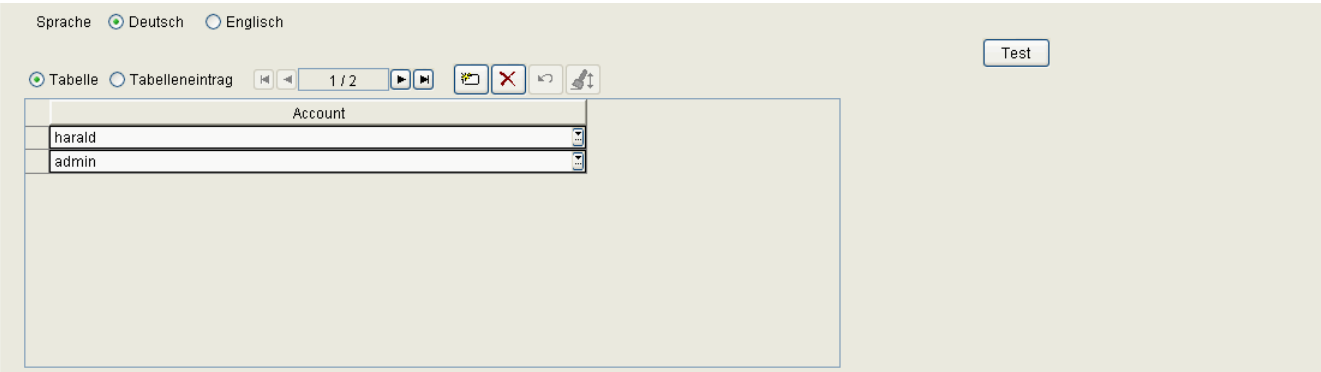
Alarmklassen bezeichnen bestimmte Funktionsbereiche des DLS, in denen bei Fehlern ein Alarm ausgelöst werden kann. Die Liste kann nicht verändert werden und hängt von den Einstellungen beim Startup des DLS ab.

Mögliche Werte:

- **DLS Service**
- **Lizenz Alarm**
- **SIP Mobility**
- **Zertifikat Ablauf**
- **DCMP**
- **DLS Cluster**
- **Element Manager Synchronisation**
- **Policy Alarm**
- **Ressourcen Alarm**
  Korrespondiert mit dem Schwellwert **Minimum freier Speicher** unter **Administration** > **File Server**.
- **IP Device Kommunikation**
- **IP Device Datei Upload**
- **IP Device Fehler Report**
- **PKI**

6.6.2 Register „Signalisierung“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „Signalisierung“



Sprache

Sprachauswahl für die Textausgabe der Signalisierung.

Mögliche Optionen:

- **Deutsch**
- **Englisch**

Account

Hier werden die DLS-Benutzer eingetragen, die bei den im Register „Alarmklassen“ ausgewählten Alarmen benachrichtigt werden sollen.

Test

Testet die Signalisierung. Das Ergebnis des Tests kann unter **Administration** > **Protokoll-Daten** > **Alarm Protokoll** überprüft werden.

6.6.3 Register „SNMP“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „SNMP“

Im Alarmfall wird ein SNMP Trap gesendet. Es wird nicht jede Art von Datenpaket unterstützt, insbesondere nicht die GET/SET-Abfragen. Der vom DLS erzeugt erzeugte Teilbaum der MIB kann aber von einem Trap-Receiver eingelesen und bearbeitet werden.

Der DLS nutzt folgenden MIB-Teil zum Generieren der Traps:

```
hiPathApplicationStatusChange NOTIFICATION-TYPE OBJECTS { hostname, appName,
appState, evtHistory-Date, evtHistoryDescr, hiPathTrapSeverity} STATUS current
DESCRIPTION "A hiPathApplicationStatusChange trap a status change of a HiPath enabled
application.    This trap is sent, if a process which is not of service type, causes
trouble. If the error state disappears there shall be a hiPathApplicationStatusChange
trap too."::= { hiPathTrapGroup 6 }
```

Die Parameter haben folgende Bedeutungen bzw. Werte:

`hostname`: Hostname des DLS-Servers.

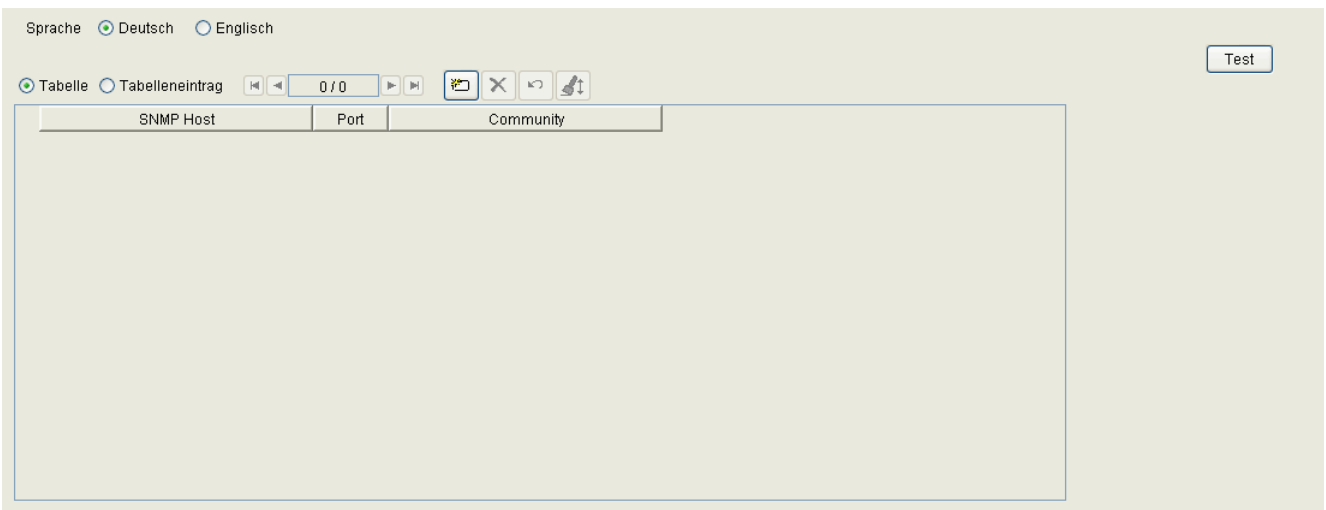
`appName`: „DLS“

`appState`: 3 (= Warnung)

`evtHistory-Date`: Datum des Auftretens des Traps.

`evtHistory-Descr`: Beschreibungstext des Traps (wie bei `createHiPathApplicationStatusChange()` mitgegeben).

`hiPathTrapSeverity`: 3 (= Warnung)



Sprache

Sprache des Beschreibungstextes des SNMP Traps.

Mögliche Optionen:

- **Deutsch**
- **Englisch**

Test

Sendet eine Test-SNMP-Trap. Das Ergebnis des Tests kann unter **Administration** > **Protokoll-Daten** > **Alarm Protokoll** überprüft werden.

SNMP Host

Name des SNMP-Servers (Manager).

Port

Port des SNMP-Servers (Manager).
Standard: **162**

Community

Community / Passwort des SNMP-Servers (Manager).

6.6.4 Register „Kommando Datei“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „Kommando Datei“

Sprache

Sprache des Textes der Alarm-Meldung.

Mögliche Optionen:

- **Deutsch**
- **Englisch**

Kommando Datei:

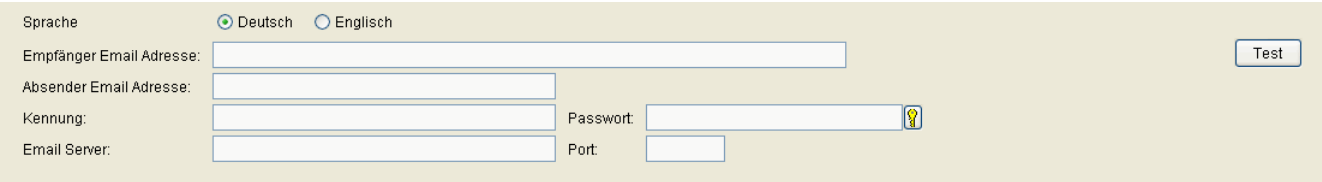
Pfad und Name der Kommandodatei, die ausgeführt wird, sobald ein Alarm ausgelöst wird. Nach der Installation des DLS referenzieren Pfad und Dateiname auf eine Musterdatei, die auch Regeln für die Kommandoerstellung enthält.

Test

Testet die Ausführung der Kommando-Datei. Das Ergebnis des Tests kann unter **Administration** > **Protokoll-Daten** > **Alarm Protokoll** überprüft werden.

6.6.5 Register „Email“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „Email“



Sprache

Sprache des Textes der Alarm-Meldung.

Mögliche Optionen:

- **Deutsch**
- **Englisch**

Empfänger Email Adresse:

Email-Adresse des Empfängers der Alarm-Mail.

Test

Testet das Absenden der Email mit den eingegebenen Account-Daten. Das Ergebnis des Tests kann unter **Administration** > **Protokoll-Daten** > **Alarm Protokoll** überprüft werden.

Absender Email Adresse:

Email-Adresse(n), die bei den gesendeten Emails als Absender-Adresse eingetragen werden soll. Es können eine oder mehrere Email Adressen getrennt durch ‘;’, ‘,’ oder ‘ (Leerzeichen)’ bis max. 255 Zeichen eingegeben werden.

Kennung:

Name des Email-Kontos.

Passwort:

Passwort für dieses Email-Konto.

Email Server:

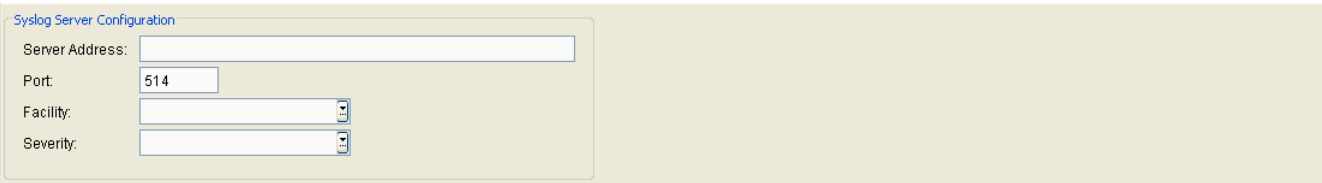
Name des SMTP-Servers, der zum Versenden der Emails verwendet werden soll.

Port:

Portnummer des SMTP-Servers. Wird kein Wert eingegeben, wird als Standard Port=25 verwendet.

6.6.6 Register „Syslog“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „Syslog“



Syslog Server Configuration

Server Address

Adresse des Syslog Servers

Port

Portnummer des Syslog Servers

Facility

Mögliche Optionen:

- **local0**
- **local1**
- **local2**
- **local3**
- **local4**
- **local5**
- **local6**
- **local7**

Severity

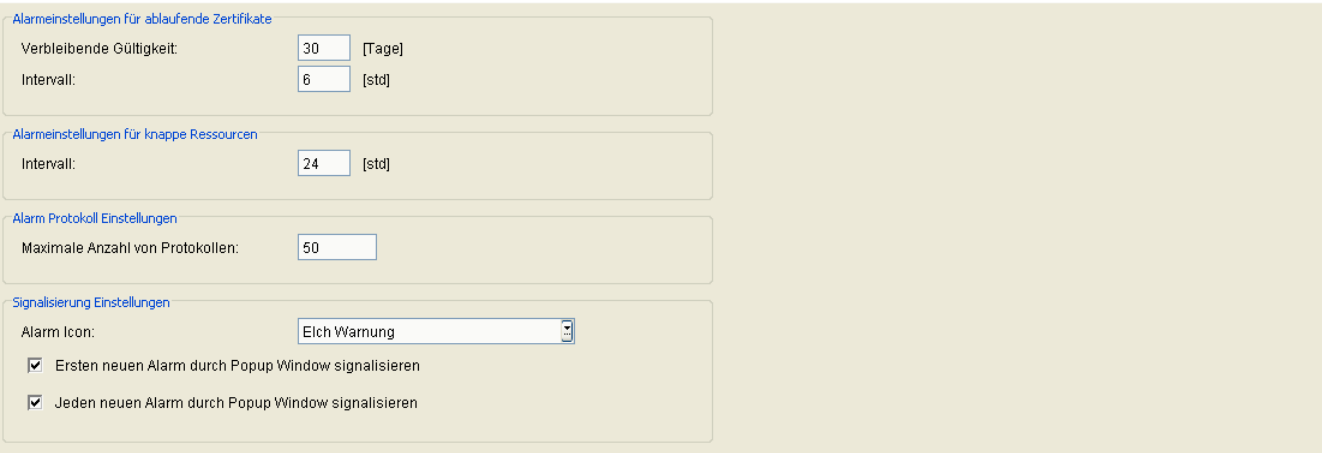
Einstellung des Trace-Levels

Mögliche Optionen:

- **emerg**
- **alert**
- **crit**
- **error**
- **warning**
- **notice**
- **info**
- **debug**
- **none**

6.6.7 Register „Einstellungen“

Aufruf: Hauptmenü > Administration > Alarm Konfiguration > Register „Einstellungen“



Alarmeinstellungen für ablaufende Zertifikate

Verbleibende Gültigkeit: [Tage]

Ein Alarm wird ausgegeben, wenn ein Zertifikat während dieses Zeitraums abläuft.

Wertebereich: **1** - **60**

Intervall: [Stunden]

Der noch verbleibende Gültigkeitszeitraum wird im hier eingestellten Zeitraum geprüft.

Wertebereich: **1** - **60**

Standardwert: **6**

Alarmeinstellungen für knappe Ressourcen

Intervall [std]

In dem hier angegeben Zeitintervall in Stunden wird die Verfügbarkeit von Ressourcen überprüft.

Wertebereich: **1** - **48**

Alarm Protokoll Einstellungen

Maximale Anzahl von Protokollen:

Maximale Anzahl von Zeilen im Protokoll.

Wertebereich: **1** - **100000**

Signalisierung Einstellungen

Alarm Icon:

Auswahlliste mit Symbolen, um DLS-Benutzers über noch offene Alarme zu informieren. Das Symbol wird in der Titelleiste des DLS-Fensters angezeigt.

Ersten neuen Alarm durch Popup Window signalisieren

Wenn aktiviert, wird der erste neue Alarm durch ein Popup-Fenster signalisiert, wenn zuvor alle vorangegangenen Alarme geschlossen wurden.

Jeden neuen Alarm durch Popup Window signalisieren

Wenn aktiviert, wird jeder neue Alarm durch ein Popup Fenster signalisiert, falls nicht schon ein Popup Fenster geöffnet war.

6.7 Backup / Restore

Aufruf: Hauptmenü > Administration > Backup / Restore

HINWEIS: Diese Funktion steht in der onboard-Variante des DLS auf OpenScape Voice nicht zur Verfügung. Die Sicherung der DLS-Daten wird hier von der umfassenden Backup/Restore-Funktion von OpenScape Voice übernommen.

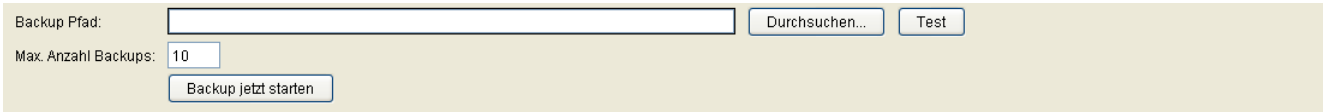
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Backup“
- Register „Restore“
- Register „Protokoll“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Weitere Informationen zum Thema Backup / Restore finden Sie im Abschnitt 15.8.1, “Automatisierte Datensicherungen”.

Allgemeine Daten



Backup Pfad:

Pfadangabe für die Sicherung eines Backups auf dem DLS-Server. Wenn der DLS eine entfernte Datenbank für seine Daten nutzt, ist hier der Pfad zu einem Verzeichnis auf dem Datenbankserver anzugeben. Dieses Verzeichnis muss vom DLS-Server aus erreichbar sein. Dies muss in einer Form geschehen, in der dieser Pfad auch lokal am Datenbankserver nutzbar ist, also z. B.
`\\<IP-Adresse DB Server>\C$\<Backup Pfad am DB Server auf Laufwerk C>`

Durchsuchen...

Bei Klick auf die Schaltfläche wird ein Dialogfenster angezeigt, mit dem ein vorhandenes Backup-Verzeichnis ausgewählt werden kann. In ein Unterverzeichnis eines Verzeichnisses gelangen Sie mit einem Doppelklick auf den Verzeichnisnamen. Auf die nächsthöhere Verzeichnisebene gelangen Sie mit einem Doppelklick auf „..\“. Um ein Verzeichnis auszuwählen, markieren Sie es per Einfachklick und klicken anschließend auf **Öffnen**.

Test

Bei Klick auf die Schaltfläche wird geprüft, ob der angegebene Pfad gültig, d. h. erreichbar ist.

Max. Anzahl Backups:

Anzahl verwalteter Backup-Files. Beim Anlegen einer neuen Backup-Datei wird die jeweils älteste Datei gelöscht.

Wertebereich: **1** ... **99**.

Backup jetzt starten

Mit der Schaltfläche wird unabhängig von der automatisierten, periodischen Backup-Erstellung sofort ein Backup durchgeführt. Dabei wird nicht der in der Datenbank gespeicherte Backup-Pfad verwendet, sondern der aktuelle (evtl. geänderte und noch nicht gesicherte) Backup-Pfad, wie er aktuell in der Maske angezeigt wird. So können Sie ein einzelnes Backup an anderer Stelle speichern, als dies für den periodischen Backup der Fall ist.

> ***HINWEIS:*** Bei jedem Klick auf die Backup-Schaltfläche variiert die Größe der Backup-Datei. Diese Variation ist bedingt durch die .trn-Dateien.

HINWEIS: .trn-Dateien sind Logdateien für Backup-Transaktionen. Sie sind dann nützlich, wenn das Restore-Transaktionsmodell der Datenbank entweder voll ist oder als Massenlog verwendet wird. Das Backup der Transaktionslogs unterscheidet sich vom Backup der Datenbank. Transaktionslogs enthalten nicht nur alle Transaktions-SQL-Befehlsanforderungen an die Datenbank, sondern auch die Differenz der Daten (also Tabellen, Indizes).

HINWEIS: Da die Transaktionslogs auch Datenänderungen enthalten, können auch in kürzeren Zeiträumen größere Unterschiede bei der Größe von Transaktionslog-Backup-Dateien auftreten. Außerdem werden beim Backup eines Transaktionslogs die gesicherten Transaktionslog-Einträge gelöscht. Wenn Sie also nach einem Transaktionslog-Backup ein erneutes Backup anstossen, ist die Größe der zweiten Backup-Datei logischerweise viel kleiner als die der vorherigen Backup-Datei.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.7.1 Register „Backup“

Aufruf: Hauptmenü > Administration > Backup / Restore > Register „Backup“

Siehe hierzu Abschnitt 15.8.1.1, “Automatisches Backup einrichten”.

Tägliche Backups ausführen

Schalter zum Aktivieren einer täglichen Sicherung.

Nächster Backup am:

Zeitpunkt (Datum und Uhrzeit) des nächsten vorgesehenen Backups (Kalender siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

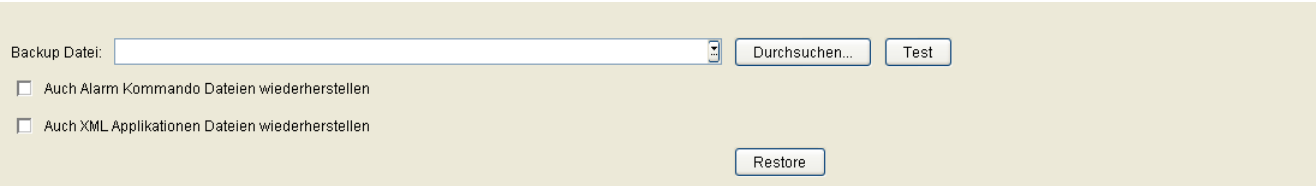
Tägliche Backups nur ausführen am:

Wenn **Tägliche Backups ausführen** aktiviert ist, können hier die Sicherungen auf bestimmte Wochentage eingeschränkt werden.

6.7.2 Register „Restore“

Aufruf: Hauptmenü > Administration > Backup / Restore > Register „Restore“

Siehe hierzu Abschnitt 15.8.1.2, “Backup wiederherstellen”.



Backup Datei:

Angabe von Pfad- und Dateiname für die Wiederherstellung eines Backups auf dem DLS-Server. Wurden bereits Backups erfolgreich erstellt, können diese über die Auswahlliste eingetragen werden.

Auch Alarm Kommando Dateien wiederherstellen:

Ist der Schalter aktiv, werden auch die Alarm Kommando Dateien wiederhergestellt.

Auch XML Applikationen Dateien wiederherstellen:

Ist der Schalter aktiv, werden auch die kundenindividuellen XML Applikationen Dateien in das Verzeichnis `<Installation directory>/XMLApplications/data/custom` wiederhergestellt.

Ist der Schalter nicht aktiv, werden die kundenindividuellen XML Applikationen Dateien in das Verzeichnis `<Installation directory>/XMLApplications/data/custom_old` kopiert.

Siehe auch Abschnitt 16.15, “Datenstrukturen für DLS-eigene XML-Applikationen”

Durchsuchen...

Bei Klick auf die Schaltfläche wird ein Dialogfenster angezeigt, mit dem eine bereits vorhandene Backup-Datei ausgewählt werden kann. Pfad- und Dateiname werden bei **Backup Datei** eingetragen.

> ***HINWEIS:*** Wenn Sie in einer Multi-Node-Umgebung auf diese Schaltfläche klicken und einen Backup-Pfad suchen, der sich lokal auf Knoten 1 oder Knoten 2 befindet, wird der ausgewählte Pfad mit der IP-Adresse der 1. Ethernet-Schnittstelle des DLS-Servers verbunden.
> Wenn die 1. Schnittstelle zufällig die Schnittstelle des externen (oder Frontend-)Netzwerks ist, schlägt die Wiederherstellung der Datenbank fehl, weil der DLS über diese Schnittstelle keine Verbindung zum SQL-Server herstellen kann.

HINWEIS: Der DLS kann eine Verbindung zum SQL-Server nur über die interne (Backend-)Netzwerkschnittstelle herstellen; diese kann jedoch nicht explizit angegeben werden, wenn der Pfad über die Schaltfläche **Browse... (Durchsuchen...)** ausgewählt wird.

Test

Bei Klick auf die Schaltfläche wird geprüft, ob die angegebene Backup-Datei gültig, d. h. erreichbar ist.

Restore

Mit dieser Schaltfläche wird ein Restore durchgeführt. In einem Dialogfenster wird abgefragt, ob Plug& Play nach dem Restore ausgeschaltet werden soll oder nicht. Wenn Plug&Play ausgeschaltet wurde, kann über **Administration** > **Server Konfiguration** > **P&P Einstellungen** > **Plug&Play eingeschaltet** wieder eingeschaltet werden, nachdem sichergestellt wurde, dass alle IP Devices in der DLS-Datenbank registriert sind.

Dabei wird nicht die in der Datenbank gespeicherte Backup-Datei verwendet, sondern die aktuelle (evtl. geänderte und noch nicht gesicherte) Backup-Datei, wie sie in der Maske angezeigt wird.

HINWEIS: Bei aktiver Datenbank-Spiegelung (siehe Abschnitt 4.6, “Spiegelung der SQL-Datenbank aufsetzen”) ist kein Restore eines Backups möglich.

HINWEIS: Einige Serverkonfigurationen werden nie zurückgeladen, um den Betrieb des DLS nach einem Restore sicherzustellen, z.B
- die Basiskonfiguration
- die Lizenzeinstellungen.

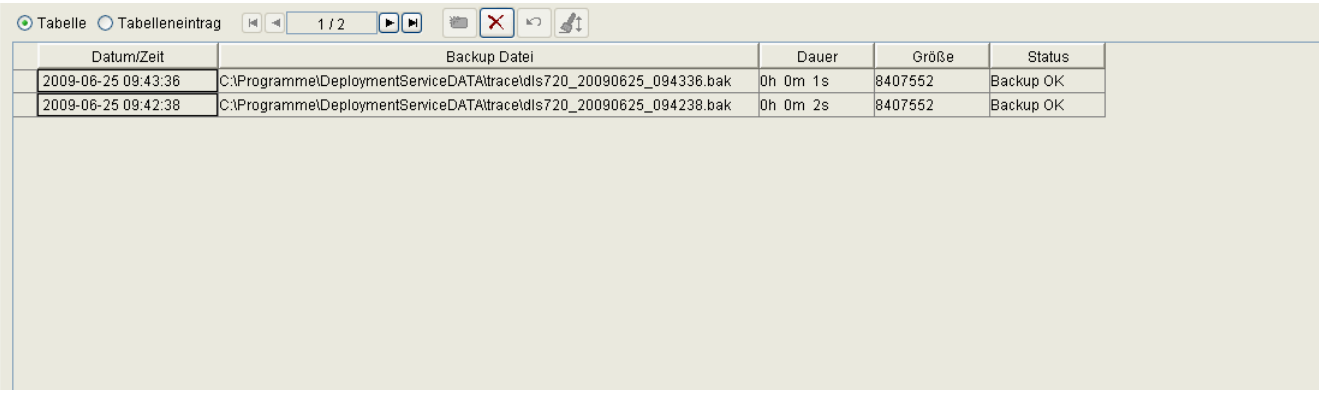
.

HINWEIS: Während eines Restores werden werden **alle** Accounts der DLS-Datenbank kurzzeitig von der Datenbank getrennt, da der Restore-Vorgang einen exklusiven Zugriff auf die Datenbank voraussetzt. Die Accounts müssen sich also erneut anmelden.

6.7.3 Register „Protokoll“

Aufruf: Hauptmenü > Administration > Backup / Restore > Register „Protokoll“

Siehe hierzu Abschnitt 15.8.1.3, “Sicherungen überwachen”.



Datum/Zeit

Zeitpunkt des Backups.

Backup Datei

Dateiname der Backup-Datei.

Dauer

Dauer des Backupvorgangs in Stunden, Minuten und Sekunden.

Größe

Größe der Backup-Datei in Bytes.

Status

Status der Sicherung/Rücksicherung.

Mögliche Werte:

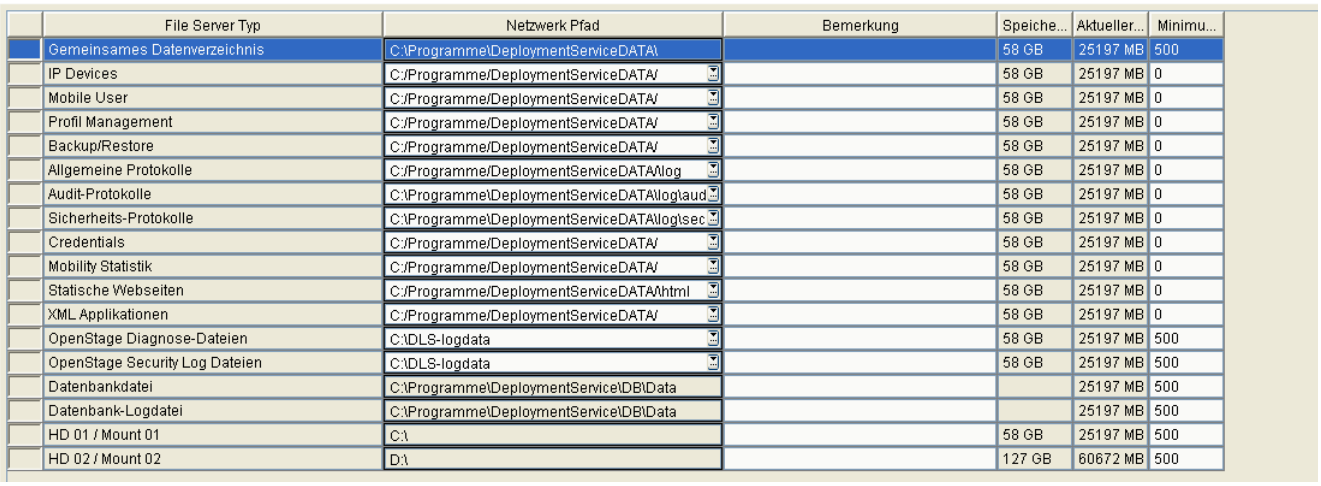
- **Backup OK**
- **Backup fehlgeschlagen**

- **gelöscht**
- **Restore OK**
- **Restore fehlgeschlagen**

6.8 File Server

Aufruf: Hauptmenü > Administration > File Server

Mit diesem Menüpunkt können Netzlaufwerke oder lokale Verzeichnisse zur Speicherung von DLS-Daten voreingestellt werden.



File Server Typ	Netzwerk Pfad	Bemerkung	Speiche...	Aktueller...	Minimu...
Gemeinsames Datenverzeichnis	C:\Programme\DeploymentServiceDATA\		58 GB	25197 MB	500
IP Devices	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
Mobile User	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
Profil Management	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
Backup/Restore	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
Allgemeine Protokolle	C:/Programme/DeploymentServiceDATA\log		58 GB	25197 MB	0
Audit-Protokolle	C:\Programme\DeploymentServiceDATA\log\aud		58 GB	25197 MB	0
Sicherheits-Protokolle	C:\Programme\DeploymentServiceDATA\log\sec		58 GB	25197 MB	0
Credentials	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
Mobility Statistik	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
Statische Webseiten	C:/Programme/DeploymentServiceDATA\html		58 GB	25197 MB	0
XML Applikationen	C:/Programme/DeploymentServiceDATA/		58 GB	25197 MB	0
OpenStage Diagnose-Dateien	C:\DLS-logdata		58 GB	25197 MB	500
OpenStage Security Log Dateien	C:\DLS-logdata		58 GB	25197 MB	500
Datenbankdatei	C:\Programme\DeploymentService\DB\Data			25197 MB	500
Datenbank-Logdatei	C:\Programme\DeploymentService\DB\Data			25197 MB	500
HD 01 / Mount 01	C:\		58 GB	25197 MB	500
HD 02 / Mount 02	D:\		127 GB	60672 MB	500

File Server Typ

Legt fest, welche DLS-Daten auf diesem File Server gespeichert werden sollen.

Mögliche Werte:

- **IP Devices**
- **Mobile User**
- **Profil Management**
- **Backup / Restore**
- **Protokolle**
- **Credentials**
- **Mobility Statistiken**
- **Statische Webseiten**
- **XML Applikationen**
- **Gemeinsames Datenverzeichnis**
  Dieser Netzwerkname wird während der Installation des DLS angegeben und kann hier nicht geändert werden.
- **OpenStage Diagnose Dateien**
- **OpenStage Security Log Dateien**

- **Datenbankdatei**
  Anzeige des Pfades, auf dem die DLS Datenbank gespeichert ist. Der Netzwerkname ist relativ zum SQL Server angegeben und kann hier nicht geändert werden. Nur verfügbar bei Datenbanktypen mit Microsoft SQL Server.
- **Datenbank Log Datei**
  Anzeige des Pfades auf dem das Transaction Log der DLS Datenbank gespeichert ist. Der Netzwerkname ist relativ zum SQL Server angegeben und kann hier nicht geändert werden. Nur verfügbar bei Datenbanktypen mit Microsoft SQL Server.
- **DLS Audit Log Dateien**
- **DLS Security Log Dateien**
- **HD 01 / Mount 01**
  Zeigt entweder die benötigten Laufwerke mit Systemdaten (bei Linux-Systemen), oder alle verfügbaren oder gemounteten Laufwerke (bei Windows-Systemen). Der Netzlaufwerkpfad kann mit dieser Maske nicht geändert werden.
- **...**
- **HD 20 / Mount 20**
  Zeigt entweder die benötigten Laufwerke mit Systemdaten bei Linux-Systemen, oder alle verfügbaren oder gemounteten Laufwerke bei Windows-Systemen. Der Netzlaufwerkpfad kann mit dieser Maske nicht geändert werden.

Netzwerk Pfad

Netzwerk-Pfad oder lokales Verzeichnis zur Speicherung der DLS-Daten.
Beispiel: `\\MyFileServer\DlsFiles\Protocols`

Bemerkung

Feld für allgemeine Informationen.

Speicherkapazität

Anzeige der gesamten Speicherkapazität dieses Netzlaufwerks in Gigabyte.

Aktueller freier Speicher

Anzeige des noch verfügbaren Speicherplatzes diese Netzlaufwerks in Megabyte. Ist dieser Wert kleiner als **Minimum freier Speicher**, wird ein gelber Rand um dieses Feld eingeblendet.

Minimum freier Speicher

Der verbleibende freie Speicher in Megabyte kann hier definiert werden. Fällt der Wert **Aktueller freier Speicher** unter diesen Wert, wird ein Alarm entsprechend der Alarmkonfiguration (siehe Abschnitt 6.6, “Alarm Konfiguration”) abgesetzt.

Wertebereich: **0** ... **15000**

0 = keine Prüfung

Erfassungszeit

Datum und Uhrzeit der Erfassung der zusätzlichen Informationen über **Speicherkapazität [GB]** und **Freier Speicher [MB]**. Diese Werte werden einmal wöchentlich gespeichert; die Einträge können nicht gelöscht werden.

Nur verfügbar in der Objekt-Darstellung.

Speicherkapazität [GB]

Anzeige der Speicherkapazität des Netzlaufwerkes zur **Erfassungszeit**.

Nur verfügbar in der Objekt-Darstellung. Der Wert wird einmal pro Woche gespeichert.

Freier Speicher [MB]

Anzeige des freien Speichers des Netzlaufwerkes zur **Erfassungszeit**.

Nur verfügbar in der Objekt-Darstellung. Der Wert wird einmal pro Woche gespeichert.

6.9 Workpoint Interface Konfiguration

Aufruf: Hauptmenü > Administration > Workpoint Interface Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Mögliche Aktionsschaltflächen
- Register „Secure Modus“
- Register „DCMP“
- Register „HTTP-Proxy“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Aktualisieren

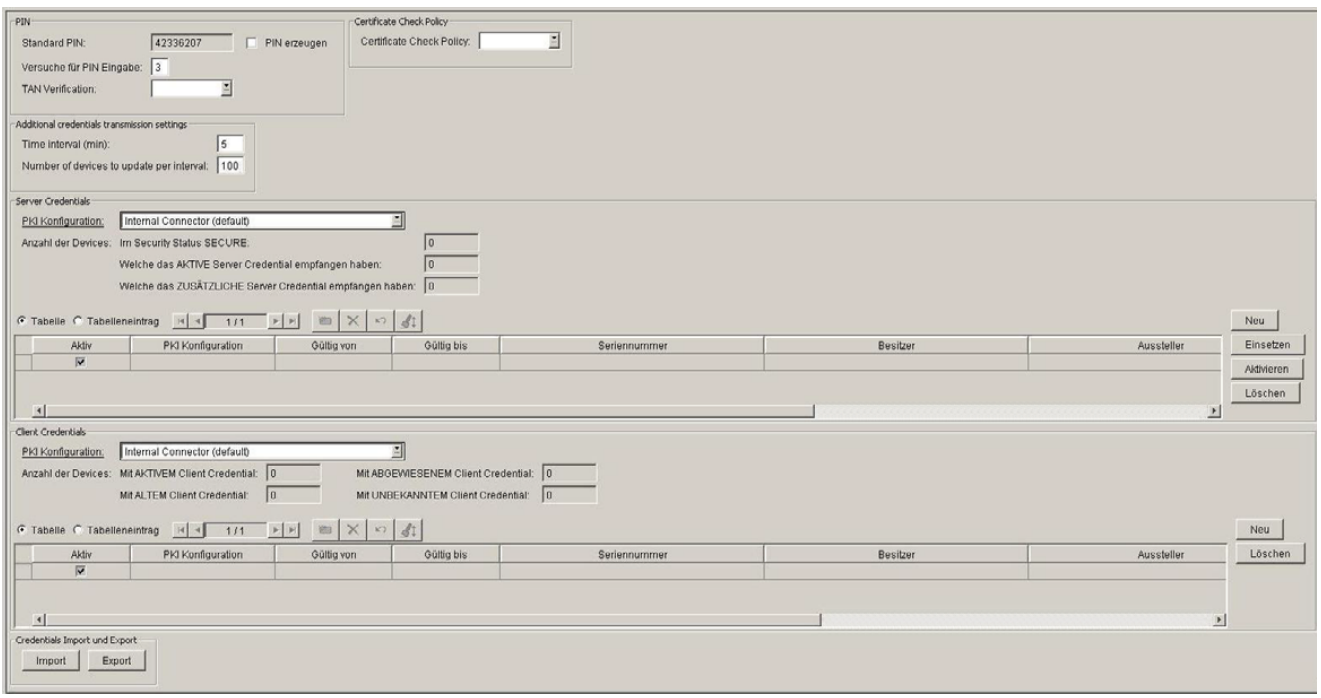
Aktualisiert den Inhalt der betroffenen Seite.

6.9.1 Register „Secure Modus“

Aufruf: Hauptmenü > Administration > Workpoint Interface Konfiguration > Register „Secure Modus“

HINWEIS: Für den reibungslosen Betrieb des Secure Mode ist es notwendig, dass Datum und Uhrzeit des DLS und des Workpoints übereinstimmen.Der Secure Modus steht bislang nur bei OpenStage-Telefonen zur Verfügung.

HINWEIS: Ein Factory Reset mit gespeicherten Plug&Play Daten kann nicht im Secure Mode durchgeführt werden. Die betroffenen IP Devices müssen zuerst auf Default Mode zurückgesetzt werden.



PIN

Standard PIN:

Automatisch vom DLS erzeugte PIN, um eine verschlüsselte Übertragung der Server Credentials an das IP Device zu ermöglichen. Diese PIN wird von IP Devices mit PIN-Modus „Standard-PIN“ verwendet.

PIN erzeugen

Sobald man diesen Schalter aktiviert und anschließend die Aktionsschaltfläche **Sichern** betätigt, generiert der DLS eine neue Standard-PIN. Diese PIN oder wahlweise eine individuelle PIN werden am IP Device eingegeben, um die vom DLS gelieferten Server Credentials zu entschlüsseln. Diese PIN wird von IP Devices im Security-Status **Unsicher** benutzt.

Versuche für PIN Eingabe:

Legt die Anzahl der erlaubten Fehlversuche bei der PIN-Eingabe am IP Device fest.

TAN Verification:

die TAN (Target's Authentication Number, Authentifizierungsnummer des Ziels) besteht aus den letzten 3 Zeichen der PIN und wird vom Bereitstellungsdienst verwendet, um das Zielgerät im sicheren Modus zu authentifizieren.

Mögliche Optionen:

- **False**
- **True**

TAN Verification can only be performed if TAN is required. Wenn das IP Device eine TAN gesendet hat, die derzeitige Konfiguration jedoch keine TAN erfordert, kann die TAN nicht verifiziert werden.

Certificate Check Policy

Certificate Check Policy

Die Einstellung wird nur für Workpoints im Secure Modus verwendet.

Mögliche Optionen:

- **Trusted**
- **Voll**

Additional credentials transmission settings (Zusätzliche Einstellungen für die Credential-Übertragung)

Time interval (min)

Zeitintervall (in Minuten), in dem neue WPI-Credentials gesendet werden.

Number of devices to update per interval

Anzahl der Geräte, an die WPI-Credentials während des Zeitintervalls gesendet werden.

Server Credentials

PKI Konfiguration

Hier wird die PKI-Konfiguration für die Server-Credetnials eingestellt, die dann aktiviert werden kann. Siehe auch Abschnitt 6.2, “PKI”.

> ***HINWEIS:*** WPI-Credentials können nicht erstellt werden, wenn der PKI Connector den „Common Name“ oder „Subject Alternative Name“ über die MAC-Adresse definiert. Dies wird nicht unterstützt.

Anzahl der Devices:

Im Security Status SECURE:

Anzahl der Geräte, die sich im Security-Status SECURE befinden.

Welche das AKTIVE Server Credential empfangen haben:

Anzahl der Geräte, die das aktive Server-Credential empfangen haben.

Welche das ZUSÄTZLICHE Server Credential empfangen haben:

Anzahl der Geräte, die das zusätzliche Server-Credential empfangen haben.

Aktiv

Zeigt an, ob ein Server Credential aktiv oder inaktiv ist. Der DLS authentisiert sich gegenüber einem Gerät im Secure Modus immer mit dem aktiven Server Credential.

Es kann höchstens ein zusätzliches Server Credential geben, welches in Vorbereitung auf den Austausch des aktiven Server Credentials erzeugt wird.

PKI Konfiguration

Zeigt die aktive PKI-Konfiguration an.

Gültig ab

Gültigkeitsbeginn des Credentials.

Gültig bis

Ende der Gültigkeit des Credentials.

Seriennummer

Zugehörige CA-Zertifikats-Seriennummer.

Besitzer

Besitzer des Credentials.

Aussteller

Aussteller des Credentials.

Fingerprint (SHA-1)

Dieser Fingerabdruck (Hash-Wert) identifiziert das Credential eindeutig (auch über verschiedene DLS-Instanzen hinweg).

Der Fingerabdruck ist Teil des Namens der Export-Datei (siehe auch Feld **Export**).

Schlüsselalgorithmus

Schlüsselalgorithmus des Credentials.

Schlüssellänge

Schlüssellänge des Credentials.

Neu

Erzeugt ein zusätzliches (nicht aktives) Server Credential. Es kann höchstens ein zusätzliches Server Credential erzeugt werden.

Eine PKI-Konfiguration muss aktiviert und ausgewählt werden (ein interner Connector ist standardmäßig aktiviert). Wenn ein MS PKI Connector verwendet wird, muss die PKI-Konfiguration aktiviert sein. Nachdem die zu verwendende PKI-Konfiguration ausgewählt wurde, wird ein neuer Trust Anchor aus der Trust Anchor-Konfiguration importiert. Der DLS fordert ein neues Server-Zertifikat für seinen eigenen für die WPI-Kommunikation verwendeten TLS-Connector an.

Deploy

Stellt allen Endgeräten bereits im sicheren Status das zusätzliche Server Credential bereit.

Der neue Trust Anchor wird den WPI-Clients bereitgestellt; diese verwenden ihn zur Authentifizierung des DLS. Für jedes Endgerät im sicheren Status wird ein Job initiiert.

Aktivieren

Aktiviert das zusätzliche (inaktive) Server-Credential im DLS (so dass der TLS-Connector einen Neustart mit dem neuen zusätzlichen Credential ausführen kann). Nach Abschluss der Aktivierung verweigern alle Geräte, an die der zu diesem Credential gehörige Trust Anchor noch nicht gesendet wurde, DLS-Anfragen.

Löschen

Löscht das zusätzliche (nicht aktive) Server Credential.

Client credentials

PKI Konfiguration

Zeigt die PKI-Konfiguration der Client Credentials.

Anzahl der Devices:

Mit AKTIVEM Client Credential:

Anzahl der (sicheren) Geräte, die sich mit dem aktiven Client Credential ausweisen.

Mit ALTEM Client Credential:

Anzahl der (sicheren) Geräte, die sich mit einem alten Client Credential ausweisen.

Mit ABGEWIESENEM Client Credential:

Anzahl der (sicheren) Geräte, deren Client Credential abgewiesen wurde. Abgewiesen werden solche Credentials, die sich nicht in der Liste befinden.

Mit UNBEKANNTEM Client Credential:

Anzahl der (sicheren) Geräte, bei denen nicht bekannt ist, mit welchem Client Credential sie sich ausweisen.

Aktiv

Zeigt an, ob ein Client Credential aktiv oder veraltet ist.

Es gibt immer genau ein aktives Client Credential. Der DLS akzeptiert aber auch Geräte, die sich mit einem veralteten Client Credential authentisieren. In einem solchen Fall wird dem Gerät automatisch das aktuell aktive Client Credential zugeschickt. Beim nächsten Mal authentisiert sich das Gerät dann mit dem aktiven Client Credential.

PKI Konfiguration

Zeigt die aktive PKI-Konfiguration an.

Gültig ab

Gültigkeitsbeginn des Credentials.

Gültig bis

Ende der Gültigkeit des Credentials.

Seriennummer

Zugehörige CA-Zertifikats-Seriennummer.

Besitzer

Besitzer des Credentials.

Aussteller

Aussteller des Credentials.

Fingerprint (SHA-1)

Dieser Fingerabdruck (Hash-Wert) identifiziert das Credential eindeutig (auch über verschiedene DLS-Instanzen hinweg).

Der Fingerabdruck ist Teil des Namens der Export-Datei (siehe auch Feld **Export**).

Schlüsselalgorithmus

Schlüsselalgorithmus des Credentials.

Schlüssellänge

Schlüssellänge des Credentials.

Neu

Erzeugt ein neues Client Credential. Dieses ist automatisch aktiv, während das zuvor aktive Client Credential deaktiviert wird und damit als veraltet gilt. Nachdem ein neues Client Credential erzeugt ist, wird es an alle Geräte gesendet.

> ***HINWEIS:*** Die Schaltfläche **Neu** löst keine Bereitstellung auf allen Endgeräten aus. Endgeräten im sicheren Status werden neue Client Credentials zugeteilt, sobald sie DLS kontaktieren.

> ***WICHTIG:*** Wird die Verbindung des Telefons zum Netz nur kurz getrennt und sofort wiederhergestellt, kann es sein, dass der Job erfolgreich beendet wird. Wenn der Gültigkeitszeitraum für die Abarbeitung des Jobs (Standardwert: 300 Sek.) überschritten wird, wird der Job für das Senden der Credentials ungültig. In jedem Fall wird das Telefon mit neuen WPI-Zertifikaten bereitgestellt (siehe Abschnitt 7.5.4, “IP Device Konfiguration”)
> Auch wenn der Job manuell abgebrochen wird, erhält das Telefon dennoch das Zertifikat, wenn es aus irgendeinem anderen Grund eine Verbindung zum DLS herstellt (z. B. infolge eines Neustarts).

Löschen

Löscht alle inaktiven, d.h. alten, Client Credentials. Nach dem Löschen der alten Client Credentials akzeptiert der DLS keine Geräte mehr, die sich mit einem alten Client Credential ausweisen.

Credentials Import und Export

Import

Importiert Client- und Server-Credentials aus einer passwortgeschützten Datei. Durch den Import werden die bestehenden Credentials ersetzt.

HINWEIS: Bootstrapping ist mit importierten Credentials nicht möglich

Export

Exportiert Client- und Server-Credentials in eine passwortgeschützte Datei.

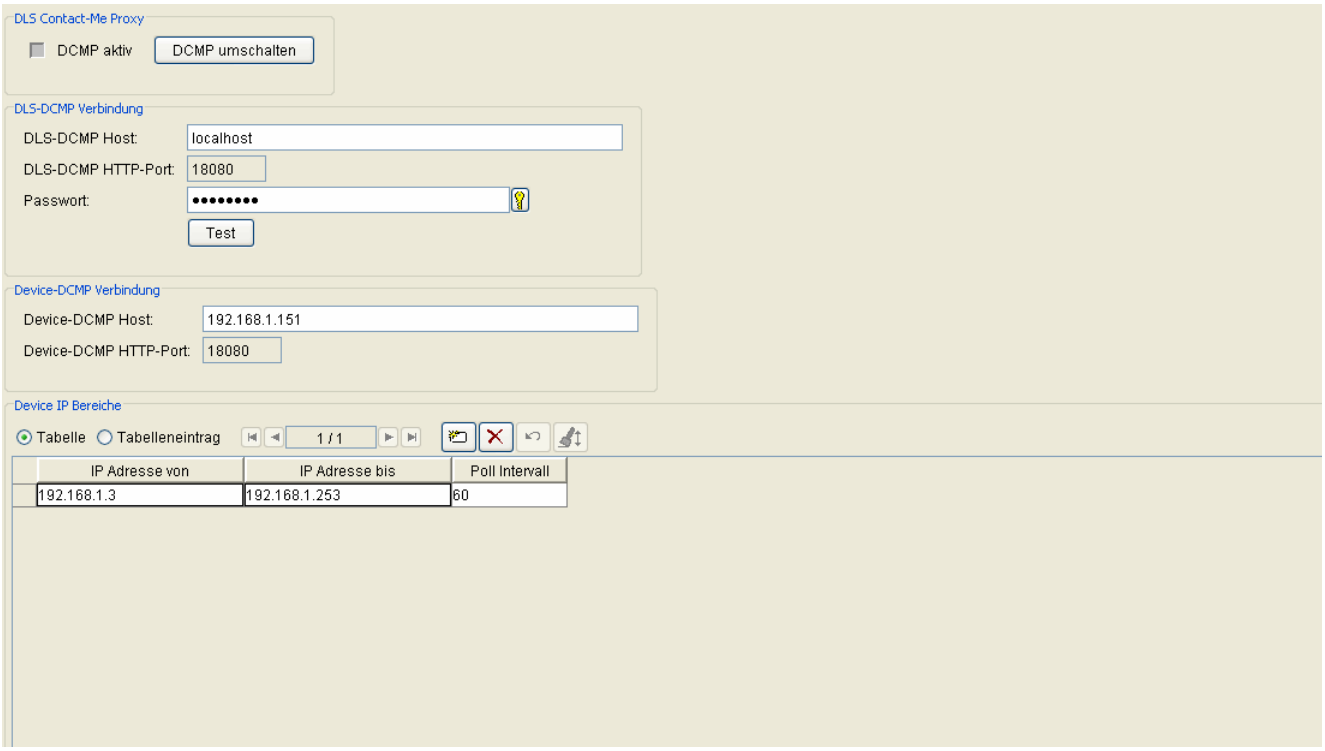
HINWEIS: Das Passwort ist nicht für die ZIP-Archiv-Datei gedacht, sondern für die in der ZIP-Archiv-Datei enthaltenen Dateien (WPI-Credentials).

HINWEIS: Die Import-Export-Funktionalität des WPI wird nur verwendet, um eine Verbindung zu Telefonen herzustellen, die sich bereits im sicheren Modus befinden

WICHTIG: Bei einem Upgrade von einer früheren DLS-Version, die noch nicht über die aktuelle PKI-Implementierung (für Credentials vor der Version V6.0) verfügte, sind die Felder leer, da diese Dateien zu dem früheren Zeitpunkt noch nicht vorhanden waren und daher leer bleiben. Diese Anzeigeinformationen gab es in älteren Versionen noch nicht. Deshalb ist das Feld PKI Konfiguration für ältere Credentials nicht relevant. Einige Anzeigeinformationen sind daher ebenfalls nicht relevant.

6.9.2 Register „DCMP“

Aufruf: Hauptmenü > Administration > Workpoint Interface Konfiguration > Register „DCMP“



DLS Contact-Me Proxy

DCMP aktiv

Aktiviert DCMP global. Wenn DCMP global deaktiviert ist, werden keine Devices über DCMP erreicht.

DCMP umschalten

Schaltet die DCMP Aktivierung um und erzeugt Jobs für betroffene Devices.

DLS-DCMP Verbindung

DLS-DCMP Host:

Hostname oder IP Adresse des DCMP-Servers. Der Host des DCMP-Servers muss für den DLS erreichbar sein.

DLS-DCMP HTTP-Port:

HTTP-Port des DCMP-Servers für die Verbindung zwischen DLS und DCMP.

Passwort:

Passwort für den Zugriff des DLS auf den DCMP-Server.

Test

Testet die Verbindung zwischen DLS und DCMP-Server mit den aktuell gespeicherten Werten für Host, Port und Passwort. Wenn Sie die Werte ändern, so Sie müssen diese vor dem Testen der DLS-Verbindung speichern.

Device-DCMP Verbindung

Device-DCMP Host:

Hostname oder IP Adresse des DCMP-Servers. Der DCMP Server Host muss für die DCMP-aktivierten Devices erreichbar sein. Benutzen Sie deshalb nicht „localhost“ oder „127.0.0.1“ als DCMP Server Host, wie es für die Verbindung DCMP-DLS möglich ist, wenn beide auf demsselben Host laufen.

Device-DCMP HTTP-Port

HTTP-Port des DCMP-Servers für die Verbindung zwischen Endgeräten und DCMP.

Device IP Bereiche

IP Adresse von:

Untergrenze des IP-Adressbereiches der IP Devices, die über DCMP administrierten werden.

IP Adresse bis:

Obergrenze des IP Adressbereiches der IP Devices, die über DCMP administrierten werden.

Poll Intervall:

Der Wert legt den Zeitabstand zwischen zwei Abfragen beim DCMP fest (in Minuten).

Der eingetragene Wert muss kleiner als der Wert für Abschnitt 7.4.6.2, “Zeitüberschreitung (sek):” sein.

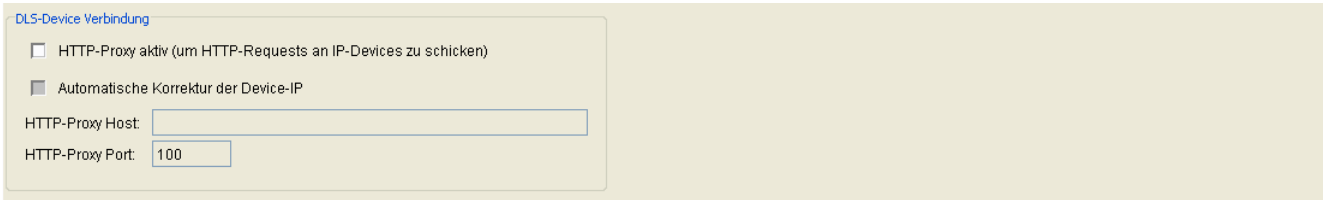
Mögliche Optionen:

0 - 1440, Standard: 60 Minuten

6.9.3 Register „HTTP-Proxy“

Aufruf: Hauptmenü > Administration > Workpoint Interface Konfiguration > Register „HTTP-Proxy“

Die in diesem Register gemachten Einstellungen sind notwendig, wenn die Endgeräte vom DLS aus nur über einen HTTP-Proxy erreicht werden können.



DLS-Device Verbindung

HTTP-Proxy aktiv (um HTTP-Requests an IP-Devices zu schicken)

Ist der Schalter aktiviert, wird ein HTTP-Proxy verwendet, um HTTP-Requests vom DLS an die IP Devices zu schicken.

Automatische Korrektur der Device-IP

Automatische Anpassung der IP-Adresse der Geräte an die Request-Addresse (nur falls HTTP-Proxy aktiv). Falls ein HTTP-Proxy verwendet wird, ist diese Option zunächst ausgeschaltet, um zu vermeiden, dass in den Requests an den DLS die IP-Adresse der Geräte durch die IP-Adresse des HTTP-Proxy ersetzt wird. Es wird empfohlen, diesen Schalter nicht zu aktivieren.

HTTP-Proxy Host

IP-Adresse oder DNS-Name des HTTP-Proxys, der verwendet werden soll, um HTTP-Requests vom DLS an die IP Devices zu schicken.

HTTP-Proxy Port

Port des HTTP-Proxy um HTTP-Requests vom DLS an IP Devices zu schicken.

6.10 Automatische SPE Konfiguration

Dieser Bereich ermöglicht dem Anwender die automatische Konfiguration von PKI-basierter Signaling and Payload Encryption (SPE). Dies ist insbesondere dann nützlich, wenn keine Kunden-PKI zur Verfügung steht.

Der DLS unterstützt das Anlegen und Verteilen von Zugangszertifikaten (SPE CA Zertifikat) an administrierte IP Devices (Gateways und Endgeräte). Beim Aktivieren dieses Zugangszertifikates wird für jedes administrierte Gateway ein SPE Zertifikat angelegt und verteilt.

Mittels Export und Import ist es möglich, CA-Zertifikate von einem DLS zum anderen umzuziehen.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „CA Administration“
- Register „Aussteller Administration“
- Register „Einstellungen“

Allgemeine Daten

PKI Konfiguration

Auswahl der PKI-Konfiguration.

Mögliche Optionen:

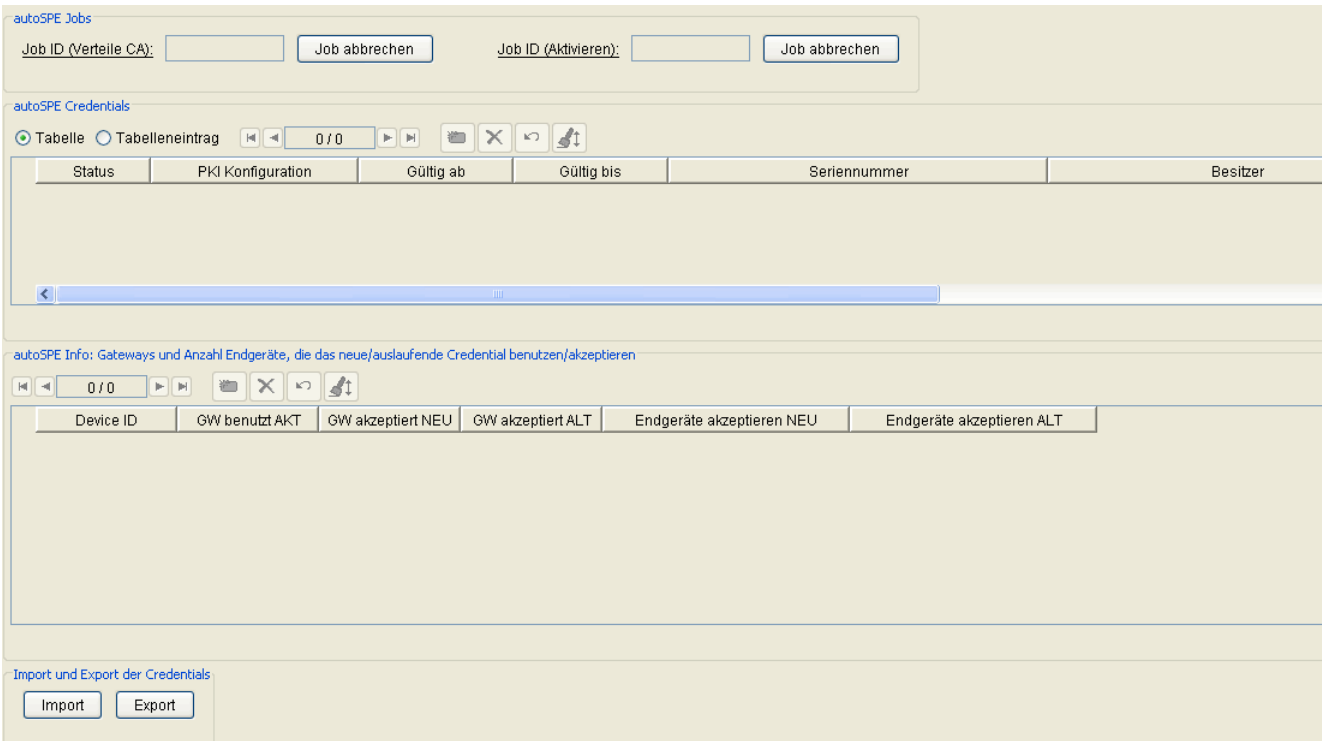
- **Internal Connector (default)**
- **Internal Root CA (default) SHA1**

  Das „Internal Root CA (default) SHA1“ wird mit dem SHA-1 Signaturalgorithmus generiert, der von HFA-Telefonen akzeptiert wird. Das Suffix SHA1 wird verwendet, um diese CA von der Default CA mit dem Signaturalgorithmus SHA256 zu unterscheiden.

HINWEIS: Abschnitt 16.4.6, “SHA1-Konfiguration für AutoSPE” enthält weitere Informationen zur PKI-Konfiguration im Zusammenhang mit HFA und Automatische SPE.

6.10.1 Register „CA Administration“

Aufruf: Hauptmenü > Administration > Automatische SPE Konfiguration > Register „CA Administration“



autoSPE Jobs

Job ID (Verteile CA)

Für das Verteilen von CAs wird ein Job gestartet. Dieser erhält eine eindeutige Job ID, über die er identifiziert werden kann. Über das Feld kann auch zur Job-Kontrolle (siehe Abschnitt 14.1, “Job Kontrolle”) gesprungen werden, um dort den Status des Jobs zu kontrollieren.

Job ID (Aktivieren)

Für das Aktivieren von CAs wird ein Job gestartet. Dieser erhält eine eindeutige Job ID, über die er identifiziert werden kann. Über das Feld kann auch zur Job-Kontrolle (siehe Abschnitt 14.1, “Job Kontrolle”) gesprungen werden, um dort den Status des Jobs zu kontrollieren.

Job abbrechen

Über diesen Button kann der jeweilige Job abgebrochen werden.

autoSPE Credentials

Status

Zeigt den aktuellen Status des Credentials.

Mögliche Werte:

- **erzeugt**
- **verteilt**
- **aktiviert**
- **auslaufend**

PKI Konfiguration

PKI Konfiguration.

Gültig ab

Gültigkeitsbeginn des Credentials.

Gültig bis

Ablaufdatum für neue autoSPE Zertifikate (mögliche Höchstdauer bis 31.12.2037).

Seriennummer

Seriennummer des CA-Zertifikates.

Besitzer

Besitzer des Credentials.

Aussteller

Aussteller des Credentials.

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1)

Der Fingerprint das CA Zertifikats identifiziert das Credential eindeutig, auch über verschiedene DLS-Instanzen. Der Fingerprint wird auch Teil des Dateinamens bei Export (siehe Button **Export**).

Erzeuge CA

Erzeugt ein neues Credential für SPE, d. h. es wird zuerst ein neues CA-Zertifikat und dann ein Zertikat mit dieser CA-Signierung erzeugt.

Verteile CA

Verteilt ein neues Credential für SPE, d. h. das CA-Zertifikat wird sofort an die entsprechenden IP Devices verteilt. Die Tabelle wird aktualisiert und der Status des Credentials in „verteilt“ geändert.

Aktivieren

Aktiviert ein neues Credential für SPE, d.h. das CA-signierte Zertifikat wird an die Gateways verteilt. Die Tabelle wird aktualisiert und der Status des neuen Credentials wird „aktiviert“, der des bisher aktiven Credentials wird „auslaufend“.

Löschen

Löscht ein nicht mehr benötigtes Credential, d. h. ein Credential im Zustand „erzeugt“ oder „verteilt“, oder das aktivierte Credential (falls nur ein Credential existiert) oder aber das auslaufende Credential (falls mehrere Credentials existieren). Anschließend wird die Tabelle aktualisiert.

autoSPE Info: Gateways und Anzahl Endgeräte, die das neue/auslaufende Credential akzeptieren

Device ID

Anzeige der Device ID des Gateways.

GW benutzt AKT

Zeigt an, ob das Gateway das aktivierte Credential benutzt.

Mögliche Werte:

- **ja**
- **nein**

GW akzeptiert NEU

Zeigt an, ob das Gateway das neue Credential akzeptiert.

Mögliche Werte:

- **ja**
- **nein**

GW akzeptiert ALT

Zeigt an, ob das Gateway das auslaufende Credential akzeptiert.

Mögliche Werte:

- **ja**
- **nein**

Endgeräte akzeptieren NEU

Zeigt die Anzahl der Geräte an, die das neue Credential akzeptieren, als auch die Gesamtzahl der am Gateway angeschlossenen Geräte. Außerdem wird die Abdeckung in Prozent angezeigt.
Beispiel: 3/5 (=60%) bedeutet, dass drei von fünf Geräten am Gateway das neue Credential akzeptieren, was 60% entspricht.

Endgeräte akzeptieren ALT

Zeigt sowohl die Anzahl der Geräte, die das auslaufende Credential akzeptieren, als auch die Gesamtzahl der am Gateway angeschlossenen Geräte. Außerdem wird die Abdeckung in Prozent angezeigt.
Beispiel: 3/5 (=60%) bedeutet, dass drei von fünf Geräten am Gateway das auslaufende Credential akzeptieren, was 60% entspricht .

Import und Export der Credentials

Import

Liest die autoSPE Credentials sowie die autoSPE-Konfiguration aus einer Datei und ersetzt die komplette derzeitige autoSPE-Konfiguration einschließlich der Verteilung zu den Gateways und Geräten.

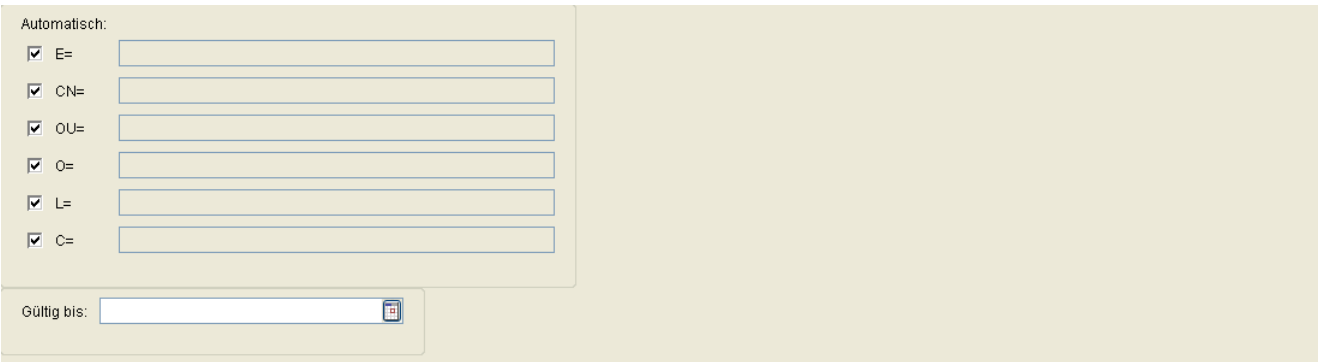
Export

Schreibt die aktuelle autoSPE Konfiguration in eine Datei. Dies kann sowohl zu Sicherungszwecken als auch für einen Umzug zu einem anderen DLS dienen.

> ***HINWEIS:*** Das Passwort ist nicht für die ZIP-Archiv-Datei gedacht, sondern für die in der ZIP-Archiv-Datei enthaltenen Dateien (WPI-Credentials).

6.10.2 Register „Aussteller Administration“

Aufruf: Hauptmenü > Administration > Automatische SPE Konfiguration > Register „Aussteller Administration“



Hier werden die Daten des Zertifikats-Ausstellers angezeigt.
HINWEIS: Ein Ändern der Zertifikatsdaten ist unter „Automatische SPE Konfiguration“ - Aussteller Administration nicht möglich.

Der Benutzer kann nur die im DLS vorgegebenen Standardeinstellungen übernehmen.

Automatisch

E=

E-Mail-Adresse des Austellers.

Beispiel: **hipath_security_office@unify.com**

CN=

Common Name (gebräuchlicher Name) des Ausstellers.

Beispiel: **Unify Security Office**.

OU=

Organizational Unit (Unterorganisation, Abteilung) des Ausstellers.

Beispiel: **Unify Systems**.

O=

Organization (Organisation, Firma) des Ausstellers.

Beispiel: **Unify GmbH & Co. KG**.

L=

Location (Standort) des Ausstellers.

Beispiel: **München**.

C=

Country (Land, Staat) des Ausstellers.

Beispiel: **DE**.

Gültig bis

Maximale Gültigkeit für neue autoSPE Credentials.

6.10.3 Register „Einstellungen“

Aufruf: Hauptmenü > Administration > Automatische SPE Konfiguration > Register „Einstellungen“

Manueller Import von Zertifikaten außerhalb autoSPE erlaubt

Wenn der Schalter aktiviert ist, kann ein Zertifikat manuell importiert werden, z. B. wenn das Verteilen mit autoSPE gescheitert ist.

Manuelles Entfernen von Zertifikaten außerhalb autoSPE erlaubt

Wenn der Schalter aktiviert ist, kann ein Zertifikat manuell entfernt werden.

HINWEIS: Manuell entfernte Zertifikate müssen auch wieder manuell importiert werden.

Manuell importierte Zertifikate durch autoSPE überschreiben

autoSPE bearbeitet bis zu 2 serverseitige CA-Zertifikate (Index 0 und 1). Vom Anwender können aber bis zu 16 serverseitige CA Zertifikate (Index 0 bis 15) importiert werden. Wenn autoSPE aktiviert wird, überschreibt es die Indizes 0 und 1 mit eigenen CA-Zertifikaten.

Ist der Schalter gesetzt, werden die Indizes 2 bis 15 dabei entfernt. Andernfalls werden nur die Indizes 0 und 1 mit autoSPE-Zertifikaten überschrieben und die übrigen Indizes bleiben unangetastet.

Bestehende Credentials beim autoSPE Import löschen

Vor einem Import werden alle bestehenden Credentials gelöscht.

Neue Gateways automatisch mit autoSPE Zertifikaten versorgen

Wenn aktiviert, werden neu hinzukommende Gateways automatisch mit bestehenden autoSPE Zertifikaten versorgt. Andernfalls können über **IP Devices** > **IP Gateway Konfiguration** > **Signaling and Payload Encryption (SPE)** > **Zertifikat importieren** Gateways mit Zertifikaten versorgt werden

Neue Endgeräte automatisch mit autoSPE Zertifikaten versorgen

Wenn aktiviert, werden neu hinzukommende Endgeräte automatisch mit bestehenden autoSPE Zertifikaten versorgt. Andernfalls können über **IP Devices** > **IP Gateway Konfiguration** > **Signaling and Payload Encryption (SPE)** > **Zertifikat importieren** Endgeräte mit Zertifikaten versorgt werden.

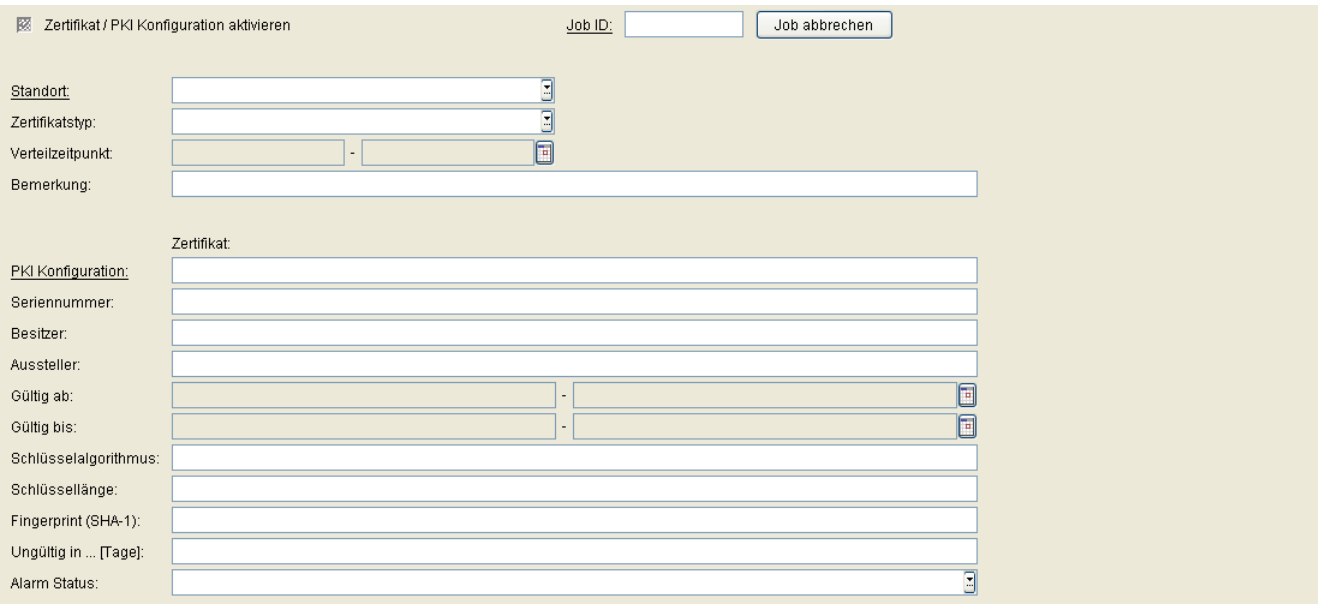
6.11 Automatische Zertifikatsverteilung

Aufruf: Hauptmenü > Administration > Automatische Zertifikatsverteilung

Dieser Bereich ermöglicht es, Zertifikate automatisch allen IP Phones eines eingerichteten Standortes zuzuordnen und die Verteilung zu einem angegebenen Zeitpunkt zu starten.

Die automatische Zertifikatsverteilung an IP Phones kann verhindert werden, indem unter **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** der Schalter **Automatische Zertifikatsverteilung** gesperrt aktiviert wird.

HINWEIS: Sollen mit automatischer Zertikatsverteilung Zertifikate aller IP Phones eines Standorts gelöscht werden, so muss ein leeres Zertifikat eingetragen werden.



Zertifikat/ PKI Konfiguration aktivieren

Das Zertifikat wird für die automatische Zertifikatsverteilung aktiviert. Mit dem Aktivieren wird das Generieren der entsprechenden Jobs zu den Devices angestoßen. Aktivierte Einträge können nicht mehr verändert werden.

Eine Zertifikatsverteilung kann gestoppt/deaktiviert werden, indem dieser Schalter deaktiviert wird. Die bereits generierten, aber noch nicht ausgeführten Jobs (Status aktiv oder laufend) werden nicht abgebrochen, dies kann aber über den Button **Job abbrechen** angestoßen werden. Es werden dann alle Jobs dieses Auftrags abgebrochen, und das Zertifikat dieses Auftrags wird nicht länger an neu registrierte IP Devices verteilt.

Job ID:

Für die Zertifikatsverteilung wird ein Job gestartet. Dieser erhält eine eindeutige Job ID, über die er identifiziert werden kann. Über das Feld kann auch zur Job-Kontrolle (siehe Abschnitt 14.1, “Job Kontrolle”) gesprungen werden, um dort den Status des Jobs zu kontrollieren.

Job abbrechen

Über diesen Button werden alle zu diesem Zertifikatsverteilungsauftrag gehörenden Jobs mit Status aktiv oder laufend abgebrochen.

Standort:

Standort, an dem die Zertifikatsverteilung durchgeführt werden soll. Standorte können wie unter Abschnitt 6.3.2, “Standort” beschrieben eingerichtet werden.

Zertifikats Typ:

Typ des Zertifikats.

Mögliche Optionen:

- **RADIUS Server CA Zertifikat 1**
- **RADIUS Server CA Zertifikat 2**
- **Phone Zertifikat**
- **WBM Server Zertifikat (IP Phone)**
- **WBM Server Zertifikat (IP Gateway: Index 0)**

Verteilzeitpunkt:

Zeitpunkt, an dem das Zertifikats-Deployment durchgeführt wird.

Bemerkung:

Bemerkung (freier Text).

Zertifikat:

Die folgenden Zertifikatsdaten werden nur angezeigt.

PKI Konfiguration

PKI Konfiguration.

Seriennummer:

Seriennummer des Zertifikats.

Besitzer:

Besitzer des Zertifikats.

Aussteller:

Aussteller des Zertifikats.

Gültig ab:

Das Zertifikat wird von diesem Zeitpunkt an gültig sein.

Gültig bis:

Das Zertifikat wird bis zu diesem Zeitpunkt gültig sein.

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

Alarm Status:

Aktueller Alarm-Status des importierten Zertifikats.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

Mögliche Aktionsschaltflächen

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Sichern

Sichert die eingegebenen/geänderten Daten.

Neu

Erstellt einen neuen Eintrag, d. h. einen neuen Zertifikatsverteilungsauftrag.

Löschen

Löscht einen Eintrag.

Zertifikat importieren

Importieren Sie entweder ein bestimmtes Zertifikat, das automatisch auf Geräten bereitgestellt werden soll, oder eine PKI-Konfiguration, die für die automatische Anforderung von Zertifikaten für alle Geräte verwendet wird.

HINWEIS: Wenn Sie nicht abschließend auf die Schaltfläche Zertifikat importieren klicken, wird ein leeres Zertifikat bereitgestellt und alle vorhandenen Zertifikate werden entfernt.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.12 Automatische Archivierung

Aufruf: Hauptmenü > Administration > Automatische Archivierung

Dieser Service ermöglicht es dem Benutzer, zeitgesteuert die Daten von ausgewählten IP Devices zu archivieren. Die archivierten Daten werden in .zip-Dateien gespeichert. Existiert noch keine Archiv-Datei, wird sie während der ersten Archivierung angelegt; ist bereits eine vorhanden, werden die aktuellen Daten in diese .zip-Datei geschrieben. Für jedes zu archivierende IP Device wird eine eigene Datei in die .zip-Archivdatei geschrieben.

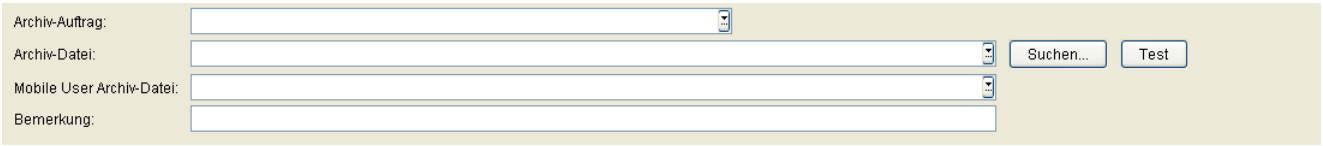
Jeder neue Archiveintrag für ein IP Device überschreibt einen bereits dafür existierenden, ohne dass ein Hinweis gegeben wird. Für die Dateihistorie werden Sicherungen von bereits existierenden Dateien der .zip-Archivdatei angelegt. Die Anzahl wird über **Max. Anzahl von Sicherungen der Archiv-Dateien** im Register „Einstellungen“ festgelegt.

Die archivierten Daten können wiederhergestellt werden über **Administration** > **Automatische Archivierung** > > Aktion „IP Device aus Archiv laden“.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einstellungen“
- Register „zu archivierende IP Devices“
- Register „zu archivierende Mobile User“
- Register „Protokoll“

Allgemeine Daten



Archiv-Auftrag:

Name eines Archivierungsauftrages.

Archiv-Datei

Dateiname und Pfad für die Archivdatei auf dem DLS-Server. Existiert noch keine Archiv-Datei, wird sie während der ersten Archivierung angelegt; ist bereits eine vorhanden, werden die aktuellen Daten in diese .zip-Datei geschrieben.

Mobile User Archiv-Datei

Dateiname und Pfad für die Archivdatei auf dem DLS-Server. Er wird vom Inhalt in **Archiv Datei** abgeleitet und entsprechend automatisch vorgegeben.

Bemerkung

Bemerkungen zum Archivauftrag.

Durchsuchen...

Ein vorhandenes Archiv-Verzeichnis kann ausgewählt werden. Der Pfad zum Verzeichnis wird in die Archiv-Datei eingetragen. Es kann nur nach Verzeichnissen, nicht nach einzelnen Dateien gesucht werden.

Test

Testen, ob der angegebene Pfad erreichbar ist.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht Suche können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Startet einen Job zur Verteilung der Konfigurationsänderungen. Siehe hierzu auch Abschnitt 15.1

„Erste Schritte: Ändern von IP Device-Parametern“.

Verwerfen

Die in der Maske vorgenommenen Änderungen werden verworfen.

Datei exportieren

Die Inventar-Daten werden im CSV-Format in eine Datei exportiert.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

6.12.1 Register „Einstellungen“

Aufruf: Hauptmenü > Administration > Automatische Archivierung > Register „Einstellungen“

Allgemeine Einstellungen

Max. Anzahl von Sicherungen der Archiv-Dateien

Gibt an, wieviele Sicherungsdateien für die Dateihistorie beim jeweiligen Überschreiben der Archiv-Datei angelegt werden.

Zeit-Einstellungen

Tägliche Archivierung ausführen

Aktiviert das tägliche Ausführen der Archivierung.

Täglicher Ausführungszeitpunkt

Uhrzeit, zu der die Archivierung gestartet wird.

HINWEIS: Die Umstellung von Sommerzeit auf Winterzeit (eine Stunde zurück) führt nicht zu einem erneuten Ausführen eines Jobs, der in dem dadurch verdoppelten Zeitintervall gestartet wurde. Allerdings wird bei der Umstellung von Winterzeit auf Sommerzeit (eine Stunde vor) ein Job, der in die dadurch übersprungene Zeit fällt, nicht ausgeführt.

Tägliche Archivierung ausführen am:

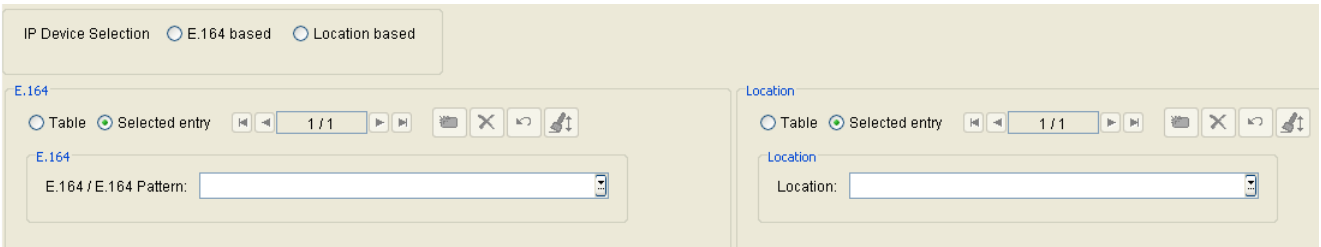
Tageweise Einschränkung der Archivierung eintragen.

Archivierung jetzt durchführen

Die Archivierung wird sofort durchgeführt, unabhängig irgendwelcher Einstellungen zur automatischen Archivierung. Die Archivierung erfolgt in die angezeigte **Archiv-Datei**.

6.12.2 Register „zu archivierende IP Devices“

Aufruf: Hauptmenü > Administration > Automatische Archivierung > Register „zu archivierende IP Devices“



IP Device Auswahl

nach E.164

Die Auswahl des zu archivierenden IP Devices erfolgt über die E.164 Nummer.

nach Standort

Die Auswahl des zu archivierenden IP Devices erfolgt über den Standort.

E.164

E.164 /E.164 Pattern

Es kann eine vollständige E.164 Nummer oder ein mit ‘*’ teilqualifizierter E.164 Nummernbereich, z.B. 31* (= alle E.164 Nummern, die mit 31... beginnen) eingegeben werden.

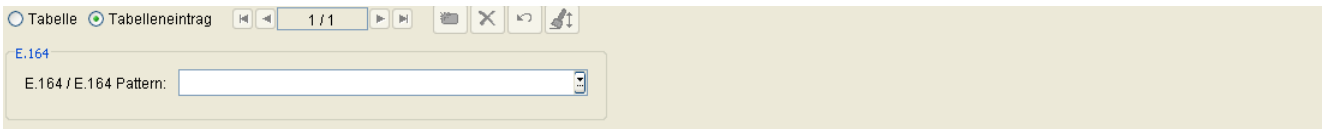
Standort

Standort

Auswahl eines definierten Standorts. Die ’Default Location’ kann nicht ausgewählt werden.

6.12.3 Register „zu archivierende Mobile User“

Aufruf: Hauptmenü > Administration > Automatische Archivierung > Register „zu archivierende Mobile User“



E.164

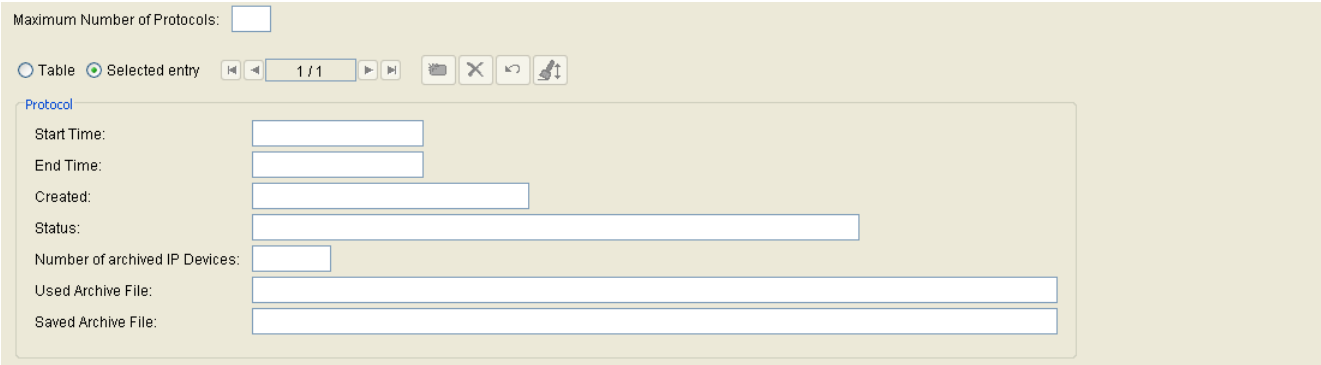
E.164 / E.164 Pattern:

Es kann eine vollständige E.164-Nummer oder ein mit ’*’ teilqualifizierter E.164-Nummernbereich eingegeben werden.

Beispiel: **31*** = alle E.164-Nummern, die mit 31 beginnen.

6.12.4 Register „Protokoll“

Aufruf: Hauptmenü > Administration > Automatische Archivierung > Register „Protokoll“



Protokoll

Maximale Anzahl von Protokollen:

Jeder Protokolleintrag kann einzeln von Hand gelöscht werden oder er wird abhängig von der eingetragenen Anzahl automatisch gelöscht.

Startzeit:

Startzeit der Archivierung.

Endzeit

Endzeit der Archivierung

Erzeugt:

Anzeige, ob es sich um eine tägliche oder eine einmalige Archivierung handelt.

- **Manuell**
- **Zeit gesteuert**

Status

Status der Archivierung.

Mögliche Werte:

- **Archivierung erfolgreich**
- **Archivierung fehlgeschlagen**
- **Alte Protokoll-Einträge automatisch gelöscht**

Anzahl archivierter IP Devices

Anzahl der archivierten IP Devices.

Aktuelle Archiv-Datei

Name der aktuellen Archiv-Datei.

Gesicherte Archiv-Datei

Namen der letzten Sicherung der aktuellen Archiv-Datei.

6.13 Automatischer Upload Diagnose- und Security Log Dateien

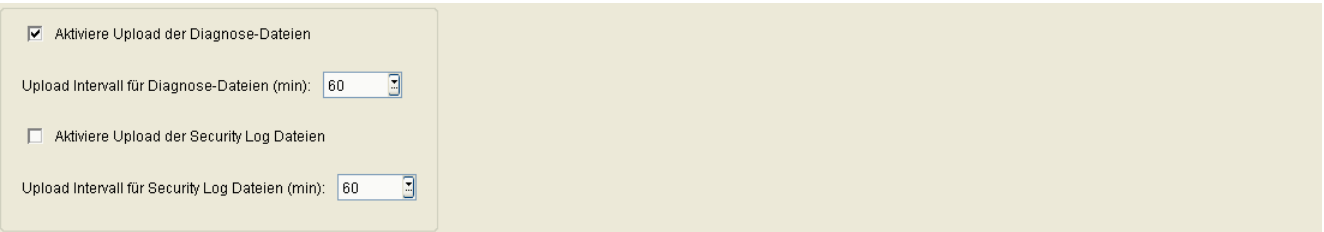
Aufruf: Hauptmenü > Administration > Automatischer Upload Diagnose- und Security Log Dateien

Dieser Service ermöglicht es dem Benutzer, zeitgesteuert die Diagnose- und Security Log Dateien von ausgewählten IP Devices zu laden. Die hochgeladene Datei wird auf einem Netzlaufwerk gespeichert. Der Pfad wird definiert unter **Hauptmenü** > **Administration** > **File Server** > **OpenStage Diagnose Dateien** oder **OpenStage Security Log-Dateien**.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Protokoll“

Allgemeine Daten



Aktiviere Upload der Diagnose Dateien

Wenn aktiviert, werden die Diagnosedateien ausgewählter IP Devices geladen.

Upload Intervall der Diagnose Dateien

Legt den Zeitabstand in Minuten zwischen zwei Ladeaufträgen fest.

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Standardwert: **60**

Aktiviere Upload der Security Log Dateien

Wenn aktiviert, werden die Security Log-Dateien ausgewählter IP Devices geladen.

Upload Intervall der Security Log Dateien

Legt den Zeitabstand in Minuten zwischen zwei Ladeaufträgen fest.

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Standardwert: **60**

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Sichern

Die Änderungen werden gesichert.

Verwerfen

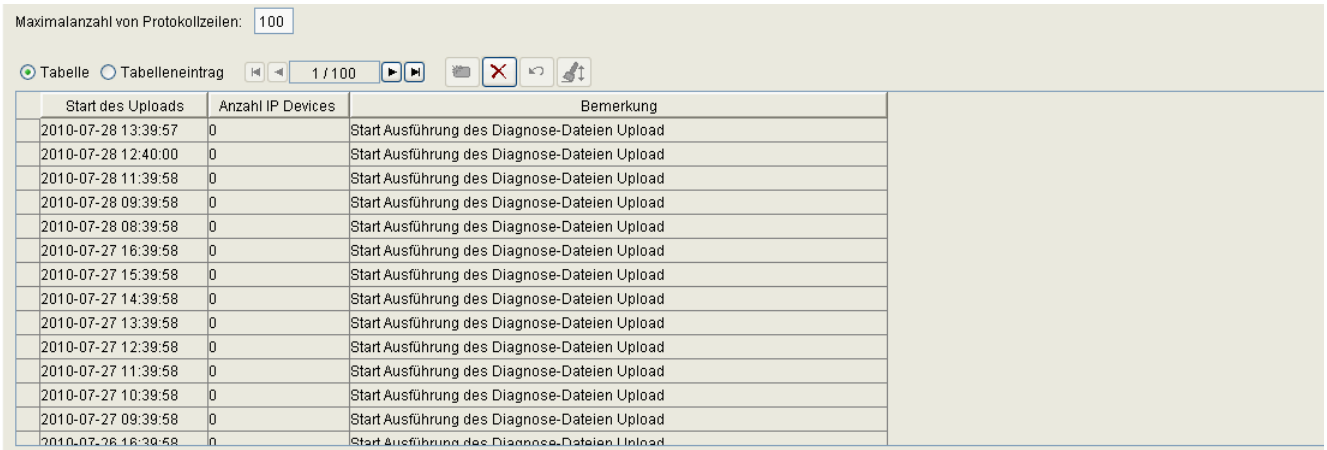
Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

6.13.1 Register „Protokoll“

Aufruf: Hauptmenü > Administration > Automatischer Upload Diagnose- und Security Log Dateien > Register „Protokoll“



Start des Uploads	Anzahl IP Devices	Bemerkung
2010-07-28 13:39:57	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-28 12:40:00	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-28 11:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-28 09:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-28 08:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 16:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 15:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 14:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 13:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 12:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 11:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 10:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-27 09:39:58	0	Start Ausführung des Diagnose-Dateien Upload
2010-07-26 16:39:58	0	Start Ausführung des Diagnose-Dateien Upload

Maximale Anzahl von Protokollen:

Jeder Protokolleintrag kann einzeln von Hand gelöscht werden oder er wird abhängig von der eingetragenen Anzahl automatisch gelöscht.

Start des Uploads

Zeitpunkt, an dem der Upload gestartet wurde.

Anzahl IP Devices

Anzahl der IP Devices, für die Dateien hochgeladen wurden.

Bemerkung

Bemerkung, die zu diesem Upload eingetragen wurde.

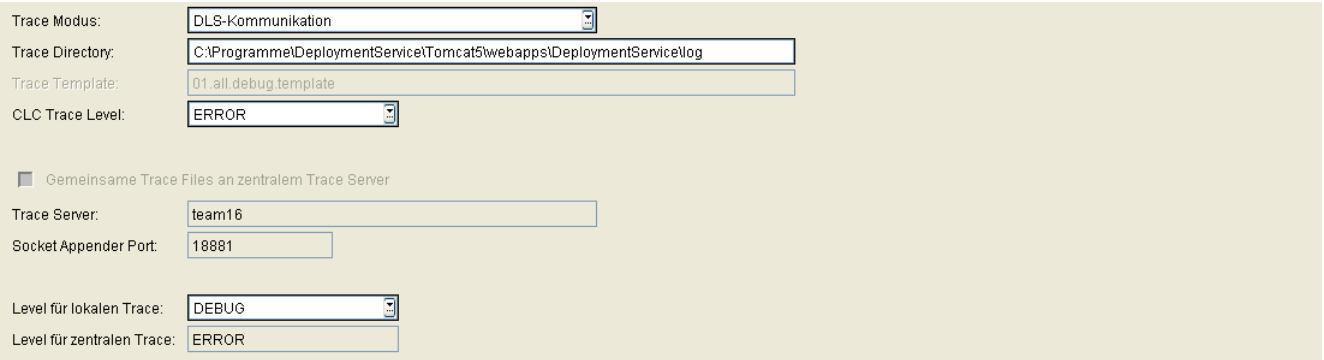
6.14 Trace Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Zusätzliche Einstellungen und Aktionen“
- Register „Wiederholungs-Filter“
- Register „Meldungs-Filter“
- Register „Filter-Test“
- Register „OSVTM Configuration“ (OSVTM-Konfiguration)
- Register „Thread Überwachung“

Allgemeine Daten

Aufruf: Hauptmenü > Administration > Trace Konfiguration



Mit diesem Menüpunkt kann das Traceverhalten konfiguriert werden. Die Einstellungen werden in der DLS-Datenbank gespeichert. Ein Timer überwacht, ob neue Einträge in der Datenbank vorhanden sind. Wenn ja, wird der Trace entsprechend geändert; ggf. werden die Änderungen auch an die anderen Server eines Clusters übermittelt.

HINWEIS: Die Änderungen werden nach einer Wartezeit von ca. 2 min wirksam.

HINWEIS: Einzelne Einstellungen können die Auswahlmöglichkeiten im Menü **Administration** > **Protokoll-Daten** einschränken.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Trace Modus

Auswahl des Trace-Modus.

Mögliche Werte:

- **Ausgeschaltet**
  Es wird kein spezieller Trace durchgeführt. Alle Fehlermeldungen werden jedoch in ein Default-Tracefile geschrieben. Dies ist die Default-Einstellung nach einer Installation.
- **DLS-Server**
  Trace im DLS Server wird mit dem eingestellten **Level für lokalen Trace** durchgeführt.
- **DLS-Kommunikation**
  Trace der Kommunikation zwischen IP Devices und DLS Server wird mit dem eingestellten **Level für lokalen Trace** durchgeführt. Zusätzlich werden alle Fehlermeldungen im Default-Tracefile gespeichert.
- **Log4j-Template**
  Trace wird mit vordefiniertem Trace Template durchgeführt, das unter **Trace Template** ausgewählt werden kann.

Trace Directory

Verzeichnis, in dem die Trace-Dateien abgelegt werden.

Trace Template

Auswahl vordefinierter Trace-Einstellungen. Die Trace-Templates sind im Dateiverzeichnis `<Laufwerk>:\Program Files\DeploymentService\Tomcat5\webapps\DeploymentService\log\templates` gespeichert. Die Einstellungen in den Templates sind nur wirksam, wenn der **Trace Modus** „Log4j-Template“ eingestellt ist.

Mögliche Werte:

- **01.all.debug.template**
  Loggen aller DLS-Aktivitäten mit Logging-Level DEBUG.
- **02.all.info.template**
  Loggen aller DLS-Aktivitäten mit Logging-Level INFO.
- **03.default.template**
  Default-Einstellung. Loggen aller DLS Aktivitäten mit Logging-Level ERROR.
- **04.gateway.template**
  Loggen aller Gateway-Aktivitäten mit Logging-Level DEBUG.
- **05.gateway.wpcomm.details.template**
  Loggen aller Gateway-Aktivitäten einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **06.gateway.wpcomm.info.template**
  Loggen aller Gateway-Aktivitäten einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **07.keyexchange.template**
  Loggen aller Gateway- und Schlüsselverteilungs-Aktivitäten mit Logging-Level DEBUG.
- **08.keyexchange.wpcomm.details.template**
  Loggen aller Gateway- und Schlüsselverteilungs-Aktivitäten einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **09.keyexchange.wpcomm.info.template**
  Loggen aller Gateway- und Schlüsselverteilungs-Aktivitäten einschließlich der Kommunikation zwischen Workpoint mit Logging-Level DEBUG.
- **10.wpcomm.details.template**
  Loggen der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **11.wpcomm.short.template**
  Loggen der Kommunikation zwischen Workpoint und DLS mit Logging-Level INFO.

- **12.wpscan.wpcomm.details.template**
  Loggen aller Scan-Aktivitäten des Workpoints einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **13.wpscan.wpcomm.short.template**
  Loggen aller Scan-Aktivitäten des Workpoints einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging Level INFO.
- **14.dlsapi.template**
  Loggen aller DLS API-Methoden mit Logging-Level DEBUG.
- **15.auth.debug.template**
  Loggen aller Authentifikationsaktivitäten einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **16.nodb.debug.template**
  Loggen aller DLS-Aktivitäten mit Ausnahme der Datenbasis-Aktivitäten einschließlich der Kommunikation zwischen Workpoint und DLS mit Logging-Level DEBUG.
- **17.pp.em.debug.template**
  Loggen aller Plug&Play- und Elementmanager-Aktivitäten mit Logging-Level DEBUG.
- **18.pki.details.template**
  Loggen aller PKI Aktivitäten mit Logging-Level DEBUG.

CLC Trace Level

Trace Level für die Kommunikation mit dem zentralen Lizenzagenten (CLA).

Mögliche Werte:

- **DEBUG**
  Ausführlicher Trace von Prozessabläufen.
- **INFO**
  Ausgewählte Informationen zu Prozessabläufen.
- **WARN**
  Anzeige von potentiell fehlerhaften Situationen.
- **ERROR**
  Anzeige von Fehlersituationen, die aber zu keinem Abbruch des DLS führen.

Gemeinsame Trace Files an zentralem Trace Server

Traces von allen Knoten eines Clusters werden in eine Datei auf einem zentralen Server geschrieben. Es werden die Dateien `dlswpcommunication.txt`, `dlslog.txt` und `dlserror.txt` angelegt.

Trace Server

Server, an dem die gemeinsamen Trace Files abgelegt werden.

Socket Appender Port

Nummer des Ports, über den die gemeinsamen Trace-Daten an einen Knoten innerhalb des Clusters geschickt werden.
Defaultwert: **18881**.

Level für lokalen Trace

Einstellung des Trace Level für lokale Traces im DLS-Server. Die Hierarchie der Level ist DEBUG < INFO < WARN < ERROR < FATAL, d.h. ist DEBUG gesetzt, werden alle anderen Level auch geloggt. Falls die Diagnose-Einstellungen über ein Template gesteuert werden, hat der dort für diesen Parameter gesetzte Wert Vorrang.

Mögliche Werte:

- **DEBUG**
  Ausführlicher Trace von Prozessabläufen.
- **INFO**
  Ausgewählte Informationen zu Prozessabläufen.
- **WARN**
  Anzeige von potentiell fehlerhaften Situationen.
- **ERROR**
  Anzeige von Fehlersituationen, die aber zu keinem Abbruch des DLS führen.
- **FATAL**
  Anzeige von Fehlersituationen, die zu einem Abbruch des DLS führen.

Level für zentralen Trace

Trace Level für gemeinsame Traces auf einem Trace Server im Cluster. Falls die Diagnose-Einstellungen über ein Template gesteuert werden, hat der dort für diesen Parameter gesetzte Wert Vorrang.

Mögliche Werte:

- **INFO**
  Ausgewählte Informationen zu Prozessabläufen.
- **WARN**
  Anzeige von potentiell fehlerhaften Situationen.
- **ERROR**
  Anzeige von Fehlersituationen, die aber zu keinem Abbruch des DLS führen.

- **FATAL**
  Anzeige von Fehlersituationen, die zu einem Abbruch des DLS führen.

Mögliche Aktionsschaltflächen

Abhängig vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

6.14.1 Register „Zusätzliche Einstellungen und Aktionen“

Aufruf: Hauptmenü > Administration > Trace Konfiguration > Register „Zusätzliche Einstellungen und Aktionen“

Maximale Anzahl Backup-Dateien

Maximale Anzahl angelegter Backup-Dateien pro Trace-Datei.

Wertebereich: **1** - **999**

Lösche Trace-Dateien

Alle Trace-Dateien werden gelöscht.

Download Trace-Dateien

Download aller Trace-Dateien in einer .zip-Datei in einen lokalen Ordner.

HINWEIS: Falls Sie den Microsoft Internet Explorer verwenden, muss die Einstellung **Automatische Eingabeaufforderung für Dateidownloads** aktiviert sein. Gehen Sie hierzu auf **Extras** > **Internetoptionen** > **Register „Sicherheit“**. Wählen Sie hier die Webinhaltszone aus, in der sich der DLS befindet, und klicken Sie **Stufe anpassen...**. Im Popup-Fenster **Sicherheitseinstellungen**, unter **Downloads**, finden Sie die oben genannte Einstellung.

Einfügen Kommentar in Trace-Dateien ...

Fügt einen Kommentar in alle Trace-Dateien ein.

Sammeln gefilterter Trace Daten ...

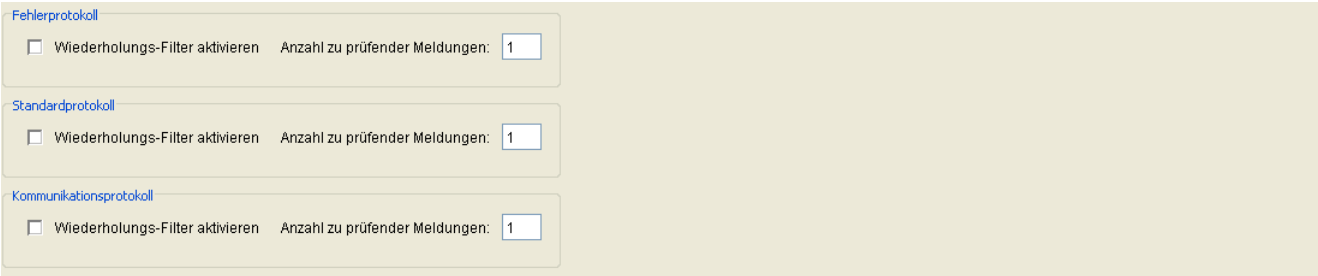
Diese Funktion filtert bereits erzeugte Trace-Dateien (`dlslog.txt` und `dlsWpCommunication.txt`) nach bestimmten Filterkriterien: E.164 Nummern, IP-Adressen, Device IDs. Eine Verknüpfung von Filterkriterien ist nicht möglich. Diese Filterkriterien werden in einem Popup-Fenster abgefragt. Datensätze, die einem Filterkriterium entsprechen, werden in eine eigene Trace-Datei abgelegt. Über **Download Trace-Dateien** können die erzeugten Dateien angesehen werden. Die erzeugten Dateien erhalten folgende Namen:

`<Filterkriterium>_FILTERED_dlslog.txt` und `<Filterkriterium>_FILTERED_dlsWpCommunication.txt`. Mit **Lösche Trace-Dateien** werden diese Dateien gelöscht.

6.14.2 Register „Wiederholungs-Filter“

HINWEIS: Durch Anwendung dieser Funktion können Meldungen verlorengehen, die unter Umständen für Analysen erforderlich sind. Daher sollte sie mit Bedacht angewendet werden, vorzugsweise nur auf Veranlassung durch den DLS-Support

Aufruf: Hauptmenü > Administration > Trace Konfiguration > Register „Wiederholungs-Filter“



Fehlerprotokoll

Wiederholungs-Filter aktivieren

Wenn aktiviert, werden Wiederholungen von Meldungen im Fehlerprotokoll herausgefiltert. Der Umfang des Kontexts, innerhalb dessen nach Wiederholungen gesucht wird, wird im Parameter **Anzahl zu prüfender Meldungen** angegeben.

Anzahl zu prüfender Meldungen

Größe eines Blocks von aufeinanderfolgenden Meldungen im Fehlerprotokoll, innerhalb dessen Wiederholungen herausgefiltert werden sollen.

Standardprotokoll

Wiederholungs-Filter aktivieren

Wenn aktiviert, werden Wiederholungen von Meldungen im Standardprotokoll herausgefiltert. Der Umfang des Kontexts, innerhalb dessen nach Wiederholungen gesucht wird, wird im Parameter **Anzahl zu prüfender Meldungen** angegeben.

Anzahl zu prüfender Meldungen

Größe eines Blocks von aufeinanderfolgenden Meldungen im Standardprotokoll, innerhalb dessen Wiederholungen herausgefiltert werden sollen.

Kommunikationsprotokoll

Wiederholungs-Filter aktivieren

Wenn aktiviert, werden Wiederholungen von Meldungen im Kommunikationsprotokoll herausgefiltert. Der Umfang des Kontexts, innerhalb dessen nach Wiederholungen gesucht wird, wird im Parameter **Anzahl zu prüfender Meldungen** angegeben.

Anzahl zu prüfender Meldungen

Größe eines Blocks von aufeinanderfolgenden Meldungen im Kommunikationsprotokoll, innerhalb dessen Wiederholungen herausgefiltert werden sollen.

6.14.3 Register „Meldungs-Filter“

Aufruf: Hauptmenü > Administration > Trace Konfiguration > Register „Meldungs-Filter“

aktiv

Ein- und Ausschalten des Filters.

Zeichenkette

Zeilen, die diese Zeichenkette enthalten, werden herausgefiltert.

Fehlerprotokoll

Wenn aktiviert, wird der Filter auf das Fehlerprotokoll angewendet.

Standardprotokoll

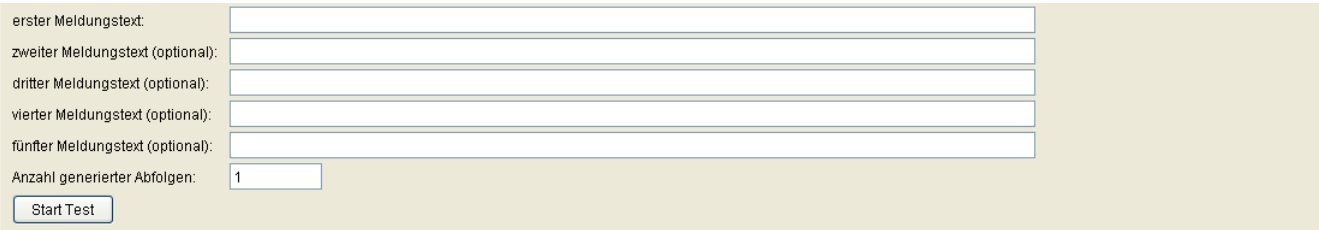
Wenn aktiviert, wird der Filter auf das Standardprotokoll angewendet.

Kommunikationsprotokoll

Wenn aktiviert, wird der Filter auf das Kommunikationsprotokoll angewendet.

6.14.4 Register „Filter-Test“

Aufruf: Hauptmenü > Administration > Trace Konfiguration > Register „Filter-Test“



erster Meldungstext

Zeichenkette als Test-Meldung, um die konfigurierten Filter zu testen.

zweiter Meldungstext (optional)

Zusätzliche Zeichenkette, um die konfigurierten Filter zu testen; erscheint als eigene Meldung.

dritter Meldungstext (optional)

Zusätzliche Zeichenkette, um die konfigurierten Filter zu testen; erscheint als eigene Meldung.

vierter Meldungstext (optional)

Zusätzliche Zeichenkette, um die konfigurierten Filter zu testen; erscheint als eigene Meldung.

fünfter Meldungstext (optional)

Zusätzliche Zeichenkette, um die konfigurierten Filter zu testen; erscheint als eigene Meldung.

Anzahl generierter Abfolgen

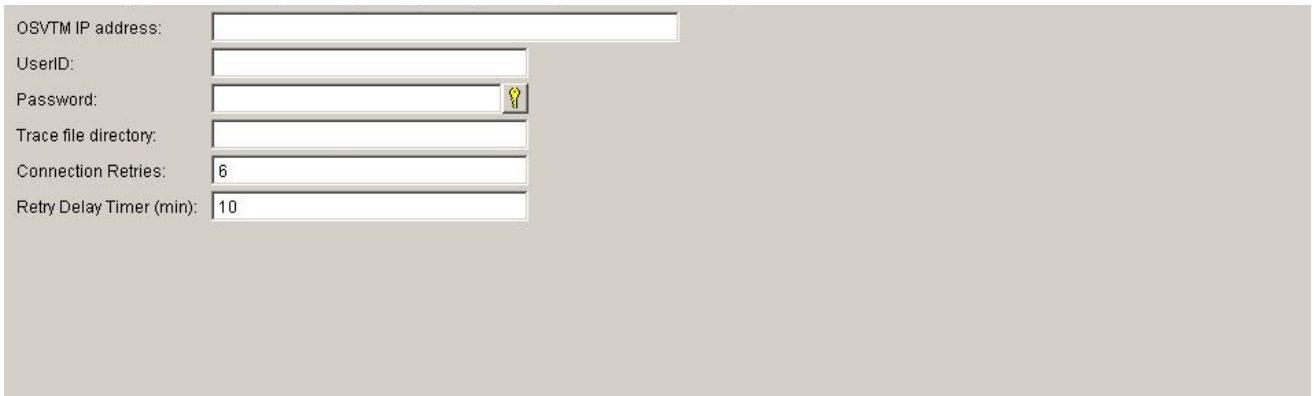
Legt fest, wie oft die definierten Test-Meldungen generiert werden sollen.

Start Test

Die Test-Meldungen werden generiert und gefiltert. Die Ergebnisse erscheinen in den Protokollen.

6.14.5 Register „OSVTM Configuration“ (OSVTM-Konfiguration)

Aufruf: Hauptmenü > Administration > Trace Konfiguration > Register „OSVTM Configuration“



OSVTM IP address (OSVTM-IP-Adresse)

Gibt die OSVTM-IP-Adresse an.

User ID

Benutzerkennung für den OSVTM-File-Transfer.

Passwort

Passwort für den OSVTM-File-Transfer.

Trace file directory (Tracedatei-Verzeichnis)

Tracedatei-Verzeichnis auf OSVTM.

Connection Retries (Verbindungswiederholungen)

Wenn der Dateitransfer fehlschlägt, wird die auf dem DLS gespeicherte Trace-Datei mindestens für die Anzahl der hier angegebenen Verbindungswiederholungen beibehalten.

Standardwert: 6.

Retry Delay Timer (min)

In regelmäßigen Abständen wird versucht, die Datei erneut zu senden. Der Standardwert ist auf 10 Minuten eingestellt, d. h. die Datei wird alle 10 Minuten erneut gesendet.

6.14.6 Register „Thread Überwachung“

Aufruf: Hauptmenü > Administration > Trace Konfiguration > Register „Thread Überwachung“

HINWEIS: Um die Thread-Überwachung zu aktivieren, müssen Sie **Trace Modus** auf **Log4j Template** setzen.
Siehe Abschnitt 6.14, “Trace Konfiguration”.

Überwachung Periode (Mindest: 600 Sekunden)

Das Zeitintervall, während dessen die Thread-Überwachung durchgeführt wird.

Standardwert: 3600 Sek.

Thread Überwachung Status

Berücksichtigen inactiv Threads

Wenn dieser Schalter aktiviert ist, werden auch inaktive Threads berücksichtigt.

Schnappschuss erhalten

Thread Überwachung Starten

Thread Überwachung Stoppen

6.15 Server Lizenzen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Lizenzstatus“
- Register „Betrieb mehrerer DLS Server“

Administration

Server Lizenzen

Allgemeine Daten

Aufruf: Hauptmenü > Administration > Server Lizenzen

Lizenzagent

IP-Adresse oder Hostname des Lizenzagenten.

Port

Port-Nummer für den Zugriff auf den Lizenzserver.

Lizenz Management

URL des Lizenz-Servers. Über die dazugehörige Aktionsschaltfläche **Lizenz Management** wird in einem eigenen Browserfenster die Web-Schnittstelle des Lizenzmanagements geöffnet.

Mögliche Aktionsschaltflächen

Sichern

Sichert die Feldinhalte in der Datenbank.

Verwerfen

Verwirft die eingetragenen Änderungen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

Lizenzen auslesen

Verfügbare Lizenzen erneut vom Lizenzagenten anfordern.

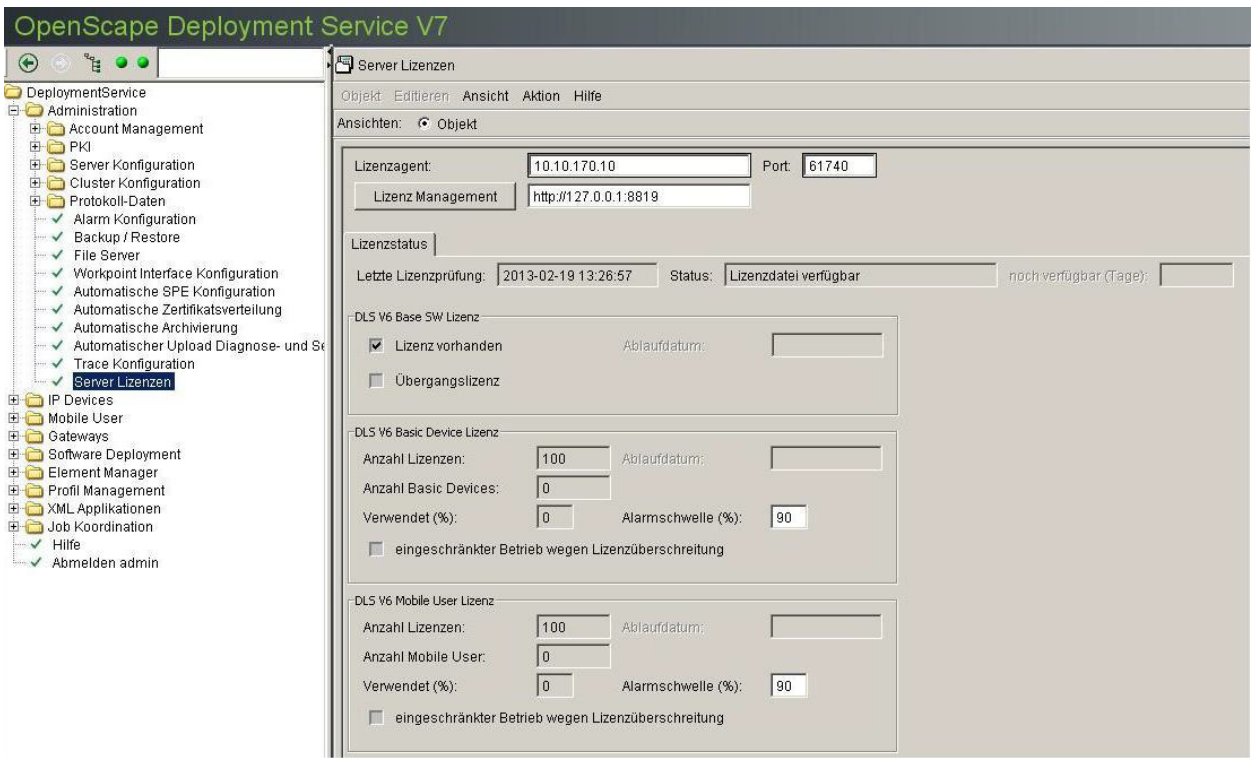
HINWEIS: Nach der Installation einer gültigen DLS-Lizenzdatei mit dem **LinuxCLM**-Tool werden die Lizenzen von LinuxDLS nach dem Einstelllen der IP-Adresse des entsprechenden Lizenzagenten nicht sofort gefunden, weil der DLS:

-(a) in regelmäßigen Abständen (alle 4 Stunden) eine Überprüfung auf Lizenzänderungen durchführt
-(b) eine Überprüfung auf Lizenzänderungen durchführt, wenn der DLS-Dienst gestartet wird (Sie können den Deployment Support-Dienst über das Dashboard-Menü des CMP manuell neu starten)

6.15.1 Register „Lizenzstatus“

Aufruf: Hauptmenü > Administration > Server Lizenzen > Register „Lizenzstatus“

Hier wird der aktuelle Status der verschiedenen Lizenzen angezeigt.



Letzte Lizenzprüfung

Datum und Uhrzeit der letzten Lizenzprüfung am Lizenzagenten werden angezeigt.

Status:

Statusanzeige der Verbindung zum CLA (Lizenzagent).

Mögliche Optionen:

- **Lizenzdatei verfügbar**
- **Aktivierungsperiode – keine Lizenzdatei verfügbar**
- **Failover Period – CLA nicht erreichbar**

noch verfügbar (Tage)

Verfügbarkeit des DLS in Tagen, falls der CLA weiterhin nicht erreichbar ist.

DLS V7 Base SW Lizenz

Lizenz vorhanden

Schalter ist aktiv, wenn eine Base SW Lizenz in der Lizenzdatei eingetragen ist.

Ablaufdatum

Ablaufdatum der Lizenz. Nach diesem Datum ist kein weiteres DLS Logon möglich. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

Übergangslizenz

Ist der Schalter aktiv, nutzen Sie V7 Base SW und V7 Basic Device Lizenzen, obwohl diese nicht in Ihren gewährten V7 Lizenzen enthalten sind. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V7 Basic Device Lizenz

HINWEIS: Falls Mandantenfähigkeit eingerichtet ist, müssen die vorhandenen V7 Basic Device Lizenzen pro Mandant eingerichtet werden, wie unter Abschnitt 6.3.1, “Mandanten” beschrieben.

Anzahl Lizenzen:

Zeigt die Anzahl der Basic Devices, die mit der vorhandenen Lizenz eingerichtet werden können.

Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf dieser Frist ist eine Registrierung von IP Devices mit DLS nicht mehr möglich. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

Anzahl Basic Devices:

Zeigt die Anzahl der bereits verwendeten Basic Device Lizenzen für IP Devices an.

Verwendet (%)

Zeigt an, wie viel Prozent der vorhandenen Lizenzen bereits verwendet sind.

Alarmschwelle (%)

Legen Sie fest, ab welchem Prozentsatz an verwendeten Lizenzen ein Lizenzalarm generiert werden soll.

eingeschränkter Betrieb wegen Lizenzüberschreitung

Ist aktiviert, wenn eine Lizenzüberschreitung vorliegt. Das Ablaufdatum wird gesetzt und nach Ablauf ist die Registrierung von IP Devices im DLS blockiert, bis die überzähligen IP Devices vom Administrator gelöscht sind.

Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V6 Mobile User Lizenz

Anzahl Lizenzen

Zeigt die Anzahl der Mobile User, die mit der vorhandenen Lizenz eingerichtet werden können.

Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf dieser Frist ist die Administration mit DLS nicht mehr möglich. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

Anzahl Mobile User

Zeigt die Anzahl der bereits verwendeten Mobile User Lizenzen für Mobile User an.

Verwendet (%)

Zeigt an, wie viel Prozent der vorhandenen Lizenzen bereits verwendet sind.

Alarmschwelle (%)

Legen Sie fest, ab welchem Prozentsatz an verwendeten Lizenzen ein Lizenzalarm generiert werden soll.

eingeschränkter Betrieb wegen Lizenzüberschreitung

Ist aktiviert, wenn eine Lizenzüberschreitung vorliegt. In diesem Fall ist nur noch das Löschen überzähliger Mobile User möglich.

Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V7 PKI User Lizenz

HINWEIS: Falls Mandantenfähigkeit eingerichtet ist, müssen die vorhandenen V7 Basic Device Lizenzen pro Mandant eingerichtet werden, wie unter Abschnitt 6.3.1, “Mandanten” beschrieben.

Anzahl Lizenzen:

Zeigt die Anzahl der IP Devices mit PKI Service, die mit der vorhandenen Lizenz eingerichtet werden können.

Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf dieser Frist steht der PKI Service für IP Devices mit DLS nicht mehr zur Verfügung. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

Anzahl Devices

Zeigt die Anzahl der bereits verwendeten PKI User Lizenzen für IP Devices an.

Verwendet (%)

Zeigt an, wie viel Prozent der vorhandenen Lizenzen bereits verwendet sind.

Alarmschwelle (%)

Legen Sie fest, ab welchem Prozentsatz an verwendeten Lizenzen ein Lizenzalarm generiert werden soll.

eingeschränkter Betrieb wegen Lizenzüberschreitung

Ist aktiviert, wenn eine Lizenzüberschreitung vorliegt. Nach Ablauf der Frist steht der PKI Service für IP Devices mit DLS nicht mehr zur Verfügung. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V7 Location Service Lizenz

HINWEIS: Diese Lizenz ist für die Nutzung der Funktion ‘Open Communications Solution for Location and Identity Assurance’ (OCS LIA) erforderlich.

Anzahl Lizenzen

Zeigt die Anzahl der Lizenzen für Location Service (IP Infrastruktur) an.

Anzahl Devices

Anzahl an IP Devices, die vom Location Service mit IP Infrastrukturdaten versorgt werden.

Verwendet (%)

Zeigt an, wie viel Prozent der vorhandenen Lizenzen bereits verwendet werden.

Alarmschwelle (%)

Legen Sie fest, ab welchem Prozentsatz an verwendeten Lizenzen ein Lizenzalarm generiert werden soll.

Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Dies ist z.B. der Fall, wenn der CLA (Lizenzagent) nicht oder nicht mehr erreichbar ist. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf des Ablaufdatums können die IP Devices nicht mehr mit IP Infrastrukturdaten versorgt werden, wobei der Notruf ausgenommen ist. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

Übergangslizenz

Ist markiert, wenn der CLA nicht erreichbar ist. In diesem Fall werden die zuletzt ermittelten Lizenzen verwendet. Wenn noch keine Verbindung zum CLA hergestellt wurde, ist für die Zeitdauer der Übergangslizenz eine (1) DLS-Knoten-Lizenz verfügbar. Der DLS versucht, den CLA alle 45 Minuten zu kontaktieren. Nach Erreichen des Ablaufdatums können die IP Devices nicht mehr mit IP Infrastrukturdaten versorgt werden. Eine Ausnahme hierzu bilden Notrufe. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

eingeschränkter Betrieb wegen Lizenzüberschreitung

Ist aktiviert, wenn eine Lizenzüberschreitung vorliegt. In diesem Fall ist nur noch das Löschen überzähliger IP Devices möglich.

Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V7 Knoten Lizenz

Anzahl Lizenzen

Gibt die Anzahl der im Lizenzagenten verfügbaren Lizenzen für DLS V7-Knoten an.

> ***HINWEIS:*** Dies sind die im CLA verfügbaren (d. h. geladenen und aktivierten) Lizenzen, nicht die vom DLS benötigten und verwendeten.

Anzahl DLS Knoten:

Zeigt an, wieviele zusätzliche DLS-Knoten im Cluster aktiv sind. Bei Single-Node-Betrieb ist hier 0 eingetragen. Dies ist die Anzahl der benötigten Knoten-Lizenzen.
Für einen Multi-Node-DLS mit n Knoten werden n-1 Knoten-Lizenzen benötigt.

Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf des Ablaufdatums ist nur noch Single Node-Betrieb möglich. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V7 Datenbankspiegelung Lizenz

Lizenz vorhanden

Zeigt an, ob eine Lizenz für Datenbankspiegelung vorhanden ist.

Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf des Ablaufdatums erfolgt keine Datenbankspiegelung mehr. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

eingeschränkter Betrieb wegen Lizenzüberschreitung

Ist aktiviert, wenn eine Lizenzüberschreitung vorliegt. In diesem Fall erfolgt keine Datenbankspiegelung.

Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

DLS V7 XML Push Lizenz

Lizenz vorhanden

XML Push kann nur mit einer gültigen Lizenz verwendet werden.

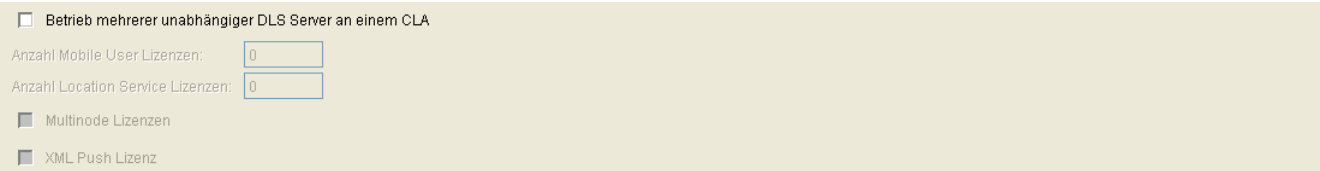
Ablaufdatum

Ein Ablaufdatum wird angezeigt, wenn mit einer Übergangslizenz gearbeitet wird. Eine über den CLA (Lizenzagent) gewährte Lizenz ist zeitlich nicht begrenzt.

Nach Ablauf des Ablaufdatums stehen die XML Push Masken nicht mehr zur Verfügung. Nehmen Sie bitte sofort Kontakt zum Lizenzadministrator auf.

6.15.2 Register „Betrieb mehrerer DLS Server“

Aufruf: Hauptmenü > Administration > Server Lizenzen > Register „Betrieb mehrerer DLS Server“



Betrieb mehrerer unabhängiger DLS Server an einem CLA

Wenn aktiviert, können die Basic Device- und Mobile User-Lizenzen mehrerer voneinander unabhängiger DLS-Server an einem zentralen Lizenzagenten (CLA) verwaltet werden.

Anzahl Mobile User Lizenzen

Maximale Anzahl von Mobile User Lizenzen, die dieser DLS am zentralen Lizenzagenten (CLA) anfordern soll.

Anzahl Location Service Lizenzen

Maximale Anzahl von Location Service-Lizenzen, die dieser DLS am zentralen Lizenzagenten (CLA) anfordern soll.

Multi-Node Lizenzen

Wenn aktiviert, werden Lizenzen für DLS-Knoten und Datenbankspiegelung vom zentralen Lizenzagenten (CLA) angefordert.

XML Push Lizenz

Wenn aktiviert, wird eine Lizenz für XML Push vom zentralen Lizenzagenten (CLA) angefordert.

7 IP Devices

Aufruf: Hauptmenü > IP Devices

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- IP Phone Konfiguration
- IP Client Konfiguration
- IP Gateway Konfiguration
- IP Device Interaktion
- IP Device Verwaltung

Nutzen Sie diesen Bereich, um die Konfigurationsdaten von IP Devices anzuzeigen und zu ändern.

HINWEIS: Werden Änderungen in Datensätzen vorgenommen, die mithilfe von Templates erstellt wurden, so werden diese Änderungen nicht automatisch in diese Templates übernommen.
Zum Übernehmen müssen die Änderungen manuell im Template gesichert werden, siehe Abschnitt 15.4, “Templates bearbeiten”.

HINWEIS: Im Bereich **IP Client Konfiguration** können für jeden IP Client sowohl Parameter für SIP als auch für HFA eingetragen sein.

HINWEIS: Ein IP Device kann erst nach dessen erfolgreicher Registrierung am DLS konfiguriert werden. Zur Registrierung muss dem IP Device die entsprechende DLS-Adresse bekannt sein. Die Registrierung beim DLS erfolgt durch:
- Auslesen der IP Device-Daten durch den DLS, siehe Abschnitt 7.4.6, “IP Devices scannen” und durch
- Einstecken des LAN-Steckers bzw. der Stromversorgung am IP Device.

7.1 IP Phone Konfiguration

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration

Dieses Menü besteht aus folgenden Untermenüs:

- Gateway / Server
- IP Routing
- Ports
- Features
- Quality of Service
- QoS Data Collection
- Security Einstellungen
- Telefonie
- Small Remote Site Redundancy
- Wahlparameter
- Uhrzeit Einstellungen
- Audio Einstellungen
- SNMP Einstellungen
- Applikationen
- LDAP
- Anwendereinstellungen
- SIP Mobility
- HFA Mobility
- Keysets / Tastenbelegung
- WLAN Einstellungen
- Signaling and Payload Encryption (SPE)
- IEEE 802.1x
- Diagnose
- Sonstiges
- File Deployment

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Phones zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Phones angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).

HINWEIS: Bei der Ansicht **Suche** werden nur die Attribute der aktuell für die ausgewählten Geräte angezeigten Maske aufgelistet und nicht die Attribute aller Masken unter **IP Phone Konfiguration** für diese Geräte wie bei früheren DLS/Telefon-Versionen.
Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des IP Phones. Für OpenStage wird hier entweder eine IPv4- oder eine IPv6-Adresse angezeigt. Siehe auch die Beschreibung zum Parameter **IP Protokoll Modus**.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device. In der Regel ist das die MAC-Adresse.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Phones. Das Icon zeigt an, ob es sich um einen virtuelles Gerät handelt.

Alle vom DLS unterstützte IP Phone-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **optiPoint 410 standard**

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

Nur für OpenStage verfügbar.

SW Version:

Software-Version des IP Phones.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des IP Phones.

Beispiele: **Unify HFA**, **Unify SIP**

Reg-Adresse

IP-Adresse oder DNS-Name des SIP- oder HFA-Servers, bei dem das Gerät angemeldet ist.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Phones.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Inhaltsbereich”.

Bemerkungen:

Felder für allgemeine Informationen.

IP Protokoll Modus

Zeigt an, welche IP-Version das IP Phone verwendet. Werden beide Versionen verwendet, steht in **IP Adresse** die IPv4-Adresse und in **IP Adresse 2** die IPv6-Adresse.

Nur für OpenStage verfügbar.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Standort

Aktueller Standort des IP Device. der bei der Registrierung ermittelt und hier angezeigt wird. (Zur Bedeutung und Konfiguration des Standorts siehe Abschnitt 6.3.2, “Standort”.)

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Phones, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Holen

Lädt ein bereits gesichertes Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Sichern

Sichert Konfigurations-Einträge als Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Verwerfen

Verwirft die Änderungen und neuen Einträge.

Lesen

Die auf der Maske dargestellten Parameter werden neu vom IP Device eingelesen.

Umbenennen

Ändert den Namen eines gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Löschen

Löscht ein gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Zertifikat importieren

Importiert ein Zertifikat für das gewählte IP Device (nur in der Zertifikatsverwaltung verfügbar). Siehe hierzu Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Zertifikat entfernen

Entfernt ein Zertifikat für das gewählte IP Device (nur in der Zertifikatsverwaltung verfügbar). Siehe hierzu Abschnitt 16.12, “Security: Administration von Zertifikaten”.

7.1.1 Gateway / Server

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server

Dieser Bereich besteht aus folgenden Inhalten:

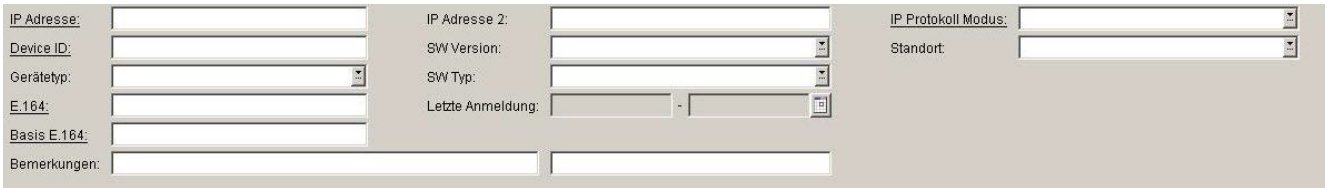
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Gateway (HFA) / SIP Server“
- Register „Gateway (Standby)“
- Register „SIP Terminaleinstellungen“
- Register „SIP Registrierung 1“
- Register „SIP Registrierung 2“
- Register „SIP Survivability“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Phones zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Phones angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des IP Phones. Für OpenStage wird hier entweder eine IPv4- oder eine IPv6-Adresse angezeigt. Siehe auch die Beschreibung zum Parameter **IP Protokoll Modus**.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device. In der Regel ist das die MAC-Adresse.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Phones.

Alle vom DLS unterstützte IP Phone-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **optiPoint 410 standard**

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

Nur für OpenStage verfügbar.

SW Version:

Software-Version des IP Phones.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des IP Phones.

Beispiele: **Unify HFA**, **Unify SIP**

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Phones.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Inhaltsbereich”.

Bemerkungen:

Felder für allgemeine Informationen.

IP Protokoll Modus

Zeigt an, welche IP-Version das IP Phone verwendet. Werden beide Versionen verwendet, steht in IP Adresse die IPv4-Adresse und in IP Adresse 2 die IPv6-Adresse.

Nur für OpenStage verfügbar.

Mögliche Optionen:

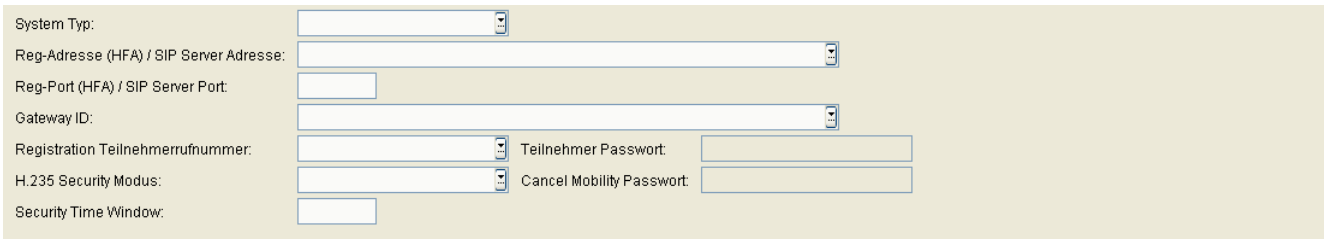
- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Standort

Aktueller Standort des IP Device. der bei der Registrierung ermittelt und hier angezeigt wird. (Zur Bedeutung und Konfiguration des Standorts siehe Abschnitt 6.3.2, “Standort”.)

7.1.1.1 Register „Gateway (HFA) / SIP Server“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server > Register „Gateway (HFA) / SIP Server“



System Typ:

Art und Version der Kommunikationsplattform, an der der Workpoint betrieben wird.

Mögliche Optionen:

- **Unbekannt**
- **HiPath 3000 generic**
- **HiPath 3000 V4.0**
- **HiPath 3000 V5.0**
- **HiPath 3000 V6.0**
- **HiPath 3000 V7.0**
- **HiPath 3000 V8.0**
- **HiPath 3000 V9.0**
- **HiPath 4000 generic**
- **HiPath 4000 V1.0**
- **HiPath 4000 V2.0**
- **HiPath 4000 V3.0**
- **HiPath 4000 V4.0**
- **HiPath 4000 V5.0**
- **HiPath 4000 V6.0**
- **HiPath 4000 V7.0**

Nur bei HFA-Workpoints verfügbar.

Reg-Adresse (HFA) / SIP Server Adresse:

IP-Adresse oder Host-Name des Gateways oder SIP-Servers, der zum Betrieb des Workpoints eingesetzt wird.

Reg-Port (HFA) / SIP Server Port:

Port, über den der Workpoint mit dem PBX, Gateway bzw. SIP-Server kommuniziert.

Gatekeeper ID:

ID von PBX, Gateway bzw. Gatekeeper, der zum Betrieb des Workpoints eingesetzt wird.

HINWEIS: Die Gateway ID entspricht dem Parameter **„**Globid**“** im AMO HFAB für HiPath 4000 bzw. der H.323 ID bei HiPath 3000.

Registration Teilnehmerrufnummer:

Rufnummer des Teilnehmers an der PBX.

Beispiel: **12345**

Nur bei HFA-Workpoints verfügbar.

H.235 Security Modus:

Mögliche Optionen:

- **Keine**
  Ohne Sprachverschlüsselung.
- **Vermindert**
  Mit einseitiger Sprachverschlüsselung (Gatekeeper sendet nicht verschlüsselt).
- **Voll**
  Mit beidseitiger Sprachverschlüsselung (Workpoint und Gatekeeper senden verschlüsselt).

Nur bei HFA-Workpoints verfügbar.

Security Time Window:

Gibt den höchstzulässigen Zeitunterschied zwischen den einzelnen Geräten an, die bei H.235 alle synchron laufen sollten.

Nur bei HFA-Workpoints verfügbar.

Teilnehmer Passwort:

Passwort des Workpoints an der PBX.

Nur bei HFA-Workpoints verfügbar.

Cancel Mobility Passwort:

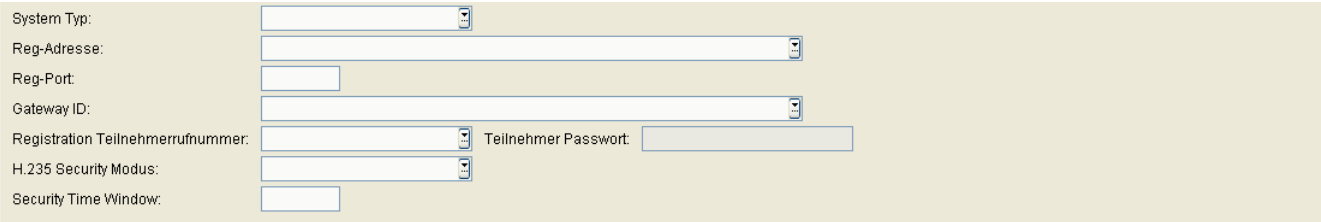
Passwort zum Aufheben der Mobility-Funktion am Home-Workpoint.

Nur bei HFA-Workpoints verfügbar.

7.1.1.2 Register „Gateway (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server > Register „Gateway (Standby)“

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „Gateway (HFA) / SIP Server“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.1.9, “Small Remote Site Redundancy”.



System Typ:

Art und Version der Kommunikationsplattform, an der der Workpoint betrieben wird.

Mögliche Optionen:

- **Unbekannt**
- **HiPath 3000 generic**
- **HiPath 3000 V4.0**
- **HiPath 3000 V5.0**
- **HiPath 3000 V6.0**
- **HiPath 3000 V7.0**
- **HiPath 3000 V8.0**
- **HiPath 3000 V9.0**
- **HiPath 4000 generic**
- **HiPath 4000 V1.0**
- **HiPath 4000 V2.0**
- **HiPath 4000 V3.0**
- **HiPath 4000 V4.0**
- **HiPath 4000 V5.0**
- **HiPath 4000 V6.0**
- **HiPath 4000 V7.0**

Nur bei HFA-Workpoints verfügbar.

Reg-Adresse:

IP-Adresse oder Host-Name von PBX bzw. Gateway, der als Standby für den Workpoint vorgesehen ist.

Reg-Port:

Portnummer von PBX bzw. Gateway, der als Standby für den Workpoint vorgesehen ist.

Gatekeeper ID:

ID von PBX, Gateway bzw. Gatekeeper, der als Standby für den Workpoint vorgesehen ist.

HINWEIS: Die Gateway ID entspricht dem Parameter „Globid“ im AMO HFAB für HiPath 4000 bzw. der H.323 ID bei HiPath 3000.

Registration Teilnehmerrufnummer:

Rufnummer des Teilnehmers an der PBX.

Beispiel: **12345**

Nur bei HFA-Workpoints verfügbar.

H.235 Security Modus:

Mögliche Optionen:

- **Keine**
  Ohne Sprachverschlüsselung.
- **Vermindert**
  Mit einseitiger Sprachverschlüsselung (Gatekeeper sendet nicht verschlüsselt).
- **Voll**
  Mit beidseitiger Sprachverschlüsselung (Workpoint und Gatekeeper senden verschlüsselt).

Nur bei HFA-Workpoints verfügbar.

Security Time Window:

Gibt den höchstzulässigen Zeitunterschied zwischen den einzelnen Geräten an, die bei H.235 alle synchron laufen sollten.

Nur bei HFA-Workpoints verfügbar.

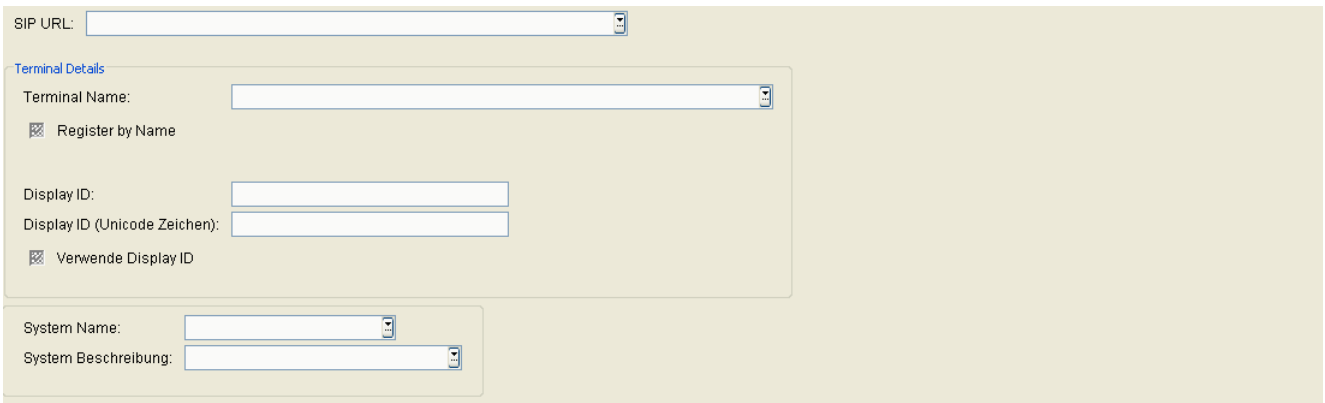
Teilnehmer Passwort:

Passwort des Workpoints an der Standby-PBX.

Nur bei HFA-Workpoints verfügbar.

7.1.1.3 Register „SIP Terminaleinstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server > Register „SIP Terminaleinstellungen“



SIP URL:

SIP-Adresse des IP Phones.

Format: **<SIP Benutzerkennung>@<Domain>**.

Terminal Details

Terminal Name:

Name des IP Phones, der als Synonym für die Rufnummer beim Registrieren verwendet wird.

Nur erforderlich, wenn der Schalter **Register by Name** aktiviert und der Registrar-Server entsprechend konfiguriert ist.

Register by Name

Ist der Schalter aktiviert, registriert sich das Telefon unter dem **Terminal Name**.

Display ID:

Name des IP Phones, das im Display des Telefons angezeigt wird.

Wertebereich: max. 24 alphanummerische Zeichen.

Display ID (Unicode Zeichen):

Name des IP Phones, das im Display des Telefons angezeigt wird, im Unicode-Zeichensatz.

HINWEIS: Unicode steht nur in der OpenStage-Familie zur Verfügung.

Wertebereich: max. 24 alphanummerische Zeichen.

Verwende Display ID

Ist dieser Schalter aktiviert, so wird die Display ID in der Statuszeile des Endgeräts angezeigt.

System Name:

Beliebiger Name, der in der unteren rechten Ecke des IP Phone-Displays erscheint (bei 2-zeiligem Display).

Beispiel: **HiPath**

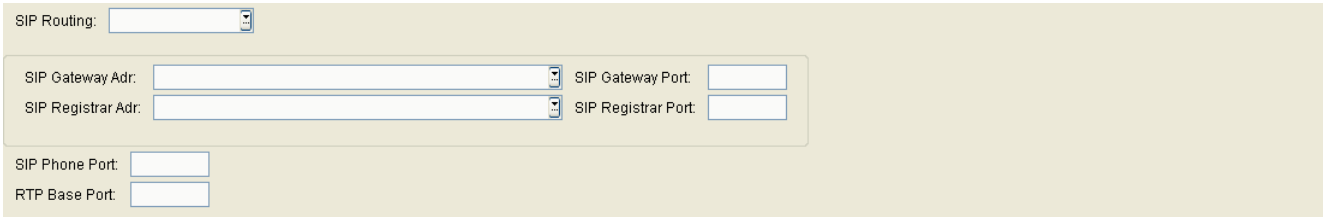
Wertebereich: max. 10 alpha-nummerische Zeichen.

System Beschreibung:

Wird benutzt, um am Workpoint eine Systembeschreibung anzuzeigen (bei 3- bzw. 4-zeiligem Display).

7.1.1.4 Register „SIP Registrierung 1“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server > Register „SIP Registrierung 1“



SIP Routing:

Mögliche Optionen:

- **Direkt**
  Nur für Testzwecke.
- **Gateway**
  Wenn ein Gateway verwendet wird.
- **Server**
  Wenn ein SIP-Proxy verwendet wird.

Wird Direkt oder Gateway gewählt, werden beim Registrieren keine Registrier-Meldungen gesendet. Beim Routing-Modus **Server** werden Registrierungs-Meldungen an den Registrar-Server gesendet.

SIP Gateway Adr:

IP-Adresse des SIP-Gateways, falls der Routing-Modus **Gateway** verwendet wird.

SIP Gateway Port:

Port-Nummer des SIP-Gateways, falls der Routing-Modus **Gateway** verwendet wird.

SIP Registrar Adr:

IP-Adresse des SIP-Registrars.

SIP Registrar Port:

Port-Nummer des SIP-Registrars.

SIP Phone Port:

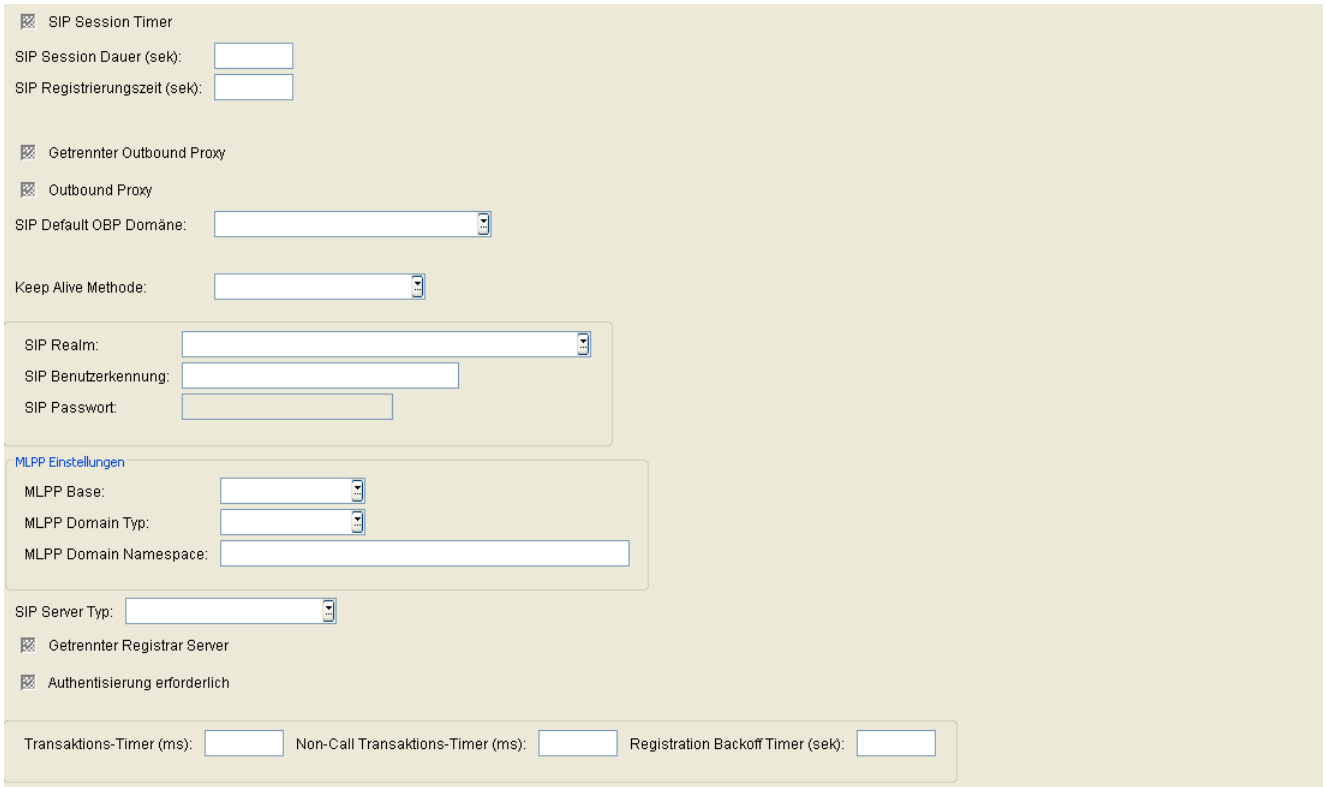
Port-Nummer des IP Phones.

RTP Base Port:

Basis Port-Nummer für den RTP-Transport.

7.1.1.5 Register „SIP Registrierung 2“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server > Register „SIP Registrierung 2“



SIP Session Timer

Schalter zum Aktivieren des SIP Session Timers. Mit dem Timer wird die Dauer einer SIP-Session überwacht.

SIP Session Dauer:

Höchstdauer in Sekunden für eine SIP-Session.

Wertebereich: **0** ... **3600** Sekunden.

SIP Registrierungszeit (sek):

Zeitspanne bis zu einer Wiederanmeldung am SIP-Server. Eine Wiederanmeldung stellt sicher, dass das SIP-Telefon weiterhin am SIP-Server angemeldet bleibt. Dadurch können auch Probleme bei der Verbindung zum Server festgestellt werden.

Wertebereich: **0** ... **4320** Sekunden.

Standard: **0**

Getrennter Outbound Proxy

Wenn aktiviert, wird ein getrennter Outbound Proxy verwendet. Dieser Parameter wird bei optiPoint WL2-Telefonen verwendet, um einen Outbound Proxy anzugeben, der nicht mit dem SIP Proxy identisch ist.

Outbound Proxy

Schalter zum Aktivieren eines SIP-Proxy bei ausgehenden Gesprächen.

Zusammen mit **SIP Default OBP Domäne** steuert dieser Schalter das Routing-Verhalten ausgehender Gespräche, abhängig von der gewählten Nummer oder Benutzerkennung.

Siehe hierzu Kapitel 17, “Outbound Proxy”.

SIP Default OBP Domäne:

Zusammen mit **Outbound Proxy** steuert dieser Eintrag das Routing-Verhalten ausgehender Gespräche, abhängig von der gewählten Nummer oder Benutzerkennung.

Siehe hierzu Kapitel 17, “Outbound Proxy”.

Keep Alive Methode:

Auswahl der Keep Alive-Methode für die Verbindung zwischen und Switch.

Mögliche Optionen:

- **Sequenz**
- **CRLF**

SIP Realm:

Namensraum, innerhalb dessen Benutzerkennung und Passwort gültig sind. Dieser SIP Realm muss auch auf der Anlage bzw. auf dem SIP-Server eingetragen sein.

SIP Benutzerkennung:

Die Benutzerkennung ist der erste Teil der SIP URL. Sie ist zusammen mit dem Passwort erforderlich für den Zugang zum SIP-Server.

SIP Passwort:

Zur Benutzerkennung gehöriges Passwort für den Zugang zum SIP-Server.

MLPP Einstellungen

MLPP Base:

Mögliche Optionen:

- **Lokal**
- **Server**

MLPP Domain Typ

Legt fest, welcher Resource Priority Namespace von einer festen Liste akzeptiert wird.

Mögliche Optionen:

- **dsn**
  dsn-000000
- **uc**
  uc-000000
- **dsn+uc**
- **Andere Domain**

MLPP Domain Namespace

Definiert einen ASCII String für einen Single Resource Priority Namespace, der akzeptiert wird.

Erlaubt sind alphanumerische Zeichen und folgende Sonderzeichen: -!%*_+` “~

Ein ‘.’ ist nicht erlaubt.

SIP Server Typ:

Auswahl des geeigneten SIP-Server-Typs.

Mögliche Optionen:

- **Broadsoft**

- **OpenScape Voice**
- **Sylantro**
- **Andere**
- **HiQ 8000**
- **Genesys**

Getrennter Registrar Server

Melden Sie sich am WLAN an, sind Sie unter Ihrer persönlichen Nummer erreichbar. Die Zuordnung der SIP-URI bzw. IP-Adresse, unter der Sie aktuell angemeldet sind, zu Ihrer persönlichen Nummer erfolgt durch einen Registrar. Es besteht die Möglichkeit, dass Ihr SIP-Provider einen getrennten Registrar-Server zur Verfügung stellt.

Aktivieren Sie den Schalter, wenn die Registrierung auf einem getrennten Registrar-Proxy-Server erfolgt. Es werden die Eingabefelder eingeblendet, in denen Sie die Server-Adresse und die Port-Nummer des Registrar-Proxy-Servers eingeben können.

Gilt nur für WLAN Phones.

Authentisierung erforderlich

Aktivieren Sie den Schalter, wenn zur Anmeldung beim SIP-Provider zusätzlich zu den regulären Zugangsdaten die von Ihnen festgelegte **SIP Benutzerkennung** angegeben werden muss.

Gilt nur für WLAN Phones.

Transaktions-Timer (ms)

Zeitdauer in Millisekunden, die das Gerät auf eine angeforderte SIP-Nachricht wartet, bevor der Server als nicht erreichbar eingestuft wird.

Non-Call Transaktions-Timer (ms)

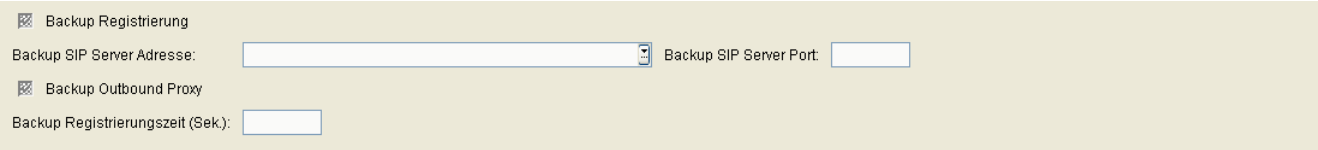
Zeitdauer in Millisekunden, die das Gerät auf eine auf non-INVITE (nonCall) basierende Nachrichten wartet (F timer).

Registration Backoff Timer (sek)

Zeitdauer in Sekunden bis zum nächsten Registrierungsversuch nach einer fehlgeschlagenen Registrierung.

7.1.1.6 Register „SIP Survivability“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway / Server > Register „SIP Survivability“



Backup Registrierung

Schalter zum Aktivieren der Backup Registrierung.

Backup SIP Server Adresse:

IP-Adresse oder Hostname des Backup SIP-Servers.

Backup SIP Server Port:

Port-Nummer zur Kommunikation mit dem Backup SIP-Server.

Backup Outbound Proxy

Schalter zum Aktivieren des Backup SIP-Proxy bei ausgehenden Gesprächen.

Siehe hierzu Kapitel 17, “Outbound Proxy”.

Backup Registrierungszeit (sek):

Zeitspanne bis zu einer Wiederanmeldung am Backup SIP-Server. Eine Wiederanmeldung stellt sicher, dass das SIP-Telefon weiterhin am Backup SIP-Server angemeldet bleibt. Dadurch können auch Probleme bei der Verbindung zum Server festgestellt werden.

Voraussetzung: Es wird ein Backup SIP-Server verwendet.

Wertebereich: **0** ... **4320** Sekunden.

Standard: **0**

7.1.2 IP Routing

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IP Routing

Dieser Bereich besteht aus folgenden Inhalten:

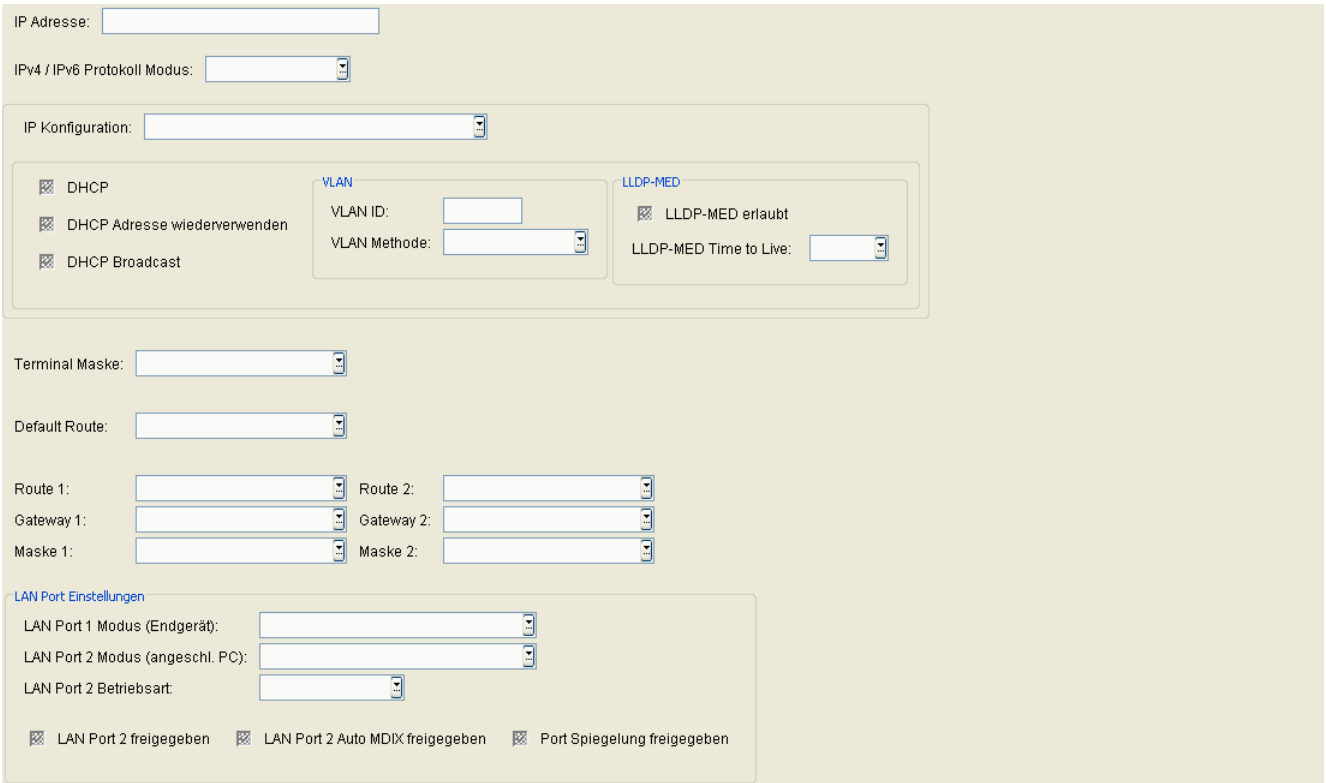
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „IP Routing“
- Register „IPv6 Einstellungen“
- Register „ANAT Einstellungen“
- Register „DNS Server“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.2.1 Register „IP Routing“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IP Routing > Register „IP Routing“



IP Adresse

IP-Adresse des IP Phones.

IPv4 / IPv6 Prokoll Modus

Auswahl des Internet-Protokolls, das vom IP Phone benutzt wird.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

IP Konfiguration

Legt fest, auf welche Weise die IP-Einstellungen konfiguriert werden; gültig ab OpenStage Version 1.5. Bei Versionen < 1.5 ist dieses Feld wie auch die restlichen LLDP-MED Parameter ausgegraut.

HINWEIS: Zu beachten ist, dass sich das Schreiben und das Lesen dieses Parameters unterschiedlich verhalten. Trifft der DLS-Benutzer eine bestimmte Auswahl (z. B. „LLDP-MED mit DHCP Konfiguration“), so werden die IP-Konfigurationsparameter entsprechend gesetzt und zum Endgerät geschickt. Beim Lesen vom Gerät hingegen wird stets der Wert „Bitte eine Option für IP-Konfiguration auswählen“ angezeigt. Dies geht darauf zurück, dass die Parameter möglicherweise nicht eindeutig ermittelt werden konnten; beispielsweise kann der Wert des Parameters **VLAN Methode** davon abhängen, ob die VLAN ID über DHCP oder über LLDP-MED festgelegt wurde.

Das Feld ist mit dem Wert „Bitte eine Option für IP-Konfiguration auswählen“ vorbelegt.

Mögliche Werte:

- **LLDP-MED mit DHCP Konfiguration**
- **DHCP Konfiguration**
- **VLAN manuell mit DHCP Konfiguration**
- **Manuelle Einstellungen**

DHCP

Dieser Schalter kann aktiviert werden, wenn ein DHCP-Server verfügbar ist. Das IP Device bezieht dann die IP-Adressdaten dynamisch vom DHCP-Server.

Ist kein DHCP-Server vorhanden, darf der Schalter nicht aktiviert werden. Stattdessen müssen für dieses IP Device die IP-Adressdaten (**IP Adresse**, **Terminal Maske** und **Default Route**) manuell festgelegt werden.

DHCP lease wiederverwenden

Dieser Schalter kann aktiviert werden, wenn ein DHCP-Server verfügbar ist. Ist der Schalter aktiviert, wird die vom DHCP zuletzt vergebene Adresse wiederverwendet.

DHCP Broadcast

Dieser Schalter kann aktiviert werden, wenn ein DHCP-Server verfügbar ist. Durch diesen Schalter wird das DHCP-Protokollelement ‘flags’ geändert. Ist der Schalter aktiviert, beantwortet der DHCP-Server die Requests des IP Devices mit ‘broadcast’, andernfalls mit ‘unicast’.

VLAN

VLAN ID:

VLAN ID beim Einsatz von Virtual LANs. Nur änderbar, wenn QoS Layer 2 aktiviert ist. Wurde der Wert per DHCP oder LLDP-MED vergeben, kann er nur gelesen werden.

Wertebereich: **0** ... **4095**.

VLAN Methode:

Legt fest, wie die VLAN ID dem Endgerät zugewiesen wird. Nur änderbar, wenn QoS Layer 2 aktiviert ist.

Mögliche Optionen:

- **Manuell**
  Die VLAN ID wir manuell eingetragen.
- **DHCP**
  Es wird die vom DHCP-Server gelieferte VLAN ID verwendet.
- **Keine**
  (Nur für WLAN)
- **LLDP-MED**
  Es wird die durch LLDP-MED (Link Layer Discovery Protocol – Media Endpoint Discovery) gelieferte VLAN ID verwendet. Verfügbar für OpenStage ab V1R5.

LLDP-MED

LLDP-MED erlaubt:

Erlaubt das Senden und Empfangen von LLDP-Daten.

LLDP-MED Time-to-Live

Mögliche Werte:

- **40**
- **60**
- **80**
- **100**
- **110**
- **120**

- **140**
- **180**
- **240**
- **320**
- **400**

Terminal Maske:

Subnet-Maske der IP-Adresse.

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Default Route:

IP-Adresse oder Hostname des Standard-Routers/Gateways.

Wurde der Wert per DHCP vergeben, kann er nur gelesen werden.

Route 1:

IP-Adresse oder Hostname der ersten statischen Route (optional).

Gateway 1:

IP-Adresse oder Hostname des Routers/Gateways der ersten statischen Route (optional).

Maske 1:

Subnetz-Maske der ersten statischen Route (optional).

Route 2:

IP-Adresse oder Hostname der zweiten statischen Route (optional).

Gateway 2:

IP-Adresse oder Hostname des Routers/Gateways der zweiten statischen Route (optional).

Maske 2:

Subnetz-Maske der zweiten statischen Route (optional).

LAN Port Einstellungen

LAN Port 1 Modus (Endgerät):

Modus der Datenrate für den ersten Ethernet-Port des IP Phones. Der erste Port wird an das LAN angeschlossen. Der Wert für die Datenrate ist davon abhängig, welche Bandbreite der angeschlossene Switch bzw. Router im Netzwerk unterstützt.

Mögliche Optionen:

- **10 Mbit/s Halb-Duplex**
- **10 Mbit/s Voll-Duplex**
- **100 Mbit/s Halb-Duplex**
- **100 Mbit/s Voll-Duplex**
- **Auto**

Standard: **Auto**

LAN Port 2 Modus (angeschl. PC):

Modus der Datenrate für den zweiten LAN-Port des IP Phones. Der Wert ist davon abhängig, welche Bandbreite der Switch bzw. Router im Netzwerk unterstützt.

Mögliche Optionen:

- **10 Mbit/s Halb-Duplex**
- **10 Mbit/s Voll-Duplex**
- **100 Mbit/s Halb-Duplex**
- **100 Mbit/s Voll-Duplex**
- **Auto**

Standard: **Auto**

LAN Port 2 Betriebsart

Auswahl zwischen den 3 Betriebsarten des PC-Ports.

Mögliche Optionen:

- **Gesperrt**
  Der LAN-Port ist inaktiv.
- **Freigegeben**
  Der LAN-Port ist aktiv.
- **Gespiegelt**
  Der gesamte Datenverkehr am LAN-Port 1 wird zum Port 2 gespiegelt.

LAN Port 2 freigegeben

Schalter zum Freigeben des LAN Port 2.

LAN Port 2 Auto MDIX freigegeben

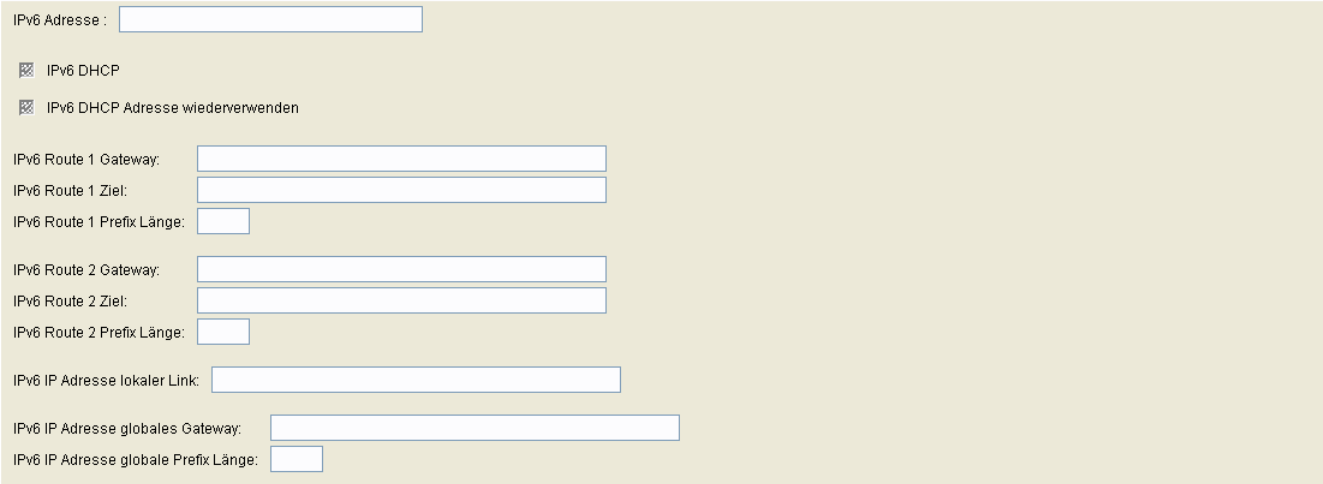
Schalter zum Freigeben des LAN Port 2 Auto MDIX. Ist Auto MDIX freigegeben, schaltet der LAN-Port automatisch zwischen normalem MDI und MDI-X (Crossover-Beschaltung) um.

Port Spiegelung freigegeben

Wenn der Schalter aktiviert ist, wird die Spiegelung des gesamten Datenverkehrs am LAN-Port 1 zum Port 2 erlaubt. Hierzu muss auch die **LAN Port 2 Betriebsart** auf **Gespiegelt** gesetzt sein.

7.1.2.2 Register „IPv6 Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IP Routing > Register „IPv6 Einstellungen“



IPv6 Adresse

IPv6-Adresse des IP Phones.

IPv6 DHCP

IPv6 DHCP

IPv6 DHCP Adresse wiederverwenden

Wenn aktiviert, wird die vom IPv6 DHCP-Server vergebene Adresse wiederverwendet.

IPv6 Route 1 Gateway

IPv6-Adresse des Routers/Gateways für die erste statische Route.

IPv6 Route 1 Ziel

Zieladresse für die erste statische Route.

IPv6 Route 1 Prefix Länge

Länge des Präfixes für die erste statische Route.

IPv6 Route 2 Gateway

IPv6-Adresse des Routers/Gateways für die zweite statische Route.

IPv6 Route 2 Ziel

Zieladresse für die zweite statische Route.

IPv6 Route 2 Prefix Länge

Länge des Präfixes für die zweite statische Route.

IPv6 IP Adresse lokaler Link

Link-local-Adresse.

IPv6 IP Adresse globales Gateway

IPv6-Adresse des globalen Gateways.

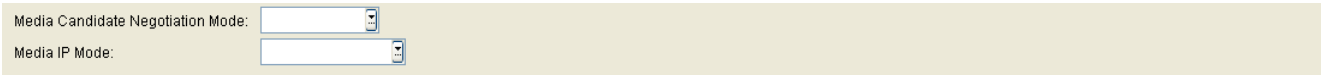
IPv6 IP Adresse globale Prefix Länge

Länge des globalen Präfixes.

7.1.2.3 Register „ANAT Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IP Routing > Register „ANAT Einstellungen“

ANAT (Alternative Network Adress Type) unterstützt einen Mechanismus zu IPv4/IPv6 Media Negotiation auf Media Stream Basis.



Media Candidate Negotiation Mode

Auswahl des Media Candidate Negotiation Mode.

Mögliche Optionen:

- **Single IP**
- **ANAT**

Media IP Mode

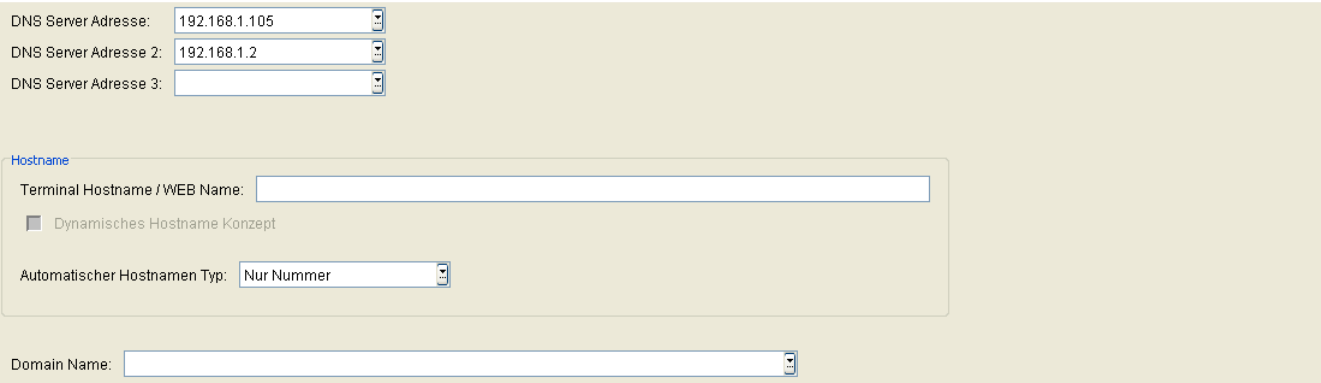
Auswahl des Media IP Mode.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 / IPv6**
- **IPv6 / IPv4**

7.1.2.4 Register „DNS Server“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IP Routing > Register „DNS Server“



DNS Server Adresse:

IP-Adresse oder Hostname des DNS-Servers.

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

DNS Server Adresse 2:

IP-Adresse oder Hostname des 2. DNS-Servers (optional).

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Bei optiPoint 400 nicht verfügbar.

DNS Server Adresse 3:

IP-Adresse oder Hostname des 3. DNS-Servers (optional).

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Bei optiPoint 400 nicht verfügbar.

Hostname

Terminal Hostname / WEB Name:

Host-Name des Terminals.

Erlaubte Zeichen: Buchstaben, Ziffern, Bindestrich, Unterstrich und Punkt; Groß-/Kleinschreibung wird unterschieden; maximale Länge: 63 Zeichen.

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Dynamisches Hostname Konzept

Ist der Schalter aktiviert, wird die E.164-Nummer als DNS-Hostname für das IP Phone verwendet.

Automatischer Hostname Typ:

Typ des automatisch generierten Hostnamen.

Mögliche Werte:

- **Kein DDNS Hostname (Kein Dynamischer DNS Hostname)**
- **Nur WEB Name**
- **Nur Nummer**
- **Prefix Nummer**
- **MAC basierend**

Domain Name:

Domain-Name des DNS-Servers.

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

7.1.3 Ports

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Ports

Dieser Bereich besteht aus folgenden Inhalten:

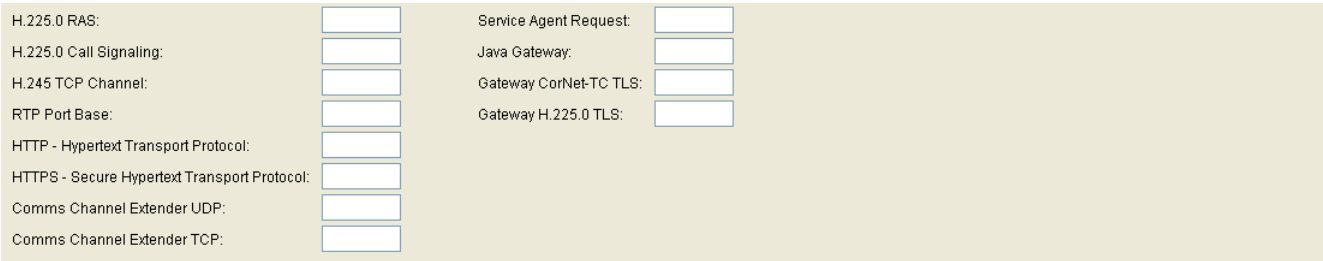
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Ports“
- Register „Ports (Standby)“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.3.1 Register „Ports“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Ports > Register „Ports“



H.225.0 RAS:

Port-Nummer für H.225 RAS.

Verwendung: Registrierung und Zulassung bei VoIP.

Zur Kommunikation mit folgenden Clients: Netmeeting, AP1120.

Verwendeter Port: **1719**

H.225.0 Call Signaling:

Port-Nummer für H.225 Call Signaling.

Verwendung: Verbindungssteuerung bei VoIP.

Zur Kommunikation mit folgenden Clients: HG1500, IP Phones, Netmeeting, AP1120.

Verwendeter Port: **1720**

H.245 TCP Channel:

Port-Nummer für H.245 TCP Channel.

RTP Port Base:

Port-Nummer für RTP.

Verwendung: Übertragung der Sprachpakete bei VoIP.

Zur Kommunikation mit folgenden Clients: HG1500, IP Phones, Netmeeting, AP11xx.

Verwendeter Portbereich: **29100** ... **29131**

HTTP – Hypertext Transport Protocol:

Port-Nummer für HTTP.

Verwendung: WEB based Management.

Zur Kommunikation mit folgenden Clients: WBM des Workpoints.

Verwendeter Port: **8085**

HTTPS – Secure Hypertext Transport Protocol:

Port-Nummer für HTTPS.

Verwendung: Web Based Management.

Zur Kommunikation mit folgenden Clients: WBM des Workpoints.

Nur bei SIP-Workpoints verfügbar.

Verwendeter Port: **443**

Comms Channel Extender UDP Port:

Verwendeter Portbereich: **0** ... **65535**

Standard: **65530**

Comms Channel Extender TCP Port:

Verwendeter Portbereich: **0** ... **65535**

Standard: **65531**

Service Agent Request:

Verwendeter Portbereich: **0** ... **65535**

Java Gateway:

Port-Nummer des von Java-Applikationen verwendeten Gateways.

Gateway CorNet-TC TLS

Nummer des Ports, den der HFA-Gateway für sichere Kommunikation mit dem Workpoint verwendet.

Portbereich: **0** .. **65535**

Standard: **4061**

Nur bei HFA-Workpoints verfügbar.

Gateway H.225.0 TLS

Nummer des Ports, der für sichere Signalisierung mit H.225 verwendet wird.

Portbereich: **0** .. **65535**

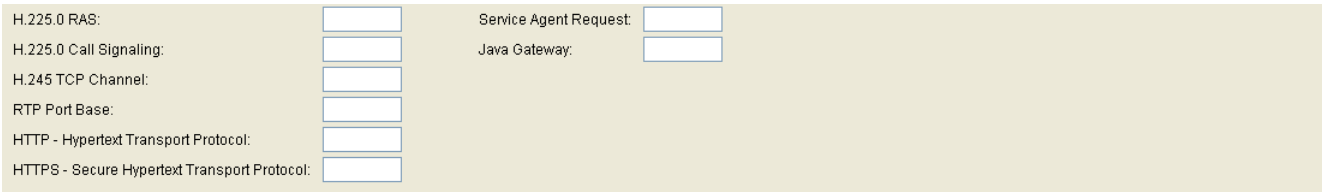
Standard: **1300**

Nur bei HFA-Workpoints verfügbar.

7.1.3.2 Register „Ports (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Ports > Register „Ports (Standby)“

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „Ports“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.1.9, “Small Remote Site Redundancy”.



H.225.0 RAS:

Port-Nummer für H.225 RAS.

Verwendung: Registrierung und Zulassung bei VoIP.

Zur Kommunikation mit folgenden Clients: Netmeeting, AP1120.

Verwendeter Port: **1719**

H.225.0 Call Signaling:

Port-Nummer für H.225 Call Signaling.

Verwendung: Verbindungssteuerung bei VoIP.

Zur Kommunikation mit folgenden Clients: HG1500, IP Phones, Netmeeting, AP1120.

Verwendeter Port: **1720**

H.245 TCP Channel:

Port-Nummer für H.245 TCP Channel.

Zur Kommunikation mit folgenden Clients:

RTP Port Base:

Port-Nummer für RTP.

Verwendung: Übertragung der Sprachpakete bei VoIP.

Zur Kommunikation mit folgenden Clients: HG1500, IP Phones, Netmeeting, AP11xx, MEB.

Verwendeter Portbereich: **29100** ... **29131**

HTTP – Hypertext Transport Protocol:

Port-Nummer für HTTP.

Verwendung: WEB based Management.

Zur Kommunikation mit folgenden Clients: WBM des Workpoints.

Verwendeter Port: **8085**

HTTPS – Secure Hypertext Transport Protocol:

Port-Nummer für HTTPS (HTTP mit SSL-Verschlüsselung).

Verwendung: WEB based Management.

Zur Kommunikation mit folgenden Clients: WBM des Workpoints.

Nur bei SIP-Workpoints verfügbar.

Verwendeter Port: **443**

Service Agent Request:

Port-Nummer für Service Agent Request.

Java Gateway:

Port-Nummer für Java Gatekeeper.

Gateway CorNet-TC TLS

Nummer des Ports, den der HFA-Gateway (Standby) für sichere Kommunikation mit dem Workpoint verwendet.

Portbereich: **0** .. **65535**

Standard: **4061**

Nur bei HFA-Workpoints verfügbar.

Gateway H.225.0 TLS

Nummer des Ports, der für sichere Signalisierung mit H.225 verwendet wird, wenn der Workpoint auf den Standby-Gateway umgeschaltet hat.

Nur bei HFA-Workpoints verfügbar.

7.1.4 Features

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features

Dieser Bereich besteht aus folgenden Inhalten:

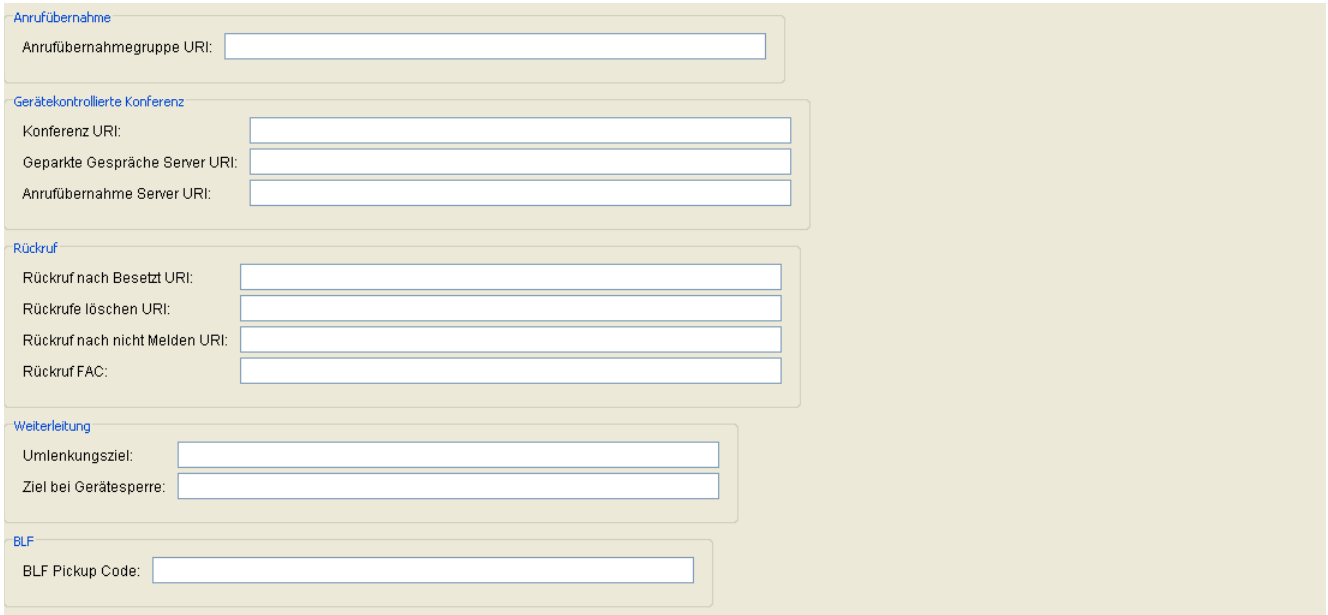
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Feature-Einstellungen 1“
- Register „Feature-Einstellungen 2“
- Register „Anrufbezogene Benutzer-Einstellungen“
- Register „Verfügbarkeit“
- Register „Server basierte Features“
- Register „Wählplan“
- Register „Signalisierungsmelodie / Ton“
- Register „Anrufumleitung“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.4.1 Register „Feature-Einstellungen 1“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Feature-Einstellungen 1“



Anrufübernahme

Anrufübernahmegruppe URI:

URI der Anrufübernahmegruppe.

Nur bei SIP-Workpoints verfügbar.

Gerätekontrollierte Konferenz

Konferenz URI:

URI zur Herstellung von Konferenz-Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Geparkte Gespräche Server URI:

URI des Servers zum Parken von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Anrufübernahme Server URI:

URI des Servers zur Anrufübernahme.

Nur bei SIP-Workpoints verfügbar.

Rückruf

Rückruf nach Besetzt URI:

URI des Servers, der das Leistungsmerkmal „Rückruf nach Besetzt“ steuert.

Nur für optiPoint und OpenStage bis V2 verfügbar.

Rückrufe löschen URI:

URI, die den Server veranlasst, die Rückrufwünsche zu löschen.

Rückruf nach nicht Melden URI:

URI des Servers, der das Leistungsmerkmal „Rückruf nach nicht Melden“ steuert.

Nur für optiPoint und OpenStage bis V2 verfügbar.

Rückruf FAC

URI, über die das Leistungsmerkmal „Rückruf“ gesteuert wird.

Nur bei OpenStage ab V3.0 verfügbar.

Weiterleitung

Umlenkungsziel

Ziel-Rufnummer für die Rufumleitung.

Ziel bei Gerätesperre:

Ziel-Rufnummer für Umleitung bei Ruf an gesperrtem Workpoint.

BLF

BLF Pickup Code:

Feature-Code für BLF Pickup mit Asterisk.

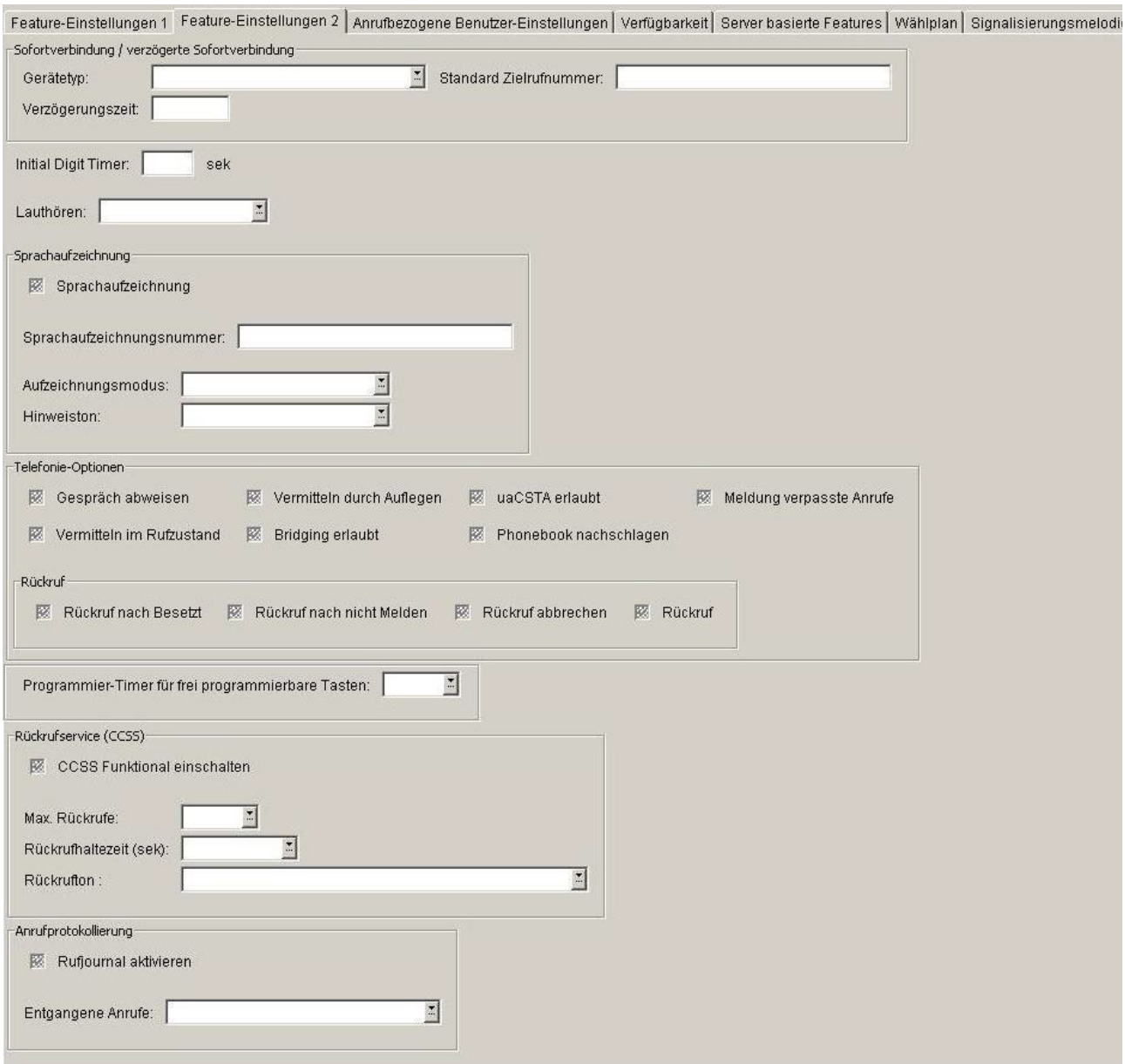
Nur bei SIP-Workpoints verfügbar.

7.1.4.2 Register „Feature-Einstellungen 2“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Feature-Einstellungen 2“

HINWEIS: Beim Betrieb von SIP-IP Phones an den Plattformen HiPath 3000 und HiPath 4000 bitte beachten, dass die folgenden Funktionen (Features) nicht verfügbar sind und deaktiviert werden müssen, damit sie für den Benutzer nicht sichtbar bzw. auswählbar sind:
- Auto. Rufannahme
- Rückruf nach Besetzt
- Auto. Wiederaufnahme
- Rückruf nach nicht Melden

Siehe auch Register „Verfügbarkeit“.



Sofortverbindung / verzögerte Sofortverbindung

Gerätetyp:

Geräteeigenschaft einstellen.

Mögliche Optionen:

- **Normal**
- **Sofortverbindungsaufbau (Hotline)**

- **verzögerter Sofortverbindungsaufbau (Warmline)**

Nur bei SIP-Workpoints verfügbar.

Standard Zielrufnummer:

Ziel-Rufnummer für Funktion „Hotline“ und „Warmline“.

Nur bei SIP-Workpoints verfügbar.

Verzögerungszeit:

Verzögerungszeit der Wahl in Sekunden für Funktion „Warmline“.

Für „Hotline“ (Notruf) ist als Zeit 0 einzutragen.

Nur bei SIP-Workpoints verfügbar.

Initial Digit Timer:

Wartezeit in Sekunden auf eine Wahlziffer, nachdem der Wählton angeschaltet wurde.

Nur bei SIP-Workpoints verfügbar.

Lauthören:

Konfiguriert das Wechseln in den Freisprech-Modus.

Mögliche Optionen:

- **Standard Mode**
  Um auf Freisprechen umzuschalten, muss der Benutzer die Lautsprechertaste gedrückt halten, während er den Hörer auflegt.
- **US Mode**
  Um auf Freisprechen umzuschalten, muss der Benutzer muss die Lautsprechertaste betätigen und danach den Hörer auflegen.

Sprachaufzeichnung

Das zentrales Sprachaufzeichnungsgerät nimmt das gesamte Gespräch von zwei oder mehreren Teilnehmern auf.

Sprachaufzeichnung

Schalter zum Aktivieren der Sprachaufzeichnung.

Sprachaufzeichnungsnummer

Rufnummer der Sprachaufzeichnung (Call Recorder).

Aufzeichnungsmodus

Legt das Verhalten der Sprachaufzeichnung fest.

Mögliche Optionen:

- **Manuell**
- **Auto Start**
- **Alle Gespräche**
- **Deaktiviert**
  (nur Anzeige)

Hinweiston

Auswahl des Hinweistons.

Mögliche Optionen:

- **Aus**
- **Ein / Einzelhinweiston**
- **Regelmässiger Hinweiston**

Telefonie-Optionen

Gespräch abweisen

Schalter zum Aktivieren der Funktion zum Abweisen von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Vermitteln im Rufzustand

Schalter zum Aktivieren des Leistungsmerkmals „Vermitteln im Rufzustand“.

Wird diese Option aktiviert, kann bei der Gesprächsübergabe der Hörer auflegt werden, obwohl der angerufene Gesprächspartner noch nicht abgehoben hat.

Nur bei SIP-Workpoints verfügbar.

Vermitteln durch Auflegen

Schalter zum Aktivieren des Leistungsmerkmals „Vermitteln durch Auflegen“.

Nur bei SIP-Workpoints verfügbar.

Bridging erlaubt

Schalter zum Aktivieren des Leistungsmerkmals „Bridging“.

Nur bei SIP-Workpoints verfügbar.

uaCSTA erlaubt

Schalter zum Aktivieren des Leistungsmerkmals „uaCSTA“.

Nur bei SIP-Workpoints verfügbar.

Phonebook nachschlagen

Schalter zum Aktivieren des Leistungsmerkmals „Phonebook nachschlagen“.

Meldung verpasste Anrufe

Ist der Schalter aktiviert, werden verpasste Anrufe im Display angezeigt.

Rückruf

Wenn ein angerufener Anschluss besetzt ist oder sich niemand meldet, kann ein Rückruf veranlasst werden. Der Benutzer erhält den Rückruf, sobald der Teilnehmer nicht mehr besetzt ist.

Rückruf nach Besetzt

Schalter zum Aktivieren des Leistungsmerkmals „Rückruf nach Besetzt“.

Nur bei SIP-Workpoints verfügbar.

Rückruf nach nicht Melden

Schalter zum Aktivieren des Leistungsmerkmals „Rückruf nach nicht Melden“.

Nur bei SIP-Workpoints verfügbar.

Rückruf abbrechen

Wenn aktiv, kann der Benutzer Rückrufaufträge abbrechen.

Rückruf

Schalter zum Aktivieren des Leistungsmerkmals „Rückruf“.

Nur bei OpenStage ab V3 verfügbar.

Programmier-Timer für frei programmierbare Tasten

Wenn „Aus“ gewählt ist, wechseln die programmierbaren Tasten (FPKs) bei langem Drücken nicht in den Programmiermodus.

Mögliche Optionen:

- **Ein**
- **Aus**

Rückrufservice (CCSS)

CCSS Funktional einschalten

Ist der Schalter aktiv, so wird der CCSS (Call Completion Supplementary Services) durch funktionale Mechanismen kontrolliert und gesteuert. Ist der Schalter inaktiv, so erfolgt die Steuerung durch Stimulus-Mechanismen (z. B. FAC).

Max. Rückrufe

Maximale Anzahl der gleichzeitigen Rückrufaufträge.

Wertebereich: **1**... **10**

Rückrufhaltezeit (sek)

Zeit in Sekunden, die die vom Server gelieferten Informationen zum Aufbau eines Rückrufs bei fehlgeschlagenem Rückrufversuch erhalten bleiben.

Mögliche Werte:

- **unbegrenzt**
- **1**
- **2**
- **3**
- **4**
- **5**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**

Rückrufton

Rückrufton, der zusammen mit der Rückrufanzeige einen anstehenden Rückruf signalisiert.

Anrufprotokollierung

Rufjournal aktivieren

Kontrollkästchen, das anzeigt, ob die Anrufprotokollierung aktiviert ist.

Entgangene Anrufe

Zeigt an, ob Anrufe, die andernorts angenommen wurden, an Ihrem Telefon protokolliert werden.

Mögliche Optionen:

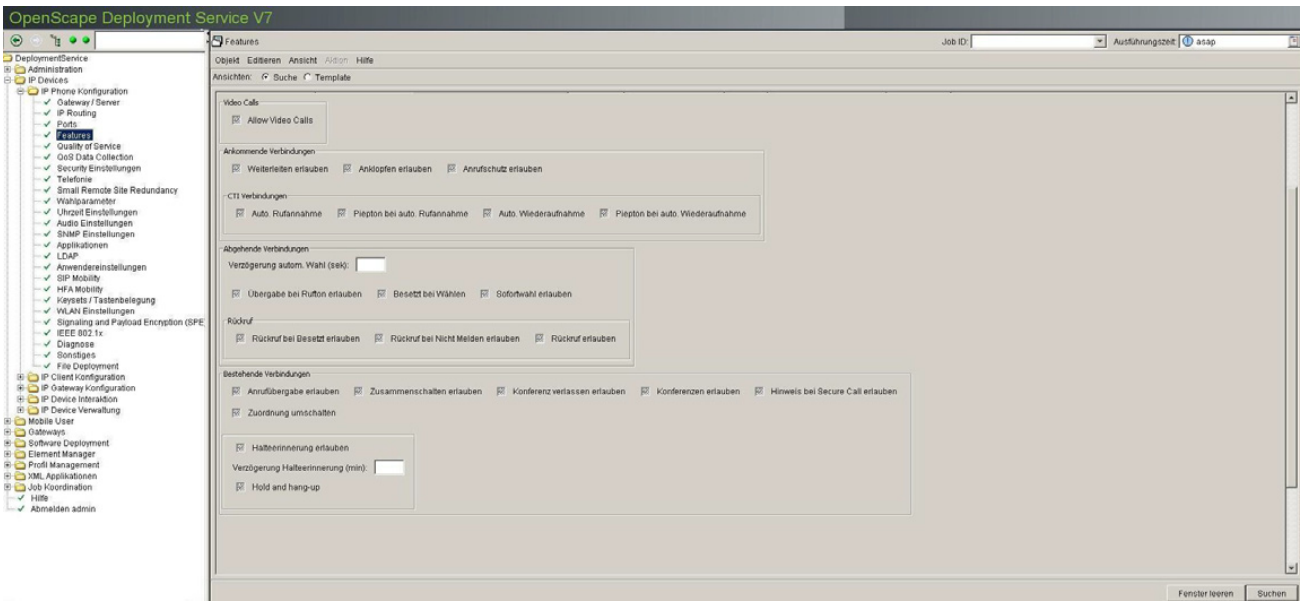
- **Alle anzeigen**

  Andernorts angenommene Anrufe werden an Ihrem Telefon protokolliert.

- **Nur unbeantwortete anzeigen**
  Anrufe, die andernorts angenommen wurden, werden an Ihrem Telefon nicht protokolliert.

7.1.4.3 Register „Anrufbezogene Benutzer-Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Anrufbezogene Benutzer-Einstellungen“



Video-Gespräche

Video Gespräche erlauben

Schalter zum Aktivieren von Video-Gesprächen.

Wenn das Kontrollkästchen aktiviert ist, sind Video-Gespräche möglich.

Ankommende Verbindungen

Weiterleiten erlauben:

Schalter zum Aktivieren der Weiterleitung.

Soll ein ankommender Anruf weitergeleitet werden, wird der Benutzer, wenn keine Zielrufnummer gespeichert ist, aufgefordert, eine Zielrufnummer einzutragen.

Anklopfen erlauben:

Schalter zum Aktivieren des Anklopfens.

Während eines Gesprächs kann ein zweiter eingehender Anruf angenommen werden. Der Anrufer hört das Freizeichen, beim Angerufenen wird in Form eines Signaltons „angeklopft“. Der Zweitanruf kann ablehnt oder angenommen werden. Wird der Zweitanruf entgegen genommen, kann das erste Gespräch zuvor beendet, aber auch auf „Halten“ gelegt und später weiterführt werden.

Anrufschutz erlauben:

Schalter zum Aktivieren des Anrufschutzes.

Ist der Anrufschutz aktiviert, läutet das Telefon nicht. Der Anrufer erhält das Besetztzeichen.

CTI Verbindungen

Auto. Rufannahme

Schalter zum Aktivieren der automatischen Rufannahme (Auto-Antwort).

Wenn man mit einer CTI-Anwendung (z. B. Outlook) eine Nummer wählt und die automatische Rufannahme (Auto-Antwort) ist eingeschaltet, geht das Telefon automatisch in den Freisprechmodus. Ist Auto-Antwort ausgeschaltet, läutet das Telefon zuerst, und der Benutzer muss die Lautsprechertaste drücken oder den Hörer abheben, um die Verbindung aufzubauen. Diese Einstellung bestimmt auch, ob eingehende Anrufe automatisch angenommen werden oder nicht. Wird ein Gespräch automatisch angenommen, ertönt ein Piepton, wenn die Funktion eingeschaltet ist.

Nur bei SIP-Workpoints verfügbar.

Piepton bei auto. Rufannahme

Schalter zum Aktivieren des Quittungstones bei automatischer Rufannahme (Auto-Antwort).

Wird ein Gespräch automatisch angenommen, ertönt ein Piepton, wenn die Funktion eingeschaltet ist.

Nur bei SIP-Workpoints verfügbar.

Auto. Wiederaufnahme

Schalter zum Aktivieren der automatischen Wiederaufnahme eines geparkten Gespräches.

Nur bei SIP-Workpoints (optiPoint) verfügbar.

Piepton bei auto. Wiederaufnahme

Schalter zum Aktivieren des Quittungstones bei automatischer Wiederaufnahme-Funktion eines geparkten Gespräches.

Man kann ein gehaltenes Gespräch sowohl über die CTI-Applikation als auch über das Telefon wieder aufnehmen. Wenn die Funktion eingeschaltet ist, ertönt ein Piepton, sobald zwischen einem aktiven Gespräch und einem gehaltenen Gespräch gewechselt wird.

Nur bei SIP-Workpoints verfügbar.

Abgehende Verbindungen

Verzögerung autom. Wahl (sek):

Verzögerung der automatischen Wahl in Sekunden.

Nach Ablauf einer konfigurierbaren Verzögerungszeit beginnt im Anschluss an die Eingabe der letzten Ziffer automatisch der Wählvorgang.

Übergabe bei Rufton erlauben

Schalter zum Aktivieren von Übergabe bei Rufton.

Wird diese Option erlaubt, kann bei der Gesprächsübergabe der Hörer auflegt werden, obwohl der angerufene Gesprächspartner noch nicht abgehoben hat.

Besetzt bei Wählen

Schalter zum Aktivieren von Besetzt bei Wählen.

Schaltet man die Funktion ein, wird ein Anruf, der während des Wählens eingeht, abgewiesen. Der Anrufer hört dann das Besetzt-Zeichen.

Sofortwahl erlauben

Ist der Schalter aktiviert, wird sofort gewählt, sobald die eingegebene Zeichenfolge mit einem Eintrag im Wählplan übereinstimmt.

Nur bei SIP-Workpoints verfügbar.

Rückruf

Wenn ein angerufener Anschluss besetzt ist oder sich niemand meldet, kann ein Rückruf veranlasst werden. Man erhält den Rückru,f sobald der Teilnehmer nicht mehr besetzt ist.

Rückruf bei Besetzt erlauben

Schalter zum Aktivieren von Rückruf bei Besetzt.

Nur bei OpenStage bis V2 verfügbar.

Rückruf bei Nicht Melden erlauben

Schalter zum Aktivieren von Rückruf bei Nicht Melden.

Nur bei OpenStage bis V2 verfügbar.

Rückruf erlauben

Rückruf erlauben.

Nur bei OpenStage ab V3 verfügbar.

Bestehende Verbindungen

Anrufübergabe erlauben

Schalter zum Aktivieren von Anrufübergabe.

Zusammenschalten erlauben

Schalter zum Aktivieren von Zusammenschalten.

Man kann den ersten Teilnehmer mit dem Teilnehmer eines Rückfragegesprächs verbinden und damit das Gespräch zu beiden Teilnehmern beenden.

Konferenz verlassen erlauben

Wenn aktiviert, kann der Benutzer die Konferenz verlassen.

Die Verbindung zur Konferenz wird getrennt und die anderen Gesprächspartner bleiben verbunden.

Konferenzen erlauben

Wenn aktiviert, kann der Benutzer Konferenzen einrichten.

Hinweis bei Secure Call erlauben

Wenn die Bearbeitung gesicherter Anrufe auf dem Telefon aktiviert und dieser Schalter markiert ist, wird der Benutzer durch ein Popup-Fenster und einen Aufmerksamkeitston auf unsichere (unverschlüsselte) eingehende Anrufe hingewiesen.

Zuordnung umschalten

Dieses Leistungsmerkmal besteht in einer weiteren Möglichkeit der Gesprächsübergabe. Wenn aktiviert, so ergibt sich der folgende Ablauf: Der Benutzer hat einen Zweitanruf angenommen, wodurch das erste Gespräch ins Halten gelegt wird. Sobald der Benutzer einmal zurück zum ersten Gespräch und danach wieder zum zweiten Gespräch gewechselt hat, kann er die beiden Gesprächspartner miteinander verbinden, indem er einfach auflegt.

Halteerinnerung erlauben

Schalter zum Aktivieren der Halteerinnerung.

Mit „Halteerinnerung“ legt man fest, wann automatisch an einen gehaltenen Teilnehmer erinnert werden soll.

Verzögerung Halteerinnerung (min)

Verzögerung der Halteerinnerung in Minuten.

Der kleinste Zeitwert ist 1, d. h. die Erinnerung erfolgt nach 1 Minute. Der Höchstwert ist 15 Minuten.

Halten und Auflegen

Schalter zum Aktivieren der Funktion „Halten und Auflegen“ bei nicht-Keyset OpenStage-Telefonen.

Mit dieser Funktion können Teilnehmer Anrufe vorübergehend halten und auflegen, ohne den Anrufer zu trennen. Diese Funktion ist standardmäßig deaktiviert.

7.1.4.4 Register „Verfügbarkeit“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Verfügbarkeit“

HINWEIS: Beim Betrieb von SIP-IP Phones an den Plattformen HiPath 3000 und HiPath 4000 bitte beachten, dass die folgenden Funktionen (Features) nicht verfügbar sind und deaktiviert werden müssen, damit sie für den Benutzer nicht sichtbar bzw. auswählbar sind:

- Auto. Rufannahme
- Anrufumlenkung
- Anrufumleitung
- Auto. Rufannahme
- Anklopfen
- Umgeleitete Anrufe protokollieren
- Music On Hold (Wartemusik
- Anruf parken
- Übergeben
- Lokale Konferenz
- Nachricht wartet
- Video Call
-
- Siehe auch Register „Feature-Einstellungen 2“.

Verfügbarkeit der Leistungsmerkmale wird nur vom DLS verwaltet

Ist dieser Schalter aktiviert, kann die Verfügbarkeit der Features ausschließlich durch DLS gesteuert werden. Die im Register „Feature-Verfügbarkeit“ gemachten Angaben verwendet. Ist dieser Schalter nicht aktiviert, kann die Verfügbarkeit auch am IP Device gesteuert werden.

Nur bei SIP-Workpoints verfügbar.

Halten

Schalter zum Aktivieren der Funktion zum Halten von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Anrufumlenkung

Schalter zum Aktivieren der manuellen Weiterleitung ankommender Anrufe (CD).

Nur bei SIP-Workpoints verfügbar.

Anrufumleitung

Schalter zum Aktivieren der automatischen Anrufweiterschaltung (CF).

Nur bei SIP-Workpoints verfügbar.

Umgeleitete Anrufe protokollieren

Schalter zum Aktivieren der Protokollierung von umgeleiteten Anrufen.

Nur bei SIP-Workpoints verfügbar.

Gesprächsdauer

Schalter zum Aktivieren der Funktion zur Anzeige der Gesprächsdauer.

Nur bei SIP-Workpoints verfügbar.

Anklopfen

Schalter zum Aktivieren der optischen und/oder akustischen Signalisierung von anklopfenden Anrufen (CW).

Nur bei SIP-Workpoints verfügbar.

Übergeben

Schalter zum Aktivieren der Funktion zum Übergeben von Gesprächen (ECT).

Nur bei SIP-Workpoints verfügbar.

Übernahme geparktes Gespräch

Schalter zum Aktivieren der Funktion zum Übernehmen von geparkten Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Auto. Wiederaufnahme

Schalter zum Aktivieren der automatischen Gesprächswiederaufnahme.

Nur bei SIP-Workpoints verfügbar.

Anzeige Rufnummer

Schalter zum Aktivieren der Rufnummernanzeige am Workpoint.

Nur bei SIP-Workpoints verfügbar.

Anzeige Name

Schalter zum Aktivieren der Anzeige des Anrufernamens am Workpoint.

Nur bei SIP-Workpoints verfügbar.

Wartemusik

Schalter zum Aktivieren der Wartemusik bei gehaltenen und geparkten Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Anrufschutz

Schalter zum Aktivieren des Anrufschutzes (nur optische Signalisierung und ein Rufton).

Nur bei SIP-Workpoints verfügbar.

Nachricht wartet

Schalter zum Aktivieren der Signalisierung von wartenden Nachrichten (MWI).

Nur bei SIP-Workpoints verfügbar.

Lokale Konferenz

Schalter zum Aktivieren der Funktion zum Aufbau einer lokalen Konferenz.

Nur bei SIP-Workpoints verfügbar.

Auto. Rufannahme

Schalter zum Aktivieren der automatischen Rufannahme.

Nur bei SIP-Workpoints verfügbar.

Telefonsperre

Schalter zum Aktivieren der Telefonsperre (Codeschloss).

Nur bei SIP-Workpoints verfügbar.

HINWEIS: Standardmäßig ist diese Funktion am OpenStage Telefon auf True (Wahr) gesetzt.
Bei SW-Versionen bis V3 ist die Funktion Telefonsperre nicht verfügbar (wird nicht angezeigt). Bei SW-Versionen ab V3 und höher ist die Verfügbarkeit der Funktion einstellbar (über WBM).
Wenn die Option Telefonsperre in der WBM-Oberfläche des Telefons deaktiviert ist, kann das Telefon nicht gesperrt werden.

HINWEIS: Die Funktion Telefonsperre wird beschrieben unter Abschnitt 7.1.16.3, “Register „gesperrte lokale Funktionen“”. Beachten Sie dabei die folgenden Optionen:
- Wenn die Funktion Telefonsperre in beiden Registern aktiviert ist, ist eine Telefonsperre nicht möglich und die Option ist ausgegraut (d. h. nicht verfügbar).
- Wenn beide Schalter deaktiviert sind, ist eine Telefonsperre nicht möglich und die dazugehörige Option wird im Menü auch nicht angezeigt.
- Ist die Funktion für den Mobile User aktiviert aber im Register „Verfügbarkeit“ deaktiviert, ist eine Telefonsperre nicht möglich und die dazugehörige Option wird im Menü auch nicht angezeigt.
- Eine Telefonsperre ist nur dann möglich, wenn die Funktion ausschließlich im Register „Verfügbarkeit“ aktiviert wurde.

PC Schnittstelle

Schalter zur Freigabe der Schnittstelle zwischen PC und Endgerät.

WAP Browser auf APM / DSM

Schalter zum Aktivieren des WAP-Browsers am optiPoint application module / display module.

Nur bei SIP-Workpoints verfügbar.

LDAP auf APM / DSM

Schalter zum Aktivieren der LDAP-Funktion am optiPoint application module / display module.

Nur bei SIP-Workpoints verfügbar.

Telefonie auf APM / DSM

Schalter zum Aktivieren der Telefonie-Funktion am optiPoint application module / display module.

Nur bei SIP-Workpoints verfügbar.

Spracherkennung auf APM / DSM

Schalter zum Aktivieren der Spracherkennungs-Funktion (Voice Dialing) am optiPoint application module / display module.

Nur bei SIP-Workpoints verfügbar.

Kurzwahl auf APM / DSM

Schalter zum Aktivieren der Kurzwahl-Funktion am optiPoint application module / display module mittels Java Midlet.

Nur bei SIP-Workpoints verfügbar.

ENB auf APM / DSM

Schalter zum Aktivieren des elektronischen Notizbuchs am optiPoint application module / display module.

Nur bei SIP-Workpoints verfügbar.

Parken

Schalter zum Aktivieren der Funktion zum Parken von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Zusammenschalten

Schalter zum Aktivieren der Funktion zum Zusammenschalten von Gesprächen.

Man kann den ersten Teilnehmer mit dem Teilnehmer eines Rückfragegesprächs verbinden und damit das Gespräch zu beiden Teilnehmern beenden.

Nur bei SIP-Workpoints verfügbar.

Aufmerksamkeitston für AUN Gruppe

Ist der Schalter aktiviert, so wird ein Aufmerksamkeitston ausgelöst, sobald für eine AUN-Gruppe (Anrufübernahmegruppe) ein Anruf wartet.

Blind Transfer

Schalter zum Aktivieren von „Blind Transfer“.

Ein aktuelles Gespräch kann an einen anderen Teilnehmer ohne Rückfrage übergeben werden.

Repertory Dial

Schalter zum Aktivieren von „Repertory Dial“.

In die Wahlfolge können Sonderzeichen auswählt und einfügt werden, um z. B. die Verbindung zu trennen, eine Rückfrage zu aktivieren oder eine Pause einzufügen.

Besetztlampenfeld (BLF)

Schalter zum Aktivieren des Besetztlampenfelds (BLF).

Es kann für die Zustandsanzeige anderer interner Telefone BLF-Tasten einrichtet werden. Jede eingerichtete BLF-Taste ist der internen Rufnummer eines anderen Telefons zugeordnet. Anhand des Zustands der LED kann feststellt werden, ob der Teilnehmer frei oder besetzt ist oder angerufen wird.

Direct Station Select (DSS)

Schalter zum Aktivieren von Direct Station Select (DSS).

Außer Leitungstasten können zusätzlich Direktruftasten (DSS) einrichtet werden. Mit einer Direktruftaste kann ein interner Teilnehmer direkt anrufen werden, Gespräche für diesen Teilnehmer übernommen oder Gespräche direkt an ihn weiterleitet werden.

CTI

Schalter zum Aktivieren von „CTI“.

Wählt der Benutzer mit einer CTI-Anwendung (z. B. Outlook) eine Nummer und Auto-Antwort ist eingeschaltet, geht das Telefon automatisch in den Freisprechmodus. Ist Auto-Antwort ausgeschaltet, läutet das Telefon zuerst, und der Benutzer muss die Lautsprechertaste drücken oder den Hörer abheben, um die Verbindung aufzubauen. Diese Einstellung bestimmt auch, ob eingehende Anrufe automatisch angenommen werden oder nicht.

Leitungsübersicht

Schalter zum Aktivieren der Leitungsübersicht.

Um den Status der Leitungen zu sehen, wechselt man im Telefondisplay von Register „Mein Telefon“ zum Register „Übersicht“.

Feature Toggle

Schalter zum Aktivieren von „Feature Toggle“.

Zum Aufrufen der Funktionen „Besetzt“(„make line busy“) und „Ende der Sammelanschluss-Kette“(„stop hunt“) kann eine freiprogrammierbare Sensortaste als Funktionswechseltaste (Feature toggle) definiert und programmiert werden. Durch Drücken der freiprogrammierbaren Taste wird dann die jeweilige OpenScape Voice-Funktion auf dem Server für diesen Anschluss ein- bzw. ausgeschaltet.

Third Call Leg

Schalter zum Aktivieren von „Third Call Leg“ (Drittgesprächen).

Für Rückfrage im Zweitgespräch: Ist das Zweitgespräch das aktive Gespräch, so kann daraus eine Rückfrage einleitet werden. Während einer Rückfrage im Zweitgespräch wird das Erstgespräch „geparkt“ und kann erst wieder „entparkt“ werden, wenn das Rückfrage- oder Zweitgespräch beendet oder diese Gespräche verbunden wurden.

Übernahme Anruf in Gruppe

Schalter zum Aktivieren von „Übernahme Anruf in Gruppe“.

Video Call

Schalter zum Aktivieren der Funktion „Video Call“.

7.1.4.5 Register „Server basierte Features“

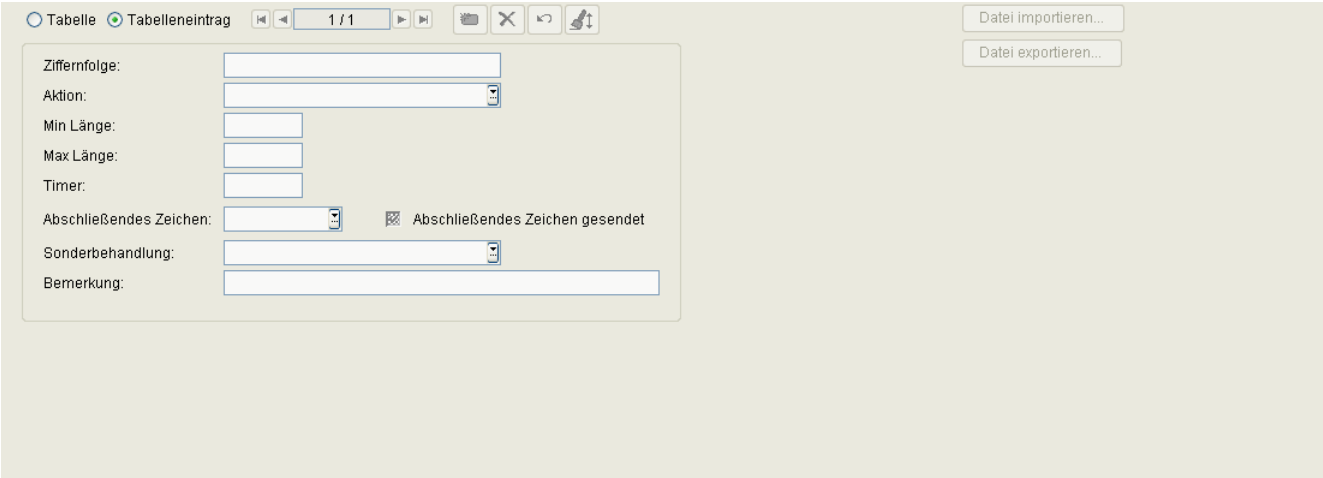
Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Server basierte Features“

Unterstützung Server basierte Features

Ist der Schalter aktiviert, so werden die serverbasierten Leistungsmerkmale des Endgeräts für den Benutzer freigegeben.

7.1.4.6 Register „Wählplan“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Wählplan“



Wählplan

Schalter zum Aktivieren des Wählplans. Ist dieser Schalter aktiviert, werden die Angaben in diesem Register interpretiert.

Nur bei SIP-Workpoints verfügbar.

Wählplan ID

Name des Wählplans, der mit einem ’!’ beginnen muss.

Wertebereich: max. 14 alphanumerische Zeichen.

Nur bei SIP-Workpoints verfügbar.

Wählplan Fehler

Gibt im Fehlerfall an, welcher Wählplaneintrag fehlerhaft ist.

Wertebereich: **1** ... **48**

Nur bei SIP-Workpoints verfügbar.

Ziffernfolge

Ziffernfolge zur Ausführung dieser Aktion.

Nur bei SIP-Workpoints verfügbar.

Aktion

Aktion, die bei dieser Ziffernfolge ausgeführt wird.

Mögliche Optionen:

- **-C- Aktion für Ziffern**
- **-S- Ziffern senden**

Nur bei SIP-Workpoints verfügbar.

Min Länge

Minimale Länge der Ziffernfolge, ab der die Ziffernfolge interpretiert wird.

Nur bei SIP-Workpoints verfügbar.

Max Länge

Maximale Länge der Ziffernfolge, bis zu der die Ziffernfolge interpretiert wird.

Nur bei SIP-Workpoints verfügbar.

Timer

Verzögerungszeit bis zum Ausführen der Aktion.

Wertebereich: **1** ... **9** Sekunden.

Nur bei SIP-Workpoints verfügbar.

Abschließendes Zeichen

Zeichen, welches die Ziffernfolge bei der Eingabe abschließt.

Mögliche Optionen:

- **#**
- *****

Nur bei SIP-Workpoints verfügbar.

Sonderbehandlung

Mögliche Optionen:

- **-E- Notruf**
- **-b- bypass**

Nur bei SIP-Workpoints verfügbar.

Bemerkung

Feld für allgemeine Informationen.

Nur bei SIP-Workpoints verfügbar.

Abschließendes Zeichen gesendet

Zeigt an, ob das abschließende Zeichen in der Ziffernfolge enthalten ist.

Datei importieren

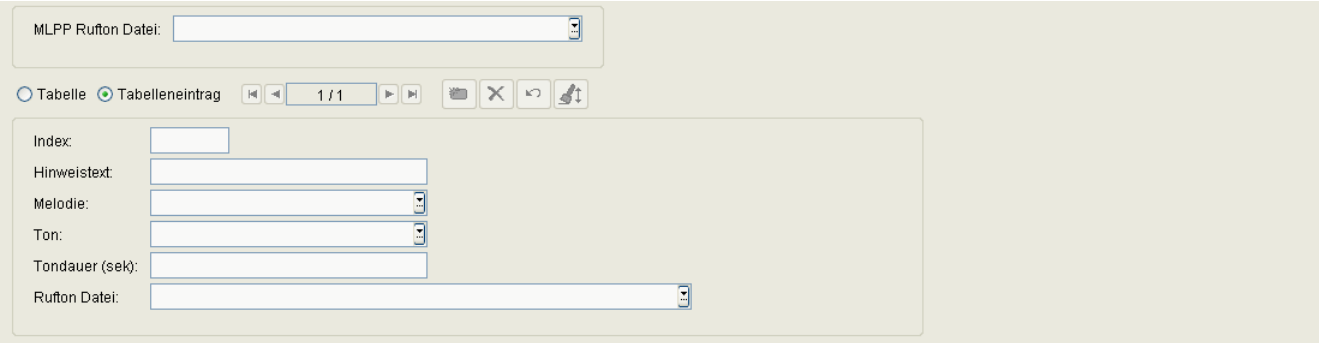
Importiert einen Wählplan aus einer Datei im CSV-Format.

Datei exportieren

Exportiert einen Wählplan aus einer Datei im CSV-Format.

7.1.4.7 Register „Signalisierungsmelodie / Ton“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Signalisierungsmelodie / Ton“



HINWEIS: Ein Template mit Einträgen zu **Signalisierung / Ton** wird erstellt, indem man ein IP Device mit **Signalisierung / Ton**-Einträgen (dies können auch leere Einträge sein) sucht und mit der Aktion **In Template kopieren** ein Template erzeugt. Es müssen immer 15 Einträge vorhanden sein, auch wenn sie keine Daten enthalten.
Dieses Template kann nun modifiziert, gespeichert und verwendet werden.

MLPP Rufton Datei

Rufton-Datei, die für Priority-Anrufe verwendet werden soll.

Index

Automatisch erzeugter Index für die einzelnen spezifischen Ruftöne.

Hinweistext

Ist der hier eingegebene String identisch mit einem speziellen String, der im SIP Alert Info Header an das Telefon gesendet wird, so wird der entsprechende Klingelton verwendet.

Nur bei SIP-Workpoints verfügbar.

Melodie

Art der Rufton-Melodie.

Mögliche Optionen: **Melodie 1** ... **Melodie 8, Melodie aus.**

Nur bei SIP-Workpoints verfügbar.

Ton

Klingeltonsequenz.

Mögliche Optionen:

- **1**
  Entspricht 1 sek EIN, 4 sek AUS.
- **2**
  Entspricht 1 sek EIN, 2 sek AUS.
- **3**
  Entspricht 0,7 sek EIN, 0,7 sek AUS, 0,7 sek EIN, 3 sek AUS.

Nur bei SIP-Workpoints verfügbar.

Tondauer

Dauer des Ruftons.

Wertebereich: **1** ... **300** Sekunden.

Standard: **60** Sekunden.

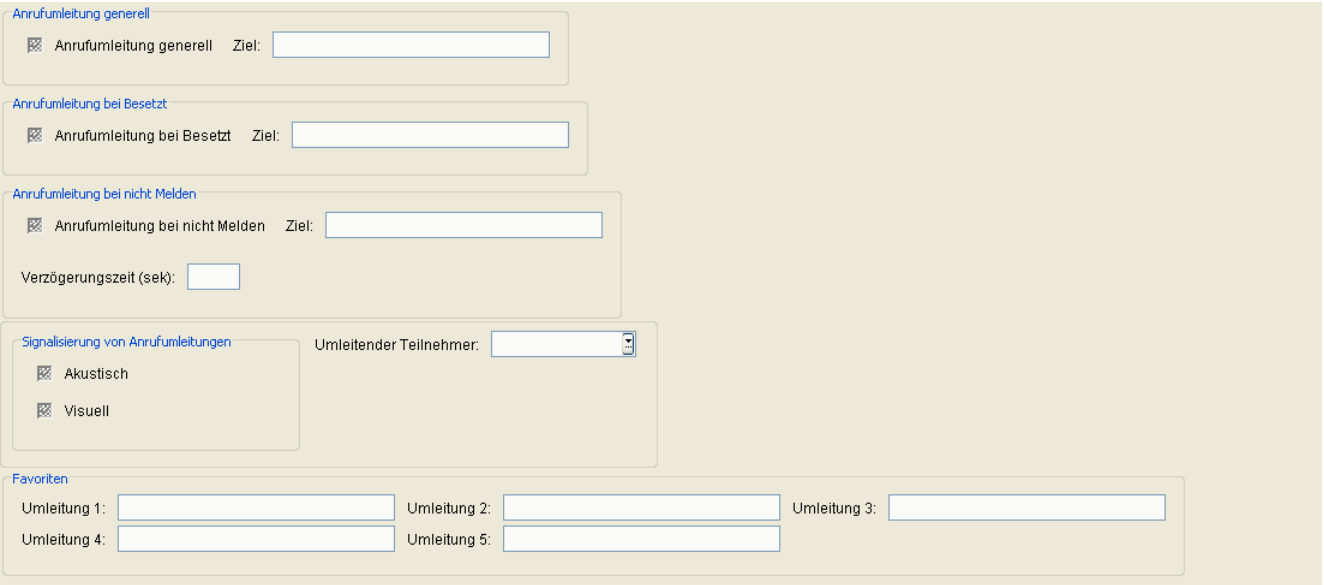
Nur bei SIP-Workpoints verfügbar.

Rufton Datei

Name der Audio-Datei, die den Rufton enthält.

7.1.4.8 Register „Anrufumleitung“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Features > Register „Anrufumleitung“



Anrufumleitung generell

Anrufumleitung generell

Schalter zum Aktivieren der „Anrufumleitung ohne weitere Bedingungen“.

Schalter zum Aktivieren der Anrufumleitung ohne weitere Bedingungen.

Ziel:

Rufnummer des Anrufumleitungsziels.

Anrufumleitung bei Besetzt

Anrufumleitung bei Besetzt

Schalter zum Aktivieren der Anrufumleitung bei Besetzt.

Ziel:

Rufnummer des Anrufumleitungsziels.

Anrufumleitung bei nicht Melden

Anrufumleitung bei nicht Melden:

Schalter zum Aktivieren der Anrufumleitung bei nicht Melden.

Ziel:

Rufnummer des Anrufumleitungsziels.

Verzögerungszeit (sek):

Ist diese Zeit abgelaufen, ohne dass der Anruf angenommen worden ist, wird der Anruf umgeleitet.

Signalisierung bei Anrufumleitung

Akustisch

Schalter zum Aktivieren eines akustischen Signals beim umleitenden Telefon.

Visuell

Schalter zum Aktivieren eines visuellen Signals beim umleitenden Telefon.

Umleitender Teilnehmer

Es kann eingestellt werden, welcher umleitende Teilnehmer bei Mehrfachumleitungen angezeigt werden soll.

Mögliche Optionen:

- **Anzeige erster**
- **Anzeige letzter**

Favoriten

Umleitung 1:

Umleitung 2:

Umleitung 3:

Umleitung 4:

Umleitung 5:

7.1.5 Quality of Service

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Quality of Service

Dieser Bereich besteht aus folgenden Inhalten:

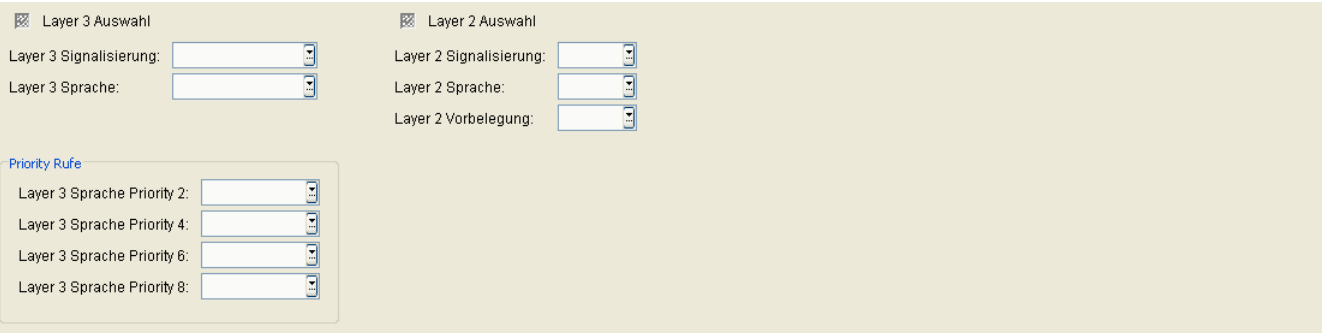
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „QoS Parameter“
- Register „QoS Parameter (Standby)“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.5.1 Register „QoS Parameter“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Quality of Service > Register „QoS Parameter“



Layer 3 Auswahl

Schalter zum Aktivieren der QoS Layer 3-Konfiguration.

Layer 3 Signalisierung:

Layer 3-Wert für die Anruf-Signalisierung.

Wertebereich für optiPoint HFA-Workpoints (kleiner optiPoint HFA V5R5) und optiPoint SIP-Workpoints bis einschl. SIP5: **0** **63**

Mögliche Werte für optiPoint SIP ab SIP6 und optiPoint HFA ab V5R5:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Mögliche Werte für OpenStage SIP/HFA:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**
- **0 - BE**
- **56 - CS7**

Mögliche Werte für WLAN HFA/SIP:

- **0 - BE**
- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**

- **46 - EF**

Layer 3 Sprache:

Layer 3-Wert für Sprache.

HINWEIS: Die Einstellungen für QoS Layer 3 Sprache können auch über LLDP-MED (Link Layer Discovery Protocol) erfolgen. In diesem Fall können sie nicht mehr mittels DLS geändert werden.

Wertebereich für optiPoint HFA-Workpoints (außer optiPoint HFA V5R5 und höher) und optiPoint SIP-Workpoints bis einschl. SIP5: **0** .... **63.**

Mögliche Werte für optiPoint HFA-Workpoints ab V5R5 und optiPoint SIP-Workpoints ab SIP6:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Mögliche Werte für OpenStage SIP/HFA:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**

- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**
- **0 - BE**
- **56 - CS7**

Werte für WLAN HFA/SIP:

- **0 - BE**
- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 2 Auswahl

Schalter zum Aktivieren der QoS Layer 2-Konfiguration.

Layer 2 Signalisierung:

Layer 2-Wert für die Anruf-Signalisierung.

Wertebereich: **0** ... **7**

Layer 2 Sprache:

HINWEIS: Die Einstellungen für QoS Layer 2 Sprache können auch über LLDP-MED (Link Layer Discovery Protocol) erfolgen. In diesem Fall können sie nicht mehr mittels DLS geändert werden.

Layer 2-Wert für Sprache.

Wertebereich: **0** ... **7**

Layer 2 Vorbelegung:

Standardwert für den Layer 2-Wert.

Wertebereich: **0** ... **7**

Priority Rufe

Layer 3 Sprache Priority 2

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

Layer 3 Sprache Priority 4

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

Layer 3 Sprache Priority 6

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

Layer 3 Sprache Priority 8

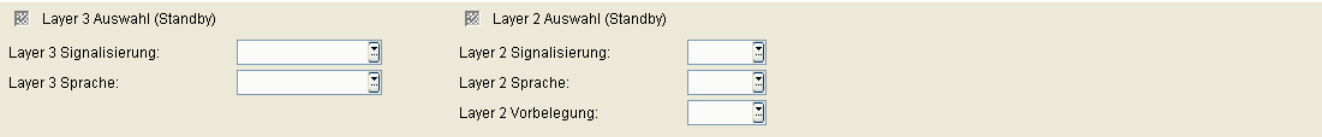
Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

7.1.5.2 Register „QoS Parameter (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Quality of Service > Register „QoS Parameter (Standby)“

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „QoS Parameter“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.1.9, “Small Remote Site Redundancy”.



Layer 3 Auswahl (Standby)

Schalter zum Aktivieren der QoS Layer 3-Konfiguration.

Layer 3 Signalisierung:

Layer 3-Wert für die Anruf-Signalisierung.

Wertebereich für optiPoint HFA-Workpoints (kleiner optiPoint HFA V5R5) und optiPoint SIP-Workpoints bis einschl. SIP5: **0** .... **63.**

Mögliche Werte für optiPoint SIP ab SIP6 und optiPoint HFA ab V5R5:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 3 Sprache:

HINWEIS: Die Einstellungen für QoS Layer 3 Sprache können auch über LLDP-MED (Link Layer Discovery Protocol) erfolgen. In diesem Fall können sie nicht mehr mittels DLS geändert werden.

Layer 3-Wert für Sprache.

Wertebereich für optiPoint HFA-Workpoints und optiPoint SIP-Workpoints bis einschl. SIP5: **0** **63**

Mögliche Werte für optiPoint SIP ab SIP6 und optiPoint HFA ab V5R5:

- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**
- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Mögliche Werte für WLAN HFA/SIP:

- **0 - BE**
- **10 - AF11**
- **12 - AF12**
- **14 - AF13**
- **18 - AF21**
- **20 - AF22**
- **22 - AF23**
- **26 - AF31**

- **28 - AF32**
- **30 - AF33**
- **34 - AF41**
- **36 - AF42**
- **38 - AF43**
- **46 - EF**

Layer 2 Auswahl (Standby)

Schalter zum Aktivieren der QoS Layer 2-Konfiguration.

Layer 2 Signalisierung:

Layer 2-Wert für die Anruf-Signalisierung.

Wertebereich: **0** ... **7**

Layer 2 Sprache:

HINWEIS: Die Einstellungen für QoS Layer 2 Sprache können auch über LLDP-MED (Link Layer Discovery Protocol) erfolgen. In diesem Fall können sie nicht mehr mittels DLS geändert werden.

Layer 2-Wert für Sprache.

Wertebereich: **0** ... **7**

Layer 2 Vorbelegung:

Standardwert für den Layer 2-Wert.

Wertebereich: **0** ... **7**

7.1.6 QoS Data Collection

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > QoS Data Collection

HINWEIS: Diese Funktion steht in der onboard-Variante des DLS auf OpenScape Voice nicht zur Verfügung.

Dieser Bereich besteht aus folgenden Inhalten:

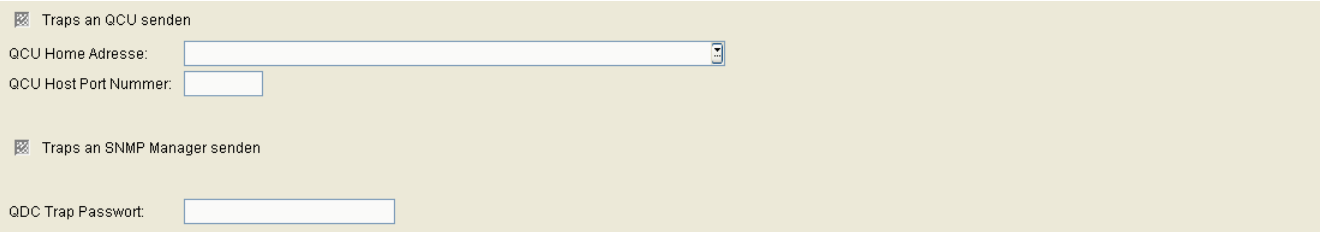
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Server Daten“
- Register „Report Einstellungen“
- Register „Schwellwerte“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.6.1 Register „Server Daten“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > QoS Data Collection > Register „Server Daten“



Traps an QCU senden

Schalter zum Aktivieren der Funktion, mit der Fehler an die QCU gesendet werden.

QCU Home Adresse:

IP-Adresse oder Hostname des Servers, der die QDC-Daten sammelt.

QCU Host Port Nummer:

Port-Nummer des Servers, der die QDC Daten sammelt.

Traps an SNMP Manager senden

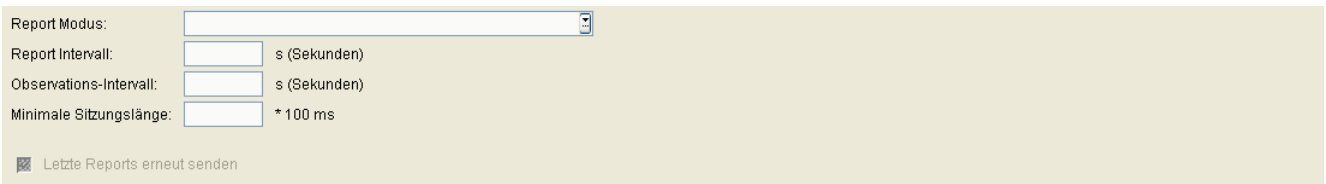
Schalter zum Aktivieren der Funktion, dass Fehler an den SNMP-Manager gesendet werden.

QDC Trap Passwort:

Passwort des Servers, der die QDC Traps sammelt.

7.1.6.2 Register „Report Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > QoS Data Collection > Register „Report Einstellungen“



Report Modus:

Gibt an, wann ein Report erstellt werden soll.

Mögliche Optionen:

- **EOS Schwellwert überschritten**
  Am Ende der Verbindung bei Schwellwertüberschreitung.
- **EOR Schwellwert überschritten**
  Am Ende des Berichtintervalls bei Schwellwertüberschreitung.
- **EOS (Ende der Verbindung)**
  Am Ende der Verbindung.
- **EOR (Ende des Berichtintervalls)**
  Am Ende des Berichtintervalls.

Report Intervall:

Zeitintervall, in dem ein QoS-Report gesendet wird.

Wertebereich: **0** ... **3600** Sekunden.

Observations-Intervall:

Zeitintervall, in dem eine Schwellwertüberschreitung geprüft wird.

Wertebereich: **0** ... **5000** Sekunden.

Minimale Sitzungslänge:

Besteht eine Sitzung (Session, das heißt z. B. eine Gesprächsverbindung) kürzer als dieses Minimum, dann wird kein QoS-Report gesendet.

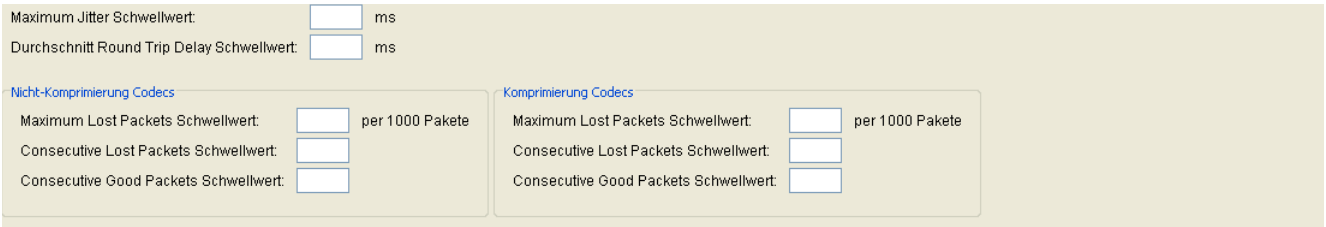
Wertebereich: **0** ... **5000** (x 100 ms).

Letzte Reports erneut senden

Bei aktiviertem Schalter werden die jeweils letzten QoS-Reports durch den Workpoint erneut gesendet.

7.1.6.3 Register „Schwellwerte“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > QoS Data Collection > Register „Schwellwerte“



Maximum Jitter Schwellwert:

Maximaler Schwellwert in Millisekunden für die Laufzeitschwankungen der Datenübertragung zur Auslösung eines Reports.

Wertebereich: **0** ... **255** ms.

Standard: **15**

Durchschnitt Round Trip Delay Schwellwert:

Durchschnittliche Rückmeldezeit in Millisekunden bei der Signalübertragung.

Standard: **100**

Nicht-Komprimierung Codecs

Maximum Lost Packets Schwellwert:

Maximale Anzahl der insgesamt verlorengegangenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Lost Packets Schwellwert:

Maximale Anzahl der nacheinander folgenden, verlorengegangenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Good Packets Schwellwert:

Minimale Anzahl der nacheinander folgenden, angekommenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Komprimierung Codecs

Maximum Lost Packets Schwellwert:

Maximale Anzahl der insgesamt verlorengegangenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Lost Packets Schwellwert:

Maximale Anzahl der nacheinander folgenden, verlorengegangenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Good Packets Schwellwert:

Minimale Anzahl der nacheinander folgenden, angekommenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

7.1.7 Security Einstellungen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

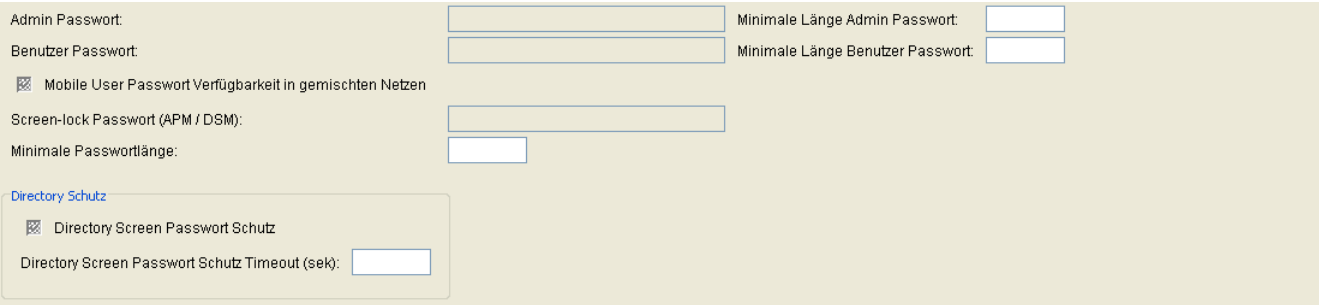
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Passwörter“
- Register „Zusätzliche Passwort Regeln“
- Register „Freigeschaltete Services (NW Stack)“
- Register „WBM Server Zertifikat“
- Register „HTTPS Server CA Zertifikate“
- Register „OCSR 1 Server CA Zertifikat“
- Register „OCSR 2 Server CA Zertifikat“
- Register „OCSR 1 Signature CA Zertifikat“
- Register „OCSR 2 Signature CA Zertifikat“
- Register „Certificate Policy“
- Register „HTTPS Client Certificates“
- Register „DLS Verbindung“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.7.1 Register „Passwörter“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „Passwörter“



Admin Passwort:

Passwort für den Zugang zum Administrationsbereich des Workpoints.

Benutzer Passwort:

Passwort für den Zugang zum Benutzerbereich des Workpoints.

Bei OpenStage-Telefonen ab V3.0 kann beim nächsten Login eine Passwortänderung durch den Benutzer erzwungen werden.

Mobile User Passwort Verfügbarkeit in gemischten Netzen

Ist dieser Schalter gesetzt und wird ein Mobile User Passwort an einem OpenStage ab V3.0 geändert, so ist dieses Passwort auch an älteren Endgerätetypen oder Software-Versionen verfügbar. Ist der Schalter nicht gesetzt, kann es geschehen, dass das Mobile User Passwort bei älteren Endgerätetypen oder älteren Software-Versionen durch das Standardpasswort „000000“ ersetzt wird.

Nur für SIP-Phones verfügbar.

Screen-lock Passwort (APM / DSM):

Passwort zur Aufhebung der Displaysperre am optiPoint 410 Application Module / Display Module.

Gilt nur, wenn ein Application Module / Display Module eingesetzt wird.

Minimale Passwortlänge:

Mindestanzahl von Zeichen, aus denen Admin- und Benutzerpasswort bestehen müssen. Nur verfügbar, wenn das aktuelle Objekt ein HFA-Telefon (ältere Version) ist, denn hier haben beide Passwörter die gleiche Länge.

Minimale Länge Admin Passwort:

Mindestanzahl von Zeichen, aus denen das Admin-Passwort bestehen muss. Nur verfügbar, wenn das aktuelle Objekt ein SIP-Telefon ist.

Minimale Länge Benutzer Passwort:

Mindestanzahl von Zeichen, aus denen das Benutzer-Passwort bestehen muss. Nur verfügbar, wenn das aktuelle Objekt ein SIP-Telefon ist.

Directory Schutz

Directory Screen Passwort Schutz

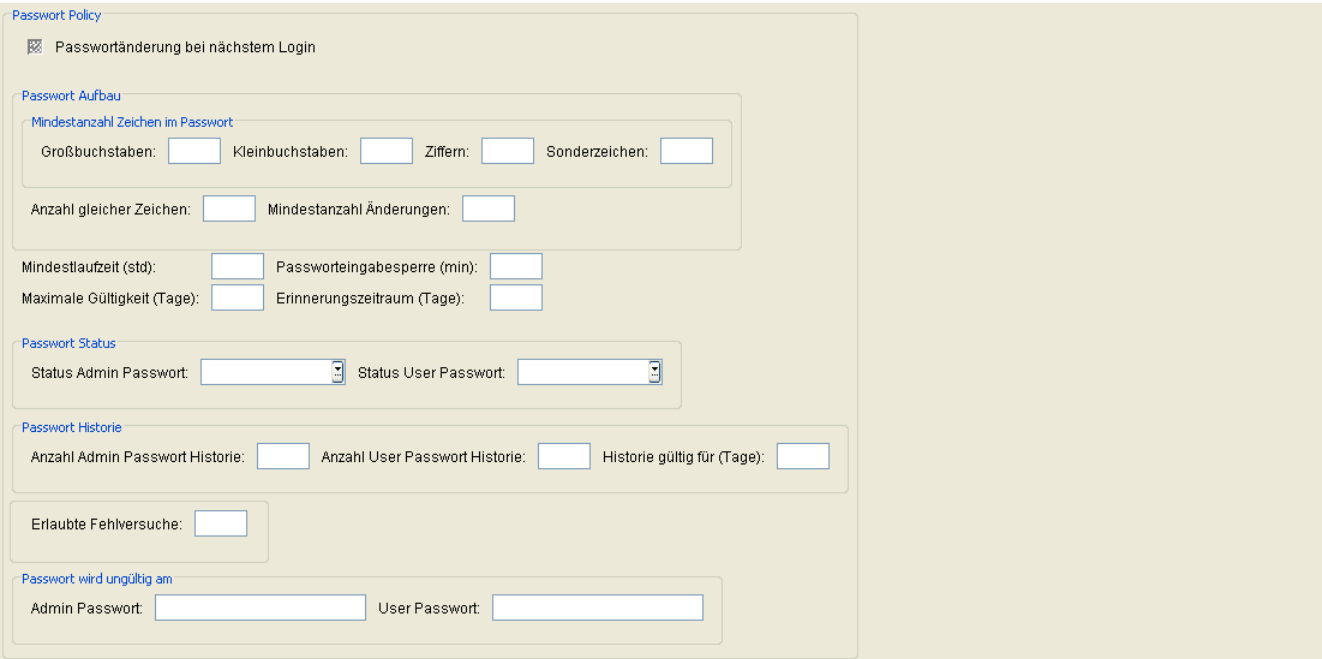
Dieser Schalter aktiviert den Passwortschutz des Directory-Bildschirms. Zur Nutzung des Bildschirms ist das Standard-Benutzerpasswort einzugeben.

Directory Screen Passwort Schutz Timeout (sek)

Nach Ablauf dieser Zeit wird der Passwortschutz aktiviert, d.h. das Passwort muss zur weiteren Nutzung des Bildschirms erneut eingegeben werden.

7.1.7.2 Register „Zusätzliche Passwort Regeln“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „Zusätzliche Passwort Regeln“



Passwort Policy

Passwortänderung bei nächstem Login

Ist dieser Schalter aktiviert, wird der Benutzer beim nächsten Login zum Ändern seines Passwort aufgefordert, bevor er Zugang zum Benutzermenü (einschl. Webseiten) erhält oder die Telefonsperre aufheben darf. Die Einstellung bleibt so lange aktiv, bis der Telefonbenutzer das Passwort ändert oder die Aufforderung zum Ändern des Passworts deaktiviert wird.

Password Aufbau

Mindestanzahl Zeichen im Passwort

Großbuchstaben

Minimale Anzahl von Großbuchstaben, die das Passwort enthalten muss.

Wertebereich: **0** ... **24**

0 = keine Prüfung

Kleinbuchstaben

Minimale Anzahl von Kleinbuchstaben, die das Passwort enthalten muss.

Wertebereich: **0** ... **24**

0 = keine Prüfung

Ziffern

Mindestanzahl Ziffern, die das Passwort enthalten muss.

Wertebereich: **0** ... **24**

0 = keine Prüfung

Sonderzeichen

Minimale Anzahl von Sonderzeichen, die das Passwort (`-=[];'#\,./!"£$%^&*()_+{}:@~|<>?) enthalten muss.

Wertebereich: **0** ... **24**

0 = keine Prüfung

Anzahl gleicher Zeichen:

Maximale Anzahl identischer Zeichen, die das Passwort enthalten darf.

Wertebereich: **0, 2** ... **24**

0 = keine Prüfung

Mindestanzahl Änderungen:

Anzahl der Zeichen, die bei einer Passwortänderung geändert werden müssen.

Wertebereich: **0** ... **24**

0 = keine Prüfung

Passwortzeichensatz

Zeichensatz, der für das Passwort erlaubt sein soll.

Mögliche Optionen:

- **Nicht eingeschränkt**
- **ASCII**
- **PIN**
- **Ziffern**

Mindestlaufzeit (std)

Minimale Zeitdauer, die zwischen zwei Passwortänderungen vergehen muss, in Stunden.

Passworteingabesperre (min)

Wenn die maximale Anzahl von Eingabeversuchen überschritten worden ist, wird das Passwort für die hier eingestellte Zeit gesperrt, in Minuten.

Maximale Gültigkeit (Tage)

Maximale Gültigkeitsdauer eines Passwortes.

Wertebereich: **0** ... **999**

0 = keine Prüfung.

Erinnerungszeitraum (Tage)

Wenn das Passwort innerhalb der hier angegebenen Anzahl von Tagen ablaufen wird, so wird der Benutzer benachrichtigt.

Wertebereich: **0** ... **999**

0 = keine Prüfung

Password Status

Status Admin Passwort

Status des Admin-Passworts.

Mögliche Optionen:

- **Aktiv**
- **Aufgeschoben**

- **Gesperrt**

Status User Passwort

Status des Benutzer-Passworts.

Mögliche Optionen:

- **Aktiv**
- **Aufgeschoben**
- **Gesperrt**

Passwort Historie

Anzahl Admin Passwort Historie

Anzahl gespeicherter alter Admin-Passwörter. Neue Passwörter dürfen mit keinem Passwort in der Historie übereinstimmen.

Wertebereich: **0** … **99**

Anzahl User Passwort Historie

Anzahl gespeicherter alter Benutzer- Passwörter. Neue Passwörter dürfen mit keinem Passwort in der Historie übereinstimmen.

Wertebereich: **0** … **99**

Historie gültig für (Tage)

Zeitdauer, innerhalb derer ein einmal benutztes Passwort nicht erneut genutzt werden darf, da es so lange in der Historie verbleibt

Erlaubte Fehlversuche

Anzahl erlaubter Fehlversuche, bevor die Passworteingabe kurzzeitig gesperrt wird

Wertebereich: **2** … **5**

Standardwert: **3**

Passwort wird ungültig am

Admin Passwort

Uhrzeit und Datum, an dem das Admin-Passwort abläuft.

User Passwort

Uhrzeit und Datum, an dem das Benutzer-Passwort abläuft.

7.1.7.3 Register „Freigeschaltete Services (NW Stack)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „Freigeschaltete Services (NW Stack)“

Service Agent

Schalter zum Aktivieren/Deaktivieren des Service Agent.

Probe Interface

Schalter zum Aktivieren/Deaktivieren des Probe Interface.

Test Interface

Schalter zum Aktivieren/Deaktivieren des Test Interface.

CTI Interface

Schalter zum Aktivieren/Deaktivieren des CTI Interface.

Bluetooth Schnittstelle

Dieser Schalter wird aktiviert, wenn am OpenStage-Telefon die Bluetooth-Schnittstelle aktivierbar sein soll.

Phone Manager

Dieser Schalter wird aktiviert, wenn die Schnittstelle zwischen OpenStage-Telefon und Phone Manager aktiv sein soll.

Der Phone Manager ist eine PC-Applikation zur Verwaltung bestimmter Telefondaten.

USB Schnittstelle

Ist der Schalter aktiviert, kann auf die USB-Schnittstelle am IP Device zugegriffen werden (Nur OpenStage 60 und OpenStage 80).

Debug Interface

Schalter zum Aktivieren/Deaktivieren des Debug Interface.

WBM Interface

Schalter zum Aktivieren/Deaktivieren des WBM Interface.

HINWEIS: Beachten Sie beim Deaktivieren der WBM-Schnittstelle, dass eine erneute Aktivierung ausschließlich mithilfe des DLS möglich ist, da das WBM hierfür nicht mehr zur Verfügung steht.

SNMP Interface

Schalter zum Aktivieren/Deaktivieren des SNMP Interface (Netzwerk Management-Funktion).

Resource Sharing

Schalter zum Aktivieren/Deaktivieren des Resource Sharing (Mitnutzen der PC-Maus und Tastatur).

PC Schnittstelle

Dieser Schalter wird aktiviert, wenn die PC-Schnittstelle benutzbar sein soll.

FTP

Dieser Schalter wird aktiviert, wenn die FTP-Schnittstelle am OpenStage-Telefon aktiv sein soll.

USB Backup / Restore

Ist der Schalter aktiviert, ist Backup / Restore für IP Device-Daten (z. B. Bildschirmschoner) über die USB Schnittstelle möglich. Backup / Restore muss am jeweiligen IP Device direkt aufgerufen werden (Nur OpenStage 60 und OpenStage 80).

Factory Reset mittels Zifferntastenkombination

Wenn aktiviert, ist ein Factory Reset mittels Zifferntastenkombination möglich.

CEE Ports

Freischalten der Comms Channel Extender (CCE) Ports für TCP (Port 65531) und/oder UDP (Port 65530) Zugang.

Mögliche Optionen:

- **Alle Sperren**
- **Alle freigeben**
- **Nur TCP**
- **Nur UDP**

Modus serieller Port

Art des Passwortschutzes für den seriellen Port.

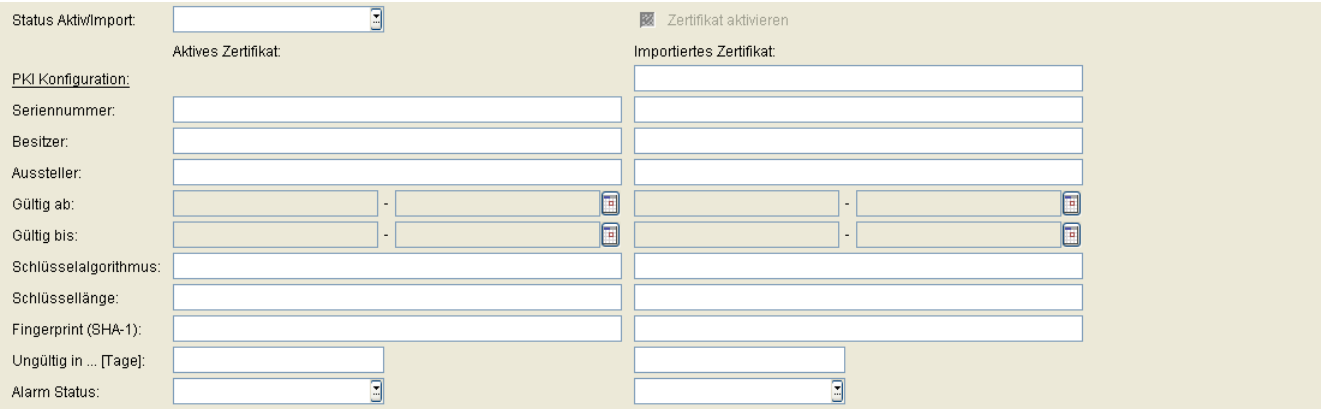
Mögliche Optionen

- **Passwort erforderlich**
- **Kein Passwort**
- **Nicht verfügbar**

7.1.7.4 Register „WBM Server Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „WBM Server Zertifikat“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.



Über dieses Register können Sie das SSL-Server-Zertifikat des Web Based Management (WBM) importieren oder entfernen. Dieses Zertifikat wird für die WBM-Geräteschnittstelle (z. B. für die Geräte-Verwaltung über einen Web-Browser) verwendet. Wenn kein Zertifikat vorhanden ist, wird standardmäßig das WBM-SSL-Zertifikat verwendet.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

Aktives Zertifikat/Importiertes Zertifikat:

PKI Konfiguration

Zeigt die PKI-Konfiguration des importierten Zertifikats an.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge des aktiven oder importierten Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus **SHA-1** (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.7.5 Register „HTTPS Server CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „HTTPS Server CA Zertifikate“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Über dieses Register können Sie Server-CA-Zertifikate importieren oder entfernen, um den HTTPS-Server für File Transfers zu authentifizieren. Bis zu zwei Zertifikate können in das Gerät importiert werden. Siehe Abschnitt 6.3.5, “HTTPS Server Konfiguration”. Weitere Konfiguration siehe Abschnitt 7.1.7.10, “Register „Certificate Policy“”.

Index

Index des Zertifikats.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

Aktives Zertifikat/Importiertes Zertifikat:

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus **SHA-1** (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.7.6 Register „OCSR 1 Server CA Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „OCSR 1 Server CA Zertifikat“

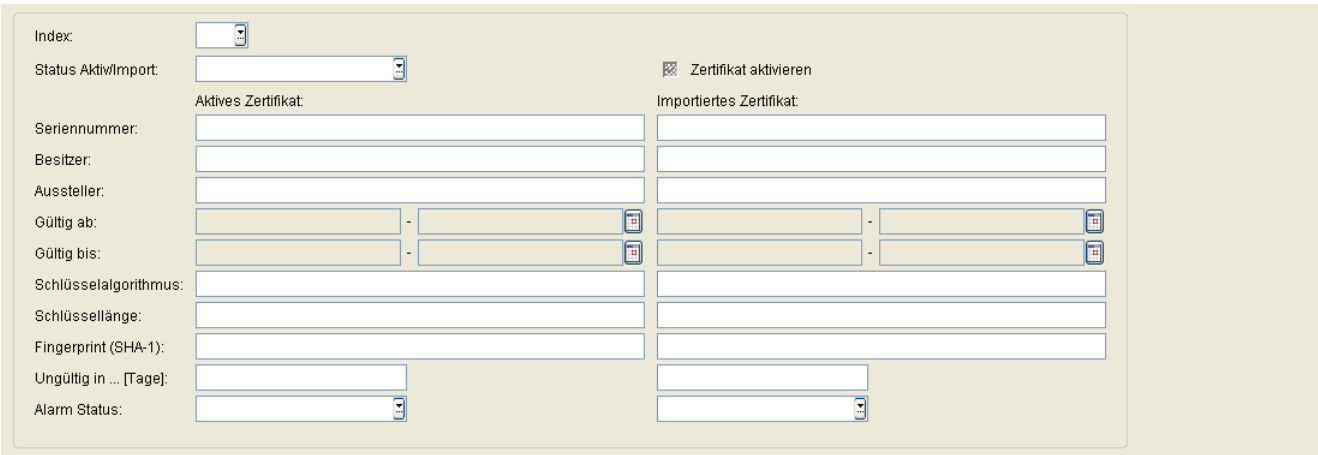
HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Parameterbeschreibung siehe Abschnitt 7.1.7.5, “Register „HTTPS Server CA Zertifikate“”.

7.1.7.7 Register „OCSR 2 Server CA Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „OCSR 2 Server CA Zertifikat“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

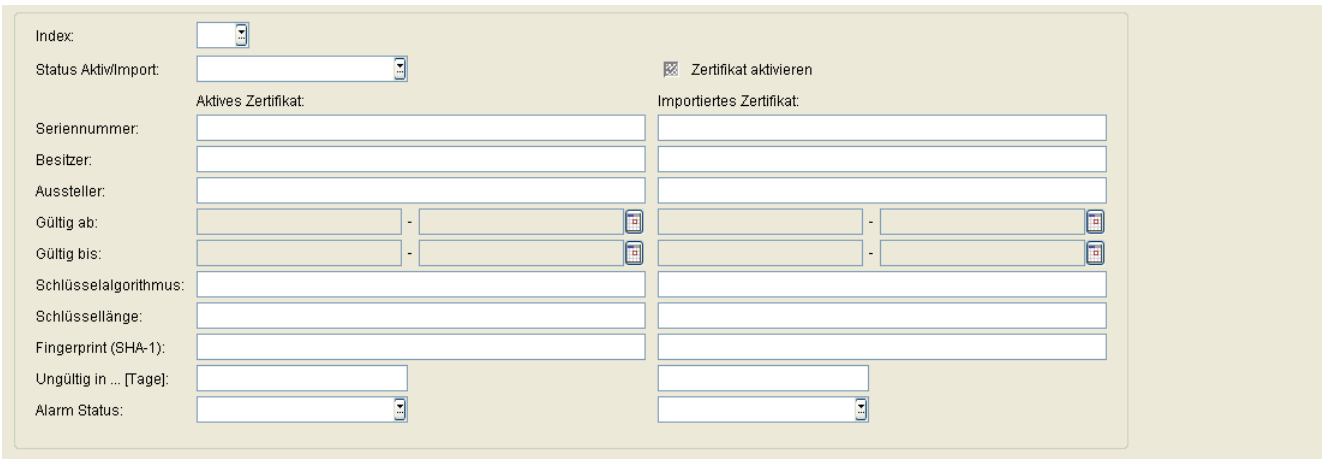


Parameterbeschreibung siehe Abschnitt 7.1.7.5, “Register „HTTPS Server CA Zertifikate“”.

7.1.7.8 Register „OCSR 1 Signature CA Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „OCSR 1 Signature CA Zertifikat“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

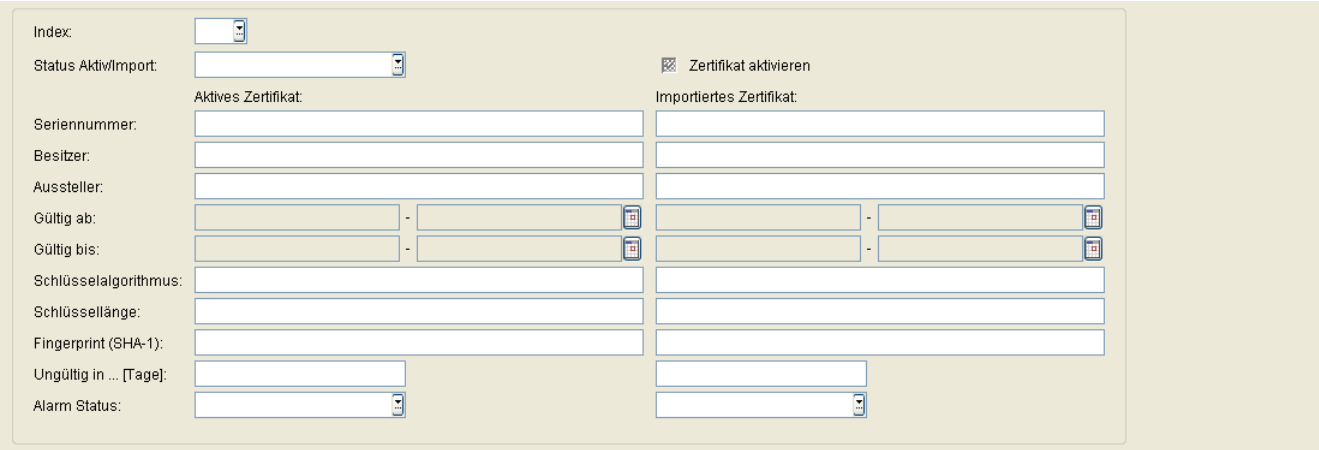


Parameterbeschreibung siehe Abschnitt 7.1.7.5, “Register „HTTPS Server CA Zertifikate“”.

7.1.7.9 Register „OCSR 2 Signature CA Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „OCSR 2 Signature CA Zertifikat“

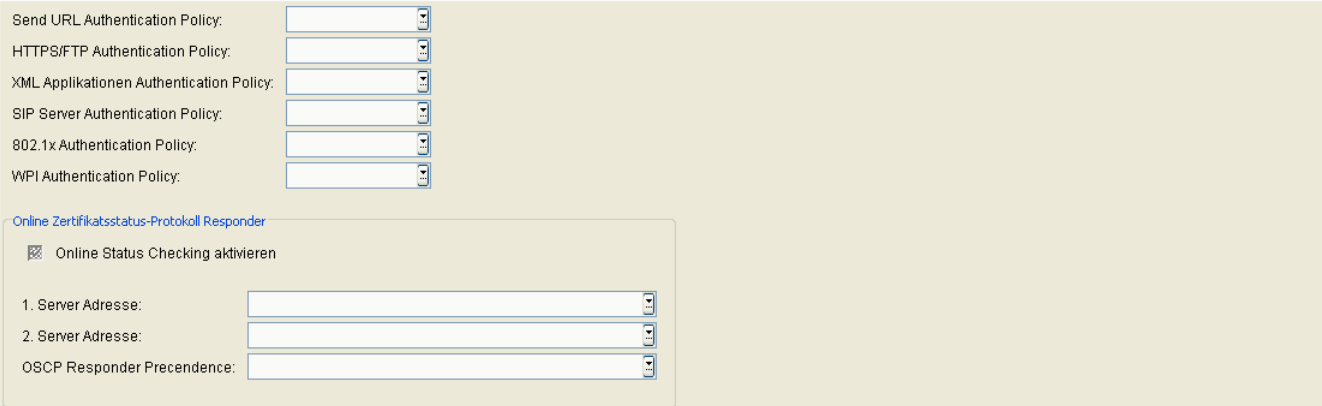
HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.



Parameterbeschreibung siehe Abschnitt 7.1.7.5, “Register „HTTPS Server CA Zertifikate“”.

7.1.7.10 Register „Certificate Policy“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „Certificate Policy“



Über dieses Register können Sie festlegen, wie sichere Verbindungen durch das Gerät authentifiziert werden.

Send URL Authentication Policy:

Die Authentifizierung des HTTPS Servers für Send URL ist hier beschrieben (siehe Abschnitt 7.1.19.3, “Register „Send URL Server CA Zertifikat“”).

Mögliche Werte:

- **Kein**
- **Trusted**
- **Voll**

HTTPS/FTP Authentication Policy

Die Authentifizierung des HTTPS-Servers für File Transfers ist hier beschrieben (siehe Abschnitt 6.3.5, “HTTPS Server Konfiguration” und Abschnitt 7.1.7.5, “Register „HTTPS Server CA Zertifikate“”).

Mögliche Werte:

- **Kein**
- **Trusted**
- **Voll**

XML Applikationen Authentication Policy:

Die Authentifizierung des XML-Applikationsservers ist hier beschrieben (siehe Abschnitt 7.1.14.5, “Register „CA Zertifikate“”).

Mögliche Werte:

- **Kein**
- **Trusted**
- **Voll**

SIP ServerAuthentication Policy:

Die Authentifizierung des SIP-Servers (nur für TLS Transport) ist hier beschrieben (siehe Abschnitt 7.1.21, “Signaling and Payload Encryption (SPE)”).

Mögliche Werte:

- **Kein**
- **Trusted**
- **Voll**

Parameter gültig ab OpenStage V3.0.

802.1x Authentication Policy:

Die Authentifizierung des 802.1x-Servers ist hier beschrieben (siehe Abschnitt 7.1.22, “IEEE 802.1x”).

Mögliche Werte:

- **Kein**
- **Trusted**
- **Voll**

Parameter gültig ab OpenStage V3.0.

WPI Authentication Policy:

Die Authentifizierung des DLS Work Point Interface (WPI) ist hier beschrieben (siehe Abschnitt 6.9.1, “Register „Secure Modus“”).

Mögliche Werte:

- **Trusted**

- **Voll**

Parameter gültig ab OpenStage V3.0.

Online Zertifikatsstatus-Protokoll Responder

Online Status Checking aktivieren

Mit diesem Schalter kann das Online Status Checking aktiviert werden.

1. Server Adresse

Erste Adresse des Servers für das Zertifikatsstatus-Protokoll.

Beispiel: „http://1.2.3.4“ oder „http://4.3.2.1:2560“ oder „http://host.example.org“.

2. Server Adresse

Zweite Adresse des Servers für das Zertifikatsstatus-Protokoll.

OSCP Responder Precendence

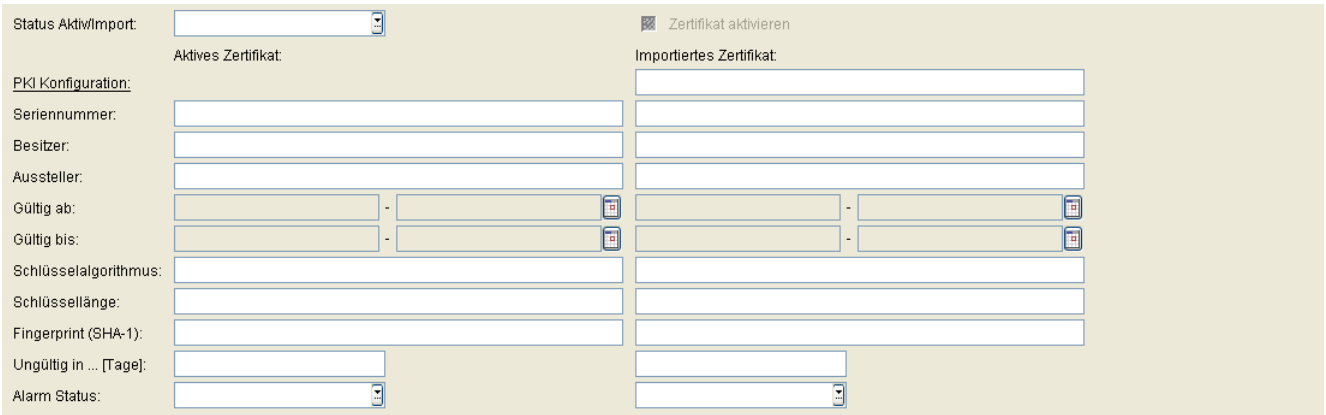
Mögliche Werte:

- **True**
- **False**

7.1.7.11 Register „HTTPS Client Certificates“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „HTTPS Client Certificates“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

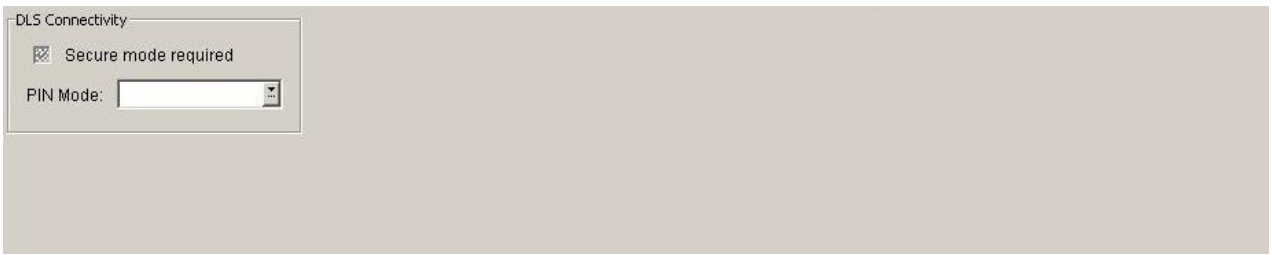


Über dieses Register können Sie ein Client-Zertifikat für die Authentifizierung des Geräts gegenüber dem HTTPS-Server für File Transfers importieren oder entfernen. Dies ist erforderlich, wenn der HTTPS-Server für die gegenseitige Authentifizierung konfiguriert ist.

Parameterbeschreibung siehe Abschnitt 7.1.7.4, “Register „WBM Server Zertifikat“”.

7.1.7.12 Register „DLS Verbindung“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Security Einstellungen > Register „DLS Verbindung“



Secure Modus erforderlich

Ist der Schalter aktiviert, wird die gegenseitige Authentifizierung von DLS und IP Device aktiviert. Der Authentifizierungsprozess (Bootstrap) wird angestoßen, sobald sich das IP Device das nächste Mal am DLS anmeldet bzw. vom DLS gescannt wird.

Dieser Schalter ist standardmäßig deaktiviert.

PIN Modus:

Mögliche Optionen:

- **Keine PIN**
  Die Zugangsdaten werden unverschlüsselt an das IP Device gesendet.
- **Standard PIN**
  Es wird eine für mehrere IP Devices definierte Standard-PIN benutzt. Diese wird automatisch vom DLS generiert (siehe Abschnitt 6.9.1, “Register „Secure Modus“”).
- **Individuelle PIN**
  Für das ausgewählte IP Device wird eine individuelle PIN erzeugt.

7.1.8 Telefonie

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Telefonie

Dieser Bereich besteht aus folgenden Inhalten:

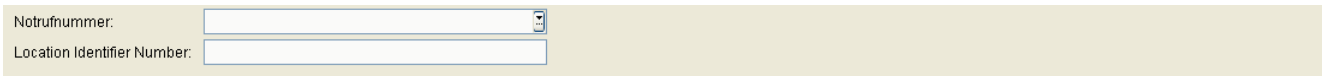
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Telefonie“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.8.1 Register „Telefonie“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Telefonie > Register „Telefonie“



Notrufnummer:

Enthält die Rufnummer, die in einem Notfall gewählt werden kann.

Location Identifier Number:

Enthält eine Identifizierungsnummer zur eindeutigen Identifizierung eines Ortes. Damit kann z. B. bei einem Notruf festgestellt werden, **wo** der Notruf abgesetzt wurde.

7.1.9 Small Remote Site Redundancy

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Small Remote Site Redundancy

Dieser Bereich besteht aus folgenden Inhalten:

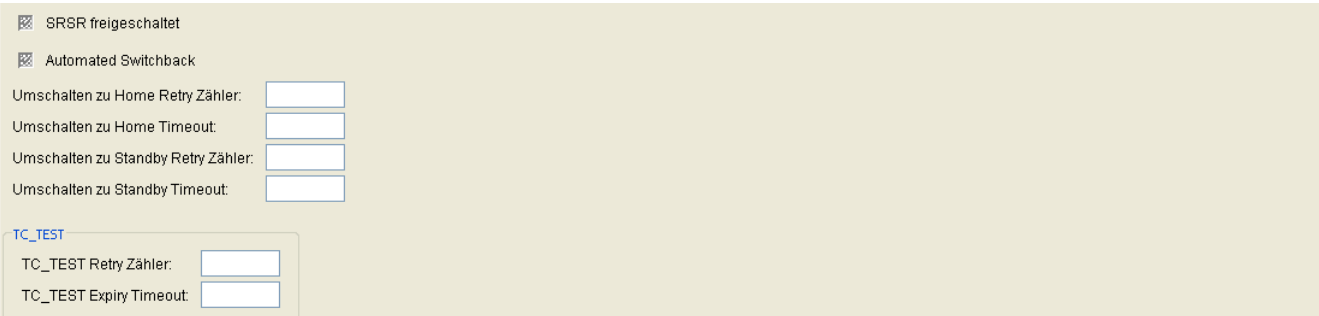
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SRSR Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.9.1 Register „SRSR Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Small Remote Site Redundancy > Register „SRSR Einstellungen“



SRSR freigeschaltet:

Schalter zum Aktivieren der Small Remote Site Redundancy.

Nur bei HFA-Workpoints verfügbar.

Automated Switchback:

Schalter zum Aktivieren der automatischen Rückschaltung zum Hauptsystem.

Nur bei HFA-Workpoints verfügbar.

Umschalten zu Home Retry Zähler:

Gibt an, wieviele Versuche bei der Umschaltung auf das Hauptsystem durchgeführt werden sollen.

Wertebereich: **1** ... **255**

Nur bei HFA-Workpoints verfügbar.

Umschalten zu Home Timeout:

Timeout für die Umschaltung auf das Hauptsystem.

Wertebereich: **1** ... **255** Sekunden.

Nur bei HFA-Workpoints verfügbar.

Umschalten zu Standby Retry Zähler:

Gibt an, wieviele Versuche bei der Umschaltung auf das Standby-System durchgeführt werden sollen.

Wertebereich: **1** ... **255**

Nur bei HFA-Workpoints verfügbar.

Umschalten zu Standby Timeout:

Timeout für die Umschaltung auf das Standby-System.

Wertebereich: **1** ... **255** Sekunden.

Nur bei HFA-Workpoints verfügbar.

TC_Test

TC_TEST Retry Zähler:

Gibt an, wieviele Versuche bei der Umschaltung auf das Hauptsystem positiv ausfallen müssen.

Wertebereich: **1** ... **255**

Nur bei HFA-Workpoints verfügbar.

TC_TEST Expiry Timeout:

Zeitraum für den erneuten Versuch zum Umschalten auf das Hauptsystem.

Wertebereich: **1** ... **255** Sekunden.

Nur bei HFA-Workpoints verfügbar.

7.1.10 Wahlparameter

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Wahlparameter

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Rufnummern“
- Register „Ziffernumwandlung“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.10.1 Register „Rufnummern“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Wahlparameter > Register „Rufnummern“

Die Wahlparameter werden benötigt, um Rufnummern im kanonischen Format korrekt aufzulösen (siehe Kapitel 17, “Kanonisches Format”).

Landeskennzahl:

Format: Ohne führende Nullen, max. 4 Stellen.

Beispiel: **49** für Deutschland.

Ortsnetzkennzahl:

Format: Ohne führende Nullen, max. 21 Stellen.

Beispiel: **89** für München.

Amtsrufnummer:

Rufnummer des Firmennetzes.

Format: Ohne führende Nullen und ohne Nebenstellen-Nummer, max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Nur für Geräte der optiPoint-Familie verfügbar.

Min. Länge lokale Nummer

Minimale Länge für eine lokale Rufnummer, d. h. für eine Nummer innerhalb eines Vorwahlbereichs.

Beispiel: In München (Vorwahlbereich 089) ist die Mindestlänge **6**.

Nur für Geräte der OpenStage-Familie verfügbar.

Operator Code(s):

Nummer/Ziffer, um mit dem Operator verbunden zu werden.

Nur für Geräte der OpenStage-Familie verfügbar.

Erweiterungsziffer(n)

Liste von Anfangsziffern aller im Firmennetz möglichen Nebenstellennummern. Wenn eine Rufnummer nicht als Nummer des öffentlichen Netzes erkannt wird, prüft das Telefon, ob sie zum lokalen Firmennetzwerk gehört. Hierzu wird die Anfangsziffer der Rufnummer mit dem/den hier angegebenen Wert(en) verglichen. Stimmen die beiden Werte überein, so wird die Rufnummer als firmeninterne Nummer erkannt und entsprechend verarbeitet.

Beispiel: Wenn die Nebenstellennummern 3000-5999 in OpenScape Voice konfiguriert sind, so beginnt jede Nummer mit 3, 4 oder 5. Somit sind hier die Ziffern **3, 4, 5** einzutragen.

Internationale Vorwahl:

Nationale Vorwahlnummer.

Format: max. 4 Stellen.

Beispiel: **00** in Deutschland.

Nationale Vorwahl:

Internationale Vorwahlnummer.

Format: max. 5 Stellen.

Beispiel: **0** in Deutschland.

Amtskennzahl:

Nummer zur „Amtsholung“ eines ausgehenden, externen Gesprächs.

Format: max. 5 Stellen.

Beispiele: **0**, **74**, **9** (USA).

Lokaler Firmencode:

Rufnummer des Firmennetzes.

Beispiel: **722** für Unify München Hofmannstraße.

Nur für Geräte der OpenStage-Familie verfügbar.

Notrufnummer(n):

Hier können eine oder mehrere Notrufnummern eingegeben werden.

Nur für Geräte der OpenStage-Familie verfügbar.

Wählformat internationale Nummern:

Mögliche Optionen:

- **Lokales Format des Unternehmens**
- **Knoten immer hinzufügen**
- **Verwende externe Nummern**

Wählformat externe Nummern:

Mögliche Optionen:

- **Lokales öffentliches Format**
- **Nationales öffentliches Format**
- **Internationales öffentliches Format**

Amtskennziffer erforderlich:

Mögliche Optionen:

- **Nicht benötigt**
- **Für externe Nummern**

Internationale Amtskennziffer erforderlich

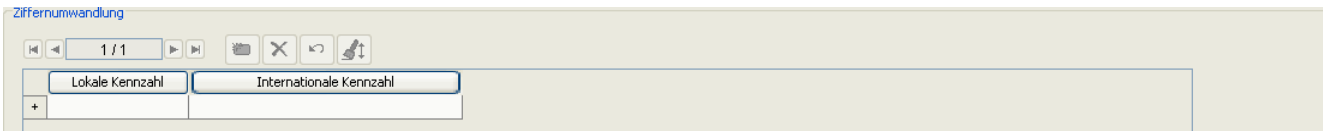
Mögliche Optionen:

- **Verwende nationalen Code**
- **Unverändert**

7.1.10.2 Register „Ziffernumwandlung“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Wahlparameter > Register „Ziffernumwandlung“

Diese Funktion ordnet die Eingabe im ersten Feld („Lokale Kennzahl“) in eine bestimmte Ziffernfolge um, die im zweiten Feld („Internationale Kennzahl“) festgelegt wird. Diese Ziffernfolge kann z. B. eine nationale oder internationale Vorwahl sein. Auf diese Weise können häufig benutzte Vorwahlen durch Eingabe nur einer Ziffer gewählt werden.



Lokale Kennzahl

Ziffer bzw. kurze Ziffernfolge, mithilfe der Benutzer z. B. eine bestimmte Vorwahl wählen will.

Internationale Kennzahl

Ziffernfolge, beispielsweise Vorwahl, die bei der Eingabe einer bestimmten Ziffer zu Beginn des Wählvorgangs gewählt wird.

7.1.11 Uhrzeit Einstellungen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Uhrzeit Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

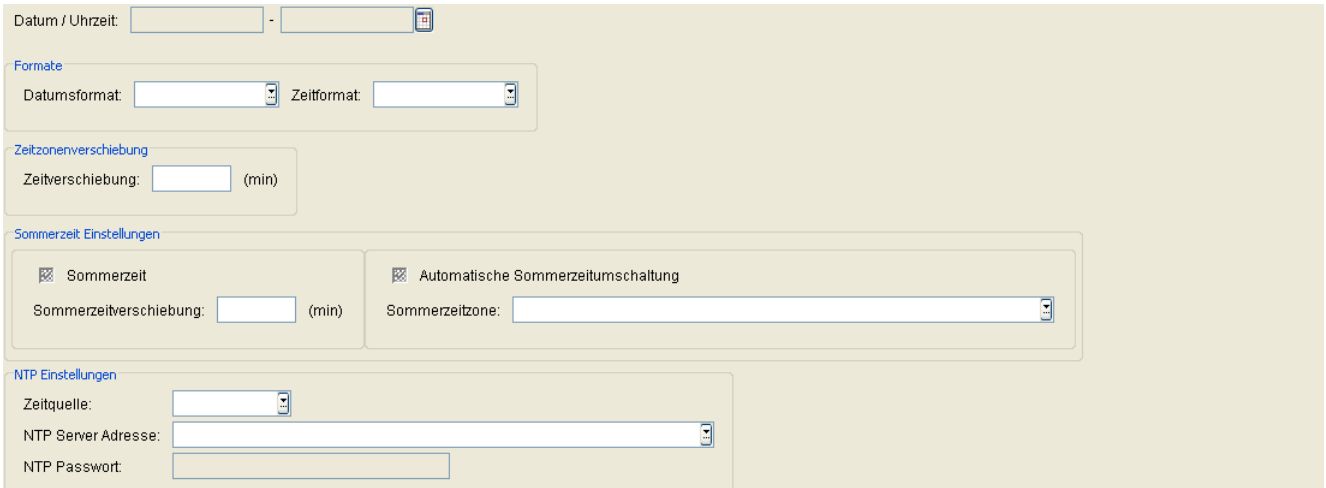
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Zeit“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-JobKapitel 14, “Job Koordination”s einfach und komfortabel automatisieren (siehe).

7.1.11.1 Register „Zeit“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Uhrzeit Einstellungen > Register „Zeit“



Datum / Uhrzeit:

Aktuelles Datum und Uhrzeit eingeben. Die manuelle Festlegung ist nur notwendig, wenn diese Informationen nicht automatisch übermittelt werden (z. B. PBX oder DHCP-Server).

Formate

Datumsformat:

Format der Datumsangabe. Die manuelle Festlegung ist nur notwendig, wenn diese Informationen nicht automatisch durch das Kommunikationssystem (z. B. OpenScape Voice) übermittelt werden.

Mögliche Optionen:

- **TT.MM.JJ**
  Beispiel: 05.10.06 für 5.10.2006
- **JJ-MM-TT**
  Beispiel: 04-10-06 für 5.10.2006
- **MM/TT/JJ**
  Beispiel: 10/05/06 für 5.10.2006

Zeitformat:

Format der Zeitangabe.

Mögliche Optionen:

- **24 Stunden**
- **12 Stunden**

Zeitzonenverschiebung

Zeitverschiebung:

Differenz zur Standardzeit UTC (Coordinated Universal Time) in Minuten.

Wertebereich: **-720** ... **720.**

Beispiele: **60** (Telefon steht in München); **-480** (Telefon steht in Los Angeles, USA).

Sommerzeit Einstellungen

Sommerzeit

Schalter zum Aktivieren der Sommerzeit-Funktion.

HINWEIS: Wenn **Automatische Sommerzeitumschaltung** deaktiviert ist oder kein SNTP-Server eingesetzt wird, muss manuell zwischen Sommer und Winterzeit umgeschaltet werden. Der Zustand des Schalters **Sommerzeit** muss hierfür zweimal jährlich geändert werden. Das ist insbesondere bei der Verwendung dieses Parameters innerhalb von Template-Daten zu beachten.

Sommerzeitverschiebung:

Differenz in Minuten zur Normal- bzw. Winterzeit.

Wertebereich: **0** ... **60**

Automatische Sommerzeitumschaltung:

Ist der Schalter aktiviert, wird die Sommerzeit nach der Regel der gewählten Sommerzeitzonen automatisch umgeschaltet. Start- und Enddatum der Sommerzeit für diese Sommerzeitzone sind damit definiert.

HINWEIS: Bei OpenStage-Telefonen muss der Schalter **Sommerzeit** aktiviert sein, damit die automatische Sommerzeitumschaltung in Kraft treten kann.

Sommerzeitzone:

Mögliche Optionen:

- **nicht gesetzt**

- **Australien 2007 (ACT, Südaustralien, Tasmanien, Viktoria)**
- **Australien 2007 (Neusüdwales)**
- **Australien (Westaustralien)**
- **Australien 2008+ (ACT, Neusüdwales, Südaustralien, Tasmanien, Viktoria)**
- **Brasilien**
- **Kanada**
- **Kanada (Neufundland)**
- **Europa (PT, UK)**
- **Europa (AT, BE, HR, DK, FR, DE, HU, IT, LU, NL, NO, PL, SK, ES, SE, CH)**
- **Europa (FI)**
- **Mexiko**
- **USA**

NTP Einstellungen

Zeitquelle:

Quelle, von der die Zeitinformation übernommen wird.

Mögliche Optionen:

- **System**
  Die Zeitinformation wird von der Kommunikationsplattform übernommen.
- **SNTP**
  Die Zeitinformation stammt vom SNTP-Server (wenn vorhanden).

NTP Server Adresse:

IP-Adresse oder Hostname des SNTP-Servers, falls ein SNTP-Server verfügbar ist.

NTP Passwort:

Falls erforderlich, wird hier ein Passwort für den SNTP-Server eingegeben. Dieser Parameter ist nur für OpenStage-Telefone verfügbar.

7.1.12 Audio Einstellungen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Audio Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

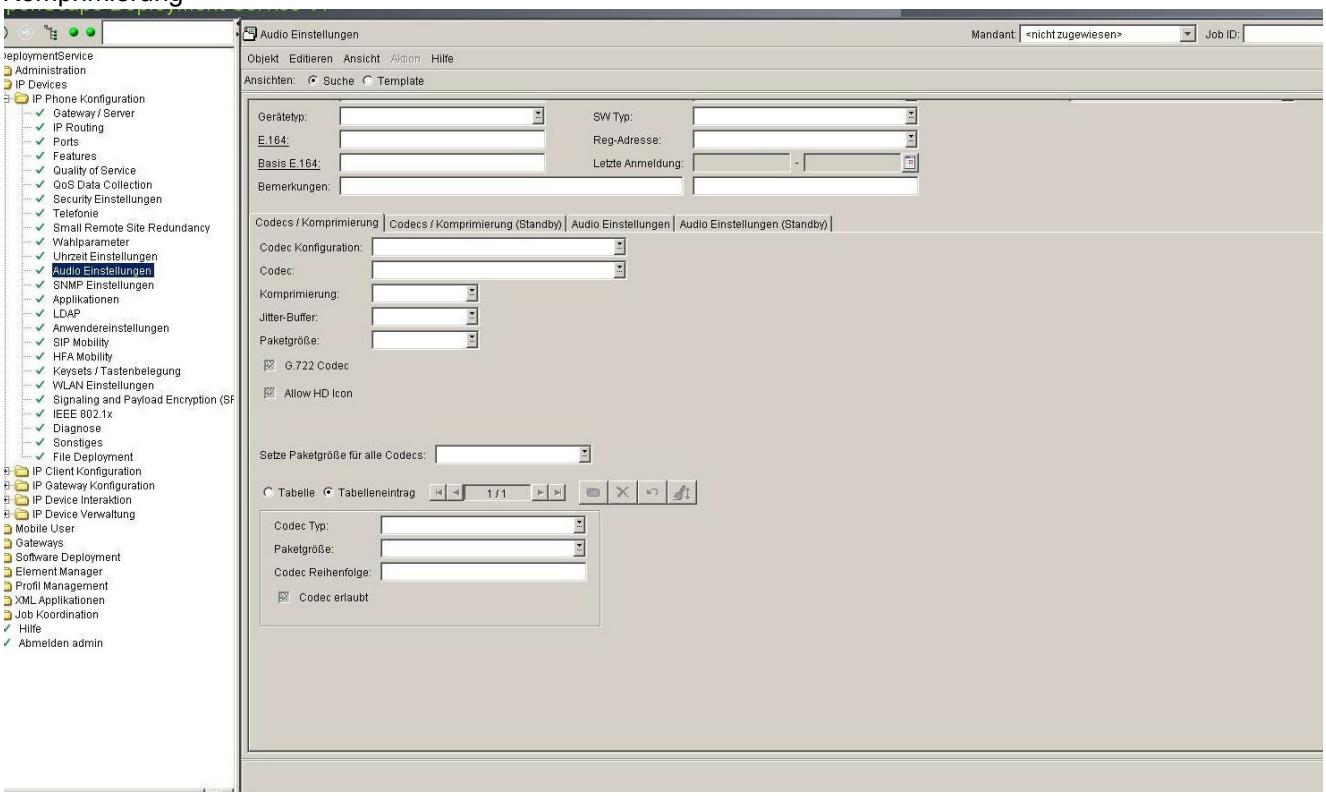
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Codecs / Komprimierung“
- Register „Codecs / Komprimierung (Standby)“
- Register „Audio Einstellungen“
- Register „Audio Einstellungen (Standby)“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.12.1 Register „Codecs / Komprimierung“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Audio Einstellungen > Register „Codecs / Komprimierung“



Für die Geräte der OpenStage-Familie werden die Einstellungen in der Tabelle vorgenommen, da bei diesen Telefone die Angabe mehrerer alternativer Codecs über eine Auflistung der einzelnen Codecs erfolgt.

Codec Konfiguration:

Eingesetztes Audio-Übertragungsprinzip (Codec) für WLAN-Phones einstellen.

Mögliche Optionen:

- **G.711 Bevorzugt (normale Qualität)**
- **G.722 Bevorzugt (hohe Qualität)**
- **G.723 Bevorzugt (niedere Bandbreite)**
- **G.729 A/B bevorzugt (niedere Bandbreite)**
- **G.723 Immer (niedere Bandbreite)**
- **G.729 A/B Immer (niedere Bandbreite)**

Codec:

Eingesetztes Audio-Übertragungsprinzip (Codec).

Mögliche Optionen:

- **Ausschließlich komprimierte Sprachübertragung**
  Für die optiPoint 410/420/600-Familien.
- **Bevorzugt High Quality Sprachübertragung**
  Für die optiPoint 410/420/600-Familien.
- **Bevorzugt komprimierte Sprachübertragung**
  Für die optiPoint 410/420/600-Familien.
- **G.711 Bevorzugt**
  Für die optiPoint 400-Familie.
- **G.723 Bevorzugt**
  Für die optiPoint 400-Familie.
- **G.723 Immer**
  Für die optiPoint 400-Familie.

Komprimierung:

Komprimierungsverfahren, wenn der Codec „LoBand“ gewählt wurde.

Mögliche Optionen:

- **G.723**
- **G.729**

Jitter-Buffer:

Dauer der Zwischenspeicherung (Anzahl der Datenpakete).

Mögliche Optionen:

- **Kurz**
  2 Pakete
- **Lang**
  6 Pakete
- **Normal**
  4 Pakete

Paketgröße:

Mögliche Optionen:

- **10mS**
- **20mS**
- **30mS**
- **Automatisch**

G.722 Codec:

Schalter zum Aktivieren des G.722-Codec.

Allow HD Icon:

Schalter zum Aktivieren des HD-Audio-Symbols mithilfe von DLS.

Diese Funktion steuert die Anzeige des HD-Breitband-Audio-Symbols. Diese Funktion ist standardmäßig aktiviert.

Setze Paketgröße für alle Codecs:

Für alle Codecs kann die Paketgröße auf einen gemeinsamen Wert gesetzt werden.

Mögliche Optionen:

- **10mS**
- **20mS**
- **30mS**
- **Automatisch**

Codec Typ

Eingesetztes Audio-Übertragungsprinzip (Codec).

Mögliche Optionen:

- **G.711**
- **G.722**
- **G.729**

Paketgröße

Größe der Pakete, in denen die Audio-Datenpakete versendet werden. Die Angabe erfolgt in Millisekunden.

- **Automatisch**
- **10 ms**
- **20 ms**
- **30 ms**

Codec Reihenfolge

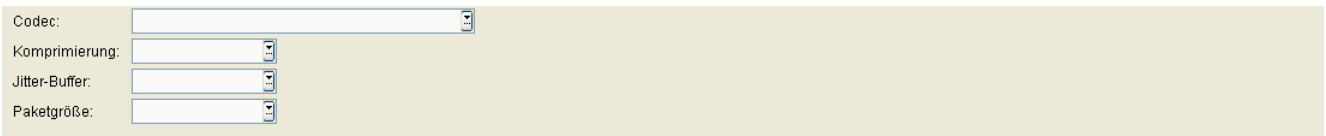
Jedem verfügbaren Codec wird eine Priorität zugeordnet. Diese wird beim Aushandeln des benützten Codecs zwischen zwei Geräten verwendet. Wertebereich: eine Zahl zwischen 1 und der Anzahl der verfügbaren Codecs.

Codec erlaubt

Die Verwendung eines Codecs kann explizit erlaubt oder untersagt werden.

7.1.12.2 Register „Codecs / Komprimierung (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Audio Einstellungen > Register „Codecs / Komprimierung (Standby)“



Codec:

Eingesetztes Audio-Übertragungsprinzip (Codec).

Mögliche Optionen:

- **Ausschließlich komprimierte Sprachübertragung**
  Für die optiPoint 410/420/600-Familien.
- **Bevorzugt High Quality Sprachübertragung**
  Für die optiPoint 410/420/600-Familien.
- **Bevorzugt komprimierte Sprachübertragung**
  Für die optiPoint 410/420/600-Familien.
- **G.711 Bevorzugt**
  Für die optiPoint 400-Familie.
- **G.723 Bevorzugt**
  Für die optiPoint 400-Familie.
- **G.723 Immer**
  Für die optiPoint 400-Familie.

Komprimierung:

Komprimierungsverfahren, wenn der Codec „LoBand“ gewählt wurde.

Mögliche Optionen:

- **G.723**
- **G.729**

Jitter-Buffer:

Dauer der Zwischenspeicherung (Anzahl der Datenpakete).

Mögliche Optionen:

- **Kurz**
  2 Pakete
- **Lang**
  6 Pakete
- **Normal**
  4 Pakete

Paketgröße:

Mögliche Optionen:

- **10mS**
- **20mS**
- **30mS**

7.1.12.3 Register „Audio Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Audio Einstellungen > Register „Audio Einstellungen“

Rauschunterdrückung bei Gesprächsruhe

Schalter zum Aktivieren der Rauschunterdrückung bei Gesprächsruhe.

Mikrophon abschalten

Schalter zum Ausschalten des Mikrophons.

Spezialwählton bei Sprachnachricht

Ist der Schalter aktiviert, so ertönt beim Abnehmen des Hörers ein spezieller Wählton, um den Benutzer auf neu eingegangene Sprachnachrichten aufmerksam zu machen.

Freisprechen einschalten

Schalter zum Einschalten der Freisprech-Funktion.

Wartemusik

Schalter zum Aktivieren der Wartemusik.

Wiedergabe DTMF (RCF 2833)

Schalter zum Aktivieren der Wiedergabe von DTMF-Tönen (RFC 2833). Nur für Endgeräte des Typs optiPoint SIP V7.

Lower IL alert notification

Schalter zum Aktivieren der Funktion „Benachrichtigungs-Popup/Ton unterdrücken“ bei Ebenenwechsel während eines Anrufs (verbunden oder Hinweis) oder beim Verbinden eines Anruf ohne Rufton. Dieses Funktion ist standardmäßig aktiviert.

Einstellungen für AUN Gruppe

Aufmerksamkeitston für AUN Gruppe erlaubt

Aktiviert oder deaktiviert die Erzeugung eines akustischen Signals für einen eingehenden Anruf innerhalb der AUN-Gruppe (Anrufübernahme-Gruppe).

Benutze Anrufton für AUN Gruppe

Ist das Kästchen angehakt, so wird ein Anruf innerhalb der AUN-Gruppe durch einem kurzen Standard-Klingelton signalisiert. Wenn nicht, wird ein solcher Anruf durch einen kurzen Aufmerksamkeitston signalisiert.

Hinweisart bei AUN Gruppe:

Auswahl der benutzerseitigen Aktionen, um einen Anruf innerhalb der AUN-Gruppe entgegenzunehmen.

Mögliche Optionen:

- **Prompt**
  Der AUN-Anruf wird auf dem Display durch einen Alert angezeigt. Sobald der Benutzer den Hörer abhebt oder die Lautsprechertaste drückt, wird der Anruf angenommen. Auch durch eine entsprechend eingerichtete Funktionstaste kann der Anruf angenommen werden.
- **Notify**
  Der AUN-Anruf wird auf dem Display durch einen Alert angezeigt. Um den Anruf anzunehmen, muss der Benutzer den Alert bestätigen oder die entsprechend eingerichtete Funktionstaste drücken.
- **FPK only**

  Der AUN-Anruf wird nur auf der entsprechend eingerichteten Funktionstaste angezeigt. Um den Anruf anzunehmen, muss der Benutzer diese Funktionstaste drücken.

Rufton-Einstellungen (SIP)

Rufton-Melodie:

Mögliche Optionen:

Kein.	SIP	HFA	Frequenzen (Hz)			Tonlängen (ms)		
			f1	f2	f3	c1	c2	c3
1	Ja	Ja	457	571	615	45	45	45
2	Ja	Ja	696	762	1067	30	30	30
3	Ja	Ja	400	444	500	35	35	35
4	Ja	Ja	1067	889	696	50	50	50
5	Ja	Ja	762	800	889	30	30	30
6	Ja	Ja	1000	1143	1333	40	40	40
7	Ja	Ja	400	457	593	50	50	50
8	Ja	Ja	533	0	667	90	150	60

Rufton-Folge:

Mögliche Optionen:

- **1 sek EIN, 4 sek AUS**
- **1 sek EIN, 2 sek AUS**
- **0,7 sek EIN, 0,7 sek AUS, 0,7 sek EIN, 3 sek AUS**

Rufton-Datei:

Name der Datei, die den Rufton enthält.

Lower IL Ringer

Name der Datei, die den spezifischen Rufton enthält, der bei Anrufen von einem Lower Impact Level anstelle des normalen Ruftons verwendet werden soll.

Rufton Einstellungen (HFA)

Rufton Modus:

Mögliche Werte:

- **HiPath**

- **Lokaler Rufton**

Rufton durch Benutzer änderbar

Ist der Schalter gesetzt, darf der Benutzer den Rufton ändern.

BLF

BLF Signalisierung

Optische Signalisierung auf Taste des akustischen Signals.

Mögliche Werte:

- **Beep**
- **Rufton**

Headset

Headset Modus

Bauart des Headsets.

Mögliche Werte:

- **Headset mit Kabel**
- **Kabelloses Headset**
- **Konferenzeinheit**

Tastenklick

Lautstärke:

Lautstärke des Tastenklicks einstellen.

Mögliche Werte:

- **Aus**
- **Niedrig**
- **Mittel**
- **Hoch**

Tasten:

Tastenart, für die Tastenklick hörbar sein soll, einstellen.

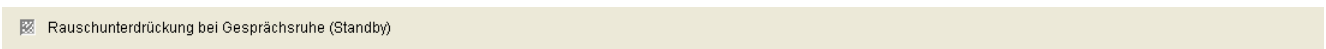
Mögliche Werte:

- **Nur Wähltastatur**
- **Alle Tasten**

7.1.12.4 Register „Audio Einstellungen (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Audio Einstellungen > Register „Audio Einstellungen (Standby)“

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „Audio Einstellungen“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.1.9, “Small Remote Site Redundancy”.



Rauschunterdrückung bei Gesprächsruhe (Standby)

Schalter zum Aktivieren der Rauschunterdrückung bei Gesprächsruhe.

7.1.13 SNMP Einstellungen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SNMP Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

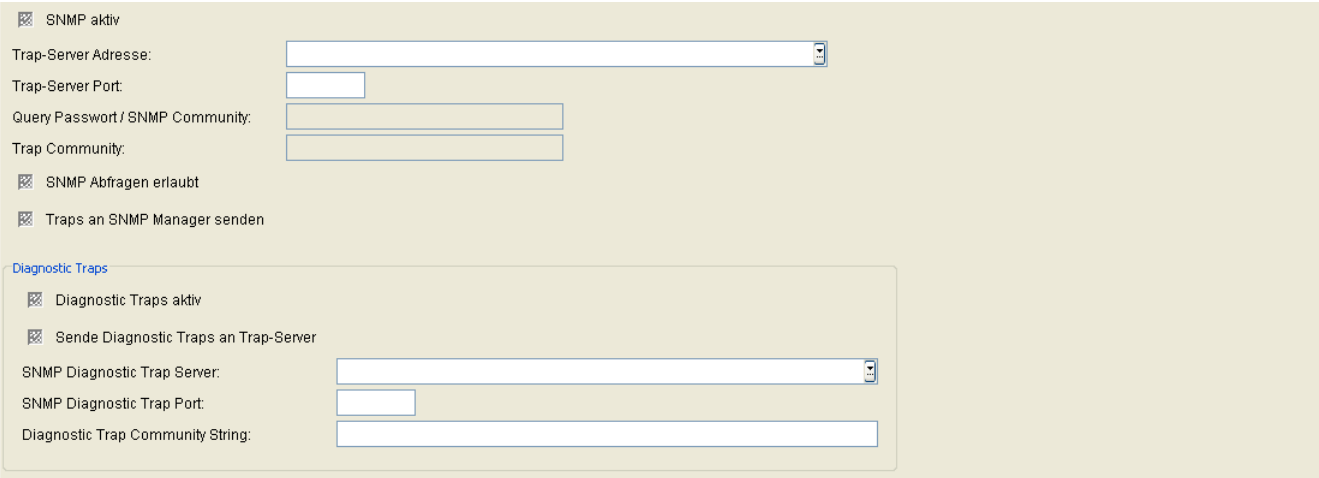
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SNMP“
- Register „Zertifikat Alarm Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.13.1 Register „SNMP“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SNMP Einstellungen > Register „SNMP“



SNMP aktiv

Schalter zum Aktivieren der SNMP-Funktion.

Trap-Server Adresse:

IP-Adresse oder Hostname des SNMP Trap-Servers.

Trap-Server Port:

Portnummer des SNMP Trap-Servers.

Query Passwort / SNMP Community:

Community String, der zum Autorisieren am SNMP-Server verwendet wird.

Trap Community:

SNMP community string für den SNMP Manager, der die Trap-Nachrichten empfängt.

SNMP Abfragen erlaubt

Schalter zum Aktivieren der Erlaubnis, QDC-Daten per SNMP abzufragen.

Traps an SNMP Manager senden

Schalter zum Aktivieren der Funktion, dass QDC-Daten zusätzlich auch an einen SNMP-Manager gesendet werden.

Diagnostic Traps

Diagnostic Traps aktiv

Ist der Schalter aktiv, werden Diagnostic Traps gesendet.

Sende Diagnostic Traps an Trap-Server

Ist der Schalter aktiv, werden die Diagnostic Traps an den konfigurierten Trap-Server gesendet.

SNMP Diagnostic Trap Server:

Hostname oder IP-Adresse des SNMP-Servers, der Diagnostic Traps empfängt.

SNMP Diagnostic Trap Port:

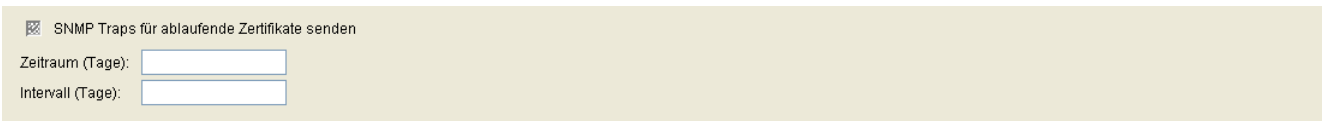
Port, auf dem der SNMP-Server Diagnostic Traps empfängt.

Diagnostic Trap Community String:

Community String zur Authentifizierung am SNMP-Server, der Diagnostic Traps empfängt.

7.1.13.2 Register „Zertifikat Alarm Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SNMP Einstellungen > Register „Zertifikat Alarm Einstellungen“



SNMP Traps für ablaufende Zertifikate senden

Ist der Schalter aktiviert, werden für das ablaufende Zertifikat SNMP-Traps an die in den SNMP Einstellungen (siehe Register „SNMP“) angegebene Adresse geschickt.

Zeitraum (Tage):

Anzahl der Tage vor Ablauf des Zertifikats bevor der erste SNMP Trap gesendet wird.

Intervall (Tage):

Anzahl der Tage bis ein SNMP Trap für ein ablaufendes Zertifikat erneut gesendet wird.

7.1.14 Applikationen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen

Dieser Bereich besteht aus folgenden Inhalten:

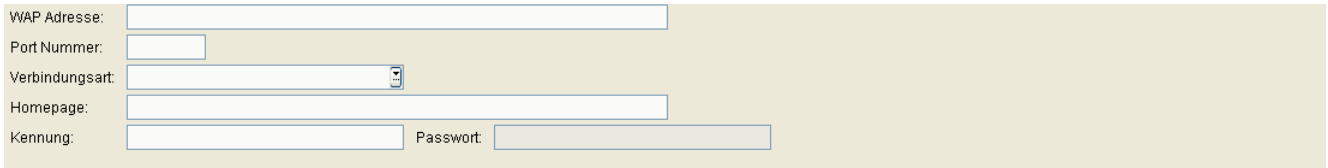
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „WAP“
- Register „Java“
- Register „XML Applikationen“
- Register „CA Zertifikate“
- Register „Applikationsliste“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.14.1 Register „WAP“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen > Register „WAP“



WAP Adresse:

IP-Adresse oder Hostname des WAP-Servers.

Port Nummer:

Portnummer des WAP-Servers.

Verbindungsart:

Protokoll-Typ der Verbindung zum WAP-Server.

Mögliche Optionen:

- **HTTP**
- **WSP**

Homepage:

URL der Startseite, auf der sich die WAP-Homepage befindet.

Kennung:

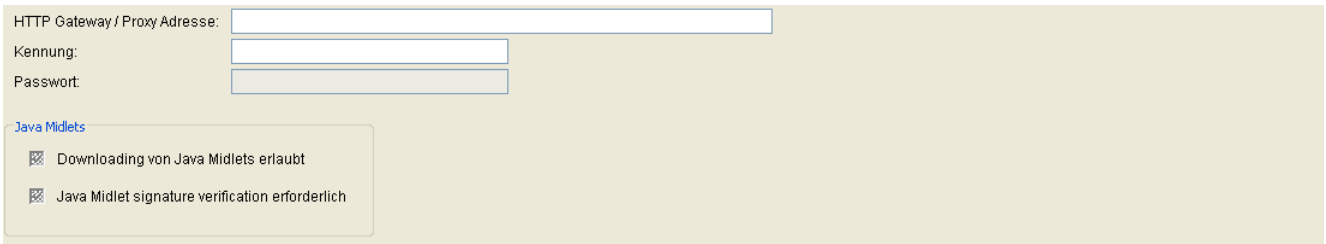
Benutzerkennung zur Identifikation am WAP-Server

Passwort:

Passwort der Benutzerkennung.

7.1.14.2 Register „Java“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen > Register „Java“



HTTP Gateway / Proxy Adresse:

IP-Adresse oder Hostname des HTTP-Servers.

Kennung:

Benutzerkennung zur Identifikation am HTTP-Gateway.

Passwort:

Passwort zur Benutzerkennung.

Java Midlets

Downloading von Java Midlets erlaubt

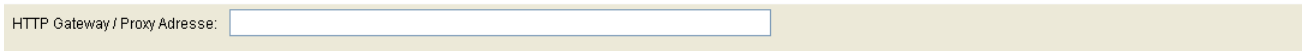
Ist der Schalter aktiviert, ist das Herunterladen von Java-Midlets auf den Workpoint erlaubt.

Java Midlet signature verification erforderlich

Ist der Schalter aktiviert, wird die Verifizierung des Java-Midlets mithilfe einer Signatur verlangt.

7.1.14.3 Register „Java (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen > Register „Java“

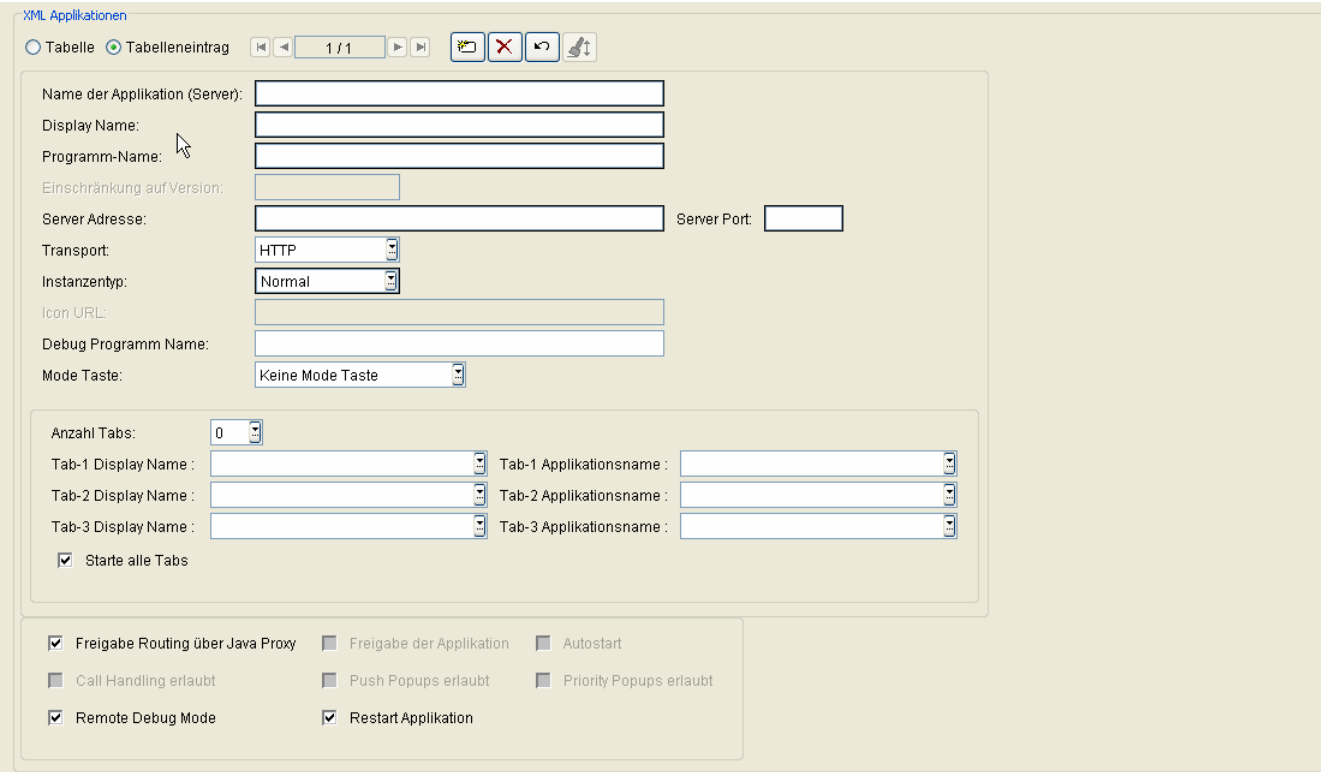


HTTP Gateway / Proxy Adresse:

IP-Adresse oder Hostname des HTTP-Servers.

7.1.14.4 Register „XML Applikationen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen > Register „XML Applikationen“



Dies sind serverseitige Applikationen, die über eine eigens definierte XML-Schnittstelle mit der Software des Telefons kommunizieren. Auch das Unified-Messaging-System HiPath Xpressions verwendet diese Schnittstelle. Sie ermöglicht es dem Workpoint, Benutzereingaben zu versenden, Daten in Text- und grafischer Form anzuzeigen, sowie Anrufe zu steuern.

Um eine XML-Applikation auf dem Workpoint einzurichten, müssen die folgenden Angaben gemacht werden: frei wählbarer Programmname; verwendetes Kommunikationsprotokoll; verwendeter Port des Servers; Startadresse des serverseitigen Programms.

XML Applikationen sind nur auf OpenStage 60/80 verfügbar.

XML Applikationen

Name der Applikation (Server):

Dieser Name wird von der Software des Workpoints intern benutzt, um die Applikation zu identifizieren.

Für DLS XML Applikationen sind die Namen unverändert einzutragen.

Mögliche Werte:

- **DeploymentService**

- **LocationService**
- **NewsService**
- **MakeCall**

Display Name:

Unter diesem Namen wird die Applikation auf dem Menü des Workpoints aufgelistet.

Programm-Name:

Pfad der Startdatei des serverseitigen Programms, relativ zur Server-Adresse. Für DLS XML Applikationen ist der WEB-Applikations-Name gefolgt vom HTTP-Servlet-Namen unverändert einzutragen.

Einschränkung auf Version:

Auswahl einer definierten Version, mit der gearbeitet werden soll.

Server Adresse:

IP-Adresse des Servers, auf dem das Programm läuft. Für DLS XML Applikationen ist die IP Adresse des DLS Server einzutragen, im Falle einer Multi-Node-Installation die IP-Adresse des Clusters.

Beispiel: **192.168.1.150.**

Server Port:

Port, auf dem das serverseitige Programm Daten vom Workpoint empfängt. Für DLS XML Applikationen ist Port 18080 einzutragen, da nur HTTP unterstützt wird.

Beispiele: **80** (Default-Port Apache); **8080** (Default-Port Tomcat).

Transport:

Transportprotokoll für die Übermittlung der XML-Daten.

Mögliche Optionen:

- **HTTP**
- **HTTPS**

Instanzentyp:

Auswahl des Instanzentyps.

Mögliche Optionen:

- **Normal**
- **Xpressions**
- **Phonebook**

Icon URL:

URL des Applikations-Icons (noch nicht implementiert).

Debug Programm Name:

Name und ggf. Verzeichnispfad des Programms auf dem Server, das Fehlermeldungen der XML-Applikationsplattform des Endgeräts entgegennimmt.

Mode Taste:

Auswahl einer Mode-Taste, mit der die Applikation gestartet wird.

Mögliche Optionen:

- **Keine Mode Taste**
- **Phonebook-Mode Taste**
- **Call-Mode Taste**
- **Message-Mode Taste**
- **Hilfe-Mode Taste**

Anzahl Tabs:

Anzahl der Tabs in einer XML Applikation, die im Display des Endgerätes angezeigt werden.

Wertebereich: **0** ... **3**

HINWEIS: Für alle XML-Applikationen, die eine Anzahl Tabs > 0 eingetragen haben, muss zwingend einer der Einträge für **Tab-1 Applikationsname** bis **Tab-3 Applikationsname** gleich dem Eintrag in **Name der Applikation (Server)** sein. Beim Start der XML-Applikation wird dann der Tab mit dem gleichen Namen als Erster geöffnet.

Tab-1 Display Name

Beschriftung des 1. Tabs zur Anzeige im Display des Endgerätes.

Tab-2 Display Name

Beschriftung des 2. Tabs zur Anzeige im Display des Endgerätes.

Tab-3 Display Name

Beschriftung des 3. Tabs zur Anzeige im Display des Endgerätes.

Tab-1 Applikationsname

Aufrufname der Applikation, die im 1. Tab aufgerufen wird. Er muss über alle XML Applikationen hinweg eindeutig sein.

Tab-2 Applikationsname

Aufrufname der Applikation, die im 2. Tab aufgerufen wird. Er muss über alle XML Applikationen hinweg eindeutig sein.

Tab-3 Applikationsname

Aufrufname der Applikation, die im 3. Tab aufgerufen wird. Er muss über alle XML Applikationen hinweg eindeutig sein.

Starte alle Tabs

Beim Start der Applikation werden alle Tabs geöffnet.

Freigabe Routing über Java Proxy

Schalter für die Freigabe des Routings über Java Proxy.

Freigabe der Applikation

Schalter zum Einschalten der Applikation.

Autostart

Schalter zum Aktivieren des Autostarts der Applikation.

Call Handling erlaubt

Schalter zum Aktivieren des Call Handlings.

Push Popups erlaubt

Schalter zum Aktivieren des Push Popups.

Priority Popups erlaubt

Schalter zum Aktivieren von priorisierten Popups.

Remote Debug Mode

Schalter zum Aktivieren des Remote Debug Modus.

Restart Applikation

Neustart der Applikation, wenn diese bereits läuft.

7.1.14.5 Register „CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen > Register „CA Zertifikate“

Die nachfolgend beschriebenen Parameter stehen einmal für das derzeit aktive und einmal für das importierte Zertifikat zur Verfügung.

Index:

Laufende Nummer des CA Zertifikats.

Status Aktiv/Import:

Gibt an, ob ein Zertifikat importiert und/oder aktiv auf dem Phone registriert ist. Daraus ergeben sich die nachfolgend genannten 5 Zustände.

Mögliche Werte:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Seriennummer:

Seriennummer des Zertifikats (nur Anzeige).

Besitzer:

Besitzer des Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Anzahl der verbleibenden Tage, bis das Zertifikat ungültig wird.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Anzeige der Gültigkeitsdauer von Zertifikaten, um in Kürze ablaufende Zertifikate zu suchen.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

Zertifikat aktivieren

Schalter zum Aktivieren des Zertifikats. Das aktive Zertifikat wird für die Verschlüsselung von Gesprächen verwendet. Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

7.1.14.6 Register „Applikationsliste“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Applikationen > Register „Applikationsliste“

Liste von Applikationen für Funktionstasten:

Liste von durch Komma getrennten Applikationsnamen, die mittels Funktionstasten gestartet werden können.

7.1.15 LDAP

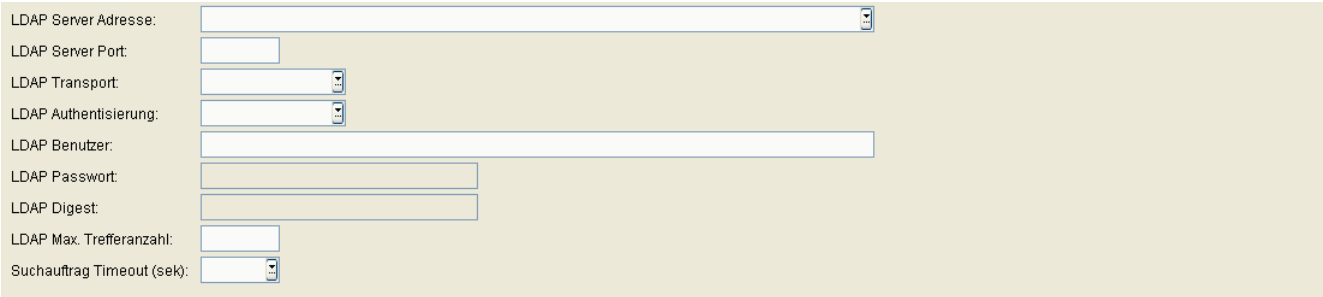
Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > LDAP

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „LDAP Einstellungen“
- Register „CA Zertifikate“

7.1.15.1 Register „LDAP Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > LDAP > Register „LDAP Einstellungen“



HINWEIS: LDAP-Servereinstellungen gelten auch für OpenStage 15/20- (nur SIP) und OpenScape Desk Phone IP 35 G-Telefone.

LDAP Server Adresse:

IP-Adresse oder Hostname des LDAP-Servers.

LDAP Server Port:

Portnummer des LDAP-Servers.

LDAP Transport:

Transportprotokoll, mit dem LDAP-Daten übertragen werden.

Mögliche Optionen:

- **TCP**

LDAP Authentifizierung:

Auswahl des LDAP-Zugangs.

Mögliche Optionen:

- **Anonym**
- **Einfach**

LDAP Benutzer:

Benutzername für den authentifizierten LDAP-Zugang.

LDAP Passwort:

Passwort für den authentifizierten LDAP-Zugang.

LDAP Digest:

Eintrag des LDAP Digest.

LDAP Max. Trefferanzahl:

Maximale Anzahl von Treffern bei der LDAP-Suche.

Suchauftrag Timeout (sek):

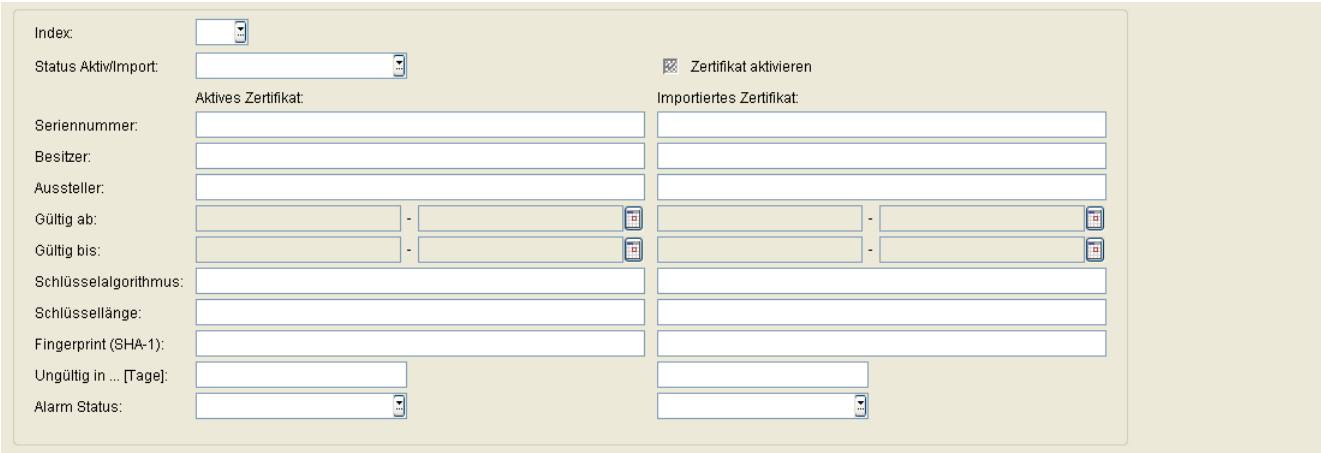
Wert für Zeitüberschreitung beim Suchauftrag für LDAP Einfachsuche in Sekunden.

Mögliche Optionen:

- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **60**

7.1.15.2 Register „CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > LDAP > Register „CA Zertifikate“



Index

Indexnummer des Zertifikats.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

Aktives Zertifikat/Importiertes Zertifikat:

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus **SHA-1** (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.16 Anwendereinstellungen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Anwendereinstellungen

Dieser Bereich besteht aus folgenden Inhalten:

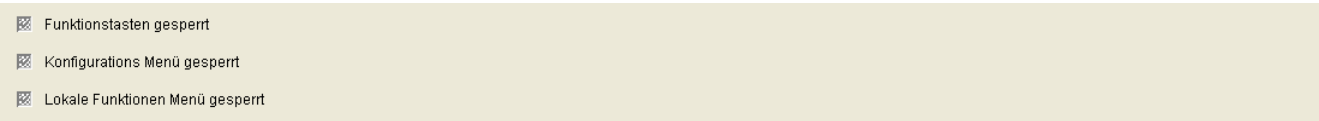
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einschränkungen“
- Register „gesperrte Konfigurationsmenüs“
- Register „gesperrte lokale Funktionen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.16.1 Register „Einschränkungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Anwendereinstellungen > Register „Einschränkungen“



Funktionstasten gesperrt

Schalter zum Sperren der Funktionstasten am Mobility Phone für Mobile User.

Konfigurationsmenüs gesperrt

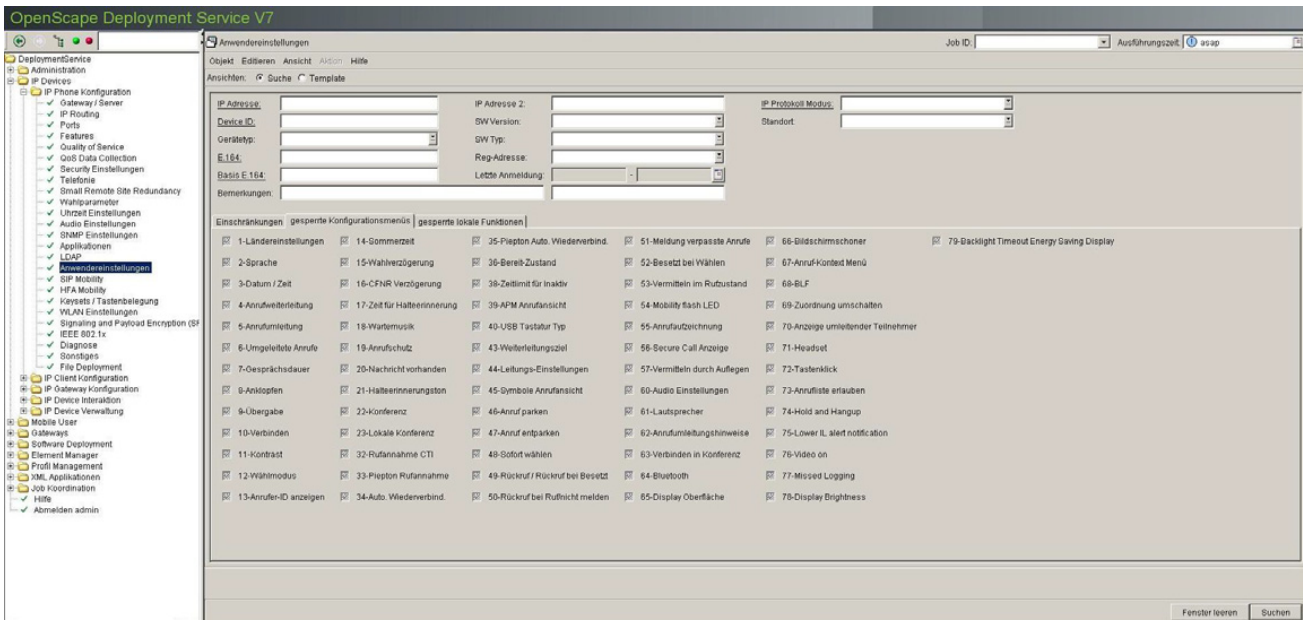
Schalter zum Sperren des Konfigurations-Menüs am Mobility Phone für Mobile User.

Lokale Funktionen Menüs gesperrt

Schalter zum Sperren des Lokale Funktionen-Menüs am Mobility Phone für Mobile User.

7.1.16.2 Register „gesperrte Konfigurationsmenüs“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Anwendereinstellungen > Register „gesperrte Konfigurationsmenüs“.



Folgende Funktionen im Konfigurations-Menü können für Mobile User gesperrt werden, indem das jeweilige Häkchen gesetzt wird:

1-Ländereinstellungen

Der Benutzer kann ein Land aus einer Liste auswählen, um das Telefon an landesspezifische Gegebenheiten anzupassen.

2-Sprache

Der Benutzer kann die Sprache für das Benutzermenü einstellen.

3-Datum / Zeit

Der Benutzer kann Ortszeit, Datum und Sommer/Winterzeit einstellen.

4-Anrufweiterleitung

Der Benutzer kann die Anrufweiterleitung aktivieren oder deaktivieren.

5-Anrufumleitung

Der Benutzer kann die Anrufumleitung aktivieren oder deaktivieren.

6-Umgeleitete Anrufe

Der Benutzer kann das Protokollieren von umgeleiteten Anrufen aktivieren oder deaktivieren.

7-Gesprächsdauer

Der Benutzer kann bestimmen, ob die Gesprächsdauer im Display angezeigt wird.

Nur bei optiPoint verfügbar.

8-Anklopfen

Der Benutzer kann bestimmen, ob ein Zweitanruf während einer bestehenden Verbindung zugelassen wird. Falls nicht, hört der Anrufer das Besetztzeichen.

9-Übergabe

Der Benutzer kann die Gesprächsübergabe zulassen.

10-Verbinden

Der Benutzer die Möglichkeit, einen aktiven und einen gehaltenen Teilnehmer miteinander zu verbinden, ein- oder ausschalten.

11-Kontrast

Der Benutzer kann den Kontrast für das Display einstellen.

12-Wählmodus

Der Benutzer kann bestimmen, ob beim Wählen nur eine Nummer oder auch ein Name eingegeben werden kann.

Nur bei optiPoint verfügbar.

13-Anrufer-ID anzeigen

Der Benutzer bestimmt, welche Informationen zum Anrufer bei einem eingehenden Anruf angezeigt werden sollen.

Nur bei optiPoint verfügbar.

14-Sommerzeit

Der Benutzer kann die Sommerzeit einstellen.

15-Wahlverzögerung

Der Benutzer kann die Verzögerung einstellen, mit der der Wählvorgang gestartet wird, nachdem die letzte Ziffer einer Rufnummer eingegeben worden ist.

16-CFNR Verzögerung

Der Benutzer kann die Verzögerung einstellen, mit der ein Anruf umgeleitet wird, wenn die Anrufumleitung bei Nichtmelden aktiviert ist.

17-Zeit für Halteerinnerung

Der Benutzer kann die Zeit einstellen, nach deren Ablauf an ein gehaltenes Gespräch erinnert wird.

18-Wartemusik

Der Benutzer kann bestimmen, ob die im Telefon gespeicherte Wartemusik (Music on Hold) verwendet wird. Ist die Wartemusik aktiviert, wird diese abgespielt, sobald das Telefon ins Halten gelegt wird.

19-Anrufschutz

Der Benutzer kann bestimmen, ob der Anrufschutz (Do Not Disturb) auf dem Telefon eingerichtet werden kann. Ist der Anrufschutz aktiviert, läutet das Telefon bei einem eingehenden Anruf nicht, und der Anrufer erhält das Besetztzeichen.

20-Nachricht vorhanden

Der Benutzer kann bestimmen, ob eine LED signalisiert, wenn neue Nachrichten in der Mailbox sind.

Nur bei optiPoint verfügbar.

21-Halteerinnerungston

Ist diese Funktion aktiviert und ein Gesprächspartner wurde ins Halten gelegt, ertönt nach einer einstellbaren Zeit ein Signal, um daran zu erinnern, dass ein Gespäch anliegt. Der Benutzer kann diese Funktion zulassen und die Verzögerung bis zum Erklingen des Erinnerungstons einstellen.

22-Konferenz

Der Benutzer kann anlagengestützte Konferenzen zulassen.

Nur bei optiPoint verfügbar.

23-Lokale Konferenz

Der Benutzer kann telefongestützte Dreierkonferenzen zulassen.

32-Rufannahme CTI

Der Benutzer kann bestimmen, ob eingehende Anrufe automatisch über die mit dem Telefon verbundene CTI-Anwendung angenommen werden.

33-Piepton Rufannahme

Der Benutzer kann bestimmen, ob bei automatisch über die mit dem Telefon verbundene CTI-Anwendung angenommenen Anrufen ein Piepton ertönt.

34-Auto. Wiederverbin.

Der Benutzer kann bestimmen, ob ein gehaltenes Gespräch über die CTI-Applikation automatisch wieder aufgenommen werden kann.

35-Piepton Auto. Wiederverbind.

Der Benutzer kann bestimmen, ob ein Piepton ertönt, wenn ein gehaltenes Gespräch über die CTI-Applikation wieder aufgenommen wird.

36-Bereit-Zustand

Der Benutzer kann die Anzeige von Systemnachrichten im Ruhezustand konfigurieren.

Nur bei optiPoint verfügbar.

38-Zeitlimit für Inaktiv.

Der Benutzer kann die Verzögerungszeit zwischen der letzten Eingabe und der Rückkehr in den Ruhezustand einstellen.

39-APM Anrufansicht

Der Benutzer kann die Anrufansicht auf dem optiPoint application module aktivieren oder deaktivieren.

40-USB Tastatur Typ

Der Benutzer kann die Sprache der USB-Tastatur eines optiPoint-Telefons festlegen.

Nur bei optiPoint verfügbar.

43-Weiterleitungsziel

Der Benutzer kann die Zielnummer für die Weiterleitung eingeben bzw. verändern.

44-Leitungs-Einstellungen

Der Benutzer kann die Eigenschaften einer Leitungstaste konfigurieren.

45-Symbole Anrufansicht

Der Benutzer kann festlegen, ob Meldungen auf dem optiPoint display module, wie z. B. die Auflistung entgangener Anrufe, als Text oder als Symbole erscheinen.

46-Anruf parken

Der Benutzer kann das Parken von Anrufen zulassen.

47-Anruf entparken

Der Benutzer kann das Entparken von Anrufen zulassen.

48-Sofortwählen

Der Benutzer kann Sofortwählen zulassen.

49-Rückruf / Rückruf bei Besetzt

Der Benutzer kann die Übermittlung eines Rückrufwunschs an die Anlage aktivieren. Bei OpenStage V3 oder höher kann der Rückrufwunsch in jedem Fall abgesetzt werden, bei anderen Endgeräten nur im Besetztfall.

50-Rückruf bei Ruf/nicht melden

Der Benutzer kann die Übermittlung eines Rückrufwunschs an die Anlage für den Fall, dass sein Anruf nicht angenommen wird, aktivieren.

Nur bei OpenStage verfügbar.

51-Meldung verpasste Anrufe

Der Benutzer kann die Meldung verpasster Anrufe auf dem Display aktivieren.

Nur bei optiPoint verfügbar.

52-Besetzt bei Wählen

Der Benutzer kann bestimmen, ob ein Abruf abgewiesen wird, der während der Eingabe einer Rufnummer eingeht.

Der Benutzer kann bestimmen, ob ein Abruf abgewiesen wird, der während der Eingabe einer Rufnummer eingeht.

53-Vermitteln im Rufzustand

Der Benutzer kann bestimmen, ob die Übergabe eines Gesprächs bereits dann erfolgt, wenn das Telefon des dritten Teilnehmers läutet, auch wenn der Übergebende den Hörer noch nicht aufgelegt hat.

54-Mobility flash LED

Der Benutzer kann bestimmen, ob die LED der Mobilitäts-Taste blinkt, während Daten zwischen Telefon und DLS ausgetauscht werden, wie z. B. bei der An- und Abmeldung.

Nur bei optiPoint verfügbar.

55-Anrufaufzeichnung

Der Benutzer kann die Aufzeichnung von Anrufen aktivieren.

Nur bei optiPoint verfügbar.

56-Secure Call Anzeige

Der Benutzer kann bestimmen, ob ein Aufmerksamkeitson ertönt, wenn die Sprachverbindung ungesichert ist.

57-Vermitteln durch Auflegen

Der Benutzer kann bestimmen, ob bei einem gehaltenen und einem aktiven Gespräch die beiden Gesprächspartner miteinander verbunden werden können, indem der Benutzer selbst auflegt.

60-Audio Einstellungen

Der Benutzer kann Einstellungen wie Klingeltöne und Raumakustik vornehmen.

Nur bei OpenStage verfügbar.

61-Lautsprecher

Der Benutzer kann die Freisprechfunktion aktivieren oder deaktivieren.

Nur bei OpenStage verfügbar.

62-Anrufumleitungshinweise

Der Benutzer kann bestimmen, ob optische oder akustische Warnhinweise gegeben werden, sobald ein Anruf bei eingeschalteter Umleitung eingeht. Nur bei OpenStage verfügbar.

63-Verbinden in Konferenz

Der Benutzer kann bestimmen, ob es möglich ist, bei einer Konferenz die beiden anderen Gesprächspartner miteinander zu verbinden und selbst die Konferenz zu verlassen.

Nur bei OpenStage verfügbar.

64-Bluetooth

Der Benutzer kann die Bluetooth-Konnektivität aktivieren oder deaktivieren.

65-Display Oberfläche

Der Benutzer kann das Design der Benutzeroberfläche auswählen.

Nur bei OpenStage 60/80 verfügbar.

66-Bildschirmschoner

Der Benutzer kann den Bildschirmschoner des Telefons aktivieren sowie die Verzögerungszeit für den Start des Bildschirmschoners einstellen.

Nur bei OpenStage 60/80 verfügbar.

67-Anruf-Kontext Menü

Der Benutzer kann das angezeigte Menü festlegen

Nur bei OpenStage 60/80 verfügbar.

68-BLF

Der Benutzer kann festlegen, wie ein ankommender Anruf für das mit der BLF-Taste überwachte Telefon angezeigt wird.

69-Zuordnung umschalten

Dieses Leistungsmerkmal besteht in einer weiteren Möglichkeit der Gesprächsübergabe. Wenn aktiviert, so ergibt sich der folgende Ablauf: Der Benutzer hat einen Zweitanruf angenommen, wodurch das erste Gespräch ins Halten gelegt wird. Sobald der Benutzer einmal zurück zum ersten Gespräch und danach wieder zum zweiten Gespräch gewechselt hat, kann er die beiden Gesprächspartner miteinander verbinden, indem er einfach auflegt.

Bei allen OpenStage-Telefonen verfügbar.

70- Anzeige umleitender Teilnehmer

Der Benutzer kann bei Mehrfachumleitungen festlegen, ob der zuerst umleitende oder der zuletzt umleitende Teilnehmer angezeigt wird.

Für alle OpenStage SIP-Telefone verfügbar.

71- Headset

Der Benutzer kann den Typ des angeschlossenen Headsets festlegen.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

72- Tastenklick

Der Benutzer kann die Art des Tastenklick festlegen.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

73- Rufjournal (Rufliste) aktivieren

Der Benutzer kann eine Rufliste aktivieren, in der alle entgangenen, gewählten, empfangenen oder weitergeleiteten Anrufe aufgeführt sind. Die Rufliste kann über das WPI gelöscht werden.

Für OpenStage 15/20/20E/40/60/80 SIP verfügbar.

74- Hold and hang-up

Der Teilnehmer kann Anrufe vorübergehend halten und auflegen, ohne den Anrufer zu trennen. Diese Funktion ist standardmäßig deaktiviert.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

75- Lower IL alert notification

Der Benutzer wird informiert, wenn ein kommender Anruf aus einer niedrigeren Sicherheitszone stammt oder wenn ein gehender Anruf in einer niedrigeren Sicherheitszone geht.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

76 - Video erlauben

Der Benutzer kann Video-Gespräche erlauben.

Für OpenStage 60/80 SIP/HFA verfügbar.

77- Entgangene Anrufe

Der Benutzer kann festlegen, ob Anrufe, die andernorts angenommen wurden, an seinem Telefon protokolliert werden.

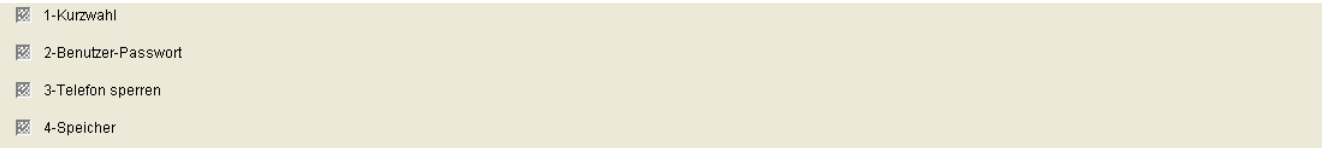
Für OpenStage 15/20/20E/40/60/80 SIP verfügbar.

78- Display Helligkeit

79- Hintergrundbeleuchtung Timeout energiesparendes Display

7.1.16.3 Register „gesperrte lokale Funktionen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Anwendereinstellungen > Register „gesperrte lokale Funktionen“



Folgende Funktionen im Konfigurations-Menü können für Mobile User gesperrt werden, indem das jeweilige Häkchen gesetzt wird:

1-Kurzwahl

Der Benutzer kann Kurzwahlnummern einrichten.

Nur bei optiPoint verfügbar.

2-Benutzer-Passwort

Der Benutzer kann sein Passwort ändern.

3-Telefon sperren

Der Benutzer kann das Telefon sperren. Ist das Telefon gesperrt, kann kein Unbefugter von diesem Telefon aus regulär telefonieren oder Einstellungen ändern. Nur Notrufnummern und vordefinierte Nummern aus dem Wählplan können gewählt werden.

> ***HINWEIS:*** Die Funktion Telefonsperre kann nur über DLS (nicht über WBM oder lokal) eingerichtet werden.
> Wenn die Funktion gesperrt ist, ist das Menü zwar sichtbar aber ausgegraut (d. h. nicht verfügbar).

4-Speicher

Der Benutzer kann alle Kurzwahlnummern löschen sowie das Telefon wieder in den Lieferzustand versetzen.

Nur bei optiPoint verfügbar.

7.1.17 SIP Mobility

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SIP Mobility

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SIP Mobility“
- Register „SIP Mobility Logon/Logoff“
- Register „SIP Mobility Data“

7.1.17.1 Register „SIP Mobility“

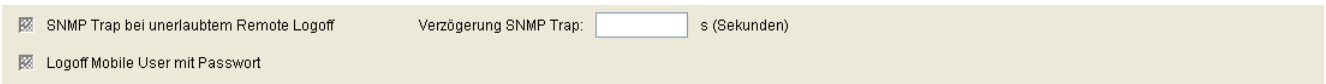
Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SIP Mobility > Register „SIP Mobility“

Endgerät verfügbar für Mobile User

Ist der Schalter aktiv, wird das Endgerät für Mobile User-Anmeldungen freigegeben.

7.1.17.2 Register „SIP Mobility Logon/Logoff“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SIP Mobility > Register „SIP Mobility Logon/Logoff“



SNMP Trap bei unerlaubtem Remote Logoff

Ist der Schalter aktiv, wird bei jedem unerlaubten Remote Logoff-Versuch eine Meldung zum SNMP-Server gesendet. Zum Eintragen der SNMP-Serverdaten siehe Abschnitt 7.1.13.1, “Register „SNMP“”.

Logoff Mobile User mit Passwort

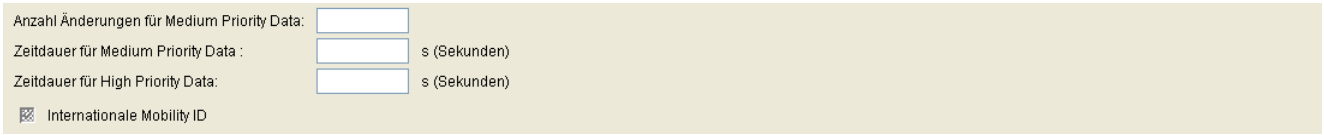
Ist der Schalter aktiv, ist das Abmelden eines Mobile Users nur möglich, wenn das Passwort des aktuell angemeldeten Mobile Users eingegeben wird.

Verzögerung SNMP Trap

Zeitdauer in Sekunden, bis der SNMP Trap gesendet wird. Zum Eintragen der SNMP-Serverdaten siehe Abschnitt 7.1.13.1, “Register „SNMP“”.

7.1.17.3 Register „SIP Mobility Data“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > SIP Mobility > Register „SIP Mobility Data“



Anzahl Änderungen für Medium Priority Data:

Angabe, nach der wievielten Änderung von Daten mittlerer Priorität im Workpoint diese Daten an den DLS geschickt werden.

Zeitdauer für Medium Priority Data:

Angabe, nach welcher Zeitspanne seit der letzten Änderung von Daten mittlerer Priorität im Workpoint diese Daten an den DLS geschickt werden.

Zeitdauer für High Priority Data:

Angabe, nach welcher Zeitspanne seit der letzten Änderung von Daten hoher Priorität im Workpoint diese Daten an den DLS geschickt werden.

Internationale Mobility ID

Ist der Schalter aktiviert, fügt das Endgerät beim Anmelden eines Mobile Users neben Amtsnummer und Ortskennzahl auch die Landeskennzahl automatisch an die Extension an. Die internationale Kennzahl wird unter **IP Devices** > **IP Phone Konfiguration** > **Wahlparameter** > **Register „Rufnummern“** -> **Internationale Vorwahl** eingerichtet.

Beispiel: Der Benutzer meldet sich am Endgerät mit der Extension/Mobility ID „31434“ an. Ist der Schalter aktiviert, schickt das Endgerät die Nummer „498972231434“. Andernfalls schickt das Endgerät „8972231434“.

7.1.18 HFA Mobility

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > HFA Mobility

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „HFA Mobility“

7.1.18.1 Register „HFA Mobility“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > HFA Mobility > Register „HFA Mobility“

HINWEIS: Soll der DLS Benutzerdaten wie Ruflisten und das Telefonbuch inklusive Picture-Clips speichern, muss für das entsprechende Endgerät bei **IP Devices** > **IP Phone Konfiguration** > **HFA Mobility** > **Register „HFA Mobility“** das Feld **Mobility Mode** auf **Data Mobility** gesetzt werden. Bei den Werten **Data Privacy** und **Basic** wird das Endgerät im DLS registriert, es werden aber keine weiteren Aktionen im DLS durchgeführt.

Mobility Mode:

Legt fest, wie mit Benutzerdaten bei HFA Mobility umgegangen wird. Benutzerdaten können grundsätzlich in zwei Kategorien unterteilt werden:

a) Allgemeine Benutzerdaten (Bildschirmschoner, Klingeltöne, Lautstärken, Raumakustik, Farbschema)

b) Private Daten (Telefonbuch & zugehörige Bilder, Rufjournal/Rufliste und Benutzerpasswort)

Telefone können so eingerichtet werden, dass sie folgende Betriebsarten unterstützen: Basic, Data Privacy oder Data Mobility.

HINWEIS: Nur Administratoren können den **Mobility-Modus** konfigurieren.

Mögliche Optionen:

- **Basic**

  Standardbetriebsart, in der Benutzerdaten für alle Benutzer zugänglich sind. Benutzer dürfen sich an jedem Telefon anmelden.

- **Data Privacy**

  Die Option Data Privacy stellt eine Erweiterung des Basic HFA Mobility-Modus dar; die privaten Daten von ehemaligen Besuchern oder des Telefonbesitzers werden gelöscht oder ausgeblendet, während ein Besucher am Telefon angemeldet ist.

  HINWEIS: Administratoren können beim Mobility-Modus zwischen den Einstellungen Basic und Data Privacy umschalten.

- **Data Mobility**

  Data Mobility ist eine Erweiterung des Data Privacy-Modus; sie unterstützt die Übertragung einer beschränkten Anzahl zusätzlicher Datenelemente zwischen Telefonen, die in der Vergangenheit von einem Benutzer verwendet wurden.
  Private Daten sind für Benutzer überall zugänglich (unabhängig davon, wo diese sich anmelden) und werden sicher gespeichert, solange die Benutzer abgemeldet sind. Außerdem nehmen Benutzer bei einem Wechsel zwischen Telefonen ihr Benutzerpasswort mit.

HINWEIS: Wenn beim Speichern von Mobility-Daten Probleme auftreten, erhält der Benutzer eine Warnmeldung und wird anschließend informiert, sobald das Problem behoben ist.

7.1.19 Keysets / Tastenbelegung

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung

Dieser Bereich besteht aus folgenden Inhalten:

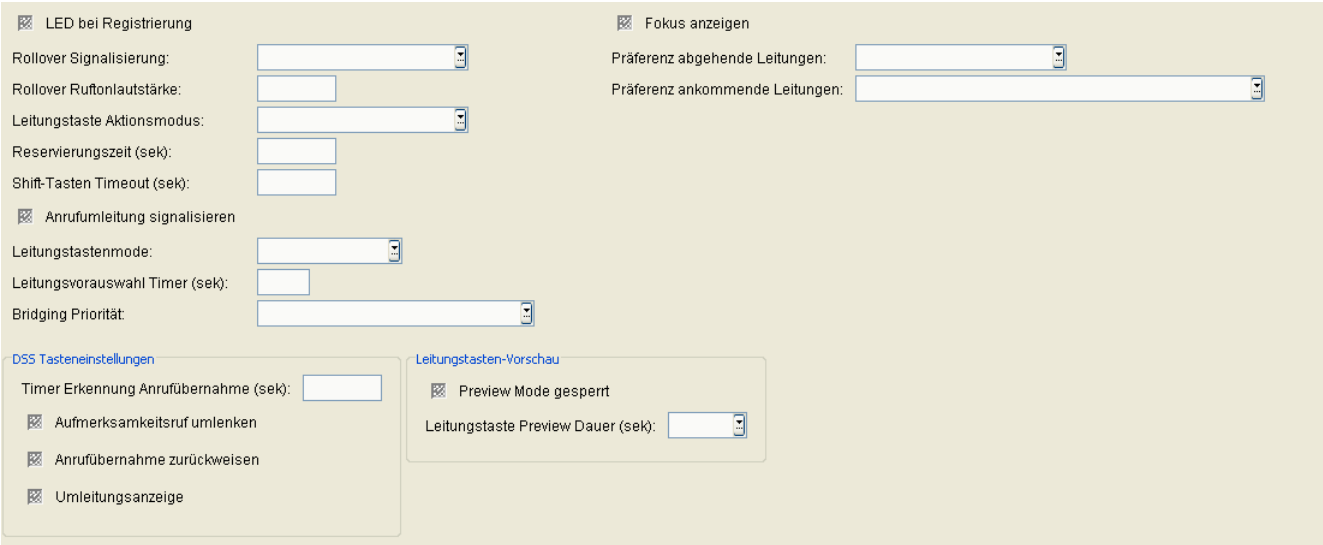
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Keysets“
- Register „Ziele“
- Register „Send URL Server CA Zertifikat“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.19.1 Register „Keysets“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung > Register „Keysets“



LED bei Registrierung

Ist der Schalter aktiv, wird beim Neustart des IP Phones angezeigt, ob der Workpoint erfolgreich registriert wurde.

Nur bei SIP-Workpoints verfügbar.

Rollover Signalisierung:

Art der der Signalisierung für den Fall, dass während eines Gesprächs ein Anruf auf einer anderen Leitung ankommt.

Mögliche Optionen:

- **Kein Ton**
- **Hinweisruf**
- **Standard**
- **Hinweiston**

Nur bei SIP-Workpoints verfügbar.

Rollover Ruftonlautstärke:

Lautstärke der Signalisierung im Besetztfall.

Nur bei SIP-Workpoints verfügbar.

Leitungstaste Aktionsmodus:

Legt fest, was mit einer Leitung (Gespräch) geschehen soll, wenn eine Verbindung über eine andere Leitung hergestellt wird.

Mögliche Optionen:

- **Halten**
  Das Gespräch der ursprünglichen Leitung wird gehalten.
- **Freigeben**
  Die Verbindung der ursprünglichen Leitung wird getrennt (das Gespräch wird beendet).

Nur bei SIP-Workpoints verfügbar.

Reservierungszeit:

Zeit in Sekunden, die angibt, wie lange eine Leitungsreservierung aufrechterhalten wird.

Standard: **60** s.

Nur bei SIP-Workpoints verfügbar.

Shift-Tasten Timeout (sek):

Zeit in Sekunden, nach deren Ablauf die Shift-Taste inaktiv wird, so dass die Tasten wieder mit den Funktionen der 1. Ebene belegt sind.

Anrufumleitung signalisieren

Schalter zum Aktivieren der Signalisierung bei einer Leitungstaste, wenn bei deren Ziel eine Rufweiterschaltung aktiv ist.

Nur bei SIP-Workpoints verfügbar.

Leitungstastenmode

Mögliche Optionen:

- **Einzeltaste**
  Die an die Leitungstaste gebundene Aktion wir sofort mit dem Betätigen der Taste ausgelöst, ohne Rücksicht darauf, ob der Hörer abgenommen oder aufgelegt ist.

- **Vorauswahl**
  Bei Betätigung der Leitungstaste erhält die Leitung den Fokus. Wenn eine Leitung benötigt wird, z. B. nach Abheben des Hörers, wird diese Leitung benutzt.

Leitungsvorauswahl Timer (sek):

Legt die Zeitspanne fest, nach der die Vorauswahl einer Leitung wieder beendet wird.

Bridging Priorität:

Mögliche Optionen:

- **Bridging vor preview**
- **Preview vor bridging**

Fokus anzeigen

Schalter zum Aktivieren der Anzeige, welche Leitung momentan aktiv ist (Leitung hat den Fokus).

Nur bei SIP-Workpoints verfügbar.

Präferenz abgehende Leitungen:

Festlegung der bevorzugt zu verwendenden Leitung bei ausgehenden Anrufen.

Mögliche Optionen:

- **Ruhende Leitung bevorzugt**
- **Primärleitung bevorzugt**
- **Letzte Leitung bevorzugt**
- **Kein Vorzug**

Nur bei SIP-Workpoints verfügbar.

Präferenz ankommende Leitungen:

Festlegung der bevorzugt zu verwendenden Leitung bei eingehenden Anrufen.

Mögliche Optionen:

- **Rufende Leitung bevorzugt**

- **Rufende Leitung bevorzugt mit Primärleitung bevorzugt**
- **Rufende Leitung bevorzugt**
- **Ankommende Leitung bevorzugt mit Primärleitung bevorzugt**
- **Kein Vorzug**

Nur bei SIP-Workpoints verfügbar.

DSS Tasteneinstellungen

Timer Erkennung Anrufübernahme (sek)

Legt fest, wie lange die Anrufübernahme an der Taste signalisiert wird.

Aufmerksamkeitsruf umlenken

Ist der Schalter aktiviert, kann der Aufmerksamkeitsruf per Tastendruck umgeleitet werden.

Anrufübernahme zurückweisen

Ist der Schalter aktiviert, kann die Anrufübernahme per Tastendruck zurückgewiesen werden.

Umleitungsanzeige

Ist der Schalter aktiviert und die anlagenbasierte Umleitung für diese Leitung eingeschaltet, so blinkt die LED der Leitungstaste.

Leitungstasten-Vorschau

Preview Mode gesperrt

Schalter zum Deaktivieren des Vorschau-Modus.

Leitungstaste Preview Dauer (sek):

Zeitdauer des Vorschau-Modus in Sekunden.

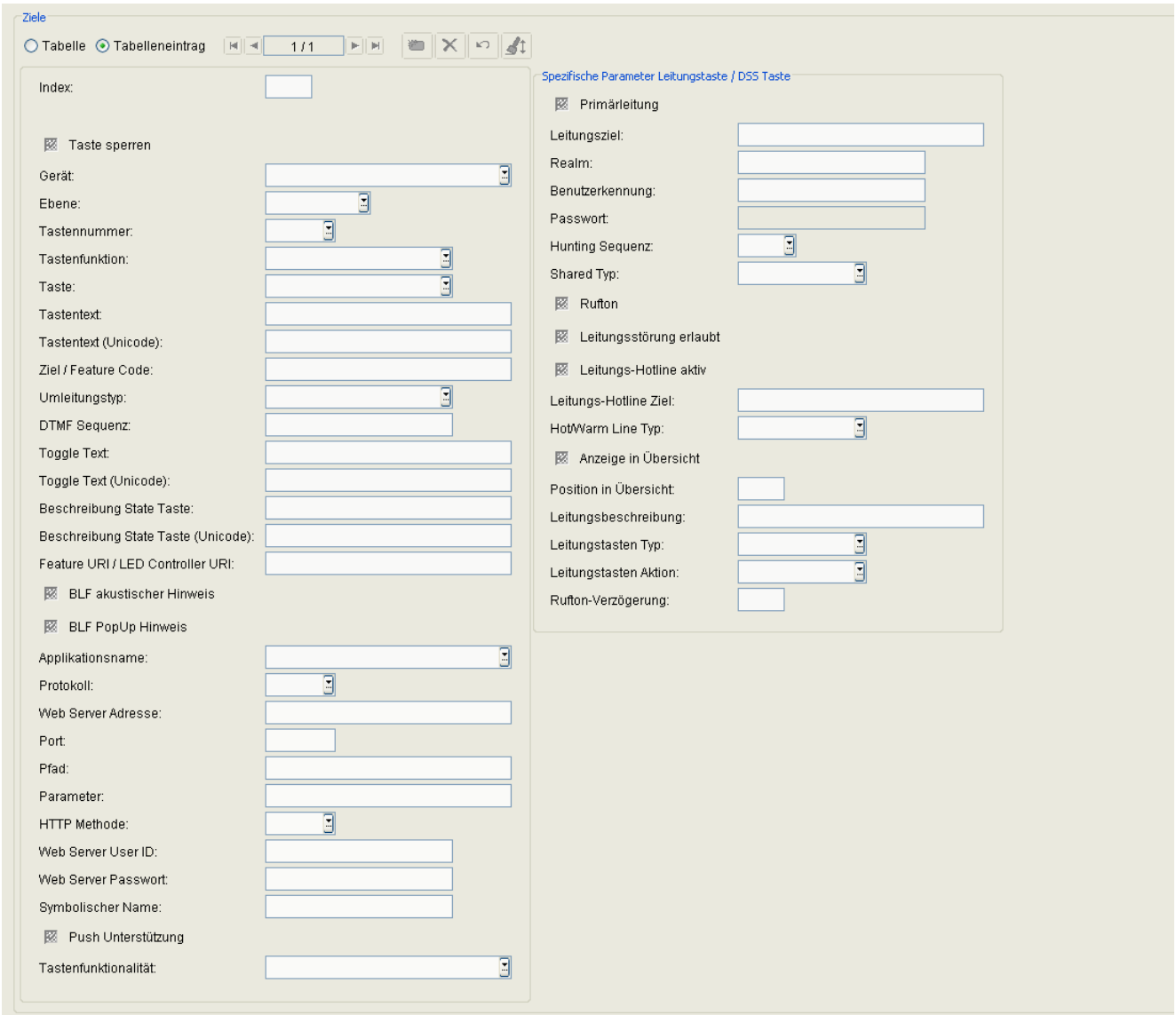
Mögliche Optionen:

- **2**
- **3**

- **4**
- **6**
- **8**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**

7.1.19.2 Register „Ziele“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung > Register „Ziele“



Index

Name der Funktion der Tastenbelegung.

Taste sperren

Schalter zum Sperren der Funktionstaste.

Gerät

Gibt an, für welches Gerät die entsprechende Tastenbelegung gültig ist.

Mögliche Optionen:

- **Basis Gerät**
- **1. Key module**
- **2. Key module**
- **1. Self Labeling Key module**
- **2. Self Labeling Key module**
- **OpenStage 15 Key module**

Nur bei SIP-Workpoints verfügbar.

Ebene

Tastenebene für Shift-Funktionalität.

Mögliche Optionen:

- **1. Ebene**
- **2. Ebene**
- **3. Ebene**
- **4. Ebene**
- **Fixed Keys**
  Diese Tasten haben feste Tastennummern und können am Endgerät weder gelöscht noch hinzugefügt werden.

Nur bei SIP-Workpoints verfügbar.

Tastennummer

Nummer der Taste, die die entsprechende Funktion zugewiesen bekommt.

Nur bei SIP-Workpoints verfügbar.

Tastenfunktion

Folgende Tastenfunktionen werden unterstützt:

- **Keine Funktion**

- **Zielwahl**
- **Kurzwahl**
- **Wahlwiederholung**
- **Anruferliste**
- **Nachrichten**
- **Anruf umleiten**
- **Lautsprecher**
- **Mikrofon aus**
- **Rufton aus**
- **Halten**
- **Makeln**
- **Ohne Rückfrage verbinden**
- **Verbinden (OpenStage) / Übergabe (optiPoint)**
- **Weiterleiten**
- **Service Menü**
- **Raum hallend**
- **Raum gedämpft**
- **SHIFT-Taste**
- **Notizbuch**
- **Einstellungen**
- **Telefon sperren**
- **Konferenz**
- **Lokale Konferenz**
- **Headset**
- **Anrufschutz**
- **Anrufübernahme**
- **Erweiterte Zielwahl**
- **Leitungstaste**
- **Funktionsumschaltung**
- **Zeige Telefon-Display**

- **Displaywechsel**
- **Mobility**
- **Parken**
- **Übernahme geparktes Gespräch**
- **Abbrechen**
- **Ok Confirm (OK)**
- **Rückruf**
- **Rückruf löschen**
- **Rückfrage (OpenStage) / Rückfrage/Übergabe (optiPoint)**
- **DSS**
- **State-Taste**
- **Anklopfen**
- **Sofortiger Ruf**
- **Preview Taste**
- **Sprachaufzeichnung**
- **AICS Zip**
- **Server Feature**
  Sowohl für frei programmierbare Tasten als auch für ‘Fixed Keys’ möglich.
- **BLF**
- **Applikation starten**
  Sowohl für frei programmierbare Tasten als auch für ‘Fixed Keys’ möglich.
- **URL senden**
  Sendet eine konfigurierbare HTTP- oder HTTPS-Anforderung an einen entfernten Server. Sowohl für frei programmierbare Tasten als auch für ‘Fixed Keys’ möglich.
  Die Anforderungszeichenfolge enthält folgende Informationen: **Web Server User ID**, **Web Server Passwort**, **Parameter**, die IP-Adresse und Rufnummer des Telefons und **Symbolischer Name**
  z. B.
  `userid=jdoe&password=00secret&mode=remote&action=start&ipaddress=192.168.1.244&phonenumber=3338&symbn=key4`
- **Built-in Anrufumleitung**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Built-in Trennen**
  Nur für Ebene ‘Fixed Keys’ möglich.

- **Built-in Sprachwahl**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Built-in Wahlwiederholung**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Telefonbuch starten**

  HINWEIS: Die Funktion „Telefonbuch starten“ kann auch auf die 1./2. FPK-Tastenebene von OpenStage 15/20 und OpenScape Desk Phone IP 35G-Telefonen gelegt werden.
- **2. Ruf**

Taste:

Zeigt an, ob es sich um eine frei programmierbare Taste oder um einen ’Fixed Key’ handelt.

Tastentext

Bei Self labeling Keys-Workpoints (z. B. optiPoint 420 standard) kann hier pro Taste eine Tastenbeschriftung angegeben werden.

Nur bei SIP-Workpoints verfügbar.

HINWEIS: Bei Fixed Keys bleibt die Tastenbeschriftung unverändert, wenn der Administrator eine andere Tastenfunktion als Standard für die Taste definiert.

Tastentext (Unicode)

Bei OpenStage-Telefonen kann der Tastentext auch in Unicode eingegeben werden.

Ziel / Feature Code

Angabe des Wahlziels. Dies kann eine Ziffernfolge bzw. eine URL sein. Feature Codes, die zu externen Servern gesendet werden müssen (nicht der SIP-Server, bei dem das Telefon registriert ist), haben das folgende Format:

<Feature code>@<IP-Adresse>

Beispiel: **123@10.2.54.2**

Wird die Zieleingabe für die Tastenfunktion „Erweiterte Zielwahl“ vorgenommen, so können in einer Ziffernfolge zusätzliche Steuerzeichen eingegeben werden:

- **$Q** = clear (CL) / auflegen (AL)
- **$R** = consult (CS) / rückfragen (RF)
- **$S** = OK
- **$T** = Pause (PA)

Nur bei SIP-Workpoints verfügbar.

Umleitungstyp

Mögliche Optionen:

- **bei besetzt**
- **bei nicht melden**
- **immer**

Nur bei SIP-Workpoints verfügbar.

DTMF Sequenz

DTMF Sequenz für dieses Ziel.

Toggle Text

Text für die Tastenfunktion „Funktionsumschaltung“.

Nur bei SIP-Workpoints verfügbar.

Toggle Text (Unicode)

Text für die Tastenfunktion „Funktionsumschaltung“, in Unicode kodiert.

Nur bei Geräten der OpenStage-Familie (SIP-Version) verfügbar.

Beschreibung State Taste

Beschreibungstext für die State-Taste.

Beschreibung State Taste (Unicode)

Beschreibungstext für die State-Taste in Unicode. Nur bei Geräten der OpenStage-Familie (SIP-Version) verfügbar.

Feature-URI / LED Controller URI:

URI, mit der dieses Leistungsmerkmal auf dem Server gesteuert wird.

BLF akustischer Hinweis

Akustischer Hinweis zusätzlich zur Anzeige auf der Taste.

BLF PopUp Hinweis

Zusätzlich zur Anzeige auf der Taste erscheint ein Hinweis im Display.

Applikationsname:

Name der Applikation, die mit der Taste gestartet werden soll.

Protokoll

Protokoll, das für die Kommunikation zwischen IP Phone und serverseitigem Programm verwendet wird.

Mögliche Optionen:

- **HTTP**
- **HTTPS**

Web Server Adresse:

Hostname, Domänenname oder IP Adresse des Webservers.

Port

Portnummer des Webservers. Wenn für Port nichts eingetragen wurde, enthält die voll qualifizierte URL kein Port-Element.

Pfad

Verzeichnispfad und Name des Programms oder der Webseite.

Beispiel: **servlet/IppGenericServlet** oder **webpage/checkin.xml**

Der Pfadname sollte mit einem Schrägstrich bzw. Slash beginnen und nicht mit einem Slash enden. Falls der Slash zu Beginn fehlt, wird er ergänzt. Falls ein zusätzlicher Slash am Ende steht, wird er gelöscht. Bei den Slashes handelt es sich um 'vorwärts'-Slashes ('/') . Bei 'Back'-Slashes findet der Web Server das Programm oder die Seite eventuell nicht.

Parameter

Kein, ein oder mehrere Parameter-Wert Paare, durch '&' getrennt, können eingegeben werden, z. B. **Parameter1=Wert1&Parameter2=Wert2**. Ein Komma darf nicht als Trennzeichen verwendet werden, da es Teil eines Parameter oder Wertes sein kann. Falls ein Parameter oder Wert ein '&' enthält, muss es durch '&' ersetzt werden.

Ein Fragezeichen wird automatisch zwischen Pfad und Parameter eingefügt. Ein Fragezeichen am Beginn der Parameter wird automatisch gelöscht.

HTTP Methode

Verwendete HTTP-Methode.

Mögliche Optionen:

- **Get**
- **Post**

Web Server User ID

Eine dem Webserver bekannte User ID. Diese Information wird zur Authentifizierung des IP Phones durch den Web Server verwendet.

Web Server Passwort

Ein dem Web Server bekanntes Passwort. Diese Information wird zur Authentifizierung des IP Phones durch den Web Server verwendet.

Symbolischer Name

Symbolischer Name, der dem Server bekannt ist. Diese Information wird zur Authentifizierung des IP Phones durch den Web Server verwendet.

Push Unterstützung

Push-Unterstützung.

Tastenfunktionalität

Mögliche Optionen:

- **Toggle Anrufumleitung**
- **unspezifizierte Anrufumleitung**
- **unspezifiziert**

Spezifische Parameter Leitungstaste / DSS Taste

Primärleitung

Bestimmt, ob die Leitung als Primärleitung fungiert.

Nur bei SIP-Workpoints verfügbar.

Leitungsziel

Rufnummer bzw. Address of Record der Leitung.

Nur bei SIP-Workpoints verfügbar.

Realm

SIP-Realm, der zum Address of Record der Leitung gehört.

Nur bei SIP-Workpoints verfügbar.

Benutzerkennung

Nur bei SIP-Workpoints verfügbar.

Passwort

Nur bei SIP-Workpoints verfügbar.

Rufton

Nur bei SIP-Workpoints verfügbar.

Hunting Sequenz

Nur bei SIP-Workpoints verfügbar.

Shared Typ

Mögliche Optionen:

- **Privat**
- **Gemeinsam**
- **Unbekannt**

Nur bei SIP-Workpoints verfügbar.

Leitungsstörung erlaubt

Schalter zum Aktivieren für das Zulassen von Leitungsstörungen.

Nur bei SIP-Workpoints verfügbar.

Leitungs-Hotline aktiv

Schalter zum Aktivieren einer Leitungs-Hotline.

Nur bei SIP-Workpoints verfügbar.

Leitungs-Hotline Ziel:

Rufnummer die als Ziel für die Leitungs-Hotline verwendet wird.

Nur bei SIP-Workpoints verfügbar.

Hot/Warm Line Typ:

Geräteeigenschaft einstellen.

- **Normal**
- **Sofortverbindungsaufbau**
- **verzögerter Sofortverbindungsaufbau**

Nur bei SIP-Workpoints verfügbar.

Anzeigen in Übersicht

Aktiviert die Leitungsanzeige in der Leitungsübersicht..

Nur bei SIP-Workpoints verfügbar.

Position in Übersicht:

Position der Taste in der Leitungsübersicht.

Nur bei SIP-Workpoints verfügbar.

Leitungsbeschreibung:

Bescheibung der entsprechenden Leitung.

Nur bei SIP-Workpoints verfügbar.

Leitungstasten Typ

Mögliche Optionen:

- **Normal**
- **Direkt**

Leitungstasten Aktion

Mögliche Optionen:

- **Rückfrage**
- **Vermitteln**

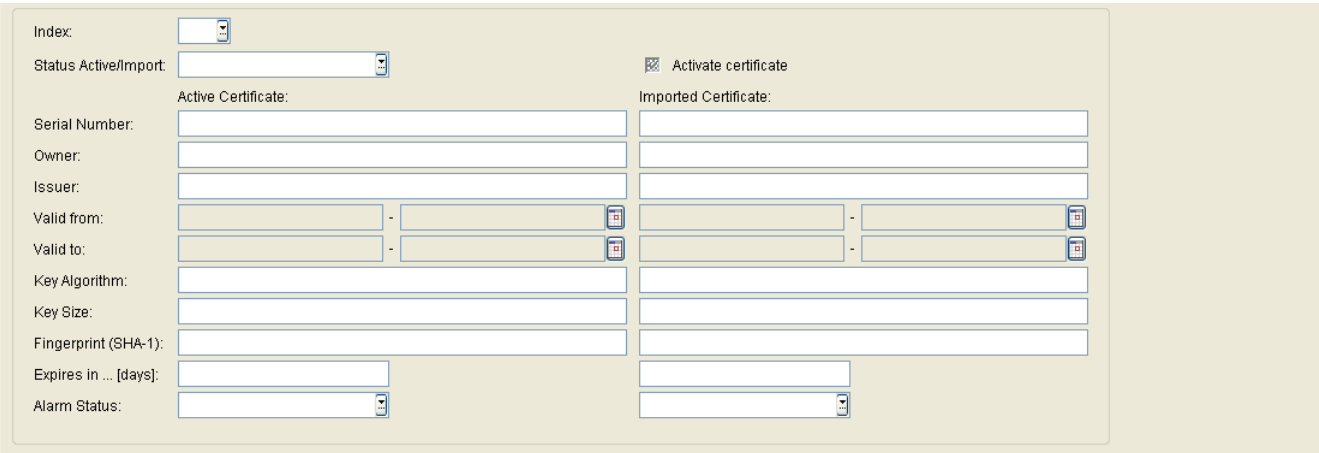
- **Keine Aktion**

Rufton-Verzögerung

Dauer der Verzögerung, bis ein eingehender Rufton signalisiert wird.

7.1.19.3 Register „Send URL Server CA Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung > Register „Send URL Server CA Zertifikat“



Eine Beschreibung der Parameter finden Sie unter **IP Devices** > **IP Phone Konfiguration** > **LDAP** > **Register „CA Zertifikate“**.

7.1.20 WLAN Einstellungen

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > WLAN Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Allgemeine Daten“
- Register „Security Verschlüsselung“
- Register „Location Server“
- Register „Erweiterte Einstellungen“
- Register „Debug Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.20.1 Register „Allgemeine Daten“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > WLAN Einstellungen > Register „Allgemeine Daten“

WICHTIG: Bei nicht konsistenter Datenänderung kann das WLAN-Phone eventuell nicht mehr erreicht werden!

Netzwerk Name (SSID)

Die SSID ist der Netzwerkname, über den das WLAN-Phone identifiziert wird. Die SSID wird im Access Point (WLAN-Router) festgelegt.

Transfer Mode:

Sie können wählen, ob die Datenübertragung nach dem Standard IEEE 802.11b (**nur 802.11b**) oder sowohl nach IEEE 802.11b als auch nach IEEE 802.11g möglich sein soll (**Mixed Mode**).

Der wesentliche Unterschied zwischen beiden Standards ist die Übertragungsrate: Sie beträgt bei IEEE 802.11g nahezu das 5fache. Nutzen die Geräte im WLAN unterschiedliche Standards, sollten Sie hier die Voreinstellung Mixed Mode beibehalten.

Ist am Access Point bzw. WLAN-Router für den Transfer-Modus IEEE 802.11g als fixer Wert eingestellt, dann müssen Sie hier **Mixed Mode** einstellen.

Mögliche Optionen:

- **nur 802.11b**
- **Mixed Mode**

Übertragungsrate:

Geschwindigkeit in Mbit/s, mit der Daten im WLAN übertragen werden sollen. Die Übertragungsrate ist abhängig vom gewählten Transfer-Modus.

Mögliche Optionen:

- **1,0 Mbit/s**
- **2,0 Mbit/s**
- **5,6 Mbit/s**
- **6,0 Mbit/s**
- **9,0 Mbit/s**
- **11,0 Mbit/s**
- **12,0 Mbit/s**
- **18,0 Mbit/s**
- **24,0 Mbit/s**
- **36,0 Mbit/s**
- **48,0 Mbit/s**
- **54,0 Mbit/s**

Kanal:

Funkkanal des WLAN. Der Kanal ist am Access Point bzw. WLAN-Router eingerichtet.

Kanalbereich:

Der jeweilig mögliche Kanalbereich kann ausgewählt werden. Die Beschränkung ist wegen des Verbots der Nutzung von Kanal 12 und 13 in einigen Ländern erforderlich. Mögliche Werte: Kanal 1-11: z. B. USA, Kanal 1-13: z. B. Deutschland, Kanal 1-14: z. B. Japan.

Scan Kanäle:

Auswahl der Kanäle, die gescannt werden sollen.

Sendeleistung (%):

Sendeleistung des Mobilteils, mit der es zum Access Point senden soll. Die maximal erlaubte Sendeleistung beträgt 100 mW bzw. 20 dBm (100%).

Mögliche Optionen:

- **5 %**
- **10 %**
- **20 %**
- **40 %**
- **100 %**

Schwellwerte

Roaming Schwellwert (%):

Prozentwert der minimalen Empfangsstärke vom Access Point. Unterschreitet die Empfangsstärke des aktuell verbundenen Access Points diesen Wert, sucht das Mobilteil nach einem Access Point mit einer besseren Verbindungsqualität und stellt eine Verbindung zu diesem Access Point her.

Fragmentierungs-Schwellwert:

Größe der Sprachpakete, ab der sie getrennt (fragmentiert) werden. Die Fragmentierung in kleinere Pakete wird verwendet, um den Datendurchsatz im WLAN bei hoher Netz-Auslastung zu verbessern.

Wertebereich: **256** ... **2346** Bytes.

Standardwert: **2346** Bytes (keine Fragmentierung).

RTS / CTS Schwellwert:

Minimale Paketgröße in Byte, für die ein RTS (Request To Send) gesendet werden soll. Kleinere Pakete werden ohne RTS direkt zum Access Point übertragen.

Wertebereich: **1** ... **2347** Bytes.

Standardwert: **2347** Bytes (RTS/CTS-Mechanismus ausgeschaltet).

HINWEIS: Das Einschalten des Mechanismus kann zu einer Verschlechterung des Datendurchsatzes führen.

Batterie Ladezustand (%): (bei letzter Anmeldung)

Ladezustand des Akkus im WLAN-Phone in Prozent bei der letzten Anmeldung.

Preamble Typ

Vor jedes Datenpaket in einem WLAN wird eine Preamble gesetzt, mit deren Hilfe sich der Empfänger auf die Taktung des Senders synchronisieren kann.

Bei einer langen Preamble ist die Synchronisation weniger fehleranfällig. Bei einer kurzen Preamble ist der Datendurchsatz höher.

Nicht jedes WLAN-Gerät unterstützt beide Preamble-Typen.

Mögliche Optionen:

- **Lang**
- **Kurz**

7.1.20.2 Register „Security Verschlüsselung“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > WLAN Einstellungen > Register „Security Verschlüsselung“

WICHTIG: Bei nicht konsistenter Datenänderung kann das WLAN-Phone eventuell nicht mehr erreicht werden!

HINWEIS: Die Verschlüsselung schützt den Datenaustausch innerhalb des WLAN, nicht den Datenaustausch mit Ethernet-Netzwerken oder mit dem Internet.

Encryption:

Auswahl des Verschlüsselungsverfahrens.

Mögliche Optionen:

- **Kein**
  Die Daten im WLAN werden unverschlüsselt übertragen.
- **WPA**
  Verschlüsselung nach dem WPA-Verfahren.
- **WPA-PSK**
  Verschlüsselung nach dem WPA-PSK-Verfahren.
- **WEP**
  Verschlüsselung nach dem WEP-Verfahren.
- **WPA2**
  Verschlüsselung nach dem WPA2-Verfahren.
- **WPA2-PSK (AES)**
  Verschlüsselung nach dem WPA2-PSKVerfahren.

Encryption WPA-PSK

WPA-PSK Encryption-Typ:

Mögliche Optionen:

- **TKIP**
  Verschlüsselung nach dem TKIP-Protokoll zum Einsatz bei WPA-PSK.

Pre-Shared Key:

Angabe des PSE-Schlüssels zur Verschlüsselung.

WPA-PSK Passwort HEX

Schalter zum Aktivieren des WPA-PSK Passwort Hex.

Encryption WPA2-PSK

Pre-Shared Key:

Angabe des WPA2-PSK-Schlüssels zur Verschlüsselung.

Encryption WPA2

OKC:

Schalter zum Aktivieren von OKC (Opportunistic Key Caching).

Encryption WEP

WEP Mode

Angabe der WEP-Schlüssellänge. Bei 128 Bit muss der Schlüssel aus 13 ASCII-Zeichen oder 26 Hexadezimal-Zeichen bestehen, bei 64 Bit aus 5 ASCII-Zeichen oder 10 Hexadezimal-Zeichen.

WEP Key:

Angabe des WEP-Schlüssels zur Verschlüsselung.

WEP Authentisierungs-Mode:

Mögliche Optionen:

- **Open System**
  Der WEP-Schlüssel wird nur zur Datenverschlüsselung verwendet, nicht zur Authentifikation.
- **Shared Key**
  Der WEP-Schlüssel wird auch für die Authentifikation im WLAN verwendet wird, d. h. das Mobilteil kann sich im WLAN nur anmelden, wenn es den richtigen Schlüssel übergibt.

WEP Passwort Hex

Schalter zum Aktivieren des WEP Passwort Hex.

Encryption WPA

WPA Encryption-Typ:

Mögliche Optionen:

- **TKIP**

Verschlüsselung nach dem TKIP-Protokoll zum Einsatz bei WPA.

Encryption WPA2-PSK

Pre-Shared Key

Angabe des PSK-Schlüssels zur Verschlüsselung.

Encryption WPA2

OKC

Schalter zum Aktivieren von OKC (Opportunistic Key Caching).

7.1.20.3 Register „Location Server“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > WLAN Einstellungen > Register „Location Server“

Location Server

Ist dieser Schalter aktiviert, werden die Daten zu einem vorhandenen Location Server verwendet.

Location Server Adresse:

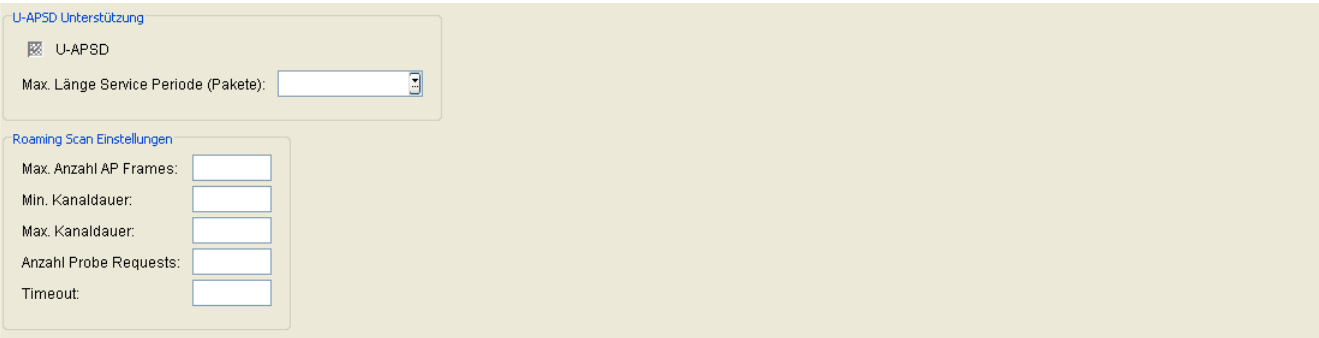
IP-Adresse oder Hostname des Location Servers.

Location Server Port:

Portnummer des Location Servers.

7.1.20.4 Register „Erweiterte Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > WLAN Einstellungen > Register „Erweiterte Einstellungen“



U-APSD Unterstützung

U-APSD

U-APSD aktivieren.

Max. Länge Service Periode (Pakete)

Maximale Länge der Service Periode, angegeben in Anzahl von Paketen.

Mögliche Optionen:

- **unbegrenzt max. 15**
- **2**
- **4**
- **6**

Roaming Scan Einstellungen

Max. Anzahl AP Frames

Maximale Anzahl von AP-Frames.

Min. Kanaldauer

Minimale Kanaldauer.

Max. Kanaldauer

Maximale Kanaldauer.

Anzahl Probe Requests

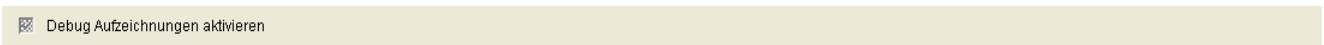
Anzahl der Probe Requests.

Timeout

Zeitüberschreitung nach Sekunden.

7.1.20.5 Register „Debug Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > WLAN Einstellungen > Register „Debug Einstellungen“



Debug Aufzeichnungen aktivieren

Ist der Schalter aktiviert, werden Debugging-Meldungen aufgezeichnet.

7.1.21 Signaling and Payload Encryption (SPE)

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Signaling and Payload Encryption (SPE)

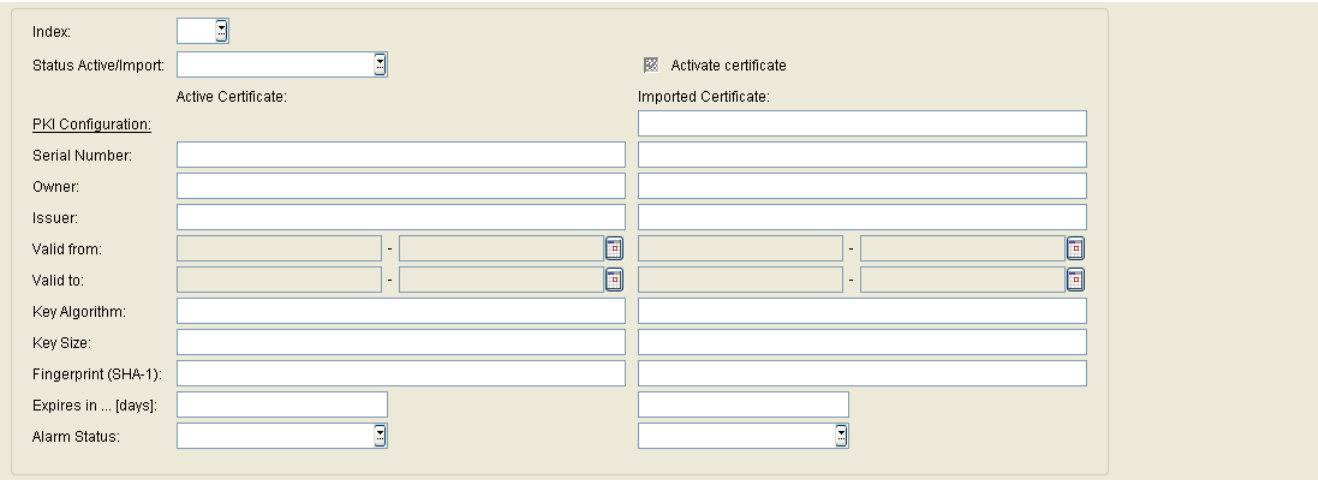
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SPE CA Zertifikate“
- Register „SIP Einstellungen“
- Register „HFA Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

7.1.21.1 Register „SPE CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Signaling and Payload Encryption (SPE) > Register „SPE CA Zertifikate“



Die nachfolgend beschriebenen Parameter stehen einmal für das derzeit aktive und einmal für das importierte Zertifikat zur Verfügung.

Index:

Laufende Nummer des CA Zertifikats.

Status Aktiv/Import:

Gibt an, ob ein Zertifikat importiert und/oder aktiv auf dem Phone registriert ist. Daraus ergeben sich die nachfolgend genannten 5 Zustände.

Mögliche Werte:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

PKI Konfiguration

Name der PKI Konfiguration.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Anzahl der verbleibenden Tage, bis das Zertifikat ungültig wird.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Anzeige der Gültigkeitsdauer von Zertifikaten, um in Kürze ablaufende Zertifikate zu suchen.

Mögliche Werte:

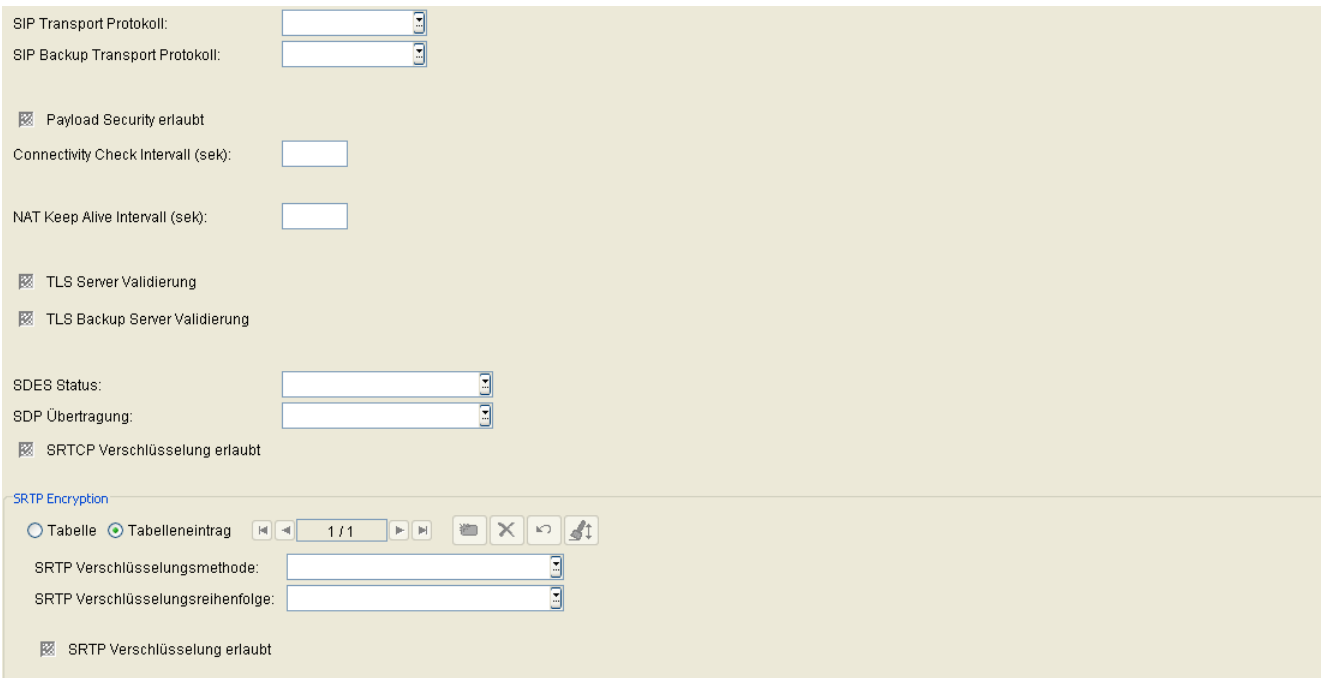
- **gültig**
- **in Kürze ungültig**
- **ungültig**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

7.1.21.2 Register „SIP Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Signaling and Payload Encryption (SPE) > Register „SIP Einstellungen“



SIP Transport Protokoll:

Protokoll für die SIP-Signalisierung.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

SIP Backup Transport Protokoll:

Mögliche Optionen:

- **UDP**
- **TCP**

Payload Security erlaubt

Ist der Schalter aktiviert, so wird die Verschlüsselung von Sprachdaten erlaubt.

Connectivity Check Intervall:

Zeitintervall, in dem die Verbindung auf Session Timeouts überprüft wird.

NAT Keep Alive Intervall (Sek):

Timer-Intervall, das die Übertragungsrate von NAT keep-alive Paketen steuert. Ist der Wert **0**, so ist der NAT keep-alive-Mechanismus abgeschaltet.

TLS Server Validierung

Bei aktiviertem Schalter wird überprüft, ob die TLS-Verbindung zum SIP-Server gültig ist.

Nur für OpenStage < 3.0

TLS Backup Server Validierung

Bei aktiviertem Schalter wird überprüft, ob die TLS-Verbindung zum Backup SIP-Server gültig ist.

Nur für OpenStage < 3.0

SDES Status

Auswahl des SDES-Status.

Mögliche Optionen:

- **deaktiviert**
- **aktiviert**

SDP Übertragung

Auswahl der SDP-Übertragung.

Mögliche Optionen:

- **SRTP und RTP**

- **nur SRTP**
- **Rückfallen auf RTP**

SRTCP Verschlüsselung erlaubt

Wenn aktiviert, wird mit SRTCP verschlüsselt.

SRTP Encryption

SRTP Verschlüsselungsmethode

Auswahl der SRTP Verschlüsselungsmethode.

Mögliche Optionen:

- **SHA1-32**
- **SHA1-80**

SRTP Verschlüsselungsreihenfolge

Auswahl der SRTP Verschlüsselungsreihenfolge.

Mögliche Optionen:

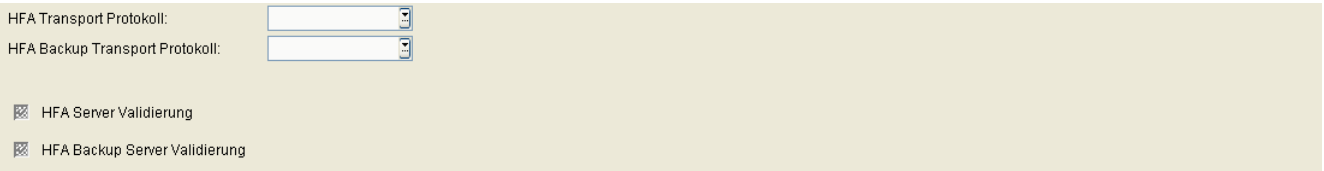
- **Auswahl 1**
- **Auswahl 2**

SRTP Verschlüsselung erlaubt

Wenn gesetzt, wird mit SRTP verschlüsselt.

7.1.21.3 Register „HFA Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Signaling and Payload Encryption (SPE) > Register „HFA Einstellungen“



HFA Transport Protokoll:

Protokoll für die HFA-Signalisierung.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

HFA Backup Transport Protokoll:

Protokoll für die HFA-Signalisierung.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

HFA Server Validierung

Ist der Schalter aktiviert, so wird die Verbindung zum HFA-Server überprüft.

HFA Backup Server Validierung

Ist der Schalter aktiviert, so wird die Verbindung zum HFA-Backupserver überprüft.

7.1.22 IEEE 802.1x

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IEEE 802.1x

HINWEIS: Ausführliche Informationen zur Einrichtung von IEE 802.1x finden Sie in der Administrationsanleitung „IEE 802.1x Konfigurations-Management“, online verfügbar unter
http://wiki.unify.com/index.php/VoIP_Security#IEEE_802.1X
und
http://wiki.unify.com/images/2/23/IEEE_802.1X_Configuration_Management.pdf

Dieser Bereich besteht aus folgenden Inhalten:

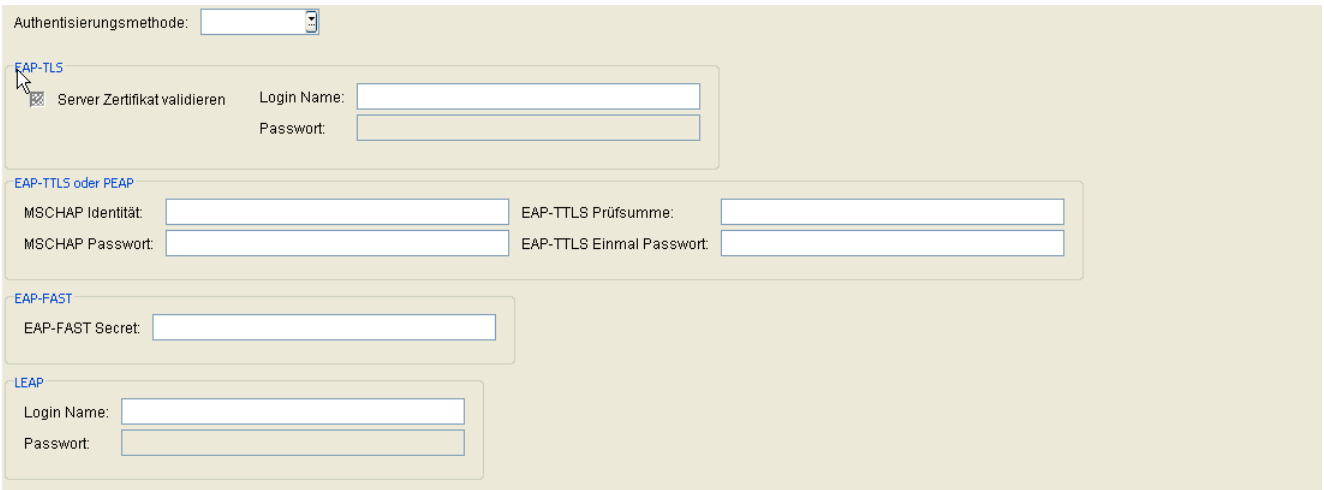
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „802.1x Einstellungen“
- Register „Phone Zertifikat“
- Register „RADIUS Server CA Zertifikat 1“
- Register „RADIUS Server CA Zertifikat 2“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.22.1 Register „802.1x Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IEEE 802.1x > Register „802.1x Einstellungen“



Authentisierungsmethode:

Mögliche Werte:

- **keine**
- **EAP-TLS**
- **LEAP**
- **PEAP**

EAP-TLS

Server Zertifikat validieren

Wenn der Schalter aktiviert ist, prüft das Endgerät das vom Access Point empfangene Server-Zertifikat auf Gültigkeit.

Login Name:

Login-Name zum Identifizieren.

Passwort:

Passwort zum Identifizieren.

EAP-TTLS oder PEAP

Bietet Unterstützung für IEEE 802.1x [802.1x], einen Standard für die portbasierte Netzwerkzugriffssteuerung. 802.1x stellt ein Authentifizierungs-Framework bereit, bei dem ein Benutzer (oder Gerät) durch eine zentrale Stelle (im RADIUS-Modell) authentifiziert wird und seinerseits die zentrale Stelle authentifiziert. Wenn dieser Schalter aktiviert ist, erfolgt die Authentifizierung über EAP-TTLS oder das PEAP-Protokoll.

MSCHAP Identität:

Gerätename für MSCHAP-V2 bei PEAP oder EAP-TTLS.

> ***HINWEIS:*** Wenn der neue Wert „PEAP“ ausgewählt wird, ist das Attribut „MSCHAP Identität“ (Element: mschap-identity) aktiviert.

MSCHAP Passwort:

Passwort für MSCHAP-V2 bei PEAP oder EAP-TTLS.
Der Wert erlaubt nur einen Schreibzugriff.

> ***HINWEIS:*** Wenn der neue Wert „PEAP“ ausgewählt wird, ist das Attribut „MSCHAP Passwort“ (Element: mschap-pw) aktiviert.

EAP-TTLS Prüfsumme

Prüfsumme anfordern für MD-Challenge bei EAP-TTLS.
Der Wert erlaubt nur einen Schreibzugriff.

EAP-TTLS Einmal Passwort

Einmal-Passwort für EAP-TTLS.
Der Wert erlaubt nur einen Schreibzugriff.

EAP-FAST

EAP-FAST Secret:

Geheimnis/Schlüssel für EAP-FAST.
Der Wert erlaubt nur einen Schreibzugriff.

LEAP

Login Name:

Login-Name zum Identifizieren am Access Point / WLAN Router.

Passwort:

Passwort zum Identifizieren am Access Point / WLAN Router.

7.1.22.2 Register „Phone Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IEEE 802.1x > Register „Phone Zertifikat“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren (Phone)

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

PKI Konfiguration

PKI Konfiguration des importierten Zertifikats.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus **SHA-1** (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.22.3 Register „RADIUS Server CA Zertifikat 1“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IEEE 802.1x > Register „RADIUS Server CA Zertifikat 1“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren (RADIUS 1)

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

PKI Konfiguration

PKI Konfiguration des importierten Zertifikats.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus **SHA-1** (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.22.4 Register „RADIUS Server CA Zertifikat 2“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > IEEE 802.1x > Register „RADIUS Server CA Zertifikat 2“

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren (RADIUS 2)

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

PKI Konfiguration

PKI Konfiguration des importierten Zertifikats.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus **SHA-1** (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.23 Diagnose

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Diagnose Einstellungen“
- Register „Datei Einstellungen“
- Register „Secure Shell (SSH) Zugang“
- Register „Remote Trace Einstellungen“
- Register „Diagnose- und Security Log Dateien“
- Register „Periodischer Datei-Upload“
- Register „Secure Trace Einstellungen“

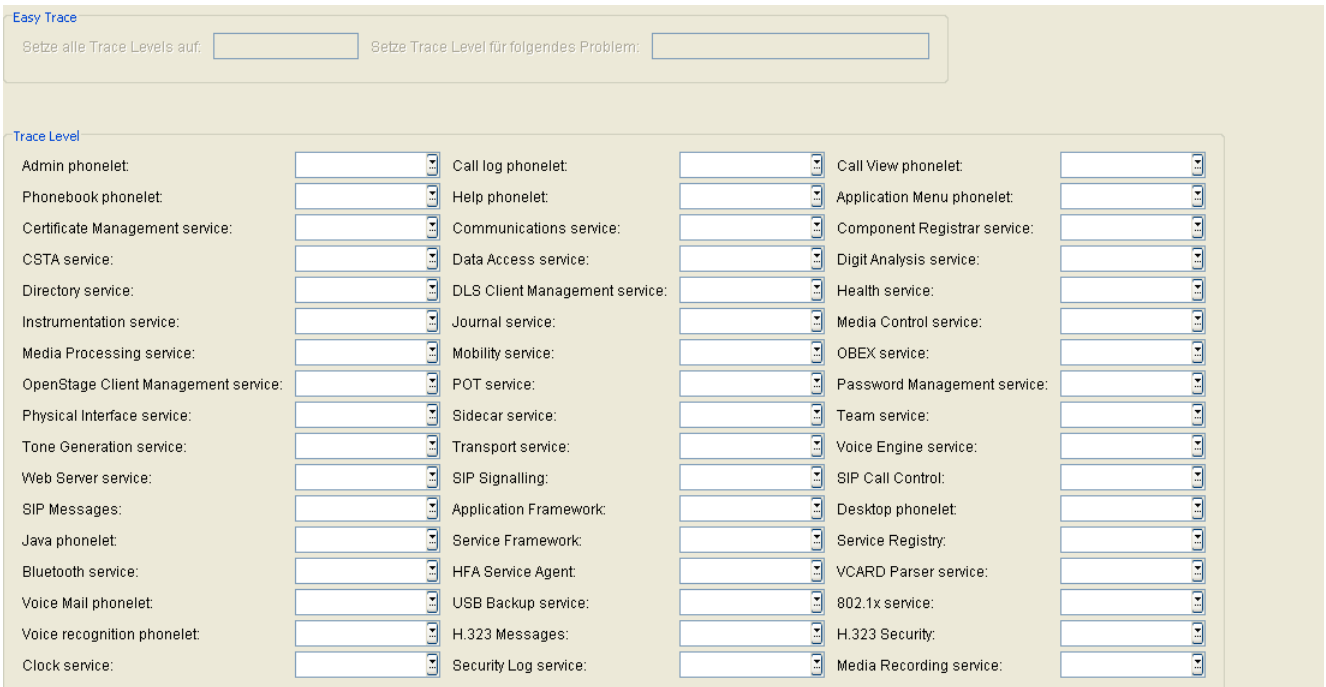
Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

7.1.23.1 Register „Diagnose Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Diagnose Einstellungen“

Hier wird das Fehler-Tracing für die einzelnen Komponenten des Telefons festgelegt. Die Tracefiles werden vom Telefon per FTP oder HTTPS auf einen Server hochgeladen.

> ***HINWEIS:*** Diese Einstellungen sind auch bei OpenStage 15/20- (nur SIP) und OpenScape Desk Phone IP 35 G-Telefonen verfügbar.



Easy Trace

Voreingestellte Profile erleichtern die Steuerung von Trace-Parametern. Es können sowohl gemeinsame Trace Level für alle Komponenten eingestellt werden, als auch Gruppen von Trace-Parametern, die zu einem bestimmten Funktionsbereich des Telefons gehören.

Setze alle Trace Levels auf:

Aktiviert alle Tracepunkte im Code von OpenStage-Telefonen. Für jeden Trace-Level kann ein eigener Wert eingestellt werden.

Mögliche Optionen:

- **Off**
- **Fatal**
- **Error**

- **Warning**
- **Trace**
- **Debug**

Setze Trace Level für folgendes Problem:

Auswahl eines bestimmten Funktionsbereich des Telefons, für den das Easy Trace-Profil gesetzt werden soll.

Mögliche Optionen:

- **Bluetooth headset profile**
- **Bluetooth handsfree profile**
- **Call connection**
- **Call log problems**
- **DAS connection**
- **DLS data errors**
- **Help application problems**
- **Key input problems**
- **LAN connectivity problems**
- **Messaging application problems**
- **Mobility problems**
- **OpenStage manager problems**
- **Phone administration problems**
- **Phonebook (LDAP) problems**
- **Phonebook (local) problems**
- **Server based application problems**
- **Sidecar problems**
- **Speech problems**
- **Tone problems**
- **USB audio features**
- **USB backup/restore**
- **Voice recognition problems**

- **Web based management**
- **802.1x problems**

Trace Level

Aktiviert bestimmte Tracepunkte im Code von OpenStage-Telefonen und dient der Fehlerlokalisierung. Für jeden Trace-Level kann ein eigener Wert eingestellt werden.

Admin phonelet:

Mögliche Optionen:

- **Off**
- **Fatal**
- **Error**
- **Warning**
- **Trace**
- **Debug**

Call log phonelet:

Mögliche Optionen wie bei Admin phonelet:

Call View phonelet:

Mögliche Optionen wie bei Admin phonelet:

Phonebook phonelet:

Mögliche Optionen wie bei Admin phonelet:

Help phonelet:

Mögliche Optionen wie bei Admin phonelet:

Application Menu phonelet:

Mögliche Optionen wie bei Admin phonelet:

Certificate Management service:

Mögliche Optionen wie bei Admin phonelet:

Communications service:

Mögliche Optionen wie bei Admin phonelet:

Component registrar service:

Mögliche Optionen wie bei Admin phonelet:

CSTA service:

Mögliche Optionen wie bei Admin phonelet:

Data Access service:

Mögliche Optionen wie bei Admin phonelet:

Digit Analysis service:

Mögliche Optionen wie bei Admin phonelet:

Directory service:

Mögliche Optionen wie bei Admin phonelet:

DLS Client Management service:

Mögliche Optionen wie bei Admin phonelet:

Health service:

Mögliche Optionen wie bei Admin phonelet:

Instrumentation service:

Mögliche Optionen wie bei Admin phonelet:

Journal service:

Mögliche Optionen wie bei Admin phonelet:

Media Control service:

Mögliche Optionen wie bei Admin phonelet:

Media Processing service:

Mögliche Optionen wie bei Admin phonelet:

Mobility service:

Mögliche Optionen wie bei Admin phonelet:

OBEX service:

Mögliche Optionen wie bei Admin phonelet:

OpenStage Client Management service:

Mögliche Optionen wie bei Admin phonelet:

POT service:

Mögliche Optionen wie bei Admin phonelet:

Password Management service:

Mögliche Optionen wie bei Admin phonelet:

Physical Interface service:

Mögliche Optionen wie bei Admin phonelet:

Sidecar service:

Mögliche Optionen wie bei Admin phonelet:

Team service:

Mögliche Optionen wie bei Admin phonelet:

Tone generation service:

Mögliche Optionen wie bei Admin phonelet:

Transport service:

Mögliche Optionen wie bei Admin phonelet:

Voice Engine service:

Mögliche Optionen wie bei Admin phonelet:

Web Server service:

Mögliche Optionen wie bei Admin phonelet:

SIP Signalling:

Mögliche Optionen wie bei Admin phonelet:

SIP Call Control:

Mögliche Optionen wie bei Admin phonelet:

SIP Messages:

Mögliche Optionen wie bei Admin phonelet:

Application Framework:

Mögliche Optionen wie bei Admin phonelet:

Desktop phonelet:

Mögliche Optionen wie bei Admin phonelet:

Java phonelet

Mögliche Optionen wie bei Admin phonelet:

Service Framework

Mögliche Optionen wie bei Admin phonelet:

Service Registry

Mögliche Optionen wie bei Admin phonelet:

Bluetooth service

Mögliche Optionen wie bei Admin phonelet:

HFA Service Agent service

Mögliche Optionen wie bei Admin phonelet:

VCARD Parser service

Mögliche Optionen wie bei Admin phonelet:

Voice Mail phonelet

Mögliche Optionen wie bei Admin phonelet:

USB Backup service

Mögliche Optionen wie bei Admin phonelet:

802.1x service

Mögliche Optionen wie bei Admin phonelet:

Voice recognition phonelet

Mögliche Optionen wie bei Admin phonelet:

H.323 Messages

Mögliche Optionen wie bei Admin phonelet:

H.323 Security

Mögliche Optionen wie bei Admin phonelet:

Clock service

Mögliche Optionen wie bei Admin phonelet:

Security Log service

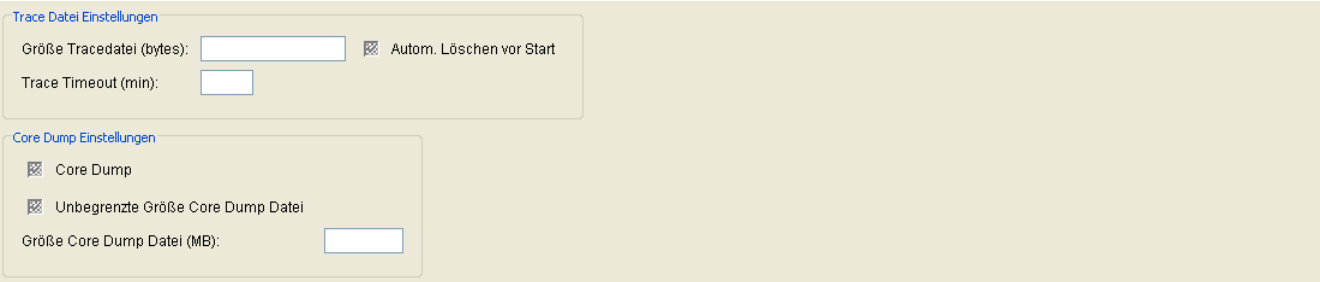
Mögliche Optionen wie bei Admin phonelet:

Media Recording service

Mögliche Optionen wie bei Admin phonelet:

7.1.23.2 Register „Datei Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Datei Einstellungen“



Trace Datei Einstellungen

Größe Tracedatei (bytes):

Gibt die Maximalgröße der Tracedatei an.

Wertebereich: **65536** ... **4194304** (64KB ... 4MB).

Trace Timeout (min):

Gibt an, nach wievielen Minuten der Timeout für das Tracing ausgelöst werden soll.

Autom. Löschen vor Start

Gibt an, ob der Tracespeicher vor einem erneuten Trace gelöscht werden soll.

Core Dump Einstellungen

Core Dump

Checkbox zum Aktivieren des Core Dumps.

Unbegrenzte Größe Core Dump Datei

Ist der Schalter aktiviert, ist eine Core Dump-Datei in unbegrenzter Größe zugelassen.

Größe Core Dump Datei (MB)

Gibt die Maximalgröße der Tracedatei an.

Wertebereich: **0** ... **1023**

Standardwert: **1000**

7.1.23.3 Register „Secure Shell (SSH) Zugang“

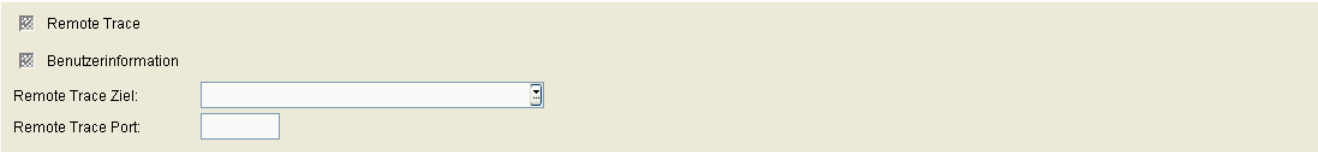
Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Secure Shell (SSH) Zugang“

Secure Shell (SSH) Zugang erlaubt

Ist dieser Schalter aktiviert, so ist ein Zugang zum Telefon über SSH möglich.

7.1.23.4 Register „Remote Trace Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Remote Trace Einstellungen“



Remote Trace

Ist dieser Schalter aktiviert, sendet das Telefon die Trace-Daten vom Endgerät direkt an die unter **Remote Trace Ziel** eingetragene Zieladresse.

Benutzerinformation

Am IP Phone wird angezeigt, wenn ein Trace auf diesem Gerät läuft.

Remote Trace Ziel

IP-Adresse oder Hostname des Servers, an den die Trace-Daten gesendet werden sollen.

Remote Trace Port

Nummer des Ports, auf dem der Server die Trace-Daten empfängt.

7.1.23.5 Register „Diagnose- und Security Log Dateien“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Diagnose- und Security Log Dateien“

Upload und Download von Diagnose- und Security Log Dateien

Upload Diagnose- und Security Log Dateien (vom Phone zum DLS Server)

Upload Dateien ...

Startet das einmalige Hochladen von Diagnose- und Security-Logdateien, unabhängig von den Einstellungen für das periodische Hochladen. Die Dateien können in einem Popup-Fenster für das Hochladen ausgewählt werden.

Geladene Diagnose-Dateien werden gespeichert unter

Pfad zum Abspeichern der Diagnosedateien, die für dieses Gerät hochgeladen wurden. Der Pfad kann über **Hauptmenü** > **Administration** > **File Server** > **OpenStage Diagnose Dateien** gesetzt werden.

Geladene Security Log Dateien werden gespeichert unter

Pfad zum Abspeichern der Security-Logdateien, die für dieses Gerät hochgeladen wurden. Der Pfad kann über **Hauptmenü** > **Administration** > **File Server** > **OpenStage Security Log Dateien** gesetzt werden.

Download aller Diagnose- und Security Log Dateien (vom DLS Server zum Client PC)

Download Dateien ...

Startet das Herunterladen von Diagnose- und Security-Logdateien in einer .zip-Datei.

Einstellungen für Security Log Upload

Security Log Datei speichern mittels DLS

Wenn aktiv, werden die Security-Logdateien des IP Device durch den DLS gespeichert.

Max. Anzahl Zeilen in Security Log Datei:

Maximale Anzahl von Zeilen, die die Security-Logdateien im IP Phone enthalten darf.

Wertebereich: **100** … **1000**

Speichern Security Log Datei nach Füllgrad

Legt den Prozentsatz an ungespeicherten Einträgen fest. Der Füllgrad hängt vom Wert von **Max. Anzahl Zeilen in Security Log Datei** ab. Ist dieser Füllgrad überschritten, wird die Security-Logdatei zum Speichern an den DLS geschickt.

Mögliche Optionen:

- **sofort sichern**
- **10%**
- **20%**
- **30%**
- **35%**
- **40%**
- **45%**
- **50%**
- **55%**
- **60%**
- **65%**
- **70%**

- **80%**
- **90%**

Security Log Datei zuletzt gespeichert

Datum der letzten Speicherung der Security-Logdatei.

Erlaube Benutzerzugriff auf Diagnosedaten

Ist der Schalter gesetzt, wird der Benutzerzugriff auf Diagnosedaten im Telefon erlaubt.

Verfügbar für OpenStage V3R0.

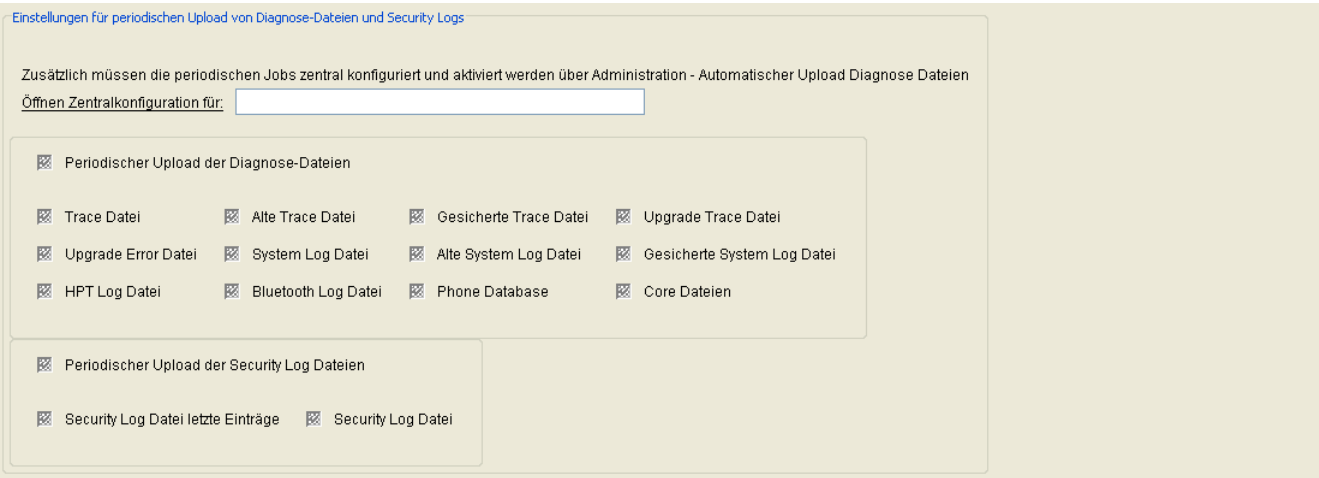
Diagnostic Call Prefix

Diagnoseanrufe können durch Wahl des „Diagnose-Anruf-Präfixes“ gefolgt von der Nummer des angerufenen Teilnehmers eingeleitet werden. Das Präfix besteht aus *(0-9)(0-9)(0-9)# .

Maximale Länge: 5 Stellen (einschließlich * und #)

7.1.23.6 Register „Periodischer Datei-Upload“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Periodischer Datei-Upload“



Einstellungen für den periodischen Upload von Diagnose- und Security-Logdateien.

Öffnen Zentralkonfiguration für:

Durch Klicken auf den Text wird die Zentralkonfiguration in **Administration** > **Automatischer Upload Diagnose- und Security Log Dateien** geöffnet. Der Name der Zielmaske wird im Textfeld angezeigt.

Periodischer Upload der Diagnose Dateien

Wenn aktiviert, werden Diagnosedateien periodisch geladen.

Trace Datei

Wenn aktiviert, wird die Tracedatei periodisch geladen.

Alte Trace Datei

Wenn aktiviert, wird die alte Tracedatei periodisch geladen.

Gesicherte Trace Datei

Wenn aktiviert, wird die gesicherte Tracedatei periodisch geladen.

Upgrade Trace Datei

Wenn aktiviert, wird die Tracedatei für den Upgrade-Vorgang periodisch geladen.

Upgrade Error Datei

Wenn aktiviert, wird die Datei für Fehlermeldungen beim Upgrade-Vorgang periodisch geladen.

System Log Datei

Wenn aktiviert, wird die System-Logdatei periodisch geladen.

Alte System Log Datei

Wenn aktiviert, wird die alte System-Logdatei periodisch geladen.

Gesicherte System Log Datei

Wenn aktiviert, wird die gesicherte System-Logdatei periodisch geladen.

HPT Log Datei

Wenn aktiviert, wird die HPT-Logdatei periodisch geladen.

Bluetooth Log Datei

Wenn aktiviert, wird die Bluetooth-Logdatei periodisch geladen.

Phone Database

Wenn aktiviert, wird die Datenbank des Telefons periodisch geladen.

Core Dateien

Wenn aktiviert, werden die Core-Dateien periodisch geladen.

Periodischer Upload der Security Log Dateien

Ist der Schalter aktiviert, werden Security Log Dateien periodisch geladen.

Security Log Datei letzte Einträge

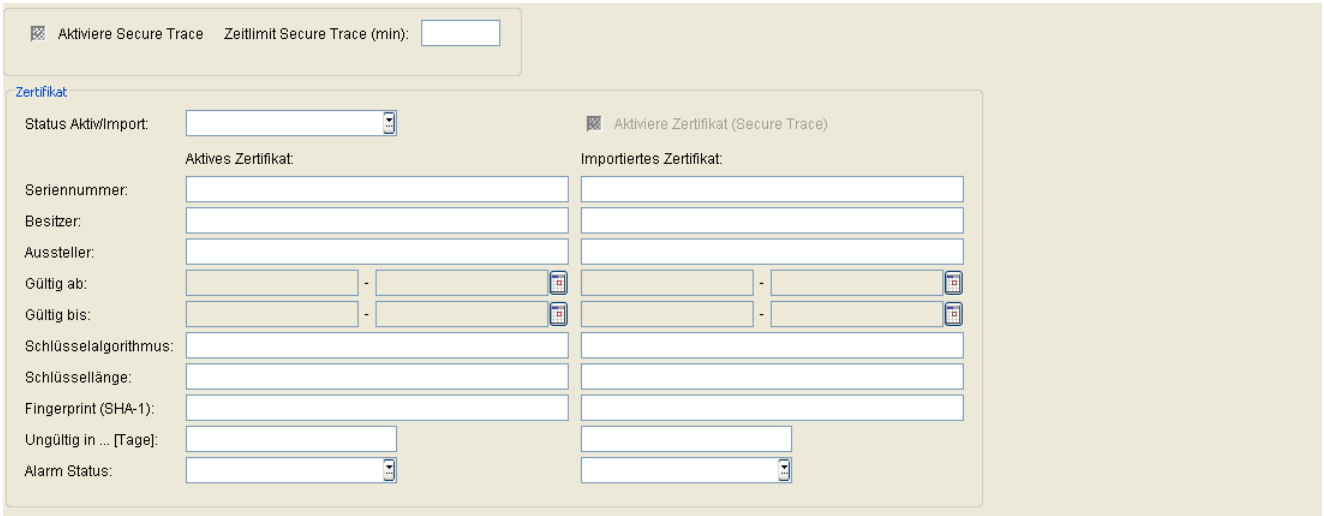
Ist der Schalter aktiviert, werden diejenigen Einträge hochgeladen, die in der Security Log Datei seit der letzten Speicherung hinzugekommen sind.

Security Log Datei

Ist der Schalter aktiviert, erfolgt ein Upload der Security Log Datei.

7.1.23.7 Register „Secure Trace Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Diagnose > Register „Secure Trace Einstellungen“



Aktiviere Secure Trace

Aktiviert Secure Tracing am Endgerät.

Zeitlimit Secure Trace (min)

Definition des Zeitraums in Minuten, innerhalb dessen Tracedaten gesammelt werden sollen.

Maximaler Wert: **43200** (= 30 Tage)

Zertifikat

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren (Secure Trace)

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird in ... Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

7.1.24 Sonstiges

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges

Dieser Bereich besteht aus folgenden Inhalten:

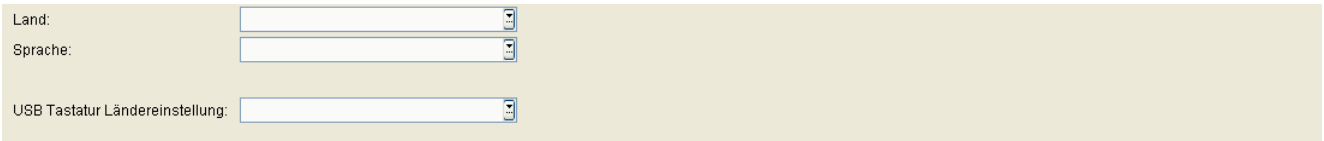
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Land & Sprache“
- Register „Messaging Services“
- Register „SIP Fehleranzeige“
- Register „Display / Geräte Einstellungen“
- Register „Internet Hilfe URL“
- Register „FTP Server“
- Register „Rufliste“
- Register „Telefonsperre“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.1.24.1 Register „Land & Sprache“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „Land & Sprache“



Land:

Land, in dem der Workpoint betrieben wird. Dieser Parameter entspricht der Ländereinstellung des Endgeräts.

Mögliche Optionen:

- **AR - Argentininen**
- **AT - Österreich**
- **AU - Australien**
- **BE - Belgien**
- **BR - Brasilien**
- **CA - Kanada**
- **CH - Schweiz**
- **CL - Chile**
- **CN - China**
- **CZ - Tschechien**
- **DE - Deutschland**
- **DK - Dänemark**
- **EE - Estland**
- **ES - Spanien**
- **FI - Finnland**
- **FR - Frankreich**
- **GB - Vereinigtes Königreich**
- **HR - Kroatien**
- **HU - Ungarn**
- **IE - Irland**
- **IN - Indien**

- **IT - Italien**
- **JP - Japan**
- **LT - Litauen**
- **LU - Luxemburg**
- **LV - Lettland**
- **MX - Mexiko**
- **NL - Niederlande**
- **NO - Norwegen**
- **NZ - Neuseeland**
- **PL - Polen**
- **PT - Portugal**
- **RU - Russische Föderation**
- **SE - Schweden**
- **SG - Singapur**
- **SK - Slowakische Republik**
- **TH - Thailand**
- **TR- Türkei**
- **US - Vereinigte Staaten**
- **VN - Vietnam**
- **ZA - Südafrika**
- **CY - Wales**

Sprache:

Sprache, die für lokale Anwendungen verwendet werden soll.

Mögliche Optionen:

- **bg - bulgarisch**
- **ca - katalanisch**
- **cs - tschechisch**
- **da - dänisch**

- **de - deutsch**
- **el - griechisch**
- **en - englisch**
- **en - englisch (US)**
- **es - spanisch**
- **et - estnisch**
- **fi - finnisch**
- **fr - französisch**
- **hr - kroatisch**
- **hu - ungarisch**
- **id - indonesisch**
- **it - italienisch**
- **ja - japanisch**
- **lt - litauisch**
- **lv - lettisch**
- **mk - mazedonisch**
- **ms - malaiisch**
- **nl - niederländisch**
- **no - norwegisch**
- **pl - polnisch**
- **pt - portugiesisch**
- **pt-br - brasilianisch**
- **ro - rumänisch**
- **ru - russisch**
- **sk - slowakisch**
- **sl - slowenisch**
- **sr - serbisch (kyrillisch)**
- **sr - serbisch (Latin)**
- **sv - schwedisch**
- **sr - serbisch**

- **tr - türkisch**
- **zh - chinesisch**
- **cy - walisisch**

USB Tastatur Ländereinstellung:

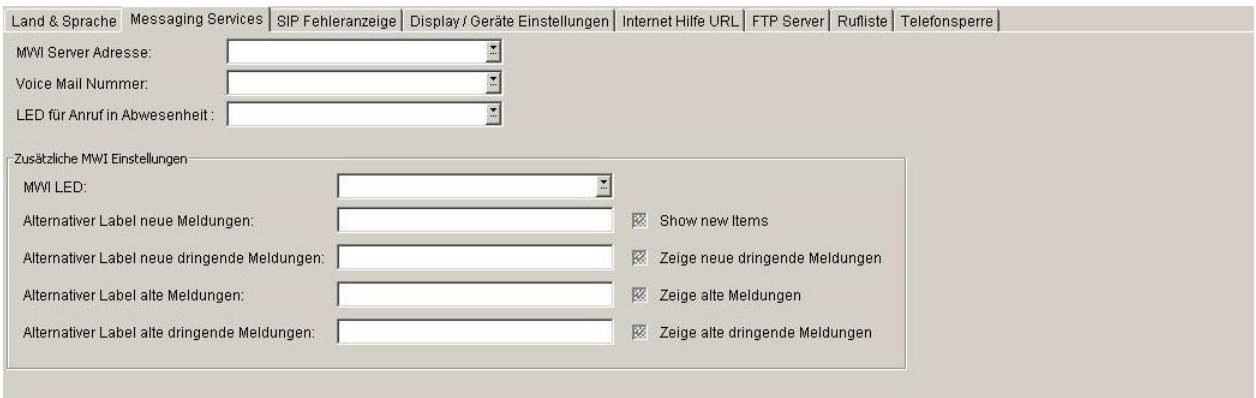
Sprachspezifisches Tastatur-Layout, beim Einsatz einer externen USB-Tastatur.

Mögliche Optionen:

- **Englisch**
- **Deutsch**
- **französisch**
- **spanisch**
- **amerikanisch**
- **italienisch**

7.1.24.2 Register „Messaging Services“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „Messaging Services“



MWI Server Adresse:

IP-Adresse oder Hostname des MWI-Servers.

Voice Mail Nummer:

Rufnummer der Voice Mail-Einrichtung (Nachrichten-Server).

LED für Anruf in Abwesenheit:

Zusätzliche MWI Einstellungen

Zeige neue Meldungen (Show new Items)

Anzahl der neuen Nachrichten anzeigen.

Zeige neue dringende Meldungen

Anzahl der neuen dringenden Nachrichten anzeigen.

Zeige alte dringende Meldungen

Anzahl der alten Nachrichten anzeigen.

Zeige alte dringende Meldungen

Anzahl der alten dringenden Nachrichten anzeigen.

Alternativer Label neue Meldungen

Titel für die Anzahl der neuen Nachrichten.

Alternativer Label neue dringende Meldungen

Titel für die Anzahl der neuen dringenden Nachrichten.

Alternativer Label alte Meldungen

Titel für die Anzahl der alten Nachrichten.

Alternativer Label alte dringende Meldungen

Titel für die Anzahl der alten dringenden Nachrichten.

7.1.24.3 Register „SIP Fehleranzeige“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „SIP Fehleranzeige“

Piepton bei Fehler

Schalter zum Aktivieren der akustischen Signalisierung von Fehlern bei der Kommunikation mit dem Microsoft RTC.

Nur bei SIP-Workpoints verfügbar.

7.1.24.4 Register „Display / Geräte Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „Display / Geräte Einstellungen“

Handset Name

Handset Name:

Name des WLAN-Handsets, der im Display des Handsets angezeigt wird.

Wertebereich: max. 16 alphanumerische Zeichen.

Display-Einstellungen

Display-Stil:

Bestimmt das Aussehen der grafischen Benutzeroberfläche von OpenStage-Telefonen.

Mögliche Optionen:

- **Silber Blau**
- **Anthrazit Orange**

Inaktivitäts-Verzögerung (min):

Zeit in Minuten, nach der der Bildschirm gedimmt wird, wenn bisher keine Aktivitäten am Bildschirm stattgefunden haben.

- **0** (Kein Timeout)

- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Display Helligkeit

Einstellung der Bildschirmhelligkeit.

Mögliche Optionen:

- **-3**
- **-2**
- **-1**
- **Standard**
- **+1**
- **+2**
- **+3**

Hintergrundbeleuchtung Timeout (std):

Sobald das Telefon länger als die hier angegebene Zeitspanne im Ruhezustand ist, wird die Hintergrundbeleuchtung abgeschaltet.

HINWEIS: Dieser Parameter ist nur für IP Devices mit **Display Hintergrundbeleuchtung = Standard** gültig, siehe auch Abschnitt 7.5.1, “Inventar Daten”.

Mögliche Optionen:

- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

- **8**

Hintergrundbeleuchtung Timeout energiesparendes Display

Sobald ein Telefon mit energiesparendem Display länger als die hier angegebene Zeitspanne im Ruhezustand ist, wird die Hintergrundbeleuchtung abgeschaltet.

HINWEIS: Dieser Parameter ist nur für IP Devices mit **Display Hintergrundbeleuchtung = CCFL** oder **Display Hintergrundbeleuchtung = LED** gültig, siehe auch Abschnitt 7.5.1, “Inventar Daten”.

Mögliche Optionen:

- **1 min**
- **5 min**
- **30 min**
- **60 min**
- **2 std**
- **3 std**
- **4 std**
- **5 std**
- **6 std**
- **7 std**
- **8 std**

Unbenutzt Timeout (min):

Zeit in Minuten, nach der der Bildschirm gedimmt wird, wenn bisher keine Aktivitäten am Bildschirm stattgefunden haben.

Mögliche Optionen:

- **0**
- **5**
- **10**
- **20**
- **30**
- **60**

- **120**

Bildschirmschoner

Bildschirmschoner aktivieren

Schalter zum Aktivieren des Bildschirmschoners.

Bildschirmschoner Übergangszeit (sek)

Zeitabstand in Sekunden, in dem die Bilder wechseln.

Mögliche Optionen:

- **5**
- **10**
- **20**
- **30**
- **60**

Allgemeine Geräteeinstellungen:

Unbenutzt Timeout (min):

Bestimmt die Zeit in Minuten, nach der das Telefon bestimmte Zustände wieder beendet, nachdem keine Eingabe erfolgt ist.

Beispiel: Beenden des Konfigurationsmenüs nach einer vorgegebenen Zeit.

Anruf-Menü (HFA)

Autom. Ausblenden Anruf-Menü:

Ist der Schalter aktiviert, so wird das Anruf-Menü nach einer einstellbaren Zeit automatisch ausgeblendet.

Autom. Ausblenden Anruf-Menü Timer (sek):

Bestimmt die Zeit in Sekunden, nach der das Ausblenden des Anruf-Menüs beginnen soll.

Mögliche Werte:

- **0**

- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Kontextmenü (SIP)

Autom. Zeigen Kontextmenü

Wenn aktiviert, wird das Kontextmenü automatisch angezeigt.

Anzeigedauer (sek)

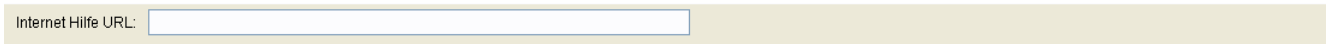
Das Kontextmenü wird nach der hier eingestellten Zeit ausgeblendet, in Sekunden.

Mögliche Werte:

- **Kein Ausblenden**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

7.1.24.5 Register „Internet Hilfe URL“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „Internet Hilfe URL“



Internet Hilfe URL:

URL der Web-Hilfeseite im Internet mit Informationen zum Telefon.

7.1.24.6 Register „FTP Server“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „FTP Server“

Verwende FTP im Passiv-Mode

Diese Checkbox aktiviert den passiven Modus für die Verbindung zwischen Telefon und FTP-Server. Der passive Modus wird benutzt, wenn es für den FTP-Server nicht möglich ist, eine Verbindung zum Client zu initiieren, z. B. weil eine Firewall dies verhindert.

7.1.24.7 Register „Rufliste“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „Rufliste“

Lösche Rufliste

Löscht den Inhalt der Rufliste.

7.1.24.8 Register „Telefonsperre“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > Sonstiges > Register „Telefonsperre“

Telefon sperren

Sperrt das Telefon.

7.1.25 File Deployment

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > File Deployment

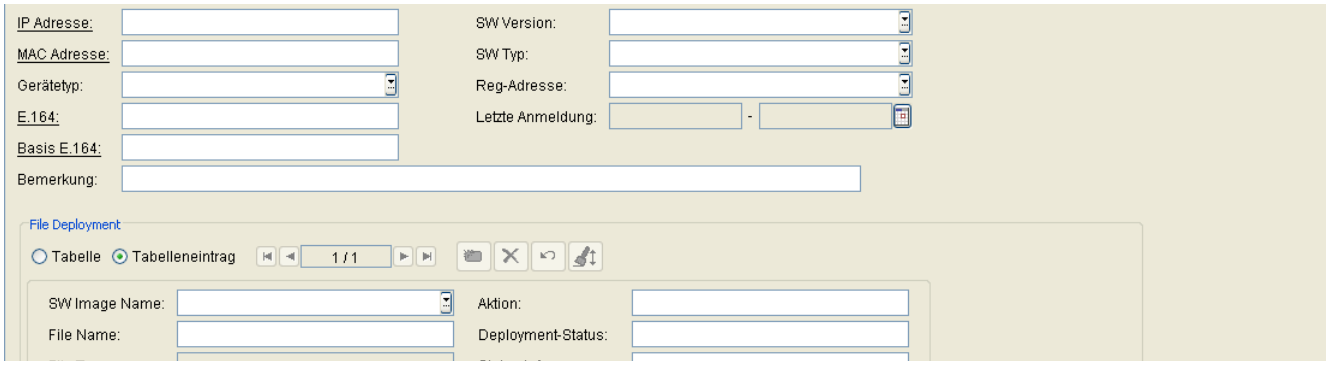
Hier können Dateien, die per Scan in die DLS-Datenbank eingelesen worden sind (siehe Abschnitt 6.3.4, “FTP Server Konfiguration”), auf ein IP Device übertragen werden. Es ist möglich, mehrere Dateien auf einmal zu übertragen. Zur Übersicht aller vom DLS unterstützten Software-Typen siehe Abschnitt 3.5, “Übersicht der Software- und Datei-Typen”.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Dateien“

7.1.25.1 Register „Dateien“

Aufruf: Hauptmenü > IP Devices > IP Phone Konfiguration > File Deployment > Register „Dateien“



HINWEIS: LDAP-Templates können auch auf OpenStage 15/20- (nur SIP) und OpenScape Desk Phone IP 35 G-Telefonen bereitgestellt werden.

File Deployment

SW Image Name:

Name des Software-Images.

Dateiname:

Name der Datei.

Dateityp:

Verwendungszweck der Datei.

HINWEIS: Viele Dateitypen auf dem FTP-Server sind für mehrere Zwecke verwendbar. In solchen Fällen gibt es für jede Verwendungsmöglichkeit einen Tabelleneintrag. Beispielsweise kann eine WAV-Datei sowohl als Klingelton als auch als Wartemusik (Music on Hold) verwendet werden. Ruftondateien dürfen nicht größer als 1Mb, Screensaver und Logo Dateien nicht größer als 300kb sein.

Beispiel: **Logo Datei** (OpenStage 40/60/80), **Bildschirmschoner** (OpenStage 40/60/80).

Server Typ:

Protokoll des Servers, der die Datei bereitstellt.

Mögliche Werte:

- **FTP**
- **HTTPS**

HTTPS-URL:

URL des Software-Images bei Verwendung eines HTTPS-Servers.

FTP Server:

ID des FTP-Servers, der die Datei bereitstellt. Wird bei Verwendung eines FTP-Servers benötigt.

FTP Pfad:

Pfad der Datei bei Verwendung eines FTP-Servers.

Aktion:

Gibt an, was mit der Datei stattfinden soll.

Mögliche Werte:

- **delete**
- **deploy**

Deployment-Status:

Status der Deployment-Aktion.

Status Info:

Informationen zum Status.

Deployment-Datum:

Datum des neuesten File Deployment.

Deployment Zeit:

Uhrzeit des neuesten File Deployment.

Deployment-Urheber:

Schnittstelle, über die das Deployment angestoßen wurde.

Mögliche Werte:

- **DLS**
- **WBM**
- **Lokal**

7.2 IP Client Konfiguration

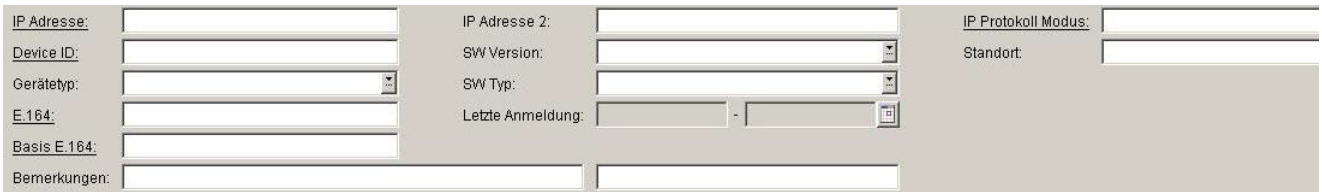
Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration

Dieses Menü besteht aus folgenden Untermenüs:

- CTI Konfiguration
- Gateway / Server
- Ports
- Quality of Service
- Telefonie
- Small Remote Site Redundancy
- Wahlparameter
- Audio / Video Einstellungen
- Verzeichnisse / Adressbücher
- Sonstiges
- Keysets / Tastenbelegung
- Signaling and Payload Encryption (SPE)
- Einwahlort
- OpenScape

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Clients zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Clients angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des IP Clients.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device.

Gerätetyp:

Gerätetyp des IP Clients.

Alle vom DLS unterstützte IP Client-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **optiClient 130**

E.164:

Vollständige E.164-Rufnummer des IP Clients.

Beispiel: **498972212345** (oder keine Angabe).

Siehe hierzu Kapitel 17, “E.164”.

SW Version:

Software-Version des IP Phones.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

Reg-Adresse:

IP-Adresse des Gateways oder des Gatekeepers, an dem sich das IP Device registrieren muss. Bei HiPath 3000 ist das die Adresse der HG 1500, bei HiPath 4000 ist es die HG 3530 oder das STMI-Board.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Clients.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Inhaltsbereich”.

Bemerkungen:

Felder für allgemeine Informationen.

Standort

Aktueller Standort des IP Device. der bei der Registrierung ermittelt und hier angezeigt wird. (Zur Bedeutung und Konfiguration des Standorts siehe Abschnitt 6.3.2, “Standort”.)

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Clients, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Deploy

Startet einen Job zur Verteilung der Konfigurationsänderungen. Siehe hierzu Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”.

Holen

Lädt ein bereits gesichertes Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Sichern

Sichert Konfigurations-Einträge als Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Umbenennen

Ändert den Namen eines gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Löschen

Löscht ein gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

7.2.1 CTI Konfiguration

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration

Dieses Menü besteht aus folgenden Untermenüs:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- CTI HFA Provider
- CSTA Service Provider

7.2.1.1 CTI HFA Provider

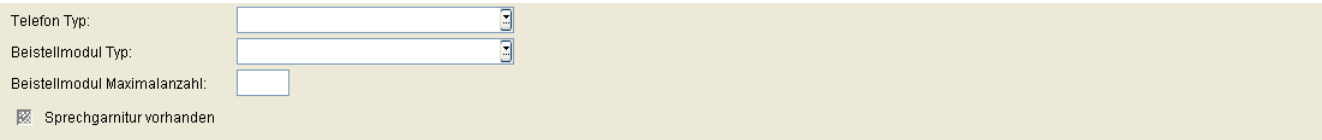
Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CTI HFA Provider

Dieses Menü besteht aus folgenden Untermenüs:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Endgerät“
- Register „Verbindung“
- Register „Netzzugang“
- Register „Lizenzierung“

Register „Endgerät“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CTI HFA Provider > Register „Endgerät“



Gerätetyp:

Typ des Telefons, das über den CTI Provider gesteuert werden soll.

Mögliche Optionen:

- **optiSet E advance China**
- **optiPoint 410 standard (DA Mode)**
- **optiPoint 410 standard**
- **optiPoint 410 advance**
- **optiPoint 420 standard**
- **optiPoint 420 advance**
- **optiSet E comfort**
- **optiSet E advance**

Beistellmodul Typ

Typ des angeschlossenen Beistellmoduls, falls vorhanden.

Mögliche Optionen:

- **optiPoint Key Module**
- **optiPoint Self Labeling Keys Module**
- **optiSet E Key Module**

Beistellmodul Maximalanzahl

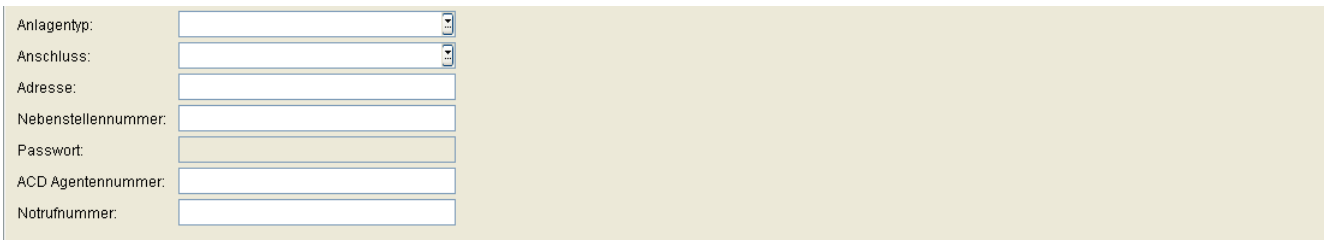
Anzahl der vorhandenen Beistellmodule.

Headset vorhanden

Ist dieser Schalter aktiviert, werden steht nur Angaben im interpretiert.

Register „Verbindung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CTI HFA Provider > Register „Verbindung“



Anlagentyp

Mögliche Optionen:

- **HiPath 3000**
  Schließt auch HiPath 5000, OpenScape Office MX/LX und OpenOffice EE ein.
- **HiPath 4000**

Anschluss

Hardware-Anschluss, der für die CTI-Kommunikation mit dem Endgerät verwendet wird. Falls USB zur Anwendung kommt, ist ein besonderer Treiber notwendig, der einen COM-Port emuliert. Näheres hierzu in der Administratordokumentation zum optiClient.

Mögliche Optionen:

- **LAN**
- **COM1**
- **COM2**
- **COM3**
- **COM4**
- **COM5**
- **COM6**
- **COM7**
- **COM8**
- **COM9**

Adresse

IP-Adresse der Anlage.

User ID:

Nebenstellennummer des Endgeräts.

Passwort:

Zur Nebenstellennummer gehöriges Passwort.

ACD Nummer:

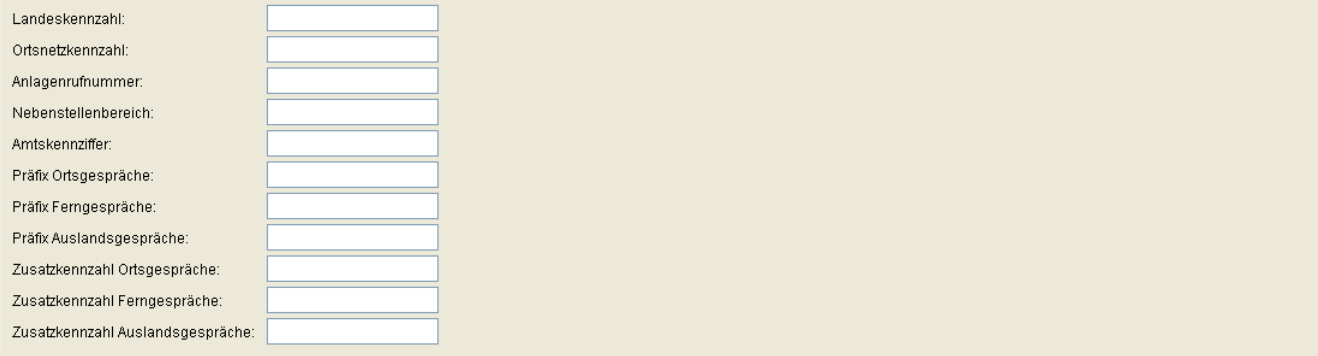
Wird benötigt, wenn der Benutzer als ACD (Automatic Call Distribution)-Agent arbeitet.

Notrufnummer:

Im Endgerät eingestellte Notrufnummer.

Register „Netzzugang“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CTI HFA Provider > Register „Netzzugang“



Landeskennzahl:

E.164-Landeskennzahl, ohne „führende“ Nullen. Maximale Länge: 4 Stellen.

Beispiel: **49** für Deutschland**,** 44 für United Kingdom.

Ortsnetzkennzahl:

Ortsnetzkennzahl ohne führende Nullen. Maximale Länge: 21 Stellen.

Beispiel: **89** for München, **20** für London.

Anlagenrufnummer:

Rufnummer der Firmenanlage/PBX, an die das Telefon angeschlossen ist. Maximale Länge: 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Nebenstellenbereich:

Dieser Parameter definiert ein Muster, anhand dessen interne Nebenstellennummern erkannt werden können. Nebenstellennummern sind aus der Sicht des Workpoints intern, wenn sie derselben Anlage zugeordnet sind. Der Nebenstellenbereich kann als regulärer Ausdruck angegeben werden.

Beispiel: 1xxx, 2xxx, 3xxx, 4xxx , 5xxx seien Nebenstellen und 6xxx, 7xxx, 8xxx, 9xxx seien externe Rufnummern. Der reguläre Ausdruck ^[12345] legt fest, dass Rufnummern, die mit einer der Ziffern 1 bis 5 beginnen, zu den internen Nebenstellennummern gehören. Wenn also beispielsweise die Anlagenrufnummer 667 ist, so werden die Rufnummern von 6671xxx bis 6675xxx als interne Nebenstellen behandelt.

Amtskennziffer:

Nummer zur „Amtsholung“ für ein externes ausgehendes Gespräch. Sind am angeschlossenen Kommunikationssystem mehrere Amtskennziffern konfiguriert, geben Sie diese mit Hilfe des Trennzeichens „|“ in diesem Feld ein. (Im Beispiel 0 und 88). Für die Ergänzung von Rufnummern zur Wahl wird immer der erste eingetragene Wert herangezogen. Maximale Länge: 5 Stellen.

Beispiele: **0**, **74**, **9** (USA).

Präfix Ortsgespräche:

Präfix für Ortsgespräche. Diese Angabe wird vom Netzbetreiber bestimmt und ist unabhängig von der Konfiguration der Anlage. Maximale Länge: 21 Stellen.

Beispiel: **01081**

Präfix Ferngespräche:

Nummer für ein ausgehendes Gespräch im Fernbereich. Diese Angabe wird vom Netzbetreiber bestimmt und ist unabhängig von der Konfiguration der Anlage. Maximale Länge: 21 Stellen.

Beispiel: **01081**

Präfix Auslandsgespräche:

Nummer für ein ausgehendes Gespräch im internationalen Bereich. Diese Angabe wird vom Netzbetreiber bestimmt und ist unabhängig von der Konfiguration der Anlage. Maximale Länge: 21 Stellen.

Beispiel: **01081**

Zusatzkennzahl Ortsgespräche:

Diese Nummer ist als Call-by-Call-Vorwahl für Ortsgespräche vorgesehen. Die Angabe ist unabhängig von der Konfiguration des angeschlossenen Providers. Maximale Länge: 21 Stellen.

Beispiel: **01019**

Zusatzkennzahl Ferngespräche:

Diese Nummer ist als Call-by-Call-Vorwahl für Ferngespräche vorgesehen. Die Angabe ist unabhängig von der Konfiguration des angeschlossenen Providers. Maximale Länge: 5 Stellen.

Beispiel: **01015**

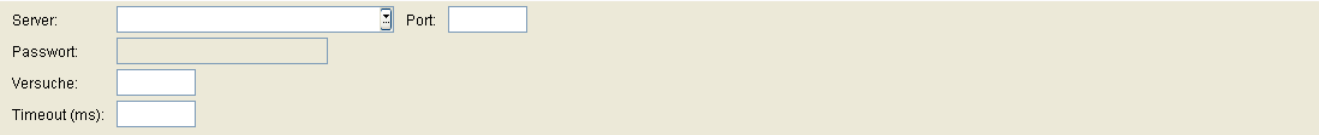
Zusatzkennzahl Auslandsgespräche:

Diese Nummer ist als Call-by-Call-Vorwahl für Ferngespräche vorgesehen. Die Angabe ist unabhängig von der Konfiguration des angeschlossenen Providers. Maximale Länge: 5 Stellen.

Beispiel: **01015**

Register „Lizenzierung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CTI HFA Provider > Register „Lizenzierung“



Server:

IP-Adresse des Servers, der die Lizenzen bereithält.

Passwort:

Passwort für den Zugang zum Lizenzserver.

Versuche:

Anzahl der Versuche, Verbindung zum Lizenzserver aufzunehmen.

Timeout (ms):

Zeitüberschreitung für Versuche, Verbindung zum Lizenzserver aufzunehmen.

Port:

Portnummer des Lizenzservers.

7.2.1.2 CSTA Service Provider

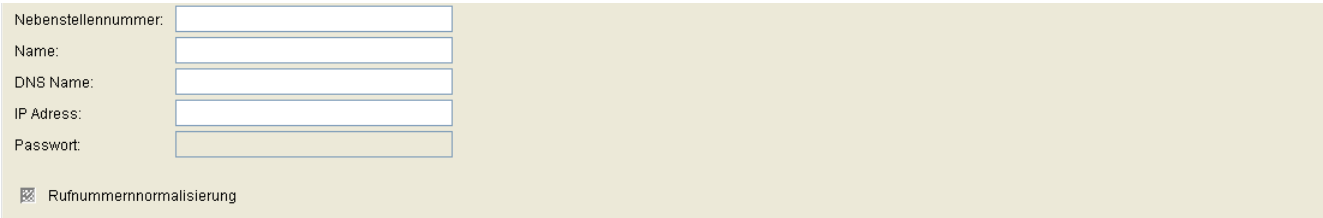
Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CSTA Service Provider

Dieses Menü besteht aus folgenden Untermenüs:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Verbindung“
- Register „Netzzugang“
- Register „Lizenzierung“

Register „Verbindung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CSTA Service Provider > Register „Verbindung“



Nebenstellennummer

Nebenstellnummer bzw. Subscriber ID, die vom CSTA Service Provider gesteuert wird.

Name

Logischer Name für die Nebenstellennummer, die vom CSTA Service Provider gesteuert wird.

DNS Name

DNS-Name des CSTA Service Providers.

IP Adresse:

IP-Adresse des CSTA Service Providers.

Passwort:

Passwort, das benötigt wird, um den CSTA Service Provider zu starten.

Rufnummernnormalisierung

Aktiviert die Normalisierung der Rufnummern zum E.164-Format.

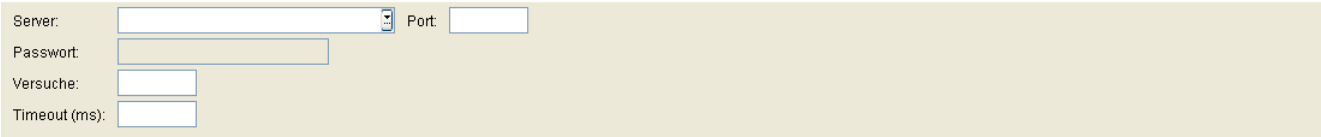
Register „Netzzugang“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CSTA Service Provider > Register „Netzzugang“

Siehe Abschnitt 7.2.7.1, “Register „HFA Wahlparameter“”.

Register „Lizenzierung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > CTI Konfiguration > CSTA Service Provider > Register „Lizenzierung“



Server:

IP-Adresse des Servers, der die Lizenzen bereithält.

Passwort:

Passwort für den Zugang zum Lizenzserver.

Versuche:

Anzahl der Versuche, Verbindung zum Lizenzserver aufzunehmen.

Timeout (ms):

Zeitüberschreitung für Versuche, Verbindung zum Lizenzserver aufzunehmen.

Port:

Portnummer des Lizenzservers.

7.2.2 Gateway / Server

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server

Dieser Bereich besteht aus folgenden Inhalten:

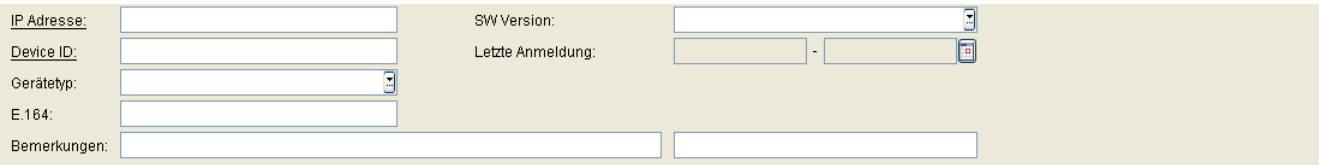
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Gateway“
- Register „Gateway (Standby)“
- Register „SW Deployment“
- Register „HFA Einstellungen“
- Register „SIP Verbindung“
- Register „SIP Registrar“
- Register „SIP Proxy“
- Register „SIP Gateway“
- Register „Systemdienste“
- Register „SIP Survivability“
- Register „Lizenzen“
- Register „VPN Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Clients zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Clients angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des IP Clients.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device.

Gerätetyp:

Gerätetyp des IP Clients.

Alle vom DLS unterstützte IP Client-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **optiClient 130**

E.164:

Vollständige E.164-Rufnummer des IP Clients.

Beispiel: **498972212345** (oder keine Angabe).

Siehe hierzu Kapitel 17, “E.164”.

SW Version:

Software-Version des IP Phones.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

Reg-Adresse:

IP-Adresse des Gateways oder des Gatekeepers, an dem sich das IP Device registrieren muss. Bei HiPath 3000 ist das die Adresse der HG 1500, bei HiPath 4000 ist es die HG 3530 oder das STMI-Board.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Clients.

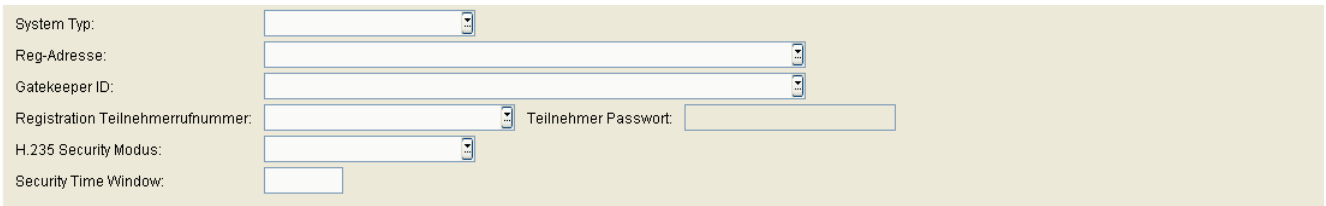
Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Inhaltsbereich”.

Bemerkungen:

Felder für allgemeine Informationen.

7.2.2.1 Register „Gateway“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „Gateway“



System Typ:

Art und Version der Kommunikationsplattform, an der der Workpoint betrieben wird.

Mögliche Optionen:

- **HiPath 3000**
  Schließt auch HiPath 5000, OpenScape Office MX/LX und OpenOffice EE ein.
- **HiPath 4000**

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Reg-Adresse:

IP-Adresse oder Host-Name der PBX, die zum Betrieb des Workpoints eingesetzt wird.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Gatekeeper ID:

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Registration Teilnehmerrufnummer:

Rufnummer des IP Clients an der PBX.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Teilnehmer Passwort:

Passwort des IP Clients an der PBX.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

H.235 Security Modus:

Mögliche Optionen:

- **Keine**
  Ohne Sprachverschlüsselung.
- **Vermindert**
  Mit einseitiger Sprachverschlüsselung (Gatekeeper sendet nicht verschlüsselt).
- **Voll**
  Mit beidseitiger Sprachverschlüsselung (Workpoint und Gatekeeper senden verschlüsselt).

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Security Time Window:

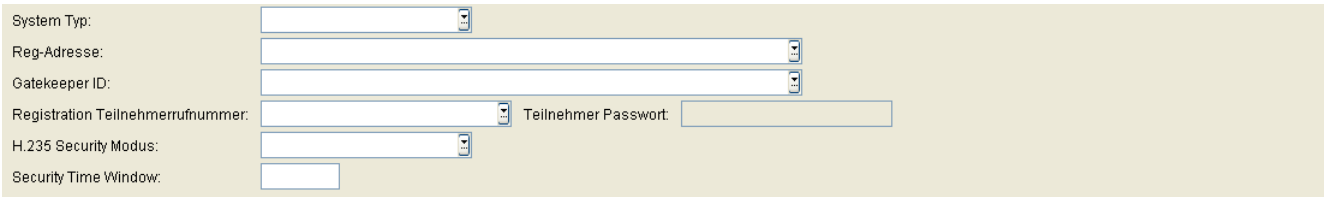
Es werden nur Nachrichten vom Gateway akzeptiert, die innerhalb des hier angegebenen Zeitfensters eintreffen.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

7.2.2.2 Register „Gateway (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „Gateway (Standby)“

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „Gateway“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.2.6, “Small Remote Site Redundancy”.



System Typ:

Art und Version der Kommunikationsplattform, an der der Workpoint betrieben wird.

Mögliche Optionen:

- **HiPath 3000**
  Schließt auch HiPath 5000, OpenScape Office MX/LX und OpenOffice EE ein.
- **HiPath 4000**
- **kein Rückfallsystem**

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Reg-Adresse (Standby):

IP-Adresse oder Host-Name der Standby-PBX, die zum Betrieb des Workpoints eingesetzt wird.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Gatekeeper ID:

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Registration Teilnehmerrufnummer:

Rufnummer des IP Clients an der Standby-PBX.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

Teilnehmer Passwort:

Passwort des IP Clients an der Standby-PBX.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

H.235 Security Modus:

Mögliche Optionen:

- **Keine**
  Ohne Sprachverschlüsselung.
- **Vermindert**
  Mit einseitiger Sprachverschlüsselung (Gatekeeper sendet nicht verschlüsselt).
- **Voll**
  Mit beidseitiger Sprachverschlüsselung (Workpoint und Gatekeeper senden verschlüsselt).

Nur bei HFA-IP Clients verfügbar.

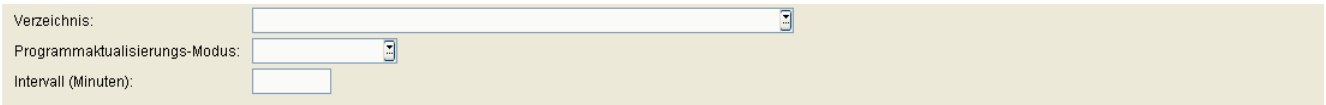
Security Time Window:

Es werden nur Nachrichten vom Gateway akzeptiert, die innerhalb des hier angegebenen Zeitfensters eintreffen.

Wirkt sich nur auf die HFA-Konfiguration des IP Clients aus.

7.2.2.3 Register „SW Deployment“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „SW Deployment“



Verzeichnis:

Vollständiger Pfad des Verzeichnisses, in dem der IP Client nach SW Updates sucht.

Programmaktualisierungs-Modus:

Mögliche Werte:

- **Kein**
  Keine Prüfung.
- **Start**
  Prüfung bei Programmstart.
- **Intervall**
  Permanente Prüfung in Intervallen.

Intervall (min):

Intervall in Minuten für die permanente Prüfung auf SW-Updates.

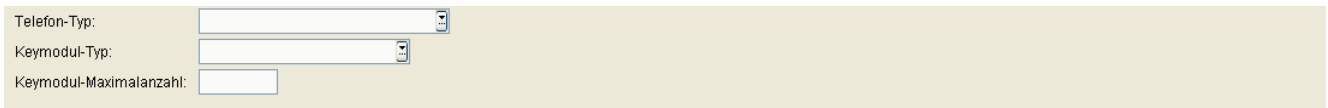
7.2.2.4 Register „HFA Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „HFA Einstellungen“

Die Darstellung des optiClient 130 Telefons lehnt sich an das Aussehen verschiedener Endgerätetypen an.

Für die Darstellung des optiClient 130 Telefons und des erweiterten Tastenfeldes können Sie unter verschiedenen Endgerätetypen für Telefon und Keymodul wählen.

Der eingestellte Telefon- und Keymodul-Typ für den optiClient 130 entspricht in Darstellung und Ausprägung den jeweiligen Tischgeräten. Keymodule werden im erweiterten Tastenfeld des optiClient 130 dabei als Spalten dargestellt.



Telefon-Typ:

Der Telefon-Typ bestimmt:

- Wieviele Displayzeilen im freien Telefon des optiClient 130 angezeigt werden (bei integriertem Telefon in der Hauptleiste immer zweizeilig).
- Ob Self Labeling Keys für den optiClient 130 verfügbar sind
- Wie viele programmierbare Funktionstasten ...
  - im optiClient 130 verfügbar sind.
  - in der ersten Spalte des erweiterten Tastenfeldes im optiClient 130 verfügbar sind.

Mögliche Optionen:

- **optiPoint 420 standard**
- **optiPoint 410 standard (DA Mode)**
- **optiPoint 410 standard**
- **optiPoint 420 advance**
- **optiSet E advance**
- **optiPoint 410 advance**
- **optiSet E comfort**
- **optiSet E advance China**

Keymodul-Typ:

Mögliche Optionen:

- **optiPoint Key Module**
- **optiPoint Self Labeling Keys Module**
- **optiSet E Key Module**

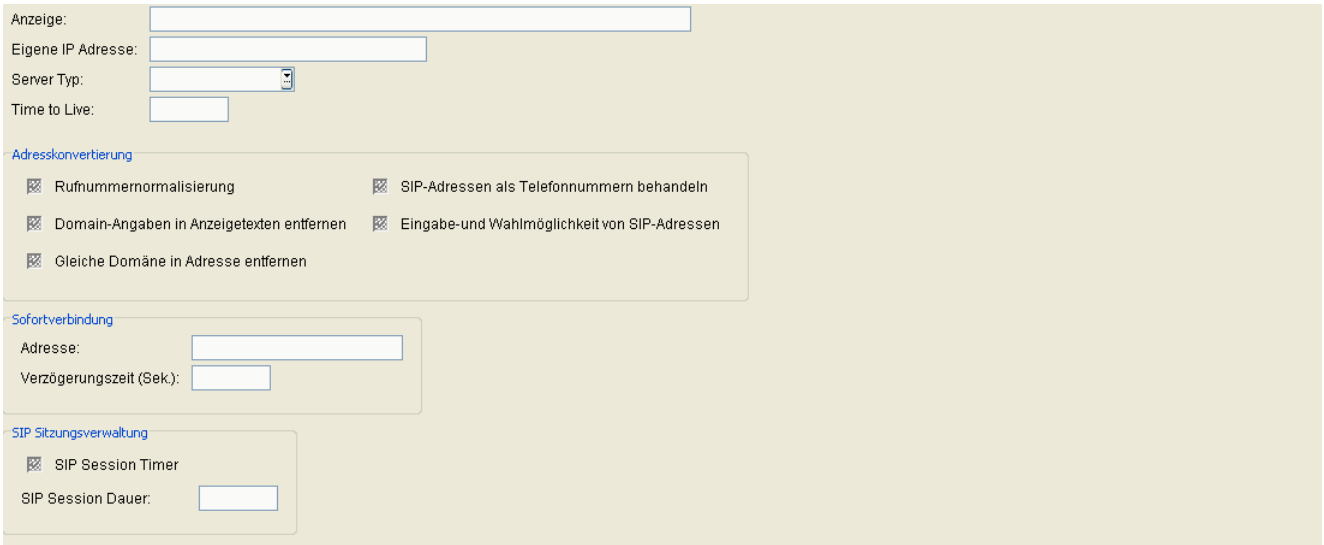
Keymodul-Maximalanzahl:

Gibt an, wieviele Keymodule dem IP Client zugeordnet werden.

Wertebereich: **0** ... **4**

7.2.2.5 Register „SIP Verbindung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „SIP Verbindung“



Terminal Name

Eigene IP Adresse

Hier kann die IP-Adresse des optiClient eingetragen werden. Wird das Feld frei gelassen, legt der optiClient seine IP-Adresse automatisch fest.

Server Typ

Mögliche Optionen:

- **Standard**
- **OpenScape Voice**
- **hiQ4200**

Time to Live

Angegeben ist die dreifache Zeit, nach der sich der Workpoint am Gatekeeper meldet, um die Gültigkeit der Registrierung aufrechtzuerhalten. Ist der Wert für Time to Live z. B. auf 3 Minuten eingestellt, so meldet sich der Workpoint jede Minute.

Wertebereich: **0** ... **4320** Minuten.

Adresskonvertierung

Rufnummernnormalisierung

Schalter zum Aktivieren der Rufnummernnormalisierung.

Domain-Angaben in Anzeigetexten entfernen

Schalter zum Unterdrücken des Domainnamens in den Anzeigetexten.

Gleiche Domäne in Adresse entfernen

Schalter zum Unterdrücken des Domainnamens in den Anzeigetexten, wenn der Gesprächspartner sich in derselben Domain befindet.

SIP-Adressen als Telefonnummern behandeln

Eingabe- und Wahlmöglichkeit von SIP-Adressen

Sofortverbindung

Adresse:

Die hier hinterlegte Adresse wird nach der definierten Verzögerungszeit bei Aktivierung der Leitung (z. B. beim Abheben des Hörers) angewählt.

Verzögerungszeit (sek)

Verzögerungszeit der Sofortwahl in Sekunden. Beträgt der Wert 0, wird die Sofortverbindung ohne Verzögerung aufgebaut.

SIP Sitzungsverwaltung

SIP Session Timer

Schalter zum Aktivieren des SIP Session Timers. Mit dem Timer wird die Dauer einer SIP-Session überwacht.

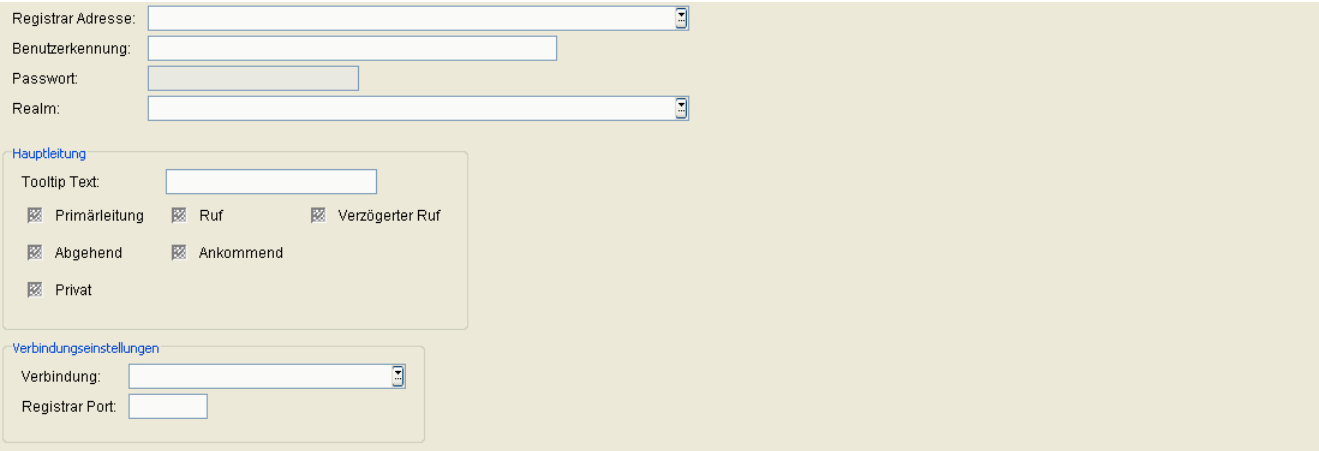
SIP Session Dauer:

Höchstdauer in Sekunden für eine SIP-Session.

Wertebereich: **0** ... **3600** Sekunden.

7.2.2.6 Register „SIP Registrar“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „SIP Registrar“



Registrar Adresse:

IP-Adresse oder Hostname des SIP-Registrars.

Diese Einstellung wirkt sich nur auf die SIP-Konfiguration des IP Clients aus.

Benutzerkennung:

Die Benutzerkennung ist der erste Teil der SIP URL.

Passwort:

Erforderliches Passwort für den Zugang zum SIP-Server.

Realm:

SIP-Bereich, in dem der Workpoint betrieben wird. SIP Realm wird verwendet, um das Telefon am SIP-Server zu identifizieren.

Hauptleitung

Tooltip Text:

Definiert den Anzeigetext für die Hauptleitung.

Primärleitung:

Schalter zum Kennzeichnen der Hauptleitung als Primärleitung.

Rufton

Schalter zum Aktivieren des Rufes.

Verzögerter Ruf

Schalter zum Aktivieren des verzögerten Rufes.

Abgehend

Ankommend

Privat

Verbindungseinstellungen

Verbindung

Mögliche Optionen:

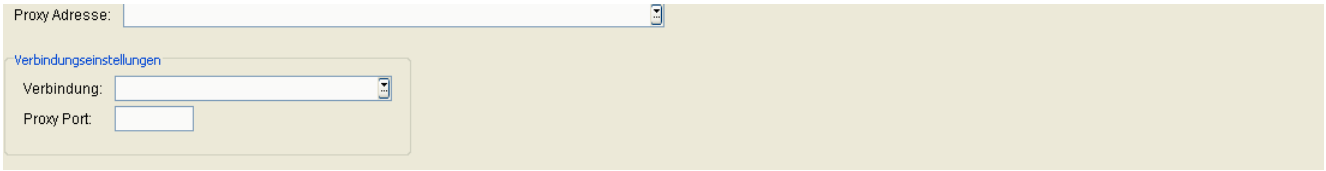
- **DNS SRV benutzen**
- **Standard Port benutzen**
- **Individuellen Port benutzen**

Registrar Port

Portnummer des Registrar-Servers.

7.2.2.7 Register „SIP Proxy“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „SIP Proxy“



Proxy Adresse

IP-Adresse oder Hostname des SIP-Proxy.

Diese Einstellung wirkt sich nur auf die SIP-Konfiguration des IP Clients aus.

Verbindungseinstellungen

Verbindung

Mögliche Optionen:

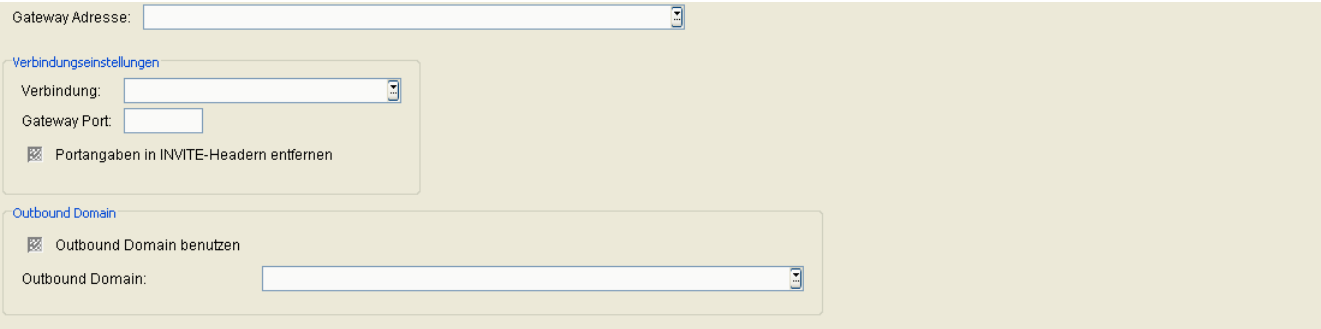
- **DNS SRV benutzen**
- **Standard Port benutzen**
- **Individuellen Port benutzen**

Proxy Port

Portnummer des Proxy-Servers.

7.2.2.8 Register „SIP Gateway“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „SIP Gateway“



Gateway Adresse:

IP-Adresse oder Hostname des Gateways.

Diese Einstellung wirkt sich nur auf die SIP-Konfiguration des IP Clients aus.

Verbindungseinstellungen

Verbindung:

Mögliche Optionen:

- **Standard Port benutzen**
- **Individuellen Port benutzen**

Gateway Port:

Port-Nummer des Gateways.

Portangaben in INVITE-Headern entfernen

Ist dieser Schalter aktiviert, werden die Portnummern aus den INVITE Headern entfernt.

Outbound Domain

Outbound Domain benutzen

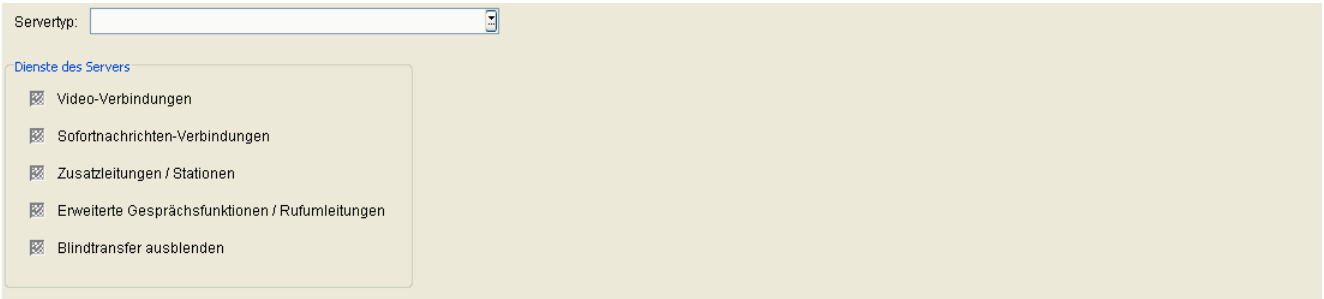
Schalter zum Aktivieren der Outbound Domäne.

Outbound Domain:

Name der Outbound Domäne.

7.2.2.9 Register „Systemdienste“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „Systemdienste“



Server Typ:

Mögliche Optionen:

- **OpenScape Voice/HQ4200 mit Sofortnachrichten**
- **OpenScape Voice/HQ4200 mit Zusatzleitungen/Stationen**
- **HiPath 3000/4000/5000, OpenOffice EE**
- **Standard ohne Video/Sofortnachrichten**
- **Individuell**
- **OpenScape Voice/hiQ4200**
- **OpenScape Voice/hiQ4200 ohne Video**
- **HiPath 3000 >= V8**
- **HiPath 4000 >= V6**

Dienste des Servers

Video-Verbindungen

Schalter zum Aktivieren von Video-Verbindungen.

Sofortnachrichten-Verbindungen

Schalter zum Aktivieren von Sofortnachrichten-Verbindungen.

Zusatzleitungen / Stationen

Schalter zum Aktivieren von Zusatzleitungen / Stationen.

Erweiterte Gesprächsfunktionen / Rufumleitungen

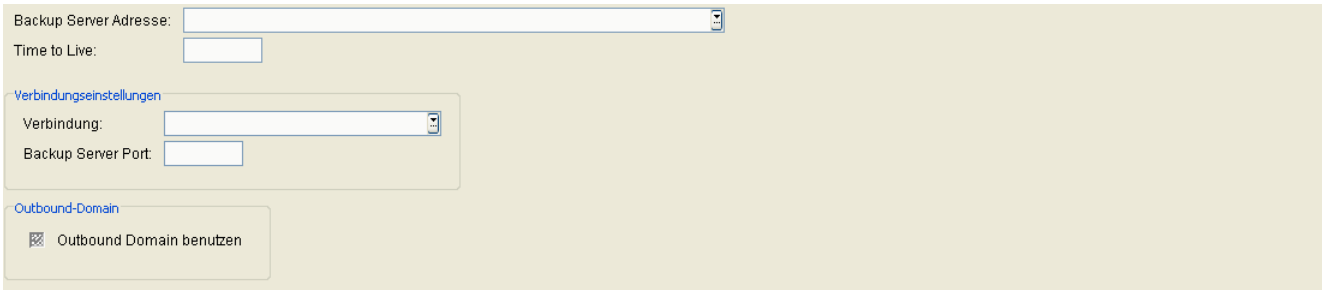
Schalter zum Aktivieren erweiterter Gesprächsfunktionen / Rufumleitungen.

Blindtransfer ausblenden

Ist der Schalter aktiviert, so wird der Blindtransfer ausgeblendet.

7.2.2.10 Register „SIP Survivability“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „SIP Survivability“



Backup Server Adresse:

IP-Adresse oder Hostname des Backup Servers.

Time to Live:

Angegeben ist die dreifache Zeit, nach der sich der Workpoint am Gatekeeper meldet, um die Gültigkeit der Registrierung aufrechtzuerhalten. Ist der Wert für Time to Live z. B. auf 3 Minuten eingestellt, so meldet sich der Workpoint jede Minute.

Wertebereich: 0 ... 4320 Minuten.

Verbindungseinstellungen

Verbindung:

Mögliche Optionen:

- **Standard Port benutzen**
- **Individuellen Port benutzen**

Backup Server Port:

Portnummer des Backup-Servers.

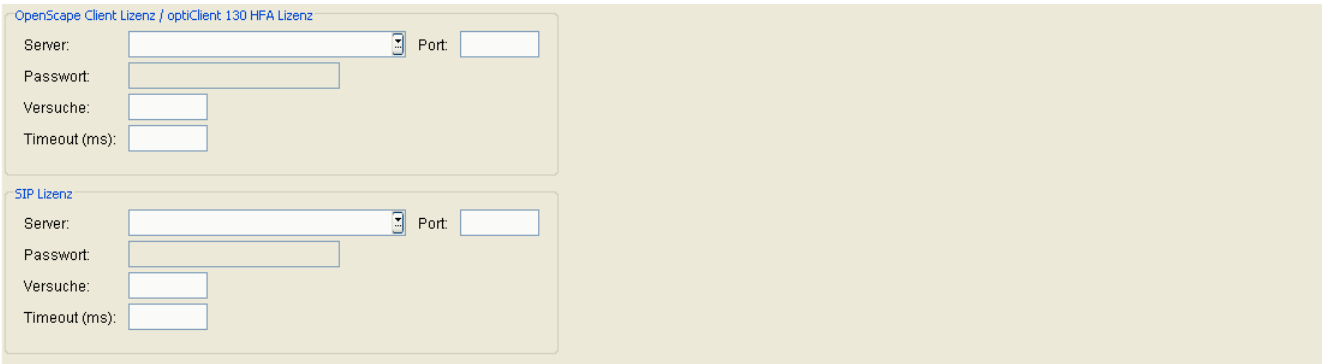
Outbound Domain

Outbound Domain benutzen

Schalter zum Aktivieren der Outbound Domain-Nutzung.

7.2.2.11 Register „Lizenzen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „Lizenzen“



OpenScape Client Lizenz / optiClient 130 HFA Lizenz

Server:

IP-Adresse oder Hostname des Lizenzservers

Port:

Port-Nummer für den Zugriff auf den Lizenzserver.

Standard: **61740**

Passwort:

Passwort für den Zugriff auf den Lizenzserver

Versuche:

Maximalanzahl der Verbindungsversuche

Timeout (ms):

Die maximale Zeit (in Millisekunden) für den Versuch eines Verbindungsaufbaus zum Lizenzserver.

SIP Lizenz

Server:

IP-Adresse oder Hostname des Lizenzservers

Port:

Port-Nummer für den Zugriff auf den Lizenzserver.

Standard: **61740**

Passwort:

Passwort für den Zugriff auf den Lizenzserver

Versuche:

Maximalanzahl der Verbindungsversuche

Timeout (ms):

Die maximale Zeit (in Millisekunden) für den Versuch eines Verbindungsaufbaus zum Lizenzserver.

7.2.2.12 Register „VPN Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Gateway / Server > Register „VPN Einstellungen“

VPN Modus:

Mögliche Optionen:

- **Kein**
  VPN (Virtual Private Network) wird nicht verwendet.
- **Automatisch**
  VPN wird mit einer automatisch ermittelten IP-Adresse verwendet.
- **Manuell**
  VPN wird mit der IP-Adresse verwendet, die bei **VPN IP** angegeben ist.

VPN IP:

IP-Adresse für das VPN (Virtual Private Network).

7.2.3 Ports

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Ports

Dieser Bereich besteht aus folgenden Inhalten:

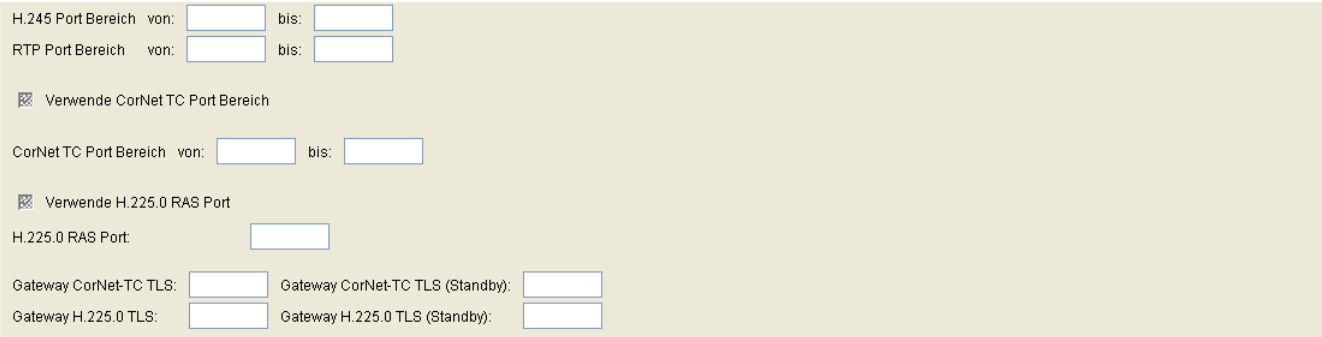
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Ports“
- Register „SIP Ports“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.3.1 Register „Ports“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Ports > Register „Ports“



H.245 Port Bereich von: ... bis:

Port-Bereich für H.245.

RTP Port Bereich von: ... bis:

Port-Bereich für RTP.

Verwende Cornet TC Port Bereich

Schalter zum Aktivieren für Cornet TC.

Cornet TC Port Bereich von: ... bis:

Port-Bereich für Cornet TC.

Verwende H.225.0 RAS Port

Schalter zum Aktivieren für Cornet TC.

H.225.0 RAS Port:

Für die Benutzung von NetMeeting parallel zum optiClient 130-Betrieb.

Gateway CorNet-TC TLS

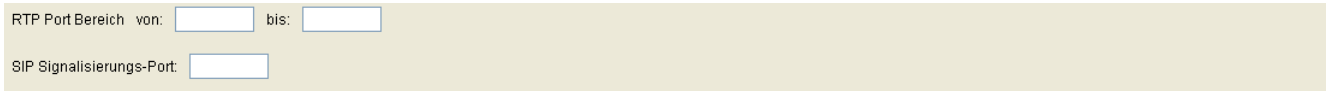
Gateway H.225.0 TLS

Gateway CorNet-TC TLS (Standby)

Gateway H.225.0 TLS (Standby)

7.2.3.2 Register „SIP Ports“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Ports > Register „SIP Ports“



RTP Port Bereich von: ... bis:

Port-Bereich für RTP.

Wirkt sich nur auf die SIP-Konfiguration des IP Clients aus.

SIP Signalisierungs-Port:

Wirkt sich nur auf die SIP-Konfiguration des IP Clients aus.

7.2.4 Quality of Service

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Quality of Service

Dieser Bereich besteht aus folgenden Inhalten:

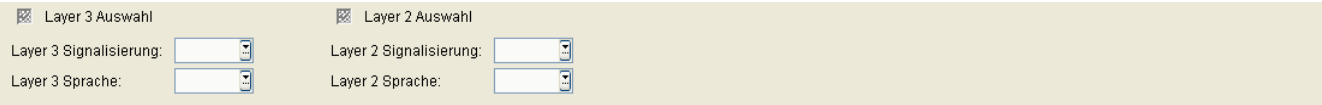
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einstellungen“
- Register „Alternative Einstellungen (SIP)“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.4.1 Register „Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Quality of Service > Register „Einstellungen“



Layer 3 Auswahl

Schalter zum Aktivieren von Layer 3 (Network Layer).

Layer 3 Signalisierung:

Prioriät für Layer 3 Signalisierung.

Nur festlegbar, wenn **Layer 3 Auswahl** aktiviert ist.

Mögliche Optionen:

- **Standard**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CST**

Layer 3 Sprache:

Priorität für Layer 3 Sprache.

Nur festlegbar, wenn **Layer 3 Auswahl** aktiviert ist.

Mögliche Optionen wie bei **Layer 3 Signalisierung**.

Layer 2 Auswahl

Schalter zum Aktivieren von Layer 2 (Data Link Layer).

Layer 2 Signalisierung:

Priorität für Layer 2 Signalisierung.

Nur festlegbar, wenn **Layer 2 Auswahl** aktiviert ist.

Wertebereich: 0 ... 7

Layer 2 Sprache:

Priorität für Layer 2 Sprache.

Nur festlegbar, wenn **Layer 2 Auswahl** aktiviert ist.

Mögliche Optionen wie bei **Layer 2 Signalisierung**.

7.2.4.2 Register „Alternative Einstellungen (SIP)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Quality of Service > Register „Alternative Einstellungen (SIP)“

Layer 2 Auswahl (SIP)

Schalter zum Aktivieren von Layer 2 (Data Link Layer).

Layer 2 Signalisierung:

Prioriät für Layer 2 Signalisierung.

Nur festlegbar, wenn **Layer 2 Auswahl** aktiviert ist.

Wertebereich: **0** ... **7**

Layer 2 Sprache:

Prioriät für Layer 2 Sprache.

Nur festlegbar, wenn Layer 2 Auswahl aktiviert ist.

Mögliche Optionen wie bei Layer 2 Signalisierung.

Layer 3 Auswahl (SIP)

Schalter zum Aktivieren von Layer 3 (Network Layer).

Layer 3 Signalisierung

Nur festlegbar, wenn **Layer 3 Auswahl (SIP)** aktiviert ist.

Mögliche Optionen:

- **Standard**
- **AF11**
- **AF12**
- **AF13**

- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CST**

Layer 3 Sprache:

Priorität für Layer 3 Sprache.

Nur festlegbar, wenn **Layer 3 Auswahl (SIP)** aktiviert ist.

Mögliche Optionen:

- **Standard**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**

- **EF**
- **CST**

7.2.5 Telefonie

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Telefonie

Dieser Bereich besteht aus folgenden Inhalten:

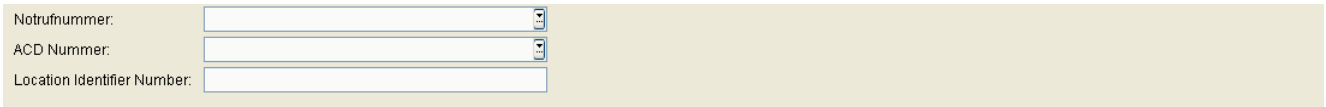
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Telefonie“
- Register „Telefonie (Standby)“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.5.1 Register „Telefonie“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Telefonie > Register „Telefonie“



Notrufnummer:

Enthält die Rufnummer, die in einem Notfall gewählt werden kann.

ACD Nummer:

ACD-Agentennummer, falls Sie als ACD-Agent arbeiten.

Location Identifier Number

Enthält eine Identifizierungsnummer zur eindeutigen Identifizierung eines Ortes. Damit kann z. B. bei einem Notruf festgestellt werden, **wo** der Notruf abgesetzt wurde.

Nur bei optiClient 130 V4.0 verfügbar.

7.2.5.2 Register „Telefonie (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Telefonie > Register „Telefonie (Standby)“

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „Telefonie“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.2.6, “Small Remote Site Redundancy”.

Notrufnummer:

Enthält die Rufnummer, die in einem Notfall gewählt werden kann.

ACD Nummer:

ACD-Agentennummer, falls Sie als ACD-Agent arbeiten.

7.2.6 Small Remote Site Redundancy

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Small Remote Site Redundancy

Dieser Bereich besteht aus folgenden Inhalten:

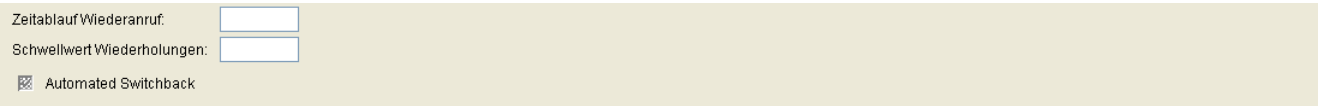
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SRSR Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.6.1 Register „SRSR Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Small Remote Site Redundancy > Register „SRSR Einstellungen“



Zeitablauf Wiederanruf:

Timeout für die Umschaltung auf das Hauptsystem.

Wertebereich: **1** ... **255** Sekunden.

Schwellwert Wiederholungen:

Gibt an, wieviele Versuche bei der Umschaltung auf das Standby-System durchgeführt werden sollen.

Wertebereich: **1** ... **255**

Automated Switchback

Schalter zum Aktivieren der automatischen Rückschaltung zum Hauptsystem.

7.2.7 Wahlparameter

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Wahlparameter

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „HFA Wahlparameter“
- Register „HFA Wahlparameter (Standby)“
- Register „SIP Wahlparameter“

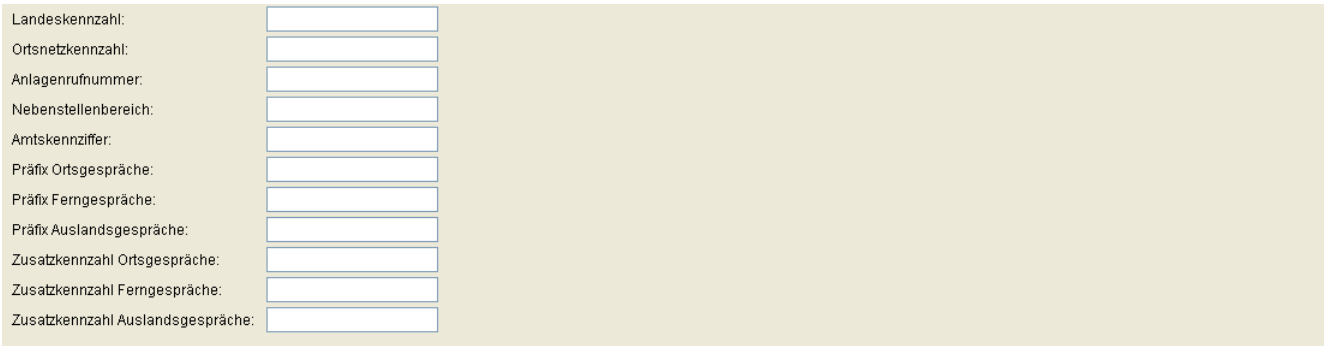
Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.7.1 Register „HFA Wahlparameter“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Wahlparameter > Register „HFA Wahlparameter“

Die Wahlparameter werden benötigt, um Rufnummern im kanonischen Format korrekt aufzulösen (siehe Kapitel 17, “Kanonisches Format”).



Landeskennzahl:

Format: Ohne führende Nullen, max. 4 Stellen.

Beispiel: **49** für Deutschland.

Ortsnetzkennzahl:

Format: Ohne führende Nullen, max. 21 Stellen.

Beispiel: **89** für München.

Anlagennummer:

Rufnummer der Nebenstelle (Anlagen-Nummer).

Format: max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Nebenstellenbereich:

Dieser Parameter definiert ein Muster, anhand dessen interne Nebenstellennummern erkannt werden können. Nebenstellennummern sind aus der Sicht des Workpoints intern, wenn sie derselben Anlage zugeordnet sind. Der Nebenstellenbereich kann als regulärer Ausdruck angegeben werden.

Beispiel: 1xxx, 2xxx, 3xxx, 4xxx , 5xxx seien Nebenstellen und 6xxx, 7xxx, 8xxx, 9xxx seien externe Rufnummern. Der reguläre Ausdruck ^[12345] legt fest, dass Rufnummern, die mit einer der Ziffern 1 bis 5 beginnen, zu den internen Nebenstellennummern gehören. Wenn also beispielsweise die Anlagenrufnummer 667 ist, so werden die Rufnummern von 6671xxx bis 6675xxx als interne Nebenstellen behandelt.

Amtskennziffer:

Nummer zur Amtsholung ein ausgehendes, externes Gespräch.

Format: max. 5 Stellen.

Beispiele: **0**, **74**, **9** (USA).

Präfix Ortsgespräche:

Format: max. 21 Stellen.

Beispiel: **01081**

Präfix Ferngespräche:

Nummer für ein ausgehendes Gespräch im Fernbereich.

Format: max. 21 Stellen.

Beispiel: **01081**

Präfix Auslandsgespräche:

Nummer für ein ausgehendes Gespräch im internationalen Bereich.

Format: max. 21 Stellen.

Beispiel: **01081**

Zusatzkennzahl Ortsgespräche:

Rufnummer z. B. Ihrer Firma.

Format: Ohne führende Nullen und ohne Nebenstellen-Nummer, max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Zusatzkennzahl Ferngespräche:

Nationale Vorwahlnummer.

Format: max. 5 Stellen.

Beispiel: **0** in Deutschland.

Zusatzkennzahl Auslandsgespräche:

Internationale Vorwahlnummer.

Format: max. 4 Stellen.

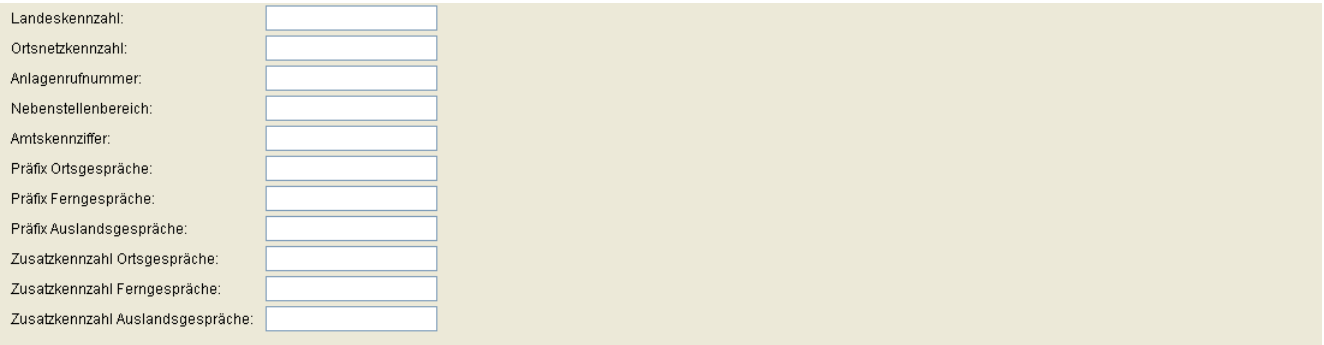
Beispiel: **00** in Deutschland.

7.2.7.2 Register „HFA Wahlparameter (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Wahlparameter > Register „HFA Wahlparameter (Standby)“

Die Wahlparameter werden benötigt, um Rufnummern im kanonischen Format korrekt aufzulösen (siehe Kapitel 17, “Kanonisches Format”).

HINWEIS: Diese „Standby“-Daten werden verwendet, wenn die „Home“-Daten bei Register „HFA Wahlparameter“ nicht verfügbar sind. Hierfür muss die SRSR-Funktionalität konfiguriert sein, siehe Abschnitt 7.2.6, “Small Remote Site Redundancy”.



Landeskennzahl:

Format: Ohne führende Nullen, max. 4 Stellen.

Beispiel: **49** für Deutschland.

Ortsnetzkennzahl:

Format: Ohne führende Nullen, max. 21 Stellen.

Beispiel: **89** für München.

Anlagennummer:

Rufnummer der Nebenstelle (Anlagen-Nummer).

Format: max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Nebenstellenbereich:

Dieser Parameter definiert ein Muster, anhand dessen interne Nebenstellennummern erkannt werden können. Nebenstellennummern sind aus der Sicht des Workpoints intern, wenn sie derselben Anlage zugeordnet sind. Der Nebenstellenbereich kann als regulärer Ausdruck angegeben werden.

Beispiel: 1xxx, 2xxx, 3xxx, 4xxx , 5xxx seien Nebenstellen und 6xxx, 7xxx, 8xxx, 9xxx seien externe Rufnummern. Der reguläre Ausdruck ^[12345] legt fest, dass Rufnummern, die mit einer der Ziffern 1 bis 5 beginnen, zu den internen Nebenstellennummern gehören. Wenn also beispielsweise die Anlagenrufnummer 667 ist, so werden die Rufnummern von 6671xxx bis 6675xxx als interne Nebenstellen behandelt.

Amtskennziffer:

Nummer zur Amtsholung ein ausgehendes, externes Gespräch.

Format: max. 5 Stellen.

Beispiele: **0**, **74**, **9** (USA).

Präfix Ortsgespräche:

Format: max. 21 Stellen.

Beispiel: **01081**

Präfix Ferngespräche:

Nummer für ein ausgehendes Gespräch im Fernbereich.

Format: max. 21 Stellen.

Beispiel: **01081**

Präfix Auslandsgespräche:

Nummer für ein ausgehendes Gespräch im internationalen Bereich.

Format: max. 21 Stellen.

Beispiel: **01081**

Zusatzkennzahl Ortsgespräche:

Rufnummer z. B. Ihrer Firma.

Format: Ohne führende Nullen und ohne Nebenstellen-Nummer, max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Zusatzkennzahl Ferngespräche:

Nationale Vorwahlnummer.

Format: max. 5 Stellen.

Beispiel: **0** in Deutschland.

Zusatzkennzahl Auslandsgespräche:

Internationale Vorwahlnummer.

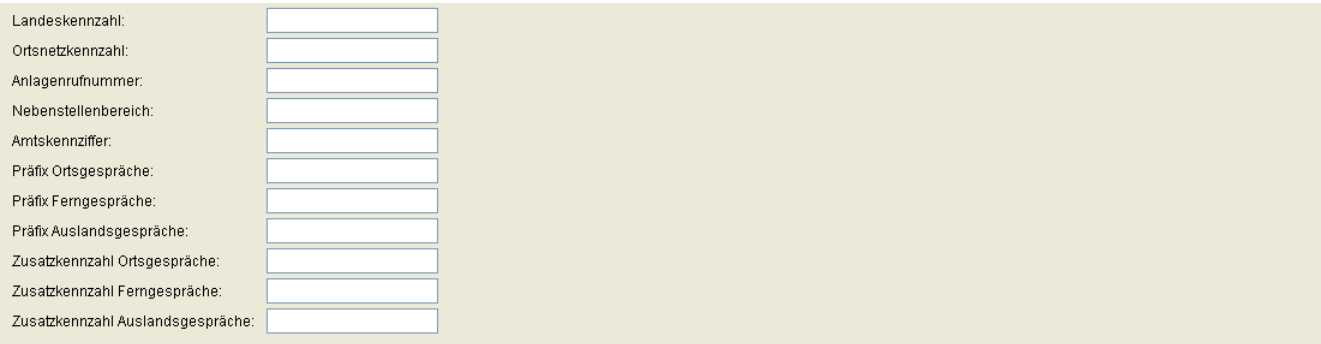
Format: max. 4 Stellen.

Beispiel: **00** in Deutschland.

7.2.7.3 Register „SIP Wahlparameter“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Wahlparameter > Register „SIP Wahlparameter“

Die Wahlparameter werden benötigt, um Rufnummern im kanonischen Format korrekt aufzulösen (siehe Kapitel 17, “Kanonisches Format”).



Landeskennzahl:

Format: Ohne führende Nullen, max. 4 Stellen.

Beispiel: **49** für Deutschland.

Ortsnetzkennzahl:

Format: Ohne führende Nullen, max. 21 Stellen.

Beispiel: **89** für München.

Anlagennummer:

Rufnummer der Nebenstelle (Anlagen-Nummer).

Format: max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Nebenstellenbereich:

Dieser Parameter definiert ein Muster, anhand dessen interne Nebenstellennummern erkannt werden können. Nebenstellennummern sind aus der Sicht des Workpoints intern, wenn sie derselben Anlage zugeordnet sind. Der Nebenstellenbereich kann als regulärer Ausdruck angegeben werden.

Beispiel: 1xxx, 2xxx, 3xxx, 4xxx , 5xxx seien Nebenstellen und 6xxx, 7xxx, 8xxx, 9xxx seien externe Rufnummern. Der reguläre Ausdruck ^[12345] legt fest, dass Rufnummern, die mit einer der Ziffern 1 bis 5 beginnen, zu den internen Nebenstellennummern gehören. Wenn also beispielsweise die Anlagenrufnummer 667 ist, so werden die Rufnummern von 6671xxx bis 6675xxx als interne Nebenstellen behandelt.

Amtskennziffer:

Nummer zur Amtsholung ein ausgehendes, externes Gespräch.

Format: max. 5 Stellen.

Beispiele: **0**, **74**, **9** (USA).

Präfix Ortsgespräche:

Format: max. 21 Stellen.

Beispiel: **01081**

Präfix Ferngespräche:

Nummer für ein ausgehendes Gespräch im Fernbereich.

Format: max. 21 Stellen.

Beispiel: **01081**

Präfix Auslandsgespräche:

Nummer für ein ausgehendes Gespräch im internationalen Bereich.

Format: max. 21 Stellen.

Beispiel: **01081**

Zusatzkennzahl Ortsgespräche:

Rufnummer z. B. Ihrer Firma.

Format: Ohne führende Nullen und ohne Nebenstellen-Nummer, max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Zusatzkennzahl Ferngespräche:

Nationale Vorwahlnummer.

Format: max. 5 Stellen.

Beispiel: **0** in Deutschland.

Zusatzkennzahl Auslandsgespräche:

Internationale Vorwahlnummer.

Format: max. 4 Stellen.

Beispiel: **00** in Deutschland.

7.2.8 Audio / Video Einstellungen

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

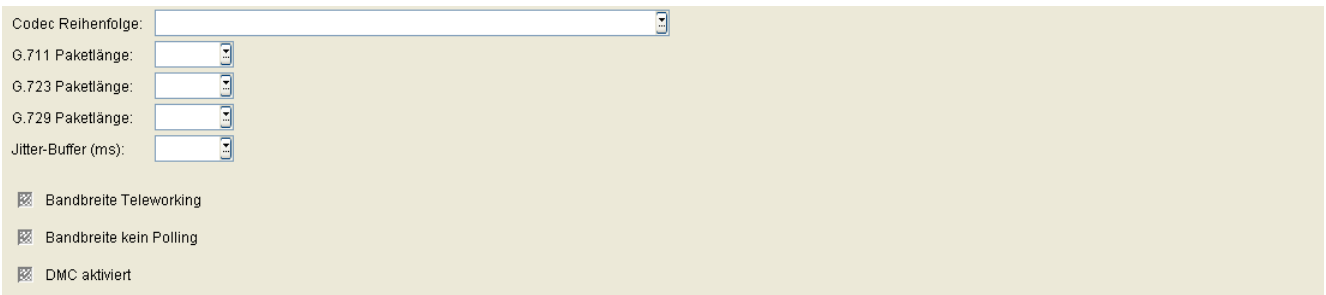
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „HFA Codec Einstellungen“
- Register „SIP Codec Einstellungen“
- Register „Audio Schemen“
- Register „Verfügbare Audiogeräte“
- Register „Video Einstellungen“
- Register „Verfügbare Videogeräte“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.8.1 Register „HFA Codec Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen > Register „HFA Codec Einstellungen“



Codec Reihenfolge:

Mögliche Optionen:

- **nicht komprimierende Codecs bevorzugt, ansonsten G.723 bevorzugt**
- **nicht komprimierende Codecs bevorzugt, ansonsten G.729 bevorzugt**
- **komprimierende Codecs bevorzugt, dabei G.723 bevorzugt**
- **komprimierende Codecs bevorzugt, dabei G.729 bevorzugt**
- **nur komprimierende Codecs, dabei G.723 bevorzugt**
- **nur komprimierende Codecs, dabei G.729 bevorzugt**

G.711 Paketlänge:

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

G.723 Paketlänge:

Mögliche Optionen:

- **30**
- **60**

G.729 Paketlänge:

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

Jitter-Buffer (ms):

Dauer der Zwischenspeicherung:

in Millisekunden.

Wertebereich: **20** ... **190** Millisekunden.

Bandbreite Teleworking

Schalter zum Aktivieren der Bandbreite bei Datenübertragung für Teleworker.

Bandbreite kein Polling

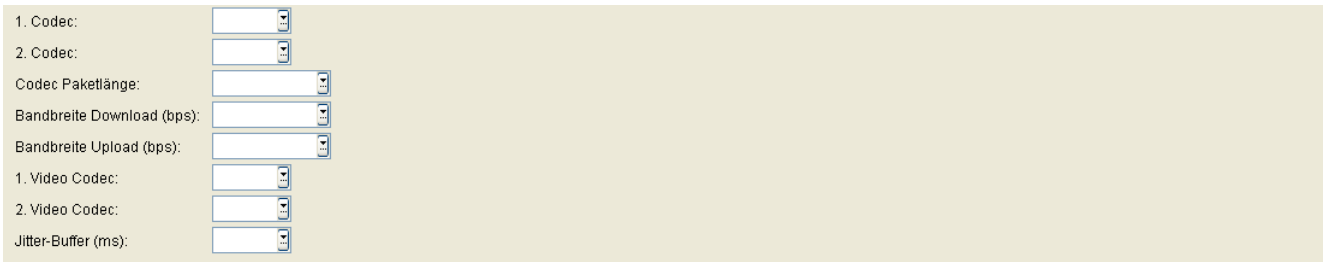
Schalter zum Aktivieren der Bandbreite bei kein Polling.

DMC aktiviert

Schalter zum Aktivieren der Bandbreite bei DMC.

7.2.8.2 Register „SIP Codec Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen > Register „SIP Codec Einstellungen“



1. Codec:

1. Komprimierungsverfahren.

Mögliche Optionen:

- **G.711**
- **G.722**
- **G.729**

2. Codec:

2. Komprimierungsverfahren.

Mögliche Optionen:

- **G.711**
- **G.722**
- **G.729**
- **Kein**

3. Codec:

3. Komprimierungsverfahren.

Mögliche Optionen:

- **G.711**
- **G.722**
- **G.729**

- **Kein**

Codec Paketlänge:

Mögliche Optionen:

- **Automatisch**
- **10**
- **20**

Bandbreite Download (bps)

Mögliche Optionen:

- **56**
- **64**
- **128**
- **256**
- **512**
- **1024**
- **2048**
- **3072**
- **6144**
- **10000**
- **12288**
- **24576**
- **100000**
- **1000000**

Bandbreite Upload (bps)

Mögliche Optionen:

- **56**
- **64**

- **128**
- **256**
- **512**
- **1024**
- **2048**
- **3072**
- **6144**
- **10000**
- **12288**
- **24576**
- **100000**
- **1000000**

1. Video Codec

Mögliche Optionen:

- **H.263**
- **H.264**

2. Video Codec

Mögliche Optionen:

- **H.263**
- **H.264**
- **Kein**

Jitter-Buffer (ms)

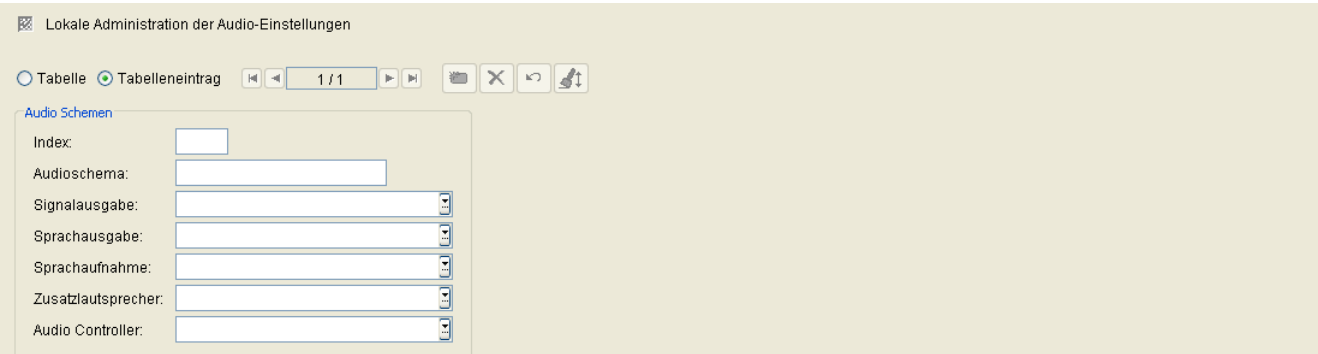
Mögliche Optionen:

- **20**
- **30**
- **40**

- **50**
- **60**
- **70**
- **80**
- **90**
- **100**
- **110**
- **120**
- **130**
- **140**
- **150**
- **160**
- **170**
- **180**
- **190**

7.2.8.3 Register „Audio Schemen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen > Register „Audio Schemen“



In diesem Register werden Hardware-Einstellungen wie z. B. für Sprachausgabe oder Klingeln zusammengefasst.

Lokale Administration der Audio-Einstellungen

Ist dieser Schalter aktiviert, können die Audio-Einstellungen nur am optiClient geändert werden, nicht aber durch den DLS. Die Felder unter **Audio Schemen** dienen dann nur zur Anzeige.

Ist dieser Schalter nicht aktiviert, können die Audio-Einstellungen nur durch den DLS geändert werden.

Index

Nummer der Einstellung.

Audioschema

Bezeichnung des Audioschemas.

Signalausgabe

Audio-Hardware für die Signalausgabe (Klingeln).

Sprachausgabe

Audio-Hardware für die Sprachausgabe.

Sprachaufnahme

Audio-Hardware für die Sprachaufnahme.

Zusatzlautsprecher

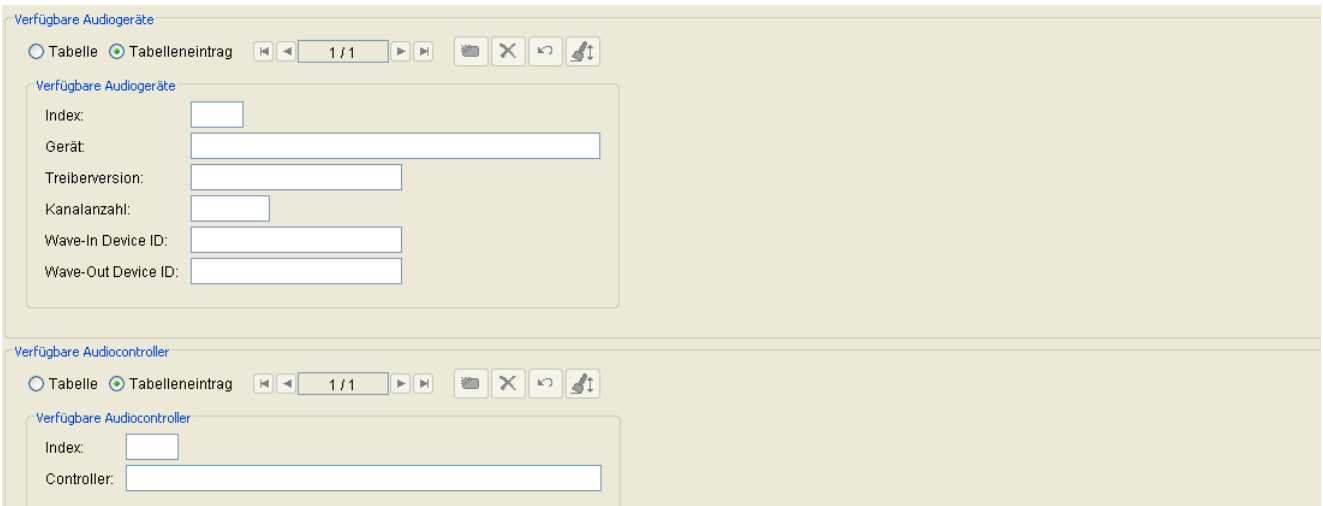
Audio-Hardware, die einen Zusatzlautsprecher repräsentiert. Wird hier ein Zusatzlautsprecher ausgewählt und dieses Audio-Schema ist aktiv, erscheint zur Steuerung des Zusatzlautsprechers ein eigenes Symbol in der Hauptleiste.

Audio Controller

Zusatzfunktion zur Steuerung besonderer Hardwarefunktionen.

7.2.8.4 Register „Verfügbare Audiogeräte“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen > Register „Verfügbare Audiogeräte“



Verfügbare Audiogeräte:

Index

Laufende Nummer des Audio-Endgeräts.

Gerät

Bezeichnung des Audio-Endgeräts für Anrufsignalisierung und Sprache.

Treiberversion

Version des Treibers für das Audio-Endgerät.

Kanalanzahl

Anzahl der verfügbaren Audiokanäle.

Wave-In Device ID

Wave-Out Device ID

Verfügbare Audiocontroller:

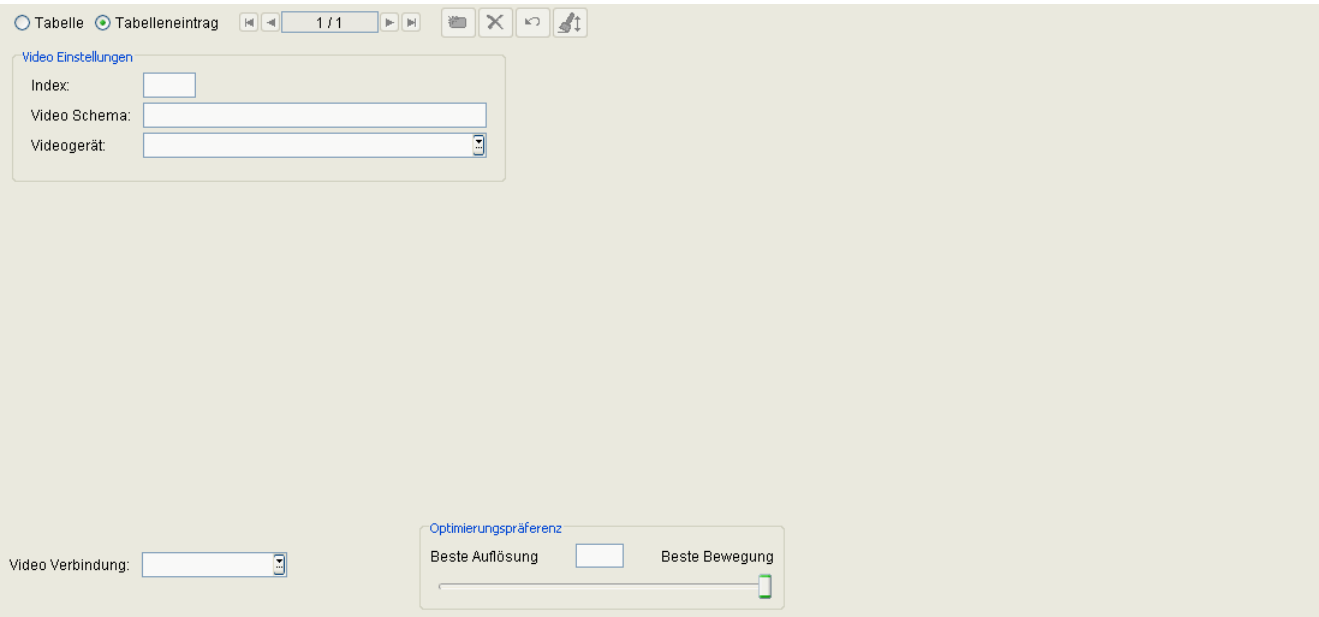
Index

Nummer der Einstellung

Controller

7.2.8.5 Register „Video Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen > Register „Video Einstellungen“



Index

Nummer der Einstellung.

Video Schema

Bezeichnung des Videoschemas.

Videogerät

Kamera zur Übermittlung des Bildes für die Videoverbindungen.

Video Verbindung

Sofern beide Verbindungspartner über eine betriebsbereite Video-Ausstattung verfügen, ermöglicht optiClient 130 die Zuschaltung ihrer jeweiligen Videobilder.

Mögliche Optionen:

- **Gesperrt**

- **Optional**

Optimierungspräferenz

Beste Auflösung

Optimierung auf bestmögliche Auflösung hin.

Beste Bewegung

Optimierung auf die bestmögliche Wiedergabe von Bewegungen hin.

7.2.8.6 Register „Verfügbare Videogeräte“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Audio / Video Einstellungen > Register „Verfügbare Videogeräte“

Index

Nummer der Einstellung.

Gerät

Die am Arbeitsplatz installierten Kameras werden aufgelistet. Wählen Sie die gewünschte aus. Sind hier keine Kameras aufgeführt, ist der PC nicht mit einer Videokamera ausgestattet.

7.2.9 Verzeichnisse / Adressbücher

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Verzeichnisse / Adressbücher

Dieser Bereich besteht aus folgenden Inhalten:

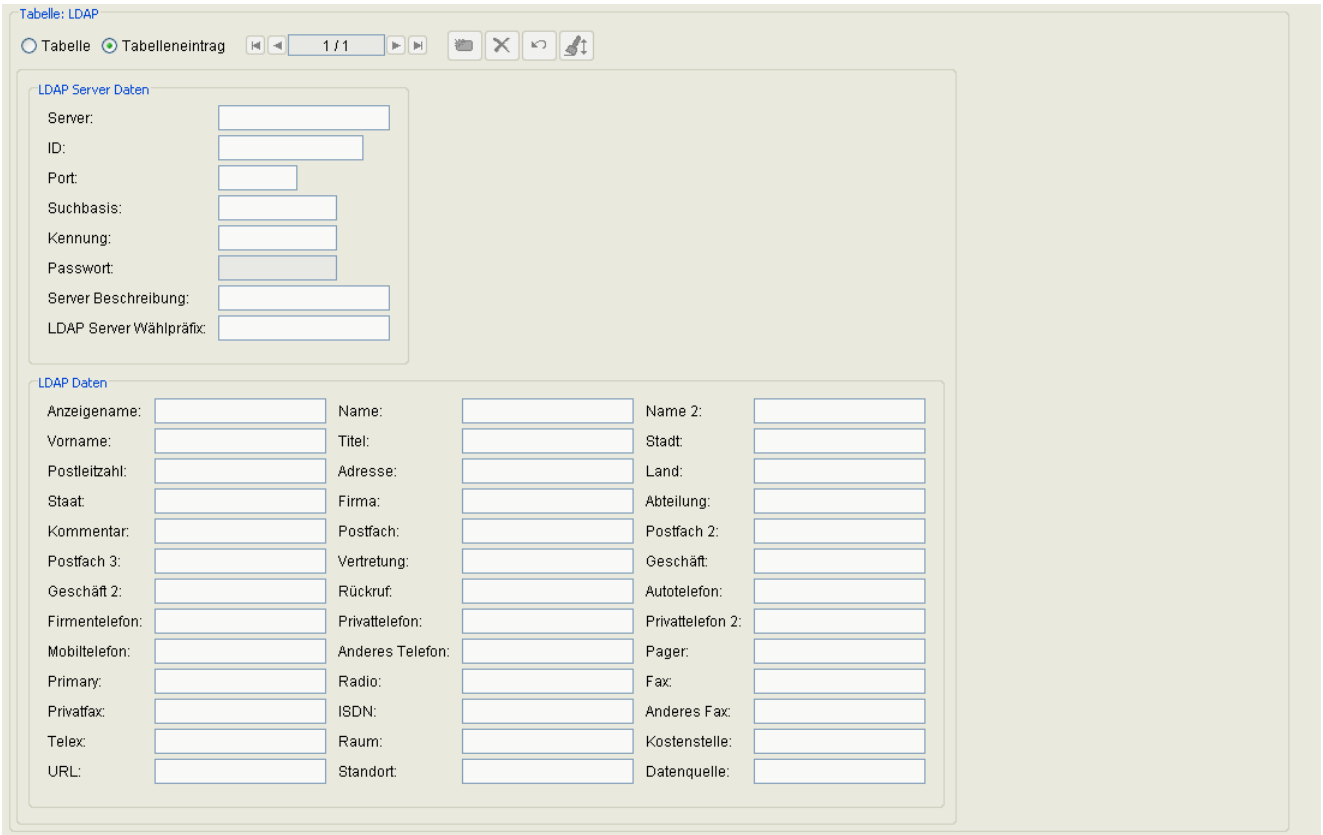
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „LDAP“
- Register „Directory Service“
- Register „Internetseiten“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.9.1 Register „LDAP“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Verzeichnisse / Adressbücher > Register „LDAP“



Sie können den Zugriff auf beliebige, im Netzwerk verfügbare LDAP-Verzeichnisse einrichten.

Server

IP-Adresse oder Hostname des LDAP-Servers.

ID

Name des LDAP-Servers.

Port

Portnummer des LDAP-Servers.

Kennung

Kennung des LDAP-Servers.

Passwort

Kennwort für den Zugriff auf den LDAP-Server.

Server Beschreibung

Beschreibender Text zum LDAP-Server.

Suchbasis

Bei der LDAP-Server Konfiguration können Sie hier eine bestimmte Basis festlegen,

ab der in diesem LDAP-Verzeichnis Einträge optiClient 130 gesucht / angezeigt werden sollen.

Die Eingabe kann wahlweise in zwei Formaten erfolgen:

`<Ebenenbez.3>=<Name>, <Ebenenbez.2>=<Name>, <Ebenenbez.1>=<Name>` oder

`<Ebenenbez.1>=<Name>/<Ebenenbez.2>=<Name>/<Ebenenbez.3>=<Name>`

Beispiel für ein LDAP-Verzeichnis mit folgenden Elementen:

- Bezeichnung Ebene 1: c (z. B. für „country“), Name z. B.: DE
- Bezeichnung Ebene 2: o (z. B. für „organisation“), Name z. B.: UNIFY
- Bezeichnung Ebene 3: ou (z. B. für „organisation unit“), Name z. B.: COM

Für die Festlegung dieser Basis als Suchbasis ist im Feld **Suchbasis** einzutragen:

`ou=COM, o=UNIFY, c=DE` oder alternativ `c=DE/o=UNIFY/ou=COM`.

Wird keine einschränkende Suchbasis festgelegt, ist das komplette LDAP-Verzeichnis die Suchbasis.

LDAP Server Wählpräfix

Sofern LDAP-Verzeichnisdienste im Netzwerk generell verfügbar sind und in den Benutzereinstellungen konfiguriert wurden, stehen diese unter dem konfigurierten Namen (z. B. „Unify Corporate Directory“) zur Verfügung. Sie können dabei die Verwendung und Nutzung mehrerer LDAP-Verzeichnisse konfigurieren.

Anzeigename

Aktivieren der Anzeige des Anzeigenamens und Eingabe eines Labels für den Anzeigenamen.

Name

Aktivieren der Anzeige des Namens und Eingabe eines Labels für den Namen.

Name2

Aktivieren der Anzeige des zweiten Namens und Eingabe eines Labels für den zweiten Namen.

Vorname

Aktivieren der Anzeige des Vornamens und Eingabe eines Labels für den Vornamen.

Titel

Aktivieren der Anzeige des Titels und Eingabe eines Labels für den Titel.

Stadt

Aktivieren der Anzeige der Stadt und Eingabe eines Labels für die Stadt.

Postleitzahl

Aktivieren der Anzeige der Postleitzahl und Eingabe eines Labels für die Postleitzahl.

Adresse

Aktivieren der Anzeige der Adresse und Eingabe eines Labels für die Adresse.

Land

Aktivieren der Anzeige des Landes und Eingabe eines Labels für das Land.

Staat

Aktivieren der Anzeige des Staats und Eingabe eines Labels für den Staat.

Firma

Aktivieren der Anzeige der Firma und Eingabe eines Labels für die Firma.

Abteilung

Aktivieren der Anzeige der Abteilung und Eingabe eines Labels für die Abteilung.

Kommentar

Aktivieren der Anzeige des Kommentars und Eingabe eines Labels für den Kommentar.

Postfach

Aktivieren der Anzeige des Postfachs und Eingabe eines Labels für das Postfach.

Postfach 2

Aktivieren der Anzeige des zweiten Postfachs und Eingabe eines Labels für des zweite Postfach.

Postfach 3

Aktivieren der Anzeige des dritten Postfachs und Eingabe eines Labels für das dritte Postfach.

Vertretung

Aktivieren der Anzeige der Vertretung und Eingabe eines Labels für die Vertretung.

Geschäft

Aktivieren der Anzeige des Geschäfts und Eingabe eines Labels für den Geschäftsbereich.

Geschäft 2

Aktivieren der Anzeige des Geschäfts und Eingabe eines Labels für den zweiten Geschäftsbereich.

Rückruf

Aktivieren der Anzeige der Rückrufnummer und Eingabe eines Labels für die Rückrufnummer.

Autotelefon

Aktivieren der Anzeige der Autotelefonnummer und Eingabe eines Labels für die Autotelefonnummer.

Firmentelefon

Aktivieren der Anzeige der Firmentelefonnummer und Eingabe eines Labels für die Firmentelefonnummer.

Privattelefon

Aktivieren der Anzeige der privaten Telefonnummer und Eingabe eines Labels für die private Telefonnummer.

Privattelefon 2

Aktivieren der Anzeige der zweiten privaten Telefonnummer und Eingabe eines Labels für die zweite private Telefonnummer.

Mobiltelefon

Aktivieren der Anzeige der mobilen Telefonnummer und Eingabe eines Labels für die mobile Telefonnummer.

Anderes Telefon

Aktivieren der Anzeige einer weiteren Telefonnummer und Eingabe eines Labels für die weitere Telefonnummer.

Pager

Aktivieren der Anzeige der Pager-Nummer und Eingabe eines Labels für die Pager-Nummer.

Primary

Radio

Fax

Aktivieren der Anzeige der Fax-Nummer und Eingabe eines Labels für die Fax-Nummer.

Privatfax

Aktivieren der Anzeige der privaten Fax-Nummer und Eingabe eines Labels für die private Fax-Nummer.

ISDN

Aktivieren der Anzeige der ISDN-Nummer und Eingabe eines Labels für die ISDN-Nummer.

Anderes Fax

Aktivieren der Anzeige einer weiteren Fax-Nummer und Eingabe eines Labels für die weitere Fax-Nummer.

Telex

Aktivieren der Anzeige der Telex-Nummer und Eingabe eines Labels für die Telex-Nummer.

Raum

Aktivieren der Anzeige der Raumnummer und Eingabe eines Labels für die Raumnummer.

Kostenstelle

Aktivieren der Anzeige der Kostenstelle und Eingabe eines Labels für die Kostenstelle.

URL

Aktivieren der Anzeige der URL und Eingabe eines Labels für die URL.

Standort

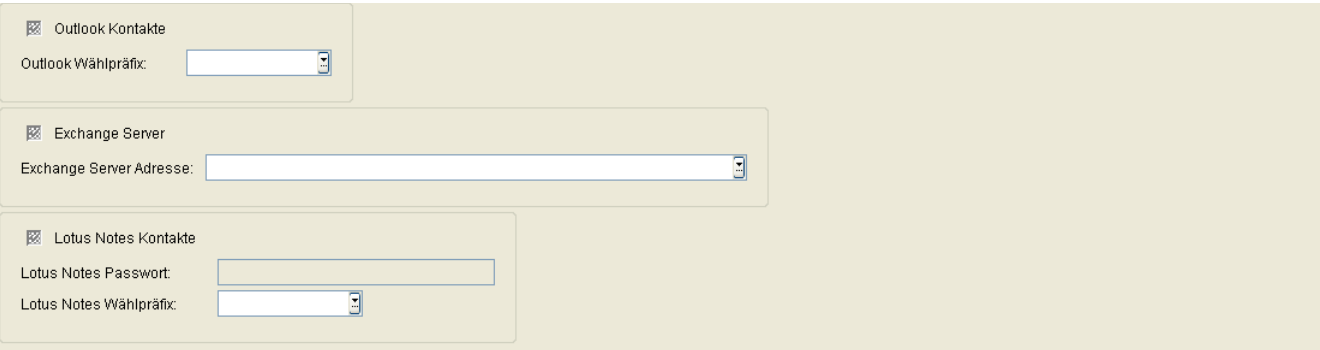
Aktivieren der Anzeige des Standorts und Eingabe eines Labels für den Standort.

Datenquelle

Aktivieren der Anzeige der Datenquelle und Eingabe eines Labels für die Datenquelle.

7.2.9.2 Register „Directory Service“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Verzeichnisse / Adressbücher > Register „Directory Service“



Für die Arbeit mit Verzeichnissen und Adressbüchern im optiClient 130 können Sie verschiedene Einstellungen für den Zugriff auf zentrale und lokale Verzeichnisse konfigurieren.

Outlook Kontakte

Dieses Verzeichnis enthält alle Einträge aus dem Kontakte-Ordner einer lokalen Microsoft Outlook-Installation. Ist Outlook nicht installiert oder ist dieses Verzeichnis für Ihren Benutzer nicht konfiguriert, so steht dieses Verzeichnis nicht zur Verfügung.

Der Schalter macht die Outlook-Kontaktinformationen als Verzeichnis im optiClient 130 verfügbar.

Outlook Wählpräfix:

Dieses Verzeichnis enthält alle Einträge aus dem Kontakte-Ordner einer lokalen Microsoft Outlook-Installation. Ist Outlook nicht installiert oder ist dieses Verzeichnis für Ihren Benutzer nicht konfiguriert, so steht dieses Verzeichnis nicht zur Verfügung.

Exchange Server

Dieses Verzeichnis enthält alle Einträge aus dem globalen Adressbuch des Microsoft Exchange Server (sofern installiert).

Der Schalter macht die Microsoft Exchange Server-Informationen als Verzeichnis im optiClient 130 verfügbar.

Exchange Server Adresse:

IP-Adresse oder Hostname des Microsoft Exchange Servers.

Lotus Notes Kontakte

Dieses Verzeichnis enthält alle Einträge aus dem Kontakte-Ordner Ihrer lokalen Lotus Notes-Installation (sofern installiert).

Der Schalter macht die Lotus Notes-Kontaktinformationen als Verzeichnis im optiClient 130 verfügbar.

Lotus Notes Passwort:

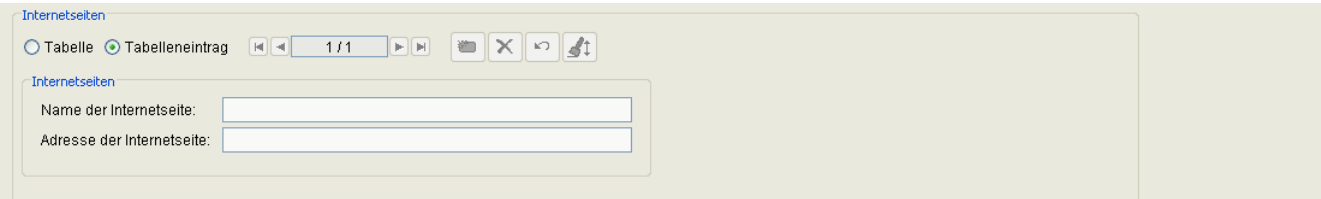
Passwort für den Zugriff auf Lotus Notes.

Lotus Notes Wählpräfix:

Dieses Verzeichnis enthält Kontakteinträge aus einer lokalen Lotus Notes-Installation. Ist Lotus Notes nicht installiert oder ist dieses Verzeichnis für den Benutzer nicht konfiguriert, so steht dieses Verzeichnis nicht zur Verfügung.

7.2.9.3 Register „Internetseiten“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Verzeichnisse / Adressbücher > Register „Internetseiten“



Name der Internetseite:

Beliebig zu vergebender Name für die Internetseite.

Adresse der Internetseite:

URL der Internetseite.

7.2.10 Sonstiges

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Sonstiges

Dieser Bereich besteht aus folgenden Inhalten:

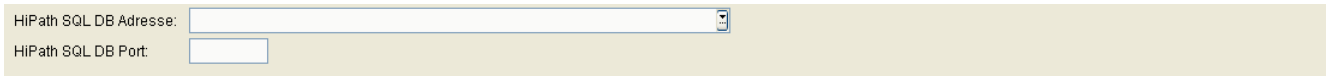
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „HiPath SQL DB“
- Register „Systemfunktionen“
- Register „SIP Leistungsmerkmale“
- Register „SIP Leistungsmerkmale 2“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.10.1 Register „HiPath SQL DB“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Sonstiges > Register „HiPath SQL DB“



HiPath SQL DB Adresse:

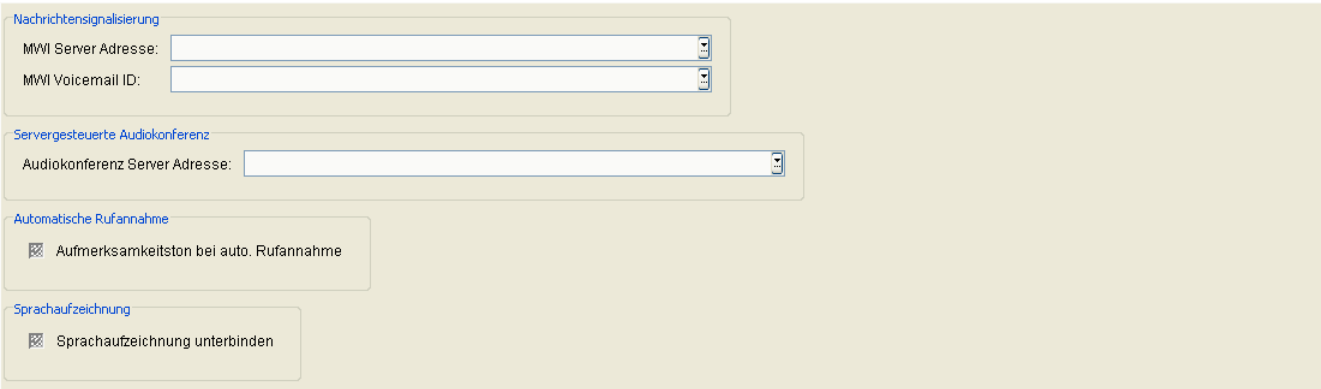
IP-Adresse oder Hostname der HiPath SQL DB.

HiPath SQL DB Port:

Portnummer der HiPath SQL DB.

7.2.10.2 Register „Systemfunktionen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Sonstiges > Register „Systemfunktionen“



Nachrichtensignalisierung

MWI Server Adresse:

IP-Adresse oder Hostname des MWI Servers.

MWI Voicemail ID:

Identifikationsnummer für den Zugriff auf den MWI-Server.

Servergesteuerte Audiokonferenz

Audiokonferenz Server Adresse:

IP-Adresse oder Hostname des Audiokonferenz-Servers.

Automatische Rufannahme

Piepton bei auto. Rufannahme

Aufmerksamkeitston bei automatischer Rufannahme einschalten.

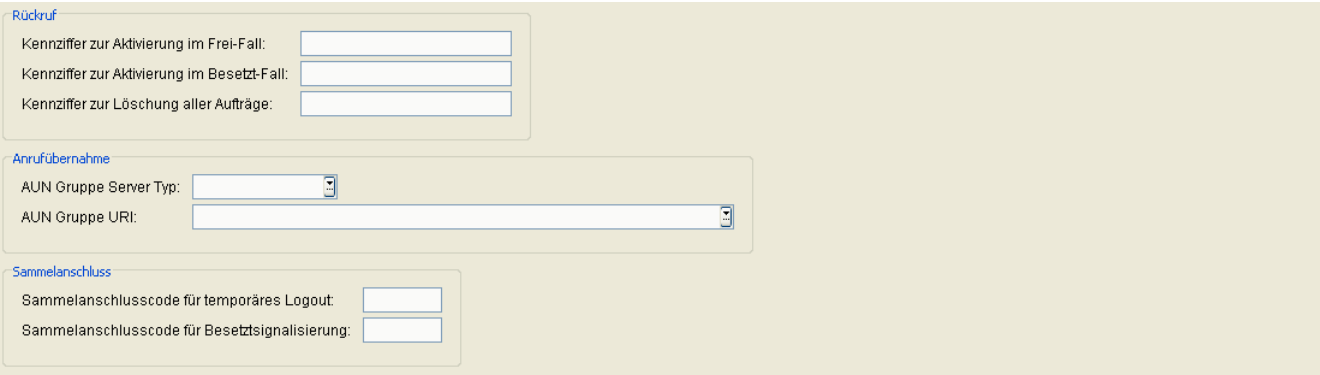
Sprachaufzeichnung

Sprachaufzeichnung unterbinden

Dieser Schalter schaltet die Sprachaufzeichnung ein oder aus.

7.2.10.3 Register „SIP Leistungsmerkmale“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Sonstiges > Register „SIP Leistungsmerkmale“



Rückruf

Kennziffer zur Aktivierung im Frei-Fall:

Kennziffer, die auf dem Server das Leistungsmerkmal „Rückruf nach nicht Melden“ steuert.

Kennziffer zur Aktivierung im Besetzt-Fall:

Kennziffer, die auf dem Server das Leistungsmerkmal „Rückruf nach Besetzt“ steuert.

Kennziffer zur Löschung aller Aufträge:

Kennziffer, die auf dem Server alle Rückrufaufträge löscht.

Anrufübernahme

AUN Gruppe Server Typ:

Mögliche Optionen:

- **Andere**
- **OpenScape Voice**
- **Broadsoft**
- **Sylantro**
- **HiQ8000**
- **Genesys**

AUN Gruppe URI:

IP-Adresse oder Hostname des Servers zur Bereitstellung des Leistungsmerkmals Anrufübernahme.

Sammelanschluss

Sammelanschlusscode für temporäres Logout

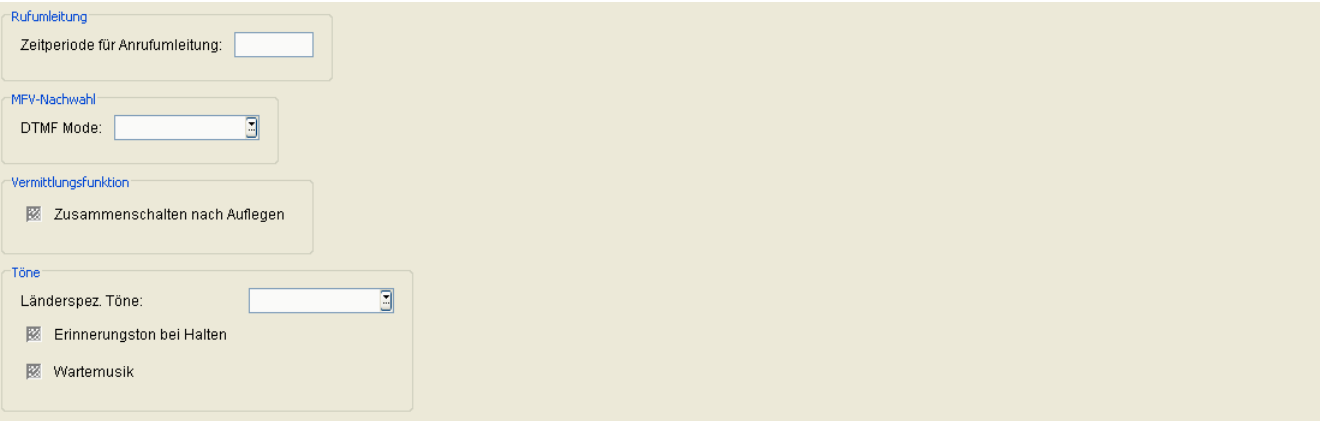
Funktionscode für das Merkmal „temporäres Logout aus der Sammelanschlussgruppe“.

Sammelanschlusscode für Besetztsignalisierung

Funktionscode für das Merkmal „Besetztsignalisierung innerhalb der Sammelanschlussgruppe“.

7.2.10.4 Register „SIP Leistungsmerkmale 2“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Sonstiges > Register „SIP Leistungsmerkmale 2“



Rufumleitung

Zeitperiode für Anrufumleitung:

Geben Sie die Zeit ein, nach der nicht angenommene Anrufe bei aktivierter Anrufumleitung weitergeleitet werden.

MFV-Nachwahl

DTMF Mode:

Mögliche Optionen:

- **Automatisch**
- **Inband**

Vermittlungsfunktion

Zusammenschalten nach Auflegen:

Aktivieren Sie den Schalter, wenn Sie zwei aktive Verbindungen haben (z. B. bei Rückfrage) und dann „auflegen“. Bei aktiver Option werden die beiden Verbindungspartner dann zusammengeschaltet, bei ausgeschalteter Option sind dann beide Verbindungen beendet.

Töne

Länderspez. Töne:

Mögliche Optionen:

- **Brasilien**
- **China**
- **Deutschland**
- **Frankreich**
- **Großbritannien**
- **International**
- **Italien**
- **Niederlande**
- **Portugal**
- **Spanien**
- **USA**

Erinnerungston bei Halten:

Aktivieren Sie den Schalter, wenn Sie einen Erinnerungston hören möchten, der Ihnen ein gehaltenes Gespräch signalisiert.

Wartemusik:

Aktivieren Sie den Schalter, wenn in bestimmten Situationen (z. B. Weiterleitung, Halten, Rückfrage) eine Wartemusik hörbar sein soll.

7.2.11 Keysets / Tastenbelegung

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „HFA Tastenbelegung“
- Register „HFA Tastenbelegung (Standby)“
- Register „SIP Keysets“
- Register „SIP Leitungstasten“
- Register „SIP Stationen (DSS)“
- Register „SIP Anrufumleitung“
- Register „SIP Keypad“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.11.1 Register „HFA Tastenbelegung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „HFA Tastenbelegung“

Index

Name der Funktion der Tastenbelegung.

Gerät

Geräteauswahl der belegten Taste.

Mögliche Optionen:

- **1. Beistellgerät**
- **2. Beistellgerät**
- **3. Beistellgerät**
- **4. Beistellgerät**
- **Basisgerät**

Ebene

Ebenennummer der belegten Taste.

Tastennummer

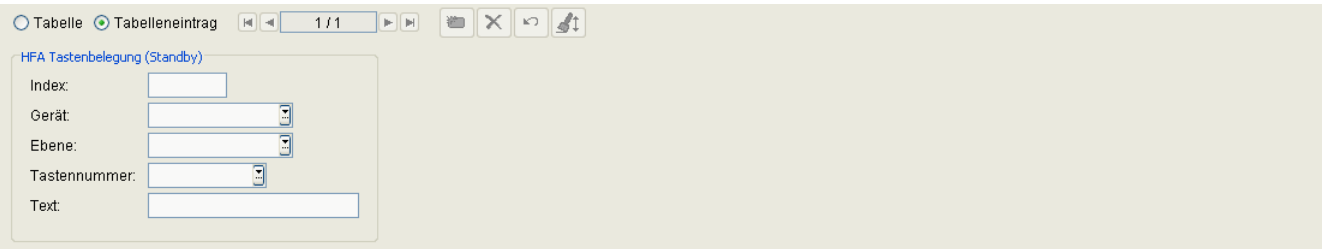
Tastennummer der belegten Taste.

Text

Dargestellter Text der belegten Taste.

7.2.11.2 Register „HFA Tastenbelegung (Standby)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „HFA Tastenbelegung (Standby)“



Index

Name der Funktion der Tastenbelegung.

Gerät

Geräteauswahl der belegten Taste.

Mögliche Optionen:

- **1. Beistellgerät**
- **2. Beistellgerät**
- **3. Beistellgerät**
- **4. Beistellgerät**
- **Basisgerät**

Ebene

Ebenennummer der belegten Taste.

Tastennummer

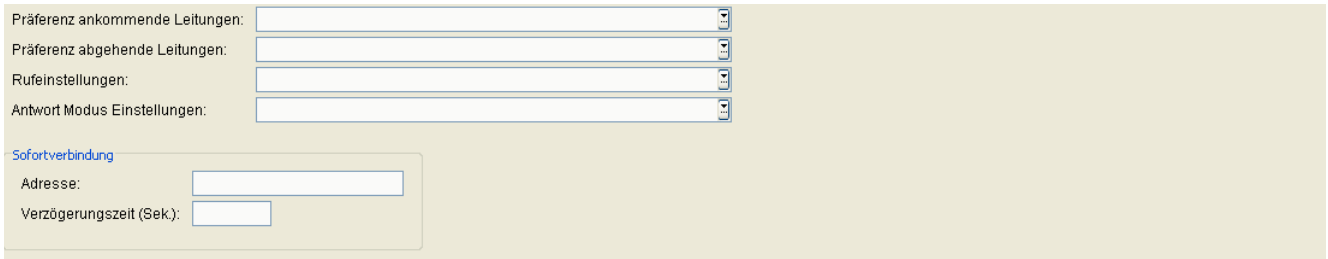
Tastennummer der belegten Taste.

Text

Dargestellter Text der belegten Taste.

7.2.11.3 Register „SIP Keysets“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „SIP Keysets“



Präferenz ankommende Leitungen:

Mögliche Optionen:

- **Ruhende Leitung bevorzugt**
- **Rufende Leitung bevorzugt**

Präferenz abgehende Leitungen:

Mögliche Optionen:

- **Ruhende Leitung bevorzugt**
- **Primärleitung bevorzugt**

Rufeinstellungen:

Art der der Signalisierung für den Fall, dass während eines Gesprächs ein Anruf auf einer anderen Leitung ankommt.

Mögliche Optionen:

- **Kein Aufmerksamkeitston**
- **Normaler Aufmerksamkeitston**
- **Spezieller Aufmerksamkeitston**

Antwort Modus Einstellungen:

Legt fest, was mit einer Leitung (Gespräch) geschehen soll, wenn eine Verbindung über eine andere Leitung hergestellt wird.

Mögliche Optionen:

- **Aktives Gepräch wird auf Halten gelegt**
- **Aktives Gepräch wird beendet (getrennt)**

Sofortverbindung

Adresse

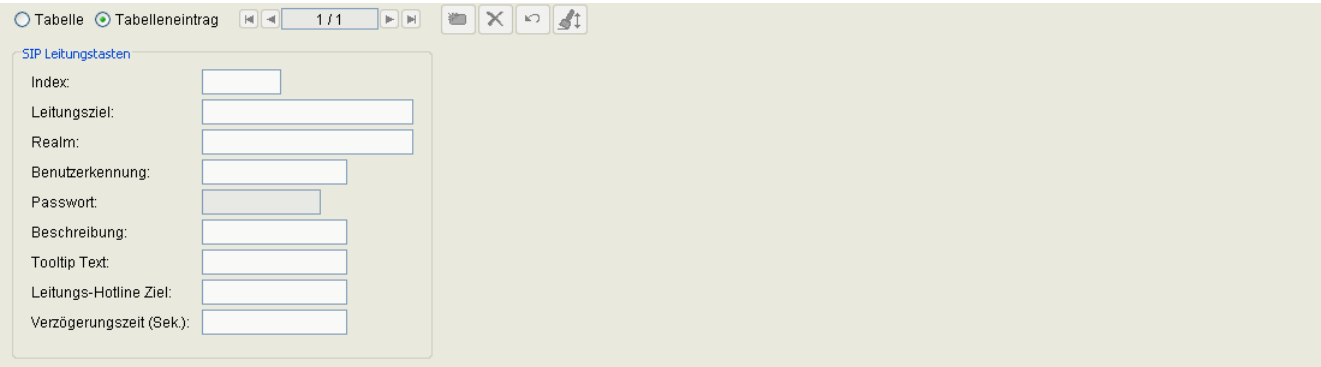
Adresse bzw. Rufnummer, die nach Aktivierung der Leitung (z. B. beim Abheben des Hörers) und Ablauf der eingestellten Verzögerungszeit angewählt wird.

Verzögerungszeit (sek)

Verzögerungszeit der Wahl in Sekunden. Bei Verzögerungszeit = 0 wird diese Sofortverbindung ohne Verzögerung aufgebaut.

7.2.11.4 Register „SIP Leitungstasten“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „SIP Leitungstasten“



Index:

Nummer der Leitungstaste

Leitungsziel:

Rufnummer der zur Leitungstaste gehörigen Leitung.

Realm:

SIP-Realm, der dem Leitungsziel zugeordnet ist.

Benutzerkennung:

SIP-Benutzername, der dem Leitungsziel zugeordnet ist.

Passwort:

Zum SIP-Benutzernamen gehöriges Passwort.

Beschreibung:

Beschreibung der Leitung.

Tooltip Text:

Text, der im Tooltip zur Leitung erscheint.

Leitungs-Hotline Ziel

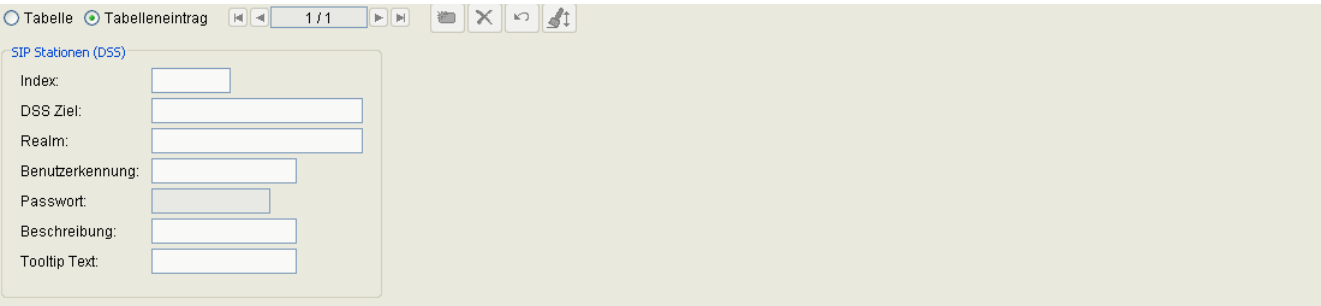
Rufnummer, die angerufen wird, wenn die Leitung als Hotline konfiguriert ist.

Verzögerungszeit (sek):

Zeitintervall, das zwischen dem Aktivieren der Leitung (z. B. Abheben des Hörers) und dem Wählen der Hotline-Rufnummer liegt.

7.2.11.5 Register „SIP Stationen (DSS)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „SIP Stationen (DSS)“



Index

Indexnummer der Tastenfunktion.

DSS Ziel

Rufnummer der DSS (Direct Station Select)-Leitung.

Realm

SIP-Realm der DSS-Leitung.

Benutzerkennung

SIP-Benutzername für die Address of Record der DSS-Leitung.

Passwort

Zum SIP-Benutzernamen gehöriges Passwort.

Beschreibung

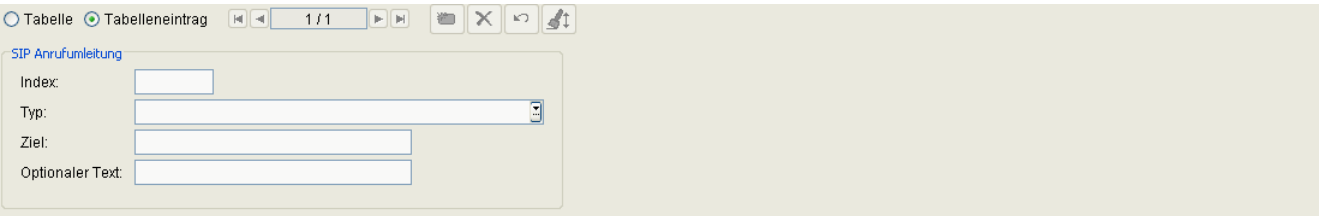
Beschreibung der DSS-Leitung.

Tooltip Text

Eingabe des Texts, der im Tooltip zur DSS-Leitungstaste erscheint.

7.2.11.6 Register „SIP Anrufumleitung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „SIP Anrufumleitung“



Index

Indexnummer der Taste für die Anrufumleitung.

Typ

Auswahl der Bedingungen, bei denen eine Anrufumleitung erfolgen soll.

- **Alle Anrufe**
- **Externe Anrufe (HiPath 3000)**
- **Interne Anrufe (HiPath 3000)**
- **Bei Besetzt (SIP HiPath 4000)**
- **Bei nicht erreichbar (SIP, HiPath 4000)**
- **Bei besetzt/nicht erreichbar (HiPath 4000)**
- **Bei nicht angemeldet (HiPath 3000, HiPath 4000)**

Ziel

Ziel der SIP Anrufumleitung.

Optionaler Text

Beschreibung der hier eingestellten SIP-Anrufumleitung.

7.2.11.7 Register „SIP Keypad“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Keysets / Tastenbelegung > Register „SIP Keypad“

Index

Indexnummer der Tastenfunktion.

Typ

Typ des SIP-Keypads.

ID

ID des SIP-Keypads.

Wert

Wert der Taste.

Benutzertext

Beschreibender Text zum SIP-Keypad.

7.2.12 Signaling and Payload Encryption (SPE)

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Signaling and Payload Encryption (SPE)

Dieser Bereich besteht aus folgenden Inhalten:

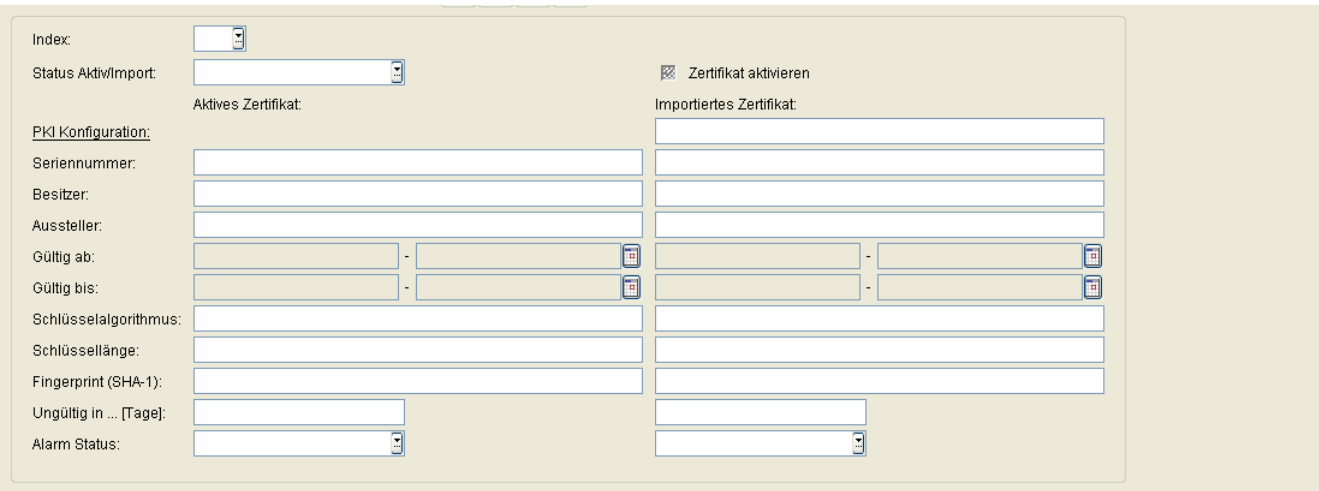
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SPE CA Zertifikate“
- Register „SIP Einstellungen“
- Register „HFA Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.2.12.1 Register „SPE CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Signaling and Payload Encryption (SPE) > Register „SPE CA Zertifikate“



Die nachfolgend beschriebenen Parameter stehen einmal für das derzeit aktive und einmal für das importierte Zertifikat zur Verfügung.

Index

Index zur Identifizierung des Peer Credentials.

Status Aktiv/Import:

Gibt an, ob ein Zertifikat importiert und/oder aktiv auf dem Phone registriert ist. Daraus ergeben sich die nachfolgend genannten 5 Zustände.

Mögliche Werte:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

PKI Konfiguration

Name der PKI Konfiguration.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Anzahl der verbleibenden Tage, bis das Zertifikat ungültig wird.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Anzeige der Gültigkeitsdauer von Zertifikaten, um in Kürze ablaufende Zertifikate zu suchen.

Mögliche Werte:

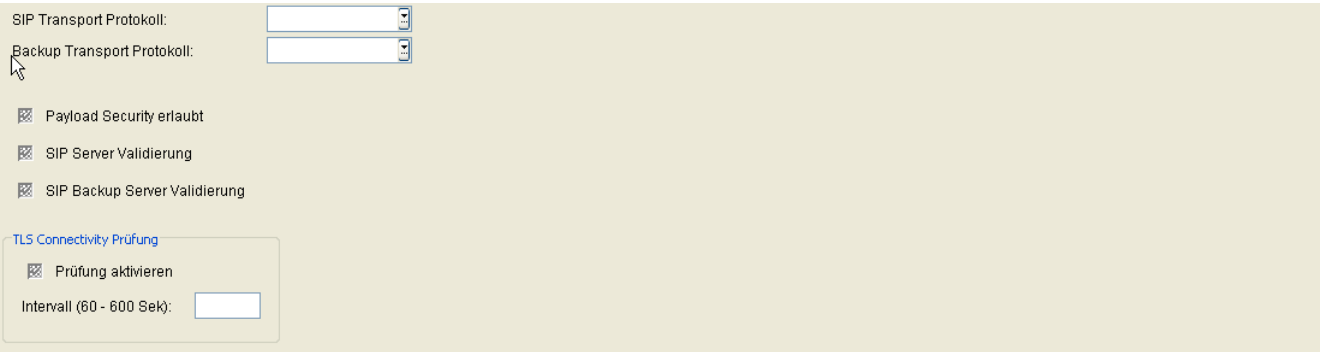
- **gültig**
- **in Kürze ungültig**
- **ungültig**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht. Das aktive Zertifikat wird für die Verschlüsselung von Gesprächen verwendet.

7.2.12.2 Register „SIP Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Signaling and Payload Encryption (SPE) > Register „SIP Einstellungen“



SIP Transport Protokoll:

Transportprotokoll, das für die SIP-Signalisierung verwendet wird.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

Backup Transport Protokoll:

Transportprotokoll, das für die SIP-Signalisierung verwendet wird, wenn der Backup-SIP-Server zum Einsatz kommt.

Mögliche Optionen:

- **UDP**
- **TCP**

Payload Security erlaubt

Ist der Schalter aktiviert, so ist die Verschlüsselung von Sprachnachrichten erlaubt.

SIP Server Validierung

Ist der Schalter aktiviert, so wird die Verbindung zum SIP-Server überprüft.

SIP Backup Server Validierung

Ist der Schalter aktiviert, so wird die Verbindung zum Backup-SIP-Server überprüft.

TLS Connectivity Prüfung

Prüfung aktivieren

Ist der Schalter aktiviert, wird die TLS Connectivity-Prüfung eingeschaltet.

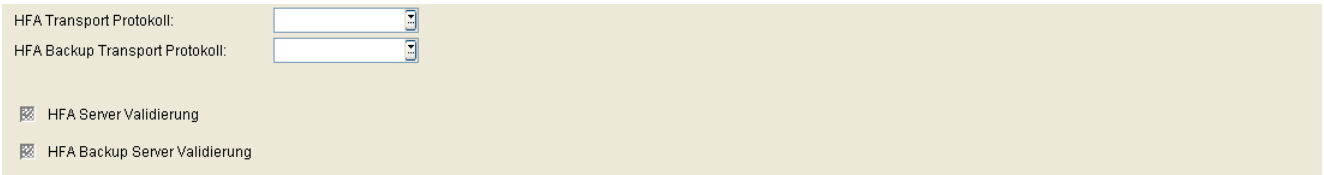
Intervall

Intervall in Sekunden, in dem die periodische TLS Connectivity-Prüfung durchgeführt wird.

Mögliche Werte: **60** - **600**

7.2.12.3 Register „HFA Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Signaling and Payload Encryption (SPE) > Register „HFA Einstellungen“



HFA Transport Protokoll:

Transportprotokoll, das für die HFA-Signalisierung verwendet wird.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

HFA Backup Transport Protokoll:

Transportprotokoll, das für die HFA-Signalisierung verwendet wird, wenn der Backup-HFA-Server zum Einsatz kommt.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

HFA Server Validierung

Ist der Schalter aktiviert, so wird die Verbindung zum HFA-Server überprüft.

HFA Backup Server Validierung

Ist der Schalter aktiviert, so wird die Verbindung zum HFA-Backupserver überprüft.

7.2.13 Einwahlort

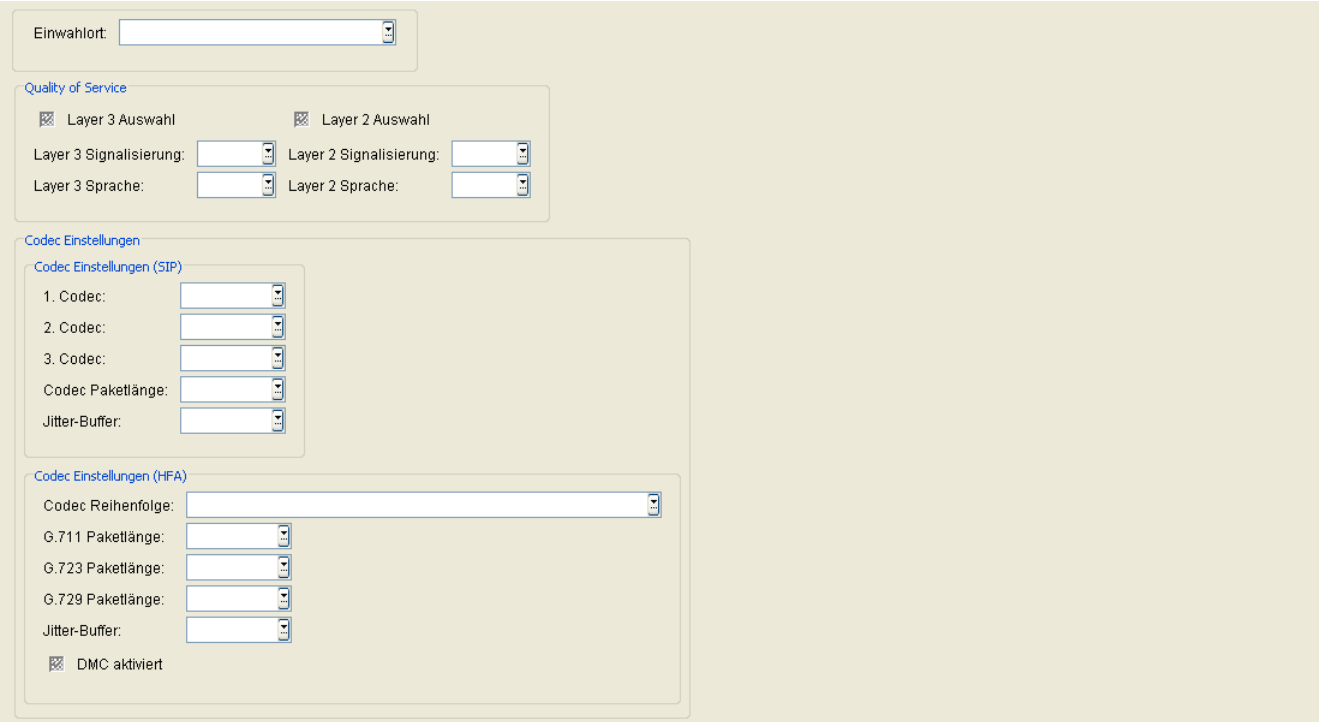
Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Einwahlort

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einwahlort Einstellungen“

7.2.13.1 Register „Einwahlort Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > Einwahlort > Register „Einwahlort Einstellungen“



Einwahlort

Der Benutzer-Profil-Name des IP-Client. Er wird beim ersten Anmelden im Login-Dialog des IP-Client definiert.

Quality of Service

Layer 3 Auswahl

Schalter zum Aktivieren der QoS-Konfiguration auf Layer 3.

Layer 3 Signalisierung:

Class of Service-Wert für die Anruf-Signalisierung auf Layer 3.

Mögliche Optionen:

- **AF11**
- **AF12**
- **AF13**

- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CS7**
- **Standard**

Layer 3 Sprache:

Class of Service-Wert für Sprache auf Layer 3.

Mögliche Optionen:

- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**

- **CS7**
- **Standard**

Layer 2 Auswahl

Schalter zum Aktivieren der QoS Layer 2-Konfiguration.

Layer 2 Signalisierung:

Class of Service-Wert für die Anruf-Signalisierung auf Layer 2.

Wertebereich: **0** ... **7**

Layer 2 Sprache:

Class of Service-Wert für Sprache auf Layer 2.

Wertebereich: **0** ... **7**

Codec Einstellungen

Codec Einstellungen (SIP)

1. Codec:

1. Komprimierungsverfahren.

Mögliche Optionen:

- **G.711**
- **G.722**
- **G.729**

2. Codec:

2. Komprimierungsverfahren.

Mögliche Optionen:

- **G.711**
- **G.722**

- **G.729**
- **Kein**

3. Codec:

3. Komprimierungsverfahren.

Mögliche Optionen:

- **G.711**
- **G.722**
- **G.729**
- **Kein**

Codec Paketlänge:

Mögliche Optionen:

- **Automatisch**
- **10**
- **20**

Jitter-Buffer:

Dauer der Zwischenspeicherung:

in Millisekunden.

Wertebereich: **20** ... **190** Millisekunden.

Codec Einstellungen (HFA)

Codec Reihenfolge:

Mögliche Optionen:

- **nicht komprimierende Codecs bevorzugt, ansonsten G.723 bevorzugt**
- **nicht komprimierende Codecs bevorzugt, ansonsten G.729 bevorzugt**
- **komprimierende Codecs bevorzugt, dabei G.723 bevorzugt**
- **komprimierende Codecs bevorzugt, dabei G.729 bevorzugt**

- **nur komprimierende Codecs, dabei G.723 bevorzugt**
- **nur komprimierende Codecs, dabei G.729 bevorzugt**

G.711 Paketlänge:

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

G.723 Paketlänge:

Mögliche Optionen:

- **30**
- **60**

G.729 Paketlänge:

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

Jitter-Buffer:

Dauer der Zwischenspeicherung

in Millisekunden.

Wertebereich: **20** ... **190** Millisekunden.

DMC aktiviert

Schalter zum Aktivieren der Bandbreite bei DMC.

7.2.14 OpenScape

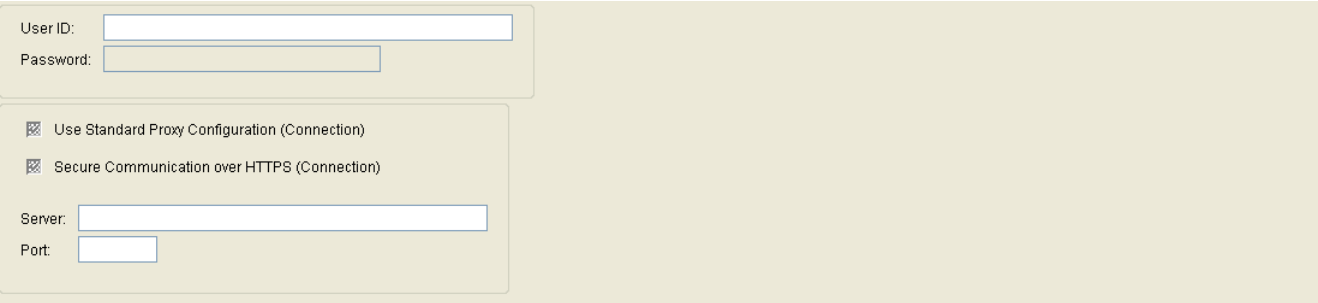
Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > OpenScape

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Verbindung“
- Register „Instant Messaging (XMP)“
- Register „WEB Zugriff“

7.2.14.1 Register „Verbindung“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > OpenScape > Register „Verbindung“



User ID:

User ID für die OpenScape Basis Verbindung.

Passwort:

Passwort für die OpenScape Basis Verbindung.

Benutze Standard Proxy Konfiguration:

Schalter zum Aktivieren der Benutzung des Standard Proxy.

Sichere Kommunikation mittels HTTPS:

Schalter zum Aktivieren der sicheren Kommunikation mittels HTTPS.

Server:

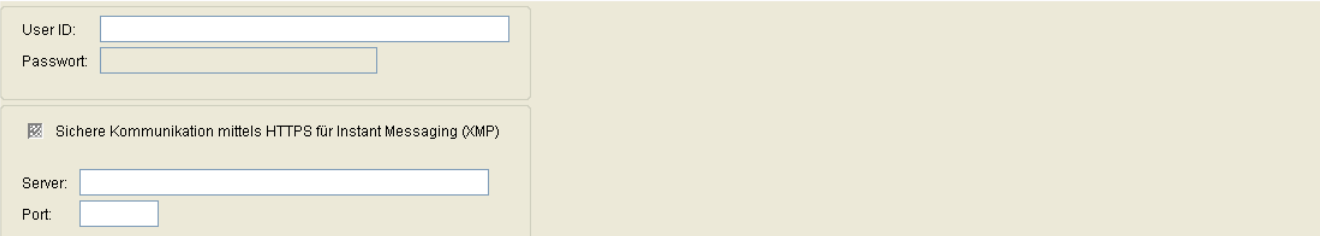
Addresse des Servers für die OpenScape Basis-Verbindung.

Port:

Portnummer des Servers für die OpenScape Basis-Verbindung.

7.2.14.2 Register „Instant Messaging (XMP)“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > OpenScape > Register „Instant Messaging (XMP)“



User ID:

User ID für den Zugang zum Server für OpenScape Instant Messaging (XMP).

Passwort:

Passwort für den Zugang zum Server für OpenScape Instant Messaging (XMP).

Sichere Kommunikation mittels HTTPS für Instant Messaging (XMP)

Schalter zum Aktivieren der sicheren Kommunikation mittels HTTPS.

Server:

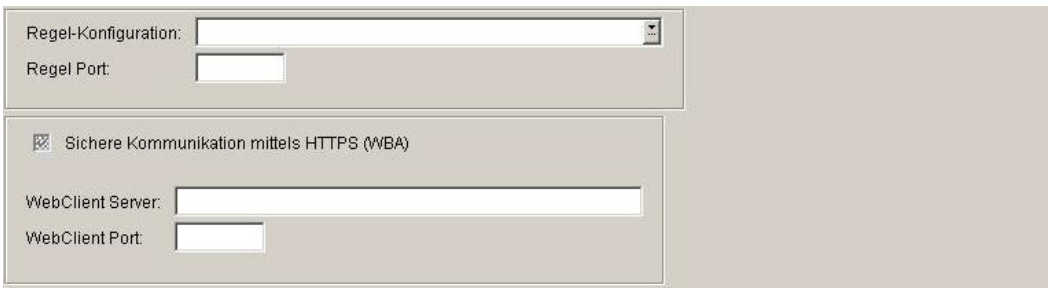
Adresse des Servers für OpenScape Instant Messaging (XMP).

Port:

Portnummer des Servers für OpenScape Instant Messaging (XMP).

7.2.14.3 Register „WEB Zugriff“

Aufruf: Hauptmenü > IP Devices > IP Client Konfiguration > OpenScape > Register „WEB Zugriff“



Regel-Konfiguration:

Regel-Konfiguration für WEB-Zugriffe.

Regel Port:

Port-Nummer des Servers für WEB-Zugriffe.

Sichere Kommunikation mittels HTTPS (WBA):

Schalter zum Aktivieren der sicheren Kommunikation mittels HTTPS.

WebClient Server:

Server-Adresse für den Zugriff auf den WebClient.

WebClient Port:

Port-Nummer des Servers für den Zugriff auf den WebClient.

7.3 IP Gateway Konfiguration

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- QoS Data Collection
- Security Einstellungen
- Signaling and Payload Encryption (SPE)
- IPSec / VPN

7.3.1 QoS Data Collection

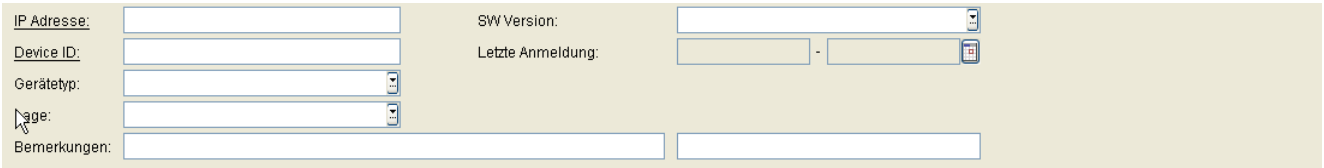
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Server Daten“
- Register „Report Einstellungen“
- Register „Schwellwerte“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > QoS Data Collection > Allgemeine Daten



Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP-Gateways zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP-Gateways angezeigt

Die in den Feldern **Bemerkungen** angezeigten Werte können geändert werden; bei allen anderen Feldern besteht keine Änderungsmöglichkeit.

IP Adresse:

IP-Adresse des IP Gateways.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID

ID, die diesen IP-Gateway eindeutig identifiziert.

Gerätetyp:

Gerätetyp des IP-Gateways.

Alle vom DLS unterstützten IP Devices finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **HG3500**

Lage:

Lage der Gateway-Baugruppe (Steckplatz).

SW Version:

Software-Version des IP-Gateways.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP-Gateways beim DLS.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Gateways, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Holen

Lädt ein bereits gesichertes Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Sichern

Sichert Konfigurations-Einträge als Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Verwerfen

Verwirft die Änderungen und neuen Einträge.

Lesen

Die auf der Maske dargestellten Parameter werden neu vom IP Device eingelesen.

Umbenennen

Ändert den Namen eines gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Löschen

Löscht ein gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Zertifikat importieren

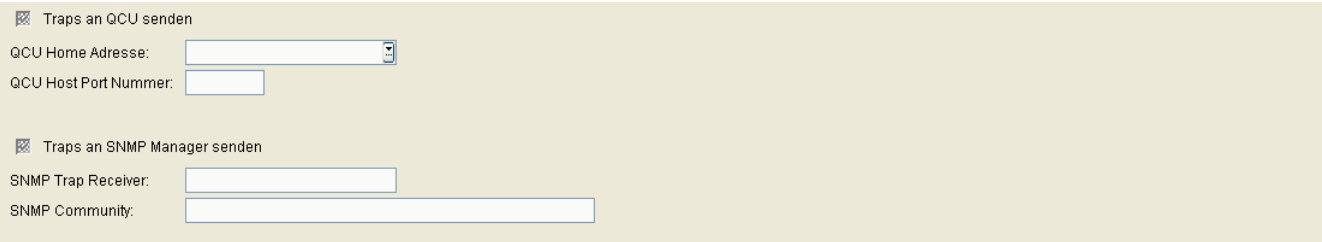
Importiert ein Zertifikat für das gewählte IP Device (nur in der Zertifikatsverwaltung verfügbar). Siehe hierzu Abschnitt 16.12, “Security: Administration von Zertifikaten”.

Zertifikat entfernen

Entfernt ein Zertifikat für das gewählte IP Device (nur in der Zertifikatsverwaltung verfügbar). Siehe hierzu Abschnitt 16.12, “Security: Administration von Zertifikaten”.

7.3.1.1 Register „Server Daten“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > QoS Data Collection > Register „Server Daten“



Traps an QCU senden

Ist der Schalter aktiviert, werden bei auftretenden Fehlern Meldungen an die QCU gesendet.

QCU Home Adresse:

IP-Adresse oder Hostname des Servers, der die QDC-Daten sammelt.

QCU Host Port Nummer:

Port-Nummer des Servers, der die QDC Daten sammelt.

Traps an SNMP Manager senden

Ist der Schalter aktiviert, werden bei auftretenden Fehlern Meldungen an den SNMP-Manager gesendet.

SNMP Community:

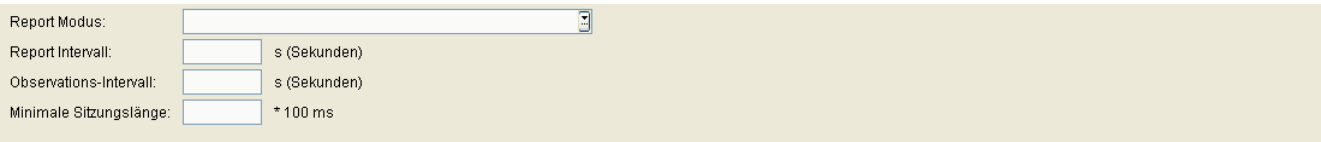
Community String, der zum Autorisieren am SNMP-Server verwendet wird.

SNMP Trap Receiver:

IP-Adresse des SNMP-Managers.

7.3.1.2 Register „Report Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > QoS Data Collection > Register „Report Einstellungen“



Report Modus:

Gibt an, wann ein Report erstellt werden soll.

Mögliche Optionen:

- **EOS Schwellwert überschritten**
  Am Ende der Verbindung bei Schwellwertüberschreitung.
- **EOR Schwellwert überschritten**
  Am Ende des Berichtintervalls bei Schwellwertüberschreitung.
- **EOS (Ende der Verbindung)**
  Am Ende der Verbindung.
- **EOR (Ende des Berichtintervalls)**
  Am Ende des Berichtintervalls.

Report Intervall:

Zeitintervall, in dem ein QoS-Report gesendet wird.

Wertebereich: **0** ... **3600** Sekunden.

Observations-Intervall:

Zeitintervall, in dem eine Schwellwertüberschreitung geprüft wird.

Wertebereich: **0** ... **5000** Sekunden.

Minimale Sitzungslänge:

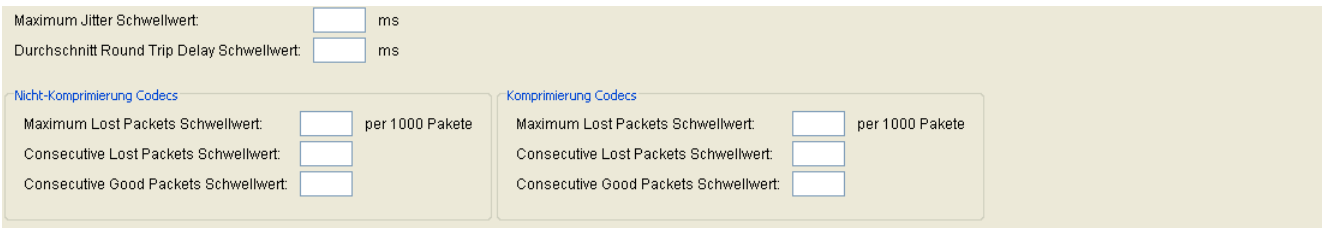
Besteht eine Sitzung (Session, das heißt z. B. eine Gesprächsverbindung) kürzer als dieses Minimum, dann wird kein QoS-Report gesendet.

Wertebereich: **0** ... **5000** (x 100 ms).

7.3.1.3 Register „Schwellwerte“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > QoS Data Collection > Register „Schwellwerte“

Hier werden die Schwellwerte eingetragen, bei deren Überchreitung ein QoS-Report refolgt.



Maximum Jitter Schwellwert:

Maximaler Schwellwert in Millisekunden für die Laufzeitschwankungen der Datenübertragung.

Wertebereich: **0** ... **255**

Standard: **15**

Durchschnitt Round Trip Delay Schwellwert:

Durchschnittliche Rückmeldezeit bei der Signalübertragung in Millisekunden. Wird dieser überschritten, erfolgt ein Report.

Standard: **100**

Nicht-Komprimierung Codecs

Maximum Lost Packets Schwellwert:

Maximale Anzahl der insgesamt verlorengegangenen Pakete bei unkomprimierter Übertragung. Die Anzahl wird in Mengen von je 1000 Paketen angegeben.

Wertebereich: **0** ... **255**

Consecutive Lost Packets Schwellwert:

Maximale Anzahl der nacheinander folgenden, verlorengegangenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Good Packets Schwellwert:

Minimale Anzahl der nacheinander folgenden, angekommenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Komprimierung Codecs

Maximum Lost Packets Schwellwert:

Maximale Anzahl der insgesamt verlorengegangenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Lost Packets Schwellwert:

Maximale Anzahl der nacheinander folgenden, verlorengegangenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

Consecutive Good Packets Schwellwert:

Minimale Anzahl der nacheinander folgenden, angekommenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

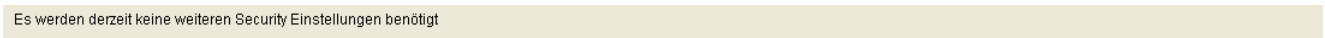
7.3.2 Security Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einstellungen“
- Register „WBM Server Zertifikate“

7.3.2.1 Register „Einstellungen“

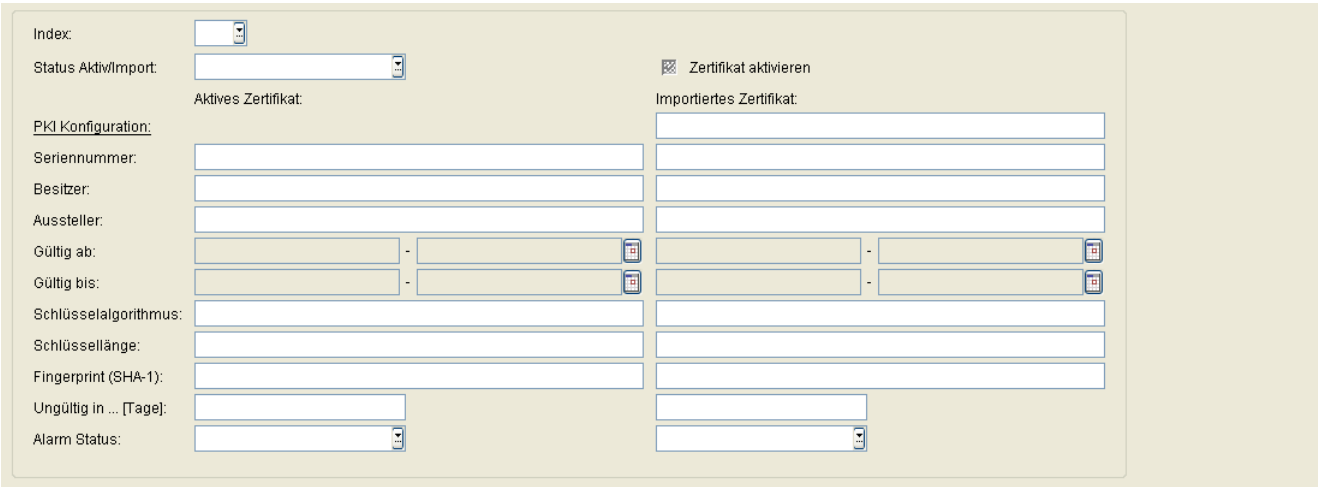
Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > Security Einstellungen > Register „Einstellungen“



Es werden derzeit keine weiteren Security Einstellungen benötigt.

7.3.2.2 Register „WBM Server Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > Security Einstellungen > Register „WBM Server Zertifikate“



Index

Index des Zertifikats.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

PKI Konfiguration

Zeigt die PKI-Konfiguration des importierten Zertifikats an.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

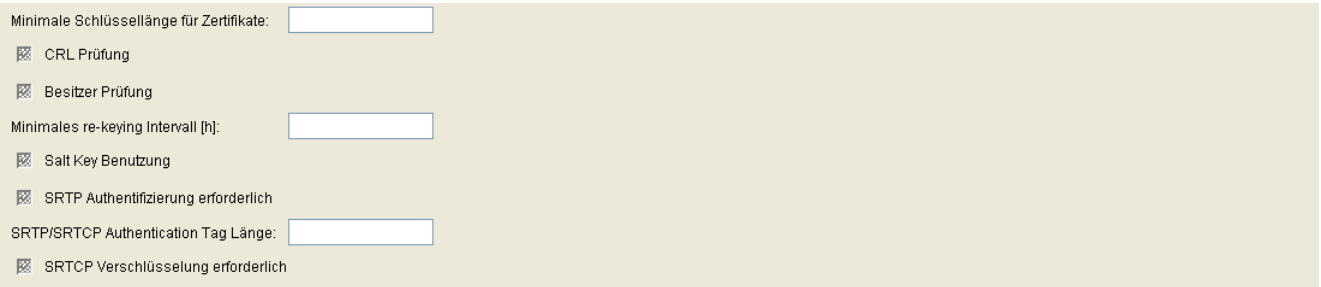
7.3.3 Signaling and Payload Encryption (SPE)

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einstellungen“
- Register „SPE Zertifikat“
- Register „SPE CA Zertifikate“
- Register „CRL Distribution Points“

7.3.3.1 Register „Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > Signaling and Payload Encryption (SPE) > Register „Einstellungen“



Minimale Schlüssellänge für Zertifikate

Minimale Schlüssellänge für Zertifikate.

CRL Prüfung

Ist der Schalter aktiviert, wird gegen die Certificate Revocation List (CRL), in der ungültige Zertifikate eingetragen werden können, geprüft.

Besitzer Prüfung

Ist der Schalter aktiviert, wird gegen den Besitzernamen geprüft (Subjectname check).

Maximales re-keying Intervall

Maximales re-keying Intervall in Stunden.

Salt Key Benutzung

Ist der Schalter aktiviert, so ist die Salt Key Benutzung erforderlich.

SRTP Authentifizierung erforderlich

Ist der Schalter aktiviert, wird eine Secure RTP-Authentifizierung erforderlich.

SRTP/SRTCP Authentication Tag Länge

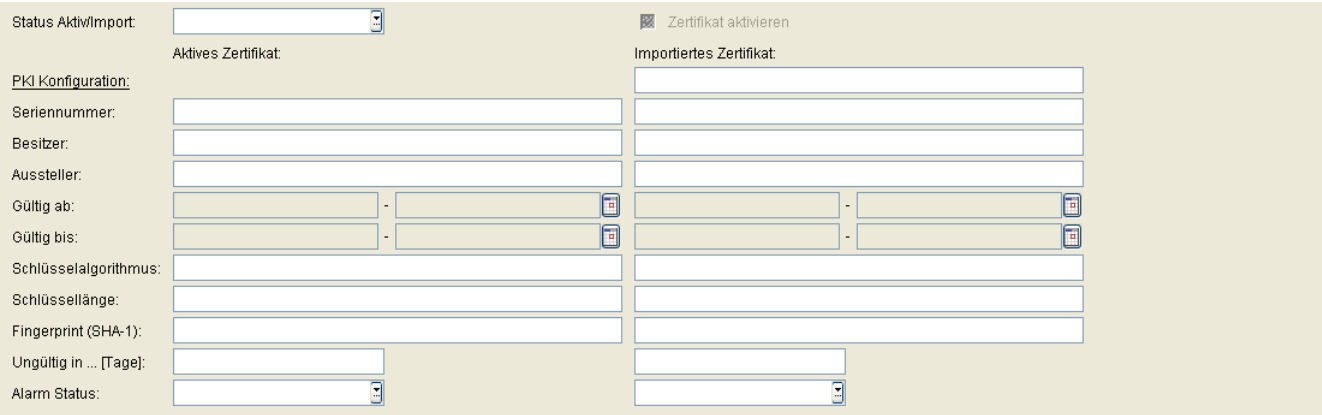
Länge des Authentifizierungsschlüssels.

SRTCP Verschlüsselung erforderlich

Ist der Schalter aktiviert, wird eine SRTCP-Verschlüsselung erforderlich.

7.3.3.2 Register „SPE Zertifikat“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > Signaling and Payload Encryption (SPE) > Register „SPE Zertifikat“



Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

PKI Konfiguration

Zeigt die PKI-Konfiguration des importierten Zertifikats an.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

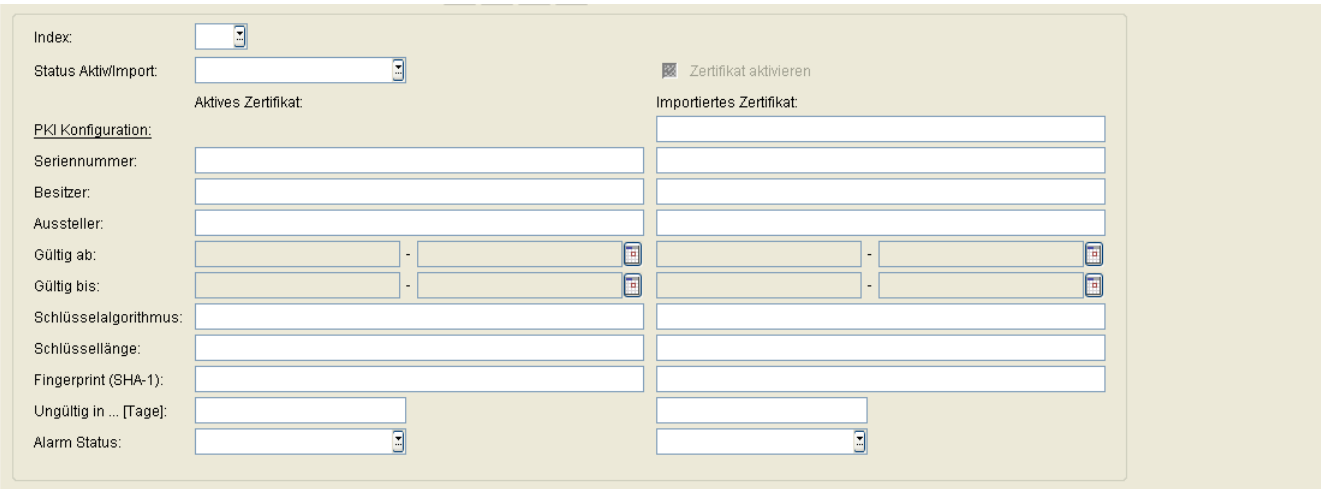
Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

7.3.3.3 Register „SPE CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > Signaling and Payload Encryption (SPE) > Register „SPE CA Zertifikate“



Index

Index zur Identifizierung der SPE CA Zertifikate.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

PKI Konfiguration

Zeigt die PKI-Konfiguration des importierten Zertifikats an.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

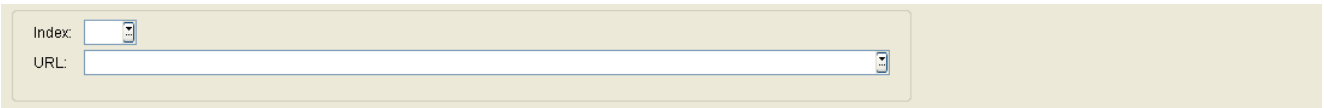
Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

7.3.3.4 Register „CRL Distribution Points“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > Signaling and Payload Encryption (SPE) > Register „CRL Distribution Points“



Index

Index zur Identifizierung der CRL Distribution Points.

URL

URL der CRL Distribution Points, z. B. http://.... oder ldap://...

7.3.4 IPSec / VPN

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einstellungen“
- Register „Peer Credentials“
- Register „CA Zertifikate“
- Register „CRL Dateien“

7.3.4.1 Register „Einstellungen“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > IPSec / VPN > Register „Einstellungen“

Es werden derzeit keine weiteren IPSec/VPN Einstellungen benötigt.

7.3.4.2 Register „Peer Credentials“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > IPSec / VPN > Register „Peer Credentials“

Index

Index zur Identifizierung des Peer Credentials.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

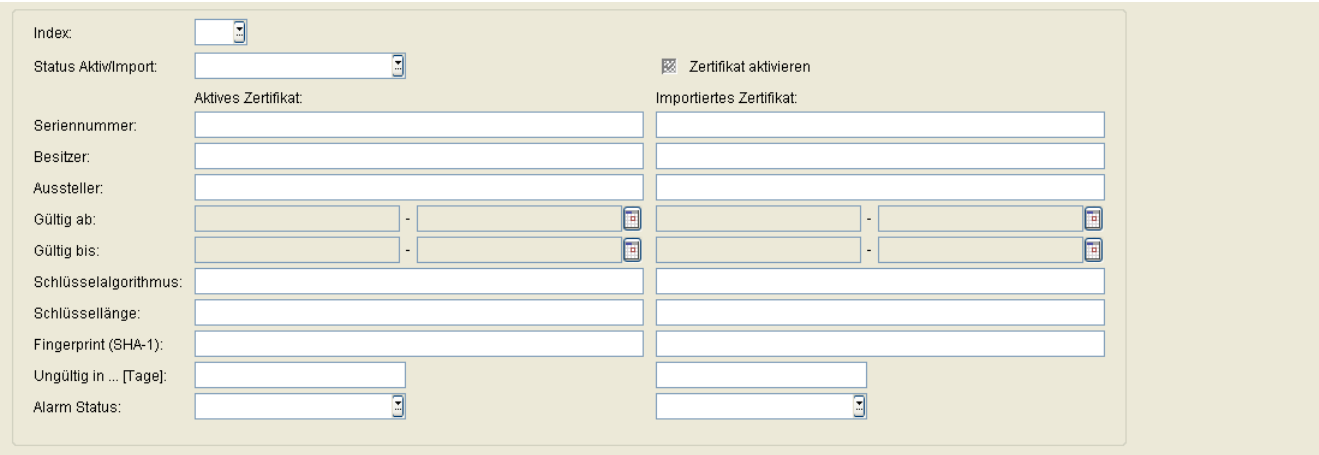
Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

7.3.4.3 Register „CA Zertifikate“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > IPSec / VPN > Register „CA Zertifikate“



Index

Index zur Identifizierung der CA Zertifikate.

Status Aktiv/Import:

Der Inhalt wird nach einem Import automatisch gesetzt, abhängig davon, ob aktive und/oder importierte Zertifikate existieren und ob diese unterschiedlich oder identisch sind.

Mögliche Optionen:

- **kein Zertifikat**
- **unterschiedlich**
- **gleich**
- **kein aktives Zertifikat**
- **kein importiertes Zertifikat**

Zertifikat aktivieren

Das importierte Zertifikat wird beim nächsten Sichern aktiviert. Durch Aktivieren eines leeren Zertifikats wird das Zertifikat am Endgerät gelöscht.

Seriennummer:

Seriennummer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Besitzer:

Besitzer des aktiven bzw. importierten Zertifikats (nur Anzeige).

Aussteller:

Aussteller des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig ab:

Zeitpunkt des Gültigkeitsbeginns des aktiven bzw. importierten Zertifikats (nur Anzeige).

Gültig bis:

Zeitpunkt des Gültigkeitsendes des aktiven bzw. importierten Zertifikats (nur Anzeige).

Schlüsselalgorithmus

Schlüsselalgorithmus.

Schlüssellänge

Schlüssellänge.

Fingerprint (SHA-1):

Prüfalgorithmus SHA-1 (160 Bit / 20 Zeichen) für das Sicherheitszertifikat.

Ungültig in ... [Tage]:

Zertifikat wird nach der angegebenen Anzahl von Tagen ungültig.

HINWEIS: Da der Wert des importierten Zertifikats abhängig von den Einstellungen in **Administration** > **Alarm Konfiguration** > **Register „Einstellungen“** > **Alarmeinstellungen für ablaufende Zertifikate** > **Intervall** periodisch aktualisiert wird, kann er bis zur nächsten Aktualisierung größer sein als der Wert des aktiven Zertifikats.

Alarm Status:

Aktueller Alarm-Status.

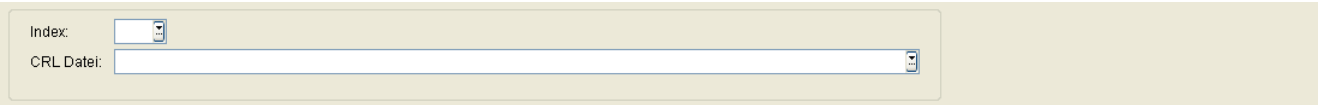
Mögliche Werte:

- **gültig**
- **in Kürze ungültig**
- **ungültig**

HINWEIS: Weitere Hinweise zum Importieren und Aktivieren von Zertifikaten finden Sie im Abschnitt 16.12, “Security: Administration von Zertifikaten”.

7.3.4.4 Register „CRL Dateien“

Aufruf: Hauptmenü > IP Devices > IP Gateway Konfiguration > IPSec / VPN > Register „CRL Dateien“



Index

Index zur Identifizierung der CRL-Dateien.

CRL Dateien

Verzeichnispfade der CRL-Dateien.

7.4 IP Device Interaktion

Mithilfe des Bereichs **IP Device Interaktion** können Sie einerseits Daten von IP Devices zum DLS übertragen, als auch einen Neustart bei IP Devices auslösen.

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion

Dieses Menü besteht aus folgenden Untermenüs:

- IP Device Daten lesen
- IP Device zurücksetzen
- IP Device Zertifikate sperren
- IP Device Response Test
- IP Devices pingen
- IP Devices scannen

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

7.4.1 IP Device Daten lesen

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device Daten lesen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Mit dieser Funktion können Sie Informationen aus den IP Devices auslesen. Es werden nur registrierte IP Devices berücksichtigt.

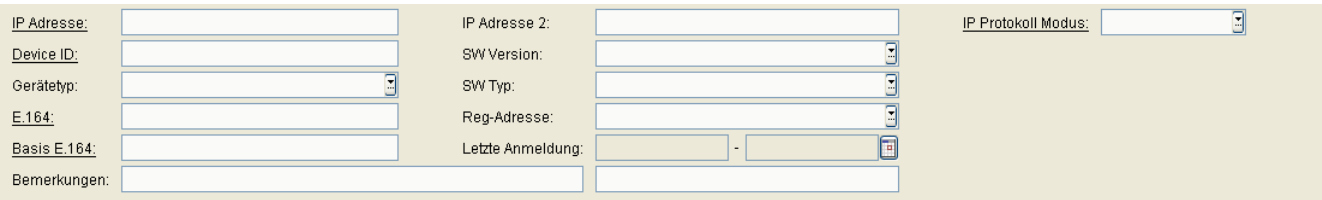
Hierbei geschieht eine Synchronisierung von Daten zwischen IP Devices und DLS-Datenbank. Die Daten werden ohne Zurücksetzen von IP Devices gelesen (siehe Abschnitt 7.4.2, “IP Device zurücksetzen”). Das heißt, es erfolgen keine weiteren Aktionen oder Eingriffe am IP Device.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für **IP Device Daten lesen** und **IP Device zurücksetzen** dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Devices zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Devices angezeigt (keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des IP Devices. Für OpenStage wird hier entweder eine IPv4 oder eine IPv6-Adresse angezeigt. Siehe auch Parameter **IP Protokoll Modus**.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device. Bei IP Phones ist das in der Regel die MAC-Adresse.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Devices.

Alle vom DLS unterstützte IP Device-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiele: **optiPoint 410 standard**, **optiClient 130**

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

Nur für OpenStage verfügbar.

SW Version:

Software-Version des IP Devices.

Beispiel für IP Phones und IP Clients: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des IP Devices.

Beispiele: **Unify HFA**, **Unify SIP**

Reg-Adresse:

IP-Adresse des Gateways oder des Gatekeepers, an dem sich das IP Device registrieren muss. Bei HiPath 3000 ist das die Adresse der HG 1500, bei HiPath 4000 ist es die HG 3530 oder das STMI-Board.

Bemerkungen:

Felder für allgemeine Informationen.

IP Protokoll Modus

Zeigt an, welche IP-Version das IP Phone verwendet. Werden beide Versionen verwendet, steht in IP Adresse die IPv4-Adresse und in IP Adresse 2 die IPv6-Adresse.

Nur für OpenStage verfügbar.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Clients, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

IP Device zurücksetzen

Stößt einen Neustart/Reset des Endgeräts an.

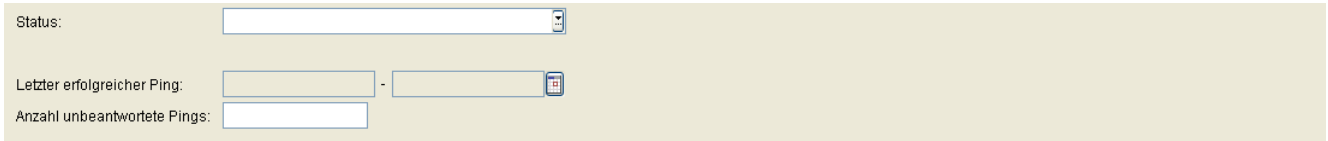
Werkseinstellung wiederherstellen

Stößt einen Neustart/Reset des Endgeräts mit Wiederherstellung des Lieferzustands an. Nach Betätigen dieser Aktionsschaltfläche muss das Reset-Passwort eingegeben werden.

Verfügbar für OpenStage, optiPoint 410 und optiPoint 420.

7.4.1.1 Register „Info“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device Daten lesen > Register „Info“



Status:

Mögliche Optionen:

- **in Betrieb**
  IP Phone, das z. Zt. in Betrieb ist.
- **Lizenz abgelaufen**
  IP Phone, bei dem die Lizenz abgelaufen ist.
- **ungültiger Lizenzeintrag**
  Unlizenziertes IP Phone.
- **ungültige SW Signatur**
  IP Phone, bei dem die Registrierung nicht erfolgreich war.

Letzter erfolgreicher Ping

Anzeige des letzten erfolgreichen PINGs.

Der Wert ist nur lesbar.

Siehe auch Abschnitt 7.4.5, “IP Devices pingen”.

Anzahl unbeantwortete Pings

Gesamte Anzahl der erfolglos durchgeführten PINGs.

Der Wert ist nur lesbar.

Siehe auch Abschnitt 7.4.5, “IP Devices pingen”.

7.4.2 IP Device zurücksetzen

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device zurücksetzen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Es ist sowohl das Zurücksetzen des IP Devices (Reboot), das Sperren aller von diesem IP Device genutzer PSE-Zertifikate (Revoke Certificates), als auch die Wiederherstellung der Werkeinstellungen (Factory Reset) möglich. CA-Zertifikate werden nicht gesperrt.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

IP Device zurücksetzen

Stößt einen Neustart/Reset des Endgeräts an.

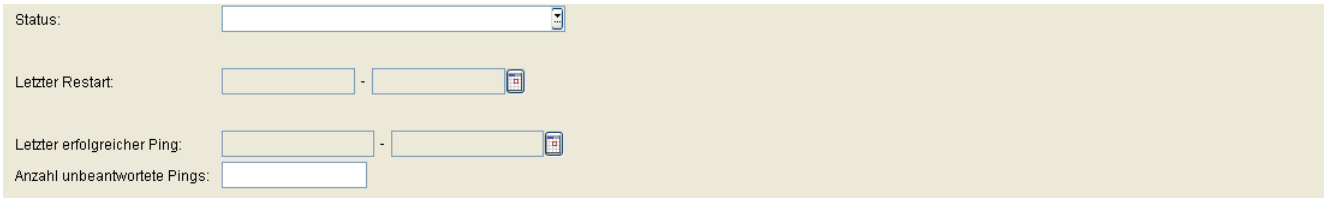
Werkseinstellung wiederherstellen

Stößt einen Neustart/Reset des Endgeräts mit Wiederherstellung des Lieferzustands an. Nach Betätigen dieser Aktionsschaltfläche muss das Reset-Passwort eingegeben werden.

Verfügbar für OpenStage, optiPoint 410 und optiPoint 420.

7.4.2.1 Register „Info“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device zurücksetzen > Register „Info“



Status:

Status des IP Phones.

Mögliche Optionen:

- **in Betrieb**
  IP Phone, das z. Zt. in Betrieb ist.
- **Lizenz abgelaufen**
  IP Phone, bei dem die Lizenz abgelaufen ist.
- **ungültiger Lizenzeintrag**
  Unlizenziertes IP Phone.
- **ungültige SW Signatur**
  IP Phone, bei dem die Registrierung nicht erfolgreich war.

Letzter Restart:

Datum /Uhrzeit des letzten Neustarts werden angezeigt.

Letzter erfolgreicher Ping

Anzeige des letzten erfolgreichen PINGs.

Der Wert ist nur lesbar.

Siehe auch Abschnitt 7.4.5, “IP Devices pingen”.

Anzahl unbeantwortete Pings

Gesamte Anzahl der erfolglos durchgeführten PINGs.

Der Wert ist nur lesbar.

Siehe auch Abschnitt 7.4.5, “IP Devices pingen”.

7.4.3 IP Device Zertifikate sperren

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device Zertifikate sperren

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Mögliche Aktionsschaltflächen

IP Device Zertifikate sperren

Durch Klicken des Buttons wird ein Eingabefenster eingeblendet, in dem die zu sperrenden Zertifikate ausgewählt werden können.

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Startet einen Job zur Verteilung der Konfigurationsänderungen. Weitere Informationen finden Sie in Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”.

Verwerfen

Die in der Maske vorgenommenen Änderungen werden verworfen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

7.4.3.1 Register „Info“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device Zertifikate sperren > Register „Info“

Status

Zeigt den Status des Zertifikats an.

Mögliche Optionen:

- **in Betrieb**
- **Lizenz abgelaufen**
- **ungültiger Lizenzeintrag**
- **ungültige SW Signatur**

7.4.4 IP Device Response Test

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device Response Test

Mittels dieser Funktion können nicht antwortende IP Devices automatisch in den Papierkorb verschoben werden. Nicht antwortende IP Devices werden mit dem Ping-Mechanismus ermittelt. Wenn die in **Maximale Anzahl erfolglose Pings** definierte Anzahl überschritten wird, wird das IP Device in den Papierkorb verschoben. IP Devices im Papierkorb werden nicht mehr angepingt. Sie können entweder wiederhergestellt oder, manuell oder automatisch, gelöscht werden.

Registriert sich ein IP Device, das sich im Papierkorb befindet, erneut, wird es automatisch wiederhergestellt.

Diese Funktion ist für IP Phones (optiPoint, OpenStage, WLAN Phones), nicht aber für IP Clients und IP Gateways verfügbar.

Weitere Informationen finden Sie in Kapitel Abschnitt 7.5.2, “Papierkorb”.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Startet einen Job zur Verteilung der Konfigurationsänderungen. Weitere Informationen finden Sie in Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”.

Verwerfen

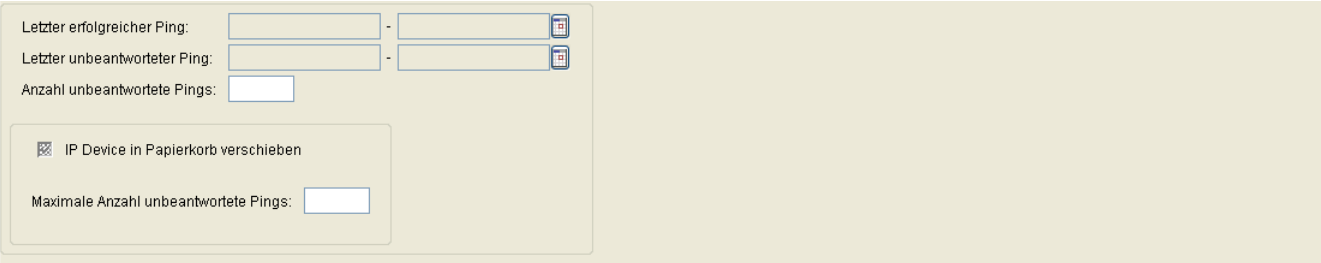
Die in der Maske vorgenommenen Änderungen werden verworfen.

Aktualisieren

Aktualisiert das Fenster anhand der Datenbank.

7.4.4.1 Register „Info“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Device Response Test > Register „Info“



Letzter erfolgreicher Ping

Zeigt Datum und Uhrzeit des letzten erfolgreichen Pings an.

Letzter unbeantworteter Ping

Zeigt Datum und Uhrzeit des letzten unbeantworteten Pings an.

Anzahl unbeantwortete Pings

Zeigt die aktuelle Gesamtanzahl unbeantworteter Pings an.

IP Device in Papierkorb verschieben

Ist der Schalter gesetzt, wird nach Überschreiten der **maximalen Anzahl unbeantworteter Pings** das IP Device in den Papierkorb verschoben.

> ***HINWEIS:*** Der Schalter **IP Device in Papierkorb verschieben** ist bei DCMP-fähigen Geräten ausgegraut.

Maximale Anzahl unbeantwortete Pings

Nach Überschreiten der maximalen Anzahl unbeantworteter Pings wird das IP Device in den Papierkorb verschoben. IP Devices im Papierkorb werden nicht mehr gepingt. Sie können entweder restauriert oder gelöscht werden.

Weitere Informationen, siehe Abschnitt 7.5.2, “Papierkorb”.

> ***HINWEIS:*** Der Schalter **Maximale Anzahl unbeantwortete Pings** ist bei DCMP-fähigen Geräten ausgegraut.

7.4.5 IP Devices pingen

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices pingen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „IP Phones“
- Register „IP Clients“
- Register „IP Gateways“

Mit der Funktion haben Sie die Möglichkeit, mithilfe von PINGs zu Prüfen, ob die IP Devices noch reagieren, d. h., noch ansprechbar sind.

Informationen über erfolgreiche/-lose Pings erhalten Sie in den folgenden DLS-Bereichen:

- IP Devices > IP Device Verwaltung > Inventar Daten > Register „Pings“
- IP Device Interaktion > IP Device Daten lesen > Register „Info“
- IP Device Interaktion > IP Device zurücksetzen > Register „Info“

Allgemeine Daten

IP Device Pings ausführen

Schalter zum Aktivieren der IP Device-PING Einstellungen.

Mögliche Aktionsschaltflächen

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

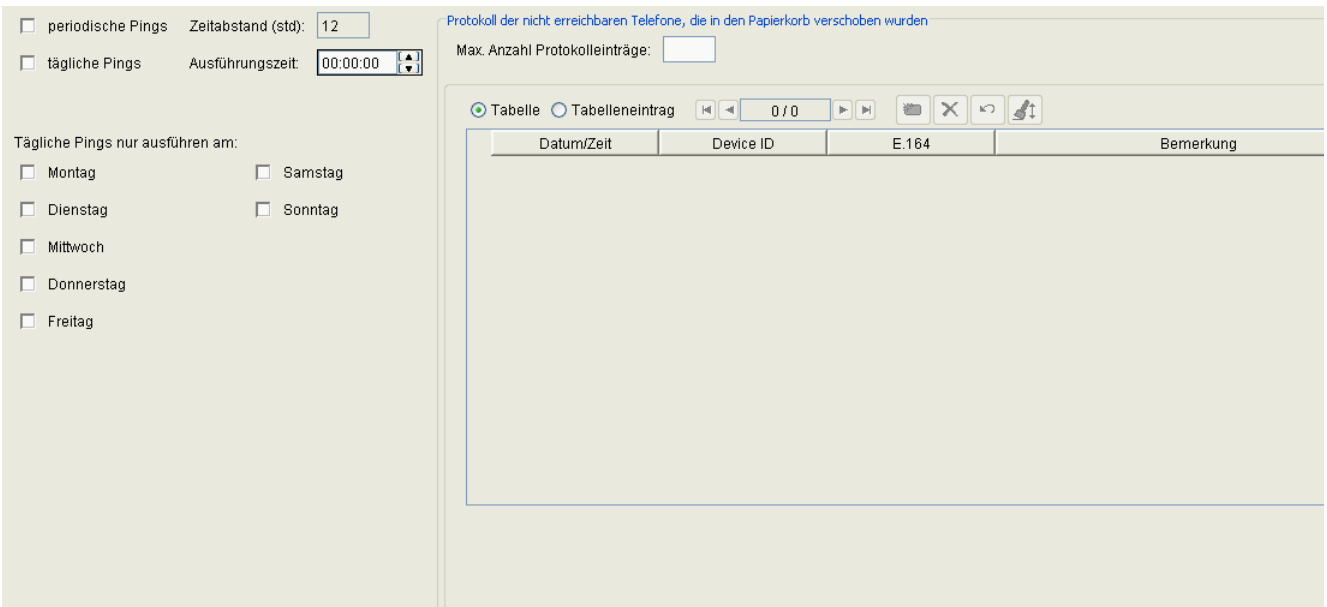
Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

7.4.5.1 Register „IP Phones“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices pingen > Register „IP Phones“

Legen Sie hier die zeitliche Abfolge der PING-Abfragen für IP Phones fest.



periodische Pings

Schalter zum Aktivieren von periodisch wiederholende PINGs.

Zeitabstand in Stunden:

Zeit zwischen zwei periodischen Pings. Gilt nur, wenn periodische Pings aktiviert sind.

Wertebereich: **1** ... **23** Stunden

tägliche Pings

Schalter zum Aktivieren von täglich wiederholende Pings.

Ausführungszeit:

Uhrzeit für den Start der täglichen Pings (Kalender siehe Abschnitt 5.4.2.4, “Inhaltsbereich”).

Gilt nur, wenn tägliche Pings aktiviert sind.

Tägliche Pings nur ausführen am:

Hier können tägliche Pings auf einzelne Wochentage beschränkt werden.

Mögliche Optionen (Mehrfachauswahl möglich):

- **Montag**
- **Dienstag**
- **Mittwoch**
- **Donnerstag**
- **Freitag**
- **Samstag**
- **Sonntag**

Gilt nur, wenn tägliche Pings aktiviert sind.

Protokoll der nicht erreichbaren Telefone, die in den Papierkorb verschoben wurden

Max. Anzahl Protokolleinträge

Maximale Anzahl der Protokolleinträge.

Datum/Zeit

Datum und Uhrzeit, als die Aktion gestartet wurde.

Device ID

Device ID des IP Device.

E.164

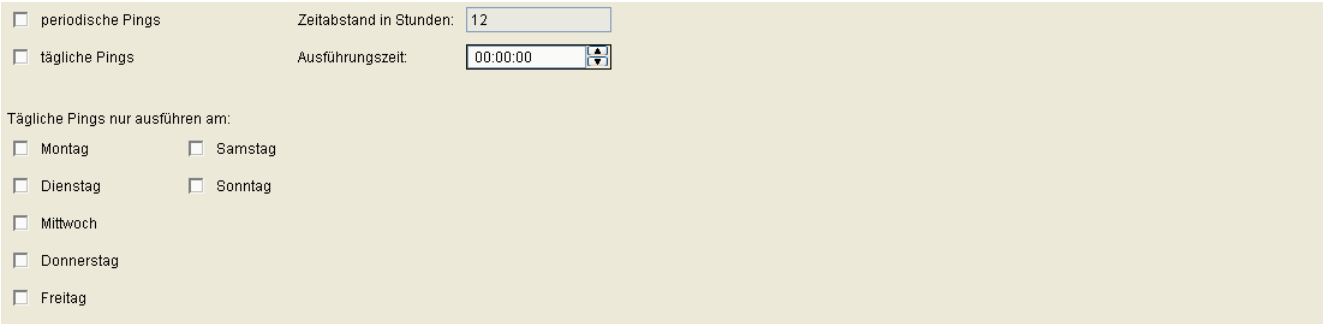
E.164 Nummer des IP Device.

Bemerkung

Bemerkung zum IP Device.

7.4.5.2 Register „IP Clients“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices pingen > Register „IP Clients“

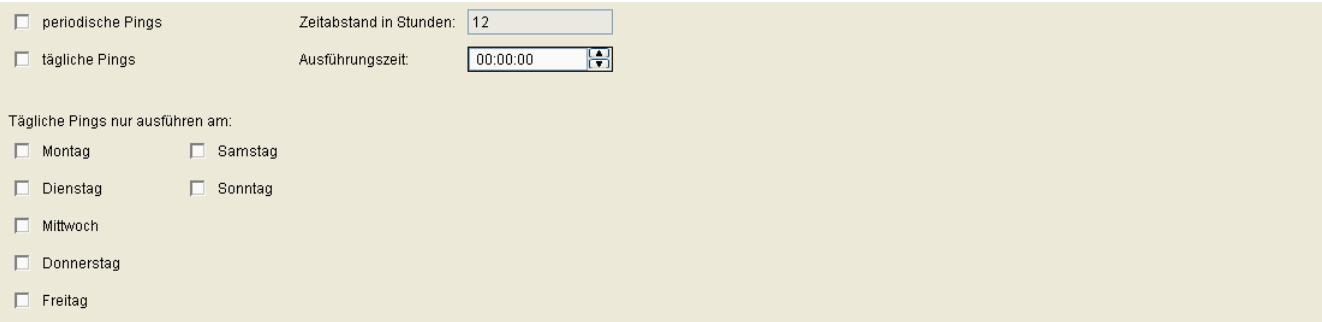


Legen Sie hier die zeitliche Abfolge der PING-Abfragen für IP Clients fest.

Zur Oberfläche und deren Beschreibung siehe Abschnitt 7.4.5.1, “Register „IP Phones“”.

7.4.5.3 Register „IP Gateways“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices pingen > Register „IP Gateways“



Legen Sie hier die zeitliche Abfolge der PING-Abfragen für IP Clients fest.

Zur Oberfläche und deren Beschreibung siehe Abschnitt 7.4.5.1, “Register „IP Phones“”.

7.4.6 IP Devices scannen

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices scannen

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „IP Bereiche“
- Register „Konfiguration“
- Register „Scan Ergebnisse“

Mit der Funktion haben Sie als DLS-Nutzer z. B. mit einem TAP die Möglichkeit, eine DLS-Datenbank aller im Netz gefundenen IP Devices für die weitere Bearbeitung anzulegen.

Bei einem Scan sendet der DLS an jede IP-Adresse innerhalb des angegebenen Bereichs einen ContactMe-Request, bestehend aus einer kurzen HTML-Nachricht. Anschließend wartet der DLS ab, ob das jeweilige Gerät einen Callback sendet. Ist für den Scanvorgang der ICMP-Ping aktiviert (siehe Register „Konfiguration“), so wird vor dem Absenden eines ContactMe-Requests jeweils ein ICMP-Ping gesendet, um herauszufinden, ob sich hinter der IP-Adresse ein Gerät befindet.

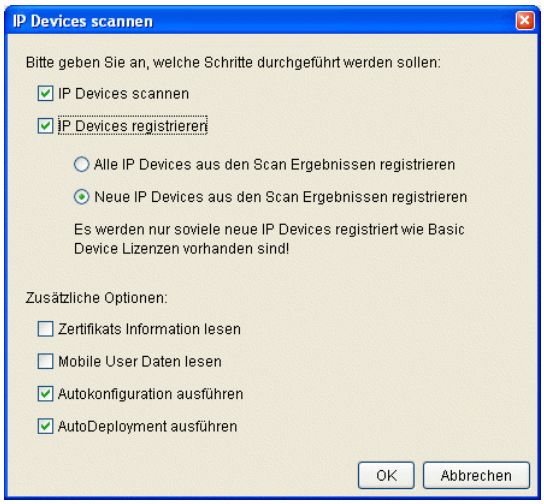
Einrichtung eines IP Scanners

Falls noch nicht geschehen, muss zunächst ein IP Scanner angelegt werden, d. h. eine Konfiguration, die besagt, welche IP-Bereiche zu scannen sind und wie der Scan erfolgen soll. Dies geschieht in folgenden Schritten:

1. Legen Sie einen neuen IP Scanner an, indem Sie auf die Aktionsschaltfläche **Neu** klicken.
2. Geben Sie im Bereich Allgemeine Daten einen Namen und eine Beschreibung für den IP Scanner ein.
3. Tragen Sie im Bereich **Register „IP Bereiche“** den Adressenbereich ein, der gescannt werden soll, sowie den Port, auf dem die Endgeräte für den DLS zu erreichen sind.
4. Legen Sie ggf. weitere Parameter im **Register „Konfiguration“** fest.

Starten des Scanvorgangs

Nach Betätigen der Aktionsfläche **IP Devices scannen** erscheint ein Auswahlfenster:



Der Administrator kann entscheiden, ob zunächst nur ein Scannen der IP Devices oder zugleich eine Registrierung stattfinden soll:

- **IP Devices scannen**
  Die IP Devices werden gescannt.
- **IP Devices registrieren**
  Die IP Devices werden registriert.

Eine Registrierung ist nötig, damit die IP Devices auch in die Inventory-Datenbank aufgenommen werden.

Der gesamte Vorgang kann auch zweistufig stattfinden, indem auf der ersten Stufe nur gescannt wird und dann auf der zweiten Stufe die Registrierung erfolgt. Beim Registrieren wird zwischen der Registrierung aller gescannten IP Devices und der Registrierung nur der noch nicht in der Inventory Datenbank erfassten IP Devices unterschieden:

- **Alle IP Devices aus den Scan Ergebnissen registrieren**
  Es werden alle in den Scan-Ergebnissen aufgeführten IP Devices registriert, auch die zuvor bereits registrierten.
- **Neue IP Devices aus den Scan Ergebnissen registrieren**
  Es werden nur diejenigen IP Devices registriert, die noch nicht registriert sind.

Will der Administrator nicht alle beim Scannen erkannten IP Devices registrieren lassen, so muss er die entprechenden Einträge aus den Scan-Ergebnissen löschen.

HINWEIS: Wenn Sie mittels TAP bei einem Kunden erstmals IP Devices scannen (z. B. zur Erfassung des Inventars), achten Sie darauf, dass **AutoDeployment ausführen** deaktiviert ist. Dadurch wird ein unerwünschtes Deployment innerhalb der Betriebszeiten im Kundennetz verhindert.

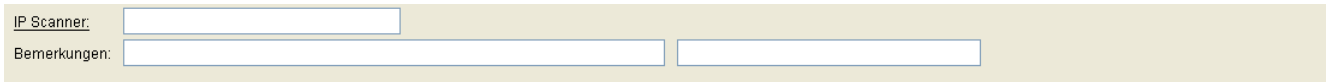
Falls beim Scanvorgang einzelne Endgeräte nicht gefunden werden, erhöhen Sie den Timeout (siehe **Zeitüberschreitung (sek):**) und starten darauf daraufhin einen neuen Scanvorgang.
Wird daraufhin immer noch ein Teil der IP Devices nicht erreicht, so wird für die betroffenen IP Devices ein zweiter Scan-Vorgang gestartet. Dieser dauert **mindestens 5 Minuten**. Während dieser Zeit zeigt der Fortschrittsbalken

99% an; die im ersten Durchlauf erkannten IP Devices können bereits administriert werden.
Für jedes IP Device, das auch beim zweiten Scan nicht erreicht wurde, wird ein Eintrag im Activity-Log hinterlegt (siehe Abschnitt 14.1, “Job Kontrolle”).

HINWEIS: Beim Scannen von IP Devices wird an das gescannte IP Device eine gültige DLS-Serveradresse übertragen, so dass er zu einem späteren Zeitpunkt den DLS-Servers eigenständig kontaktieren kann.
Dies geschieht jedoch nicht, wenn das IP Device von einem DHCP-Server bereits mit einer DLS-Serveradresse versorgt wurde. In diesem Fall bleibt die vom DHCP-Server gelieferte DLS-Adresse erhalten.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten



IP Scanner:

Name des IP-Scanners.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen Scannern, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Neu

Legt einen neuen IP-Scanner an.

Löschen

Löscht einen oder mehrere IP-Scanner (Mehrfachauswahl in Tabellenansicht möglich).

IP Devices scannen

Startet den IP-Scanner, der in der Ansicht **Objekt** angezeigt wird.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

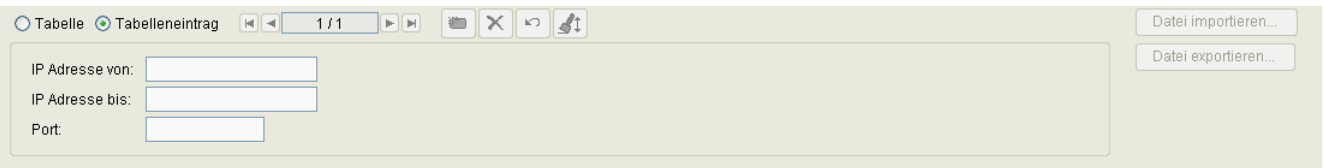
7.4.6.1 Register „IP Bereiche“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices scannen > Register „IP Bereiche“

Legen Sie hier jeweils eine Kombination aus IP-Adressbereich und Portnummer der zu scannenden IP Devices fest. Eine weitere Kombination können Sie in der Ansicht **Neu** und **Objekt** mit der Schaltfläche hinzufügen und mit löschen.

Darüber hinaus können Sie eine CSV-Datei mit bereits vorhandenen IP/Port-Kombinationen sowohl importieren als auch diese Daten im CSV-Format exportieren.

> ***HINWEIS:*** Zur Vermeidung großer Netzlast sollte der Bereich der IP-Adressen so gewählt werden, dass möglichst nur IP Devices gescannt werden.
>
> Falls sich in dem angegebenen IP-Bereich auch andere IP-Clients (keine IP Devices) befinden, kann es in bestimmten Fällen zu Funktionsstörungen an den Geräten kommen.



IP Adresse von

IP-Adresse für die Untergrenze des zu scannenden IP-Bereichs.

Format: **000.000.000.000**, 000 = Wert zwischen 000 und 255.

IP Adresse bis

IP-Adresse für die Obergrenze des zu scannenden IP-Bereichs.

Format: **000.000.000.000**, 000 = Wert zwischen 000 und 255.

> ***HINWEIS:*** Das jeweilige Wertepaar **IP Adresse von** und **IP Adresse bis** muss identisch sein. Administratoren können nicht nur IP-Adressen sondern auch DNS-Namen konfigurieren.

Port

Portnummer der zu scannenden IP-Adressen.

Folgende Standard-Ports werden von den verschiedenen IP Device-Typen verwendet und sind hier entsprechend einzutragen:

- IP Phone: **8085**

- IP Client: **8082**
- WLAN-Phone: **80**

Format: max. 5 Stellen.

Datei importieren...

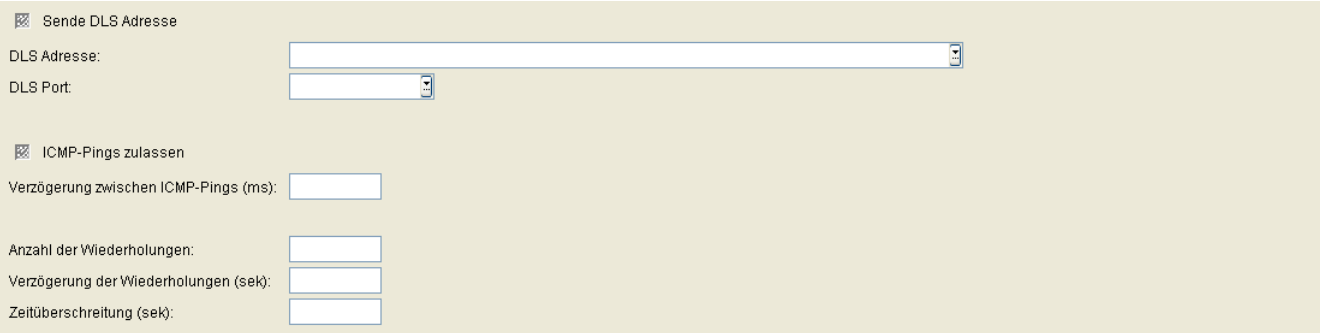
Lädt eine Datei im CSV-Format mit bereits vorhandenen IP-Bereichen und Portnummern in die IP-Bereichstabelle.

Datei exportieren...

Speichert IP-Bereiche und Portnummern aus der IP-Bereichstabelle in eine Datei im CSV-Format.

7.4.6.2 Register „Konfiguration“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices scannen > Register „Konfiguration“



Sende DLS Adresse

Nutzen Sie den DLS auf einem TAP, aktivieren Sie die Checkbox **Sende DLS Adresse** und geben Sie die DLS-Adresse und die DLS-Portnummer auf dem TAP bekannt. Den IP Devices werden so beim Scannen die Adressdaten des sie bearbeitenden DLS bekannt gegeben.

HINWEIS: Das Senden der DLS-Adresse darf nicht bei permanentem DLS-Server im Netz verwendet werden.

DLS Adresse:

IP-Adresse des DLS-Servers auf dem TAP.

Format: **000.000.000.000** (000 = Wert zwischen 000 und 255)

DLS Port:

Portnummer des DLS-Servers auf dem TAP.

Wertebereich: max. 5 Ziffern.

ICMP Pings zulassen:

Ist der Schalter aktiviert, werden beim Scannen ICMP-Pings verwendet. Dies ermöglicht einen schnelleren Scan der IP Devices, da ein ContactMe-Request nur an solche IP-Adressen egschickt wird, bei denen der ICMP-Ping erfolgreich war.

HINWEIS: Sind in einem Netz keine ICMP-Pings erlaubt, muss der Schalter deaktiviert werden, da der IP Device Scan sonst kein Ergebnis liefert.

Verzögerung zwischen ICMP-Pings (ms)

Abstand zwischen ICMP-Pings in Millisekunden, um sicherzustellen, dass die ICMP-Pings nicht vom Betriebssystem blockiert werden.

Anzahl der Wiederholungen:

Anzahl der maximalen Wiederholungsversuche für einen Scan. Der Wert wird pro IP-Adresse ausgewertet.

Standard: **1**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Wiederholungsversuchen liegen soll. Der Wert wird pro IP-Adresse ausgewertet.

Standard: **10**

Zeitüberschreitung (sek):

Zeit, die maximal verstreichen darf zwischen ContactMe-Request des DLS und erfolgter Registrierung des betreffenden IP Devices.

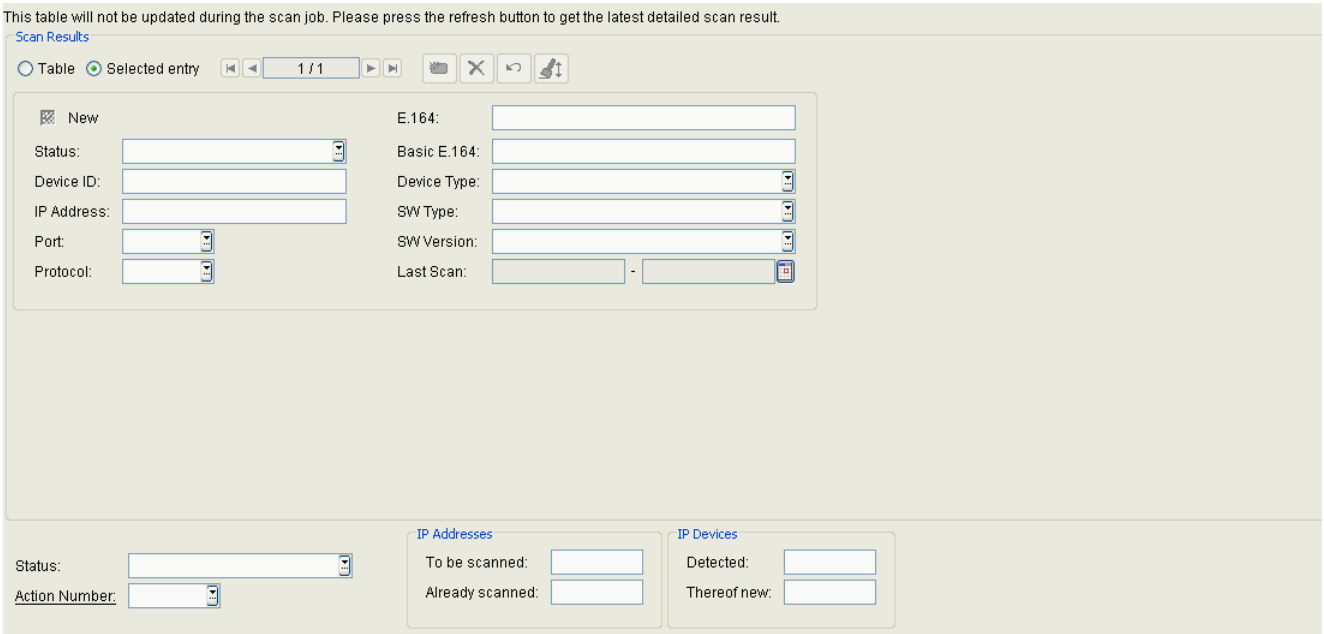
Der eingetragene Wert muss größer als der Wert für Abschnitt 6.9.2, “Register „DCMP“” sein.

Mögliche Optionen:

0 - 3600, Standard: **60** Sekunden.

7.4.6.3 Register „Scan Ergebnisse“

Aufruf: Hauptmenü > IP Devices > IP Device Interaktion > IP Devices scannen > Register „Scan Ergebnisse“



Neu

Ist ein IP Device beim Scan neu erfasst worden, so wird das durch ein Häkchen angezeigt.

Status

Zeigt den Status des Scanvorgangs für jeweils ein IP Devices an.

Mögliche Werte:

- **läuft**
- **bestätigt**
- **fertig**
- **fehlgeschlagen**

Device ID

Zeigt die Device ID des gescannten IP Devices an. Diese dient zur eindeutigen Identifizierung des IP Device. Bei IP Phones ist sie in der Regel mit der MAC-Adresse identisch.

IP Adresse

Zeigt die IP-Adresse des gescannten IP Devices an.

Port

Zeigt den Port an, über den das gescannte IP Device mit dem DLS kommuniziert.

Protokoll

Zeigt das Protokoll an, über das gescannte IP Device mit dem DLS kommuniziert.

E.164

Zeigt die E.164-Nummer des gescannten IP Devices an.

Basis E.164

Zeigt die Basis-E.164-Nummer des gescannten IP Devices an.

Gerätetyp

Zeigt den Gerätetyp des gescannten IP Devices an.

Beispiel: **optiPoint 410 advance.**

SW Typ

Zeigt den Software-Typ des gescannten IP Devices an.

Beispiel: **Unify SIP**, **Unify HFA.**

SW Version

Zeigt die Version der Software an, die auf dem gescannten IP Device installiert ist.

Beispiel: **6.0.53.**

Letzter Scan

Zeigt Datum und Uhrzeit des zuletzt vorgenommenen Scans an.

Status:

Zeigt den Status des aktuellen Scanvorgangs an.

Beispiel: **läuft**, **fertig.**

Aktionsnummer:

Zeigt die Aktionsnummer des aktuellen Scanvorgangs an.

IP Adressen

Zu scannen:

Zeigt an, wieviele der im IP-Bereich angegebenen IP-Adressen noch zu scannen sind.

Gescannt:

Zeigt an, wieviele der im IP-Bereich angegebenen IP-Adressen bereits gescannt sind.

IP Devices

Gefunden:

Zeigt an, wieviele IP Devices beim Scanvorgang gefunden worden sind.

Davon neu:

Zeigt an, wieviele der beim Scanvorgang gefundenen IP Devices noch nicht registriert sind.

7.5 IP Device Verwaltung

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Inventar Daten
- Papierkorb
- IP Infrastruktur
- IP Device Konfiguration

7.5.1 Inventar Daten

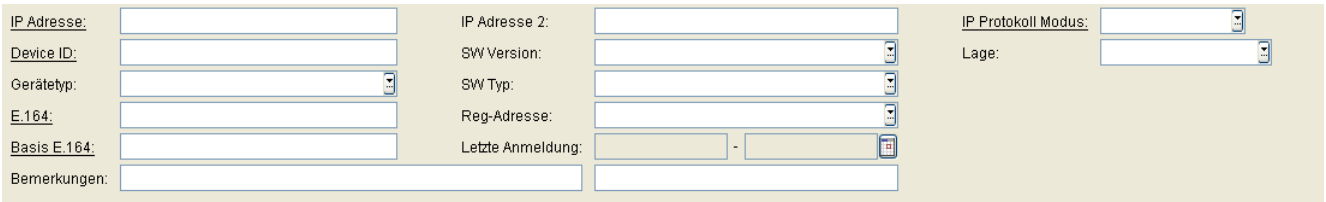
Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Inventar Daten

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Inventar Daten“
- Register „Information“
- Register „Accounting“
- Register „Pings“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Devices zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Devices angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des Workpoints. Für OpenStage wird hier entweder eine IPv4 oder eine IPv6-Adresse angezeigt. Siehe auch Parameter **IP Protokoll Modus**.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device. Bei IP Phones ist das in der Regel die MAC-Adresse.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Devices.

Alle vom DLS unterstützte Workpoint-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **optiPoint 410 standard**

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

Nur für OpenStage verfügbar.

SW Version:

Software-Version des Workpoints.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des Workpoints.

Beispiele: **Unify HFA**, **Unify SIP**

Lage:

Lage der Gateway-Baugruppe (Steckplatz).

Reg-Adresse:

IP-Adresse des Gateways oder des Gatekeepers, an dem sich das IP Device registrieren muss. Bei HiPath 3000 ist das die Adresse der HG 1500, bei HiPath 4000 ist es die HG 3530 oder das STMI-Board.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Devices.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Inhaltsbereich”.

Bemerkungen:

Felder für allgemeine Informationen.

IP Protokoll Modus

Zeigt an, welche IP-Version das IP Phone verwendet. Werden beide Versionen verwendet, steht in IP Adresse die IPv4-Adresse und in IP Adresse 2 die IPv6-Adresse.

Nur für OpenStage verfügbar.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Startet einen Job zur Verteilung der Konfigurationsänderungen. Siehe hierzu Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”.

Verwerfen

Die in der Maske vorgenommenen Änderungen werden verworfen.

Datei exportieren

Die Inventar-Daten werden im CSV-Format in eine Datei exportiert.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

Papierkorb leeren

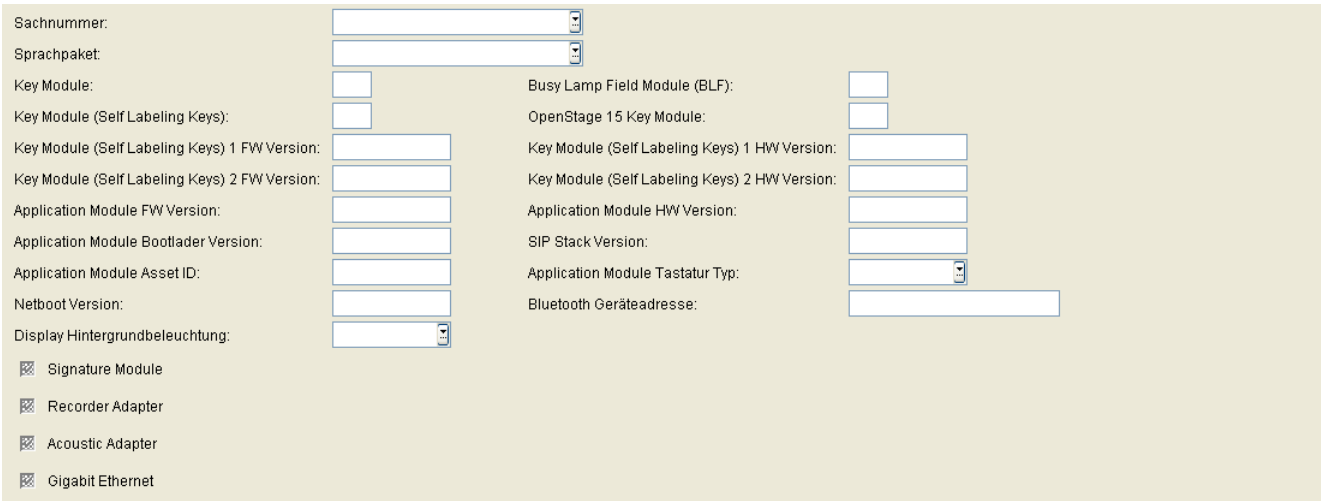
Löscht alle IP Devices, die zum Löschen markiert sind, vollständig aus dem DLS.

IP Device wiederherstellen

Das IP Device wird dem Papierkorb entnommen und kann über DLS wieder bearbeitet werden.

7.5.1.1 Register „Inventar Daten“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Inventar Daten > Register „Inventar Daten“



Sachnummer:

Sachnummer des IP Devices, die eine Identifizierung der entsprechenden Hardware ermöglicht.

Der Wert ist nur lesbar.

Sprachpaket:

Name des Installierten Sprachpakets.

Der Wert ist nur lesbar.

Key Module:

Anzahl der angeschlossenen Tastenmodule mit Self Labeling Keys.

Der Wert ist nur lesbar.

Key Module (Self Labeling Keys):

Anzahl der angeschlossenen Tastenmodule mit Self Labeling Keys.

Der Wert ist nur lesbar.

Key Module (Self Labeling Keys) 1 FW Version:

Firmware-Version des ersten Tastenmoduls mit Self Labeling Keys.

Der Wert ist nur lesbar.

Key Module (Self Labeling Keys) 2 FW Version:

Firmware-Version des zweiten Tastenmoduls mit Self Labeling Keys.

Der Wert ist nur lesbar.

Application Module FW Version:

Firmware-Version des optiPoint Application Module.

Der Wert ist nur lesbar.

Application Module Bootlader Version:

Bootloader-Version des optiPoint Application Module.

Der Wert ist nur lesbar.

Application Module Asset ID:

Mit der Asset-ID kann ein optiPoint Application Module eindeutig identifiziert werden.

Codierung:

Byte 1	Byte 2	Byte 3	Byte 4
yyyywwww	wwdddlll	aassssss	ssssttt

Erklärung:

Abschnitt	**Länge**	**Bedeutung**	**Beispiel**
yyyy	4 Bit	Letzte Stelle des Jahres	0001 = 2001
w...w	6 Bit	Kalenderwoche des Jahres	000001 = 1. Woche
ddd	3 Bit	Tag	001 = Montag, 111 = Sonntag
lll	3 Bit	Design Line	000 = Unify, else : reserviert
aa	2 Bit	Tester Group	0 - 3 , vom Werk verwaltet
s...s	11 Bit	Seriennummer	0 ... 2047
ttt	3 Bit	Tester Number	0,1 ... 6,7

Der Wert ist nur lesbar.

Netboot Version:

Version des Netboot.

Der Wert ist nur lesbar.

Display Hintergrundbeleuchtung

Zeigt die Art der Hintergrundbeleuchtung an.

Mögliche Optionen:

- **Standard**
- **CCFL**
- **LED**

Signature Module

Aktiv, wenn ein optiPoint signature module angeschlossen ist.

Der Wert ist nur lesbar.

Recorder Adapter

Aktiv, wenn ein optiPoint recorder adapter angeschlossen ist.

Der Wert ist nur lesbar.

Acoustic Adapter

Aktiv, wenn ein optiPoint acoustic adapter angeschlossen ist.

Der Wert ist nur lesbar.

Gigabit Ethernet

Zeigt an, ob das Gerät eine Gigabit-LAN-Schnittstelle besitzt.

Busy Lamp Field (BLF):

Anzahl der angeschlossenen BLFs.

Der Wert ist nur lesbar.

OpenStage 15 Key Module:

Anzahl der OpenStage 15 Key Module.

Key Module (Self Labeling Keys) 1 HW Version:

Hardware-Version des ersten Tastenmoduls mit Self Labeling Keys.

Der Wert ist nur lesbar.

Key Module (Self Labeling Keys) 2 HW Version:

Hardware-Version des zweiten Tastenmoduls mit Self Labeling Keys.

Der Wert ist nur lesbar.

Application Module HW Version:

Hardware-Version des optiPoint Application Module.

Der Wert ist nur lesbar.

SIP Stack Version:

Version des SIP-Stack.

Der Wert ist nur lesbar.

Application Module Tastatur Typ:

Layout der Tastatur des angeschlossenen optiPoint Application Module.

Mögliche Optionen:

- **QWERTZ**
  (deutsches Layout)

- **QWERTY**
  (amerikanische Layout)

Der Wert ist nur lesbar.

Bluetooth Geräteadresse

Bluetooth-Adresse des Gerätes.

7.5.1.2 Register „Information“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Inventar Daten > Register „Information“

Info 1 ... Info 10:

In diesen Feldern kann zusätzliche Information zum IP Device abgelegt werden, wie z. B. Abrechnungsdaten usw. Diese Informationen werden lediglich in der DLS-Datenbank hinterlegt. Es erfolgt keine Administration am IP Device.

7.5.1.3 Register „Accounting“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Inventar Daten > Register „Accounting“

Department:

Abteilung des zugehörigen Business Group-Teilnehmers.

Accounting ID:

Accounting ID des Teilnehmers.

Accounting ID des Standard-Teilnehmers (Teilnehmerkennung/Nebenstellennummer).

Retailer ID:

Retailer ID des Teilnehmers.

Retailer ID des Standard-Teilnehmers (Teilnehmerkennung/Nebenstellennummer).

Billing ID:

Billing ID des Teilnehmers.

Billing ID des Standard-Teilnehmers (Teilnehmerkennung/Nebenstellennummer).

7.5.1.4 Register „Pings“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Inventar Daten > Register „Pings“

Zum Thema PING siehe auch Abschnitt 7.4.5, “IP Devices pingen”.

Letzter erfolgreicher Ping

Anzeige des letzten erfolgreichen PINGs.

Der Wert ist nur lesbar.

Anzahl unbeantwortete Pings

Gesamte Anzahl der erfolglos durchgeführten PINGs.

Der Wert ist nur lesbar.

7.5.2 Papierkorb

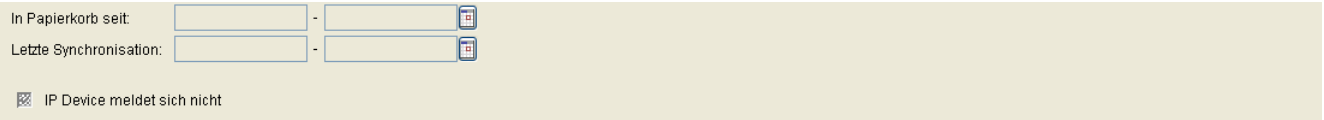
Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Papierkorb

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Information“

7.5.2.1 Register „Information“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > Papierkorb > Register „Information“



In Papierkorb seit

Datum, an dem das IP Device in Papierkorb geworfen wurde.

Letzte Synchronisation:

Datum der letzten Element Manager-Synchronisation für diese E.164-Nummer.

IP Device meldet sich nicht

Der Schalter wird gesetzt, wenn das IP Device sich im Papierkorb befindet, weil es sich auf PING nicht gemeldet hat.

7.5.3 IP Infrastruktur

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Infrastruktur

Diese Maske zeigt dem Benutzer die von einer Applikation an den DLS gesandten Daten zur IP-Infrastruktur. Die Infrastruktur Policy wird für automatische Anpassungen verwendet, wobei nach dem Standard-Device Profil gesucht wird, das demjenigen Standort zugeordnet ist, für den auch diese Infrastruktur Policy eingerichtet ist. Dieses Profil wird dann dem IP Phone zugeordnet.

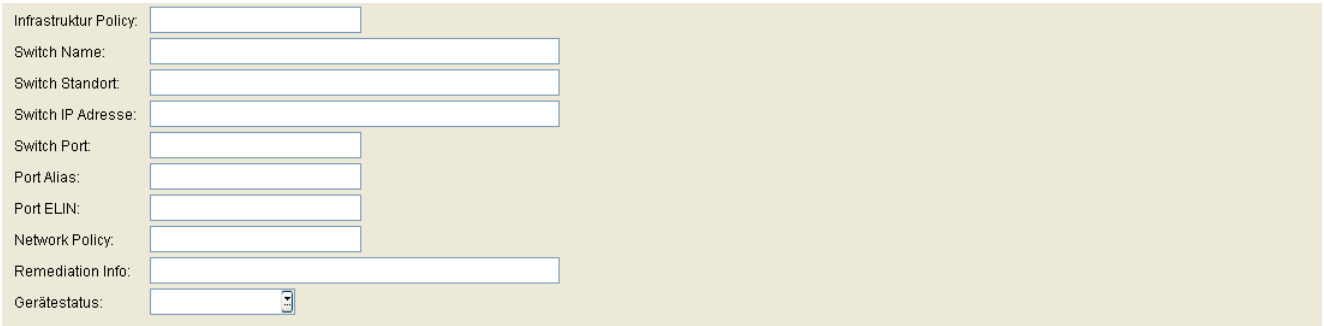
Die Zuordnung einer Infrastruktur Policy erfolgt über Switch IP Adresse, Switch Port und Network Policy. Die Infrastruktur Policy wird nicht über die API Schnittstelle versorgt, sondern muss unter **Administration** > **Server Konfiguration** > **Infrastruktur Policy** eingerichtet werden.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „IP Switch Daten“

7.5.3.1 Register „IP Switch Daten“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Infrastruktur > Register „IP Switch Daten“



Infrastruktur Policy:

Aktuell aktivierte Richtlinie mit folgendem Mapping: **Switch IP Adresse**, **Switch Port** und **Network Policy**.

Switch Name

Name des Switches, an dem das Gerät zur Zeit eingesteckt ist.

Switch Standort

Standort des Switches, an dem das Gerät zur Zeit eingesteckt ist.

Switch IP Adresse

IP Adresse des Switches, an dem das Gerät zur Zeit eingesteckt ist.

Switch Port

Port des Switches, an dem das Gerät zur Zeit eingesteckt ist.

Port Alias

Port Alias

IP Devices

IP Device Verwaltung

Port ELIN

Port ELIN

Network Policy

Policy, die derzeit im Gerät aktiv ist.

Remediation Info

Beschreibung der Network Policy.

Gerätestatus

Verbindungsstatus des Gerätes

Mögliche Optionen:

- **eingesteckt**
- **nicht eingesteckt**
- **unbekannt**

7.5.4 IP Device Konfiguration

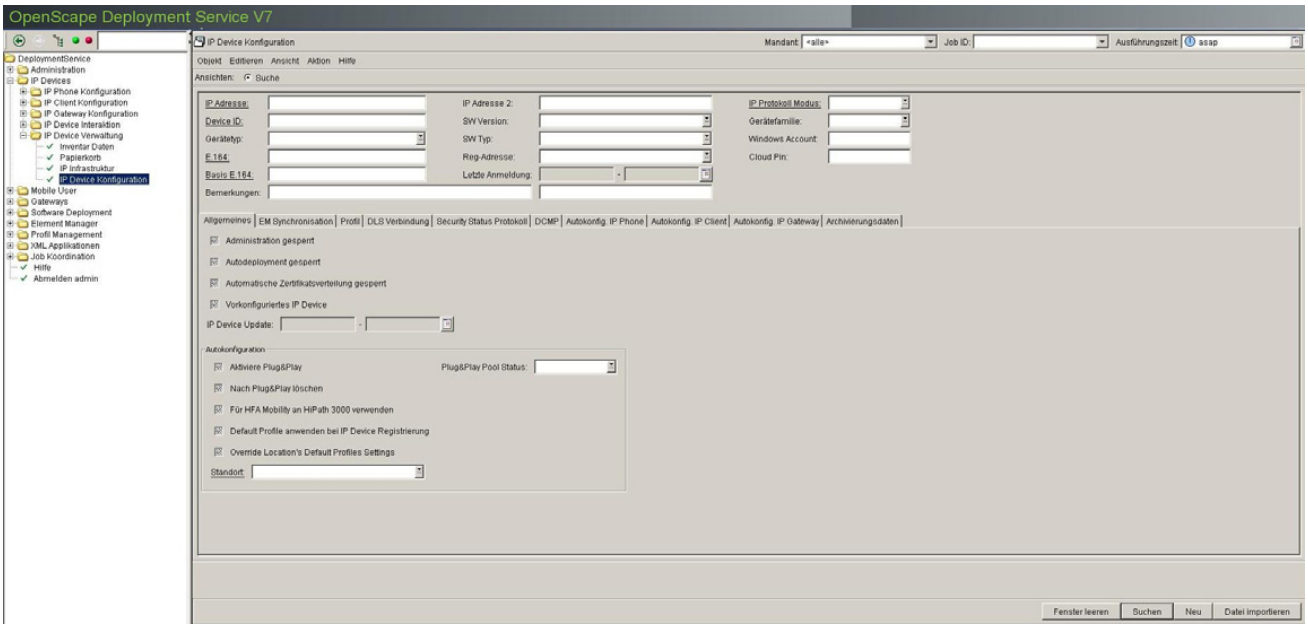
Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Allgemeines“
- Register „EM Synchronisation“
- Register „Profil“
- Register „DLS Verbindung“
- Register „Security Status Protokoll“
- Register „DCMP“
- Register „Autokonfig. IP Phone“
- Register „Autokonfig. IP Client“
- Register „Autokonfig. IP Gateway“
- Register „Archivierungsdaten“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Devices zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Devices angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des IP Devices.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Device. Bei IP Phones ist das in der Regel die MAC-Adresse.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Devices.

Alle vom DLS unterstützte IP Device-Typen finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiel: **optiPoint 410 standard**

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

Nur für OpenStage verfügbar.

SW Version:

Software-Version des IP Devices.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des IP Devices.

Beispiele: **Unify HFA**, **Unify SIP**

Reg-Adresse:

IP-Adresse des Gateways oder des Gatekeepers, an dem sich das IP Device registrieren muss. Bei HiPath 3000 ist das die Adresse der HG 1500, bei HiPath 4000 ist es die HG 3530 oder das STMI-Board.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Devices.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Inhaltsbereich”.

IP Protokoll Modus

Zeigt an, welche IP-Version das IP Phone verwendet. Werden beide Versionen verwendet, steht in IP Adresse die IPv4-Adresse und in IP Adresse 2 die IPv6-Adresse.

Nur für OpenStage verfügbar.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Optionen:

- **IP Phone**
- **IP Client**
- **IP Gateway**

Windows Account :

Jeweilige Domäne \ Windows-Account des Client. Wenn das Gerät ein Client ist, enthält das Feld einen Wert, ansonsten ist es leer.

Cloud-PIN:

Die Cloud-PIN-Zeichenfolge besteht nur aus Ziffern. Als Teil des Cloud-Bereitstellungsprozesses wird aus der vom Telefonbenutzer eingegebenen PIN ein Redirect-Code extrahiert.

Die Cloud-PIN ist ein neues optionales Element in allen Workpoint-Nachrichten, die für den Verbindungsaufbau mit DLS genutzt werden; DLS gibt dieser PIN bei der Geräteidentifikation Vorrang vor der E.164-Nummer. Der Wert der Cloud-PIN wird vom Telefon im SHA-256 Hash-Format übermittelt.

HINWEIS: Wenn der DLS das Telefon nicht alleine auf Basis des mac-addr-Attributs konfigurieren kann, wird zusätzlich der Cloud-PIN-Wert herangezogen. Wenn der DLS den Cloud-PIN-Wert eindeutig zuordnen kann, wird das Telefon ordnungsgemäß konfiguriert. Dabei wird ein neuer Wert für E.164 eingetragen (wenn eine entsprechende E.164-Rufnummer vom DLS ermittelt werden konnte). Wenn der Cloud-PIN-Wert nicht in den Inventardaten enthalten oder leer ist, zieht der DLS den E.164-Inventareintrag heran, um das Gerät zu identifizieren.

HINWEIS: In das Textfeld ‘Cloud Pin’ sollte dieselbe Zeichenfolge eingegeben werden, die dem Telefon nach Rücksetzung auf die Werkseinstellungen zugewiesen wurde. Die Cloud-PIN enthält den Redirect-Code; daher handelt es sich um eine längere Zeichenfolge.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Startet einen Job zur Verteilung der Konfigurationsänderungen. Siehe hierzu Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”.

Verwerfen

Die in der Maske vorgenommenen Änderungen werden verworfen.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

Neu

Erstellt eine neue Konfiguration.

Löschen

Löscht den Datensatz des aktuell ausgewählten IP Devices aus der DLS-Datenbank.

Datei exportieren

Die Konfigurations-Daten werden im CSV-Format in eine Datei exportiert.

Datei importieren

Konfigurations-Daten können aus einer Datei im CSV-Format importiert werden. Das Format ist unter Abschnitt 15.11, “Import und Export von Plug&Play-Daten” beschrieben.

IP Device kopieren

Daten eines IP Devices kopieren; siehe auch Kapitel Abschnitt 16.5, “Austausch eines IP Devices”, Abschnitt 16.7, “Austausch von HFA- durch SIP-Software und umgekehrt bei identischer Device ID”, Abschnitt 16.12.7, “IP Phone austauschen”.

Ausgewählte IP Devices in Archiv speichern

Ausgewählte IP Devices werden in ein .zip Archiv gespeichert.

IP Device aus Archiv laden

IP Devices werden aus einem .zip Archiv geladen.

Alle Templates generieren

Für alle Objekte bzw. Masken des ausgewählten IP Device-Typs werden Templates generiert

Plug&Play simulieren

Überprüft die Standort- und Default Profil-Konfiguration. Hierzu werden zunächst standortrelevante Daten eingegeben. Mit einem Klick auf Plug&Play simulieren kann dann kontrolliert werden, was an ein Phone geschickt werden würde, das sich mit diesen Daten beim DLS meldet.

7.5.4.1 Register „Allgemeines“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Allgemeines“

Administration gesperrt

Ist der Schalter aktiviert, so ist die Administration des IP Devices per DLS gesperrt. Die vorübergehende Sperre dient zur Vermeidung versehentlicher Einstellungsänderungen am IP Device.

Autodeployment gesperrt

Ist der Schalter aktiviert, so wird das Autodeployment (siehe Abschnitt 15.6.2, “Automatisches Deployment”) für das IP Device gesperrt.

Automatische Zertifikatsverteilung gesperrt

Ist der Schalter aktiviert, wird die automatische Zertifikatsverteilung (Abschnitt 6.11, “Automatische Zertifikatsverteilung”) für dieses IP Device gesperrt.

Vorkonfiguriertes IP Device

Ist der Schalter automatisch aktiviert, handelt es sich um ein vorkonfiguriertes IP Device.

IP Device Update:

Gibt an, wann der letzte IP Device-Update durchgeführt wurde.

Autokonfiguration

Aktiviere Plug&Play

Ist der Schalter aktiviert, werden bei der nächsten Registrierung alle Daten dieses Datensatzes dem IP Device zugewiesen.

Nach Plug&Play löschen

Ist der Schalter aktiviert, wird das virtuelle Gerät in das reale, registrierte Gerät umgewandelt. Somit existiert das virtuelle Gerät nach erfolgtem Plug&Play nicht mehr. Andernfalls wird der Datensatz kopiert, und das virtuelle Gerät bleibt erhalten.

Für HFA Mobility an HiPath 3000 verwenden

Ist dieser Schalter aktiviert, wird dieser Datensatz zur Übertragung der Gateway-Registrierungsdaten für HFA Mobility an HiPath 3000 verwendet.

Default Profile anwenden bei IP Device Registrierung

Ist der Schalter aktiviert, werden bei jeder Registrierung die in **Profil Management** > **Geräteprofil** für einen bestimmten Standort definierten Default-Profile ermittelt und angewendet. (Zur Bedeutung und Konfiguration des Standorts siehe Abschnitt 6.3.2, “Standort”.)

Override Location’s Default Profiles Settings

Ist der Schalter aktiviert, ist die Option „Default Profile anwenden bei IP Device Registrierung“ ausgegraut und steht daher nicht zur Verfügung.

Dieser Schalter ist standardmäßig deaktiviert.

Standort

Aktueller Standort des IP Device. der bei der Registrierung ermittelt und hier angezeigt wird. (Zur Bedeutung und Konfiguration des Standorts siehe Abschnitt 6.3.2, “Standort”.)

Plug&Play Pool Status

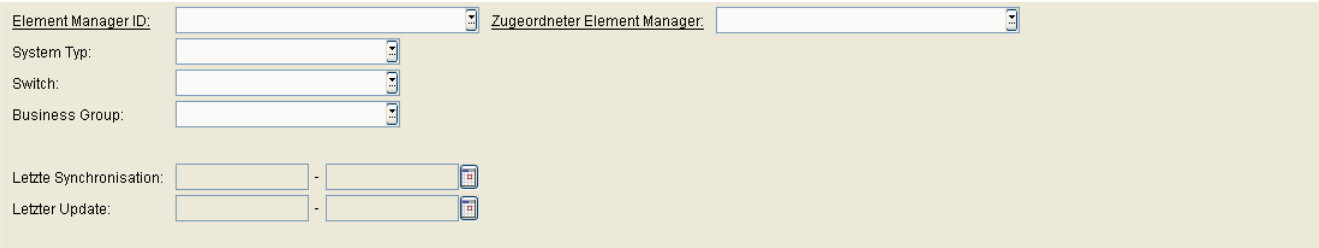
Zeigt an, ob dieser Datensatz für automatische Rufnummernvergabe bei Plug&Play verwendet wird oder nicht.

Mögliche Optionen:

- **kein**
- **frei**
- **in Verwendung**
- **Mehrfachverwendung**

7.5.4.2 Register „EM Synchronisation“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „EM Synchronisation“



Element Manager ID:

ID des Element Managers, der dem IP Device zugeordnet ist.

System Typ:

Typ des Element Managers, der dem IP Device zugeordnet ist.

Mögliche Werte:

- **HiPath 4000**
- **HiPath DXWeb Pro**
- **HiPath 3000/5000**
- **Andere**
- **OpenScape Voice**
- **Importierte Daten**
- **OpenOffice EE**
- **OpenScape Office MX/LX**

Switch:

Name des Switches (Nur für OpenScape Voice Assistant mit Multiple Switch Support).

Business Group:

Name der Business Group (Nur für OpenScape Voice Assistant).

Zugeordneter Element Manager

Ist hier ein Element Manager eingetragen, wird bei der EM-Synchronisation der Datensatz nur dann geändert, wenn die Daten vom hier spezifizierten Element Manager kommen. Siehe hierzu Abschnitt 15.2, “Änderung der Element Manager-Konfiguration und Joberzeugung”.

Letzte Synchronisation:

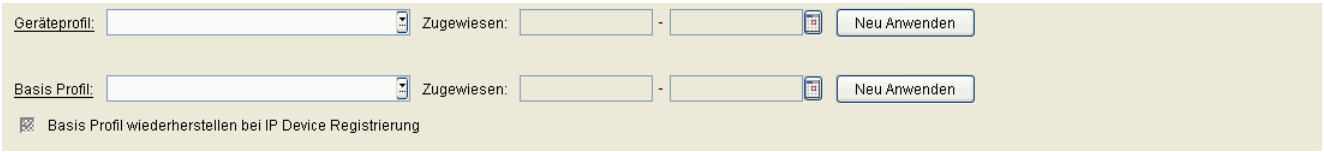
Zeitpunkt der letzten Synchronisation mit der Anlage.

Letzter Update:

Zeitpunkt der letzten Änderung dieser Einstellungen.

7.5.4.3 Register „Profil“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Profil“



HINWEIS: Das Register „Profil“ enthält die Informationen des zuletzt verteilten Profils. Es enthält keine Informationen zum Teilnehmerdatensatz und verknüpft diesen auch nicht mit dem zugewiesenen Profil, da die Profilparameter nur einmal propagiert werden. Wenn ein Administrator den Namen (oder den Inhalt) eines Profil ändert, wird die Änderung in diesem Bereich der Bedienoberfläche angezeigt. Der Name verweist immer noch auf das zuletzt verteilte Profil und nicht auf den neuen anpassbaren Profilnamen.

HINWEIS: Da nach der Erstverteilung des Profils keine direkte Verknüpfung besteht, erfordert die Verwendung dieser Felder als Suchkriterien durch Administratoren zunächst eine manuelle Überprüfung auf Konfigurationsänderungen, da nachträgliche Änderungen möglicherweise nicht mehr angezeigt werden. Das Profil Management von DLS gibt nur dann eine Benachrichtigung an der Benutzeroberfläche aus, wenn Profildaten geändert wurden und die entsprechenden Profile bereits Teilnehmern zugewiesen sind und die Änderungen erst dann wirksam werden, wenn ein Profil neu zugewiesen wird.

Geräteprofil:

Auswahl einer in **Profil Management > Geräteprofil** definierten Standard-Gerätekonfiguration, die zum IP Device gesendet werden soll. Dabei werden alle im Profil vorhandenen Parameter gesetzt; zuvor gesetzte Werte werden gegebenenfalls überschrieben. Solche Parameter, die nicht durch das Profil gesetzt werden, behalten ihre Werte bei.

HINWEIS: Wenn Sie unter **IP Device Konfiguration** einem virtuellen Device ein Profil zuweisen, wird Ihnen eine gefilterte Profilliste angeboten, die den auf dem Register „Unterstützte Geräte“ angezeigten Profilen entspricht.

Zugewiesen:

Zeitpunkt, an dem das Geräteprofil dem IP Device zuletzt zugewiesen wurde.

Neu Anwenden:

Geräteprofil erneut auf das IP Device anwenden.

Basis Profil:

Auswahl einer in **Profil Management > User Data Profile** definierten Standard-Userkonfiguration, die zum IP Device gesendet werden soll. Dabei werden alle Parameter neu gesetzt. Diejenigen Parameter, die nicht durch das Profil gesetzt werden, erhalten Default-Werte.

Zugewiesen:

Zeitpunkt, an dem das **Basis Profil** dem IP Device zuletzt zugewiesen wurde.

Neu Anwenden:

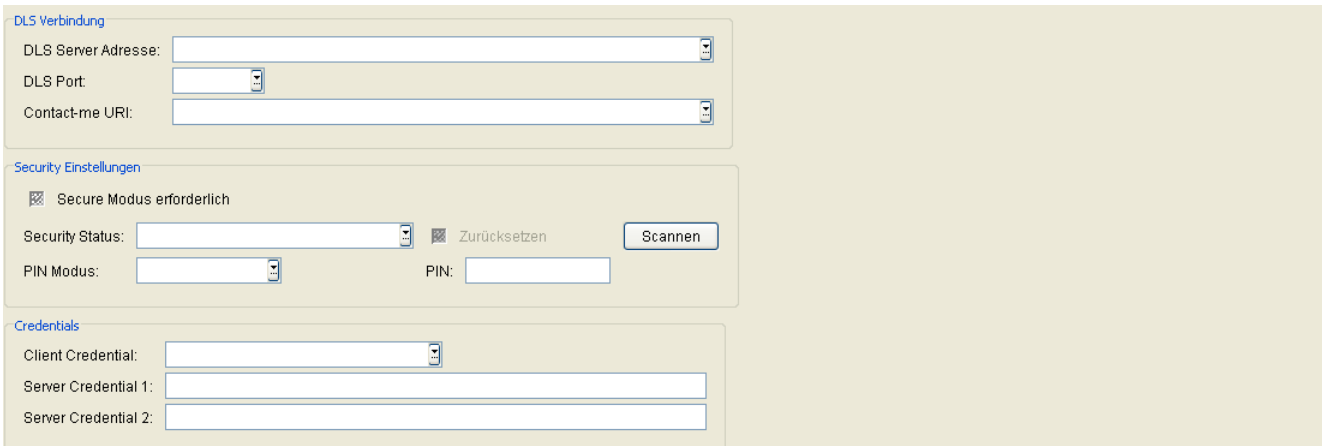
Basis Profil neu auf das IP Device anwenden.

Basis Profil wiederherstellen bei IP Device Registrierung

Ist dieser Schalter aktiv, wird dem IP Device bei der Registrierung das ausgewählte **Basis Profil** zugewiesen.

7.5.4.4 Register „DLS Verbindung“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „DLS Verbindung“



DLS Verbindung

DLS Server Adresse:

IP-Adresse oder Host-Name des DLS-Servers. Ist ein DHCP-Server vorhanden und entsprechend konfiguriert (siehe Abschnitt 4.12.4.3, “DHCP-Server für DLS konfigurieren”), wird dieser Wert automatisch im IP Device eingetragen.

DLS Port:

Portnummer des DLS-Servers. Ist ein DHCP-Server vorhanden und entsprechend konfiguriert (siehe Abschnitt 4.12.4.3, “DHCP-Server für DLS konfigurieren”), wird dieser Wert automatisch im IP Device eingetragen.

Standard: **18443**

Contact-me URI:

Dieses Feld dient der Anzeige und enthält die vollständige URL, die das IP Device für den Verbindungsaufbau zum DLS benutzt.

Security Einstellungen

Secure Modus erforderlich

Ist der Schalter aktiviert, wird die wechselseitige Authentifizierung von DLS und IP Device aktiviert. Der Authentifizierungsprozess (Bootstrap) wird angestoßen, sobald sich das IP Device das nächste Mal beim DLS meldet bzw. vom DLS gescannt wird.

Security Status:

Gibt den Sicherheitsmodus der Kommunikation zwischen DLS und IP Device an.

Mögliche Optionen:

- **Standard**
  In diesem Modus authentisiert sich das DLS mit einem Standardzertifikat, das für alle DLS-Installationen gleich ist.
- **Unsicher**
  Sobald der Schalter „Secure Modus erforderlich“ aktiviert ist, gilt der bisher als „Standard“ bezeichnete Modus als unsicher.
- **Sicher**
  Dieser Status wird angezeigt, wenn sich DLS und IP Device wechselseitig authentifiziert haben.
- **Schwebend**
  Die Credentials wurden an das Gerät übermittelt, das Gerät hat geantwortet, aber der Aufbau einer sicheren Verbindung zwischen DLS und Gerät ist noch nicht abgeschlossen.
- **Berechtigung übermittelt**
  Die Credentials wurden an das Gerät übermittelt, aber das Gerät hat noch nicht geantwortet.
- **Berechtigung verweigert**
  Das Device verweigert eine sichere Authentisierung (z. B. weil es dazu technisch nicht in der Lage ist).
- **Falsche TAN**
  Im PIN Modus Standard PIN oder individuelle PIN verifiziert sowohl das Device als auch DLS einen Teil der PIN. Schlägt die Verifikation auf Seiten des DLS mehr als die erlaubte Anzahl von Fehlversuchen für die PIN fehl, so wird der Sicherheitsstatus auf „Falsche TAN“ gesetzt.
- **Blockiert**
  Dieser Security Status wird derzeit noch nicht genutzt.
- **zurück zu Standard**
  Security Status wurde auf Standard zurückgesetzt, vom IP Device aber noch nicht bestätigt.

PIN Modus:

Mögliche Optionen:

- **Keine PIN**
  Die Zugangsdaten werden unverschlüsselt an das IP Device gesendet.
- **Standard PIN**
  Es wird eine für mehrere IP Devices definierte Standard-PIN benutzt. Diese wird automatisch vom DLS generiert (siehe Abschnitt 6.9.1, “Register „Secure Modus“”).

- **Individuelle PIN**
  Für das ausgewählte IP Device wird eine individuelle PIN erzeugt.
- **Unbekannt**
  Dieser PIN-Modus kann nur bei der **Suche** im DLS ausgewählt werden. Nach einem Umzug des DLS auf einen anderen Server kann der PIN-Modus nicht mehr reproduziert werden. Er wird dann automatisch auf „Unbekannt“ gesetzt. Dies führt aber zu keiner Funktionseinschränkung.

Zurücksetzen

Ist der Schalter aktiviert, kann der Security Modus durch Betätigen der Aktionsschaltfläche **Sichern** auf „Unsicher“ zurückgesetzt werden. Daraufhin muss der DLS eine neue Security-Konfiguration an das IP Device senden, d. h. es wird ein erneutes Bootstrapping durchgeführt (siehe auch **Secure Modus erforderlich**).

PIN:

Wird lokal am IP Device eingegeben und dient zur Entschlüsselung der vom DLS gesendeten Zugangsdaten, die zum Übertritt in den Secure Modus erforderlich sind. Standardmäßig erfolgt am Endgerät eine Aufforderung zur Eingabe der PIN. Alternativ zur Eingabe auf Aufforderung kann die PIN im lokalen Administrationsmenü vorkonfiguriert werden.

Scannen

Startet den Scan nach IP-Geräten (nur mit Gerätefamilie - IP Gateway). Während des Scanvorgangs läuft der Bootstrapping-Prozess. Bootstrapping ist der Prozess, bei dem die Sicherheitsstufe der Schnittstelle zwischen einem IP Device und dem DLS vom Default Modus auf den Secure Modus angehoben wird.

> ***HINWEIS:*** Wenn Sie bei Nicht-IP-Gateway-Geräten (d. h. IP Phone und IP Client) auf „Scannen“ klicken, erhalten Sie die folgende Fehlermeldung: „1355: Server is not able to create a job: Device is not a IP Gateway“.

Credentials

Client Credential

Mit diesem Credential authentisiert sich das Gerät beim DLS.

Mögliche Optionen:

- **Aktiv**
  Das Gerät hat sich zuletzt mit dem aktiven Client Credential authentisiert.

- **Veraltet**
  Das Gerät hat sich zuletzt mit einem veralteten Client Credential gemeldet.
- **Unbekannt**
  Im DLS ist derzeit nicht bekannt, ob das Gerät das aktive, ein veraltetes oder ein ungültiges Client Credential besitzt (z. B. nachdem ein neues Client Credential erzeugt oder Client Credentials importiert wurden).
- **Abgewiesen**
  Das Device hat zuletzt versucht, sich mit einem ungültigen Client Credential zu authentisieren.

Server Credential 1

Fingerabdruck des Trust Anchors für Credential 1; wir auf dem IP Device bereitgestellt und für die Authentifizierung des DLS verwendet.

Server Credential 2

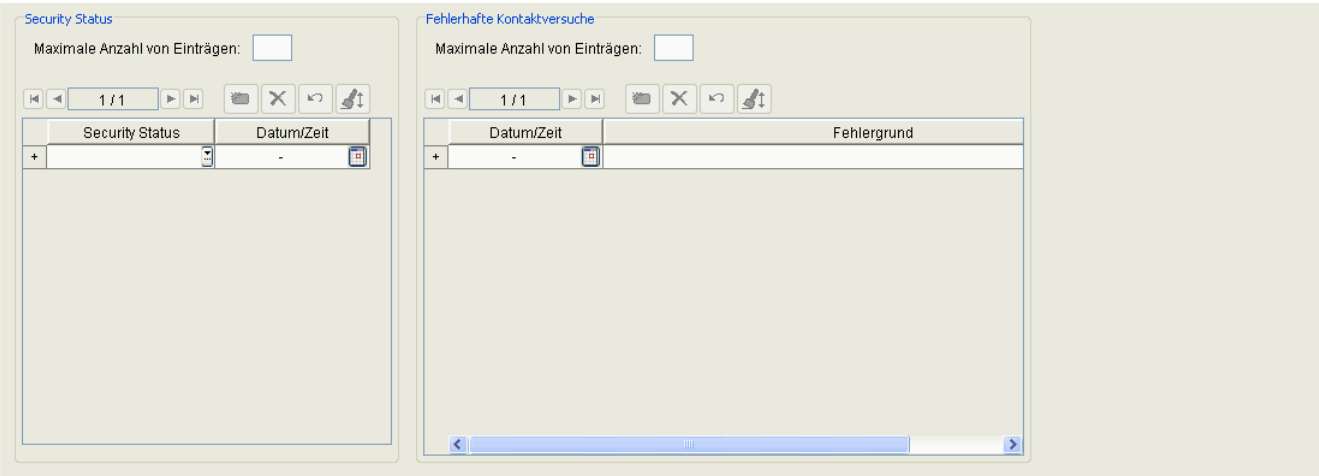
Fingerabdruck des Trust Anchors für Credential 2; wir auf dem IP Device bereitgestellt und für die Authentifizierung des DLS verwendet.

> ***HINWEIS:*** Jeder DLS, der sich entweder über Credential 1 oder Credential 2 authentifiziert, wird vom IP Device akzeptiert.

7.5.4.5 Register „Security Status Protokoll“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Security Status Protokoll“

Hier werden die Änderungen des Security Modus für das ausgewählte IP Device protokolliert.



Security Status

Maximale Anzahl von Einträgen

Maximale Anzahl von Einträgen in der Protokolldatei ‚Security Status’.

Security Status

Zeigt den Security-Status des IP Devices zu einem bestimmten Zeitpunkt an.

Datum/Zeit

Zeigt an, zu welchem Zeitpunkt sich das IP Device in einem bestimmten Security-Status befunden hat.

Fehlerhafte Kontaktversuche

Maximale Anzahl von Einträgen

Maximale Anzahl von Einträgen in der Protokolldatei ‚Fehlerhafte Kontaktversuche’.

Wertebereich: **0** - **100** für Devices im Default Modus, **1** - **100** für Devices im Secure Modus.

Datum/Zeit

Zeitpunkt des Kontaktversuches.

Fehlergrund

Fehlermeldung.

Mögliche Meldungen:

Fehlergrund	Beschreibung
DLS internal authentication failure (no transition)	Während des Bootstrapping erkannte der DLS eine unbekannte Meldungsabfolge (z. B. eine unerwartete Meldung, abweichend zu der erwarteten) und beendete den Kontaktversuch aus Sicherheitsgründen.
Workpoint with given id could not be found.	Das IP Device ist im DLS unbekannt. Möglicherweise ein DLS-interner Fehler (Datenbank oder Konfigurationsproblem).
Encountered invalid PIN	Die Bootstrapping-PIN enthält unzulässige Zeichen oder überschreitet die definierte Länge.
TAN Verification can only be performed if TAN is required.	Das IP Device hat eine TAN gesendet, die derzeitige Konfiguration verlangt aber keine und so kann die TAN nicht verifiziert werden.
Verification of DlsObjWorkpointBase failed.	DLS interner Fehler.
Error while updating DlsObjWorkpointBase.	DLS interner Fehler.
Invalid security state.	Der Meldungsverkehr entspricht nicht dem derzeitigen Security Status im DLS (z. B. falsche Meldungsabfolge, geänderte Konfiguration oder Fehler).
Invalid security transition.	Der Meldungsverkehr entspricht nicht dem derzeitigen Security Status im DLS (z. B. falsche Meldungsabfolge, geänderte Konfiguration oder Fehler).
Error while generating new client certificate.	DLS-interner Fehler während des Erzeugen und Verteilen eines neuen Client-Zertikates.
Fatal server error. See log file for additional information.	DLS interner fataler Server Fehler. **Behebung:** Weitere Informationen finden Sie unter `..\DeploymentService\Tomcat5\webapps\DeploymentService\log\dlslog.txt`
An active dls server ca could not be found.	DLS-interner Fehler wegen eines fehlenden CA-Zertifikats.
Active server ca is corrupt.	DLS-interner Fehler wegen eines falschen oder zerstörten CA-Zertifikats.
An additional dls server ca could not be found.	DLS-interner Fehler wegen eines fehlenden zusätzlichen zweiten CA-Zertifikats.
An additional dls server ca already exists.	DLS-interner Konfigurationsfehler.

Fehlergrund	Beschreibung
Additional server ca is corrupt.	DLS-interner Fehler wegen eines falschen oder zerstörten zweiten CA-Zertifikats.
An item with name mac-addr is missing in item list.	IP Device-Meldung enthält keine Device ID (Attributname: mac-addr).
AES encoding failed due to an internal error.	Auswertung der Meldung mittels AES scheiterte wegen eines DLS-internen Fehlers.
Client must provide a certificate.	Das IP Device muss ein Client Zertifikat liefern.
Client certificate with invalid signature.	Das IP Device lieferte ein ungültiges oder zerstörtes Zertifikat.
Client certificate invalid.	Das IP Device-Zertifikat ist aus unbekannten Gründen ungültig (z. B. Abgelaufen, usw.).
Client ca not found or corrupt.	DLS-interner Fehler wegen eines fehlenden oder zerstörten Client CA Zertifikats.
DLS internal authentication failure.	DLS-interner Fehler wegen Problemen bei der Authentifikation (z. B. ungültiger oder zerstörter Zertifikatsschlüssel, internen Zertifikatsproblemen).
Export of CAs could not be performed.	DLS-interner Konfigurationsfehler: Export der CA Zertifikate konnte nicht durchgeführt werden.
Import of CAs could not be performed.	DLS-interner Konfigurationsfehler: Import der CA Zertifikate konnte nicht durchgeführt werden.
Client cert state is invalid.	DLS-interner Konfigurationsfehler: Der Status des Client-Zertifikats ist ungültig.
String is not a X509 PEM.	DLS-interner Konfigurationsfehler: Zeichen entsprechen nicht X509 PEM Regeln.
DCMP URI is not valid.	DLS-interner Konfigurationsfehler: DCMP URI ist ungültig.
Invalid dcmp state.	DLS-interner Konfigurationsfehler: DCMP Status ist ungültig.
Invalid dcmp transition.	DLS-interner Konfigurationsfehler: DCMP Übergang ist ungültig.
client certificate not accepted by device	Das IP Device hat das vom DLS gesandte neue Client Zertifikat nicht akzeptiert.
device is blocked	Jegliche Kommunikation mit diesem IP Device ist aus Sicherheitsgründen blockiert.
device must use secure port	Das IP Device muss den sicheren Port verwenden (z. B. 18444) und nicht den Standardport (z. B. 18443).
wrong TAN from device	Eine TAN wurde vom IP Device ein oder mehrmals angefordert, aber auch nach einer definierten Anzahl von Wiederholungen wurde keine gültige TAN gesandt. Aus Sicherheitsgründen wurde das IP Device blockiert.
No DLS license	Keine DLS-Lizenz vorhanden.
licenses exceeded	Die Anzahl der DLS Lizenzen wurde überschritten.
unexpected solicited message from workpoint	Eine (unbeabsichtigte) Anforderungsmeldung wurde vom IP Device zum DLS gesandt, dort aber nicht erwartet (Kein vorangegangenes contact-me vom DLS).

Fehlergrund	Beschreibung
empty items list but items expected	Meldungsliste ist leer, obwohl vom DLS mehrere Items erwartet werden.
timeout during read items	Zeitüberschreitung beim Lesen von einem IP Device.
synchronisation exception	DLS-interner Synchronisationsfehler.
missing e164	E.164 wurde vom DLS erwartet, vom IP Device aber nicht gesandt.
missing items	Die erwarteten Items sind nicht in der Meldungsliste enthalten.
try later	HFA Mobility Logoff.
mobility save disabled	HFA Mobility.

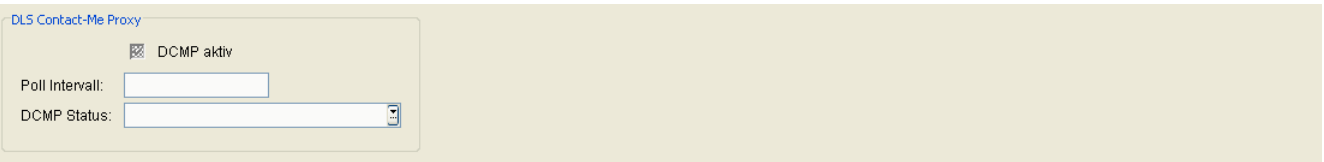
7.5.4.6 Register „DCMP“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „DCMP“

Der DLS-Contact-Me-Proxy (DCMP) kann über Firewall oder NAT (Network Address Translation) hinweg mit dem DLS kommunizieren und so ggf. zwischen Endgeräten und vor der Firewall liegendem DLS vermitteln. Die Endgeräte fragen den DCMP regelmäßig ab (Poll). Wenn Nachrichten vom DLS vorliegen, stellt der DCMP eine Verbindung zwischen Endgerät und DLS her.

Ein DCMP-Proxy kann einem bestimmten Standort und damit einem bestimmten IP-Adressbereich zugewiesen werden; siehe Abschnitt 6.9.2, “Register „DCMP“”.

Die Werte in dieser Maske werden nur angezeigt; sie können nicht verändert werden.



DLS Contact-Me Proxy

DCMP aktiv

Ist der Schalter aktiviert, benutzt das Endgerät den DCMP zur Kommunikation mit dem DLS und fragt diesen regelmäßig ab. Voraussetzung hierfür ist die globale Aktivierung des DCMP, siehe **Administration** > **Workpoint Interface Konfiguration** > **Register „DCMP“**.

Poll Intervall:

Legt das Zeitintervall fest, in dem das Endgerät den DCMP abfragt.

DCMP Status:

Gibt Auskunft über die Kommunikation zwischen Gerät und DCMP.

Mögliche Werte:

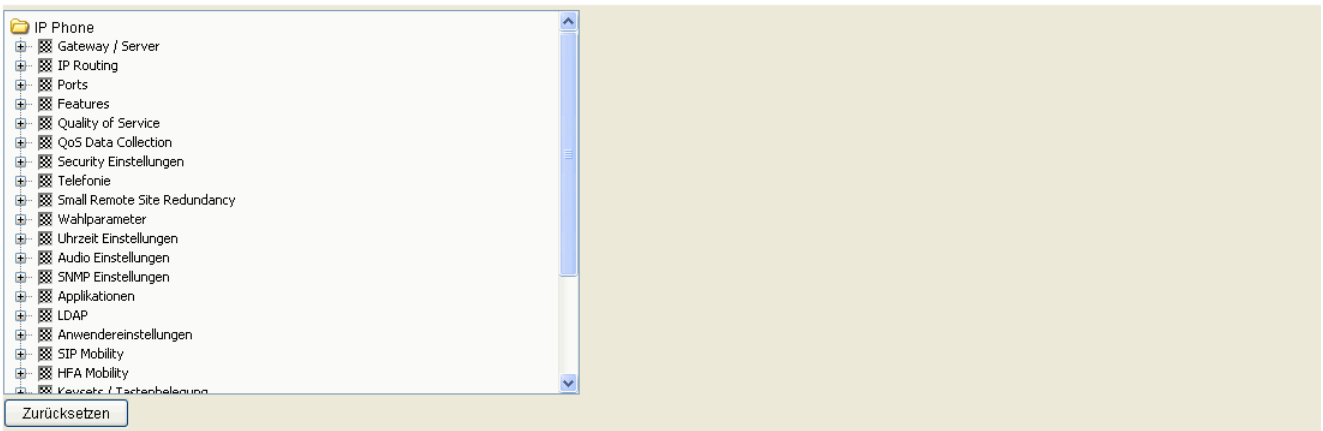
- **Aktiviert**
  Das Gerät läuft im DCMP-Modus, d. h. der DLS kontaktiert das Device via DCMP-Server.
- **Deaktiviert**
  Das Gerät läuft nicht im DCMP-Modus, d. h. der DLS kontaktiert das Device direkt.
- **Abgewiesen**
  Das Gerät verweigert den DCMP-Modus (z. B. wenn es technisch nicht in der Lage ist, im DCMP Modus zu arbeiten).

- **Veraltet**
  Die DCMP-Daten im DLS wurden geändert und müssen dem Gerät mitgeteilt werden.
- **Deaktivierung läuft**
  DCMP für dieses Gerät wurde im DLS deaktiviert und die geänderte Konfiguration muss dem Gerät mitgeteilt werden.

7.5.4.7 Register „Autokonfig. IP Phone“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Autokonfig. IP Phone“

Hier wird für noch nicht gesteckte Geräte (= virtuelle Geräte) gezeigt, welche Attribute bei der Autokonfiguration (Plug&Play) zum IP Device geschickt werden sollen. Die einzelnen Häkchen werden automatisch gesetzt, sobald ein Attribut direkt oder durch ein Profil konfiguriert ist. Es können aber auch einzelne Häkchen durch den Administrator gesetzt werden; in diesem Fall werden Default-Werte für den jeweils angehakten Parameter an das IP Device geschickt.



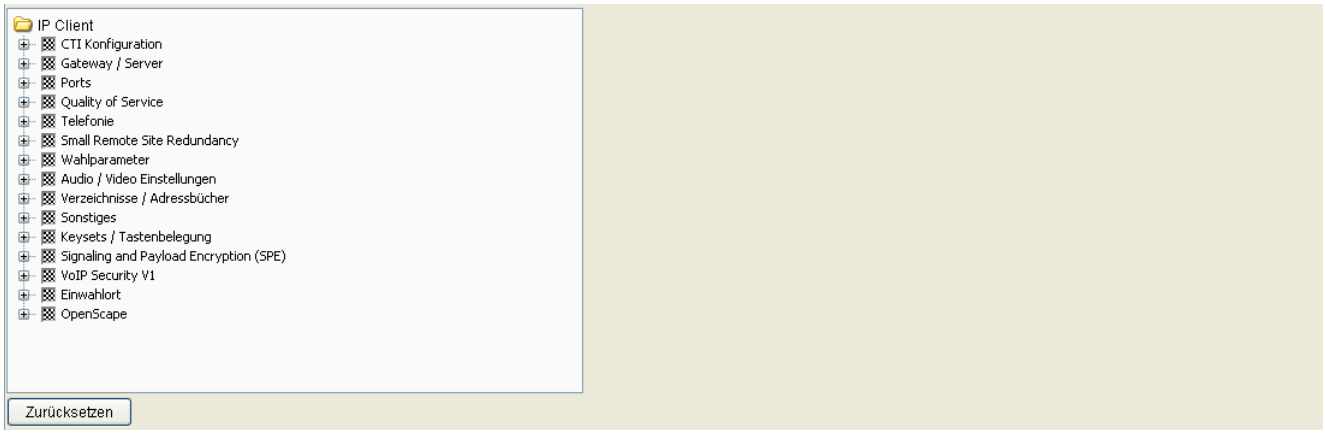
Zurücksetzen

Mit diesem Button können alle Felder auf nicht aktiv gesetzt werden.

7.5.4.8 Register „Autokonfig. IP Client“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Autokonfig. IP Client“

Hier wird für noch nicht angeschlossene IP Clients gezeigt, welche Attribute bei der Autokonfiguration (Plug&Play) zum IP Device geschickt werden sollen. Die einzelnen Häkchen werden automatisch gesetzt, sobald ein Attribut direkt oder durch ein Profil konfiguriert ist. Es können aber auch einzelne Häkchen durch den Administrator gesetzt werden; in diesem Fall werden Default-Werte für den jeweils angehakten Parameter an das IP Device geschickt.



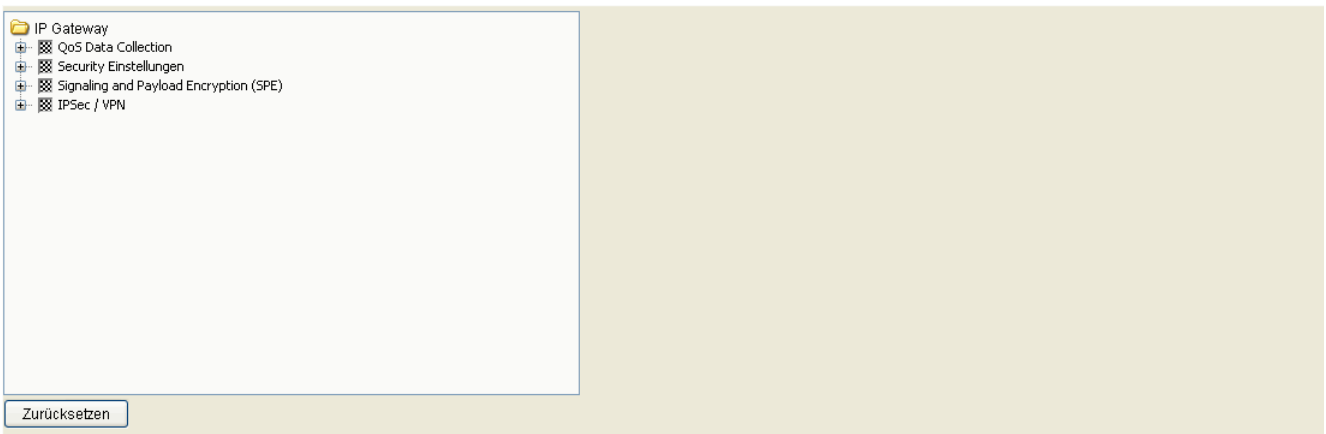
Zurücksetzen

Mit diesem Button können alle Felder auf nicht aktiv gesetzt werden.

7.5.4.9 Register „Autokonfig. IP Gateway“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Autokonfig. IP Gateway“

Hier wird für noch nicht angeschlossene IP Gateways gezeigt, welche Attribute bei der Autokonfiguration (Plug&Play) zum IP Device geschickt werden sollen. Die einzelnen Häkchen werden automatisch gesetzt, sobald ein Attribut direkt oder durch ein Profil konfiguriert ist. Es können aber auch einzelne Häkchen durch den Administrator gesetzt werden; in diesem Fall werden Default-Werte für den jeweils angehakten Parameter an das IP Device geschickt.

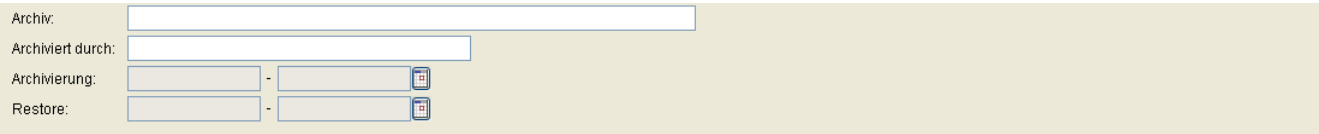


Zurücksetzen

Mit diesem Button können alle Felder auf nicht aktiv gesetzt werden.

7.5.4.10 Register „Archivierungsdaten“

Aufruf: Hauptmenü > IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Archivierungsdaten“



Archiv:

Pfad der ZIP-Archivdatei auf dem DLS-Rechner.

Archiviert durch

Name des DLS-Benutzers, der das Archiv erzeugt hat.

Archivierung

Datum und Uhrzeit der Archivierung.

Restore

Datum und Uhrzeit der Wiederherstellung aus dem Archiv.

8 Mobile User

Aufruf: Hauptmenü > Mobile User

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- SIP Mobile User Konfiguration
- SIP Mobile User Interaktion
- User Daten Administration
- Mobility Statistiken
- Mobility Statistiken Konfiguration

Nutzen Sie den Bereich **Mobile User**, um Parameter für Mobile User anzuzeigen und zu ändern. Eine Einführung zum Thema Mobility finden Sie im Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

WICHTIG: Werden Datenänderungen in IP Device-Konfigurationsmasken vorgenommen, die mithilfe von Templates erstellt wurden, so werden diese Änderungen nicht automatisch in diese Templates übernommen.
Zum Übernehmen müssen die Änderungen manuell im Template gesichert werden, siehe Abschnitt 15.4, “Templates bearbeiten”.

HINWEIS: Ein IP Device kann erst nach dessen erfolgreicher Registrierung am DLS konfiguriert werden. Zur Registrierung muss dem IP Device die entsprechende DLS-Adresse bekannt sein. Die Registrierung beim DLS erfolgt durch:

- Auslesen der IP Device-Daten durch den DLS, siehe Abschnitt 7.4.6, “IP Devices scannen” und durch
- Einstecken des LAN-Steckers bzw. der Stromversorgung am IP Device.

8.1 SIP Mobile User Konfiguration

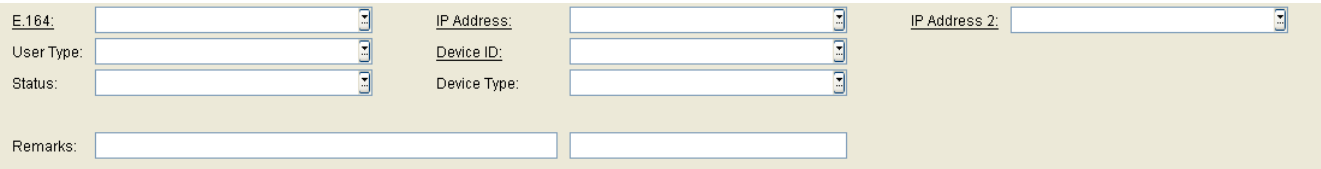
Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration

Dieses Menü besteht aus folgenden Untermenüs:

- Gateway / Server
- IP Routing
- Features
- Quality of Service
- Security Einstellungen
- Telefonie
- Wahlparameter
- Uhrzeit Einstellungen
- Audio Einstellungen
- Applikationen
- LDAP
- Anwendereinstellungen
- SIP Mobility
- Keysets / Tastenbelegung
- Signaling and Payload Encryption (SPE)
- Sonstiges

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Phones zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Phones angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

E.164:

Vollständige E.164-Rufnummer (Mobility ID oder Rufnummer von Basis-User).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Anwender Typ:

Zeigt an, um welche Art von Daten es sich handelt.

Mögliche Optionen:

- **Endgerät für Mobile User**
  Es sind Daten des Mobility Phones.
- **Mobil User**
  Es sind Daten des Mobile Users.

Weitere Informationen zum Thema Mobility siehe Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Status:

Zeigt den Mobility-Status an.

Mögliche Optionen:

- **Mobile User angemeldet**
  Bei Mobile User Daten: Es ist ein Mobile User angemeldet.
- **Mobile User abgemeldet**
  Bei Mobile User Daten: Es ist kein Mobile User angemeldet.

- **Endgerät verfügbar für Mobile User**
  Bei Daten zum Mobility Phone: Am Mobile User ist kein Mobility Phone angemeldet.
- **Endgerät belegt durch Mobile User**
  Bei Daten zum Mobility Phone: Am Mobile User ist ein Mobility Phone angemeldet.

Weitere Informationen zum Thema Mobility siehe Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

IP Adresse:

IP-Adresse des IP Phones.

Beispiel: **192.117.1.193**

An dieser Stelle kann der Wert nur gelesen werden.

Device ID:

Physikalische MAC-Adresse des IP Phones.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Phones.

Alle vom DLS unterstützten IP Phone-Typen finden Sie im Abschnitt 3.4, “Unterstützte IP Devices/Versionen”.

Beispiel: **optiPoint 410 standard**

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

An dieser Stelle kann der Wert nur gelesen werden.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Phones, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Startet einen Job zur Übertragung der Konfigurationsänderungen an das ausgewählte Objekt. Siehe hierzu Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”. In der Ansicht Templates weren die Parameter im jeweils ausgewählten Template gespeichert. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Verwerfen

Die eingetragenen Änderungen werden nicht an das ausgewählte Objekt übertragen und aus der Eingabemaske gelöscht.

Aktualisieren

Die Parameter werden erneut aus der Datenbank geladen.

Holen

Lädt ein bereits gesichertes Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Umbenennen

Ändert den Namen eines gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Löschen

Löscht ein gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

8.1.1 Gateway / Server

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Gateway / Server

Dieser Bereich besteht aus folgenden Inhalten:

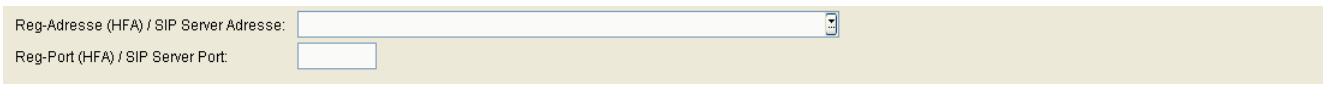
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Gateway (HFA) / SIP Server“
- Register „SIP Terminaleinstellungen“
- Register „SIP Registrierung 1“
- Register „SIP Registrierung 2“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.1.1 Register „Gateway (HFA) / SIP Server“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Gateway / Server > Register „Gateway (HFA) / SIP Server“



Reg-Adresse (HFA) / SIP Server Adresse:

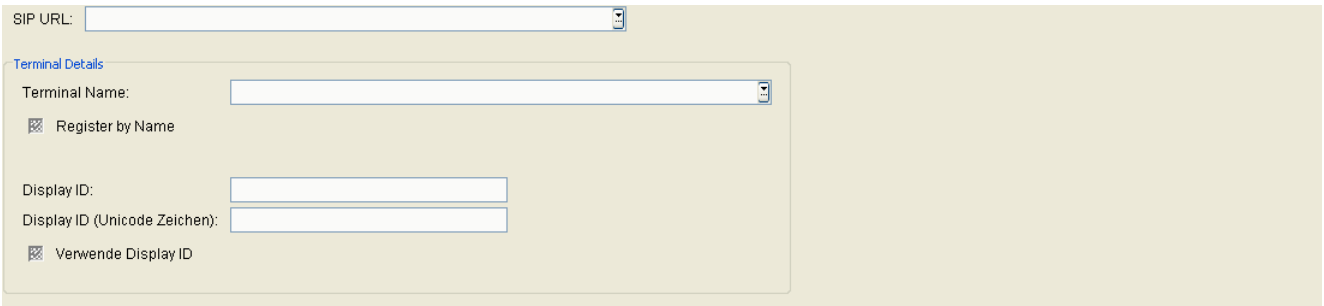
IP-Adresse oder Host-Name von PBX, Gateway bzw. SIP-Server, der zum Betrieb des IP Devices eingesetzt wird.

Reg-Port (HFA) / SIP Server Port:

Port, über den der Workpoint mit dem PBX, Gateway bzw. SIP-Server kommuniziert.

8.1.1.2 Register „SIP Terminaleinstellungen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Gateway / Server > Register „SIP Terminaleinstellungen“



SIP URL:

SIP-Adresse des IP Phones.

Format: **<SIP Benutzerkennung>@<Domain>**.

Terminal Details

Terminal Name:

Name des IP Phones, der als Synonym für die Rufnummer beim Registrieren verwendet wird.

Nur erforderlich, wenn der Schalter **Register by Name** aktiviert und der Registrar-Server entsprechend konfiguriert ist.

Register by Name

Schalter zum Aktivieren der Funktion, dass beim Registrieren Inhalt des Feldes **Terminal Name** mitgesendet wird.

Ist der Schalter nicht aktiv, wird beim Registrieren der Inhalt des Feldes **E.164 Nummer** mitgesendet.

Display ID:

Name des IP Phones, der im Display des Workpoints angezeigt wird.

Wertebereich: max. 24 alphanummerische Zeichen.

> ***HINWEIS:*** In Abschnitt 15.11.1, “Export von Plug&Play-Daten” finden Sie Hinweise zur Verwendung von Makrokommandos; ohne diese kann der DLS die Display ID nicht korrekt speichern.

Display ID (Unicode Zeichen):

Name des IP Phones in Unicode-Zeichen, der im Display des Workpoints angezeigt wird.

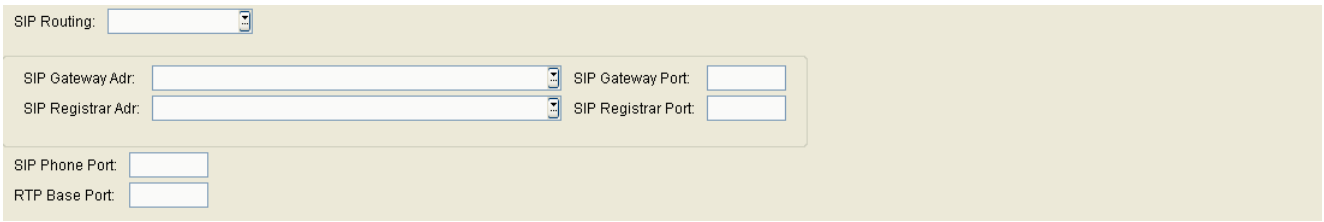
Diese Option wird nur von OpenStage-Geräten unterstützt.

Verwende Display ID

Ist der Schalter aktiviert, wird am Workpoint die Display-ID angezeigt.

8.1.1.3 Register „SIP Registrierung 1“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Gateway / Server > Register „SIP Registrierung 1“



SIP Routing:

Mögliche Optionen:

- **Gateway**
  Für das SIP-Routing wird ein Gateway verwendet.
- **Server**
  Für das SIP-Routing wird ein SIP-Proxy verwendet.
- **Direkt**

Wird **Direkt** oder **Gateway** gewählt, werden keine Registrierungs-Meldungen gesendet. Beim Routing-Modus **Server** werden Registrierungs-Meldungen an den Registrar-Server gesendet.

SIP Gateway Adr.:

IP-Adresse des Gateways. Dieser Parameter wird verwendet, wenn bei SIP Routing der Modus **Gateway** ausgewählt ist.

SIP Gateway Port:

Port-Nummer des Gateways. Dieser Parameter wird verwendet, wenn bei SIP Routing der Modus **Gateway** ausgewählt ist.

SIP Registrar Adr:

IP-Adresse des SIP-Registrars.

SIP Registrar Port:

Port-Nummer des SIP-Registrars.

SIP Phone Port:

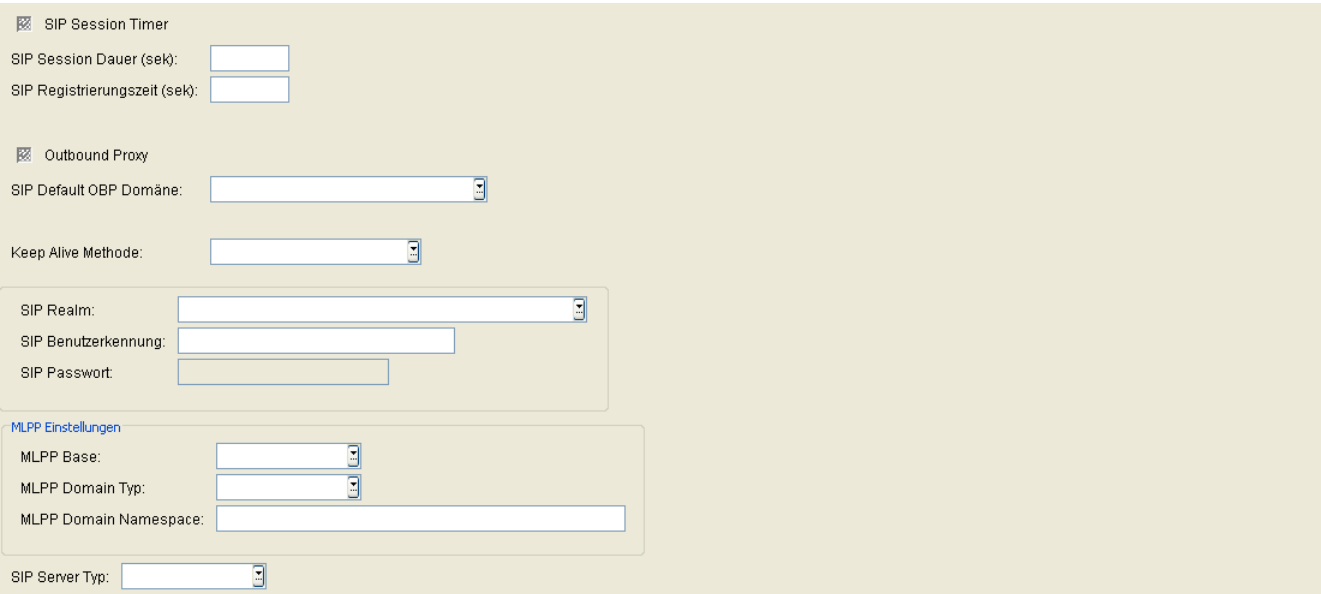
Port-Nummer des IP Phones.

RTP Base Port:

Basis Port-Nummer für den RTP-Transport.

8.1.1.4 Register „SIP Registrierung 2“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Gateway / Server > Register „SIP Registrierung 2“



SIP Session Timer

Schalter zum Aktivieren der SIP Session Timers. Mit dem Timer wird die Dauer einer SIP-Session überwacht.

SIP Session Dauer:

Höchstdauer in Sekunden für eine SIP-Session.

Wertebereich: **0** ... **3600** Sekunden.

SIP Registrierungszeit:

Zeitspanne einer Wiederanmeldung am SIP-Server. Eine Wiederanmeldung stellt sicher, dass das SIP-Telefon weiterhin am SIP-Server angemeldet bleibt. Dadurch können auch Probleme bei der Verbindung zum Server festgestellt werden.

Wertebereich: **0** ... **4320** Sekunden.

Standard: **0**

Outbound Proxy

Schalter zum Aktivieren eines SIP-Proxy bei abgehenden Gesprächen.

Zusammen mit **SIP Default OBP Domäne** steuert dieser Schalter das Routing-Verhalten abgehender Gespräche, abhängig von der gewählten Nummer oder Benutzerkennung.

Siehe hierzu Kapitel 17, “Outbound Proxy”.

SIP Default OBP Domäne:

Zusammen mit **Outbound Proxy** steuert dieser Eintrag das Routing-Verhalten ausgehender Gespräche, abhängig von der gewählten Nummer oder Benutzerkennung.

Siehe hierzu Kapitel 17, “Outbound Proxy”.

Keep Alive Methode:

Mögliche Optionen:

- **Sequenz**
- **CRLF**

SIP Realm:

SIP-Bereich, in dem der Workpoint betrieben wird. SIP Realm wird verwendet, um das Telefon am SIP-Server zu identifizieren.

SIP Benutzerkennung:

Die Benutzerkennung ist der erste Teil der SIP URL.

SIP Passwort:

Erforderliches Passwort für den Zugang zum SIP-Server.

MLPP Einstellungen

MLPP Base:

Mögliche Optionen:

- **Lokal**
- **Server**

MLPP Domain Typ

Legt fest, welcher Resource Priority Namespace von einer festen Liste akzeptiert wird.

Mögliche Optionen:

- **dsn**
  dsn-000000
- **uc**
  uc-000000
- **dsn+uc**
- **Andere Domain**

MLPP Domain Namespace

Definiert einen ASCII String für einen Single Resource Priority Namespace, der akzeptiert wird.

Erlaubt sind alphanumerische Zeichen und folgende Sonderzeichen: -!%*_+` “~

Ein ‘.’ ist nicht erlaubt.

SIP Server Typ:

Mögliche Optionen:

- **Broadsoft**
- **OpenScape Voice**
- **Sylantro**
- **andere**
- **HiQ8000**
- **Genesys**

8.1.2 IP Routing

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > IP Routing

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „DNS Server“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.2.1 Register „DNS Server“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > IP Routing > Register „DNS Server“

Terminal Hostname:

Host-Name des Terminals.

Erlaubte Zeichen: Buchstaben, Ziffern, Bindestrich, Unterstrich und Punkt; Groß-/Kleinschreibung wird unterschieden; maximale Länge: 63 Zeichen.

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

8.1.3 Features

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features

Dieser Bereich besteht aus folgenden Inhalten:

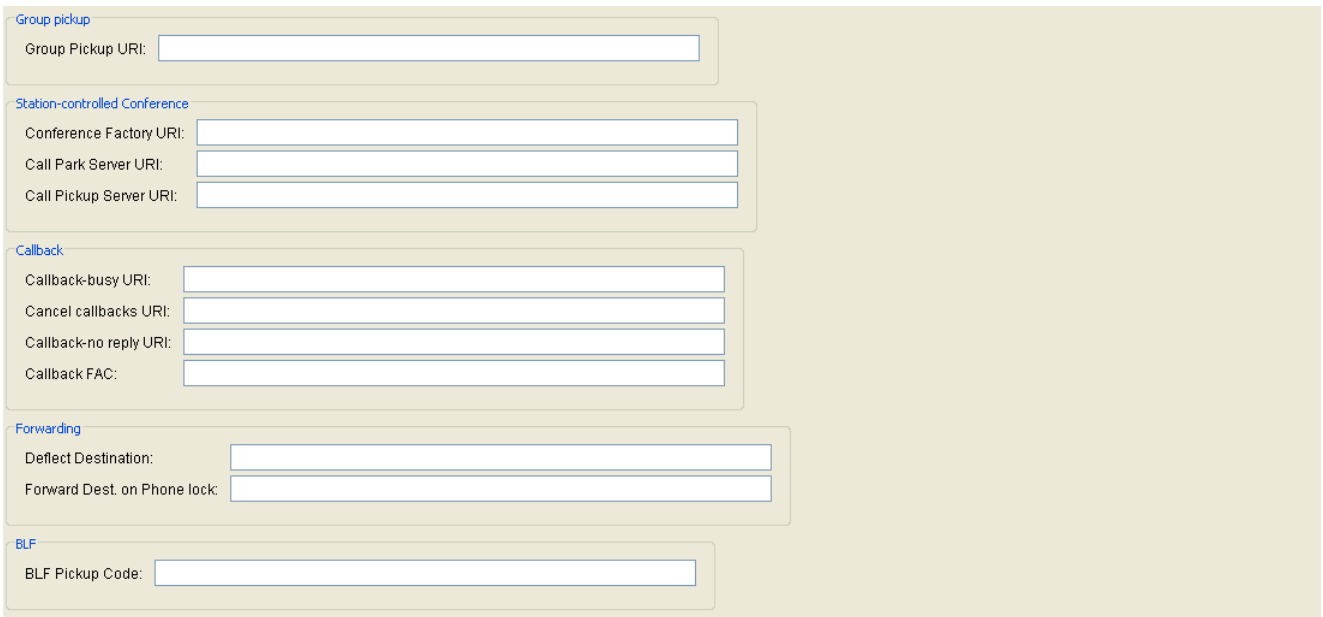
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Feature-Einstellungen 1“
- Register „Feature-Einstellungen 2“
- Register „Anrufbezogene Benutzer-Einstellungen“
- Register „Verfügbarkeit“
- Register „Server basierte Features“
- Register „Wählplan“
- Register „Signalisierungsmelodie / Ton“
- Register „Anrufumleitung“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.3.1 Register „Feature-Einstellungen 1“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Feature-Einstellungen 1“



Anrufübernahme

Anrufübernahmegruppe URI:

URI der Anrufübernahmegruppe.

Nur bei SIP-Workpoints verfügbar.

Gerätekontrollierte Konferenz

Konferenz URI:

URI zur Herstellung von Konferenz-Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Geparkte Gespräche Server URI:

URI des Servers zum Parken von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Anrufübernahme Server URI:

URI des Servers zur Anrufübernahme.

Nur bei SIP-Workpoints verfügbar.

Rückruf

Rückruf nach Besetzt:

URI des Servers, der das Leistungsmerkmal „Rückruf nach Besetzt“ steuert.

Nur für optiPoint und OpenStage bis V2 verfügbar.

Rückrufe löschen URI:

URI des Servers, der das Leistungsmerkmal „Rückruf löschen“ steuert.

Rückruf nach nicht Melden URI:

URI des Servers, der das Leistungsmerkmal „Rückruf nach nicht Melden“ steuert.

Nur für optiPoint und OpenStage bis V2 verfügbar.

Rückruf FAC

URI, über die das Leistungsmerkmal „Rückruf“ gesteuert wird.

Nur bei OpenStage ab V3.0 verfügbar.

Weiterleitung

Umlenkungsziel:

Ziel-Rufnummer für die Rufumleitung.

Nur bei SIP-Workpoints verfügbar.

Ziel bei Gerätesperre:

Ziel-Rufnummer für Umleitung bei Ruf an gesperrtem Workpoint.

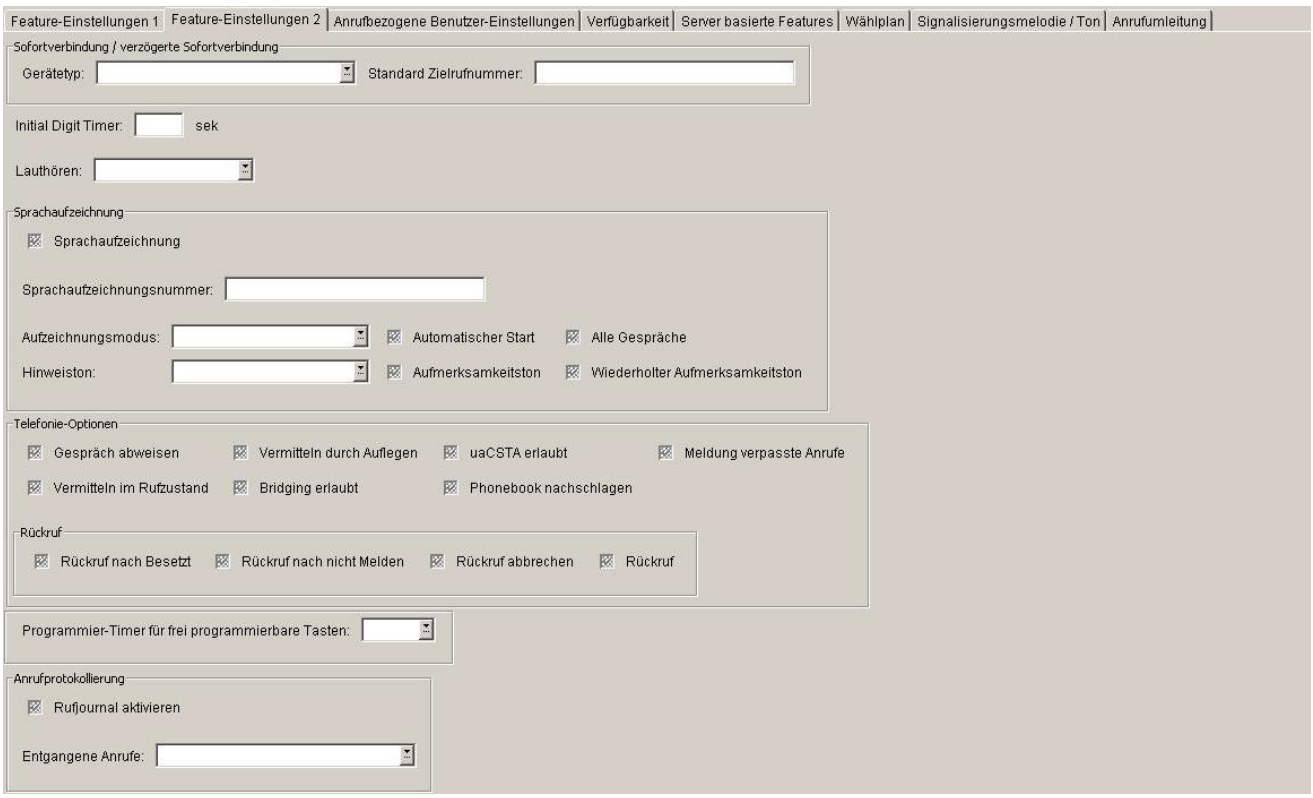
BLF

BLF Pickup Code:

BLF Pickup Code.

8.1.3.2 Register „Feature-Einstellungen 2“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Feature-Einstellungen 2“



Sofortverbindung / verzögerte Sofortverbindung

Gerätetyp:

Zeitverzögerung für die Funktion „Hotline“ und „Warmline“.

Mögliche Optionen:

- **Normal**
- **Sofortverbindungsaufbau**
- **verzögerter Sofortverbindungsaufbau**

Nur bei SIP-Workpoints verfügbar.

Standard Zielrufnummer:

Ziel-Rufnummer für Funktion „Hotline“ und „Warmline“.

Nur bei SIP-Workpoints verfügbar.

Initial Digit Timer:

Wartezeit in Sekunden auf eine Wahlziffer, nachdem der Wählton angeschaltet wurde.

Nur bei SIP-Workpoints verfügbar.

Lauthören:

Einstellen des Lautsprechermodus.

Mögliche Optionen:

- **Standard Mode**
  Um auf Freisprechen umzuschalten, muss der Benutzer die Lautsprechertaste gedrückt halten, während er den Hörer auflegt.
- **US Mode**
  Um auf Freisprechen umzuschalten, muss der Benutzer muss die Lautsprechertaste betätigen und danach den Hörer auflegen.

Sprachaufzeichnung

Sprachaufzeichnung

Schalter zum Aktivieren der Sprachaufzeichnung.

Sprachaufzeichnungsnummer

Rufnummer der Sprachaufzeichnung (Call Recorder).

Aufzeichnungsmodus

Legt das Verhalten der Sprachaufzeichnung fest.

Mögliche Optionen:

- **Manuell**
- **Auto Start**
- **Alle Gespräche**

- **Deaktiviert**
  (nur Anzeige)

Hinweiston

Auswahl des Hinweistons.

Mögliche Optionen:

- **Aus**
- **Ein / Einzelhinweiston**
- **Regelmässiger Hinweiston**

Automatischer Start

Wenn aktiviert, wird die Sprachaufzeichnung automatisch gestartet, sowohl bei eingehenden als auch bei ausgehenden Anrufen. Der Benutzer kann die Aufnahme während des Gesprächs ein- oder ausschalten.

Der Schalter ist nur wirksam, wenn die Sprachaufzeichnung auf dem Telefon aktiviert ist.

Alle Gespräche

Wenn aktiviert, wird die Sprachaufzeichnung automatisch gestartet, sowohl bei eingehenden als auch bei ausgehenden Anrufen. Der Benutzer hat keinen Einfluss auf die Aufnahme.

Der Schalter ist nur wirksam, wenn die Sprachaufzeichnung auf dem Telefon aktiviert ist.

Aufmerksamkeitston

Der Aufmerksamkeitston signalisiert dem Gesprächspartner, dass das Telefongespräch aufgezeichnet wird.

Wiederholter Aufmerksamkeitston

Ein wiederholter Aufmerksamkeitston signalisiert dem Gesprächspartner, dass das Telefongespräch aufgezeichnet wird.

Dieser Schalter ist nur wirksam, wenn **Aufmerksamkeitston** aktiviert ist.

Telefonie-Optionen

Gespräch abweisen

Schalter zum Aktivieren der Funktion zum Abweisen von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Vermitteln im Rufzustand

Schalter zum Aktivieren des Leistungsmerkmals „Vermitteln im Rufzustand“.

Nur bei SIP-Workpoints verfügbar.

Vermitteln durch Auflegen

Schalter zum Aktivieren des Leistungsmerkmals „Vermitteln durch Auflegen“.

Nur bei SIP-Workpoints verfügbar.

Bridging erlaubt

Schalter zum Aktivieren des Leistungsmerkmals „Bridging“.

Nur bei SIP-Workpoints verfügbar.

uaCSTA erlaubt

Schalter zum Aktivieren des Leistungsmerkmals „uaCSTA“.

Nur bei SIP-Workpoints verfügbar.

Phonebook nachschlagen

Schalter zum Aktivieren des Leistungsmerkmals „Phonebook nachschlagen“.

Meldung verpasste Anrufe

Ist der Schalter aktiviert, werden verpasste Anrufe im Display angezeigt.

Rückruf

Rückruf nach Besetzt

Schalter zum Aktivieren des Leistungsmerkmals „Rückruf nach Besetzt“.

Nur bei SIP-Workpoints verfügbar.

Rückruf nach nicht Melden

Schalter zum Aktivieren des Leistungsmerkmals „Rückruf nach nicht Melden“.

Nur bei SIP-Workpoints verfügbar.

Rückruf abbrechen

Wenn aktiv, kann der Benutzer Rückrufaufträge abbrechen.

Rückruf

Schalter zum Aktivieren des Leistungsmerkmals „Rückruf“.

Nur bei OpenStage ab V3 verfügbar.

Programmier-Timer für frei programmierbare Tasten

Wenn „Aus“ gewählt ist, wechseln die programmierbaren Tasten (FPKs) bei langem Drücken nicht in den Programmiermodus.

Mögliche Optionen:

- **Ein**
- **Aus**

Anrufprotokollierung

Rufjournal aktivieren

Kontrollkästchen, das anzeigt, ob die Anrufprotokollierung aktiviert ist.

Entgangene Anrufe

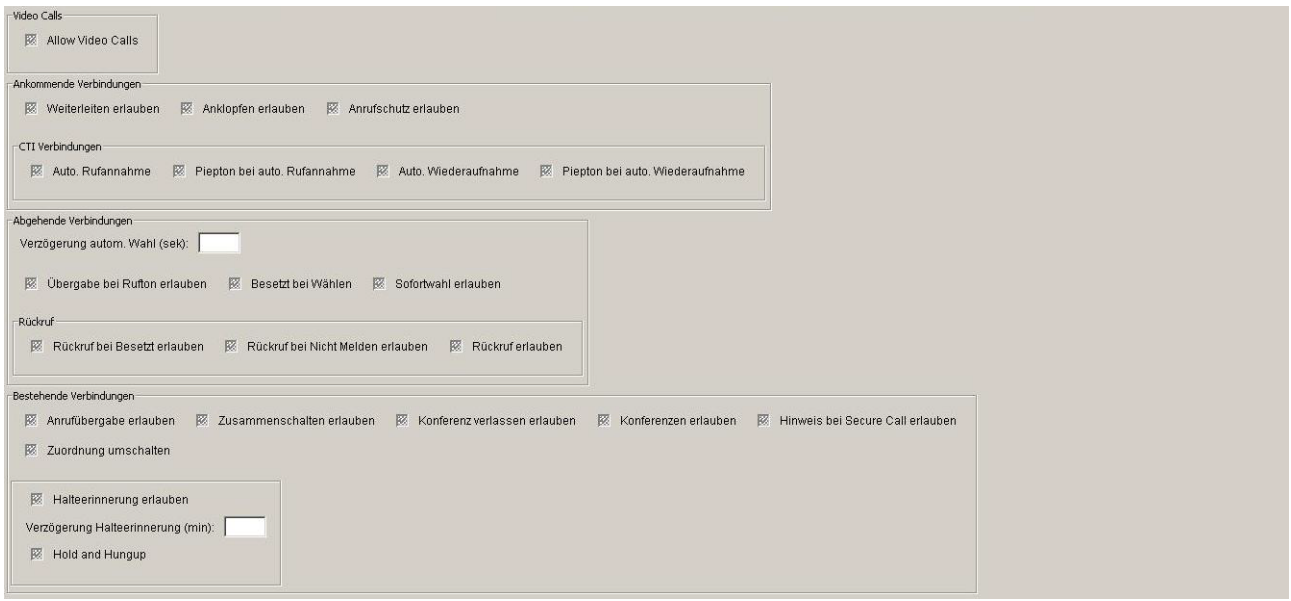
Zeigt an, ob Anrufe, die andernorts angenommen wurden, an Ihrem Telefon protokolliert werden.

Mögliche Optionen:

- **Alle Anrufe anzeigen**
  Auch Anrufe, die andernorts angenommen wurden, werden an Ihrem Telefon protokolliert.
- **Nur unbeantwortete anzeigen**
  Anrufe, die andernorts angenommen wurden, werden an Ihrem Telefon nicht protokolliert.

8.1.3.3 Register „Anrufbezogene Benutzer-Einstellungen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Anrufbezogene Benutzer-Einstellungen“



Video-Gespräche

Video Gespräche erlauben

Schalter zum Aktivieren von Video-Gesprächen.

Wenn das Kontrollkästchen aktiviert ist, sind Video-Gespräche möglich.

Ankommende Verbindungen

Weiterleiten erlauben:

Schalter zum Aktivieren der Weiterleitung.

Anklopfen erlauben:

Schalter zum Aktivieren des Anklopfens.

Anrufschutz erlauben:

Schalter zum Aktivieren des Anrufschutzes.

CTI Verbindungen

Auto. Rufannahme

Schalter zum Aktivieren der automatischen Rufannahme.

Nur bei SIP-Workpoints verfügbar.

Piepton bei auto. Rufannahme

Schalter zum Aktivieren des Quittungstones bei automatischer Rufannahme.

Nur bei SIP-Workpoints verfügbar.

Auto. Wiederaufnahme

Schalter zum Aktivieren der automatischen Wiederaufnahme eines geparkten Gespräches.

Nur bei SIP-Workpoints verfügbar.

Piepton bei auto. Wiederaufnahme

Schalter zum Aktivieren des Quittungstones bei automatischer Wiederaufnahme-Funktion eines geparkten Gespräches.

Nur bei SIP-Workpoints verfügbar.

Sofortwahl erlauben

Ist der Schalter aktiviert, wird sofort gewählt, sobald die eingegebene Zeichenfolge mit einem Eintrag im Wählplan übereinstimmt.

Nur bei SIP-Workpoints verfügbar.

Abgehende Verbindungen

Verzögerung autom. Wahl (sek):

Verzögerung der automatischen Wahl in Sekunden.

Übergabe bei Rufton erlauben

Schalter zum Aktivieren von Übergabe bei Rufton.

Besetzt bei Wählen

Schalter zum Aktivieren von Besetzt bei Wählen.

Sofortwahl erlauben

Schalter zum Aktivieren der **Sofortwahl**.

Rückruf

Rückruf bei Besetzt erlauben

Schalter zum Aktivieren von Rückruf bei Besetzt.

Nur bei OpenStage bis V2 verfügbar.

Rückruf bei Nicht Melden erlauben

Schalter zum Aktivieren von Rückruf bei Nicht Melden.

Nur bei OpenStage bis V2 verfügbar.

Rückruf erlauben

Rückruf erlauben.

Nur bei OpenStage ab V3 verfügbar.

Bestehende Verbindungen

Anrufübergabe erlauben

Schalter zum Aktivieren der Anrufübergabe.

Zusammenschalten erlauben

Schalter zum Aktivieren von Zusammenschalten.

Konferenz verlassen erlauben

Wenn aktiviert, kann der Benutzer die Konferenz verlassen.

Konferenzen erlauben

Schalter zum Aktivieren von Konferenzen.

Hinweis bei Secure Call erlauben

Wenn die Bearbeitung gesicherter Anrufe auf dem Telefon aktiviert und dieser Schalter markiert ist, wird der Benutzer durch ein Popup-Fenster und einen Aufmerksamkeitston auf unsichere (unverschlüsselte) eingehende Anrufe hingewiesen.

Zuordnung umschalten

Schalter zum Aktivieren von Zuordnung umschalten.

Halteerinnerung erlauben

Schalter zum Aktivieren der Halteerinnerung.

Verzögerung Halteerinnerung (min)

Verzögerung der Halteerinnerung in Minuten.

Halten und Auflegen

Schalter zum Aktivieren der Funktion „Halten und Auflegen“ bei nicht-Keyset OpenStage-Telefonen.

Mit dieser Funktion können Teilnehmer Anrufe vorübergehend halten und auflegen, ohne den Anrufer zu trennen. Diese Funktion ist standardmäßig deaktiviert.

8.1.3.4 Register „Verfügbarkeit“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Verfügbarkeit“

Halten

Schalter zum Aktivieren der Funktion zum Halten von Gesprächen.

Gültigkeitsbereich: Gilt nur für SIP-Workpoints.

Anrufumlenkung

Schalter zum Aktivieren der manuellen Umleitung ankommender Anrufe (CD).

Nur bei SIP-Workpoints verfügbar.

Anrufumleitung

Schalter zum Aktivieren der automatischen Anrufweiterschaltung (CF).

Nur bei SIP-Workpoints verfügbar.

Umgeleitete Anrufe protokollieren

Schalter zum Aktivieren der Protokollierung von umgeleiteten Anrufen.

Nur bei SIP-Workpoints verfügbar.

Gesprächsdauer

Schalter zum Aktivieren der Funktion zur Anzeige der Gesprächsdauer.

Nur bei SIP-Workpoints verfügbar.

Anklopfen

Schalter zum Aktivieren der optischen und/oder akustischen Signalisierung von anklopfenden Anrufen (CW).

Nur bei SIP-Workpoints verfügbar.

Übergeben

Schalter zum Aktivieren der Funktion zum Übergeben von Gesprächen (ECT).

Nur bei SIP-Workpoints verfügbar.

Übernahme geparktes Gespräch

Schalter zum Aktivieren der Funktion zum Übernehmen von geparkten Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Auto. Wiederaufnahme

Schalter zum Aktivieren der automatischen Gesprächswiederaufnahme.

Nur bei SIP-Workpoints verfügbar.

Anzeige Rufnummer

Schalter zum Aktivieren der Rufnummernanzeige am Workpoint.

Nur bei SIP-Workpoints verfügbar.

Anzeige Name

Schalter zum Aktivieren der Anzeige des Anrufernamens am Workpoint.

Nur bei SIP-Workpoints verfügbar.

Wartemusik

Schalter zum Aktivieren der Wartemusik bei gehaltenen und geparkten Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Anrufschutz

Schalter zum Aktivieren des Anrufschutzes (nur optische Signalisierung und ein Rufton).

Nur bei SIP-Workpoints verfügbar.

Nachricht wartet

Schalter zum Aktivieren der Signalisierung von wartenden Nachrichten (MWI).

Nur bei SIP-Workpoints verfügbar.

Lokale Konferenz

Schalter zum Aktivieren der Funktion zum Aufbau einer lokalen Konferenz.

Nur bei SIP-Workpoints verfügbar.

Auto. Rufannahme

Schalter zum Aktivieren der automatischen Rufannahme.

Nur bei SIP-Workpoints verfügbar.

PC Schnittstelle

Schalter zum Aktivieren der PC-Schnittstelle.

WAP Browser auf APM / DSM

Schalter zum Aktivieren des WAP-Browsers am optiPoint Application Module / Display Module.

Nur bei SIP-Workpoints verfügbar.

LDAP auf APM / DSM

Schalter zum Aktivieren der LDAP-Funktion am optiPoint Application Module / Display Module.

Nur bei SIP-Workpoints verfügbar.

Telefonie auf APM / DSM

Schalter zum Aktivieren der Telefonie-Funktion am optiPoint Application Module / Display Module.

Nur bei SIP-Workpoints verfügbar.

Spracherkennung auf APM / DSM

Schalter zum Aktivieren der Spracherkennungs-Funktion (Voice Dialing) am optiPoint Application Module / Display Module.

Nur bei SIP-Workpoints verfügbar.

Kurzwahl auf APM / DSM

Schalter zum Aktivieren der Kurzwahl-Funktion am optiPoint Application Module / Display Module mittels Java Midlet.

Nur bei SIP-Workpoints verfügbar.

ENB auf APM / DSM

Schalter zum Aktivieren des elektronischen Notizbuchs am optiPoint Application Module / Display Module.

Nur bei SIP-Workpoints verfügbar.

Parken

Schalter zum Aktivieren der Funktion zum Parken von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Zusammenschalten

Schalter zum Aktivieren der Funktion zum Zusammenschalten von Gesprächen.

Nur bei SIP-Workpoints verfügbar.

Aufmerksamkeitston für AUN Gruppe

Schalter zum Aktivieren des Leistungsmerkmals „Aufmerksamkeitston für AUN Gruppe“.

Blind Transfer

Schalter zum Aktivieren von „Blind Transfer“.

Repertory Dial

Schalter zum Aktivieren von „Repertory Dial“.

Besetztlampenfeld (BLF)

Schalter zum Aktivieren des Besetztlampenfelds (BLF).

Direct Station Select (DSS)

Schalter zum Aktivieren von Direct Station Select (DSS).

CTI

Schalter zum Aktivieren von der Schnittstelle CTI.

Leitungsübersicht

Schalter zum Aktivieren der Leitungsübersicht.

Feature Toggle

Schalter zum Aktivieren von „Feature Toggle“.

Third Call Leg

Schalter zum Aktivieren von „Third Call Leg“ (Drittgesprächen).

Übernahme Anruf in Gruppe

Schalter zum Aktivieren von „Übernahme Anruf in Gruppe“.

Video Call

Schalter zum Aktivieren der Funktion „Video Call“.

8.1.3.5 Register „Server basierte Features“

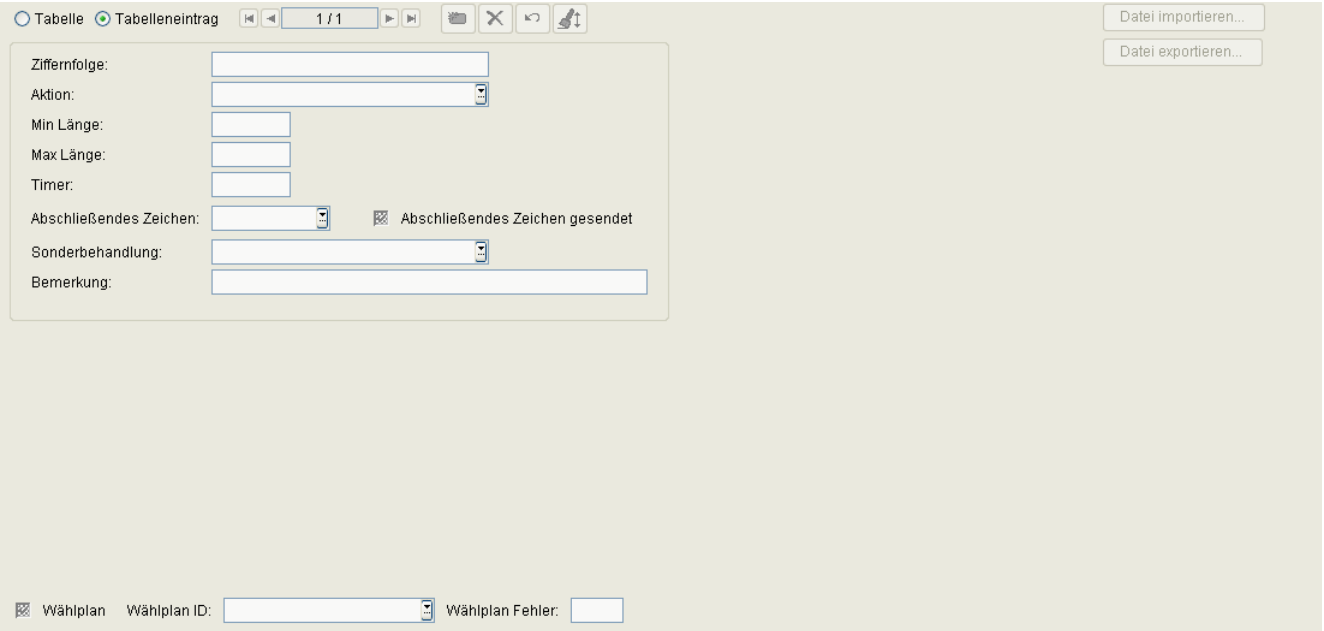
Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Server basierte Features“

Unterstützung Server basierte Features

Ist der Schalter aktiviert, so werden die serverbasierten Leistungsmerkmale des Endgeräts für den Benutzer freigegeben.

8.1.3.6 Register „Wählplan“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Wählplan“



Ziffernfolge

Ziffernfolge zur Ausführung dieser Aktion.

Nur bei SIP-Workpoints verfügbar.

Aktion

Aktion, die bei dieser Ziffernfolge ausgeführt wird.

Mögliche Optionen:

- **-C- Aktion für Ziffern**
- **-CD1- Aktion für Ziffern, Wählton**
- **-D1- Wählton**
- **-S- Ziffern senden**
- **-SD1- Ziffern senden, Wählton**

Nur bei SIP-Workpoints verfügbar.

Min Länge

Minimale Länge der Ziffernfolge, ab der die Ziffernfolge interpretiert wird.

Nur bei SIP-Workpoints verfügbar.

Max Länge

Maximale Länge der Ziffernfolge, bis zu der die Ziffernfolge interpretiert wird.

Nur bei SIP-Workpoints verfügbar.

Timer

Verzögerungszeit bis zum Ausführen der Aktion.

Wertebereich: 1 ... 9 Sekunden.

Nur bei SIP-Workpoints verfügbar.

Abschließendes Zeichen

Zeichen, welches die Ziffernfolge bei der Eingabe abschließt.

Mögliche Optionen:

- **#**
- *****

Nur bei SIP-Workpoints verfügbar.

Sonderbehandlung

Mögliche Optionen:

- **-E- Notruf**
- **-b- bypass**

Nur bei SIP-Workpoints verfügbar.

Abschließendes Zeichen gesendet

Zeigt an, ob das abschließende Zeichen in der Ziffernfolge enthalten ist.

Wählplan

Schalter zum Aktivieren des Wählplans. Ist diese Checkbox aktiviert, werden die Angaben im Register „Wählplan“ interpretiert.

Nur bei SIP-Workpoints verfügbar.

Wählplan ID:

Name des Wählplans, der mit einem ’!’ beginnen muss.

Wertebereich: max. 14 alphanumerische Zeichen.

Nur bei SIP-Workpoints verfügbar.

Wählplan Fehler:

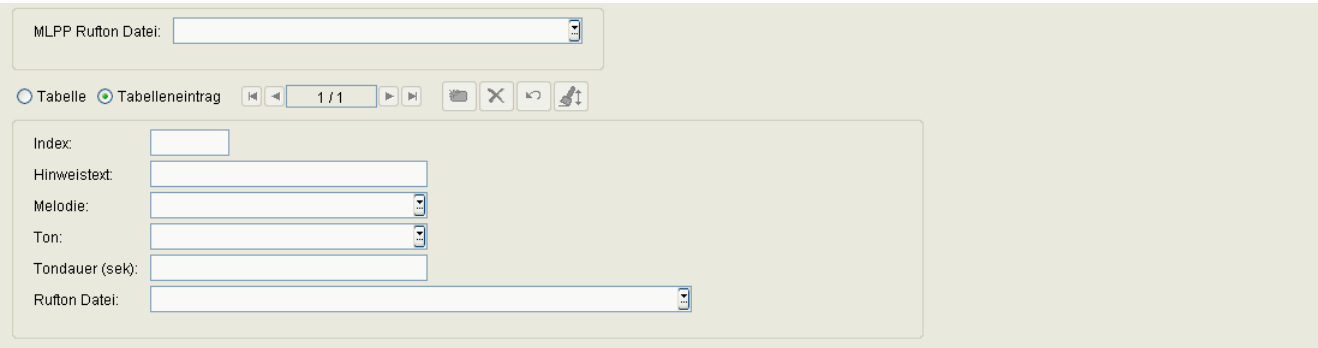
Gibt im Fehlerfall an, welcher Wählplaneintrag fehlerhaft ist.

Wertebereich: **1** ... **48**

Nur bei SIP-Workpoints verfügbar.

8.1.3.7 Register „Signalisierungsmelodie / Ton“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Signalisierungsmelodie / Ton“



HINWEIS: Ein Template mit Einträgen zu **Signalisierung / Ton** wird erstellt, indem man ein IP Device mit **Signalisierung / Ton**-Einträgen (dies können auch leere Einträge sein) sucht und mit der Aktion **In Template kopieren** ein Template erzeugt. Es müssen immer 15 Einträge vorhanden sein, auch wenn sie keine Daten enthalten.
Dieses Template kann nun modifiziert, gespeichert und verwendet werden.

MLPP Rufton Datei

Klingeltondatei für Priority-Anrufe.

Index

Gibt die Reihenfolge der Signalisierungseinträge an.

Diese werden automatisch vergeben. Das Feld dient nur der Anzeige.

Hinweistext

Ist der hier eingegebene String identisch mit einem speziellen String, der im SIP Alert Info Header an das Telefon gesendet wird, so wird der entsprechende Klingelton verwendet.

Nur bei SIP-Workpoints verfügbar.

Melodie

Art der Rufton-Melodie.

Mögliche Optionen: **Melodie 1** ... **8**, **Melodie aus**.

Nur bei SIP-Workpoints verfügbar.

Ton

Klingeltonsequenz.

Mögliche Optionen:

- **1**
  Entspricht 1 sek EIN, 4 sek AUS.
- **2**
  Entspricht 1 sek EIN, 2 sek AUS.
- **3**
  Entspricht 0,7 sek EIN, 0,7 sek AUS, 0,7 sek EIN, 3 sek AUS.

Nur bei SIP-Workpoints verfügbar.

Tondauer

Dauer des Ruftons.

Wertebereich: **1** ... **300** Sekunden.

Standard: **60** Sekunden.

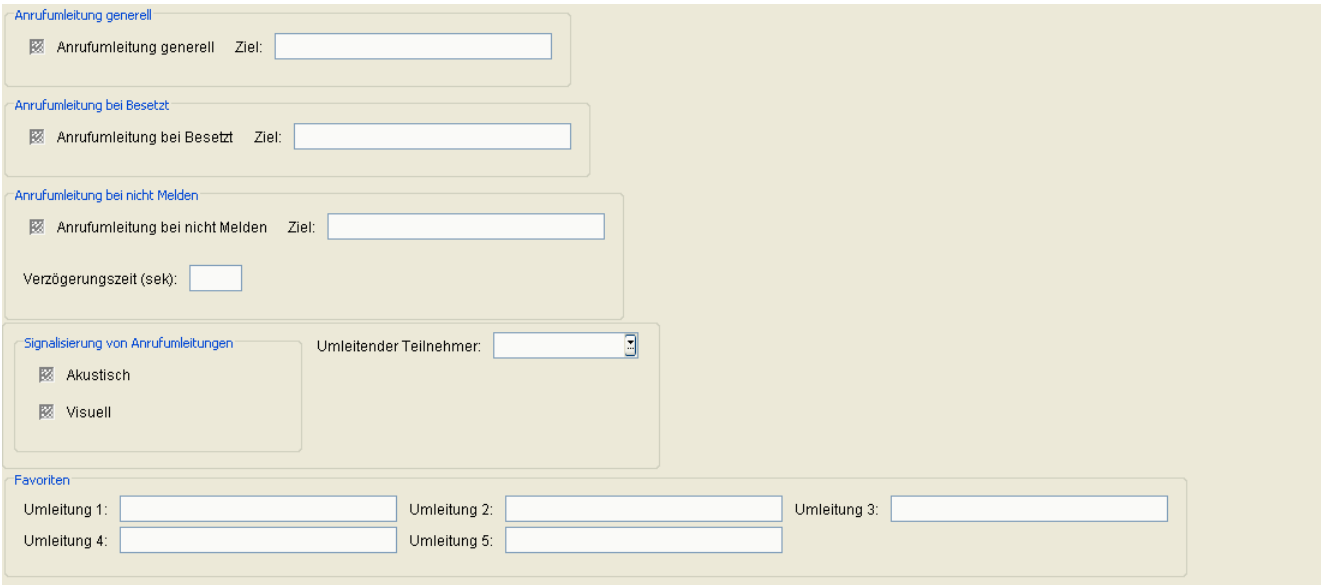
Nur bei SIP-Workpoints verfügbar.

Rufton Datei

Name der Audio-Datei, die den Rufton enthält.

8.1.3.8 Register „Anrufumleitung“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Features > Register „Anrufumleitung“



Anrufumleitung generell

Anrufumleitung generell

Schalter zum Aktivieren der „Anrufumleitung ohne weitere Bedingungen“.

Ziel:

Rufnummer des Anrufumleitungsziels.

Anrufumleitung bei Besetzt

Anrufumleitung bei Besetzt

Schalter zum Aktivieren der „Anrufumleitung bei Besetzt“.

Ziel:

Rufnummer des Anrufumleitungsziels.

Anrufumleitung bei nicht Melden

Anrufumleitung bei nicht Melden:

Schalter zum Aktivieren der „Anrufumleitung bei nicht Melden“.

Ziel:

Rufnummer des Anrufumleitungsziels.

Verzögerungszeit (sek):

Ist diese Zeit abgelaufen, ohne dass der Anruf angenommen worden ist, wird der Anruf umgeleitet.

Signalisierung bei Anrufumleitung

Akustisch

Schalter zum Aktivieren eines akustischen Signals beim Umleitenden.

Visuell

Schalter zum Aktivieren eines visuellen Signals beim Umleitenden.

Umleitender Teilnehmer

Es kann eingestellt werden, welcher umleitende Teilnehmer bei Mehrfachumleitungen angezeigt werden soll.

Mögliche Optionen:

- **Anzeige erster**
- **Anzeige letzter**

Favoriten

Umleitung 1:

Umleitung 2:

Umleitung 3:

Umleitung 4:

Umleitung 5:

8.1.4 Quality of Service

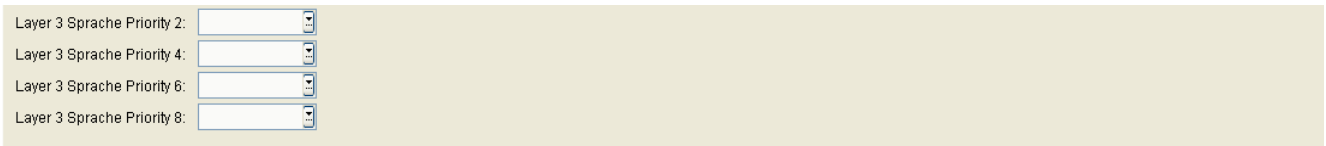
Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Quality of Service

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „QoS Parameter“

8.1.4.1 Register „QoS Parameter“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Quality of Service > Register „QoS Parameter“



Layer 3 Sprache Priority 2

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

Layer 3 Sprache Priority 4

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

Layer 3 Sprache Priority 6

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

Layer 3 Sprache Priority 8

Layer 3-Werte für Sprache bei Priority-Rufen.

Wertebereich: **DSCP00** ... **DSCP63**

8.1.5 Security Einstellungen

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Security Einstellungen

Dieser Bereich besteht aus folgenden Inhalten:

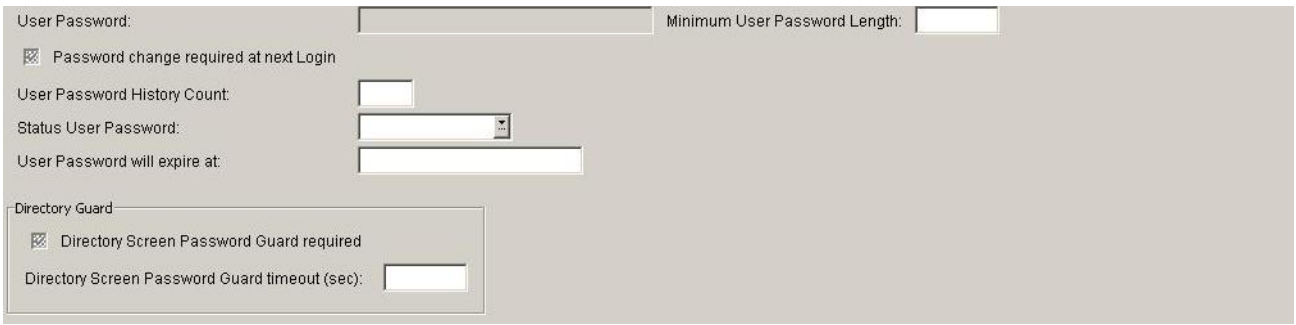
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Passwörter“
- Register „Freigeschaltete Services (NW Stack)“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.5.1 Register „Passwörter“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Security Einstellungen > Register „Passwörter“



Benutzer Passwort:

Passwort für den Zugang zum Benutzerbereich des Workpoints.

Minimale Länge Benutzer Passwort:

Mindestanzahl von Zeichen, aus denen das Passwort bestehen muss.

Passwortänderung bei nächstem Login

Ist der Schalter aktiviert, wird der Benutzer aufgefordert, das Passwort zu ändern.

Anzahl User Passwort Historie

Zeigt die Anzahl der Passwortänderungen an.

Status User Passwort:

Status des Benutzer-Passworts.

Mögliche Optionen:

- Aktiv
- Aufgeschoben
- Gesperrt

User Passwort wird ungültig am:

Zeit & Datum für den Ablauf des Benutzer-Passworts

Directory Schutz

Directory Screen Passwort Schutz

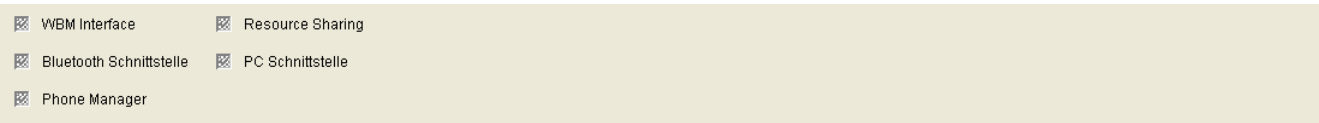
Dieser Schalter aktiviert den Passwortschutz des Directory-Bildschirms. Zur Nutzung des Bildschirms ist das Standard-Benutzerpasswort einzugeben.

Directory Screen Passwort Schutz Timeout (sek)

Nach Ablauf dieser Zeit wird der Passwortschutz aktiviert, d.h. das Passwort muss zur weiteren Nutzung des Directory-Bildschirms erneut eingegeben werden.

8.1.5.2 Register „Freigeschaltete Services (NW Stack)“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Security Einstellungen > Register „Freigeschaltete Services (NW Stack)“



WBM Interface

Schalter zum Aktivieren des WBM Interface.

Resource Sharing

Schalter zum Aktivieren des Resource Sharing (Mitnutzen der PC-Maus und Tastatur).

Bluetooth Schnittstelle

Schalter zum Aktivieren der Bluetooth-Schnittstelle.

Phone Manager

Schalter zum Aktivieren des Phone Managers.

PC Schnittstelle

Schalter zum Aktivieren der Schnittstelle zwischen PC und Gerät.

8.1.6 Telefonie

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Telefonie

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Telefonie“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.6.1 Register „Telefonie“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Telefonie > Register „Telefonie“

Notrufnummer:

Enthält die Rufnummer, die in einem Notfall gewählt werden kann.

8.1.7 Wahlparameter

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Wahlparameter

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Rufnummern“
- Register „Ziffernumwandlung“

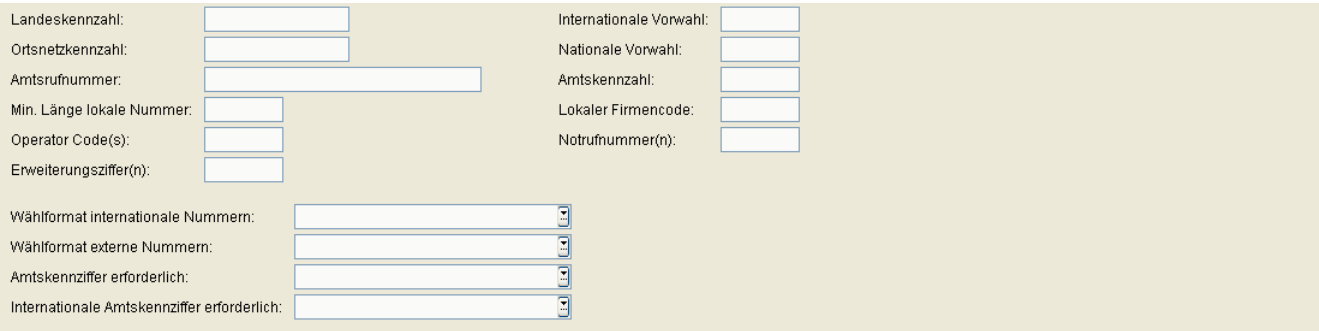
Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.7.1 Register „Rufnummern“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Wahlparameter > Register „Rufnummern“

Die Wahlparameter werden benötigt, um Rufnummern im kanonischen Format korrekt aufzulösen (siehe Kapitel 17, “Kanonisches Format”).



Landeskennzahl:

Format: Ohne führende Nullen, max. 4 Stellen.

Beispiel: **49** für Deutschland.

Ortsnetzkennzahl:

Format: Ohne führende Nullen, max. 21 Stellen.

Beispiel: **89** für München.

Amtsrufnummer:

Rufnummer des Firmennetzes.

Format: Ohne führende Nullen und ohne Nebenstellen-Nummer, max. 21 Stellen.

Beispiel: **722** für Unify München Hofmannstraße.

Nur für Geräte der optiPoint-Familie verfügbar.

Min. Länge lokale Nummer

Minimale Länge der lokalen Nummer.

Operator Code(s)

Nummer des Operators. Die Eingabe mehrerer, durch Komma getrennter, Nummern ist möglich.

Erweiterungsziffer(n)

Liste von Anfangsziffern aller im Firmennetz möglichen Nebenstellennummern. Wenn eine Rufnummer nicht als Nummer des öffentlichen Netzes erkannt wird, prüft das Telefon, ob sie zum lokalen Firmennetzwerk gehört. Hierzu wird die Anfangsziffer der Rufnummer mit dem/den hier angegebenen Wert(en) verglichen. Stimmen die beiden Werte überein, so wird die Rufnummer als firmeninterne Nummer erkannt und entsprechend verarbeitet.

Beispiel: Wenn die Nebenstellennummern 3000-5999 in OpenScape Voice konfiguriert sind, so beginnt jede Nummer mit 3, 4 oder 5. Somit sind hier die Ziffern **3, 4, 5** einzutragen.

Internationale Vorwahl:

Nationale Vorwahlnummer.

Format: max. 4 Stellen.

Beispiel: **00** in Deutschland.

Nationale Vorwahl:

Internationale Vorwahlnummer.

Format: max. 5 Stellen.

Beispiel: **0** in Deutschland.

Amtskennzahl:

Nummer zur „Amtsholung“ eines ausgehenden, externen Gesprächs.

Format: max. 5 Stellen.

Beispiele: **0**, **74**, **9** (USA).

Lokaler Firmencode:

Rufnummer des Firmennetzes.

Beispiel: **722** für Unify München Hofmannstraße.

Nur für Geräte der OpenStage-Familie verfügbar.

Notrufnummer(n)

Die Eingabe mehrerer, durch Komma getrennter, Notrufnummern ist möglich.

Wählformat internationale Nummern

Mögliche Optionen:

- **Lokales Format des Unternehmens**
- **Knoten immer hinzufügen**
- **Verwende externe Nummern**

Wählformat externe Nummern

Mögliche Optionen:

- **Lokales öffentliches Format**
- **Nationales öffentliches Format**
- **Internationales öffentliches Format**

Amtskennziffer erforderlich

Mögliche Optionen:

- **Nicht benötigt**
- **Für externe Nummern**

Internationale Amtskennziffer erforderlich

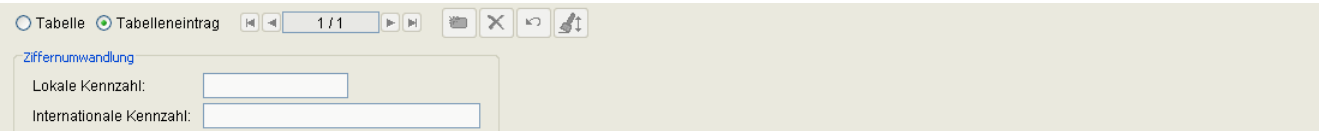
Mögliche Optionen:

- **Verwende nationalen Code**
- **Unverändert**

8.1.7.2 Register „Ziffernumwandlung“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Wahlparameter > Register „Ziffernumwandlung“

Diese Funktion ordnet die Eingabe im ersten Feld („Lokale Kennzahl“) in eine bestimmte Ziffernfolge um, die im zweiten Feld („Internationale Kennzahl“) festgelegt wird. Diese Ziffernfolge kann z. B. eine nationale oder internationale Vorwahl sein. Auf diese Weise können häufig benutzte Vorwahlen durch Eingabe nur einer Ziffer gewählt werden.



Lokale Kennzahl

Ziffer bzw. kurze Ziffernfolge, mithilfe der der Benutzer z. B. eine bestimmte Vorwahl wählen kann.

Internationale Kennzahl

Ziffernfolge, beispielsweise Vorwahl, die bei der Eingabe einer bestimmten Ziffer zu Beginn des Wählvorgangs gewählt wird.

8.1.8 Uhrzeit Einstellungen

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Uhrzeit Einstellungen

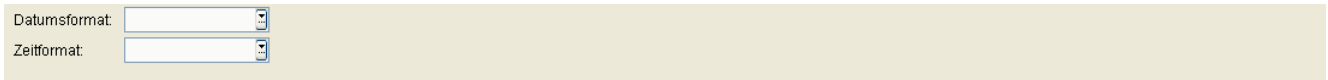
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Zeit“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

8.1.8.1 Register „Zeit“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Uhrzeit Einstellungen > Register „Zeit“



Datumsformat:

Format der Datumsangabe. Die manuelle Festlegung ist nur notwendig, wenn diese Informationen nicht automatisch übermittelt werden (z. B. PBX oder DHCP-Server).

Mögliche Optionen:

- **JJ-MM-TT**
  Beispiel: 04-10-05 für 5.10.2004
- **MM/TT/JJ**
  Beispiel: 10/05/04 für 5.10.2004
- **TT.MM.JJ**
  Beispiel: 05.10.04 für 5.10.2004

Zeitformat:

Format der Zeitangabe.

Mögliche Optionen:

- **12 Stunden**
- **24 Stunden**

8.1.9 Audio Einstellungen

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Audio Einstellungen

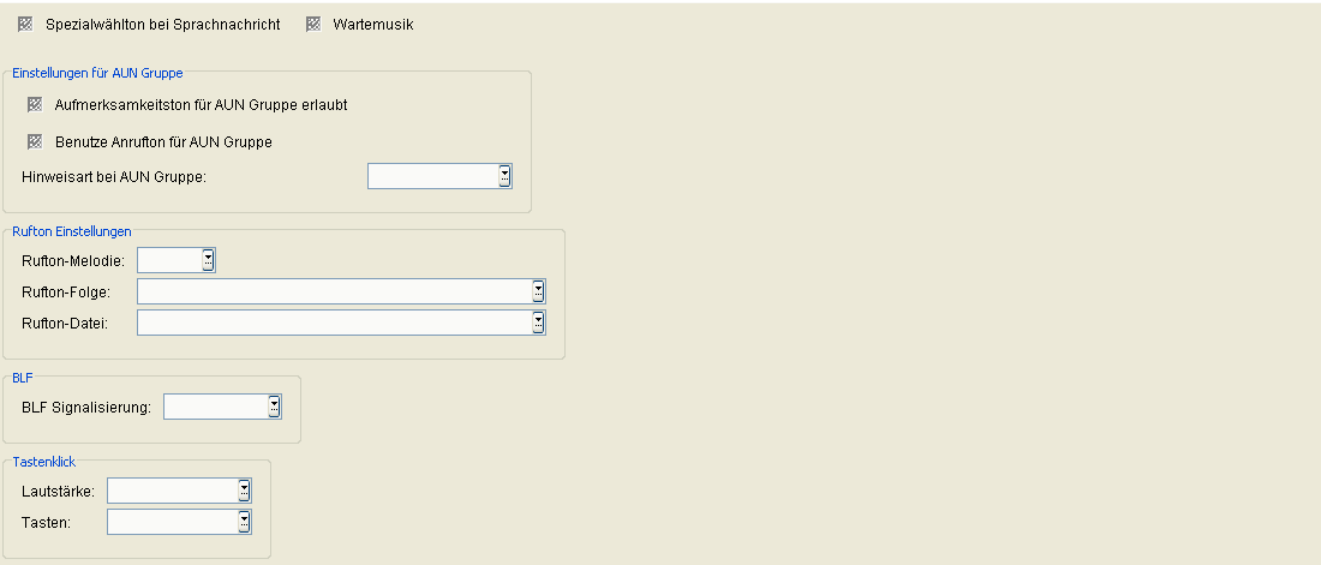
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Audio Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

8.1.9.1 Register „Audio Einstellungen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Audio Einstellungen > Register „Audio Einstellungen“



Spezialwählton bei Sprachnachricht

Schalter zum Einschalten eines Spezialwähltons bei Sprachnachrichten.

Wartemusik

Wenn dieser Schalter aktiviert ist, spielt das Telefon dem Anrufer Wartemusik vor, sobald dieser ins Halten gelegt wird.

Einstellungen für AUN Gruppe

Aufmerksamkeitston für AUN Gruppe erlaubt

Aktiviert oder deaktiviert die Erzeugung eines akustischen Signals für einen eingehenden Anruf innerhalb der AUN-Gruppe (Anrufübernahme-Gruppe).

Benutze Anrufton für AUN Gruppe

Ist das Kästchen angehakt, so wird ein Anruf innerhalb der AUN-Gruppe durch einem kurzen Standard-Klingelton signalisiert. Wenn nicht, wird ein solcher Anruf durch einen kurzen Aufmerksamkeitston signalisiert.

Hinweisart bei AUN Gruppe:

Auswahl der benutzerseitigen Aktionen, um einen Anruf innerhalb der AUN-Gruppe entgegenzunehmen.

Mögliche Optionen:

- **Prompt**
  Der AUN-Anruf wird auf dem Display durch einen Alert angezeigt. Sobald der Benutzer den Hörer abhebt oder die Lautsprechertaste drückt, wird der Anruf angenommen. Auch durch eine entsprechend eingerichtete Funktionstaste kann der Anruf angenommen werden.
- **Notify**
  Der AUN-Anruf wird auf dem Display durch einen Alert angezeigt. Um den Anruf anzunehmen, muss der Benutzer den Alert bestätigen oder die entsprechend eingerichtete Funktionstaste drücken.
- **FPK only**

  Der AUN-Anruf wird nur auf der entsprechend eingerichteten Funktionstaste angezeigt. Um den Anruf anzunehmen, muss der Benutzer diese Funktionstaste drücken.

Rufton-Einstellungen

Rufton-Melodie:

Mögliche Optionen, siehe Abschnitt 7.1.12.3, “Rufton-Melodie:”

Rufton-Folge:

Mögliche Optionen:

- **1 sek EIN, 4 sek AUS**
- **1 sek EIN, 2 sek AUS**
- **0,7 sek EIN, 0,7 sek AUS, 0,7 sek EIN, 3 sek AUS**

Rufton-Datei:

Name der Datei, die den Rufton enthält.

Tastenklick

Lautstärke:

Lautstärke des Tastenklicks einstellen.

Mögliche Werte:

- **Aus**
- **Niedrig**
- **Mittel**
- **Hoch**

Tasten:

Tastenart, für die Tastenklick hörbar sein soll, einstellen.

Mögliche Werte:

- **Nur Wähltastatur**
- **Alle Tasten**

8.1.10 Applikationen

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Applikationen

Dieser Bereich besteht aus folgenden Inhalten:

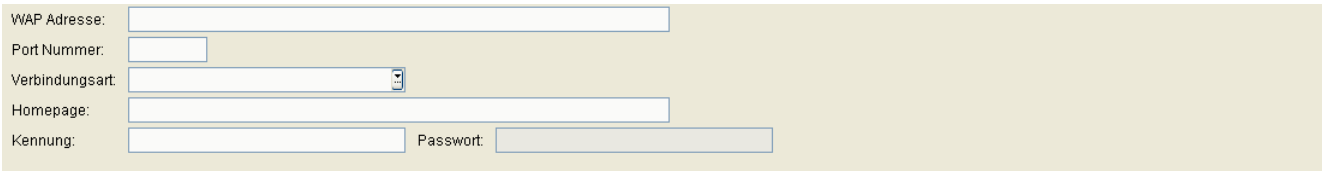
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „WAP“
- Register „Java“
- Register „XML Applikationen“
- Register „Applikationsliste“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.10.1 Register „WAP“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Applikationen > Register „WAP“



WAP Adresse:

IP-Adresse oder Hostname des WAP-Servers.

Port Nummer:

Portnummer des WAP-Servers.

Verbindungsart:

Protokoll-Typ der Verbindung zum WAP-Server.

Mögliche Optionen:

- **HTTP**
- **WSP**

Homepage:

URL der Startseite, auf der sich die WAP-Homepage befindet.

Kennung:

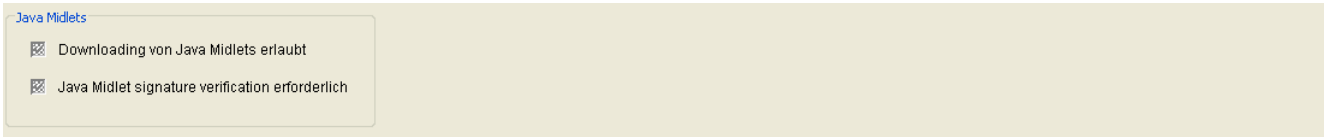
Benutzerkennung zur Identifikation am WAP-Server.

Passwort:

Passwort der Benutzerkennung.

8.1.10.2 Register „Java“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Applikationen > Register „Java“



Java Midlets

Downloading von Java Midlets erlaubt

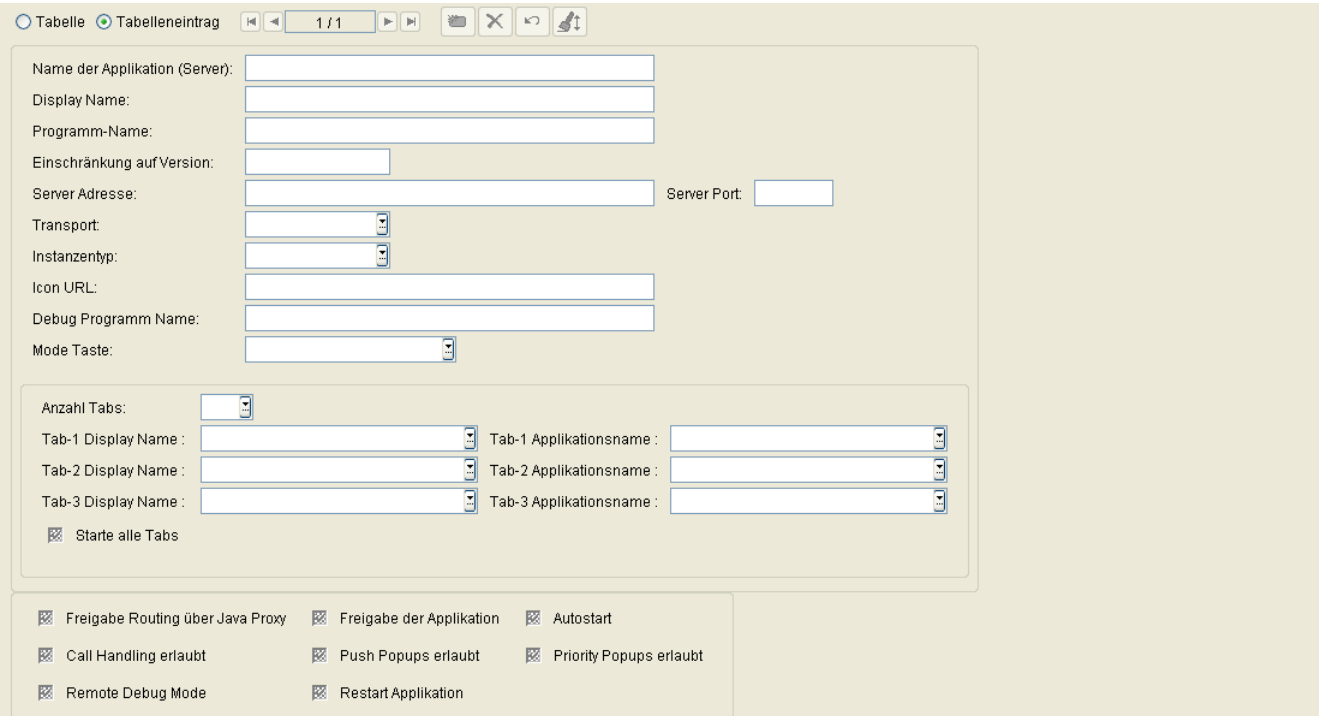
Ist der Schalter aktiviert, wird das Herunterladen von Java-Midlets auf den Workpoint erlaubt.

Java Midlet signature verification erforderlich

Ist der Schalter aktiviert, wird das Verifizieren des Java-Midlets mithilfe einer Signatur verlangt.

8.1.10.3 Register „XML Applikationen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Applikationen > Register „XML Applikationen“



Informationen zu den XML-Applikationen finden Sie unter Abschnitt 7.1.14.4, “Register „XML Applikationen“”.

XML Applikationen

Name der Applikation (Server):

Dieser Name wird von der Software des Workpoints intern benutzt, um die Applikation zu identifizieren.

Display Name:

Unter diesem Namen wird die Applikation auf dem Menü des Workpoints aufgelistet.

Programm-Name:

Pfad der Startdatei des serverseitigen Programms, relativ zur Server-Adresse.

Einschränkung auf Version:

Auswahl einer definierten Version, mit der gearbeitet werden soll.

Server Adresse:

IP-Adresse des Servers, auf dem das Programm läuft.

Beispiel: **192.168.1.150.**

Server Port:

Port, auf dem das serverseitige Programm Daten vom Workpoint empfängt.

Beispiele: **80** (Default-Port Apache); **8080** (Default-Port Tomcat).

Transport:

Transportprotokoll für die Übermittlung der XML-Daten.

Mögliche Optionen:

- **HTTP**
- **HTTPS**

Instanzentyp:

Auswahl des Instanzentyps.

Mögliche Optionen:

- **Normal**
- **Xpressions**
- **Phonebook**

Icon URL:

URL des Applikations-Icons (noch nicht implementiert).

Debug Programm Name:

Name und ggf. Verzeichnispfad des Programms auf dem Server, das Fehlermeldungen der XML-Applikationsplattform des Endgeräts entgegennimmt.

Mode Taste:

Auswahl einer Mode-Taste, mit der die Applikation gestartet wird.

Mögliche Optionen:

- **Keine Mode Taste**
- **Phonebook-Mode Taste**
- **Call-Mode Taste**
- **Message-Mode Taste**
- **Hilfe-Mode Taste**

Anzahl Tabs:

Anzahl der Tabs in einer XML Applikation, die im Display des Endgerätes angezeigt werden.

Wertebereich: **0** ... **3**

HINWEIS: Für alle XML-Applikationen, die eine Anzahl Tabs > 0 eingetragen haben, muss zwingend einer der Einträge für **Tab-1 Applikationsname** bis **Tab-3 Applikationsname** gleich dem Eintrag in **Name der Applikation (Server)** sein. Beim Start der XML-Applikation wird dann der Tab mit dem gleichen Namen als Erster geöffnet.

Tab-1 Display Name

Beschriftung des 1. Tabs zur Anzeige im Display des Endgerätes.

Tab-2 Display Name

Beschriftung des 2. Tabs zur Anzeige im Display des Endgerätes.

Tab-3 Display Name

Beschriftung des 3. Tabs zur Anzeige im Display des Endgerätes.

Tab-1 Applikationsname

Aufrufname der Applikation, die im 1. Tab aufgerufen wird. Er muss über alle XML Applikationen hinweg eindeutig sein.

Tab-2 Applikationsname

Aufrufname der Applikation, die im 2. Tab aufgerufen wird. Er muss über alle XML Applikationen hinweg eindeutig sein.

Tab-3 Applikationsname

Aufrufname der Applikation, die im 3. Tab aufgerufen wird. Er muss über alle XML Applikationen hinweg eindeutig sein.

Starte alle Tabs

Beim Start der Applikation werden alle Tabs geöffnet.

Freigabe Routing über Java Proxy

Schalter für die Freigabe des Routings über Java Proxy.

Freigabe der Applikation

Schalter zum Einschalten der Applikation.

Autostart

Schalter zum Aktivieren des Autostarts der Applikation.

Call Handling erlaubt

Schalter zum Aktivieren des Call Handlings.

Push Popups erlaubt

Schalter zum Aktivieren des Push Popups.

Priority Popups erlaubt

Schalter zum Aktivieren von priorisierten Popups.

Remote Debug Mode

Schalter zum Aktivieren des Remote Debug Modus.

Restart Applikation

Neustart der Applikation, wenn diese bereits läuft.

8.1.10.4 Register „Applikationsliste“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Applikationen > Register „Applikationsliste“

Liste von Applikationen für Funktionstasten:

Liste von durch Komma getrennten Applikationsnamen, die mittels Funktionstasten gestartet werden können.

8.1.11 LDAP

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > LDAP

Dieser Bereich besteht aus folgenden Inhalten:

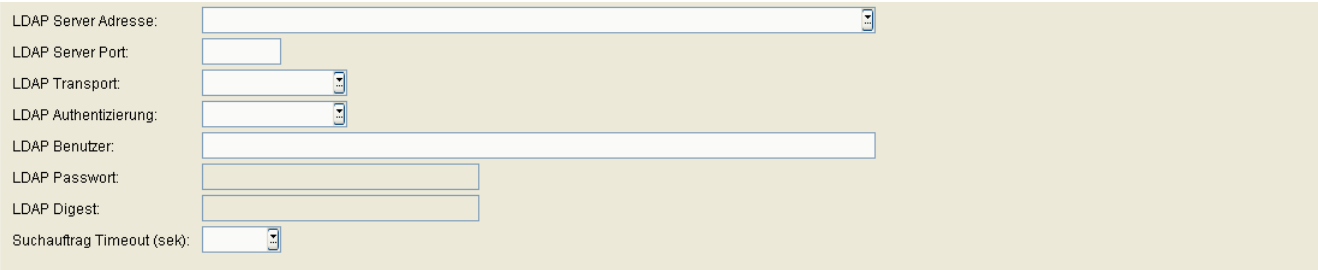
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „LDAP Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”

8.1.11.1 Register „LDAP Einstellungen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > LDAP > Register „LDAP Einstellungen“



LDAP Server Adresse:

IP-Adresse oder Hostname des LDAP-Servers.

LDAP Server Port:

Portnummer des LDAP-Servers.

LDAP Transport:

Transportprotokoll, mit dem LDAP-Daten übertragen werden.

Mögliche Optionen:

- **TCP**

LDAP Authentifizierung:

Auswahl des LDAP-Zugangs.

Mögliche Optionen:

- **Anonym**
- **Einfach**

LDAP Benutzer:

Benutzername für den authentifizierten LDAP-Zugang.

LDAP Passwort:

Passwort für den authentifizierten LDAP-Zugang.

LDAP Digest:

Einstellung des LDAP Digest.

Suchauftrag Timeout (sek):

Wert für Zeitüberschreitung beim Suchauftrag für LDAP Einfachsuche in Sekunden.

Mögliche Optionen:

- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **60**

8.1.12 Anwendereinstellungen

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Anwendereinstellungen

Dieser Bereich besteht aus folgenden Inhalten:

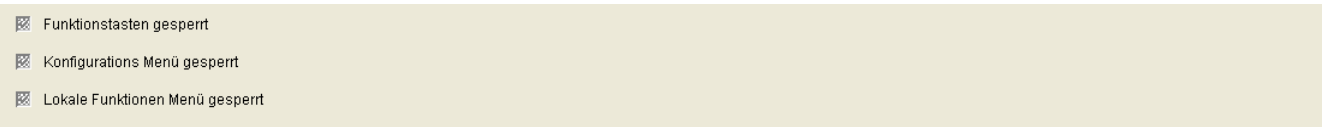
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Einschränkungen“
- Register „gesperrte Konfigurationsmenüs“
- Register „gesperrte lokale Funktionen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.12.1 Register „Einschränkungen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Anwendereinstellungen > Register „Einschränkungen“



Funktionstasten gesperrt

Schalter zum Sperren der Funktionstasten am Mobility Phone für Mobile User.

Konfigurationsmenüs gesperrt

Schalter zum Sperren des Konfigurations-Menüs am Mobility Phone für Mobile User.

Lokale Funktionen Menüs gesperrt

Schalter zum Sperren des Lokale Funktionen-Menüs am Mobility Phone für Mobile User.

8.1.12.2 Register „gesperrte Konfigurationsmenüs“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Anwendereinstellungen > Register „gesperrte Konfigurationsmenüs“

Folgende Funktionen im Konfigurations-Menü können für den Mobile User gesperrt werden, indem das jeweilige Häkchen gesetzt wird:

1-Ländereinstellungen

Der Benutzer kann ein Land aus einer Liste auswählen, um das Telefon an landesspezifische Gegebenheiten anzupassen.

2-Sprache

Der Benutzer kann die Sprache für das Administrations- und Benutzermenü einstellen.

3-Datum / Zeit

Der Benutzer kann Ortszeit, Datum und Sommer/Winterzeit einstellen.

4-Anrufweiterleitung

Der Benutzer kann die Anrufweiterleitung aktivieren oder deaktivieren.

5-Anrufumleitung

Der Benutzer kann die Anrufumleitung aktivieren oder deaktivieren.

6-Umgeleitete Anrufe

Der Benutzer kann das Protokollieren von umgeleiteten Anrufen aktivieren oder deaktivieren.

7-Gesprächsdauer

Der Benutzer kann bestimmen, ob die Gesprächsdauer im Display angezeigt wird.

Nur bei optiPoint verfügbar.

8-Anklopfen

Der Benutzer kann bestimmen, ob ein Zweitanruf während einer bestehenden Verbindung zugelassen wird. Falls nicht, hört der Anrufer das Besetztzeichen.

9-Übergabe

Der Benutzer kann die Gesprächsübergabe zulassen.

10-Verbinden

Der Benutzer die Möglichkeit, einen aktiven und einen gehaltenen Teilnehmer miteinander zu verbinden, ein- oder ausschalten.

11-Kontrast

Der Benutzer kann den Kontrast für das Display einstellen.

12-Wählmodus

Der Benutzer kann bestimmen, ob beim Wählen nur eine Nummer oder auch ein Name eingegeben werden kann.

Nur bei optiPoint verfügbar.

13-Anrufer-ID anzeigen

Der Benutzer bestimmt, welche Informationen zum Anrufer bei einem eingehenden Anruf angezeigt werden sollen.

Nur bei optiPoint verfügbar.

14-Sommerzeit

Der Benutzer kann die Sommerzeit einstellen.

15-Wahlverzögerung

Der Benutzer kann die Verzögerung einstellen, mit der der Wählvorgang gestartet wird, nachdem die letzte Ziffer einer Rufnummer eingegeben worden ist.

16-CFNR Verzögerung

Der Benutzer kann die Verzögerung einstellen, mit der ein Anruf umgeleitet wird, wenn die Anrufumleitung bei Nichtmelden aktiviert ist.

17-Zeit für Halteerinnerung

Der Benutzer kann die Zeit einstellen, nach deren Ablauf an ein gehaltenes Gespräch erinnert wird.

18-Wartemusik

Der Benutzer kann bestimmen, ob die im Telefon gespeicherte Wartemusik (Music on Hold) verwendet wird. Ist die Wartemusik aktiviert, wird diese abgespielt, sobald das Telefon ins Halten gelegt wird.

19-Anrufschutz

Der Benutzer kann bestimmen, ob der Anrufschutz (Do Not Disturb) auf dem Telefon eingerichtet werden kann. Ist der Anrufschutz aktiviert, läutet das Telefon bei einem eingehenden Anruf nicht, und der Anrufer erhält das Besetztzeichen.

20-Nachricht vorhanden

Der Benutzer kann bestimmen, ob eine LED signalisiert, wenn neue Nachrichten in der Mailbox sind.

Nur bei optiPoint verfügbar.

21-Halteerinnerungston

Ist diese Funktion aktiviert und ein Gesprächspartner wurde ins Halten gelegt, ertönt nach einer einstellbaren Zeit ein Signal, um daran zu erinnern, dass ein Gespäch anliegt. Der Benutzer kann diese Funktion zulassen und die Verzögerung bis zum Erklingen des Erinnerungstons einstellen.

22-Konferenz

Der Benutzer kann anlagengestützte Konferenzen zulassen.

Nur bei optiPoint verfügbar.

23-Lokale Konferenz

Der Benutzer kann telefongestützte Dreierkonferenzen zulassen.

32-Rufannahme CTI

Der Benutzer kann bestimmen, ob eingehende Anrufe automatisch über die mit dem Telefon verbundene CTI-Anwendung angenommen werden.

33-Piepton Rufannahme

Der Benutzer kann bestimmen, ob bei automatisch über die mit dem Telefon verbundene CTI-Anwendung angenommenen Anrufen ein Piepton ertönt.

34-Auto. Wiederverbin.

Der Benutzer kann bestimmen, ob ein gehaltenes Gespräch über die CTI-Applikation automatisch wieder aufgenommen werden kann.

35-Piepton Auto. Wiederverbind.

Der Benutzer kann bestimmen, ob ein Piepton ertönt, wenn ein gehaltenes Gespräch über die CTI-Applikation wieder aufgenommen wird.

36-Bereit-Zustand

Der Benutzer kann die Anzeige von Systemnachrichten im Ruhezustand konfigurieren.

Nur bei optiPoint verfügbar.

38-Zeitlimit für Inaktiv.

Der Benutzer kann die Verzögerungszeit zwischen der letzten Eingabe und der Rückkehr in den Ruhezustand einstellen.

39-APM Anrufansicht

Der Benutzer kann die Anrufansicht auf dem optiPoint application module aktivieren oder deaktivieren.

40-USB Tastatur Typ

Der Benutzer kann die Sprache der USB-Tastatur eines optiPoint-Telefons festlegen.

Nur bei optiPoint verfügbar.

43-Weiterleitungsziel

Der Benutzer kann die Zielnummer für die Weiterleitung eingeben bzw. verändern.

44-Leitungs-Einstellungen

Der Benutzer kann die Eigenschaften einer Leitungstaste konfigurieren.

45-Symbole Anrufansicht

Der Benutzer kann festlegen, ob Meldungen auf dem optiPoint display module, wie z. B. die Auflistung entgangener Anrufe, als Text oder als Symbole erscheinen.

46-Anruf parken

Der Benutzer kann das Parken von Anrufen zulassen.

47-Anruf entparken

Der Benutzer kann das Entparken von Anrufen zulassen.

48-Sofortwählen

Der Benutzer kann Sofortwählen zulassen.

49-Rückruf / Rückruf bei Besetzt

Der Benutzer kann die Übermittlung eines Rückrufwunschs an die Anlage aktivieren. Bei OpenStage V3 oder höher kann der Rückrufwunsch in jedem Fall abgesetzt werden, bei anderen Endgeräten nur im Besetztfall.

50-Rückruf bei Ruf/nicht melden

Der Benutzer kann die Übermittlung eines Rückrufwunschs an die Anlage für den Fall, dass sein Anruf nicht angenommen wird, aktivieren.

Nur bei OpenStage verfügbar.

51-Meldung verpasste Anrufe

Der Benutzer kann die Meldung verpasster Anrufe auf dem Display aktivieren.

Nur bei optiPoint verfügbar.

52-Besetzt bei Wählen

Der Benutzer kann bestimmen, ob ein Abruf abgewiesen wird, der während der Eingabe einer Rufnummer eingeht.

Der Benutzer kann bestimmen, ob ein Abruf abgewiesen wird, der während der Eingabe einer Rufnummer eingeht.

53-Vermitteln im Rufzustand

Der Benutzer kann bestimmen, ob die Übergabe eines Gesprächs bereits dann erfolgt, wenn das Telefon des dritten Teilnehmers läutet, auch wenn der Übergebende den Hörer noch nicht aufgelegt hat.

54-Mobility flash LED

Der Benutzer kann bestimmen, ob die LED der Mobilitäts-Taste blinkt, während Daten zwischen Telefon und DLS ausgetauscht werden, wie z. B. bei der An- und Abmeldung.

Nur bei optiPoint verfügbar.

55-Anrufaufzeichnung

Der Benutzer kann die Aufzeichnung von Anrufen aktivieren.

Nur bei optiPoint verfügbar.

56-Secure Call Anzeige

Der Benutzer kann bestimmen, ob ein Aufmerksamkeitson ertönt, wenn die Sprachverbindung ungesichert ist.

57-Vermitteln durch Auflegen

Der Benutzer kann bestimmen, ob bei einem gehaltenen und einem aktiven Gespräch die beiden Gesprächspartner miteinander verbunden werden können, indem der Benutzer selbst auflegt.

60-Audio Einstellungen

Der Benutzer kann Einstellungen wie Klingeltöne und Raumakustik vornehmen.

Nur bei OpenStage verfügbar.

61-Lautsprecher

Der Benutzer kann die Freisprechfunktion aktivieren oder deaktivieren.

Nur bei OpenStage verfügbar.

62-Anrufumleitungshinweise

Der Benutzer kann bestimmen, ob optische oder akustische Warnhinweise gegeben werden, sobald ein Anruf bei eingeschalteter Umleitung eingeht. Nur bei OpenStage verfügbar.

63-Verbinden in Konferenz

Der Benutzer kann bestimmen, ob es möglich ist, bei einer Konferenz die beiden anderen Gesprächspartner miteinander zu verbinden und selbst die Konferenz zu verlassen.

Nur bei OpenStage verfügbar.

64-Bluetooth

Der Benutzer kann die Bluetooth-Konnektivität aktivieren oder deaktivieren.

65-Display Oberfläche

Der Benutzer kann das Design der Benutzeroberfläche auswählen.

Nur bei OpenStage 60/80 verfügbar.

66-Bildschirmschoner

Der Benutzer kann den Bildschirmschoner des Telefons aktivieren sowie die Verzögerungszeit für den Start des Bildschirmschoners einstellen.

Nur bei OpenStage 60/80 verfügbar.

67-Anruf-Kontext Menü

Der Benutzer kann das angezeigte Menü festlegen

Nur bei OpenStage 60/80 verfügbar.

68-BLF

Der Benutzer kann festlegen, wie ein ankommender Anruf für das mit der BLF-Taste überwachte Telefon angezeigt wird.

69-Zuordnung umschalten

Dieses Leistungsmerkmal besteht in einer weiteren Möglichkeit der Gesprächsübergabe. Wenn aktiviert, so ergibt sich der folgende Ablauf: Der Benutzer hat einen Zweitanruf angenommen, wodurch das erste Gespräch ins Halten gelegt wird. Sobald der Benutzer einmal zurück zum ersten Gespräch und danach wieder zum zweiten Gespräch gewechselt hat, kann er die beiden Gesprächspartner miteinander verbinden, indem er einfach auflegt.

Bei allen OpenStage-Telefonen verfügbar.

70- Anzeige umleitender Teilnehmer

Der Benutzer kann bei Mehrfachumleitungen festlegen, ob der zuerst umleitende oder der zuletzt umleitende Teilnehmer angezeigt wird.

Für alle OpenStage SIP-Telefone verfügbar.

71- Headset

Der Benutzer kann den Typ des angeschlossenen Headsets festlegen.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

72- Tastenklick

Der Benutzer kann die Art des Tastenklick festlegen.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

73- Rufjournal (Rufliste) aktivieren

Der Benutzer kann eine Rufliste aktivieren, in der alle entgangenen, gewählten, empfangenen oder weitergeleiteten Anrufe aufgeführt sind. Die Rufliste kann über das WPI gelöscht werden. Für OpenStage 15/20/20E/40/60/80 SIP/HFA verfügbar.

74- Hold and hang-up

Schalter zum Aktivieren der Funktion „Halten und Auflegen“ bei nicht-Keyset OpenStage-Telefonen.

Mit dieser Funktion können Teilnehmer Anrufe vorübergehend halten und auflegen, ohne den Anrufer zu trennen. Diese Funktion ist standardmäßig deaktiviert.

75- Lower IL alert notification

Der Benutzer wird informiert, wenn ein kommender Anruf aus einer niedrigeren Sicherheitszone stammt oder wenn ein gehender Anruf in einer niedrigeren Sicherheitszone geht.

Für OpenStage 40/60/80 SIP/HFA verfügbar.

76 - Video erlauben

Schalter zum Aktivieren der Funktion „Video Call“ bei nicht-Keyset OpenStage-Telefonen.

Diese Funktion ermöglicht Video-Anrufe.

Für OpenStage 60/80 SIP/HFA verfügbar.

77- Entgangene Anrufe

Der Benutzer kann festlegen, ob Anrufe, die andernorts angenommen wurden, an seinem Telefon protokolliert werden.

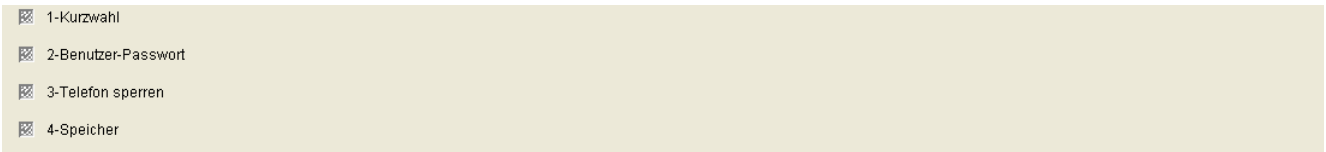
Für OpenStage 15/20/20E/60/80 SIP/HFA verfügbar.

78- Display Helligkeit

79- Hintergrundbeleuchtung Timeout energiesparendes Display

8.1.12.3 Register „gesperrte lokale Funktionen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Anwendereinstellungen > Register „gesperrte lokale Funktionen“



Folgende lokale Funktionen können für den Mobile User gesperrt werden, indem das jeweilige Häkchen gesetzt wird:

1-Kurzwahl

Der Benutzer kann Kurzwahlnummern einrichten.

Nur bei optiPoint verfügbar.

2-Benutzer-Passwort

Der Benutzer kann sein Passwort ändern.

3-Telefon sperren

Der Benutzer kann das Telefon sperren. Ist das Telefon gesperrt, kann kein Unbefugter von diesem Telefon aus regulär telefonieren oder Einstellungen ändern. Nur Notrufnummern und vordefinierte Nummern aus dem Wählplan können gewählt werden.

4-Speicher

Der Benutzer kann alle Kurzwahlnummern löschen sowie das Telefon wieder in den Lieferzustand versetzen.

Nur bei optiPoint verfügbar.

8.1.13 SIP Mobility

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > SIP Mobility

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Mobility Logon/Logoff“
- Register „Mobility Data“

8.1.13.1 Register „Mobility Logon/Logoff“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > SIP Mobility > Register „Mobility Logon/Logoff“

Einstellungen für Forced Logon

Ist der Schalter aktiv, kann der Mobile User während eines Gesprächs vom Endgerät angemeldet werden. Die Anmeldung findet nach der im Feld **Zeitdauer bis Forced Logon** festgelegten Zeit statt. Ist der Schalter inaktiv, wird eine während des Gesprächs versuchte Anmeldung auch dann nicht erzwungen, wenn das Gespräch beendet ist. Die erzwungene Anmeldung muss dann erneut gestartet werden.

Einstellungen für Forced Logoff

Ist der Schalter aktiv, kann der Mobile User während eines Gesprächs vom Endgerät abgemeldet werden. Die Abmeldung findet nach der im Feld **Zeitdauer bis Forced Logoff** festgelegten Zeit statt. Ist der Schalter inaktiv, wird eine während des Gesprächs versuchte Abmeldung auch dann nicht erzwungen, wenn das Gespräch beendet ist. Die erzwungene Abmeldung muss dann erneut gestartet werden.

Einstellungen für SNMP Trap

Ist der Schalter aktiv, wird bei jedem unerlaubten Remote Logoff-Versuch eine Meldung zum SNMP-Server gesendet. Zum Eintragen der SNMP-Serverdaten siehe Abschnitt 7.1.13.1, “Register „SNMP“”.

Logon ohne SIP Server / Registrar / Gateway Adressen

Ist der Schalter aktiv, werden beim Logon des Mobile Users folgende Daten nicht an das Endgerät geschickt: SIP Server Adresse/Port, SIP Registrar Adresse/Port, SIP Gateway Adresse/Port.

Logon mit Forced Logoff

Ist der Schalter aktiv, wird die Abmeldung des Mobile Users erzwungen, sobald sich ein anderer Benutzer am Endgerät anmeldet.

Logoff Mobile User mit Passwort

Ist der Schalter aktiv, ist das Abmelden eines Mobile Users nur möglich, wenn das Passwort des aktuell angemeldeten Mobile Users eingegeben wird.

Zeitdauer bis Forced Logon

Zeitdauer in Sekunden, bis die erzwungene Anmeldung stattfindet. Die Angabe ist nur dann relevant, wenn die Option **Forced Logon während Gespräch** aktiviert ist. Es kann ein Wert von 0 bis 180 eingegeben werden.

Zeitdauer bis Forced Logoff

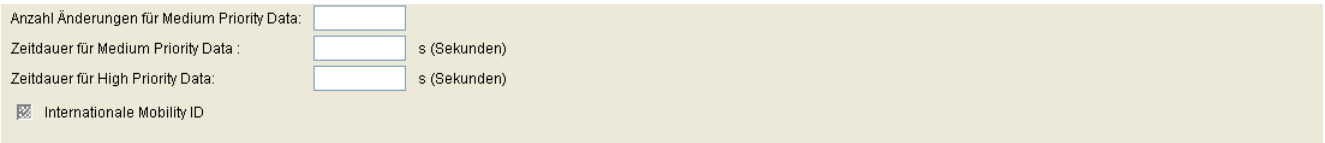
Zeitdauer in Sekunden, bis die erzwungene Abmeldung stattfindet. Die Angabe ist nur dann relevant, wenn die Option „Forced Logoff während Gespräch“ aktiviert ist. Es kann ein Wert von 0 bis 180 eingegeben werden.

Verzögerung SNMP Trap

Zeitdauer in Sekunden, bis der SNMP Trap gesendet wird. Zum Eintragen der SNMP-Serverdaten siehe Abschnitt 7.1.13.1, “Register „SNMP“”.

8.1.13.2 Register „Mobility Data“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > SIP Mobility > Register „Mobility Data“



Anzahl Änderungen für Medium Priority Data:

Angabe, nach der wievielten Änderung von Daten mittlerer Priorität im Workpoint diese Daten an den DLS geschickt werden.

Zeitdauer für Medium Priority Data:

Angabe, nach welcher Zeitspanne seit der letzten Änderung von Daten mittlerer Priorität im Workpoint diese Daten an den DLS geschickt werden.

Zeitdauer für High Priority Data:

Angabe, nach welcher Zeitspanne seit der letzten Änderung von Daten hoher Priorität im Workpoint diese Daten an den DLS geschickt werden.

Internationale Mobility ID

Ist der Schalter aktiviert, fügt das Endgerät beim Anmelden eines Mobile Users neben Amtsnummer und Ortskennzahl auch die Landeskennzahl automatisch an die Extension an. Die internationale Kennzahl wird unter **Mobile User** > **SIP Mobile User Konfiguration** > **Wahlparameter** > **Register „Rufnummern“** -> **Internationale Vorwahl** eingerichtet.

Beispiel: Der Benutzer meldet sich am Endgerät mit der Extension/Mobility ID „31434“ an. Ist der Schalter aktiviert, schickt das Endgerät die Nummer „498972231434“. Andernfalls schickt das Endgerät „8972231434“.

8.1.14 Keysets / Tastenbelegung

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Keysets / Tastenbelegung

Dieser Bereich besteht aus folgenden Inhalten:

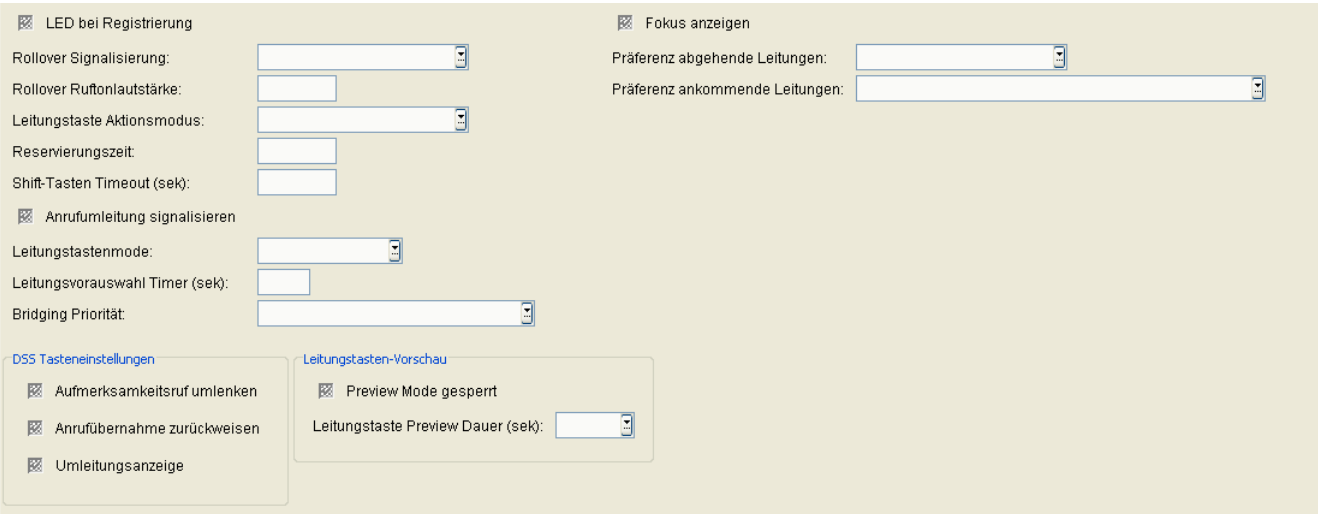
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Keysets“
- Register „Ziele“
- Register „Send URL Server CA Zertifikat“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.14.1 Register „Keysets“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Keysets / Tastenbelegung > Register „Keysets“



LED bei Registrierung

Schalter zum Aktivieren der Anzeige beim Neustart des IP Phones, ob der Workpoint erfolgreich registriert wurde.

Nur bei SIP-Workpoints verfügbar.

Rollover Signalisierung:

Art der der Signalisierung im Besetztfall.

Mögliche Optionen:

- **Kein Ton**
- **Hinweisruf**
- **Standard**
- **Hinweiston**

Nur bei SIP-Workpoints verfügbar.

Rollover Ruftonlautstärke:

Lautstärke der Signalisierung im Besetztfall.

Nur bei SIP-Workpoints verfügbar.

Leitungstaste Aktionsmodus:

Legt fest, was mit einer Leitung (Gespräch) geschehen soll, wenn eine Verbindung über eine andere Leitung hergestellt wird.

Mögliche Optionen:

- **Halten**
  Das Gespräch der ursprünglichen Leitung wird gehalten.
- **Freigeben**
  Die Verbindung der ursprünglichen Leitung wird getrennt (das Gespräch wird beendet).

Nur bei SIP-Workpoints verfügbar.

Reservierungszeit:

Zeit in Sekunden, die angibt, wie lange eine Leitungsreservierung aufrechterhalten wird.

Standard: 60 s.

Nur bei SIP-Workpoints verfügbar.

Shift-Tasten Timeout (sek):

Zeit in Sekunden, nach deren Ablauf die Shift-Taste inaktiv wird, so dass die Tasten wieder mit den Funktionen der 1. Ebene belegt sind.

Anrufumleitung signalisieren

Schalter zum Aktivieren der Signalisierung bei einer Leitungstaste, wenn bei deren Ziel eine Rufweiterschaltung aktiv ist.

Nur bei SIP-Workpoints verfügbar.

Leitungstastenmode

Funktionsweise der Leitungstaste.

Mögliche Optionen:

- **Einzeltaste**
  Die an die Leitungstaste gebundene Aktion wir sofort mit dem Betätigen der Taste ausgelöst, ohne Rücksicht darauf, ob der Hörer abgenommen oder aufgelegt ist.

- **Vorauswahl**
  Bei Betätigung der Leitungstaste erhält die Leitung den Fokus. Wenn eine Leitung benötigt wird, z. B. nach Abheben des Hörers, wird diese Leitung benutzt.

Leitungsvorauswahl Timer (sek)

Zeitdauer der Leitungsvorauswahl in Sekunden.

Bridging Priorität

Mögliche Optionen:

- **Bridging vor preview**
- **Preview vor bridging**

Fokus anzeigen

Schalter zum Aktivieren der Anzeige, welche Leitung momentan aktiv ist (Leitung hat den Fokus).

Nur bei SIP-Workpoints verfügbar.

Präferenz abgehende Leitungen:

Festlegung der bevorzugt zu verwendenden Leitung bei abgehenden Anrufen.

Mögliche Optionen:

- **Ruhende Leitung bevorzugt**
- **Primärleitung bevorzugt**
- **Letzte Leitung bevorzugt**
- **Kein Vorzug**

Nur bei SIP-Workpoints verfügbar.

Präferenz ankommende Leitungen:

Festlegung der bevorzugt zu verwendenden Leitung bei eingehenden Anrufen.

Mögliche Optionen:

- **Rufende Leitung bevorzugt**

- **Rufende Leitung bevorzugt mit Primärleitung bevorzugt**
- **Rufende Leitung bevorzugt**
- **Ankommende Leitung bevorzugt mit Primärleitung bevorzugt**
- **Kein Vorzug**

Nur bei SIP-Workpoints verfügbar.

DSS Tasteneinstellungen

Aufmerksamkeitsruf umlenken

Schalter zum Aktivieren der Funktion „Aufmerksamkeitsruf umlenken“.

Anrufübernahme zurückweisen

Schalter zum Aktivieren der Funktion „Anrufübernahme zurückweisen“.

Umleitungsanzeige

Schalter zum Aktivieren der Umleitungsanzeige.

Leitungstasten-Vorschau

Preview Mode gesperrt

Schalter zum Deaktivieren des Vorschau-Modus.

Leitungstaste Preview Dauer (sek):

Zeitdauer des Vorschau-Modus in Sekunden.

Mögliche Optionen:

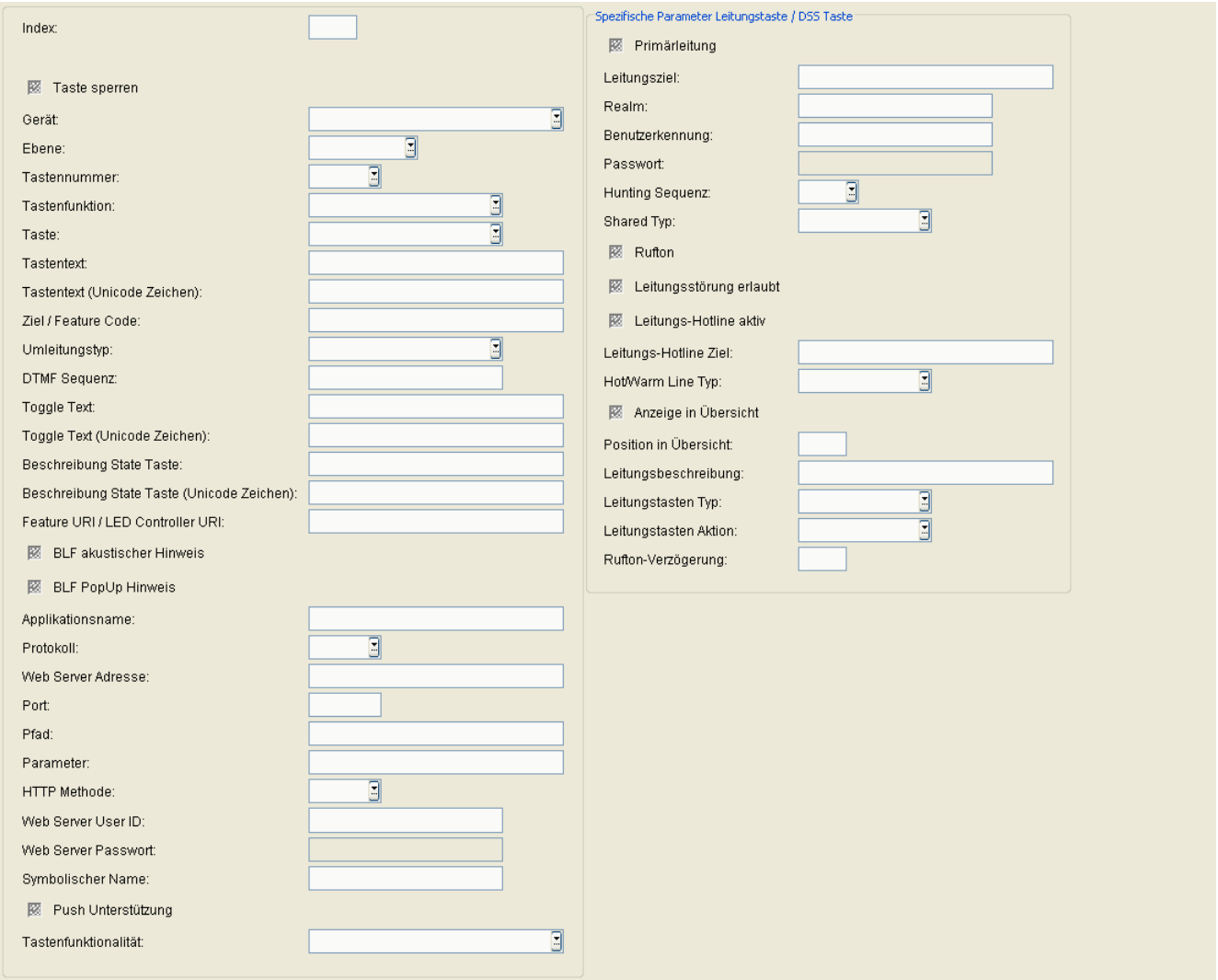
- **2**
- **3**
- **4**
- **6**
- **8**

- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**

8.1.14.2 Register „Ziele“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Keysets / Tastenbelegung > Register „Ziele“

HINWEIS: Sorgen Sie beim Erstellen einer Tastenbelegung dafür, dass die von einem Mobile User für die Primärleitung verwendete Taste auf alle Gerätetypen verfügbar ist.
Wenn die Primärleitung einer Taste zugewiesen ist, die auf dem Gerät, an dem der Mobile User angemeldet ist, nicht existiert, steht dem Mobile User keine Primärleitungstaste zur Verfügung. Dies kann man vermeiden, indem man entsprechende Einstellungen in der Maske **SIP Mobile User Interaktion** > **SIP User Tastenbelegung** anwendet.



Index:

Name der Funktion der Tastenbelegung.

Taste sperren

Sperrt die Taste für den Benutzer.

Gerät

Gibt an, für welches Gerät die entsprechende Tastenbelegung gültig ist.

Mögliche Optionen:

- **Basis Gerät**
- **1. Key module**
- **2. Key module**
- **1. Self Labeling Key module**
- **2. Self Labeling Key module**
- **OpenStage 15 Key module**

Nur bei SIP-Workpoints verfügbar.

Ebene

Tastenebene für Shift-Funktionalität.

Mögliche Optionen:

- **1. Ebene**
- **2. Ebene**
- **3. Ebene**
- **4. Ebene**
- **Fixed Keys**
  Diese Tasten haben feste Tastennummern und können am Endgerät weder gelöscht noch hinzugefügt werden.

Nur bei SIP-Workpoints verfügbar.

Tastennummer

Nummer der Taste, die die entsprechende Funktion zugewiesen bekommt.

Wurde bei **Ebene** „Fixed Keys“ ausgewählt, haben folgende Tastennummern feste Funktionen:

1 Fixed Keys – Trennen

2 Fixed Keys – Anrufumleitung

3 Fixed Keys – Sprachwahl

9 Fixed Keys – Wahlwiederholung

Entsprechend der eingetragen Tastennummer wird bei **Tastenfunktion** eine Auswahl der möglichen Funktionen angezeigt.

Nur bei SIP-Workpoints verfügbar.

Tastenfunktion

Folgende Tastenfunktionen werden unterstützt:

- **Keine Funktion**
- **Zielwahl**
- **Kurzwahl**
- **Wahlwiederholung**
- **Anruferliste**
- **Nachrichten**
- **Anruf umleiten**
- **Lautsprecher**
- **Mikrofon aus**
- **Rufton aus**
- **Halten**
- **Makeln**
- **Ohne Rückfrage verbinden**
- **Verbinden (OpenStage) / Übergabe (optiPoint)**
- **Weiterleiten**
- **Service Menü**
- **Raum hallend**
- **Raum gedämpft**
- **SHIFT-Taste**
- **Notizbuch**
- **Einstellungen**

- **Telefon sperren**
- **Konferenz**
- **Lokale Konferenz**
- **Headset**
- **Anrufschutz**
- **Anrufübernahme**
- **Erweiterte Zielwahl**
- **Leitungstaste**
- **Funktionsumschaltung**
- **Zeige Telefon-Display**
- **Displaywechsel**
- **Mobility**
- **Parken**
- **Übernahme geparktes Gespräch**
- **Abbrechen**
- **Ok Confirm (OK)**
- **Rückruf**
- **Rückruf löschen**
- **Rückfrage (OpenStage) / Rückfrage/Übergabe (optiPoint)**
- **DSS**
- **State-Taste**
- **Anklopfen**
- **Sofortiger Ruf**
- **Preview Taste**
- **Sprachaufzeichnung**
- **AICS Zip**
- **Server Feature**
  Sowohl für frei programmierbare Tasten als auch für ‘Fixed Keys’ möglich.
- **BLF**
- **Applikation starten**
  Sowohl für frei programmierbare Tasten als auch für ‘Fixed Keys’ möglich.

- **Sende URL**
  Sowohl für frei programmierbare Tasten als auch für ‘Fixed Keys’ möglich.
- **Built-in Anrufumleitung**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Built-in Trennen**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Built-in Sprachwahl**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Built-in Wahlwiederholung**
  Nur für Ebene ‘Fixed Keys’ möglich.
- **Telefonbuch starten**
- **2. Ruf**

Taste:

Zeigt an, ob es sich um eine frei programmierbare Taste oder um einen ’Fixed Key’ handelt.

Tastentext:

Bei Self labeling Keys-Workpoints (z. B. optiPoint 420 standard) kann hier für jede Funktionstaste eine Tastenbeschriftung angegeben werden.

Nur bei SIP-Workpoints verfügbar.

Tastentext (Unicode):

Bei OpenStage-Telefonen kann der Tastentext auch in Unicode eingegeben werden.

Ziel / Feature Code:

Angabe des Wahlziels. Dies kann eine Ziffernfolge bzw. eine URL sein. Feature Codes, die zu externen Servern gesendet werden müssen (nicht der SIP-Server, bei dem das Telefon registriert ist), haben das folgende Format:

<Feature code>@<IP-Adresse>

Beispiel: **123@10.2.54.2**

Wird die Zieleingabe für die Tastenfunktion „Erweiterte Zielwahl“ vorgenommen, so können in einer Ziffernfolge zusätzliche Steuerzeichen eingegeben werden:

- **$Q** = clear (CL) / auflegen (AL)

- **$R** = consult (CS) / rückfragen (RF)
- **$S** = OK
- **$T** = Pause (PA)

Nur bei SIP-Workpoints verfügbar.

Umleitungstyp:

Auswahl, in welchem Fall eine Rufumleitung erfolgt.

Mögliche Optionen:

- **bei besetzt**
- **bei nicht melden**
- **immer**

Nur bei SIP-Workpoints verfügbar.

DTMF Sequenz

DTMF Sequenz für dieses Ziel.

Toggle Text:

Text zur Bezeichnung der Server-Funktion, die bei der Funktionsumschaltung angewählt wird.

Nur bei SIP-Workpoints verfügbar.

Toggle Text (Unicode Zeichen):

Text zur Bezeichnung der Server-Funktion, die bei der Funktionsumschaltung angewählt wird, in Unicode.

Nur bei OpenStage-Geräten verfügbar.

Beschreibung State Taste:

Beschreibungstext für die State-Taste.

Beschreibung State Taste (Unicode Zeichen):

Beschreibungstext für die State-Taste in Unicode. Nur bei Geräten der OpenStage-Familie (SIP-Version) verfügbar.

Feature-URI / LED Controller URI:

URI, mit der dieses Leistungsmerkmal auf dem Server gesteuert wird.

BLF akustischer Hinweis

Akustischer Hinweis zusätzlich zur Anzeige auf der Taste.

BLF PopUp Hinweis

Zusätzlich zur Anzeige auf der Taste erscheint ein Hinweis im Display.

Applikationsname:

Name der XML-Applikation, die mit der Taste gestartet werden soll.

Protokoll

Protokoll, das für die Kommunikation zwischen IP Phone und serverseitigem Programm verwendet wird.

Mögliche Optionen:

- **HTTP**
- **HTTPS**

Web Server Adresse:

Hostname, Domänenname oder IP Adresse des Webservers.

Port

Portnummer des Webservers. Wenn für Port nichts eingetragen wurde, enthält die voll qualifizierte URL kein Port-Element.

Pfad

Verzeichnispfad und Name des Programms oder der Webseite.

Beispiel: **servlet/IppGenericServlet** oder **webpage/checkin.xml**

Der Pfadname sollte mit einem Schrägstrich bzw. Slash beginnen und nicht mit einem Slash enden. Falls der Slash zu Beginn fehlt, wird er ergänzt. Falls ein zusätzlicher Slash am Ende steht, wird er gelöscht. Bei den Slashes handelt es sich um 'vorwärts'-Slashes ('/') . Bei 'Back'-Slashes findet der Web Server das Programm oder die Seite eventuell nicht.

Parameter

Kein, ein oder mehrere Parameter-Wert Paare, durch '&' getrennt, können eingegeben werden, z. B. **Parameter1=Wert1&Parameter2=Wert2**. Ein Komma darf nicht als Trennzeichen verwendet werden, da es Teil eines Parameter oder Wertes sein kann. Falls ein Parameter oder Wert ein '&' enthält, muss es durch '&' ersetzt werden.

Ein Fragezeichen wird automatisch zwischen Pfad und Parameter eingefügt. Ein Fragezeichen am Beginn der Parameter wird automatisch gelöscht.

HTTP Methode

Verwendete HTTP-Methode.

Mögliche Optionen:

- **Get**
- **Post**

Web Server User ID

Eine dem Webserver bekannte User ID. Diese Information wird zur Authentifizierung des IP Phones durch den Web Server verwendet.

Web Server Passwort

Ein dem Web Server bekanntes Passwort. Diese Information wird zur Authentifizierung des IP Phones durch den Web Server verwendet.

Symbolischer Name

Symbolischer Name.

Push Unterstützung

Push-Unterstützung.

Tastenfunktionalität

Mögliche Optionen:

- **Toggle Anrufumleitung**
- **unspezifizierte Anrufumleitung**
- **unspezifiziert**

Spezifische Parameter Leitungstaste / DSS Taste

Primärleitung

Nur bei SIP-Workpoints verfügbar.

Leitungsziel:

Nur bei SIP-Workpoints verfügbar.

Realm:

Angabe des SIP-Realms.

Nur bei SIP-Workpoints verfügbar.

Benutzerkennung:

Nur bei SIP-Workpoints verfügbar.

Passwort:

Nur bei SIP-Workpoints verfügbar.

Hunting Sequenz:

Nur bei SIP-Workpoints verfügbar.

Shared Typ:

Mögliche Optionen:

- **Privat**
- **Gemeinsam**
- **Unbekannt**

Nur bei SIP-Workpoints verfügbar.

Rufton

Nur bei SIP-Workpoints verfügbar.

Leitungsstörung erlaubt

Schalter für das Zulassen von Leitungsstörungen.

Nur bei SIP-Workpoints verfügbar.

Sofortverbindungsaufbau (Hotline)

Schalter zum Aktivieren einer Leitungs-Hotline.

Leitungs-Hotline Ziel

Nur bei SIP-Workpoints verfügbar.

Hot/Warm Line Typ:

Mögliche Optionen:

- **Normal**
- **Sofortverbindungsaufbau**

- **verzögerter Sofortverbindungsaufbau**

Nur bei SIP-Workpoints verfügbar.

Anzeigen in Übersicht

Aktiviert die Leitungsanzeige in der Leitungsübersicht..

Nur bei SIP-Workpoints verfügbar.

Position in Übersicht:

Position der Taste in der Leitungsübersicht.

Nur bei SIP-Workpoints verfügbar.

Leitungsbeschreibung

Bescheibung der entsprechenden Leitung.

Nur bei OpenStage-Geräten verfügbar.

Leitungstasten Typ:

Mögliche Optionen:

- **normal**
- **direkt**

Leitungstasten Aktion

Mögliche Optionen:

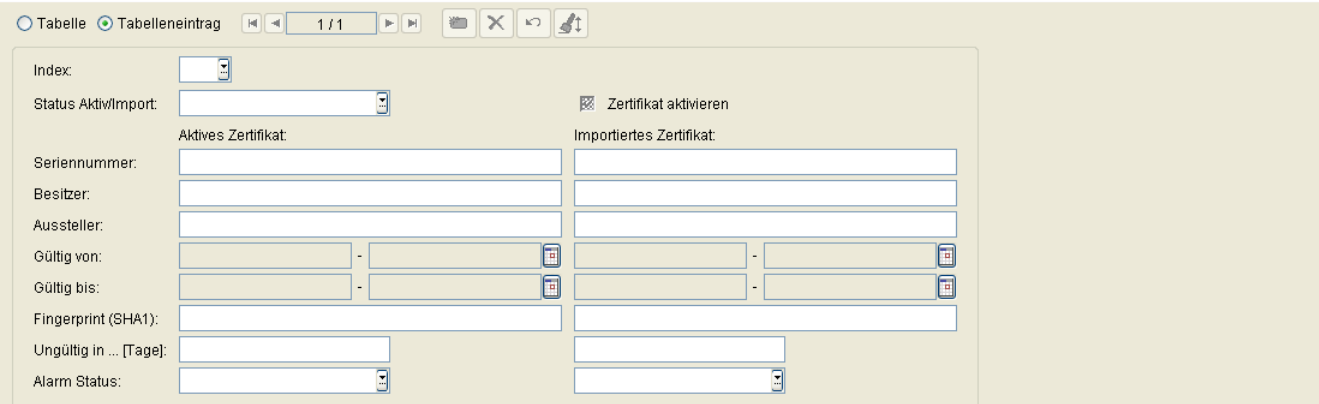
- **Rückfrage**
- **Vermitteln**
- **Keine Aktion**

Rufton-Verzögerung:

Dauer der Verzögerung, bis ein eingehender Rufton signalisiert wird.

8.1.14.3 Register „Send URL Server CA Zertifikat“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Keysets / Tastenbelegung > Register „Send URL Server CA Zertifikat“



Eine Beschreibung der Parameter finden Sie unter **IP Devices** > **IP Phone Konfiguration** > **LDAP** > **Register „CA Zertifikate“**.

8.1.15 Signaling and Payload Encryption (SPE)

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Signaling and Payload Encryption (SPE)

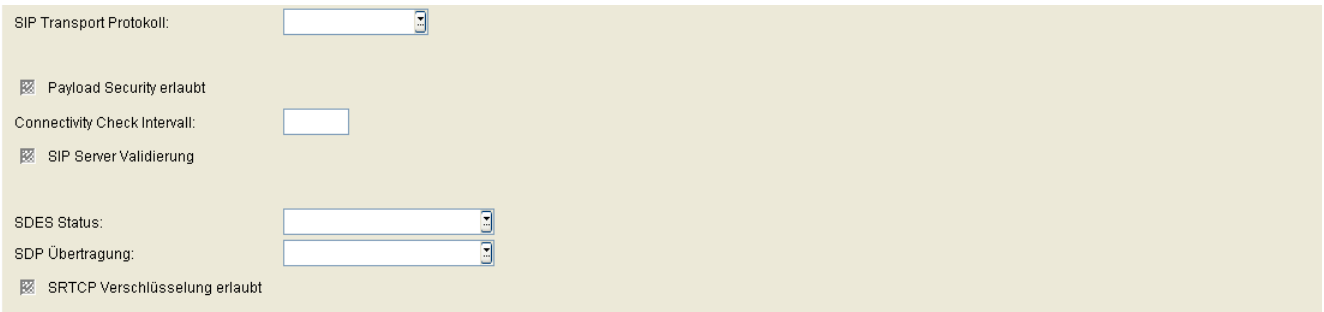
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SIP Einstellungen“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

8.1.15.1 Register „SIP Einstellungen“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Signaling and Payload Encryption (SPE) > Register „SIP Einstellungen“



SIP Transport Protokoll:

Protokoll für die SIP-Signalisierung.

Mögliche Optionen:

- **UDP**
- **TCP**
- **TLS**

Payload Security erlaubt

Ist der Schalter aktiviert, so wird die Verschlüsselung von Sprachdaten erlaubt.

Connectivity Check Intervall:

Zeitintervall, in dem die Verbindung auf Session Timeouts überprüft wird.

SIP Server Validierung

Bei aktiviertem Schalter wird überprüft, ob die TLS-Verbindung zum SIP-Server gültig ist.

SDES Status

Auswahl des SDES-Status.

Mögliche Optionen:

- **deaktiviert**
- **aktiviert**

SDP Übertragung

Auswahl der SDP-Übertragung.

Mögliche Optionen:

- **SRTP und RTP**
- **nur SRTP**
- **Rückfallen auf RTP**

SRTCP Verschlüsselung erlaubt

Wenn aktiviert, wird mit SRTCP verschlüsselt.

8.1.16 Sonstiges

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges

Dieser Bereich besteht aus folgenden Inhalten:

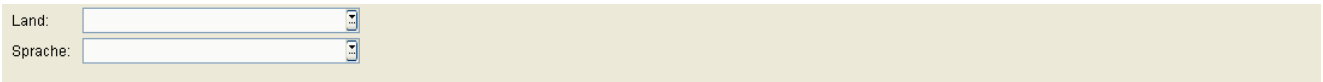
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Land & Sprache“
- Register „Messaging Services“
- Register „SIP Fehleranzeige“
- Register „Display / Geräte Einstellungen
- Register „Internet Hilfe URL“
- Register „Telefonsperre“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

8.1.16.1 Register „Land & Sprache“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges > Register „Land & Sprache“



Land:

Land, in dem der Workpoint betrieben wird.

Mögliche Optionen:

- **AE - Vereinigte Arabische Emirate**
- **AF - Afghanistan**
- **AL - Albanien**
- **AM - Armenien**
- **AR - Argentininen**
- **AT - Österreich**
- **AU - Australien**
- **AZ - Aserbaidschan**
- **BA - Bosnien und Herzegowina**
- **BD - Bangladesch**
- **BE - Belgien**
- **BG - Bulgarien**
- **BO - Bolivien**
- **BR - Brasilien**
- **BY - Weißrussland**
- **CH- Schweiz**
- **CI - Elfenbeinküste**
- **CL - Chile**
- **CM - Kamerun**
- **CN - China**
- **CO - Columbien**
- **CR - Costa Rica**

- **CR - Serbien**
- **CY - Zypern**
- **CZ - Tschechien**
- **DE - Deutschland**
- **DZ - Algerien**
- **DK - Dänemark**
- **EC - Ecuador**
- **EE - Estland**
- **EG - Ägypten**
- **ES - Spanien**
- **FI - Finnland**
- **FR - Frankreich**
- **GB - Großbritannien**
- **GE - Georgien**
- **GR - Griechenland**
- **GT - Guatemala**
- **HN - Honduras**
- **HK - Hong Kong**
- **HR - Kroatien**
- **HU - Ungarn**
- **ID - Indonesien**
- **IE - Irland**
- **IL - Israel**
- **IN - Indien**
- **IR - Iran**
- **IT - Italien**
- **JO - Jordanien**
- **JP - Japan**
- **KE - Kenia**
- **KG - Kirgistan**

- **KR - Korea**
- **KW - Kuwait**
- **KZ - Kasachstan**
- **LB - Libanon**
- **LK - Sri Lanka**
- **LT - Litauen**
- **LU - Luxemburg**
- **LV - Lettland**
- **MA - Marokko**
- **MD - Moldawien**
- **MK - Mazedonien**
- **MV - Malediven**
- **MX - Mexiko**
- **MY - Malaysia**
- **NA - Namibia**
- **NG - Nigeria**
- **NI - Nicaragua**
- **NL - Niederlande**
- **NO - Norwegen**
- **NP - Nepal**
- **NZ - Neuseeland**
- **OM - Oman**
- **PA - Panama**
- **PE - Peru**
- **PH - Philippinen**
- **PK - Pakistan**
- **PL - Polen**
- **PT - Portugal**
- **PY - Paraguay**
- **Ro - Rumänien**

- **RU - Russland**
- **SA - Saudi Arabien**
- **SE - Schweden**
- **SG - Singapur**
- **SI - Slowenien**
- **SK - Slowakische Republik**
- **SV - El Salvador**
- **TH - Thailand**
- **TJ - Tatschikistan**
- **TN - Tunesien**
- **TR- Türkei**
- **TM - Turkmenistan**
- **TZ - Tansania**
- **UA - Ukraine**
- **US - Vereinigte Staaten**
- **UY - Uruguay**
- **UZ - Usbekistan**
- **VE - Venezuela**
- **VN - Vietnam**
- **ZA - Südafrika**
- **ZW - Simbabwe**

Sprache:

Sprache, die für lokale Anwendungen verwendet werden soll.

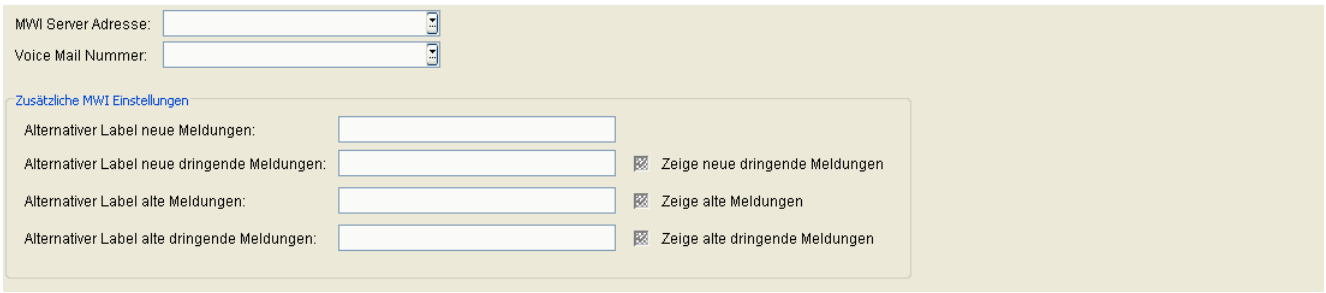
Mögliche Optionen:

- **bg - bulgarisch**
- **ca - katalanisch**
- **cs - tschechisch**
- **da - dänisch**

- **de - deutsch**
- **el - griechisch**
- **en_GB - englisch (GB)**
- **en_US- englisch (US)**
- **en - englisch**
- **es - spanisch**
- **et - estnisch**
- **fi - finnisch**
- **fr - französisch**
- **hr - kroatisch**
- **hu - ungarisch**
- **it - italienisch**
- **ja - japanisch**
- **lv - lettisch**
- **mk - mazedonisch**
- **ms - malaiisch**
- **nl - niederländisch**
- **no - norwegisch**
- **pl - polnisch**
- **pt - portugiesisch**
- **pt_Br - Brasilianisch**
- **ro - rumänisch**
- **ru - russisch**
- **sk - slowakisch**
- **sl - slowenisch**
- **sr - serbisch (kyrillisch)**
- **sr_Latn - serbisch (Latin)**
- **sv - schwedisch**
- **tr - türkisch**
- **zh - chinesisch**

8.1.16.2 Register „Messaging Services“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges > Register „Messaging Services“



MWI Server Adresse:

IP-Adresse oder Hostname des MWI-Servers.

Voice Mail Nummer:

Rufnummer der Voice Mail-Einrichtung (Nachrichten-Server).

Zusätzliche MWI Einstellungen

Zeige neue dringende Meldungen

Anzahl der neuen dringenden Nachrichten anzeigen.

Zeige alte Meldungen

Anzahl der alten Nachrichten anzeigen.

Zeige alte dringende Meldungen

Anzahl der alten dringenden Nachrichten anzeigen.

Alternativer Label neue Meldungen

Titel für die Anzahl der neuen Nachrichten.

Alternativer Label neue dringende Meldungen

Titel für die Anzahl der neuen dringenden Nachrichten.

Alternativer Label alte Meldungen

Titel für die Anzahl der alten Nachrichten.

Alternativer Label alte dringende Meldungen

Titel für die Anzahl der alten dringenden Nachrichten.

8.1.16.3 Register „SIP Fehleranzeige“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges > Register „SIP Fehleranzeige“

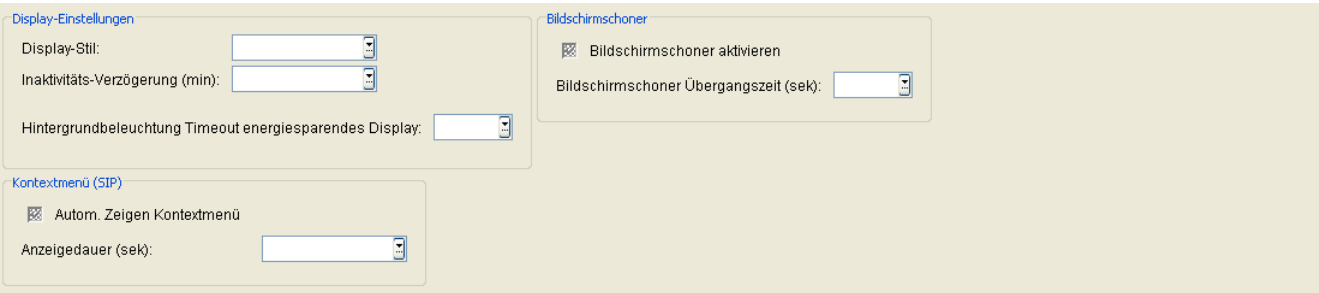
Piepton bei Fehler

Schalter zum Aktivieren der akustischen Signalisierung von Fehlern bei der Kommunikation mit dem Microsoft RTC.

Nur bei SIP-Workpoints verfügbar.

8.1.16.4 Register „Display / Geräte Einstellungen

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges > Register „Display / Geräte Einstellungen



Display-Einstellungen

Display-Stil:

Bestimmt das Aussehen der grafischen Benutzeroberfläche von OpenStage-Telefonen.

Mögliche Optionen:

- **Silber Blau**
- **Anthrazit Orange**

Unbenutzt Timeout (min):

Zeit in Minuten, nach der der Bildschirm gedimmt wird, wenn bisher keine Aktivitäten am Bildschirm stattgefunden haben.

Mögliche Optionen:

- **0**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Hintergrundbeleuchtung Timeout energiesparendes Display

Sobald ein Telefon mit energiesparendem Display länger als die hier angegebene Zeitspanne im Ruhezustand ist, wird die Hintergrundbeleuchtung abgeschaltet.

HINWEIS: Dieser Parameter ist nur für IP Devices mit **Display Hintergrundbeleuchtung = CCFL** oder **Display Hintergrundbeleuchtung = LED** gültig, siehe auch Abschnitt 7.5.1, “Inventar Daten”.

Mögliche Optionen:

- **1 min**
- **5 min**
- **30 min**
- **60 min**
- **2 std**
- **3 std**
- **4 std**
- **5 std**
- **6 std**
- **7 std**
- **8 std**

Bildschirmschoner

Bildschirmschoner aktivieren

Schalter zum Aktivieren des Bildschirmschoners.

Bildschirmschoner Übergangszeit (sek)

Zeitabstand in Sekunden, in dem die Bilder wechseln.

Mögliche Optionen:

- **5**
- **10**
- **20**
- **30**
- **60**

Kontextmenü (SIP)

Autom. Zeigen Kontextmenü

Wenn aktiviert, wird das Kontextmenü automatisch angezeigt.

Anzeigedauer (sek)

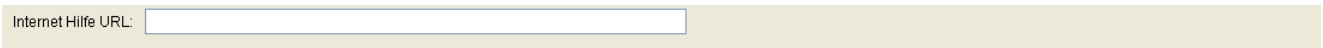
Das Kontextmenü wird nach der hier eingestellten Zeit ausgeblendet, in Sekunden.

Mögliche Werte:

- **Kein Ausblenden**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

8.1.16.5 Register „Internet Hilfe URL“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges > Register „Internet Hilfe URL“



Internet Hilfe URL:

URL der Web-Hilfeseite im Internet mit Informationen zum Telefon.

8.1.16.6 Register „Telefonsperre“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Konfiguration > Sonstiges > Register „Telefonsperre“

Telefon sperren

Sperrt das Telefon.

8.2 SIP Mobile User Interaktion

Mithilfe dieses Bereichs können Sie Mobile User einrichten, ändern und löschen. Außerdem gibt es die Möglichkeit, Mobile User abzumelden, sich über An- und Abmeldungen zu informieren, User Data Profiles zu erstellen und Voreinstellungen für Tastenbelegungen zu definieren.

> ***HINWEIS:*** DLS ermöglicht es, Mobile User zu löschen, die noch (an einem Endgerät für Mobile User) angemeldet sind, aber „vergessen“ wurden; darüber hinaus ermöglicht es die Abmeldung von Endgeräten für Mobile User, bei denen der Mobile User selbst gelöscht wurde.

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion

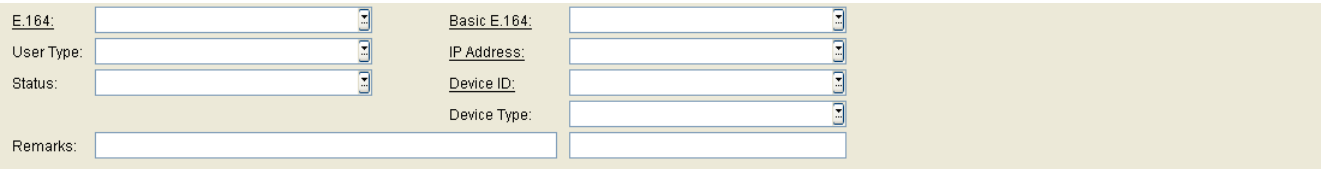
Dieses Menü besteht aus folgenden Untermenüs:

- SIP Mobile User
- Logon / Logoff
- Automatisches Logoff
- SIP User Tastenbelegung
- Mobile User Response Test Einstellungen

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für **SIP Mobile User** und **Logon / Logoff** dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von Workpoints zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen Workpoints angezeigt (keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

E.164:

Aktuelle vollständige E.164-Rufnummer (Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Anwender Typ:

Zeigt an, um welche Art von Daten es sich in den restlichen Feldern handelt.

Mögliche Optionen:

- **Endgerät für Mobile User**
  Es sind Daten des Mobility Phones.
- **Mobil User**
  Es sind Daten des Mobile Users.

Weitere Informationen zum Thema Mobility siehe Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Status:

Zeigt den Mobility-Status an.

Mögliche Optionen:

- **Mobile User angemeldet**
  Bei Mobile User Daten: Es ist ein Mobile User angemeldet.
- **Mobile User abgemeldet**
  Bei Mobile User Daten: Es ist kein Mobile User angemeldet.

- **Endgerät für Mobile User**
  Bei Daten zum Mobility Phone: Am Mobile User ist kein Mobility Phone angemeldet.
- **Endgerät belegt durch Mobile User**
  Bei Daten zum Mobility Phone: Am Mobile User ist ein Mobility Phone angemeldet.

Weitere Informationen zum Thema Mobility siehe Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Basis E.164:

E.164-Rufnummer des Mobility-Telefons.

Beispiel: **498972212345**

IP Adresse:

IP-Adresse des Workpoints.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

Physikalische MAC-Adresse des Workpoints.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Devices.

Alle vom DLS unterstützte Workpoint-Typen finden Sie im Abschnitt 3.4, “Unterstützte IP Devices/Versionen”.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach entsprechenden Einträgen in der Datenbank.

Fenster leeren

Löscht den Inhalt aller Felder in der Ansicht **Suche**. So können vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Sichert die Änderungen.

Verwerfen

Verwirft die vorgenommenen Änderungen.

Logon Mobile User

Meldet einen Mobile User an einem mobility-fähigen Endgerät an.

Klickt man auf die Aktionsschaltfläche, erscheint ein Dialogfenster. Wenn im Allgemeinen Teil der Maske ein Mobile User ausgewählt ist, ist im Dialogfenster die E.164-Rufnummer des Endgeräts anzugeben. Ist im Allgemeinen Teil ein Endgerät angegeben, so wird die Mobility ID des Mobile Users eingetragen.

Logoff Mobile User

Meldet einen Mobile User vom Endgerät ab.

Ist im Allgemeinen Teil der Maske ein Mobile User ausgewählt, wird dieser vom Endgerät abgemeldet. Ist ein Endgerät ausgewählt, wird der dort angemeldete Mobile User abgemeldet.

Reset Mobile User

Anzuwenden, falls das Endgerät für den DLS nicht erreichbar ist. Der Mobile User und das Telefon, an dem er gerade angemeldet ist, werden in der DLS-Datenbank auf „Abgemeldet“ gesetzt.

Neu

Legt einen neuen Mobile User bzw. einen Mobile User Standard an.

Migration zu Mobile User

Verwandelt einen Basis User in einen Mobile User. Siehe auch Abschnitt 16.13.4.2, “Erstellen durch Migrieren”.

Migration zu Device

Wandelt einen angemeldeten Mobile User in einen Basis User um.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

Löschen

Löscht das Objekt.

8.2.1 SIP Mobile User

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > SIP Mobile User

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Mobile / Basis User“
- Register „Archivierungsdaten“
- Register „Response Test Einstellungen“

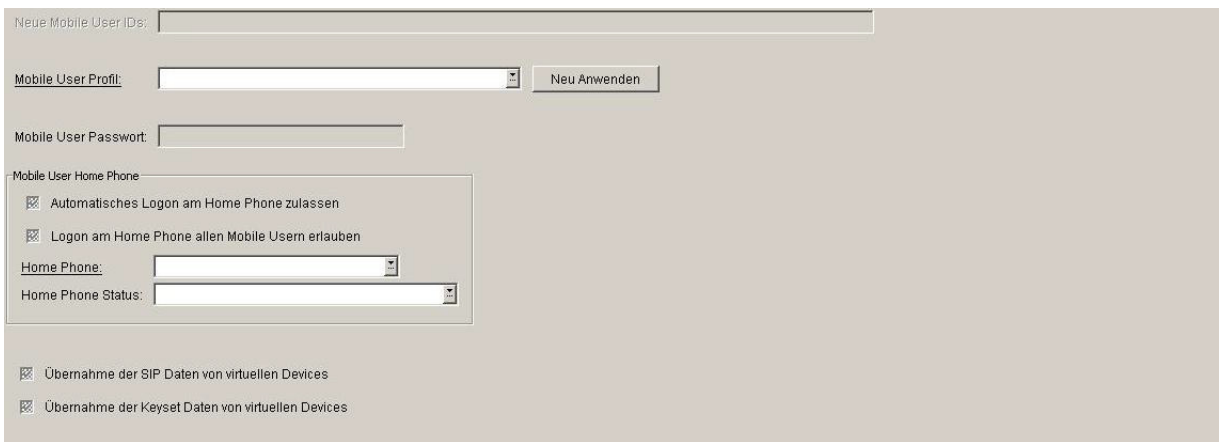
Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

8.2.1.1 Register „Mobile / Basis User“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > SIP Mobile User > Register „Mobile / Basis User“

HINWEIS: Eine Einführung zum Thema Mobility finden Sie im Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Informationen zur Mobility-Administration siehe Abschnitt 16.13, “Mobility:EinrichtenMobility:Administrieren”.



Neue Mobile User IDs:

E.164-Rufnummern aller Mobility-Telefone, für die jeweils ein Mobile User erstellt werden soll. Bei mehr als einem Mobility-Telefon werden die E.164-Rufnummern kommagetrennt eingegeben.

Durch einen Klick auf die Schaltfläche wird eine Liste mit allen verfügbaren Rufnummern angezeigt, aus der Sie, ähnlich der Mehrfachauswahl in der Tabellen-Ansicht (siehe Abschnitt 5.4.2.4), die gewünschten Nummern selektieren können.

Mobile User Profil:

Auswahl einer in **Profil Management** > **User Data Profile** definierten Mobile User Konfiguration.

> ***HINWEIS:*** Wenn ein Endgerät mit einem bereits angemeldeten User versucht, eine Verbindung zum DLS herzustellen, UND dieser User zum Zeitpunkt der Kontaktaufnahme mit dem DLS nicht mehr existiert, erstellt DLS den User automatisch.
> In diesem Fall wird dem User der Profilname **@#####** zugewiesen (die Rufnummer des Mobile User wird automatisch mit dem Präfix „@“ versehen).

Neu Anwenden:

Mobile User-Profil erneut auf den Mobile User anwenden. Nach dem Start dieser Funktion wird der DLS-Benutzer gefragt, ob dies als Mischen der Daten oder als Ersetzen aller User-Daten durch Profil- oder Default-Daten geschehen soll. Wenn die Option Mischen ausgewählt ist (Klick auf „Ja“), werden diejenigen User-Parameter, die auch im Profil konfiguriert sind, durch die Profildaten überschrieben. Diejenigen User-Daten, die nicht im Profil enthalten sind, werden belassen. Wenn beispielsweise das Profil zusätzliche Tasten enthält, werden diese zu den bereits auf dem Telefon des Mobile Users konfigurierten Tasten hinzugefügt; im Falle konkurrierender Tastendefinitionen hingegen werden die Tastendefinitionen des Profils die aktuell auf dem Telefon gesetzten überschreiben.

Wenn anstelle der Option Mischen die Option Ersetzen gewählt ist (Klick auf „Nein“), werden diejenigen User-Parameter, die auch im Profil enthalten sind, durch die Profildaten ersetzt. Diejenigen User-Parameter, die nicht im Profil enthalten sind, werden durch Default-Werte überschrieben.

Mobile User Passwort:

Mit diesem Passwort kann sich der Benutzer am Telefon anmelden, sowohl am Gerät selbst als auch über den WBM (Web Based Manager).

Mobile User Home Phone

Automatisches Logon am Home Phone zulassen

Wenn aktiviert, wird der Mobile User automatisch an dem Home Phone angemeldet, dessen E.164-Nummer unter **Home Phone** eingetragen wurde.

Logon am Home Phone allen Mobile Usern erlauben

Wenn aktiviert, wird allen Mobile Usern erlaubt, sich an dem Home Phone anzumelden, dessen E.164-Nummer unter **Home Phone** eingetragen wurde.

Home Phone

E.164 Nummer des Home Phone, das diesem Mobile User zugeordnet ist.

Home Phone Status

Zeigt den aktuellen Zustand des Mobile Users am Home Phone.

Mögliche Werte:

- **Mobile User am Home Phone angemeldet**

- **Mobile User am Home Phone abgemeldet**

Übernahme der SIP Daten von virtuellen Devices

Ist der Schalter aktiviert, werden die Daten für die SIP-Zugangsdaten aus der korrespondierenden Plug&Play-Konfiguration übernommen, d. h. aus dem virtuellen Gerät, das dieselbe E.164-Nummer besitzt wie der neu erstellte Mobile User. Die Zugangsdaten zum SIP-Server befinden sich im Bereich **IP Phone Konfiguration** > **Gateway / Server**.

Übernahme der Keyset Daten von virtuellen Devices

Dieser Schalter bestimmt, ob die Keyset-Konfiguration des jeweiligen virtuellen Geräts vom Mobile User geerbt wird oder nicht. Ist der Schalter aktiviert, werden die Daten für die Keyset-Attribute aus der zugehörigen Plug&Play-Konfiguration übernommen, d. h. aus dem virtuellen Gerät, das dieselbe E.164-Rufnummer besitzt wie der neu erstellte Mobile User.

Mandant

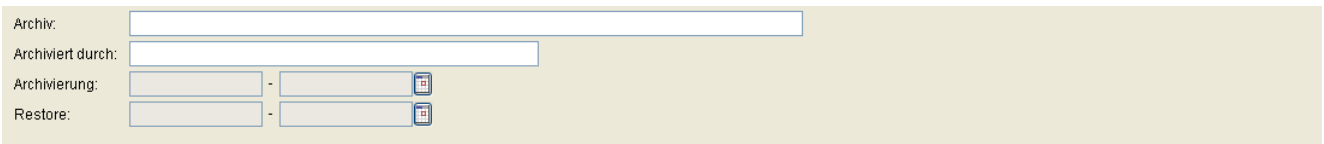
Name des Mandanten, zu dem der Mobile User gehört.

8.2.1.2 Register „Archivierungsdaten“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > SIP Mobile User > Register „Archivierungsdaten“

HINWEIS: Eine Einführung zum Thema Mobility finden Sie im Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Informationen zur Mobility-Administration siehe Abschnitt 16.13, “Mobility:EinrichtenMobility:Administrieren”.



Archiv:

Pfad der ZIP-Archivdatei auf dem DLS-Rechner.

Archiviert durch:

Name des DLS-Benutzers, der das Archiv erzeugt hat.

Archivierung:

Zeigt Datum und Uhrzeit der Archivierung an.

Restore:

Zeigt Datum und Uhrzeit der Wiederherstellung aus dem Archiv an.

8.2.1.3 Register „Response Test Einstellungen“

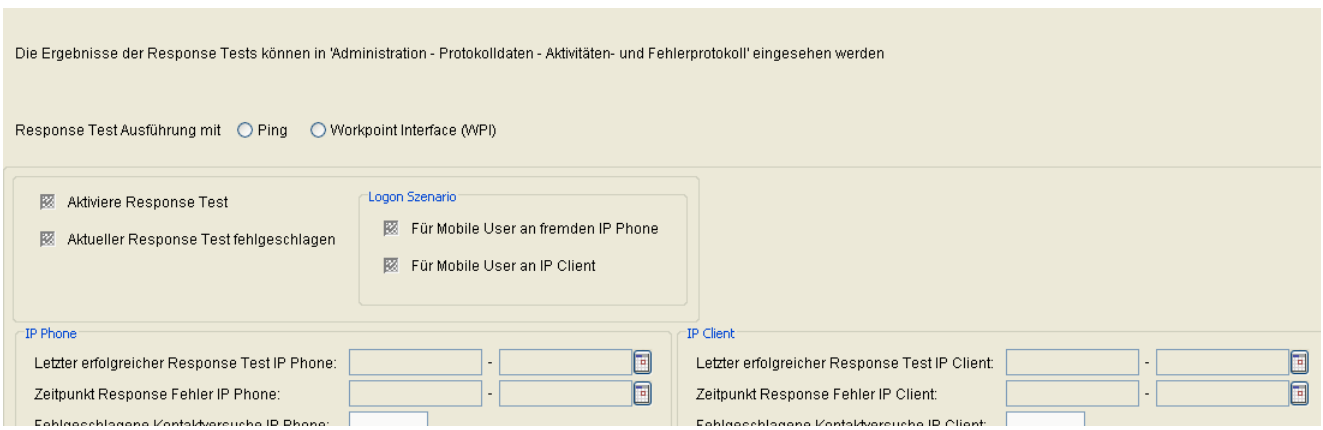
Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > SIP Mobile User > Register „Response Test Einstellungen“

Diese Funktion überprüft, ob ein IP Phone oder IP Client, an dem ein Mobile User angemeldet ist, vom DLS aus noch erreichbar ist.

Ist das IP Phone oder der IP Client entsprechend den Einstellungen (siehe Abschnitt 8.2.5, “Mobile User Response Test Einstellungen”) nicht mehr erreichbar und dem Mobile User ist ein Home Phone zugewiesen, wird versucht, den Mobile User vom aktuellen IP Phone oder IP Client abzumelden und ihn an dem entsprechenden Home Phone anzumelden. Somit wird verhindert, dass der Mobile User nicht mehr erreichbar ist.

Als Fehlversuch wird gewertet, wenn innerhalb von 10 Sekunden kein Kontakt hergestellt werden konnte. Der Response Test gilt als fehlgeschlagen, wenn die Anzahl ‘Fehlgeschlagene Kontaktversuche IP Phone’ oder ‘Fehlgeschlagene Kontaktversuche IP Client’ größer ist als die Anzahl ‘Response Test Wiederholungen’ in der Maske ‘Mobile User Response Test Einstellungen’.

Ein Kontaktversuch gilt als fehlgeschlagen, wenn innerhalb von 10 Sekunden kein Kontakt hergestellt werden konnte. Der Response Test ist fehlgeschlagen, wenn der Zähler **Fehlgeschlagene Kontaktversuche IP Phone** bzw. **Fehlgeschlagene Kontaktversuche IP Client** größer ist als der Wert von **Response Test Wiederholungen** in der Maske **Mobile User** > **SIP Mobile User Interaktion** > .



Response Test Ausführung mit

- **Ping**
  Der DLS versucht, das IP Phone oder den IP Client mittels Ping zu erreichen.
- **Workpoint Interface (WPI)**
  Der DLS versucht, das IP Phone oder den IP Client mit einem ContactMe-Request über dessen Workpoint Interface zu erreichen. Sendet das IP Phone oder der IP Client eine entsprechende Message, in der der Parameter „ReasonForContact“ den Wert „solicited“ hat, so war der Response Test erfolgreich. Andernfalls gilt der Test als fehlgeschlagen.

Aktiviere Response Test

Aktiviert oder deaktiviert den Response Test für diesen Mobile User.

Aktueller Response Test fehlgeschlagen

Konnte nach 10 Sekunden kein Kontakt hergestellt werden, so wird der Fehlerzähler inkrementiert.

Logon Szenario

Für Mobile User an fremden IP Phone

Ist der Schalter aktiviert, so werden Response Tests für einen Mobile User an einem fremden IP Phone durchgeführt, d h. an einem IP Phone, das nicht das Home Phone dieses Mobile Users ist.

Für Mobile User an IP Client

Ist der Schalter aktiviert, so werden Response Tests für einen Mobile User an einem IP Client durchgeführt, d h. an einem IP Client, der nicht das Home Phone dieses Mobile Users ist.

IP Phone

Letzter erfolgreicher Response Test IP Phone

Datum des letzten erfolgreichen Response Tests bei diesem IP Phone.

Zeitpunkt Response Fehler IP Phone

Datum des letzten fehlerhaften Response Tests für dieses IP Phones.

Fehlgeschlagene Kontaktversuche IP Phone

Anzahl der fehlgeschlagenen Kontaktversuche für dieses IP Phone.

Nicht erreichtes IP Phone

IP Adresse des nicht erreichten IP Phones.

IP Client

Letzter erfolgreicher Response Test IP Client

Datum des letzten erfolgreichen Response Tests bei diesem IP Client.

Zeitpunkt Response Fehler IP Client

Datum des letzten fehlerhaften Response Tests für diesen IP Client.

Fehlgeschlagene Kontaktversuche IP Client

Anzahl der fehlgeschlagenen Kontaktversuche für diesen IP Client.

Nicht erreichter IP Client

IP Adresse des nicht erreichten IP Clients.

8.2.2 Logon / Logoff

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > Logon / Logoff

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Protokoll“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

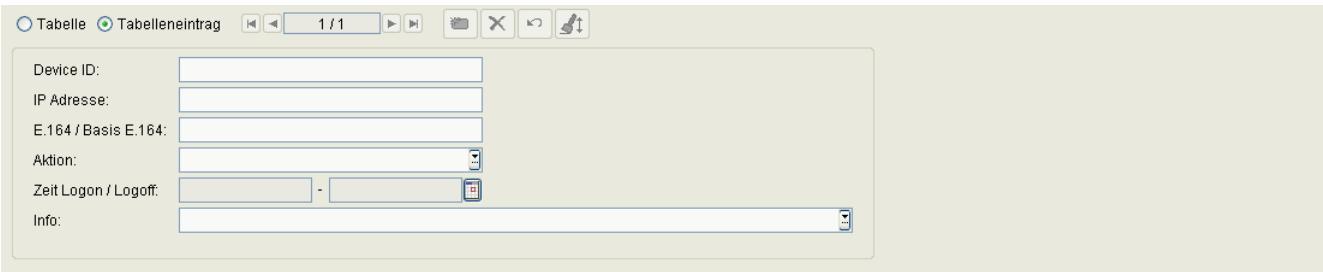
8.2.2.1 Register „Protokoll“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > Logon / Logoff > Register „Protokoll“

Hier werden sämtliche gelungenen oder fehlgeschlagenen Aktionen verzeichnet, die Mobile User betreffen.

HINWEIS: Eine Einführung zum Thema Mobility finden Sie im Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

Informationen zur Mobility-Administration siehe Abschnitt 16.13, “Mobility:EinrichtenMobility:Administrieren”.



Device ID

Device ID des Mobility Phones, mit dem die hier protokollierte Aktion stattgefunden hat (nur Anzeige).

IP Adresse

IP-Adresse des Mobility Phones, mit dem die hier protokollierte Aktion stattgefunden hat (nur Anzeige).

E.164 / Basis E.164

E.164- bzw. Basis E.164-Rufnummer des Mobility Phones, mit dem die hier protokollierte Aktion stattgefunden hat (nur Anzeige).

Aktion

Typ der Aktion, die stattgefunden hat (nur Anzeige).

Mögliche Einträge:

- **Logon**
- **Logoff**

Zeit Logon / Logoff

Zeitpunkt der Logon- oder Logoff-Aktion bzw. des Fehlversuchs (nur Anzeige).

Info

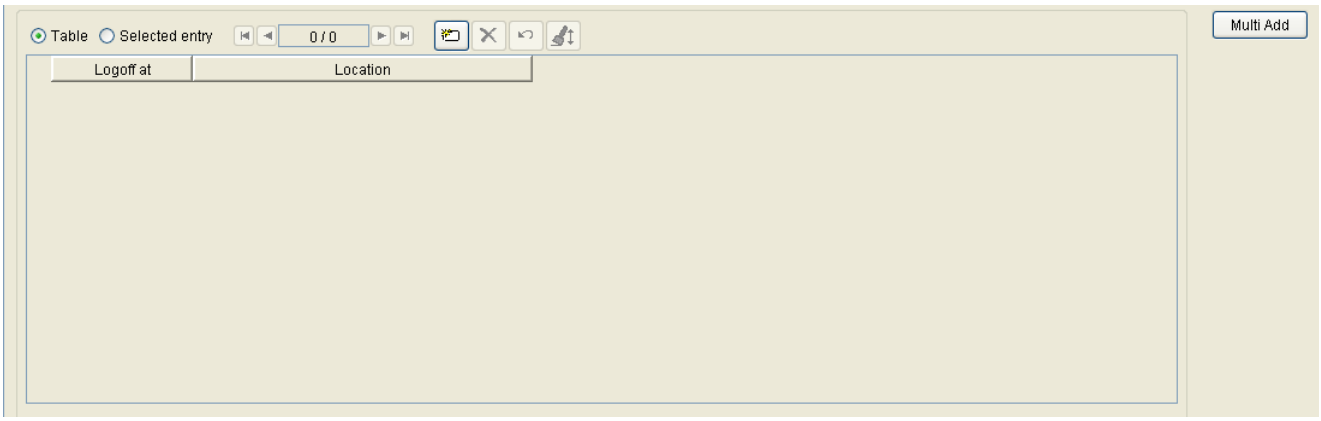
Zusatzinformation zur Logon- oder Logoff-Aktion bzw. zum Fehlversuch (nur Anzeige).

Mögliche Einträge:

- **Passwort oder E.164 falsch**
- **Interner Fehler**
- **Anmeldung an einem anderen Telefon noch vorhanden**
- **Zweite Anmeldung nicht zulässig**
- **Abmeldung durch DLS**
- **Abmeldung durch DLS fehlgeschlagen**
- **Abmeldung durch DLS wegen zweiter Anmeldung**
- **Erfolgreiche Anmeldung**
- **Erfolgreiche Abmeldung**
- **Abmeldung nicht möglich (Gespräch aktiv)**

8.2.3 Automatisches Logoff

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > Automatisches Logoff



Dieser Bereich ermöglicht dem Anwender, für bestimmte Standorte jeweils ein tägliches automatisches Logoff aller SIP Mobile User festzulegen. So kann z.B. gewährleistet werden, dass bei Arbeitsbeginn alle Benutzer ausgeloggt sind, so dass die Endgeräte für SIP Mobile User zur Verfügung stehen.

Abmeldung um:

Uhrzeit, zu der das tägliche automatische Logoff durchgeführt werden soll. Es wird die tatsächliche Uhrzeit der für diesen Standort definierten Zeitzone verwendet.

HINWEIS: Die Umstellung von Sommerzeit auf Winterzeit (eine Stunde zurück) führt nicht zu einem erneuten Ausführen eines Jobs, der in dem dadurch verdoppelten Zeitintervall gestartet wurde. Allerdings wird bei der Umstellung von Winterzeit auf Sommerzeit (eine Stunde vor) ein Job, der in die dadurch übersprungene Zeit fällt, nicht ausgeführt.

Standort

Standorte, für die das automatische Logoff durchgeführt werden soll. Standorte können wie unter Abschnitt 6.3.2, “Standort” beschrieben, eingerichtet werden.

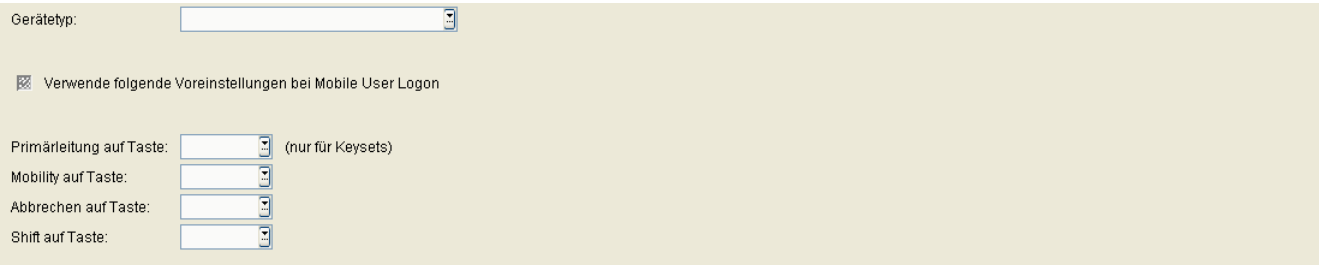
Mehrfach hinzufügen

Einer Abmeldezeit kann über diese Funktion mehreren Standorten zugeordnet werden.

8.2.4 SIP User Tastenbelegung

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > SIP User Tastenbelegung

HINWEIS: Die hier voreingestellte Tastenbelegung kann nicht umgehend geändert werden, indem man ein Template ändert und das dazugehörige User Data Profile erneut anwendet. Jedoch treten die Änderungen in Kraft, nachdem sicher Mobile User abgemeldet und erneut angemeldet hat.



Gerätetyp:

Auswahl der Gerätetyps für die Tastenbelegung.

Mögliche Optionen:

- **OpenStage 15**
- **OpenStage 40**
- **OpenStage 60**
- **OpenStage 80**
- **optiPoint 410 advance**
- **optiPoint 410 economy**
- **optiPoint 410 economy plus**
- **optiPoint 410 standard**
- **optiPoint 420 advance**
- **optiPoint 420 economy**
- **optiPoint 420 economy plus**
- **optiPoint 420 standard**
- **OpenScape Desk Phone IP 35 G**
- **OpenScape Desk Phone IP 55 G**

Verwende folgende Voreinstellung bei Mobile User Logon

Schalter zum Aktivieren der u. g. Voreinstellungen.

Primärleitung auf Taste:

Tastennummer, auf die die Primärleitungs-Taste gelegt werden soll (nur bei Telefonen, für die im Mobile User Profile bereits eine Primärleitungs-Taste vorhanden ist).

Wertebereich: **1 ... 19** oder keine.

Standard: **5**

Bei OS60 ist bei der Standard-Tastenbelegung die Position 5 für die Primärleitung reserviert. Jegliche

Änderung dieser Taste wird daher nicht an das Telefon übermittelt. Sie wird erst an das Telefon übermittelt, wenn

Sie sich abmelden und wieder anmelden. Beliebige Änderungen an anderen Tasten oder das Zuweisen einer neuen Taste zu einer anderen Position

funktionieren problemlos.

Um dieses Problem zu umgehen, sollten Sie die Position der Primärleitungstaste in der Standard-Tastenbelegung

auf Null ändern.

Mobility auf Taste:

Tastennummer, auf die die Mobility-Taste gelegt werden soll.

Wertebereich: **1** ... **19** oder keine.

Standard: **10**

Abbrechen auf Taste:

Tastennummer, auf die die Abbrechen-Taste gelegt werden soll.

Wertebereich: **1 ... 19** oder keine.

Standards:
optiPoint 410/420 economy/economy plus/standard: **11**
optiPoint 410 advance: **18**
optiPoint 420 advance: **17**

Shift auf Taste:

Tastennummer, auf der die Shift-Taste gelegt werden soll.

Wertebereich: **1** ... **19** oder keine.

Standards:
optiPoint 410/420 economy/economy plus/standard: **12**
optiPoint 410 advance: **19**
optiPoint 420 advance: **18**

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen registrierten IP Phones, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

8.2.5 Mobile User Response Test Einstellungen

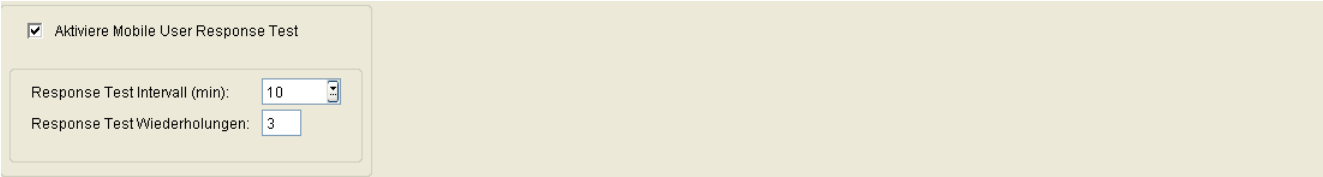
Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > Mobile User Response Test Einstellungen

Hier können Response Tests für angemeldete Mobile User angezeigt und verwaltet werden. (Siehe auch Abschnitt 8.2.1.3, “Register „Response Test Einstellungen“”)

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Protokoll“

Allgemeine Daten



Aktiviere Mobile User Response Test:

Zentraler Schalter zum Aktivieren oder Deaktivieren der Mobile User Response Tests.

Response Test Intervall (min):

Zeitabstand, in welchem der Response Test durchgeführt werden soll, in Minuten.

Mögliche Optionen:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Standardwert: **30**

Response Test Wiederholungen:

Anzahl der Response Test-Wiederholungen, wenn keine Verbindung zustande kam.

Wertebereich: **0** ... **9**

Standardwert: **5**

Mögliche Aktionsschaltflächen

Sichern

Sichert die Änderungen.

Verwerfen

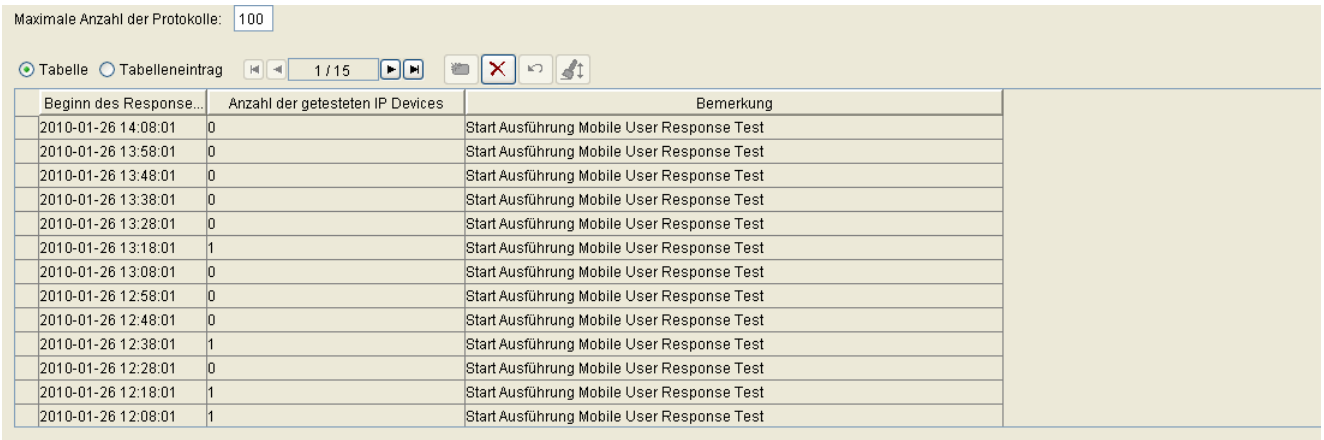
Verwirft die vorgenommenen Änderungen.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

8.2.5.1 Register „Protokoll“

Aufruf: Hauptmenü > Mobile User > SIP Mobile User Interaktion > Mobile User Response Test Einstellungen > Register „Protokoll“



Beginn des Response...	Anzahl der getesteten IP Devices	Bemerkung
2010-01-26 14:08:01	0	Start Ausführung Mobile User Response Test
2010-01-26 13:58:01	0	Start Ausführung Mobile User Response Test
2010-01-26 13:48:01	0	Start Ausführung Mobile User Response Test
2010-01-26 13:38:01	0	Start Ausführung Mobile User Response Test
2010-01-26 13:28:01	0	Start Ausführung Mobile User Response Test
2010-01-26 13:18:01	1	Start Ausführung Mobile User Response Test
2010-01-26 13:08:01	0	Start Ausführung Mobile User Response Test
2010-01-26 12:58:01	0	Start Ausführung Mobile User Response Test
2010-01-26 12:48:01	0	Start Ausführung Mobile User Response Test
2010-01-26 12:38:01	1	Start Ausführung Mobile User Response Test
2010-01-26 12:28:01	0	Start Ausführung Mobile User Response Test
2010-01-26 12:18:01	1	Start Ausführung Mobile User Response Test
2010-01-26 12:08:01	1	Start Ausführung Mobile User Response Test

Maximale Anzahl von Protokollen

Es werden maximal so viele Protokolleinträge erstellt, wie hier angegeben ist.

Beginn des Response Tests

Datum und Uhrzeit des Testbeginns.

Anzahl des getesteten IP Devices

Anzahl der gestesteten IP Phones oder IP Clients

Bemerkung

Erläuterung zum jeweiligen Protokolleintrag.

8.3 User Daten Administration

Dieser Bereich dient zur Anzeige und Verwaltung der Mobile User Daten. Dabei handelt es sich um nicht durch den DLS veränderbare Daten wie z. B. Einträge ins Elektronische Telefonbuch. Die Daten werden beim Abmelden (Logoff) eines Mobile Users zur Speicherung an den DLS gesandt; beim Anmelden (Logon) werden sie vom DLS an das Endgerät gesandt.

Angezeigt werden der Speicherbedarf je Mobile User sowie Datum, Device ID und IP-Adresse des Endgerätes. Außerdem kann der gesamte belegte Speicherplatz ermittelt werden.

Die angezeigten Userdaten können gelöscht werden. Dies sollte nur bei gelöschten Mobile Usern geschehen.

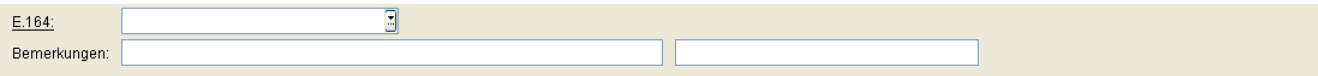
HINWEIS: Für Mobile User steht die Export-Funktionalität aus Sicherheitsgründen nicht zur Verfügung. Mobile User-Daten (z. B. die Rufliste) sind für den DLS-Administrator nicht zugänglich. Sie werden in der DLS-Datenbank in verschlüsselter Form gespeichert.

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Statistik“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Phones zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen IP Phones angezeigt.



E.164:

Aktuelle vollständige E.164-Rufnummer (Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Phones, die den Suchkriterien entsprechen.

Fenster leeren

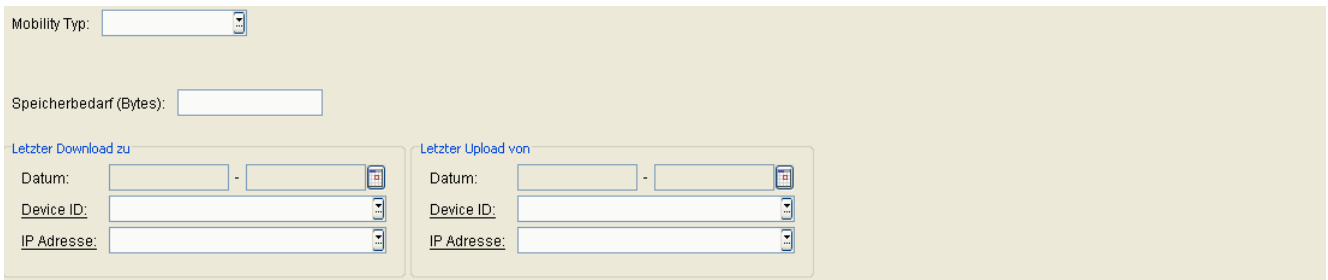
Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Ermittle gesamten Speicherbedarf

Zeigt den gesamten Speicherbedarf der User-Daten aller Workpoints in Kilobytes.

8.3.1 Register „Statistik“

Aufruf: Hauptmenü > Mobile User > User Daten Administration > Register „Statistik“



Mobility Typ

Zeigt den Mobility-Typ (HFA oder SIP) an.

Speicherbedarf (Bytes):

Durch User-Daten dieses Workpoints belegter Speicherplatz in Bytes.

Letzter Download zu

Datum:

Datum und Uhrzeit des letzten Sendens der User-Daten an den Workpoint.

Device ID:

ID des Workpoints, an den die User-Daten gesendet wurden.

IP Adresse:

IP-Adresse des Workpoints, an den die User-Daten gesendet wurden.

Letzter Upload von

Datum:

Datum und Uhrzeit des letzten Speicherns der User-Daten, die vom Workpoint gesendet wurden.

Device ID:

ID des Workpoints, dessen User-Daten gespeichert wurden.

IP Adresse:

IP Adresse des Workpoints, dessen User-Daten gespeichert wurden.

8.4 Mobility Statistiken

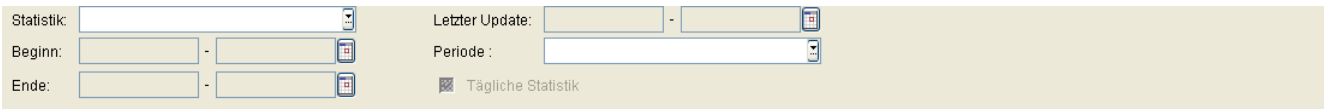
Dieser Bereich dient zur Anzeige der Mobility-Statistiken. Der Administrator kann sich damit einen Überblick über alle Aktionen von Mobile Usern in einem definierten Zeitraum verschaffen. So können z. B. Spitzenbelegungszeiten identifiziert werden. Hierfür wird die Mobile User Logon/Logoff History ausgewertet ((siehe Hauptmenü > Mobile User > SIP Mobile User Interaktion > Logon / Logoff).

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „SIP Mobility“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. In der Ansicht **Suche** dient er zur Eingabe von Parametern, um eine bestimmte Gruppe von Statistiken zu finden. In der Ansicht **Objekt** werden die Basis-Daten der gefundenen Statistiken angezeigt oder die Basis-Daten für eine neue Statistik festgelegt.



Statistik:

Name der Statistik.

Beginn:

Beginn des Beobachtungszeitraums der Aktionen. Ist **Tägliche Statistik** aktiviert, dient dieses Feld nur zur Anzeige.

Ende:

Ende des Beobachtungszeitraums der Aktionen. Ist **Tägliche Statistik** aktiviert, dient dieses Feld nur zur Anzeige.

Letzter Update:

Erstellungsdatum der aktuell angezeigten Statistik.

Periode:

Stellt das Zeitintervall innerhalb des Beobachtungszeitraums ein. Jeweils nach dem Ablauf einer Periode wird ein Eintrag in der Tabelle erzeugt.

Mögliche Optionen:

- **1 min**
- **2 min**
- **3 min**
- **4 min**
- **5 min**

- **10 min**
- **15 min**
- **20 min**
- **30 min**
- **1 std**
- **2 std**
- **3 std**
- **4 std**
- **6 std**
- **24 std**

Tägliche Statistik

Die Checkbox zeigt an, ob die aktuell angezeigte Statistik eine **Tägliche Statistik** ist.

Mögliche Aktionsschaltflächen

Suchen

Suchen nach vorhandenen Statistiken.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht Suche können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Löschen

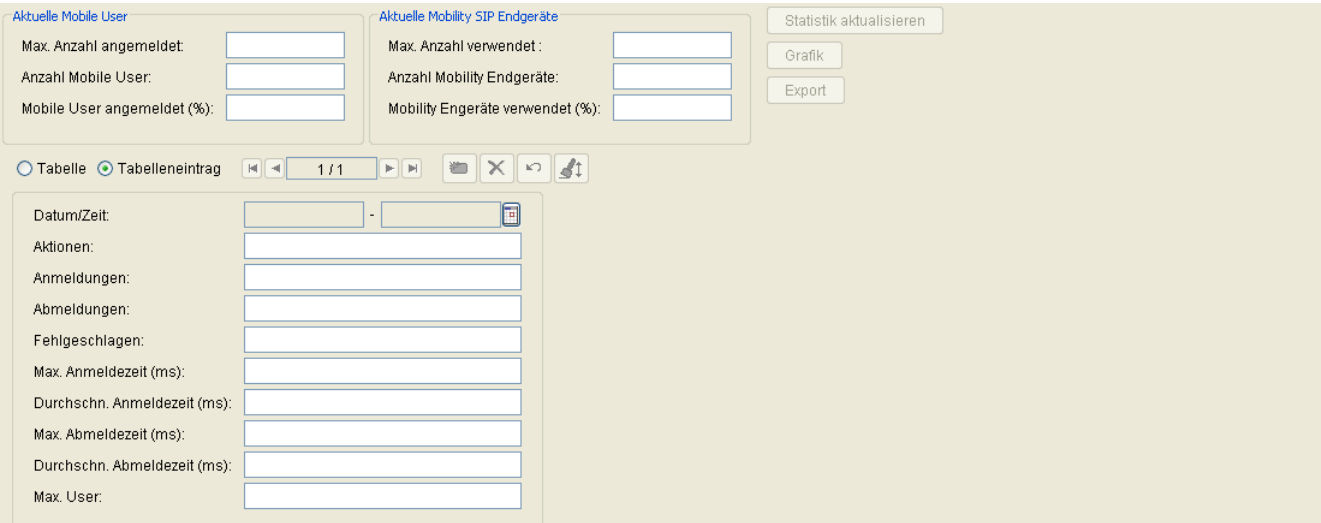
Löschen der aktuell angezeigten Statistik.

Neu

Anlegen einer neuen Statistik.

8.4.1 Register „SIP Mobility“

Aufruf: Hauptmenü > Mobile User > Mobility Statistiken > Register „SIP Mobility“



Aktuelle Mobile User

Max. Anzahl angemeldet:

Maximale Anzahl der gleichzeitig angemeldeten Mobile User im Beobachtungszeitraum.

Anzahl Mobile User:

Anzahl der am Ende des Beobachtungszeitraums eingerichteten Mobile User.

Mobile User angemeldet (%):

Gibt an, wieviel Prozent der eingerichteten Mobile User im Beobachtungszeitraum angemeldet waren.

Aktuelle Mobility SIP Endgeräte

Max. Anzahl verwendet:

Maximale Anzahl der Mobility-fähigen SIP-Endgeräte, auf denen im Beobachtungszeitraum Mobile User angemeldet waren.

Anzahl Mobility Endgeräte:

Anzahl der am Ende des Beobachtungszeitraums eingerichteten Mobility SIP Endgeräte.

Mobility Endgeräte verwendet (%):

Gibt den Prozentsatz an Mobility-fähigen Endgeräten an, auf denen im Beobachtungszeitraum Mobile User angemeldet waren.

Statistik aktualisieren

Liegt das Datum für **Ende** (des Beobachtungszeitraums) nach dem Datum für **Letzter Update,** so kann die Statistik über diesen Button aktualisiert werden. Der Button ist inaktiv, wenn sowohl das Datum für **Beginn** als auch für **Ende** in der Vergangenheit liegen.

Grafik

Über diesen Button wird der Inhalt der aktuellen Statistik grafisch dargestellt.

Export

Über diesen Button wird der Inhalt der aktuellen Statistik in eine Datei im csv-Format ausgegeben. Der Dateiname wird über ein Dialogfenster abgefragt.

Datum/Zeit:

Zeitstempel mit Datum und Uhrzeit zu Beginn der Beobachtungsperiode. Wird z. B. als Periode der Wert 5 min eingegeben, so werden die nachfolgenden Werte, Aktionen usw. im Abstand von 5 Minuten ermittelt und in die Tabelle eingetragen. Dabei werden sie mit dem entsprechenden Zeitstempel versehen.

Aktionen:

Gesamtanzahl der Aktionen innerhalb der angegebenen Periode.

Anmeldungen:

Anzahl der Anmeldungen innerhalb der angegebenen Periode.

Abmeldungen:

Anzahl der Anmeldungen innerhalb der angegebenen Periode.

Fehlgeschlagen:

Anzahl der fehlgeschlagenen Aktionen innerhalb der angegebenen Periode.

Max. Anmeldezeit (ms):

Maximale Bearbeitungszeit einer Anmeldung innerhalb der angegebenen Periode in Milliesekunden.

Durchschn. Anmeldezeit (ms):

Durchschnittliche Bearbeitungszeit von Anmeldungen innerhalb der angegebenen Periode in Millisekunden.

Max. Abmeldezeit (ms):

Maximale Bearbeitungszeit einer Abmeldung innerhalb der angegebenen Periode in Millisekunden.

Durchschn. Abmeldezeit (ms):

Durchschnittliche Bearbeitungszeit von Abmeldungen innerhalb der angegebenen Periode in Millisekunden.

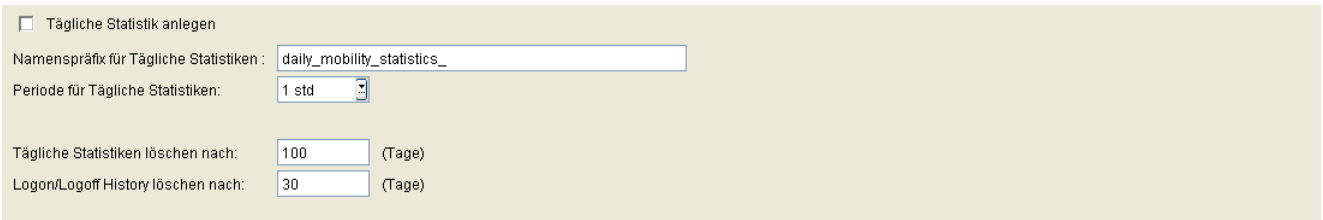
Max. User:

Maximale Anzahl der gleichzeitig angemeldeten Mobile User innerhalb der angegebenen Periode.

8.5 Mobility Statistiken Konfiguration

Aufruf: Hauptmenü > Mobile User > Mobility Statistiken Konfiguration

Dieser Bereich dient zur Konfiguration der täglichen Mobility-Statistiken (siehe Mobility Statistiken). Die Generierung von täglichen Statistiken findet einmal täglich statt, in der Regel kurz nach Mitternacht. Dies ist auch der Zeitpunkt, an dem vorgenommene Konfigurationsänderungen erstmals wirksam werden.



Tägliche Statistik anlegen

Ist dieser Schalter aktiviert, wird täglich eine Statistik entsprechend den weiteren Parametern angelegt.

Namenspräfix für Tägliche Statistiken:

Namenspräfix für automatisch angelegte Statistiken.

Periode für Tägliche Statistiken:

Einstellung des Zeitintervalls für die tägliche Statistik. Für jeden Periode wird ein Eintrag in der Tabelle erzeugt.

Mögliche Optionen:

- **1 min**
- **2 min**
- **3 min**
- **4 min**
- **5 min**
- **10 min**
- **15 min**
- **20 min**
- **30 min**
- **1 std**
- **2 std**

- **3 std**
- **4 std**
- **6 std**
- **24 std**

Tägliche Statistiken löschen nach:

Tägliche Statistiken nach eingegebener Anzahl von Tagen löschen. Wenn 0 eingegeben ist, wird nicht automatisch gelöscht.

Logon/Logoff History löschen nach:

Einträge in der Logon/Logoff History nach eingegebener Anzahl von Tagen löschen. Bei Eingabe von **0** Tage wird nicht automatisch gelöscht.

Mögliche Aktionsschaltflächen

Sichern

Sichert die Konfiguration.

Verwerfen

Verwirft bislang ungesicherte Änderungen der Konfiguration.

Aktualisieren

Aktualisiert die Anzeige der Konfigurationsdaten aus der Datenbank.

9 Gateways

Aufruf: Hauptmenü > Gateways

Dieser Menüpunkt besteht aus dem folgenden Bereich:

- Gateway Konfiguration
- QoS Data Collection

9.1 Gateway Konfiguration

Aufruf: Hauptmenü > Gateways > Gateway Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

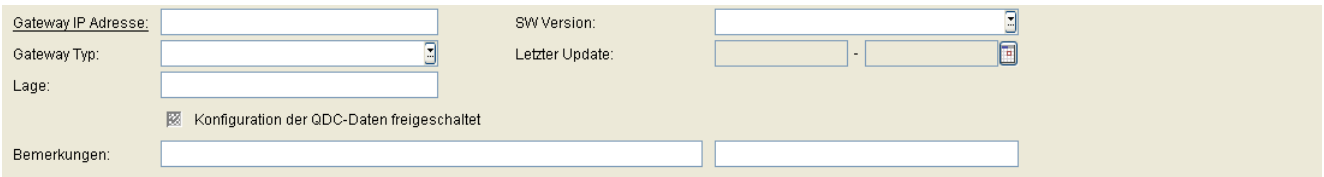
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Gateway Verbindung“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches bezieht sich nur auf die **Gateway Konfiguration**. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von Gateways zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen Gateways angezeigt (keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

Gateway IP Adresse:

IP-Adresse des Gateways.

Beispiel: **192.117.1.193**

Gateway Typ:

Typ des Gateways.

Mögliche Optionen:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

Lage:

Steckplatz der Gateway-Baugruppe (Slot).

Beispiel: **1-17-3**

SW Version:

Software-Version des Gateways. In Suchergebnissen ist dies ein schreibgeschützter Wert.

Letzter Update:

Zeitpunkt der letzten Aktualisierung des Gateways. In Suchergebnissen ist dies ein schreibgeschützter Wert.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”.

Konfiguration der QDC-Daten freigeschaltet

Schalter, der angibt, ob das Gateway in der Lage ist, QDC-Daten zu verarbeiten. Der Schalter wird beim Lesen der Gateway-Daten gesetzt und kann nur gelesen werden.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suche

Sucht nach allen Gateways, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Erstellt eine neues Gateway.

Sichern

Sichert an Konfigurationseinträgen vorgenommene Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Löschen

Löscht alle ausgewählten Objekte.

Gateway Daten lesen

Liest die Daten aller ausgewählten Gateways. Das Gateway wird im DLS eingegeben und kann im DLS geändert werden.
Die Gateway-Daten bestehen aus der Lage (Steckplatznummer einer Gateway-Baugruppe), der Software-Version und der MAC-Adresse.

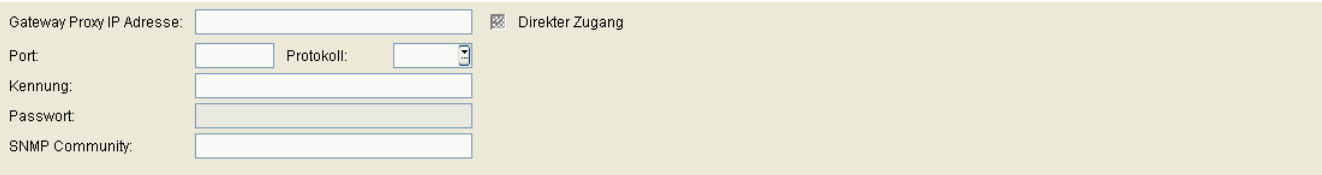
Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

9.1.1 Register „Gateway Verbindung“

Aufruf: Hauptmenü > Gateways > Gateway Konfiguration > Register „Gateway Verbindung“

HINWEIS: Je nach Gateway-Typ werden verschiedenen Konfigurationsparametern entweder Standardwerte zugewiesen oder die Parameter werden deaktiviert (falls sie nicht benötigt werden). Zur Konfiguration, siehe Abschnitt 16.3, “Einrichten eines Gateways im DLS”.



Gateway Proxy IP Adresse:

Proxy-IP-Adresse des Gateways.

Direkter Zugang

Wenn dieser Schalter aktiviert ist, wird die Verbindung zwischen HiPath 4000/HG 3550 und dem DLS über einen direkten Zugang hergestellt und nicht über den Assistant.

Port:

Proxy-Port des Gateways.

Protokoll:

Protokoll für die Kommunikation zwischen dem DLS und dem Gateway.

Mögliche Optionen:

- **http**
- **https**

Kennung:

Benutzername für den Zugriff auf den Gateway-Proxy. Die Benutzerkennung ist der erste Teil der URL.

Passwort:

Das für den Zugriff auf den Gateway-Proxy erforderliche Passwort.

SNMP Community:

Community String, der für die Authentifizierung am SNMP-Server verwendet wird.

9.2 QoS Data Collection

Aufruf: Hauptmenü > Gateways > QoS Data Collection

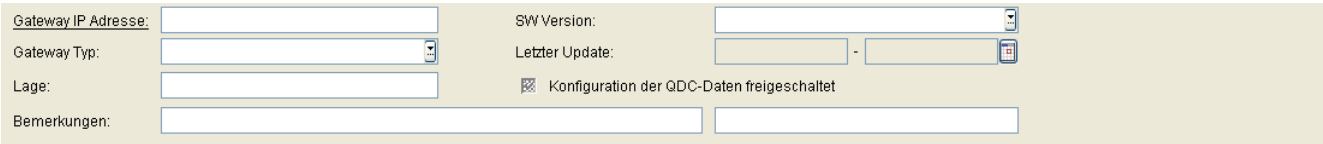
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Server Daten“
- Register „Report Einstellungen“
- Register „Schwellwerte“

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von Gateways zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen Gateways angezeigt (bis auf **Bemerkungen** keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

Gateway IP Adresse:

IP-Adresse des Gateways.

Beispiel: **192.117.1.193**

Gateway Typ:

Typ des Gateways.

Mögliche Optionen:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

Lage:

Steckplatz der Gateway-Baugruppe (Slot).

Beispiel: **1-17-3**

SW Version:

Software-Version des Gateways. In Suchergebnissen ist dies ein schreibgeschützter Wert.

Letzter Update:

Zeitpunkt der letzten Aktualisierung des Gateways. In Suchergebnissen ist dies ein schreibgeschützter Wert.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”.

Konfiguration der QDC-Daten freigeschaltet

Schalter, der angibt, ob das Gateway in der Lage ist, QDC-Daten zu verarbeiten. Der Schalter wird beim Lesen der Gateway-Daten gesetzt und kann nur gelesen werden.

Bemerkungen:

Felder für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suche

Sucht nach allen Gateways, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Holen

Lädt ein bereits gesichertes Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Sichern

Sichert Konfigurations-Einträge als Template. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

Umbenennen

Ändert den Namen eines gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

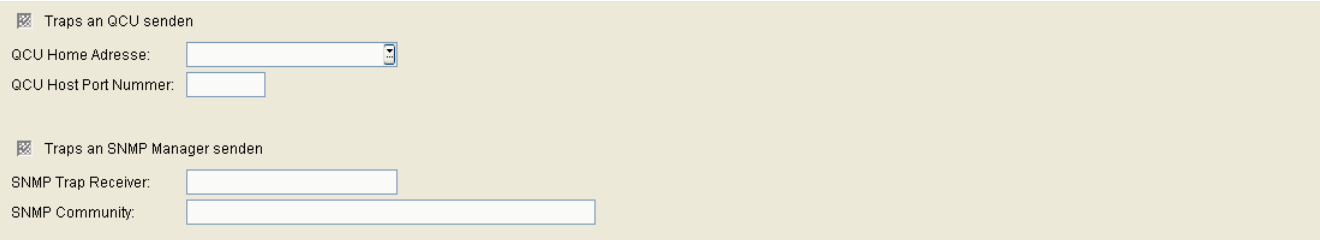
Löschen

Löscht ein gesicherten Templates. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

9.2.1 Register „Server Daten“

Aufruf: Hauptmenü > Gateways > QoS Data Collection > Register „Server Daten“

Weitere Informationen über QDC finden Sie in der QDC Interface Description (P31003-H1000-X104-*-7618) und im QDC Service Manual (P31003-H1000-S104-*-7620).



Traps an QCU senden

Schalter für das Senden von Traps an QCU.

QCU Home Adresse:

IP-Adresse oder Hostname des Servers, der die QDC-Daten protokolliert. Entspricht dem im Gateway unter **Explorer - Payload - QDC** eingetragenen Wert.

QCU Host Port Nummer:

Port-Nummer des Servers, der die QDC-Daten protokolliert. Entspricht dem im Gateway unter **Explorer - Payload - QDC** eingetragenen Wert.

Traps an SNMP Manager senden

Schalter für das Senden von Traps an den SNMP-Manager.

SNMP Trap Receiver:

Schalter zum Aktivieren der Funktion, dass Fehler an den SNMP-Manager gesendet werden. Entspricht dem im Gateway unter **Wartung - SNMP - Communities - Trap Communities** eingetragenen Wert.

SNMP Community:

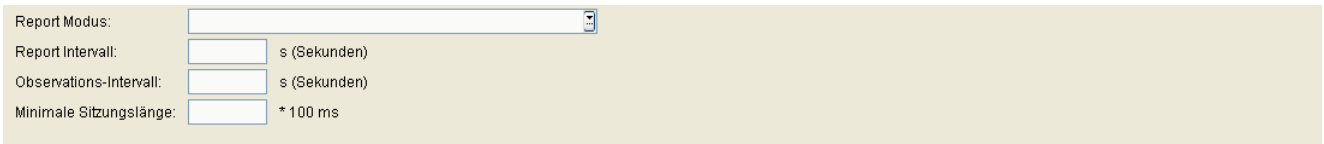
Name der SNMP-Community. Entspricht dem im Gateway unter **Wartung - SNMP - Communities - Trap Communities** eingetragenen Wert.

Standard: **Öffentlich**

9.2.2 Register „Report Einstellungen“

Aufruf: Hauptmenü > Gateways > QoS Data Collection > Register „Report Einstellungen“

Weitere Informationen über QDC finden Sie in der QDC Interface Description (P31003-H1000-X104-*-7618) und im QDC Service Manual (P31003-H1000-S104-*-7620).



Report Modus:

Mögliche Optionen:

- **Aus**
  Kein Report.
- **EOS Schwellwert überschritten**
  Report am Ende der Verbindung und bei Schwellwertüberschreitung senden.
- **EOR Schwellwert überschritten**
  Report am Ende des Reportintervalls und bei Schwellwertüberschreitung senden.
- **EOS (Ende der Verbindung)**
  Report am Ende der Verbindung senden.
- **EOR (Ende des Reportintervalls)**
  Report am Ende des Reportintervalls senden.

Report Intervall:

Wertebereich: **0** ... **3600** Sekunden.

Standard: **60** Sekunden.

Observations-Intervall:

Wertebereich: **0** ... **3600** Sekunden.

Standard: **10** Sekunden.

Minimale Sitzungslänge:

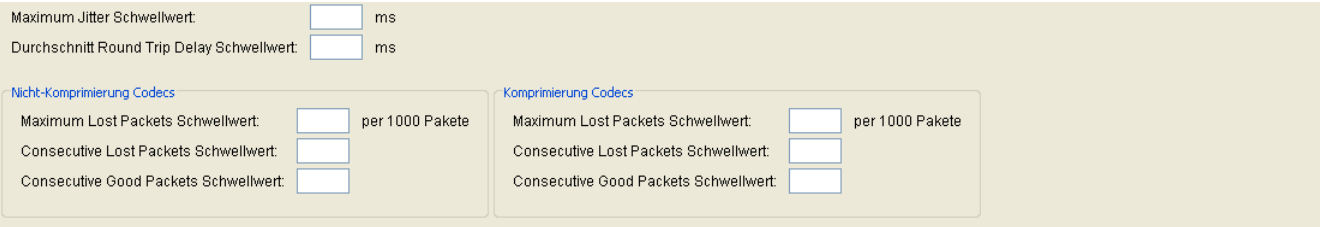
Wertebereich: **0** ... **5000** (x 100 ms)

Standard: **20** (= 2 Sekunden)

9.2.3 Register „Schwellwerte“

Aufruf: Hauptmenü > Gateways > QoS Data Collection > Register „Schwellwerte“

Weitere Informationen über QDC finden Sie in der QDC Interface Description (P31003-H1000-X104-*-7618) und im QDC Service Manual (P31003-H1000-S104-*-7620).



Maximum Jitter Schwellwert:

Maximaler Schwellwert in Millisekunden für die Laufzeitschwankungen der Datenübertragung zur Auslösung eines Reports.

Wertebereich: **0** ... **255** ms.

Standard: **15**

Durchschnitt Round Trip Delay Schwellwert:

Durchschnittliche Rückmeldezeit in Millisekunden bei der Signalübertragung.

Standard: **100**

Nicht-Komprimierung Codecs

Maximum Lost Packets Schwellwert:

Maximale Anzahl der insgesamt verlorengegangenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255** (pro 1000 Pakete).

Standard: **10**

Consecutive Lost Packets Schwellwert:

Maximale Anzahl der nacheinander folgenden, verlorengegangenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Standard: **2**

Consecutive Good Packets Schwellwert:

Minimale Anzahl der nacheinander folgenden, angekommenen Pakete bei unkomprimierter Übertragung.

Wertebereich: **0** ... **255**

Standard: **8**

Komprimierung Codecs

Maximum Lost Packets Schwellwert:

Maximale Anzahl der insgesamt verlorengegangenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255** (pro 1000 Pakete).

Standard: **10**

Consecutive Lost Packets Schwellwert:

Maximale Anzahl der nacheinander folgenden, verlorengegangenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

Standard: **2**

Consecutive Good Packets Schwellwert:

Minimale Anzahl der nacheinander folgenden, angekommenen Pakete bei komprimierter Übertragung.

Wertebereich: **0** ... **255**

Standard: **8**

10 Software Deployment

Aufruf: Hauptmenü > Software Deployment

Dieses Menü besteht aus folgenden Untermenüs:

- Workpoint Deployment
- Regeln bearbeiten

Der Bereich **Software Deployment** dient zum komfortablen Verteilen von Software-Images und sonstiger Workpoint-Software.

HINWEIS: Beachten Sie die Unterscheidung zwischen **Software Deployment** und **Datei Deployment** in der Oberfläche des DLS (siehe Abschnitt 10.1.1 und Abschnitt 10.1.2). Unter

Software Deployment versteht man das Verteilen von Software für Workpoints (IP Phones und IP Clients). Mit **Datei Deployment** ist hingegen das Verteilen von beliebigen Binär- oder ASCII-Dateien gemeint, die im Workpoint eine bestimmte Aufgabe erledigen.

Beide Funktionen sind im DLS im Hauptmenü unter **Software Deployment** zusammengefasst.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

HINWEIS: Achten Sie beim Verteilen von Software für Workpoints des Typs optiPoint WL2 professional darauf, dass die Workpoints über eine ausreichende Batteriekapazität verfügen. Ansonsten ist ein erfolgreiches Deployment ggf. nicht möglich.

10.1 Workpoint Deployment

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment

Die Versorgung einzelner IP Clients bzw. IP Phones mit Software (Firmware) sowie weiterer Daten kann vom DLS gesteuert werden.

Voraussetzung ist, dass sowohl die zu verteilenden Dateien als auch die gewünschten Workpoints im DLS registriert sind. Zudem müssen die FTP-Server und Netzlaufwerke im DLS registriert sein, denn diese liefern die Daten an die Workpoints (siehe Abschnitt 6.3.4, “FTP Server Konfiguration” und Abschnitt 6.3.7, “Netzlaufwerk Konfiguration”).

HINWEIS: Das Deployment über ein Netzlaufwerk steht in der onboard-Variante des DLS auf OpenScape Voice nicht zur Verfügung.

Dieser Bereich kann wie folgt in Gruppen eingeteilt werden:

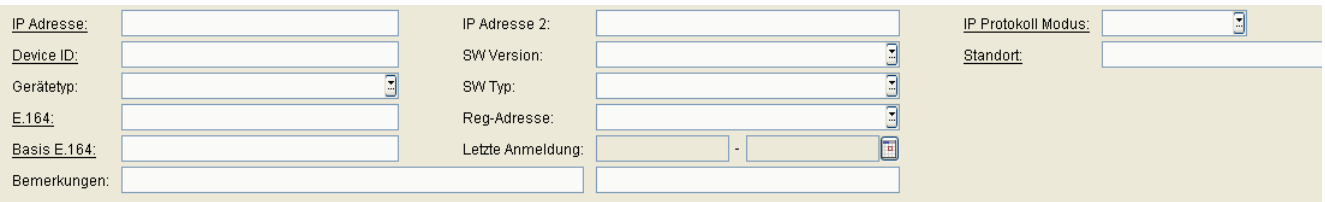
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Software- und Datei-Deployment
  bestehend aus:
  - Register „Software Deployment“
  - Register „Datei Deployment“
- Inventar-Datenanzeige
  bestehend aus:
  - Register „Software Inventar“
  - Register „LDAP Inventar“
  - Register „Wartemusik Inventar“
  - Register „INCA Inventar“
  - Register „Java Midlet Inventar“
  - Register „LOGO Datei Inventar“
  - Register „System-/Rufton Inventar“
  - Register „APM Inventar“
  - Register „NETBOOT Inventar“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Wenn Sie diese Funktion häufig benötigen, können Sie die Funktion durch den Einsatz von Deployment-Jobs einfach und komfortabel automatisieren (siehe Kapitel 14, “Job Koordination”).

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für alle Oberflächen dieses Menüs identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von Workpoints zu finden. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen Workpoints angezeigt (bis auf **Bemerkung** keine Änderungsmöglichkeit).



In manchen Bereichen stehen nicht alle beschriebenen Felder zur Verfügung.

HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse des Workpoints. Für OpenStage wird hier entweder eine IPv4- oder eine IPv6-Adresse angezeigt. Siehe auch die Beschreibung zum Parameter **IP Protokoll Modus**.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

Physikalische MAC-Adresse des Workpoints.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Devices.

Alle vom DLS unterstützte Workpoint-Typen finden Sie im Abschnitt 3.4, “Unterstützte IP Devices/Versionen”.

Beispiele: **optiPoint 410 standard**, **optiClient 130**.

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

IP Adresse 2:

Zweite IP-Adresse des IP Phones, falls dieses eine IPv6-Adresse hat.

Nur für OpenStage verfügbar.

SW Version:

Software-Version des Workpoints.

Beispiel für IP Phone und IP Client: **5.0.12**.

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des Workpoints.

Beispiele: **Unify HFA**, **Unify SIP**.

Reg-Adresse:

IP-Adresse des Gateways oder des Gatekeepers, an dem sich das IP Device registrieren muss. Bei HiPath 3000 ist das die Adresse der HG 1500, bei HiPath 4000 ist es die HG 3530 oder das STMI-Board.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Phones.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”.

Standort:

Aktueller Standort des IP Device.

Bemerkungen:

Felder für allgemeine Informationen.

IP Protokoll Modus

Zeigt an, welche IP-Version das IP Phone verwendet. Werden beide Versionen verwendet, steht in IP Adresse die IPv4-Adresse und in IP Adresse 2 die IPv6-Adresse.

Nur für OpenStage verfügbar.

Mögliche Optionen:

- **IPv4**
- **IPv6**
- **IPv4 und IPv6**

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

In der Ansicht **Suche** wird nach allen registrierten Workpoints gesucht, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Deploy

In der Ansicht **Objekt** und **Tabelle** wird ein Job zum Software- bzw. Datei-Deployment gestartet. Siehe hierzu Abschnitt 15.6, “Verteilen von Workpoint-Software”.

10.1.1 Register „Software Deployment“

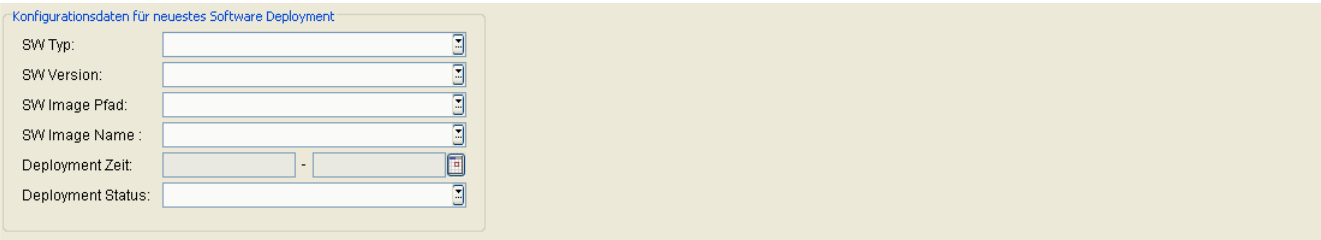
Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „Software Deployment“

In diesem Register werden die Daten zum letzten Software-Deployment für Workpoints angezeigt, das mit dem DLS durchgeführt wurde.

Software bezeichnet immer eine Applikationssoftware für eine bestimmte Ausprägung eines Workpoints (z. B. optiPoint 410 standard). Diese Software liegt in der Regel als sogenanntes Software-Image (meistens eine Datei mit einer Extension *.app*) vor, die auf Workpoints verteilt („deployed“) werden kann.

HINWEIS: Alle Software-Images, die mit und nach der Einführung des DLS verfügbar sind, enthalten eine DLS-Schnittstelle zur Kommunikation mit dem DLS (Terminologie: „Software im neuen Format“). Alle existierenden und vorher verfügbaren Software-Images enthalten diese Schnittstelle nicht (Terminologie: „Software im alten Format“).

Zur Übersicht aller vom DLS unterstützten Software-Typen siehe Abschnitt 3.5, “Übersicht der Software- und Datei-Typen”.



Konfigurationsdaten für neuestes Software Deployment

SW Typ:

Software-Typ des Workpoints.

Beispiel: **Unify HFA**, **Unify SIP**

SW Version:

Software-Version des Workpoints.

Beispiel für IP Phone und IP Client: **5.0.12**

SW Image Pfad:

Pfadname des Verzeichnisses, in dem die Datei mit dem Software-Image abgelegt ist.

Beispiele: **/Verzeichnis1/Subverzeichnis2** für IP Phone-Dateien, **\Verzeichnis1\Subverzeichnis2** für IP Client-Dateien.

SW Image Name:

Dateiname des Software-Image.

Beispiele: **vxworks.app**, **op410std-siemens-hfa-V5.0.12-L12345678.app**

Deployment Zeit:

Zeitbereich bzw. Zeitpunkt des letzten Starts eines Software-Deployments (Kalender siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

Deployment-Status:

Ergebnis (Status) des letzten Software-Deployments.

Mögliche Optionen:

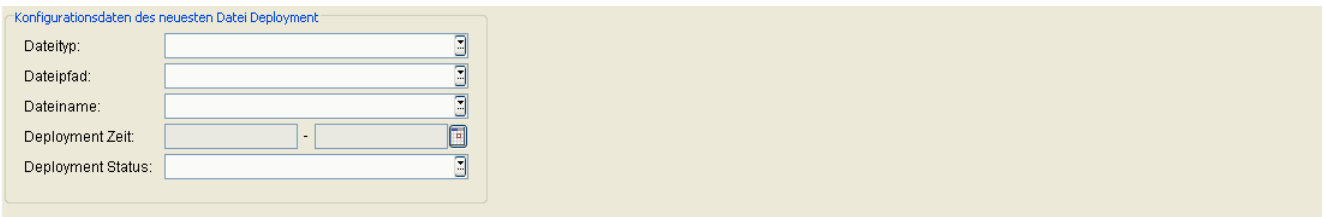
- **Deployment abgewiesen**:
  Das Deployment konnte nicht gestartet werden. Möglicher Grund: Das Deployment war so konfiguriert, dass es nur im Ruhezustand des Workpoints durchgeführt werden durfte, was nicht der Fall war.
- **Deployment angestoßen**:
  Das Deployment wurde begonnen, ist jedoch noch nicht abgeschlossen.
- **Deployment beendet**
  Das Deployment wurde erfolgreich abgeschlossen.
- **Deployment fehlgeschlagen**
  Während des Deployments ist ein Fehler aufgetreten.

10.1.2 Register „Datei Deployment“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „Datei Deployment“

In diesem Register werden die Daten (Dateityp) zum letzten Datei-Deployment für Workpoints angezeigt, das mit dem DLS durchgeführt wurde.

Zur Übersicht aller vom DLS unterstützten Datei-Typen siehe Abschnitt 3.5, “Übersicht der Software- und Datei-Typen”.



Konfigurationsdaten des neuesten Datei Deployment

Dateityp:

Typ der Datei (siehe Abschnitt 3.5, “Übersicht der Software- und Datei-Typen”).

Beispiel: **Java Midlet**, wenn als letzte Aktion eine Java-Applikation an das IP Phone verteilt wurde.

Dateipfad:

Pfadname des Verzeichnisses, in dem die Datei vom entsprechendens Typ abgelegt ist.

Beispiele: **/Verzeichnis1/Subverzeichnis2** für IP Phone-Dateien, **\Verzeichnis1\Subverzeichnis2** für IP Client-Dateien.

Dateiname:

Name der verteilten Datei.

Deployment Zeit:

Zeitbereich bzw. Zeitpunkt des letzten Starts eines Software-Deployments (Kalender siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

Deployment-Status:

Hier wird das Ergebnis (Status) des letzten Software-Deployments angezeigt.

Möglicher Status:

- **Deployment abgewiesen**:
  Das Deployment konnte nicht gestartet werden.
- **Deployment angestoßen**:
  Das Deployment wurde begonnen, ist jedoch noch nicht abgeschlossen.
- **Deployment beendet**
  Das Deployment wurde erfolgreich abgeschlossen.
- **Deployment fehlgeschlagen**
  Während des Deployments ist ein Fehler aufgetreten.

10.1.3 Register „Software Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „Software Inventar“

Inventar/Status Daten der Software Installation

SW Server:

Adresse des FTP Servers (für IP Phones) oder Netzwerkrechners (für IP Clients), von dem die Software runtergeladen wurde. Die Adresse kann entweder eine IP-Adresse oder ein Hostname sein.

SW Image Name:

Dateiname der Software, die heruntergeladen wird.

Installationsdatum:

Datum, zu dem die letzte Software heruntergeladen bzw. installiert wurde.

Installationsstatus:

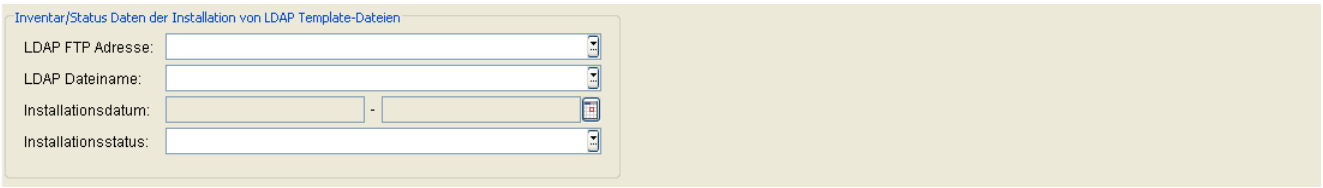
Hier wird der Status der Software-Installation angezeigt.

Sprachpaket:

Zeigt an, welches Sprachpaket installiert ist.

10.1.4 Register „LDAP Inventar“

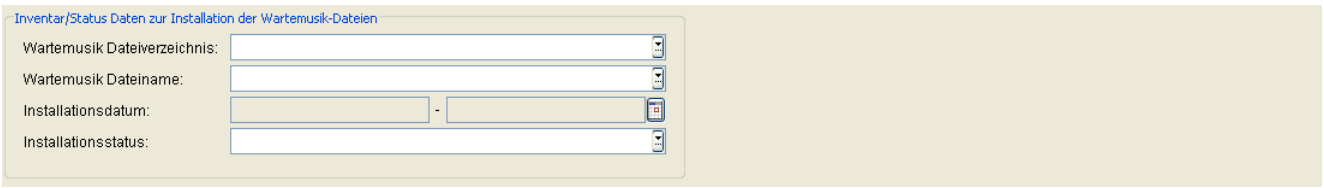
Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „LDAP Inventar“



HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

10.1.5 Register „Wartemusik Inventar“

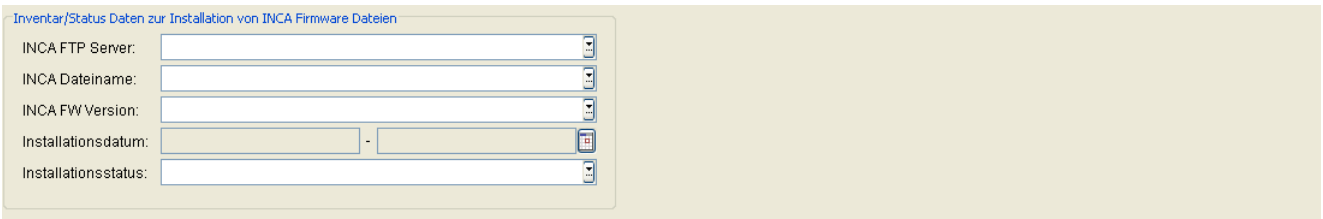
Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „Wartemusik Inventar“



HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

10.1.6 Register „INCA Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „INCA Inventar“



HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

INCA FW Version:

Version der INCA-Firmware.

10.1.7 Register „Java Midlet Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „Java Midlet Inventar“

HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

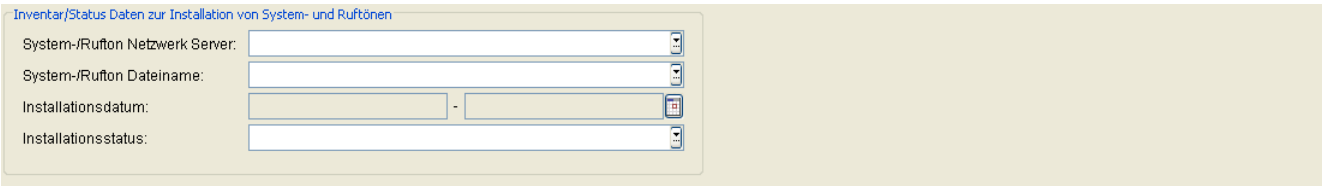
10.1.8 Register „LOGO Datei Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „LOGO Datei Inventar“

HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

10.1.9 Register „System-/Rufton Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „System-/Rufton Inventar“



System-/Rufton Netzwerk Server:

Adresse des Netzwerkrechners, von dem die System- und Ruftöne heruntergeladen wurden. Die Adresse kann entweder eine IP-Adresse oder ein Hostname sein.

System-/Rufton Dateiname:

Verzeichnis auf dem Netzwerkcomputer, von dem die Ruftöne heruntergeladen wurden, beginnend mit dem Pfad der Netzwerkfreigabe.

System-/Rufton Dateiname:

Name der Datei, die den System-/Rufton enthält.

Installationsdatum:

Datum, zu dem die letzten System- und Ruftöne runtergeladen bzw. installiert wurden.

Installationsstatus:

Hier wird der Status der Installation der System- und Ruftöne angezeigt.

10.1.10 Register „APM Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „APM Inventar“

HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

APM FW Version:

Version der APM Firmware.

10.1.11 Register „NETBOOT Inventar“

Aufruf: Hauptmenü > Software Deployment > Workpoint Deployment > Register „NETBOOT Inventar“

HINWEIS: Für alle Felder dieses Registers gilt sinngemäß die Beschreibung wie in Abschnitt 10.1.3, “Register „Software Inventar“”.

NETBOOT FW Version:

Version der NETBOOT Firmware.

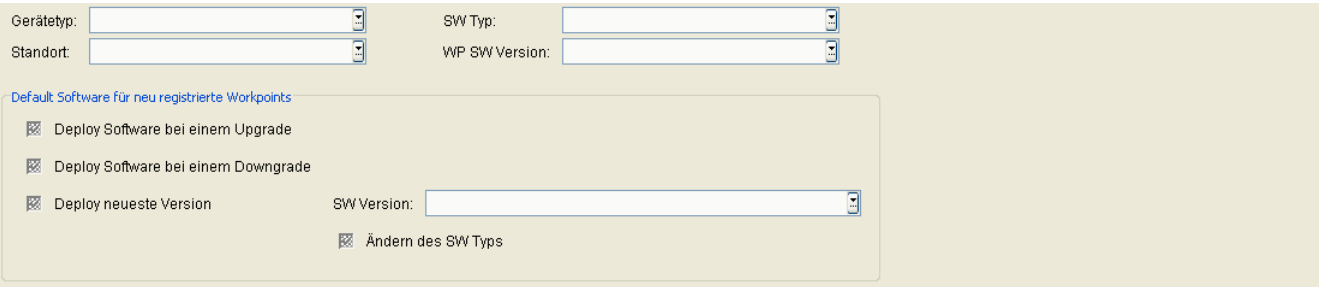
10.2 Regeln bearbeiten

Aufruf: Hauptmenü > Software Deployment > Regeln bearbeiten

Mithilfe von Deployment-Regeln können Sie die Verteilung von Software steuern und den entstehenden Übertragungs-Traffic eingrenzen.

Wird die automatische Software-Verteilung für einen Workpoint angestoßen, so prüft diese zunächst, ob es eine Regel für den Gerätetyp des Workpoints gibt. Gibt es keine Regel oder ist die Regel deaktiviert, so wird keine Software an diesen Workpoint verteilt.

Informationen zur Anwendung der Deployment-Regeln finden Sie im Abschnitt 15.6.2, “Automatisches Deployment”.



Gerätetyp:

Gerätetyp des Workpoints, für den die Regel gelten soll.

Beispiele: **optiPoint 410 standard**, **optiClient 130**.

> ***HINWEIS:*** Wenn Sie eine Software unabhängig vom aktuellen Standort der Geräte auf allen Geräten bereitstellen wollen, erstellen Sie eine Default Location mit dem Typ **ALLE**.
> Die Geräte DÜRFEN jedoch KEINER anderen Standort-Regel entsprechen.

SW Typ:

Typ der Software, die aktuell auf den Workpoints installiert ist, für die die Regel gelten soll.

Beispiele: **Unify HFA**, **Unify SIP**.

WP SW Version:

Version der Software, die aktuell auf den Workpoints installiert ist, für die die Regel gelten soll.

Standort

Name des Standorts (IP-Bereich und Gatekeeper), dem die Deployment-Regeln zugeordnet werden.

Default Software für neu registrierte Workpoints

Deploy Software bei einem Upgrade

Schalter zum Aktivieren der Deployment-Funktion im Falle eines Upgrades.
Dies bedeutet, dass ein Deployment stattfindet, wenn die Software am Workpoint **älter** ist als die neueste bzw. in der Regel selektierte Software.

> ***HINWEIS:*** Soll die Regel deaktiviert (aber nicht gelöscht) werden, deaktivieren Sie diese und die nachfolgende Option.

Deploy Software bei einem Downgrade

Schalter zum Aktivieren der Deployment-Funktion im Falle eines Downgrades.
Dies bedeutet, dass ein Deployment stattfindet, wenn die Software am Workpoint eine höhere Versionsnummer hat als die in der Regel selektierte Software.

> ***HINWEIS:*** Soll die Regel deaktiviert (aber nicht gelöscht) werden, deaktivieren Sie diese und die vorhergehende Option.

Deploy neueste Version

Schalter zum Aktivieren der Deployment-Funktion mit der neuesten Version eines Software-Typs.
Dies bedeutet, dass bei einem Update (Downgrade) die neueste Software an all die Workpoints übertragen wird, die noch nicht diese Software-Version besitzen.

SW Version:

Dropdown-Liste mit allen verfügbaren Software-Images für die angegebenen Geräte- und SW-Typen.

> ***HINWEIS:*** Die Dropdown-Liste „SW Version“ enthält die Software-Images, die auf dem zum ausgewählten Standort gehörenden FTP-Server liegen. Wenn dem Standort kein FTP-Server zugeordnet ist, erscheint die Fehlermeldung: „**Choice list not available**“.

Beispiel für optiPoint und optiClient: **5.0.12**.

Ändern des SW Typs

Ist der Schalter aktiviert, wird der Software-Typ des Workpoints beim Deployment durch den des ausgewählten Software-Images ersetzt.

Mögliche Aktionsschaltflächen

Suchen

Sucht nach konfigurierten Deployment-Regeln entsprechend den angegebenen Kriterien.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Fügt eine neue Deployment-Regel hinzu.

Sichern

Sichert die Änderungen. Eine neu angelegte Regel ist anschließend sofort aktiv.

Verwerfen

Verwirft die vorgenommenen Änderungen.

Löschen

Löscht eine bestehende Deployment-Regel.

Anwenden

Startet die automatische Software-Verteilung.

11 Element Manager

Aufruf: Hauptmenü > Element Manager

Hier werden die Angaben zu den jeweiligen Anlagentypen verwaltet.

Dieses Menü besteht aus folgenden Untermenüs:

- Element Manager Konfiguration

Um die Plug&Play-Funktionalität nutzen zu können, müssen hier einige Konfigurationen vorgenommen werden.

Grundlageninformationen zum Thema Plug&Play finden Sie in Abschnitt 15.5, “Autokonfiguration von Workpoints (Plug&Play)”.

Informationen zur Einrichtung eines DHCP-Servers für vollständiges Plug&Play finden Sie im Abschnitt 4.12.4, “DHCP-Server in einer Windows-Umgebung” bzw. Abschnitt 4.12.5, “DHCP-Server in einer Linux/Unix-Umgebung”.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

11.1 Element Manager Konfiguration

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration.

Die Angaben zu den jeweiligen Anlagentypen werden in den einzelnen Registern des Element Managers eingetragen.

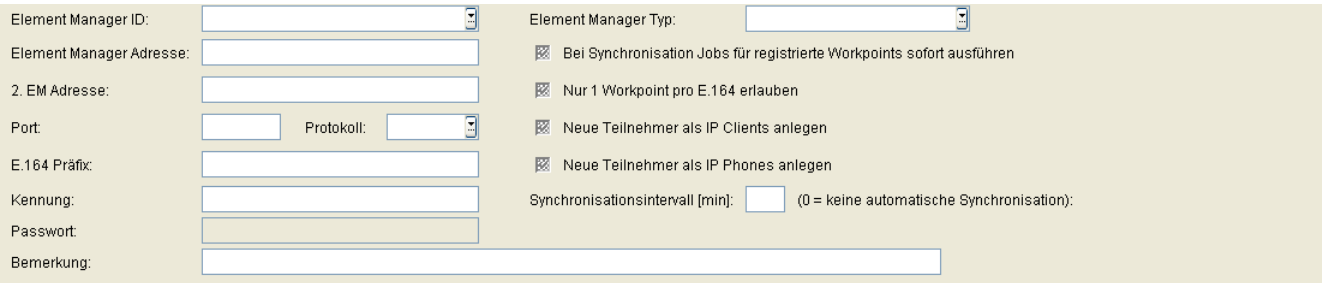
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „OpenScape Voice“
- Register „OpenScape Voice Assistant“
- Register „OpenScape Voice Assistant V3.0“
- Register „HiPath 4000 Assistant“
- Register „HiPath 3000/5000“
- Register „OpenScape Office MX/LX“
- Register „OpenOffice EE“
- Register „HiPath DXWeb Pro“
- Register „Protokoll“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht Suche, um eine bestimmte Gruppe von Element Managern zu finden. In der Ansicht Objekt werden hier die Basis-Daten der gefundenen Element Manager angezeigt (bis auf Bemerkung keine Änderungsmöglichkeit).

Weiteres zur Änderung der Konfiguration siehe Abschnitt 15.2, “Änderung der Element Manager-Konfiguration und Joberzeugung”.



Element Manager ID:

Frei vorgebbare ID (Pflichtfeld). Dient zur eindeutigen Identifizierung des Element Managers, der ggf. die Daten zu Workpoints liefert.

Element Manager Adresse:

Hostname oder IP-Adresse des Element Managers.

2. EM Adresse:

Hostname oder IP Adresse des 2. Knotens.

HINWEIS: Dieser Parameter ist nur für geographisch separierte OpenScape Voice-Cluster relevant.

Port

Port, über den der Element Manager mit dem DLS kommuniziert. Die folgende Auflistung gibt die von den einzelnen Element Managern für verschiedene Protokolle verwendeten Ports an:

- OpenOffice EE: **443** (HTTPS)
- HiPath 3000 / 5000: **8085** (HTTP) oder **443** (HTTPS)
- HiPath 4000 (Webservice): **443** (HTTPS)
- HiPath 4000 (JDBC): **1527**
- OpenScape Voice: **8767** (HTTP)

- OpenScape Voice Assistant: **443** (HTTPS)
- OpenScape Office MX/LX: **443** (HTTPS)

Protokoll

Protokoll, das für den Datenaustausch mit dem Element Manager verwendet wird.

Mögliche Optionen:

- **http**
- **https**

E.164 Präfix

Präfix der E.164-Nummer. Wird für Workpoints bei OpenScape Voice, HiPath 3000/5000, OpenOffice EE und HiPath DXWebPro verwendet. Für Hipath 3000/5000 Version < V7 nur für HFA-Endgeräte. Wenn nichts eingegeben wird, muss die Rufnummer des Workpoints im Netz eindeutig sein. In anderen Oberflächen des DLS ist dann für E.164 nur die Rufnummer einzugeben.Für HiPath 4000 wird dieses Feld nicht ausgewertet; stattdessen sind im Register „HiPath 4000 Assistant“ die entsprechenden Werte in der Tabelle **Virtuelle Knoten IDs (HFA)** einzutragen. Wenn hier nichts eingegeben wird, muss die Rufnummer des IP Phones oder IP Clients im Netz eindeutig sein. In anderen Oberflächen des DLS ist dann in E.164-Feldern nur die Rufnummer einzugeben.

Beispiel: **4989722** (oder keine Angabe).

Kennung:

Die Zugansgskennung ist für den HiPath 4000 Assistant und für den OpenScape Voice Assistant erforderlich. Für den HiPath 4000 Assistant ist die Kennungs „uas_read“ erforderlich; diese muss dort aktiviert sein.

Z. B. JDBC-Kennung bei HiPath 4000.

Passwort

Erfordeliches Passwort für den Element Manager-Zugang. Die Eingabe erfolgt durch Klick auf das Schlüssel-Symbol in einem Dialogfenster.

Z. B. JDBC-Passwort bei HiPath 4000.

Element Manager Typ:

Element Manager Typ auswählen. Es können nur Daten in das entsprechende Register eingetragen werden.

Mögliche Optionen:

- **HiPath 4000 (JDBC)** (siehe **Register „HiPath 4000 Assistant“**)
- **OpenScape Voice Assistant V3.0** (siehe **Register „OpenScape Voice Assistant V3.0“**)
- **OpenScape Voice Assistant** (siehe **Register „OpenScape Voice Assistant“**)

  HINWEIS: Bei dieser Option ist das Register OpenScape Voice deaktiviert.

  WICHTIG: Bei mehreren Element Manager IDs unterstützt der DLS Element Manager mehrere OSVs nur, wenn es bei der Bereitstellung keine Überlappung gibt.
- **HiPath 3000 / 5000** (siehe **Register „HiPath 3000/5000“**)
- **HiPath DXWeb Pro** (siehe **Register „HiPath DXWeb Pro“**)
- **OpenScape Voice** (siehe **Register „OpenScape Voice“**)
- **HiPath 4000 (Webservice)** (siehe **Register „HiPath 4000 Assistant“**)
- **OpenOffice EE** (siehe **Register „OpenOffice EE“**)
- **OpenScape Office MX/LX** (siehe **Register „OpenScape Office MX/LX“**)

Bei EM Synchronisation Jobs für registrierte Workpoints sofort ausführen

Ist der Schalter aktiviert, werden bei der Element Manager-Synchronisation die Jobs sofort ausgeführt.

Nur 1 Workpoint pro E.164 erlauben

Ist der Schalter aktiviert, werden nur diejenigen Workpoints mit Daten versorgt, die schon bisher von diesem Element Manager aktualisiert wurden oder diesem zugeordnet sind (**IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „EM Synchronisation“** > **Zugeordneter Element Manager**). Damit wird das Sicherheitsrisiko vermieden, dass Workpoints mit manipulierten E.164-Nummern automatisch mit Registrierungsdaten versorgt werden können, falls mehrere Workpoints unter derselben E.164 registriert sind.

Neue Teilnehmer als IP Clients anlegen

Ist der Schalter aktiviert, werden für die bei der Synchronisation mit der Telefonanlage übertragenen und im DLS noch nicht vorhandenen Teilnehmer (d. h. E.164-Nummern) neue IP Clients angelegt.

Neue Teilnehmer als IP Phones anlegen

Ist der Schalter aktiviert, werden für die bei der Synchronisation mit der Telefonanlage übertragenen und im DLS noch nicht vorhandenen Teilnehmer (d. h. E.164-Nummern) neue IP Phones angelegt. Dieser Schalter ist standardmäßig gesetzt.

Synchronisationsintervall [min]

Bestimmt das Zeitintervall, in dem periodische Synchronisationsvorgänge zwischen der im Element Manager eingestellten Telefonanlage und dem DLS erfolgen.

Wertebereich: **10 ... 1440** Minuten oder **0** für keine automatische Synchronisation.

Standard: **0**

HINWEIS: Bei dieser Option ist das Register OpenScape Voice deaktiviert.

WICHTIG: Stellen Sie sicher, dass der Wert für das Synchronisierungsintervall mindestens **60** Minuten beträgt.
Obwohl der Wert **0** grundsätzlich erlaubt ist, müssen alle Element Manager mit einem Synchronisierungsintervall von weniger als **60** Minuten während des Upgrades auf den neuen Mindestwert von 60 Minuten aktualisiert werden.

Bemerkung

Feld für allgemeine Informationen.

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen im DLS eingetragenen Element Managern, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Legt eine neue Element Manager-Konfiguration an.

Sichern

Sichert eine Element Manager-Konfiguration.

Verwerfen

Verwirft die Änderungen und neuen Einträge.

Löschen

Löscht die Element Manager-Konfiguration.

Synchronisieren

Durch das Synchronisieren werden Registrierungsdaten aus dem Element Manager in die Datenbank des DLS übernommen. Dieser Vorgang erfolgt im Hintergrund. Am Ende der Synchronisation, die mehrere Minuten dauern kann, wird eine Protokolldatei erstellt.

Die Synchronisation erzeugt oder ändert Workpoints; dabei kann es zur Job-Erzeugung kommen. Diese Jobs werden ohne Rückfrage erzeugt.

> ***HINWEIS:*** Läuft bereits eine Synchronisation und wird während dieser Zeit erneut versucht, eine Synchronisation bei dem gleichen Element Manager zu starten, so wird eine Fehlermeldung ausgegeben.

HINWEIS: Eine neue Element Manager-Synchronisation sollte erst dann ausgelöst werden, wenn die vorherige Synchronisation abgeschlossen ist (egal ob diese erfolgreich war oder nicht).

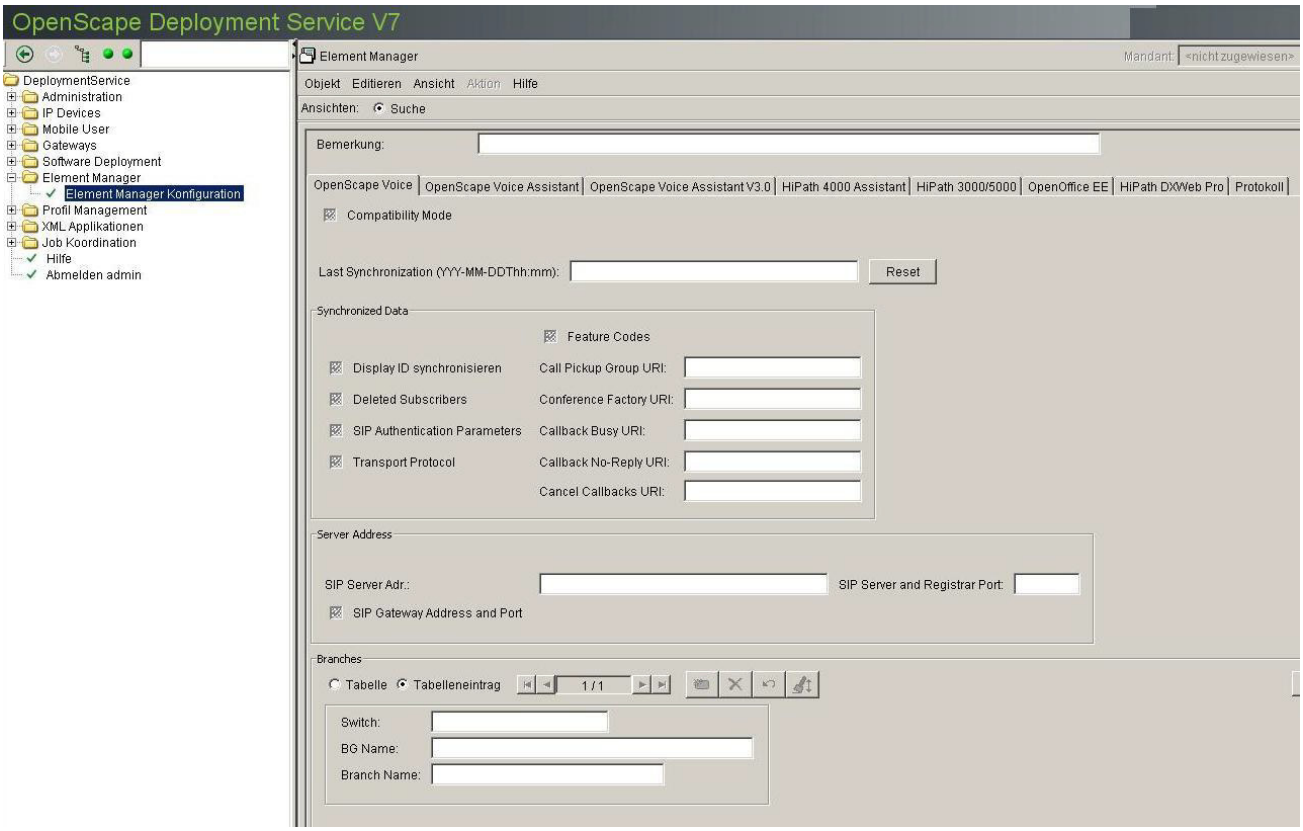
Aktualisieren

Aktualisiert den Inhalt der aktuellen Maske aus der Datenbank.

11.1.1 Register „OpenScape Voice“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „OpenScape Voice“.

Weiteres zur Änderung der Konfiguration siehe Abschnitt 15.2, “Änderung der Element Manager-Konfiguration und Joberzeugung”.



HINWEIS: Um eine Synchronisation mit OpenScape Voice durchzuführen, müssen Sie zunächst die entsprechende Paketfilterregel* für den lokalen OpenScape Voice-Port 8769 erstellen und eingehende TCP-Verbindungen von der Remote-IP-Adresse des Windows-DLS-Servers zulassen.
* Firewall-Regel über OpenScape Voice Assistant

Compatibility Mode (Kompatibilitätsmodus)

Schalter zur Konfiguration des Kompatibilitätsmodus Falls dieser Schalter aktiviert ist, erfolgte die letzte Synchronisierung im Kompatibilitätsmodus. Falls dieser Schalter nicht aktiviert ist, erfolgte die letzte Synchronisierung im Normalmodus.

Last Synchronization (Letzte Synchronisation)

Zeit & Datum der letzten Synch. Schreibgeschütztes Feld mit Text im folgenden Format:

YYYY-MM-DDThh:mm

Beispiel: 2011-05-29T19:00

Standardwert: leer

Reset (Zurücksetzen)

Dieser Button dient zum Löschen/Rücksetzen des Feldwerts für die letzte Synchronisierung.

Synchronized Data (Synchronisierte Daten)

Display ID synchronisieren

Schalter zum Aktivieren der Display ID-Synchronisation.

Deleted Subscribers (Gelöschte Teilnehmer)

Schalter zum Aktivieren der Löschung von OSV-Teilnehmern. Wenn dieser Schalter aktiviert ist, werden Endgeräte und Leitungstasten/Direktruftasten, deren Leitungsziel einem nicht vorhandenen (oder gelöschten) OSV-Teilnehmer entspricht, in den Papierkorb übertragen.

Wenn dieser Schalter nicht aktiviert ist, verbleiben Endgeräte und Leitungstasten/Direktruftasten, die nicht vorhandenen (oder gelöschten) OSV-Teilnehmern entsprechen, in der DLS-Datenbank.

Dieser Schalter ist standardmäßig deaktiviert.

SIP Authentication Parameters (SIP-Authentifizierungsparameter)

Schalter zur Konfiguration der SIP-Authentifizierungsparameter Wenn dieser Schalter aktiviert ist, wird allen Endgeräten und Leitungstasten/Direktruftasten, die während der Synchronisierung eingerichtet/aktualisiert wurden, derselbe SIP Realm, Benutzername und dasselbe Passwort des entsprechenden OSV-Teilnehmeranschlusses zugewiesen.

Wenn dieser Schalter nicht aktiviert ist, werden die Angaben SIP Realm, Benutzername und Passwort des OSV-Teilnehmers während der Synchronisation mit OSV ignoriert.

Dieser Schalter ist standardmäßig deaktiviert.

Transport Protocol (Transportprotokoll)

Schalter zur Konfiguration des Transportprotokolls. Wenn dieser Schalter aktiviert ist, wird dem Transportprotokoll für alle Endgeräte, die während der Synchronisation eingerichtet/aktualisiert wurden, derselbe Wert des jeweiligen OSV-Teilnehmers zugewiesen.

Wenn dieser Schalter nicht aktiviert ist, wird das Transportprotokoll der in DLS vorhandenen Endgeräte verwendet und das Transportprotokoll der OSV-Teilnehmer wird ignoriert, obwohl CMP es nach einer Geräteänderung (außerhalb des Synchronisierungskontextes) dem DLS-Endgerät zuordnen könnte. Unabhängig davon wird das Transportprotokoll aber bei der Einstellung des SIP-Gateway-Ports verwendet, sofern dieser aktiviert ist.

Dieser Schalter ist standardmäßig deaktiviert.

Feature Codes

Schalter zur Konfiguration von Feature Codes (Leistungsmerkmalkennzahlen) Wenn dieser Schalter aktiviert ist, werden allen Endgeräten, die während der Synchronisation eingerichtet/aktualisiert wurden, die Feature Access Codes zugewiesen, die im OSV Element Manager als Attribute konfiguriert sind.

Wenn dieser Schalter nicht aktiviert ist, werden keine Feature Access Codes zugewiesen.

Dieser Schalter ist standardmäßig deaktiviert.

Call Pickup Group URI (Anrufübernahmegruppe URI)

Textfeld zur Konfiguration der Anrufübernahmegruppe URI.

Zulässiger Wert: max. 15 Zeichen (0-9,*,#).

Standardwert: *7.

Conference Factory URI (Konferenz URI)

Textfeld zur Konfiguration der Konferenz URI.

Zulässiger Wert: max. 15 Zeichen (0-9,*,#).

Standardwert: 1234567890.

Callback Busy URI (Rückruf nach Besetzt URI)

Textfeld zur Konfiguration der Rückruf nach Besetzt URI.

Zulässiger Wert: max. 15 Zeichen (0-9,*,#).

Standardwert: *6.

Callback No-Reply URI (Rückruf nach nicht Melden URI)

Textfeld zur Konfiguration der Rückruf nach nicht Melden URI.

Zulässiger Wert: max. 15 Zeichen (0-9,*,#).

Standardwert: *6.

Cancel Callbacks URI (Rückrufe löschen URI)

Textfeld zur Konfiguration der Rückrufe löschen URI.

Zulässiger Wert: max. 15 Zeichen (0-9,*,#).

Standardwert: #6.

Server Adresse

SIP Server Adr.

IP-Adresse des SIP-Servers und SIP-Registrars. Dieser Wert wird nicht von OpenScape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Server Port

Portnummer des SIP-Servers. Dieser Wert wird nicht von OpenScape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Gateway Address and Port (SIP-Gateway-Adresse und -Port)

Schalter zur Konfiguration von SIP-Gateway-Adresse und -Port. Wenn dieser Schalter aktiviert ist, wird die mittels OSV-SOAP-Anforderung ermittelte Adresse (IP des FQDN) des zugehörigen Teilnehmer-Endpunktes als Gateway-IP-Adresse der Endgeräte festgelegt, die während der Synchronisierung erstellt/aktualisiert wurden. Die Gateway-Port-Nummer wird entsprechend des Transportprotokolls des synchronisierten Teilnehmers auf 5060 (TCP/UCP) oder 5061 (TLS) gesetzt.

Wenn dieser Schalter nicht aktiviert ist, werden Gateway-Adresse und Port für die während der Synchronisierung erstellten/aktualisierten Endgeräte nicht festgelegt.

Dieser Schalter ist standardmäßig deaktiviert.

Branches

Switch

Name des Switches an dem die OS Branch eingerichtet sind.

BG Name

Name der Business Goup

Branch Name

Name des Branches

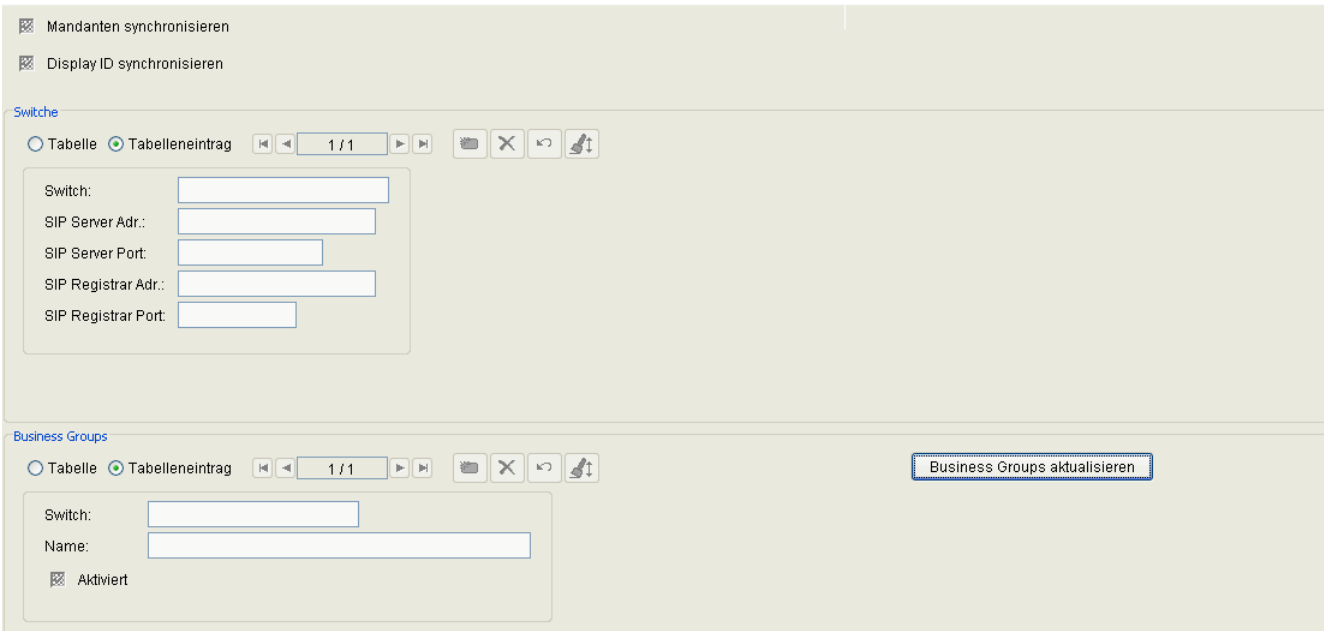
Branches erhalten

Startet das Aktualisieren der Branches und Synchronisieren der Mandanten. Das Aktualisieren erfolgt im Hintergrund; erst am Ende wird eine Protokolldatei erstellt. Es kann eventuell einige Minuten dauern, bis diese Datei zur Verfügung steht.

> ***HINWEIS:*** Wenn der ausgewählte Element Manager Typ „OpenScape Voice Assistant“ ist, kann „Branches erhalten“ (Get Branches) nicht ausgeführt werden.

11.1.2 Register „OpenScape Voice Assistant“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „OpenScape Voice Assistant“.



Mandanten synchronisieren

Ist der Schalter aktiviert, werden mit der Funktion **Business Groups aktualisieren** auch die Mandanten synchronisiert.

Display ID synchronisieren

Schalter zum Aktivieren der Display ID-Synchronisation.

Switche

Switch

Name des administrierten Switches. Die Eingabe eines Namens ist optional; bei **Business Groups aktualisieren** wird der Switchname vom OpenScape Voice Assistant ausgelesen. Der Switchname muss dem im OpenScape Voice Assistant entsprechen, wobei auf Groß-/Kleinschreibung zu achten ist.

SIP Server Adr.:

IP-Adresse oder Hostname des SIP-Servers. Dieser Wert wird nicht von OpenScape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Server Port:

Portnummer des SIP-Servers. Dieser Wert wird nicht von OpenScape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Registrar Adr:

IP-Adresse oder Hostname des SIP-Registrars. Dieser Wert wird nicht von OpenScape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Registrar Port:

Portnummer des SIP-Registrars. Dieser Wert wird nicht von OpenScape Voice geliefert, sondern muss eigens konfiguriert werden.

Business Groups

Name

Name der Business Group.

Aktiviert

Nur aktivierte Business Groups werden synchronisiert.

Business Groups aktualisieren

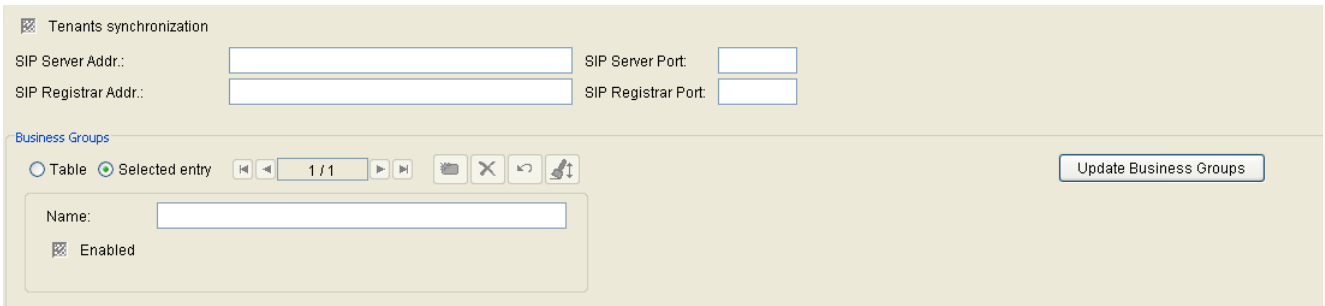
Die Teilnehmer sind in Business Groups unterteilt. Bevor man eine Synchronisation startet, muss man erst die verfügbaren Business Groups ermitteln und dann die entsprechenden Checkboxen aktivieren. Ist die Checkbox **Mandanten synchronisieren** aktiviert, werden hierbei auch die Mandanten synchronisiert. Das Aktualisieren erfolgt im Hintergrund; erst am Ende wird eine Protokolldatei erstellt. Es kann eventuell einige Minuten dauern, bis diese Datei zur Verfügung steht.

HINWEIS: Während die Business Groups aktualisiert werden, kann keine Synchronisation gestartet werden. Wird es dennoch versucht, erscheint eine entsprechende Hinweismeldung.

11.1.3 Register „OpenScape Voice Assistant V3.0“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „OpenScape Voice Assistant V3.0“.

HINWEIS: Diese Konfigurationsmaske gilt für OpenScape Voice Assistant V3.0 und darunter.



Mandanten synchronisieren

Ist der Schalter aktiviert, werden bei der Funktion **Business Groups aktualisiere**n auch die Mandanten synchronisiert.

SIP Server Adr.:

IP-Adresse des SIP-Servers. Dieser Wert wird nicht von der Open Scape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Server Port:

Portnummer des SIP-Servers. Dieser Wert wird nicht von der Open Scape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Registrar Adr:

IP-Adresse des SIP-Registrars. Dieser Wert wird nicht von der Open Scape Voice geliefert, sondern muss eigens konfiguriert werden.

SIP Registrar Port:

Portnummer des SIP-Registrars. Dieser Wert wird nicht von der Open Scape Voice geliefert, sondern muss eigens konfiguriert werden.

Business Groups

Name

Name der Business Group.

Aktiviert

Nur aktivierte Business Groups werden synchronisiert.

Business Groups aktualisieren

Die Teilnehmer sind in Business Groups unterteilt. Bevor man eine Synchronisation startet, muss man erst die verfügbaren Business Groups ermitteln und dann die entsprechenden Checkboxen aktivieren. Ist die Checkbox **Mandanten synchronisieren** aktiviert, werden hierbei auch die Mandanten synchronisiert. Das Aktualisieren erfolgt im Hintergrund; erst am Ende wird eine Protokolldatei erstellt. Es kann eventuell einige Minuten dauern, bis diese Datei zur Verfügung steht.

HINWEIS: Während die Business Groups aktualisiert werden, kann keine Synchronisation gestartet werden.
Wird dies dennoch versucht, erscheint eine entsprechende Hinweismeldung.

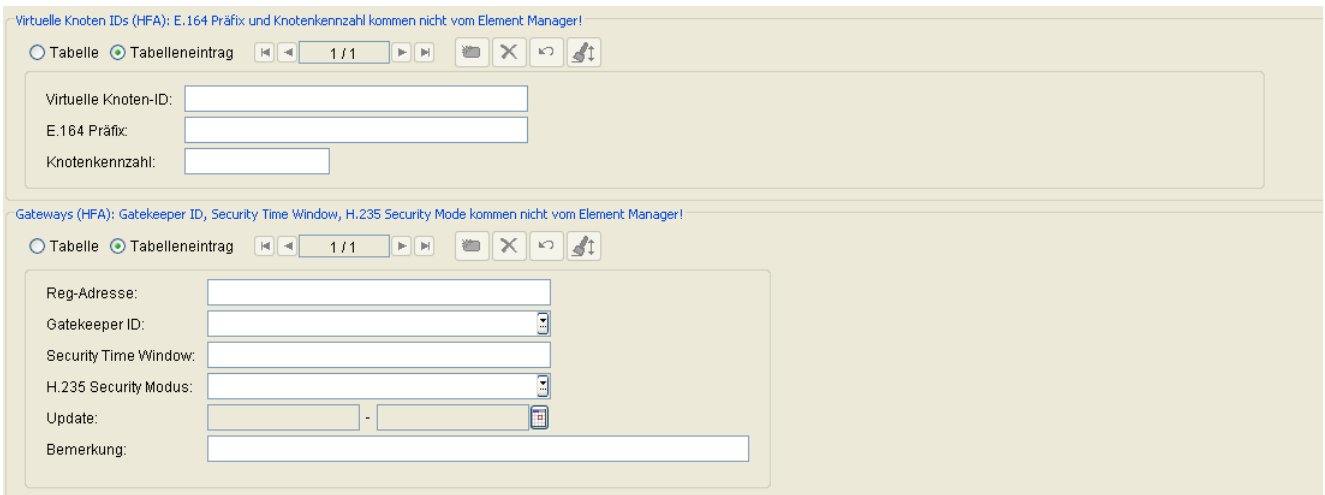
11.1.4 Register „HiPath 4000 Assistant“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „HiPath 4000 Assistant“.

HINWEIS: Die Synchronisation der DLS-Elementmanagerdaten mit denen des HiPath 4000 Assistant (H4K Assistant) ist nur möglich, wenn die Daten innerhalb des H4K Assistant synchronisiert sind. D.h. der Upload-Status im H4K Assistant unter **Configuration Management** > **Netzwerk** > **Anlage** > **Basisdaten** muss SYNCHRONOUS sein. Andernfalls muss zuerst eine Synchronisation der Daten im H4K Assistant mit AMO UPLOA über die H4K Assistant Aktion „Upload“ angestoßen werden.

HINWEIS: Die Einstellungen in diesem Register gelten auch für HiPath 4000 V6.

Weiteres zur Änderung der Konfiguration siehe Abschnitt 15.2, “Änderung der Element Manager-Konfiguration und Joberzeugung”.



Virtuelle Knoten-IDs (HFA) : E.164 Präfix und Knotenkennzahl kommen nicht vom Element Manager!

Virtuelle Knoten-ID

ID des virtuellen Knotens bei Unterteilung einer HiPath 4000 auf mehrere virtuelle Knoten und Nutzung verschiedener Amtszugänge innerhalb der Knoten. Dadurch ist es möglich, durch Kombination aus Rufnummer und Knotennummer den Teilnehmern über alle Knoten hinweg eindeutige E.164-Nummern zuzuweisen. Dieser Wert wird von der HiPath 4000 geliefert.

Ist weder ein Eintrag für **Virtuelle Knoten** noch für **E.164 Präfix** vorhanden, werden keine HFA-Workpoints übernommen. Ist kein Eintrag für **Virtuelle Knoten** vorhanden, jedoch ein Eintrag für **E.164 Präfix**, erhalten alle HFA-Workpoints dieses Präfix.

E.164 Präfix

Präfix der E.164-Nummer. Dieser Wert wird nicht von der HiPath 4000 geliefert, sondern muss konfiguriert werden.

Ist die Tabelle leer oder sind nur **Virtuelle Knoten-ID**s ohne **E.164-Präfix** eingetragen, werden keine Workpoints erzeugt. Ist eine Zeile vorhanden, die nur ein **E.164-Präfix** beinhaltet und keine **Virtuelle Knoten-ID**, erhalten alle HFA-Workpoints dieses Präfix (Default-Präfix). Gibt es aber weitere Einträge, die jeweils eine **Virtuelle Knoten-ID** und ein **E.164-Präfix** einander zuordnen, dann wird jeweils das entsprechende Präfix verwendet. Gibt es Zeilen nur mit **Virtuelle**r **Knoten-ID** ohne zugeordnetes E.164-Präfix, dann wird das Default-Präfix verwendet.

Wird das E.164-Präfix modifiziert und existieren diesbezüglich Workpoint-Einträge, dann werden unmittelbar alle zugehörigen E.164-Nummern angepaßt (die E.164 setzt sich ja aus der Extension und dem E.164-Präfix zusammen). Je nach Anzahl der betroffenen Workpoints kann der Vorgang kann einige Minuten dauern, läuft aber im Hintergrund ab. Während dieser Zeit kann keine Synchronisation durchgeführt werden. Versucht man es dennoch, erscheint eine entsprechende Fehlermeldung.

Knotenkennzahl

Knotenkennzahl für den Rufnummernplan.

Gateways (HFA): Gatekeeper ID, Security Time Window, H.235 Security Mode kommen nicht vom Element Manager!

Reg-Adresse:

Hostname oder des Gateway-Servers. Dieser Wert wird von der HiPath 4000 geliefert.

Gatekeeper ID

Eindeutige Bezeichnung des Gatekeepers. Dieser Wert wird nicht von der HiPath 4000 geliefert, sondern muss eigens konfiguriert werden.

Security Time Window:

Gibt den höchstzulässigen Zeitunterschied zwischen den einzelnen Geräten an, die bei H.235 synchron laufen sollten. Dieser Wert wird nicht von der HiPath 4000 geliefert, sondern muss eigens konfiguriert werden.

H.235 Security Modus:

Einstellung der Sprachverschlüsselung. Dieser Wert wird nicht von der HiPath 4000 geliefert, sondern muss eigens konfiguriert werden.

Mögliche Optionen:

- **Keine**
  Ohne Sprachverschlüsselung.
- **Vermindert**
  Mit einseitiger Sprachverschlüsselung (Gatekeeper sendet nicht verschlüsselt).
- **Voll**
  Mit beidseitiger Sprachverschlüsselung (Workpoint und Gatekeeper senden verschlüsselt).

Update

Zeitpunkt der letzten Aktualisierung der PBX bzw. des Gateway-Servers.

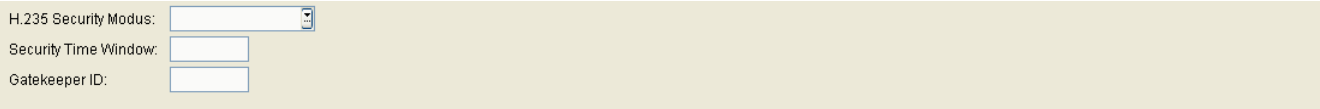
Bemerkung

Feld für allgemeine Informationen.

11.1.5 Register „HiPath 3000/5000“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „HiPath 3000/5000“.

Weiteres zur Änderung der Konfiguration siehe Abschnitt 15.2, “Änderung der Element Manager-Konfiguration und Joberzeugung”.



H.235 Security Modus:

Einstellung der Sprachverschlüsselung. Dieser Wert wird nicht von der HiPath 3000/5000 geliefert, sondern muss eigens konfiguriert werden.

Mögliche Optionen:

- **Keine**
  Ohne Sprachverschlüsselung.
- **Vermindert**
  Mit einseitiger Sprachverschlüsselung (Gatekeeper sendet nicht verschlüsselt).
- **Voll**
  Mit beidseitiger Sprachverschlüsselung (Workpoint und Gatekeeper senden verschlüsselt).

Security Time Window:

Gibt den höchstzulässigen Zeitunterschied zwischen den einzelnen Geräten an, die bei H.235 alle synchron laufen sollten. Dieser Wert wird nicht von der HiPath 3000/5000 geliefert, sondern muss eigens konfiguriert werden.

Gatekeeper ID:

ID des Gatekeepers. Dieser Wert wird nicht von der HiPath 3000/5000 geliefert, sondern muss eigens konfiguriert werden.

11.1.6 Register „OpenScape Office MX/LX“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „OpenScape Office MX/LX“.

Für OpenScape Office MX/LX werden keine zusätzlichen Daten benötigt.

11.1.7 Register „OpenOffice EE“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „OpenOffice EE“.

Für OpenOffice EE werden keine zusätzlichen Daten benötigt

Für OpenOffice EE werden keine zusätzlichen Daten benötigt.

11.1.8 Register „HiPath DXWeb Pro“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „HiPath DXWeb Pro“.

Für HiPath DXWeb Pro werden keine zusätzlichen Daten benötigt

Für HiPath DXWebPro werden keine zusätzlichen Angaben benötigt.

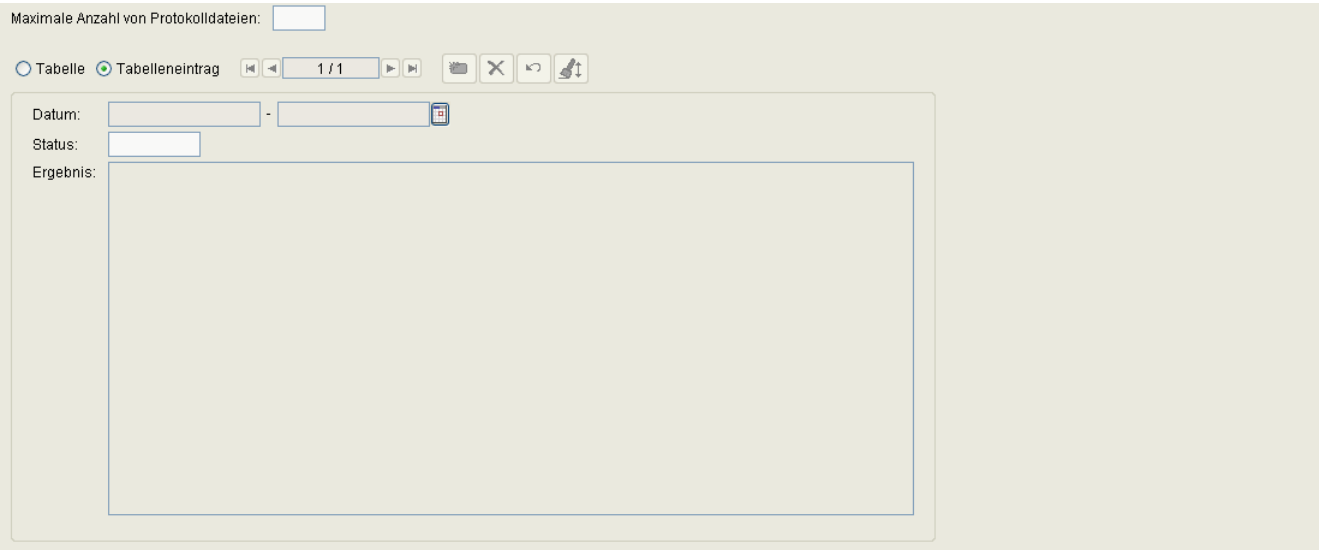
Schnittstellenbeschreibung

Die Daten (Reg-Adresse, Teilnehmerrufnummer, Teilnehmer-Passwort, E.164 Präfix) der HiPath DXWeb Pro werden mittels einer Datenbank-Tabelle an den DLS übergeben. Zuerst wird geprüft, ob eine Tabelle namens „dls“ in einer ACCESS-DB namens „HiPathDX“ (JDBC-URL=jdbc:odbc:HiPathDX) auf dem PC existiert, auf dem der DLS installiert ist. Wenn nicht, dann werden die Daten in der DLS-internen DB (Tabelle „dls“) erwartet. Aus Kompatibilitätsgründen gibt es diese beiden Möglichkeiten bzw. Tabellen. Neuere Versionen der HiPath DXWeb Pro verwenden die ACCESS-Datenbank. Wenn der DLS feststellt, dass die ACCESS-Datenbank/ Tabelle verwendet wird, wird die Tabelle „dls“ in der DLS-internen DB gelöscht, und es ist nicht mehr möglich, mit älteren HiPath DXWebPro Versionen zu arbeiten.

Wenn das E.164-Präfix nicht von der DX geliefert wird, wird der Parameter **E.164-Präfix (HFA)** aus der DLS-Maske verwendet. Das E.164-Präfix und die Teilnehmerrufnummer ergeben zusammen die vollständige E164-Nummer.

11.1.9 Register „Protokoll“

Aufruf: Hauptmenü > Element Manager > Element Manager Konfiguration > Register „Protokoll“



Maximale Anzahl von Protokollen

Maximale Anzahl von Protokollen.

Wertebereich: 1 - 20.

Datum

Zeitpunkt der Synchronisation mit dem durch die Spalte **Element Manager ID** identifizierten Element Manager.

Status

Status der Identifizierung. Folgende Werte sind möglich:

- **OK**
- **Nicht OK**
- **Abgebrochen**
- **OK (teilweise fehlgeschlagen)**

Ergebnis

Inhalt der Protokolldatei.

Mögliche Aktionsschaltflächen

Logfile

Über diesen Button lässt sich die Protokolldatei ansehen.

HINWEIS: Wenn auf dem Register „Protokoll“ kein Inhalt angezeigt wird, sollten Sie den IE-Cache löschen.
Gehen Sie hierzu folgendermaßen vor:

1. Gehen Sie im Windows-Startmenü zu **Start** > **Einstellungen** > **Systemsteuerung**.
2. Doppelklicken Sie auf **Internetoptionen**.
3. Klicken Sie auf das Register **Allgemein**.
4. Klicken Sie auf die Schaltfläche **Löschen** im Bereich **Browserverlauf**.
5. Klicken Sie im Dialog **Browserverlauf löschen** auf die Schaltfläche **Löschen**, nachdem Sie sichergestellt haben, dass nur die Optionen **Temporäre Internetdateien** und **Cookies** ausgewählt sind.
6. Klicken Sie auf **OK** und anschließend auf **Schließen**.
7. Starten Sie Ihren Browser neu.

12 Profil Management

Aufruf: Hauptmenü > Profil Management

Dieses Menü besteht aus folgenden Untermenüs:

- Geräteprofil
- User Data Profile
- Template Übersicht

12.1 Geräteprofil

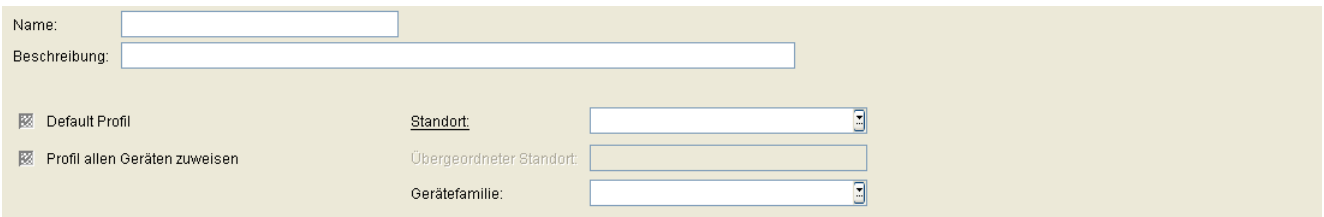
Aufruf: Hauptmenü > Profil Management > Geräteprofil

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Templates“
- Register „Unterstützte Geräte“
- Register „Mandanten“
- Register „Profile des übergeordneten Standortes“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht Suche, um eine bestimmte Gruppe von Profilen zu finden, sowie der Eingabe von Parametern, die für alle Register gelten. In der Ansicht Objekt werden hier die Basis-Daten der gefundenen Profile angezeigt.



Name:

Name des Profils.

Beschreibung:

Kurze Beschreibung des Profils.

Default Profil

Ist der Schalter aktiviert, wird das Profil auch auf IP Devices angewendet, die dieses Profil in **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „Profil“** > **Feld** „Geräteprofil“ nicht eingetragen haben. Bedingung für die Anwendung des Profils ist, dass Standort und Gerätetyp bei Profil und IP Device übereinstimmen - es sei denn, der Schalter „**Profil allen Geräten zuweisen**“ ist aktiviert. Das Profil wird außerdem angewendet bei der Registrierung eines IP Device, das den Schalter **Default Profile anwenden bei IP Device Registrierung** gesetzt hat (**IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „Allgemeines“**).

Um Einstellungen für alle Standorte zu konfigurieren, erstellen Sie Profile, die Sie dem Standort **Default Location** zuordnen. Diese Profile werden dann auf alle IP Devices mit entsprechendem Gerätetyp angewendet bzw. auf alle IP Devices, wenn der Schalter **Profil allen Geräten zuweisen** aktiviert ist. Weitere, standortspezifische Einstellungen können Sie vornehmen, indem Sie Profile für die speziellen Standorte erstellen. Diese Profile überschreiben dann ggf. die Einstellungen derjenigen Profile, die dem Standort **Default Location** zugeordnet sind.

Soll Location Service IP-Infrastruktur genutzt werden, muss ein Default-Profil definiert und dem zugehörigen Standort zugewiesen werden.

Profil allen Geräten zuweisen

Ist der Schalter aktiviert, wird der aktuelle Standard auch den Geräten zugewiesen, die nicht in der Liste **Unterstützte Geräte** eingetragen sind.

Standort

Standort, für den das ausgewählte Profil als Default-Profil gelten soll.

Übergeordneter Standort

Falls vorhanden, werden auch die Templates der Default Profile des übergeordneten Standorts angezeigt.

Gerätefamilie:

Das Profil ist gültig für die Gerätefamilie, die hier angegeben ist.

Mögliche Optionen:

- **IP Phone**
- **IP Client**
- **IP Gateway**

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen Geräteprofilen, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Erstellt ein neues Geräteprofil.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Profil exportieren

Die selektierten Geräteprofile werden in eine Datei im zip-Format exportiert.

Profil importieren

Profile werden aus einer Datei im zip-Format importiert.

12.1.1 Register „Templates“

Aufruf: Hauptmenü > Profil Management > Geräteprofil > Register „Templates“

Legen Sie hier jeweils ein Template fest. Ein weiteres Template können Sie in der Ansicht **Neu** und **Objekt** mit der Schaltfläche hinzufügen und mit löschen.

Template Name

Name des ausgewählten Templates.

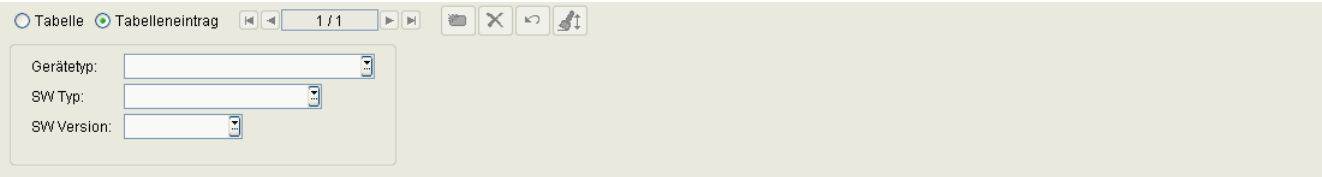
Mehrfach hinzufügen

Es können mehrere Templates zu einem Geräteprofil hinzugefügt werden.

12.1.2 Register „Unterstützte Geräte“

Aufruf: Hauptmenü > Profil Management > Geräteprofil > Register „Unterstützte Geräte“

Legen Sie hier jeweils fest, welche Workpoints vom aktuellen Profil unterstützt werden sollen. Ein weiteres Gerät können Sie in der Ansicht **Neu** und **Objekt** mit der Schaltfläche hinzufügen und mit löschen.



Gerätetyp

Gerätetyp des IP Devices.
Alle vom DLS unterstützte IP Devices finden Sie im Abschnitt 3.4, “Einsatzgebiet”.

Beispiele: **optiPoint 410 standard**, **optiClient 130**.

SW Typ:

Software-Typ für das Gerät.

Beispiele: **Unify HFA**, **Unify SIP**.

SW Version

Beispiel **für optiPoint und optiClient:** 5.0.12.

12.1.3 Register „Mandanten“

Aufruf: Hauptmenü > Profil Management > Geräteprofil > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.

Mandant

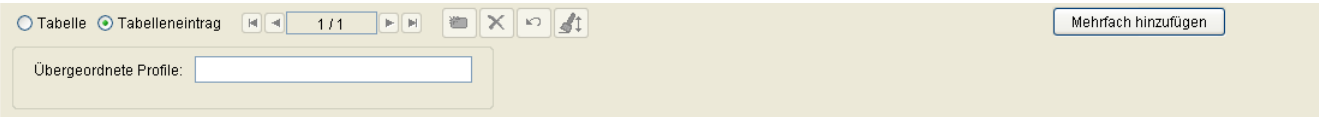
Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

12.1.4 Register „Profile des übergeordneten Standortes“

Aufruf: Hauptmenü > Profil Management > Geräteprofil > Register „Profile des übergeordneten Standortes“



Übergeordnete Profile

Profile des übergeordneten Standorts.

Mehrfach hinzufügen

Mehrere Templates zu einem Profil hinzufügen.

12.2 User Data Profile

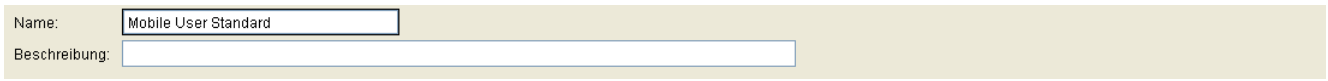
Aufruf: Hauptmenü > Profil Management > User Data Profile

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Templates“
- Register „Mandanten“

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht Suche, um eine bestimmte Gruppe von Profilen zu finden, sowie der Eingabe einer Beschreibung. In der Ansicht Objekt werden hier die Basis-Daten der gefundenen Profile angezeigt.



Name:

Name des Profils. Die angelegten Profile können entweder als Mobile User Profil bei **Mobile User** > **SIP Mobile User Interaktion** > **SIP Mobile User** > **Register „Mobile / Basis User“** oder als Basis Profil bei **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „Profil“** verwendet werden.

Beschreibung:

Kurze Beschreibung des Profils.

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen User Data-Profilen, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Neu

Neue User Data-Profile werden angelegt.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Profil exportieren

Selektierte Profile werden in eine Datei im zip-Format exportiert.

Profil importieren

Profile werden aus einer Datei im zip-Format importiert.

12.2.1 Register „Templates“

Aufruf: Hauptmenü > Profil Management > User Data Profile > Register „Templates“

Legen Sie hier ein oder mehrere Templates für das User Data Profil fest. Ein weiteres Template können Sie in der Ansicht **Neu** und **Objekt** mit der Schaltfläche hinzufügen und mit löschen.

Template Name

Name des Templates.

Mehrfach hinzufügen

Es können mehrere Templates zu einem User Data Profil hinzugefügt werden.

12.2.2 Register „Mandanten“

Aufruf: Hauptmenü > Profil Management > User Data Profile > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.

Mandant

Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

12.3 Template Übersicht

Aufruf: Hauptmenü > Profil Management > Template Übersicht

Nutzen Sie diesen Bereich, um

- existierende Templates zu suchen,
- den Namen und die Beschreibung von Templates zu ändern,
- Templates zu löschen und
- alle Templates im XML-Format in eine .zip-Datei zu exportieren oder aus einer .zip-Datei zu importieren. Es können auch einzelne Templates aus der .zip-Datei importiert werden.

Änderungen der Attribute und Attributwerte von Templates sind hier nicht möglich. Siehe hierzu Abschnitt 15.4, “Templates bearbeiten”.

WICHTIG: Werden Datenänderungen in Konfigurationsmasken vorgenommen, die mithilfe von Templates erstellt wurden, so werden diese Änderungen nicht automatisch in diese Templates übernommen.
Zum Übernehmen müssen die Änderungen manuell im Template gesichert werden, siehe Abschnitt 15.4, “Templates bearbeiten”.

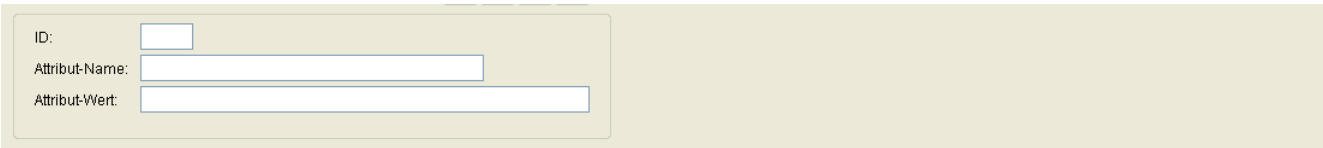
Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Template-Daten“
- Register „Profile“
- Register „Mandanten“

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von Templates zu finden, sowie zum Import und Export von Template-Daten. In der Ansicht **Objekt** werden hier die Basis-Daten der gefundenen Templates angezeigt (keine Änderungsmöglichkeit).



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

Name:

Name des Templates.

Beschreibung:

Beschreibung zum Template.

Objekt:

Objekt-Typ des Templates.

Beispiel: **IP Phone SNMP Einstellungen**

Typ:

Gibt den Typ von Parametern an, der im Template gespeichert ist.

Mögliche Einträge:

- **IP Client**
- **IP Phone**
- **User Daten**

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen Templates, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Sichert bislang ungesicherte Änderungen.

Verwerfen

Verwirft bislang ungesicherte Änderungen.

Löschen

Löscht einen oder mehrere Templates (Mehrfachauswahl in Tabellenansicht möglich).

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

Templates importieren

Importiert Templates im XML-Format aus einer .zip-Datei. Es können auch einzelne Templates aus der .zip-Datei importiert werden. die Auswahl erfolgt in einem Popup-Fenster.

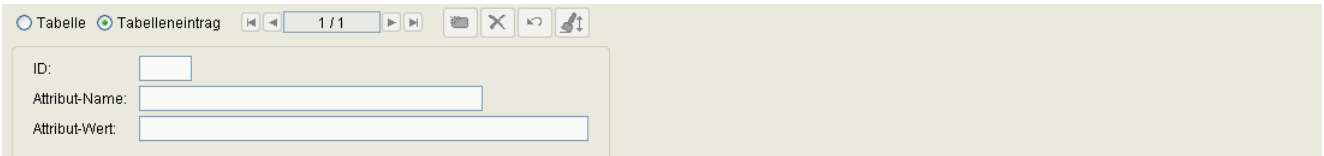
HINWEIS: Beim Import werden bestehende Templates mit gleichem Namen überschrieben.

Templates exportieren

Exportiert die selektierten Templates im XML-Format in eine .zip-Datei. Die Mehrfachselektion von Templates ist in der Tabellenansicht möglich. Der Dateipfad wird in einem Popup-Fenster abgefragt.

12.3.1 Register „Template-Daten“

Aufruf: Hauptmenü > Profil Management > Template Übersicht > Register „Template-Daten“



ID

ID zur besseren Sortiermöglichkeit (z. B. bei Tastenbelegungen).

Attribut-Name

Name des im Template definierten Attributes.

Attribut-Wert

Wert des entsprechenden Attribut-Namens.

12.3.2 Register „Profile“

Aufruf: Hauptmenü > Profil Management > Template Übersicht > Register „Profile“

Geräteprofile

Profil

Name des Geräteprofils.

Beschreibung

Beschreibung des Geräteprofils.

Standort

Standort des Geräteprofils.

User Data Profile

Profil

Name des User Data Profils.

Beschreibung

Beschreibung des User Data Profils

12.3.3 Register „Mandanten“

Aufruf: Hauptmenü > Profil Management > Template Übersicht > Register „Mandanten“

HINWEIS: Dieses Register steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Siehe auch Abschnitt 16.16.1, “Mandantenfähigkeit installieren /deinstallieren”.

Mandant

Name des Mandanten.

Bemerkung

Bemerkung zum Mandanten.

13 XML Applikationen

Aufruf: Hauptmenü > XML Applikationen

Der DLS kann nicht nur zum Installieren von XML Applikationen, sondern auch selbst als Applikations-Server verwendet werden.

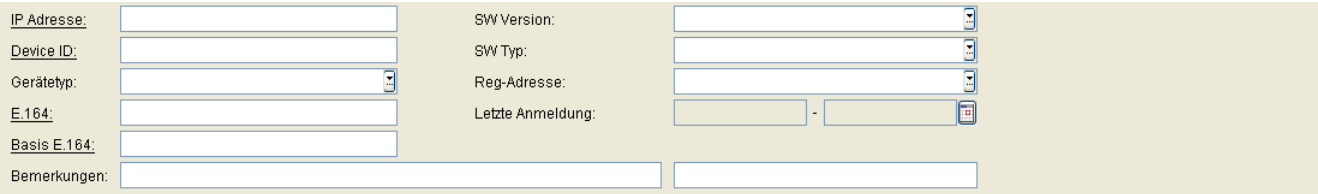
HINWEIS: XML Applikationen stehen nur für OpenStage 60 und OpenStage 80 mit den Firmware-Versionen SIP V1, SIP V2 und HFA V2 zur Verfügung.

Dieser Menüpunkt besteht aus den folgenden Bereichen:

- MakeCall
- NewsService
- NewsService Archiv

Allgemeine Daten

Dieser Teil des Inhaltsbereiches ist für die Applikationen **MakeCall** und **NewsService** identisch. Er dient der Eingabe von Parametern in der Ansicht **Suche**, um eine bestimmte Gruppe von IP Phones für die Konfiguration und Ausführung von XML-Applikationen zu finden. Ist die Ansicht **Objekt** ausgewählt, so werden hier die Basis-Daten der gefundenen IP Phones angezeigt.



IP Adresse:

IP-Adresse des IP Phones. Für OpenStage wird hier entweder eine IPv4- oder eine IPv6-Adresse angezeigt.

Beispiel: **192.117.1.193**

Wurde der Wert per DHCP dynamisch vergeben, kann er nur gelesen werden.

Device ID:

ID zur eindeutigen Identifizierung des IP Phones. In der Regel ist das die MAC-Adresse.

Beispiel: **00:0E:A6:85:71:80**

Gerätetyp:

Gerätetyp des IP Phones. Das Icon zeigt an, ob es sich um einen virtuelles Gerät handelt.

Alle vom DLS unterstützten IP Phone-Typen finden Sie im Abschnitt 3.4, “Unterstützte IP Devices/Versionen”.

Beispiel: **OpenStage 60**

E.164:

Vollständige E.164-Rufnummer (Basic Profile oder Mobile Profile).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

Basis E.164:

Vollständige E.164-Rufnummer (Mobility Phone).

Beispiel: **498972212345**

Informationen zur Bedeutung der E.164-Rufnummer bzgl. Mobility siehe Abschnitt 3.8.3, “Mobility ID”.

SW Version:

Software-Version des IP Phones.

Beispiel: **5.0.12**

Informationen zum Unterschied zwischen Software- und Lizenz-Version finden Sie im Abschnitt 15.6, “Verteilen von Workpoint-Software”.

SW Typ:

Software-Typ des IP Phones.

Beispiele: **Unify HFA**, **Unify SIP**

Reg-Adresse

IP-Adresse oder DNS-Name des SIP- oder HFA-Servers, bei dem das Gerät angemeldet ist.

Letzte Anmeldung:

Zeitpunkt der letzten Anmeldung des IP Phones.

Zur Auswahl eines Zeitbereichs bei der Suche siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”.

Bemerkungen:

Felder für allgemeine Informationen.

13.1 MakeCall

Aufruf: Hauptmenü > XML Applikationen > MakeCall

Diese Maske ermöglicht den Start (=Push) der XML Applikation „MakeCall“. Es werden dabei Anrufe von ausgewählten Endgeräten zu einem Zielendgerät initiiert. In der Anruf-Liste des Zielendgerätes kann dann überprüft werden, ob alle Rufe durchgeführt wurden. Diese Überprüfung ist sinvoll z. B. nach einem Software-Update. Die Applikation kann nur von DLS gestartet werden und nicht von Endgeräten.

Zum Starten der Funktion drücken Sie die Aktionsschaltfläche **MakeCall**. In einem Dialogfenster wird dann die Zielrufnummer abgefragt.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

Mögliche Aktionsschaltflächen

Abhängig von der gewählten Ansicht, der gewählten XML-Applikation und vom DLS-Status sind unterschiedliche Aktionsschaltflächen verfügbar.

Suchen

Sucht nach allen registrierten IP Devices, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

MakeCall

Starten der XML Applikation ‘MakeCall’. In einem nachfolgenden Dialogfenster wird die **Zielrufnummer** abgefragt.

Hinweis senden

Starten der XML Applikation ‘NewsService’ zum Versenden eines Textes. In einem nachfolgenden Dialogfenster werden die **Überschrift** und der **Text** des Hinweises abgefragt.

Text-/Bilddatei senden

Starten der XML Applikation ‘NewsService’ zum Versenden einer Text- oder Bilddatei. In einem nachfolgenden Dialogfenster wird der **Dateiname** abgefragt.

Löschen

Löscht gespeicherte Nachrichten.

Aktualisieren

Aktualisiert den Inhalt der Maske aus der Datenbank.

13.1.1 Register „Info“

Aufruf: Hauptmenü > XML Applikationen > MakeCall > Register „Info“

MakeCall Zielrufnummer:

Anzeige der Zielrufnummer des letzten automatischen Anrufs, den die XML Applikation ‘MakeCall’ dorthin initiiert hat.

13.2 NewsService

Aufruf: Hauptmenü > XML Applikationen > NewsService

Diese Maske ermöglicht den Start (=Push) der XML Applikation „NewsService“. Es werden dabei Nachrichten zu ausgewählten Endgeräten gesandt. Bei den Nachrichten kann es sich um Hinweise oder um Text- oder Bilddateien handeln. Es wird dabei zwischen Hinweis und Datei unterschieden. Ein Hinweis wird mit dem Symbol ‘INFO’ am Endgerät angezeigt und muss dort durch Knopfdruck bestätigt werden. Bei einer Text- oder Bilddatei wird die Nachricht am Endgerät im Applikationsregister ’News Service’ angezeigt.

Das Erstellen und Versenden wird von DLS gestartet. Am Endgerät können gespeicherte Nachrichten erneut gelesen werden. Zum Starten drücken Sie **Hinweis senden** oder T**ext-/Bilddatei senden**. In einem Dialogfenster wird dann die **Überschrift** und der **Text** oder der **Name der Text-/Bilddatei** abgefragt.

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“

13.2.1 Register „Info“

Aufruf: Hauptmenü > XML Applikationen > NewsService > Register „Info“

Hinweisüberschrift

Überschrift des letzten Hinweises, der mittels der XML Applikation ‘NewsService’ an ein Endgerät geschickt wurde.

Hinweistext

Text des letzten Hinweises, der mittels der XML Applikation ‘NewsService’ an ein Endgerät geschickt wurde.

Text-/Bilddatei

Dateiname der letzten Text- (.txt) oder Bilddatei (.jpg, .bmp, .gif, .png), die mittels der XML Applikation ‘NewsService’ an ein Endgerät geschickt wurde.

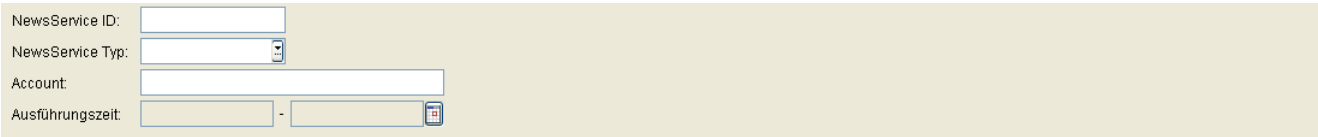
13.3 NewsService Archiv

Aufruf: Hauptmenü > XML Applikationen > NewsService Archiv

Dieser Bereich besteht aus folgenden Inhalten:

- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Info“
- Register „IP Devices“

Allgemeine Daten



NewsService ID

Fortlaufende Nummerierung.

NewsService Typ

Art der Nachrichten.

Mögliche Werte:

- **Hinweis**
- **Bilddatei**
- **Textdatei**

Account

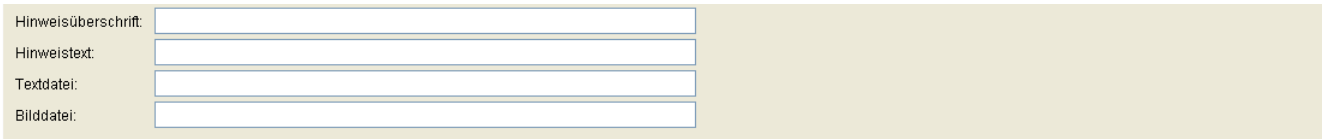
Account des Auftraggebers der Nachricht.

Ausführungszeit

Ausführungszeit des Jobs zum Nachrichtenversand.

13.3.1 Register „Info“

Aufruf: Hauptmenü > XML Applikationen > NewsService Archiv > Register „Info“



Hinweisüberschrift

Überschrift des Hinweises, der an die Endgeräte gesendet wurde.

Hinweistext

Text des Hinweises, der an die Endgeräte gesendet wurde.

Textdatei

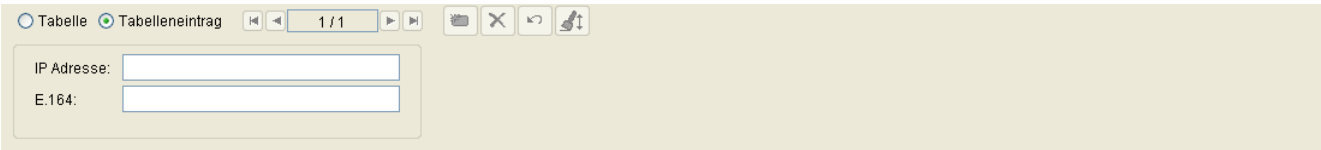
Name der Textdatei, die an die Endgeräte gesendet wurde.

Bilddatei

Name der Bilddatei, die an die Endgeräte gesendet wurde.

13.3.2 Register „IP Devices“

Aufruf: Hauptmenü > XML Applikationen > NewsService Archiv > Register „IP Devices“



IP Adresse

IP Adresse des Endgerätes, an das die Nachricht geschickt wurde.

E.164

Vollständige E.164-Rufnummer des Endgerätes, an das die Nachricht geschickt wurde.

14 Job Koordination

Aufruf: Hauptmenü > Job Koordination

Dieses Menü besteht aus folgenden Untermenüs:

- Job Kontrolle
- Täglicher Status
- Job Konfiguration

Um komplexere Deployment-Aufgaben durchzuführen, nutzen Sie den Bereich **Job Koordination**. Er dient der Konfiguration, Durchführung und Protokollierung von Deployment-Jobs (siehe auch den Bedienablauf in Abschnitt 15.7).

14.1 Job Kontrolle

Aufruf: Hauptmenü > Job Koordination > Job Kontrolle

Dieser Bereich besteht aus folgenden Inhalten:

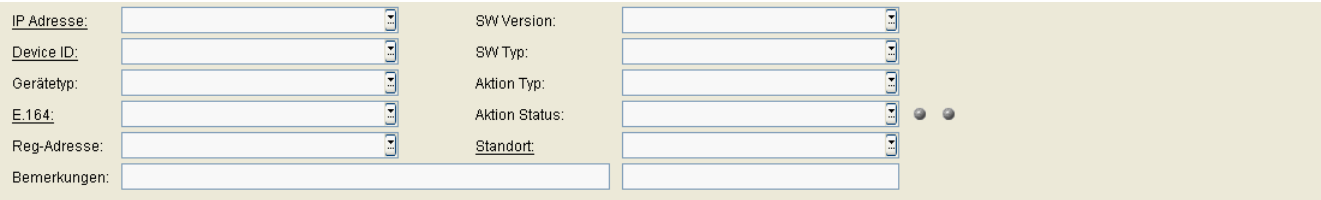
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Basis Daten“
- Register „Deployment Daten“
- Register „Konfiguration Daten“
- Register „XML Applikationen Daten“

Mittels dieser Funktion können Sie umfangreiche Informationen zu den einzelnen Jobs ansehen, vorhandene Jobs abbrechen, löschen oder erneut aktivieren. Das Anlegen neuer Jobs geschieht nicht hier, sondern durch das Festlegen der im Job zu erledigenden Tätigkeiten (Beispiel siehe Abschnitt 15.7, “Nutzen der Job-Koordination”).

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht Suche, um eine bestimmte Gruppe von Jobs zu finden. In der Ansicht Objekt werden hier die Basis-Daten der gefundenen Jobs angezeig.



HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

IP Adresse:

IP-Adresse eines IP Devices oder ein Adressbereich.

Bei Jobs für IP-Bereiche wird in der Ansicht **Suche** hier **000.000.000.000** angezeigt.

Format: **000.000.000.000**, 000 = Wert zwischen 000 und 255.

Device ID:

Device ID eines IP Devices oder ein Adressbereich.

Bei Jobs für Device ID-Bereiche wird in der Ansicht **Suche** hier **00:00:00:00:00:00** angezeigt.

Format: XX:XX:XX:XX:XX:XX, XX = Hex-Wert zwischen 00 und FF.

Gerätetyp:

Gerätetyp des IP Devices.

Bei Jobs für verschiedene Gerätetypen wird in der Ansicht **Suche** hier nichts angezeigt.

Format: max. 30 Zeichen.

Alle vom DLS unterstützte IP Devices finden Sie im Abschnitt 3.4, “Unterstützte IP Devices/Versionen”.

Beispiel: **optiPoint 410 standard**, **optiClient 130**

E.164:

Vollständige Rufnummer eines IP Devices.

Bei Jobs für verschiedene Rufnummern wird in der Ansicht **Suche** hier nichts angezeigt.

Job Koordination
Job Kontrolle

Format: max. 15 Zeichen.

Siehe auch Abschnitt 17.1, “E.164”.

Reg-Adresse

IP-Adresse oder Hostname des Registrar-Servers, an dem das IP Device registriert ist.

SW Version:

Software-Version eines IP Devices.

Bei Jobs für verschiedene Versionsnummern wird in der Ansicht **Suche** hier nichts angezeigt.

Beispiel für optiPoint und optiClient: **5.0.12**.

SW Typ:

Typ der Software, die heruntergeladen wird.

Bei Jobs für verschiedene Software-Typen wird in der Ansicht **Suche** nichts angezeigt.

Beispiele: **Unify HFA**, **Unify SIP**.

Aktion Typ:

Mögliche Optionen:

- **IP Device Konfiguration**
- **IP Device Notifizierung**
- **Mobile User Konfiguration**
- **Mobile User Migration**
- **Software Deployment**
- **Wartemusik Datei Deployment**
- **LDAP Template Datei Deployment**
- **INCA Firmware Deployment**
- **Java Midlet Deployment**
- **Logo Datei Deployment**
- **Applikation und Systemton Deployment**

- **System und Rufton Deployment**
- **APM Firmware Deployment**
- **Netboot Deployment**
- **IP Device Notifizierung**
- **Bildschirmschoner Deployment**
- **File Deployment**
- **IP Devices scannen**
- **IP Device Daten lesen**
- **IP Device Daten lesen**
- **IP Device zurücksetzen**
- **Werkseinstellung wiederherstellen**
- **Gateway Konfiguration**
- **Gateway Daten lesen**
- **Gateway Probe**
- **Logon Mobile User**
- **Logoff Mobile User**
- **Push XML Applikation**
- **File Upload**

Aktion Status:

Mögliche Aktionsstatus:

- **Zeit überschritten**
  Bei der Ausführung des Deployment-Jobs gab es eine Zeitüberschreitung, weil die bei **Job Konfiguration** eingetragene Zeit z. B. durch ein längerfristig nicht bereites IP Device überschritten wurde. Der Job kann abgebrochen und gelöscht werden, wodurch keine Aktion des Jobs mehr ausgeführt wird.
- **abgebrochen**
  Der Deployment-Job wurde abgebrochen. Bei abgebrochenen Jobs kann ausschließlich der Ausführungszeitpunkt geändert werden (um den Job zu einem künftigen Zeitpunkt neu zu starten). Der Job kann gelöscht werden.
- **aktiv**
  Der Deployment-Job wurde in der Job-Tabelle aufgenommen, läuft aber noch nicht, weil z. B. Ausführungszeit noch nicht erreicht wurde. Der Job kann abgebrochen und gelöscht werden, wodurch keine Aktion des Jobs mehr ausgeführt wird.

- **bestätigt**
  Der Deployment-Job wurde vom IP Device angenommen und wartet, bis der Zustand des IP Devices die Bearbeitung zulässt. Der Job kann abgebrochen und gelöscht werden, wodurch die weitere Ausführung des Jobs jedoch nicht unterbrochen wird.
- **fehlgeschlagen**
  Der Deployment-Job wurde gestartet, konnte jedoch nicht ausgeführt werden. Der Job kann abgebrochen und gelöscht werden.
- **fertig**
  Der Deployment-Job wurde korrekt ausgeführt. Der Job kann abgebrochen und gelöscht werden.
- **läuft**
  Der Deployment-Job wird gerade ausgeführt. Der Job kann abgebrochen und gelöscht werden, wodurch die weitere Ausführung des Jobs jedoch nicht unterbrochen wird.

Statusanzeige für Jobs

Die Statusanzeige für einen Job kann mit über ein Pop-Up-Menü mit **Reset Status** zurückgesetzt werden (siehe Abschnitt 5.4.1, “Hauptmenü”).

Anzeige Kugel links:
Job läuft nicht.
Job läuft.

Anzeige Kugel rechts:
Job ist fehlerfrei durchgeführt worden.
Job ist fehlerhaft abgebrochen worden.

Standort:

Aktueller Standort des IP Device.

Bemerkungen:

Felder für allgemeine Informationen, Anmerkungen (z. B. Kommentare) zum jeweiligen Job.

Diese Felder sind für alle Job-Typen und Job-Status bearbeitbar.

> ***HINWEIS:*** Bearbeitbare Felder unter Job Kontrolle, die Werte aus einer zuvor durchgeführten Aktion darstellen (z. B. eine Bemerkungsnotiz zu einem Teilnehmer), gelten nur im direkten Zusammenhang mit Job-Parametern als „bearbeitbar“; etwaige Änderungen in diesen Feldern werden nicht auf den ursprünglichen Datensatz zurück übertragen, aus dem der Job erstellt wurde.

Mögliche Aktionsschaltflächen

Suchen

Sucht nach allen Deployment-Jobs, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

Sichern

Sichert Änderungen an einem bestehenden Deployment-Job. Das Sichern ist nur nach einer Änderung bei einem abgebrochenen Job verfügbar.

Verwerfen

Verwirft Änderungen an einem bestehenden Deployment-Job. Das Verwerfen ist nur nach einer Änderung bei einem abgebrochenen Job verfügbar.

Löschen

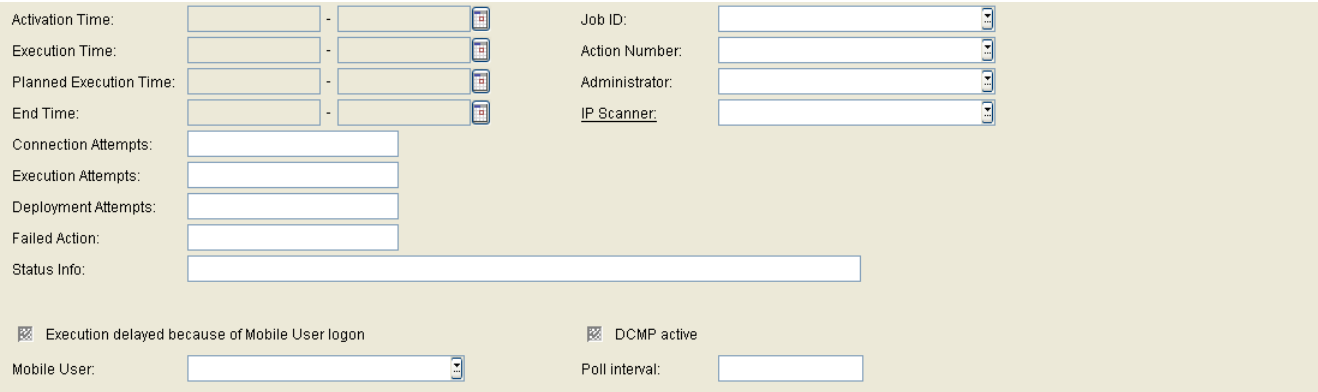
Löscht den Deployment-Job, der in der Ansicht **Objekt** angezeigt wird.

Job abbrechen

Bricht den Deployment-Job ab, der in der Ansicht **Objekt** angezeigt wird.

14.1.1 Register „Basis Daten“

Aufruf: Hauptmenü > Job Koordination > Job Kontrolle > Register „Basis Daten“



Aktivierungszeit:

Zeitbereich bzw. Zeitpunkt für die Aktivierung des Deployment-Jobs (siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

Ausführungszeit:

Zeitbereich bzw. Zeitpunkt für die Ausführung des Deployment-Jobs (siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

> ***HINWEIS:*** Bei abgebrochenen Deployment-Jobs können Sie durch Eingabe eines in der Zukunft liegenden Zeitpunktes diesen Job reaktivieren.
> Bei allen anderen Job-Status wird hier der Zeitpunkt der Ausführung angezeigt; egal, ob in der Vergangenheit oder in der Zukunft liegend.

Geplante Ausführungszeit:

Geplanter Zeitpunkt für die Ausführung des Deployment-Jobs. Die geplante Ausführungszeit bezieht sich auf die Server-Ortszeit.

> ***HINWEIS:*** Daher wird für Jobs, die auf Devices in anderen Zeitzonen ausgeführt werden sollen, hier die Device-Ortszeit +- Zeitverschiebung eingetragen.

Endzeit:

Zeitbereich bzw. Zeitpunkt für die Beendigung des Deployment-Jobs (siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

HINWEIS: Bei bereits ausgeführten Deployment-Jobs wird hier der Zeitpunkt angezeigt, zu dem der Job beendet wurde.

Verbindungsversuche:

Anzahl der Versuche, die zum Durchführen des Jobs benötigt wurden (**0** bedeutet: noch nicht ausgeführt).

Ausführungsversuche:

Anzahl der Ausführungsversuche, die zum Durchführen des Jobs benötigt wurden (**0** bedeutet: noch nicht ausgeführt).

Installationsversuche:

Anzahl der Installationsversuche, die zum Durchführen des Jobs benötigt wurden (**0** bedeutet: noch nicht ausgeführt).

Fehlaktion:

Nummer der Aktion in der Job Tabelle, die nicht erfolgreich beendet werden konnte und dazu geführt hat, dass vom DLS automatisch ein **IP Device Daten lesen** generiert und ausgeführt wurde.

Das Feld enthält nur einen Wert für vom DLS erzeugte Aufträge vom Typ **IP Device Daten lesen**. Als Administrator dieser Aufträge wird **@DLS** angezeigt.

Status Info:

Die Meldungen können sich sowohl auf den erfolgreichen Ablauf eines Deployment-Jobs als auch auf den Fehlerfall beziehen. Folgende Status-Meldungen werden ausgegeben (alphabetisch nach **Status Info** sortiert):

Status Info	Beschreibung	Auslöser
action type not implemented	-	neutral
equal item names	Identische Eintragnamen.	IP Phone
failed	Fehlgeschlagen.	IP Phone
file-not-found	Fehler z. B. beim Öffnen von abgespeicherten Templates oder beim Öffnen des Deployment-Files.	IP Client
ignored - dial plan error	Fehler im Rufnummernplan.	IP Phone
image path not contactable	Entfernter Image-Pfad ist nicht verfügbar.	IP Client

Status Info	Beschreibung	Auslöser
initiated	Der Job wurde angestoßen, jedoch noch nicht zu Ende ausgeführt.	neutral
internal ERROR[1]	-	neutral
invalid data	Ungültige Daten.	IP Phone
invalid format	Ungültiges Format.	IP Phone
invalid function key	Ungültige Funktionstaste.	IP Phone
invalid index	Ungültiger Index.	IP Phone
invalid item name	Ungültiger Eintragname.	IP Phone
local deployment path not specified	Item „dls-deployment-local-path“ ist nicht gesetzt.	IP Client
local deployment path not writable	Lokaler Pfad ist nicht beschreibbar.	IP Client
missing item content	Fehlender Eintraginhalt.	IP Phone
missing item name	Fehlender Eintragname.	IP Phone
nonce not valid	-	neutral
not a feature toggle key	Keine Funktionsumschaltetaste.	IP Phone
not a line key	Keine Leitungstaste.	IP Phone
not a repertory dialing key	Keine Erweiterte Zielwahltaste.	IP Phone
not a selected dialing key	Keine Direktruftaste.	IP Phone
not implemented	Nicht implementiert.	IP Phone
not readable	Nicht lesbar.	IP Phone
not supported	Nicht unterstützt.	IP Phone
OK	Das Deployment ist erfolgreich ausgeführt worden.	neutral
read only	Nur lesbar.	IP Phone
server-not-contactable	Entfernter Server ist nicht verfügbar.	IP Client
Self Labeling Key Sidecar not available	optiPoint Self Labeling Key module ist nicht verfügbar.	IP Phone
unknown item	Unbekannter Eintrag.	IP Phone
not a DSS key	Kein DSS key.	IP Phone

1 Nur für die internes Debugging; für den DLS-Benutzer nicht relevant.

Job ID:

ID des Jobs. Die Job-ID ist der Name, der beim Anlegen des Jobs eingetragen wurde (siehe Abschnitt 5.4.2.1, “Werkzeugleiste”). Wurde kein Name eingetragen, wird für die Job-ID die Aktionsnummer verwendet.

Bei Jobs zur Verteilung und Aktivierung eines PSS (Pre-shared Secret) werden der Job-ID das Merkmal PSS vorangestellt.

Aktionsnummer:

Aktionsnummer des Jobs. Bei jeder Aktion in jedem Deployment-Job wird automatisch diese laufende Nummer generiert (pro bearbeiteter IP-Adresse eine).

Administrator:

Benutzernamen zu diesem Job. Der Name entspricht dem Benutzer, der die Aktion definiert hat. Geben Sie für automatisch generierten Aktionen den Namen **@DLS** ein.

> ***HINWEIS:*** Dieses Feld entspricht dem DLS Account, das eine Aktion ausgeführt hat, für die in der Job-Kontrollliste des DLS ein Job angelegt wurde.

> ***HINWEIS:*** **@DBUpdateVirtualDevices** ist ein Alias für den Administrator-Benutzer, der für Element Manager-bezogene geplante Aufgaben verwendet wird.

IP Scanner:

IP-Scanner zu diesem Job. Der Name wird beim Einrichten eines IP-Scanners festgelegt, siehe Abschnitt 7.4.6, “IP Devices scannen”.

Ausführung verzögert wegen Mobile User Anmeldung

Die Ausführung des Jobs wird wegen eines angemeldeten Mobile Users nicht zu dem bei Ausführungszeit angegebenen Zeitpunkt, sondern dazu verzögert, ausgeführt.

Mobile User:

Aktuell angemeldeter Mobile User.

DCMP aktiv

Ist der Schalter aktiviert, prüft das Gerät in periodischen Abständen beim DCMP (DLS Contact-Me Proxy), ob DLS-Jobs anstehen.

Poll Intervall

Zeitabstand zwischen zwei Abfragen (Polls) des Geräts beim DCMP in Minuten.

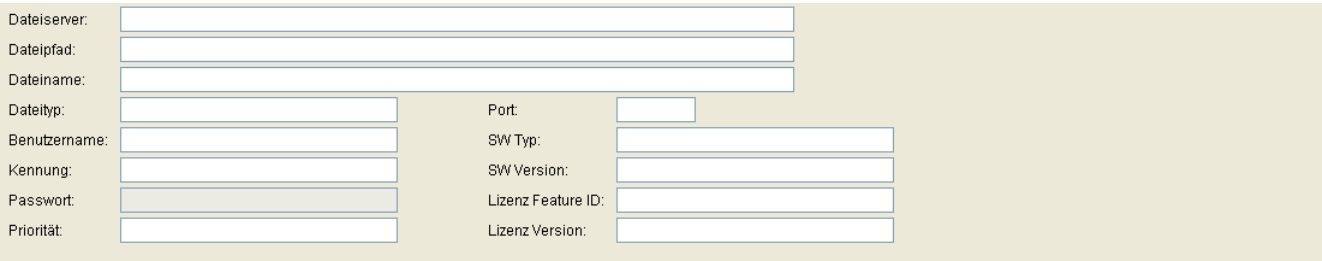
14.1.2 Register „Deployment Daten“

Aufruf: Hauptmenü > Job Koordination > Job Kontrolle > Register „Deployment Daten“

Hier werden bei Jobs der folgenden Aktionstypen die Daten des Software-Deployments angezeigt.

- **INCA Firmware Deployment**
- **Java Midlet Deployment**
- **LDAP Template Datei Deployment**
- **Logo Datei Deployment**
- **System und Rufton Deployment**
- **Software Deployment**
- **Wartemusik Datei Deployment**

Für einen Job können entweder Daten im Register „Deployment Daten“ oder im Register „Konfiguration Daten“ vorhanden sein.



Dateiserver:

IP-Adresse oder Hostname des FTP Servers (für IP Phones) oder Netzwerkrechners (für IP Clients), von dem die Software heruntergeladen wird.

Dateipfad:

Verzeichnis am FTP-Server (für IP Phones) oder am Netzwerkrechner (für IP Clients), von dem die Software heruntergeladen wird. Bei IP Phone-Software beginnt der Pfad ab dem eingerichteten „virtuellen“ Wurzelverzeichnis, bei IP Client-Software ab dem freigegebenen Netzwerkpfad.

Dateiname:

Dateiname der Software, die heruntergeladen wird.

Job Koordination
Job Kontrolle

Dateityp:

Deploymenttyp der Datei, die heruntergeladen wird.

Beispiele:
INCA (INCA Firmware Deployment)
MIDLET (Java Midlet Deployment)
LDAP (LDAP Template Datei Deployment)
LOGO (Logo Datei Deployment)
RINGTONE (System und Rufton Deployment)
APP (Software Deployment)
MOH (Wartemusik Datei Deployment)

Benutzername:

Benutzername („Login“) des FTP-Zugangs zum Server, von dem die Software heruntergeladen wird.

Kennung:

Wird zur Zeit im DLS nicht verwendet.

Passwort:

Passwort des FTP-Zugangs zum Server, von dem die Software heruntergeladen wird.

Priorität:

Signalisiert, ob mit dem Deployment bei einem belegtem IP Device abgewartet wird, bis dieses wieder frei ist (**normal)**, oder ob das Deployment zu dem Zeitpunkt unabhängig vom Status des IP Devices durchgeführt wird (**hoch**).

Port:

Verwendeter Port des FTP-Servers, von dem die Software heruntergeladen wird. Ist fest auf Port 21 eingestellt.

SW Typ:

Softwaretyp der Software, die heruntergeladen wird (für Software-Deployment).

Beispiele: **Unify HFA**, **Unify SIP**.

SW Version:

Softwareversion des IP Devices.

Beispiel für **optiPoint:** 5.0.12.

Lizenz Feature ID:

Ist die heruntergeladene Software lizenzpflichtig, so steht hier die Produkt-ID (HLM-Terminologie) mit der die Software im HiPath License Management registriert ist (für Software-Deployment).

Beispiel für optiPoint 410 standard HFA: **OPTI410STDHFA**.

Lizenz Version:

Ist die heruntergeladene Software lizenzpflichtig, so steht hier die Produkt-Version (HLM-Terminologie), mit der die Software im HiPath License Management registriert ist (für Software-Deployment).

Beispiel nur für optiPoint: **6.0.0**

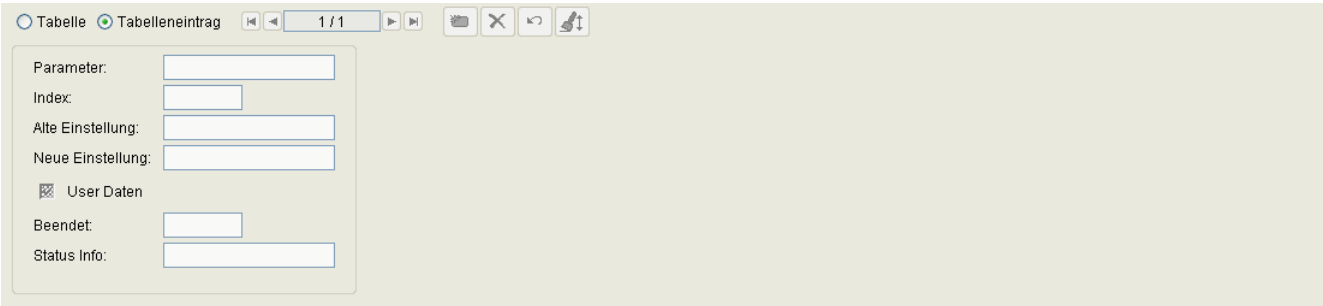
14.1.3 Register „Konfiguration Daten“

Aufruf: Hauptmenü > Job Koordination > Job Kontrolle > Register „Konfiguration Daten“

Hier werden bei Jobs des Aktionstyps **IP Device Konfiguration** die Konfigurationsdaten des Jobs angezeigt.

Alle Konfigurationsdaten dieses Jobs werden tabellarisch dargestellt.

Für einen Job können entweder Daten im Register „Deployment Daten“ oder im Register „Konfiguration Daten“ vorhanden sein.



Parameter

Name des Parameters, der zur Änderung in diesem Job vorgesehen wurde.

Index

Index innerhalb des zu ändernden Parameters (wenn vorhanden).
Kann ein Parameter eines IP Devices mehrere Werte annehmen (Werteliste), wird pro Wert ein Index geführt. Das Feld bleibt leer, wenn nur ein Wert existiert.

Alte Einstellung

Wert des Parameters vor der Änderung. Ist der Parameter ein Passwort, werden hier nur Platzhalter angezeigt.

Neue Einstellung

Wert des Parameters nach der Änderung. Ist der Parameter ein Passwort, werden hier nur Platzhalter angezeigt.

User Daten

Ist diese Checkbox aktiviert, handelt es sich bei den Daten, die zum IP Device gesendet wurden, um benutzer- und nicht um gerätespezifische Daten (nur Anzeige).

Beendet

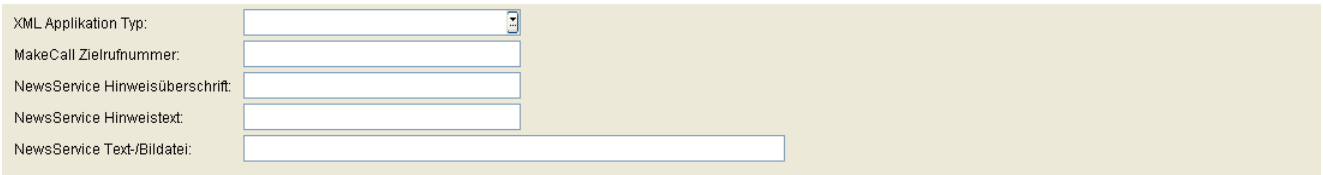
Anzeige, ob die Änderung des Parameters bereits durchgeführt wurde.

Status Info

Informationen zum Job-Status.

14.1.4 Register „XML Applikationen Daten“

Aufruf: Hauptmenü > Job Koordination > Job Kontrolle > Register „XML Applikationen Daten“



XML Applikation Typ:

Typ der mit diesem Job gestarteten XML-Applikation.

Mögliche Optionen:

- **MakeCall**
- **NewsService Datei-Anzeige**
- **NewsService Hinweis**

MakeCall Zielrufnummer

Rufnummer des Endgeräts, für das mit der XML-Applikation ’MakeCall’ ein automatischer Testanruf initiiert wurde.

NewsService Hinweisüberschrift

Überschrift des letzten Hinweises, der mittels der XML Applikation ‘NewsService’ an das Endgerät geschickt wurde.

NewsService Hinweistext

Text des letzten Hinweises, der mittels der XML Applikation ‘NewsService’ an das Endgerät geschickt wurde.

NewsService Text-/Bilddatei

Dateiname der letzten Text- (.txt) oder Bilddatei (.jpg, .bmp, .gif, .png), die mittels der XML Applikation ‘NewsService’ an das Endgerät geschickt wurde.

14.2 Täglicher Status

Aufruf: Hauptmenü > Job Koordination > Täglicher Status

Dieser Bereich besteht aus folgenden Inhalten:

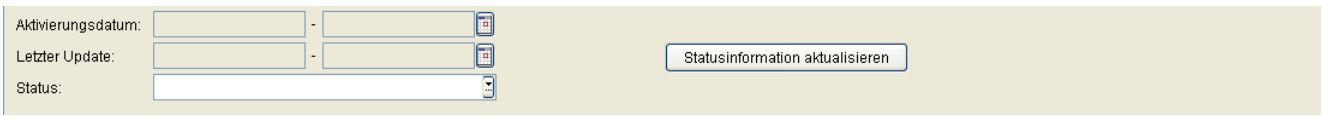
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „Statusinformation“

Diese Funktion dient zur übersichtlichen Anzeige aller Jobs in tabellarischer Form. Des weiteren kann nach einem gewünschten Job-Status oder einer Job-ID gesucht werden. Im Suchergebnis werden alle Täglichen Status angezeigt, die Jobs passend zum Suchkriterium beinhalten. In der Statusinformation der Objektansicht kann die Ansicht der ganzen Tabelle oder nur der einzelnen Tabelleneinträge ausgewählt werden. Die Tabelle kann nach Job ID, Job Status, Aktivierungszeit oder Endzeit sortiert werden.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern in der Ansicht Suche, um eine bestimmte Gruppe von Jobs zu finden. In der Ansicht Objekt werden hier die Daten der gefundenen Jobs angezeigt.



Aktivierungsdatum:

Zeitbereich bzw. Zeitpunkt für die Aktivierung des Deployment-Jobs (siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).

Letzer Update:

Datum des letzten Updates der Statusinformation.

Status:

Mögliche Aktionsstatus:

- **aktiv**
  Der Deployment-Job wurde in der Job-Tabelle aufgenommen, läuft aber noch nicht, weil z. B. Ausführungszeit noch nicht erreicht wurde.
- **fehlgeschlagen**
  Der Deployment-Job wurde gestartet, konnte jedoch nicht ausgeführt werden.
- **fertig**
  Der Deployment-Job wurde korrekt ausgeführt.
- **läuft**
  Der Deployment-Job wird gerade ausgeführt.

Statusinformation aktualisieren

Statusinformation auf den aktuellen Stand bringen, einschließlich aller an diesem Tag erzeugten Jobs.

Mögliche Aktionsschaltflächen

Suchen

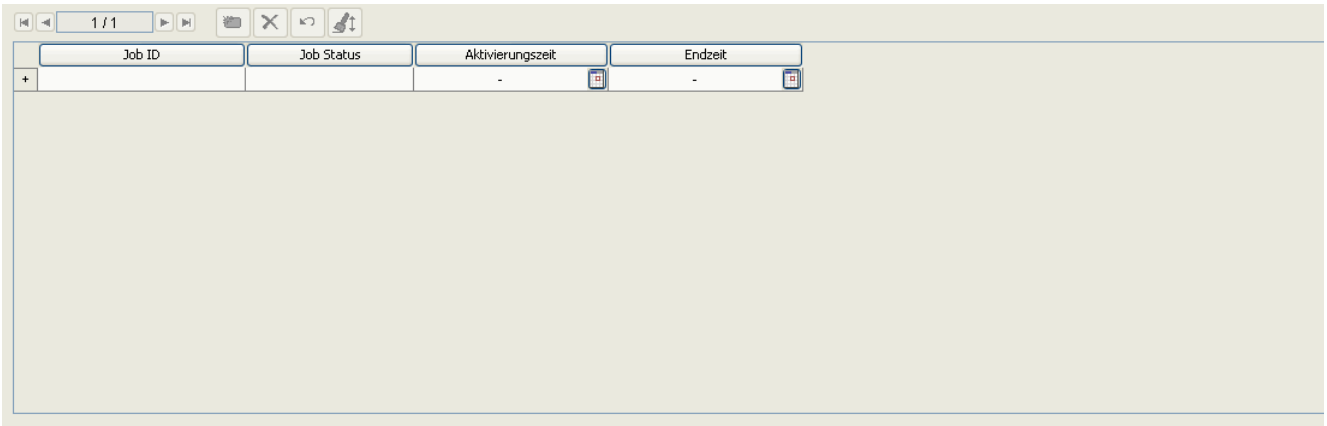
Sucht nach allen Statistik-Daten, die den Suchkriterien entsprechen.

Fenster leeren

Löscht den Inhalt aller Felder dieser Ansicht. In der Ansicht **Suche** können so vor dem Eintragen neuer Suchkriterien die bisherigen gelöscht werden.

14.2.1 Register „Statusinformation“

Aufruf: Hauptmenü > Job Koordination > Täglicher Status > Register „Statusinformation“



Job ID

Job-ID (bzw. die Aktionsnummer) des Deployment-Jobs.

Job Status

Status des Deployment-Jobs.

Aktivierungszeit

Zeitpunkt der Aktivierung des Deployment-Jobs.

Endzeit

Bei Jobs mit dem Status **fertig**: Zeitpunkt des Ausführungsendes.

14.3 Job Konfiguration

Aufruf: Hauptmenü > Job Koordination > Job Konfiguration

Dieser Bereich besteht aus folgenden Inhalten:

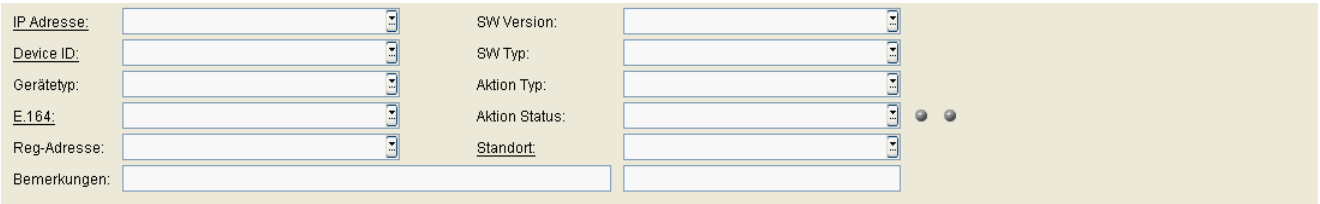
- Allgemeine Daten
- Mögliche Aktionsschaltflächen
- Register „IP Phones“
- Register „IP Clients“
- Register „IP Gateways“
- Register „Gateways“

Mittels dieser Funktion kann das Verhalten der Jobs beeinflusst werden. Einige Konfigurationsdaten können für IP Phones und IP Clients unterschiedlich eingetragen werden.

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

Allgemeine Daten

Dieser Teil des Inhaltsbereiches dient der Eingabe von Parametern, die für alle Register gelten.



Max. Anzahl gleichzeitiger Jobs:

Maximale Anzahl der gleichzeitig auszuführenden Deployment-Jobs. Müssten laut Ausführungszeit mehr als die angegebenen Jobs gestartet werden, würden für alle betroffenen Jobs automatisch Wiederholungsversuche gestartet.

Standard: 100.

Beendete Jobs löschen nach Tagen:

Anzahl an Tagen, nach denen beendete Jobs gelöscht werden sollen. Jobs mit anderen Status bleiben hiervon unberührt.

Standard: 10.

Abgebrochene Jobs löschen nach Tagen:

Anzahl an Tagen, nach denen abgebrochene Jobs gelöscht werden sollen. Jobs mit anderen Status bleiben hiervon unberührt.

Standard: 10.

Abgelaufene Jobs löschen nach Tagen:

Anzahl an Tagen, nach denen abgelaufene Jobs gelöscht werden sollen. Jobs mit anderen Status bleiben hiervon unberührt.

Standard: 10.

Fehlerhafte Jobs löschen nach Tagen:

Anzahl an Tagen, nach denen abgebrochene Jobs gelöscht werden sollen. Jobs mit anderen Status bleiben hiervon unberührt.

Standard: 99999 (die fehlerhaften Jobs werden nicht gelöscht).

Standard Job Ausführungsart:

Standardwert für den Zeitpunkt der Jobausführung.

Mögliche Optionen:

- **Sofort ausführen**
  Der Job wird sofort gestartet.
- **Sofort oder nach Registrierung**
  Der Job wird sofort gestartet. Wird er abgebrochen, so wird beim Registrieren des Geräts ein erneuter Versuch unternommen.
- **Nach Workpoint Registierung**
  Der Job wird bei Registrierung des Geräts gestartet.

Beendete Jobs sichern

Schalter zum Aktivieren der Option, dass Jobs in der Job-Tabelle belassen werden und in der Job-Statistik angezeigt werden können.

Standard: **aktiviert**

Mögliche Aktionsschaltflächen

Sichern

Sichert die Änderungen, die Sie bei **Job Konfiguration** vorgenommen haben.

Verwerfen

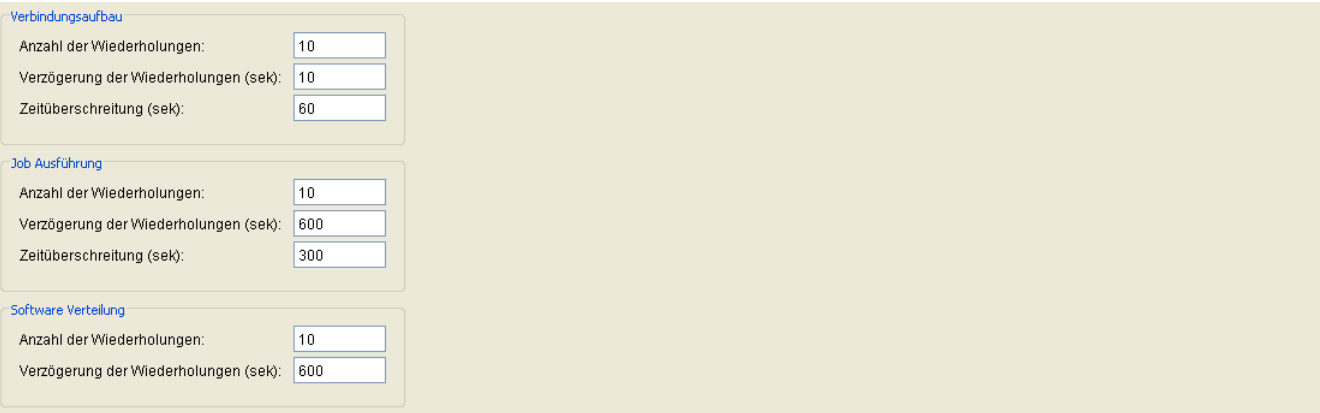
Verwirft die Änderungen, die Sie bei **Job Konfiguration** vorgenommen haben.

Aktualisieren

Aktualisiert den Inhalt der betroffenen Seite.

14.3.1 Register „IP Phones“

Aufruf: Hauptmenü > Job Koordination > Job Konfiguration > Register „IP Phones“



Verbindungsaufbau

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für IP Phones bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10.**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für IP Phones liegen soll.

Standard: **10**. Wertebereich: **1** - **3600**

Zeitüberschreitung (sek):

Zeit in Sekunden, die der DLS pro Versuch auf eine Antwort von den IP Phones wartet, wenn ein Job ausgeführt wird.

Wertebereich: **1** - **3600**

Standard: **60.**

Job Koordination

Job Konfiguration

Job Ausführung

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für IP Phones bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10.**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für IP Phones liegen soll.

Wertebereich: **1** - **3600**

Standard: **600.**

Zeitüberschreitung (sek):

Zeitlimit für die vollständige Jobausführung, über alle Versuche hinweg.

Wertebereich: **30** - **3600**

Standard: **300.**

Software Deployment

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, falls der erste Versuch fehlschlug und der Job nach automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10**.

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen liegen soll.

Wertebereich: **1** - **3600**

Standard: **600.**

Zeitüberschreitung (sek):

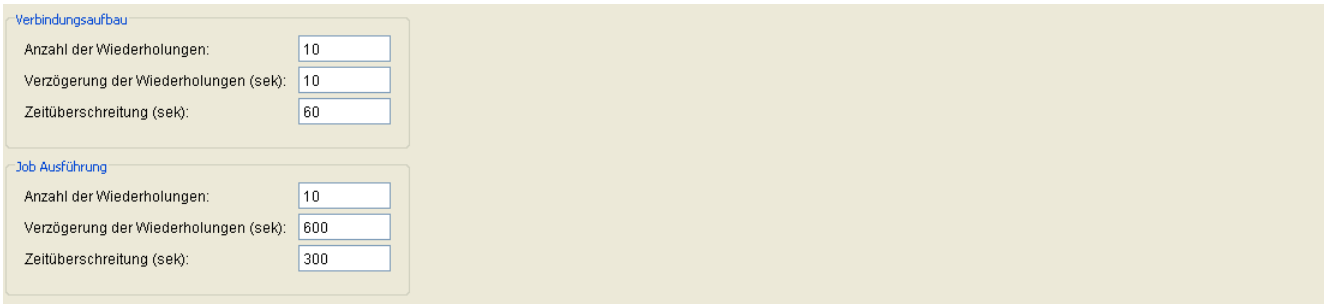
Zeit in Sekunden, die der DLS pro Versuch auf eine Antwort wartet, wenn ein Job ausgeführt wird.

Wertebereich: **30** - **3600**

Standard: **300**

14.3.2 Register „IP Clients“

Aufruf: Hauptmenü > Job Koordination > Job Konfiguration > Register „IP Clients“



Verbindungsaufbau

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für IP Phones bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10**.

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für IP Phones liegen soll.

Wertebereich: **1** - **3600**

Standard: **10**

Zeitüberschreitung (sek):

Zeit in Sekunden, die der DLS pro Versuch auf eine Antwort von den IP Phones wartet, wenn ein Job ausgeführt wird.

Wertebereich: **1** - **3600**

Standard: **60**.

Job Ausführung

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für IP Phones bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10.**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für IP Phones liegen soll.

Wertebereich: **1** - **3600**

Standard: **600.**

Zeitüberschreitung (sek):

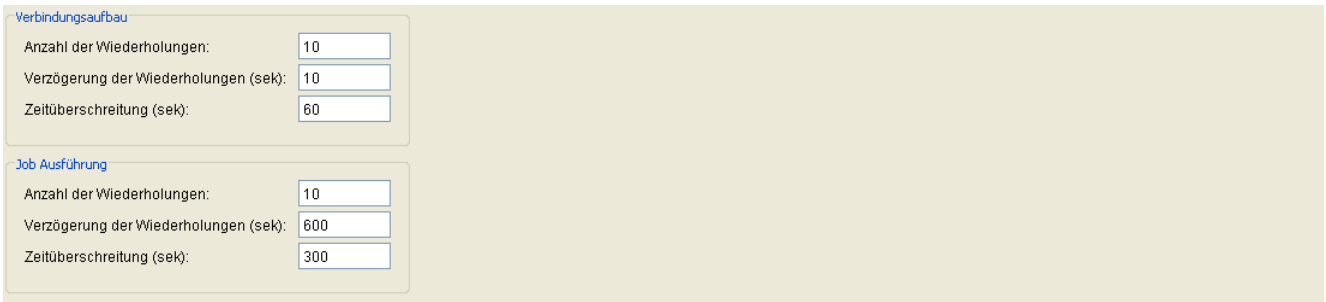
Zeitlimit für die vollständige Jobausführung, über alle Versuche hinweg.

Wertebereich: **30** - **3600**

Standard: **300.**

14.3.3 Register „IP Gateways“

Aufruf: Hauptmenü > Job Koordination > Job Konfiguration > Register „IP Gateways“



Verbindungsaufbau

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für IP Gateways bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für IP Gateways liegen soll.

Wertebereich: **1** - **3600**

Standard: **10**

Zeitüberschreitung (sek):

Zeit in Sekunden, die der DLS pro Versuch auf eine Antwort von den IP Gateways wartet, wenn ein Job ausgeführt wird.

Wertebereich: **1** - **3600**

Standard: **60.**

Job Ausführung

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für IP Gateways bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **100**

Standard: **10**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für IP Gateways liegen soll.

Wertebereich: **1** - **3600**

Standard: **600.**

Zeitüberschreitung (sek):

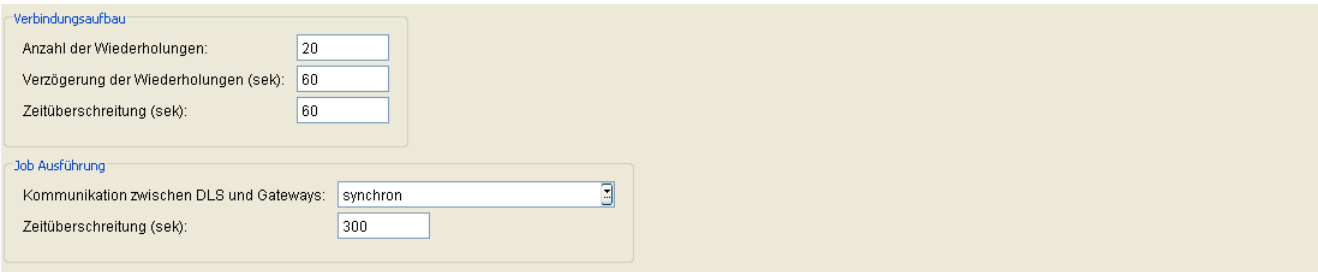
Zeitlimit für die vollständige Jobausführung, über alle Versuche hinweg.

Wertebereich: **30** - **3600**

Standard: **300.**

14.3.4 Register „Gateways“

Aufruf: Hauptmenü > Job Koordination > Job Konfiguration > Register „Gateways“



Verbindungsaufbau

Anzahl der Wiederholungen:

Anzahl der Wiederholungen, bis die Ausführung eines Jobs für Gateways bei mehreren automatischen Wiederholungsversuchen mit dem Status **abgebrochen** beendet werden soll.

Wertebereich: **1** - **200**

Standard: **20**

Verzögerung der Wiederholungen (sek):

Zeit in Sekunden, die zwischen zwei automatischen Job-Wiederholungsversuchen für Gateways liegen soll.

Wertebereich: **10** - **3600**

Standard: **60.**

Zeit in Sekunden, die der DLS pro Versuch auf eine Antwort, wenn ein Job ausgeführt wird.

Zeit in Sekunden, die der DLS pro Versuch auf eine Antwort von den Gateways wartet, wenn ein Job ausgeführt wird.

Wertebereich: **1** - **3600**

Standard: **60**

Job Ausführung

Kommunikation zwischen DLS und Gateways:

Mögliche Optionen:

- **synchron**
  Die Jobs werden synchron ausgeführt, was zu einem Blockieren der Anzeige im DLS führt (Anzeige der Sanduhr), bis die Jobs vollständig ausgeführt sind. Durch **Aktualisieren** erhält man stets den aktuellen Datensatz.
- **asynchron**
  Die Jobs werden „im Hintergrund“ ausgeführt, und es kann parallel weitergearbeitet werden. Um das Ergebnis zu sehen, muss etwas gewartet und dann **Aktualisieren** durchgeführt werden. Erfolgt das Aktualisieren zu früh, erhält man den alten Datensatz.

Zeitüberschreitung (sek):

Zeitlimit für die vollständige Jobausführung, über alle Versuche hinweg.

Wertebereich: **1** - **3600**

Standard: **300.**

15 Bedienabläufe

Dieses Kapitel enthält folgende praxisorientierte Abläufe:

- Erste Schritte: Ändern von IP Device-Parametern

  HINWEIS: In diesem Abschnitt erhalten Sie grundsätzliche Bedienungshinweise, die auch beim Durchführen anderer Funktionen hilfreich sind.

- Änderung der Element Manager-Konfiguration und Joberzeugung
- Registrieren von Workpoint-Software und -Dateien
- Templates bearbeiten
- Autokonfiguration von Workpoints (Plug&Play)
- Verteilen von Workpoint-Software
- Nutzen der Job-Koordination
- Backup / Restore
- Automatische Wiederherstellung bei fehlerhaftem Upgrade
- Import und Export von Plug&Play-Daten
- Copy-Makro für P&P und Templates

Zur allgemeinen Bedienung der Oberfläche siehe Abschnitt 5.4.2, “Arbeitsbereich”.

HINWEIS: Die hier genannten Ablaufbeschreibungen haben beispielhaften Charakter. Durch Besonderheiten in der Konfiguration des DLS, der eingesetzten Server oder der IP Devices sowie durch Weiterentwicklung des DLS kann der tatsächliche Ablauf von der Beschreibung abweichen.

15.1 Erste Schritte: Ändern von IP Device-Parametern

Mithilfe der im DLS arbeitenden Datenbank haben Sie die Möglichkeit, in vielen Bereichen des DLS (z. B. **IP Devices**) aus der Gesamtzahl der verfügbaren IP Devices alle oder eine Untermenge zu bestimmen, um sie nachfolgend zu administrieren.
Dies geschieht im Arbeitsbereich mittels der Ansicht **Suche** (siehe Abschnitt 5.4.2.3).

Voraussetzung für dieses Beispiel: Der DLS, die Server und IP Devices sind betriebsbereit.

1. Wählen Sie im Hauptmenü bei **IP Devices** einen Bereich aus, in dem Sie eine Änderung machen möchten.
2. Wählen Sie die Ansicht **Suche** (siehe Abschnitt 5.4.2.3), falls diese noch nicht angezeigt wird.
3. Legen Sie fest, welche IP Devices Sie auswählen möchten.
   Wählen Sie hierzu z. B. bei **Gerätetyp** einen Eintrag im Auswahllistenfeld aus (siehe Abschnitt 5.4.2.4) oder geben Sie einen IP-Adressbereich ein.

   HINWEIS: Weitere Informationen zur Ansicht **Suche** finden Sie im Abschnitt 5.5, “Suchfunktionalität”.

   Soll über alle verfügbaren IP Devices gesucht werden, tragen Sie nichts in die Felder der Suchansicht ein.
4. Klicken Sie auf die Schaltfläche **Suchen** (siehe Abschnitt 5.4.2).
5. Wenn keine übereinstimmenden Daten gefunden wurden, wird eine Meldung im Meldungsfenster angezeigt (siehe Abschnitt 5.4.2.6).

   Bei erfolgreicher Suche wechselt die Anzeige in die Ansicht **Objekt**, die immer die Daten eines einzelnen IP Devices darstellt. Mithilfe der Schaltflächen zur Navigation (siehe Abschnitt 5.4.2.5) können Sie nun zwischen allen IP Device-Daten wechseln, die dem Suchfilter entsprechen.

6. Mit Klick auf **Tabelle** in der Ansichtenleiste wechseln Sie in die Listenansicht. Klicken Sie auf einen Spaltenkopf, um die gesamte Tabelle nach dem im Kopf angegebenen Wert zu sortieren (jeweils auf-/absteigend).

   Durch Klicken zwischen zwei Spaltenköpfen und Ziehen nach rechts/links ändern Sie die Breite der jeweils links davon liegenden Spalte.

   Klicken auf einen Spaltenkopf und Ziehen nach rechts/links ändert die Reihenfolge der Spalten.

7. Sie können nun Änderungen in allen nicht ausgegrauten Feldern vornehmen. Dies ist sowohl in der Ansicht **Objekt** als auch in der Ansicht **Tabelle** (in jeweils einer Zeile) möglich.

8. Um die Änderungen an ein einziges IP Device zu übertragen, klicken Sie auf die Schaltfläche **Sichern**. Damit werden die Daten sofort an das IP Device übertragen.

   HINWEIS: Möchten Sie die Änderungen gleichzeitig an mehrere IP Devices übertragen, wechseln Sie vor dem Sichern in die Ansicht **Tabelle** und markieren Sie weitere IP Device-Einträge in der Liste (siehe hierzu Abschnitt 5.4.2.4, “Mehrfachauswahl und Datenübernahme in der Tabellen-Ansicht”).

   Klicken Sie auf die Schaltfläche **Sichern**. Damit werden die Daten sofort an die ausgewählten IP Devices übertragen.

15.2 Änderung der Element Manager-Konfiguration und Joberzeugung

Änderungen innerhalb der Element Manager-Konfiguration unter **Element Manager** > **Element Manager Konfiguration** (z. B. E.164 Präfix, Gatekeeper ID, SIP Server Adr., etc.) werden an die betreffenden IP Devices weitergegeben. Das sind diejenigen IP Devices, die unter **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „EM Synchronisation“** die ID dieses Element Managers im Feld **Element Manager ID** eingetragen haben. Ist allerdings unter Zugeordneter Element Manager ein anderer Element Manager (bzw. Element Manager ID) eingetragen, dann ist diese gültig.[1] Je nach Anzahl der IP Devices kann eine Änderung, z. B. des E.164 Präfixes, mehrere Minuten dauern.

Für registrierte IP Devices werden bei Änderungen innerhalb der Element Manager-Konfiguration Jobs erzeugt. Bevor diese Änderungen durchgeführt werden, erscheint ein Dialog, der die Anzahl der Jobs anzeigt und um Bestätigung dieser Aktion bittet. Hier gibt es die Möglichkeit, die Konfigurationsänderungen zu sichern ohne sofortige Joberzeugung. Dann werden die Jobs aber bei der nächsten automatischen oder manuellen Synchronisation ohne Nachfrage erzeugt.

Ist eine Synchronisation gestartet worden und noch nicht beendet, dann kann bezüglich dieses Element Managers bzw. dieser Element Manager-ID keine weitere Synchronisation gestartet werden. Eine entsprechende Meldung wird im Fenster ausgegeben. Die gleiche Meldung erhält man, wenn man versucht, die Elementmanagerkonfiguration zu ändern, und gerade eine (automatische) Synchronisation läuft.

1 Dieser Parameter findet Verwendung bei der Vorbereitung des Umzugs eines Teilnehmers zu einer anderen Anlage. Während der Vorbereitung existieren 2 Datensätze mit derselben E.164-Nummer und unterschiedlichen Device IDs. Dabei ist ein Datensatz der Anlage A, der zweite Datensatz der Anlage B zugeordnet. Der hier definierte Parameter sorgt dafür, dass Synchronisationen mit den beiden Anlagen jeweils nur denjenigen Datensatz aktualisieren, der zu der entsprechenden Anlage gehört.

15.3 Registrieren von Workpoint-Software und -Dateien

Hier wird erläutert, wie Sie Software und Dateien im DLS registrieren können, damit diese vom DLS für das Deployment genutzt werden können.

Die Funktionen befinden sich unter **Hauptmenü** > **Administration** > **Server Konfiguration** > **FTP Server Konfiguration**, ...> **HTTPS Server Konfiguration**, ... > **Netzlaufwerk Konfiguration**.

HINWEIS: Bereits während der Registrierung erfolgt eine Prüfung der zu registrierenden Datei.
Es wird geprüft:
- Ob die Datei am Quell-Speicherort vorhanden ist.
- Wenn vorhanden und wenn es sich um eine Software handelt, ob Datei in einem unbekannten, im alten oder im neuen SPA vorliegt.
- Wenn sie im neuen Format vorliegt, werden weitere Daten wie **SW Typ** (Typ der Software: HFA oder SIP), **SW Version** (Versionsnummer der Software) usw. ausgelesen.

Dieser Ablauf kann je nach Netzwerk einige Zeit dauern.

Zur Übersicht aller vom DLS unterstützten Objekt-Typen siehe Abschnitt 3.5, “Übersicht der Software- und Datei-Typen”.

Zur Übersicht aller vom DLS unterstützten IP Devices und Plattformen siehe Abschnitt 3.4, “Einsatzgebiet”.

HINWEIS: Auch IP Client-Software-Installationen müssen im DLS registriert werden, jedoch wird bei IP Client-Software keine Lizenzprüfung im DLS vorgenommen, da dies während der Laufzeit (beim Starten der Software) geschieht.

Voraussetzungen

- Ein eingerichteter FTP-Server Abschnitt 6.3.4für Abschnitt 6.3.7IP Phone Software-Images bzw. ein konfiguriertes Windows-Netzlaufwerk für IP Client-Software (siehe bzw).
- Es sind passende Dateien im Quell-Speicherort vorhanden.

15.3.1 Automatische Registrierung

Die automatische Registrierung unterscheidet sich je nach der Art des Quell-Speicherortes.

1. Um Software und Daten auf einem FTP-Server zu registrieren, wählen Sie unter **Administration** > **Server Konfiguration** > **FTP Server Konfiguration mit der Aktionsschaltfläche** Suchen einen FTP-Server aus der Auswahlliste. Klicken Sie dann auf **Start Scan**, um die Registrierung auszulösen.

   Installationen für IP Clients registrieren Sie über **Administration** > **Server Konfiguration** > **Netzlaufwerk Konfiguration** > **Scan Server**.

   Um Software und Daten auf einem HTTP-Server zu registrieren, wählen Sie **Administration** > **Server Konfiguration** > **Netzlaufwerk Konfiguration** > **Scan Server**.

   Zum Konfigurieren von FTP-Server und Netzwerk-Laufwerk siehe Abschnitt 6.3.4 bzw Abschnitt 6.3.7.

2. Klicken Sie auf **Start**. Die automatische Registrierung startet und aktualisiert den Status sowie die Eintragsinformation im Dialogfenster.

   HINWEIS: Während des Vorgangs können Sie das Dialogfenster bereits schließen. Die automatische Registrierung läuft im Hintergrund davon unbeeinflusst weiter.

15.3.2 Verstehen der Lizenzinformationen bei IP Phone-Software

HINWEIS: Zur Zeit steht keine lizenzpflichtige IP Phone-Software zur Verfügung. Das heißt, bezüglich Lizenzierung gelten für IP Phones ausschließlich die hier gemachten Angaben für lizenzfreie Software.

Beim Registrieren von IP Phone-Software werden u. a. auch Informationen aus dem „License Trailer“ des Software-Image gelesen.

Die License Trailer Information besteht aus folgenden möglichen Werten:

- Device Type (enthält die Gerätetyp-Bezeichnung)
- SW Version (enthält die Versionsnummer der Software)
- SW Type (enthält die Softwaretyp-Bezeichnung)
- License Feature ID (enthält die Kennung zum License Feature)
- Licensed SW Version (enthält die Versionsnummer der Software-Lizenz)
- Expiry Date (enthält das Ablaufdatum der Software)

15.4 Templates bearbeiten

Der DLS bietet die Möglichkeit, für alle Parameter im Bereich **IP Devices** Vorlagen, sprich „Templates“, zu erzeugen. Dadurch können Sie häufig verwendete Konfigurationen einfach und komfortabel wiederverwenden.

Zudem können vorhandene Templates zu Profilen zusammengefasst werden, was die Handhabung umfangreicher Workpoint-Konfigurationen stark vereinfacht.

Für jede Oberfläche im Inhaltsbereich (siehe Abschnitt 5.4.2, “Arbeitsbereich”) können Sie ein Template anlegen und zur späteren Wiederverwendung sichern. Über Buttons können Sie zudem alle gesicherten Templates in eine ZIP-Datei exportieren und importieren (siehe Abschnitt 12.3, “Template Übersicht”).

WICHTIG: Werden Datenänderungen in Konfigurationsmasken vorgenommen, die mithilfe von Templates erstellt wurden, so werden diese Änderungen nicht automatisch in diese Templates übernommen.
Zum Übernehmen müssen die Änderungen manuell im Template gesichert werden, siehe unten.

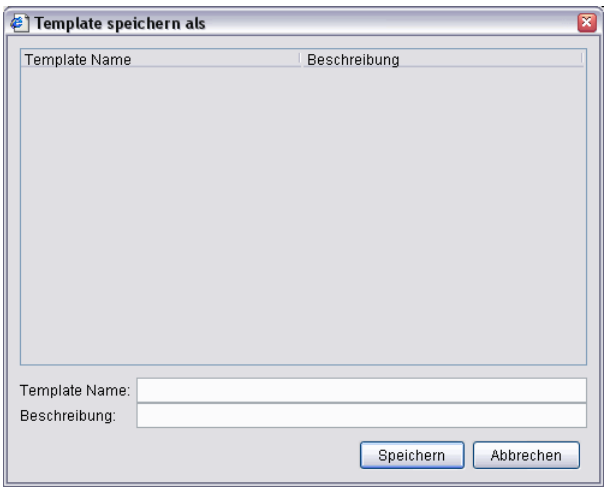
15.4.1 Template manuell anlegen

1. Wählen Sie im Hauptmenü bei **IP Devices** > **IP Phone Konfiguration** bzw. **IP Client Konfiguration** einen Bereich aus, für den Sie das Template anlegen möchten.
2. Wählen Sie die Ansicht **Template** (siehe Abschnitt 5.4.2.3, “Ansichtenleiste”).
3. Tragen Sie alle erforderlichen Daten ein.

   Ein Template umfasst immer den Inhalt einer Oberfläche unter **IP Devices**, mit allen verfügbaren Registern.

   HINWEIS: In vielen Fällen ist es sinnvoll, den Umfang eines Templates nicht zu groß zu wählen. So kann es z. B. von Vorteil sein, zwei getrennte Templates statt eines für WAP und LDAP anzulegen, um diese flexibler, d. h. getrennt voneinander verschiedenen Profilen zuordnen zu können.
4. Klicken Sie auf die Schaltfläche **Sichern**.

5. Das Dialogfenster zum Sichern des Templates erscheint.



   Geben Sie bei **Template Name** einen aussagekräftigen Namen ein, z. B. „QoS Konfiguration 1“. Bei **Beschreibung** können Sie einen erklärenden Text zu diesem Template hinterlegen.

6. Klicken Sie auf **Speichern**.

   In der Ansichtenleiste wird nun hinter **Template** der Name des aktuellen Templates angezeigt.

Sie können zu einem Bereich auch mehrere, verschiedene Templates mittels unterschiedlicher Template-Namen sichern.

Gespeicherte Templates können Sie exportieren (siehe Abschnitt 12.3, “Template Übersicht”).

15.4.2 Template aus vorhandener Konfiguration erstellen

Sie können bereits vorhandene Konfigurationsdaten aus der Ansicht **Objekt** in ein Template übernehmen.

1. Wählen Sie im Hauptmenü bei **IP Devices** einen Bereich in der Ansicht **Objekt** aus, von dem Sie die Daten in ein Template kopieren möchten.
2. Wählen Sie in der Menüleiste bei **Aktion** den Eintrag **In Template kopieren**. Die Ansicht **Template** wird mit den kopierten Daten angezeigt.

Sichern Sie das Template zur weiteren Verwendung wie oben beschrieben (siehe „Template aus vorhandener Konfiguration erstellen“ ab Schritt 4).

15.4.3 Template laden

Um ein bereits gesichertes Template zu ändern oder manuell zu nutzen, muss es zunächst in die Ansicht **Template** geladen werden.

1. Wählen Sie in dem Bereich die Ansicht **Template**, für den Sie ein bereits gespeichertes Template laden möchten und klicken Sie auf **Holen**.
2. Wenn für diesen Bereich mindestens ein Template vorliegt, erscheint das Dialogfenster zum Laden eines Templates.

3. Wählen Sie ein Template aus der Liste aus und klicken Sie auf **Holen**.
4. Der Inhalt des Templates wird in der Ansicht **Template** angezeigt und der Template-Name erscheint in der Ansichten-Leiste.

   Um die Daten zum Konfigurieren oder als Suchkriterium nutzen zu können, wählen Sie die entsprechende Ansicht (**Objekt** oder **Suche**) und wählen Sie in der Menüleiste bei **Aktion** den Eintrag **Template anwenden**.

   HINWEIS: Beim Anwenden eines Templates werden immer nur die im Template definierten Inhalte übernommen. Leere oder ausgegraute Felder bzw. Checkboxen überschreiben bzw. löschen keine aktuellen Werte in der Konfiguration.

   Über **Profil Management** > **Template Übersicht** kann geprüft werden, welche einzelnen Attribute im aktuellen Template gesetzt sind.

15.4.4 Weitere Funktionen

Mit Klick auf **Template umbenennen** in der Ansicht **Template** können Sie ein bereits gesichertes Template umbenennen und die Beschreibung zum Template ändern. Mit **Template löschen** können Sie einzelne oder mehrere gesicherte Templates löschen.

15.5 Autokonfiguration von Workpoints (Plug&Play)

Ziel des Plug&Play im DLS ist es, die unterstützten Workpoints automatisch mit den zur Registrierung an einem Gatekeeper oder SIP-Server notwendigen Parametern zu versorgen. Dies soll immer dann geschehen, sobald ein Workpoint eingeschaltet bzw. angeschlossen wird.

Man kann zwischen verschiedenen Plug&Play-Arten unterscheiden:

- **Vollständiges Plug&Play**
  - Versorgung des Workpoints mit IP-Basisdaten und DLS-Adressdaten mittels DHCP-Server.
- **Eingeschränktes Plug&Play**
  - Manuelles Eintragen der IP-Basisdaten und der DLS-Adressdaten am Workpoint.

HINWEIS: Es wird empfohlen, einen DHCP-Server im DLS-Umfeld einzusetzen, um :

- vollständiges Plug&Play zu unterstützen und
- die Authentizität des DLS-Servers sicherzustellen

Detaillierte Informationen zum Einrichten eines DHCP-Servers finden Sie im Abschnitt 4.12.4, “DHCP-Server in einer Windows-Umgebung” bzw. Abschnitt 4.12.5, “DHCP-Server in einer Linux/ Unix-Umgebung”.

HINWEIS: Ein Factory Reset mit gespeicherten Plug&Play Daten kann nicht im Secure Mode durchgeführt werden. Die betroffenen IP Devices müssen zuerst auf Default Mode zurückgesetzt werden.

15.5.1 Voraussetzungen

Voraussetzungen für vollständiges Plug&Play

- Eine funktionierende DHCP-Infrastruktur. Abhängig von der Netzwerktopologie besteht diese aus mindestens einem DHCP-Server und ggf. mehreren DHCP Relay Agents.
- Auf dem DHCP-Server sind die IP-Basisdaten einschließlich der DLS-Adressdaten eingetragen, so dass sie automatisch an die Endgeräte verteilt werden können. Zur Konfiguration des DHCP-Servers siehe Abschnitt 4.12.4.3 (Windows) bzw. Abschnitt 4.12.5 (Linux/Unix).

Auf diese Weise erhält ein IP Phone, das sich im Werks-Lieferzustand befindet, beim Booten seine initiale IP-Konfiguration.

Voraussetzungen für eingeschränktes Plug&Play

- Manuelles Eintragen der kompletten IP-Basisdaten (IP-Adresse, Subnetzmaske, Default IP-Gatekeeper, DNS-Server, DNS-Domain-Suffix, usw.) und DLS-Adressdaten am IP Phone.

Damit haben Sie auch in Netzen ohne DHCP-Infrastruktur die Möglichkeit eines, wenn auch eingeschränkten, Plug&Play.

HINWEIS: Für IP Clients gestaltet sich das vollständige Plug&Play etwas anders.

Dadurch, dass IP Clients in der Regel auf einem bereits „wohl konfigurierten“ Host laufen, was die IP-Konfiguration anbelangt, kann der IP Client entweder mittels eines „DHCP-Informs“ oder mit einem „DNS Text Resource Request“ die noch fehlende DLS-Adressdaten versorgt werden.

Beide Wege können als vollständiges Plug&Play angesehen werden, da keine manuelle Konfiguration notwendig ist, im Vergleich zum ausschließlichen Einsatz eines DNS bei IP Phones.

15.5.2 Plug&Play-Registrierung einrichten

15.5.2.1 Zuordnungsverfahren

Bei der Plug&Play-Registrierung wird zwischen zwei Verfahren unterschieden. Der Unterschied besteht in der Art und Weise, wie die Plug&Play-Daten einem physikalischen Workpoint zugeordnet werden.

- **Zuordnung mittels Device ID**

  Hierbei wird zu einem bereits bestehenden Datensatz, d. h. einem virtuellen Gerät, eine bestimmte Device ID eingetragen (siehe Abschnitt 15.5.2.2, “Plug&Play-Daten anlegen”). Der DLS erkennt anhand der Device ID, welche Plug&Play-Daten er an den Workpoint schicken muss.

- **Zuordnung mittels E.164**

  Alternativ kann der Datensatz mit einer E.164-Nummer zugeordnet werden, die manuell am Workpoint einzugeben ist. Der DLS prüft dann nacheinander alle ihm bekannten auf Rufnummern basierenden Quellen von Plug&Play-Daten (z. B. konfigurierte HiPath 4000 Assistant-Datenbanken, HiPath 3000/5000) daraufhin ab, ob eine eindeutige Zuordnung der Rufnummer zu einem System möglich ist.

  Meldet sich der Workpoint bei seiner Installation am DLS an, erkennt der DLS anhand der mitgesendeten E.164-Nummer, welche Plug&Play-Daten er an den Workpoint schicken muss.

- **Zuordnung mittels Rufnummernband**

  Ist ein Rufnummernband konfiguriert und aktiviert, so erhält jedes IP Phone, das sich am DLS ohne eine E.164-Nummer registriert, eine „Dummy“-E.164-Nummer aus diesem Rufnummernband. Voraussetzung ist, dass es mindestens eine freie Nummer gibt. Das zu der jeweiligen E.164-Nummer gehörige virtuelle Device wird dem IP Phone zugeordnet, indem seine Device ID in „@<MAC-Adresse des IP Phones>“ und sein Plug&Play Pool Status in „in Verwendung“ geändert wird. Daraufhin wird Plug&Play ausgeführt, unter Verwendung dieses virtuellen Geräts. Vor dem Plug&Play-Vorgang wird möglicherweise noch ein Software-Upgrade durchgeführt.

Die dem IP Phone zugewiesene E.164-Nummer steht im Rufnummernband solange nicht mehr zur Verfügung, bis das IP Phone seine endgültige Nummer erhalten hat, sei es durch den Administrator, durch eine Applikation mithilfe von DlsAPI, über das WBM oder lokal am Phone, oder aber das IP Phone wird aus der DLS-Datenbank gelöscht.

Sobald die E.164-Nummer wieder als frei erkannt wird, erhält das virtuelle Device eine neue **Device ID**, der Schalter **Aktiviere Plug&Play** wird wieder auf aktiv gesetzt, und der Plug&Play Pool Status wird auf „frei“ zurückgesetzt. Nun ist das virtuelle Device wieder im Rufnummernband verfügbar. Siehe auch Abschnitt 6.3.2.6, “Register „P&P Rufnummernband“”.

15.5.2.2 Plug&Play-Daten anlegen

Für das Anlegen von Plug&Play-Daten gibt es folgende alternative Vorgehensweisen:

- **Anlegen durch Synchronisation mit dem jeweiligen Element Manager**
  Die Synchronisation des DLS mit einem Element Manager erzeugt für jeden Teilnehmer, der im Element Manager, aber noch nicht im DLS gespeichert ist, einen neuen Datensatz. Näheres zur Verbindung zwischen Element Manager und DLS siehe **Element Manager** > **Element Manager Konfiguration**.
- **Import der Plug&Play-Daten**
  Unter **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** ist der Import von Plug&Play-Daten aus einer Datei möglich.
- **Manuelles Einrichten der Teilnehmer im DLS**

  Mithilfe des Bereichs **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** lässt sich ein neuer Teilnehmer-Datensatz im DLS als virtuelles Gerät anlegen.
- **Einrichten über ein Provisioning Tool unter Verwendung der DlsAPI**

15.5.3 Registrierungsvorgang

1. Schließen Sie den oder die Workpoints an (siehe Installations- bzw Administrationsanleitung zum Workpoint). Der Workpoint erhält, wenn die Voraussetzungen für das vollständige Plug&Play erfüllt sind, die DLS-Adressdaten mittels DHCP.

   Mit diesen Daten registriert sich der Workpoint am DLS.

2. Ist der DLS in der Lage, die Plug&Play-Daten für den sich registrierenden Workpoint eindeutig zu ermitteln, sendet er diese automatisch an den Workpoint..

   Zur Bestimmung der passenden Plug&Play-Daten bietet der DLS prinzipiell zwei Varianten an; Siehe hierzu Abschnitt 15.5.2.1, “Zuordnungsverfahren”.

   - **Zuordnung mittels Device ID**

     Bei dieser Variante prüft der DLS, ob es anhand der vom Workpoint präsentierten Device ID einen Satz Plug&Play-Datensatz ermitteln kann. Dies setzt am DLS z. Zt. jedoch eine rein manuelle Verknüpfung von Device ID und Plug&Play-Daten voraus.

   - **Zuordnung mittels E.164**

     Anhand der am Workpoint manuell eingegebenen E.164-Nummer prüft der DLS, ob er einen korrespondierenden Datensatz ermitteln kann.
     Beispiel einer vollständigen E.164-Nummer: **498972212345**.

   - **Zuordnung mittels Rufnummernband**

     Ist ein Rufnummernband konfiguriert und aktiviert, so erhält jedes IP Phone, das sich am DLS ohne eine E.164-Nummer registriert, eine „Dummy“-E.164-Nummer aus diesem Rufnummernband. Voraussetzung ist, dass es mindestens eine freie Nummer gibt.

3. Wurden Konfigurations-Templates definiert (siehe Abschnitt 15.4) und als Standard gruppiert, wird der Workpoint mit den Daten aus den Templates versorgt.
4. Mit der erfolgreichen Versendung aller zugeordneten Daten ist der Plug&Play-Ablauf abgeschlossen.

15.6 Verteilen von Workpoint-Software

Hier erfahren Sie, wie Sie manuell Software- bzw. Datei-Deployments durchführen und welche Konfigurationen zum automatischen Deployment erforderlich sind.

HINWEIS: Beachten Sie die Unterscheidung zwischen **Software Deployment** und **Datei Deployment** in der Oberfläche des DLS (siehe Abschnitt 10.1.1 und Abschnitt 10.1.2). Unter

Software Deployment versteht man das Verteilen von Software für Workpoints (IP Phones und IP Clients). Mit **Datei Deployment** ist hingegen das Verteilen von beliebigen Binär- oder ASCII-Dateien, die im Workpoint eine bestimmte Aufgabe erledigen.

Beide Funktionen sind im DLS im Hauptmenü unter **Software Deployment** zusammengefasst.

Zum automatischen Deployment siehe Abschnitt 15.6.2, “Automatisches Deployment”.

HINWEIS: Für jedes Workpoint kann parallel ein Software- und ein Datei-Deployment stattfinden, jedoch nicht mehrere Software-Deployments oder mehrere Datei-Deployments zur gleichen Zeit.

Soll ein Update von Workpoint-Software mithilfe eines Netboot Servers durchgeführt werden und das Update ist mittels Crosslink-Kabel (gekreuztes LAN-Kabel) nicht möglich, muss der Workpoint über einen Hub am Netboot Server angeschlossen werden.

HINWEIS: Achten Sie beim Verteilen von Software für Workpoints des Typs optiPoint WL2 professional darauf, dass die Workpoints über eine ausreichende Batteriekapazität verfügen. Ansonsten ist ein erfolgreiches Deployment ggf. nicht möglich.

Eigenschaften von Software-Images

Software-Images können sich durch folgende Eigenschaften von einander unterscheiden:

- Art der unterstützten Hardware (Gerätetyp, z. B. optiPoint 410 Standard).
- Softwaretyp (z. B. Unify HFA).
- Software Version (z. B. CLA, DHCP, DNS und FTP-Server).
- Integrierte DLS-Schnittstelle (ja = neues, nein = altes SPA).
- Lizenzpflichtig (ja oder nein).

  HINWEIS: Zur Zeit steht keine lizenzpflichtige IP Phone-Software zur Verfügung. Die momentan angebotene IP Phone-Software ist ausschließlich lizenzfrei.

15.6.1 Manuelles Deployment

Grundsätzlich können Sie beim manuellen Deployment folgende Parameter festlegen:

- Welche Workpoints mit der Software versorgt werden sollen.
- Welche Software zur Verteilung verwendet werden soll.
- Wann das Verteilen stattfinden soll.

Voraussetzungen

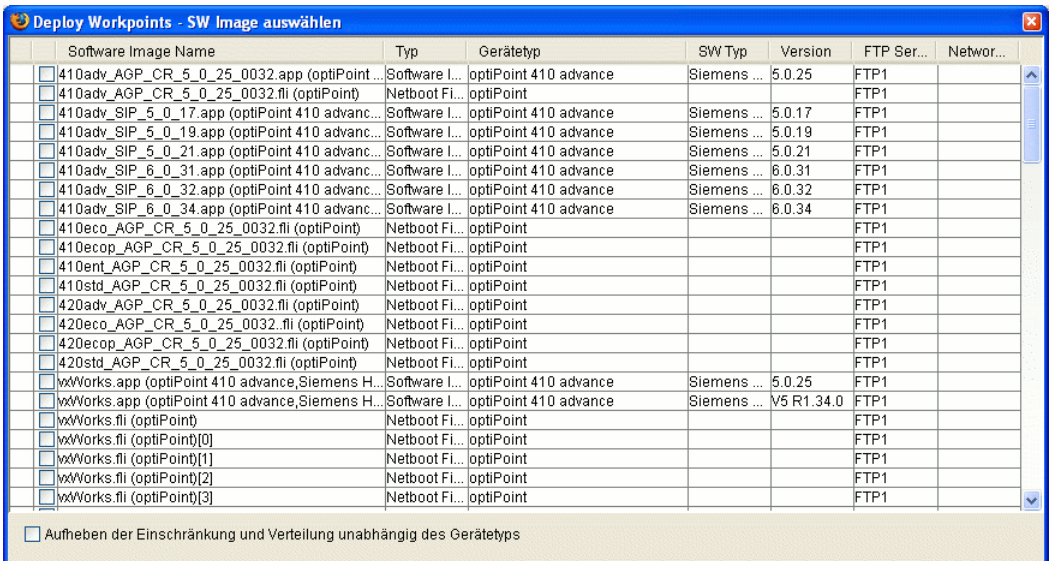
- Eine funktionsfähige DLS-Infrastruktur
- Die zu versorgenden Workpoints haben sich beim DLS automatisch registriert oder wurden durch manuelles Scannen vom DLS gefunden (siehe Abschnitt 7.4.6, “IP Devices scannen”).
- Die zu verteilende Software wurde entweder automatisch oder manuell am DLS registriert (siehe Abschnitt 15.3, “Registrieren von Workpoint-Software und -Dateien”).

Durchführen der Verteilung

1. Legen Sie zunächst fest, welche Workpoints Sie mit der Software versorgen möchten.
   Wählen Sie dazu den Bereich **Software Deployment** > **Workpoint Deployment** und tragen Sie ggf. Suchkriterien in der Ansicht **Suche** ein. Klicken Sie auf die Schaltfläche **Suche**, um die Suche zu starten.
2. Wenn ein oder mehrere Workpoints gefunden wurden, wird der erste Eintrag in der Ansicht **Objekt** angezeigt. Um mehrere Workpoints auszuwählen, wechseln Sie in die Ansicht **Tabelle** und selektieren Sie mit gedrückter <STRG>-Taste weitere einzelne Workpoints oder mit gedrückter <UMSCHALT>-Taste Workpoint-Bereiche.
3. Klicken Sie auf **Deploy**.

   HINWEIS: Durch Klick auf **Deploy** wird überprüft, ob für die gewählten Workpoints eine geeignete Software vorhanden, d. h. registriert ist.
   Ist dies nicht der Fall, wird eine entsprechende Meldung ausgegeben. Dies gilt auch für den Fall, dass in einer Mehrfachselektion sowohl IP Clients als auch unterschiedliche IP Phones (optiPoint, OpenStage) ausgewählt wurden.

Wurde passende Software gefunden, erscheint folgendes Dialogfenster (Beispiel):



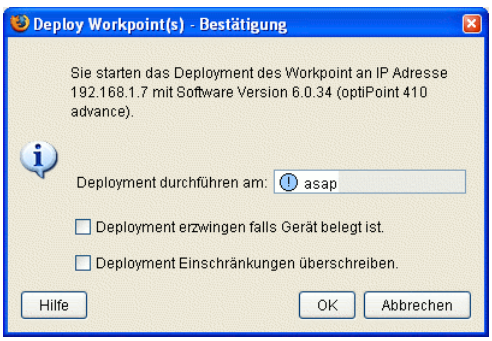
Ist ein Software-Image für diesen Workpoint-Typ nicht geeignet, so wird der Eintrag mit einem gelben Dreieck markiert und gegraut dargestellt. Wenn Sie den Mauszeiger über dieses Icon bewegen, erscheint ein ToolTip mit einer Begründung.
Beispielsweise sagt der ToolTip „Software nicht anwendbar für diesen Gerätetyp.“ aus, dass eine bestimmte registrierte HFA-Software nicht auf Unify HFA Workpoints verteilt werden kann.

WICHTIG: Mit der Checkbox **Aufheben der Einschränkung und Verteilung unabhängig des Gerätetyps** können Sie ein Software-Deployment auch für solche Workpoints durchführen, die aufgrund der Lizenzinformationen der Software nicht zu den Workpoints passen (siehe Abschnitt 15.3.2, “Verstehen der Lizenzinformationen bei IP Phone-Software”).
Dies ist in der Regel nur dann erforderlich, wenn Sie ein Deployment für einen neuen, dem DLS unbekannten Gerätetyp durchführen möchten.
Das Ergebnis kann der Verlust der gesamten Workpoint-Funktionalität sein.
Ist die Checkbox aktiviert, können alle, auch die bislang gegraut dargestellten Einträge der Liste ausgewählt werden.

4. Wählen Sie in der Werkzeugleiste eine **Ausführungszeit**. Klicken Sie hierzu auf das Kalendersymbol  aund wählen Sie eine der Optionen für den Zeitpunkt bzw. die Bedingungen des Deployments aus. Näheres zur Kalender-Schaltfläche siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”.

5. Wählen Sie den gewünschten Eintrag und klicken Sie auf die Schaltfläche **Deploy**, um den Durchführungszeitpunkt festzulegen.

6. Es erscheint ein Dialogfenster, in dem Sie die Software-Verteilung starten können. Per Voreinstellung wird die Software entsprechend den konfigurierten Restriktionen (siehe Abschnitt 6.3.2.7, “Register „SW Deployment Einschränkungen“”). Falls Sie **Deployment Einschränkungen überschreiben** aktivieren, werden diese Einschränkungen nicht beachtet.



7. Das Aktivieren von **Deployment erzwingen falls Gerät belegt ist** erzwingt eine nicht verzögerte Durchführung des Deployment-Vorganges, auch bei einem (durch einen Anruf) belegten Workpoint. Dies sollte nur in Ausnahmefällen aktiviert werden, da dabei eine Telefonverbindung am Workpoint unterbrochen wird..
8. Das Aktivieren von **Deployment Einschränkungen überschreiben** erzwingt ein Deployment, unabhängig von den ggf. konfigurierten Einschränkungen.
9. Klicken Sie auf **OK**. Wenn die Lizenzprüfung erfolgreich war, werden die einzelnen Jobs zur Verteilung an die selektierten Workpoints erzeugt, die zum angegebenen Zeitpunkt ausgeführt werden. Der Fortschritt der Job-Erzeugung ist anhand eines Balkens zu sehen (siehe Abschnitt 5.4.2.6, “Meldungsfenster”).

Mehr zum Thema Job-Koordination siehe Abschnitt 15.7, “Nutzen der Job-Koordination”.

15.6.2 Automatisches Deployment

Wie der Name schon sagt, können Sie Workpoint-Software zusätzlich zur manuellen Verteilung (siehe Abschnitt 15.6.1, “Manuelles Deployment”) auch automatisiert, d. h. ohne Benutzereingriff verteilen.

Wird ein Workpoint am DLS registriert, sei es durch manuelles Scannen (siehe Abschnitt 7.4.6, “IP Devices scannen”) oder durch erstmalige Registrierung eines Workpoints mit Software im neuen Format (mit DLS-Schnittstelle), so wird am DLS ein den Deployment-Regeln entsprechendes Deployment angestoßen.

Nachfolgend ist beschrieben, wie die Regeln konfiguriert werden, die dieses Verhalten steuern.

Voraussetzungen

- Eine laufende DLS-Infrastruktur (z. B. CLA-, DHCP-, DNS- und FTP-Server).
- Die zu versorgenden Workpoints haben sich beim DLS automatisch registriert oder wurden durch manuelles Scannen vom DLS gefunden (siehe Abschnitt 7.4.6, “IP Devices scannen”).
- Die zu verteilende Software wurde am DLS registriert (siehe Abschnitt 15.3, “Registrieren von Workpoint-Software und -Dateien”).

Deployment-Regel neu einrichten

1. Wählen Sie den Bereich **Software Deployment** > **Regeln bearbeiten** und klicken Sie auf die Schaltfläche **Neu**.
2. Wählen Sie im Feld **Gerätetyp** den Workpoint-Typ aus, für den die Regel gelten soll.

   HINWEIS: Pro Kombination aus Standort, Gerätetyp, Software-Typ und Software-Version kann nur eine Regel eingerichtet werden.
3. Wählen Sie im Feld **Standort** den Standort aus, für den die Regel gelten soll.
4. Wählen Sie im Feld **SW Typ** den Typ der Software aus, die aktuell auf den Workpoints installiert ist, für die die Regel gelten soll.
5. Wählen Sie im Feld **WP** SW Version die Version der Software aus, die aktuell auf den Workpoints installiert ist, für die die Regel gelten soll.
6. Aktivieren Sie ggf. **Deploy neueste SW Version**, wenn Sie möchten, dass nur dann ein Software-Deployment durchgeführt wird, wenn eine neuere Version zur Verteilung vorliegt, als die z. Zt. installierte Version. Beispiel: Die Version 5.1.9 wird auf Workpoints mit der Version 5.1.1 verteilt, während die Version 5.2.0 am Workpoint belassen wird.
7. Um eine ganz bestimmte Software-Version zu verteilen, müssen Sie **Deploy neueste SW Version** deaktivieren. Nur mit dieser Einstellung ist es möglich, die Änderung eines Softwaretypes der Workpoint-Software zu erzwingen.
   In diesem Fall wählen Sie im Feld **SW Image** und **SW Version** das gewünschte Software-Image in der verfügbaren Software-Version aus den Listen aus oder geben Sie Image und Version ein.
8. Klicken Sie auf **Sichern**, um die neue Regel zu speichern.

9. Klicken Sie auf **Anwenden**, um eine Auflistung aller Workpoints zu erhalten, auf die die Regel zutrifft. Es öffnet sich ein Dialogfenster, in dem Sie diejenigen Workpoints selektieren können, auf die die Regel tatsächlich angewendet werden soll. Bestätigen Sie anschließend mit **Anwenden** im Dialogfenster.

Wiederholen Sie den Vorgang für jede Regel, die Sie einrichten möchten.

Automatischer Ablauf der Verteilung

Eine automatische Softwareverteilung wird immer von Workpoint-Seite aus angestoßen.

Beim Registrieren eines Workpoints prüft der DLS zunächst, ob es eine Regel für den Gerätetyp des Workpoints gibt. Gibt es keine Regel, oder ist die Regel durch Abwahl von **Deploy Default-Software** deaktiviert, so erfolgt keine weitere Abarbeitung.

Ist die Verteilung der neuesten Software in der Regel aktiviert, so wird die neueste Software (Software mit der höchsten Software-Versionsnummer) auf alle Workpoints mit dem gleichen Softwaretyp verteilt. Workpoints mit davon abweichenden Softwaretypen erhalten keine neue Software.

Ist **Deploy neueste Version** deaktiviert, so bekommt jeder Workpoint die eingetragene Software, ohne Rücksicht auf die Softwareversion.

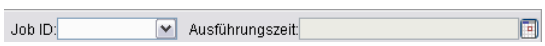
15.7 Nutzen der Job-Koordination

Im DLS werden alle Aufgaben mithilfe von Jobs geplant, abgearbeitet und protokolliert. Einzelne Jobs können aus mehreren Aktionen bestehen.

Jobs können Sie in den folgenden Bereichen einrichten:

- Standort
- Workpoint Interface Konfiguration
- Automatische SPE Konfiguration
- IP Phone Konfiguration
- IP Client Konfiguration
- IP Gateway Konfiguration
- IP Device Interaktion
- SIP Mobile User Konfiguration
- SIP Mobile User Interaktion
- Gateways
- Software Deployment

In diesen Bereichen können Sie in der Werkzeugleiste durch Eingabe eines Namens bei **Job ID** und Festlegen der Ausführungszeit (siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”) und Ausführungsart gezielt Konfigurations-, Deployment- und Interaktionsaufgaben bestimmten Jobs zuordnen.



Wurde ein Name vor dem Sichern eines Objektes festgelegt, erscheint dieser dann später bei **Job Kontrolle** zusätzlich zur Aktionsnummer. Durch manuelle Angabe einer **Job ID** können einzelne Aktionen zu Jobs gruppiert und dadurch eine größere Übersichtlichkeit hergestellt werden.

HINWEIS: Die Umstellung von Sommerzeit auf Winterzeit (eine Stunde zurück) führt nicht zu einem erneuten Ausführen eines Jobs, der in dem dadurch verdoppelten Zeitintervall gestartet wurde. Allerdings wird bei der Umstellung von Winterzeit auf Sommerzeit (eine Stunde vor) ein Job, der in die dadurch übersprungene Zeit fällt, nicht ausgeführt.

Eigenschaften zur Ausführung und Protokollierung von Jobs können Sie Konfigurieren (siehe Abschnitt 14.3, “Job Konfiguration”).

15.7.1 Festlegen eines Jobs

Das Festlegen eines Jobs geschieht durch das Eintragen einer **Job ID** in der Werkzeugleiste. Rechts neben der **Job ID** kann ein in der Zukunft liegender Zeitpunkt eingetragen werden. In diesem Fall werden die gewünschten Aktionen (z. B. Änderungen an IP Device-Parametern) nicht sofort, sondern zum angegebenen Zeitpunkt ausgeführt.

Um weitere Aktionen nicht mehr dem angegebenen Job zuzuordnen, wählen Sie bei **Job ID** einfach den leeren Eintrag aus der Auswahlliste. Ein festgelegter Zeitpunkt kann im Kalender-Dialogfenster durch Klick auf **Löschen** entfernt werden.

15.7.2 Eigenschaften und Status von Jobs ansehen

Zum Kontrollieren und Protokollieren von Jobs stehen Ihnen zwei Werkzeuge zur Verfügung.

Job Kontrolle

Mittels dieser Funktion können Sie umfangreiche Informationen zu den einzelnen Jobs ansehen, vorhandene Jobs abbrechen, löschen oder erneut aktivieren.

1. Wählen Sie den Bereich **Job Koordination** > **Job Kontrolle**.
2. Geben Sie ggf. Filterkriterien ein, um nur nach Jobs mit bestimmten Eigenschaften zu suchen. Sie können so z. B. Jobs heraussuchen, die zur Zeit aktiv, das heißt noch nicht abgearbeitet sind.
3. Klicken Sie auf die Schaltfläche **Suche**, um die Suche zu starten.

   Als Suchergebnis werden alle relevanten Daten zu jedem gefundenen Job bzw. Aktion angezeigt (siehe Abschnitt 14.1, “Job Kontrolle”).
4. Sie können ausgewählte Jobs bzw. Aktionen in der Ansicht **Objekt** und **Tabelle** löschen, das heißt vollständig entfernen. Dies kann sowohl vor als auch nach der Ausführung des Jobs geschehen.

   Durch **Job abbrechen** wird der Job nicht ausgeführt, bleibt aber in der Liste aller Jobs enthalten und wird auch bei **Job Statistik** weiter angezeigt.

   HINWEIS: Sie können jeden Job abbrechen, egal welchen Status er hat. Bei Jobs mit dem Status **fertig** haben Sie die Möglichkeit, durch das Abbrechen eine neue Ausführungszeit einzugeben. Dadurch können Sie den Job reaktivieren, d. h. erneut ausführen.

Täglicher Status

Diese Funktion dient zur übersichtlichen Anzeige aller Jobs in tabellarischer Form mit der Möglichkeit, nach Zeitraum und Job-Status zu filtern. Die hier angezeigten Jobs können auch gelöscht werden.

1. Wählen Sie den Bereich **Job Koordination** > **Täglicher Status**.
2. Grenzen Sie ggf. die Statistik durch Angabe eines Aktivierungsdatums und des Job-Status ein, um nur nach Jobs mit diesen Eigenschaften zu suchen.
3. Klicken Sie auf die Schaltfläche **Suche**, um die Suche zu starten.

   Als Suchergebnis werden Job ID, Job Status, Aktivierungszeit und Endzeit tabellarisch angezeigt (siehe Abschnitt 14.2, “Täglicher Status”).

   Sind mehrere Aktionen zu einer Job ID zusammengefasst, und mindestens eine Aktion hat den Status **Zeit überschritten**, **abgebrochen** oder **fehlgeschlagen**, so wird der gesamte Job mit diesem Status angezeigt.
4. Klicken Sie auf **Löschen**, um den Job vollständig zu entfernen. Sind mehrere Aktionen zu einer Job ID zusammengefasst, werden alle dazugehörigen Aktionen gelöscht.

15.8 Backup / Restore

Die Oberfläche des DLS-CLient bietet komfortable Möglichkeiten, automatisiert DLS-Daten zu sichern und Sicherungen wieder herzustellen.

15.8.1 Automatisierte Datensicherungen

Sie haben die Möglichkeit, automatisiert Sicherungen der gesamten DLS-Datenbank zu erstellen und diese wieder herzustellen. Darüber hinaus können Sie Backup-Protokolle ansehen.

15.8.1.1 Automatisches Backup einrichten

1. Wählen Sie den Bereich **Administration** > **Backup / Restore** > **Register „Backup“**.
2. Wenn noch nicht geschehen, geben Sie bei **Backup Pfad** den Pfad ohne Dateiname zum Sichern des Backups ein oder wählen Sie einen geeigneten Pfad mit Hilfe der Schaltfläche **Durchsuchen**. Mit einem Klick auf **Test** können Sie sofort die Verfügbarkeit des Pfades prüfen.
3. Ändern Sie bei **Max. Anzahl Backups** ggf. die maximale Anzahl der Backup-Dateien, die gesichert werden sollen. Bei Überschreiten der maximalen Anzahl wird die am längsten gesicherte Backup-Datei gelöscht.
4. Sie haben nun die folgenden Möglichkeiten, Backups zu organisieren:
   - Ein einmaliges Backup sofort durchführen.
     Klicken Sie dazu einfach auf die Schaltfläche **Backup jetzt starten**.
   - Ein einmaliges Backup zu einem festgelegten Zeitpunkt in der Zukunft durchführen.
     1. Geben Sie einen Zeitpunkt bei **Starte Backups an** ein (Kalender siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).
     2. Klicken Sie auf **Sichern**.
   - An einem, mehreren oder allen Wochentagen wiederkehrend ein Backup durchführen.
     1. Geben Sie einen Zeitpunkt bei **Starte Backups an** ein (Kalender siehe Abschnitt 5.4.2.4, “Zeitfeld mit Kalender-Schaltfläche und Ausführungsart”).
     2. Setzen Sie einen Haken bei **Tägliche Backups ausführen**.
     3. Setzen/Entfernen Sie die Haken bei **Tägliche Backups nur ausführen an** so, wie es Ihren Wünschen entspricht.
     4. Klicken Sie auf **Sichern**.

Die Backup-Datei wird mit dem Namen `dls_JJJJMMTT_HHMMSS.bak` im angebenen Verzeichnis angelegt.

15.8.1.2 Backup wiederherstellen

HINWEIS: Ein Restore der DLS-Datenbank setzt ein vorheriges Backup voraus, siehe Abschnitt 15.8.1.1, “Automatisches Backup einrichten”.
Handelt es sich bei der Rücksicherung um eine ältere Datenbank (geänderte Datenbank-Definition), führen Sie statt einem Restore bitte eine Migration durch (siehe Abschnitt 15.8.2.3, “Migration von DLS-Datenbankdaten”). Führen Sie die Migration auch durch, wenn Sie sich nicht sicher sind, ob die gesicherte Datenbank noch kompatibel ist.
Einige Serverkonfigurationen werden nie zurückgeladen, um das Laufen des DLS nach einem Restore sicherzustellen, z.B.
- den Account, mit dem der DLS lief
- die Lizenzeinstellungen.

1. Wählen Sie den Bereich **Administration** > **Backup / Restore** > **Register „Restore“**.
2. Geben Sie bei **Backup** den Namen des wiederherzustellenden Backups ein oder wählen Sie eine geeignete Datei mit Hilfe der Schaltfläche **Durchsuchen**. Mit einem Klick auf **Test** können Sie sofort die Verfügbarkeit der Datei prüfen.
3. Klicken Sie auf **Restore**, um die Rücksicherung zu starten.
4. In einem Dialogfenster wird abgefragt, ob Plug&Play nach Restore ausgeschaltet werden soll. Wenn Plug&Play ausgeschaltet wurde, kann es über **Administration** > **Server Konfiguration** > **P&P Einstellungen** > **Plug&Play eingeschaltet** wieder eingeschaltet werden. Dazu muss sichergestellt sein, dass alle IP Devices in der DLS-Datenbank registriert sind.

15.8.1.3 Sicherungen überwachen

1. Wählen Sie den Bereich **Administration** > **Backup / Restore** > **Register „Protokoll“**.
2. Klicken Sie auf **Aktualisieren**, um das Backup-Protokoll anzuzeigen. Informationen zum Zeitpunkt und Status der Sicherungen bzw. Rücksicherungen sowie der verwendeten Backup-Dateien werden aufgelistet. Mögliche Werte für Status der Sicherung/Rücksicherung: **Backup OK**, **Backup fehlgeschlagen**, **gelöscht**, **Restore OK**, **Restore fehlgeschlagen**.

15.8.2 Manuelle Datenbank-Manipulation

Hier erfahren Sie, wie Sie Daten der SQL-Datenbank des OpenScape DLS „von Hand“ manipulieren können. Die Daten werden auf dem PC abgelegt, auf dem auch der OpenScape Deployment Service, sprich der DLS-Server läuft.

> ***HINWEIS:*** Es wird dringend empfohlen, die automatische Backup / Restore-Funktion des DLS zu nutzen (siehe Abschnitt 15.8.1, “Automatisierte Datensicherungen”), da diese einfacher und sicherer ist.

Sie können:

- eine Sicherung aller Daten durchführen, siehe Abschnitt 15.8.2.1,
- gesicherte Daten wiederherstellen, siehe Abschnitt 15.8.2.2,
- eine Datenbanksicherung mit einer aktuellen Datenbank-Definition migrieren (zusammenführen), siehe Abschnitt 15.8.2.3,
- die Datenbank zurücksetzen (alle Datenbankdaten löschen), siehe Abschnitt 15.8.2.4.

15.8.2.1 Sicherung von DLS-Datenbankdaten

Um die SQL-Datenbank des DLS-Servers zu sichern, gehen Sie wie folgt vor.

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Stop Service**.
3. Sichern Sie das Verzeichnis **[Installationspfad]\DeploymentService\DB** komplett mit Unterverzeichnissen, indem Sie das folgende Kommando ausführen:

   ```
   [Installationspfad]\DeploymentService\Tomcat5\webapps\
   DeploymentService\database\dbexport.bat <filename>.zip
   ```

4. Starten Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Start Service**.

15.8.2.2 Wiederherstellungvon DLS-Datenbankdaten

> ***HINWEIS:*** Ein Restore der DLS-Datenbank setzt ein vorheriges Backup voraus, siehe Abschnitt 15.8.2.1, “Sicherung von DLS-Datenbankdaten”.
>
> Handelt es sich bei der Rücksicherung um eine ältere Datenbank (geänderte Datenbank-Definition), führen Sie statt einem Restore bitte eine Migration durch (siehe Abschnitt 15.8.2.3, “Migration von DLS-Datenbankdaten”). Führen Sie die Migration auch durch, wenn Sie sich nicht sicher sind, ob die gesicherte Datenbank noch kompatibel ist.

HINWEIS: Einige Serverkonfigurationen werden nie zurückgeladen, um das Laufen des DLS nach einem Restore sicherzustellen, z.B.

- den Account, mit dem der DLS lief
- die Lizenzeinstellungen.

Gehen Sie beim Wiederherstellen einer gesicherten Datenbank ähnlich vor, wie beim Backup beschrieben.

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Stop Service**.
3. Importieren Sie die DLS-Daten, indem Sie folgendes Befehl ausführen:

   ```
   [Installationspfad]\DeploymentService\Tomcat5\webapps\
   DeploymentService\database\dbimport.bat <filename>.zip
   ```

4. Starten Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Start Service**.

15.8.2.3 Migration von DLS-Datenbankdaten

Mit „Migration“ ist in diesem Fall gemeint, dass Sie eine gesicherte Datenbank wiederherstellen können, obwohl sich die Datenbank-Definition inzwischen geändert hat. Die Datenbank-Definition kann sich im Verlauf der Zeit z. B. dadurch ändern, in dem Konfigurationsparameter der Workpoints hinzugefügt werden.

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Stop Service**.
3. Um die Migration durchzuführen, führen Sie das folgende Kommando aus:

   ```
   [Installationspfad]\DeploymentService\Tomcat5\webapps\
   DeploymentService\database\migrate.bat <exportfilename>.zip
   ```

   Die Datei `<exportfilename>` muss durch Backup von DLS-Datenbankdaten (siehe Abschnitt 15.8.2.1, “Sicherung von DLS-Datenbankdaten”) erzeugt worden sein.

4. Starten Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Start Service**.

15.8.2.4 Reset der DLS-Datenbank

Sie können die DLS-Datenbank zurücksetzen, das heißt, alle Daten löschen. Dies führt, was die Daten der Datenbank betrifft, zum gleichen Ergebnis wie eine Deinstallation (Abschnitt 4.14, “Deinstallation des OpenScape Deployment Service”) und erneute Installation der kompletten DLS-Anwendung.

WICHTIG: Bei einem Reset werden alle Daten der DLS-Datenbank gelöscht.
Um einen Datenverlust zu vermeiden, erstellen Sie vor dem Reset ein Backup der Datenbank, siehe Abschnitt 15.8.2.1, “Sicherung von DLS-Datenbankdaten”.

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Stop Service**.
3. Löschen Sie die Datenbank, indem Sie die folgenden Kommandos ausführen:
   - `cd[Installationspfad]\DeploymentService\Tomcat5\webapps\DeploymentService\database`
   - `dbinstall.bat delete`
4. Erstellen Sie eine neue Datenbank, indem Sie die folgenden Kommandos ausführen:
   - `cd[Installationspfad]\DeploymentService\Tomcat5\webapps\DeploymentService\database`
   - `dbinstall.bat create <Passwort>`
     `Mit <Passwort>` wird das Passwort für die Benutzerkennung „admin“ festgelegt.
5. Starten Sie den Dienst *DeploymentService* am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Start Service**.

15.8.2.5 Behebung: Lizenzagent ist nicht erreichbar

Ist der DLS aufgrund von Verbindungsproblemen mit dem Lizenzagenten nicht mehr aufrufbar, kann ein anderer Lizenzagent in die DLS-Datenbank eingetragen werden. Dies geschieht in den folgenden Schritten:

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Dienst „DeploymentService“ am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Programme** > **Deployment Service** > **Stop Service**.
3. Führen Sie das zur jeweils gewünschten Aktion gehörige Kommandos aus:
   - zur Änderung des Lizenzagenten:
     ```
     [Installationspfad]\DeploymentService\Tomcat5\webapps\
     DeploymentService\database\dbinstall.bat setcla <hostname> <port>
     ```
   - zur Änderung des Lizenzmanagers:
     ```
     [Installationspfad]\DeploymentService\Tomcat5\webapps\
     DeploymentService\database\dbinstall.bat setclm <hostname> <port>
     ```
   - wenn sich mehrere DLS einen Lizenzagenten teilen:
     ```
     [Installationspfad]\DeploymentService\Tomcat5\webapps\
     DeploymentService\database\dbinstall.bat setmaxbasicdevices <Anzahl Devices>
     [Installationspfad]\DeploymentService\Tomcat5\webapps\
     DeploymentService\database\dbinstall.bat setmaxmobileusers
     <Anzahl Mobile User>
     ```
   - um CLA/CLM-Werte festzulegen:
     ```
     [Installationspfad]\DeploymentService\Tomcat5\webapps\
     DeploymentService\database\dlslicense.bat setclm <IP von CLM> <CLM-Port>
     setcla <IP von CLA> <CLM-Port>
     z. B.
     dlslicense.bat setclm 10.6.25.11 8819 setcla 10.6.25.15 61740
     ```

     HINWEIS: Falls die CLM/CLA-Einrichtung mit dem oben genannten Befehl nicht funktioniert, sollten Sie denselben Befehl für CLA und CLM separat ausführen:
     - `dlslicense.bat setclm 10.6.25.11 8819`
     - `dlslicense.bat setcla 10.6.25.15 61740`

4. Starten Sie den Dienst „DeploymentService“ am DLS-Server. Klicken Sie hierzu im WindowsStartmenü auf **Programme** > **Deployment Service** > **Start Service**.

15.8.3 DLS-Wiederherstellungspunkt

Erstellen Sie einen DLS-Wiederherstellungspunkt, um die DLS-Software und den Zustand der Datenbank zu speichern, um zu einem späteren Zeitpunkt wieder darauf zugreifen zu können. Diese Funktion unterstützt nur einen einzigen (1) Wiederherstellungspunkt. Software, Datenbank und Registry können bei Bedarf gesichert und wiederhergestellt werden.

So erstellen Sie einen DLS-Wiederherstellungspunkt :

1. Gehen Sie zu `C:<Program Files>\DeploymentService\tools` und führen Sie `DlsSync.bat` aus. Dieser Befehl sichert den aktuellen Zustand der DLS-Software und der Datenbank. Beim Einsatz von entfernten Datenbanken müssen Sie als ersten Parameter vor der Ausführung von `DlsSync.bat` auch ein Datenbank-Backup-Verzeichnis angeben (normalerweise eine Netzwerkfreigabe).

So kehren Sie zu einem DLS-Wiederherstellungspunkt zurück:

1. Gehen Sie zu `C:<Program Files>\DeploymentService\tools` und führen Sie `DlsRestore.bat` aus. Dieses Kommando stellt den Zustand der DLS-Software und der Datenbank anhand des zuvor erstellten Wiederherstellungspunktes wieder her. Beim Einsatz von entfernten Datenbanken müssen Sie als ersten Parameter vor der Ausführung von `DlsSync.bat` auch ein Datenbank-Backup-Verzeichnis angeben (normalerweise eine Netzwerkfreigabe).

HINWEIS: Nur ein einziger (1) DLS-Wiederherstellungspunkt wird unterstützt. Wenn Sie versuchen, einen DLS-Wiederherstellungspunkt zu erstellen und es existiert bereits ein älterer Wiederherstellungspunkt, wird der ältere Wiederherstellungspunkt gelöscht und der neue Wiederherstellungspunkt wird erstellt.

HINWEIS: Wenn Sie ein DLS-Upgrade anstoßen, erstellt das Installationsprogramm automatisch einen DLS-Wiederherstellungspunkt und löscht dabei alle zuvor erstellten Wiederherstellungspunkte.

HINWEIS: Um das Upgrade zu beschleunigen und die duplizierten Datenmengen zu reduzieren, sollten Administratoren die DLS-Tracedaten löschen (oder, falls eine Kopie benötigt wird, diese außerhalb des DLS-Pfades verschieben und dort pflegen) und jegliche generierte Headdump-bezogene Dateien (heapdump.<data>.<id>.phd, javacore.<data>.<id>.txt, Snap.<data>.<id>.trc) von `<DLS-Installationspfad>\Tomcat5\bin` in einen externen Pfad kopieren.

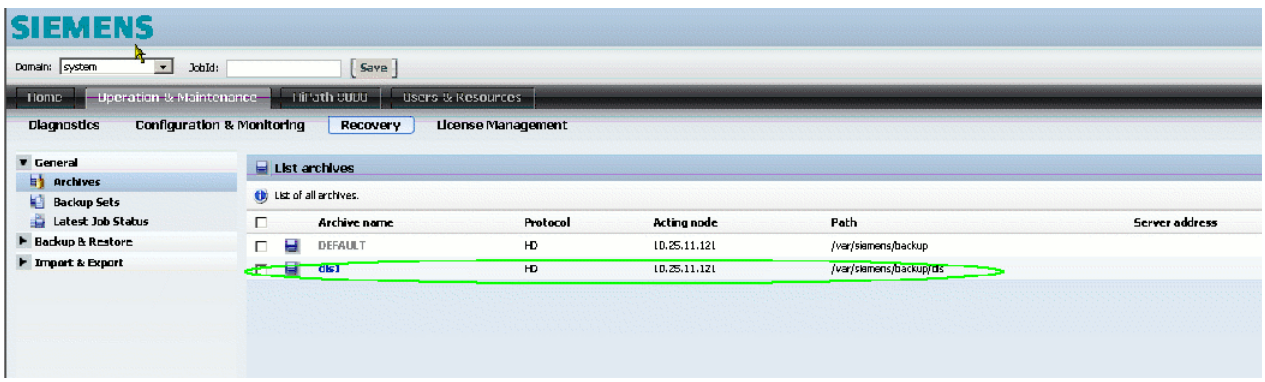
HINWEIS: Aufgrund von Microsoft SQL Servereinschränkungen können bei Bereitstellungen mit aktiver Datenbankspiegelung keine Wiederherstellungen durchgeführt werden.
Wenn in solchen Fällen bei Bereitstellungen mit entfernter Datenbank ein Upgrade durchgeführt wird, erscheint zu Beginn des Upgrades ein Popup-Fenster mit der Aufforderung, die Spiegelung zu entfernen und den Vorgang zu wiederholen (**retry**), den Vorgang abzubrechen (**abort**) oder ohne Rollback-Funktion weiterzumachen (**ignore**).
Wenn zu diesem Zeitpunkt die Spiegelung aktiviert ist, kann keine Wiederherstellung durchgeführt werden.

15.9 Backup & Restore auf OpenScape Voice und Linux Standalone-Installationen

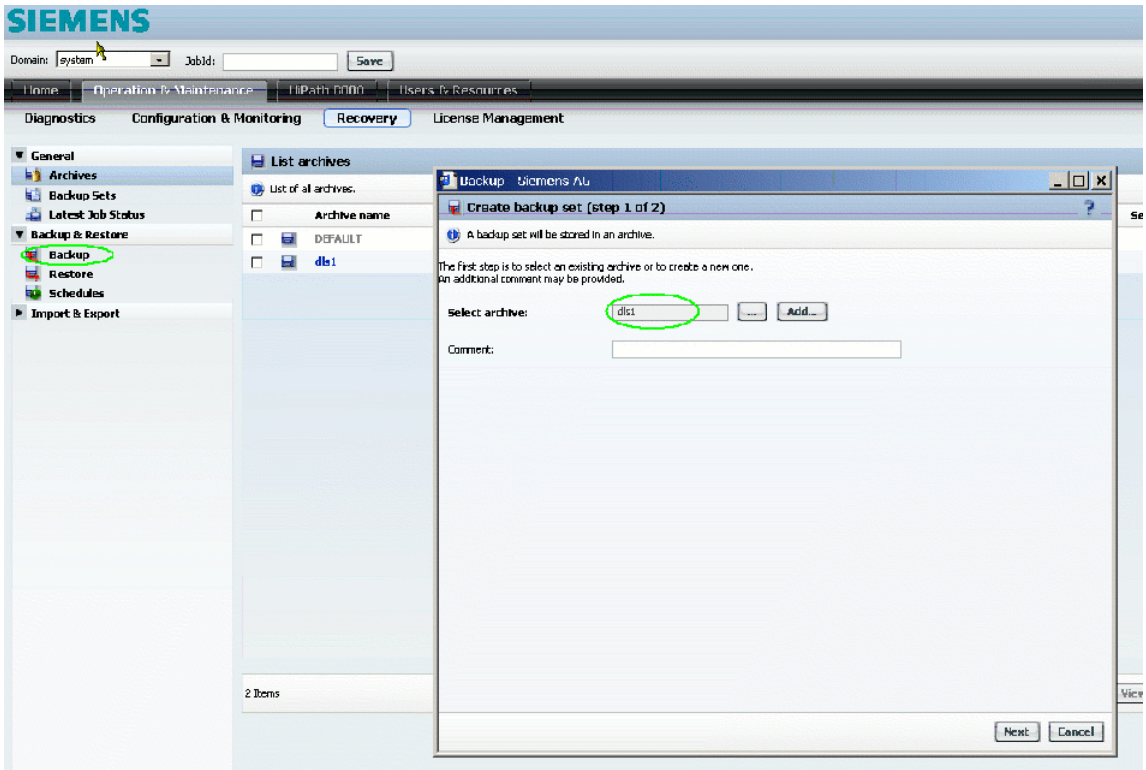
Dieses Kapitel beschreibt die Sicherung und Wiederherstellung (Backup & Restore) der DLS-Datenbank für die OpenScape Voice onboard-Version und für die Linux Standalone-Version.

15.9.1 Backup

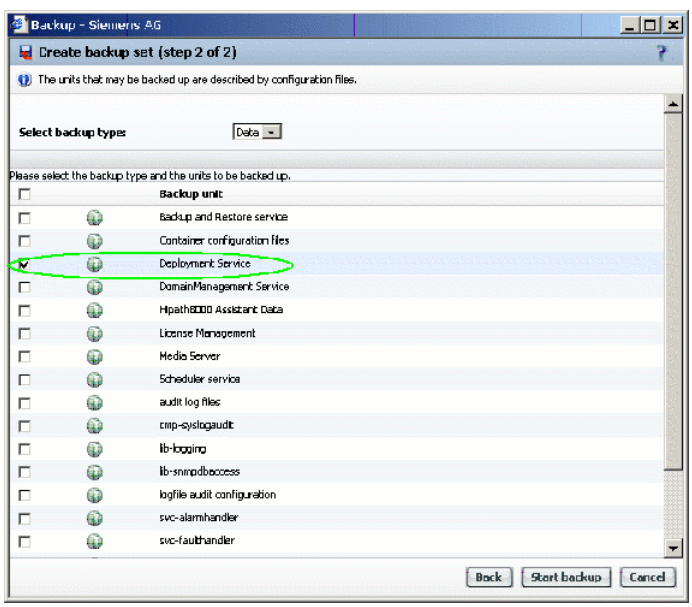
1. Melden Sie sich an der **Common Management Platform** an. Sie erreichen die Common Management Platform unter
   `https://<IP des Servers>`
2. Gehen Sie auf **Operation & Mainentance** > Register **„Recovery“**. Erstellen Sie ein Archiv für DLS-Backups, z. B. in `/var/siemens/backup/dls`.



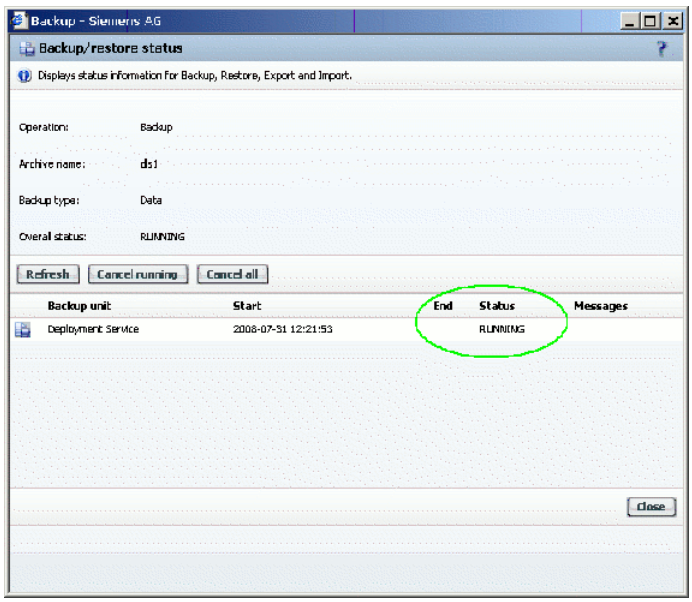
3. Um ein Backup zu erstellen, öffnen Sie zunächst den Ordner **Backup & Restore** und klicken Sie auf **Backup**. Wählen Sie im Fenster **Backup** im Feld **Select archive** das neu erstellte Archiv aus.



4. Als **Backup unit** wählen Sie **Deployment Service**. Anschließend klicken Sie auf **Start backup**.

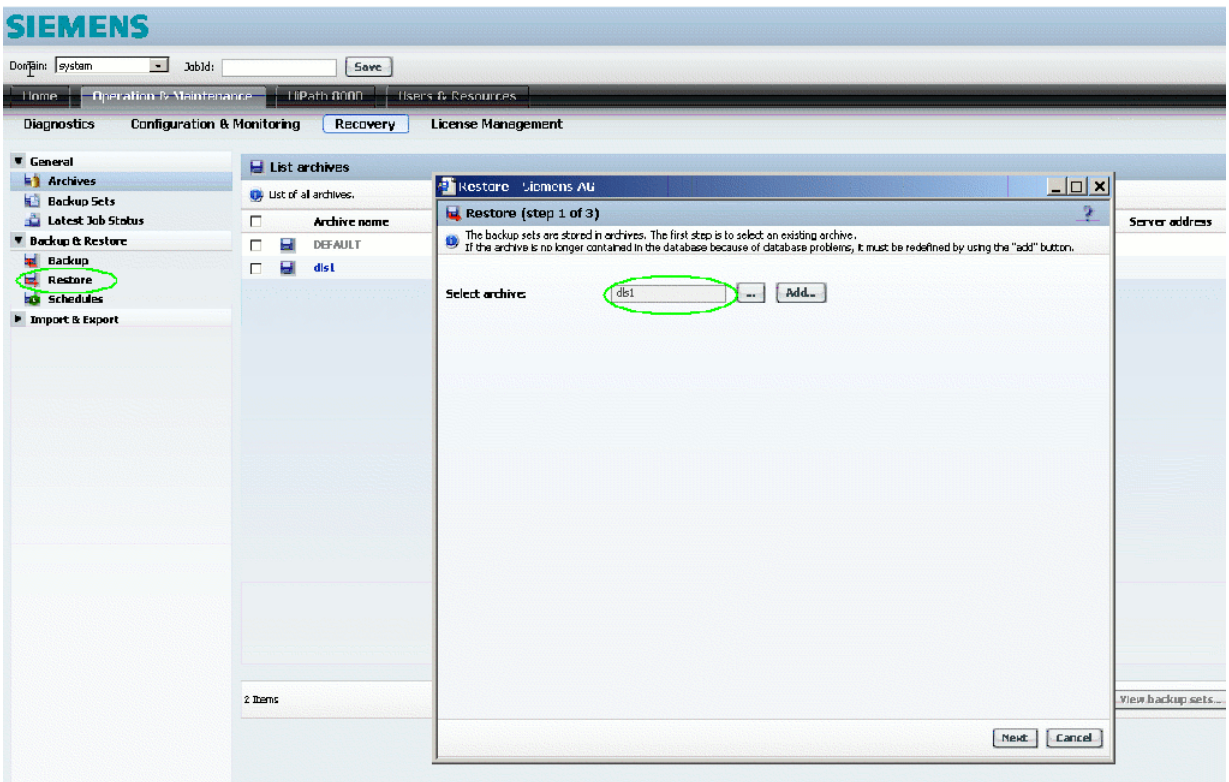


5. Warten Sie, bis sich der Wert von **Status** von **RUNNING** zu **OK** ändert.

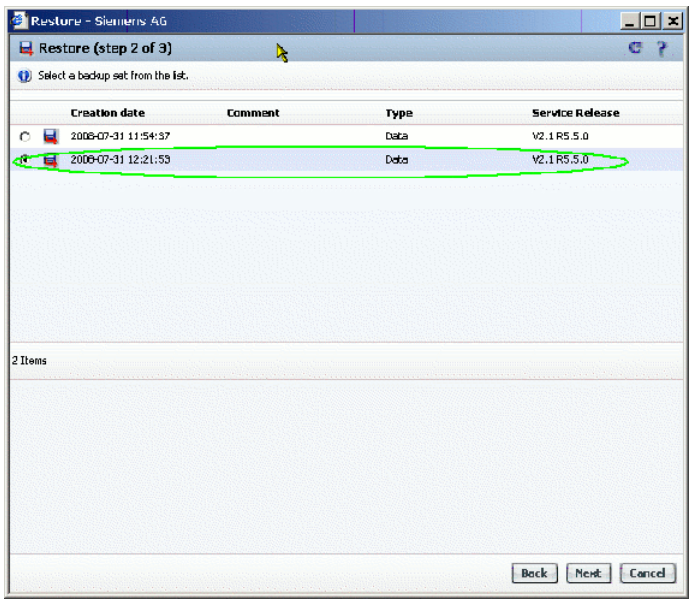


15.9.2 Wiederherstellung (Restore)

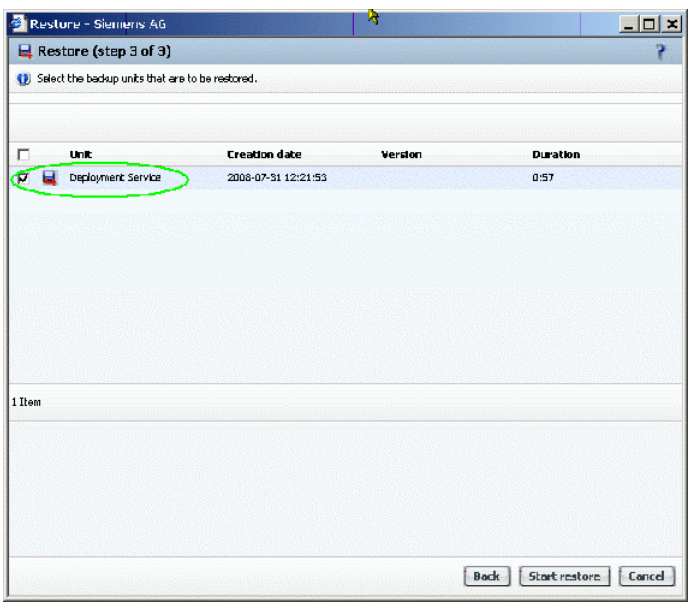
1. Um eine Datenbank wiederherzustellen, öffnen Sie zunächst den Ordner **Backup & Restore** und klicken Sie **Restore**. Im **Restore**-Fenster, im Feld **Select archive**, wählen Sie dasjenige Archiv, das das gewünschte Backup enthält, und klicken Sie **Next**.



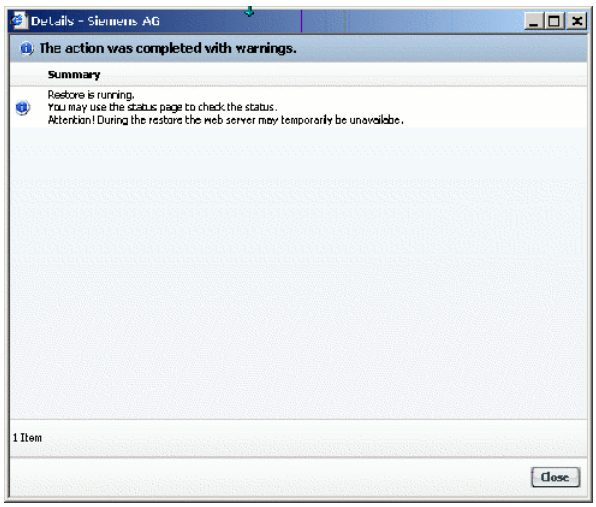
2. Wählen Sie das gewünschte Backup aus der Liste. Die Backups sind anhand eines Zeitstempels oder eines optionalen Kommentars identifizierbar. Klicken Sie auf **Next**.



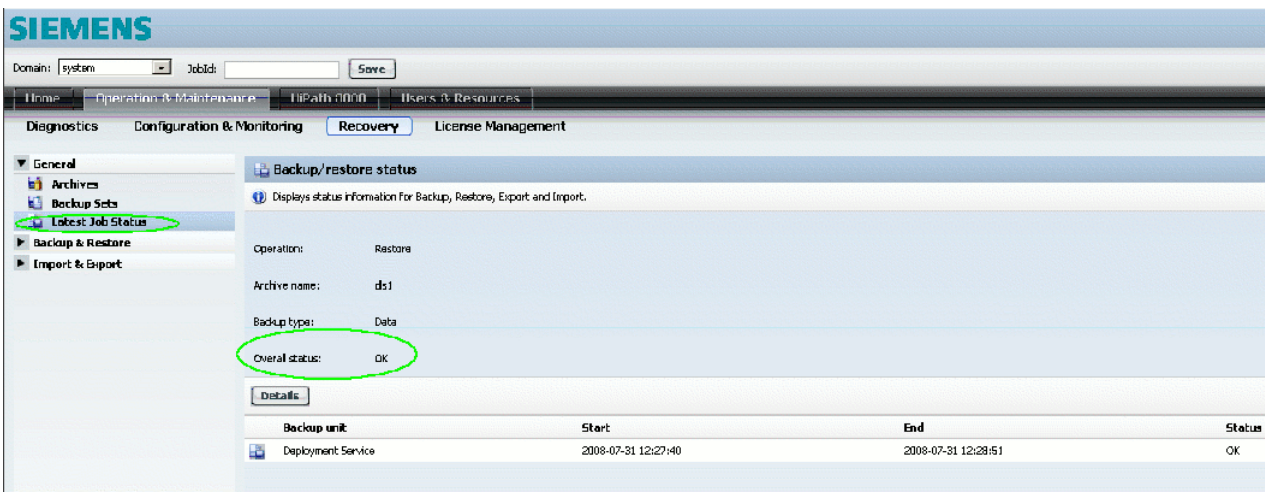
3. Unter **Unit** wählen Sie **Deployment Service** und klicken **Start restore**.



4. Sie erhalten ein Bestätigungsfenster. Da dieses Fenster nicht automatisch aktualisiert wird, können Sie es jederzeit schließen.



5. Um den Status des Wiederherstellungsvorgangs zu überprüfen, verwenden Sie das Fenster **Latest Job Status**.



15.9.3 Nach der Wiederherstellung

Nach einer erfolgreichen Wiederherstellung sind noch die folgenden manuellen Schritte vorzunehmen; hierzu werden Shell-Kommandos am Server eingegeben.

1. Melden Sie sich am Linux-Server oder an der OpenScape Voice an (für OpenScape Voice-Cluster: an beiden Knoten).
2. Stoppen Sie den DeploymentService:
   `sh /etc/init.d/symphoniad stop TomcatServletContainer`

   OpenScape Voice-Cluster: Nehmen Sie diesen Schritt auf beiden Knoten vor.
3. Passen Sie die DLS-Datenbank dem aktuellen Layout an. Der Kommandopfad variiert je nach Plattform.

   Auf Linux Standalone:

   ```
   cd /opt/siemens/share/tomcat/webapps/DeploymentService/database
   sh dbinstall.sh update
   ```

   Auf der OpenScape Voice:

   ```
   cd /enterprise/share/tomcat/webapps/DeploymentService/database
   sh dbinstall.sh update
   ```

   Auf einem OpenScape Voice-Cluster müssen Sie diesen Schritt nur auf demjenigen Knoten vornehmen, auf dem sich die PRIMARY-Datenbank befindet. Sie können das Ergebnis mit dem folgenden Kommando überprüfen:

   ```
   su - srx -c "RtpSolid -l"
   ```

Starten Sie den DeploymentService:

```
sh /etc/init.d/symphoniad start TomcatServletContainer
```

Auf einem OpenScape Voice-Cluster nehmen Sie diesen Schritt auf beiden Knoten vor.

15.10 Automatische Wiederherstellung bei fehlerhaftem Upgrade

Aufgrund der DLS-eigenen Struktur, der Vielzahl möglicher Bereitstellungsszenarien und der Möglichkeit zur kundenspezifischen Anpassung des Basis-Betriebssystem, stellen Software-Upgrades eine Verwaltungsaufgabe dar, die mit relativ hohen Risiken verbunden ist. Bis vor kurzem war es noch so, dass nach fehlerhaften Upgrades das Kundensystem nicht mehr funktionierte. Um dies zu korrigieren waren manuelle Eingriffe nötig. DLS musste neu installiert und die Datenbank anhand einer Sicherung wiederhergestellt werden.

Nun versetzt der DLS-Installer das System bei einem fehlerhaften Upgrade vor Durchführung des Upgrades automatisch wieder in einen betriebsfähigen Zustand. Diese Funktion ist nur für DLS-Bereitstellungen unter Microsoft Windows verfügbar. Unter Linux ist die DLS-Bereitstellung aufgrund der Abhängigkeit vom Symphonia-Framework und dem DVD-Bereitstellungsmechanismus leider nicht verfügbar.

HINWEIS: Wenn die Wiederherstellung fehlschlägt, wird der Benutzer durch den Installer dementsprechend benachrichtigt, und der Installationsvorgang wird beendet. Das System befindet sich dann in einem nicht definierten Zustand und der Benutzer sollte sich an den Support wenden, um das Problem beheben zu lassen.

HINWEIS: Nach einer erfolgreichen Wiederherstellung werden die Software und das Datenbank-Backup nicht gelöscht, sodass Kunden das System später gegebenenfalls wieder auf einen früheren Zustand zurücksetzen können (siehe Abschnitt 15.8.3, “DLS-Wiederherstellungspunkt”).

15.11 Import und Export von Plug&Play-Daten

Im Folgenden wird beschrieben, wie die Plug&Play-Daten von Workpoints als Datei im Format CSV exportiert und importiert werden können.

15.11.1 Export von Plug&Play-Daten

Mit den folgenden Schritten werden die Plug&Play-Daten von bestimmten Workpoints in eine CSV-Datei auf dem DLS-Server abgelegt

HINWEIS: Falls bereits eine Datei mit dem angegebenen Namens existiert, wird sie überschrieben.

1. Wählen Sie den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration**.
2. Suchen und selektieren Sie die Workpoints, für die Sie Plug&Play Daten exportieren möchten und klicken Sie auf **Datei exportieren**.
3. Geben Sie im folgenden Dialog den Namen der Exportdatei auf dem Server an und bestätigen Sie mit **Speichern**.
4. In einem Meldungsfenster erscheint die Bestätigung, dass der Export erfolgreich durchgeführt, oder ggf. eine Fehlermeldung.

15.11.2 Import von Plug&Play-Daten

Mit den folgenden Schritten werden Plug&Play-Daten aus einer CSV-Datei in den DLS importiert. Die detaillierten Ergebnisse des Importes, d. h. welche Workpoints neu angelegt, welche geändert wurden oder bei welchen Fehler auftraten, können der Protokolldatei entnommen werden. Sie wird unter **Administration** > **Protokoll-Daten** > **P&P Import Protokolle** angezeigt.

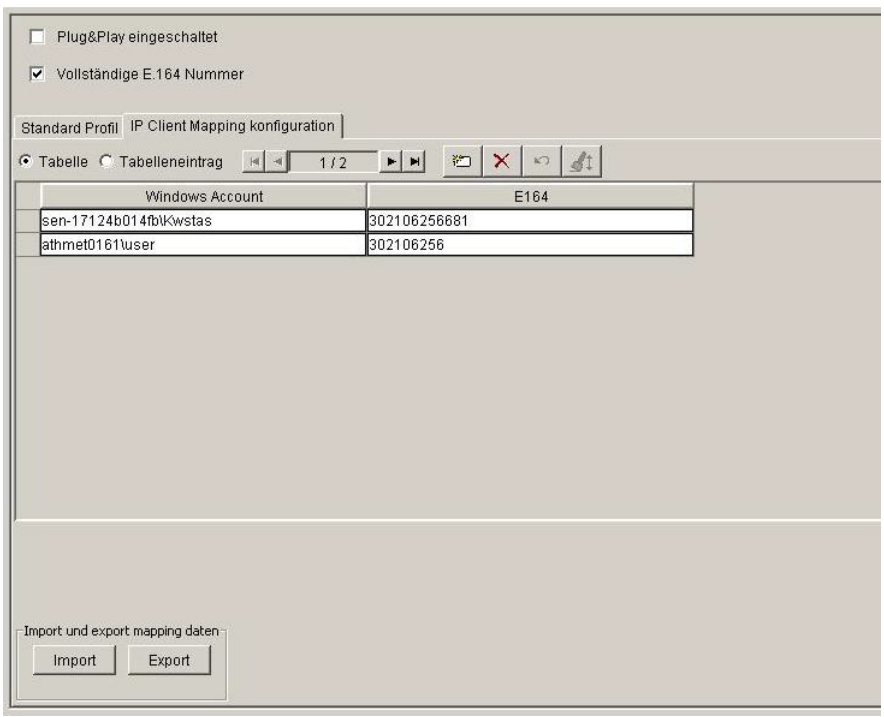
1. Wählen Sie den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration**.
2. In der Suchansicht klicken Sie auf **Datei importieren**.
3. Geben Sie im folgenden Dialog den Namen der zu importierenden CSV-Datei an. In diesem Dialog können Sie auch angeben, ob beim Import erstellte Workpoints als IP-Telefone und/oder als IP-Clients erstellt werden sollen. Bestätigen Sie den Dialog danach mit **Öffnen**.
4. Am Client erscheint im Meldungsfenster die Bestätigung, dass der Import durchgeführt wurde und in welcher Protokolldatei die Ergebnisse des Importes hinterlegt wurden.

15.11.3 Plug&Play-Daten über OpenScape Desktop-Clients

OpenScape Desktop-Clients müssen mit Bezug auf virtuelle DLS-Device-Datensätze eingerichtet werden, um die IP-Adresse des DLS für den Verbindungsaufbau zum DLS nutzen zu können.

Nachfolgend wird beschrieben, wie Plug&Play-Daten vom DLS verarbeitet werden, wenn der OpenScape-Client ausgeführt wird.

1. Gehen Sie zu **Administration** > **Server Konfiguration** > **P&P Einstellungen** > **Register „IP Client Mapping Konfiguration“**
2. Bereiten Sie eine .csv-Datei vor, indem Sie auf das Symbol **Eintrag hinzufügen** klicken.



HINWEIS: Klicken Sie auf das Symbol , um den Eintrag ggf. zu löschen.

HINWEIS: Klicken Sie auf das Symbol , um einzelne Einträge nacheinander hinzuzufügen.

3. Verwenden Sie die Ansicht **Ausgewählter Eintrag**, um Mapping-Daten für einen Windows PE/WE-Client zu importieren.
4. Geben Sie im Textfeld Windows Account die jeweilige Domäne/ das Windows-Account des Client ein.
5. Geben Sie im Textfeld E.164 die Nummer für diesen Client ein.
6. Klicken Sie im Feld **Import und export mapping daten** auf die Schaltfläche **Import**. Wählen Sie die gerade bearbeitete .csv-Datei aus.
7. Klicken Sie auf **Speichern**.
8. Überprüfen Sie in der Ansicht **Tabelle**, ob der Import erfolgreich war.

9. Melden Sie sich beim PE-Client (OpenScape Desktop Client Personal Edition) bzw. beim WE (Web Embedded)-Client mit dem Windows Account aus dem vorherigen Mapping an.

   HINWEIS: Dem Teilnehmer wird die angegebene E.164-Rufnummer zugewiesen.

15.11.4 Syntax der .csv-Dateien

Die für Import und Export von Plug&Play-Daten verwendete .csv-Datei hat folgenden Aufbau:

- 1. Zeile: Beschreibung des Spalteninhalts in vorgegebener Reihenfolge.
- 2. und weitere Zeilen: Kommando und die entsprechenden Parameter.

Wird ein Parameter nicht benötigt, muss ein ';' gesetzt werden, um einen leeren Parameter zu kennzeichnen.

Leere Zeilen und Zeilen, die mit einem '#' beginnen, werden ignoriert.

Falls eine virtuelle ID verwendet wird (keine MAC-Adresse) wird ein zweiter Versuch ignoriert und in der Protokolldatei dokumentiert. Wenn verschiedene MAC-Adressen verwendet werden, können mehrere Geräte mit der gleichen E.164 Nummer erzeugt werden.

HINWEIS: Es muss zuerst ein Gerät eingerichtet werden, bevor Keys und Keysets geändert werden können.

HINWEIS: Dieses Format wird ab DLS Version V2R2 unterstützt. Ältere Formate werden weiterhin unterstützt, wobei alle Devices als IP Phones importiert werden. Sollen IP Clients importiert werden, muss in das beschriebene Format konvertiert werden.

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.10, "Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen".

15.11.4.1 SIP Phone erzeugen (CreateSIPPhone)

Syntax des Kommandos, um ein SIP Phone zu erzeugen:

```
CreateSIPPhone;<DeviceID>;<e164 number>;<IP Phone Type>;<Software Type>;<Software Version>;<Device Profile>;<Remark>;<Basic Profile>;<Restore Basic Profile after Workpoint Reset>;<Terminal Name>;<Display ID>;<SIP User ID>;<SIP Password>;<SIP Realm>;<SIP Server Addr.>;<SIP Server Port>;<SIP Registrar Addr.>;<SIP Registrar Port>;<SIP Routing>;<SIP Gateway Addr.>;<SIP Gateway Port>;<Cloud Pin code>;<Secure Mode Required>;<PIN Mode>;
```

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.10, "Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen".

Beispiel:

```
CreateSIPPhone;00:1A:E8:34:4F:BE;302109998062;OpenStage 80;Siemens SIP;V3 R0.61.0;;;;false;302109998062;302109998062;;;;10.11.221.54;5060;10.11.221.54;5060;0;;5060;;true; Individual PIN;
```

15.11.4.2 HFA Phone erzeugen (CreateHFAPhone)

Syntax des Kommandos, um ein SIP Phone zu erzeugen:

```
CreateHFAPhone; <DeviceID>;<e164 number>;<IP Phone Type>;<Software Type>;<Software
Version>;<Device Profile>;<Remark>;<Basic Profile>;<Restore Basic Profile after
Workpoint Reset>;<Subscriber Number>;<Gatekeeper>;<Gatekeeper Password>;<Subscriber
Number (Standby)>;<Gatekeeper (Standby)>;<Gatekeeper Password (Standby)>
```

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.10, “Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen”.

Beispiel:

```
CreateHFAPhone;00:01:E3:25:E2:19;498972221456;OpenStage 80;Siemens HFA;V1
R0.0.93;;;;false;21456;218.1.16.211;;;;;
```

15.11.4.3 SIP Client erzeugen (CreateSIPClient)

Syntax des Kommandos, um ein SIP Phone zu erzeugen:

```
CreateSIPClient;<DeviceID>;<e164 number>;<IP Client Type>;<Software Type>;<Software
Version>;<Device Profile>;<Remark>;<Basic Profile>;<Restore Basic Profile after
Workpoint Reset>;<Terminal Name>;<SIP User ID>;<SIP Password>;<SIP Realm>;<SIP
Server Addr.>;<SIP Registrar Addr.>;<SIP Registrar Port>;<SIP Gateway Addr.>;<SIP
Gateway Port>;
```

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.10, “Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen”.

Beispiel:

```
CreateSIPClient;00:19:99:03:5B:0E;498972221458;optiClient 130;
Siemens oC-Bundle;5.1.182.0000;;;;;;;;218.1.16.211;218.1.16.211;5060
;;5060;;
```

15.11.4.4 HFA Client erzeugen (CreateHFAClient)

Syntax des Kommandos, um einen HFA Client zu erzeugen:

```
CreateHFAClient; <DeviceID>;<e164 number>;<IP Client Type>;<Software
Type>;<Software Version>;<Device Profile>;<Remark>;<Basic Profile>;<Restore Basic
Profile after Workpoint Reset>;<Subscriber Number>;<Gatekeeper>;<Gatekeeper
Password>;<Subscriber Number (Standby)>;<Gatekeeper (Standby)>;<Gatekeeper Password
(Standby)>
```

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.10, “Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen”.

Beispiel:

```
CreateHFAClient;00:19:99:03:5B:0E;498972221458;optiClient 130;
Siemens oC-Bundle;5.1.182.0000;;;;;21458;;;;;;
```

15.11.4.5 IP Gateway erzeugen (CreateIpGateway)

Syntax des Kommandos, um einen IP Gateway zu erzeugen:

```
CreateIpGateway; <DeviceID>;<IP Gateway Type>;<Software Type>;
<Software Version>;<Device Profile>;<Remark>
```

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.10, “Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen”.

Beispiel:

```
CreateIpGateway;139.21.93.205;HG1500;Siemens CGW;HXG_V7_R0.215.4;;;
```

15.11.4.6 Tastenbelegung ändern (ModifyKey)

Dieses Kommando erlaubt das Anlegen oder Ändern der Gerätetastenkonfiguration. Es kann jede Gerätetaste gesetzt werden, abhängig von Typ, Software und Version des IP Phones. Mit dem Reset-Parameter können alle Tastenfunktionen gelöscht werden, bevor sie neu gesetzt werden. Ist das Feld leer, bleiben die bestehenden Tastenbelegungen unverändert.

Syntax:

```
ModifyKey;<reset>;<e164 number>|deviceId=<deviceId>;
<key function>;<level>;<module>;<key-number>[;<name>=<value>]+
```

HINWEIS: Der Defaultwert ist `e164`. Soll eine Device ID verwendet werden, muss `deviceId=<deviceId>` geschrieben werden.

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.11, “Parameterbeschreibung für Tastenbelegung ändern, Keyset ändern”.

Beispiele

1. Ein OptiPoint 410 advance soll eine Taste zur Kontrolle des Kopfhörer erhalten:
   `ModifyKey;false;218116231;024;001;0;1;locked-function-keys=false;`
   Alternativ kann anstelle der Funktionsnummer (hier 024) auch die UI Bezeichnung „headset“ zur Definition der Tastenfunktion verwendet werden. Es dürfen nur die englischen Bezeichnungen für key function und name verwendet werden!

2. Das Einrichten einer Direktruftaste (DSS) benötigt 2 Schritte:
   1. Einrichten einer Primärleitung
   `ModifyKey;false;218116230;line;000;0;1;`
   `line-sip-uri=49897223500;line-primary=true;`
   2. Einrichten der Direktruftaste
   `ModifyKey;false;218116230;dss;000;0;3;line-sip-uri=498972233439`
3. Um eine Funktionstaste zu löschen, wird die Tastenfunktion auf „Key Unused“ gesetzt. Im folgenden Beispiel wird Taste Nr. 3 gelöscht:
   `ModifyKey;false;218116232;Key Unused;0;0;3`

15.11.4.7 Keyset ändern (ModifyKeyset)

Die Werte eines Keysets können geändert werden. Mit dem Reset-Parameter können alle Tastenfunktionen gelöscht werden, bevor sie neu gesetzt werden. Ist das Feld leer, bleiben die bestehenden Keysetwerte unverändert.Es dürfen nur die englischen Bezeichnungen für key function und name verwendet werden!

Syntax:

`ModifyKeyset;<reset>;<e164 number>|deviceId=<deviceId>[;<attribute-name>=`
`<attribute-value>]+`

HINWEIS: Der Defaultwert ist `e164`. Soll eine Device ID verwendet werden, muss `deviceId=<deviceId>` geschrieben werden.

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.11, “Parameterbeschreibung für Tastenbelegung ändern, Keyset ändern”.

Beispiel

Im folgenden Beispiel werden mehrere Parameter gesetzt:

1. Rollover Ruftonlautstärke wird auf 2 gesetzt (line-rollover-volume).
2. Fokus anzeigen wird zurückgesetzt (keyset-use-focus => 0, es kann auch false/true zum aktivieren / deaktivieren verwendet werden).
3. Registrierungs-LEDs ist gesetzt (line-registration-leds, es kann auch 0/1 verwendet werden).

```
ModifyKeyset;false;218116230;line-rollover-volume=2;
keyset-use-focus=0;line-registration-leds=true;
```

15.11.4.8 Geräteattribute ändern (ModifyDevice)

Dieses Kommando erlaubt das Anlegen oder Ändern der Geräteattribute, abhängig von Typ, Software und Version des IP Phones. Die erlaubten Geräteattribute sind beschrieben unter:

`...\DeploymentService\api\doc\v200\dlsapi\device\index_Device_DE.html`

`...\DeploymentService\api\doc\v200\dlsapi\device\index_SIPRegistration_DE.html`

`...\DeploymentService\api\doc\v200\dlsapi\device\index_HFARegistration_DE.html`

Syntax:

```
ModifyDevice;<e164>|deviceId=<deviceId>[;<attribute-name>=<attribute-value>]+
```

HINWEIS: Der Defaultwert ist `e164`. Soll eine Device ID verwendet werden, muss `deviceId=<deviceId>` geschrieben werden.

Eine Liste der Parameter finden Sie im Abschnitt 15.11.4.12, “Parameterbeschreibung für Geräteattribute ändern (ModifyDevice)”.

Beispiel:

```
ModifyDevice;218116230;remark=Testgerätekonfiguration;
display-id=6230;display-id-unicode=6230;
```

15.11.4.9 OpenScape Daten ändern (ModifyOpenScape)

Dieses Kommando erlaubt OpenScape Daten zu ändern.

Die erlaubten Attribute und deren Werte sind beschrieben unter:

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_OpenScapeParam_DE.html
```

Syntax:

```
ModifyOpenScape;<reset>;<e164 number>|<deviceId=anyDeviceId>
[;<attribute-name>=<attribute-value>]+
```

HINWEIS: Der Defaultwert ist `e164`. Soll eine Device ID verwendet werden, muss `deviceId=<deviceId>` geschrieben werden.

Beispiel:

```
ModifyOpenScape;false;498972231234;osc-connection-userid=31234;
osc-connection-port=4709;osc-connection-use-standardproxy=true;
osc-connection-use-https=true;osc-xmp-port=5222;
osc-xmp-use-https=false;osc-rules-port=8443;
```

15.11.4.10 Parameterbeschreibung für SIP/HFA Phone erzeugen, SIP/HFA Client erzeugen, IP Gateway erzeugen

Soweit nicht anders vermerkt, handelt es sich um Parameter auf der Maske IP Devices > IP Phone Konfiguration > Gateway / Server.

Parameter	optional/verpflichtend	DLS Parameter	Beschreibung
Device ID	optional	Device ID	MAC Adresse. Wenn kein Eintrag vorhanden ist, wird vom DLS eine virtuelle ID erstellt.
e164 number	verpflichtend	E.164	Eindeutige E.164 Nummer, max. 24 Zeichen.

Tabelle 11

Parameter	optional/verpflichtend	DLS Parameter	Beschreibung
IP Phone Type, IP Client Type, IP Gateway Type	optional	Gerätetyp	Gerätetyp oder virtuelles Gerät. Alphanumerisch, max. 50 Zeichen Mögliche Werte: IP Phone Type: siehe Liste „Mögliche Werte für IP-Telefontyp (IP Phone Type)“ IP Client Type: siehe Liste „Mögliche Werte für IP-Client-Typ (IP Client Type)“ IP Gateway Type: siehe Liste „Mögliche Werte für IP-Gateway-Typ (IP Gateway Type)
Software Type	optional	SW Typ	Alphanumerisch, max. 30 Zeichen
Software Version	optional	SW Version	Alphanumerisch, max. 30 Zeichen
Geräteprofil	optional	Geräteprofil	Alphanumerisch, max. 30 Zeichen
Bemerkung	optional	Bemerkung	Alphanumerisch, max. 256 Zeichen
Basis Profil	optional	IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „Profil“ > Basis Profil	Alphanumerisch, max. 40 Zeichen
Restore Basic Profil after Workpoint Reset	optional	Basis Profil wiederherstellen bei IP Device Registrierung	Mögl. Werte: true / false oder 1/ 0.
Terminal Name	optional	Terminal Name	Alphanumerisch, max. 255 Zeichen
Display ID	optional	Display ID	Alphanumerisch, max. 24 Zeichen
SIP User ID	optional	Benutzerkennung	1. Teil der SIP URL, alphanumerisch, max. 20 Zeichen.
SIP Password	optional	Passwort	Passwort, max. 25 Zeichen.
SIP Realm	optional	SIP Realm	Alphanumerisch, max. 93 Zeichen
SIP Server Adr.	optional	Reg-Adr	IP Adresse, max. 25 Zeichen.
SIP Server Port	optional	Reg-Port	Portnummer, numerisch, max. 5 Zeichen, Standard: 5060.
SIP Registrar Adr	optional	SIP Registrar Adr	IP Adresse, alphanumerisch, max. 255 Zeichen.

Tabelle 11

Parameter	optional/verpflichtend	DLS Parameter	Beschreibung
SIP Registrar Port	optional	SIP Registrar Port	Portnummer, numerisch, max. 5 Zeichen.
SIP Routing	optional	SIP Routing	Mögl. Werte: Server, Gateway, Direct.
SIP Gateway Adr	optional	SIP Gateway Adr	IP Adresse, alphanumerisch, max. 255 Zeichen.
SIP Gateway Port	optional	SIP Gateway Port	Portnummer, numerisch, max. 5 Zeichen,Standard: 5060.
Subscriber Number	optional	Registration Teilnehmerrufnummer	HFA Parameter, E.164 Nummer, max. 24 Zeichen.
Gatekeeper	optional	Gatekeeper ID	HFA Parameter, Domain-ID, max. 255 Zeichen.
Gatekeeper Password	optional	Teilnehmer Passwort	HFA Parameter, Passwort, max. 24 Zeichen.
Subscriber Number (Standby)	optional	Registration Teilnehmernummer (Standby)	HFA Parameter, E.164 Nummer, max. 24 Zeichen.
Gatekeeper (Standby)	optional	Gatekeeper ID (Standby)	HFA Parameter, Domain ID, max. 255 Zeichen.
Gatekeeper Password (Standby)	optional	Teilnehmer Passwort (Standby)	HFA Parameter, Passwort, max. 24 Zeichen.

Tabelle 11

15.11.4.11 Parameterbeschreibung für Tastenbelegung ändern, Keyset ändern

Parameter	optional/verpflichtend	DLS Parameter	Beschreibung
Device ID	optional	Device ID	MAC Adresse. Wenn kein Eintrag vorhanden ist, wird vom DLS eine virtuelle ID erstellt.
e164 number	verpflichtend	E.164	Eindeutige E.164 Nummer, max. 24 Zeichen.
key function	optional	IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung > Register „Ziele“ > Tastenfunktion	Mögl. Werte siehe Tabelle „Mögliche Werte für Keyfunction“.
level	optional	IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung > Register „Ziele“ > Ebene	Mögl. Werte: 0 = 1. Ebene,1= 2. Ebene, 2 = 3. Ebene, 3 = 4. Ebene
module	optional	Gerät	Mögl. Werte: 0 ... 4
key-number	optional	IP Devices > IP Phone Konfiguration > Keysets / Tastenbelegung > Register „Ziele“ > Tastennummer	Numerisch Mögliche Werte siehe Tabelle „Mögliche Werte für attribute-name bei ModifyKey“.
attribute-name	optional	----	Mögliche Werte siehe Tabelle „Mögliche Werte für attribute-name bei ModifyKey“.
name	optional	----	Mögliche Werte siehe Tabelle „Mögliche Werte für attribute-name bei ModifyKey“.
reset	optional	Kein DLS Parameter	Mögliche Werte: true/false, 1/ 0

15.11.4.12 Parameterbeschreibung für Geräteattribute ändern (ModifyDevice)

Parameter	optional/verpflichtend	DLS Parameter	Beschreibung
Device ID	optional	Device ID	MAC Adresse. Wenn kein Eintrag vorhanden ist, wird vom DLS eine virtuelle ID erstellt.
e164 number	verpflichtend	E.164	Eindeutige E.164 Nummer, max. 24 Zeichen.
attribute-name	optional	----	Mögliche Werte: siehe Tabelle „Mögliche Werte für attribute-name in Geräteattribute ändern (ModifyDevice)“.

Mögliche Werte für attribute-name in Geräteattribute ändern (ModifyDevice)

- `...\DeploymentService\api\doc\v200\dlsapi\device\index_Device_DE.html`
- `...\DeploymentService\api\doc\v200\dlsapi\device\index_SIPRegistration_DE.html`
- `...\DeploymentService\api\doc\v200\dlsapi\device\index_HFARegistration_DE.html`

Mögliche Werte für IP-Telefontyp (IP Phone Type)

- Mobile User SIP60
- OpenStage 5
- OpenStage 15
- OpenStage 20
- OpenStage 20E
- OpenStage 40
- OpenStage 60
- OpenStage 80
- optiPoint 410 advance
- optiPoint 410 economy
- optiPoint 410 economy plus
- optiPoint 410 entry
- optiPoint 420 economy

- optiPoint 420 economy plus
- optiPoint 420 standard
- optiPoint 420 advance

Mögliche Werte für IP-Client-Typ (IP Client Type)

- optiPoint 130
- Unify OpenScape Desktop Client
- AC-Win 2Q IP
- AC-Win MQ IP

Mögliche Werte für IP-Gateway-Typ (IP Gateway Type)

- HG1500
- HG3500
- HG3575
- HOOEE
- HOOME V1
- HP2K V2.0

Mögliche Werte für Keyfunction

Keyfunction (DLS Funktion)	Code
Keine Funktion	000
Selected Dialing (Zielwahl)	001
Abbreviated Dialing (Kurzwahl)	002
Repeat Dialing (Wahlwiederholung)	003
Missed Calls (Anruferliste)	004
Voice Messages (Nachrichten)	005
Forwarding (Anrufumleitung)	006
Loudspeaker (Lautsprecher)	007
Mute (Mikrofon aus)	008
Ringer Off (Rufton aus)	009
Hold (Halten)	010
Alternate (Makeln)	011
Blind Transfer (Ohne Rückfrage verbinden)	012
Join (Übergabe) (optiPoint)	013
Transfer Call (Verbinden) (OpenStage)	013

Tabelle 12

Keyfunction (DLS Funktion)	Code
Deflect (Weiterleiten)	014
Setup Menu (Service Menü)	015
Room Echoing (Raum hallend)	016
Room Muffled (Raum gedämpft)	017
SHIFT-Taste	018
Notebook (Notizbuch)	019
Settings (Einstellungen)	020
Telefonsperre	021
Conference (Konferenz)	022
Local Conference (Lokale Konferenz)	023
Headset (Kopfhörer)	024
Do Not Disturb (Anrufschutz)	025
Group Pickup (Anrufübernahme)	029
Repertory Dial (Erweiterte Zielwahl)	030
Line (Leitungstaste)	031
Feature Toggle (Funktionsumschaltung)	032
Show Phone Screen (Zeige Telefon-Display)	033
Swap Screen (Displaywechsel)	041
Mobility	042
Call Park (Anruf parken)	044
Call Pickup (Rücknahme Parken)	045
Cancel/Release (Abbrechen)	046
Ok Confirm (OK)	047
Callback Request (Rückruf)	048
Rückruf löschen	049
consultation transfer (Rückfrage/Übergabe)	050
DSS	051
State Key (State-Taste)	052
Call Waiting Toggle (Umschalten wartende Anrufe)	053
Immediate Ring (Sofortiger Ruf)	054
Preview Key (Preview Taste)	055
Call Recording (Sprachaufzeichnung)	056
AICS Zip	057
Server Feature (Server Feature-Taste)	058
BLF	059
start application (Applikation starten)	060
send url (URL senden)	063

Tabelle 12

Keyfunction (DLS Funktion)	Code
built-in forwarding (Eingebaute Anrufumleitung)	064
built-in release (Eingebaute Trennen)	065
built-in voice dial (Eingebaute Sprachwahl)	066
built-in redial (Eingebaute Wahlwiederholung)	067
start phonebook (Telefonbuch starten)	068
2nd alert (2. Ruf)	069

Tabelle 12

Mögliche Werte für attribute-name bei ModifyKey

Name	DLS Parameter	DLS-Beschreibung	Typ
key-destination	Ziel	Angabe des Wahlziels. Dies kann eine Ziffernfolge bzw. eine URL sein.	Alphanumerisch, max. 255 Zeichen
state-key-uri	Feature-URI	URI, mit der dieses Leistungsmerkmal auf dem Server gesteuert wird.	Alphanumerisch, max. 48 Zeichen
line-primary	Primärleitung	Bestimmt, ob die Leitung als Primärleitung fungiert.	Mögliche Werte: true/false
line-sip-uri	Leitungsziel	Rufnummer bzw. Address of Record der Leitung.	E.164 Nummer
line-sip-realm	Realm	SIP-Realm, der zum Address of Record der Leitung gehört.	Alphanumerisch, max. 48 Zeichen
line-sip-user-id	Benutzerkennung	Benutzerkennung	Alphanumerisch, max. 48 Zeichen
line-sip-pwd	Passwort	Passwort	Alphanumerisch, max. 48 Zeichen
line-ring	Rufton	Rufton	Mögliche Werte: true/false
line-hunt-sequence	Hunting Sequenz	Hunting Sequenz	0 ... 10
line-shared-type	Shared Typ	Shared Typ	Mögliche Werte: • Privat • Gemeinsam • Unbekannt
feature-toggle-description	Toggle Text	Text für die Tastenfunktion „Funktionsumschaltung“.	Alphanumerisch, max. 24 Zeichen
feature-toggle-code-description-unicode	Toggle Text (Unicode)	Text für die Tastenfunktion „Funktionsumschaltung“, in Unicode kodiert.	Alphanumerisch, max. 24 Zeichen
state-key-description-text	Beschreibung State Taste	Beschreibungstext für die State-Taste.	Alphanumerisch, max. 22 Zeichen

Tabelle 13

Name	DLS Parameter	DLS-Beschreibung	Typ
state-key-description-text-unicode	Beschreibung State Taste (Unicode)	Beschreibungstext für die State-Taste in Unicode.	Alphanumerisch, max. 22 Zeichen
key-label	Tastentext	Bei Self labeling Keys-Workpoints (z. B. optiPoint 420 standard) kann hier pro Taste eine Tastenbeschriftung angegeben werden.	Alphanumerisch, max. 24 Zeichen
key-label-unicode	Tastentext (Unicode)	Bei OpenStage-Telefonen kann der Tastentext auch in Unicode eingegeben werden.	Alphanumerisch, max. 24 Zeichen
line-hidden	Anzeigen am APM/DSM	Schalter zum Aktivieren der Leitungsanzeige am optiPoint Application Module / Display Module.	Mögliche Werte: true/false
line-int-allow	Leitungsstörung erlaubt	Schalter zum Aktivieren für das Zulassen von Leitungsstörungen.	Mögliche Werte: true/false
line-hld-active	Leitungs-Hotline aktiv	Schalter zum Aktivieren einer Leitungs-Hotline.	Mögliche Werte: true/false
line-hld	Leitungs-Hotline Ziel	Rufnummer die als Ziel für die Leitungs-Hotline verwendet wird.	Alphanumerisch, max. 60 Zeichen
line-mlo-pos	Pos. Leitungsübersicht am APM / DSM	Pos. Leitungsübersicht am APM / DSM	Nummer, 2
line-short-desc	Leitungsbeschreibung	Bescheibung der entsprechenden Leitung.	Alphanumerisch, max. 10 Zeichen
line-hot-line-warm-line	Hot/Warm Line Typ		Mögliche Werte: • Normal • Sofortverbindungsaufbau • verzögerter Sofortverbindungsaufbau
line-ring-delay	Rufton-Verzögerung	Dauer der Verzögerung, bis ein eingehender Rufton signalisiert wird.	Nummer, 5
forwarding-type	Umleitungstyp	Umleitungstyp	Mögliche Werte: • bei besetzt • bei nicht melden • immer
locked-function-keys	Taste sperren	Schalter zum Sperren der Funktionstaste.	Mögliche Werte: true/false

Tabelle 13

Name	DLS Parameter	DLS-Beschreibung	Typ
dss-sip-line-type	Leitungstasten Typ	Leitungstasten Typ	Mögliche Werte: • normal • direkt
dss-sip-line-action	Leitungstasten Aktion	Leitungstasten Aktion	Mögliche Werte: • Rückfrage • Vermitteln • Keine Aktion

Tabelle 13

Mögliche Werte für attribute-name bei ModifyKeyset

Attribut-Name	DLS-Parameter	DLS-Beschreibung	Typ
dss-sip-deflect	Aufmerksamkeitsruf umlenken	Ist der Schalter aktiviert, kann der Aufmerksamkeitsruf per Tastendruck umgeleitet werden.	Mögliche Werte: true/false
dss-sip-detect-timer	Timer Erkennung Anrufübernahme (sek)	Legt fest, wie lange die Anrufübernahme an der Taste signalisiert wird.	Nummer
dss-sip-refuse	Anrufübernahme zurückweisen	Ist der Schalter aktiviert, kann die Anrufübernahme per Tastendruck zurückgewiesen werden.	Mögliche Werte: true/false
line-key-operating-mode	Leitungstaste Operationsmodus	Legt fest, was mit einer Leitung (Gespräch) geschehen soll, wenn eine Verbindung über eine andere Leitung hergestellt wird. Halten: Das Gespräch der ursprünglichen Leitung wird gehalten. Freigeben: Die Verbindung der ursprünglichen Leitung wird getrennt.	Mögliche Werte: • Halten • Freigeben

Tabelle 14

Attribut-Name	DLS-Parameter	DLS-Beschreibung	Typ
originating-line-preference	Präferenz abgehende Leitungen	Festlegung der bevorzugt zu verwendenden Leitung bei ausgehenden Anrufen.	Mögliche Werte: • Ruhende Leitung bevorzugt • Primärleitung bevorzugt • Letzte Leitung bevorzugt • Kein Vorzug
line-registration-leds	Registrierungs-LEDs	Ist der Schalter aktiv, wird beim Neustart des IP Phones angezeigt, ob der Workpoint erfolgreichregistriert wurde.	Mögliche Werte: true/false
keyset-remote-forward-ind	Remote Forward Indication	Schalter zum Aktivieren der Signalisierung bei einer Leitungstaste, wenn bei deren Ziel eine Rufweiterschaltung aktiv ist.	Mögliche Werte: true/false
keyset-reservation-timer	Reservierungszeit (sek)	Zeit in Sekunden, die angibt, wie lange eine Leitungsreservierung aufrechterhalten wird.	Nummer
line-rollover-type	Rollover Typ	Art der der Signalisierung für den Fall, dass während eines Gesprächs ein Anruf auf einer anderenLeitung ankommt.	Mögliche Werte: • Kein Ton • Hinweisruf • Standard • Hinweiston
line-rollover-volume	Rollover Lautstärke	Lautstärke der Signalisierung im Besetztfall.	Nummer

Tabelle 14

Attribut-Name	DLS-Parameter	DLS-Beschreibung	Typ
terminating-line-preference	Präferenz ankommende Leitung	Festlegung der bevorzugt zu verwendenden Leitung bei eingehenden Anrufen.	Mögliche Werte: • Rufende Leitung bevorzugt • Rufende Leitung bevorzugt mit Primärleitung bevorzugt • Rufende Leitung bevorzugt • Ankommende Leitung bevorzugt mit Primärleitung bevorzugt • Kein Vorzug
keyset-use-focus	Fokus anzeigen	Schalter zum Aktivieren der Anzeige, welche Leitung momentan aktiv ist (Leitung hat den Fokus).	Mögliche Werte: true/false
line-button-mode	Leitungstastenmode	Leitungstastenmodus	Mögliche Werte: • Einzeltaste • Vorauswahl
line-preselection-timer	Leitungsvorauswahl Timer (sek)	Legt die Zeitspanne fest, nach der die Vorauswahl einer Leitung wieder beendet wird.	Nummer
line-preview-period	Leitungstaste Preview Dauer (sek)	Legt die Zeitspanne fest, nach der der Preview einer Leitungstaste wieder beendet wird.	Nummer
shift-key-timeout	Shift-Tasten Timeout	Zeit in Sekunden, nach deren Ablauf die Shift-Taste inaktiv wird, so dass die Tasten wieder mit den Funktionen der 1. Ebene belegt sind.	Nummer
stimulus-dtmf-sequence	DTMF Sequenz	DTMF Sequenz	Alphanumerisch, max. 255 Zeichen
blf-audible	BLF akustischer Hinweis	BLF akustischer Hinweis	Mögliche Werte: true/false
blf-popup	BLF PopUp Hinweis	BLF PopUp Hinweis	Mögliche Werte: true/false
fpk-app-name	Applikationsname	Applikationsname	Alphanumerisch, max. 48 Zeichen

Tabelle 14

Attribut-Name	DLS-Parameter	DLS-Beschreibung	Typ
send-url-address	Web Server Adresse	Hostname, Domänenname oder IP Adresse des Web Servers	Alphanumerisch, max. 255 Zeichen
send-url-protocol	Protokoll	Protokoll	Mögliche Werte: 0: http 1: HTTPS
send-url-port	Port	Portnummer des Web Servers	Nummer
send-url-path	Pfad	Verzeichnispfad und Name des Programms oder der Webseite. Beispiele: “servlet/IppGenericServlet” oder “webpage/checkin.html”	Alphanumerisch, max. 255 Zeichen
send-url-query	Parameter	Parameter im HTTP-Request. Beispiele:Parameter1=Wert1 &Parameter2=Wert2	Alphanumerisch, max. 255 Zeichen
send-url-method	HTTP Methode	HTTP Methode	Mögliche Werte: 0: Get 1: Post
send-url-user-id	Web Server User ID	Dem Web Server bekannte User ID	Alphanumerisch, max. 48 Zeichen
send-url-passwd	Web Server Passwort	Dem Web Server bekanntes Passwort	Alphanumerisch, max. 48 Zeichen
key-functionality	Tastenfunktionalität	Tastenfunktionalität	Mögliche Werte: 0: Anrufumleitung umschalten 1: unspezifizierte Anrufumleitung 2: unspezifiziert

Tabelle 14

15.12 Copy-Makro für P&P und Templates

Diese Funktion ermöglicht das automatische Kopieren von Werten von einem Feld in ein anderes. Mit einem Makro können zum Beispiel die Registrierungsdaten für HFA-Telefone in die Standby-Konfiguration kopiert werden.

Um den Wert eines Feldes oder Teile des Wertes in ein anderes Feld zu kopieren, richten Sie ein Template ein, das ein Makro-Kommando enthält.

Sie können zum Beispiel ein Template definieren, das die Reg-Adresse des Haupt-Gateway in das Feld Reg-Adresse des Standby-Gateway kopieren soll. Dazu muss folgendes in das Feld **Standby Reg-Adresse** eingetragen werden: `%reg-number%`

Beim Zuweisen des Templates wird das Makro-Kommando ausgeführt sowie das Ergebnis in das Feld geschrieben und zum Endgerät geschickt.

Es ist auch möglich, Makro-Kommandos direkt für virtuelle Devices einzutragen. Diese werden dann bei Plug & Play oder, falls es sich um ein bereits registriertes Device handelt, sofort per Job ausgeführt.

15.12.1 Makrokommando Syntax

Die Syntax des Makrokommandos

`%<item name >[begin index, end index]%`

setzt sich aus folgenden Teilen zusammen:

- `%` markiert den Anfang und das Ende des Makrokommandos
- `item name` Name des Feldes, dessen Werte kopiert werden sollen
- `begin index` bis `end index` (optional) können auch nur Teile eines Wertes kopiert werden. Hierbei steht `$` für den letzten Index des Wertes.

  Beispiele: `%e164%` kopiert die ganze E.164 Nummer; `%e164[1,5]%` kopiert die ersten 5 Zeichen der E.164 Nummer; `%e164[$-4,$]%` kopiert die letzten 5 Zeichen der E.164 Nummer.

15.12.2 Verfügbare <item name>

Die Kopierfunktion steht nur für eine Auswahl von Feldern zur Verfügung. Das Quellfeld `<item name>` muss auf derselben Maske wie das Zielfeld sein.

Es kann von folgenden Feldern kopiert werden:

Maske	Feld	Item name
IP Devices > IP Phone Konfiguration > Gateway / Server	E.164	`e164`
	Reg-Adresse	`reg-addr`
	Registration Teilnehmerrufnummer	`reg-number`
	Gatekeeper ID	`reg-id`
	H.235 Security Modus	`h235securitymode`
IP Devices > IP Client Konfiguration > Gateway / Server	System Typ	`hfa-pbx-type`
	E.164	`e164`
	Reg-Adresse	`reg-addr`
	Registration Teilnehmerrufnummer	`registration-phone-no`
	Gatekeeper ID	`gatekeeper-id`
	H.235 Security Modus	`h235securitymode`

Tabelle 15

15.12.3 Verfügbare Zielfelder

Maske	Feld
IP Devices > IP Phone Konfiguration > Gateway / Server	E.164
IP Devices > IP Phone Konfiguration > Gateway / Server > Register Gateway	Registration Teilnehmerrufnummer
IP Devices > IP Phone Konfiguration > Gateway / Server > Register Gateway (Standby)	Reg-Adresse
	Registration Teilnehmerrufnummer
	Gatekeeper ID
	H.235 Security Modus
IP Devices > IP Phone Konfiguration > Gateway / Server > Register SIP Terminaleinstellungen	Display ID
	Display ID (Unicode Zeichen)
	Terminal Name
IP Devices > IP Phone Konfiguration > Sonstiges > Register Display/Geräte Einstellungen	Handset Name
IP Devices > IP Phone Konfiguration > IP Routing > Register DNS Server	Terminal Hostname
IP Devices > IP Client Konfiguration > Gateway / Server	E.164

Tabelle 16

Maske	Feld
IP Devices > IP Client Konfiguration > Register Gateway	Registration Teilnehmerrufnummer
IP Devices > IP Client Konfiguration > Register Gateway (Standby)	System Typ
	Reg-Adresse
	Registration Teilnehmerrufnummer
	Gatekeeper ID
	H.235 Security Modus
IP Devices > IP Client Konfiguration > SIP Verbindung	Terminal Name
IP Devices > IP Phone Konfiguration > Keyset / Keylayout > Registerkarte „Ziele“	Leitungsziel
	Benutzerkennung
	Tastentext
	Tastentext (Unicode)
Mobile User > SIP Mobile User Konfiguration > Keysets / Tastenbelegung > Registerkarte „Ziele“	Leitungsziel
	Benutzerkennung
	Tastentext
	Tastentext (Unicode)

Tabelle 16

16 Administrations-Szenarien

Dieses Kapitel enthält folgende Administrations-Szenarien:

- Neuinstallation eines Workpoints bei HiPath 4000
- Neuinstallation eines Workpoints bei HiPath 3000
- Einrichten eines Gateways im DLS
- Austausch eines IP Devices
- Austausch eines alten Workpoints (TDM) durch einen neuen (IP)
- Austausch von HFA- durch SIP-Software und umgekehrt bei identischer Device ID
- Einrichten eines IP Client 130 im DLS
- Ändern der IP-Adresse und/oder Portnummer des DLS
- Einsatz eines TAP mit DLS in einem Kundennetz ohne permanenten DLS
- Steuern des DLS über die Programmschnittstelle (DlsAPI)
- Security: Administration von Zertifikaten
- Mobility:EinrichtenMobility:Administrieren
- HFA Mobility an HiPath 3000
- Datenstrukturen für DLS-eigene XML-Applikationen
- Mandantenfähigkeit
- Migrationsszenarien

HINWEIS: Die hier genannten Ablaufbeschreibungen haben beispielhaften Charakter. Durch Besonderheiten in der Konfiguration des DLS, der eingesetzten Server oder der IP Devices und durch Weiterentwicklung des DLS kann der tatsächliche Ablauf von der Beschreibung abweichen.

16.1 Neuinstallation eines Workpoints bei HiPath 4000

Voraussetzungen

- Eine laufende DLS-Infrastruktur (z. B. DHCP- und DNS-Server).
- Ein HiPath 4000 Assistant mit deaktivierter Zugangssperre[1], der im DLS eingerichtet ist (siehe Abschnitt 11.1.4).

Durchführen der Neuinstallation

1. Richten Sie den Teilnehmer im System z. B. mithilfe des HiPath 4000 Manager bzw. durch AMO-Konfiguration ein. Informationen dazu finden Sie in der jeweiligen Dokumentation.
2. Wählen Sie den Bereich **Element Manager** > **Element Manager Konfiguration**> **Register „HiPath 4000 Assistant“**.
3. Klicken Sie auf **Synchronisieren**. Hiermit werden alle Daten der im System eingerichteten Teilnehmer zum DLS übertragen.
4. Wählen Sie den Bereich **IP Device Verwaltung** > **IP Device Konfiguration**.
   Klicken Sie auf **Suche**, um alle konfigurierten Workpoints zu finden. Der erste der gefundenen Workpoints wird in der Ansicht **Objekt** angezeigt.
5. Wechseln Sie in die Ansicht **Tabelle** und sortieren Sie die Tabelle nach **E.164**.
6. Selektieren Sie in der Tabelle das gewünschte, vorkonfigurierte virtuelle Gerät. Der vom DLS generierten **Device ID** eines virtuellen Geräts ist ein „@“ vorangestellt.
7. Geben Sie die **Device ID** des Workpoints ein.
8. Klicken Sie auf **Sichern**.
9. Schließen Sie den Workpoint an.

Damit ist die Neuinstallation abgeschlossen.

1 Zum Deaktivieren der Zugangssperre wählen Sie im HiPath 4000 Assistant **Zugangsverwaltung** > **Kennungsverwaltung** > **Systemkennungsverwaltung** > Kennung **uas_read** und deaktivieren Sie die Option **Kennung sperren**. Passwort eingeben und Änderungen sichern.

16.2 Neuinstallation eines Workpoints bei HiPath 3000

Voraussetzungen

- Eine laufende DLS-Infrastruktur (z. B. DHCP- und DNS-Server).
- Ein HiPath 3000/5000, der im DLS eingerichtet ist (siehe Abschnitt 11.1.5).

Durchführen der Neuinstallation

1. Richten Sie den Teilnehmer im System ein. Informationen dazu finden Sie in der jeweiligen Dokumentation.
2. Wählen Sie den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration**, um einen entsprechenden Teilnehmer, d. h. ein virtuelles Gerät, im DLS anzulegen. Das virtuelle Gerät erhält anstelle der Device ID einen vom DLS generierten Platzhalter, der mit „@“ beginnt.
3. Tragen Sie die **E.164** des neuen Teilnehmers ein.
4. Wählen Sie den Bereich **Element Manager** > **Element Manager Konfiguration** > **Register „HiPath 3000/ 5000“**.
5. Klicken Sie auf **Synchronisieren**. Sollte die E.164 in einem der konfigurierten HiPath 3000/ 5000 DB Feature Server existieren, wird der Datensatz um die entsprechende Gatekeeper-Adresse erweitert.
6. Geben Sie in **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** die Device ID des Workpoints ein.
7. Klicken Sie auf **Sichern**.
8. Schließen Sie den Workpoint an.

Damit ist die Neuinstallation abgeschlossen.

16.3 Einrichten eines Gateways im DLS

Voraussetzungen

- Eine laufende DLS-Infrastruktur.
- Ein konfiguriertes Gateway (HG1500, HG3530, HG3550, HG3570, HG3575 oder RG2700).

16.3.1 Gateway hinzufügen

1. Wählen Sie den Bereich **Gateways** > **Gateway Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie bei Gateway Typ das passende Gateway aus. Durch die Auswahl werden alle nicht erforderlichen Felder deaktiviert (ausgegraut).

   HINWEIS: Falls bereits ein Gateway des gleichen Typs eingerichtet ist, können von diesem die Daten übernommen und danach angepasst werden. Suchen Sie dazu zunächst das Gateway, von dem Sie die Daten ableiten möchten und klicken Sie danach auf **Neu**.
4. Geben Sie ggf. bei **Bemerkung** eine Beschreibung zu diesem Gateway ein.
5. Geben Sie die erforderlichen Daten im Register „Gateway Verbindung“ ein. Nachfolgend sind die erforderlichen Einträge für die verschiedenen Gateway-Typen aufgelistet.

   - **HG1500** (für HiPath 3000/5000, direkte Anbindung), **RG2700**

     Gateway IP Adresse: IP-Adresse des Gateways.

     Kennung: Zugangskennung zum Gateway (wie am Gateway eingerichtet, Standard-Kennung: **31994**).

     Passwort: Zugangspasswort zum Gateway (wie für die o. g. Kennung auf dem Gateway eingerichtet).

   - **HG3550** (für HiPath 4000, Anbindung über HiPath 4000 Assistant)

     Gateway IP Adresse: IP-Adresse des Gateways.

     Gateway Proxy IP Adresse: IP-Adresse des zugehörigen HiPath 4000 Assistant.

     Gateway Proxy Port: 443.

     Kennung: Zugangskennung zum HiPath 4000 Assistant (wie auf dem Assistant eingerichtet). Es muss eine Kennung auf dem HiPath 4000 Assistant verwendet werden, welche die Zugangsrechte für HG3550Mgr besitzt.
     Zum Einrichten von Kennungen und Zuweisen von Rechten im HiPath 4000 Assistant siehe die dortige Online-Hilfe unter „Zugangsverwaltung“ (bzw. „Access Management“).

     Passwort: Zugangspasswort zum HiPath 4000 Assistant (wie für die o. g. Kennnung auf dem HiPath 4000 Assistant eingerichtet).

   - **HG3530**, **HG3570**, **HG3575** (für HiPath 4000, Anbindung über SNMP-Proxy, welcher integraler Bestandteil des DLS Servers ist)

     Gateway IP Adresse: IP-Adresse des Gateways.

SNMP Community: Community String (zur Authentisierung der SNMP-Kommunikation zum Gateway). Standard-Community String: **nbcs**.
Der Cummunity String muss auf denselben Wert gesetzt warden, wie für das betroffene Gateway in der HiPath 4000 konfiguriert (AMO HFAB: TYP=SNMP, Parameter: CS2).

HINWEIS: Der SNMP-Proxy wird gleichzeitig mit dem DLS während der DLS-Installation auf dem DLS-Server PC als lokaler Service mit installiert und automatisch gestartet. Der SNMP-Proxy kann dort manuell angehalten und gestartet werden.
Pfad zum Aufrufen: Start > Einstellungen > Systemsteuerung > Verwaltung > Dienste > DeploymentServiceSNMPProxy

6. Klicken Sie auf **Sichern**, um die Einträge zu übernehmen.

16.3.2 Angaben zur Freigabe (QDC und VoIP Security)

QoS Data Collection

- HG1500: V5.0
- HG3550: V2.0
- HG3530: V2.0
- HG3570: V2.0
- HG3575: V2.0
- RG2700: V1.0

VoIP Security

- HG1500: V6.0
- HG3550: V3.0 (nach „außen“ evtl. noch V2.0)
- HG3530: V3.0 (nach „außen“ evtl. noch V2.0)
- HG3570: Keine VoIP Security
- HG3575: Keine VoIP Security
- RG2700: Keine VoIP Security

16.4 Konfigurieren von Zertifikaten in DLS

Zur Verteilung von Massenzertifikaten an Telefone und Clients unterstützt der OpenScape Deployment Service (DLS) eine eigene interne Public Key Infrastructure (PKI), um zwischen folgenden Komponenten eine sichere Kommunikation zu ermöglichen:

- DLS und Telefonen/Clients
- DLS und OpenScape Voice Assistant sowie
- DLS und Webbrowsern.

Diese interne PKI funktioniert ähnlich wie die meisten anderen PKIs. Sie kann ihre eigene Zertifizierungsstelle (Certificate Authority, CA) erstellen, Zertifikate erstellen, die von dieser CA signiert sind und diese Zertifikate sogar automatisch verteilen. Darüber hinaus kann diese interne PKI auch mehrere interne PKIs verwalten und ermöglicht so eine Zertifikatverwaltung für unterschiedliche Funktionen innerhalb des Telefons.

HINWEIS: Zertifikatformat: Schlüsselspeicher (Keystore) im Format PKCS#12 oder Verwendung der DLS-internen PKI-Infrastruktur.

Bild 1 und Bild 2 zeigen Beispiele für Zertifikate und PKI-Hierarchien.

In Bild 1 verwenden die der Öffentlichkeit zugewendeten Schnittstellen des Deployment Service ein Zertifikat der Kunden-CA, während die Zertifikate der Telefone von der internen PKI des Deployment Service verwaltet werden. Der Deployment Service kann mehr als eine PKI verwalten, um unterschiedliche Telefonfunktionen, die Zertifikate erfordern, zu verwalten. Darüber hinaus gibt es auch die Möglichkeit, eine einzige interne PKI zu verwenden.

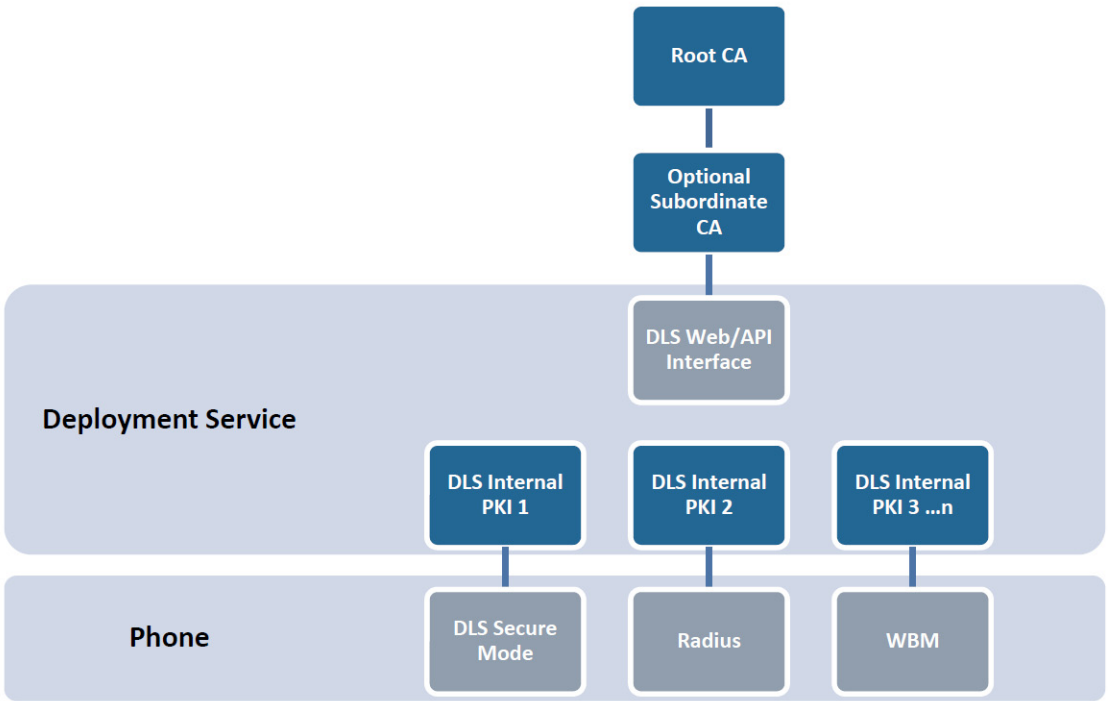


Bild 1 Beispiel für eine Deployment Service-Zertifikathierarchie

Der OpenScape Deployment Service unterstützt auch die Integration mit einer externen Microsoft-Zertifizierungsstelle. In diesem Fall ist überlässt die Deployment Service-PKI der Microsoft-CA das Erstellen und Verwalten von Zertifikaten, während der DLS selbst deren Verteilung übernimmt. Die Verwendung der Microsoft-CA wird in diesem Dokument nicht behandelt. Die entsprechende Beschreibung finden Sie stattdessen im Dokument „OpenScape Deployment Service PKI Basic Configuration“.
Bild 2 zeigt eine Beispiel-Zertifikathierarchie mit einer Microsoft-CA. Der Deployment Service verwendet eine einzige interne PKI, um sowohl die der Öffentlichkeit zugewendeten Schnittstellen des Deployment Service als auch alle Funktionen des Telefons, die Zertifikate erfordern, zu verwalten.

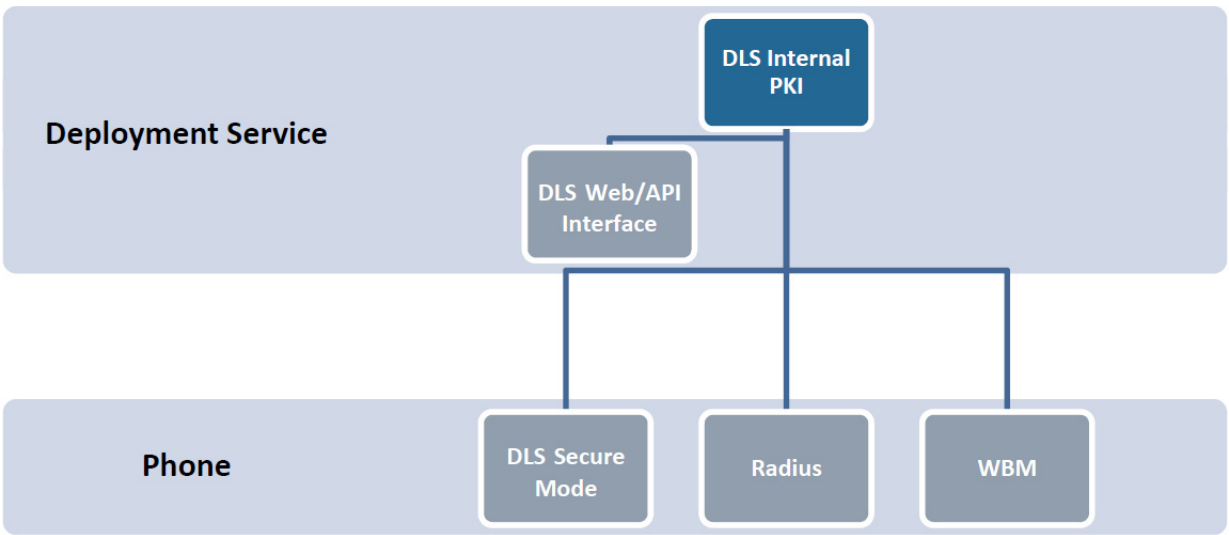


Bild 2 *Beispiel 2 für eine Deployment Service-Zertifikathierarchie*

16.4.1 Erstellen einer neuen PKI

Es ist möglich, mehr als eine PKI zu erstellen. Für unterschiedliche Zwecke können unterschiedliche PKIs verwendet werden. Beispielsweise könnte eine PKI alle WBM-Zertifikate verwalten, während eine andere die Verteilung der RADIUS-Serverzertifikate übernimmt. Auch die Verwendung einer einzigen PKI zur Verwaltung aller Zertifikate ist möglich.

Die Erstellung einer neuen PKI erfolgt in drei (3) grundlegenden Schritten, die alle zusammen eine neue PKI ergeben.

Erforderliche Schritte:

1. Erstellen Sie eine neue interne CA
2. Erstellen Sie eine neue Plug-In-Konfiguration
3. Erstellen Sie eine neue Connector-Konfiguration

16.4.1.1 Erstellen einer neuen internen CA

1. Melden Sie sich beim Deployment Service and und navigieren Sie zu **Administration** >**PKI** >**Interne CA;CA intern**.
2. Klicken Sie auf **Neu** und geben Sie einen **CA-Namen** und eine **CA-Beschreibung** ein. Klicken Sie auf **Sichern**.
3. Klicken Sie auf **Erzeuge CA**. Geben Sie unter **Subject (Antragsteller) / Aussteller DN** die erforderlichen Informationen ein. In diesem Schritt wird die Identität der CA festgelegt; die zur Identität gehörigen Informationen werden später in jedem von dieser CA erstellten Zertifikat angezeigt.

   Zertifikate sollten mindestens folgende Informationen enthalten: Land, Bundesland oder Provinz, Organisation, Organisationseinheit (OU) und Allgemeiner Name (Common Name, CN).

   Beispiel: C=US,ST=FL,L=Boca Raton,O=Unify,OU=Sales,CN=MyNewCA
4. Alternative zu Schritt 3). Sie können eine neue interne CA auch anhand einer vordefinierten CA erstellen. In diesem Fall wird das vordefinierte CA-Zertifikat in die interne CA importiert. Klicken Sie auf **Import CA (CA importieren)**. Klicken Sie auf **Browse (Durchsuchen)**, um den CA-Schlüsselspeicher zu suchen. Der Schlüsselspeicher muss im Format PKCS#12 vorliegen. Geben Sie die **Passphrase** für den Schlüsselspeicher ein und klicken Sie auf **OK**.
5. Setzen Sie den **Schlüsselalgorithmus** auf RSA. Setzen Sie die **Schlüssellänge** auf 2048. 1024 und 4096 sind ebenfalls möglich.
6. Geben Sie unter **Gültig ab** und **Gültig bis** die entsprechenden Werte ein. Standardmäßig ist die Gültigkeitsdauer auf 1 Jahr eingestellt. Ändern Sie dies auf einen für eine CA angemesseneren Wert (z. B. 10 Jahre).
7. Klicken Sie auf **OK**. Die neue CA wird erstellt und ihre Informationen werden angezeigt.

8. Aktivieren Sie abschließend die Option **Interne CA aktivieren** und klicken Sie dann auf **Sichern**.

16.4.1.2 Erstellen einer neuen Plug-In-Konfiguration

1. Erstellen Sie eine neue interne CA wie in Abschnitt 16.4.1.1, “Erstellen einer neuen internen CA” beschrieben.
2. Gehen Sie zu **Administration** >**PKI** >**Plug-In Konfiguration**.
3. Klicken Sie auf Neu und geben Sie in den Feldern **PKI Connector Plug-In** und **Beschreibung** einen Namen und eine Beschreibung ein. Klicken Sie auf **Sichern**.
4. Navigieren Sie zum Register **Plug-In Properties** und wählen Sie im Ansicht-Optionsfeld **Tabelle** aus.
5. Ändern Sie die beiden folgenden Standard-Zertifikat-Werte: **internal.default.validity.days** und **internal.x509name.template**.
6. Wählen Sie **internal.default.validity.days** aus. Dieses Feld legt die Anzahl der Tage fest, die ein vom Deployment Service erstelltes Zertifikate gültig ist. Ein typischer Wert für die Gültigkeitsdauer ist 3 Jahre. Klicken Sie auf **Sichern**.
7. Wählen Sie **internal.x509name.template** aus. Dieses Feld enthält die Antragstellerinformationen (Subject) für Zertifikate, die vom Deployment Service erstellt werden. Dieses Feld dient als Template. Die meisten Informationen sind vorbelegt; einzige Ausnahme ist der Allgemeine Name (Common Name, CN). Beim Ausstellen eines Zertifikats trägt der Deployment Service automatisch den CN ein, der anhand der IP-Adresse oder des FQDN ermittelt wurde. Dies ermöglicht eine einfache Zerfikatbereitstellung (Point-and-Click oder automatisiert). Dieses Template sollte bis auf das Feld CN mit den für die Root-CA in Schritt 1 angegebenen Ausstellernamen-Informationen übereinstimmen. Das CN-Feld MUSS ein ‘?’ enthalten. Klicken Sie auf **Sichern**.

   Beispiel: C=US,ST=FL,L=Boca Raton,O=Unify,OU=Sales,CN=?
8. Klicken Sie auf das Register **Ausstellende Zertifizierungsstellen**. Klicken Sie auf **Synchronisieren**. Die Informationen zu allen aktivierten internen CA werden übernommen. Wir verwenden nur die interne CA, die wir in Schritt 1) erstellt haben. Dies wird ersichtlich in den nächsten Schritten.
9. Wählen Sie abschließend die Option **Plug-In aktivieren** und klicken Sie auf **Sichern**.

16.4.1.3 Erstellen einer neuen Connector-Konfiguration

1. Erstellen Sie eine neue interne CA und eine Plug-In-Konfiguration wie in Abschnitt 16.4.1.1, “Erstellen einer neuen internen CA” und Abschnitt 16.4.1.2, “Erstellen einer neuen Plug-In-Konfiguration” beschrieben.
2. Gehen Sie zu **Administration** >**PKI** >**Connector Konfiguration**.
3. Klicken Sie auf **Neu** und geben Sie in den Feldern **Name der Konfiguration** und **Beschreibung** einen Namen und eine Beschreibung ein.
   Klicken Sie auf **Sichern**.
4. Wählen Sie die Option **Plug-In Konfiguration** aus. Wählen Sie den Namen der in Abschnitt 16.4.1.2, “Erstellen einer neuen Plug-In-Konfiguration” erstellten Plug-In-Konfiguration aus, klicken Sie auf **OK** und dann auf **Sichern**.
5. Wählen Sie die Option **Ausstellende Zertifizierungsstelle** aus. Wählen Sie den Namen der in Abschnitt 16.4.1.1, “Erstellen einer neuen internen CA” erstellten ausstellenden Zertifizierungsstelle aus, klicken Sie auf **OK** und dann auf **Sichern**.
6. Gehen Sie zum Register **Trust Anchor** und klicken Sie auf **Zertifikat importieren**. Aktivieren Sie das Optionsfeld **PKI** und wählen Sie unter **Importieren vom Connector** den Namen der in Abschnitt 16.4.1.1, “Erstellen einer neuen internen CA” erstellten ausstellenden Zertifizierungsstelle aus. Klicken Sie auf **OK** und dann wieder auf **OK**. Die in Abschnitt 16.4.1.1, “Erstellen einer neuen internen CA” definierte CA ist jetzt der Trust Anchor (Root-CA) für diese PKI. Dies sollte nun in den Trust Anchor-Feldern angezeigt werden.
7. Navigieren Sie zum Register **Request Parameter**. Die Standardeinstellungen sollten stimmen. Klicken Sie auf **Test**. Der Deployment Service erstellt intern ein neues Zertifikat und signiert dieses, um seine ordnungsgemäße Funktionsweise zu gewährleisten. Im Anschluss daran sollte eine Erfolgsmeldung angezeigt werden.

   Beispiel: C=US,ST=FL,L=Boca Raton,O=Unify,OU=Sales,CN=?
8. Aktivieren Sie abschließend die Option **Connector aktivieren** und klicken Sie dann auf **Sichern**. Eine neue interne PKI für die DLS wurde erstellt. Diese neue PKI kann nun zum Erstellen und Verteilen von Zertifikaten an Telefone und Clients verwendet werden.

16.4.2 Verteilen des Signaling and Payload Encryption (SPE)-Zertifikats

Das Signaling and Payload Encryption (SPE)-Zertifikat ist nichts anderes als das CA-Zertifikat (bzw. die Kette von CA-Zertifikaten), das zum Signieren des OpenScape Voice-Zertifikats verwendet wird. Wenn dieses CA-Zertifikat auf den Telefonen vorhanden ist, können diese die OpenScape Voice anhand des von der OpenScape Voice empfangenen Zertifikats identifizieren und verifizieren. Standardmäßig führen Telefone keine Verifizierung des Zertifikats durch. Die Telefone können dennoch über TLS eine Verbindung zur OpenScape Voice herstellen und sichere Anrufe tätigen.

Bevor Sie die Zertifikatverifizierung für alle Telefone aktivieren, empfiehlt es sich, das CA-Zertifikat manuell auf einige Telefone hochzuladen und die Zertifikatverifizierung zu aktivieren. Wenn dieser Test fehlschlägt, kann sich das Telefon nicht an der OpenScape Voice registrieren. Ist der Test erfolgreich, dann können Sie die automatische Zertifikatsverteilung verwenden, um das CA-Zertifikat auf alle Telefone zu verteilen.

16.4.2.1 Manuelle Verteilung

HINWEIS: Zur Durchführung der in diesem Abschnitt aufgeführten Schritte ist die Erstellung einer PKI nicht erforderlich.

1. Gehen Sie zu **IP Devices** >**IP Phone Konfiguration** >**Signaling and Payload Encryption (SPE)** >**Register „SPE CA Zertifikate“**.
2. Klicken Sie auf **Zertifikat importieren**.
3. Aktivieren Sie die Option **Zertifikate in DLS importieren und auf Gerät aktivieren (1-Step)**. Wählen Sie **Import über: Datei**.
   Klicken Sie auf **Durchsuchen** und suchen Sie die Datei, die die CA-Zertifikate enthält.
4. Klicken Sie abschließend auf **OK**. Das Zertifikat wird importiert und ein neuer Eintrag mit den Informationen des CA-Zertifikats wird angezeigt.
5. Jetzt können Sie die Zertifikatverifizierung aktivieren. Siehe Abschnitt 16.4.2.2, “Wie Sie die SPE-Zertifikatverifizierung aktivieren”.

16.4.2.2 Wie Sie die SPE-Zertifikatverifizierung aktivieren

Die Telefone unterstützen drei Stufen der Zertifikatverifizierung: Keine, Voll und Trusted (Vertrauenswürdig). Jede dieser Stufen ist strikter als die vorherige. Wenn eine Überprüfung auf der Stufe Trusted oder Voll fehlschlägt, kann sich das Telefon nicht mehr an der OpenScape Voice registrieren.

- **Keine**:
  Die Standardeinstellung. Es erfolgt keine Überprüfung des empfangenen Zertifikats. Das empfangene Zertifikat wird nur verwendet, um eine verschlüsselte Verbindung bereitzustellen.
- **Trusted**:
  Das Telefon überprüft das Ablaufdatum und die Signatur des empfangenen Zertifikats.

- **Voll**:
  Das Telefon überprüft das Ablaufdatum, die Signatur und die Zertifikatnutzungs-Felder des empfangenen Zertifikats.

Um die Verifizierung zu aktivieren, führen Sie die folgenden Schritte aus:

> ***HINWEIS:*** Bei OpenStage-Telefonen mit der Firmware-Version V3 oder höher wird Schritt 1 ausgeführt. Bei älteren Firmware-Versionen und optiPoint-Telefonen wird Schritt 2 ausgeführt.

1. Gehen Sie zu **IP Devices** >**IP Phone Konfiguration** >**Security Einstellungen** >**Register „Certificate Policy“**. Wählen Sie unter **SIP Server Authentication Policy** eine Verifizierungsstufe aus. Klicken Sie auf **Sichern**.
2. Gehen Sie zu **IP Devices** >**IP Phone Konfiguration** >**Signaling und Payload Encryption**>**SIP Einstellungen** und aktivieren Sie die Option **TLS Server Validierung**.

16.4.3 Verteilen von neuen Web Based Management (WBM)-Zertifikaten an Telefone

Unify-Telefone werden über eine sichere WBM-Schnittstelle verwaltet und alle Telefone werden standardmäßig mit einem Zertifikat ausgeliefert. Die Zertifikate für die WBM-Schnittstelle können manuell oder automatisch über den Deployment Service verteilt werden.

16.4.3.1 Manuelle Verteilung

1. Gehen Sie zu **IP Devices** >**IP Phone Konfiguration** >**Security Einstellungen**>**Register „WBM Server Zertifikat“**.
2. Klicken Sie auf **Zertifikat importieren**. Unter **Zertifikatstyp** wählen Sie **WBM Server Zertifikat**. Aktivieren Sie die Option **Zertifikat in DLS importieren und auf Gerät aktivieren (1-Step)**. Wählen Sie **Import über: PKI**. Wählen Sie unter **Import von PKI** die PKI, die Sie verwenden möchten. Klicken Sie abschließend auf **OK**.
3. Das Zertifikat wird von DLS automatisch generiert und an das Telefon verteilt. Warten Sie einige Sekunden und klicken Sie dann auf **Aktualisieren**. In den Feldern für Importiertes Zertifikat und Aktives Zertifikat sollten nun die Informationen des neuen Zertifikats angezeigt werden. Wenn nur das Feld Importiertes Zertifikat Informationen enthält, wurde möglicherweise in Schritt 2 die Option “Auf dem Gerät aktivieren” nicht ausgewählt. In diesem Fall aktivieren Sie die Option **Zertifikat aktivieren** und klicken auf **Sichern**. Dadurch wird das Zertifikat auf dem Telefon aktiviert.

16.4.3.2 Automatische Verteilung

1. Gehen Sie zu **Administration** >**Automatische Zertifikatsverteilung**.
2. Klicken Sie auf **Neu**. Wählen Sie unter**Standort** einen Standort aus. Unter **Zertifikatstyp** wählen Sie **WBM Server Zertifikat (IP Phone)**. Klicken Sie auf **Sichern**.

HINWEIS: Alle Telefone, die über diesen Standort definiert sind, erhalten neue WBM-Zertifikate. Standorte können definiert werden unter **Administration** >**Server Konfiguration** >**Standort**.

3. Klicken Sie auf **Zertifikat importieren**. Wählen Sie **Import über: PKI**. Wählen Sie Ihre PKI unter **Import von PKI**. Klicken Sie auf **OK**.
4. Wählen Sie unter **Verteilzeitpunkt** ein Datum und eine Uhrzeit für die Verteilung der Zertifikate. Klicken Sie auf **Sichern**.
5. Aktivieren Sie das Kontrollkästchen **Zertifikat / PKI Konfiguration aktivieren**. Klicken Sie auf **Sichern**.

Wenn Sie auf **Sichern** klicken, erstellt der Deployment Service automatisch Jobs für die Verteilung neuer WBM-Zertifikate an alle Telefone, die über diesen Standort definiert sind. Der Job-Fortschritt kann unter **Job Koordination** > **Job Kontrolle** überwacht werden. Sobald der Job abgeschlossen ist, können Sie sich die neuen Zertifikatsinformationen anzeigen lassen über **IP Devices** >**IP Phone Konfiguration** >**Security Einstellungen** >**Register „WBM Server Zertifikate“**.

Ein Zertifikat, dass automatisch verteilt wurde, wird nur im Feld Aktives Zertifikat angezeigt, jedoch nicht im Feld Importiertes Zertifikat. Das Feld Importiertes Zertifikat wird für die manuelle Verteilung verwendet. Wenn Sie in der Vergangenheit bereits Zertifikate „manuell“ verteilt haben, ist ggf. noch ein älteres Zertifikat vorhanden. Dieses hat keine Auswirkungen auf das derzeit aktive Zertifikat.

16.4.4 Sicherer Modus für Telefone (Secure Modus)

Standardmäßig kommunizieren Telefone mit dem Deployment Service über eine Standard-TLS-Verbindung. Wenn ein höherer Grad an Sicherheit gewünscht wird, können die Telefone so konfiguriert werden, das sie mit dem Deployment Service im Secure Modus kommunizieren. Im Secure Modus erfolgt die Kommunikation über Mutual TLS (MTLS).

MTLS bietet den Vorteil einer gegenseitig authentifizierten Verbindung, d. h. der Deployment Service verifiziert das Telefon und das Telefon verifiziert den Deployment Service. Wenn eine der beiden Seiten die Gegenseite nicht verifizieren kann, schlägt die Verbindung fehl. Diese Methode bietet einen zusätzlichen Schutz für das Telefon, da sie verhindert, dass ein beliebiger anderer Deployment Service eine Verwaltungsverbindung zum Telefon herstellt.

16.4.4.1 Einstellen der Workpoint Interface Konfiguration (PKI)

In diesem Abschnitt wird beschrieben, wie Sie die PKI anpassen müssen, um die Telefone im Secure Modus zu betreiben.

1. Erstellen Sie eine neue PKI oder verwenden Sie eine vorhandene, wie beschrieben in Abschnitt 16.4.1, “Erstellen einer neuen PKI”.
2. Gehen Sie zu **Administration** > **Workpoint Interface Konfiguration**.

3. Wählen Sie im Register **Secure Modus** unter **Server Credentials** den Eintrag **PKI Konfiguration**. Wählen Sie Ihre PKI, klicken Sie auf **OK** und dann auf **Sichern**.
4. Klicken Sie auf **Neu**. Auf Basis der in Schritt 1 ausgewählten PKI wird ein neues Server Credential für den Deployment Service erstellt und als neuer Eintrag in der Tabelle angezeigt. Es sollte standardmäßig aktiviert sein. Wenn dies nicht der Fall ist, wählen Sie das Credential aus und klicken auf **Aktivieren**.
5. Wiederholen Sie die Schritte 2 und 3 für **Client Credentials**.
6. Nachdem die neue PKI aktiviert wurde, können Sie die Standard-Credentials problemlos löschen.

16.4.4.2 Einrichten des Secure Modus für Telefone

1. Erstellen Sie die PKI in der Workpoint Interface Konfiguration wie beschrieben im Abschnitt 16.4.4.1, “Einstellen der Workpoint Interface Konfiguration (PKI)”.
2. Um den Secure Modus für Telefone einzustellen, gehen Sie zu **IP Devices**>**IP Device Verwaltung**> **IP Device Konfiguration** >**Register „DLS Verbindung“**
3. Aktivieren Sie unter **Sicherheitseinstellungen** die Option **Secure Modus erforderlich**. Beim **PIN Modus** haben Sie die Wahl zwischen Keine PIN, Standard PIN oder Individuelle PIN. Eine PIN verschlüsselt die Zertifikatinformationen des Telefons bei deren Übertragung auf das Telefon. Die Standardeinstellung lautet Standard PIN. Dies bedeutet, dass die vom DLS generierte PIN verwendet wird. Diese finden Sie auf dem Bildschirm Workpoint Interface Konfiguration. Wenn eine PIN verwendet wird, dann muss diese PIN am Telefon eingegeben werden, um die Einrichtung des Secure Modus abzuschließen.
4. Klicken Sie auf **Sichern**. Der Deployment Service übermittelt die neuen Zertifikatsinformationen an das Telefon. Wenn eine PIN verwendet wird, dann muss diese PIN am Telefon eingegeben werden, um die Einrichtung des Secure Modus abzuschließen. Melden Sie sich an einem OpenStage-Telefon als Admin an und gehen Sie zu **Admin** >**Network** >**Update Service (DLS)**. Unter **Security Status** wird die Eingabe der PIN erwartet. Geben Sie die PIN in das Feld **Security PIN** ein. Nach Eingabe der PIN drücken Sie auf **Save & Exit** (Speichern & beenden). Die Einrichtung des Secure Modus ist nun abgeschlossen.
5. Der Übergang vom unsicheren zum sicheren Modus (Secure Modus) kann auf dem Register **Security Status Protokoll** überwacht werden. Sie können den Secure Modus für ein Telefon ausschalten, indem Sie das Kontrollkästchen Secure Modus erforderlich deaktivieren.

> ***HINWEIS:*** Wenn ein Telefon sich im Secure Modus befindet und deshalb nicht mit einem DLS kommunizieren kann, können Sie den Secure Mode für das Telefon manuell deaktivieren. Melden Sie sich an einem OpenStage-Telefon als Admin an, gehen Sie zu **Admin** >**Network** >**Update Service (DLS)** >**Options** und wählen Sie **Default Security**. Dadurch wird das Telefon in den Standard-Sicherheitsmodus zurückgesetzt, und kann mit jedem beliebigen Deployment Service kommunizieren. Wenn das Telefon wieder mit dem vorhandenen Deployment Service kommunizieren soll, muss der Deployment Service den Secure Modus auf dem Telefon deaktivieren.

16.4.5 Ersetzen der DLS-Web-Schnittstelle und der API-Zertifikate

Der Deployment Service verfügt über eine Web-Schnittstelle und eine API-Schnittstelle. Diese Schnittstellen werden für die Kommunikation mit einem Webbrowser oder dem OpenScape Voice Assistant verwendet. Daher kann es wünschenswert sein, diese Schnittstellen in die PKI des Kunden zu integrieren und nicht in die interne PKI des Deployment Service.

1. Gehen Sie zu **Administration**>**Server Konfiguration**>**TLS Connector Konfiguration**.
2. Klicken Sie auf **Zertifikat importieren und aktivieren**. Wählen Sie die Option **DLS Client GUI**. Wählen Sie **Import über: Datei** und dann **Durchsuchen** und suchen Sie nach dem Schlüsselspeicher im Format PKCS#12. Klicken Sie auf **OK**. Das Zertifikat wird importiert und aktiviert.

3. Wiederholen Sie Schritt 2 für die DLS API. Verwenden Sie denselben PKCS#12-Schlüsselspeicher.

16.4.6 SHA1-Konfiguration für AutoSPE

Das interne Plug-In, das von DLS-intern standardmäßig für die Erzeugung von internen CAs verwendet wird, hat zwei CA-Roots:

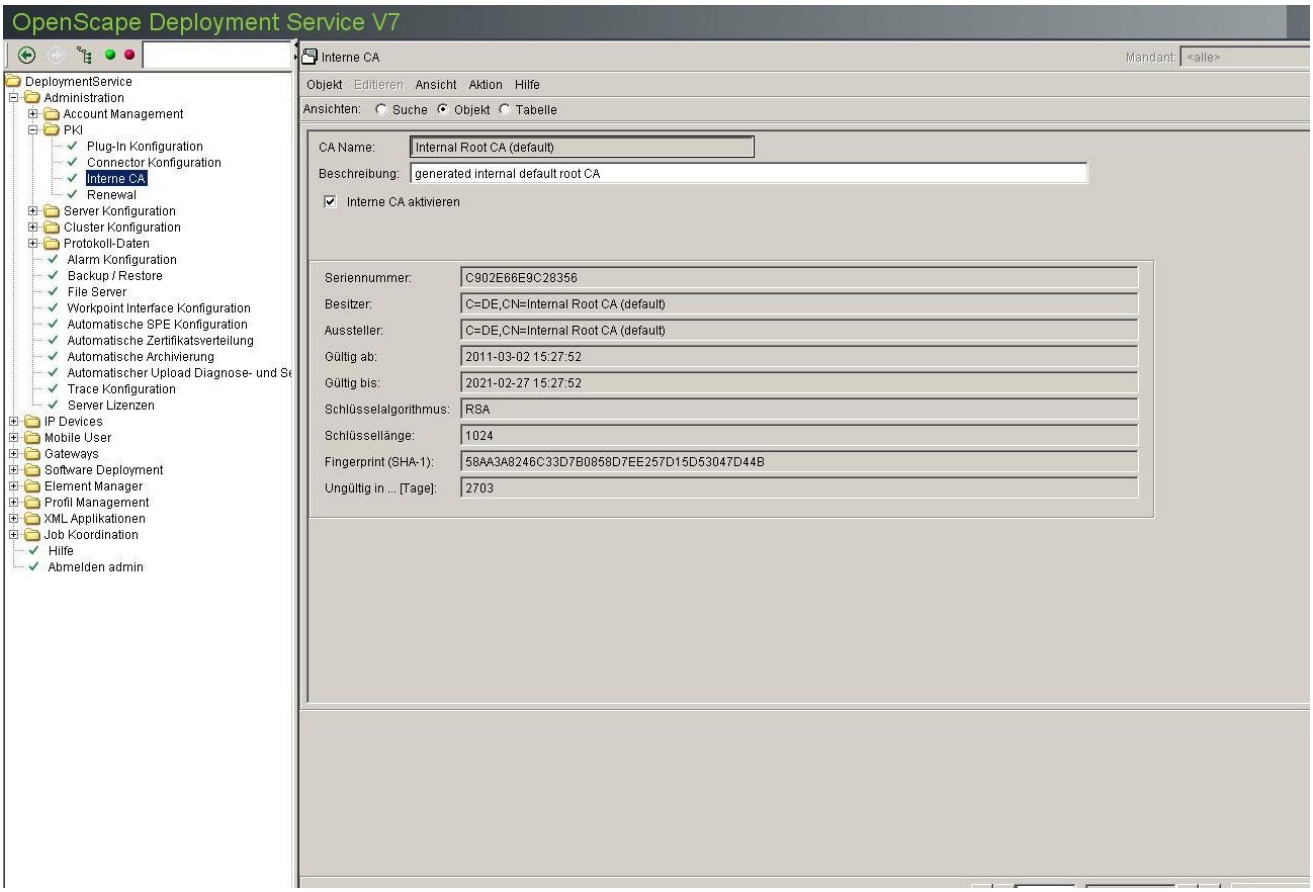
- **Internal Root CA (default)**
- **Internal Root CA (default) SHA1**

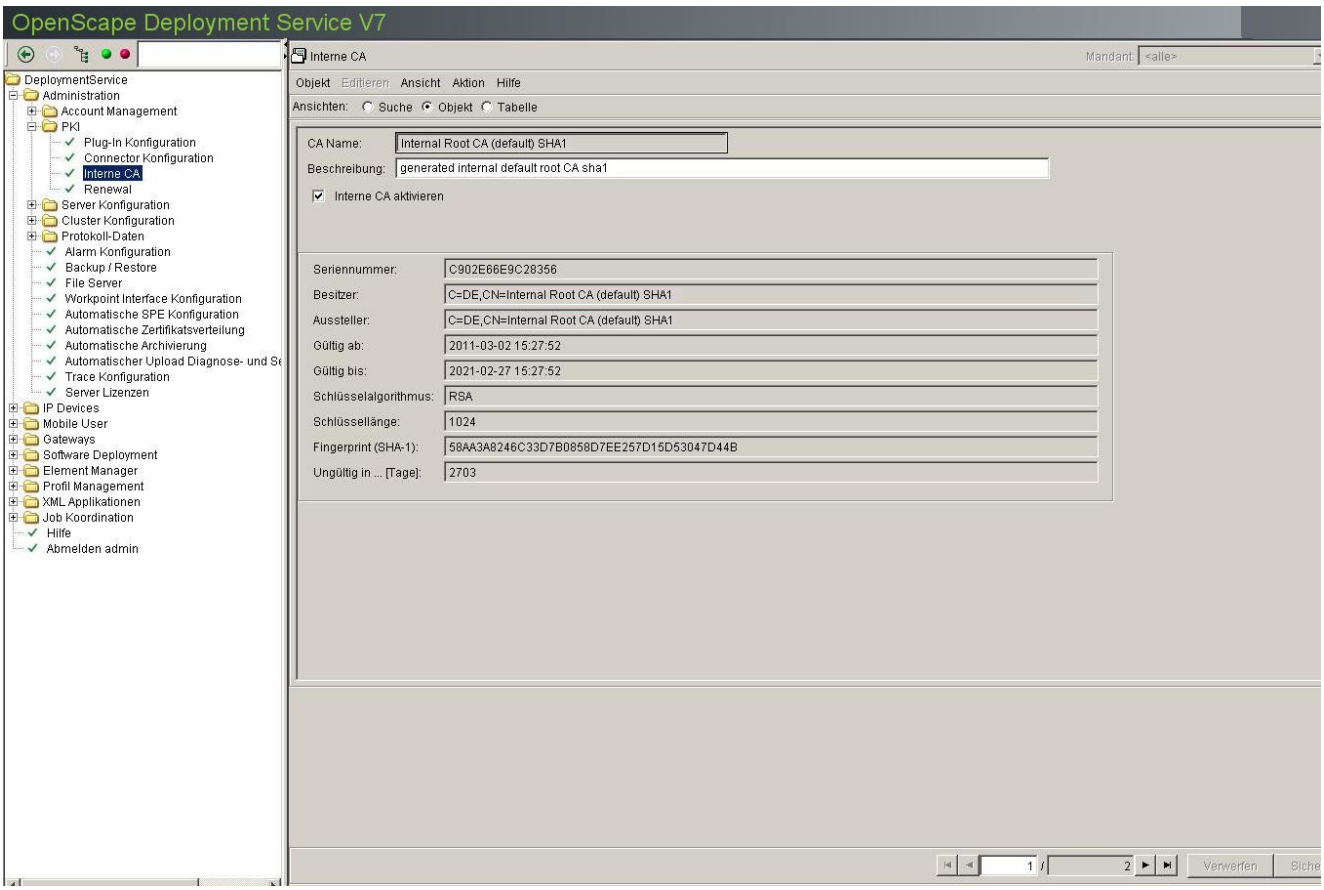
  „Internal Root CA (default) SHA1“ wird mit dem SHA-1 Signaturalgorithmus generiert, der von HFA-Telefonen akzeptiert wird. Das Suffix SHA1 wird verwendet, um diese CA von der Default CA mit dem Signaturalgorithmus SHA256 zu unterscheiden.

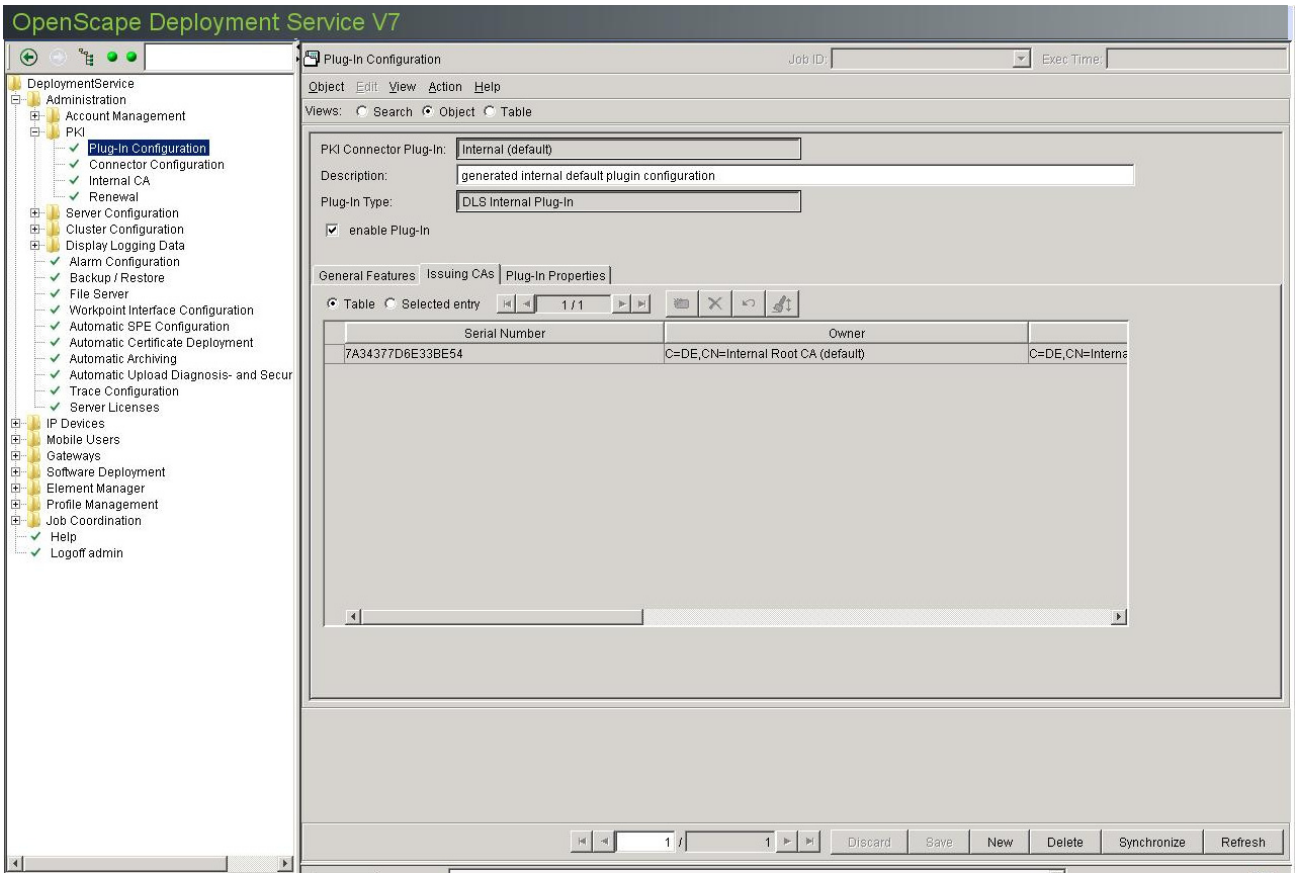
Wählen Sie Administration > PKI > Interne CA;CA intern

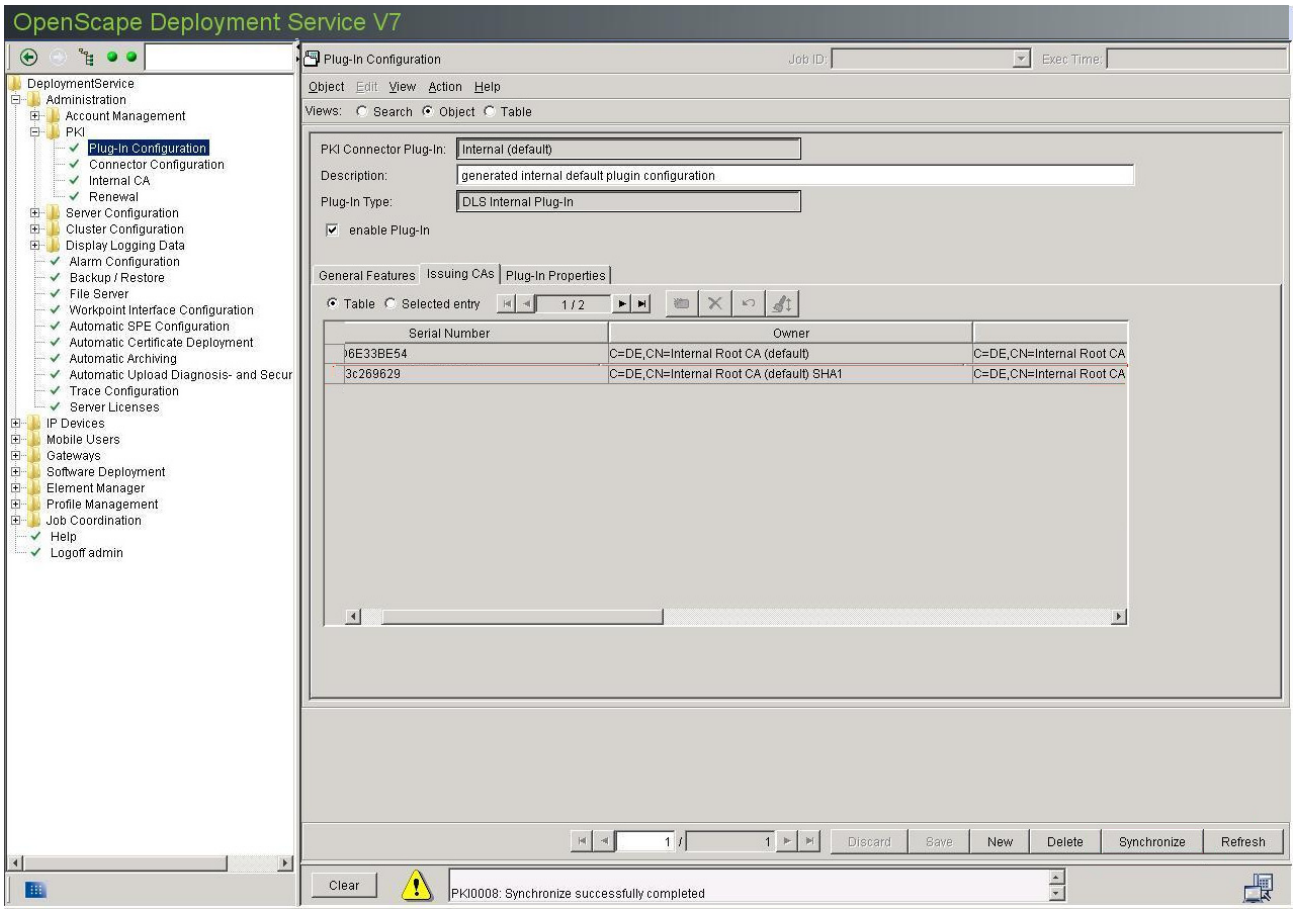
Unter Register „Ausstellende Zertifizierungsstellen“ wird ein Zertifikat angezeigt. Klicken Sie auf die Schaltfläche **Synchronisieren**. Unter CA (SHA-1) erscheint ein zweites Zertifikat.

> ***HINWEIS:*** Nach einer Aktualisierung auf die DLS-Version mit diesem Patch (oder einer Neuinstallation) sollten Sie in der Lage sein, die beiden Einträge in internen Oberflächenmaske zu sehen.


OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Konfiguration
Connector Konfiguration
Interne CA
Renewal
Server Konfiguration
Cluster Konfiguration
Protokoll-Daten
Alarm Konfiguration
Backup / Restore
File Server
Workpoint Interface Konfiguration
Automatische SPE Konfiguration
Automatische Zertifikatsverteilung
Automatische Archivierung
Trace Konfiguration
Server Lizenzen
IP Devices
Mobile User
Gateways
Software Deployment
Element Manager
Profil Management
XML Applikationen
Job Koordination
Hilfe
Abmelden admin
Interne CA
Mandant: <alle>
Objekt Editieren Ansicht Aktion Hilfe
Ansichten: Suche Objekt Tabelle
CA Name: Internal Root CA (default)
Beschreibung: generated internal default root CA
Interne CA aktivieren
Seriennummer: C902E66E9C28356
Besitzer: C=DE,CN=Internal Root CA (default)
Aussteller: C=DE,CN=Internal Root CA (default)
Gültig ab: 2011-03-02 15:27:52
Gültig bis: 2021-02-27 15:27:52
Schlüsselalgorithmus: RSA
Schlüssellänge: 1024
Fingerprint (SHA-1): 58AA3A8246C33D7B0858D7EE257D15D53047D44B
Ungültig in ... [Tage]: 2703


OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Konfiguration
Connector Konfiguration
Interne CA
Renewal
Server Konfiguration
Cluster Konfiguration
Protokoll-Daten
Alarm Konfiguration
Backup / Restore
File Server
Workpoint Interface Konfiguration
Automatische SPE Konfiguration
Automatische Zertifikatsverteilung
Automatische Archivierung
Trace Konfiguration
Server Lizenzen
IP Devices
Mobile User
Gateways
Software Deployment
Element Manager
Profil Management
XML Applikationen
Job Koordination
Hilfe
Abmelden admin
Interne CA
Mandant:
<alle>
Objekt Editieren Ansicht Aktion Hilfe
Ansichten: Suche Objekt Tabelle
CA Name: Internal Root CA (default) SHA1
Beschreibung: generated internal default root CA sha1
Interne CA aktivieren
Seriennummer: C902E66E9C28356
Besitzer: C=DE,CN=Internal Root CA (default) SHA1
Aussteller: C=DE,CN=Internal Root CA (default) SHA1
Gültig ab: 2011-03-02 15:27:52
Gültig bis: 2021-02-27 15:27:52
Schlüsselalgorithmus: RSA
Schlüssellänge: 1024
Fingerprint (SHA-1): 58AA3A8246C33D7B0858D7EE257D15D53047D44B
Ungültig in ... [Tage]: 2703
1 / 2
Verwerfen


OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Configuration
Connector Configuration
Internal CA
Renewal
Server Configuration
Cluster Configuration
Display Logging Data
Alarm Configuration
Backup / Restore
File Server
Workpoint Interface Configuration
Automatic SPE Configuration
Automatic Certificate Deployment
Automatic Archiving
Automatic Upload Diagnosis- and Secur
Trace Configuration
Server Licenses
IP Devices
Mobile Users
Gateways
Software Deployment
Element Manager
Profile Management
Job Coordination
Help
Logoff admin
Plug-In Configuration
Job ID:
Exec Time:
Object Edit View Action Help
Views: Search Object Table
PKI Connector Plug-In: Internal (default)
Description: generated internal default plugin configuration
Plug-In Type: DLS Internal Plug-In
enable Plug-In
General Features Issuing CAs Plug-In Properties
Table Selected entry
1 / 1
Serial Number
Owner
7A34377D6E33BE54
C=DE,CN=Internal Root CA (default)
C=DE,CN=Interna
Discard
Save
New
Delete
Synchronize
Refresh

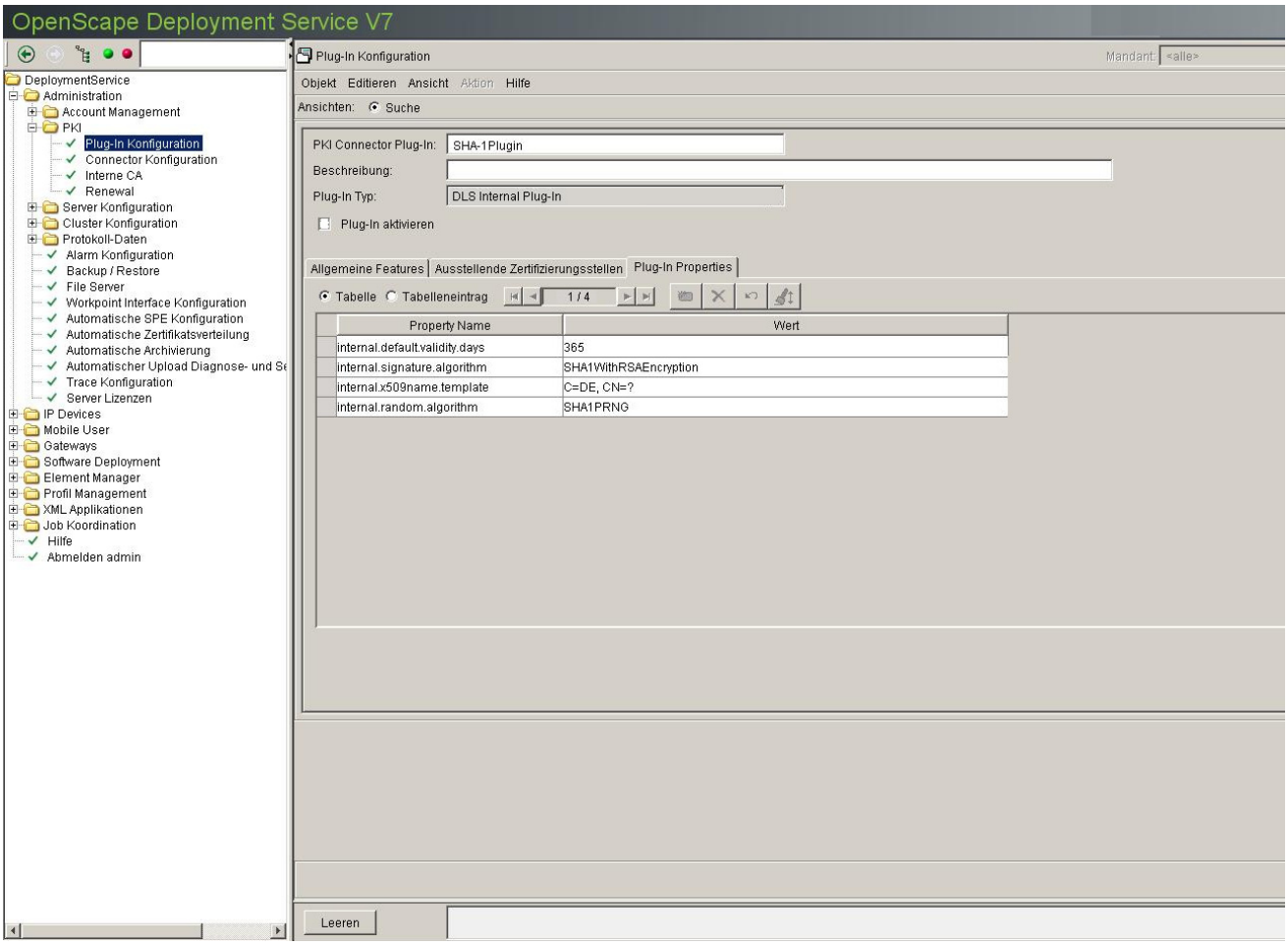


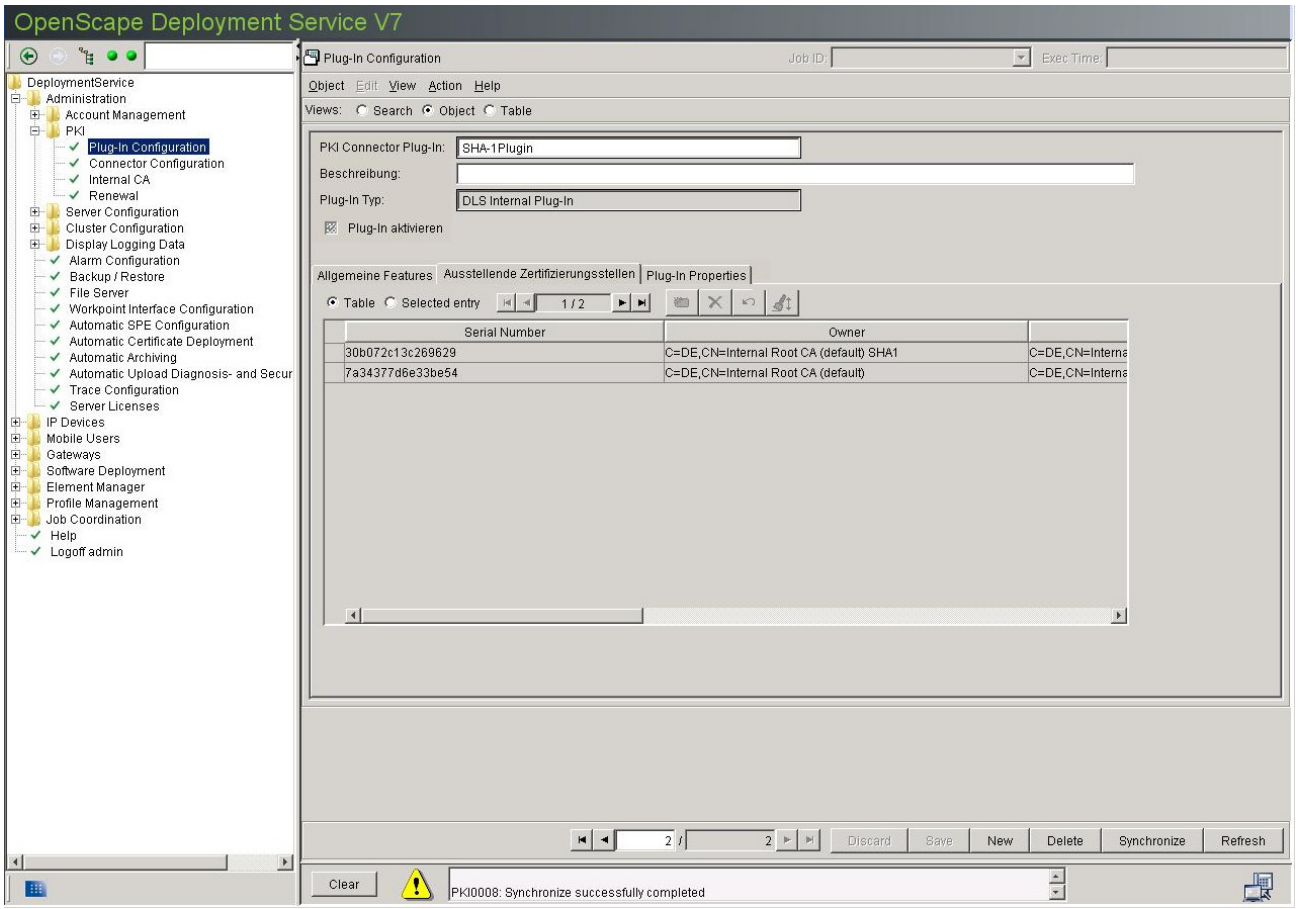
16.4.6.1 Erstellen einer PKI Konfiguration zur Verwendung durch HFA und AutoSPE

Nachfolgend wird beschrieben, wie Sie SHA1 innerhalb des CA-Zertifikats für AutoSPE konfigurieren:

1. Erstellen Sie ein neues Plug-In

   Erstellen Sie ein neues Plug-In mit dem Signaturalgorithmus SHA1 (so dass HFA die Zertifikate akzeptiert); siehe Abschnitt 6.2.1, “Plug-In Konfiguration”.

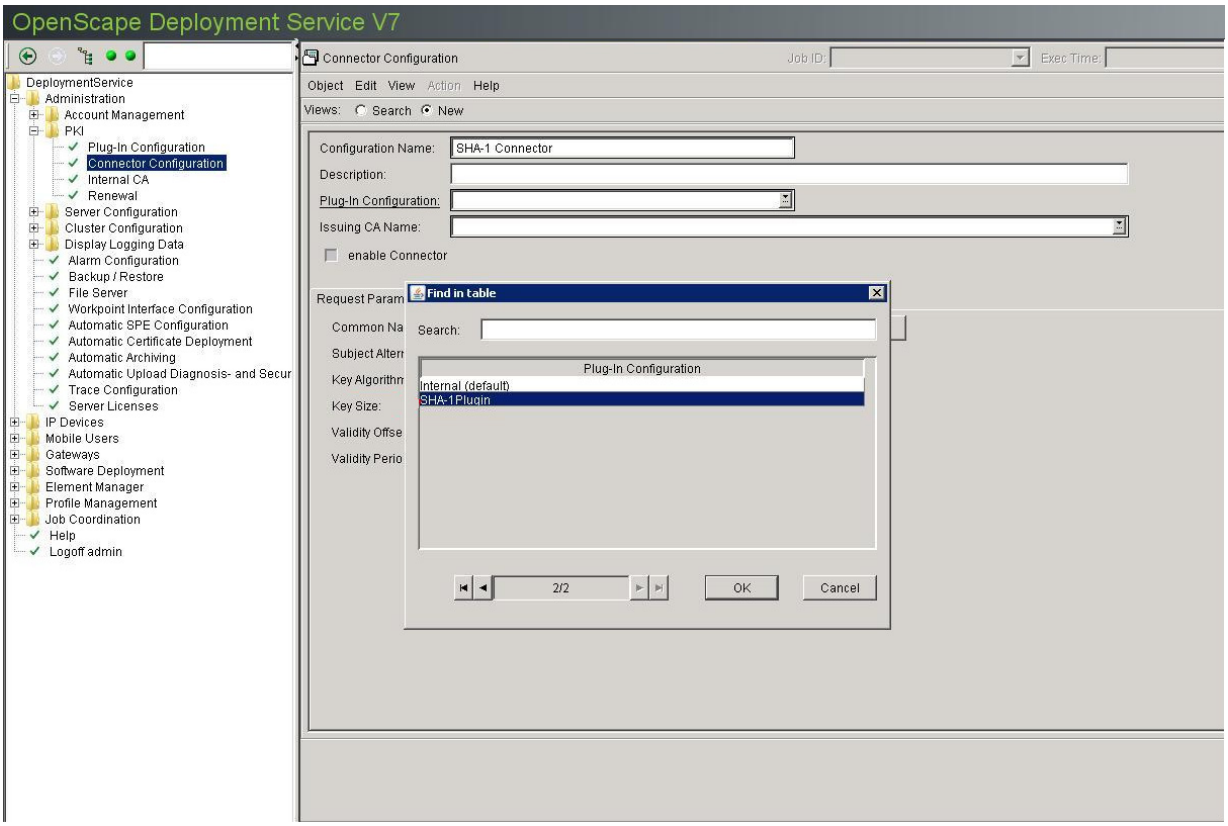

OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Konfiguration
Connector Konfiguration
Interne CA
Renewal
Server Konfiguration
Cluster Konfiguration
Protokoll-Daten
Alarm Konfiguration
Backup / Restore
File Server
Workpoint Interface Konfiguration
Automatische SPE Konfiguration
Automatische Zertifikatsverteilung
Automatische Archivierung
Trace Konfiguration
Server Lizenzen
IP Devices
Mobile User
Gateways
Software Deployment
Element Manager
Profil Management
XML Applikationen
Job Koordination
Hilfe
Abmelden admin
Plug-In Konfiguration
Mandant:
Objekt Editieren Ansicht Aktion Hilfe
Ansichten: Suche
PKI Connector Plug-In: SHA-1Plugin
Beschreibung:
Plug-In Typ: DLS Internal Plug-In
Plug-In aktivieren
Allgemeine Features
Ausstellende Zertifizierungsstellen
Plug-In Properties
Tabelle
Tabelleneintrag
1 / 4
Property Name
Wert
internal.default.validity.days
365
internal.signature.algorithm
SHA1WithRSAEncryption
internal.x509name.template
C=DE, CN=?
internal.random.algorithm
SHA1PRNG
Leeren

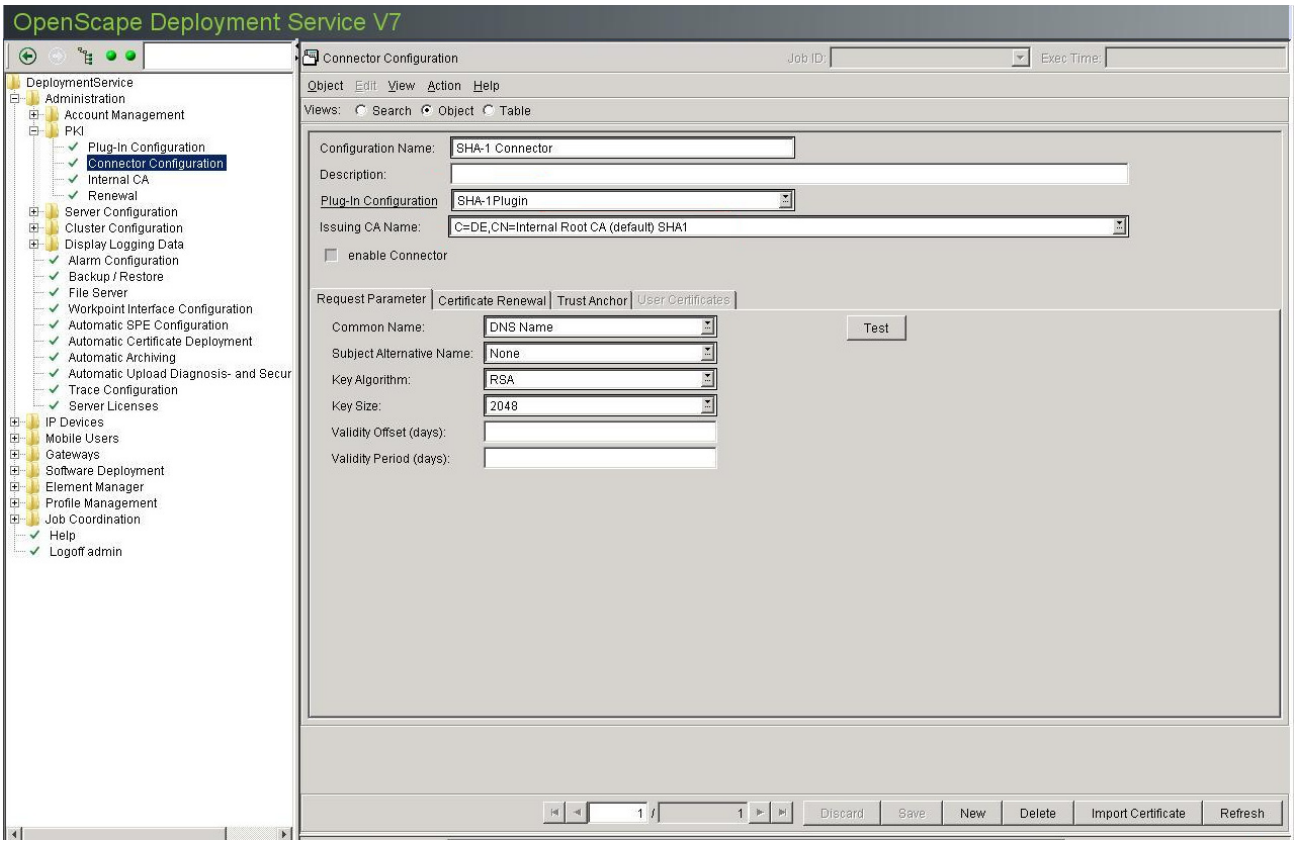


2. Erstellen Sie eine Connector Konfiguration für AutoSPE

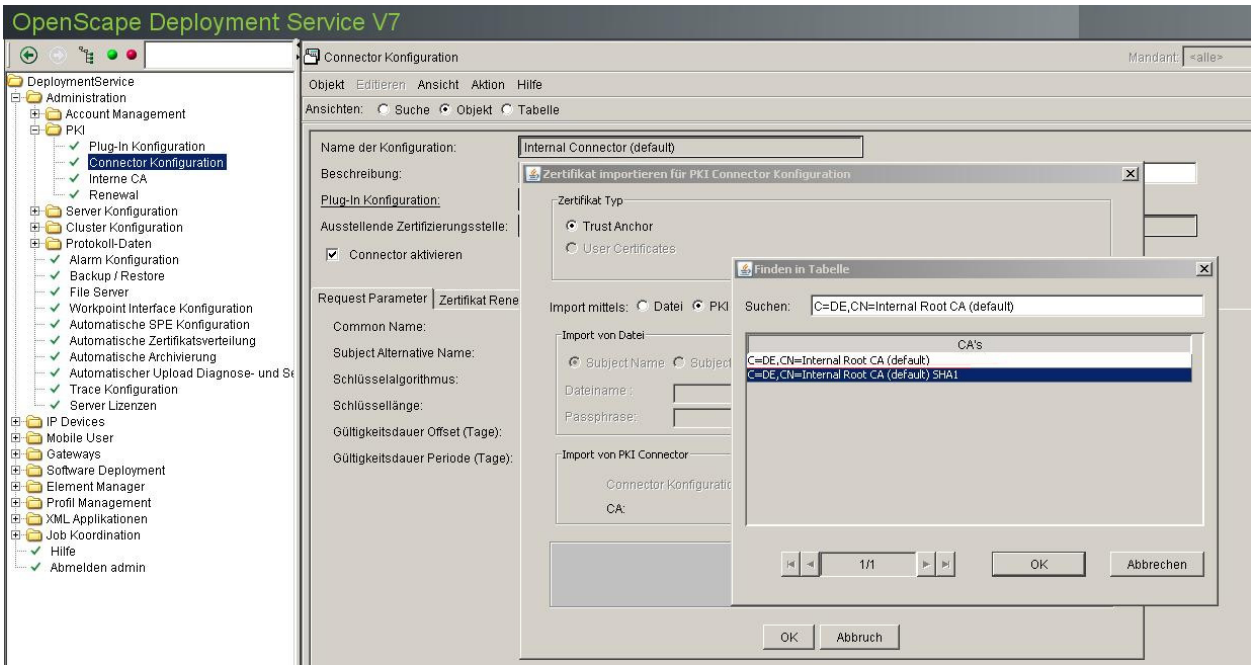
   Erstellen Sie eine neue Connector Konfiguration, die auf das neu erstellte Plug-In verweist.

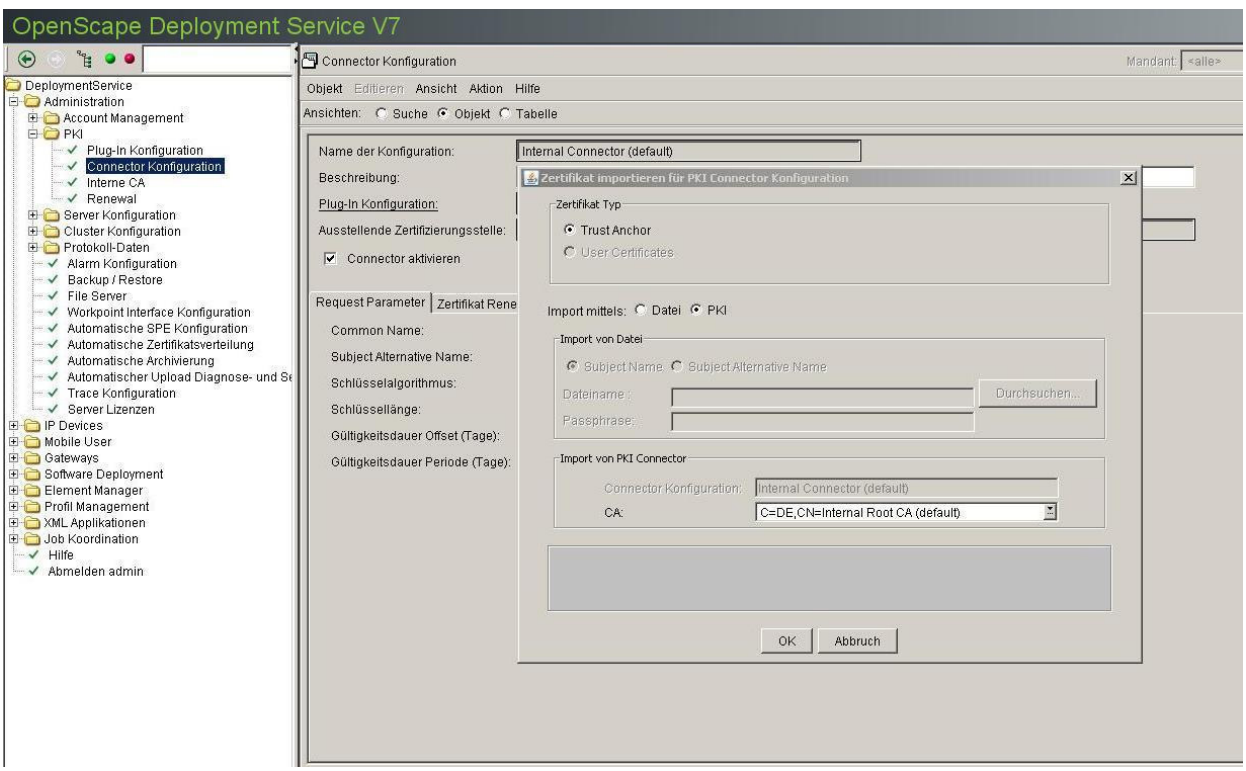
   WICHTIG: Es ist sehr wichtig, dass Sie die richtige ausstellende Zertifizierungsstelle auswählen, und zwar sowohl für den Trust Anchor als auch für die Connector Konfiguration (hier MUSS das SHA1-Zertifikat ausgewählt werden).

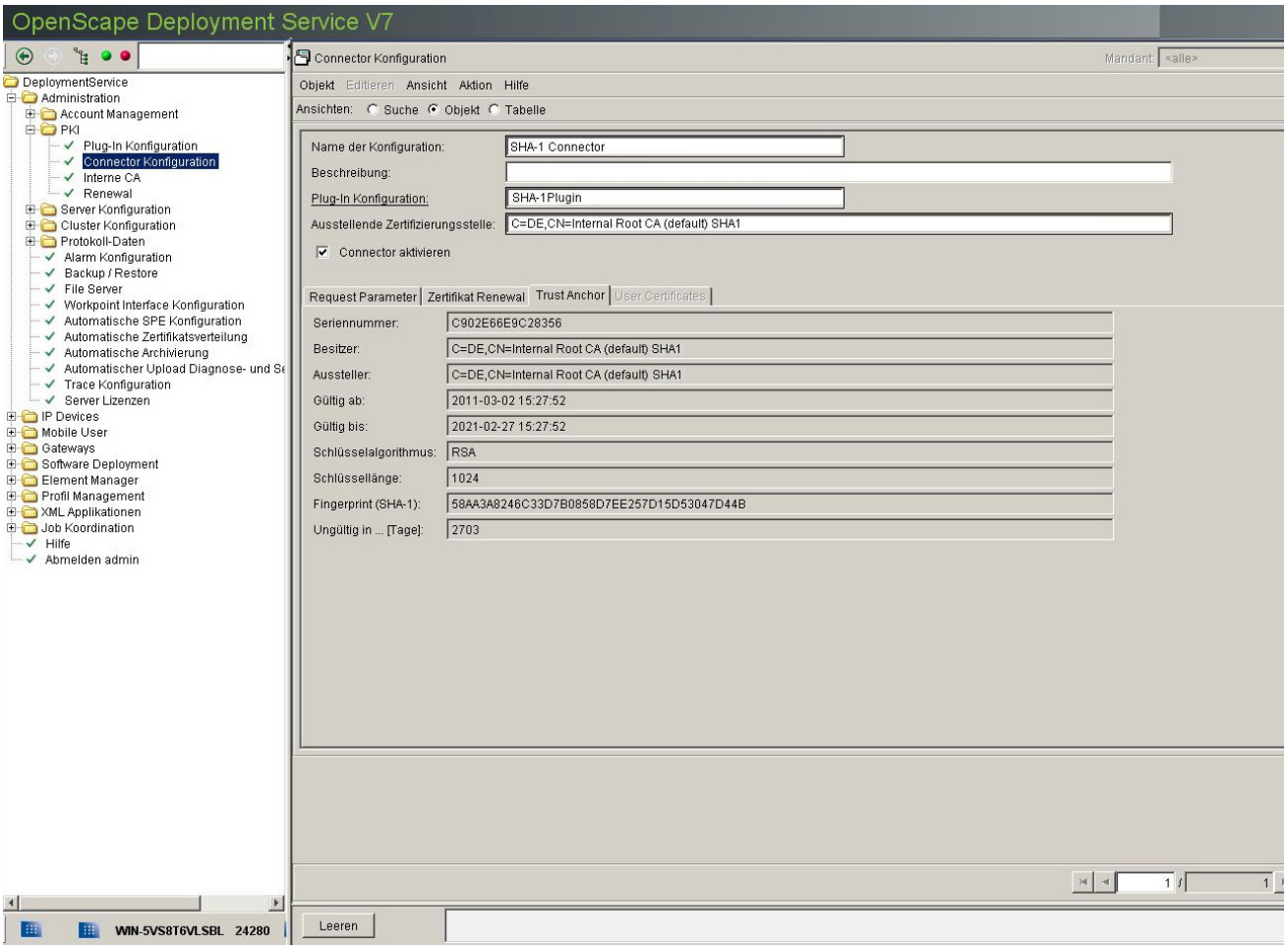

OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Configuration
Connector Configuration
Internal CA
Renewal
Server Configuration
Cluster Configuration
Display Logging Data
Alarm Configuration
Backup / Restore
File Server
Workpoint Interface Configuration
Automatic SPE Configuration
Automatic Certificate Deployment
Automatic Archiving
Automatic Upload Diagnosis- and Secur
Trace Configuration
Server Licenses
IP Devices
Mobile Users
Gateways
Software Deployment
Element Manager
Profile Management
Job Coordination
Help
Logoff admin
Connector Configuration
Job ID:
Exec Time:
Object Edit View Action Help
Views: Search New
Configuration Name: SHA-1 Connector
Description:
Plug-In Configuration:
Issuing CA Name:
enable Connector
Request Param
Common Na
Subject Alter
Key Algorithm
Key Size:
Validity Offse
Validity Perio
Find in table
Search:
Plug-In Configuration
Internal (default)
SHA-1Plugin
2/2
OK
Cancel

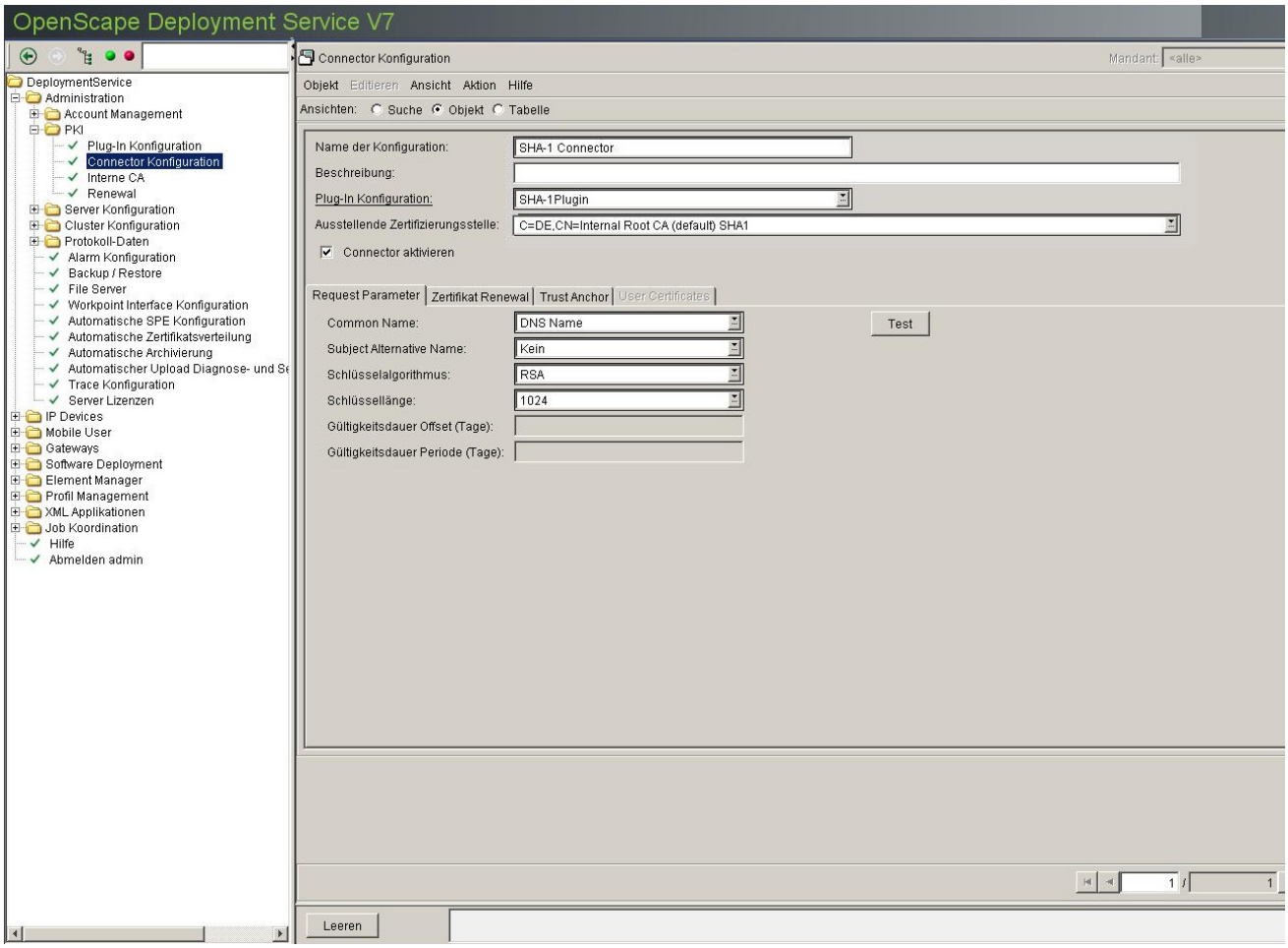


3. Importieren Sie den Trust Anchor für diese Konfiguration


OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Konfiguration
Connector Konfiguration
Interne CA
Renewal
Server Konfiguration
Cluster Konfiguration
Protokoll-Daten
Alarm Konfiguration
Backup / Restore
File Server
Workpoint Interface Konfiguration
Automatische SPE Konfiguration
Automatische Zertifikatsverteilung
Automatische Archivierung
Automatischer Upload Diagnose- und Se
Trace Konfiguration
Server Lizenzen
IP Devices
Mobile User
Gateways
Software Deployment
Element Manager
Profil Management
XML Applikationen
Job Koordination
Hilfe
Abmelden admin
Connector Konfiguration
Mandant:
<alle>
Objekt Editieren Ansicht Aktion Hilfe
Ansichten: Suche Objekt Tabelle
Name der Konfiguration:
Internal Connector (default)
Beschreibung:
Plug-In Konfiguration:
Ausstellende Zertifizierungsstelle:
Connector aktivieren
Request Parameter
Zertifikat Rene
Common Name:
Subject Alternative Name:
Schlüsselalgorithmus:
Schlüssellänge:
Gültigkeitsdauer Offset (Tage):
Gültigkeitsdauer Periode (Tage):
Zertifikat importieren für PKI Connector Konfiguration
Zertifikat Typ
Trust Anchor
User Certificates
Import mittels: Datei PKI
Import von Datei
Subject Name
Dateiname :
Passphrase:
Import von PKI Connector
Connector Konfiguratio
CA:
Finden in Tabelle
Suchen:
C=DE,CN=Internal Root CA (default)
CA's
C=DE,CN=Internal Root CA (default)
C=DE,CN=Internal Root CA (default) SHA1
1/1
OK
Abbrechen
OK
Abbruch


OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Konfiguration
Connector Konfiguration
Interne CA
Renewal
Server Konfiguration
Cluster Konfiguration
Protokoll-Daten
Alarm Konfiguration
Backup / Restore
File Server
Workpoint Interface Konfiguration
Automatische SPE Konfiguration
Automatische Zertifikatsverteilung
Automatische Archivierung
Automatischer Upload Diagnose- und Se
Trace Konfiguration
Server Lizenzen
IP Devices
Mobile User
Gateways
Software Deployment
Element Manager
Profil Management
XML Applikationen
Job Koordination
Hilfe
Abmelden admin
Connector Konfiguration
Mandant:
<alle>
Objekt Editieren Ansicht Aktion Hilfe
Ansichten: Suche Objekt Tabelle
Name der Konfiguration:
Internal Connector (default)
Beschreibung:
Plug-In Konfiguration:
Ausstellende Zertifizierungsstelle:
Connector aktivieren
Request Parameter
Zertifikat Rene
Common Name:
Subject Alternative Name:
Schlüsselalgorithmus:
Schlüssellänge:
Gültigkeitsdauer Offset (Tage):
Gültigkeitsdauer Periode (Tage):
Zertifikat importieren für PKI Connector Konfiguration
Zertifikat Typ
Trust Anchor
User Certificates
Import mittels: Datei PKI
Import von Datei
Subject Name Subject Alternative Name
Dateiname :
Durchsuchen...
Passphrase:
Import von PKI Connector
Connector Konfiguration:
Internal Connector (default)
CA:
C=DE,CN=Internal Root CA (default)
OK
Abbruch

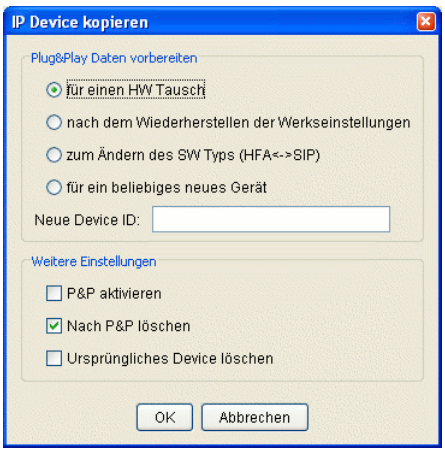

OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Konfiguration
Connector Konfiguration
Interne CA
Renewal
Server Konfiguration
Cluster Konfiguration
Protokoll-Daten
Alarm Konfiguration
Backup / Restore
File Server
Workpoint Interface Konfiguration
Automatische SPE Konfiguration
Automatische Zertifikatsverteilung
Automatische Archivierung
Automatischer Upload Diagnose- und Se
Trace Konfiguration
Server Lizenzen
IP Devices
Mobile User
Gateways
Software Deployment
Element Manager
Profil Management
XML Applikationen
Job Koordination
Hilfe
Abmelden admin
WIN-5VS8T6VLSBL 24280
Connector Konfiguration
Mandant: <alle>
Objekt Editieren Ansicht Aktion Hilfe
Ansichten: Suche Objekt Tabelle
Name der Konfiguration: SHA-1 Connector
Beschreibung:
Plug-In Konfiguration: SHA-1Plugin
Ausstellende Zertifizierungsstelle: C=DE,CN=Internal Root CA (default) SHA1
Connector aktivieren
Request Parameter
Zertifikat Renewal
Trust Anchor
User Certificates
Seriennummer: C902E66E9C28356
Besitzer: C=DE,CN=Internal Root CA (default) SHA1
Aussteller: C=DE,CN=Internal Root CA (default) SHA1
Gültig ab: 2011-03-02 15:27:52
Gültig bis: 2021-02-27 15:27:52
Schlüsselalgorithmus: RSA
Schlüssellänge: 1024
Fingerprint (SHA-1): 58AA3A8246C33D7B0858D7EE257D15D53047D44B
Ungültig in ... [Tage]: 2703
Leeren



4. Der Vorgang ist damit abgeschlossen. Dieser Connector kann nun für AutoSPE verwendet werden.

16.5 Austausch eines IP Devices

1. Wählen Sie den Bereich **IP Device Verwaltung** > **IP Device Konfiguration**. Klicken Sie in der Menüleiste auf **Aktion** und wählen Sie die Aktion **IP Device kopieren**.
2. Es öffnet sich folgendes Dialogfenster:



Wählen Sie in der Rubrik **Plug&Play-Daten vorbereiten** die Option **für einen HW Tausch**.

Wenn Sie die Konfigurationsdaten auf dem derzeitigen Stand belassen wollen, aktivieren Sie die Option **P&P aktivieren**. Damit wird der Datensatz für die Übertragung an den Workpoint freigegeben.

3. Stecken Sie den defekten Workpoint ab und stecken Sie den Austausch-Workpoint an.
4. Wenn für den Workpoint vollständiges Plug&Play möglich ist, geschieht die Registrierung und Konfiguration des Austausch-Workpoints automatisch (wie bei Neuinstallation, Abschnitt 16.1 bzw. Abschnitt 16.2).

   Fehlt die Plug&Play-Möglichkeit, muss die Registrierung des Workpoints im DLS manuell unterstützt werden. Die Registrierung ist abhängig vom Vorhandensein eines DHCP-Servres:

   - Ist ein **DHCP-Server nicht vorhanden**:

     Am Workpoint müssen im Menü *Configuration* folgende Daten eingerichtet sein:

     1. DHCP muss auf *off* stehen.
     2. Die IP-Adresse des Workpoints muss eingegeben sein.
     3. Die Netzmaske des Workpoint-Subnetzes muss eingegeben sein.
     4. Die IP-Adresse des Default-Routers muss eingeben sein.
     5. Die *Fully qualified Subscriber Number* muss eingetragen sein.

     Nach dem Speichern der Änderungen und einem Neustart des IP Phones kann vom DLS aus ein Scan durchgeführt werden, um das IP Phone im DLS zu registrieren (siehe Abschnitt 7.4.6, “IP Devices scannen”). Beim Scannen muss die DLS-Adresse mitgesendet werden.

   - Ist ein **DHCP-Server vorhanden**:

Wenn vom DHCP keine DLS-Adressdaten an den Workpoint gesendet werden, starten Sie das IP Device-Scannen. Aktivieren Sie im Scan-Dialog die Optionen **IP Device registrieren** und **Neue IP Device aus den Scan-Ergebnissen registrieren** (siehe Abschnitt 7.4.6, “IP Devices scannen”), um den neuen Workpoint im DLS zu registrieren.

Wenn die DLS-Adressdaten automatisch vom DHCP an den Workpoint gesendet werden, geschieht die Registrierung im DLS automatisch.

Zum Konfigurieren eines DHCP-Servers, um die DLS-Zugangsdaten an die Workpoints zu übertragen, siehe Abschnitt 4.12.4.3, “DHCP-Server für DLS konfigurieren”.

HINWEIS: Erst wenn der neue Workpoint funktioniert, sollten die Daten des alten Workpoints aus der DLS-Datenbank gelöscht werden.

Damit ist der Austausch abgeschlossen.

16.6 Austausch eines alten Workpoints (TDM) durch einen neuen (IP)

Voraussetzungen

- Eine laufende DLS-Infrastruktur (z. B. CLA-, DHCP-, DNS- und FTP-Server).

Durchführen des Austauschs

1. Konfigurieren Sie den Teilnehmer im System neu durch Löschen und neu Anlegen z. B. mithilfe des HiPath 4000 Manager bzw. durch AMO-Konfiguration. Informationen dazu finden Sie in der jeweiligen Dokumentation.
2. Gehen Sie für den weiteren Ablauf wie bei der Neuinstallation eines Workpoints vor (siehe Abschnitt 16.1, “Neuinstallation eines Workpoints bei HiPath 4000”).

Damit ist der Austausch abgeschlossen.

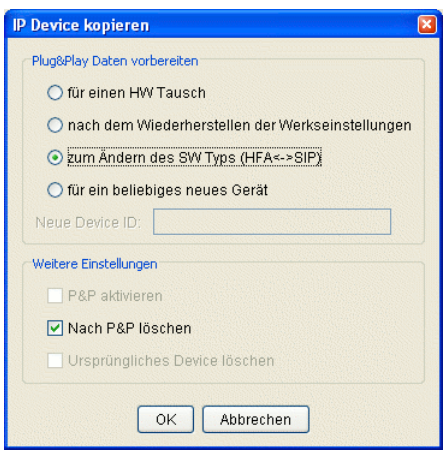
16.7 Austausch von HFA- durch SIP-Software und umgekehrt bei identischer Device ID

Voraussetzungen

- Eine laufende DLS-Infrastruktur (z. B. CLA-, DHCP-, DNS- und FTP-Server).

16.7.1 Austausch HFA- durch SIP-Software

1. Stellen Sie die SIP-Software im DLS bereit (siehe Abschnitt 15.3, “Registrieren von Workpoint-Software und -Dateien”).
2. Klicken Sie in der Menüleiste auf **Aktion** und wählen Sie die Aktion **IP Device kopieren**.
3. Es öffnet sich folgendes Dialogfenster:



   Wählen Sie in der Rubrik **Plug&Play-Daten vorbereiten** die Option **zum Ändern des SW Typs (HFA <-> SIP)**.

   Wenn Sie die Konfigurationsdaten auf dem derzeitigen Stand belassen wollen, aktivieren Sie die Option **P&P aktivieren**. Damit wird der Datensatz für die Übertragung an den Workpoint freigegeben.

4. Legen Sie die erforderlichen Registrierungsdaten fest. Diese Konfiguration ist abhängig vom verwendeten SIP-Server. Bei OpenScape Voice sind dies bei einer Minimalkonfiguration:

   IP Devices > **IP Phone Konfiguration** > **Gateway / Server**

   – **Register „Gateway (HFA) / SIP Server“**:
   Reg-Adr., **Reg-Port**.

   – **Register „SIP Registrierung 1“**:
   SIP Routing, SIP Registrar Adr., **SIP Registrar Port**, **SIP Phone Port**, **RTP Base Port**.

   Es ist empfehlenswert, die Konfigurationsdaten mithilfe von Templates zu verwalten. Siehe hierzu Abschnitt 15.4.1, “Template manuell anlegen”.

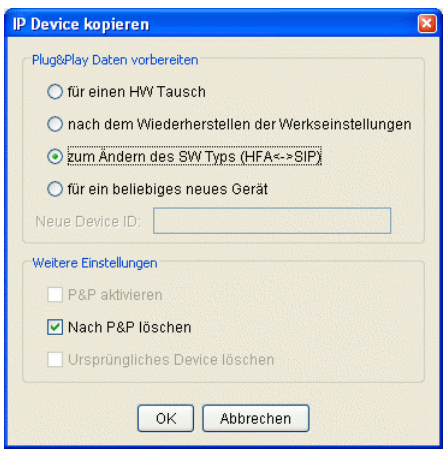
Gegebenenfalls können Sie die Registrierungsdaten auch durch Synchronisation mit der Anlage übernehmen. Siehe hierzu Abschnitt 11.1, “Element Manager Konfiguration”.

5. Starten Sie das Software-Deployment (siehe Abschnitt 15.6.1, “Manuelles Deployment”).

   Nachdem die Software in das Telefon geladen ist, erfolgt ein Neustart des Workpoints. Damit ist der Software-Tausch abgeschlossen.

16.7.2 Austausch SIP- durch HFA-Software

1. Stellen Sie die HFA-Software im DLS bereit (siehe Abschnitt 15.3, “Registrieren von Workpoint-Software und -Dateien”).
2. Klicken Sie in der Menüleiste auf **Aktion** und wählen Sie die Aktion **IP Device kopieren**.
3. Es öffnet sich folgendes Dialogfenster:



   Wählen Sie in der Rubrik **Plug&Play-Daten vorbereiten** die Option **zum Ändern des SW Typs (HFA <-> SIP)**.

   Wenn Sie die Konfigurationsdaten auf dem derzeitigen Stand belassen wollen, aktivieren Sie die Option **P&P aktivieren**. Damit wird der Datensatz für die Übertragung an den Workpoint freigegeben.

4. Legen Sie die erforderlichen Zugangsdaten für den Gateway fest.

   Optional können Sie die Konfigurationsdaten mithilfe von Templates verwalten. Siehe hierzu Abschnitt 15.4.1, “Template manuell anlegen”.

   Gegebenenfalls können Sie die Zugangsdaten auch durch Synchronisation mit der Anlage übernehmen. Siehe hierzu Abschnitt 11.1, “Element Manager Konfiguration”.

5. Starten Sie das Software-Deployment (siehe Abschnitt 15.6.1, “Manuelles Deployment”).

   Nachdem die Software in das Telefon geladen ist, erfolgt ein Neustart des Workpoints. Damit ist der Software-Tausch abgeschlossen.

16.8 Einrichten eines IP Client 130 im DLS

Die nachfolgende Anleitung beschreibt beispielhaft das Einrichten eines optiClient 130 V5.0 als HFA-Client in einer HiPath 4000-Umgebung.

Voraussetzungen

- Eine laufende DLS-Infrastruktur (inklusive vorhandener Anbindung an HiPath 4000).

Ablauf

1. Anlegen der Templates
2. Einstellungen am optiClient 130

16.8.1 Anlegen der Templates

Template: Gateway / Server

In diesem Template werden die Daten für System-Typ (inkl. Standby), Programmaktualisierung, Telefon-Typ und Lizensierung eingetragen.

1. Wählen Sie den Bereich **IP Devices** > **IP Client Konfiguration** > **Gateway / Server** > **Register „Gateway“**.
2. Wählen Sie in der Ansichtenleiste (siehe Abschnitt 5.4.2.3, “Ansichtenleiste”) die Ansicht **Template**.
3. Wählen Sie aus der Liste **System Typ** den Wert **HiPath 4000**.
4. Wechseln Sie zu **Register „Gateway (Standby)“.**
5. Wählen Sie aus der Liste **System Typ** den Wert **Kein Rückfallsystem**.
6. Wechseln Sie zu **Register „SW Deployment“**.
7. Aktivieren Sie die Checkbox **DLS Deployment**, und tragen Sie **Verzeichnis** und **Programmaktualisierungs-Modus** ein.

   Die Angaben bei **Programmaktualisierungs-Modus** bedeuten:

   – **Start**: es wird beim Starten des optiClient 130 überprüft, ob eine neue Version verfügbar ist.

   – **Intervall**: es wird entsprechend dem Wert bei **Update Mechanismus Intervall** alle x Minuten überprüft, ob eine neue Version vorliegt.
8. Wechseln Sie zu **Register „HFA Einstellungen“**.
9. Wählen Sie aus der Liste **Telefon Typ** das Telefon (einschließlich der Beistellgeräte), als das der optiClient 130 dargestellt ist. Zum Beispiel: **Telefon-Typ:** optiPoint 420 standard, **Keymodul-Typ:** optiPoint 420 Key Module und **Keymodul-Maximalanzahl:** 2.
10. Wechseln Sie zu **Register „Lizenzen“**.
11. Tragen Sie unter **HFA Lizenz** bei **Server** und **Port** die IP-Adresse und die Portnummer des Lizenzservers ein.

12. Klicken Sie auf die Schaltfläche **Sichern** und legen Sie im Dialogfenster den Template-Namen fest, z. B. **oC130 Gateway/DLS HP4000**.
13. Wählen Sie den Bereich **IP Devices** > **IP Client Konfiguration** > **Wahlparameter** > **Register „HFA Wahlparameter“**.
14. Wählen Sie in der Ansichtenleiste die Ansicht **Template**.
15. Tragen Sie hier die erforderlichen Daten für den Haupt-Netzzugang ein, z. B. bei Landeskennzahl **49**.
16. Klicken Sie auf die Schaltfläche **Sichern** und legen Sie im Dialogfenster den Template-Namen fest, z. B. **oC130 Wahlparameter HP4000**.
17. Der Name wird nach dem Speichern in der Ansichtenleiste angezeigt.Legen Sie bei Bedarf weitere Templates an, z. B. bei Verfügbarkeit eines LDAP-Servers die entsprechenden Daten im Bereich **LDAP**.

16.8.2 Erstellung eines Profils aus den Templates

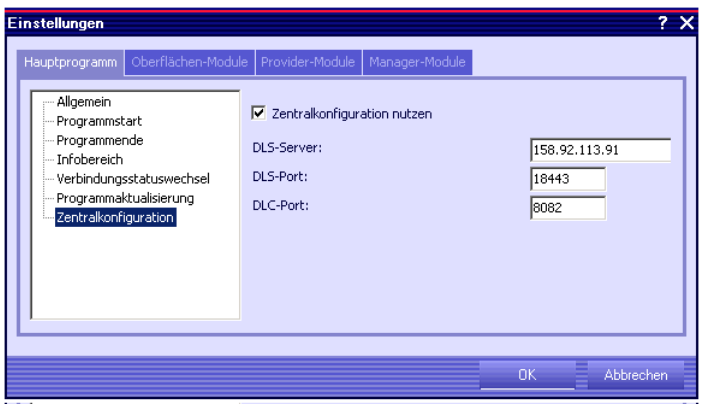
1. Wählen Sie den Bereich **Profil Management** > **Geräteprofil**.
2. Klicken Sie in der Ansichtenleiste auf **Neu**, um ein neues Profil anzulegen.
3. Tragen Sie im Feld **Name** einen passenden Namen für Ihr Profil ein, beispielsweise **oC 130 Gerät**, sowie eine kurze Beschreibung im Feld **Beschreibung**.
4. Falls das Profil für einen bestimmten **Standort** (siehe Abschnitt 6.3.2, “Standort”) als Standardprofil dienen soll, aktivieren Sie den Schalter **Default Profil**.
5. Stellen Sie in **Profil Management** > **Geräteprofil** > **Register „Templates“** die Templates zusammen, die das Profil bilden sollen. Hierzu klicken Sie für jedes Template, das Sie hinzufügen wollen, auf  und wählen anschließend ein Template aus der Auswahlliste.
6. Tragen Sie in **Profil Management** > **Geräteprofil** > **Register „Templates“** den passenden **Gerätetyp** sowie den **SW Typ** (Software-Typ) und die **SW Version** (Softwareversion) ein.
7. Klicken Sie auf die Schaltfläche Sichern, um das Profil zu speichern.

16.8.3 Einstellungen am optiClient 130

Damit der optiClient 130 mit dem DLS zusammenarbeitet, müssen am optiClient 130 einige Daten zusätzlich eingetragen werden.

Kennung (entsprechende der Nebenstelle des optiClient 130), Kennwort und Standort:

Unter **Einstellungen...** die Daten zum DLS-Server:



HINWEIS: Für weitere Informationen zur Konfiguration des optiClient 130 lesen Sie in der Online-Help oder im Administrationshandbuch zum optiClient 130 nach.

16.8.4 optiClient in Callcentern

In Callcentern ist es erforderlich, dass optiClient-Benutzer an jedem PC mit ihrer eigenen Rufnummer arbeiten können. Bei jedem erstmaligen Anmelden eines Benutzers an einem bestimmten PC wird dann P&P (Plug&Play) durchgeführt. Dafür muss das Flag Aktiviere Plug&Play gesetzt sein.

1. Richten Sie erstmalig an einem PC den optiClient mit der zum Benutzer gehörigen E.164-Nummer (z.B. 497224711) sowie das dazugehörige Profil ein.

   Achten Sie darauf, dass die DLS-Adresse im optiClient definiert ist und die Daten im Homelaufwerk der Domäne im Netz gespeichert werden.

2. Legen Sie nun im DLS einen einen entsprechenden Teilnehmer, d. h. ein virtuelles Gerät an. Wählen Sie hierzu den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** und klicken Sie auf die Aktionsschaltfläche **Neu**.

3. Tragen Sie die E.164-Nummer ein.

4. Tragen Sie als **Device ID** nochmals die E.164 Nummer ein und schließen Sie sie mit einem ‚.' (Punkt) ab (z.B. ‚497224711.').

5. Klicken Sie auf **Sichern**.

16.9 Ändern der IP-Adresse und/oder Portnummer des DLS

Sollen während eines laufenden DLS Änderungen an den Adressdaten (IP-Adresse und Portnummer) des DLS geändert werden, z. B. weil der DLS auf einen alternativen Rechner umziehen muss, ist bei der Änderung dieser Daten eine bestimmte Reihenfolge einzuhalten.

Die bisherige DLS-Installation wird nachfolgend mit „alt“ und der DLS mit den geänderten Daten „neu“ genannt.

1. Nehmen Sie zunächst den neuen DLS in Betrieb. Installieren Sie dazu alle nötigen Komponenten und starten Sie den neuen DLS.

   Der neue DLS läuft nun bereits mit neuer IP-Adresse und Portnummer, wird jedoch von den IP Devices noch nicht genutzt.

2. Damit die IP Devices den neuen DLS kontaktieren, müssen die IP-Adressdaten des DLS in den IP Devices geändert werden. Abhängig davon, wie die IP Devices mit IP-Adresse und Portnummer des DLS versorgt werden, nehmen Sie die Änderung dieser Daten vor:

   - Mit DHCP (vollständiges Plug&Play):

     Ändern Sie die Daten in der „Vendor Class“ des DHCP-Servers (siehe Abschnitt 4.12.4.3).

   - Ohne DHCP (eingeschränktes Plug&Play):

     a) Wählen Sie im DLS den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** > **Register „DLS Verbindung“** mit allen verfügbaren IP Devices (siehe auch Abschnitt 15.1, “Erste Schritte: Ändern von IP Device-Parametern”).

     b) Geben Sie bei **DLS Server Adresse** und **DLS Port** die IP-Adressdaten des neuen DLS ein und übernehmen Sie diese für alle IP Devices (siehe Abschnitt 5.4.2.4, “Mehrfachauswahl und Datenübernahme in der Tabellen-Ansicht”).

     c) Übertragen Sie die IP-Adressdaten des DLS an die IP Devices durch Klick auf **Sichern**.

3. Führen Sie einen Neustart an allen betroffenen Workpoints durch (**IP Devices** > **IP Device Interaktion** > **IP Device zurücksetzen**).

   HINWEIS: Beachten Sie, dass nach einem Neustart die IP Devices ausschließlich mit dem neuen DLS kommunizieren. Das bedeutet, es gibt für den alten DLS keine Rückmeldung, ob die Aktion erfolgreich ausgeführt werden konnte.

   Die IP Devices registrieren sich am neuen DLS.

4. Deaktivieren Sie den alten DLS (zum Deinstallieren des DLS siehe Abschnitt 4.14, “Deinstallation des OpenScape Deployment Service”).

16.10 Einsatz eines TAP mit DLS in einem Kundennetz ohne permanenten DLS

Voraussetzungen

- DLS ab KV45 und höher.
- Ein am TAP installierter FTP-Server. Zur Installation siehe Abschnitt 4.12.1, “FTP Server”.
- Die Workpoint-Software, die deployed werden soll, muss sich auf dem TAP befinden und im DLS registriert sein (siehe Abschnitt 6.3.4, “FTP Server Konfiguration”, Abschnitt 6.3.5, “HTTPS Server Konfiguration” oder Abschnitt 6.3.7, “Netzlaufwerk Konfiguration”) .
- Der TAP muss mit dem Kunden-LAN verbunden werden und eine freie IP-Adresse aus dem Kunden-LAN erhalten. Die IP-Adresse kann mithilfe des IP-Changers geändert werden.

Einschränkung

Am Workpoint kann DHCP ein- oder ausgeschaltet sein (*DHCP=ON* oder *DHCP=OFF*). Jedoch darf vom DHCP keine DLS-Info zum Workpoint gesendet werden. Im DHCP darf keine „Vendor Class“, wie unter Abschnitt 4.12.4.3 beschrieben, eingerichtet sein. Sollte der Workpoint die DLS-Info schon vom DHCP erhalten haben, so kann dieser Wert nur durch ein *Factory Reset* zurückgesetzt werden.

16.10.1 Installation und Erstkonfiguration des DLS auf dem TAP

1. Installieren Sie das Java 2 Runtime Environment 1.6.0_13.
2. Installieren Sie die aktuelle DLS-Version.
3. Führen Sie die Erstkonfiguration des DLS durch (siehe Abschnitt 4.10, “Erstkonfiguration”). Hier müssen unter anderem die Daten für den/die FTP-Server konfiguriert werden.
4. Um die Workpoints aus dem Kundennetz in den DLS zu übernehmen, muss zuerst der IP-Adressbereich eingerichtet werden, in dem sich die Workpoints befinden (**IP Devices** > **IP Device Interaktion**> **IP Devices scannen** > **Register „IP Bereiche“**).

   Zusätzlich muss die aktuelle IP-Adresse des TAP als **DLS Adresse** eingegeben werden (Anzeige der aktuellen IP-Adresse z. B. durch Eingabe von *ipconfig/all* in der DOS-Shell). Die Option **Sende DLS Adresse** muss aktiviert sein (**IP Devices** > **IP Device Interaktion**> **IP Devices scannen** > **Register „Konfiguration“**). Anschließend wird dieser IP-Adressbereich mittels **IP Devices scannen** abgescannt.

16.10.2 Manipulation der DLS-Datenbank zur Verwendung des TAP bei verschiedenen Kunden

Um am TAP mit mehreren Datenbänken arbeiten zu können, müssen an der Datenbank, mit der der DLS arbeitet, verschiedene Manipulationen vorgenommen werden.

16.10.2.1 Einrichten einer Datenbank bei einem neuen Kunden

1. Sichern Sie am TAP die Datenbank des DLS, wenn diese bereits Daten enthält. Siehe Abschnitt 15.8.1, “Automatisierte Datensicherungen”.
2. Legen Sie am TAP eine neue Datenbank an. Siehe Abschnitt 15.8.2.4, “Reset der DLS-Datenbank”.

16.10.2.2 Datenbank-Wechsel zwischen Kunde A und B

1. Sichern Sie am TAP die zur Zeit aktive DLS-Datenbank des **Kunden A**. Siehe Abschnitt 15.8.1, “Automatisierte Datensicherungen”.
2. Führen Sie ein Restore einer bereits gesicherten DLS-Datenbank des **Kunden B** durch. Siehe Abschnitt 15.8.1, “Automatisierte Datensicherungen”.

16.11 Steuern des DLS über die Programmschnittstelle (DlsAPI)

Neben der herkömmlichen Bedienung über die GUI kann der DLS auch über ein Web Services-Interface durch externe Applikationen gesteuert werden. Hierzu muss zunächst ein Account eingerichtet sein, der zum Zugang über die Schnittstelle DlsAPI berechtigt ist (siehe Abschnitt 6.1, “Account Management”).

Der DLS in der Version 2 stellt sowohl das DlsAPI v100 (wie DLS Version 1) zur Verfügung als auch neue Methoden, die Teil des DlsAPI v200 sind. Die Methoden des DlsAPI v100 unterstützen nur IP Phones, die Methoden des DlsAPI v200 auch IP Clients und IP Gateways.

16.11.1 Web Service-Schnittstelle der DlsAPI

Die DlsAPI wird bei der DLS-Installation mitgeliefert und befindet sich im Verzeichnis:

`<DLS-Installationsverzeichnis>\Programme\DeploymentService\api`

Enthalten sind folgende Daten:

1. `dlsapiv100.wsdl`
   Beschreibt die DlsAPI v100 in WSDL (Web Services Description Language).
2. `dlsapiv100.jar`
   Wurde von WSDL2JAVA generiert. Diese JAR-Datei enthält insbesondere die Client Stubs und den Service Locator und kann von JAVA-Clients als Schnittstelle zum DlsAPI v100 verwendet werden.
3. `dlsapiv200.wsdl`
   Beschreibt die DlsAPI v200 in WSDL (Web Services Description Language).
4. `dlsapiv200.jar`
   Wurde von WSDL2JAVA generiert. Diese JAR-Datei enthält insbesondere die Client Stubs und den Service Locator und kann von JAVA-Clients als Schnittstelle zum DlsAPI v200 verwendet werden.
5. `doc`
   In diesem Unterverzeichnis befindet sich die Beschreibung der DlsAPI-Schnittstelle im Javadoc-Format.

Die WSDL-Beschreibungen finden sich auf dem DLS-Server unter folgenden URLs:

```
https://<DLS-Server>:10444/DeploymentService/services/
DlsAPIv100?wsdl
```

```
https://<DLS-Server>:10444/DeploymentService/services/
DlsAPIv200?wsdl
```

Unter folgender URL finden Sie die Online-Dokumentation zur DlsAPI:

```
https://<DLS-Server>:10443/DeploymentService/dlsapidoc
```

HINWEIS: Falls der HTTP-Port des DLS nicht deaktiviert ist, kann dieser alternativ zum HTTPS-Port benutzt werden. Entsprechend ändern sich dann die URLs:
`https://<DLS-Server>:10443/DeploymentService/...`

Für die DlsAPI steht ein PHP-Testskript zur Verfügung. Damit ist es u. a. möglich, die SOAP-Kommunikation zu beobachten, bestimmte IP Phones in der DLS-Datenbank abzufragen sowie Konfigurationsparameter für ein ausgewähltes IP Phone zu modifizieren. Weitere Informationen finden Sie in den DLS Release Notes.

16.12 Security: Administration von Zertifikaten

Zertifikate werden zur sicheren Authentisierung zwischen Server und Clients eingesetzt. Ein Zertifikat ist vergleichbar mit einem digitalen Ausweis, der von einer autorisierten Stelle, der Certification Authority (CA), ausgestellt wird.

Im DLS können Zertifikate für die folgenden Server/Client-Konstellationen administriert werden:

- **Server**: WBM-Server im IP Phone
  Client: Web-Browser zu Administration des IP Phones (siehe Abschnitt 16.12.1, “WBM Server Zertifikat importieren”)
  Oberflächenbeschreibung siehe Abschnitt 7.1.7.4, “Register „WBM Server Zertifikat“”.

- **Server**: RADIUS-Server
  Client: IP Phone (siehe Abschnitt 16.12.2, “Phone bzw. RADIUS Zertifikat importieren”)
  Oberflächenbeschreibung siehe Abschnitt 7.1.22.2, “Register „Phone Zertifikat“”.

- **Server**: RADIUS-Server
  Client: IP Phone (siehe Abschnitt 16.12.2, “Phone bzw. RADIUS Zertifikat importieren”)
  Oberflächenbeschreibung siehe Abschnitt 7.1.22.3, “Register „RADIUS Server CA Zertifikat 1“” und Abschnitt 7.1.22.4, “Register „RADIUS Server CA Zertifikat 2“”.

- **Server**: SIP Server
  Client: IP Phone (siehe Abschnitt 16.12.3, “SPE CA Zertifikate”)
  Oberflächenbeschreibung siehe Abschnitt 7.1.21.1, “Register „SPE CA Zertifikate“”.

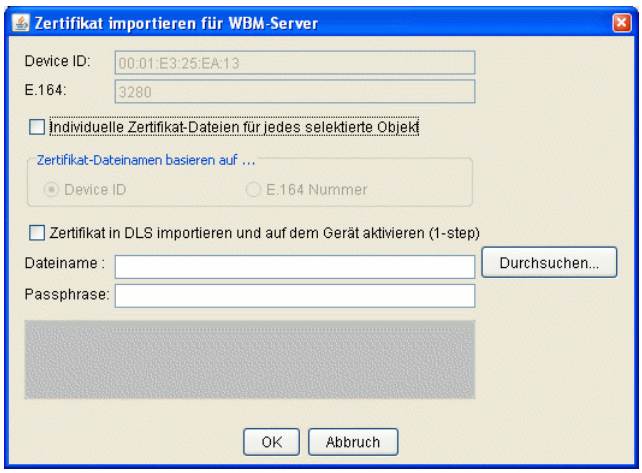
- **Server**: SIP Server
  Client: IP Client (siehe Abschnitt 16.12.4, “SPE CA Zertifikate für IP Client importieren”)
  Oberflächenbeschreibung siehe Abschnitt 7.2.12.1, “Register „SPE CA Zertifikate“”.

- **Server**: SIP Server
  Client: IP Gateway (siehe Abschnitt 16.12.5, “SPE Zertifikate und SPE CA Zertifikate für IP Gateway importieren”)
  Oberflächenbeschreibung siehe Abschnitt 7.3.3.3, “Register „SPE CA Zertifikate“”.

  HINWEIS: Das Administrieren von Zertifikaten ist ausschließlich mittels DLS und nicht über Deployment Tool, WBM oder direkt am Telefon möglich.

16.12.1 WBM Server Zertifikat importieren

1. Wählen Sie den Bereich **IP Devices** > **IP Phone Konfiguration** > **Security Einstellungen** > **Register „WBM Server Zertifikat“** und suchen bzw. wählen Sie das IP Phone, für dessen Kommunikation mit dem WBM-Client (Web-Browser) das Zertifikat importiert werden soll.
2. Klicken Sie auf **Zertifikat importieren**. Ein Dialogfenster zum Importieren erscheint:



   Für das ausgewählte IP Phone wird die Device ID angezeigt.
3. Geben Sie bei **Dateiname** den kompletten lokalen Pfad einschließlich Name des Zertifikates ein oder klicken Sie auf **Durchsuchen**, um den Pfad einzutragen.

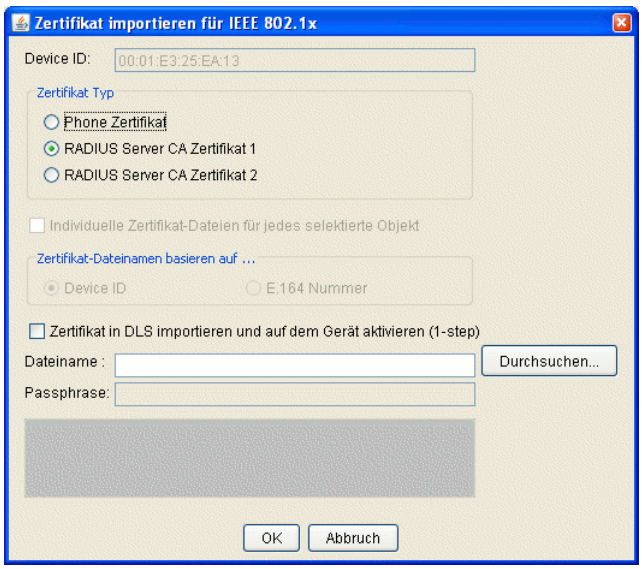
   Das Zertifikat wird im Format `PKCS#12` erwartet.
4. Geben Sie bei **Passphrase** den Schlüssel ein, mit dem die zu importierende PKCS#12 Datei verschlüsselt wurde.
5. Wenn das Zertifikat sofort aktiv werden soll, aktivieren Sie **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)**.
6. Klicken Sie auf **OK**, um das Zertifikat zu importieren.
   Bei Mehrfachauswahl (siehe Abschnitt 5.4.2.4) auf **Allen zuweisen** klicken, um die Zertifikate für alle gewählten Objekte zu importieren. Es erfolgt daraufhin eine Sicherheitsabfrage, bei der **Alle zuweisen** bestätigt werden muss.
7. Um das importierte Zertifikat zu aktivieren, klicken Sie auf **Zertifikat aktivieren** und danach auf **Sichern**, , falls **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)** nicht ausgewählt wurde.

HINWEIS: Zertifikate sollten auf Geräten bereitgestellt werden, wenn das entsprechende Template (mit dem gespeicherten PKI Connector) über Plug-and-Play angewendet wird.

HINWEIS: Zertifikate werden nicht auf bereits registrierten Geräten bereitgestellt, selbst wenn ein Template mit gespeichertem PKI Connector angewendet wird.

16.12.2 Phone bzw. RADIUS Zertifikat importieren

1. Wählen Sie den Bereich **IP Devices** > **IP Phone Konfiguration** > **IEEE 802.1x**.
2. Wählen Sie das Register entsprechend dem gewünschten Zertifikat **Register „Phone Zertifikat“, Register „RADIUS Server CA Zertifikat 1“** bzw. **Register „RADIUS Server CA Zertifikat 2“** und suchen bzw. wählen Sie das IP Phone, für das das Zertifikat importiert werden soll.
3. Klicken Sie auf **Zertifikat importieren**. Ein Dialogfenster zum Importieren erscheint:



   Für das ausgewählte IP Phone wird die Device ID angezeigt.
4. Wählen Sie zunächst bei **Zertifikat Typ** das gewünschte Zertifikat aus. Die zum gewählten Register passende Option ist bereits ausgewählt.
5. Aktivieren Sie die Checkbox
   Individuelle Zertifikat-Dateien für jedes selektierte Objekt, um für jedes IP Phone ein individuelles Zertifikat zu importieren (siehe dazu auch Schritt 6).
6. Geben Sie bei **Dateiname** (bzw. **Verzeichnis** bei aktivierter Checkbox in Schritt 5) den kompletten lokalen Pfad einschließlich Name des Zertifikates (ohne Name bei aktivierter Checkbox in Schritt 5) ein oder klicken Sie auf **Durchsuchen**, um den Pfad einzutragen.

   HINWEIS: Wurde bei Schritt 5 gewählt, dass individuelle Zertifikate für jedes IP Phone importiert werden sollen, müssen diese Zertifikate bereits wie folgt vorliegen:
   Alle Dateinamen der Zertifikate basieren entweder auf
   - den Device IDs der Telefone oder
   - den E.164-Rufnummern der Telefone

   Wählen Sie bei **Zertifikat-Dateinamen basieren auf ...** die dazu passende Option.

   Phone-Zertifikate werden im Format `PKCS#12` und RADIUS-Zertifikate im Format `.pem` erwartet.

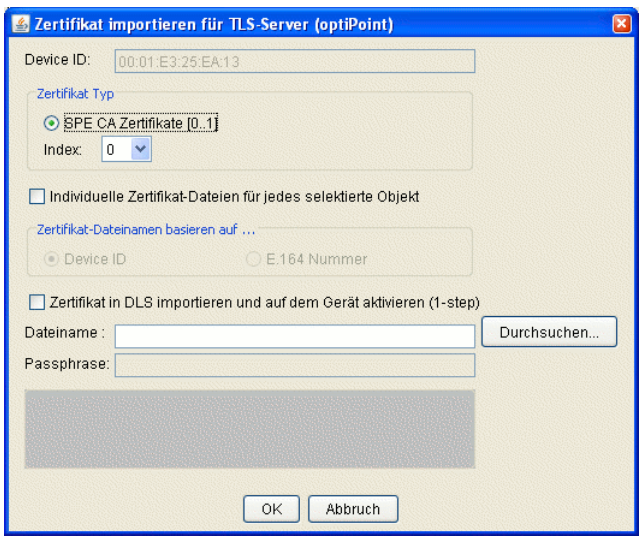
7. Nur für Phone-Zertifikate: Geben Sie bei **Passphrase** den Schlüssel ein, mit dem die zu importierende PKCS#12 Datei verschlüsselt wurde. (bei RADIUS-Zertifikaten nicht erforderlich).
8. Wenn das Zertifikat sofort aktiv werden soll, aktivieren Sie **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)**.
9. Klicken Sie auf **OK**, um das Zertifikat zu importieren.
   Bei Mehrfachauswahl (siehe Abschnitt 5.4.2.4) auf **Allen zuweisen** klicken, um die Zertifikate für alle gewählten Objekte zu importieren. Es erfolgt daraufhin eine Sicherheitsabfrage, bei der **Alle zuweisen** bestätigt werden muss.
10. Um das importierte Zertifikat zu aktivieren, klicken Sie auf **Zertifikat aktivieren** und danach auf **Sichern**, falls **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)** nicht ausgewählt wurde.

HINWEIS: Zertifikate sollten auf Geräten bereitgestellt werden, wenn das entsprechende Template (mit dem gespeicherten PKI Connector) über Plug-and-Play angewendet wird.

HINWEIS: Zertifikate werden nicht auf bereits registrierten Geräten bereitgestellt , selbst wenn ein Template mit gespeichertem PKI Connector angewendet wird.

16.12.3 SPE CA Zertifikate

1. Wählen Sie den Bereich **IP Devices** > **IP Phone Konfiguration** > **Signaling and Payload Encryption (SPE)** > **Register „SPE CA Zertifikate“** und suchen bzw. wählen Sie das IP Phone, für dessen Kommunikation mit dem SIP-Server das Zertifikat importiert werden soll.
2. Klicken Sie auf **Zertifikat importieren**. Ein Dialogfenster zum Importieren erscheint:



   Für das ausgewählte IP Phone wird die Device ID angezeigt.
3. Da es sich um ein indiziertes Zertifikat handelt, müssen Sie den entsprechenden **Index** auswählen.
4. Geben Sie bei **Dateiname** den kompletten lokalen Pfad einschließlich Name des Zertifikates ein oder klicken Sie auf **Durchsuchen**, um den Pfad einzutragen.

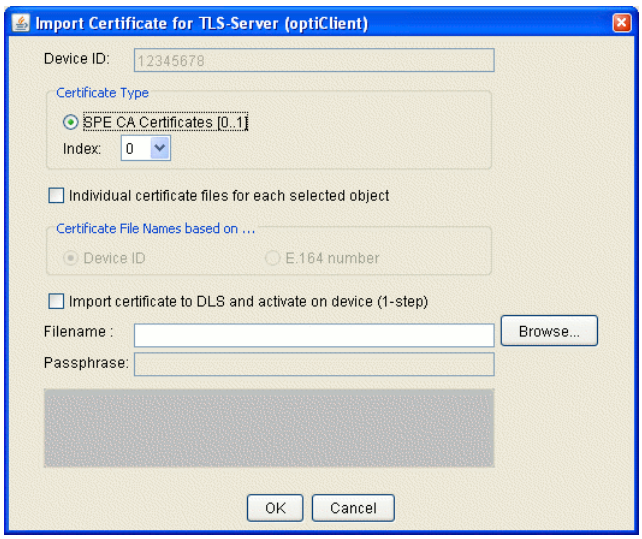
   Das Zertifikat wird im Format `.pem` erwartet.
5. Geben Sie bei **Passphrase** den Schlüssel ein, mit dem die zu importierende PKCS#12 Datei verschlüsselt wurde.
6. Klicken Sie auf **OK**, um das Zertifikat zu importieren.
   Bei Mehrfachauswahl (siehe Abschnitt 5.4.2.4) auf **Allen zuweisen** klicken, um die Zertifikate für alle gewählten Objekte zu importieren. Es erfolgt daraufhin eine Sicherheitsabfrage, bei der **Alle zuweisen** bestätigt werden muss.
7. Wenn bei **Aktiviertes Zertifikat aktivieren** die Checkbox aktiviert ist, wird das importierte Zertifikat beim nächsten **Sichern** aktiviert.
8. Um ein zweites Zertifikat zu importieren, verfahren Sie analog zum ersten Zertifikat.

HINWEIS: Zertifikate sollten auf Geräten bereitgestellt werden, wenn das entsprechende Template (mit dem gespeicherten PKI Connector) über Plug-and-Play angewendet wird.

HINWEIS: Zertifikate werden nicht auf bereits registrierten Geräten bereitgestellt , selbst wenn ein Template mit gespeichertem PKI Connector angewendet wird.

16.12.4 SPE CA Zertifikate für IP Client importieren

1. Wählen Sie den Bereich **IP Devices** > **IP Client Konfiguration** > **Signaling and Payload Encryption (SPE)** > **Register „SPE CA Zertifikate“** und suchen bzw. wählen Sie den IP Client, für dessen Kommunikation mit dem SIP-Server das Zertifikat importiert werden soll.
2. Klicken Sie auf **Zertifikat importieren**. Ein Dialogfenster zum Importieren erscheint:



   Für das ausgewählte IP Phone wird die Device ID angezeigt.
3. Geben Sie bei **Dateiname** den kompletten lokalen Pfad einschließlich Name des Zertifikates ein oder klicken Sie auf **Durchsuchen**, um den Pfad einzutragen.

   Das Zertifikat wird im Format `.pem` erwartet.
4. Wenn das Zertifikat sofort aktiv werden soll, aktivieren Sie **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)**.
5. Klicken Sie auf **OK**, um das Zertifikat zu importieren.
   Bei Mehrfachauswahl (siehe Abschnitt 5.4.2.4) auf **Allen zuweisen** klicken, um die Zertifikate für alle gewählten Objekte zu importieren. Es erfolgt daraufhin eine Sicherheitsabfrage, bei der **Alle zuweisen** bestätigt werden muss.
6. Um das importierte Zertifikat zu aktivieren, klicken Sie auf **Zertifikat aktivieren** und danach auf **Sichern**, falls **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)** nicht ausgewählt wurde.
7. Um ein zweites Zertifikat zu importieren, verfahren Sie analog zum ersten Zertifikat.

HINWEIS: Zertifikate sollten auf Geräten bereitgestellt werden, wenn das entsprechende Template (mit dem gespeicherten PKI Connector) über Plug-and-Play angewendet wird.

HINWEIS: Zertifikate werden nicht auf bereits registrierten Geräten bereitgestellt , selbst wenn ein Template mit gespeichertem PKI Connector angewendet wird.

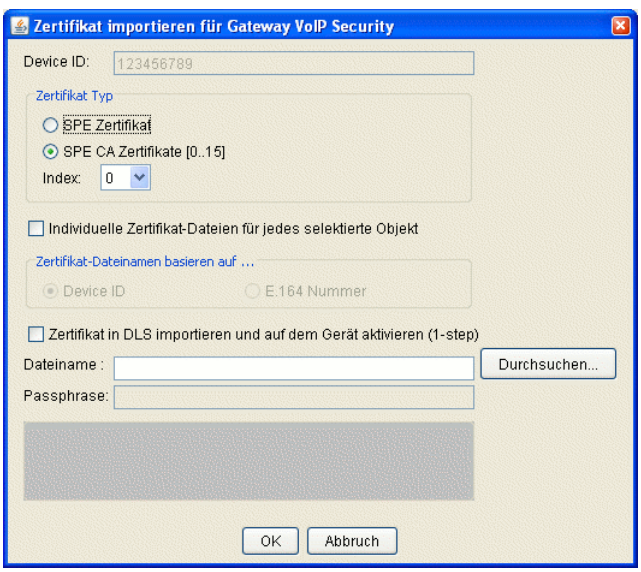
16.12.5 SPE Zertifikate und SPE CA Zertifikate für IP Gateway importieren

Zur Nutzung von Signaling and Payload (SPE) Zertifikaten müssen IP Phones an einem IP Gateway betrieben werden, das wiederum als virtuelles Device vorkonfiguriert sein muss.

1. Wählen Sie den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration** und tragen Sie die IP Adresse des IP Gateways bei **Device ID** ein, sowie bei **Gerätefamilie** „IP Gateway“.
2. Tragen Sie beim ersten Einrichten eines IP Gateways im Register **DLS Verbindung** die **DLS Server Adresse** und den **DLS Server Port** (Standard: 18443) ein. Wollen Sie weitere IP Gateways einrichten, werden diese Werte intern verwendet.
3. **Secure Modus erforderlich** ist automatisch aktiviert, da IP Gateways nur in diesem Modus betrieben werden dürfen. Wählen Sie den **PIN Modus** aus.

   HINWEIS: Wurde **Standard PIN** gewählt, können Sie diese unter **Administration** > **Workpoint Interface Konfiguration** administrieren.

   Die PIN muss der IP Gateway Baugruppe vor der Registrierung bekannt gemacht werden. Dies geschieht über das CLI-Interface (activate dls pin <pin>).
4. Über den Button **Scannen** wird die Registrierung einschließlich Bootstrapping durchgeführt.
5. Wechseln Sie zu **IP Devices** > **IP Gateway Konfiguration** > **Signaling and Payload Encryption (SPE)** > **Register „SPE Zertifikat“** und klicken Sie auf **Zertifikat importieren**. Ein Dialogfenster zum Importieren erscheint:



HINWEIS: Die zu importierenden Zertifikate müssen vorher von einer Kunden-PKI erzeugt werden.

Es wird empfohlen, auf jedem Gateway ein individuelles Zertifikat einzuspielen, bei dem bei **Besitzer (CN)** die eigene IP-Adresse eingetragen ist. Falls **Besitzer Prüfung** aktiviert ist, ist dies sogar zwingend notwendig. Falls ein DNS vorhanden ist, kann anstatt der IP Adresse ein entsprechender Name für das Gateway eingetragen sein.

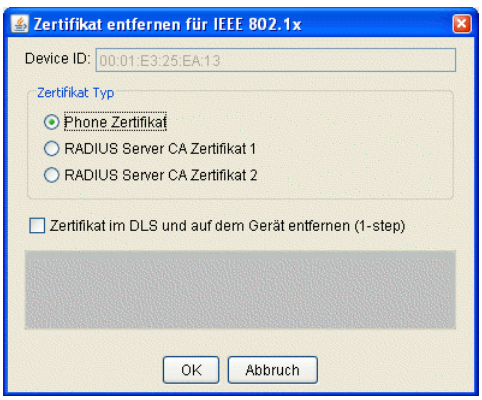
6. Wählen Sie aus, ob sie ein SPE Zertifikat oder ein SPE CA Zertifikat importieren wollen. Da es sich beim SPE CA Zertifikat um ein indiziertes Zertifikat handelt, müssen Sie den entsprechenden **Index** auswählen.
7. Geben Sie bei **Dateiname** den kompletten lokalen Pfad einschließlich Name des Zertifikates ein oder klicken Sie auf **Durchsuchen**, um den Pfad einzutragen.
   Das SPE Zertifikat wird im Format PKCS#12 erwartet, das SPE CA Zertifikat im Format `.pem`.
8. Nur für SPE Zertifikate: Geben Sie bei **Passphrase** den Schlüssel ein, mit dem die zu importierende PKCS#12 Datei verschlüsselt wurde.
9. Wenn das Zertifikat sofort aktiv werden soll, aktivieren Sie **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)**.
10. Klicken Sie auf **OK**, um das Zertifikat zu importieren. Bei Mehrfachauswahl (siehe Abschnitt 5.4.2.4, “Mehrfachauswahl und Datenübernahme in der Tabellen-Ansicht”) auf **Allen zuweisen** klicken, um die Zertifikate für alle gewählten Objekte zu importieren. Es erfolgt daraufhin eine Sicherheitsabfrage, bei der **Alle zuweisen** bestätigt werden muss.
11. Um das importierte Zertifikat zu aktivieren, klicken Sie auf **Zertifikat aktivieren** und danach auf **Sichern**, falls **Zertifikat in DLS importieren und auf dem Gerät aktivieren (1-step)** nicht ausgewählt wurde.
12. Es sind sowohl das SPE Zertifikat als auch die SPE CA Zertifikat für IP Gateway einzurichten.
13. Anschließend müssen die SPE CA Zertifikate für IP Phone / IP Client importiert werden, wie in Abschnitt 16.12.3, “SPE CA Zertifikate” / Abschnitt 16.12.4, “SPE CA Zertifikate für IP Client importieren” beschrieben.
14. Unter **IP Devices** > **IP Phone Konfiguration** > **Signaling and Payload Encryption (SPE)** > **Register „SIP Einstellungen“** oder **Register „HFA Einstellungen“** muss für **SIP Transport Protokoll** bzw. **HFA Transport Protokoll** der Wert „TLS“ eintragen werden. Für IP Clients sind die Werte analog einzutragen.

HINWEIS: Zertifikate sollten auf Geräten bereitgestellt werden, wenn das entsprechende Template (mit dem gespeicherten PKI Connector) über Plug-and-Play angewendet wird.

HINWEIS: Zertifikate werden nicht auf bereits registrierten Geräten bereitgestellt , selbst wenn ein Template mit gespeichertem PKI Connector angewendet wird.

16.12.6 Zertifikat entfernen (am Beispiel IEEE 802.1x Phone)

1. Wählen Sie den gewünschten Bereich unter **IP Devices** > **IP Phone Konfiguration** (siehe Abschnitt 16.12.1 bis Abschnitt 16.12.5).
2. Suchen bzw. wählen Sie das IP Phone, dessen Zertifikat Sie entfernen möchten oder wechseln Sie zur Ansicht **Template**, um in einem Template ein Zertifikat zu löschen.
3. Klicken Sie auf **Zertifikat entfernen**. Ein Dialogfenster erscheint (Beispiel):



4. Wählen Sie bei IEEE 802.1x-Zertifikaten ggf. das zu entfernende Zertifikat. Die zum gewählten Register passende Option ist bereits ausgewählt.
5. Wenn das Zertifikat sofort gelöscht werden soll, aktivieren Sie **Zertifikat im DLS und auf dem Gerät entfernen (1-step)**.
6. Klicken Sie auf **OK**, um das Zertifikat zu entfernen.
   Bei Mehrfachauswahl (siehe Abschnitt 5.4.2.4) auf **Allen zuweisen** klicken, um die Zertifikate für alle gewählten Objekte zu entfernen.
7. Um das Zertifikat auf dem Endgerät zu löschen, klicken Sie **Zertifikat aktivieren** und anschließend **Sichern**, falls **Zertifikat im DLS und auf dem Gerät entfernen (1-step)** nicht ausgewählt wurde.

16.12.7 IP Phone austauschen

1. Wählen Sie den Bereich **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration**. Klicken Sie in der Menüleiste auf **Aktion** und wählen Sie die Aktion **IP Device kopieren** (siehe Abschnitt 16.5, “Austausch eines IP Devices”).
2. Prüfen Sie, ob in der Kopie alle Zertifikate als importierte Zertifikate vorliegen oder in einem Default-Profil enthalten sind. Sind nur aktivierte Zertifikate vorhanden, werden sie bei Plug&Play nicht weiterverwendet.

16.13 Mobility:EinrichtenMobility:Administrieren

Mit der Mobility-Funktion lassen sich Rufnummern alternativ zu Endgeräten bestimmten Personen zuteilen. Neben seiner Rufnummer kann der Benutzer persönliche Einstellungen, wie etwa die Tastenbelegung, von einem zum anderen Endgerät mitnehmen. Am jeweiligen Endgerät muss er sich hierzu mit seiner Rufnummer und einem Passwort anmelden. Das zuvor genutzte Endgerät erhält nach Abmelden des Benutzers sein Basisprofil wieder, und damit auch eine andere Rufnummer als die des mobilen Benutzers.

HINWEIS: Grundlageninformationen zum Thema Mobility im DLS finden Sie im Abschnitt 3.8, “Mobility im DLS – Grundlagenwissen”.

16.13.1 Mobility-Funktion auf dem Endgerät einrichten

Wählen Sie im Bereich **IP Devices > IP Phone Konfiguration > SIP Mobility** das Register **Mobility** und aktivieren Sie die Option **Endgerät verfügbar für Mobile User**.

16.13.2 Taste „Mobility“ einrichten

Erstellen Sie ein Template mit einer Tastenbelegung, die eine Mobility-Taste bereitstellt:

1. Wählen Sie im Bereich > **IP Devices >** IP Phone KonfigurationKeysets / Tastenbelegung die Ansicht  Template **und klicken Sie im Register** Ziele auf das Symbol . Es öffnet sich eine neue Tabellenzeile, in der Sie die gewünschten Einträge machen können.
2. Da sich die Tastenfunktion **Mobility** in der 1. Ebene befindet, treffen Sie in der Spalte **Ebene** die Auswahl „1. Ebene“.
3. Wählen Sie nun in der Spalte **Tastennummer** die Taste aus, der die neue Funktion zugewiesen werden soll. Siehe hierzu Abschnitt 7.1.19.2, “Register „Ziele“”.
4. In der Spalte **Tastenfunktion** wählen Sie „Mobility“.
5. Schließlich können Sie noch in der letzten Spalte einen Tastentext eintragen. Dieser wird nur bei Modellen der optiPoint 420-Famile sichtbar, da diese über eine LCD-Tastenbeschriftung verfügen.
6. Wenn Sie auf **Sichern** klicken, öffnet sich ein Dialogfenster, in dem Sie einen Namen sowie eine Beschreibung für das Template eingeben können. Speichern Sie das Template ab, indem Sie auf **Speichern** klicken.

   Näheres zum Erstellen von Templates finden Sie in Abschnitt 15.4.1, “Template manuell anlegen”.
7. Ordnen Sie das Template einem Profil zu und laden Sie dieses Profil in die gewünschten Workpoints.

16.13.3 Mobile User:Profil

1. Erstellen Sie Templates, die die gewünschten Konfigurationen für den Mobile User enthalten. Wählen Sie die Ansicht **Templates** jeweils in dem Bereich, der konfiguriert werden soll, beispielsweise in **Mobile User** > **SIP Mobile User Konfiguration** > **Sonstiges**.
2. Wenn Sie auf **Sichern** klicken, öffnet sich ein Dialogfenster, in dem Sie einen Namen sowie eine Beschreibung für das Template eingeben können. Speichern Sie das Template ab, indem Sie auf **Speichern** klicken.
3. Klicken Sie im Bereich **Profil Management** > **User Data Profile** auf **Neu**, um ein neues Profil zu erstellen. Klicken Sie auf das Symbol  . In der sich nun öffnenden Auswahlliste wählen Sie die gewünschten Templates aus.
4. Im Feld **Name** geben Sie den Namen für das neue Profil an und im Feld **Beschreibung** ggf. eine kurze Beschreibung des Profils.
5. Durch **Sichern** speichern Sie das Profil.

16.13.4 Mobile User erstellen

Voraussetzungen

- Eine laufende DLS-Infrastruktur.
- Die Mobile User sind bereits in der OpenScape Voice konfiguriert.

16.13.4.1 Erstellen durch Hinzufügen

1. Wählen Sie den Bereich **Mobile User** > **SIP Mobile User Interaktion** > **SIP Mobile User > Register „Mobile / Basis User“**.
2. Klicken Sie auf **Neu**.

   Klicken Sie auf die Schaltfläche  rechts neben dem Feld **Neue Mobile User IDs**. Ein Dialogfenster erscheint. Die Liste zeigt alle in der Telefonanlage registrierten Rufnummern an, die noch verfügbar sind, d. h. noch keinem Workpoint oder Mobile User zugeordnet sind. Durch Klick auf **OK** übernehmen Sie die Daten. Alternativ zur Auswahlliste können Sie die Rufnummer des Mobile Users auch per Hand in das Feld eintragen, wobei mehrere Nummern durch Komma getrennt werden müssen.
3. Geben Sie bei **Mobile User Passwort** das Passwort für den Zugriff des Mobile Users auf das Mobility Phone ein.

   HINWEIS: Bei OpenStage v3 und höher wird das Passwort für Mobile User unter Verwendung von Hash-Werten übermittelt. Daher kann der DLS beim Klicken auf die Schaltfläche „Refresh (Aktualisieren)“ das Passwort nicht im Passwort-Feld anzeigen.
   Das Passwort ist nicht verloren gegangen; es ist in der grafischen Benutzeroberfläche von DLS nur nicht sichtbar.

4. Wählen Sie bei **Mobile User Profil** das Profil (siehe Abschnitt 16.13.3, “Mobile User:Profil”), das für die zu erstellenden Mobile User gelten soll.
5. Setzen Sie ggf. einen Haken bei **Übernahme der SIP Daten** von virtuellen Devices**, um die im Geräteprofil (**Profil Management **>** GeräteprofilMobile User) angegebenen SIP-Daten automatisch für den zu übernehmen.
6. Klicken Sie auf **Sichern**.

16.13.4.2 Erstellen durch Migrieren

1. Gehen Sie auf **Mobile User > Mobile User Interaction > Mobile User**. Wenn Sie im Feld **Anwender Typ** „Endgerät für Mobile User“ wählen, danach auf **Suchen** klicken, bekommen Sie in der Ansicht **Tabelle** eine Auflistung all derjenigen Endgeräte, die für einen Mobile User verfügbar sind.
2. Klicken Sie auf **Migration zu Mobile User**. Es öffnet sich ein Dialogfenster.
3. Geben Sie eine neue E.164 zur Verwendung als Basis-E.164-Nummer für das Mobile User Endgerät ein. Dies ist die E.164-Nummer, die vom Gerät verwendet wird, wenn kein Benutzer am Gerät angemeldet ist.
4. Bestimmen Sie ein Mobile User Profil, das vom Mobile User Endgerät verwendet wird, wenn kein Benutzer am Gerät angemeldet ist.
5. Geben Sie das Mobile User Passwort für den neu erstellten Basis-User ein.
6. Starten Sie den Migrationsprozess.

HINWEIS: Während der Migration werden die Benutzerdaten des Mobile User Endgeräts verwendet, um einen neuen Mobile User zu erstellen. Die neue E.164-Nummer und die neuen Benutzerdaten werden auf das Mobile User Endgerät kopiert und werden immer dann verwendet, wenn kein Benutzer am Gerät angemeldet ist.

HINWEIS: Im Rahmen der Migration wird der bisherige Basis-User in einen Mobile User umgewandelt. Das Standard-Passwort für den neuen Mobile User lautet „000000“.

16.13.5 Home Phone einrichten

Unter Home Phone versteht man ein dem SIP Mobile User zugeordnetes Endgerät, an dem er standardmässig eingeloggt ist. Das Einrichten des Home Phone ist optional. Mit dem Einrichten eines Home Phone wird aber erreicht, dass der Mobile User nach dem Abmelden von einem beliebigen Endgerät automatisch am Home Phone angemeldet und somit erreichbar ist. Meldet sich der Mobile User am Home Phone ab, ist er nicht mehr erreichbar.

1. Gehen Sie auf **Mobile User > SIP Mobile User Interaktion > SIP Mobile User**. Wenn Sie im Feld **Anwender Typ** „Endgerät für Mobile User“ wählen, danach auf **Suchen** klicken, bekommen Sie in der Ansicht **Tabelle** eine Auflistung all derjenigen Endgeräte, die für einen Mobile User verfügbar sind. Für Mobile User mit Status „Mobile User abgemeldet“ stehen Felder unter **Mobile User Home Phone** zur Verfügung.
2. Aktivieren Sie **Automatisches Logon am Home Phone zulassen**, damit die Anmeldung des Mobile User am Home Phone sofort aktiv wird.
3. Für **Home Phone** wählen Sie die Rufnummer eines Endgerätes aus der Auswahlliste aus. Das Feld **Home Phone Status** zeigt den Status des ausgewählten Home Phones an.
4. Bestätigen Sie abschließend mit **Sichern**.

16.13.6 Mobile User anmelden (Forced Logon)

Die Anmeldung eines Mobile Users kann nicht nur am Endgerät selbst sondern auch per DLS erfolgen.

1. Wählen Sie im Bereich **Mobile User > SIP Mobile User Interaktion > Logon / Logoff** über **Suche** > **Ansicht Tabelle > Ansicht Objekt** den Mobile User aus, den Sie anmelden wollen. Alternativ können Sie auch das Endgerät auswählen, an dem der Mobile User angemeldet werden soll.
2. Klicken Sie auf **Logon Mobile User**.
3. Es öffnet sich ein Dialogfenster. Wenn Sie zuvor einen Mobile User ausgewählt hatten, tragen Sie nun die Basis E.164-Nummer des Endgeräts ein, an dem der Mobile User angemeldet werden soll. Hatten Sie ein Endgerät ausgewählt, ist die Mobility ID des Mobile Users einzutragen.

16.13.7 Mobile User abmelden (Forced Logoff)

Mithilfe des DLS kann der Administrator einen Mobile User, der an einem beliebigen Workpoint angemeldet ist, abmelden. Bestehende Gesprächsverbindungen werden dabei unterbrochen.

1. Wählen Sie im Bereich **Mobile User > SIP Mobile User Interaktion > Logon / Logoff** über **Suche** > **Ansicht Tabelle > Ansicht Objekt** den Mobile User aus, den Sie abmelden wollen. Alternativ können Sie auch das Endgerät auswählen, an dem der Mobile User angemeldet ist.
2. Mit **Logoff Mobile User** melden Sie den Mobile User vom jeweiligen Endgerät ab.

16.13.8 Fehlersuche bei An- und Abmeldungsvorgängen

Das Register **Protokoll** im Bereich **Mobile User > SIP Mobile User Interaktion > Logon / Logoff** enthält Informationen zu Aktionen. Diese Informationen sind erhältlich sowohl für Mobile User als auch für Endgeräte, die für Mobile User verfügbar sind.

Einen Überblick über alle Mobile User-bezogenen Daten in einem bestimmten Zeitraum findet man im Bereich **Mobile User** > **Mobility Statistiken**.

Eine Vielzahl von Gründen kann dazu führen, dass ein Mobile User an zwei Telefonen (A und B) gleichzeitig angemeldet ist. Dies führt nicht zu einem Fehlerzustand bei OpenScape Voice! Der DLS verfügt dennoch über ein spezielles Fehlerhandling, das versucht diesen Zustand zu bereinigen, indem es den Mobile User am Telefon A abmeldet, sobald dieses wieder erreichbar ist.

Mögliche Ursachen für Probleme beim Logoff:

1. Telefon A ist nicht erreichbar: macht einen Restart, ist ausgesteckt, das Netzwerk ist unterbrochen, hat Hardware-Probleme. Dies sind die wahrscheinlichsten Ursachen.
2. Telefon A hat ein Software-Problem und kann den Logoff nicht vollständig durchführen. In den meisten dieser Fälle kann der DLS den Logoff aktivieren, das Telefon kann den Auftrag aber nicht durchführen.
3. Am Telefon A ist DCMP erlaubt. SIP Mobility und DCMP arbeiten nicht zusammen, weshalb DCMP immer ausgeschaltet sein muss, wenn mit SIP Mobility gearbeitet werden soll.

4. Telefon A wird nicht vom DLS akzeptiert, da es sich im Secure Modus befindet, aber kein gültiges Zertifikat besitzt.
5. Telefon A hat keine korrekte DLS-Adresse.
6. Telefon A befindet sich im Gesprächszustand (siehe auch Zeitdauer bis Logoff während eines Gesprächs in **Hauptmenü** > **Mobile User** > **SIP Mobile User Konfiguration** > **SIP Mobility** > **Register „Mobility Logon/ Logoff“**).

16.13.9 Voreinstellung für die Tastenbelegung bei Mobility-Telefonen

Für jeden Gerätetyp können die Tastenbelegungen für die 4 grundlegenden Tastenfunktionen „Primärleitung“, „Mobility“, „Abbrechen“ und „Shift“ vorgegeben werden. Diese Vorgaben überschreiben die jeweils im Profil des Mobile Users definierte Tastenbelegung.

1. Wählen Sie den Bereich **Mobile User** > **SIP Mobile User Interaktion** > **SIP User Tastenbelegung**.
2. Wählen Sie den passenden **Gerätetyp**.
3. Aktivieren Sie **Verwende folgende Voreinstellungen bei Mobile User Logon**.

16.13.10 Datensicherung in einem .zip-Archiv

Sämtliche Daten eines Mobile Users können in Form eines Archivs im .zip-Format gespeichert werden. Innerhalb des .zip-Archivs liegen diese Daten dann in dem XML-Format vor, das zum Datenaustausch zwischen Workpoint und DLS zur Anwendung kommt.

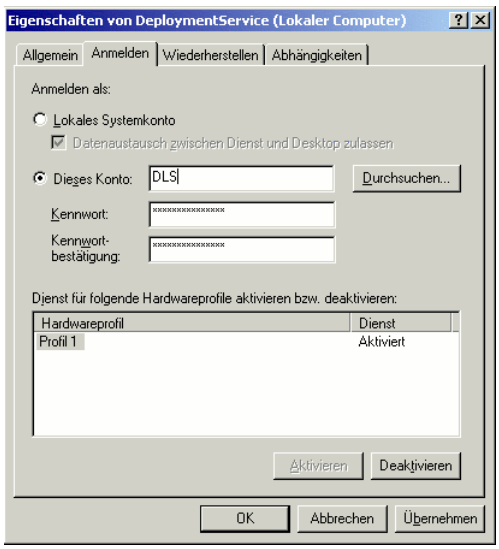
16.13.10.1 Vorbereitung

In vielen Fällen empfiehlt es sich, die Datensicherung auf einem Netzlaufwerk durchzuführen. Zudem sollte nur ein bestimmtes Verzeichnis zur Sicherung von Mobile User-Daten freigegeben werden. Hierzu sind folgende Schritte erforderlich:

1. Stoppen Sie den DeploymentService, d.h. den Webservice des DLS. Gehen Sie hierzu im Windows-Startmenü auf **Programme** > **DeploymentService** > **Stop Service**.
2. Da der DeploymentService nach der Installation mit dem Account localadmin läuft, für den normalerweise keine Laufwerke gemappt sind, sieht er zunächst nur lokale Laufwerke. Weisen Sie daher dem DeploymentService einen Account zu, der über die Berechtigung für das zu mappende Netzlaufwerk verfügt.

   WICHTIG: Achten Sie darauf, dass der Account des DeploymentService Administratorrechte hat. Einschränkungen können zu Problemen mit dem DLS führen.

   Um dem DeploymentService einen neuen Account zuzuweisen, wählen Sie im Windows-Startmenü **Einstellungen** > **Verwaltung** > **Dienste** oder **Einstellungen** > **Systemsteuerung** > **Administrative Tools** > **Services**. Durch Doppelklick auf den Eintrag **DeploymentService** öffnet sich ein Fenster, in dem Sie die Eigenschaften des Dienstes verändern können. Im Register **Anmelden** aktivieren Sie nun die Checkbox **Dieses Konto** und wählen mithilfe von **Durchsuchen** den Benutzeraccount aus.



3. Benennen Sie in
   „`C:\Program Files\DeploymentService\Tomcat5\bin`"die folgenden Dateien wie beschrieben um:

   `initdlsservice.template` > `initdlsservice.bat`

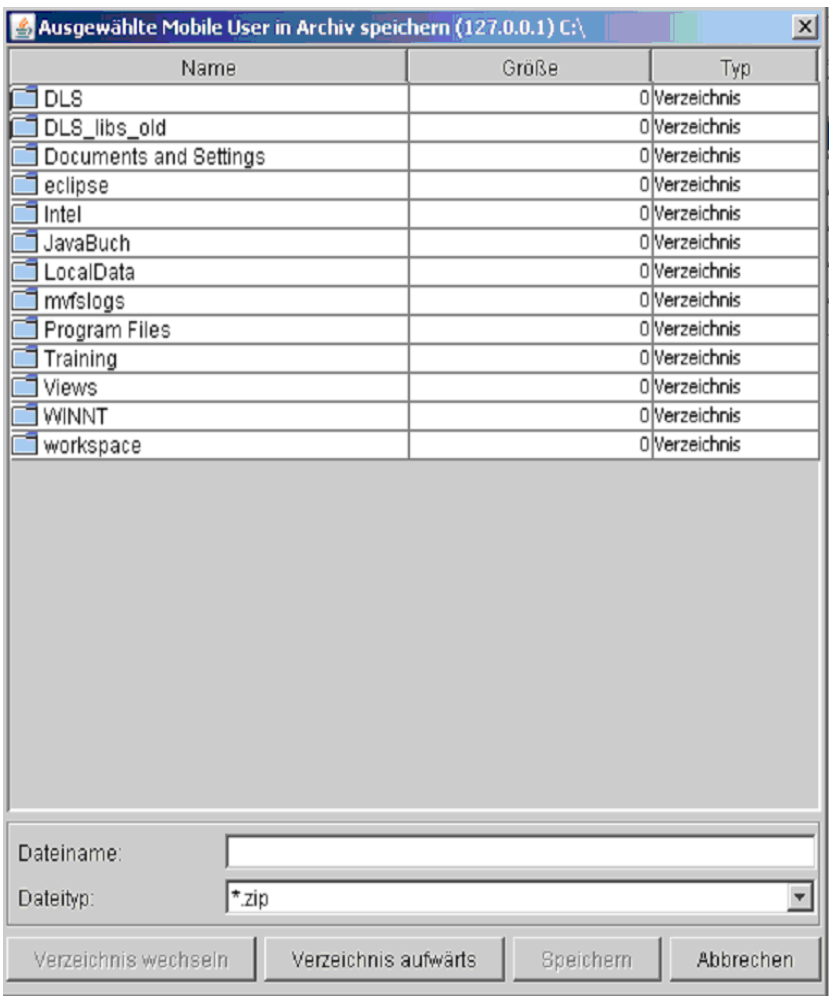
   `releasedlsservice.template` > `releasedlsservice.bat`

4. In den Dateien „`initdlsservice.bat`" und „`releasedlsservice.bat`" tragen Sie die Verbindung bzw. die Trennung der Netzlaufwerke entsprechend der Beschreibung ein.

5. Mit **Programme** > **DeploymentService** > **Start Service** starten Sie den Service neu.

16.13.10.2 Mobile User:Daten speichern

1. Wählen Sie den Bereich **Mobile User** > **SIP Mobile User Interaktion** > **SIP Mobile User**.
2. Klicken Sie auf die Aktionsschaltfläche **Suche**, um alle verfügbaren Mobile User aufzufinden.
3. Wählen Sie unter **Ansichten** die Option **Tabelle**. Markieren Sie die Mobile User, deren Daten Sie speichern wollen.
4. Wählen Sie nun in der Menüleiste unter **Aktion** den Eintrag **Ausgewählte Mobile User in Archiv speichern**. Es öffnet sich ein Dialogfenster zur Auswahl des Speicherorts.



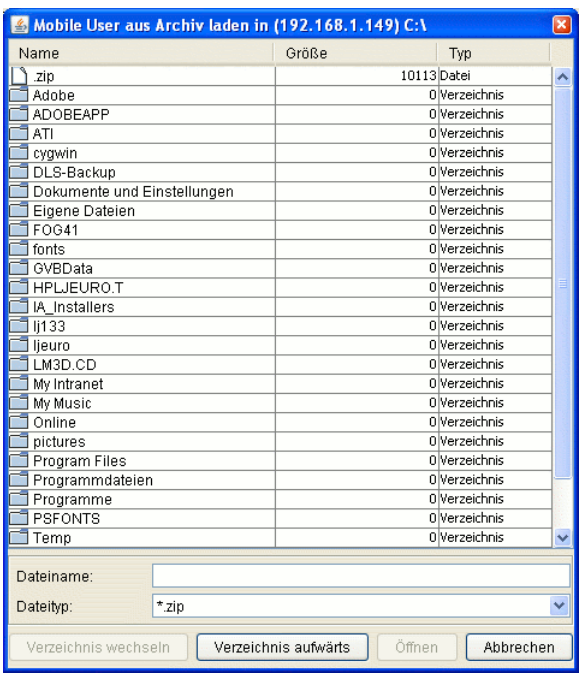
5. Standardmäßig wird der Inhalt desjenigen Laufwerks angezeigt, auf dem der DLS installiert ist. Durch Markieren eines Verzeichnisnamens und anschließendes Klicken von **Verzeichnis wechseln** oder Doppelklick auf den Verzeichnisnamen wählen Sie das gewünschte Zielverzeichnis. Mit **Verzeichnis aufwärts** gelangen Sie eine Verzeichnisebene höher.

6. Geben Sie einen Dateinamen für das ZIP-Archiv ein und bestätigen Sie mit **Speichern**. Alternativ können Sie ein bereits existierendes Archiv in der Liste durch Einfachklick markieren und darauf **Speichern** betätigen. Im daraufhin erscheinenden Auswahlfenster können Sie wählen, ob Sie die Mobile User-Daten in das vorhandene Archiv einfügen (**Existierendes Archiv erweitern**) oder das vorhandene Archiv überschreiben (**Neues Archiv erstellen**) wollen.

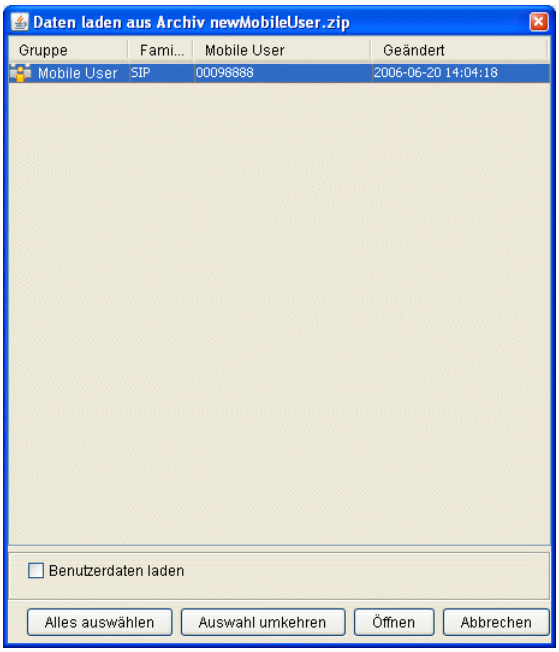
16.13.10.3 Mobile User-Daten laden

HINWEIS: Das Laden von Mobile User-Daten ist nur dann möglich, wenn die betreffenden Mobile User abgemeldet sind. Die Daten eines angemeldeten Mobile Users werden nicht überschrieben.

1. Wählen Sie den Bereich **Mobile User** > **SIP Mobile User Interaktion** > **SIP Mobile User**.
2. Wählen Sie nun in der Menüleiste unter **Aktion** den Eintrag **Mobile User importieren**. Es öffnet sich ein Dialogfenster zur Auswahl des Pfads. Durch Markieren eines Verzeichnisnamens und anschließendes Klicken von **Verzeichnis wechseln** oder Doppelklick auf den Verzeichnisnamen wählen Sie das gewünschte Zielverzeichnis. Mit **Verzeichnis aufwärts** gelangen Sie eine Verzeichnisebene höher.



3. Markieren Sie ein .zip-Archiv aus der Liste und klicken Sie auf **Öffnen**. Es wird eine Liste aller in diesem Archiv gespeicherten Mobile User-Datensätze angezeigt.



4. Markieren Sie die die gewünschten Datensätze oder betätigen Sie ggf. **Alles auswählen**. Sie können auch die **Auswahl umkehren**. Mithilfe der Checkbox **Benutzerdaten laden** bestimmten Sie, ob auch die nicht konfigurierbaren Daten des Benutzers wie z.B. Ruflisten oder Telefonbuchdaten in die DLS-Datenbank geladen werden.

   HINWEIS: Ruflisten und Telefonbuchdaten werden verschlüsselt gespeichert.

5. Wenn Sie nun **Öffnen** betätigen, werden die ausgewählten Mobile User-Daten in die DLS-Datenbank geladen.

   HINWEIS: Je nach Datenmenge kann das Laden von Mobile User-Daten einige Zeit dauern.
   Die Größe der nicht konfigurierbaren Daten des Benutzers kann über **Mobile User** > **User Daten Administration abgefragt werden.**

16.13.11 Mobile User Daten importieren

Es besteht die Möglichkeit, eine manuell erzeugte Datei mit Mobile User-Daten im csv-Format zu importieren. Ein Export von Mobile User Daten ist aus Datenschutzgründen nicht möglich.

Die Datei muss folgenden Aufbau haben:

1. Zeile: Beschreibung des Spalteninhalts in dieser Reihenfolge:

<E.164>	Pflichteintrag, gültige E.164 Nummer
<Mobile User Passwort>	Pflichteintrag
<Mobile User Profil>	Pflichteintrag
<Übernahme der SIP Daten von virtuellen Devices>	optional
<Home Phone>	optional
<Automatisches Logon am Home Phone zulassen>	Pflichteintrag, mögliche Werte: true, false
Übernahme der Keyset-Konfiguration vom virtuellen Device	Optional

Tabelle 17

2. und folgende Zeilen: Inhalte der jeweiligen Spalten getrennt durch ';'

Beispiel einer Import-Datei:

```
<E.164>;<Mobile User Passwort>;<Mobile User Profil>;<Übernahme der SIP Daten von
virtuellen Devices>;<Home Phone>;
<Automatisches Logon am Home Phone zulassen>
12345;000000;@profile;;;false
33333;000000;@profile;;;false
4411594311111;000000;MobUser;;;false
4411594312334566789;000000;MobUser;;12345;true
```

Beispiel - Importdaten zur Erstellung eines Mobile User mit SIP-Registrierung und Keyset-Daten:

1.Import eines virtuellen Device mit dazugehörigen SIP-Registrierungsdaten und Keyset-Konfiguration :

##CreateSIPPhone <ID> <E.164> <Typ>...<SIP-Server-Adr.><SIP-Server-Port><SIP-Reg-Adr.><SIP-Reg-Port>…

CreateSIPPhone 302108189656 OpenStage 80... 10.7.1.54 5060 10.7.1.54 5060…

Keysets

ModifyKeyset<Reset><E.164-Nummer><Attributname>=<Attributwert>]+

ModifyKeysetFALSE302108189656line-registration-leds=true...

Tasten

ModifyKey<Reset><E.164-Nummer><Tastenfunktion><Ebene><Modul>...

ModifyKeyFALSE302108189656Halten00...

ModifyKeyFALSE302108189656Anrufschutz00...

ModifyKeyFALSE302108189656Konferenz00...

ModifyKeyFALSE302108189656Headset00...

ModifyKeyFALSE302108189656Mobility00...

ModifyKeyFALSE3021081896567010...

ModifyKeyFALSE302108189656Integr. Trennen40...

ModifyKeyFALSE302108189656Integr. AUL40...

ModifyKeyFALSE302108189656Integr. Sprachwahl40...

2.Import des Mobile User :

302108189656;000000;temp;true;;false;true

Um eine Datei mit Mobile User-Daten zu importieren, verfahren Sie wie folgt:

1. Klicken Sie im Bereich **Mobile User** > **SIP Mobile User Interaktion** > **SIP Mobile User** auf **Mobile User importieren**. Anschließend öffnet sich ein Dialogfenster, in dem Sie die gewünschte Datei auswählen können.
2. Bestätigen Sie abschließend mit **Sichern**.

16.13.12 Mobility zwischen optiPoint und OpenStage

Mobility zwischen optiPoint und OpenStage ist zwar möglich, aber nicht ohne Einschränkungen. Für weitere Informationen siehe
http://wiki.siemens-enterprise.com/images/7/72/SIP_Mobility_User_-_optiPoint_and_OpenStage_Regression_Test.pdf

16.14 HFA Mobility an HiPath 3000

Dieses Leistungsmerkmal erlaubt die Verwendung von HiPath 3000 IP Mobility in einer Netzwerkumgebung (TDM oder IP-Sätze) mit geschlossenem Rufnummernbereich.

> ***HINWEIS:*** Technisch ist nur ein passender HiPath 3000 LCR Wählplan für IP Clients an anderen Knoten erforderlich, das LCR Routing ist aber irrelevant. Ohne einen passenden LCR Wählplan ist es nur möglich, lokale E.164-Nummer des Teilnehmers einzugeben, wenn dieses Leistungsmerkmal genutzt werden soll. Die Netzwerk-Trunks werden nicht für dieses Leistungsmerkmal verwendet.

Bei HiPath 3000 Anlagen ist der DLS dafür verantwortlich, dass die korrekten Registrierungsdaten an diejenigen IP Clients gesendet werden, die sich nicht an ihrer Home Location anmelden.

HFA Mobility an HiPath 3000-Anlagen funktioniert wie folgt: Ein Teilnehmer einer anderen HiPath 3000-Anlage meldet sich an einem IP Phone an, was zunächst bewirkt, dass dieses aufgrund der modifizierten Registrierungsdaten nicht mehr mit dem Gateway kommunizieren kann. Das IP Phone wendet sich an den DLS, der darauf das zur E.164-Nummer des Teilnehmers gehörende virtuelle Device heraussucht. Die Registrierungsdaten dieses virtuellen Devices werden nun an das IP Phone geschickt, so dass es sich registrieren kann.

Weitere Einstellungen siehe Abschnitt 7.1.18, “HFA Mobility”.

16.14.1 HiPath 3000 Konfiguration Voraussetzungen

IP Mobility ist eingerichtet und arbeitet an jedem HiPath 3000 Knoten gemäß der HiPath 3000/5000 Featurebeschreibung.

16.14.2 DLS Konfiguration für netzwerkweite HFA Mobility

Hier wird nur die zusätzliche DLS Konfiguration, die für HFA Mobility mit HiPath 3000 notwendig ist, berücksichtigt:

- Importieren Sie die Konfiguration jedes Knotens in den DLS mittels „Element Manager“ (einschließlich der mobilen IP Clients). Die mobilen IP Clients sind virtuelle Devices im DLS.
- In **IP Devices** > **IP Device Verwaltung** > **IP Device Konfiguration**> **Register „Allgemeines“** muss der Schalter **Für HFA Mobility an HiPath 3000 verwenden** für jeden mobilen IP Client in jedem Knoten eingeschaltet werden.

16.14.3 Bedienablauf

1. Aktivieren (Mobile User Logon) mit der Eingabe:
   *9419 + E.164 Teilnehmerrufnummer + Passwort (Passwort ist optional, falls nicht eingerichtet)
2. Das IP Phone wird versuchen, sich mit der eingebenen E.164 Teilnehmerrufnummer am aktuellen HiPath 3000 Knoten anzumelden. Die Meldung „Logging On To Home“ wird kurz angezeigt. Der Logon wird fehlschlagen, weil der mobile IP Client nicht am HiPath 3000-Knoten eingerichtet ist. Die Meldung „Mobile Log On Failed“ wird in der obersten Zeile des Displays angezeit; in der untersten Zeile wird „Contacting DLS“ angezeigt.

   Das IP Phone wird einen „mobility-configuration-request“ zum DLS senden. Der DLS wird daraufhin die korrekten Registrierungsdaten senden, mit denen sich der mobile IP Client dann am korrekten Heimatknoten anmelden kann.
3. Deaktivieren (Mobile User Logoff) mit der Eingabe #9419.

16.15 Datenstrukturen für DLS-eigene XML-Applikationen

Im Folgenden wird beschrieben, wo die von DLS-eigenen XML-Applikationen verwendeten Daten gespeichert sind. Dies ermöglicht eigene Anpassungen durch den Benutzer bzw. Administrator.

16.15.1 Verzeichnisstruktur

- Texte und Default-Bilder werden unter `<DLS Installationspfad>/DeploymentService/Tomcat5/webapps/XMLApplications/data/default gesucht.`
- Für Kundenanpassungen mittels eigener Texte und Bilder kann ein Verzeichnis `<DLS Installationspfad>/DeploymentService/Tomcat5/webapps/XMLApplications/data/custom` angelegt werden, das dann Such-Pfad für die Texte und Bilder ist.

  HINWEIS: Es wird empfohlen, dass das Verzeichnis `.../XMLApplications/data/default` nach `.../XMLApplications/data/custom` zu kopieren und dort die Änderungen einzubringen.
- Unter `.../XMLApplications/data/DeploymentService`, `.../XMLApplications/data/LocationService`, `.../XMLApplications/data/MakeCall`, `.../XMLApplications/data/NewsService` werden Texte für die jeweiligen XML-Applikationen abgelegt. Diese Verzeichnisse dürfen vom Anwender nicht verändert werden.

16.15.2 Verzeichnisse bei Upgrade-Installationen

Bei Upgrade-Installationen ist folgendes zu beachten:

- Das Verzeichnis `.../XMLApplications/data/default` wird aktualisiert.
- Das Verzeichnis `.../XMLApplications/data/custom` wird in `.../XMLApplications/custom_old umbenannt.`

  HINWEIS: Eventuelle Kundenanpassungen müssen erneut vorgenommen werden. Kopieren Sie hierzu `.../XMLApplications/data/default` wieder nach `.../XMLApplications/data/custom` oder benennen Sie `.../XMLApplications/data/custom_old` in `.../XMLApplications/data/custom um.`
- Die Verzeichnisse `.../XMLApplications/data/DeploymentService`, `.../XMLApplications/data/LocationService`, `.../XMLApplications/data/MakeCall`, `.../XMLApplications/data/NewsService` bleiben unverändert erhalten.

16.15.3 Dateiverzeichnisse bei Backup/Restore

Bei einem Restore ist folgendes zu beachten:

- Das Verzeichnis `.../XMLApplications/data/default` wird nicht gesichert.
- Das Verzeichnis `.../XMLApplications/data/custom` wird gesichert und abhängig von der Schaltereinstellung von **Administration** > **Backup / Restore** > **Register „Restore“** > **Auch XML Applikationen Dateien wiederherstellen** entweder wiederhergestellt oder nach `.../XMLApplications/data/custom_<alte Version>` kopiert.

  HINWEIS: Eventuelle Kundenanpassungen müssen erneut vorgenommen werden. Kopieren Sie hierzu
  `.../XMLApplications/data/default` wieder nach
  `.../XMLApplications/data/custom` oder benennen Sie
  `.../XMLApplications/data/custom_old` in `.../XMLApplications/data/custom um`.
- Die Verzeichnisse `.../XMLApplications/data/DeploymentService`,
  `.../XMLApplications/data/LocationService`,
  `.../XMLApplications/data/MakeCall`,
  `.../XMLApplications/data/NewsService` werden gesichert und bei Restore zurückgespielt. Diese Verzeichnisse dürfen vom Anwender nicht verändert werden.

16.16 Mandantenfähigkeit

Im Folgenden wird beschrieben, wie die Daten mehrerer Kunden (= Mandanten) in einem DLS verwaltet werden können.

HINWEIS: Dieses Funktion steht nur zur Verfügung, wenn die Mandantenfähigkeit des DLS installiert wurde. Dies wird vom Installationsassistenten abgefragt

Bei mandantenfähigen Masken steht Ihnen die Auswahlbox **Mandanten** zur Verfügung. Ansonsten ist sie ausgegraut.

HINWEIS: Beim Anlegen neuer Objekte erscheint eine Fehlermeldung, wenn kein Mandant ausgewählt ist.

Bei mandantenfähigen Masken wird unterschieden, ob das Objekt einem Mandanten zugeordnet ist oder nicht, d.h. es wird in der Werkzeugleiste unter **Mandant** der Mandantenname oder <nicht zugewiesen> angezeigt.

Beim Hinzufügen lizenzpflichtiger Objekte werden die mandantenspezifischen Grenzen geprüft. Bei Neuanlage oder Änderungen von Mandanten werden die lizenzabhängigen Daten geprüft. Die jeweiligen Alarmschwellen werden mandantenspezifisch eingerichtet (siehe Abschnitt 6.3.1, “Mandanten”). Grundsätzlich wird bei den Alarmen zwischen mandantenabhängigen und -unabhängigen unterschieden.

16.16.1 Mandantenfähigkeit installieren /deinstallieren

16.16.1.1 Erstinstallation

Folgen Sie den Anweisungen des Installationsassistenten und klicken Sie bei **Komponenten** auf **Mandantenfähigkeit**.

16.16.1.2 Updateinstallation

Folgen Sie den Anweisungen des Installationsassistenten und klicken Sie bei **Komponenten** auf **Mandantenfähigkeit**.

Allen Daten, die mandantenspezifisch sein werden können, wird als Mandant <nicht zugewiesen> eingetragen. Sie können später definierten Mandanten zugeordnet werden.

16.16.1.3 Deinstallation

Führen Sie eine Updateinstallation durch und deaktivieren Sie bei **Komponenten** die **Mandantenfähigkeit**.

16.16.1.4 Mandanten von OpenScape Voice Assistant importieren

1. Abhängig von der verwendeten OpenScape Voice Assistant Version öffnen Sie, wenn Sie eine Version > V3.0 verwenden,
   Element Manager > **Element Manager Konfiguration** > **Register „OpenScape Voice Assistant“**
   oder
   Element Manager > **Element Manager Konfiguration** > **Register „OpenScape Voice Assistant V3.0“**.
2. Markieren Sie **Mandanten synchronisieren** und klicken Sie auf **Business Groups aktualisieren**.

Es werden für jede Business Group ein Mandant sowie ein Standort angelegt. Die dabei verwendeten Namen werden aus <BusinessGroups Switchname (OpenScape Voice Assistant Version > V3.0) ><BusinessGroups Name> gebildet. Bereits vorhandene Mandanten und Standorte werden aktualisiert.

16.16.2 Mandanten einrichten

1. Wählen Sie den Bereich **Administration** > **Server Konfiguration** > **Mandanten**.
2. Tragen Sie die benötigte Anzahl an Lizenzen ein. Die Gesamtanzahl der Lizenzen kann über **Administration** > **Server Lizenzen** überprüft werden.
3. Ist bereits ein geeigneter Standort vorhanden, ordnen Sie diesen jetzt unter **Administration** > **Server Konfiguration** > **Mandanten** > **Register „Standorte“** dem Mandanten zu. Die möglichen Werte werden in einer Auswahlliste angezeigt. Es können auch mehrere Standorte zugewiesen werden. Fahren Sie anschließend mit Schritt 6 fort.
4. Sollte noch kein geeigneter Standort eingerichtet sein, klicken Sie zunächst **Sichern**, um den Mandanten zu erzeugen, denn dieser wird für die Einrichtung des Standorts benötigt. Dann wählen Sie **Administration** > **Server Konfiguration** > **Standort und** richten Sie einen Standort ein.

   HINWEIS: Alle IP Devices müssen einem definierten Standort (nicht Default Location) zugeordnet sein. Werden IP Clients eingesetzt, muss beim Eintrag von IP-Bereichen darauf geachtet werden, dass alle für die IP Clients möglichen IP Adressen berücksichtigt sind.

   HINWEIS: Werden IP Clients eingesetzt, so muss beim Eintrag von IP Bereichen darauf geachtet werden, dass alle für die IP Clients möglichen IP Adressen berücksichtigt sind.
5. Wechseln Sie zu **Administration** > **Server Konfiguration** > **Standort** > **Register „Mandanten“** und weisen Sie den Standort einem Mandanten zu. Ein Standort kann immer nur einem Mandanten zugeordnet werden.
6. Wechseln Sie **Administration** > **Account Management** > **Account Konfiguration** und weisen Sie dem Account, der auf die Daten dieses Mandanten zugreifen soll, diesen Mandanten zu.

HINWEIS: Der neu eingerichtete Mandant wird automatisch dem ‘admin’-Account zugewiesen. Diese Zuweisung kann nicht über das GUI erfolgen.

16.16.3 Mandanten löschen

Zum Löschen eines Mandanten müssen zuerst alle Referenzen auf diesen Mandanten gelöscht werden.

1. Wählen Sie den Bereich **Administration** > **Server Konfiguration** > **Mandanten**.
2. Markieren Sie den gewünschten Mandanten und löschen Sie die eingetragenen Standorte im **Register „Standorte“**.
3. Klicken Sie auf **Löschen** und bestätigen Sie im Dialogfenster, dass der Mandant gelöscht werden soll.

   HINWEIS: Beim Löschen eines Mandanten wird dieser automatisch vom ‘admin’-Account entfernt. Dies kann nicht über das GUI erfolgen.

16.16.4 Mandantenfähigen Account einrichten

1. Wählen Sie den Bereich **Administration** > **Account Management** > **Account Konfiguration**.
2. Richten Sie einen Account ein, wie in Abschnitt 6.1, “Account Management” beschrieben. Wählen Sie dabei als **Zugangsart DLS-GUI** aus.
3. Weisen Sie die gewünschten Rollen zu. Die Rolle EDIT_GENERAL_ONE stellt sicher, dass vom Account nur mandantenabhängige Masken bearbeitet werden können. Mit der Rolle EDIT_SYSTEM können auch systemrelevante Masken, die alle Mandanten betreffen, bearbeitet werden.
4. Wechseln Sie in das **Register „Mandanten“**. Unter **Mandant** können die Mandanten eingetragen werden, die durch diesen Account bearbeitet werden können.

Mandantenfähige Accounts können Daten ihrer zugeordneten Mandanten sowie Daten, die mit <nicht zugewiesen> markiert sind, bearbeiten. Dem „admin“-Account steht zusätzlich noch die Auswahl <alle> zur Verfügung, mit der alle in der Datenbank eingetragenen Daten angezeigt und bearbeitet werden können.

16.16.5 Mandantenfähige Alarm-Konfiguration

Beim Einrichten von Mandanten wird automatisch eine mandantenspezifische Alarm-Konfiguration angelegt. Die Daten der allgemeinen (<nicht zugewiesen>) Alarm Konfiguration werden dabei kopiert. Durch Eintrag eines Mandanten in der Werkzeugliste wird die mandantenabhängige Alarm-Konfiguration ausgewählt. Es können dann mandantenabhängig für Lizenz, Mobility und Zertifikatsablauf jeweils email-Adressen, Kommandodateien und SNMP-Traps eingetragen werden.

16.16.6 Serverzuweisungen

Für FTP Server, HTTPS Server und Netzlaufwerke müssen die Mandanten in den jeweiligen Masken unter Register „Mandanten“ zugewiesen werden. Die Zuordnung eines Standortes (siehe Mandanten einrichten), reicht nicht aus, auch wenn dem Standort seinerseits Server zugeordnet sind.

16.16.7 Mobile User

Hinlichtlich der Mobile User-Funktionalität ist Folgendes zu beachten:

- Beim Standort des Mandanten sollte ein E.164-Pattern eingetragen ist, da somit sichergestellt werden kann, dass die eingerichtete Mobile User Rufnummer zulässig ist.
- Werden Rufnummernbänder zwischen Mandanten verschoben, müssen die Mobile User manuell den neuen Mandanten zugeordnet werden. Gehen Sie hierzu auf **Mobile User**> **SIP Mobile User Interaktion** > **SIP Mobile User** und wählen Sie den Mandanten im Menü **Mandant** der Werkzeugleiste.

16.16.8 Mandantenfähiges Profil Management

Beim Hinzufügen eines Standorts zu einem Mandanten werden die Default-Profile auch diesem Mandanten zugewiesen, einschließlich der verwendeten Templates. Alle übrigen Profile, User Data Profile und Templates können über die jeweiligen Register „Mandanten“ einzelnen Mandanten zugewiesen werden.

16.16.9 Rufnummernband bei Mandantenfähigkeit

Die virtuellen Devices, die Teil des Plug&Play sind, werden dem Standort zugeordnet, dessen Rufnummernband ihre jeweilige E.164-Nummer enthält. Ist Mandantenfähigkeit in dieser DLS-Installation verfügbar, wird die E.164-Nummer entsprechend einem Mandanten zugeordnet.

16.17 Migrationsszenarien

Migrationsszenarien beinhalten u. a. auch Deployment-Änderungen, während Upgrade-Szenarien sich ausschließlich auf die Installation einer neuen DLS-Version über eine vorhergehende beziehen, und zwar bei gleichem Deployment.

OpenScape Deployment Service unterstützt die folgenden Szenarien:

- **Upgrade-Szenarien**

Von	Nach
Onboard DLS bei Integrated Simplex V3R1/V6R1/V7	Onboard DLS bei Integrated Simplex V7R1
Windows DLS Single Node V3R1/V6R1/V7	Windows DLS Single Node V7R1
Windows DLS Multi-Node V3R1/V6R1/V7	Windows DLS Multi-Node V7R1

- **Migrationsszenarien**

  Beginnend mit **CV319** unterstützt DLS V7R1 derzeit folgende Szenarien:

Von	Nach
Onboard DLS bei Integrated Simplex V3R1/V6R1/V7	Windows DLS Single Node V7R1
Onboard DLS bei Integrated Simplex V3R1/V6R1/V7	Windows DLS Multi-Node V7R1
Windows DLS Single Node V3R1/V6R1/V7	Windows DLS Multi-Node V7R1

HINWEIS: Windows DLS Single Node mit lokaler oder Remote-Datenbank wird ebenfalls unterstützt.

16.17.1 Von Onboard DLS bei Integrated Simplex V3R1/V6R1/V7 nach Windows DLS Single Node V7R1

Sichern der DLS-Datenbankdaten für Onboard DLS bei Integrated Simplex

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Deployment Service für Onboard DLS bei Integrated Simplex, indem Sie den Befehl „`./symphoniad stop“ in folgendem Verzeichnis ausführen: `/etc/init.d/`
3. Führen Sie unter `/enterprise/share/tomcat/webapps/DeploymentService/database` den Befehl „sh dbexport.sh /tmp/Dateiname.zip“ aus.

   Mit diesem Befehl wird die DLS-DB in das Verzeichnis `/tmp` exportiert. Alternativ können Sie auch ein anderes Verzeichnis auswählen, um die exportierten Daten dort in einer Datei namens „Dateiname.zip“ zu archivieren.

4. Starten Sie den Deployment Service für Onboard DLS bei Integrated Simplex, indem Sie den Befehl „./symphoniad start“ in folgendem Verzeichnis ausführen: `/etc/init.d`

Migrieren der DLS-Datenbankdaten auf den Windows DLS Single Node

1. Neuinstallation für Windows DLS V7R1 Single Node.
2. Kopieren Sie die Datei „Dateiname.zip“ in den Ordner:
   `[Installationspfad]\DeploymentService\Tomcat\webapps\DeploymentService\database\`
3. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
4. Beenden Sie den Deployment Service am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Stop Service**.
5. Um die DLS-Daten zu migrieren, führen Sie (als Administrator) den folgenden Befehl an der Eingabeaufforderung aus:

   `[Installationspfad]\DeploymentService\Tomcat\webapps\DeploymentService\database\ migrate.bat Dateiname.zip`
6. Starten Sie den Dienst Deployment Service am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** >**Programme** > **Deployment Service** > **Start Service**.

16.17.2 Von Onboard DLS bei Integrated Simplex V3R1/V6R1/V7 nach Windows DLS Multi-Node V7R1

Sichern der DLS-Datenbankdaten für Onboard DLS bei Integrated Simplex

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Deployment Service für Onboard DLS bei Integrated Simplex, indem Sie den Befehl „`./symphoniad stop`“ in folgendem Verzeichnis ausführen: `/etc/init.d/`
3. Führen Sie unter `/enterprise/share/tomcat/webapps/DeploymentService/database` den Befehl „sh dbexport.sh /tmp/Dateiname.zip“ aus.

   Mit diesem Befehl wird die DLS-DB in das Verzeichnis `/tmp` exportiert. Alternativ können Sie auch ein anderes Verzeichnis auswählen, um die exportierten Daten dort in einer Datei namens „Dateiname.zip“ zu archivieren.
4. Starten Sie den Deployment Service für Onboard DLS bei Integrated Simplex, indem Sie den Befehl „./ symphoniad start“ in folgendem Verzeichnis ausführen: `/etc/init.d`

Migrieren der DLS-Datenbankdaten auf den Windows DLS Multi-Node

Das folgende Beispiel veranschaulicht die Migration eines Multi-Node mit zwei (2) DLS-Knoten:

1. Neuinstallation für Windows DLS V7R1 Multi-Node.
2. Kopieren Sie die Datei „Dateiname.zip“ auf dem ersten DLS-Knoten in den Ordner:
   `[Installationspfad]\DeploymentService\Tomcat\webapps\DeploymentService\database\`
3. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.

4. Beenden Sie den Deployment Service für beide Knoten am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Stop Service**.
5. Um die DLS-Daten zu migrieren, führen Sie für den ersten DLS-Knoten (als Administrator) den folgenden Befehl an der Eingabeaufforderung aus:

   ```
   [Installationspfad\DeploymentService\Tomcat\webapps\DeploymentService\database\
   migrate.bat Dateiname.zip
   ```

6. Starten Sie den Deployment Service für beide Knoten am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Start Service**.

16.17.3 Von DLS Single Node V3R1/V6R1/V7 nach Windows DLS Multi-Node V7R1

Sichern der DLS-Datenbankdaten für den Windows DLS Single Node

1. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
2. Beenden Sie den Deployment Service am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Stop Service**.
3. Um die DLS-Daten zu sichern, führen Sie (als Administrator) an der Eingabeaufforderung für den DLS Single Node den folgenden Befehl aus:
   ```
   [Installationpath\DeploymentService\Tomcat\webapps\DeploymentService\database\
   dbexport.bat Dateiname.zip
   ```
   Mit diesem Befehl wird die DLS-DB exportiert und in einer Datei namens „Dateiname.zip“ archiviert.
4. Starten Sie den Deployment Service am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Start Service**.

Migrieren der DLS-Datenbankdaten auf den Windows DLS Multi-Node

Das folgende Beispiel veranschaulicht die Migration eines Multi-Node mit zwei (2) DLS-Knoten:

1. Neuinstallation für Windows DLS V7R1 Multi-Node.
2. Kopieren Sie die Datei „Dateiname.zip“ auf dem ersten DLS-Knoten in den Ordner:
   ```
   [Installationspfad]\DeploymentService\Tomcat\webapps\DeploymentService\database
   \
   ```
3. Schließen Sie alle Browser-Fenster mit Verbindung zum DLS.
4. Beenden Sie den Deployment Service für beide Knoten am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Stop Service**.
5. Um die DLS-Daten zu migrieren, führen Sie (als Administrator) an der Eingabeaufforderung für den ersten DLS-Knoten den folgenden Befehl aus:
   ```
   [Installationpath\DeploymentService\Tomcat\webapps\DeploymentService\database\
   migrate.bat Dateiname.zip
   ```

6. Starten Sie den Deployment Service für beide Knoten am DLS-Server. Klicken Sie hierzu im Windows Startmenü auf **Start** > **Programme** > **Deployment Service** > **Start Service**.

   HINWEIS: Wenn für einen Windows DLS Multi-Node die Datenbankspiegelung aktiviert ist, ist keine Migration von Backups (Sicherungen) möglich.

   HINWEIS: Um den Befehl „migrate.bat“ auszuführen, müssen Sie die Eingabeaufforderung als Administrator öffnen (Windows-Benutzerkontensteuerungsfunktion).

   HINWEIS: Fast alle Daten der Ziel-DLS-Installation, sofern vorhanden, werden gelöscht.
   Nur die folgenden Daten bleiben erhalten, wenn Daten zur Ziel-Load migriert werden:
   - die Konfiguration des Lizenzservers (hierdurch wird vermieden, dass sofort alle auf dem Lizenzserver vorhandenen Lizenzen aufgebraucht werden, wenn ein zweiter DLS mit den gleichen Daten gestartet wird)
   - die Konfiguration der lokalisierten Daten (die noch an die aktuelle Installation angepasst werden müssen, z. B. Trace-Dateiverzeichnisse).

   HINWEIS: Aufgrund von Erweiterungen in V6R1 ergeben sich ab **CV111.00** folgende Änderungen: die Datenbankdarstellung der Sprachen für die Kommando Datei, SNMP und E-Mail-Alarme wurde ausgetauscht.
   Bei dem Versuch, einen beliebige DLS (Linux oder Windows) mit **CV110.00** oder niedriger auf **CV111.00** oder höher zu migrieren, sollten Sie also damit rechnen, dass die o.g. Alarmsprachenkonfiguration ausgetauscht wird (d. h. Deutsch wird zu Englisch und Englisch zu Deutsch).

Im Anschluss an eine erfolgreiche Migration muss eine IP-Anpassung durchgeführt werden, da der neue DLS-Server nun auch eine neue IP-Adresse hat. Die hierzu benötigten Schritte werden im folgenden Abschnitt beschrieben.

16.17.3.1 Anschließende IP-Anpassung

Der DLS verwendet alle aktivierten LAN-Schnittstellenkarten des Servers, auf dem er installiert ist. Beim Ändern der IP-Adresse einer LAN-Karte (oder beim Austausch der DLS-Server-Hardware) oder während einer Migrationsroutine müssen folgende Aktionen durchgeführt werden:

1. Der DLS muss neu gestartet werden.
2. Alle DLS-Objekte, die die alte IP-Adresse verwenden, müssen angepasst werden; dies betrifft u. a. die DLS-Adresse in SCAN-Objekten und die Adresse des FTP-Servers, falls ein FTP-Server auf dem DLS-Host installiert ist.
3. Alle Geräte und Applikationen, die mit DLS kommunizieren, müssen neu konfiguriert werden:

- **Die Telefone werden über DHCP konfiguriert**: Passen Sie den DHCP-Server an; die Telefone verwenden nach Ablauf des DHCP-Lease die neue DLS-Adresse. Da der Lease möglichweise nie abläuft und Sie daher zu lange warten müssten, wird Folgendes empfohlen:
  - *Alle Telefone neu starten* (außerhalb der Geschäftszeiten) - Dies kann einige Zeit dauern. Nachdem alle Jobs beendet sind, sollten Sie die fehlerhaften Jobs überprüfen und/oder nach allen Telefonen suchen, denen noch die alte DLS-IP-Adresse zugewiesen ist. Versuchen Sie es dann erneut oder lösen Sie das Problem manuell (d. h. für den Fall, dass das Mobiltelefon ausgeschaltet ist).
- **Die Telefone werden nicht über DHCP konfiguriert**: Geben Sie **vor** Änderung der IP-Adresse die neue IP-Adresse manuell im DLS ein oder scannen Sie diese Telefone mit der neuen IP-Adresse.
- **Gateways, HiPath 4000 Manager, HiPath 8000 Assistant, HiPath QoS**: Konfigurieren Sie die DLS-Adresse manuell neu und verwenden Sie hierzu die für das jeweilige Produkt geltenden Mechanismen. Passen Sie beispielsweise in der CMP die DLS-Parameter an die neue IP-Adresse des DLS-Servers an.

16.17.4 DLS Multi-Node-Systeme mit Datenbankspiegelung bei Upgrade bzw. Migration des Betriebssystems

Dieser Prozess ist so konzipiert, dass das Upgrade bzw. die Migration des Betriebssystems (von Windows Server 2003 auf Windows Server 2008 R2) mit möglichst minimalen Ausfallzeiten für den DLS-Dienst durchgeführt wird.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Alle Geräte, Browser und API-Clients sind so konfiguriert, dass die Cluster-IP-Adresse und nicht die DLS-Knoten-IPs verwendet wird
- Während dieses Vorgangs dürfen keinerlei administrative Aufgaben durchgeführt werden. Mobility und Device Registrierung sind Funktionen, die (abgesehen von der Ausfallzeit, während der der Dienst angehalten wird) garantiert und erwartungsgemäß arbeiten. Alle administrativen Aufgaben, die automatisch ausgelöst werden, sollten deaktiviert sein (z. B. Element Manager Synchronisation, Plug & Play).
- Alle geplanten Jobs müssen vor Durchführung dieses Vorgangs gelöscht oder abgebrochen werden.
- Alle GUI-Browsersitzungen wurden abgemeldet.
- Wenn DCMP auf den DLS-Knoten installiert ist, muss wie im DLS-Admin-Handbuch beschreiben (siehe Abschnitt 4.4.2, Schritt 3) für jeden Knoten eine DCMP-Instanz im Cluster-Modus konfiguriert werden. Wenn DCMP auf einem externen System installiert ist, gibt es keine Auswirkungen auf DCMP.
- Nehmen Sie das DLS-Admin-Handbuch zur Hilfe. Alle nachfolgend aufgeführten Installations- und Konfigurationsschritte sollten wie im Admin-Handbuch des OpenScape Deployment Service beschrieben durchgeführt werden.

Computer und ihre Bezeichnungen/Abkürzungen:

Front End 1 (FE1): Dies ist der als DLS Knoten 1 ausgewiesene Computer des DLS-Clusters.

Front End 2 (FE2): Dies ist der als DLS Knoten 2 ausgewiesene Computer des DLS-Clusters.

Back End 1 (BE1) : Dies ist der als Datenbank-Server ausgewiesene Computer, dem bei der Systeminstallation die Rolle „Principal“ zugewiesen wurde. Wenn seit der Installation des Systems ein Failover stattgefunden hat, hat **BE1** inzwischen die Rolle „Mirror“ angenommen. **BE1** ist das System, das bei der Erstinstallation des Systems als Datenbank-Server mit der Rolle „Principal“ eingerichtet wurde.

Back End 2 (BE2): Dies ist der als Datenbank-Server mit der Rolle „Mirror“ ausgewiesene Computer. Weitere Details hierzu finden Sie oben unter **BE1**.

Back End 3(BE3): Dies ist der als Datenbank-Server mit der Rolle „Witness“ ausgewiesene Computer.

Abkürzungen und weiterführende Informationen finden Sie auch unter Abschnitt 17.1, “Abkürzungen und Fachbegriffe”

Voraussetzungen

- Eine DLS-Multi-Node-Umgebung in funktionsfähigem Zustand.
- Der Ordner CommonDlsData muss sich auf einem externen Computer befinden (nicht auf **FEx** oder **BEx**).
- Der CLA muss auf einem externen Computer installiert sein (nicht auf **FEx** oder **BEx**).

Gehen Sie folgendermaßen vor:

1. Vorbereitung der Datenbank-Server
   a) Überprüfen Sie, ob **BE2** die Rolle „Principal“ zugewiesen ist. Falls ja, machen Sie mit Schritt d weiter.
   b) Führen Sie in SQL Server Management Studio ein manuelles Datenbank-Failover durch; der Mirror-Datenbank-Server wird zum Principal-Datenbank-Server und der Principal-Datenbank-Server wird zum Mirror-Datenbank-Server.
   c) Überprüfen Sie, ob **FE2** funktionsfähig ist. Melden Sie sich direkt über die **FE2**-GUI (nicht die virtuelle IP-Adresse) an und überprüfen Sie, ob Ihre Anmeldung erfolgreich war.
   d) Deaktivieren Sie die Datenbankspiegelung über Microsoft SQL Management Studio.
2. Herunterfahren des **FE1** & **BE1** & **BE3**
   HINWEIS: Die Angabe des **BE3** (Witness-Server) ist optional und wird daher auch nicht von allen Konfigurationen verwendet. Wenn kein **BE3** vorhanden ist, überspringen Sie bitte die Anweisungen, die sich auf **BE3** beziehen.
   a) Fahren Sie **FE1**, **BE1** und **BE3 herunter.**
   b) Überprüfen Sie, ob **FE2** der Master ist und der DLS-Dienst läuft, indem Sie sich über die virtuelle Cluster-IP einloggen.
   c) Entfernen Sie **FE1** aus der Netzwerkkonfiguration des Load Balancers.
   - Für Microsoft NLB: NLB ist automatisch deaktiviert, wenn der DLS-Dienst angehalten wurde (siehe Schritt a). Überprüfen Sie in der NLB-Manager-Konsole von **FE2**, dass **FE1** in rot erscheint und **FE2** weiterhin auf „zusammengeführt“ (converged) steht.
   - Für einen externen Load Balancer: Konfigurieren Sie den externen Load-Balancer ordnungsgemäß.

   HINWEIS: Zum jetzigen Zeitpunkt unterstützt das DLS-Cluster weder Hohe Verfügbarkeit noch Load Balancing, allerdings ist der DLS-Dienst immer noch von **FE2** und **BE2** aus erreichbar.
3. Installation von Windows Server 2008 R2
   a) Installieren Sie Windows Server 2008 R2 inkl. Service Packs auf **FE1**, **BE1** und **BE3**.
   b) Führen Sie für **FE1**, **BE1** und **BE3** die Netzwerk-Konfiguration durch.

c) Installieren Sie den Microsoft NLB; bei Verwendung eines externen Load Balancers überspringen Sie diesen Schritt.

- Installieren Sie Microsoft NLB auf **FE1**, indem Sie ihn im Server-Manager als Feature hinzufügen.

WICHTIG: Fahren Sie bei der NLB-Konfiguration NICHT mit der Cluster-Erstellung fort.

d) Installieren und konfigurieren Sie den Windows-FTP-Server ordnungsgemäß auf **FE1**; überspringen Sie diesen Schritt, wenn kein Windows-FTP-Server verwendet wird.

e) Installieren Sie den SQL Server Native Client 2008 R2.

4. Installieren Sie SQL Server 2008 R2 auf **BE1** und **BE3**

5. Installieren Sie den DLS auf **FE1.**

a) Erstellen einen neuen Ordner for gemeinsame DLS-Daten (CommonDlsData).

HINWEIS: Statten Sie den Ordner mit den erforderlichen Berechtigungen aus. Verwenden Sie NICHT den gemeinsamen DLS-Daten-Ordner der vorherigen Installation.

- Der gemeinsame DLS-Daten-Ordner sollte idealerweise auf **BE3** oder einem externen Computer liegen, NICHT jedoch auf dem Computer, auf dem der CLA installiert ist.

b) Installieren Sie den DLS auf **FE1.**

- Verwenden Sie exakt die gleiche Konfiguration wie beim alten System. Wenn DCMP auf dem alten System installiert war, installieren Sie DCMP auch auf dem Neuen.

- Installieren Sie einen Hotfix NICHT direkt. Installieren Sie immer zuerst die Basisversion des Hotfixes und führen Sie daran anschließend ein Upgrade auf den Hotfix durch. Die Basisversion von **V6 R1 127.05** lautet beispielsweise **V6 R1 127.00**.

c) Stoppen Sie den DLS-Dienst auf **FE1.**

6. Datenbankmigration

a) Sichern Sie die DLS-Datenbank von **BE2** aus – und führen Sie das Backup über die DLS-Benutzeroberfläche fort. Stellen Sie sicher, dass die Backup-Datei unter einem Netzwerkpfad gespeichert wird, der erreichbar ist für **FE1** – **BE1**. (z.B. auf **BE3**)

HINWEIS: Alle Aktionen und Anforderungen, die erst nach Beginn des Backup-Vorgangs an den DLS gesendet werden, werden bei einer Wiederherstellung/Neuinstallation NICHT berücksichtigt.

WICHTIG: Ab diesem Zeitpunkt ist der DLS-Dienst nicht mehr verfügbar.

b) Halten Sie den DLS-Dienst auf **FE2** an. Wenn Sie Microsoft NLB verwenden, prüfen Sie über den NLB Manager, dass der Konsolenhost für **FE2** angehalten wurde. Wenn dies nicht der Fall ist, stoppen Sie den Host manuell über den NLB.

- Entfernen Sie **FE2** aus der Netzwerkkonfiguration des Load Balancers.

- Für Microsoft NLB: NLB ist automatisch deaktiviert, wenn der DLS-Dienst angehalten wurde (siehe Schritt b).

- Für einen externen Load Balancer: Konfigurieren Sie den externen Load-Balancer ordnungsgemäß.

c) Deinstallieren Sie den CLA und installieren Sie ihn neu. Aktivieren Sie anschließend die Lizenzen für den DLS.

HINWEIS: Wenn auch andere Produkte den gleichen CLA verwenden, müssen zusätzliche Lizenzen für diese Produkte aktiviert werden.

d) Stellen Sie die DLS-Datenbank auf **BE1** wieder her. Fahren Sie über die DLS-Benutzeroberfläche mit der Wiederherstellung fort. Stellen Sie sicher, dass die Backup-Datei unter einem Netzwerkpfad gespeichert wird, der erreichbar ist für **FE1** und **BE1.**

7. NLB-Konfiguration und Start des neuen Clusters

a) Konfigurieren Sie die Netzwerkkonfiguration des Load Balancers für **FE1**.

- Erstellen Sie den Cluster mit der gleichen IP und Konfiguration wie beim alten System.
- Für Microsoft NLB: Fügen Sie **FE1** zum Cluster hinzu. Wählen Sie in der NLB-Manager-Konsole die Option „Create New Cluster“ (Neues Cluster erstellen) und fahren Sie beim neuen Cluster mit Host 1 = **FE1** und Cluster-IP = Virtuelle IP-Adresse fort.
- Für einen externen Load Balancer: Konfigurieren Sie den externen Load-Balancer ordnungsgemäß.

b) Starten Sie den DLS auf **FE1.**

c) Überprüfen Sie, ob die DLS-Neuinstallation funktionsfähig ist, indem Sie sich über die virtuelle IP-Adresse des Systems anmelden.

HINWEIS: Ab diesem Zeitpunkt ist der DLS-Dienst wieder vom neu installierten Windows Server 2008 R2-System aus verfügbar.

8. Installation von Windows Server 2008 R2

a) Installieren Sie Windows Server 2008 R2 auf **FE2** und **BE2.**

b) Führen Sie für **FE2** und **BE2** die Netzwerk-Konfiguration durch.

c) Installieren Sie den Microsoft NLB; bei Verwendung eines externen Load Balancers überspringen Sie diesen Schritt.

- Installieren Sie Microsoft NLB auf **FE1**, indem Sie ihn im Server-Manager als Feature hinzufügen.

WICHTIG: Fahren Sie bei der NLB-Konfiguration NICHT mit der Cluster-Erstellung fort.

d) Wenn für die Dateibereitstellung ein FTP-Server auf **FE2** installiert wurde, installieren, konfigurieren, testen Sie den FTP-Dienst unter Windows.

9. Installieren Sie SQL Server 2008 R2 auf **BE2.**

10. Richten Sie zwischen **BE1**, **BE2** und **BE3** eine Datenbankspiegelung ein (siehe Admin-Handbuch).

11. Installieren Sie den DLS auf **FE2.**

a) Verwenden Sie exakt die gleiche Konfiguration wie beim vorherigen System. Wenn DCMP auf dem alten System installiert war, installieren Sie DCMP auch auf dem Neuen.

b) Installieren Sie einen Hotfix NICHT direkt. Installieren Sie immer zuerst die Basisversion des Hotfixes und führen Sie daran anschließend ein Upgrade auf den Hotfix durch. Die Basisversion von **V6 R1 127.05** lautet beispielsweise **V6 R1 127.00**.

c) Überprüfen Sie, ob Sie sich mit der **FE2**-IP-Adresse (nicht die Cluster-IP-Adresse) am DLS anmelden können.

d) Konfigurieren Sie die Netzwerkkonfiguration des Load Balancers für **FE2**.

- Für Microsoft NLB: Fügen Sie **FE2** zum Cluster hinzu. Stellen Sie über die NLB-Manager-Konsole eine Verbindung zum vorhandenen Cluster her und fügen Sie dann **FE2** als Host zum Cluster hinzu.
- Für einen externen Load Balancer: Konfigurieren Sie den externen Load-Balancer ordnungsgemäß.

12. Überprüfen Sie, ob Sie sich mit der virtuellen IP-Adresse des Clusters am DLS anmelden können.

a) Aktivieren Sie alle automatischen Verwaltungsaufgaben, die vor Beginn der Migration deaktiviert wurden (z. B. Element Manager Synchronisation, P&P).

b) Aktivieren Sie alle geplanten Jobs, die vor Beginn der Migration abgebrochen wurden.

Der Upgrade-/Migrationsvorgang ist damit abgeschlossen. Der DLS-Cluster sollte nun wieder ohne jeglichen Datenverlust einsatzbereit sein.

Die IP- und MAC-Adress-Zuordnungen der Computer, die Reihenfolge des DLS-Knotens im Cluster und die Datenbankspiegelung bleiben unverändert.

17 Anhang

Im Anhang finden Sie ein Abkürzungsverzeichnis und weitere Informationen.

17.1 Abkürzungen und Fachbegriffe

Zusätzliche Informationen erhalten Sie in der einschlägigen Literatur zu den Themen Netzwerk-Technik und Voice over IP (VoIP).

HINWEIS: Erklärungen zu Mobility-Begriffen finden Sie im Abschnitt 3.8.1, “Mobility-Begriffserklärungen”.

AKZ

Abkürzung für „**A**mts**k**enn
ziffer“.Die Amtskennziffer (oder auch „Externer Zugangscode“) muss, wenn entsprechend konfiguriert, einer Rufnummer vorangestellt werden, wenn es sich bei der Nummer um eine externe Rufnummer handelt. Siehe auch Kanonisches Format.

AMO

Abkürzung für „**A**dministration and **m**aintenance **o**rder“.
Eine Anweisung, die Administrations- oder Wartungsinformationen direkt der CBX (**C**omputerized **b**ranch **e**xchange) anbietet. Ein AMO wird mittels EMML (Extended Maintenance Maschinensprache) übertragen.

ANAT

Abkürzung für „**A**lternative **N**etwork **A**ddress **T**ype“ bei SIP.

ASCII-Code

Standardisierter Zeichensatz zur Textdarstellung und -verarbeitung an Computern und Kommunikationsanalgen (siehe ASCII-Tabellen auf den nächsten Seiten).

ASCII-Tabelle (Standard)

Zeichen	ASCII (hex)	ASCII (dez)	Zeichen	ASCII (hex)	ASCII (dez)	Zeichen	ASCII (hex)	ASCII (dez)	Zeichen	ASCII (hex)	ASCII (dez)
	0	0	SP	20	32	@	40	64		`60	96
^A	1	1	!	21	33	A	41	65	a	61	97
^B	2	2		“22	34	B	42	66	b	62	98
^C	3	3	#	23	35	C	43	67	c	63	99
^D	4	4	$	24	36	D	44	68	d	64	100
^E	5	5	%	25	37	E	45	69	e	65	101
^F	6	6	&	26	38	F	46	70	f	66	102
^G	7	7		‘27	39	G	47	71	g	67	103
^H	8	8	(	28	40	H	48	72	h	68	104
^I	9	9	)	29	41	I	49	73	i	69	105
^J	0A	10	*	2A	42	J	4A	74	j	6A	106
^K	0B	11	+	2B	43	K	4B	75	k	6B	107
^L	0C	12	,	2C	44	L	4C	76	l	6C	108
^M	0D	13	-	2D	45	M	4D	77	m	6D	109
^N	0E	14	.	2E	46	N	4E	78	n	6E	110
^O	0F	15	/	2F	47	O	4F	79	o	6F	111
^P	10	16	0	30	48	P	50	80	p	70	112
^Q	11	17	1	31	49	Q	51	81	q	71	113
^R	12	18	2	32	50	R	52	82	r	72	114
^S	13	19	3	33	51	S	53	83	s	73	115
^T	14	20	4	34	52	T	54	84	t	74	116
^U	15	21	5	35	53	U	55	85	u	75	117
^V	16	22	6	36	54	V	56	86	v	76	118
^W	17	23	7	37	55	W	57	87	w	77	119
^X	18	24	8	38	56	X	58	88	x	78	120
^Y	19	25	9	39	57	Y	59	89	y	79	121
^Z	1A	26	:	3A	58	Z	5A	90	z	7A	122
	1B	27	;	3B	59	[	5B	91	{	7B	123
	1C	28	<	3C	60	\	5C	92	|	7C	124
	1D	29	=	3D	61	]	5D	93	}	7D	125
	1E	30	>	3E	62	^	5E	94	~	7E	126
	1F	31	?	3F	63	_	5F	95	DEL	7F	127

ASCII-Tabelle (Erweitert)

Zeichen	ASCII (hex)	ASCII (dez)	Zeichen	ASCII (hex)	ASCII (dez)	Zeichen	ASCII (hex)	ASCII (dez)	Zeichen	ASCII (hex)	ASCII (dez)
_	80	128		A0	160	À	C0	192	à	E0	224
_	81	129	¡	A1	161	Á	C1	193	á	E1	225
‚	82	130	¢	A2	162	Â	C2	194	â	E2	226
ƒ	83	131	£	A3	163	Ã	C3	195	ã	E3	227
"	84	132	¤	A4	164	Ä	C4	196	ä	E4	228
...	85	133	¥	A5	165	Å	C5	197	å	E5	229
†	86	134	¦	A6	166	Æ	C6	198	æ	E6	230
‡	87	135	§	A7	167	Ç	C7	199	ç	E7	231
ˆ	88	136	¨	A8	168	È	C8	200	è	E8	232
‰	89	137	©	A9	169	É	C8	201	é	E9	233
Š	8A	138	ª	AA	170	Ê	CA	202	ê	EA	234
‹	8B	139	«	AB	171	Ë	CB	203	ë	EB	235
Œ	8C	140	¬	AC	172	Ì	CC	204	ì	EC	236
_	8D	141	-	AD	173	Í	CD	205	í	ED	237
_	8E	142	®	AE	174	Î	CE	206	î	EE	238
_	8F	143	¯	AF	175	Ï	CF	207	ï	EF	239
_	90	144	°	B0	176	Đ	D0	208	ð	F0	240
‘	91	145	±	B1	177	Ñ	D1	209	ñ	F1	241
’	92	146	²	B2	178	Ò	D2	210	ò	F2	242
"	93	147	³	B3	179	Ó	D3	211	ó	F3	243
”	94	148	´	B4	180	Ô	D4	212	ô	F4	244
•	95	149	µ	B5	181	Õ	D5	213	õ	F5	245
–	96	150	¶	B6	182	Ö	D6	214	ö	F6	246
—	97	151	·	B7	183	×	D7	215	÷	F7	247
˜	98	152	¸	B8	184	Ø	D8	216	ø	F8	248
™	99	153	¹	B9	185	Ù	D9	217	ù	F9	249
š	9A	154	º	BA	186	Ú	DA	218	ú	FA	250
›	9B	155	»	BB	187	Û	DB	219	û	FB	251
œ	9C	156	¼	BC	188	Ü	DC	220	ü	FC	252
_	9D	157	½	BD	189	Ý	DD	221	ý	FD	253
_	9E	158	¾	BE	190	Þ	DE	222	þ	FE	254
Ÿ	9F	159	¿	BF	191	ß	DF	223	ÿ	FF	255

AUN

Abkürzung für „**A**nruf**ü**bernahme“.
Sie haben einen Workpoint im Büro, einen weiteren im Labor und wollen unter einer Rufnummer erreichbar sein? Dann können diese Workpoints in eine Anrufübernahmegruppe geschaltet werden. Der angerufene Workpoint läutet. Der Anruf kann angenommen werden. Zusätzlich leuchtet ein einem anderen Workpoint die LED „Anruf übernehmen“. Das Gespräch kann durch einen Druck auf die entsprechende Taste angenommen werden.

BE1

Abkürzung für „**B**ack **E**nd **1**“.
Dies ist der als Datenbank-Server ausgewiesene Computer, dem bei der Systeminstallation die Rolle „Principal“ zugewiesen wurde. Wenn seit der Installation des Systems ein Failover stattgefunden hat, hat BE1 inzwischen die Rolle „Mirror“ angenommen. BE1 ist das System, das bei der Erstinstallation des Systems als Datenbank-Server mit der Rolle „Principal“ eingerichtet wurde.

BE2

Abkürzung für „**B**ack **E**nd **2**“.
Dies ist der als Datenbank-Server mit der Rolle „Mirror“ ausgewiesene Computer. Weitere Details hierzu finden Sie oben unter BE1.

BE3

Abkürzung für „**B**ack **E**nd **3**“.
Dies ist der als Datenbank-Server mit der Rolle „Witness“ ausgewiesene Computer.

C-SWS

Abkürzung für „**C**entral **S**oft**w**are **S**upply Server“.
Bezeichnung für den zentralen Software Supply-Server in Brüssel.

CA

Abkürzung für „**C**ertification **A**uthority“ = Zertifizierungsstelle.

CAP

Abkürzung für „**C**ommon **A**pplication **P**latform“.

CAT NetInstall

In Deutschland kann zur Installation am ⑦ TAP der CAT NetInstall verwendet werden.

CD

Abkürzung für „**C**all **D**eflection“.
ISDN-Merkmal zur Rufumlenkung im Rufzustand.

CF

Abkürzung für „**C**all **F**orwarding“.
ISDN-Merkmal zur automatischen Rufweiterschaltung.

CF kann wie folgt unterschieden werden:

- **CFU**
  Call **F**orwarding **U**nconditional (sofortige Anrufweiterschaltung)
- **CFNR**
  Call **F**orwarding **N**o **R**eply (Anrufweiterschaltung bei Nichtmelden)
- **CFB**
  Call **F**orwarding **B**usy (Weiterschaltung im Besetztfall)

CLA

Abkürzung für „**C**ustomer **L**icense **A**gent“.
Die Komponente des HLM, die Lizenzen am Produkt entschlüsselt und den jeweiligen Produkten zuteilt.

CLI

Abkürzung für „**C**ommand **L**ine **I**nterface“.
Bedienung von Netzwerk-Geräten durch Eingaben in einer Kommandozeile. Diese Schnittstelle ist meistens durch Passwort geschützt und wird per Telnet erreicht.

CLM

Abkürzung für „**C**ustomer **L**icense **M**anager“.
Der Bestandteil des HLM, der HiPath-Produktlizenzen für den Kunden verwaltet.

CSV

Abkürzung für „**C**omma **S**eparated **V**alues“.
Datei mit tabellarischen Daten. Teilweise sind in der ersten Zeile die Spaltenüberschriften eingetragen. Generell wird eine Spalte durch ein Semikolon oder Komma abgetrennt und ein Zeilenwechsel durch den Beginn einer neuen Zeile angezeigt. Importierbar z. B. mit Microsoft Excel.

CTI

Abkürzung für „**C**omputer **T**elephony **I**ntegration“ (Computer-Telefonintegration).
Bei CTI handelt es sich um die Unterstützung des Telefondienstes durch die Computertechnik. Dazu gehören neben der Unterstützung von Dienstleistungsmerkmalen mit ihren diversen Vermittlungsfunktionen auch das Management der Anlage und das Accounting.

CTS

Abkürzung für „**C**lear **t**o **s**end“ (frei zum Senden).
Die Sendebereitschaft ist ein Schnittstellen-Steuersignal. Es ist Bestandteil der Modem-Steuerung im Handshake-Betrieb als auch der Zugriffsberechtigung im CSMA/CA-Verfahren. Bei diesem Verfahren, das auch in WLANs nach 802.11 eingesetzt wird, sendet die Station, die einen Übertragungswunsch hat, ein RTS-Paket (Ready to Send). Ist die Übertragungstrecke zum Empfänger frei, erhält sie als Antwort ein CTS-Paket.

CW

Abkürzung für „**C**all **W**aiting“.
ISDN-Merkmal zur Signalisierung von Zweitanrufen während des Gespräches.

DBFS

Abkürzung für „**D**ata**b**ase **F**eature **S**erver“.
Manager für HiPath 3000/5000-Kommunikationsplattform.

Default Route

Eine Default Route ist eine Route die für jede Zieladresse passt. Das bedeutet, die Route kann für jede Zieladresse verwendet werden. Die Default Route hat die geringste Priorität und wird nur dann verwendet, wenn alle anderen Routen nicht passen. Im wesentlichen bestimmt eine Route, welchen Weg die Pakete beim Transport im Netzwerk nehmen sollen bzw. können – ist kein Weg vorgeschrieben oder bekannt, so wird die Default Route verwendet.

DCMP

Abkürzung für „**D**LS-**C**ontact-**M**e-**P**roxy“. Der DCMP dient als Proxy zur Vermittlung zwischen DLS und Endgeräten, wenn eine Firewall oder NAT das Senden von Contact-Me-Nachrichten vom DLS an die Endgeräte verhindert. Der DCMP kann über die Firewall bzw. NAT hinweg mit dem DLS kommunizieren und wird von den Endgeräten regelmäßig abgefragt (Poll), ob Nachrichten vom DLS vorliegen. Sobald das der Fall ist, stellt der DCMP eine Verbindung zwischen Endgerät und DLS her. Der DLS kann nun seine Steuer- und Konfigurationsdaten an das Endgerät senden.

DHCP

Abkürzung für „**D**ynamic **H**ost **C**onfiguration **P**rotocol“.
Dynamische Vergabe von IP-Adressen für Teilnehmer eines IP-Netzes mittels eines zentralen DHCP-Servers.

DLS

Abkürzung für „OpenScape **D**ep**l**oyment **S**ervice“.
DLS ist eine OpenScape Management-Anwendung zum Administrieren von IP Devices (IP Phones, IP Client-Installationen und IP Gateways) in HiPath- und nicht-HiPath-Netzwerken.

DMC

Abkürzung für „**D**irect **M**edia **C**onnection“.
Bislang tauschen Workpoints, die mittels Signalisierung über eine Koppelinstanz (z. B. ein Gateway) miteinander Verbindungen aufbauen, ihre Nutzdaten in der Regel auch über diese Koppelinstanz aus. Verwenden die beiden Workpoints das gleiche Signalisierungsprotokoll und ist die Art der Nutzdatenübertragung gleich, dann ist es möglich, über die Vermittlung des Gateway die Workpoints ihre Nutzdaten direkt austauschen zu lassen. Das direkte Austauschen von Nutzdaten wird auch als Direktkopplung „**D**irect **M**edia **C**onnection“ bezeichnet.

DNS

Abkürzung für „**D**omain **N**ame **S**ervice“.
Der DNS-Dienst wandelt eine alphanumerische Namensanfrage (z. B. www.unify.com/de/) in eine IP-Adresse um.

Dazu besitzen die grossen Primery Nameserver von Internic und den nationalen Registrierungsstellen (z. B.: DE-NIC für Deutschland) Datenbanken-Server, in denen die jeweiligen IP-Adressen den Hostnamen zugeordnet sind.

Domain

Eine Domain ist ein logischer Verbund von Rechnern und kann sich auch in sogenannte Subdomains aufteilen. Für die Auflösung von Domainnamen werden DNS-Server benutzt. Ein Beispiel für einen Domainnamen wäre z. B. www.microsoft.com. Wobei der „.“ (Punkt) für die ROOT des DNS-Servers, .com für die kommerzielle Top-Level Domain, .microsoft für die Firma und www für den Rechner steht. Domainnamen werden von rechts nach links aufgelöst.

Downgrade

Installation einer Software mit einer niedrigeren als die zur Zeit aktuelle Versionsnummer.

DSM

Abkürzung für „optiPoint **d**i**s**play **m**odule“.
Beistellgerät für ein optiPoint Workpoint mit Touch-Screen und komfortablen Funktionen wie Telefonbuch, Browser, Java-Programme, usw.

DTMF

Abkürzung für „**D**ual **T**one **M**ulti **F**requency“.
Das Zweiton-Verfahren dient dem Wählvorgang in Telefoneinrichtungen. Dieses Verfahren löste das Pulswahlverfahren von älteren Telefonapparaten mit Drehscheibenwahl ab und dient dem schnelleren Verbindungsaufbau in den Kommunikationsnetzen. Das DTMF-Signal besteht aus zwei Tönen, die von dem Telefon-Tastenfeld erzeugt und an die Vermittlungsstelle gesendet werden. Die zwei Töne werden aus acht verschiedenen Tönen gewonnen und sind den Reihen (1, 4, 7, Stern) und den Spalten (1, 2, 3) der Telefontastatur zugeordnet. Über das DTMF-Verfahren können darüber hinaus auch menügesteuerte Dienste (z. B. Anrufbeantworter, Sprachboxen) direkt über die Telefontastatur angesteuert werden.

E.164

Standardisierte Rufnummer nach dem internationalen Rufnummernplan der ITU mit max. 15 Stellen. Üblicherweise zusammengesetzt aus den Teilen: Landeskennzahl (CC, **C**ountry **C**ode), Ortskennzahl (NDC, **N**ational **D**estination **C**ode) und Teilnehmernummer (SN, **S**ubscriber **N**umber).

EAP
Abkürzung für „**E**xtensible **A**uthentication **P**rotocol“.

ECT

Abkürzung für „**E**xplizit **C**all **T**ransfer“.
ISDN-Merkmal zur Gesprächsweitervermittlung während des Gesprächs.

ENB

Abkürzung für „**E**lectronic **N**ote **B**ook“.
Persönliches Telefonbuch im display module bzw. application module.

EOR

Abkürzung für „**E**nd **o**f **r**ecord“.
Beschreibt das Ende eines Datensatzes bzw. eines Berichtintervalls.

EOS

Abkürzung für „**E**nd **o**f **S**ession“.
Beschreibt das Ende einer Verbindung.

FE1

Abkürzung für „**F**ront **E**nd **1**“.
Dies ist der als DLS Knoten 1 ausgewiesene Computer des DLS-Clusters.

FE2

Abkürzung für „**F**ront **E**nd **2**“.
Dies ist der als DLS Knoten 2 ausgewiesene Computer des DLS-Clusters.

FTP

Abkürzung für „**F**ile **T**ransfer **P**rotocol“.
Wird zur Übertragung von Dateien in Netzwerken verwendet, z. B. um Telefon-Software zu aktualisieren.

G.711

Audioprotokoll zur unkomprimierten Sprachübertragung nach dem Pulse code modulation Verfahren (PCM). Benötigt eine Bandbreite von 64 kbit/s („ISDN-Qualität“).

G.722

Audioprotokoll zur komprimierten Sprachübertragung mit max. 7 kHz. Benötigt eine Bandbreite von 64 kbit/s.

G.723

Audioprotokoll zur komprimierten Sprachübertragung. Die Qualität ist schlechter als bei G.711 und G.729. Benötigt eine Bandbreite von ca. 6 kbit/s.

G.729

Audioprotokoll zur komprimierten Sprachübertragung. Die Qualität ist schlechter als bei G.711 und besser als bei G.723. Benötigt eine Bandbreite von ca. 8 kbit/s.

Gatekeeper

Ein Gatekeeper ist eine logische Komponente des H.323-Standards, welcher sowohl als Windows- oder UNIX-Software, als Router-Option, als Teil einer MCU oder eines Gateway implementiert sein kann.

Gateway

Ein System (Rechner oder Baugruppe), das Daten zwischen unterschiedlichen Netzwerken überträgt. Von Gateways werden – falls erforderlich – unterschiedliche Protokolle aufeinander abgestimmt z. B. IP-Netz und ISDN-Netz. Ein Gateway kann zugleich auch einen Router beinhalten.

H.323-Standard

Der Standard besteht aus mindestens den folgenden Bestandteilen:

- Terminals
- Gateways
- Gatekeeper
- Multipoint Control Units (MCUs)

HFA

Abkürzung für „**H**icom **F**eature **A**ccess“ oder „**H**iPath **F**eature **A**ccess“.
Stellt die Verbindung mittels Gateway (z. B. HG 1500 oder HG 3530) zwischen IP-Telefonie und einer PBX dar.

HLM

Abkürzung für „**H**iPath **L**icense **M**anagement“.

HTTP

Abkürzung für „**H**yper**t**ext **T**ransfer **P**rotocol“.
Protokoll zur Übertragung von Daten in IP-Netzen.

INCA

Abkürzung für „**I**nterleaved **N**ative **C**ompiled **A**rchitecture“.
Teil der Soft- und Hardwarearchitektur der Workpoints.

IP

Abkürzung für „**I**nternet **P**rotokoll“.

IP-Adresse

Auch kurz „IP“ genannt. Eindeutige Adresse eines Endgerätes im Netzwerk; sowohl IPv4 als auch IPv6 können verwendet werden.

Eine IPv4-Adresse besteht aus 4 Zahlenblöcken, jeweils zwischen 0 und 255, getrennt durch „.“. Beispiel:
1.222.44.123

Eine IPv6-Adresse besteht aus 8 hexadezimalen Zahlenblöcken, getrennt durch „:“. Beispiel:
2001:0db8:85a3:08d3:1319:8a2e:0370:7347
oder, falls nicht alle Blöcke benutzt werden:
2000:1::3

IPSec

Abkürzung für „**I**nternet **P**rotocol **S**ecurity“.

Jitter

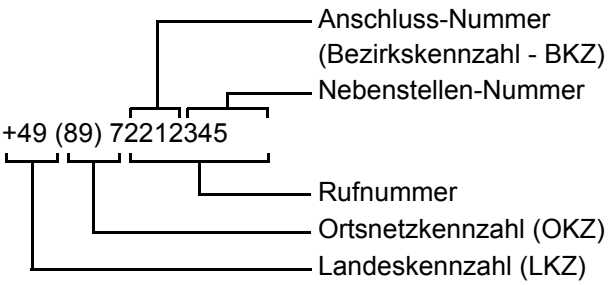
Laufzeitschwankungen bei der Datenübertragung in IP-Netzen.

JDBC

Abkürzung für „**J**ava **D**ata**b**ase **C**onnectivity“.
JDBC ist eine Schnittstelle mit der man eine Verbindung zwischen einem Java-Programm und einer Datenbank herstellen kann.

Kanonisches Format

Beispiel einer Rufnummer im kanonischen Format:



Um Rufnummern wählen zu können, die im kanonischen Format vorliegen, müssen diese mithilfe von Wählregeln bzw. Wahlparametern „wählbar“ gemacht werden. Hierzu werden die verschiedenen Kennzahlen als Teil in der Rufnummer erkannt und ggf. mit den entsprechenden Verkehrsausscheidungsziffern (siehe VAZ) bzw. der Amtskennziffer (siehe AKZ) ersetzt.

Nummernauflösung (Beispiele):

Gespeicherte Rufnummer im kanonischen Format	LKZ / IVAZ	OKZ / NVAZ	BKZ / AKZ	Gewählte Rufnummer
+49 (89) 722 12345	49 / 00	89 / 0	722 / 0	12345
+49 (89) 5593 22581	49 / 00	89 / 0	722 / 0	0559322581
+49 (9721) 884 6543	49 / 00	89 / 0	722 / 0	0097218846543
+43 (562) 2186 22415	49 / 00	89 / 0	722 / 0	00043562218622415
+43 (562) 2186 22415	43 / 00	562 / 0	2186 / 9	22415
+49 (89) 722 12345	49 / 00	89 / 0	5593 / 9	972212345
+49 (89) 722 12345	49 / 00	9721 / 0	5593 / 74	7408972212345
+49 (89) 722 12345	43 / 00	562 / 0	2186 / 74	7400498972212345

Tabelle 18 Nummernauflösung (Beispiele):

KDC

Abkürzung für „**K**ey **D**istribution **C**enter“ (Schlüsselverteilungscenter).

LAN

Abkürzung für „**L**ocal **A**rea **N**etwork“.

Layer 2

2. Schicht (Data Link Layer) im 7-schichtigen OSI-Modell zur Beschreibung von Datenübertragungs-Schnittstellen.

Auf Layer 2 befinden sich das sogenannte Netzzugangsprotokoll im LAN. Dahinter verbirgt sich der Zugriffsmechanismus (z. B. CSMA/CD bei Ethernet) und die MAC Adressierung.

Layer 3

3. Schicht (Network Layer) im 7-schichtigen OSI-Modell zur Beschreibung von Datenübertragungs-Schnittstellen.

Auf Layer 3 befindet sich das Netzwerkprotokoll, also zum Beispiel IP (Internet Protocol). Dieses ist in der Lage Datenpakete aufgrund der Adressierung eindeutig zu vermitteln. Geräte die diese Aufgabe übernehmen nennt man Router.

LDAP

Abkürzung für „**L**ightweight **D**irectory **A**ccess **P**rotocol“.
Vereinfachtes Protokoll für den Zugriff auf standardisierte Verzeichnissysteme, z. B. ein Firmentelefonbuch.

LCD

Abkürzung für „**L**iquid **C**rystal **D**isplay“.
Ziffern-, Text- oder Grafik-Anzeige mittels Flüssigkristall-Technik.

LEAP

Abkürzung für „**L**ightweight **E**xtensible **A**uthentication **P**rotocol“.

LED

Abkürzung für „**L**ight **E**mitting **D**iode“.
Kaltlichtlampe mit niedrigem Stromverbrauch und unterschiedlichen Farben.

LLDP-MED

Abkürzung für „**L**ink **L**ayer **D**iscovery **P**rotocol - **M**edia **E**ndpoint **D**iscovery“.

LOGO

Bezeichnet ein grafisch gestaltetes Signet.

Mask

Die Subnet Mask klassifiziert Netzwerke in A-, B- und C-Netze. Zu jeder Klasse gehört eine Subnet Mask, die die relevanten Bits ausmaskiert. 255.0.0.0 für Class A, 255.255.0.0 für Class B und 255.255.255.0 für Class C. In einem Klasse C-Netzwerk sind z. B. 254 ⑦ IP-Adressen verfügbar.

MAC

Abkürzung für „**M**edium **A**ccess **C**ontrol **A**ddress“.
Eine 48 bit-Adresse, mit der sich jedes Endgerät (z. B. ⑦ IP-Telefon oder Netzwerkkarte) in einem Netzwerk weltweit eindeutig identifiziert.

MCU

Eine MCU (**M**ultipoint **C**ontrol **U**nit) ermöglicht eine Konferenz zwischen drei oder mehr Teilnehmern, welche geografisch voneinander getrennt sind. Die MCU ist dabei eine Art „Sternverteiler“, welche die Endgeräte miteinander verbindet.

MD5

Abkürzung für „**M**essage-**D**igest“. Die **5** steht für eine neuere Variante des MD-Algorithmus. MD5 ist ein reiner Hash-Algorithmus und erzeugt aus beliebigen Datenlängen eine eindeutige, 128 Bit (16 Zeichen) umfassende Prüfsumme.

MDIX

Abkürzung für „**M**ultiple **D**ocument **I**nterface“. Auch Mehrfachdokumentenschnittstelle genannt.
Es erlaubt ein oder mehrere Dokumente in verschiedenen Ansichten innerhalb eines Fensters zu betrachten.

MDI-X

Abkürzung für **M**edia **D**ependent **I**nterface crossover. Ermöglicht das Verbinden von zwei Netzwerk-Endgeräten ohne Crossover-Kabel. Wenn Auto MDI-X zur Verfügung steht, kann das MDI automatisch zwischen normaler Anschlussbelegung und Crossover-Belegung umschalten, je nach angeschlossenem Gerät.

MEB

Abkürzung für „**M**edia **E**xtension **B**ridge“.

MIB

Abkürzung für „**M**anagement **I**nformation **B**ase“.
Datenbank, die Beschreibungen und Fehlermeldungen der Geräte und Funktionen in einem Netzwerk enthält.

MoH

Die Datei enthält die **M**usik **o**n **H**old (Wartemelodie).

MWI

Abkürzung für „**M**essage **W**aiting **I**ndicator“.
Signalisierung einer neuen, d. h. noch nicht gelesenen/gehörten Nachricht.

NAT

Abkürzung für „**N**etwork **A**ddress **T**ranslation“.
Durch einen Router, eine Firewall oder eine andere Netzwerkkomponente werden die Source NAT (Quelladdresse) und/oder die Destination NAT durch jeweils andere Addressen ersetzt. Diese Übersetzung findet üblicherweise zwischen zwei Netzen, etwa zwischen lokalem Netz und Internet statt.

OCK

Eine durch 802.11i mögliche schnelle Roaming-Technik wird auch als „**O**pportunistic **K**ey **C**aching“ oder „Proactive Key Caching“ bezeichnet.
Wenn mehrere Access Points PMKs (Pairwise Master Keys) miteinander teilen, ist es möglich, dass ein IP Phone zu einem zuvor noch nicht besuchten Access Point wechselt, ohne eine Pre-Authentication durchgeführt zu haben. Der beim letzten Access Point verwendete PMK wird dabei wiederverwendet.

Outbound Proxy

SIP-Proxy (=Stellvertreter), der bei einer gewählten SIP-URI entscheidet, wohin das abgehende Gespräch geroutet wird.

Im nachfolgenden Beispiel befindet sich der Registrar-Server in *dom1.com* und löst nach IP-Adresse *w.x.y.z* auf; *dom2.com* löst nach *a.b.c.d* auf.

Gewählte URI (vor Proxy)	Outbound Proxy			

Payload

Der Teil der IP-Daten bzw. eines IP-Datenpaketes, der die Nutzdaten, bei VoIP z. B. die Sprachdaten, enthält.

PBX

Abkürzung für „**P**rivate **B**ranch e**X**change“.
Private Telefonanlage, die verschiedene interne Geräte mit dem ISDN-Netzwerk verbindet.

PING

Abkürzung für „**P**acket **In**ternet **G**roper“.
Programm, um zu testen, ob eine Verbindung zu einem definierten IP-Ziel aufgebaut werden kann. Bei dem Test werden Daten zu dem Ziel gesendet und von dort zurückgeschickt. Als Ergebnis wird der Erfolg/Misserfolg der Übertragung und ggf. Zusatzinformationen wie Übertragungszeit ausgegeben.

Port

In IP-Netzen werden Ports verwendet, um mehrere Kommunikationsverbindungen gleichzeitig zuzulassen. Dabei habe verschiedene Dienste oftmals unterschiedliche Port-Nummern.

Proxy

Ein Proxy-Server ist ein Zwischenspeicher, der Informationen lokal vorhält.

PSE

Abkürzung für „**P**ersonal **S**ecurity **E**nvironment“.
Dazu gehören z. B. Phone Zertifikate, WPI Client Zertifikate usw.

PSK

Abkürzung für „**P**re-**S**hared **K**ey“.

Vorab ausgetauschte Passphrase zur Authentifizierung einer verschlüsselter Verbindung.

PSS

Abkürzung für „**P**re-**S**hared **S**ecret“.
Passwort zur Authentifizierung bei VoIP Security.

PSTN

Abkürzung für „**P**ublic **S**witched **T**elephone **N**etwork“, analoges Telefonnetz oder analoge Anschlüsse an digitalen Netzknoten auch öffentliches internationale Telefonnetz.

QCU

Abkürzung für „**Q**uality **C**ontrol **U**nit“.

QDC

Abkürzung für „**Q**uality **D**ata **C**ollection“.
Konzept zur zentralen Erfassung der Qualität von Sprechverbindungen über IP-Netze.

QoS

Abkürzung für „**Q**uality **o**f **S**ervice“.
Beschreibt die subjektiv wahrnehmbare Qualität (Dienstgüte) einer Sprech-Verbindung über IP-Netze. Eigenschaften der QoS sind Paketverlustrate, Paketverzögerung, Verzögerungsabweichung, reservierte Bandbreite, Art der Bitrate (variabel, konstant oder unspezifiziert) und Bitrate.

RADIUS

Abkürzung für „**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice“.
Protokoll bzw. Software zur Benutzer-Authentisierung mittels Wählleitung.

RAM

Abkürzung für „**R**andom **A**ccess **M**emory“.
Speicher mit Schreib/Lese-Zugriff.

RCC

Abkürzung für „**R**outing **C**ontrol **C**enter“.
Bei der Verwendung der zentralisierten Leitwegbestimmung senden die einzelnen Knoten im Netzwerk in regelmäßigen Abständen dem RCC die bei ihnen lokal anstehende, für die Wegewahl relevante Information. Das RCC speichert diese Information und berechnet dann aufgrund seiner globalen Kenntnis des Netzwerks die optimalen Verbindungswege zwischen den einzelnen Knoten.

Regulärer Ausdruck

Zeichenkette, die der Beschreibung von Mengen beziehungsweise Untermengen von Zeichenketten mit Hilfe bestimmter syntaktischer Regeln dient. Erstens stellen reguläre Ausdrücke eine Art Filterkriterium für Texte dar, indem der Ausdruck in Form eines Musters mit dem Text abgeglichen wird. So ist es beispielsweise möglich, alle Zeichenketten zu finden, die mit 1 oder 2 beginnen, ohne die nachfolgenden Ziffern vorgeben zu müssen. Zweitens können reguläre Ausdrücke als eine Art Schablone dienen, um Mengen von Ziffernkombinationen zu erzeugen, ohne jede Ziffernkombination einzeln angeben zu müssen.

ROM

Abkürzung für „**R**ead **O**nly **M**emory“.
Speicher mit Nur-Lese-Zugriff.

Router

Router bauen Verbindung zu Gateways auf und haben Zugang zu mehreren Subnetzen und anderen Routern. Er ermittelt anhand der IP-Adresse, in welches Subnetz bzw. an welchen anderen Router er die Daten senden muss. Er entscheidet, welcher Weg für die Daten im Augenblick der günstigste ist.

RSM

Abkürzung für „**R**ealtime **S**ervice **M**anager“.

RTC

Abkürzung für „**R**eal-**T**ime **C**ommunications Server“ von Microsoft.

RTS

Abkürzung für „**R**eady **t**o **s**end“ (bereit zum Senden).
Die Sendeanforderung wird bei Modem-Steuerungen benutzt sowie beim kollisionsfreien LAN-Zugangsverfahren CSMA/CA, wie es in 802.11 eingesetzt wird. In der Modem-Steuerung ist das RTS-Signal Bestandteil des Handshake-Betriebs; ein Kontrollsignal zwischen einem Modem und einem digital genutzten Endgerät, das die Datenübertragung auf der Übertragungsleitung initiiert.

SDLP

Abkürzung für „**S**tandard **D**evice **L**evel **P**rotocol“.

SHA-1

Abkürzung für „**S**ecure **H**ash **A**lgorithmus“. Die **1** für eine neuere Version davon. SHA1 ist ein Hash-Algorithmus und erzeugt aus Datenlängen unter 264 Bit eine Prüfsumme von 160 Bit (20 Zeichen) Länge.

SIP

Abkürzung für „**S**ession **I**nitiation **P**rotocol“.
Protokoll-Standard zur Initialisierung von Anrufen in IP-Netzen.

SNMP

Abkürzung für „**S**imple **N**etwork **M**anagement **P**rotocol“.
Das Protokoll wird für die Kommunikation mit Servern eingesetzt, die Netzwerk-Management-Funktionen übernehmen. Dazu gehört z. B. das Protokollieren von Fehlern, die an Netzwerk-Komponenten auftreten (SNMP-Trap).

SNTP

Abkürzung für „**S**imple **N**etwork **T**ime **P**rotocol“.
Das Protokoll wird zwischen Timeservern und Endgeräten eines Netzwerks eingesetzt, um die Uhrzeit der Endgeräte zu synchronisieren.

SPA

Abkürzung für „**S**oftware **P**roduct **A**ssurance“.

SQL

Die Abkürzung steht für Structured Query Language. Diese Programmiersprache zur Abfrage von Datenbanken wurde von IBM zur Abfrage von relationalen Datenbanken (z. B. Microsoft Access) entwickelt.
Bei der Entwicklung gab man besonders auf Client-Server-Umgebungen (Client fragt an, Server gibt Lösung zurück) acht.

SRSR

Abkürzung für „**S**mall **R**emote **S**ide **R**edundancy“.
Gibt an, dass ein Rückfallsystem vorhanden ist (Redundanzsystem).

SRTP

Abkürzung für „**S**ecure **R**ealtime **T**ransport **P**rotocol“.
Protokoll zur sicheren Übertragung von Multimedia-Daten durch symmetrische Verschlüsselung.

SSID

Abkürzung für „**S**ervice **S**et **ID**entifier“.
Netzwerkname in einem WLAN.

SSL

Abkürzung für „**S**ecure **S**ocket **L**ayer“.
Technik zur verschlüsselten Datenübertragung zwischen Client und Server durch Authentifizierung.

SSSO

Abkürzung für „**S**ecure **S**ingle **S**ign **O**n“.
Der Zugang zum DLS ist passwortgeschützt. Das SSSO und alle Informationen im DLS werden mittels SSL verschlüsselt übertragen.

Switch

Vermittlungsstelle in einem sternförmigen Netzwerk z. B. HiPath 4000 Anlage.

TAP

Abkürzung für „**T**echniker **A**rbeits**P**latz“.

TCP

Abkürzung für „**T**ransmission **C**ontrol **P**rotocol“.
Ist neben IP das zentrale Protokoll im Internet. Es stellt einen verbindungsorientierten, zuverlässigen, vollduplex Dienst in Form eines Datenstroms zur Verfügung.

TKIP

Abkürzung für „**T**emporal **K**ey **I**ntegrity **P**rotocol“.
Algorithmus zur Verschlüsselung in WLANs.

TLS

Abkürzung für „**T**ransport **L**ayer **S**ecurity“.
Standardprotokoll, um die Authentifizierung mittels Zertifikaten und Verschlüsselung durchzuführen.

TTL

Abkürzung für „**T**ime **T**o **L**ive“.
Mit diesem Wert wird die Lebensdauer eines IP-Datenpakets festgelegt. Bei der Übertragung von Daten in IP-Netzen versuchen Datenpakete auf verschiedenen Wegen ihr Ziel zu erreichen. Bei jedem Wechsel eines Netzes passiert das Datenpaket einen Router, wobei der TTL-Wert des Pakets um eins heruntergezählt wird. Sobald der Wert 0 erreicht ist, wird das Paket verworfen. Dadurch wird erreicht, dass Pakete, die ihr Ziel nach längerer Suche nicht finden, nicht endlos im Internet „herumirren“. Je höher also der ursprüngliche TTL-Wert eines Datenpaketes, umso länger kann das Paket versuchen, das Ziel zu erreichen.

UDP

Abkürzung für „**U**ser **D**atagram **P**rotocol“.
Kann alternativ zu TCP verwendet werden, wenn keine Anforderungen über die Zuverlässigkeit gestellt werden. UDP garantiert weder die Zustellung der Pakete, noch ist eine bestimmte Reihenfolge des Eintreffens von Paketen gewährleistet.

URI / URL

Abkürzung für „**U**niform **R**esource **I**dentifier“ bzw. „**U**niform **R**esource **L**ocator“.
Hiermit ist die Adresse einer Datei oder eines Verzeichnisses gemeint. Die häufigste Form einer URI ist eine URL. Ein typischer URI bezeichnet:

- den Zugriffsmechanismus auf den Inhalt (z. B. ein Protokoll wie http, ftp oder file),
- den Rechner, auf dem der Inhalt zu finden ist und

- den spezifischen Namen des Inhalts auf diesem Computer (üblicherweise ein Dateiname).

Die Teile sind optional, darum ist ein Dateiname für sich (auch ein relativer) ein URI.

VAZ

Abkürzung für „**V**erkehrs**a**usscheidungsziffer“.
Es wird zwischen nationaler VAZ (NVAZ oder „Nationale Vorwahl“) und internationaler VAZ (IVAZ oder „Internationale Vorwahl“) unterschieden. Beispielsweise für München ist die nationale VAZ die „0“ bei „**0**89“. Siehe auch Kanonisches Format.

VLAN

Abkürzung für „**V**irtual **L**ocal **A**rea **N**etwork“.
Unterteilung eines IP-Netzes in autonome Verwaltungsgruppen (Domains). Eine Möglichkeit der Kennzeichnung der Zugehörigkeit zu einem VLAN ist der Einsatz einer VLAN ID.

VLAN ist also eine Netzstruktur mit allen Eigenschaften eines gewöhnlichen LAN, jedoch ohne räumliche Bindung. Während die Stationen eines LAN nicht beliebig weit auseinander liegen können, ermöglicht es ein VLAN hingegen, weiter entfernte Knoten zu einem virtuellen lokalen Netzwerk zu verbinden.

VoIP

Abkürzung für „**V**oice **o**ver **IP**“.
D. h. Sprachübermittlung mittels IP-Technologie.

VoIP Security

Abkürzung für „**V**oice **o**ver **IP S**ecurity“.
Meint Maßnahmen zur sicheren Sprachübermittlung bei VoIP.

VPN

Abkürzung für „**V**irtual **P**rivate **N**etwork“.
Ein VPN verbindet zwei Netzwerke, einen Computer mit einem Netzwerk oder zwei Computer über öffentliche Verbindungen (z. B. Internet).
Damit die Datenübertragung nicht von außen eingesehen werden kann gibt es ein sogenanntes Tunneling-Protokoll, das die Daten, die ausgetauscht werden, ver- bzw. entschlüsselt.
Hintergrund für solch eine Technologie: Um Kosten zu sparen können so Außenarbeiter über öffentliche Leitungen wesentlich billiger Daten zur Zentrale schicken, als das ein eigenes Netz errichtet werden müßte.

WAP

Abkürzung für „**W**ireless **A**pplication **P**rotocol“.
Synonym für grafische Anwendungen auf Mobiltelefonen, Organizern und anderen geeigneten Endgeräten, übertragen nach dem gleichnamigen Protokoll.

WBM

Abkürzung für „**W**eb **B**ased **M**anagement“.
Web-basierte Schnittstelle für Workpoints (IP Phones) zum Administrieren von Konfigurationen und Ändern von Benutzereinstellungen per Fernzugriff.

WEP

Abkürzung für „**W**ired **E**quivalent **P**rivacy“.
Standard-Verschlüsselung für WLANs. Dabei wird von allen Teilnehmern im WLAN und dem Access Point/WLAN Router derselbe Schlüssel zum Ver- und Entschlüsseln der Daten verwendet. WEP unterscheidet zwischen 64- und 128-Bit-Verschlüsselung.

Siehe auch WPA, WPA-PSK.

WLAN

Abkürzung für „**W**ireless **L**ocal **A**rea **N**etwork“.

Workpoint

Mit Workpoints sind sowohl IP-Telefone wie z. B. optiPoint 410 standard als auch Softclients wie der optiClient 130 gemeint.

WPA

Abkürzung für „**W**I-FI **P**rotected **A**ccess“.
WPA bietet Sicherheit durch Verschlüsselung mit dynamischen Schlüsseln in WLANs. Der Austausch der dynamischen Schlüssel erfolgt mit Hilfe des Authentifikation-Protokolls EAP (Extensible Authentication Protocol) beim Aufbau einer Verbindung/Session.

Siehe auch WEP, WPA-PSK.

WPA-PSK

Abkürzung für „**W**I-FI **P**rotected **A**ccess mit **P**re-**S**hared **K**ey“.
Verschlüsselungsverfahren zum Einsatz in WLANs. Das Verfahren verwendet teilnehmerspezifische Schlüssel, die aus einem Pre-Shared Key und der MAC-Adresse des jeweiligen Geräts erzeugt und automatisch in periodischen Abständen (Rekeying-Intervall) geändert werden.

Siehe auch WEP, WPA.

WSP

Abkürzung für „**W**ireless **S**ession **P**rotocol“.
Protokoll zur Übertragung von Daten auf WAP-fähige Endgeräte.

Index

802.1x
Einstellungen 233

A

Abschnitt 6.6.7 Register „Einstellungen“ 55
Administration von Zertifikaten 45
Adressbücher 371
Aktionsschaltflächen 21, 7, 212
Aktivitäten- und Fehlerprotokoll 143, 145, 146
Alarm Konfiguration 156, 169
Alarm Protokoll 152, 154
Alarmklassen 159
Allgemeine Features 34
ANAT Einstellungen 36
Anmelden/Abmelden Mobile User 62
Anrufumleitung 77, 399, 44
Ansichtenleiste 11
Anwendereinstellungen 173, 78
Anwendungsoberfläche 3
Anzeigebereich 22
API Notifizierungen 118
APM Inventar 18
Applikationsliste 166, 74
Archivierung 216
Archivierung automatisch 213
Archivierungsdaten 536, 141
Audio
Einstellungen 144
Schemen 364
Audio Einstellungen 62
Audiogeräte verfügbar 366
Audit- und Security Log Dateien 147, 149, 150
Aufruf der Hilfe 3
Ausbaugrenzen des DLS 12
Ausstellende Zertifizierungsstellen 35
Aussteller Administration 204
Austausch eines alten Workpoints 33
Austausch HFA- durch SIP-Software 34
Austausch SIP- durch HFA-Software 35
Auswahl der Ansichten 11
Auswahllistenfeld 12
Autokonfig. IP Client 534
Autokonfig. IP Gateway 535
Autokonfig. IP Phone 533
Autokonfiguration 10
Automatische Archivierung 220

B

Backup 175
Backup / Restore 171
Backup der DLS-Datenbank 25, 27
Basis Daten 8
Basis E.164 15
Baum-Menü 4
Benutzer-Einstellungen
Anrufbezogen 58, 28
Business Groups 72

C

CA Administration 199
CA Zertifikate 163, 170
IPSec / VPN 449
Canonical Dial Lookup 132
Certificate Policy 117
Checkbox 12
Cluster Einstellungen 141
Cluster Konfiguration 136
Codecs/Komprimierung 138
Copy-Makro für P&P 61
CRL Dateien 452
CRL Distribution Points 443
CSTA Service Provider 303
CTI HFA Provider 294
CTI Konfiguration 293

D

Datei Einstellungen 255
Dateien
im DLS registrieren 5
Unterschied zu Software 1
Datei-Typen 7
DCMP 193, 531
Debug WLAN 223
Deployment Daten 13
Deployment Server 137
Deployment Service 122
DHCP 1
Diagnose 246
Diagnose- und Security 259
Diagnose-Dateien upload 222
Directory Service 379
Display/Geräte 276
Display/Geräte Einstellungen 127
DLS API 5, 134

DLS auf dem TAP 41
DLS Client GUI 131
DLS Server mehrere 251
DlsAPI 43
DLS-Client
  beenden 2
  starten 1
  starten am Server/Client 130
DLS-Datenbank
  Backup 25, 27
  Manipulieren 42
  Migration 28
  Reset 28
  Restore 26, 27
DLS-Device Verbindung 196
DLS-GUI 5
DLS-Server deinstallieren 162
DNS Server 17
DNS-Server 37
DSS 397

E

E.164-Patterns 71
Einsatzgebiet des DLS 4
Einschränkungen 79
Einschränkungen des DLS 12
Einstellungen
  802.1x 233
  Alarm Konfiguration 169
  ANAT 36
  Archivierung 216
  Audio 144
  Codecs 138
  Diagnose 246
  Display/Geräte 276
  HFA 231, 315
  IPSec/VPN 445
  Remote Trace 258
  Report 92
  Secure Trace 265
  SIP 228
  Sommerzeit 135
  SPE 435
  SPE Konfiguration 206
  SRSR 125, 346
  Trace Konfiguration 232
  Video 368
  Zeit 134
Einwahlort 409
Element Manager 2
  Protokoll 25
Elemente 12
EM Synchronisation 519
Export von Plug&Play-Daten 40

F

Feature
  Einstellungen 1 47, 19
  Einstellungen 2 50, 22
Features
  Server basiert 71
Feldbeschreibung im Wizard
  FTP Server Konfiguration 82
  Protokoll Konfiguration 78
Fenster für Meldungen 21
File Deployment 286, 9
File Server 180
Filter-Test 237, 238, 240
Format-Aktualisierung der DLS-Datenbank (Migration) 28
Freigeschaltete Services 52
FTP Server 282
FTP Server Konfiguration 83
FTP-Konfiguration 10

G

Gateway 310, 323
  Konfiguration 2
  QoS Data Collection 9
  Report Einstellungen 15
  Schwellwerte 17
  Server Daten 13
  Standby 15
  Verbindung 7
Gateway (HFA) / SIP Server 12
Gateway (HFA)/SIP Server 8
Gateway / Server 8
Gateway/Server 7
Gateways 34
Geräteattribute ändern 47
Geräteprofil 2

H

Hauptmenü 4
Herstellerspezifisches Informationselement 138
HFA
  Client erzeugen 44
  Codec Einstellungen 358
  Einstellungen 231, 315
  Einstellungen SPE 407
  Mobility 191
  Mobility an HiPath 3000 71
  Phone erzeugen 44
  Tastenbelegung 390

Wahlparameter 348
Hilfe 3
Hilfe-Funktion 3
HiPath 3000/5000 21
HiPath 4000 Assistant 18
HiPath DXWeb Pro 24
HiPath SQL DB 383
HTTP-Proxy 196
HTTPS Server CA Zertifikate 98, 110
HTTPS Server Konfiguration 92
HTTPS-Konfiguration 10

I

IEEE
802.11b (Transfer Mode) 213
802.1x (Phone- und RADIUS-Zertifikate) 232
802.1x (Zertifikat entfernen) 56
802.1x (Zertifikat importieren) 48
IEEE 802.1x 48
Images auf dem Server 96
Import von Plug&Play-Daten 40
Importieren WBM Server Zertifikat 46
INCA Inventar 14
Info
Deployment Server 140
Interne CA 52
IP Device Daten lesen 459
IP Device Response Test 469
IP Device Zertifikate sperren 466
IP Device zurücksetzen 462
XML Applikationen 6
Infrastruktur Policies 73
Infrastruktur Policy 114
Infrastruktur Policy Tabelle 117
Installation
DHCP-Server 136
DNS-Server (Konfiguration) 148
FTP-Server 132
Instant Messaging (XMP) 417
Interaktion 132
Interne CA 49
Internet Hilfe URL 281, 130
Internetseiten 381
Inventar Daten 496
Inventardaten
Management 11
Pings 503
Register 496
IP Bereiche 69
IP Devices scannen 483
IP Client Konfiguration 289
IP Clients 476, 30
IP Device
Interaktion 453
IP Device Konfiguration 516, 31
DCMP 531
DLS Verbindung 523
Profil 521
IP Devices 12
archivieren 218
Pingen 476
Scannen 13
IP Devices pingen 474
IP Devices scannen
Konfiguration 485
Scan Ergebnisse 487
IP Gateway erzeugen 45
IP Gateways 477, 32
IP Phone Konfiguration 2
IP Phones 27
IP Routing 27, 16
IP Switch Daten 507
IP-Adresse und/oder Portnummer ändern 40
IPSec/VPN
Einstellungen 445
IPv6 Einstellungen
Einstellungen
IPv6 34

J

Java 156, 68
Java Midlet Inventar 15
Job
eintragen in der Werkzeugleiste 7
Konfiguration (Oberfläche) 23
Kontrolle (Oberfläche) 2
Nutzen der Job-Koordination 22
Job Konfiguration 23
Job Kontrolle 2

K

Kalender-Schaltfläche 12
Keyset ändern (ModifyKeyset) 46
Keysets 193, 194
Ziele 199
Kommando Datei 164
Konfiguration
Aktivitäten- und Fehlerprotokoll 145
Audit- und Security Log Dateien 149
Daten 16
Konfigurationsmenüs gesperrt 175, 80
Konfigurationsvorlagen 8
Kontextsensitive Hilfe 3
Kopfzeile 7

L

Land 269
Land & Sprache 118
LDAP 372, 75
    Einstellungen 168
    Inventar 12
Leistungsmerkmale 10
Leitungstasten 395
Liste der verwendeten Ports 12
Lizensierung 6
Lizenzen 329
Lizenzinformationen 7
Lizenzstatus 244
Location Server 220
Location Service 123
Login Policy 19
Login-Fenster 1
LOGO Datei Inventar 16
Logoff automatisch 148
Logon/Logoff 145
Lokale Funktionen gesperrt 185, 90

M

MakeCall 125
Makrokommando Syntax 61
Mandanten 57, 8, 22
    Account Konfiguration 10
    FTP Server Konfiguration 90
    HTTPS Server Konfiguration 103
    Netzlaufwerk Konfiguration 113
    Profil Management 8, 14, 22
    Standort 77
Mandantenfähigkeit verwenden 75
Meldungsfenster 21
Meldungs-Filter 236
Menü
    Treeview 4
Menüzeile 8
Messaging Services 273, 124
Migration
    DLS-Datenbank 28
Migrationsszenarien 1
Mobile
    User 1
Mobile User 78
    Anmelden/abmelden 62
    Anrufumleitung 44
    Anwendereinstellungen 78
    Applikationsliste 74
    Archivieren 219
    Archivierungsdaten 141
    Audio Einstellungen 62
Benutzer-Einstellungen
    Anrufbezogen 28
Display/Geräte Einstellungen 127
DNS Server 17
Einschränkungen 79
Feature-Einstellungen 1 19
Feature-Einstellungen 2 22
Freigeschaltete Services 52
Gateway (HFA)/SIP Server 8
Gateway/Server 7
Interaktion 132
Internet Hilfe URL 130
IP Routing 16
Java 68
Konfigurationsmenüs gesperrt 80
Land & Sprache 118
LDAP 75
Logoff automatisch 148
Logon/Logoff 145
Lokale Funktionen gesperrt 90
Messaging Services 124
Mobile/Basis User 138
Mobility Data 94
Mobility Logon/Logoff 92
Passwörter 50
Protokoll 146, 156
QoS Parameter 48
Quality of Service 47
Response Test Einstellungen 142, 153
Security Einstellungen 49
Send URL Server CA Zertifikat 113
Server basierte Features 38
Signalisierungsmelodie 42
SIP Einstellungen 115
SIP Fehleranzeige 126
SIP Mobility 165
SIP Registrierung 1 11
SIP Registrierung 2 13
SIP Terminaleinstellungen 9
Sofortverbindung 22
Statistik 159, 168
Tastenbelegung 95
Telefonie 54
Telefonsperre 131
Uhrzeit 60
User Tastenbelegung 149
Verfügbarkeit 32
verzögerte Sofortverbindung 22
Wahlparameter 55, 56
Wählplan 39
WAP 67
XML Applikationen 69

Zeitparameter 60
Ziele 101
Ziffernumwandlung 59
Mobile User Daten importieren 68
Mobile User Profil erstellen 59
Mobile User-Daten speichern 65
Mobile/Basis User 138
Mobility 187, 191
Begriffserklärungen 14
einrichten (Überblick) 16
Funktion einrichten 58
Profil-Konzept 17
Rufnummer 16
Übersicht 14
Mobility Data 94
Mobility einrichten und administrieren 58
Mobility Logon/Logoff 92
Mobility-Funktion 15

N

NETBOOT Inventar 19
Netzlaufwerk Konfiguration 108
News Service 124

O

Oberfläche des DLS 3
OCSR 1 Server CA Zertifikat 113
OCSR 1 Signature CA Zertifikat 115
OCSR 2 Signature CA Zertifikat 116
OpenOffice EE 23
OpenScape Daten ändern 48
OpenScape Office MX/LX 22
OpenScape Voice 9, 32
optiClient in Callcentern 39
Optionen 126
Optionsfeld 12

P

P&P Import Protokolle 151
P&P Rufnummernband 74
Papierkorb 505
Parameter ändern (erste Schritte) 2
Passwort Policy 14
Passwort Regeln zusätzliche 99
Passwortänderung 18
Passwörter 97, 50
Ändern 9
Peer Credentials 446
Periodischer Datei-Upload 262
Phone Zertifikat 236
Ping 471
Plattform 6
Plug&Play
Funktionsübersicht 11
Workpoints registrieren 11
Plug-In Properties 37
Policy Einstellungen 12
Port-Liste 12
Ports 40, 333
Standby 43
Profil Management 8, 22
Mandanten 14
Templates 6, 13
übergeordnete Profile 9
Programmschnittstelle DlsAPI 43
Protokoll 146, 156
Aktivitäten- und Fehlerprotokoll 146
Audit- und Security Log Dateien 150
Automatische Archivierung 220
Backup / Restore 178
Backup/Restore 178
Upload Diagnose, Security Log Dateien 225
Protokoll-Daten 142
Proxy 322

Q

QoS Data Collection 9
QoS Parameter 81, 48
Standby 87
Quality of Service 337, 47

R

RADIUS Server CA Zertifikat 239
RADIUS Zertifikat 48
Rechte
Account Konfiguration 9
Rollen und Rechte 26
Reg-Adressen 70
Regeln bearbeiten 20
Regeln bearbeiten (Deployment) 20
Register
Darstellung 12
Inventardaten 496
Registerkarte
Standard Profil 80, 81
Registrar 320
Registrieren
durch Scannen von Workpoints 478
Software, automatisch 6
Workpoints durch Lesen von Daten 454
Remote Trace 258
Renewal 54
Report
Einstellungen 426, 15

Report Einstellungen 92
Request Parameter 42
Reset
DLS-Datenbank 28
Workpoints 460, 464, 467
Response Test Einstellungen 142, 153
Restore 176
DLS-Datenbank 26, 27
Rollen 8
Rollen und Rechte 22
Routing 27
Rufliste 283

S

Scannen von IP Devices 13
Schaltflächen 21
Schwellwerte 94, 427, 17
Secure Modus 185
Secure Shell (SSH) Zugang 257
Secure Trace 265
Security Einstellungen 430, 49
Security Log Dateien upload 222
Security Status Protokoll 527
Security Verschlüsselung 217
Send URL Server CA Zertifikat 211, 113
Server basierte Features 38
Server Daten 91, 425, 13
Server Konfiguration 56
Server Lizenzen 241
Serverzuweisungen 78
Services (NW Stack) freigeschaltet 104
Services freigeschaltet 52
Service-Schnittstelle 43
Session Policy 21
Sicherheitsmodus 6
Sichern der DLS-Datenbank 25, 27
Signaling and Payload Encryption (SPE) 224, 402, 435
Signalisierung 161
Signalisierungsmelodie 75, 42
SIP 323
Anrufumleitung 399
Codec Einstellungen 360
Einstellungen 228, 115
Einstellungen SPE 405
Fehleranzeige 275, 126
Keypad 400
Keysets 393
Leistungsmerkmale 385
Leitungstasten 395
Mobile User Konfiguration 2
Mobility 187, 165
Ports 335
Proxy 322
Registrar 320
Registrierung 1 20, 11
Registrierung 2 22, 13
Stationen (DSS) 397
Survivability 26, 327
Terminaleinstellungen 18, 9
User Tastenbelegung 149
Verbindung 317
Wahlparameter 354
SIP Client erzeugen 44
SIP Phone erzeugen 43
SIP-Telefone an HiPath 3000/4000
(Feature-Verfügbarkeit) 50, 63
SNMP 162
Einstellungen 151
Sofortverbindung 22
Software
Deployment, verschiedene Abläufe 16
im DLS registrieren 5
Images 11
Lizenzinformationen 7
Unterschied zu Dateien 1
Software Deployment 7
Software Inventar 11
Sommerzeit 135
SPE CA Zertifikate 225, 402, 440, 50
SPE Konfiguration 197, 206
SPE Zertifikat 437
Sprache 269
SQL DB 383
SRSR
Einstellungen 125, 346
SSH 257
Standard Profil 80, 81
Standort 63
Standorte 62
Standort-Konfiguration 9
Statistik 159, 168
Statusinformation 22
Suchfunktionalität 25
Survivability 327
SW Deployment 314
Einschränkungen 75
System-/Rufton Inventar 17
Systemdienste 325
Systemfunktionen 384
Systemvoraussetzungen 2

T

Tastenbelegung 193, 95
Tastenbelegung ändern (ModifyKey) 45

Telefonie 123, 343, 54
Telefonsperre 284, 131
Templates 6, 13, 8
Textfeld 12
TLS Connector Konfiguration 129
Trace Konfiguration 226, 232
Trust Anchor 45, 46
Truststore DLS API 135
Truststore DLS Client GUI 133

U

Übergeordnete Profile 9
Uhrzeit 60
Uhrzeit Einstellungen 133
Unterstützte Geräte 7
Update 314
Upload Diagnose, Security Log Dateien 225
User Data Profile 10
User Tastenbelegung 149

V

Vendor Specific Information Element 138
Verbindung
    OpenScape 416
Verfügbarkeit 63, 32
Verwendung des DLS 1
Verzeichnisse 371
Verzögerte Sofortverbindung 22
Video Einstellungen 368
Videogeräte verfügbar 370
Voraussetzungen
    personelle 3
    technische 1
Vorteile des DLS 10
VPN Einstellungen 331

W

Wahlparameter 128, 55, 56
    Ziffernumwandlung 132
Wählplan 72, 39
WAP 155, 67
Wartemusik Inventar 13
WBM Server Zertifikat 107
WBM Server Zertifikat importieren 46
WBM Server Zertifikate 431
Web Service-Schnittstelle 43
WEB Zugriff 418
Wiederherstellen der DLS-Datenbank 26, 27
Wiederholungs-Filter 234
WLAN
    Debug 223
    Einstellungen 213
    Location Server 220
    Security Verschlüsselung 217
Workpoint Interface Konfiguration 183
Workpoint-Firmware installieren 11
Workpoint-Parameter ändern (erste Schritte) 2
Workpoints pingen 471

X

XML Applikationen 120, 158, 69, 1, 73
    Info 6
    IP Devices 12
XML Applikationen Daten 18

Z

Zeit 134
Zeitparameter 60
Zertifikat Alarm Einstellungen 153
Zertifikat Renewal 44
Zertifikate 17
    Administration von Zertifikaten 45
    CA 163, 170
    Phone Zertifikat 236
    RADIUS Server CA Zertifikat 239, 242
    WBM Server Zertifikat 107, 120, 121
Zertifikatsverteilung automatisch 208
Zertifikatsverteilung Einschränkungen 76
Ziele 199, 101
Ziffernumwandlung 132, 59
Zurücksetzen der DLS-Datenbank 28