A MITEL
PRODUCT
GUIDE

Unify OpenScape Deployment Service

Deployment Service

Deployment Service V10

Administration & Installation Manual
03/2026

A31003-S23A0-M101-24-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

History of Changes **13**

1 Introduction **17**
1.1 Target Group 17
1.2 Conventions Used 17
1.3 Constraint Notes 18
1.4 DLS and file naming schemes 18

2 Getting Started **21**
2.1 DLS Installation 22
2.1.1 System Requirements 22
2.1.2 System Capacities 25
2.1.3 Licensing. 28
2.1.4 Installing DLS Software 30
2.2 Starting the DLS for the First Time (Single Mode) 30
2.3 Required Workpoint Firmware Installation 33
2.3.1 Creating Software Images Automatically 33
2.3.2 Auto Deployment 34
2.3.3 Manual Deployment 34
2.4 Frequently Used Functions 35
2.4.1 Scan IP Devices 35
2.4.2 Configuring Parameters: Example Key Layout 35
2.4.3 Jobs 37
2.5 Using the Mobility Function 37
2.6 Security 39
2.6.1 Certificates 39
2.7 Recommendation for Antivirus 39

3 Concept and Features **41**
3.1 Overview 41
3.2 Deployment Service Components 42
3.3 Operating Fundamentals 43
3.4 Area of Application 44
3.5 Overview of Software and File Types 47
3.6 The Most Important Features 51
3.6.1 Capacity Limits and Restrictions 53
3.6.2 Ports Used 53
3.7 Deployment Service supported deployments 54
3.8 DLS Mobility - General Information 55
3.8.1 Mobility Definitions 55
3.8.2 Using Mobility 55
3.8.3 Mobility ID 57
3.8.4 Configuring Mobility 57
3.8.5 Profile Concept in DLS 58
3.8.6 Mobile user data size 60
3.9 DLS System Monitoring 61
3.9.1 System Monitoring Tools-DLS RapidStat 61
3.10 DLS Toolkit 67

4 Installation and Initial Configuration 69
4.1 Requirements 69
4.1.1 General Server Requirements 69
4.1.2 General Client PC Requirements. 70
4.1.3 Personnel Requirements 71
4.1.4 DLS Availability 71
4.1.5 Infrastructure For Cluster Operation 72
4.2 Install MS SQL Server for Multi-Node DLS 73
4.2.1 How to install Microsoft SQL Server 73
4.2.2 Upgrading SQL Server. 73
4.2.3 SQL Native Client - When Multi-Node DLS is installed 73
4.2.4 Change Service Password. 74
4.3 Configure the Network Load Balancer 74
4.4 Set Up DCMP 75
4.4.1 Install DCMP 75
4.4.2 Configure DCMP 78
4.4.3 Configure DLS for DCMP. 80
4.4.4 Configure Phone for DCMP 81
4.4.5 Test DCMP 83
4.5 Installing the DLS 85
4.5.1 Single Node Operation with Local Database 85
4.5.2 Multi-Node Operation with Remote or Custom Specific Database 90
4.5.3 Multi-Node Operation. 91
4.6 SQL Database Mirroring Setup 109
4.7 DLS Database Restore in a Multi-Node environment 109
4.8 Upgrading a DLS Multi-Node Environment 109
4.9 Start DLS. 110
4.10 Initial Configuration 111
4.11 Starting the DLS Client 113
4.11.1 Starting the Client 113
4.11.2 Starting the Client with OpenWebStart and Adoptium OpenJDK 114
4.12 Installing Network Components 124
4.12.1 FTP Server 125
4.12.2 HTTPS Server 127
4.12.3 General Information on DHCP 128
4.12.4 DHCP Server in a Windows Environment 129
4.12.5 DHCP Server in a Linux/Unix Environment 130
4.12.6 Configuring the DNS Server for DLS 132
4.12.7 DHCP Server with Infoblox Appliance 133
4.13 Uninstalling the Deployment Service 143
4.13.1 Uninstalling the DLS 143
4.13.2 Uninstalling the SQL Server. 143

5 The DLS User Interface 145
5.1 Starting and Logging On 145
5.2 Ending 146
5.3 Opening the Context-Sensitive Help Function 147
5.4 Application Interface 147
5.4.1 Main Menu 148
5.4.2 Work Area 150
5.4.3 Status Area 167
5.5 Search Functionality 170

6 Administration 171
6.1 Account Management 172
6.1.1 Account Configuration 174
6.1.2 Policy Settings 182
6.1.3 Roles and Rights 193
6.2 PKI 201
6.2.1 Plug-In Configuration 202
6.2.2 Connector Configuration 209
6.2.3 Internal CA 221
6.2.4 Renewal 226
6.3 Server Configuration 228
6.3.1 Tenants 229
6.3.2 Location 235
6.3.3 P&P Settings 250
6.3.4 FTP Server Configuration 255
6.3.5 HTTPS Server Configuration 264
6.3.6 HTTPS Client Configuration 277
6.3.7 Network Drive Configuration 281
6.3.8 Infrastructure Policy 287
6.3.9 API Notifications 291
6.3.10 XML Applications 293
6.3.11 Options 300
6.3.12 TLS Connector Configuration 304
6.4 Cluster Configuration 311
6.4.1 Deployment Server 312
6.4.2 Cluster Settings 316
6.5 Display Logging Data 317
6.5.1 Activity and Error Log 318
6.5.2 Audit and Security Log 322
6.5.3 P&P Import Protocols 328
6.5.4 Alarm Protocol 329
6.5.5 Alarm List 332
6.6 Alarm Configuration 334
6.6.1 "Alarm Classes" Tab 337
6.6.2 "Notification" Tab 340
6.6.3 "SNMP" Tab 341
6.6.4 "Batch File" Tab 344
6.6.5 "Email" Tab 345
6.6.6 „Syslog“ Tab 347
6.6.7 "Settings" Tab 349
6.7 Backup/Restore 351
6.7.1 "Backup" Tab 355
6.7.2 "Restore" Tab 356
6.7.3 "Protocol" Tab 358
6.8 File Server 360
6.9 Workpoint Interface Configuration 363
6.9.1 "Secure mode" Tab 365
6.9.2 "DCMP" Tab 373
6.9.3 "HTTP-Proxy" Tab 376
6.9.4 "Contact Me Notify" Tab 377
6.10 Automatic SPE Configuration 383
6.10.1 "CA Administration" Tab 385

6.10.2 "Issuer Administration" Tab . . . 389
6.10.3 "Settings" Tab . . . 391
6.11 Automatic Certificate Deployment . . . 393
6.12 Automatic Archiving . . . 398
6.12.1 "Settings" Tab . . . 401
6.12.2 "IP Devices to archive" Tab . . . 403
6.12.3 "Mobile Users to archive" Tab . . . 404
6.12.4 "Protocol" Tab . . . 405
6.13 Automatic Upload Diagnosis- and Security Log Files . . . 407
6.13.1 "Protocol" Tab . . . 410
6.14 Trace Configuration . . . 411
6.14.1 "Additional Settings and Actions" Tab . . . 417
6.14.2 "Repeat filter" Tab . . . 419
6.14.3 "Message Filter" Tab . . . 421
6.14.4 "Filter test" Tab . . . 422
6.14.5 "OSVTM Configuration" Tab . . . 423
6.14.6 "Thread Monitoring" Tab . . . 425
6.15 Server Licenses . . . 426
6.15.1 "License state" Tab . . . 429

7 IP Devices . . . 437
7.1 IP Phone Configuration . . . 438
7.1.1 Gateway/Server . . . 444
7.1.2 IP Routing . . . 465
7.1.3 Ports . . . 483
7.1.4 Features . . . 490
7.1.5 Quality of Service . . . 536
7.1.6 QoS Data Collection . . . 547
7.1.7 Security Settings . . . 553
7.1.8 Telephony . . . 582
7.1.9 Small Remote Site Redundancy . . . 589
7.1.10 Dialing Properties . . . 592
7.1.11 Time Parameters . . . 599
7.1.12 Audio Settings . . . 604
7.1.13 SNMP Settings . . . 619
7.1.14 Applications . . . 623
7.1.15 Service Integrations . . . 636
7.1.16 User Settings . . . 667
7.1.17 SIP Mobility . . . 681
7.1.18 HFA Mobility . . . 685
7.1.19 Keysets/Keylayout . . . 687
7.1.20 Wi-Fi Settings . . . 708
7.1.21 WLAN Settings . . . 719
7.1.22 Signaling and Payload Encryption (SPE) . . . 731
7.1.23 IEEE 802.1x . . . 745
7.1.24 Diagnosis . . . 758
7.1.25 Miscellaneous . . . 781
7.1.26 File Deployment . . . 805
7.2 IP Client Configuration . . . 809
7.2.1 CTI Configuration . . . 813
7.2.2 General . . . 827
7.2.3 Gateway/Server . . . 836

7.2.4 Ports . . . 862
7.2.5 Quality of Service . . . 866
7.2.6 Telephony . . . 872
7.2.7 Small Remote Site Redundancy . . . 875
7.2.8 Dialing Properties . . . 877
7.2.9 Audio/Video Settings . . . 887
7.2.10 Directories/Address Books . . . 903
7.2.11 Miscellaneous . . . 914
7.2.12 Keysets/Keylayout . . . 923
7.2.13 Signaling and Payload Encryption (SPE) . . . 935
7.2.14 Dialup Site . . . 943
7.2.15 OpenScape . . . 950
7.2.16 HotKeys . . . 955
7.2.17 Outlook . . . 959
7.3 IP Gateway Configuration . . . 960
7.3.1 QoS Data Collection . . . 961
7.3.2 Security Settings . . . 969
7.3.3 Signaling and Payload Encryption (SPE) . . . 974
7.3.4 IPSec/VPN . . . 984
7.4 Mediatrix Gateway Configuration . . . 993
7.4.1 Configuration . . . 994
7.5 IP Device Interaction . . . 1002
7.5.1 Read IP Device Data . . . 1003
7.5.2 Reset IP Devices . . . 1009
7.5.3 IP Device Revoke Certificates . . . 1013
7.5.4 IP Device Response Test . . . 1016
7.5.5 Ping IP Devices . . . 1019
7.5.6 Scan IP Devices . . . 1026
7.6 IP Device Management . . . 1038
7.6.1 Inventory Data . . . 1039
7.6.2 Trash . . . 1052
7.6.3 IP Infrastructure . . . 1054
7.6.4 IP Device Configuration . . . 1057

8 Mobile Users . . . 1089
8.1 SIP Mobile User Configuration . . . 1090
8.1.1 Gateway/Server . . . 1096
8.1.2 IP Routing . . . 1106
8.1.3 Features . . . 1108
8.1.4 Quality of Service . . . 1141
8.1.5 Security Settings . . . 1143
8.1.6 Telephony . . . 1147
8.1.7 Dialing Properties . . . 1149
8.1.8 Time Parameters . . . 1155
8.1.9 Audio Settings . . . 1157
8.1.10 Applications . . . 1161
8.1.11 Service Integrations . . . 1170
8.1.12 User Settings . . . 1183
8.1.13 SIP Mobility . . . 1197
8.1.14 Keysets/Keylayout . . . 1201
8.1.15 Signaling and Payload Encryption (SPE) . . . 1224
8.1.16 Miscellaneous . . . 1229

8.1.17 File Deployment 1248
8.2 SIP Mobile User Interaction 1252
8.2.1 SIP Mobile User 1257
8.2.2 Logon/Logoff 1265
8.2.3 Automatic Logoff 1268
8.2.4 SIP User Keylayout 1270
8.2.5 Mobile User Response Test Settings 1274
8.3 User Data Administration 1278
8.3.1 "Statistics" Tab 1280
8.4 Mobility Statistics 1282
8.4.1 "SIP Mobility" Tab 1286
8.5 Mobility Statistics Configuration 1289

9 Gateways 1291
9.1 Gateway Configuration 1292
9.1.1 "Gateway Connection" Tab 1297
9.2 QoS Data Collection 1299
9.2.1 "Server Data" Tab 1303
9.2.2 "Report Settings" Tab 1305
9.2.3 "Threshold Values" Tab 1307

10 Software Deployment 1309
10.1 Workpoint Deployment 1310
10.1.1 "Software Deployment" Tab 1315
10.1.2 "File Deployment" Tab 1317
10.1.3 "Software Inventory" Tab 1319
10.1.4 "LDAP Inventory" Tab 1320
10.1.5 "MOH Inventory" Tab 1321
10.1.6 "INCA Inventory" Tab 1322
10.1.7 "Java Midlet Inventory" Tab 1323
10.1.8 "Logo File Inventory" Tab 1324
10.1.9 "SYSTEM/RINGTONE Inventory" Tab 1325
10.1.10 "APM Inventory" Tab 1326
10.1.11 "NETBOOT Inventory" Tab 1327
10.2 Manage Rules 1328

11 Element Manager 1333
11.1 Element Manager Configuration 1334
11.1.1 "OpenScape Voice" Tab 1341
11.1.2 "OpenScape Voice Assistant" Tab 1346
11.1.3 "HiPath 4000 Assistant" Tab 1349
11.1.4 "HiPath 3000/5000" Tab 1352
11.1.5 "Protocol" Tab 1353
11.2 Element Manager Security 1355

12 Profile Management 1357
12.1 Device Profile 1358
12.1.1 "Templates" Tab 1362
12.1.2 "Supported Devices of IP Device" Tab 1363
12.1.3 "Tenants" Tab 1364
12.1.4 "Parent Profiles" Tab 1365
12.2 User Data Profile 1366
12.2.1 "Templates" Tab 1369
12.2.2 "Tenants" Tab 1370

12.3 Template Overview . . . 1371
12.3.1 "Template data" Tab . . . 1375
12.3.2 "Profiles" Tab . . . 1376
12.3.3 "Tenants" Tab . . . 1378
13 XML Applications . . . 1379
13.1 MakeCall . . . 1382
13.1.1 "Info" Tab . . . 1384
13.2 NewsService . . . 1385
13.2.1 "Info" Tab . . . 1386
13.3 NewsService Archive . . . 1387
13.3.1 "Info" Tab . . . 1389
13.3.2 "IP Devices" Tab . . . 1390
14 Job Coordination . . . 1391
14.1 Job Control . . . 1392
14.1.1 "Basic Data" Tab . . . 1399
14.1.2 "Deployment Data" Tab . . . 1403
14.1.3 "Configuration Data" Tab . . . 1406
14.1.4 "XML Application Data" Tab . . . 1408
14.2 Daily Status . . . 1409
14.2.1 "Status Information" Tab . . . 1412
14.3 Job Configuration . . . 1413
14.3.1 "IP Phones" Tab . . . 1417
14.3.2 "IP Clients" Tab . . . 1420
14.3.3 "IP Gateways" Tab . . . 1422
14.3.4 "Gateways" Tab . . . 1424
15 Operating Sequences . . . 1427
15.1 Configure a user account that never expires . . . 1428
15.2 Bulk deletion of default device files . . . 1431
15.3 First Steps: Changing IP Device Parameters . . . 1432
15.4 Changing the Element Manager Configuration and Creating Jobs . . . 1434
15.5 How to replace OSV Assistant Manager with OSV Element Manager . . . 1435
15.6 Registering Workpoint Software and Files . . . 1440
15.6.1 Automatic Registration . . . 1441
15.6.2 Understanding License Information for IP Phone Software . . . 1442
15.7 Editing Templates . . . 1443
15.7.1 Creating a Template Manually . . . 1443
15.7.2 Creating a Template From an Existing Configuration . . . 1444
15.7.3 Loading the Template . . . 1445
15.7.4 Additional Functions . . . 1445
15.8 Workpoint Autoconfiguration (Plug&Play) . . . 1446
15.8.1 Requirements . . . 1446
15.8.2 Setting Up Plug&Play Registration . . . 1447
15.8.3 Registration . . . 1449
15.9 Distribution of Workpoint Software . . . 1451
15.9.1 Manual Deployment . . . 1452
15.9.2 Automatic Deployment . . . 1455
15.10 Using Job Coordination . . . 1457
15.10.1 Defining a Job . . . 1457
15.10.2 Viewing Job Properties and Status . . . 1458
15.11 Backup/Restore . . . 1459

15.11.1 Automatic Data Backups . . . 1459
15.11.2 Manual Database Manipulation . . . 1461
15.11.3 DLS Restore Point . . . 1466
15.12 Backup & Restore On OpenScape Voice Integrated and Linux Standalone Installations . . . 1467
15.12.1 Backup . . . 1467
15.12.2 Restore . . . 1470
15.12.3 Post-Restore Procedures . . . 1473
15.13 Automatic Restore on Upgrade Failure . . . 1474
15.14 Importing and Exporting Plug&Play Data . . . 1475
15.14.1 Exporting Plug&Play Data . . . 1475
15.14.2 Importing Plug&Play Data . . . 1475
15.14.3 Plug&Play Data over OpenScape Desktop Clients . . . 1475
15.14.4 Syntax of the .csv Files . . . 1478
15.15 Copy Macro for P&P and Templates . . . 1495
15.15.1 Macro Command Syntax . . . 1495
15.15.2 Available <item name>s . . . 1496
15.15.3 Available Destination fields . . . 1496

16 Administration Scenarios . . . 1499
16.1 Overload Protection with HiPath 4000 . . . 1500
16.2 Workpoint Reinstallation with HiPath 4000 . . . 1502
16.3 Workpoint Reinstallation with HiPath 3000 . . . 1503
16.4 Configuring a Gateway in DLS . . . 1504
16.4.1 Adding Gateways . . . 1504
16.4.2 Release Information (QDC and VoIP Security) . . . 1505
16.5 Configuring Certificates in DLS . . . 1506
16.5.1 Creating a New PKI . . . 1508
16.5.2 Deploying the Signaling and Payload Encryption (SPE) Certificate . . . 1512
16.5.3 Deploying new Web Based Management (WBM) certificates to phones . . . 1513
16.5.4 Phone Secure Mode Operation . . . 1514
16.5.5 Replacing the DLS Web Interface & API Certificates . . . 1516
16.5.6 Internal CA Configuration for AutoSPE . . . 1517
16.6 Replacing an IP Device . . . 1536
16.7 Copy a Registered Device to a Virtual Device . . . 1538
16.8 Replacing an Old Workpoint (TDM) with a New One (IP) . . . 1539
16.9 Replacing HFA with SIP Software and Vice Versa with Identical Device IDs . . . 1540
16.9.1 Replacing HFA with SIP Software . . . 1540
16.9.2 Replacing SIP with HFA Software . . . 1541
16.10 Configuring an IP Client in DLS . . . 1542
16.10.1 Configuring an IP Client 130 in the DLS . . . 1542
16.10.2 Configuring an ODC Client in DLS . . . 1545
16.11 Changing the IP Address and/or Port Number of the DLS . . . 1547
16.12 Using an EWS with DLS in a Customer Network Without Permanent DLS . . . 1548
16.12.1 Installation and Initial Configuration of DLS on the EWS . . . 1548
16.12.2 Manipulating the DLS Database for Using the TAP at Different Customer Facilities . . . 1549
16.13 Operating the DLS via the Program Interface (DlsAPI) . . . 1550
16.13.1 DLS API Web Service Interface . . . 1550
16.14 Security: Administering Certificates . . . 1552
16.14.1 Importing WBM Server Certificates . . . 1553
16.14.2 Importing Phone and RADIUS Certificates . . . 1554
16.14.3 Importing SPE CA Certificates for IP Phones . . . 1556
16.14.4 Importing SPE CA Certificates for IP Clients . . . 1558

16.14.5 Importing SPE Certificates and SPE CA Certificates for IP Gateways . . . 1559
16.14.6 Remove Certificate (IEEE 802.1x Phone as an example) . . . 1561
16.14.7 Replace IP Phone . . . 1562
16.15 How to remove browser's Certificate Error message when logging in to DLS . . . 1563
16.16 Configuring and Administrating Mobility . . . 1565
16.16.1 Configuring the Mobility Function on the Device . . . 1565
16.16.2 Programming the "Mobility" Button . . . 1565
16.16.3 Creating a Mobile User Profile . . . 1566
16.16.4 Creating Mobile Users . . . 1566
16.16.5 Create a Home Phone . . . 1568
16.16.6 Logging On Mobile Users (Forced Logon) . . . 1569
16.16.7 Logging Off Mobile Users (Forced Logoff) . . . 1569
16.16.8 Troubleshooting for Mobile User Logon/Logoff . . . 1569
16.16.9 Default Setting for the Key Layout in Mobility Telephones . . . 1570
16.16.10 Data Backup to a .zip Archive . . . 1572
16.16.11 Import Mobile User Data . . . 1577
16.16.12 Mobility between optiPoint and OpenStage . . . 1579
16.16.13 IP Client Mobility . . . 1580
16.17 HFA Mobility with HiPath 3000 . . . 1581
16.17.1 HiPath 3000 Configuration Prerequisites . . . 1581
16.17.2 DLS Configuration for Network-wide HFA Mobility . . . 1581
16.17.3 Operating procedure . . . 1581
16.18 Data Structures for DLS-hosted XML applications . . . 1583
16.18.1 Directory Structure . . . 1583
16.18.2 Directories at Upgrade Installations . . . 1583
16.18.3 Directories at Backup/Restore . . . 1584
16.19 Deactivation of XML Push feature on Linux DLS . . . 1585
16.20 Migration Scenarios . . . 1586
16.20.1 Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/V7R3 to Windows DLS Single-Node V10 . . . 1586
16.20.2 Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/V7R3 to Windows DLS Multi-Node V10 1587
16.20.3 Windows DLS Single-Node V6R1/V7R1/V7R2/V7R3 to Windows DLS Multi- Node V10 . . . 1588
16.20.4 DLS Multi-Node Systems with Database Mirroring Operating System Upgrade/Migration Procedure. 1591
16.21 Syslog Configuration for Event (and security) logging . . . 1596
16.22 Automatic certificate renewal . . . 1597
16.22.1 How to set up an automatic certification renewal . . . 1597
16.22.2 Scenarios . . . 1601

17 Appendix . . . 1609
17.1 Abbreviations and Technical Terms . . . 1609

History of Changes

Date	Version	Major Modifications
5 December 2019	**DLS V10 CV602**	• A new **Server TLS interfaces** item is introduced (Section 7.1.7.3, ""Enabled Services (NW Stack)" Tab") • A new **Recording Mode** item is introduced (Section 7.1.4.2, ""Feature Settings 2" Tab") • A new **Recording Mode** item is introduced (Section 8.1.3.2, ""Feature Settings 2" Tab")
16 January 2020	**DLS V10 CV604**	• A new button is added under Section 6.5.5, "Alarm List" • Minor documentation enhancements under Section 7.2.9.2, ""SIP Codec Settings" Tab" • New items have been added(Section 7.2.16.1, "’’System-wide keyboard tokens(Hotkeys)’’Tab") • New items have been added(Section 7.2.2.2, "" " Tab")
27 February 2020	**DLS V10 CV605**	• New items have been added (Section 7.1.4.9, ""Direct Video" Tab") • New items have been added (Section 7.1.4.10, ""Door Opener" Tab") • A new checkbox is added under Section 7.2.15.1, ""UC Settings" Tab" • A new field is added under Section 7.2.10.1, ""LDAP" Tab"
11 March 2020	**DLS V10 CV606**	• New items have been added ("SendURL for HFA" Tab) • A new checkbox is added under Section Section 7.1.19.1, ""Keysets" Tab"
26 March 2020	**DLS V10 CV607**	• New items have been added (Section 7.1.25.2, ""Messaging Services" Tab") • A new checkbox is added under Section 7.2.10.1, ""LDAP" Tab" • A new checkbox is added under Section 8.1.5.1, ""Passwords" Tab" • A new checkbox is added under Section 8.1.13.1, ""Mobility Logon/Logoff" Tab"

Date	Version	Major Modifications
7 April 2020	**DLS V10 CV608**	• A new field is added under Section 7.1.19.1, ""Keysets" Tab"
21 April 2020	**DLS V10 CV609**	• Minor documentation enhancements under Section 7.1.19.1, ""Keysets" Tab" • A new checkbox is added under Section 7.1.25.2, ""Messaging Services" Tab" • A new checkbox is added under Section 8.1.16.2, ""Messaging Services" Tab"
20 May 2020	**DLS V10 CV610**	• A new checkbox is added under Section 7.1.2.1, ""IP Routing" Tab" • New items have been added Section 7.1.2.6, ""Wi-Fi Settings" Tab" • New options have been added (Section 7.2.3.9, ""System Services" Tab") • A new checkbox is added under Section 8.1.14.2, ""Destinations" Tab" • A new checkbox is added under Section 7.1.19.2, ""Destinations" Tab" • Minor documentation enhancements under Section 2.1.1, "System Requirements" • Minor documentation enhancements under Section 4.1.1, "General Server Requirements"
15 June 2020	**DLS V10 CV611**	• Minor documentation enhancements under Section 7.1.2.6, ""Wi-Fi Settings" Tab" • A new option has been added under Section 7.1.19.1, ""Keysets" Tab" • A new option has been added under Section 8.1.14.1, ""Keysets" Tab"
	DLS V10 CV612	• Minor documentation enhancements under "SIP Registering 2" Tab • Minor documentation enhancements under Section 7.1.4.2, ""Feature Settings 2" Tab"
11 September 2020	**DLS V10 CV613**	• Minor documentation enhancements under Section 7.1.7.2, ""Additional Password Policy Settings" Tab" • Changes in **Ringer Settings** under Section 7.1.12.3, ""Audio Settings" Tab" • **Lower IL Ringer** setting added under Section 8.1.9.1, ""Audio Settings" Tab"

Date	Version	Major Modifications
25 February 2021	**DLS V10 CV620**	• **Invert display color** setting added under Section 7.1.25.4, ""Display / Phone Settings" Tab" and Section 8.1.16.4, ""Display/Phone Settings" Tab" • **Directed pickup URI** item added under Section 7.1.4.1, ""Feature Settings 1" Tab" and Section 8.1.3.1, ""Feature Settings 1" Tab" • **Permanent Ldap Lookup** item added under Section 7.1.15.1, ""LDAP Settings" Tab" and Section 8.1.11.1, ""LDAP Settings" Tab" • **Manual LDAP search only** item added under Section 7.1.15.1, ""LDAP Settings" Tab" and Section 8.1.11.1, ""LDAP Settings" Tab" • **Allow firstname and lastname for quick search** item added under Section 7.1.15.1, ""LDAP Settings" Tab" and Section 8.1.11.1, ""LDAP Settings" Tab" • **Disable local features** setting added under Section 7.2.11.4, ""SIP Features 2" Tab" • Minor documentation enhancements under Section 4.5.1.2, "Install DLS" • **RTCP-XR Server** item added under Section 7.1.4.1, ""Feature Settings 1" Tab"
2 December 2021	**DLS V10 CV625**	• **MSSQL Server 2017** item added under Chapter 2, "System Requirements" and Chapter 4, "Uninstalling the SQL Server".
15 March 2022	**DLS V10 CV626**	• Added Chapter 2, "Recommendation for Antivirus".
29 August 2022	**DLS V10 CV627**	• Added Section 7.1.7.13, ""SCEP" Tab" under Section 7.1, "IP Phone Configuration".
2 February 2023	**V10 R3.1.0 CV629**	• Added note under Section 6.9.1, ""Secure mode" Tab". 2
1 February 2023	**V10 R3.1.0 CV630**	• Added item DHCP options under Section 7.1.2.1, ""IP Routing" Tab"
31 July 2024	**DLS V10**	• Added item Remote database connectivity under Section 11.1.3 "HiPath 4000 Assistant" Tab
12 December 2024	**DLS V10**	• Removed notes for 2.1.1 System Requirements and added information regarding processor capability.
23 March 2026	**DLS V10**	• Add details for default certificate in chapter 16.

1 Introduction

The document describes the OpenScape Deployment Service V10 (DLS) client in version V10 and contains information about initial DLS server configuration.

This manual is also available as online help on the DLS client's interface, see Section 5.3, "Opening the Context-Sensitive Help Function".

NOTE: For a quick start guide, please read the same-titled Chapter 2.

1.1 Target Group

This manual is intended both for administrators who install and configure the DLS server and for users who carry out configuration and deployment tasks on the DLS client. Users must have prior experience of LAN administration and an in-depth knowledge of IP Device configuration.

For more information on the skills that a DLS administrator must have, see Section 4.1.3, "Personnel Requirements".

1.2 Conventions Used

The following conventions are use for presenting information in this manual:

Convention	Example
`courier`	Input and output Example: enter `LOCAL` as the file name
Italics	Variable Example: *Name* can be up to eight characters long
Bold	Indicates user interface elements Example: Click **OK** Select **Exit** from the **File menu**
Bold	Special emphasis Example: You are **not** permitted to delete this name
Element	User Interface elements with supplementary information
`<Courier>`	Key combinations Example: `<CTRL>+<ALT>+<ESC>`
>	Menu sequence Example: **File** > **End**
NOTE :	Additional information
IMPORTANT :	Warning on critical aspects of a process

Table 1 Typographic conventions

1.3 Constraint Notes

Some of the settings configurable via DLS are available only for particular end devices resp. particular firmware versions. In such cases, an appropriate note is given.

1.4 DLS and file naming schemes

DLS may not be able to handle special characters for filenames under certain circumstances. Furthermore, while some special filenames might be qualified over DLS checks, those files may not be acceptable from the devices side.
Problems may also arise from very long filenames. While the maximum length is Operating System related (and the underlined file system in use, e.g. FAT32, NTFS etc.), an application or device could still have different specifications.

> ***NOTE:*** It is a fact that special characters for filenames must be avoided as a good naming scheme technique. Strange filenames can have many side effects for DLS, especially for deployment of custom data like logos, ringertones etc. and it is advised to be avoided if possible.

Try as much as possible to use the following naming schemes for your files:

- If possible, follow the 8.3 format.
  Where 8 is the max. number of the filename and 3 the max. number for its extension (also called the DOS naming format).
- Use only letters and numbers (abcdefghijklmnopqrstuvwxyz1234567890).
  Non-English letters, like for example German umlauts, are also not allowed in addition to verbal symbols.
- A dash "-" or underscore "_" may be allowed by some applications but characters such as: ( ) { } @ # $ % ^ & ! ' / ~ have special meaning and should not be used.
- Avoid also a dot "." which separates a filename and its extension.
  Use an underscore as a separator where necessary.
- Keep filenames all lowercase, no CAPITAL letters (some applications may allow caps).
  Use lowercase even when it is grammatically incorrect.
- Never use spaces in a filename or its extension. They are extremely troublesome.

2 Getting Started

This brief guide should enable administrators to quickly start the OpenScape Deployment Service V10, perform basic configuration, and connect new telephones, without detailed background knowledge.

NOTE: In order to keep this chapter as short as possible, we have intentionally left the following information out:
- Various application scenarios
Here only one standard scenario is provided as an example.
- Parameter descriptions
Here we will only explain what you need to do, not why.
- Background information
Only the most important information is summarized here.

Detailed information is provided in the rest of the manual, in particular in the chapters:
- Chapter 3: Concept and feature overview
- Chapter 4: Installation of the DLS and additional software components
- Chapter 5: General information about the user interface
- Chapter 6 to Chapter 14: Information on individual parameters
- Chapter 15 and Chapter 16: Practical examples with process descriptions.

The following processes are described here:

- Section 2.1, "DLS Installation"
- Section 2.2, "Starting the DLS for the First Time (Single Mode)"
- Section 2.4, "Frequently Used Functions"
- Section 2.5, "Using the Mobility Function"
- Section 2.6, "Security"
- Section 2.7, "Recommendation for Antivirus"

2.1 DLS Installation

2.1.1 System Requirements

- **Minimum hardware requirements for the DLS client PC**
  - Pentium IV-compatible CPU with 1,4GHz
  - 2048 MB RAM (recommended >= 2048 MB)
  - 10Mbit Ethernet card
  - OpenWebStart for DLS UI access - see chapter 4.11.2 Starting the Client with OpenWebStart and Adoptium OpenJDKi
- **Minimum Hardware Requirements for the Single Node DLS Server**

	DLS Standalone
CPU	3.1 GHz CPU (Intel Xeon E3-1220, 4C/4T), or equivalent newer quad core processor
RAM	8 GB
Ethernet	100 MBit (1GBit is recommended)
Disk Space	80 GB

- **Minimum Hardware Requirements for the DLS Server on a Multi-Node Deployment**

	DLS Multi-Node
CPU	Intel Xeon Quad Processor >= 2.9 GHz, or equivalent newer quad core processor
RAM	8 GB
Ethernet	100 MBit (1GBit is recommended)
Disk Space	300 GB

- **Minimum Hardware Requirements for the DB Server on a Multi-Node Deployment**

	Database Server
CPU	Intel Xeon Quad Processor >= 2.9 GHz, or equivalent newer quad core processor

	Database Server
RAM	8 GB
Ethernet	100 MBit (1GBit is recommended)
Disk Space	80 GB

- **Minimum Hardware Requirements for a Witness Server**

	Witness Server
CPU	Intel Dual Core Processor 3 GHz, or equivalent newer quad core processor
RAM	2 GB
Ethernet	100 MBit (1GBit between the servers)
Disk Space	20 GB

- **Database Requirements**
  - Microsoft® SQL Server™ 2012/2016/2017 Enterprise Edition can be used, but requires 4 GB at minimum. This database must be provided by the customer.
  - DLS supports Microsoft® SQL Server™ 2012/2016 Enterprise Edition

  NOTE: For usage of Microsoft SQL 2012/2016/2017 Enterprise Edition, appropriate Microsoft licences are needed. As a rule CPU licenses should be used, usage of device CAL (Client Access License) is possible as well where one device CAL is needed for each supported device.
  The provision of hardware and Microsoft licenses is not part of the DLS order items and need to be considered separately.

- **Operating Systems for all Deployments**
  - All servers (DLS, Witness, Mirror) must be installed with Windows 2016 / 2019 Standard, Enterprise or Datacenter Edition
  - SUSE Linux Enterprise Edition (Only for the Integrated Simplex Deployment) with the latest service pack & security patches

  DLS Standalone installation over Linux OS is not supported.

NOTE: Make sure that the free disk space requirements are met prior to any upgrade installations.

IMPORTANT: In Multi-Node installations, Network Interface card drivers for the virtual IP address of NLB should support dymanic changes of MAC address, therefore must support **Unicast**.
When you use the Unicast method, all cluster hosts share an identical unicast MAC address. Network Load Balancing overwrites the original MAC address of the cluster adapter with the unicast MAC address that is assigned to all the cluster hosts.
For further information, please refer to Section 4.3, "Configure the Network Load Balancer".

2.1.2 System Capacities

In general the maximum number of devices & mobile users that the OpenScape Deployment Service can manage is :

Scenario	Max.number of :	Maximum	Total Number (devices & mobile users)
Generic scenario for the **OpenScape Deployment Service**	Devices	100,000	200,000
	Mobile Users	100,000	

The following tables show the recommended maximum number of devices that can be controlled by a Single Node DLS :

- If used with Microsoft SQL Server 2008 R2 Express Edition

Scenario	Max.number of :	Maximum
HFA only	HFA Devices	50,000
SIP only	SIP Devices	40,000
DLS Mobility	Mobile Users	20,000
DLS Mobility	Log on /Log off of Mobile Users per hour (30K data)	20,000
DlsAPI	DlsAPI Sessions	100
Element Manager Synchronization	Element Managers	100

- If used with Microsoft SQL Server 2008 R2 Enterprise Edition

Scenario	Max.number of :	Maximum
HFA only	HFA Devices + SIP Devices +Mobile Users	200,000
SIP only		
DLS Mobility		
DLS Mobility	Log on /Log off of Mobile Users per hour (30K data)	20,000
DlsAPI	DlsAPI Sessions	100

Scenario	Max.number of :	Maximum
Element Manager Synchronization	Element Managers	100

- If used with Microsoft SQL Server 2008 R2 Enterprise or DataCenter Edition in a Multi-Node Deployment with two DLS nodes including synchronous database mirroring and automatic failover (Redundancy Scenario)

Scenario	Number of	Maximum
Number of Nodes : 2		
DLS Mobility	Log on /Log off of Mobile Users per hour (30K data)	20,000
Number of Nodes : 3		
DLS Mobility	Log on /Log off of Mobile Users per hour (30K data)	22,000
Number of Nodes : 4		
DLS Mobility	Log on /Log off of Mobile Users per hour (30K data)	24,000

NOTE: Uniform request arrivals within the 1 hour time window is assumed. For instance, 20000 /hour is equivalent to 330/min or even 5.5/sec.

NOTE: In the case of Multi-Node environments, actual system capacities may differ dependent on the server hardware. Higher figures might be possible with higher hardware performance.

The following table illustrates the Maximum Log-on Request rate for DLS Deployments:

Deployment	Logon requests/ sec
Single Node DLS with internal MS SQL Express **Single Node DLS with remote Microsoft SQL Server 2008 R2 Enterprise or DataCenter**	5.5

Deployment	Logon requests/ sec
2 DLS front-end nodes **2 Microsoft SQL Server 2008 R2 Enterprise or DataCenter (Synchronous Mirroring)**	6
4 DLS Front-end nodes **2 Microsoft SQL Server 2008 R2 Enterprise or DataCenter (Synchronous Mirroring)**	6.5

2.1.3 Licensing

For configuring base software, basic devices, mobile users, and PKI users, using DLS-Nodes in a cluster, database mirroring, the XML push functionality, or the location service (IP infrastructure), licenses must be purchased. All further DLS functions are free of cost.

You can use HiPath License Management to load the relevant licenses for this onto the license agent. The license agent can be specified when you install the DLS or later under **Administration** > **Server Licenses**.

The license agent and HiPath License Management are available for download on C-SWS.

Demo licenses are available for test installations and include:

- 1 Base Software License (30 days)
- 500 Basic Device Licenses (= registered IP Devices) (30 days)
- 10 Mobile User Licenses (30 days)
- 10 PKI User Licenses (30 days)
- 1 Location Service License (30 days)
- 1 Node License (30 days)
- 1 Database Mirroring License (30 days)
- 1 XML Push License (30 days)
- 1 Activation Period License (30 days)

License Installation on an OpenScape onboard

In the case of Linux DLS in Integrated Simplex where DLS licenses are loaded in the CLA of the OSV (internal) the following instructions rshould take place :

1. Copy the DLS license file into directory: `/opt/unisphere/srx3000/cla/import` .
2. Wait a few minutes until the license is activated.

   NOTE: The license file will be copied into: `/opt/unisphere/srx3000/cla/license`.
3. Finally,check if the license file exists in: `/opt/unisphere/srx3000/cla/license`.

Re-assigning Licenses

In the case of re-assigning licenses to DLS (another DLS or the same DLS on another/previous snapshot) the following instructions should take place :

1. Activate the same (.lic) license file on CLA you own.
2. Restart CLA service (On windows, you can use service manager)
3. On CLM synchronize with CLA
4. Restart DLS to contact CLA and load the available/required licenses (or wait for DLS to contact CLA - which happens approximately every 4 hours).

2.1.4 Installing DLS Software

Installation is performed as follows:

1. Download the DLS Software from the SWS-Server and unzip the downloaded file.
2. Click *setup.exe*.
3. Follow the user prompts in the installation shield.

The components required by the DLS, such as the database and web server, are installed if they are not already available on the system.

2.2 Starting the DLS for the First Time (Single Mode)

1. Starting the program

To start the DLS client, use the following URL syntax :

- **https://<DLS Server IP>:10443/DeploymentService/** (secure Windows DLS / https)
- **https://<DLS Server IP>/DeploymentService/** (Linux / OSV integrated)
  or
  https://[Server IP address]:10443/DeploymentService/ (encrypted connection via Secure HTTP).

NOTE: For Integrated Simplex, when generating a Device Management connection, the connection port for Internal DLS is **443** and NOT 10443.

NOTE: DLS Security checklist recommends using secure access methods.

2. Logging on

Log on under the "admin" account with the password set during installation.

The default credentials for logging on to DLS are as follows:

Account : **admin**

Password : **Asd123!.**

NOTE: Notice the capital 'A' since passwords are case sensitive.

3. Modifying passwords/configuring accounts

You must create a separate account in the DLS for each DLS administrator. This is only possible with the default "admin" account. To do this, select **Administration > Account Management** in the menu bar. Click **Search**. If you switch to **Table** view, information is provided on all user IDs in a table overview. You can create a new account with **New**.

4. **Location configuration**

   You can use the location criterion to define groups for terminals that share the same range of IP addresses and/or are connected to certain systems. Proceed as follows for basic configuration of the location:

   Define the IP address range for the location in **Administration** > **Server Configuration** > **Location** > **"IP Ranges" Tab**.

   Enter the IP addresses or host names of the systems (PBX/gateway or SIP server) for the location in **Administration** > **Server Configuration** > **Location** > **"Reg-Addresses" Tab**.

   Additional configuration options are provided under **Administration** > **Server Configuration** > **Location**.

   If you do not define a location, the "Default Location" is assigned for all location-specific parameters.

5. FTP configuration

To load IP phone software and other files to the devices, you will need an FTP server that provides the software images. The DLS supports the configuration and use of unlimited numbers of FTP servers. To enter the access data for an FTP server, go to **Administration > Server Configuration > Configure FTP Server**. Click the action button **New** to create a new FTP server.

In the **Server ID** field, enter a name for the FTP server you wish to use to transfer IP phone software.

In the **Hostname** field, enter the network name or the IP address of the FTP server.

In the field **SW Image Path**, the path to the directory containing the software image files is specified. This path is relative to the root directory of the FTP user ID used by the DLS. If the image files are contained directly in the root directory, enter "./" as your path.

In the **User** field, enter the user ID that the DLS should use to log on to the FTP server. In the **Password** field, enter the corresponding password.

You can use **Test** to check if the settings are correct using an FTP connection test. Apply your entries by clicking **Save**.

You can find a description of all fields and additional information in Section 6.3.4, "FTP Server Configuration".

6. HTTPS configuration (for OpenStage terminals)

OpenStage phones can alternatively use an HTTPS server for downloading files.

In the **HTTPS Server ID** field, enter a name for the HTTPS server you wish to use to transfer files.

In the **HTTPS Server URL** field, enter the network name or the IP address of the HTTPS server.

You can find a description of all fields and additional information in Section 6.3.5, "HTTPS Server Configuration".

7. Plug & Play/Autoconfiguration

DLS provides an option for preconfiguring IP devices to go into operation as soon as they are connected to the network. To do this, the DLS transfers the necessary configuration parameters to the IP device. In the case of IP Devices (IP phones, IP clients, IP Gateways), these parameters include, in particular, phone-number-dependent data for registration at the telephone system. The DLS must receive the system access data before it can incorporate the necessary data from the telephone system in the DLS database. Enter this under **Element Manager** > **Element Manager Configuration**.

Using profiles, you can create standard configurations for multiple devices. Device profiles are created from templates composed of a collection of settings from individual masks plus information about the devices, gatekeepers, and IP ranges supported by each profile. To perform configuration, select **Profile Management** > **Device Profile**.

If you want to create individual parameters for a particular device, you can create what is known as a virtual device. To do this, go to **IP Device Management** > **IP Device Configuration** and click **New**. The virtual device is assigned a placeholder beginning with "@" instead of the device

ID and the IP address and E.164 number are set to 0. To assign a physical device, enter either an E.164 number or a real device ID (generally, the MAC address). The  icon beside the **Device Type** field indicates that the IP device is not yet registered at the DLS. Otherwise, configuration is the same as for a connected, registered device.

NOTE: DLS records a device on the basis of the device ID/E.164 number value pair. In all configuration masks, this information is provided in the upper half of the user interface. Make sure that the data displayed here refers to the IP device you wish to configure so that the configuration data can be assigned to the correct IP device.

2.3 Required Workpoint Firmware Installation

If a device is connected for the first time when the DLS is running, it is automatically installed with the latest software available. Auto Deployment is used to upgrade devices that have already been connected. This requires a running FTP server and correct FTP configuration in the DLS (see Section 2.2, "FTP configuration"). The firmware image files must be saved in the directory that was specified as the **SW Image Path** during FTP configuration. They can also be divided into subdirectories.

2.3.1 Creating Software Images Automatically

Once the images are available on the FTP server, the DLS can register these automatically. The files are then assigned information, such as, the matching device type, the software type (SIP or HFA), and the software version. You can activate automatic registration by going to Software **Deployment** > **Manage Software Images** and then clicking **Autocreate...**. Click **Start** in the ensuing dialog window.

2.3.2 Auto Deployment

Software deployment is implemented in accordance with previously defined rules as soon as a new terminal has been registered at the DLS. These rules are defined as follows:

1. Click **New** in the area **Software Deployment > Manage Rules**.
2. Select the device type in the **Device Type** field. Remember, only one rule is permitted per device type.
3. In the field **SW Type**, select the correct software type.
4. If you want the software deployment to be performed using the latest available software, activate **Deploy latest version**.

   If you want the software version you have specified to be installed if the previously installed software is older, activate **Deploy software on an upgrade** and select the required firmware image in the field **SW Image**.

   If you want the software version you have specified to be installed if the previously installed software is newer, activate **Deploy software on a downgrade** and select the required firmware image in the field **SW Image**.

2.3.3 Manual Deployment

1. Go to **Software Deployment > Workpoint Deployment**. In the upper half of the user interface, select the device where you would like to install the software. Click **Deploy**.
2. A window is displayed with a list of all available software. The default setting only allows you to select data that matches the currently-selected device type. Select the required software and click **Deploy**.
3. A dialog opens where you can define when deployment should take place. The check boxes **Enforce deployment if phone is busy** and **Overwrite deployment restrictions** should not be activated. Click **OK** to start deployment.

2.4 Frequently Used Functions

2.4.1 Scan IP Devices

The DLS records IP Devices data during scanning. The IP Devices do not have to be registered at the DLS for this.

1. Go to **Call: Main Menu > Call: Main Menu > > IP Device Interaction > Scan IP Devices**. To activate a scan, you need a scanner object. If one has already been created, you can search for it by clicking **Search**. Otherwise, you must create a scanner object. To do so, click **New**. In the field **IP Scanner** in **"IP Ranges" Tab**, enter a name for the object, for example, **Scanner 1**. Next, enter the IP address range to be scanned. Click the  icon to do this. Enter appropriate values in the fields that are now active (**IP Address from** and **IP address to**). The **Port** field contains the default setting 8085; this is the default port for HTTP with IP phones. If you click **Save** now, the scanner object is ready for use.

   NOTE: In the default setting, the DSL sends an ICMP ping to each IP address of the area to be scanned. If the network does not support ICMP pings, the check box **Allow ICMP-Pings** under **Call: Main Menu > Call: Main Menu >** > **IP Device Interaction** > **Scan IP Devices** > **"Configuration" Tab** must be deactivated.

2. Click **Scan IP Devices** to activate scanning.

For more information on this subject, see Section 7.5.6, "Scan IP Devices".

2.4.2 Configuring Parameters: Example Key Layout

Configuring parameters for individual IP Devices is demonstrated below using the key layout. The function and text of a function key are to be configured. The example function in this case is the mobility key, which a user can use to log on to the telephone.

1. Go to **Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/ Keylayout**. Click **Search** and then select the device in **Table** view. For more information on the settings in the **Keysets** tab, see Section 7.1.19.1, ""Keysets" Tab".
2. To create a new entry, go to the **Destinations** tab and click the  icon. A new row is displayed in the table.
3. As the key function **Mobility** is on the first level, select "1st **Level** " in the Level column.
4. In the **Key number** column, select the key to which the new function should be assigned. For more information, see Section 7.1.19.2, ""Destinations" Tab".
5. Select "Mobility" in the **Key function** column.
6. You can now enter a key label in the final column. This is only displayed with optiPoint 420 telephones that provide automatic key labeling.

Complete the action by pressing **Save**.

2.4.3 Jobs

All actions that can be performed on IP Devices using DLS, such as, configuring the key layout, are managed by the DLS as jobs.

Using job control, you can view information on individual jobs, and cancel, delete or reactivate jobs. To do so, go to **Job Coordination > Job Control**.

Essentially jobs can be started either immediately or later at a specific, predefined time. For example, in order to perform the actions described in Section 2.4.2, "Configuring Parameters: Example Key Layout" at a specific time, perform all the steps described except the final **Save** action. Then, in the top right field **Job ID**, enter an arbitrary job ID and click the  icon beside the field **Execution Time** to define when the action should be executed. Once this has been completed, activate the job with **Save**.

For further information on job coordination, see Section 14, "Job Coordination".

2.5 Using the Mobility Function

With the Mobility function, call numbers can be assigned to specific persons instead of devices. As well as their call number, users can transfer their personal settings, such as their key layout, from one device to another. To enable this, users must log on to a device that has been activated for this purpose with their call number and a password. As a result of logging on, the call number of the device and all other user data is replaced with the data of the new user. Following logoff, the device is reassigned its original number and user data.

In order to use the mobility function, a mobile user profile must be created. This profile is identified by a call number and password. There are two possibilities here: creation by adding or creation by migrating a basic profile. The second option is described below.

1. A prerequisite for using the mobility function is that the workpoint is activated for mobile user logon. To do so, go to **Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SIP Mobility**, and in the **"SIP Mobility" Tab**, activate the option **"**Device available for Mobile User**"**. Activation takes a few seconds and is carried out in the background.
2. Go to **Mobile Users > SIP Mobile User Interaction > SIP Mobile User**. If you now select "Mobility enabled Device" in the **User Type** field and then click **Search**, a list of all devices available for a mobile user is shown in **Table** view.
3. Click on **Migration to Mobile User**. After this, a dialog window appears.
4. Now, in the field **New Basic E.164**, enter a new basic call number for the end device currently selected, whose basic profile is to be migrated. This must exist on the OSV database.A new basic call number is necessary so that the end device remains ready to use. Further on, a virtual device must exist which provides the required Plug&Play data (see Section 15.8.2.2, "Creating Plug&Play Data"). As soon as the migration has succeeded, the previous basic call number is assigned to the mobile user. The call number of a mobile user is also referred to as mobility ID.

5. In the field **Basic Mobile User Profile**, a new profile for the basic user (the basic call number) must be entered. The mobile user adopts the data and the call number of the end device, these data automatically constituting his new individual profile. If you search for the mobile user after this action is completed, the mobile user’s call number is displayed with a prefixed "@". This is a placeholder for his individual profile.
6. Start the migration via **Start Migration**.
7. Now, enter a new password for the mobile user in the field Mobile User Password (the default password is "000000"). Finally, confirm by clicking **Save**.

2.6 Security

2.6.1 Certificates

Certificates enable secure authentication between servers and clients. They can be implemented for the following server-client scenarios:

- WebServer Certificates for web-based Management (WBM of IP Phones/IP Gateways)
- Certificate for IEEE 802.1x/EAP-TLS authentication (IP Phones only)
- TLS-based Signaling Encryption (all device types)
- additional Server Applications for IP Phones (e.g. LDAPS)

DLS can be used for certificate administration.

For more information, see Section 16.14, "Security: Administering Certificates".

2.7 Recommendation for Antivirus

Please configure the following processes as trusted exceptions in your antivirus software to ensure optimum use of OpenScape Deployment Service (DLS):

- **Under** C:\Program Files\DeploymentService:

the installation directory of DLS.

- **Under** C:\Program Files\DeploymentServiceDATA:

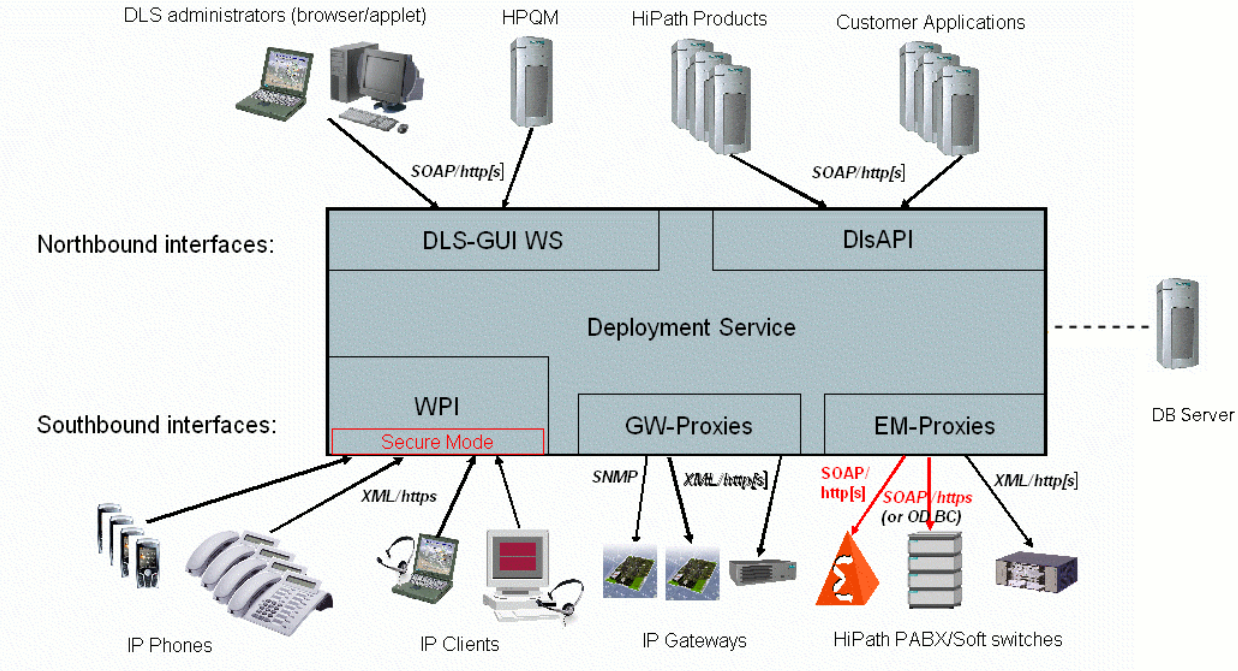
the DB backup directory of DLS.

3 Concept and Features

3.1 Overview

The Deployment Service (DLS) is a HiPath Management application for administering workpoints (IP phones and IP client installations) in both HiPath and non-HiPath networks. The DLS database can be exported to a separate server (optional).

The following overview shows possible components that can work together with the DLS in a network.



NOTE: We recommend that you use a DHCP server in the DLS environment to

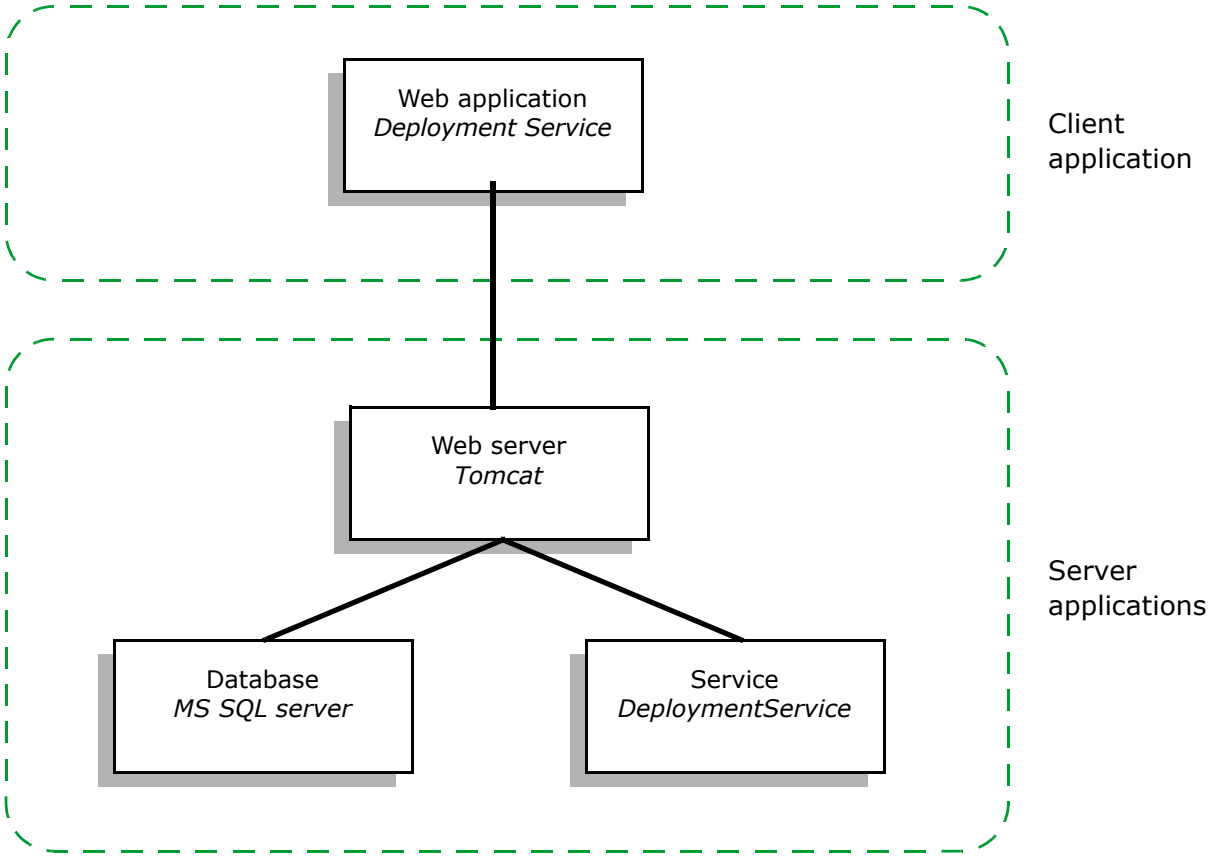
-support Plug&Play and
-ensure the authenticity of the DLS server.

Setting up the DHCP server should be one of the first tasks you perform, if possible, even before you install the workpoints.

Only one DLS server is allowed per DHCP domain at the customer facility.

3.2 Deployment Service Components

The following overview shows the components that are involved in operation of the Deployment Service on the server and client sides.



The client applications can be executed both on a client PC that can be reached in the IP network and on the server PC itself.

NOTE: When server and client are being used separately, ensure that the operating system times are synchronized.

3.3 Operating Fundamentals

Before you can configure IP Devices with the DLS, you must first collate all IP Device data following initial DLS startup. This means that the IP Device configuration data first has to be incorporated in the DLS server database.
The IP Devices do this by registering at the DLS and transmitting this data to the DLS.

The IP Devices data is read out by

- scanning the IP Devices with DLS, see Section 7.5.6, "Scan IP Devices" (recommended if there are already a number of IP Devices operating after the initial DLS startup)

  or by

- plugging the LAN connector or power supply into the IP Device (recommended if putting separate additional IP Devices into operation).

All actions performed with the DLS, for example, an IP Device software update or a modification of the configuration data, are logged in the DLS.

Job coordination helps you in this process. This allows you to see the status of each action and to determine the cause if there is an error. For more information, see Section 14, "Job Coordination".

3.4 Area of Application

NOTE: Please refer to the Release Notes or Sales Release for the appropriate version for information on current supports/restrictions.

You can administer the following IP Devices with the DLS:

IP Device	HFA Version	SIP Version
AC-Win 2Q IP	all versions	all versions
AC-Win MQ IP	all versions	all versions
HG1500		
HG3500		
HG3575		
Mediatrix C7		
Mediatrix G7		
Mediatrix S7		
HOOEE (HiPath OpenOffice EntryEdition)	all versions	all versions
HOOME (HiPath OpenOffice MediumEdition)	from V1.0	from V1.0
HP2K V2.0	from V2.0	from V2.0
optiClient 130	from V5.0 onwards	V2.0
Unify OpenScape Desktop Client	all versions	all versions
optiPoint 400 economy	from V5.0 onwards	-
optiPoint 400 standard	from V5.0 onwards	-
optiPoint 410 entry	from V5.0 onwards	from V4.1 onwards
optiPoint 410 economy	from V5.0 onwards	from V4.1 onwards
optiPoint 410 economy plus	from V5.0 onwards	from V4.1 onwards
optiPoint 410 standard	from V5.0 onwards	from V4.1 onwards
optiPoint 410 advance	from V5.0 onwards	from V4.1 onwards
optiPoint 420 economy	from V5.0 onwards	from V4.1 onwards
optiPoint 420 economy plus	from V5.0 onwards	from V4.1 onwards
optiPoint 420 standard	from V5.0 onwards	from V4.1 onwards
optiPoint 420 advance	from V5.0 onwards	from V4.1 onwards
optiPoint 600 office	all versions	-
optiPoint WL2 professional S	-	V1.0 (50/70)
optiPoint WL2 professional	V1.0 (50)	-
OpenStage 5	all versions	all versions
OpenStage 15	all versions	all versions

Table 2 IP Devices / versions supported

IP Device	HFA Version	SIP Version
OpenStage 20E	all versions	all versions
OpenStage 20	all versions	all versions
OpenStage 40	all versions	all versions
OpenStage 60	all versions	all versions
OpenStage 80	all versions	all versions
OpenScape Desk Phone CP200/205/400/ 600/600E	all versions	-
OpenScape Desk Phone IP 35 G	all versions	V3R3
OpenScape Desk Phone IP 35 G Eco	-	V3R3
Wave Evolution Lo	-	V3R3
OpenScape Desk Phone IP 55 G	all versions	V3R3

Table 2 IP Devices / versions supported

NOTE: On the following device types, the mobility function is available in SIP V6.0 or later: 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.

On the following device types, the mobility function is available in all versions: OpenStage 20E, OpenStage 20, OpenStage 40, OpenStage 60, OpenStage 80.

Administration is possible for various communication platforms. Both HiPath and non-HiPath platforms are supported:

Platform	P&P connection	Plug& Play	QDC connection	QDC	SRTP connection	SRTP
OpenOffice EE V1.0	standalone	no	no	no	no	no
OpenScape Office MX/LX	standalone	no	no	no	no	no
HiPath 3000/5000 <V5.0	standalone	no	no	no	no	no
HiPath 3000/5000 V5.0	HG1500	yes	HG1500	yes	no	no
HiPath 3000/5000 V6.0	HG1500	yes	HG1500	yes	HG1500	yes
HiPath 3000/5000 V7.0	HG1500	yes	HG1500	yes	HG1500	yes
HiPath 4000 V1.0	Assistant	yes	no	no	no	no
HiPath 4000 V2.0	Assistant	yes	HG3530/50/ 70/75	yes	no	no
HiPath 4000 V3.0	Assistant	yes	HG3530/50/ 70/75	yes	HG3530/50	yes
HiPath 4000 V4.0 / V5	Assistant	yes	HG3500/75	yes	HG3500/75	yes
HiPath 4000 V6[1]	Assistant	yes	HG3500/75	yes	HG3500/75	yes
OpenScape Voice V4.1	Assistant	yes	no	no	no	no
OpenScape Voice V9.x	Assistant	yes	no	no	no	no
HiPath DX V9	DX WebPro	yes	no	no	no	no
HiPath RG2700 V1.0	not relevant	no	RG2700	yes	no	no

Table 3 Communication platforms supported

1 Parameter settings for HiPath 4000 are also valid for HiPath 4000 V6, except as noted otherwise.

NOTE: If SIP IP phones are connected to the platforms HiPath 3000 and HiPath 4000, some features are not available. Please deactivate these at the IP Device, so that they are not visible resp. selectable by the user.

For more information on this, see Section 7.1.4.4, ""Availability" Tab".

3.5 Overview of Software and File Types

The following table displays how DLS maps file extensions to file types in standard configuration.

NOTE: The administrator can define the extensions as desired in the `file_map.xml` file found under `DeploymentService\Tomcat\webapps\DeploymentService\WEB-INF\classes`.
To return to the standard configuration copy and rename `default_file_map.xml` to `file_map.xml`.

Object type (name in the DLS)	File extension	Example	Contents
Software objects			
Software image	*.img	opera_bind.img	OpenStage firmware
Software image	*.app	optiPoint410std-V5.0.0.app	DLS-compatible optiPoint firmware ("new format")
Software image (old)	*.app	vxWorks.app	non-compatible optiPoint firmware ("old format")
Software image	*.exe	setup.exe	PC software installation
Firmware (Netboot)	*.fli	vxWorks.fli	Software image for transfer via Netboot server
		netboot308.fli	Netboot firmware
File objects			
LDAP Template	*.ldap	ldap_temp.ldap	LDAP template for optiPoint and OpenStage 40/60/80
	*.txt	ldap_temp.txt	LDAP template for OpenStage 40/60/80

Table 4 Software and file types supported

Music on hold [1] [2]	*.moh	opti410.moh	Audio file in proprietary format for optiPoint and OpenStage.
	*.wav	music.wav	Audio file in WAV format for OpenStage. Recommended Specifications: Audio format: PCM Bitrate: 16 kB/sec Sampling rate: 8 kHz Quantization level: 16 bit
	*.mp3	music.mp3	Audio file in mp3 format for OpenStage 60/80.
	*.mid	music.mid	MIDI-Datei for OpenStage.
Screen Saver[2]	*.jpg	screenPic1.jpg	Image file for the OpenStage 60/80 screensaver. Resolution: OpenStage 60: 320x240 OpenStage 80: 640x480
	*.png	screenPic1.png	
INCA Firmware	*.h86	inca.h86	INCA firmware for optiPoint 600 office
JAVA Midlet	*.jad	?	Java application
-	*.jar [3]	?	Java archive
Logo file[2]	?	?	
	*.jpg		Image file for a logo on OpenStage. Recommended specifications for OpenStage 60: Width: 240 px Height: 70 px Resolution: 70,55 dpi Recommended specifications for OpenStage 80: Width: 480 px Height: 148 px Resolution: 124,5 dpi
	*.png		
System and Ringtone[1] -	*.xml	?	System and ringing tones
	*.wav	?	
	*.mp3	?	
	*.mid	?	
	*.app	bootrom.app	Boot loader for the optiPoint 600 office
-	?	?	New/other applications

Table 4 Software and file types supported

-	?	?	DSM firmware
-	*.csv	?	For ENB import and export
Dongle Keys	*.key	dongle.key	Dongle Keys for OpenStage Remote Test Tool

Table 4 Software and file types supported

1 Only for SIP versions.
2 Ringtones and music on hold files must not exceed 1MB in size, while screensavers/logos should not be larger than 300kB.
3 Only in combination with a *.jad file.

In the case of LDAP, an LDAP template is deployed to the phone in order for the phone to have access to a Corporate Directory. The template file is a simple and short list of attributes in the form of a text file.This file is employed by the phone in order to communicate with an LDAP server (usually located in DNS) and make a directory query (for example search for a company contact and find its telephone number).The template serves as a mapping between the phones and the LDAP servers items. The attributes contained in the template depend on the phone Corporate Directory menu items and the type of the LDAP (e.g. Microsoft 2008 R2 LDAP).

Please refer to the following example template of a Microsoft 2008 R2 LDAP server for OpenStages & DPIP's.
It shall provide useful info not to mention the time saving process each time an LDAP Corporate directory is set up for the first time:

```
OpenStage LDAP TEMPLATE (v.2)
SEARCHBASE="ou=DINGO,o=SCD"
ATTRIB01="sn"
ATTRIB02="givenName"
ATTRIB03="telephoneNumber"
ATTRIB04="facsimileTelephoneNumber"
ATTRIB05="mobile"
ATTRIB06=""
ATTRIB07="o"
ATTRIB08="street"
ATTRIB09="l"
ATTRIB10="job-title-text"
ATTRIB11="mail"
EOF
```

NOTE: The correct SEARCHBASE should be entered by the admin for each LDAP directory. It can be seen as a tree where the contact will be searched in the directory. The left column of numbered attributes depend on the phone menu. Their equivalents (the right column) depend on the type of the LDAP server.

3.6 The Most Important Features

Security:

DLS provides extensive functions that guarantee a high level of security for VoIP communication. The following is an overview of the most important elements:

- PSS generation and distribution within an SRTP security domain (password identification).
- Import and distribution of individual certificates for secure authentication.
  See Section 16.14, "Security: Administering Certificates".
- Secure mode can be configured for mutual authentication between the workpoint and the DLS.
  Area: **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"DLS Connectivity" Tab**.
- Minimum password length specification for user, administration, and screenlock passwords as well as for the SNMP community string.
  Area: **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Security Settings** > **"Passwords" Tab**.
- Systematic deactivation of workpoint services (for example, WBM interface).
  Area: **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Security Settings** > **"Enabled Services (NW Stack)" Tab**.

Mobility for SIP IP phones:

DLS is a tool that supports the mobility feature on SIP IP phones and permits the configuration and administration of Mobile Users. You can use these options to migrate existing workpoints and implement mobile user standards.

For basic information on mobility in DLS, see Section 3.8, "DLS Mobility - General Information".

Multi-Tenancy:

Multi-Tenancy is offered yet requires PSR (Process Submit Request) approval.

Software deployment:

DLS is a user-friendly tool for upgrading software on all workpoints available or on a definable number of workpoints.

For more information, see Section 10, "Software Deployment".

Inventory data management:

The DLS is the central inventory data manager. Inventory data describes the hardware configuration and capacity of the workpoint and includes information on items, such as, add-on devices or adapters available.

Inventory data can be exported over the CSV interface.

Plug&Play function:

The DLS supports Plug&Play. Plug&Play means that the IP phone is ready to work as soon as it is plugged into the network - no user intervention required. Ideally, the workpoint automatically downloads all necessary software and configuration data and can be used after a few minutes.

For more information, see Section 15.8, "Workpoint Autoconfiguration (Plug&Play)".

User interface:

The DLS has a Java-supported, Web-based user interface, and runs on an Internet browser.

Configuration Management:

Configuration Management is the DLS's central tool for displaying and administering workpoint parameters in a HiPath environment. It can be operated either at the customer facility or by Service (via remote administration).

Workpoints can also be restarted with the Reset function.

Additional functions:

The following basic functions are supported:

- Import/Export:

  This function is particularly useful during the initial configuration of the DLS, and can also be used in later operation for backing up configuration data.

  The Import/Export function is a user-friendly tool for transmitting a DLS configuration from one DLS installation to another.

- Access protection:

  Access to the DLS is password-protected.

- Error and activity logging and trace function.

- Support for the configuration of QDC features for HG3550 V2.0, HG1500, RG2700, and HiPath HG3530/70/75 (over SNMP proxy).
  The SNMP proxy is installed together with the DLS during startup and start automatically (runs as a local "DeploymentServiceSNMPProxy" service).

3.6.1 Capacity Limits and Restrictions

- You can only use the plug&play functionality in DLS if there is a DHCP/DNS infrastructure in the network and this has been configured for working with the DLS (see Section 15.8, "Workpoint Autoconfiguration (Plug&Play)").
- You can only install one DLS per domain in the network.
- The DLS user interface is available in German and English.

3.6.2 Ports Used

The Security Checklist Planning Guide documentation contains an overview of the ports used by the DLS.

3.7 Deployment Service supported deployments

DLS deployments
Single Node Local Database[1]
Multi-Node remote DataBase in Synchronous Mirroring[2]
OpenScape Voice Entry (Integrated Simplex Deployment)[3]

Table 5 DLS deployments

1 DCMP service can optionally be installed as part of the DLS Server or in a seperate server
2 DCMP service can optionally be installed as part of the DLS Server or in a seperate server
3 DLS Service included as a component in the OpenScape Voice Entry Server

NOTE: Single node DLS with MSSQL remote DB deployment is replaced by Single node DLS with PostgreSQL (which is a local DB deployment only)

3.8 DLS Mobility - General Information

You can use the mobility feature in DLS to carry out the following functions (for definitions of these terms, see below):

- Create, refresh and delete Mobile Users
- Create user profiles for Mobile Users.
- Modify Mobile Profile parameters
- Migrate Basic Profiles to Mobile Profiles
- Log Mobile User on or off and monitor activities.
- Archive mobile users.

For additional information on operation, refer to Section 16.16, "Configuring and Administrating Mobility".

3.8.1 Mobility Definitions

The following terms are frequently used in connection with mobility in this document:

Term	Definition
Mobility Function	This function enables Mobile Users to log on to a Mobility Phone and operate it with their personal settings.
Mobility Phone	A phone that supports the Mobility Function. In other words, Mobile Users can log on to this kind of phone and operate it with their personal settings.
Mobility ID	Phone number of the Mobile User. The Mobility ID and password are used for authentication when logging on to a Mobility Phone.
Basic User	Phone number and user data of a Mobility Phone if there are no mobile users logged on.
Mobile User	A user who can log on to a random Mobility Phone and operate it with his or her personal settings.
User Data Profile	This is a configurable user data (sub)set, depending on the scope of the associated templates. The parameters are not device-specific.
Device Profile	User-independent telephone parameters. These parameters are entirely device-specific (dependent on the telephone used).
Mobile User Archive	Can be created to save mobile user data.

Table 6 Definition of mobility terms

3.8.2 Using Mobility

Mobility grants appropriately configured users access to their individual settings on all telephones that support the mobility function. Transferable parameters include user-specific configurations (for example, authorizations) and user-defined settings (for example, language settings).

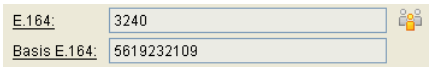
To use this function, just press the "Mobility" function key on a Mobility Phone (or use the corresponding telephone menu), and log on as a Mobile User with your call number (Mobility ID) and user password.

After logging on, Mobile Users can make and receive calls via Mobility Phones and can always be reached at their personal number. Outgoing calls are also made using these numbers.

Mobile Users can log off a phone either locally at the phone or remotely via Web-based Management (WBM) or DLS ("forced logoff").

3.8.3 Mobility ID

These two call numbers are displayed as **E.164** and **Basic E.164** in the area **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** in the DLS client.



E.164 is the Mobile User's call number (Mobility ID) and **Basic E.164** is the Mobility Phone call number when no Mobile Users are currently logged on.
The smiley to the right of the **E.164** field indicates that a Mobile User is currently logged on.

3.8.4 Configuring Mobility

The Mobility Function can only be configured for a phone via DLS. To configure this function, the telephone must be released by activating the Mobility function.

NOTE: The "Mobility" function can only be assigned to a key on the actual telephone; keys on connected optiPoint key modules or optiPoint self labeling key modules cannot be used.

A Mobile User can be created in two ways:

- **Creating a Mobile User by adding a number**

  A new Mobile User is generated by assigning a new call number together with a password. The remaining parameters are assigned to the Mobile User from a User Data Profile. When the mobile user is logged on, only device-specific parameters are retained in the telephone.

- **Creating a Mobile User by migrating a number**

  The telephone's existing call number becomes the Mobility ID and the telephone is assigned a new basic number. The mobile user accepts the telephone's parameters. Use this option, for example, if you want to change an existing workstation into a mobile workstation. You can then continue to use the existing number to contact the user at the mobile workstation, providing he or she is logged on to a Mobility Phone.

For more information on configuring the Mobility Function for SIP IP phones, see Section 16.16, "Configuring and Administrating Mobility".

3.8.5 Profile Concept in DLS

The following table illustrates the Profile assignment sequence :

Priority	Profile Data Deployment	Definition
1	Standard Profiles	Profiles generated under Main Menu > Administration > Server Configuration > P&P Settings > "Standard Profile" Tab
2	Parent Location Default	This refers to a Profile that points to a Location that has been configured under Administration > Server Configuration > Location as a Parent one.
3	Child Location Default	This refers to a Profile that points to a Location that has been configured under Administration > Server Configuration > Location to be a Child Location.
4	IP Device Configuration Profile	This refers to an explicit definition of a Profile under Call: Main Menu > Call: Main Menu >> IP Device Management >IP Device Configuration > "Profile" Tab.

3.8.5.1 Difference between Device Profile and User Data Profile

The following examples of parameters and the profiles they belong to highlight the difference between Device Profiles and User Data Profiles.

The parameters in the example are displayed in the following DLS client area:
Call: Main Menu > Call: Main Menu > > **IP Phone Configuration** > **Miscellaneous** > **"Country & Language" Tab**

Parameter	Profile	Definition
IP address	Device Profile	The IP address is connected to a physical phone, regardless of who is logged on to the phone. This makes it part of the Device Profile.
Layout	User Data Profile	The Mobile User should be able to use a telephone's key layout with any Mobility Phone. This makes it part of the User Data Profile.
QoS parameters	Device Profile	QoS parameters are location-specific and therefore part of the Device Profile.
Language	User Data Profile	Once a language is configured on a phone, it should be available to a Mobile User on every Mobility Phone. This makes it part of the User Data Profile.

Table 7 Sample parameters with profile classification

A User Data Profile can be either a Basic Profile or a Mobile Profile, Section 3.8.5.2, "Parameter Configuration Availability".

3.8.5.2 Parameter Configuration Availability

Device Profile parameters can always be modified in the **IP Phone Configuration** area. Device Profile parameters are not Mobile User data. As a result, they are not available in the **SIP Mobile User Configuration** area.

Different configuration options are available in the DLS client depending on whether the Mobility Function is configured on a phone and, if so, whether a Mobile User is logged on.

This section only deals with the Basic Profile and Mobile Profile, as the Device Profile is always available in the **IP Phone Configuration** area and never in the **SIP Mobile User Configuration** area.

Status	**Parameters under:** **IP Phone Configuration**	**Parameters under:** **SIP Mobile User Configuration**
No Mobility Phone	All profiles can be modified	Not available
Mobility Phone, Mobile User is not logged on	Basic Profile: can be modified Mobile Profile: not available	Basic Profile: can be modified Mobile Profile: can be modified. Both profiles are visible as two objects in the DLS.
Mobility Phone, Mobile User is logged on	Basic Profile: not available Mobile Profile: read-only.	Basic Profile: can be modified (changes transferred to phone after Mobile User logoff). Mobile Profile: can be modified

Table 8 Parameter availability in DLS

Please note the different parameter displays in the **IP Phone Configuration** and **SIP Mobile User Configuration** areas:

- In the **IP Phone Configuration** area, a *single* object (displayed in **Object** view or as a row in **Table** view) always corresponds to a physical SIP IP phone (mobility-enabled or standard).
- In the **SIP Mobile User Configuration** area, two different object types exist:
  - an object for the Mobility Phone and
  - an object for the Mobile User.

3.8.6 Mobile user data size

According to the default DLS configuration, there is limit in the size of the mobile user data that can be exchanged between DLS and phoned during logon/logoff. This occurs due to the fact that phones/DLS truncate the user binary data into "pieces" of ~5500 bytes and add 10 of these pieces in every WPI message, making a total of ~50k per message.

By default Tomcat allows 100 http requests/responses over the same connection, which means that the size of data that can be transferred is ~5MB.Therefore mobile user data with size bigger than 5MB can cause issues in the logon/logoff functionality.

In order to override this restriction in the mobile user data size, a configuration in the DLS Tomcat server is needed.Proceed with the following steps:

1. In the DLS installation directory, go to: `...\DeploymentService\Tomcat\conf` and edit the "server.xml" file.
2. In the connector of the WPI interface (port 18443, if secure mode is not used), add the the following (in bold):

   ```
   <Connector port="18443" maxThreads="500" backlog="50000" maxQueueSize="50000"
   acceptCount="20000" enableLookups="false" connectionTimeout="150000"
   maxPostSize="1048576" maxKeepAliveRequests=”-1”

   redirectPort="-1" scheme="https" SSLEnabled="true" sslProtocol="TLS"
   ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_128_CBC_SHA,
   TLS_RSA_WITH_AES_256_CBC_SHA" clientAuth="false" algorithm="IbmX509"

   keystoreType="PKCS12" trustStoreType="PKCS12" protocols="TLSv1.2,TLSv1"

   SSLImplementation="de.siemens.icn.hipath.dls.connector.jsse.bsafe.BSAFEJSSE_WPI
   _Implementation"

   />
   ```

3. Restart the DLS service.

> ***IMPORTANT:*** It is highly recommended not to change the above value, due to possible security issues and the fact that mobility logon/logoff times are increased proportionally to the size of the user data. So, it is recommended to keep the size of the mobile user data at a reasonable level (<5MB)

3.9 DLS System Monitoring

DLS System Monitoring delivers information on the system, especially alarms and fault messages automatically from the system components as base for maintenance actions.

3.9.1 System Monitoring Tools-DLS RapidStat

DLS RapidStat is the Monitoring feature tool that is responsible for running diagnostic checks on a DLS machine.A separate tool, **traceDls**, is responsible for collecting all log files, traces and any other files useful for troubleshooting,as well as archiving and placing them to an easily accessible directory for retrieval.

The **DLS RapidStat** is a diagnostic and information collection tool that helps the DLS administrator both prepare a system for a DLS installation / upgrade and helps him troubleshoot a possible problem. The name of the tool is taken from the OSV equivalent .DLS RapidStat is as similar to the OSV as possible in order to help an OpenScape Voice user familiarize himself with the tool quicker.

NOTE: While OSV RapidStat runs only on Linux, **DLS RapidStat** runs on Windows only. In future versions it shall run on both Windows & Linux,depending on the deployment.

RapidStat provides a means to collect system health status information before and after scheduled maintenance activities such as the following:

- Generic software upgrades
- patching
- system maintenance releases
- hardware repair
- log file retrieval for debugging & repair
- other activities as determined by administrators and/or local operating procedures.

This tool eliminates the need to manually perform the system interrogation required to verify system health, which reduces human error and escalations. As a result, maintenance activities are reduced and potential service impacts (outages) can be avoided.

In the case of an existing problem with the DLS service, RapidStat can help in two ways:

- Let the administrator diagnose and fix the problem himself, or
- Provide the support team with valuable information about the system and help identify possible causes

3.9.1.1 RapidStat Functions

RapidStat operates the following functions :

1. Information Gathering

RapidStat gathers non-DLS specific information about the targer system :

- Hardware Information
  - Machine brand /model
  - CPU type
  - CPU clock speed
  - CPU load (per core)
  - Total Memory
  - Page file size
  - Paged memory
  - Storage
  - Physical disks
  - Total space
  - Used space
  - Network interfaces
- Operating system
- Operating system version
- Operating system bit length
- Date & Time
- .NET framework & version (if on Windows)
- Java version
- Antivirus check

  Check for the presence of an Antivirus software.If an Antivirus exists, DLS RapidStat displays the product name of the software.

2. DLS specific checks

DLS RapidStat runs various checks that help the administrator of the system verify that the service is running smoothly without any problems. This can be run periodically in order to identify possible problems either ahead of time or soon after a failure has occurred :

- Installation
- Version
- Deployment type
  - Single-Node
  - Multi-Node
  - Custom Database
- Service Status
  - Service Registration
  - Running / stopped
  - User under which the service is running
  - Check & Report of any services that are not needed or cannot be identified. Report with a warning if unexpected processes are found running
- Process check
  - Check & Report of any processes that are not needed or cannot be identified. Report with a warning if unexpected processes are found running
- Database status
  - Running / stopped
  - Connection to Database
  - User under which the service is running
  - Availability of DlsDB
- If RapidStat runs as part of a DLS upgrade (during installer startup) , check if the upgrade that is about to happen can proceed (upgrade path check) & verify if all migration scripts are available.
- SNMP Proxy
  - Check if 'DeploymentServiceSNMPProxy' service is running. Report with an error if no access is possible.

3. DLS Server upgrade preparation

In the case that a DLS server must be upgraded, running DLS RapidStat before the upgrade can provide a good indication whether the system is in good health to proceed with the upgrade. This can prevent a failed upgrade.
Due to the uncontrolled nature of the underlying operating system (Windows Server) as well as the coexistence of the DLS software with other software on the same machine, the environment can often be modified in an unexpected manner. DLS RapidStat will help ensure that the software environment is as expected.

3.9.1.2 Using the DLS RapidStat

DLS RapidStat is a Windows application command-line tool, written in Java & executed either as a stand-alone or through the NSIS Installer. It is installed along with the installation of DLS without any manual actions.

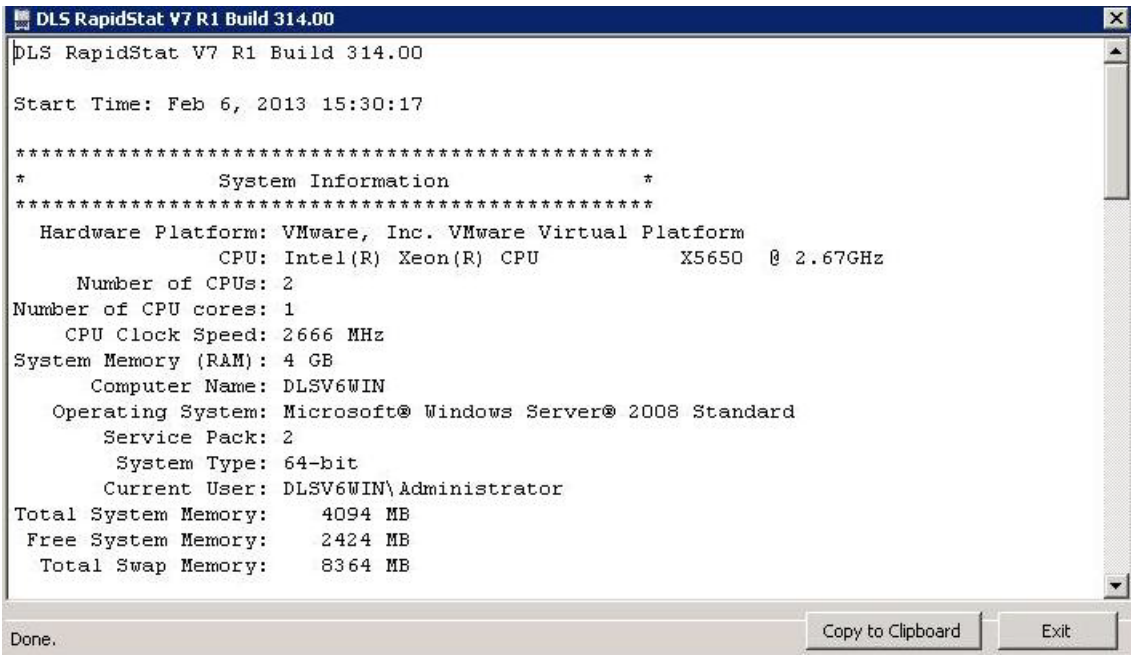
Go to `C:<Program Files>\DeploymentService\tools` and run `DlsRapidStat.exe`.

Upon executing, DLS RapidStat performs a series of validation actions & checklists and reports them using the OSV RapidStat format. The beginning of the report will contain various operating system, hardware and software information such as OS type/versions, CPU, memory, storage etc and will then continue with the DLS specific checks, one by one. At the end of the execution it should produce a summary with any found warnings or errors.

The results shall be presented either on the command shell.



or in a text area window along with two buttons :



- Copy to Clipboard : Copy the text result into the clipboard

- Exit :Close RapidStat & either return to the installer or to the operating system ,depending on how RapidStat was launched

On every run, RapidStat will save a report and an operational log file in the current user's "`%LOCALAPPDATA%\DeploymentService\RapidStat`" directory. The file name will be unique by containing the date and time of the execution.

For instance :

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

or

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

3.10 DLS Toolkit

The following table illustrates the functionality of the **dlstoolkit.bat** located under:

`[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\`

Command	Functionality
export templates <zip file.zip>	exports all DLS templates to a given zip file
import templates <zip file.zip> [tenant <tenant name>]	imports templates to DLS - for a given tenant (optional) - from a zip file. Note that tenant is ignored when multitenancy is not enabled.
export profiles <zip file.zip>	exports device profiles DLS profiles to a given zip file.
import profiles <zip file.zip> [tenant <tenant name>]	imports device profiles to DLS for a given tenant (optional) from a given zip file. Note that tenant is ignored when multitenancy is not enabled.
export locations <zip file.zip>	exports DLS locations to a given zip file
import locations <zip file.zip> [tenant <tenant name>]	imports locations to DLS for a given tenant (optional) from a given zip file. Note that tenant is ignored when multitenancy is not enabled.
export devices <csv file.csv>	exports DLS devices to a given csv file
import devices <csv file.csv>	imports devices to DLS for from a given csv file
export https <zip file.zip>	exports all HTTPS Server Configuration entries to a given zip file
import https <zip file.zip> [tenant <tenant name>]	imports HTTPS Server Configuration to DLS for a given tenant (optional) from a given zip file. Note that tenant is ignored when multitenancy is not enable
export manage_rules <zip file.zip>	exports all Manage Rules entries to a given zip file
import manage_rules <zip file.zip> [tenant <tenant name>]	import Manage Rules to DLS for a given tenant (optional) from a given zip file. Note that tenant is ignored when multitenancy is not enabled
read license	read license information and display licences.
export em <zip file.zip>	exports all element manager data to a given zip file.

Command	Functionality
import em <zip file.zip>	imports all element manager data from a given zip file.
export snmp <zip file.zip>	exports alarm snmp configuration to a given zip file.
import snmp <zip file.zip>	imports alarm snmp configuration from a given zip file.

4 Installation and Initial Configuration

There are multiple variants for DLS installation and operation:

- **Single node operation (local database):** DLS server and DLS database are located on the same machine.
- **Multi node operation (cluster):** The DLS server is running in a distributed way on multiple machines. The DLS database is hosted on another machine or on one of the DLS node machines.

In addition, if a remote database is used, database mirroring is possible (mode for enhanced data security / high availability). Mirroring can be carried out in a synchronous manner, that is, main database and mirror database are refreshed simultaneously.

The following chapters are arranged in order of their relevance for a particular DLS installation variant.

Variant	Chapter
Single Node with local database	• Section 4.5.1, "Single Node Operation with Local Database"
Multi node / cluster	• Section 4.1.5, "Infrastructure For Cluster Operation" • Section 4.2, "Install MS SQL Server for Multi-Node DLS" • Section 4.3, "Configure the Network Load Balancer" • Section 4.5.3, "Multi-Node Operation"
Enhanced database security / High availability through database mirroring	• Section 4.6, "SQL Database Mirroring Setup"

4.1 Requirements

4.1.1 General Server Requirements

For information on the hardware needed, see Section 2.1.1, "System Requirements".

The DLS server runs on the German or English version of one of the following operating systems:

- Windows Server 2016 Standard & Datacenter Edition
- Windows Server 2019 Standard & Datacenter Edition

with the latest service pack & security patches

NOTE: For larger-scale installations, particularly for cluster operation, a server operating system is required.

NOTE: In order to avoid high CPU usage issues,proceed with the following :

1. Click on **Control Panel** > **Power Options**> **Change Advance Power Settings**.
2. Switch to ’’ **High Performance**".

This is applicable only to 64-bit Operating System variants post Windows 2008.

The DLS client runs as Java applet in a web browser. Required are:

- Java PlugIn
- Any browser that supports Java plug-in, e.g. Internet Explorer, Firefox,Chrome, Opera, Safari

NOTE: If a 64-bit browser is installed in the client then a 64-bit JRE should be also installed.

4.1.2 General Client PC Requirements

The PC on which the DLS client runs should provide the following hardware features:

- Space on hard disk: no special requirements.
- CPU Pentium IV with at least 1.4 GHz clock speed.
- At least 512 MB RAM.
- Network device with 10 Mbit, 100 Mbit or more, or modem.
- Screen resolution: at least 1024 × 768 pixels with at least 16-bit color depth.

4.1.3 Personnel Requirements

Remote Service Engineer (RSE):

- Sound knowledge of LAN technology and IP networks.
- Sound knowledge of the IP Devices supported by the DLS (see Section 3.4).
- For multi node (cluster): sound knowledge of Microsoft operating systems and MS SQL Server 2012/2016.

Field Service Engineer (FSE)

- Sound knowledge of the IP Devices supported by the DLS (see Section 3.4).
- Basic knowledge of LAN technology, IP networks, and the operating systems supported.
- For multi node (cluster): sound knowledge of Microsoft operating systems and MS SQL Server 2012/2016.

4.1.4 DLS Availability

For more information on DLS licensing resp. specific DLS functionalities, see Section 2.1.3, "Licensing".

For service, additional installation options are available:

- For DLS installation at the customer facility (for example, HiPath SPA Server), the software can be acquired from BE1 using RCC.
- Installation in service can take place as follows:
  - In the international market, you can also use the BE1 for installation on the service laptop.

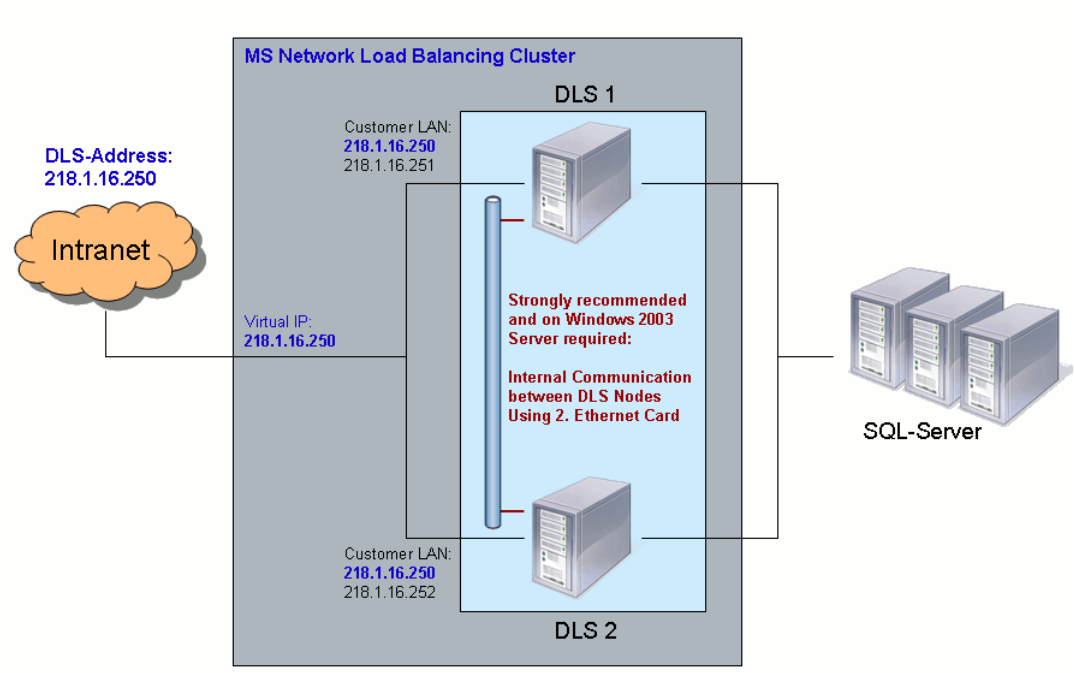
4.1.5 Infrastructure For Cluster Operation

A DLS cluster consists of up to 4 DLS nodes and up to 3 SQL servers. DLS nodes and SQL server may share common hardware, but the use of separate machines is recommended. From the end devices' point of view, the DLS nodes constitute a cluster with one virtual IP address, which is provided by the Windows Network Load Balancing Manager. The Network Load Balancer runs as a service on all DLS nodes and forwards the requests to the DLS nodes. For communication between the individual DLS nodes, all DLS nodes need a secondary IP address, and thus an additional network card.

NOTE: The nodes administered by the NLB must not be configured by DHCP.

NOTE: The network cards for SQL communication (internal network) at each node should not have a default gateway configured.

The DLS database operates as a remote database on one or more machines, depending on whether database mirroring is desired or not. However, the DLS will connect to only one machine. It is also possible to operate both DLS server and database server on one and the same machine.



4.2 Install MS SQL Server for Multi-Node DLS

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/How_to_install_Microsoft_SQL_Server_for_Multi-Node_DLS

4.2.1 How to install Microsoft SQL Server

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/How_to_install_Microsoft_SQL_Server

4.2.2 Upgrading SQL Server

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/How_to_upgrade_SQL_Server

4.2.3 SQL Native Client - When Multi-Node DLS is installed

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/How_to_configure_SQL_Native_Client

4.2.4 Change Service Password

If a password change should be necessary, proceed as following:

- Refer to `<DLS installation directory>\Tomcat\webapps\DeploymentService\database`

and execute `dlsSetServicePW.bat <new password>`.

- Change the password for the service '*DeploymentService*' on each DLS Node.
  1. Change the password on **Node 1**
  2. Go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services** > **DeploymentService** > [right-click] **Properties** > **Log On** tab and change the logon properties for deployment service
  3. Restart the service (if needed)
  4. Repeat steps **1**-**3** for each DLS Node (Multi Node purposes)

4.3 Configure the Network Load Balancer

All relevant info on the Network Load Balancer configuration can be found at the **How to** overview of **Unify Experts Wiki Portal**:
http://wiki.unify.com/wiki/How_to_configure_the_Network_Load_Balancer

under the **Network Load Balancer (NLB)** tab.

4.4 Set Up DCMP

To set up the DCMP (DLS Contact-Me Proxy), proceed with the following steps:

- Install DCMP
- Configure DCMP
- Configure DLS for DCMP
- Configure Phone for DCMP
- Test DCMP

4.4.1 Install DCMP

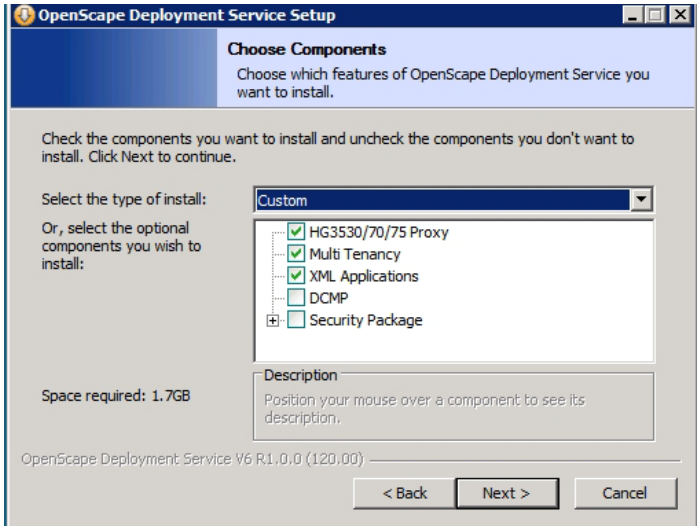
First, ensure that the DCMP is not installed already. For this purpose, navigate to **https://<IP Address>:10443/dcmp** with a web browser. If you receive an error message, you must install the DCMP. The DCMP can be installed on the DLS machine as well as on a different machine.

In the installation medium, navigate to the directory **dcmp** and start the **dcmp-installer** with a double click.

> ***IMPORTANT:*** Do not execute the "**dcmp-installer.exe**" command on a machine already running DLS. The DCMP installer itself also prompts for this restriction and should be avoided.

4.4.1.1 Installation on the DLS Machine

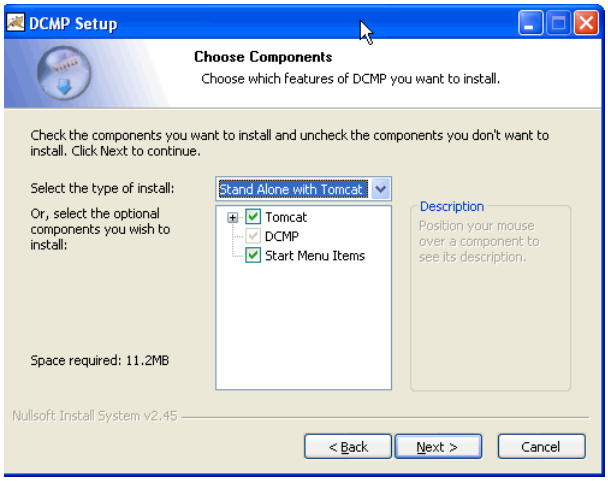
If you wish to install both DCMP and DLS on the same machine, choose the option **DCMP**.



Follow the installation instructions.

4.4.1.2 Installation on a Different Machine

For installation on a different machine, select the option **DCMP** and **Service Startup**.

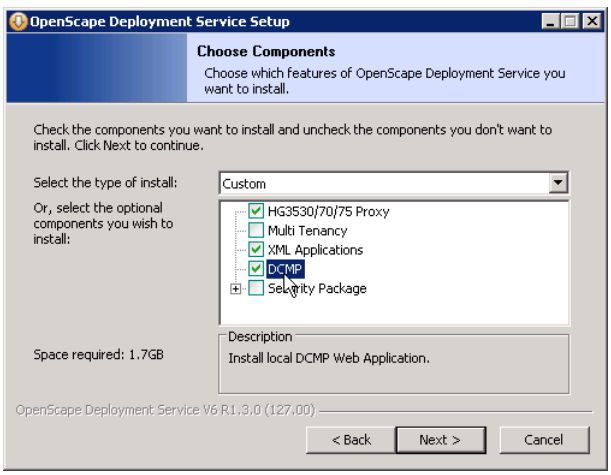


During the installation, you will be asked for the password for the DCMP.

4.4.1.3 Installation on a Multi Node Environment

In the case of a Multi Node environment with 4 nodes (maximum supported ,see Section 4.1.5, "Infrastructure For Cluster Operation")and no DCMP in use,proceed with the following steps:

1. Start the DLS installer over Node 1. DCMP can be added as an option.So when offered to install DCMP select it from the list. This will update the installation configuration file.Run a DLS "upgrade" installation to the same DLS load as already installed on a system just so that you can be offered for the additional modules to be installed.



2. Proceed with a ’’ fake ’’ DLS upgrade over Node 2,3 and 4 in order for the updated installation configuration file located over Node 1 gets acknowledged and as such DCMP is transparently installed over the remaining nodes.

   NOTE: You have to re-run the installer on the second (or further) node(s) for DCMP to be installed, since the installer of the remaining nodes will have to trigger the updated installation configuration file in the common data of the environment (which is resident on the first node), and as such transparently install DCMP over the remaining nodes.

3. Navigate to **https://<IP Address>:10443/dcmp** to login at the DCMP server. Proceed with the DCMP clustering configuration if required (see Section 4.4.2, "Configure DCMP"), and connect to the DCMP via the virtual IP address of the DLS clustering. Proceed with the DCMP clustering configuration if required (and of course within the DLS UI accordingly).

   When the DCMP server is ready, DLS can be configured for DCMP operation.

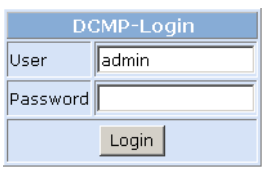
4. In **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**, click the **Toggle DCMP** button to activate the DCMP. A message is displayed that the DCMP server contact is successful. (see Section 4.4.3, "Configure DLS for DCMP")

5. To verify that the job is running, look in **Job Coordination** > **Job Control** and click on the **Search** button. Then click on the specific entry and select the "Object" view. In the **"Basic Data" Tab** you can see that the job will be handled via DCMP.

6. Navigate to **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"DCMP" Tab**. The **DCMP active** switch should be checked, and the settings should be as set for this IP address in **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**.

4.4.2 Configure DCMP

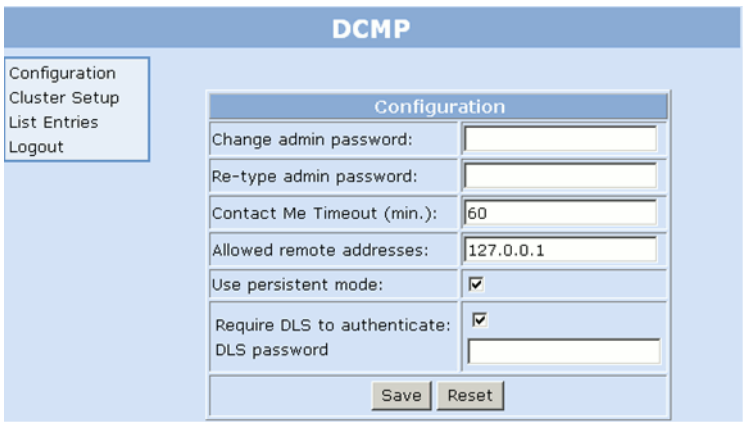
1. With a web browser, navigate to **https://<IP Address>:10443/dcmp** to login at the DCMP server. The user name is **admin**. The password is identical with the admin password for the DLS if the DCMP has been installed along with the DLS. If the DCMP has been installed subsequently, the default password is **Asd123!.**. This should be changed after installation. If the DCMP has been installed on a dedicated server, enter the password you had defined during installation.



2. After login, the initial configuration screen opens up. If desired, you can change the password with **Change admin password** and **Re-type admin password**.

   In the **Allowed remote addresses** field, you enter the addresses of the DLS servers as a comma-separated list, or as a single address, if there is only one DLS server. If the DCMP is installed on the DLS machine, the value is 127.0.0.1.

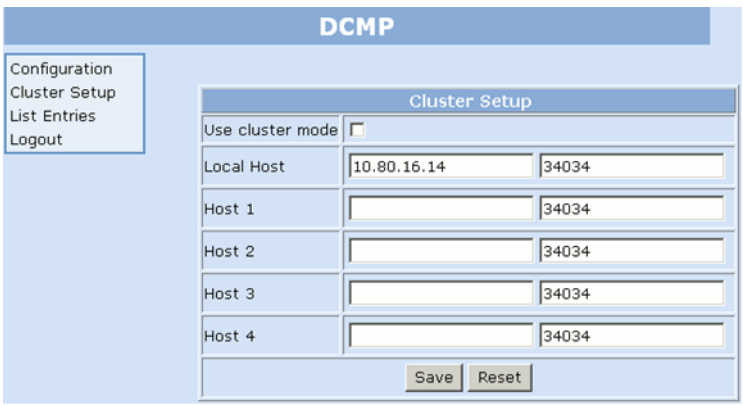
   If **Require DLS to authenticate** is checked, the DLS must authenticate to communicate with the DCMP. For this option, a **DLS password** must be entered; the DLS must present this password to authenticate with the DCMP.



3. In the **Cluster Setup** screen, you can check or configure the appropriate addresses and ports for one or more DLS machines. If a DLS cluster is to be used, check **Use cluster mode**.

   The **Local Host** field contains the IP address of the DCMP server.

   When operating the DLS as a cluster, the IP addresses of each machine in the cluster must be entered in **Host 1 ... 4**.

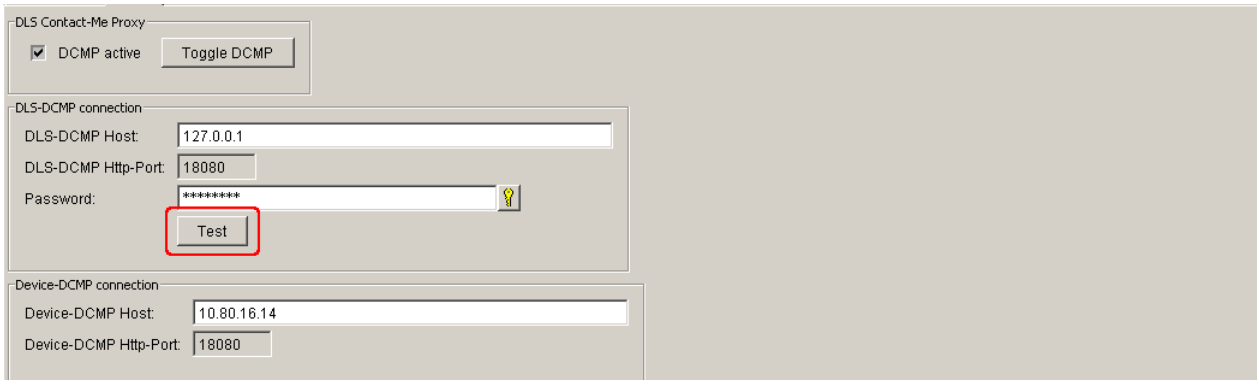


   In the **List Entries** screen, you can view all Contact-Me messages from the DLS.

4.4.3 Configure DLS for DCMP

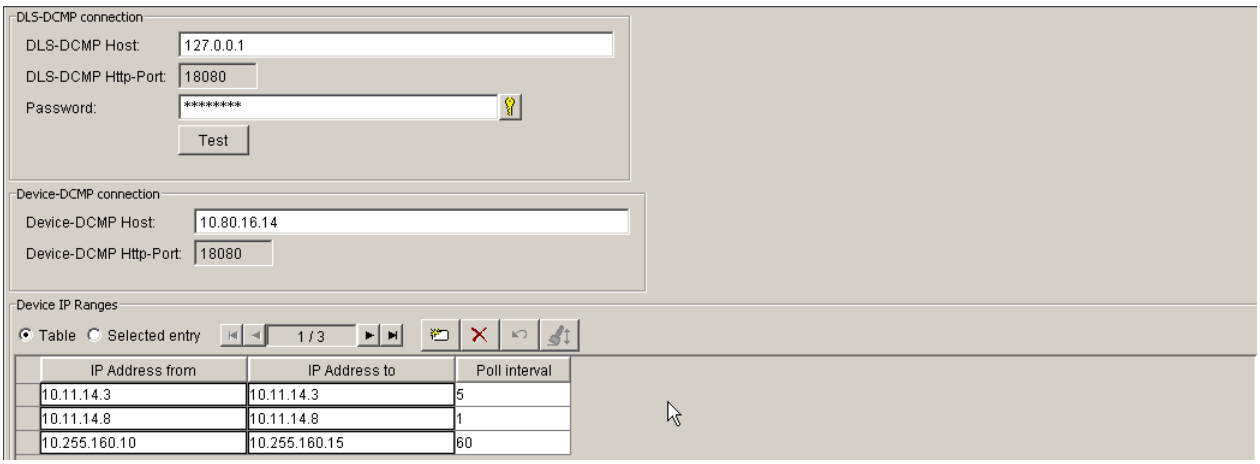
When the DCMP server is ready, the DLS can be configured for DCMP operation.

1. In **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**, click the **Toggle DCMP** button to activate the DCMP.
2. If the DCMP is located on the DLS machine, the IP address of the DCMP server will be shown in **DLS-DCMP Host**; otherwise, it must be entered here.
3. If you have activated the **Require DLS to authenticate** option in the DCMP configuration (see Section 4.4.2, "Configure DCMP"), you must enter the **DLS password** previously defined in the DCMP configuration in the **Password** field.
4. To test communications between DLS and DCMP, click on the **Test** button.



For testing purposes, a very short **Poll interval** can be chosen; however, in a live environment, longer intervals are recommended.

5. Define one or more **Device IP Ranges**. Any IP Devices within the IP ranges defined by **IP address from** and **IP address to** will be updated via DCMP. Hence, whenever a change is made to an IP device within an IP range listed here, the DLS will send a message to the DCMP to set the Contact-Me entry for that phone.

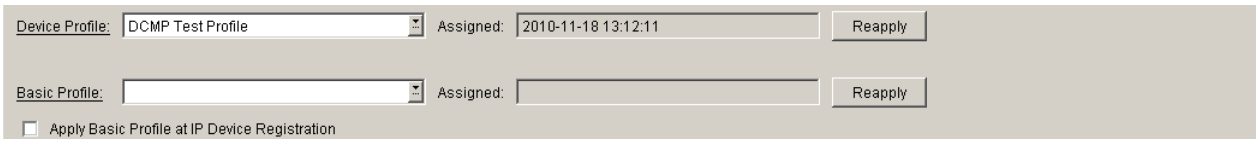


4.4.4 Configure Phone for DCMP

1. The phone should be configured to use passive FTP transfers so it can download software and other data even if it is behind a firewall doing NAT. This is done in **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Miscellaneous** > **"FTP Server" Tab**. As this flag cannot be changed in an already deployed device, it is recommended to create a "DCMP Miscellaneous" template with this flag set and use that template in the profile for DCMP users.



2. Navigate to **Profile Management** > **Device Profile** and create a device profile using the newly created "DCMP Miscellaneous" template.
3. Navigate to **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration**. Use the **Search** function, the "Table" view, and the "Object" view to select the subscriber number for the phone to be configured. In the **"Profile" Tab**, select the profile you just created, and assign it to the phone.



4.4.4.1 Configure Home User Devices for DLS / DCMP

DCMP is developed for cases that DLS cannot communicate with devices.

In the case of DLS communication with Home / Office User Devices, DLS can see the IP address of the device but this IP address is actually the public IP address assigned to each user modem/router. Once DLS tries to pass a configuration change to this IP address, this change will never pass to the device behind the modem/router and this is where DHCP is used. Once the DCMP is active and the IP range is included in the DCMP configuration, phones included in this range enter in DCMP mode.

1. DLS requests a change from a phone that is in DCMP mode
2. The above request goes to DCMP instead of the device directly.
3. The device contacts DCMP in the configured interval and receives the request that DLS has changes for this device.
4. The device contacts DLS to request the available changes.

In order to be able to administer home user devices, the machine that will be used for DLS and DCMP shall have 2 network interfaces. One will get the internal IP and the other one the external one. In order to achieve this,two IP addresses have been configured,one as internal for intra network devices (172.x.x.x) and one external where only the required ports were opened in the Firewall.

The ports that were opened in the Firewall were DLS port 18443, which is the default port that devices communicate with DLS and the FTP port 21 for device Firmware upgrades (Communication between the DLS server and DLS client is set up using the port number 18080).

The configuration order is as follows:

- Install DCMP in the same server as DLS
- Completed configuration as described in the DLS documentation (section 4.4, " Configure Phone for DCMP ")
- Configured network firewall for the required ports 18443,18080 and 21.

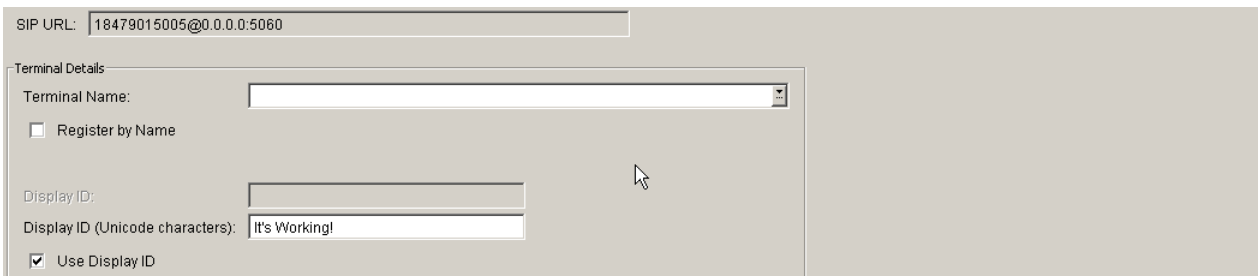
IMPORTANT: The supported IP clients - ODC (WE/PE/FC) don’t support DCMP. Therefore IP Clients are not supported for a DCMP integration.

4.4.5 Test DCMP

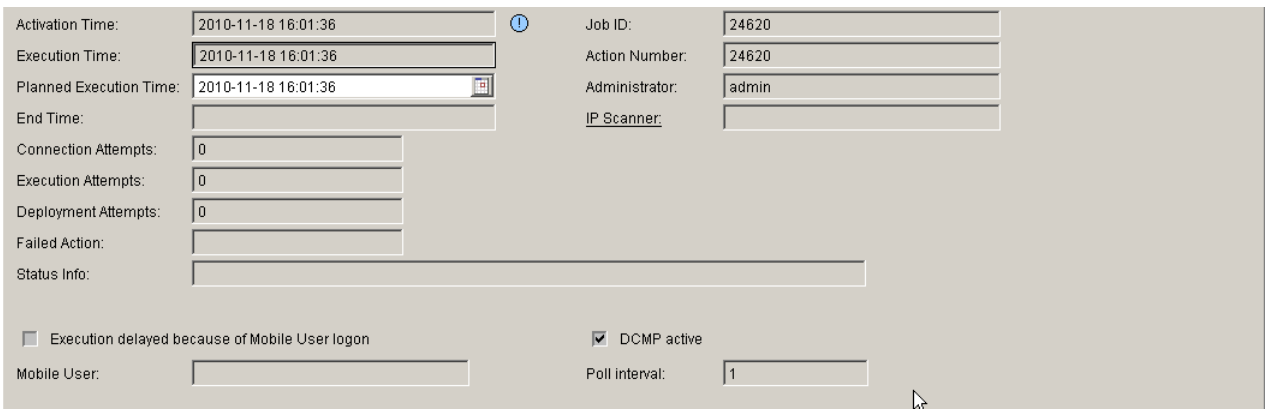
1. First, choose a phone that has an IP address within an IP range configured for DCMP operation (see Section 4.4.3, "Configure DLS for DCMP") and perform a factory default on that phone.
2. When the phone has rebooted, give it the subscriber number you just assigned the DCMP Profile to.
3. Navigate to **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"DCMP" Tab**. The **DCMP active** switch should be checked, and the settings should be as set for this IP address in **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**.



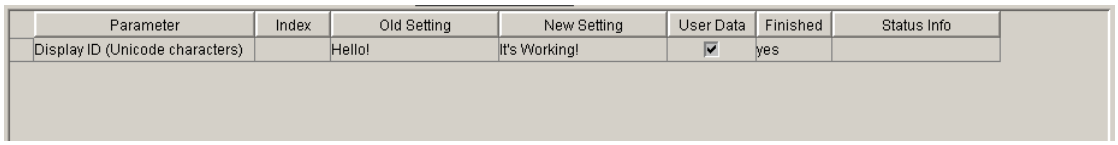
4. As a test case for a configuration change, modify the display name on the phone. Navigate to **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Gateway/Server** > **"SIP Terminal Settings" Tab**. Activate **Use Display ID** (or **Use Display ID (Unicode characters)**) and set the **Display ID** to "It's Working!", for instance. Save the change in DLS.



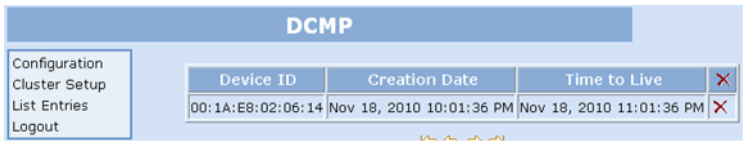
5. To verify that the job is running, look in **Job Coordination** > **Job Control** and click on the **Search** button. Then click on the specific entry and select the "Object" view. In the **"Basic Data" Tab** you can see that the job will be handled via DCMP.



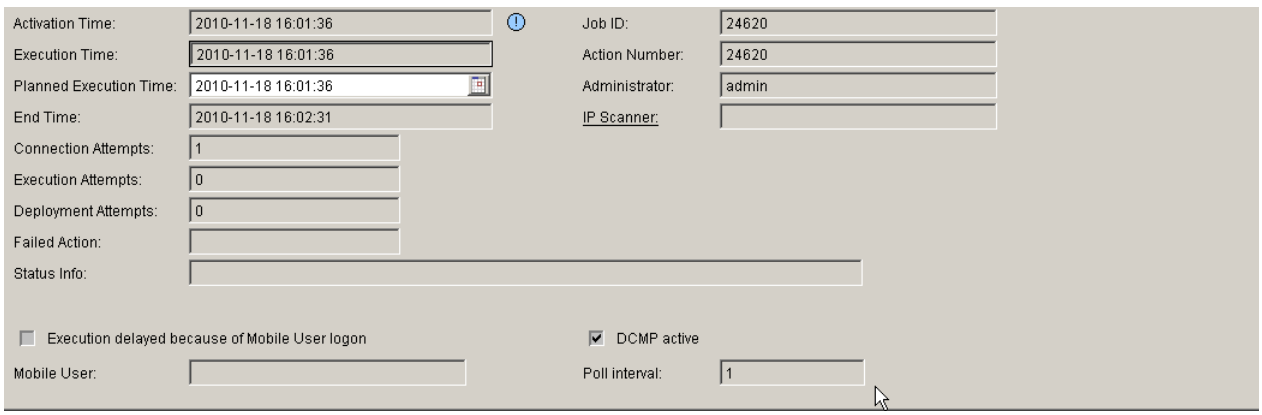
6. In the **"Configuration Data" Tab** you can see the specific change that was requested.



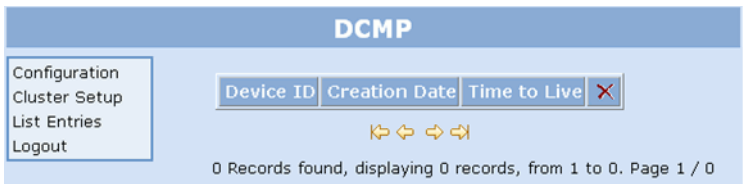
7. In the DCMP GUI, click on the **List Entries** menu. You should see the Contact Me setting in the list. The **Device ID** should be the MAC address of the phone.



8. In the DLS GUI, in **Job Coordination** > **Job Control** > **"Basic Data" Tab**, you will see an "End Time" once the change is made.



9. In the DCMP GUI, you will see the Contact Me entry is removed.



The test is finished.

4.5 Installing the DLS

4.5.1 Single Node Operation with Local Database

This is the standard DLS installation. Thus, follow the instructions of the installation assistant.

4.5.1.1 Install Microsoft .NET v3.51 / v4

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/How_to_Install_Microsoft_.NET

4.5.1.2 Install DLS

Follow the instructions of the OpenScape Deployment Service Setup Wizard contained in the DLS software package.

IMPORTANT: Do NOT install a hotfix directly. Instead first install the base version of the hotfix and then upgrade to the hotfix (e.g. the base version of **V7R2 408.05** is the **V7R2 408.00**).

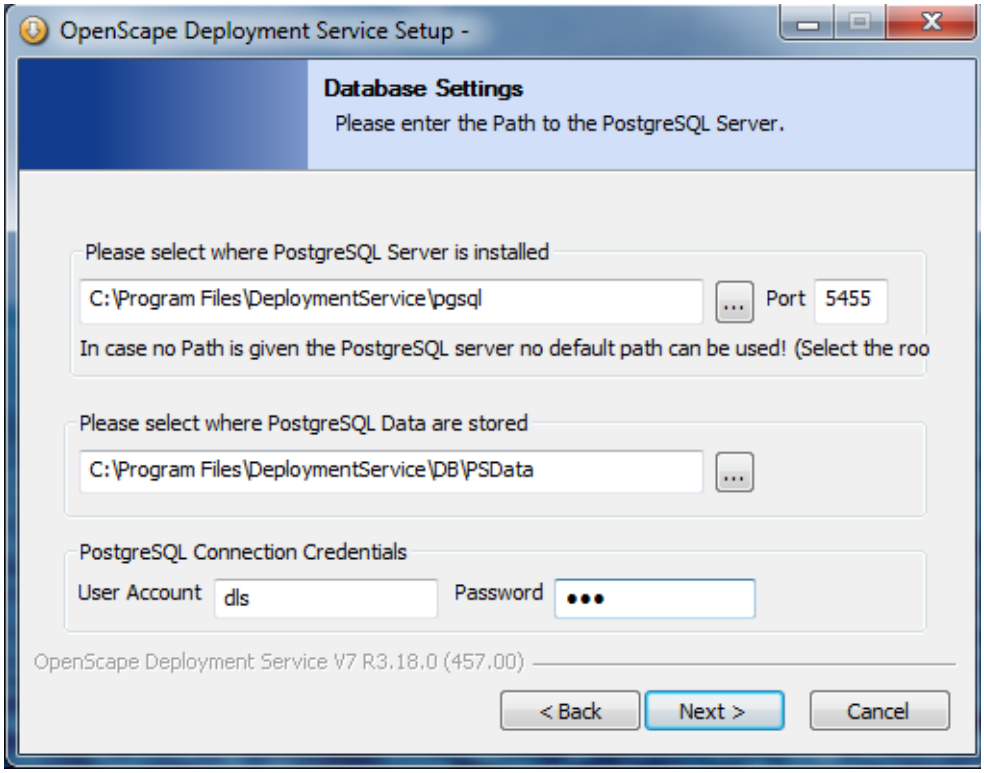
NOTE: Hotfixes deliver the complete DLS package & they're also cumulative, e.g **CV408.03** contains all the fixes delivered in **CV408.01** & **CV408.02**.

IMPORTANT: Single-node DLS with local database is installed with PostgreSQL. Visual C++ Redistributable Packages for Visual Studio 2015 is a prerequisite.

IMPORTANT: As a prerequisite, refer to the **Visual C++ Redistributable Packages 2015** under:
https://www.microsoft.com/en-us/download/details.aspx?id=48145
The Visual C++ Redistributable Packages install run-time components that are required to run C++ applications that are built by using Visual Studio 2015. Choose the version you wish to install (32/ 64 bit).

Proceed with the following:

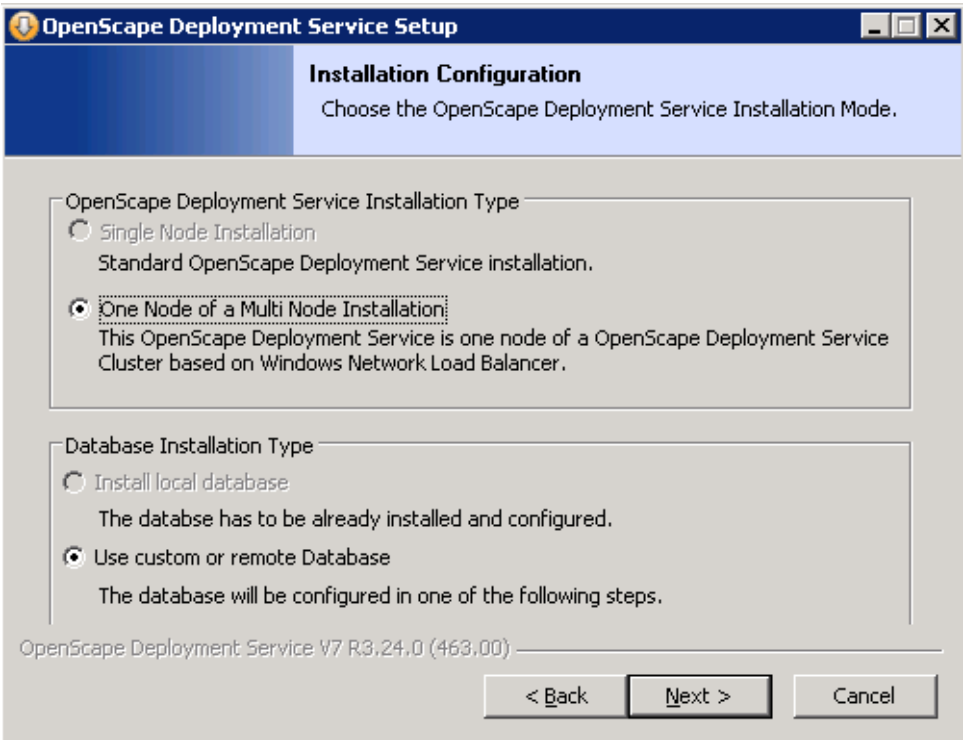
1. DLS fresh installation shall proceed as usual.The installer wizard will install PostgreSQL as well.
2. Install PostgreSQL. Proceed with the User Account & Password credentials.**5455** is the default port value although you may configure your preferred port.


OpenScape Deployment Service Setup -
Database Settings
Please enter the Path to the PostgreSQL Server.
Please select where PostgreSQL Server is installed
C:\Program Files\DeploymentService\pgsql
...
Port
5455
In case no Path is given the PostgreSQL server no default path can be used! (Select the roo
Please select where PostgreSQL Data are stored
C:\Program Files\DeploymentService\DB\PSData
...
PostgreSQL Connection Credentials
User Account
dls
Password
OpenScape Deployment Service V7 R3.18.0 (457.00)
< Back
Next >
Cancel

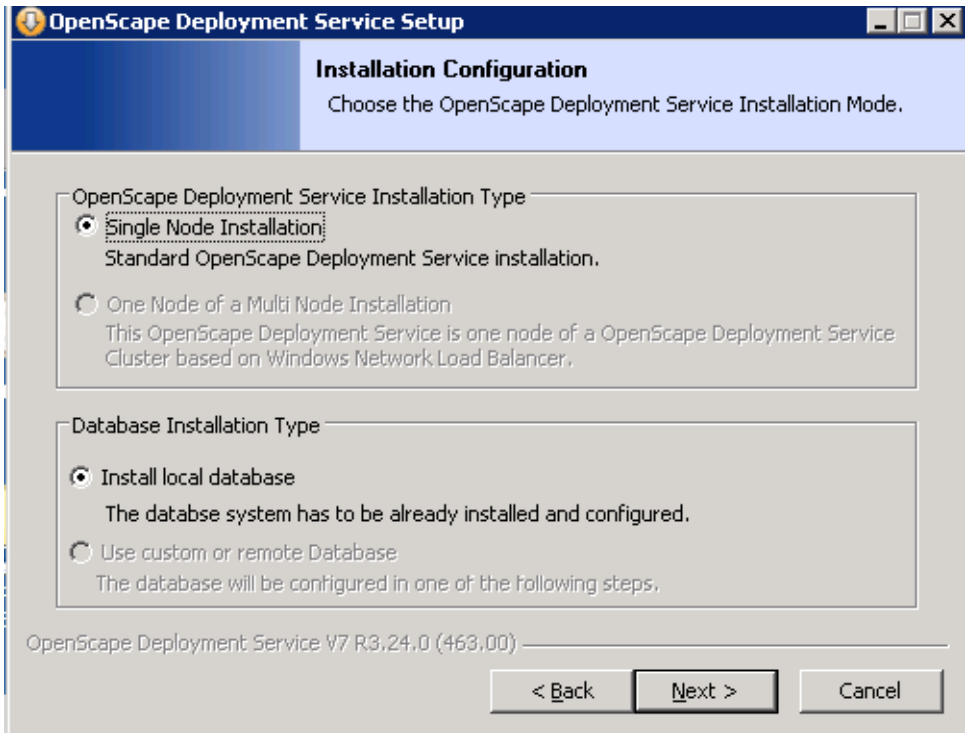
4.5.1.3 Installation Scenarios

In the case of a DLS new installation, the following options should be available on each of the scenarios below:

1. The fresh installation of Single Node using MSSQL installer is not possible (the "Single Node Installation" and "Install Local Database" options are disabled).

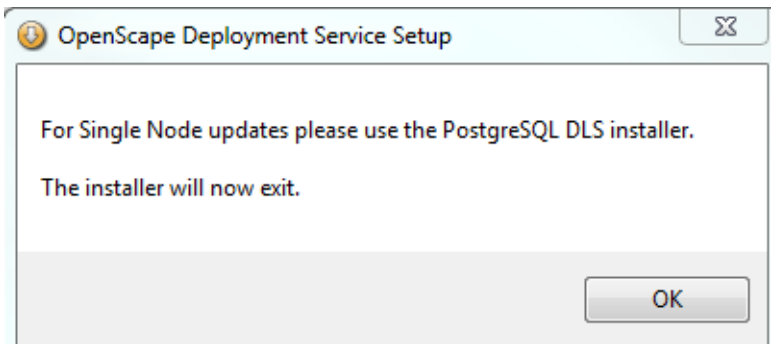


2. The fresh installation of Multi Node using PostgreSQL installer is not possible (not supported, options are disabled).

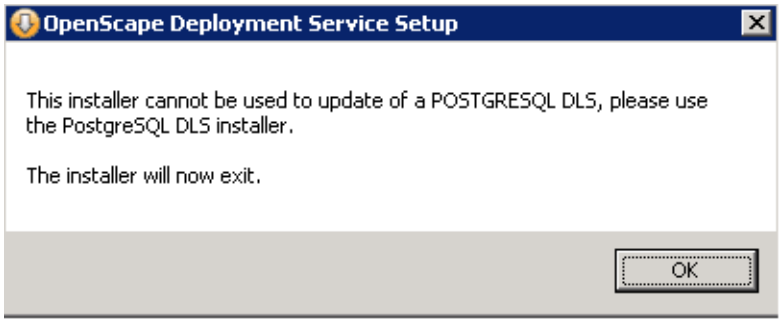


In the case of a DLS update installation, the following messages appear for each of the scenarios below:

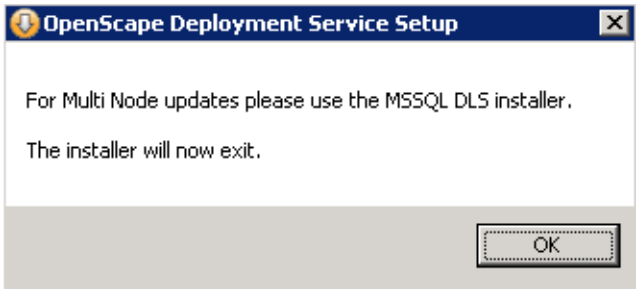
1. Update of a MSSQL Single Node using MSSQL installer (should be blocked)



2. Update of a PostgreSQL Singlenode using MSSQL installer (should be blocked)



3. Update of a MSSQL multinode using postgreSQL installer (should be blocked)



4.5.2 Multi-Node Operation with Remote or Custom Specific Database

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/Multi-Node_Operation_with_Remote_or_Custom_Specific_Database

4.5.3 Multi-Node Operation

The following example demonstrates the installation of two DLS nodes with mirrored SQL database.

NOTE: The first installation as well as the update installation must not be carried out on more than one nodes at a time, as the nodes access common files. Therefore, install the nodes one after another.

IMPORTANT: Microsoft .NET v3.51 must be installed in both Nodes first, in order for RapidStat to operate (please refer to Section 4.5.1.1, "Install Microsoft .NET v3.51 / v4")

4.5.3.1 First Node

Login to the node by using 'dls' account that was created previously during Multi-Node SQL installation for DLS access.

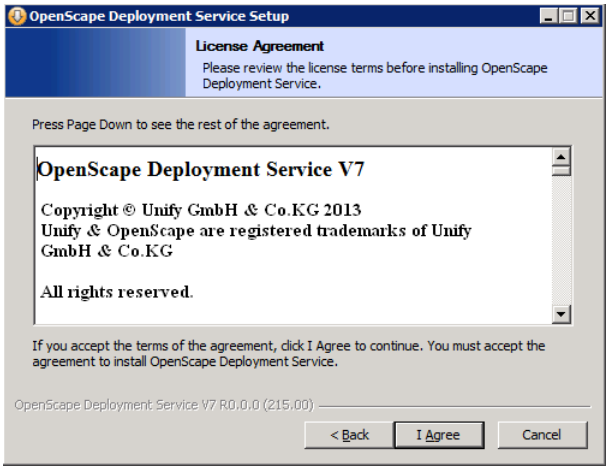
NOTE: SQL Native Client should be installed first, manually.It's version should be that of the installed remote SQL server. Backward compatibility is not assumed. It is not installed by DLS automatically. If the native client is not installed,Step 6 will come up with an error message about connectivity to SQL server.

1. Start the setup program. After selecting the language, you see a welcome screen.

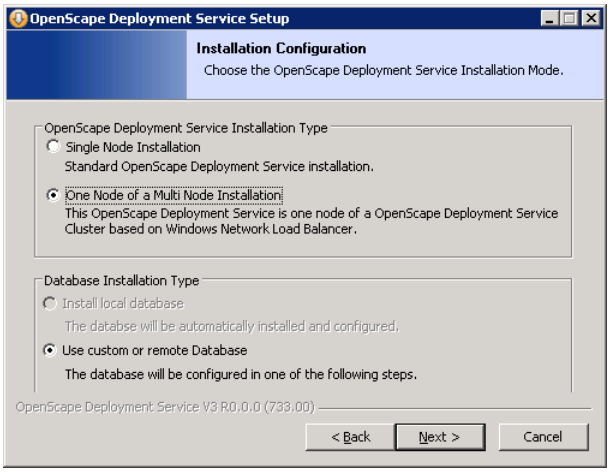


   Click on **Next**.

2. Click on **I Agree** to accept the license agreement.


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

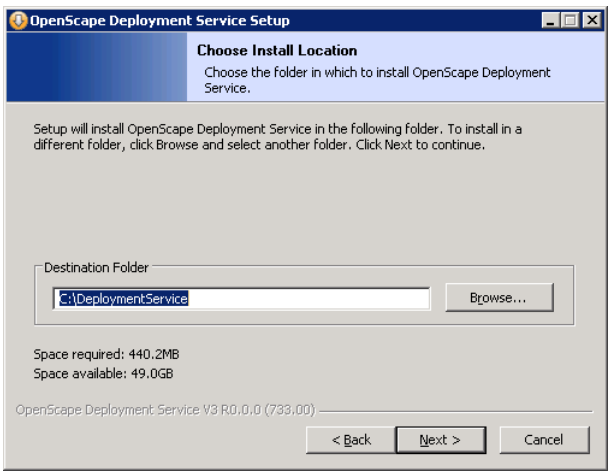
3. In the **Installation Configuration** screen, under **DLS Installation Type**, select the option **One Node of a Multinode Installation**.



Click on **Next**.

4. In the **Choose Install Location** screen, choose the target directory in which the DLS shall be installed.

NOTE: The directory path must not contain blanks, as in "Program Files", for instance.



Click on **Next**.

5. In the **Default Data Path** screen, enter the path of a directory, to which all nodes must have access. Here, configuration data common to all DLS nodes are stored. This directory must exist, and writing access for this directory must be granted to the DLS, also for installation purposes. The IP address must be that of the Witness SQL server. In case there is no Witness server then it is recommended to be at a different server (i.e. File Server) on the same domain. The least recommended is to have the Default Data Path could be in Node1.

   NOTE: In case a notification window appears here, asking whether another node shall be installed, in addition to existing ones, click on "No". The notification window will appear if the file `common_dls.properties` exists in the specified directory.

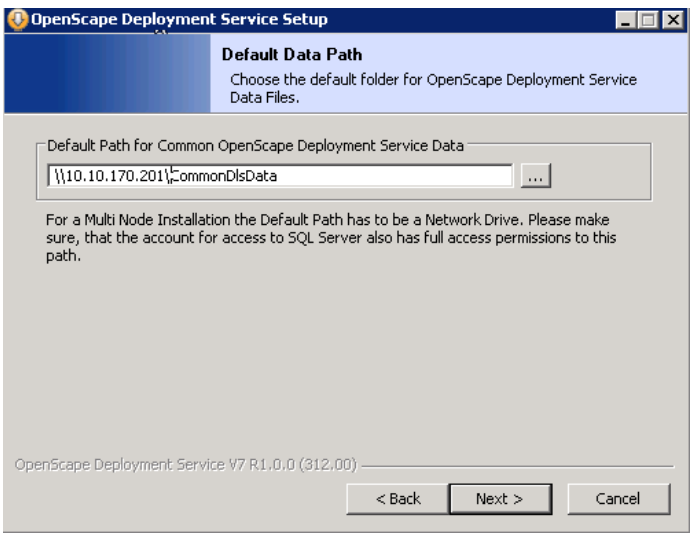
   NOTE: To avoid any kind of problems with backup/restore actions when DLS Node 1 is down/unreachable for any reason, you need to modify the default path for common Openscape Deployment Service Data to be on different server (i.e. File Server), on the same domain like the rest of the Multinode servers i.e.
   `\\POSTM3-FileServer\MultinodeShare\CommonDlsData`

   or

   `\\10.10.170.100\MultinodeShare\CommonDlsData`

   NOTE: CommonDLSData should be in the witness server if one exists (in the case of synchronous mirroring). If a witness doesn't exist then the folder should be located on an external server other that that of CLA. Any other option could obstruct multinode migration scenarios (see Section 16.20, "Migration Scenarios") with minimum outage.

   IMPORTANT: The Common Data Path should not be used to store files outside the scope of DLS's own node clustering purposes and DLS administrative tasks (e.g. csv/ archive exports, Profile/Template exports etc).



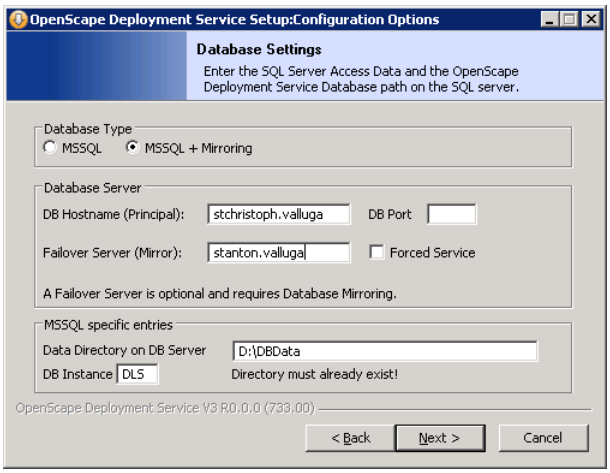
   Click on **Next**.

6. In the **Database Settings** screen provide the necessary specifications for the database. If you wish to deploy a mirrored database for maximum reliability, select the option **MSSQL + Mirroring** under **Database Type**. Under **Database Server**, in the field **DB Hostname (Principal)**, specify the "Principal" database server, and in the field **Failover Server (Mirror)**, specify the backup database server, which will fill in in case the Principal fails.

   Under **MSSQL specific entries**, in the field **Data Directory on Server**, enter the directory on the database server in which the DLS database is located. This directory must exist already. It should have been created before theSQL server installation (see Section 4.2, "Install MS SQL Server for Multi-Node DLS", step 2).

   NOTE: It is recommended to use the same directory path both on the Mirror and on the Principal.

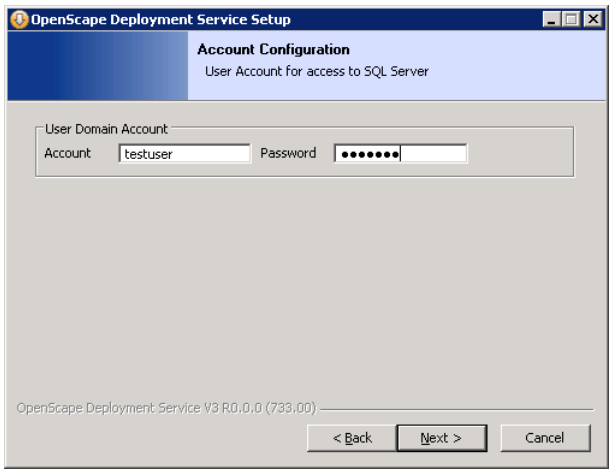
   Under **DB Instance**, enter the instance under which the DLS database is to operate (see Section 4.2, "Install MS SQL Server for Multi-Node DLS", step 4 resp. Section 4.2.1, "How to install Microsoft SQL Server", step 9).



   Click on **Next**.

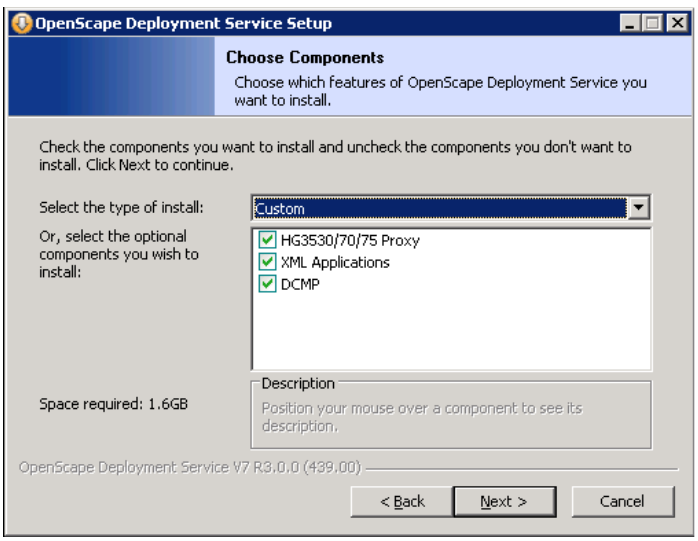
7. In the **Account Configuration** screen, in the fields **Account** and **Password**, enter the access data of the user the DLS shall run under. The user must be a member of the administrator group, and it must exist already.

   NOTE: In case of a DLS installation in DNS environment you have to enter the full FQDN account i.e., testuser@multinode.local or multimode.local\testuser. If you use plain "testuser" it denotes a local machine (**Workgroup** environment) user and not a domain user.



   Click on **Next**.

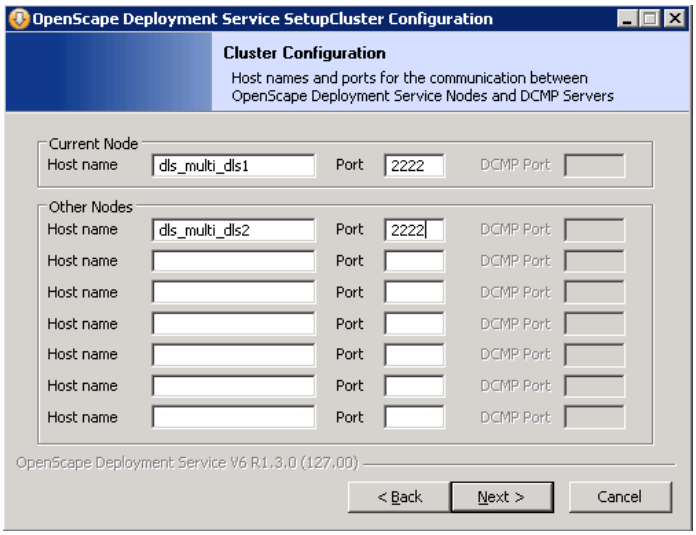
8. Now, in the **Choose Components** screen, select the desired DLS components.



   Click on **Next**.

9. In the **Cluster Configuration** screen, under **Current Node**, you see the node machine on which you are currently installing the DLS. Under **Other Nodes**, in the **Host Name** fields, enter the names of the corresponding node machines, and in the **Port** fields, enter the port used by the DLS running on the corresponding machine for communication with the other nodes. If you have selected the DCMP in step 8, you must specify the port on which the DLS receives data from the DCMP in the field **DCMP-Port**.

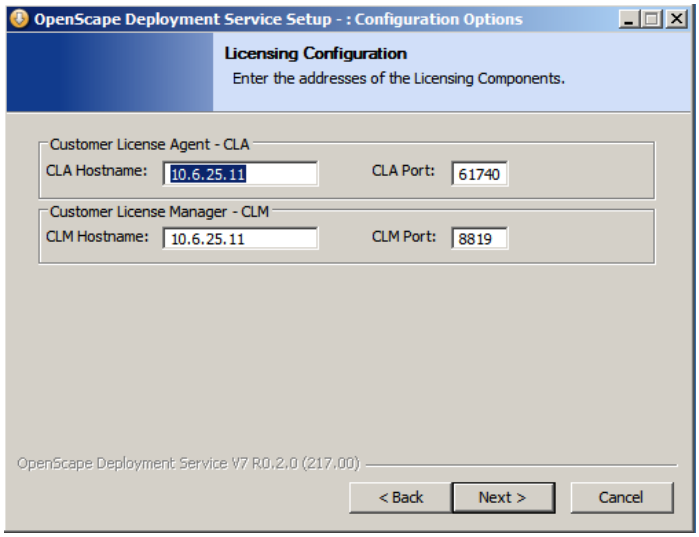
   NOTE: In case of a workgroup or DNS with no FQDN orientation,an IP address will be added instead.



   Click on **Next**.

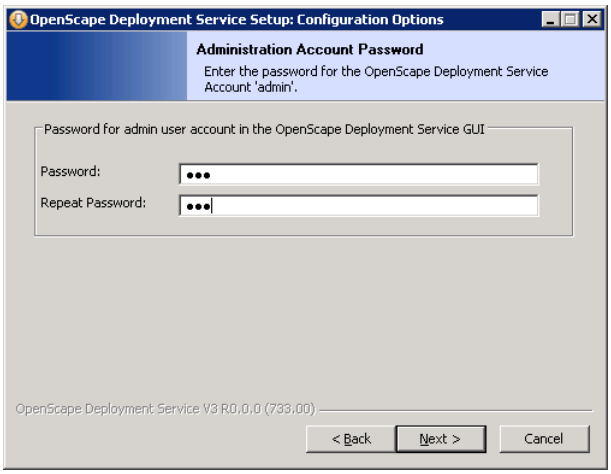
10. In the **Licensing Configuration** field, you provide the specifications required for licensing. Under **Customer License Agent - CLA**, in the field **CLA Hostname**, you enter the IP address of the CLA server, and in the field **CLA Port**, you enter the corresponding port. Under **Customer License Manager - CLM**, in the field **CLM Hostname**, enter the IP address of the CLM server, and in the field **CLM Port**, you enter the corresponding port.

    NOTE: CLA and CommonDLSData folders should be located on different servers. In any other option, Mirroring is not possible and could also obstruct multinode migration scenarios (see Section 16.20, "Migration Scenarios") with minimum outage.



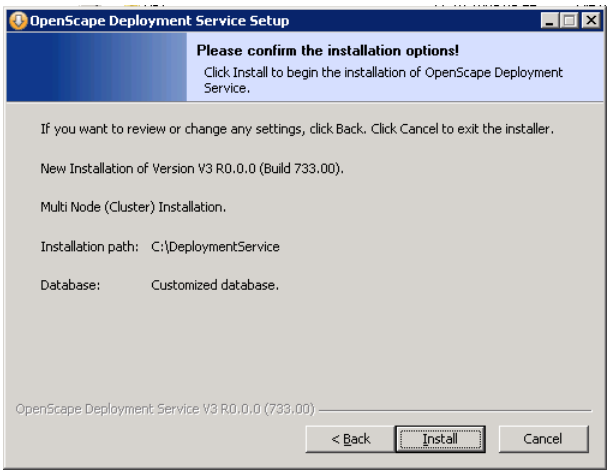
Click on **Next**.

11. In the **Administration Account Password** screen, in the fields **Password**/**Repeat Password**, enter the password for the DLS user "admin".

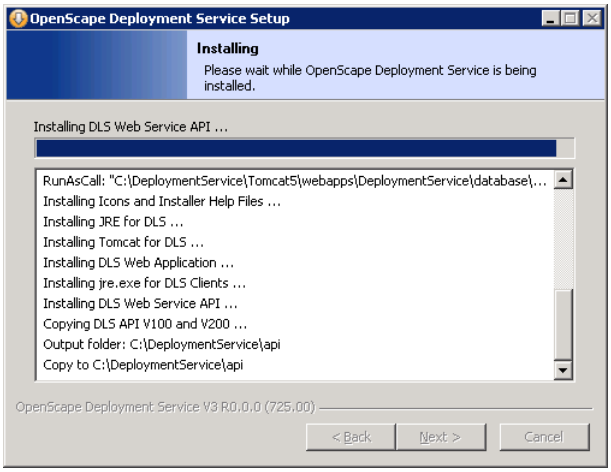


Click on **Next**.

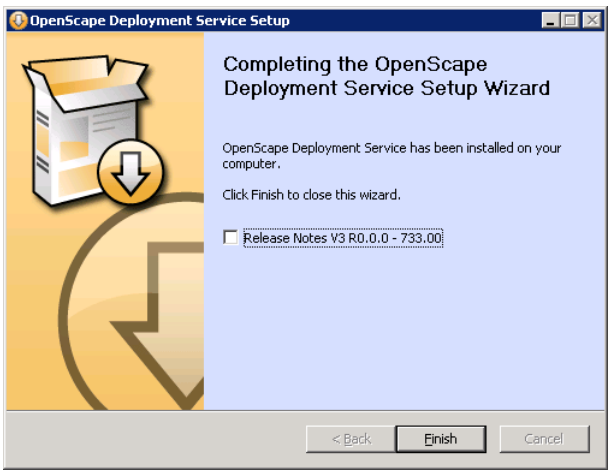
12. In the next screen, you see a brief overview on the installation settings. To start the installation, click on **Install**; to revise settings, click on **Back**.


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

13. If you have clicked on **Install** previously, you will be presented with messages about the installation process.



14. The installation is complete.



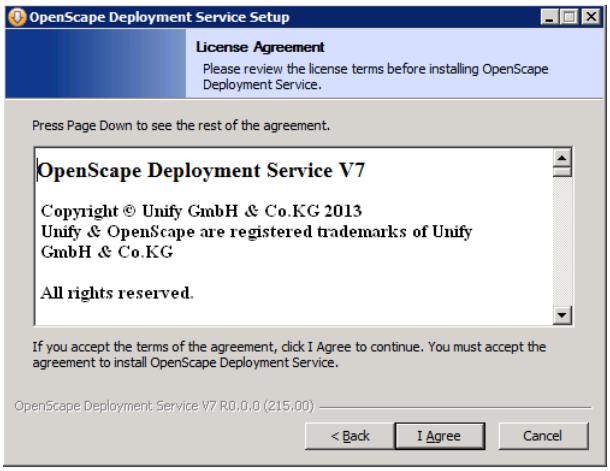
4.5.3.2 Second And Further Nodes

1. Start the setup program. After selecting the language, you see a welcome screen.

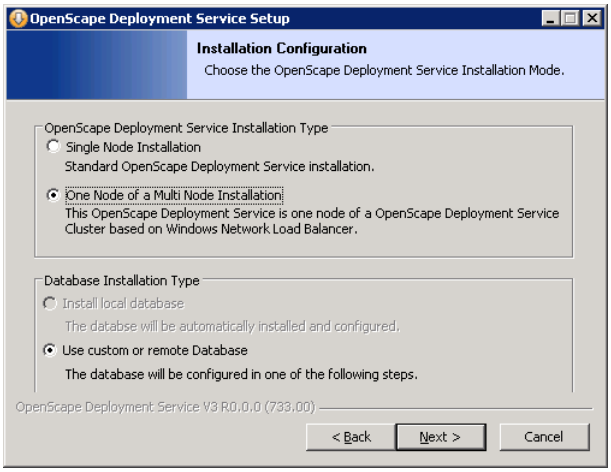


   Click on **Next**.

2. Click **I Agree** to accept the license agreement.



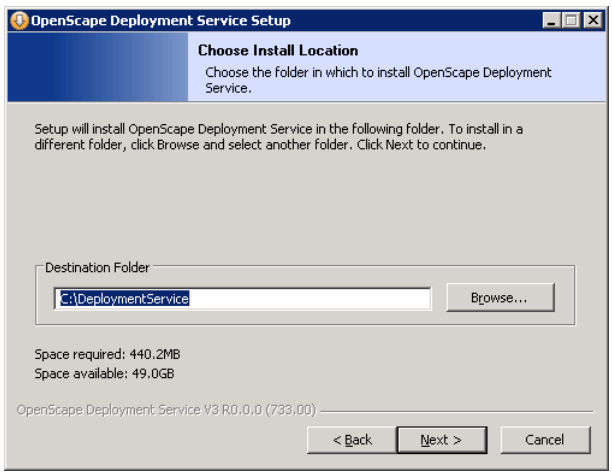
3. In the **Installation Configuration** screen, under **DLS Installation Type**, select the option **One Node of a Multinode Installation**.



Click on **Next**.

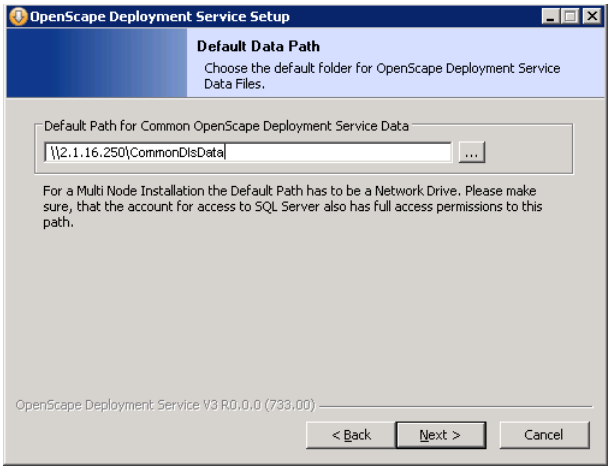
4. In the **Choose Install Location** screen, choose the target directory, wherein the DLS is to be be installed.

NOTE: The directory path must not contain blanks, as in "Program Files", for instance.



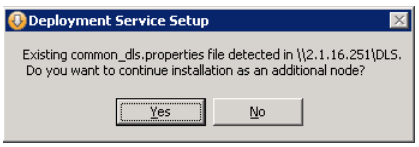
Click on **Next**.

5. In the **Default Data Path** screen, specify the path of the directory for common DLS configuration data. This path has been specified in Section 4.5.3.1, "First Node", step 5.



Click on **Next**.

6. As the first DLS node is already installed and has stored the file `common_dls.properties` in the appropriate directory, you will be presented with a notification:



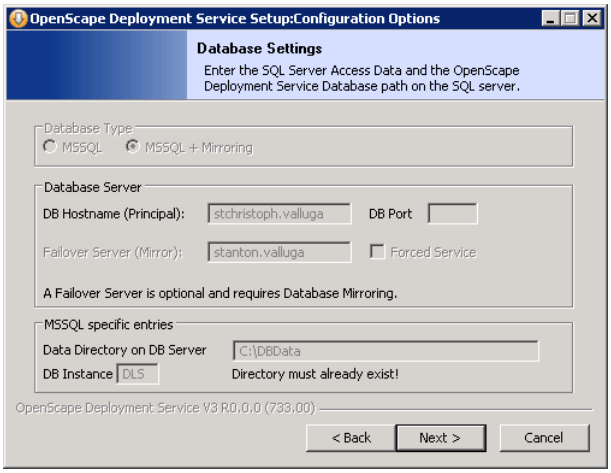
Click on **Yes**.

7. In the **Database Settings** screen provide the necessary specifications for the database. If you wish to deploy a mirrored database for maximum reliability, select the option **MSSQL + Mirroring** under **Database type**.

   Under **MSSQL specific entries**, in the field **Data Directory on Server**, enter the directory on the database server, in which the DLS database resides. This directory must exist already. It should have been created before the SQL Server installation.

   NOTE: It is recommended to use the same directory path both on the Mirror and on the Principal Server.

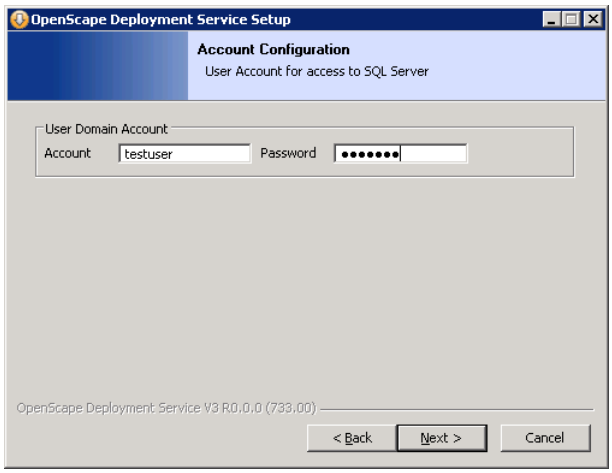
   Under **DB Instance**, enter the instance under which the DLS database is to operate.



   Click on **Next**.

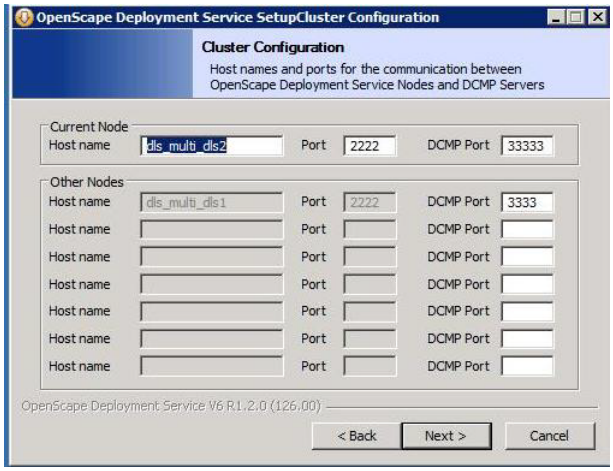
8. In the **Account Configuration** screen, in the fields **Account** and **Password**, enter the access data of the user the DLS shall run under. The user must be a member of the administrator group, and it must exist already.

   NOTE: In case of a DLS installation in DNS environment you have to enter the full FQDN account i.e., testuser@multinode.local or multimode.local\testuser. If you use plain “testuser” it denotes a local machine (**Workgroup** environment) user and not a domain user.



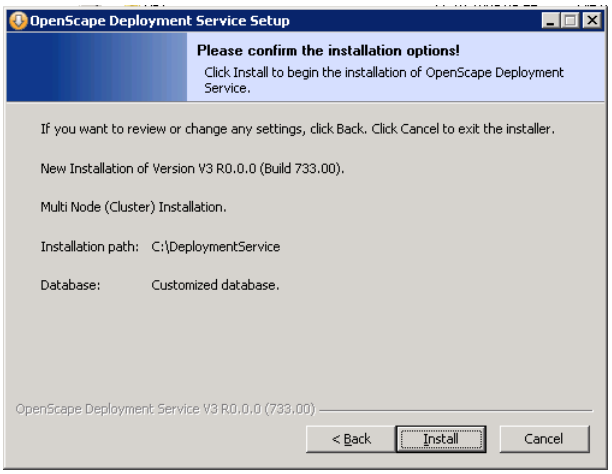
Click on **Next**.

9. In the **Cluster Configuration** screen, under **Current Node**, you see the node machine on which you are currently installing the DLS. Under **Other Nodes**, in the **Host name** fields, enter the names of the corresponding node machines, and in the **Port** fields, enter the port used by the DLS running on the corresponding machine for communication with the other nodes. If you have selected the DCMP in step 8, you must specify the port on which the DLS receives data from the DCMP in the field **DCMP-Port**. If the data have already been input at the first node, they can be checked, modified, or extended once more.

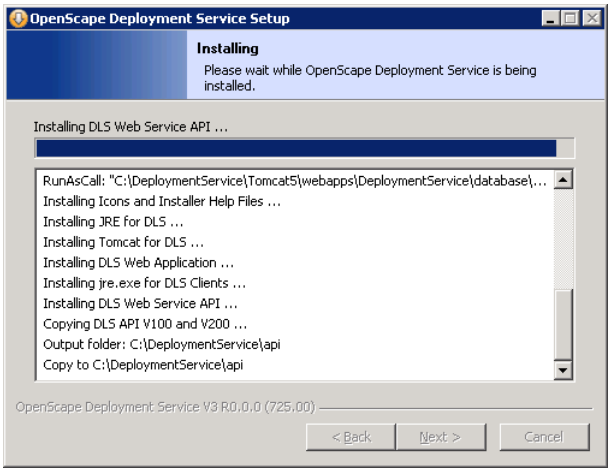


Click on **Next**.

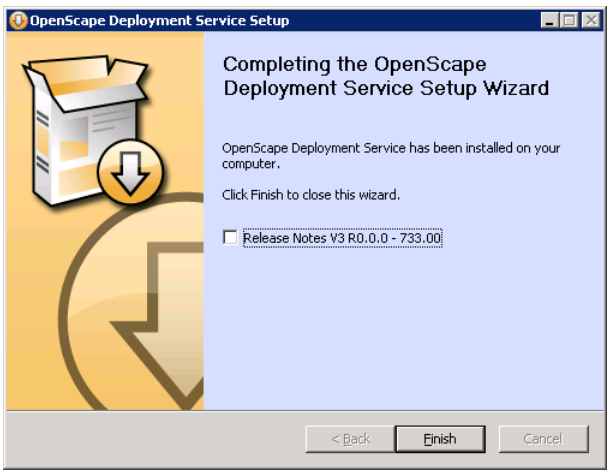
10. In the next screen, you see a brief overview on the installation settings. To start the installation, click on **Install**; to revise settings, click on **Back**.



11. If you have clicked on **Install** previously, you will be presented with messages about the installation process.



12. The installation is complete.



4.5.3.3 Installation of DLS Nodes with existing DLS Database

If the DLS nodes have to be installed again (no upgrade), but a DLS database still exists on the SQL server,

- stop database mirroring on SQL server Principal by means of "MS SQL Management Studio",
- remove the DLS database on Principal and Mirror,
- remove the Stored Procedures assigned by DLS on Principal and Mirror,
- install first node again and restore last available backup,
- install all additional nodes,
- set up mirroring following the instructions in Section 4.6, "SQL Database Mirroring Setup", except the SQL statements for configuring endpoints.

4.6 SQL Database Mirroring Setup

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/How_to_setup_a_synchronously_Mirrored_Database

4.7 DLS Database Restore in a Multi-Node environment

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/DLS_Database_Restore_in_a_Multi-Node_environment

4.8 Upgrading a DLS Multi-Node Environment

Please refer to the **Unify Experts Wiki Portal** under:
http://wiki.unify.com/wiki/Upgrading_a_DLS_Multi-Node_Environment

4.9 Start DLS

Before you start the DLS, please ensure that the system time is synchronous on all machines. This will be the case if the DNS server included in Windows 2003 Server is used, as the time is provided here. In case you use a workgroup instead of this DNS server, you must guarantee synchronizity by other means.

1. Start the DLS on each node.
2. Start the cluster by means of the Network Load Balancer Manager.

   NOTE: If you wish to shut down a DLS node, perhaps for maintenance purposes, first remove the machine using the Network Load Balancer Manager. Thus, it is granted that this DLS instance will not receive requests any more.

4.10 Initial Configuration

For initial DLS configuration, we recommend configuring the following areas one after the other:

1. **Change Password/Configure Account**

   Call: Main Menu > Administration > Account Management > Account Configuration

   If necessary, change the admin password that has been set during installation and configure new accounts, if necessary.

   You can find a description of the fields in Section 6.1, "Account Management".

2. **Configure FTP Server**

   Call: Main Menu > Administration > Server Configuration > FTP Server Configuration

   Enter the data for the connection to one or more FTP servers.

   You must connect to an FTP server in order to download IP phone software.

   You can find a description of the fields and additional information in Section 6.3.4, "FTP Server Configuration".

3. **Configure HTTP Server**

   Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration

   Enter the data for the connection to one or more HTTPS servers.

   OpenStage terminals can use an HTTPS server instead of an FTP server for downloading IP phone software.

   You can find a description of the fields and additional information in Section 6.3.5, "HTTPS Server Configuration".

4. **Windows Network Drive Configuration**

   Call: Main Menu > Administration > Server Configuration > Network Drive Configuration

   Enter the data for the Windows network drive.

   The specifications for the Windows network drive are needed for downloading IP client software.

   You can find a description of the fields and additional information in Section 6.3.7, "Network Drive Configuration".

5. **Settings (Logging)**

   Call: Main Menu > Administration > Display Logging Data > Activity and Error Log OR > P&P Import Protocols

   If necessary, change the information on which events should be logged and how long log data should be saved.

   You can find a description of the fields and additional information in Section 6.5, "Display Logging Data".

6. **Import Templates**

   Call: Main Menu > Profile Management > Template Overview > "Template data" Tab

   You have the option to load existing DLS templates stored in ZIP files.

   Please refer to Section 15.7, "Editing Templates" for more information on templates.

7. **Element Manager**

   Call: Main Menu > Element Manager > Element Manager Configuration

   Select the element manager type you want to configure under **Element Manager type**. For configuration options, see Section , "Element Manager".

4.11 Starting the DLS Client

4.11.1 Starting the Client

Before you start the DLS, you should have completed initial configuration (see Section 4.10, "Initial Configuration").

Start the DLS client as follows:

- On the server computer:
  - Using the Windows Start menu **Start** > **Programs** > **Deployment Service** > **DeploymentService**.
  - Using the **DeploymentService** program shortcut on the desktop.
- On the client computer:
  - By entering the following URL in the Web browser:
    https://[IP address]:10443/DeploymentService/ (for an encrypted connection)

You can find information on operating the DLS client from Chapter 5 onwards.

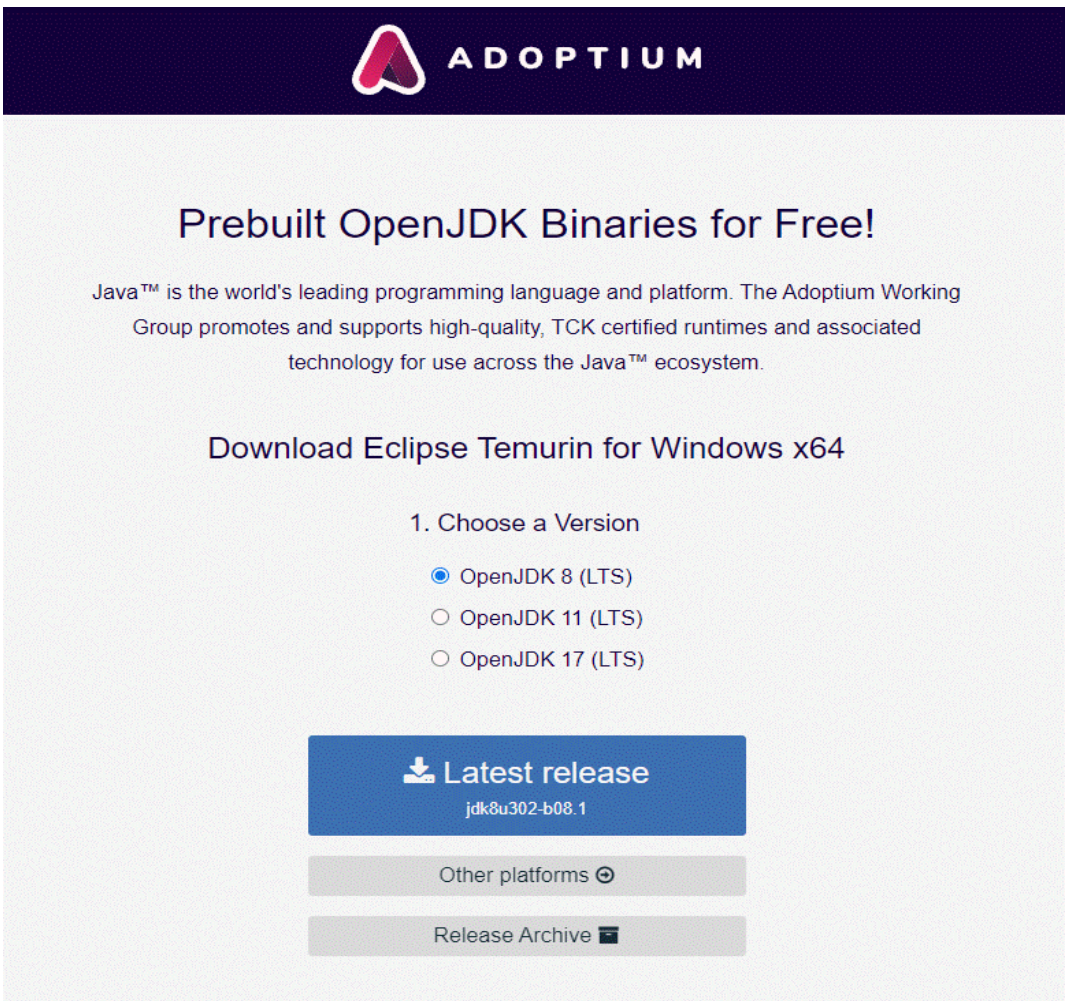
4.11.2 Starting the Client with OpenWebStart and Adoptium OpenJDK

DLS V10R2 supports OpenWebStart for DLS UI access in the client. This requires Adoptium OpenJDK V8 to be installed in the client as a replacement of the Oracle JRE.

4.11.2.1 Downloads and Installations

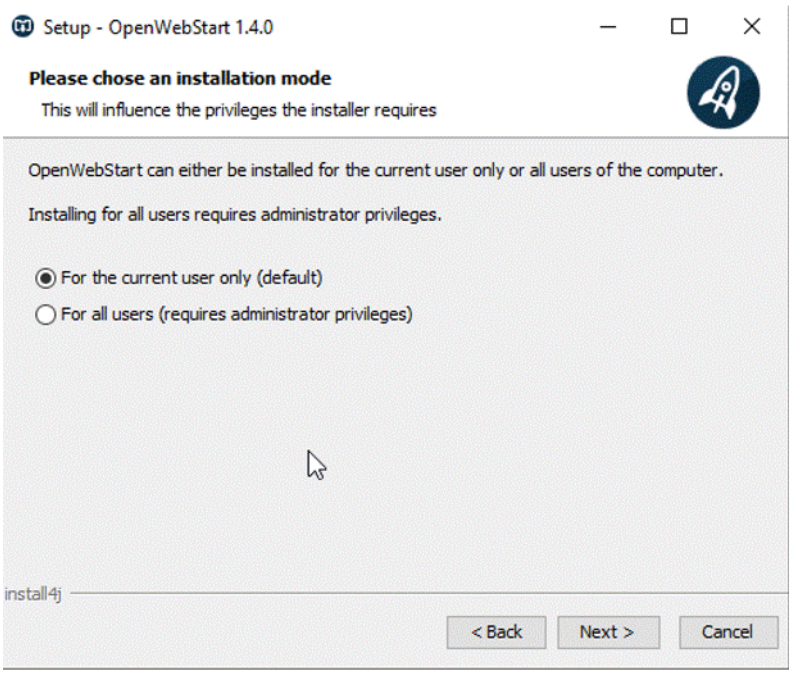
1. Download and install in the client PC the latest v.8 (Hotspot JVM) Adoptium OpenJDK for Windows from

https://adoptium.net/?variant=openjdk8&jvmVariant=hotspot

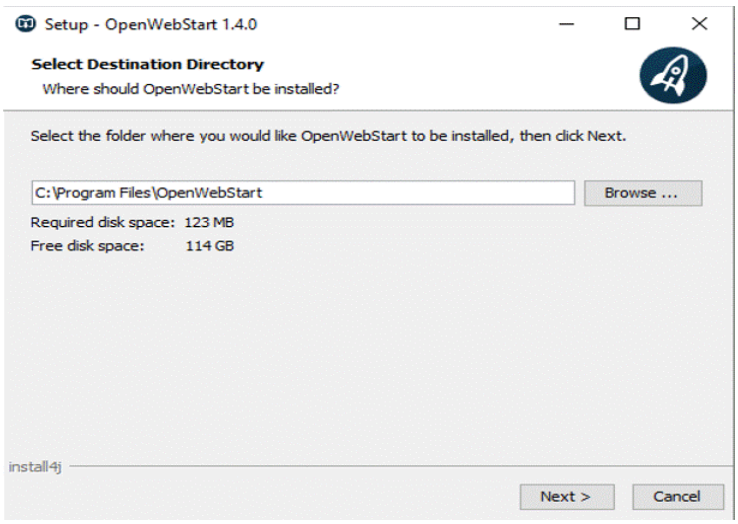


2. Download the latest stable release of OpenWebStart for Windows from https://openwebstart.com/download/

   a) Run the installer and select mode either **for the current users only** or **for all users**.

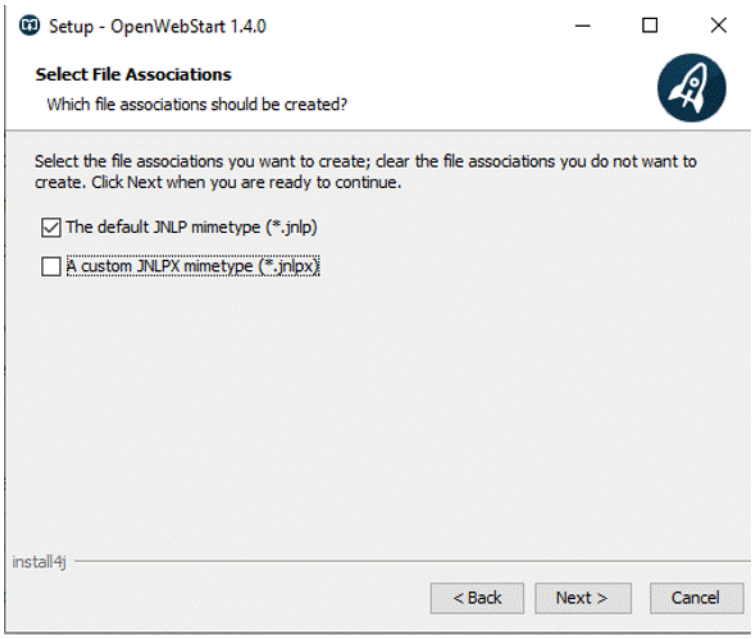


   b) Select path to install OpenWebStart and click **Next**.



c) Click **The deafult JNLP mimetype (*jnlp)** to select file associations.

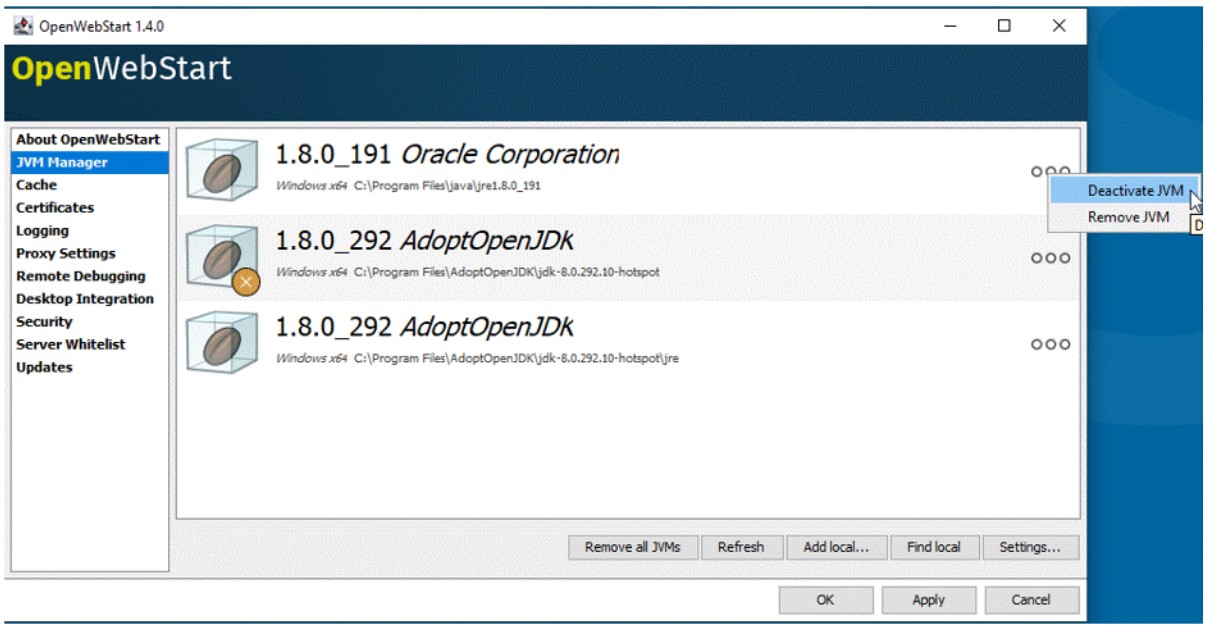
NOTE: A JNLPX mimetype is not necessary as it allows to run OpenWebStart in parallel to JavaWeb-Start. User can run DLS client with OpenWebStart only.



4.11.2.2 OpenWebStart Configuration

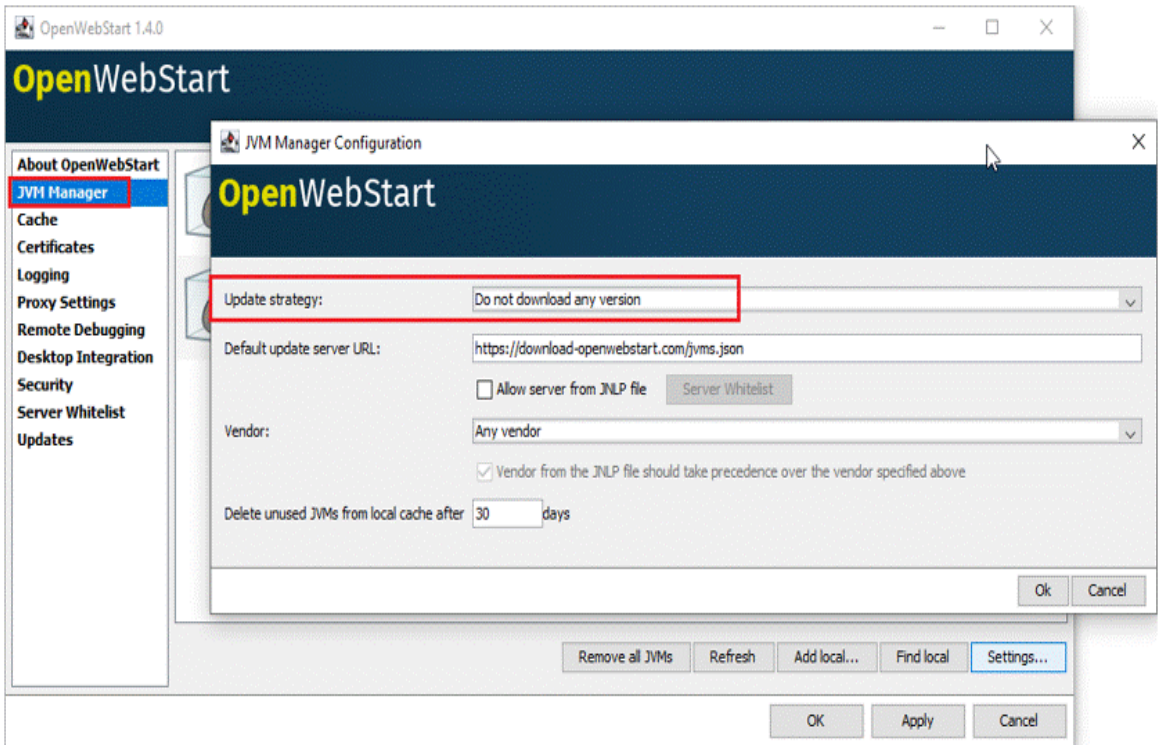
Follow the guidelines below to configure OpenWebStart.

1. Navigate to the Windows Start menu and run **OpenWebStart Settings**.
   - A new **OpenWebStart** window is displayed with a left side panel.
2. In the **JVM Manager** tab:
   a) Click **Find local** to populate list with the available Java. If you have an Oracle JRE, this is not required by DLS anymore and it can be deactivated or removed in the JVM Manager. The previously installed Adoptium OpenJDKs will be listed too.Only JDK in \jre is required to be activated. An 'x' sign appears on each deactivated Java.



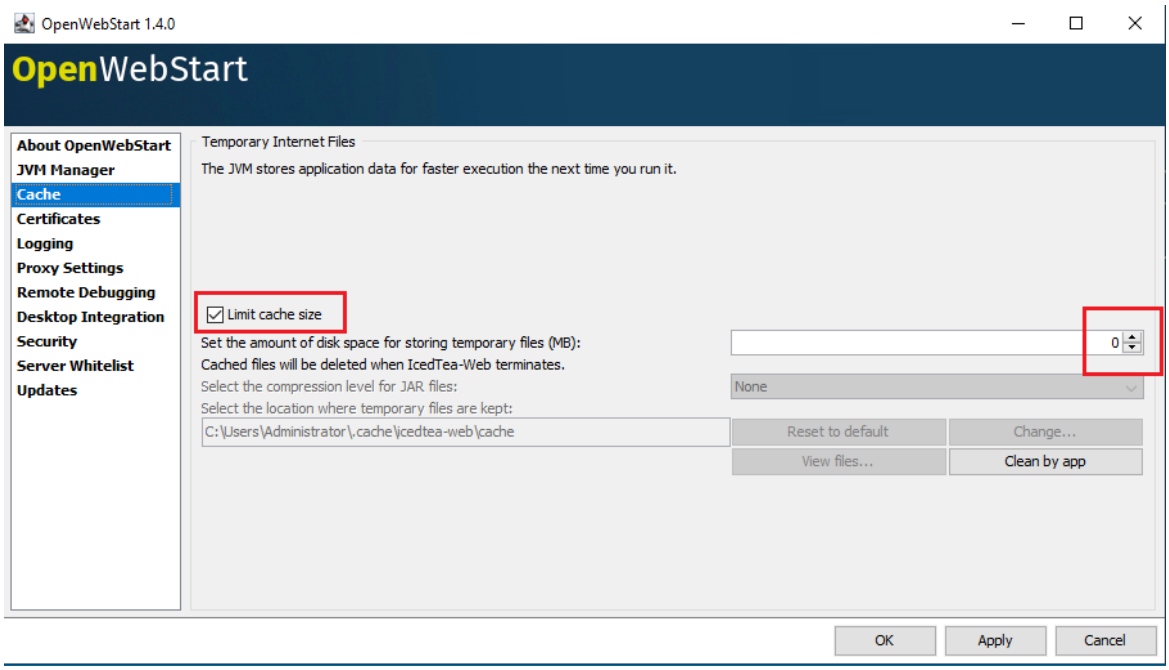
b) Click **Settings** and deactivate JVM updates.

NOTE: This is necessary not to end up with a non-working OpenWebStart.



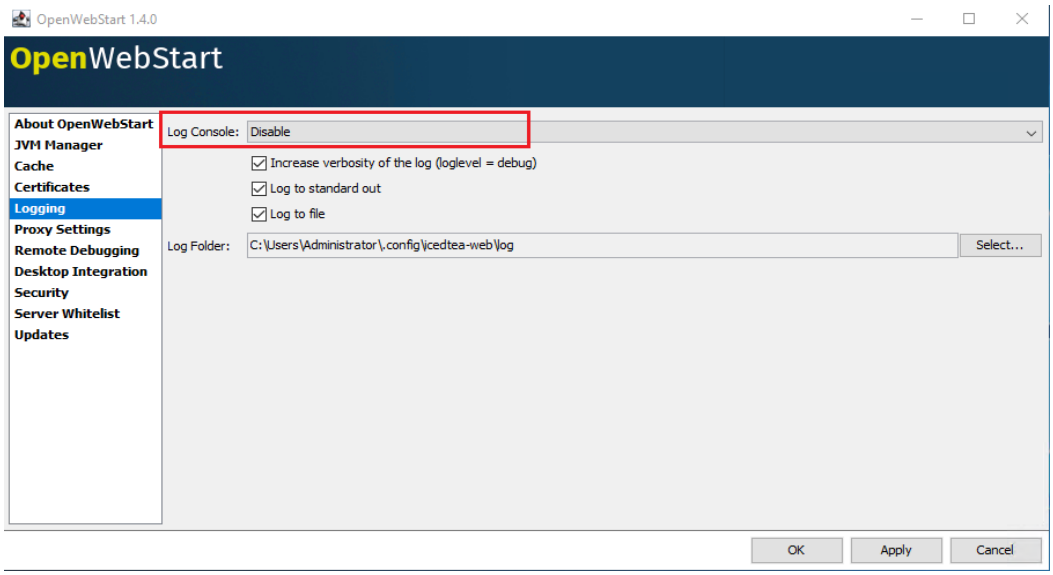
3. In the **Cache** tab:

   a) **Limit cache size** to zero.



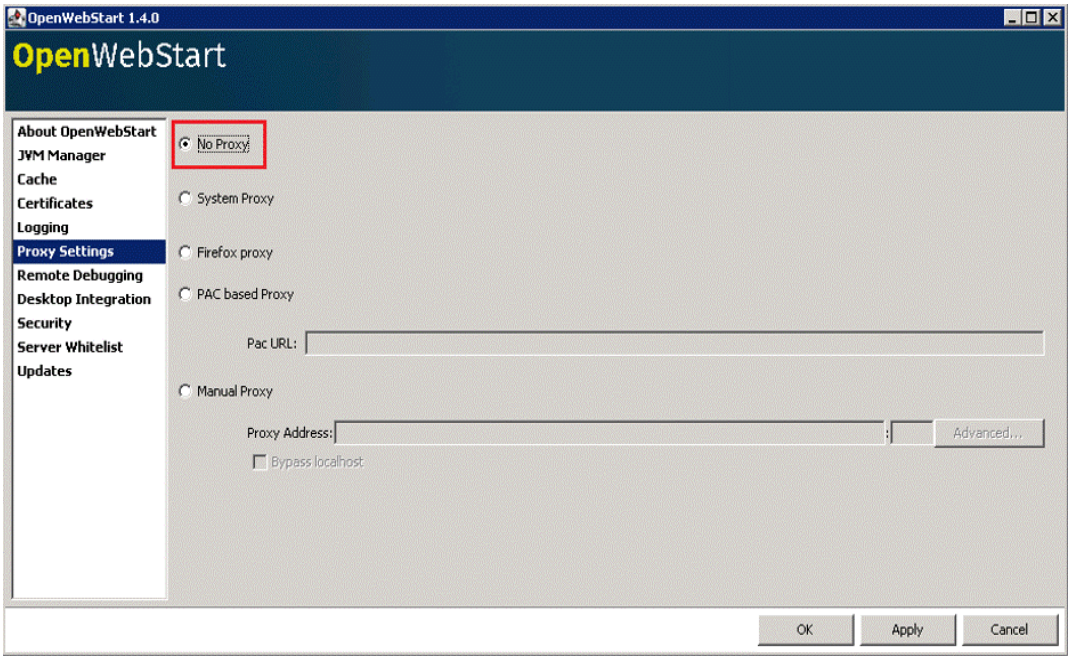
4. In the **Logging** tab:

- Disable logging unless troubleshooting is required.



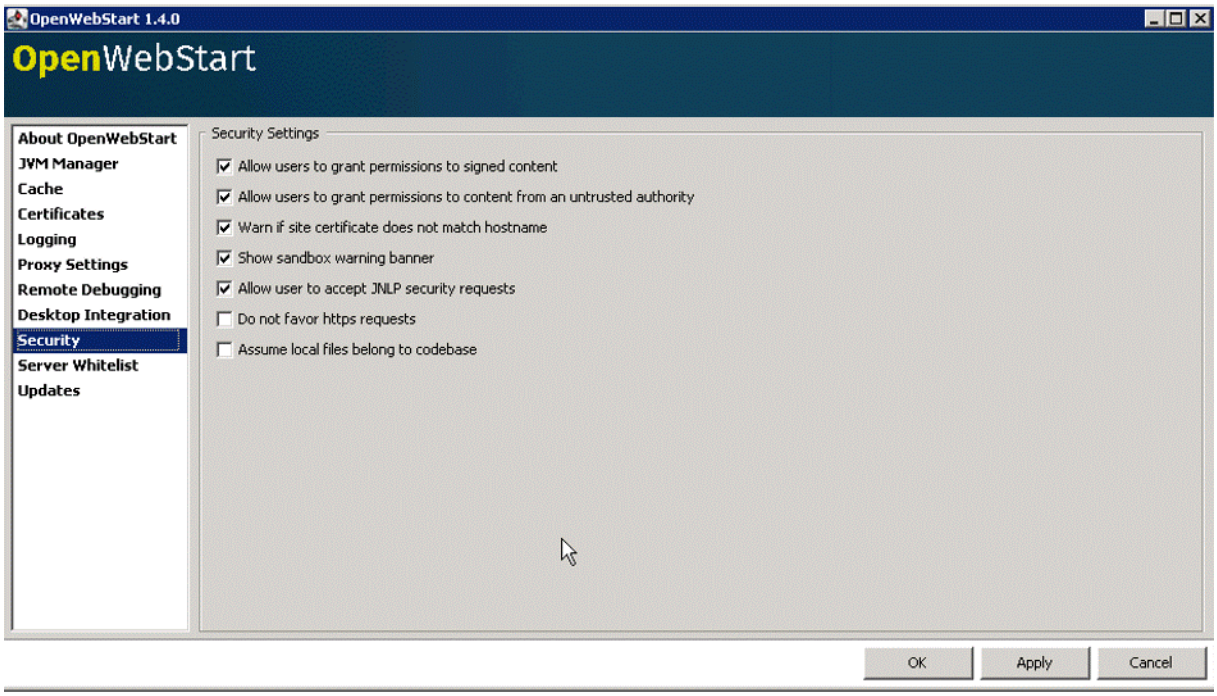
5. In the **Proxy Settings** tab:

- Select **No Proxy**. In a DLS client where there is no Internet, this setting will prevent a failure of OpenWebStart to run DLS client.



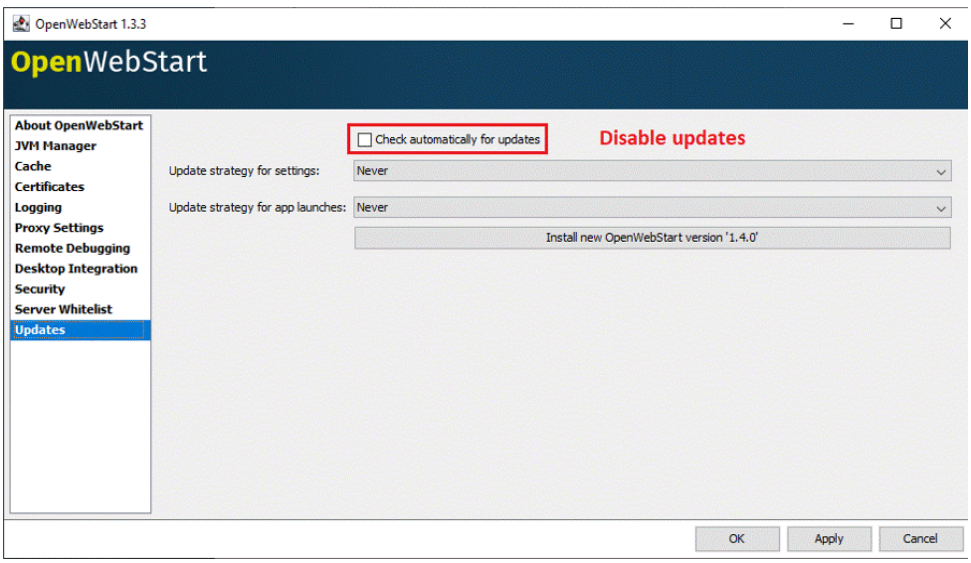
6. In the **Security** tab:

   a) Check the checkboxes as shown in the image below.

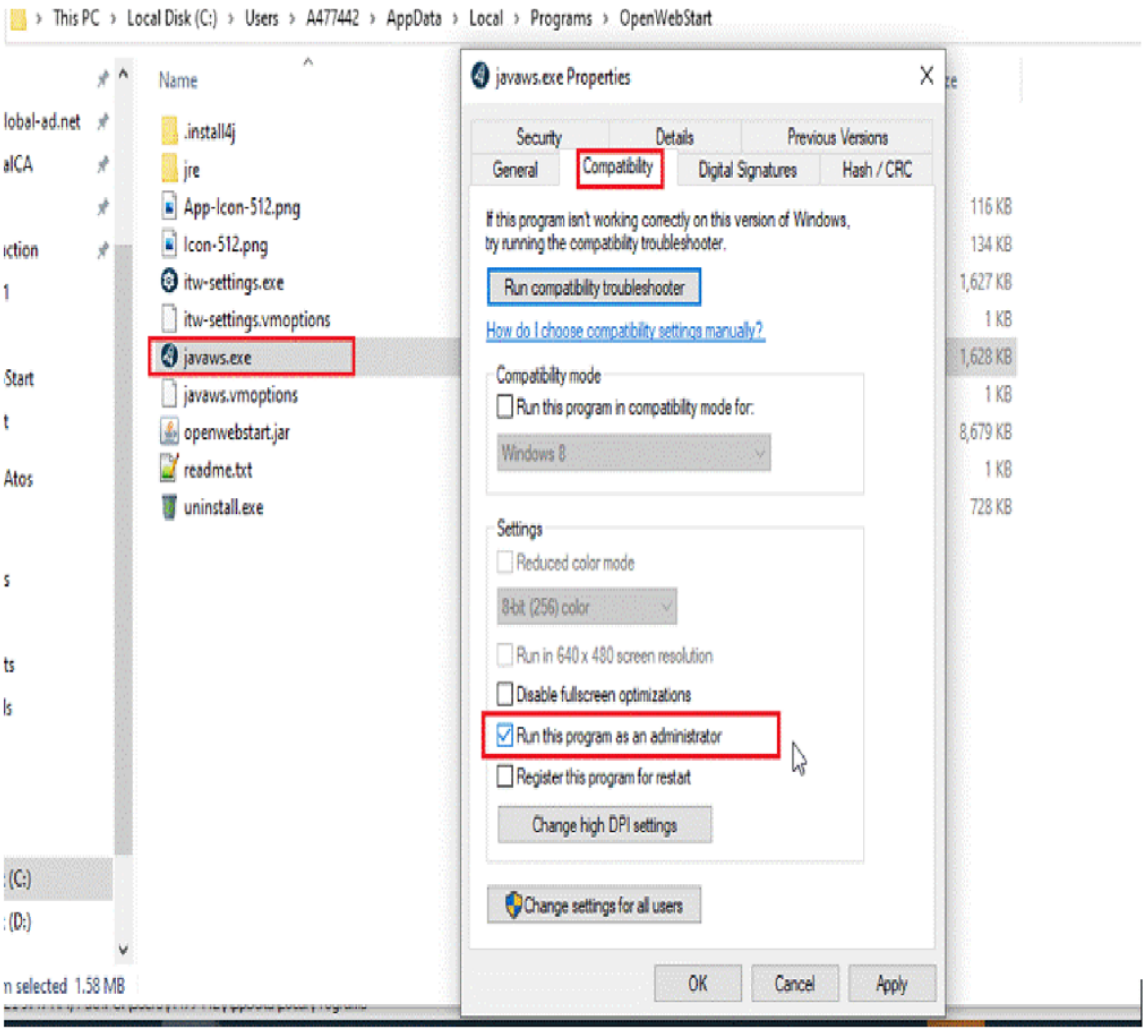


7. In the **Updates** tab:

- Disable automatic updates, DLS does not support every version of OpenWebStart.



8. **Elevation Option**: In case the rights of the DLS Client Windows account are not enough for OpenWebStart then elevate the rights of it's executable as shown in the image below.



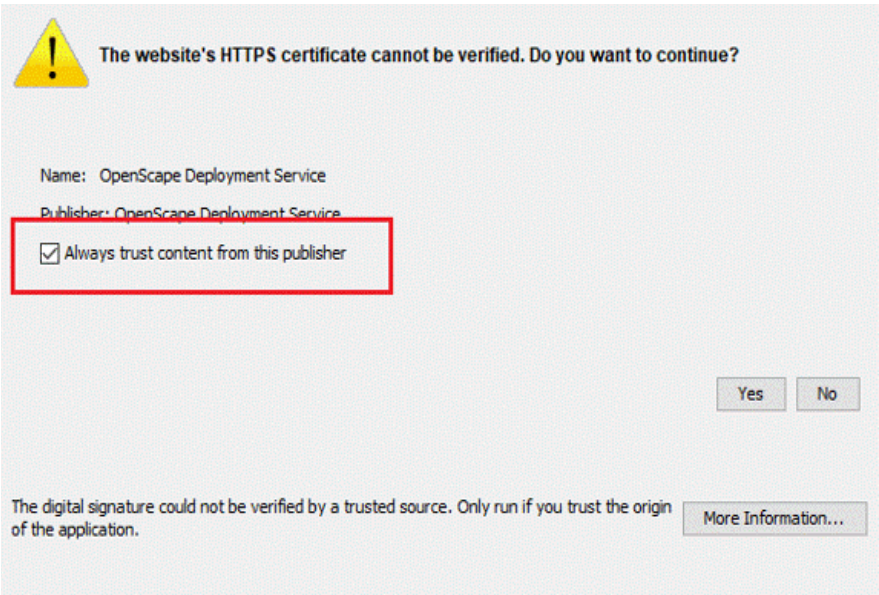
4.11.2.3 Open DLS UI

Access DLS URL https://<DLS server IP>:10443/DeploymentService/ via a browser. In case you have disabled JVM updates, you will not get any prompt. In case you are prompted to upgrade, select "NO". Only Adoptium OpenJDK V8 is currently supported.

NOTE: Do not upgrade from JVM V8 as it is not supported by DLS.



A jnlp file will be downloaded and opened by OpenWebStart. Trust the publisher of DLS certificate when prompted.



DLS UI should open with the Adoptium OpenJDK icon in the upper left edge.

4.12 Installing Network Components

Normally, the network components that are described here are already in place. However, if any of the components have to be retrofitted, this chapter provides you with the description that you will need.

It describes the following components:

- FTP Server
- HTTPS Server
- General Information on DHCP
- DHCP Server in a Windows Environment
- DHCP Server in a Linux/Unix Environment
- Configuring the DNS Server for DLS
- DHCP Server with Infoblox Appliance

4.12.1 FTP Server

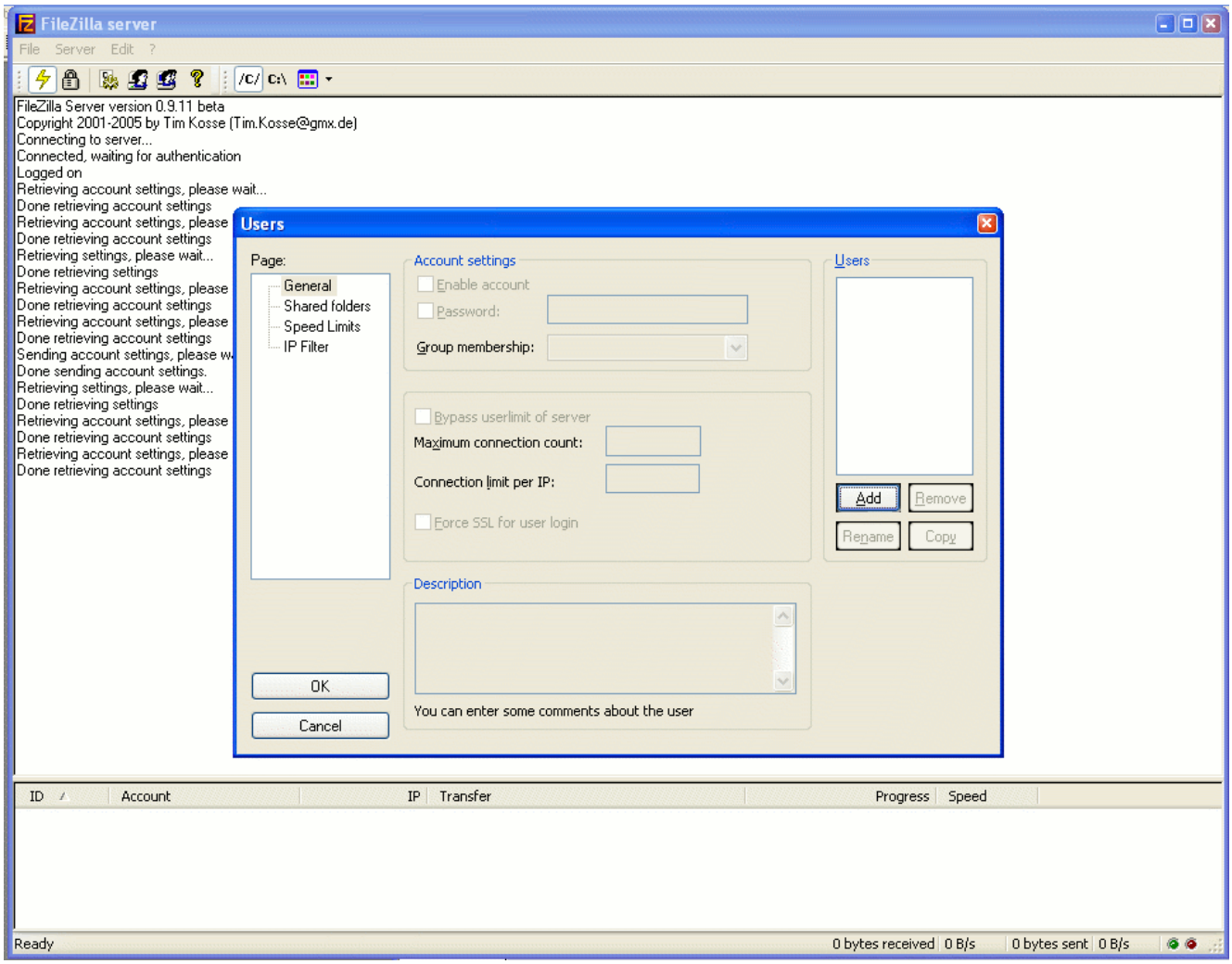
The following example shows how to configure the *FileZilla* server program.

4.12.1.1 Installation and Configuration

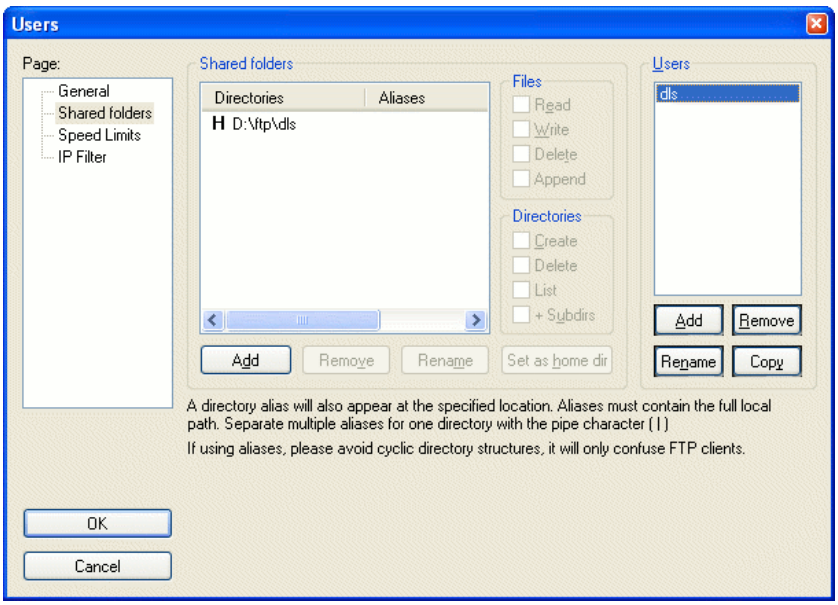
Install the software (*FileZilla Server* in this example, available at http://sourceforge.net/projects/filezilla/).

Start the server program.

Configure a user. To do this, select **Edit** > **Users** from the menu. Select **General** from the **Page** area. Click the **Add** button under the left section of the dialog window. An input window is displayed. Enter the user name in this window. Activate the **Enable account** option in the **Account Settings** area. If you want to assign the user a password, activate the **Password** option in the same area and enter a password.



To assign the new user a directory, select **Shared Folders** in the **Page** area and click **Add**. In the subsequent window, select the directory where you want to store the software subdirectories. To assign read access to the DLS, activate the **Read** option in the **Files** area.



Click **OK**. The FTP server is now available. Current connections are displayed in the server's status window.

4.12.2 HTTPS Server

Terminals in the OpenStage series can download files over HTTPS. To use this option, you must install an HTTPS server. For installation help, consult the instructions supplied with the relevant software.

4.12.3 General Information on DHCP

IP phones feature a DHCP client so that the parameters required for full Plug&Play can be transferred via DHCP.

In addition to the standard parameters (IP address, network mask, and default router), you can configure the following options via DHCP:

- IP routing/route 1 & 2 (option 33)
- IP address of the SNTP server (option 42)
- Time zone adjustment (option 2)
- IP addresses for the primary and secondary DNS servers (option 6)
- DNS domain name for the phone (option 15)
- IP addresses for the SIP server and SIP registrar (option 120))

In Unify IP phones, the DLS IP address and the VLAN ID can be communicated via vendor-specific parameters.

VLAN ID assignment via DHCP works as follows on optiPoint 410/420 phones:

If the "DHCP" VLAN method is set on the phone and QoS is active on layer 2, the VLAN ID is assigned by a DHCP server. This procedure is made up of two steps. The phone starts by issuing a *discovery* message with the "OptiPoint" *vendor class* to try to obtain an IP address for a DHCP server. In the second step, the phone sends a tagged *discovery* message in the VLAN whose ID it received in the first step. This time, the "OptiIpPhone" vendor class is used.

If the VLAN method is set to "manual", only a lease with the "OptiIpPhone" vendor class is obtained from the phone.

4.12.4 DHCP Server in a Windows Environment

For all relevant info please refer to the **How to** overview of **Unify Experts Wiki Portal** :
http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment

under the **DHCP Server in a Windows Environment** tab.

4.12.5 DHCP Server in a Linux/Unix Environment

This section describes how to configure vendor-specific options under Linux and Unix to enable Plug&Play functionality.

NOTE: We recommend that you use a DHCP server in the DLS environment to support full Plug&Play and ensure the authenticity of the DLS server.

The configuration of vendor-specific options may differ from the example shown here depending on the DHCP server used. Refer to the Linux and Unix help pages (man-pages) for more information (for example, dhcp-options and dhcpd.conf).

The options are configured in the /etc/dhcpd.conf file. You can use a text editor to modify this file. Normally, this file contains a sample configuration which you can edit to meet your individual requirements.
Please make a backup of the configuration file before making any changes.

The following configuration contains all necessary parameters:

```
21
Line    Contents
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      }
```

The instructions in lines 10 to 15 transfers DLS addresses to workpoints. Lines 12 and 13 contain two hexadecimal values consisting of:
Option - Length - Value.

The first of the two lines contains the value "Siemens". The second line contains "sdlp://192.168.3.6:18443" (DLS address).

Line 10 contains a freely selectable name and line 14 determines the vendor class to which the configuration applies.

Lines 17 to 21 contains the allocation of the VLAN ID. The VLAN ID is handed over in line 20 with the option 2, the length 4 and the value as a hexadecimal number (here 0A = 10). In contrast to the other options, the decimal VLAN ID is converted into a hexadecimal number.

NOTE: For information on converting ASCII characters to hexadecimal values, see "ASCII Table (Standard)" and "ASCII Table (Enhanced)" on page 17-1606 and on page 17-1607.

Restart the DHCP service once you have modified the configuration. Use the `rcdhcpd restart` or alternatively the `etc/init.d/dhcp stop` command and then `/etc/init.d/dhcp start` to do this. To check syntax, enter `rcdhcp check-syntax` via the console.

If the configuration is correct, terminals should register independently on the DLS after a restart. If the configuration is not correct, you can use a "network sniffer", for example, *Ethereal* (V 0.10.11 or higher), to locate any errors.

4.12.6 Configuring the DNS Server for DLS

NOTE: The following only describes the settings that are necessary for configuring the DNS server for DLS. For general installation and configuration, please read the documentation on the DNS server.

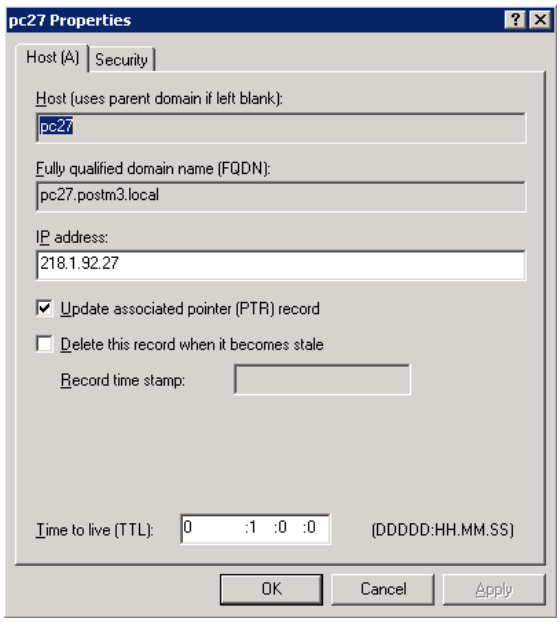
To be able to enter the DLS as a host name, there must be a DNS server with the appropriate configuration.

Example:

DLS IP address: 218.1.92.27

Requested host name: sdlp://pc27.postm3.local:18443

For this example, you must make the following entry in the DNS server:



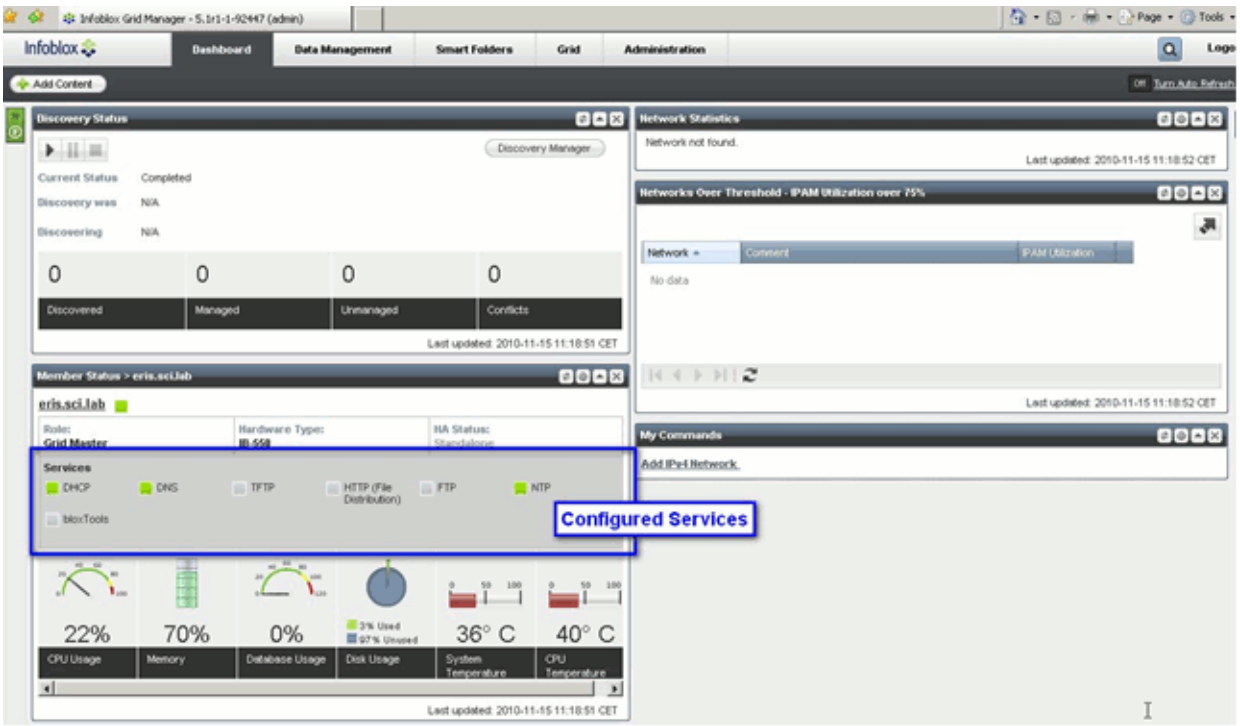
4.12.7 DHCP Server with Infoblox Appliance

As an alternative to a conventional DHCP server under Windows or Unix, the DHCP service can be taken over by the Infoblox appliance.

Additionally, the Infoblox appliance can provide the following core network services:

- DNS
- NTP
- FTP
- TFTP

The following screenshot shows the dashboard of an Infoblox 550 appliance, here configured as DHCP, DNS, and NTP server for an OpenScape Voice environment:



4.12.7.1 Installation

After the Infoblox appliance is cabled to the network (please refer to the installation guide shipped with your appliance) you can access the device remotely across your Ethernet network.

You can administrate and configure the appliance via HTTPS or via command line interface (CLI) using SSH. If you wish to use SSH, you have to login via HTTPS once and enable SSH first.

This manual describes the adminstration via HTTPS; for detailed information on administration via CLI, please refer to the "Infoblox CLI Guide".

Access via HTTPS

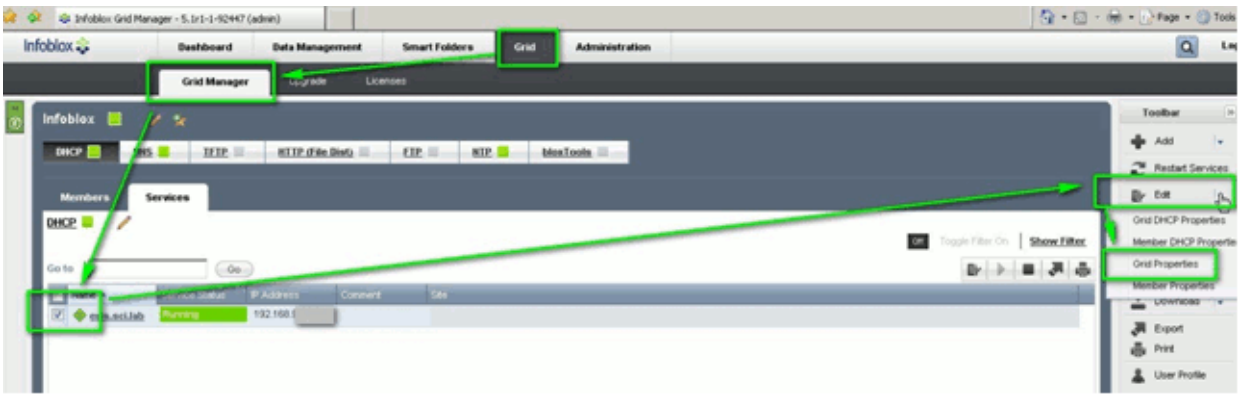
To log in, proceed as follows:

1. Open a web browser and enter
   https://<IP address or hostname of your Infoblox appliance>
2. Enter user name and password.
   The default user name is "admin", and the corresponding password is "infoblox". Please change the password after the first login.

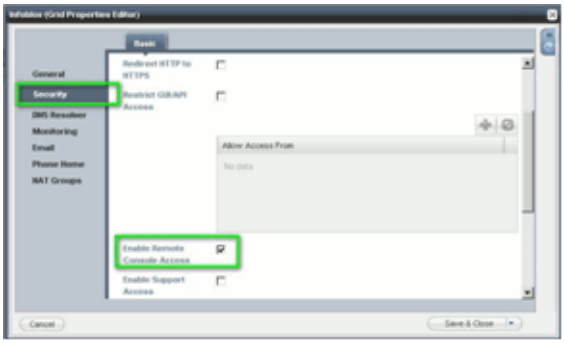
Access for CLI via SSH

To enable access for the CLI, you must be logged in via HTTPS (see Access via HTTPS).

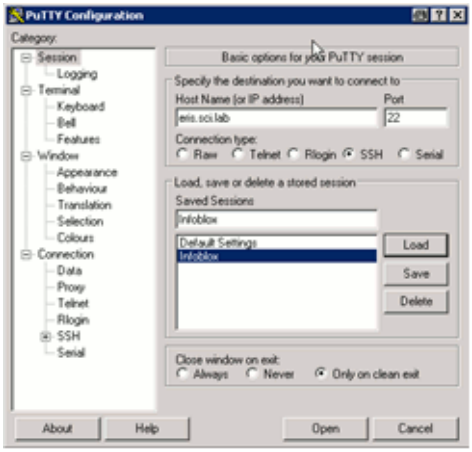
1. Select **Grid** > **Grid Manager** and expand the toolbar. In the **Edit** menu, select Grid **Properties**.

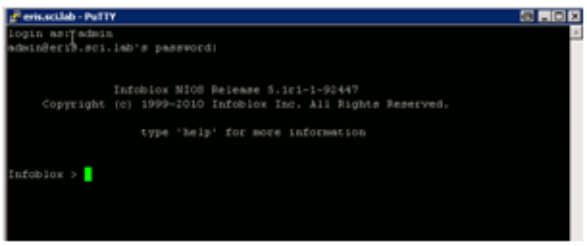


2. The **Grid Properties Editor** opens up. In the **Security** tab, check the **Enable Remote Console Access** field.



3. Now you can administrate and configure your Infobox appliance using the CLI via SSH. For this purpose, every SSH v2 client can be used, for instance, PuTTY for Windows.





Basic Configuration

1. Open a web browser and establish an HTTPS connection with the IP address of the LAN1 port. To reach the default address, enter **https://<192.168.1.2>**.

   NOTE: During the login process, several certificate warnings may appear, but they can be ignored at this stage of configuration. To stop these warning messages, a new self-signed certificate or an import of a third-party certificate is necessary. For more information on how to implement certificates, see the Infoblox Administration Guide.

2. Log in as "admin" with the default password "infoblox".
3. Read the license agreement and accept it.
4. The **Grid Setup Wizard** appears. Select **Configure a Grid Master** > **Next**.
5. Set the **grid properties**:

   - **Grid Name**
     This name (text string) is used by the grid master and by appliances joining the grid to authenticate each other when establishing a VPN tunnel between them. The default grid name is "Infoblox".
   - **Shared Secret**
     This text string is used as a shared secret by the grid master and by appliances joining the grid to authenticate each other when establishing a VPN tunnel between them.
   - **Show Password**
     Activate the switch to have the password displayed, or deactivate it to have the password hidden.
   - **Hostname**
     Specify a valid DNS host name for the Infoblox appliance.
   - **Is the Grid Master an HA pair?**
     Select **No**.

   Afterwards, click **Next**.

6. Configure the network settings.

   - **Host Name**
     Specify a valid DNS host name for the Infoblox appliance.
   - **IP Address**
     Shows the IP address of the LAN port.
   - **Subnet Mask**
     Shows the subnet mask of the LAN port.
   - **Gateway**
     Shows the IP address of the gateway resp. router for the subnet in which the LAN port is located.
   - **Port Settings**
     Select the appropriate settings for the port from the list.

   Afterwards, click **Next**.

7. Enter a new password. The password must be a single hexadecimal string with a minimum length of 4 characters.
   Afterwards, click **Next**.

8. Choose a time zone for the grid master and specify whether the grid master should synchronize its time with the NTP server.

   When you whish to use NTP, click on the **Add** symbol and enter the IP address of an NTP server. You can also enter multiple NTP servers.

   When you do not wish to use NTP, set date and time manually.

   Afterwards, click **Next**.

9. In the final screen, you can check all settings you have made with the wizard.

   Click **Finish**.

   After this, a restart is performed.

4.12.7.2 Configuration

General DHCP Configuration

First, you must specify a network and a range of IP addresses to be leased.

NOTE: For enabling active DNS forwarding over DHCP, a working DNS must be present in your network. You can check this by means of the following CLI commands:

- Determine the IP address of the DNS server which has been configured for your network. Under Windows, this is done using the command:
`ipconfig /all`

- With a ping, you can check if this DNS server is reachable:
`ping <IP address of the DNS server>`

- With nslookup and a random IP address or a random host name, you can determine if the DNS server is working correctly:
`nslookup 172.21.101.15` or
`nslookup wsname.domain.net`

Adding a Network

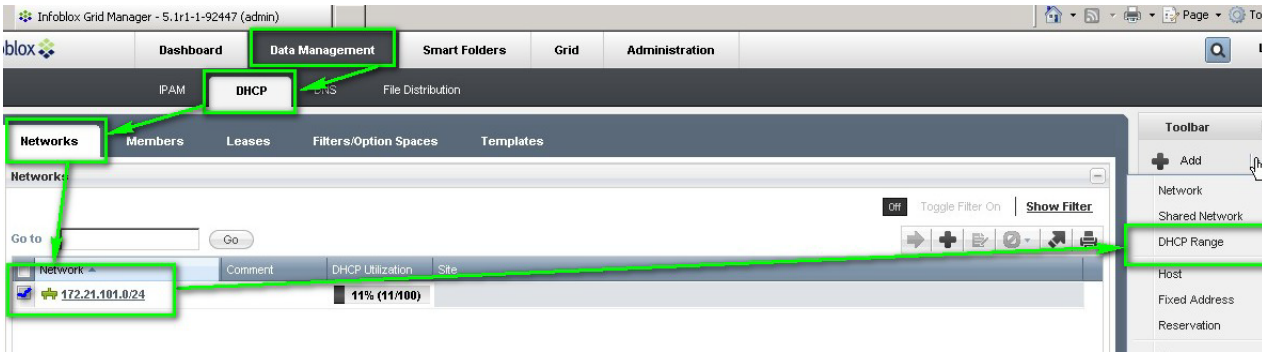
1. Select **Data Management** > **IPAM** and in the toolbar under **Add**, click **Add IPv4 Network**.



2. In the **Add Network** wizard, complement the following specifications:
   - **Adress:**
     Address of the network. Example: **172.21.101.0**
   - **Netmask:**
     By means of the netmask slider, select the netmask **/24 (255.255.255.0)** .
3. Click **Save&Close**.

Creating a DHCP Range

1. Under **Data Management** > **DHCP** > **Networks**, select your network (e.g. 172.21.101.0), click **Add** in the toolbar, and then **DHCP Range**.



2. In the **Add Range** wizard complement the following specifications:

   - **Start:**
     Beginning of the address range. Example: **172.21.101.100**
   - **End:**
     End of the address range. Example: **172.21.101.199**

3. Click **Save&Close**.

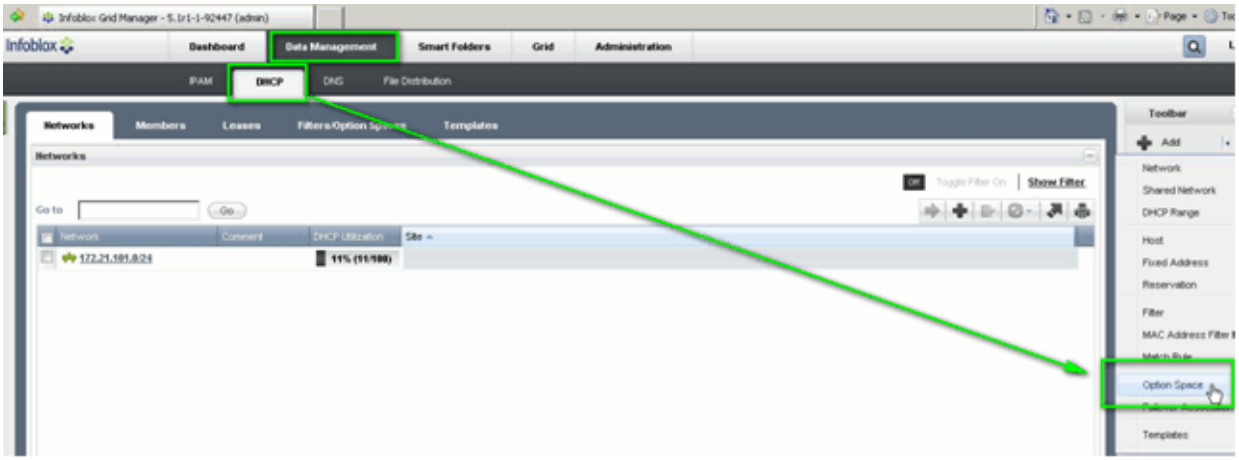
   NOTE: Please note that every DHCP server in your environment should have at least one range which does not overlap with a range of another DHCP server in the same environment.

Configuring the DHCP Server for DLS

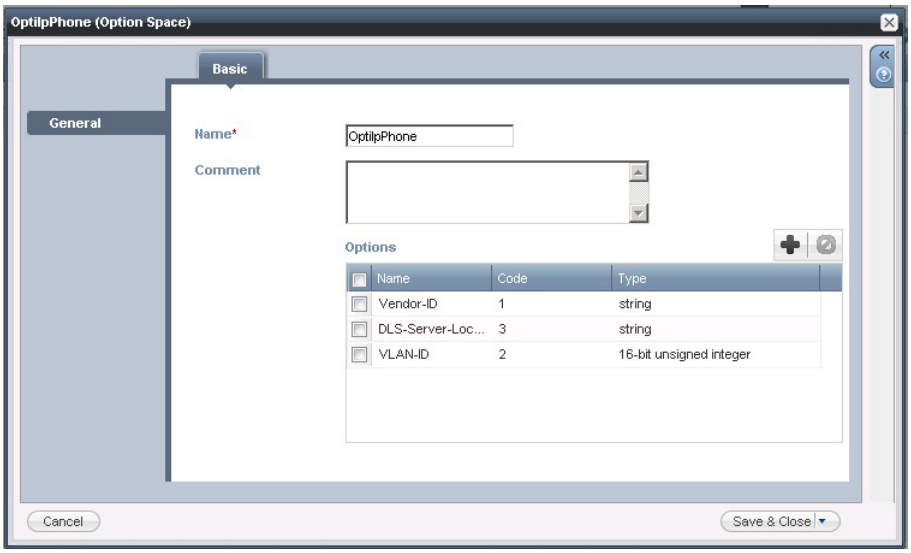
For full Plug&Play, the DHCP server must communicate the IP address and port number of the DLS to the phone during startup. Subsequently, the phone will contact the DLS to receive the required settings.

The Infoblox appliance transmits the DLS-relevant information in the form of vendor specific options.

1. Navigate to **Data Management** > **DHCP** > **Filters/Option Spaces** and on the right side, select **Add**.



2. Specify the DHCP options as follows:
   - In the **Name** field, enter "OptiIpPhone".
   - Add a new option with the properties **Name**="Vendor-ID", **Code**= "1" and **Type**="String".
   - Add another option with the properties **Name**="Vendor-ID", **Code**="1" and **Type**="String".
   - If a virtual LAN (VLAN) is used: Add another option with the properties **Name**="VLAN-ID", **Code**="2" and **Type**="16-bit unsigned integer".

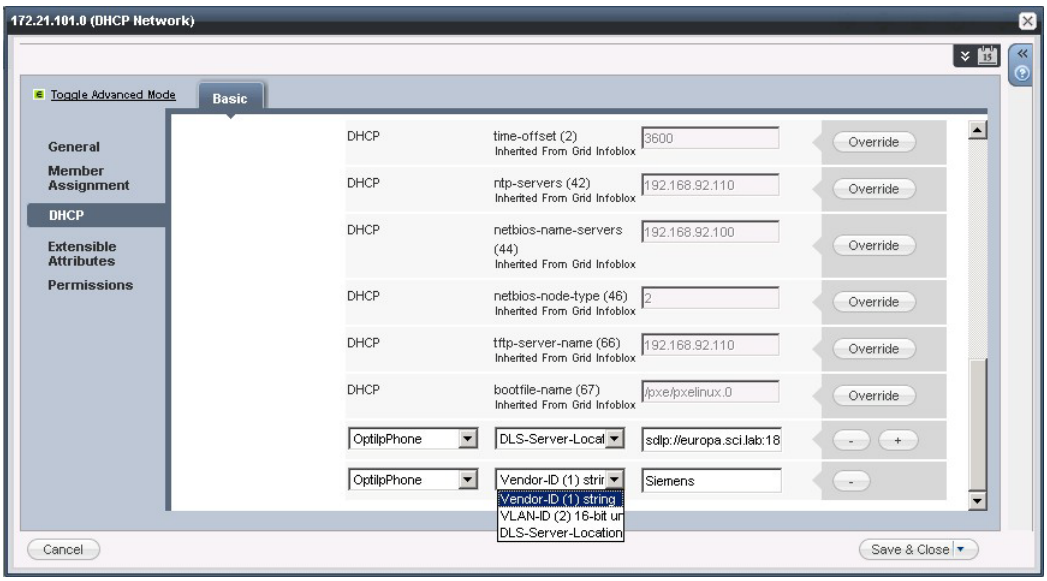


3. Navigate to **Data Management** > **DHCP** > **Networks**, select your network (e.g. 172.21.101.0/24) and in the toolbar, click **Edit**.

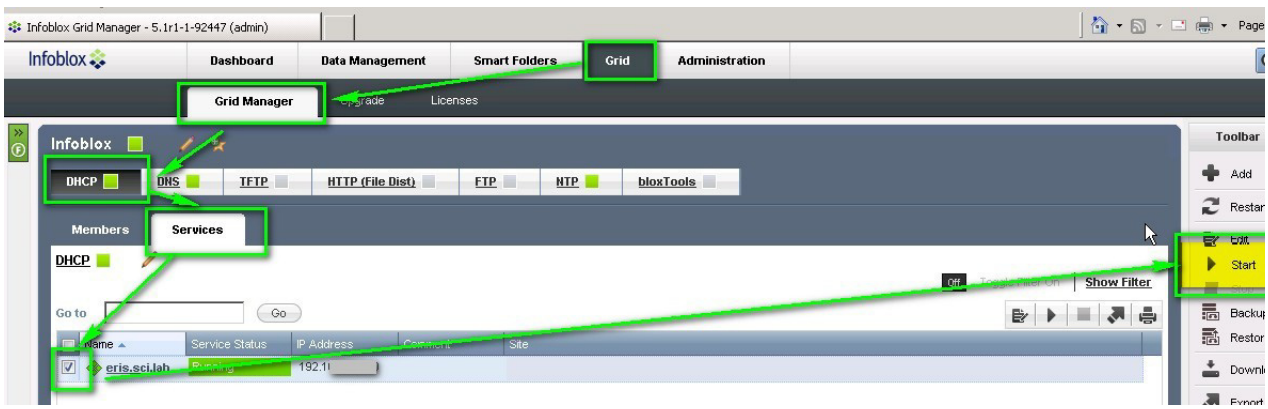


4. Navigate to **Basic** > **DHCP** and perform the following actions.

   - Add a new entry with the properties **space**=„OptiIpPhone“, **name**=„DLS-Server-Location“, **value**=„sdlp://<name or hostname of your DLS server>:18443“.
   - Add a new entry with the properties **space**= „OptiIpPhone“, **name**= „Vendor ID (1) string“, **value**= „Unify“.
   - If a virtual LAN (VLAN) is used, the VLAN ID must be specified in a similar way.



5. Navigate to **Grid** > **Grid Manager** > **DHCP** > **Services**. Check your network and click the play button. The DHCP service starts.



4.13 Uninstalling the Deployment Service

To completely remove a DLS installation from a computer, you must uninstall two components one after the other.

IMPORTANT: An uninstallation also deletes all data in the DLS database. To avoid data loss, create a backup of the database before you carry out the uninstallation (see Section 15.11, "Backup/Restore").

IMPORTANT: The Uninstaller removes any rollback related directories except the rollback database backup for remote database deployments since it does not know the user supplied directory for the database backup during an upgrade installation.

IMPORTANT: After uninstallation in remote database deployments,the database must be deleted manually by the administrators.

4.13.1 Uninstalling the DLS

1. In the Windows Start menu, select **Settings** > **Control Panel** > **Add/Remove Programs** and then click the **Deployment Service** entry in the list of installed software.
2. Click **Remove** and follow the rest of the procedure.

When the uninstallation is complete, both the DLS application and the Web server that was installed (*Tomcat*) are removed from the server PC.

NOTE: The root directory created during DLS installation, "DeploymentService", is emptied during uninstallation, but must be deleted manually.

4.13.2 Uninstalling the SQL Server

If you want to reinstall the DLS, the installation routine will give you an option for uninstalling the existing Microsoft SQL Server. Otherwise you can remove it manually:

1. In the Windows Start menu, select **Settings** > **Control Panel** > **Add/Remove Programs** and click the **Microsoft SQL Server** entry in the list of installed software.
2. Click **Remove** and follow the rest of the procedure.

When the uninstallation is complete, the SQL database application is removed from the server PC.

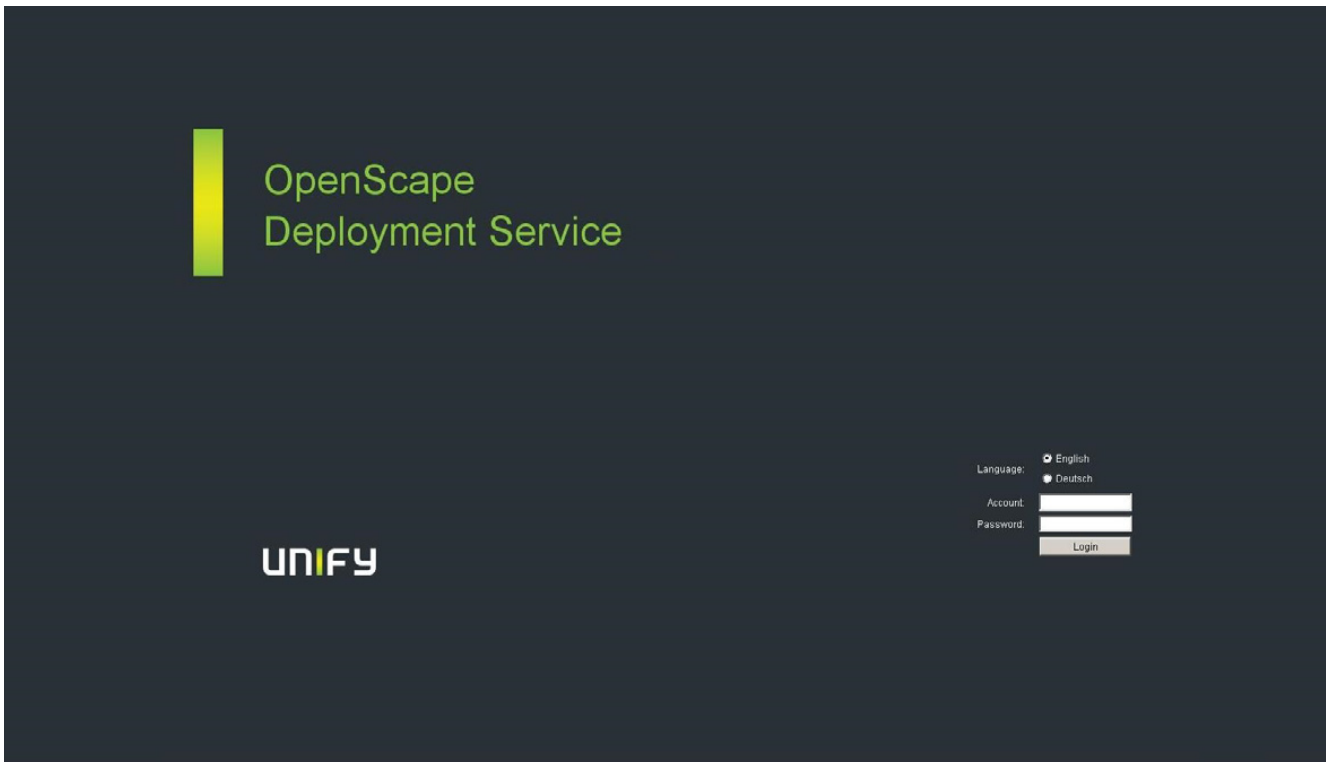
5 The DLS User Interface

5.1 Starting and Logging On

1. Enter the following URL in the Web browser:
   https://[IP address]:10443/DeploymentService/ (for an encrypted connection)

   For [IP address], enter the IP address of the computer on which the Deployment Service is running (DLS server).

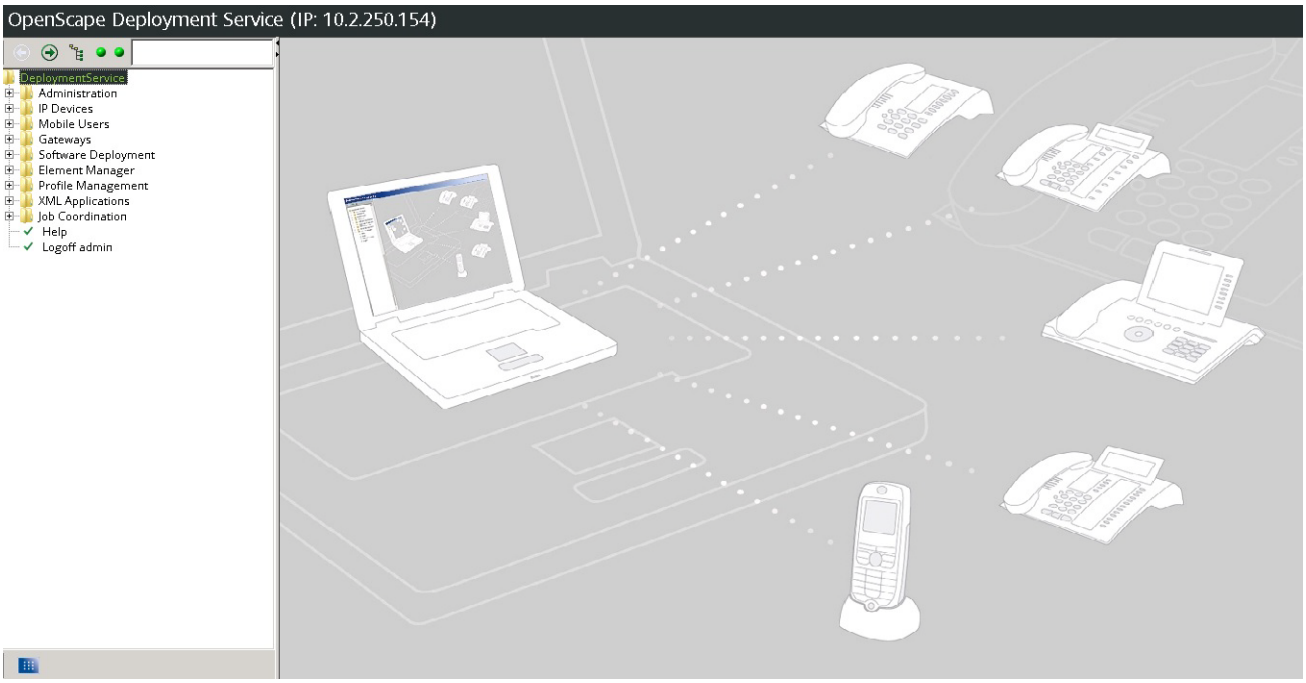
2. The Login window appears:



   Enter "admin" for **Account** and the password set during installation for **Password**.

   If applicable, select your language and confirm with **Login**.

3. The startup screen is displayed:



NOTE: The DLS User Interface startup screen provides info of the connected DLS server at the upper left side of the window. (i.e.OpenScape Deployment Service (**IP:10.2.250.154**).

NOTE: Communication between the DLS server and **DLS client** is set up using the port number **10443** (secured connection).
Note that communication between the DLS server and **IP device** takes place over port **18443** (default mode) or **18444** (secure mode).
For more information, refer to Section 7.6.4.4, ""DLS Connectivity" Tab".

5.2 Ending

1. In the main menu (see Section 5.4.1), select **Logoff <account>**.
2. Confirm the security prompt with **Yes**.

   The login window reappears in readiness for a new account to log on.
3. Close the browser window.

5.3 Opening the Context-Sensitive Help Function

This manual can be viewed in online help format for each DLS client interface topic (page in content area, see Section 5.4.2). For help, select the entry **Help Topics** under **Help** in the menu bar.

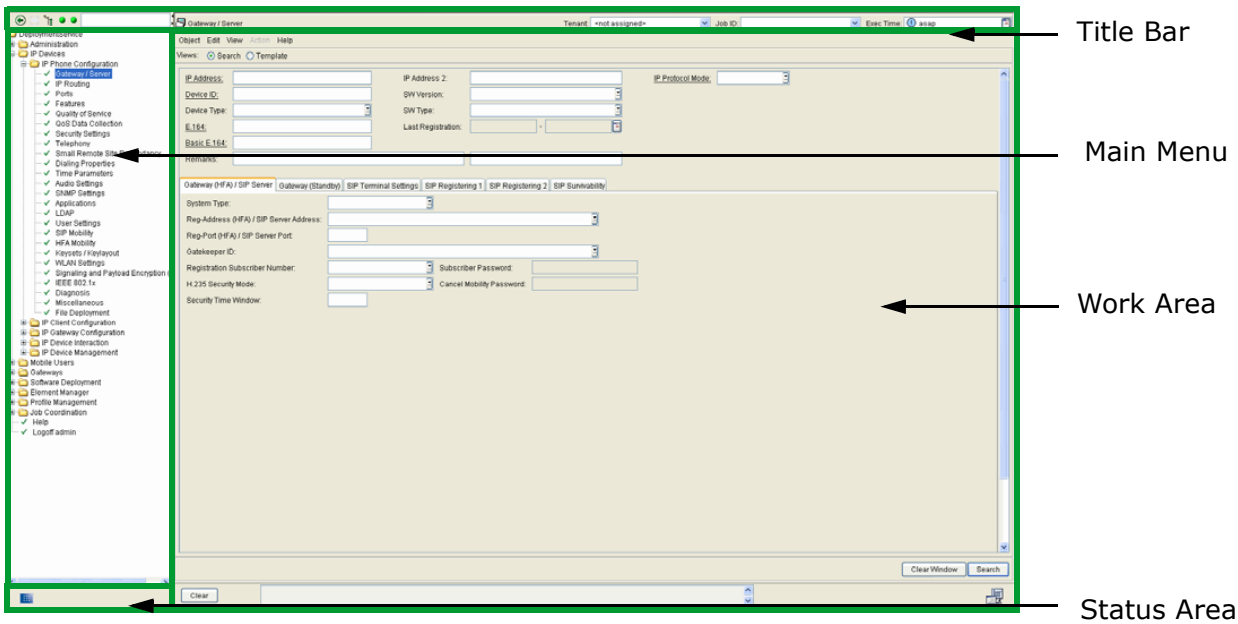
The local version of the DLS (OpenScape Deployment Service local) does not support the context sensitive help function. The general help will be opened.

You can call up help without a special topic by clicking **Help** in the main menu (see Section 5.4.1).

Help is displayed in a new browser window.

5.4 Application Interface

The application interface has three parts:

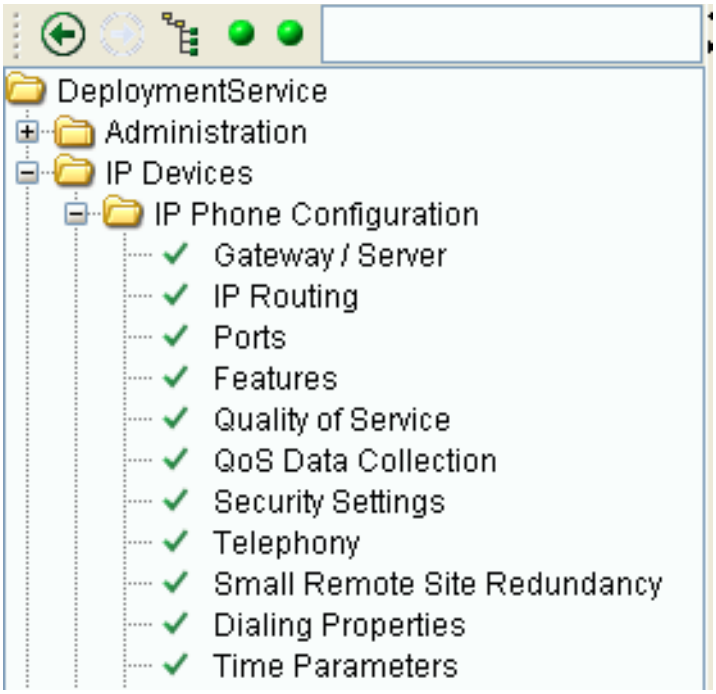


You can change the position of the division between the main menu and the working area by clicking and dragging the separator. Clicking one of the arrow icons in the upper area of the separator moves the division all the way to the right or left, so that the working area or main menu is removed from the display.

NOTE: You can also use the operating sequence in Section 15.3, "First Steps: Changing IP Device Parameters" to get to know the interface better.

5.4.1 Main Menu

The structure of this manual from Chapter 6, "Administration" onwards largely reflects the structure of this main menu.



The main menu contains the following buttons:

With the aid of these buttons, you can navigate between menus that have been opened before. The back button will get active as soon as a menu has been opened. The forward button will get active as soon as the back button has been clicked.

By clicking on this button, you can open and close all submenus.

The status display for current jobs is updated with every server access, but it can also be triggered via a popup menu. For this purpose, click on the status display and, in the popup menu, select **Update Status**. If a specific job shall be observed, it is recommended to reset the display by selecting **Reset Status**. Via **Show Jobs**, you can navigate to the **Job Control** menu; there, you can see details on each job. Timer controlled jobs appear in the display not till then when they are started.
The display on the left informs about running jobs. The following states are possible:
There are no running jobs.
Job running.
The display on the right informs about finished and failed jobs. The following states are possible:
Jobs have been executed without errors.
A job has failed. If the job is cancelled (see Section 14.1, "Job Control"), the display is set to green again.

admin This field allows the user to filter leaf tree entries matching the search string of the DLS tree menu. Only the filtered leaf tree entries are shown in the tree menu.

You can use the structured main menu to reach all DLS components. Simply click the "+" or "-" in front of a directory symbol (or double-click the directory name) to open or close the directory. Click a contents icon to display the contents in the work area.

The contents icons may look like this:

 Directory with further subdirectories or pages.

 Page in normal mode (action completed without encountering error or not yet completed).

 Page where an action is currently running, for example, when scanning IP Devices.

 Page with an action that ended incorrectly.

 Page not accessible due to missing account rights.

In addition, the main menu features these special functions:

 Help

Opens the online help.

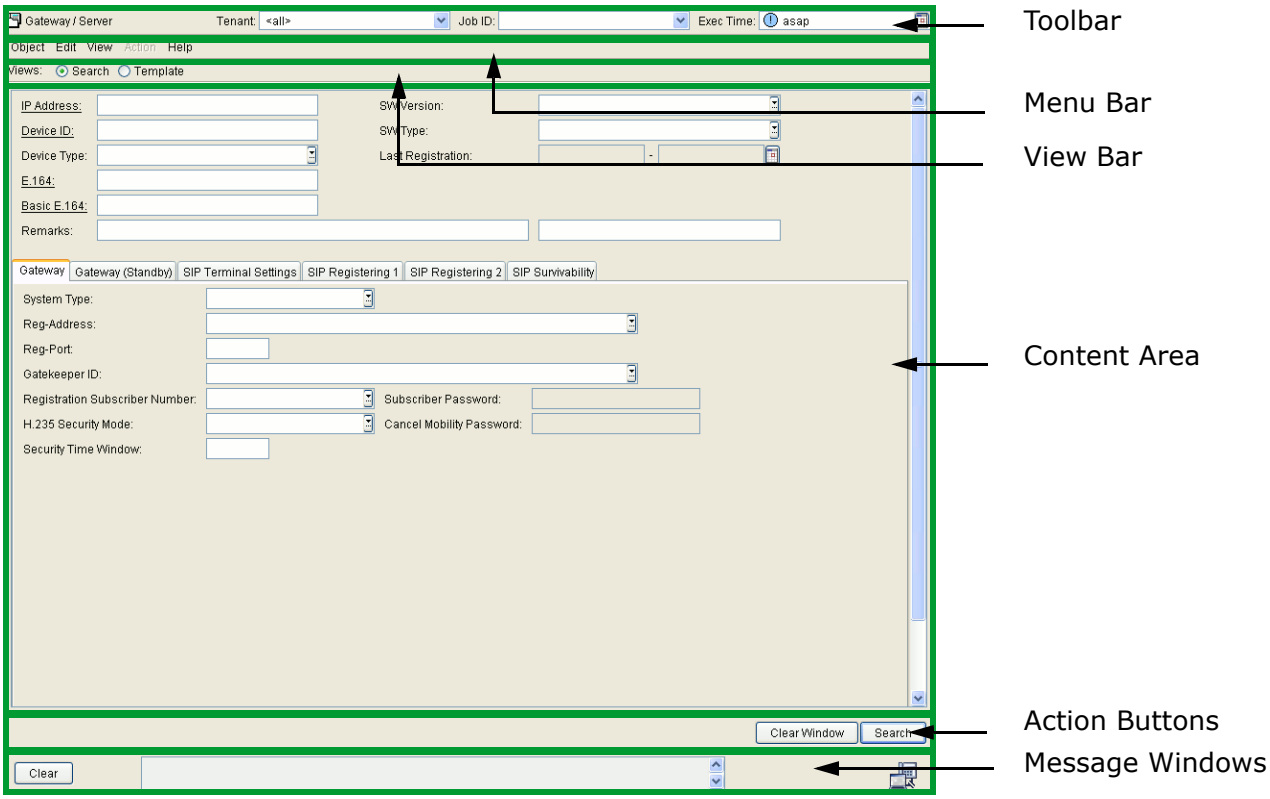
 Logoff <account>

Logs off the user indicated in <account>.

For information on other icons, see Section 5.4.2.4, "Icons beside entry fields".

5.4.2 Work Area

To the right of the main menu is the work area which is split up as follows:



5.4.2.1 Toolbar



The component currently open in the main menu is displayed on the left.

On the right hand side, elements for

- Tenants
- Job ID
- Exec Time

are displayed.

Tenant

All tenants associated with the current account are shown. Additionally, for the ’admin’ account,

- <all> = all tenants, and
- <not assigned> = tenants which are not assigned to any account,

are shown.

Job ID

A job is a combination of deployment actions that should be executed at a fixed time.

NOTE: Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

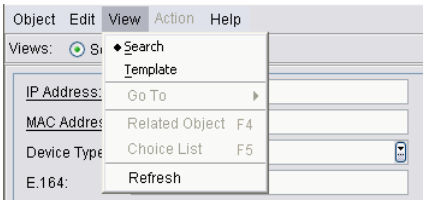
For more information, see the interface description in Chapter 14, "Job Coordination" and sequence descriptions in Section 15.10, "Using Job Coordination".

Exec Time

Specify the execution time for the job. The defaut is „asap“, that is, the job is executed immediately. By clicking on the calendar symbol, you can define a point in time and conditions for job execution with the aid of a separate calendar dialog.

5.4.2.2 Menu Bar

The number of entries shown by the menu bar varies depending on the content area.



NOTE: In many cases, different options are available for executing a function. Sample function: **Search**: this can be performed using the **Object** entry in the menu bar, the button of the same name, or the <F3> function key.

The following lists all entries that can be found in the menu bar:

- **Object**
  - **New** (create new data record)
  - **Save** (save data record, <F3>)
  - **Discard** (discard changes to a data record)
  - **Delete** (delete data record)
  - **Search** (search for data record, <F3>)
  - **Copy** (copy data record)
  - **Paste** (insert copied data record)
- **Edit**
  - **Undo Window** (undo last change in a page of the content area)
  - **Clear Window** (delete all entries in a content area page)
  - **Undo Field** (undo last change in a field)
  - **Cut** (cut out the marked content)
  - **Copy** (copy the marked content)
  - **Paste** (insert marked content)
  - **Clear Selection** (remove marking)
  - **Select All** (mark all objects)

- **View**
  - **Search** (Search view)
  - **Object** (Object view)
  - **Table** (Table view)
  - **New** (view for creating a new object)
  - **Template** (Template view)
  - **Go To**
    - **First Object** (jump to first data record)
    - **Previous Object** (jump to previous data record)
    - **Next Object** (jump to next data record)
    - **Last Object** (jump to last data record)
  - **Related Object** (related objects, <F4>)
  - **Choice List** (show the selection list field,<F5>)
  - **Refresh** (refresh the view)
- **Action**
  - **Discard Job** (cancel the job currently running)
  - **Import File** (import job file)
  - **Export File** (export job file)
  - **Get Template** (load template data)
  - **Save As Template** (save template data)
  - **Rename Template** (change name of saved template)
  - **Delete Template** (delete saved template)
  - **Copy To Template** (copy data to template)
  - **Apply Template** (transfer template data to current view)
  - **Generate All Templates** (templates are generated for all objects or masks associated with the selected IP Device type)
  - **Save Selected Mobile User to Archive** (save mobile user data in a ZIP archive; see Section 16.16.10.2, "Saving Mobile User Data")
  - **Load Mobile User from Archive** (retrieve mobile user data from a ZIP archive; see Section 16.16.10.3, "Loading Mobile User Data")

  - **Copy IP Device** (Copy data of an IP Device, see also Section 16.6, "Replacing an IP Device", Section 16.9, "Replacing HFA with SIP Software and Vice Versa with Identical Device IDs", Section 16.14.7, "Replace IP Phone")
  - **Save Selected IP Device to Archive** (Selected IP Devices are written into zip archive).
  - **Load IP Device from Archive** (Loads data of IP Devices from .zip archive.)
  - **Simulate Plug&Play** (Test of location and default profile configuration. Location data are entered and after clicking **Simulate Plug&Play**, the data sent to the phone which might register with the DLS can be checked.)
  - **Import Certificate** (Imports a certificate for the selected IP Device (only available in Certificate Management). For more information, see Section 16.14, "Security: Administering Certificates".)
  - **Remove Certificate** (Deletes a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.14, "Security: Administering Certificates".)

- **Help**
  - **Help Topics** (open context-sensitive help for DLS)
  - **About...** (information on DLS)

5.4.2.3 View Bar

There are several views available for some contents.
You can select a view under the menu bar.

NOTE: You can also call up all view bar options using the **View** menu (see Section 5.4.2.2, "Menu Bar").



The following lists all options available for the views:

- **Search**

  Shows a search mask in the content area for filtering individual IP Devices from the total set of registered IP Devices. See Section 5.5, "Search Functionality".

- **Object**

  Shows an individual data record for an IP Device in the content area.

- **Table**

  Shows a list of all available data records in the content area.

- **New**

  Creates a new data record.

- **Template**

  Shows a template in the content area that you can save and then use later for searches.

NOTE: If you are in the **Search** view, you can change all elements (for example, by entering values in fields or activating check boxes) in order to define the search criteria or enter data.
In the **Template** and **New** views, only data that can be edited and saved in the DLS database is visible. All other fields are dimmed. General data from the content area cannot be saved as a template.
Frequently, when the search result contains data from existing IP Devices (**Object** or **Table** view), some elements are uneditable and therefore also dimmed.

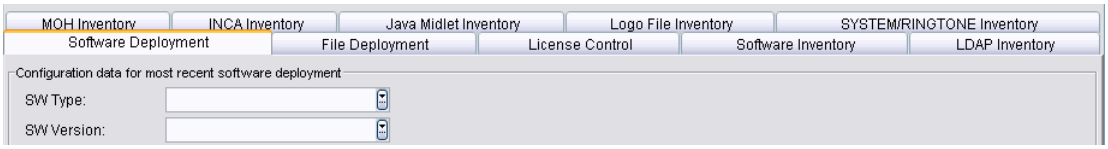
5.4.2.4 Content Area

This is where information is shown and where you can enter or select data.

> ***NOTE:*** If necessary, a distinction can be made between the views available (see Section 6, "Administration") when setting element parameters in the content area (starting in Section 5.4.2.3, "View Bar").
> These settings dictate whether you can change elements or only view them.

Tabs

In the case of large content volumes, it is advisable to split the contents into individual groups. The content groups can then be selected and displayed via tabs in the content area.



Click the tab containing the contents you want to view or edit. Information on the various tab interfaces can be found in Chapter 6, "Administration" to Chapter 14, "Job Coordination".

The most important control elements

- **Text field**

  For displaying / entering freely selected alphanumerical characters as well as allowing the data reset for text items.The boolean data items already provide this option. At DLS GUI level, when creating DLS templates, the boolean items support the following options:

  - **Not Included in the template**:

  - **Included with specific value**:

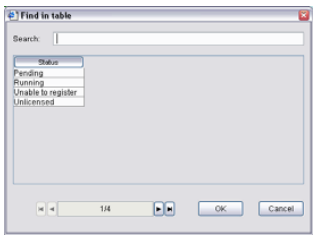
  - **Included as empty value:**

- **Selection list field**

For selecting an item from a list and for entering freely selected text.
If available, the **Find in Table** dialog opens with several entries when you click the list button at the right of the field.

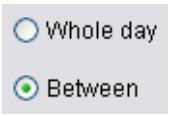


- **Choice field**



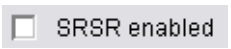
Click a value (for example, 17) and increase or decrease the value by clicking the appropriate arrow.

- **Options**



For selecting one of several possible options.

- **Check box**

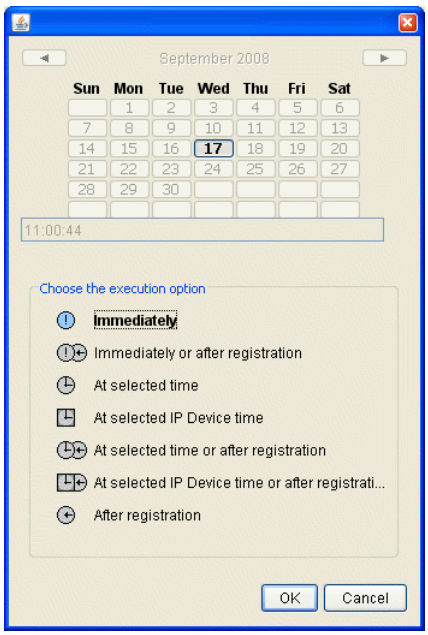


For activating or deactivating a property. There is also a third status for a check box in the **Search** view, which is known as "undefined" (half-tone display).

- **Time field with calendar button**



This button provides you with a separate calendar dialog for selecting a point in time and conditions for job execution.



The following options are available:

- **Immediately**: The job is executed immediately. If the IP Device should be unreachable, the job will be cancelled.
- **Immediately or after registration**: The job is executed immediately. If the IP Device should be unreachable, the job will be started anew when the IP Device is registered.
- **At selected time**: The job is started at the point in time selected in the calender field.

- **At selected IP Device time**: The job is started at the point in time selected in the calender field. However, here, not the system time on the DLS server is valid, but the local time in the IP Device. This option is expedient when the DLS server and the IP Devices are in separate time zones.
- **At selected time or after registration**: The job is started at the point in time selected in the calender field. If the IP Device should be unreachable, the job will be started anew when the IP Device is registered.
- **At selected IP Device time or after registration**: The job is started at the point in time selected in the calender field. However, here, not the system time on the DLS server is valid, but the local time in the IP Device. This option is expedient when the DLS server and the IP Devices are in separate time zones. If the IP Device should be unreachable, the job will be started anew when the IP Device is registered.
- **After registration**: The job is executed when the IP Device is registered.

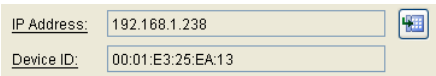
OK accepts the value in the time field, **Cancel** closes the calendar without accepting the data.

- **Time field with calendar button and Exec Time**

NOTE: Please note that no new execution time will be calculated when the IP Device is moved to another timezone meanwhile.

- **Open WBM with a current IP address**

If you click the browser button beside the **IP Address** field, Web-Based Management (WBM) opens for the workpoint in a new browser window with this IP address.



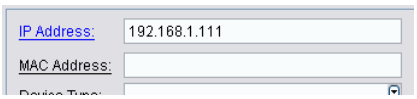
The button is only active if the field contains an IP address. For information on how to operate the WBM, refer to the Workpoint Administration Manual.

- **More icon buttons**

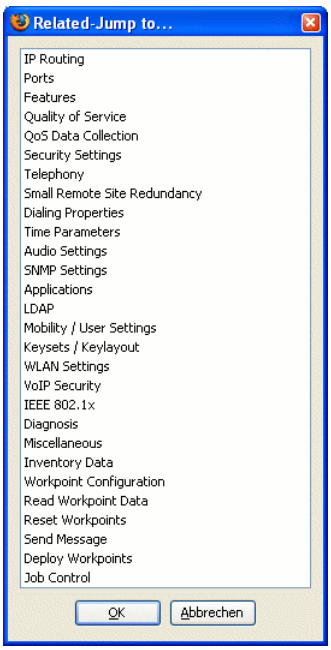
Icon buttons (for example,) appear within an object (for example, for an IP phone) when more than one entry is available or can be inserted for each object (see Section 5.4.2.4, "Multiple objects").

- **Search with parameter acceptance (Related Jump)**

  User-friendly interface links help you to search for the value entered for different fields, such as, **IP address** and **device ID**) in other interfaces under **Call: Main Menu > Call: Main Menu >** .



  Click the underlined link (shown in bright green when the mouse hovers over it).



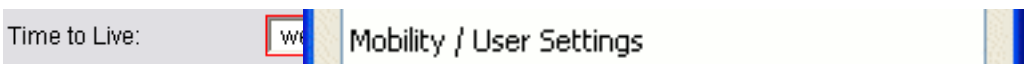
  A dialog window opens with a list of all additional topics involving **Call: Main Menu > Call: Main Menu >.**
  Select an entry from the list and click **OK**. The display then shows the interface that you selected with the value that was transferred, and a search is performed automatically.

Entry field display

Elements that do not allow direct input are dimmed on the screen). Fields that are not relevant to the current configuration are also dimmed, for example, an SIP parameter in a HFA workpoint.

Mandatory fields are shown with a black frame.

Elements that contain an invalid value are shown with a red frame after you leave the field or when an action is executed.



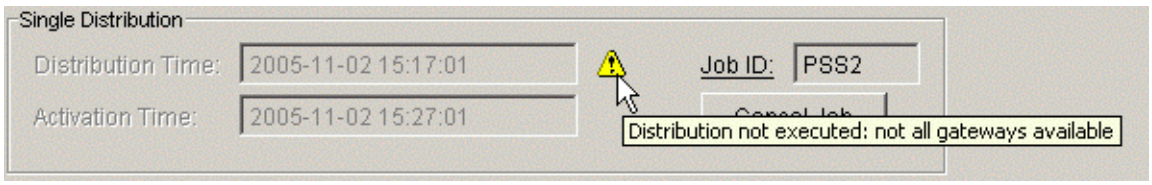
If this is the case, correct the value and perform the action again.

Often when you hover the mouse over elements, information known as "ToolTips" appears at the mouse pointer (example).



Icons beside entry fields

In certain instances, information or warning icons may appear next to some input fields. An explanation (or ToolTip) appears if you place the cursor over the icon. Example:



Icon	Area Field	Meaning
	IP Phone Configuration **IP Client Configuration** **Device Type**	Workpoint authentication at the DLS has failed. This may be due to an invalid authentication mode, for example. See Section 7.6.4.4, ""DLS Connectivity" Tab".
	IP Phone Configuration **IP Client Configuration** **Device ID**	The IP address is assigned to another device (IP address conflict). In many cases, the DHCP server has assigned the same address twice.
	IP Phone Configuration **IP Client Configuration** **Device Type**	The device type specified is not supported.
	Title Bar **Pending Alarms**	Alarm notification for selected DLS users. For further information, see Section 6.6, "Alarm Configuration".
	IP Phone Configuration **E.164**	The telephone is set up as a Mobility Phone, but no Mobile User is logged on. For more information on mobility, see Section 3.8, "DLS Mobility - General Information".
	IP Phone Configuration **E.164**	A Mobile User is logged on to the IP phone. For more information on mobility, see Section 3.8, "DLS Mobility - General Information".
	IP Phone Configuration **Device Type**	The current configured device is not yet attached, that is, it is a virtual device.
	IP Phone Configuration **IP Client Configuration** **IP Gateway Configuration** **Device Type**	The device has been deleted via API interface. If it is to be used again, it can be recovered by initiating **Read IP Device Data**.

Table 9 Information and warning icons in the content area

Icon	Area Field	Meaning
	**IP Phone Configuration** **IP Client Configuration** **Device Type**	The synchronization icon which is displayed after a database restore on all physical devices (and which indicates that the devices need to be registered - again - in DLS) does not disappear on mobility logged on devices until a log-off action is performed because only then the DLS database and the device will be synchronized. This is a functionality by designed. While a mobile user is logged on there is no way to 'Read' the base device data since a Read is executed over the active E164 number. By the negotiation of communication to acknowledge proper states in between logon and logoff actions the Arrow Icon conditions are also reflected over the GUI accordingly.
	**IP Phone Configuration**	The Remote Control button launches a new browser window with the URL of the jHPT application and the needed devices specific parameters so that the user is redirected to the HPT page for selected device. The Remote Control button is added in the IP Phone configuration mask next to the IP address field This option is offered for the following devices (SIP and HFA): OpenStage 15 OpenStage 20 OpenStage 30 OpenStage 40 OpenStage 40 US OpenStage 60 OpenStage 80 OpenStage 80 Deskphone IP 35G
	**IP Phone Configuration** **IP Client Configuration** **SIP Mobile User Configuration**	The eye view button is applied to all password fields to allow conceal /show the password content.
	**Title Bar**	An indicator that high debug trace logging is actively running. Slow performance is caused due to the high level of tracing actively running in the background. When clicked,the UI refers to Main Menu > Administration > Trace Configuration
	**Title Bar**	Alarm notification for selected DLS users. For further information, see Section 6.6, "Alarm Configuration"

Table 9 Information and warning icons in the content area

Some icons are also displayed in a separate column in Table view. This means that workpoints with particular properties (error messages) can be easily sorted and filtered out. Icons are also displayed in the main menu (Section 5.4.1, "Main Menu") and in the message window (Section 5.4.2.6, "Message Windows").

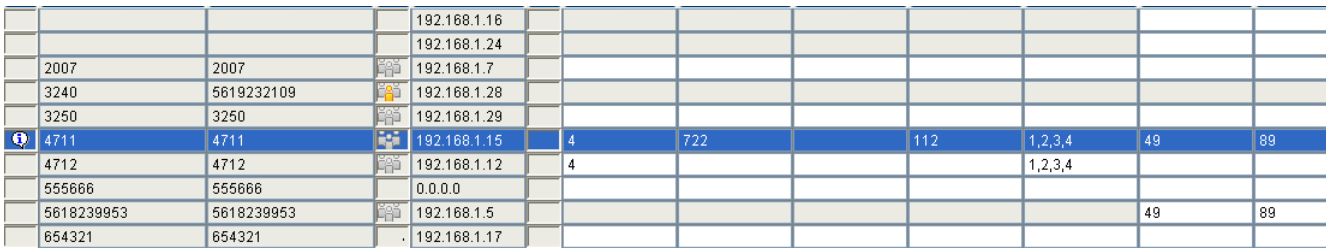
Multiple selection and data transfer in Table view

If changes were made in the **Call: Main Menu > Call: Main Menu >** area, you can transfer these changes to additional devices in the search selection.

NOTE: If running a DLS client on Windows XP, check that your color scheme is set to "Default (blue)". The list display may not work properly if your color scheme is set to "Olive Green" or "Silver".

Call: "Display Properties" > "Appearance" > "Color scheme".

Change to **Table** view **before** saving. The entry with the changed parameters is shown in dark blue.

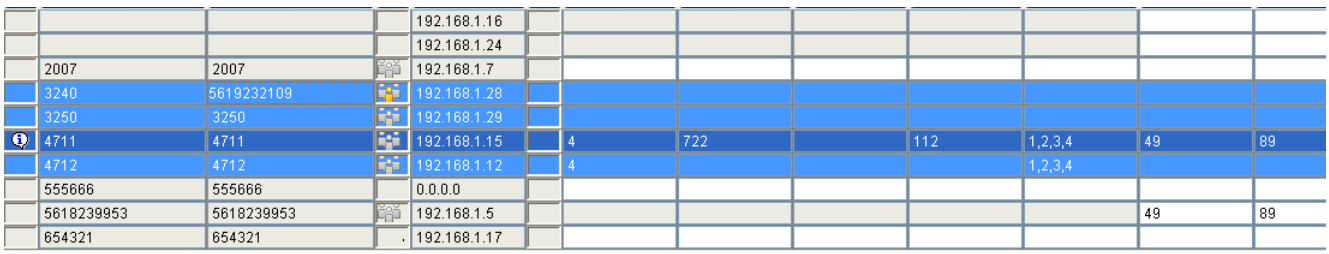


			192.168.1.16								
			192.168.1.24								
2007	2007		192.168.1.7								
3240	5619232109		192.168.1.28								
3250	3250		192.168.1.29								
4711	4711		192.168.1.15	4	722		112	1,2,3,4	49	89
4712	4712		192.168.1.12	4				1,2,3,4		
555666	555666		0.0.0.0							
5618239953	5618239953		192.168.1.5						49	89
654321	654321		192.168.1.17							

Select additional IP devices to which the changes should also apply:

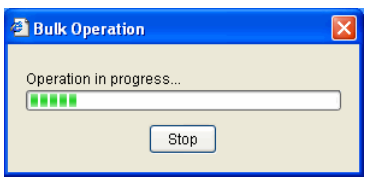
- Hold the <SHIFT> button down and click the top and bottom rows to mark all the rows in between (including the selected rows).
- Hold the <CTRL> button down and click individual entries to add or remove them from the selection.
- If you select **Edit** - **Select All** in the menu bar, you can add all selection entries.

All additional entries are shown in light blue.



			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							

Click Save to apply the data.



If you click **Stop**, the changes to the current workpoint are completed, but no additional data is transferred. To proceed, start the entire procedure anew.

After the data has been successfully transferred, a green check mark appears beside each updated entry. A note icon is displayed for entries where the job is not yet complete.



✓	192.168.1.123	Bevorzugt High Quality Sprachübertragung	Auto	G.729
✓	192.168.1.124	Bevorzugt High Quality Sprachübertragung	Auto	G.729
✓	192.168.1.125	Bevorzugt High Quality Sprachübertragung	Auto	G.729
✓	192.168.1.159	Bevorzugt High Quality Sprachübertragung	Auto	G.729
✓	192.168.1.198	Bevorzugt High Quality Sprachübertragung	Auto	G.729

Individual Layout of Table View

The user can accommodate the table view to his individual needs. These settings are stored user-specific in the DLS database, so that the individual settings are available to the user on each client.

To alter the order of table columns, click on the title of a column with the left mouse key and drag the column to the desired position.

To adjust the width of a column, move the mouse pointer to one of the margins of the column title. As soon as the pointer changes to a double arrow, press the left mouse key and drag the margin to the desired position.

Furthermore, you can determine which columns are to be displayed und which columns shall have a fixed position. For this purpose, click on the column title using the right mouse key. In the context menu which is opening up now, you can define the desired settings.

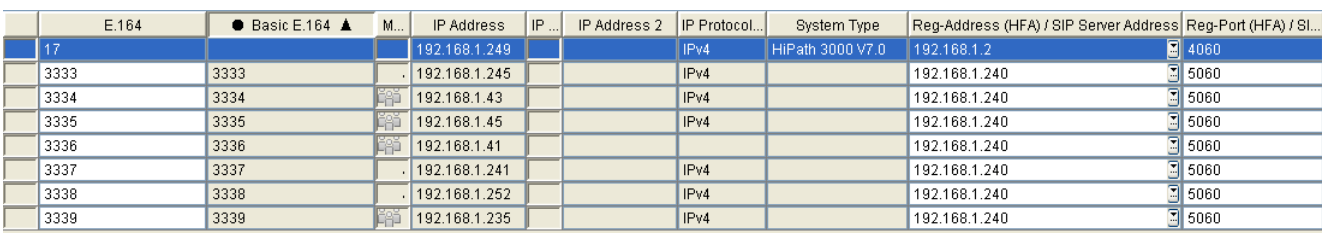
NOTE: It is possible that the individual table view settings are reset on a DLS update, if objects in the database are modified during the update.

Additional sorting columns

The user has the possibility to select more than one column in the table view for sorting. All selected columns will be combined.

The first selected column will be the main column used for sorting, while the additional selected columns will be used as sub columns.

The main column will be selected by clicking on the column header with the left mouse button. All subsequent sub-columns will be selected by pressing the “Shift” key and simultaneously clicking with the left mouse button on the desired columns. The main column will be marked with a bullet in front of the column name. The sort direction (ascending, descending) is displayed behind the column name by a triangle in up or down direction. The sort direction can be changed by clicking on the column header again.



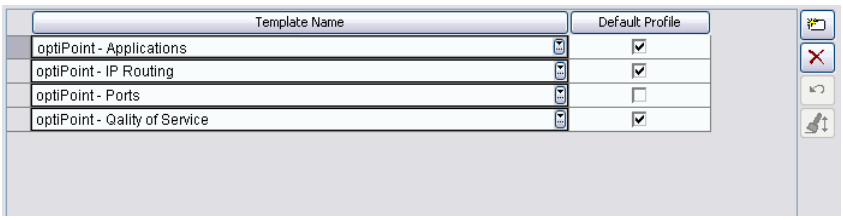
E.164	● Basic E.164 ▲	M...	IP Address	IP ...	IP Address 2	IP Protocol...	System Type	Reg-Address (HFA) / SIP Server Address	Reg-Port (HFA) / SI...
17			192.168.1.249			IPv4	HiPath 3000 V7.0	192.168.1.2	4060
3333	3333		192.168.1.245			IPv4		192.168.1.240	5060
3334	3334		192.168.1.43			IPv4		192.168.1.240	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

Selecting additional sort columns as sub sort columns may be useful if the main sort column contains multiple identical values.

Selecting additional sort columns is available only in the table view of objects. It is not available for embedded tables in the content area. For those tables, only the sort direction can be changed.

Multiple objects

Certain objects, on the other hand, allow you to create and display several different entries per object (for example, with Profile Management > Device Profile > "Templates" Tab).



The buttons have the following meaning:

Inserts a new entry.

Deletes all selected entries.

Cancels the last changes to selected entries and removes a selection.

Transfers the content of the selected row (row containing the cursor) to all selected entries.

The selected row is marked in gray in the left column. This column may contain one of the following symbols:

- * (asterisk): The entry has been changed but the changes have not yet been saved.
- + (Plus): The entry has been added to but the additions have not yet been saved.
- - (Minus): The entry has been deleted but the deletion has not yet been saved.

If any of these symbols is displayed, you can undo the change with .

The following applies when transferring data from one row to another:

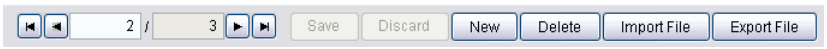
- Data is moved from the current row (the row with the cursor).
- The data is transferred to all marked rows.
- Hold the <SHIFT> button down and click the top and bottom rows to mark all the rows in between (including the selected rows).
- Hold the <CTRL> button down and click individual rows to add or remove them from the selection.
- Click the button to transfer the data (all target rows are marked with an * (asterisk) until you save the changes).

5.4.2.5 Action Buttons

Action buttons vary depending on the content area and can be used to perform various actions.



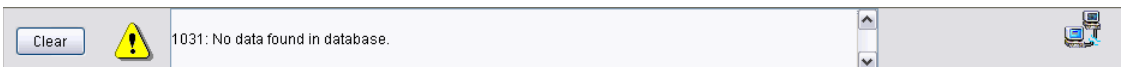
In **Object** and **Table** view, navigation buttons are shown for selecting data records. If one element is selected, the number of the selected data record is shown in the field to the left. In the window to the right, the total number of data records in the table is shown. If several elements are selected, the highest number of the selected data records is shown in the field to the left. In the field to the right, the total number of data records in the table is shown, followed by the number of selected data records in brackets.



For additional information on operating the DLS interface, refer to Section 15.3, "First Steps: Changing IP Device Parameters".

5.4.2.6 Message Windows

The message window displays status and error messages after an action is started and shows the progress of the action.



Messages are categorized by icons:

A warning message is shown, for example, if a search was unsuccessful.

An error message is shown, for example, if you enter an invalid value.

You can delete all messages that were output at any time with **Clear**.

A progress bar is displayed on the right for certain actions, such as, scanning IP devices.

You can change the size of the message window by clicking and dragging the separator between the message window and the remaining work area.

5.4.3 Status Area

This area informs about the load on each node of a DLS cluster. In the appropriate DLS screen, the name of each node and the number of requests on this node during the last hour are displayed. The display is also available on a single node DLS configuration; in this case, it will not change, but the number of requests could be important in case of an overload situation.

NOTE: This feature is available for the adminstrator only.

In the status area, the following symbols are used:

Server is running with full capacity.

Server is running with half capacity. This is the case when

- the number of requests is lesser than 50% of the maximum number, and
- the difference between the maximum and the actual request count is greater than 10.

Server is set to inactive.

Two different status views are available:

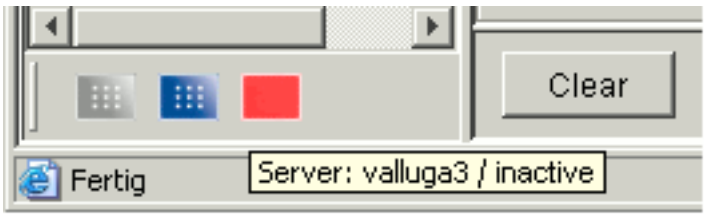
Basic View

The basic view (default) displays the nodes of a DLS Cluster as server symbols in the left lower corner. The names of the DLS nodes and the number of requests during the last hour are displayed as tooltip.

This example shows a node called "valluga2" which is running at full capacity, and has received 49 requests during the last hour:



In this example, the DLS node "valluga3" has been integrated in the cluster, but is currently not active:



Extended View

To arrive at the extended view, click on a server symbol with the right mouse key. The DLS cluster menu opens up; select **Switch Layout**.

The extended view displays detailed informations, e.g. the names of DLS nodes and number of requests.

In the following example, one node is running at half capacity, one at full capacity, and one node is set to inactive.



Cluster Menu

In basic view or extended view, click on a server symbol with the right mouse key to get the DLS cluster menu.



The following functions are available here:

- **Refresh Cluster** Status: Refreshes the data (symbol, request count) for all nodes.
- **Reset Requests**: Sets the request count to 0 for all nodes.
- **Show Cluster Data**: Forwards to **Administration** > **Cluster Configuration** > **Deployment Server**.
- **Switch Layout**: Toggles between basic view and extended view.

5.5 Search Functionality

You can use the following wildcards or special characters in all text fields in **Search** view. All fields are combined internally using a logical AND. For example, if you specify a device type and an IP address range, only those IP Phones that correspond to the specified device type and that also belong to the specified IP address range are selected. When searching in embedded tables, all objects are found which match at least the search criterion. After the search, these objects are displayed completely.

- * (asterisk): Stands for any sequence of characters. It may be combined with other wildcards. Partial inputs, such as, 192.168.*, are consequently possible for an IP address range from 192.168.0.0 to 192.168.255.255.
- ? (Question mark): Stands for exactly one character. It may be combined with other wildcards. For example: ab??c finds all records where the field has 5 chars starting with ab and ending with c
- ^ (Circumflex): Stands for an empty field. It cannot be combined with wildcards. For example: ^ finds records with empty field, a^a finds records with field containing the string "a^a"
- ! (Exclamation mark): As first character of a string, the search string will be inverted. Therefore "!search string" finds all records where the regarding field contains anything else than „search string”. The exclamation mark may be combined with *,? and |. The ‘!’ must be marked with a leading ‚\’ when itself is the first character of the search string. It may be combined with other wildcards. For example: !a* finds records with field not starting with a
- < (Lower than): As first character of a string "<search string" all values lower than the “search string” will be found. The ‘<’ must be marked with a leading ‚\’ when itself is the first character of the search string. It cannot be combined with other wildcards. For example: <100 finds all records with field value lower than 100
- > (Greater than): As first character of a string ">search string" all values greater than the “search string” will be found. The ‘>’ must be marked with a leading ‚\’ when itself is the first character of the search string. It cannot be combined with other wildcards. For example: >Munich finds all records with field value greater than Munich, that means Paris, Oslo but not Berlin and Athens
- | (Vertical bar): Different search strings are separated from each other and are used for OR search. All elements containing "search string1|search string2| search string3" are found. The combination with wildcards is not allowed, but the search can be inverted ('!'). Therefore all elements not containing "search string1|search string2| search string3" are found. The ‘|’ must be marked with a leading ‚\’ when itself is to be searched. For example: abc|def|ghi finds all records where the field contains abc, def, OR ghi !abc|def|ghi finds all records where the field contains anything but abc, def, OR ghi.

6 Administration

Call: Main Menu > Administration

Basic settings for operating the DLS are made in the **Administration** area.

This menu contains the following submenus:

- Account Management
- PKIDLS-2790
- 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 Security Log Files
- Trace Configuration
- Server Licenses

6.1 Account Management

This area features the following components:

- Account Configuration
- Policy Settings
- Roles and Rights

For maintenance issues it is helpful to delegate tasks to multiple persons. These may obtain different accounts. For security reasons it is not wanted that each account has access to every area of the DLS. Hence, the several areas can be allowed or disallowed individually.

To each administrative function, an access right is assigned, and only accounts with this access right are allowed to call this function. In some cases, multiple functions are combined in a single right, for instance, the right to create jobs comprehends the right to edit jobs, like, e. g., update the job status or reset the job.

There is no right which disallows an access explicitly.

The DLS offers a role concept. Each role groups bundles a number of rights. It is possible to define as much roles as necessary.

Some important roles are preconfigured and cannot be changed or deleted, only the default description text can be modified. These system roles are primarily used as patterns for self-defined roles. Not each of these roles makes sense when used all by themselves.

To each account, as many roles as needed can be assigned. The resulting right is the sum of all rights of all assigned roles.

After a new installation of the DLS, an 'admin' account exists, which has all rights based on system defined roles. This account remains undeletable and it's name remains unchangeable, and the system roles cannot be removed from it.

When logging with the admin account on DLS user interface via Assistant for the first time after the installation, the default password must be changed for security reasons. The password must be updated in Assistant too.

With an update installation from a DLS without Account Management to a DLS with Account Management, an 'admin' account with all system defined roles is created. Therefore, the admin account has all rights. To all other accounts, the INFO role is assigned. This enables them to open all screens and to search for all data, but all other functions are disabled. All other roles and rights have to be set manually.

With future DLS upgrades, new functions and new masks will be accessible by system roles only. New rights must be added to user defined roles manually. Therefore it is recommended to set rights by combination of system roles and small user defined roles, rather than copying and modifying system roles.

Example

Goal: An account shall receive editing rights (except bulk-change and create-template) for gateways only.

- Variant A: Define a new role completely based on empty rights table.
- Variant B: Define a new role based on EDIT_ONE and additionally set the 'Search' right in every relevant mask (Gateway Configuration, QoS Data Collection).
- Variant C: Define a new role with 'Search' right for all gateway masks (Gateway Configuration, QoS Data Collection) PLUS system role EDIT_ONE.

Only in variant C, the account automatically obtains the right to use newly added functions in the three gateway masks.

NOTE: Changes on currently used roles will take effect after next login.

6.1.1 Account Configuration

Call: Administration > Account Management > Account Configuration

Here you can configure additional accounts, change passwords, and add or remove roles to/ from existing accounts.

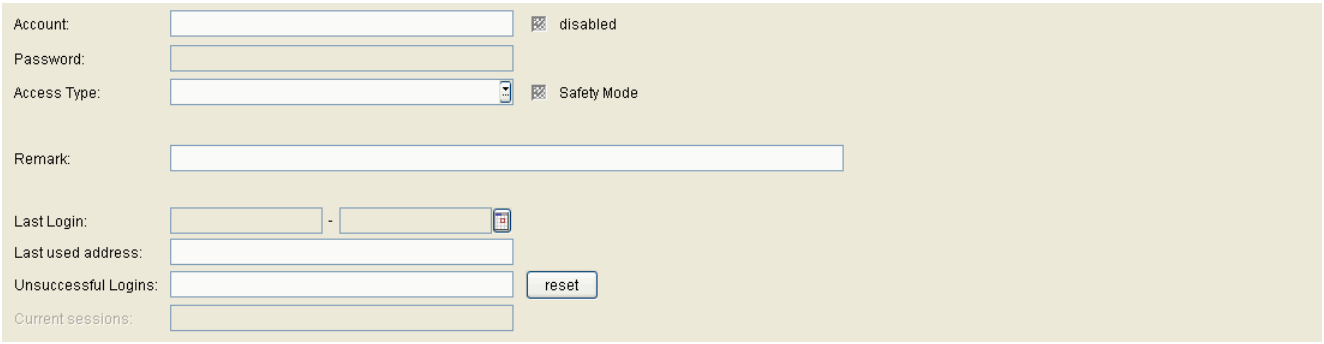
Only those accounts which have the account handling right are authorized to edit accounts, i. e. set up new accounts, or change, or delete existing ones.

If multi-tenancy is used, it is recommended to assign the account management role only to those accounts which have editing rights for **all** tenants. If an account does not have permissions for all tenants, it cannot see all tenants that have been set up. Thereby, the user of this account might try to set up a new account with a name that already exists. In such a case, an accordant error message will appear, and the account will not be set up.

This area features the following components:

- General Data
- Possible Action Buttons
- "Roles" Tab
- "Rights" Tab
- "Tenants" Tab
- "User certificates" Tab

General Data



Account:

Name of the account.

disabled

This checkbox is activated if this account is disabled.

Password:

New (modified) password for this account.

The password should contain at least six characters and should be non-trivial. Unsuitable entries include words that can be found in dictionaries and lexica. Ideally, you should choose a combination of numbers, special characters, and letters that do not contain a personal reference.

Access Type:

Select the allowed interfaces to the DLS server.

Possible options:

- **DLS-GUI**
  Access to the DLS server is exclusively permitted via the DLS user interface.
- **DLS API (Webservice Interface)**
  Access to the DLS server is permitted exclusively via the programming interface.

NOTE: For information on using the DLS program interface (DLS API), see Section 16.13, "Operating the DLS via the Program Interface (DlsAPI)"

Safety Mode

If this checkbox is activated, configuration changes which may cause an IP Device malfunction must be acknowledged in an additional dialog window.

Remark:

Field for general information.

Last Login

Shows the date and time of the last successful login.

Last used address

Address from which the last login (both successful and unsuccessful) was initiated.

Unsuccessful Logins

Number of unsuccessful logins since last successful login.

reset

Resets the number of unsuccessful logins in order to unlock this account.

Current Sessions

Shows the number of current sessions.

Possible Action Buttons

Search

Searches for all registered accounts that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new account.

Save

Saves the data entered/modified.

Discard

Discards any unsaved changes.

Delete

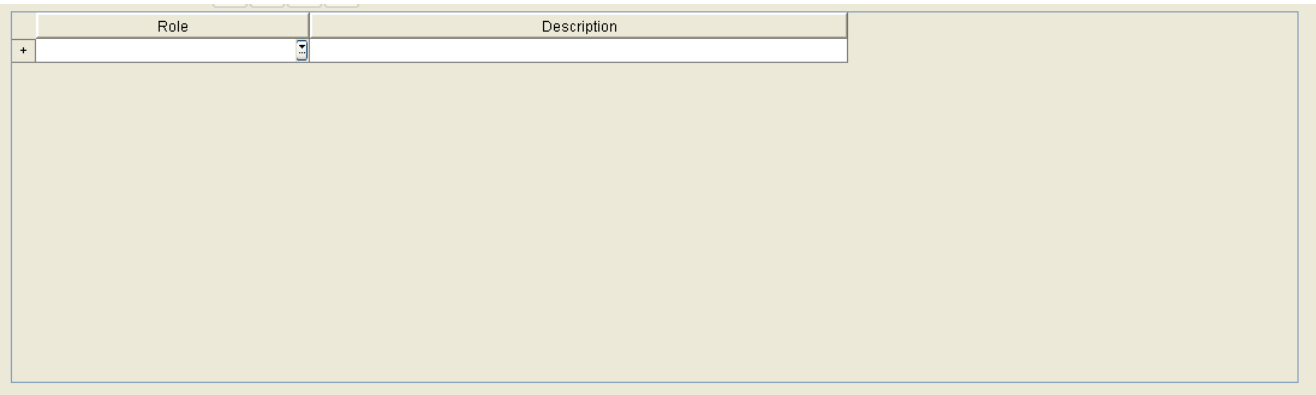
Deletes one or more accounts (multiple selections possible in Table view) except 'admin' account.

Refresh

Refreshes the content of the relevant page.

6.1.1.1 "Roles" Tab

Call: Administration > Account Management > Account Configuration > "Roles" Tab



Role

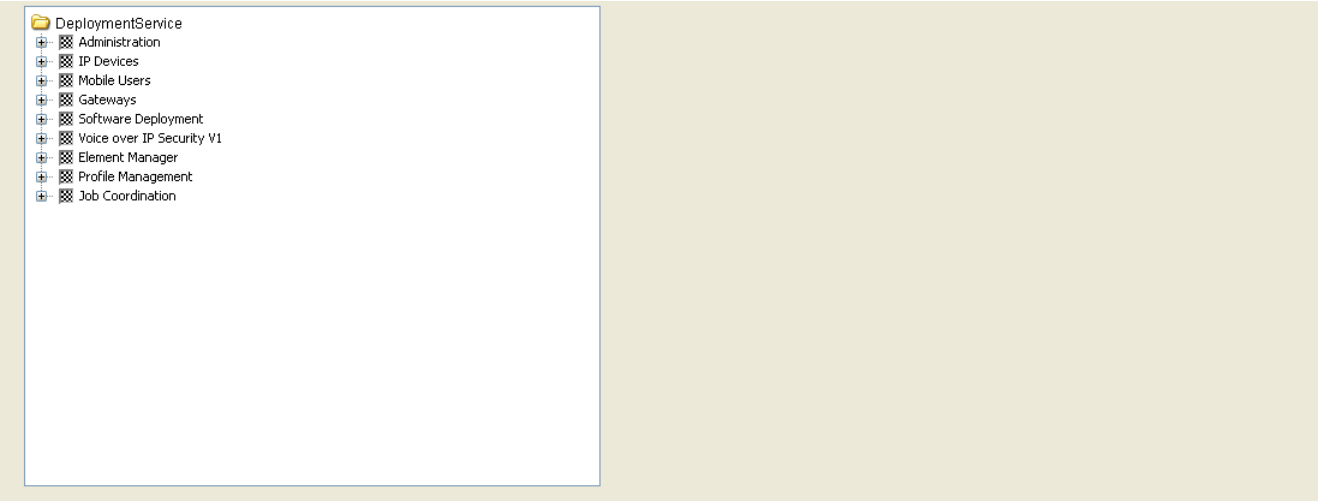
Name of roles which are assigned to this account. System defined roles cannot be removed from the 'admin' account.

Description

Detailed description of this role.

6.1.1.2 "Rights" Tab

Call: Administration > Account Management > Account Configuration > "Rights" Tab

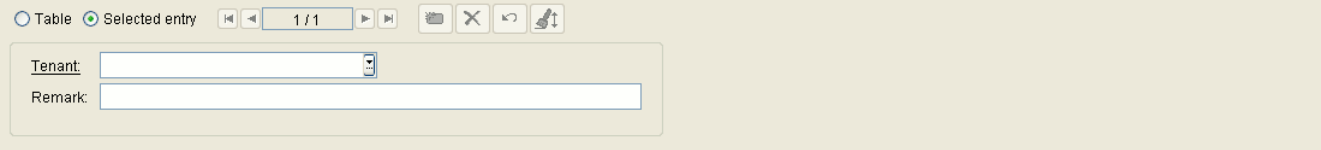


Here, the sum of all rights from the different roles is displayed for each account.

6.1.1.3 "Tenants" Tab

Call: Administration > Account Management > Account Configuration > "Tenants" Tab

NOTE: This tab is available only if the DLS multi tenancy function is installed.



Tenant

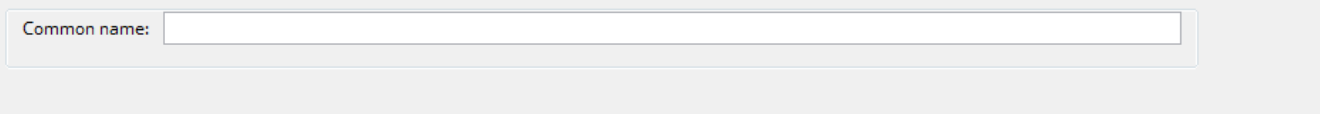
Name of tenants which are assigned to this account.

Remark

Information on the tenant.

6.1.1.4 "User certificates" Tab

Call: Administration > Account Management > Account Configuration > "User certificates" Tab



When the administrator logs in to create new accounts he should additionally map each account to a number of user certificates. This is possible with ''User Certificates'' Tab which includes the list of the Common names (CN) mapped to the DLS user and the ability to add or delete.

> ***IMPORTANT:*** This mapping is used only for the smart-card based login to DLS and works if the "**Use CaC Authentication Method**" checkbox is enabled in "Policy Settings" menu under ''Login Policy'' Tab (refer to Section 6.1.2.2, ""Login Policy" Tab"

Common name

Common names (CN) that are assigned to this DLS account. One DLS account can be mapped to more than one CNs, but a certain CN can't be mapped to more than one DLS account. This mapping is used when Common Access Card (CAC) sign-on to DLS web client is enabled.Refer to Section 6.1.2.2, ""Login Policy" Tab"

6.1.2 Policy Settings

Call: Administration > Account Management > Policy Settings

In this area, the policy for the DLS users (accounts) is defined, such as length, or special character content.

This area features the following components:

- General Data
- Possible Action Buttons
- "Password Policy" Tab
- "Login Policy" Tab
- "Session Policy" Tab

General Data



Access Type:

Shows the interface to the DLS server that is relevant for these policy settings. To switch to another access type, use the navigation in the action button area:



Possible valuse:

- **no access**
  This user account is disabled.
- **DLS-GUI**
  Access to the DLS server is exclusively permitted via the DLS user interface.
- **DLS API (Webservice Interface)**
  Access to the DLS server is permitted exclusively via the programming interface.

NOTE: For information on using the DLS program interface (DLS API), see Section 16.13, "Operating the DLS via the Program Interface (DlsAPI)"

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the data entered/modified.

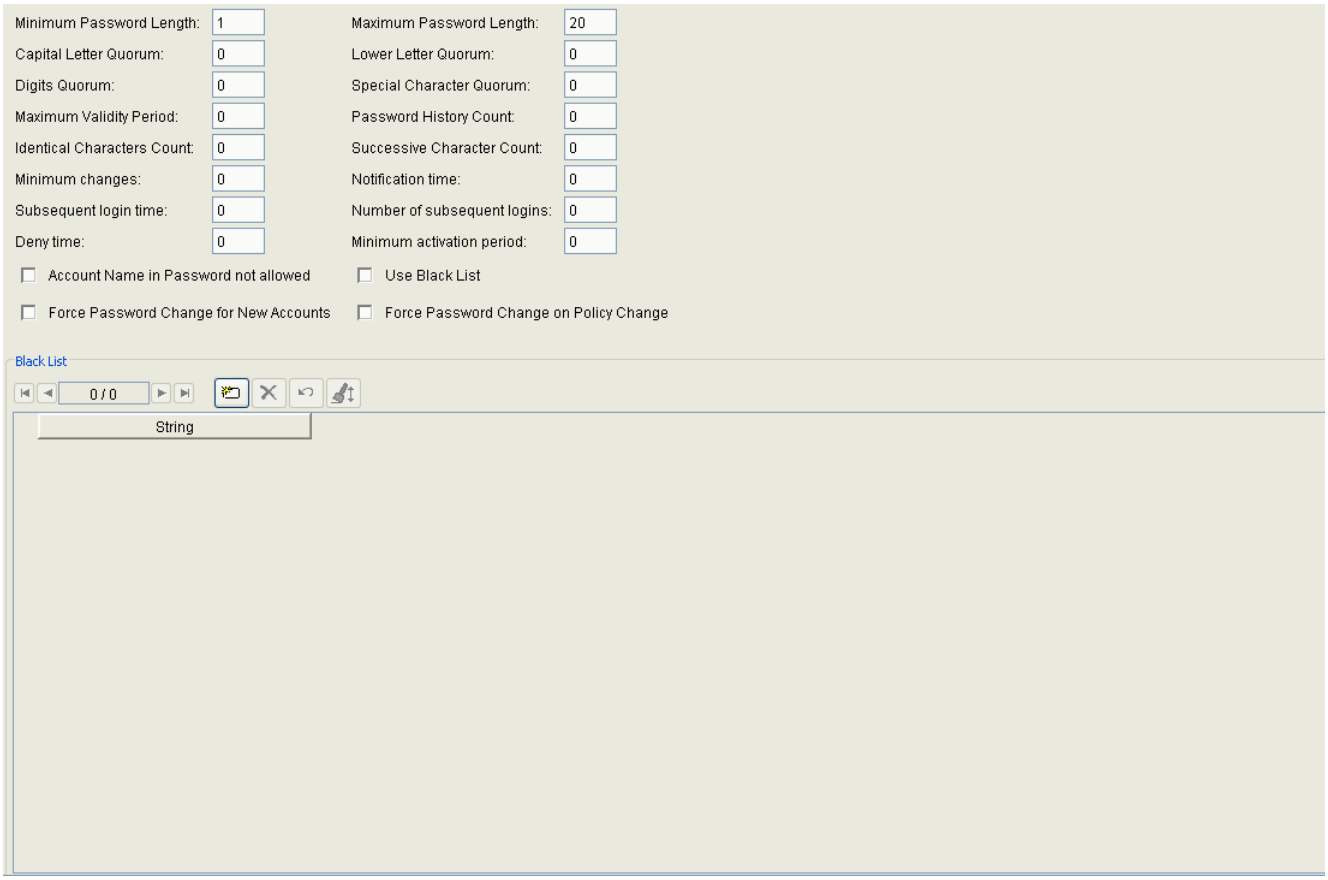
Refresh

Refreshes the content of this mask from the database.

6.1.2.1 "Password Policy" Tab

Call: Administration > Account Management > Policy Settings > "Password Policy" Tab

In this area, the password policy for the DLS user accounts is defined, such as length, or special character content.



Minimum Password Length

Minimum password length.

Value range: **1** - **20**

Default: **1**

Maximum Password Length

Maximum password length.

Value range: **1** - **20**

Default: **20**

Capital Letter Quorum

Minimum count of capital letters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Lower Letter Quorum

Minimum count of lower case letters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Digits Quorum

Minimum count of numeric characters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Special Character Quorum

Minimum count of special characters in the password.

Value range: **0** - **20**

Default: **0** (= no check)

Maximum Validity Period

Maximum age of password in days, must be greater than the **Notification Time** value.

Value range: **0** - **180**

Default: **0** (= no check)

Password History Count

Count of stored old passwords which cannot be used again.

Value range: **0** - **10**

Default: **0** (= no check)

Identical Characters Count

Allowed length of a sequence of identical characters.

Value range: **0** - **20**

Default: **0** (= no check)

Successive Character Count

Count of ascending or descending characters in a sequence.

Value range: **0** - **20**

Default: **0** (= no check)

Minimum changes

Minimum number of characters that must be altered at password change.

Value range: **0** - **20**

Notification time

Period before password expiration within which the users are notified of a password change that will become due. Value must be less than the **Maximum Validity Period** value.

Value range: **0** - **30**

Subsequent login time

Grace period in days within which the use of an expired password may be continued.

Value range: **0** - **90**

Number of subsequent logins

Number of logins at which the use of an expired password may be continued.

Value range: **0** - **3**

Deny time

Interval in days during which a password my not be selected again as a new password by the same account.

Value range: **0** - **180**

Default: **0** (=no check)

Minimum activation period

Minimum time interval in hours that must pass before an existing password can be changed again.

Value range: **0** - **168**

Account Name in Password not allowed

If this check box is set, the DLS will check whether the account name is part of the password, neither in correct nor in reversed sequence. If this is the case, the password will not be accepted. Default: no check.

Use Black List

If this check box is set, the desired password will be checked against the black list (see **String** parameter). Default: no check.

Force Password Change for New Accounts

If this check box is set, the password must be changed with the first logon of a newly registered account.

The concerning GUI user is able to login with the pre-defined password; after this, he will be prompted by a message window to change the password. Before then, all other functions are locked.

A concerning API user will not be able to logon initially. For this purpose, a GUI user with the appropriate account management rights must change the password of the API account. Default: not set (no password change required).

Force Password Change on Policy Change

If this check box is set, a password must be changed with the next logon in case it does not conform to the current password policy.

The concerning GUI account is able to login to DLS GUI with its old password; after this, he will be prompted by a message window to change the password. Before then, all other functions are locked.

A concerning API user will not be able to logon initially. For this purpose, a GUI user with the appropriate account management rights must change the password of the API account. Default: set (password change is required).

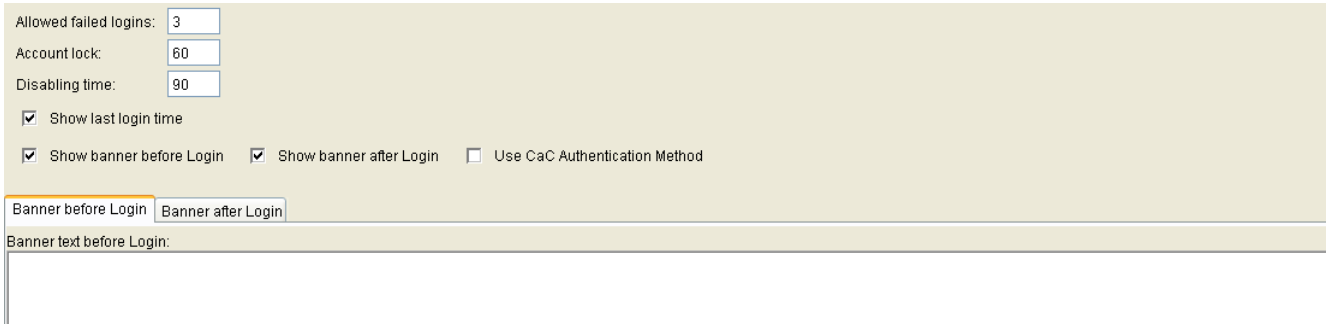
Black List

String

List of customer defined strings which may not be contained in new defined passwords (Black list). The check will be case insensitive.

6.1.2.2 "Login Policy" Tab

Call: Administration > Account Management > Policy Settings > "Login Policy" Tab



> ***IMPORTANT:*** The following policy settings apply to all users except for administrator user ’’ admin’’. in case of a user with name "admin" (the user that is automatically created from dls and cannot be deleted in any case) the "lock out" policy setting is not taken into consideration.

Allowed failed logins

Allowed number of consecutive failed logins. When this number is exceeded, the account is locked for the time specified in **Account lock**.

Value range: **2** - **5**

Account lock

When the allowed number of failed logins (**Allowed failed logins**) has been exceeded, the account will be locked for the time span specified here.

Value range: **0** - **300**

Disabling time

When an account has not been used for the number of days specified here, it will be disabled.

Value range: **0** - **180**

Show last login time

When active, the time of the last login is shown after each successful login in a separate dialog box.

Show banner before Login

When active, the pre-login banner is shown after the DLS client has been started.

Show banner after Login

When active, the post-login banner is shown after every login.

Use CaC Authentication Method

This switch enables the Common Access Card (CAC) sign-on to DLS web client. CAC sign-on enables users to log in to the DLS web client directly with a smart card that stores a valid user certificate, and users only need to enter a card PIN, instead of a user name and password. A CAC smart card enables two-factor authentication: the CARD being something you have, and the CAC PIN being something you know.
The sign-on process is as follows:

5. The user inserts a CAC into a card reader.
6. The smart card middle-ware automatically loads the user's personal certificate ("user certificate") from the CAC to the browser.
7. The browser prompts the user to select an installed certificate to log in and user selects the user certificate to log in.
8. The user is prompted to enter the PIN of the user's CAC.
9. The user enters the correct PIN.
10. The web server passes the user certificate to the web application server for validation which can include any combinations of the following checks:
    issuer check for trusted CA (It depends on the trust policy settings in Administration > Server Configuration > TLS Connector Configuration), using the OCSP, certificate is not expired, etc. The certificate type must be Smart Card.
11. The DLS server extracts the Common name (CN) from the user certificate and verifies if this CN is assigned to a DLS GUI user. If the CN value matches a name in the assigned CNs, the server logs the user in; otherwise the server rejects the login request.

NOTE: By default, the authentication based on DLS username and password is enabled. Only one authentication method is recommended be active at a time.

Banner before Login

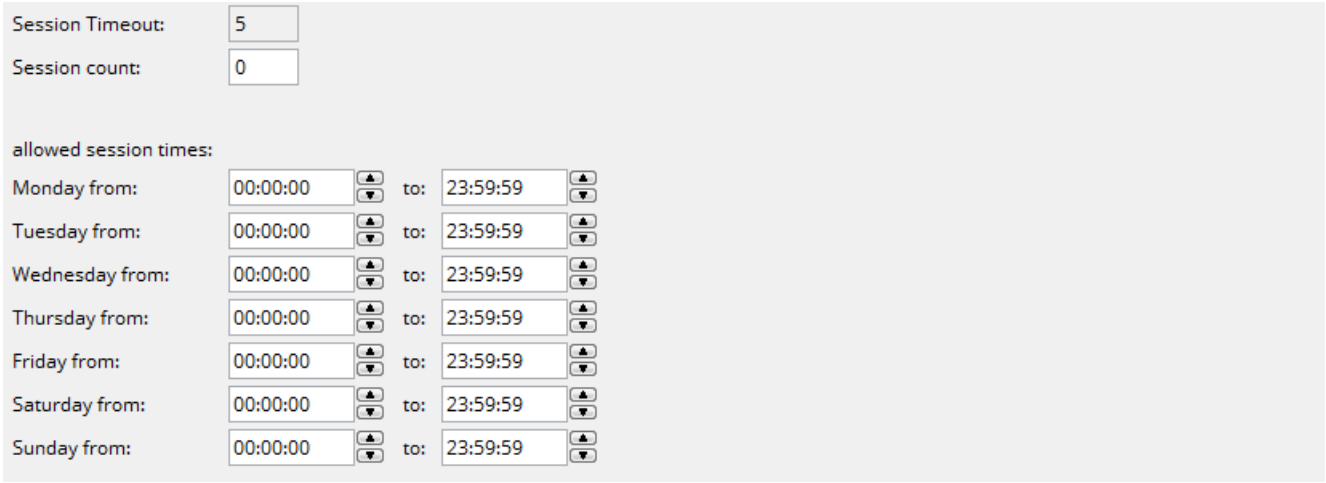
Text for the pre-login banner which is shown after DLS client startup. It is recommended to provide a bilingual text.

Banner after Login

Text for the post-login banner which is shown after every login. It is recommended to provide a bilingual text.

6.1.2.3 "Session Policy" Tab

Call: Administration > Account Management > Policy Settings > "Session Policy" Tab



Session Timeout

In case of inactivity, sessions will be closed after the time span specified here (in minutes).

Default value :.1440 min

Session Count

Allowed number of sessions for an account at the same time.

(**0** = no limit)

Allowed session times

Outside of these periods, no account is allowed to login, except the admin account.

Monday ... Sunday from... to

Defines start time and end time of the allowed session time periods for each day.

6.1.3 Roles and Rights

Call: Administration > Account Management > Roles and Rights

Here you can define new roles with the appropriate rights or modify existing ones. System defined roles cannot be modified or deleted.

There are some system defined default roles which cannot be modified or deleted:

Role	Rights	Weight
ACCOUNT_MGM	All existing rights for the **Account Configuration** area.	90
EDIT_BULK	All editing rights (new, delete, and edit) for all masks, except: • Roles and Rights • Account Configuration • all template activities This role is appropriate for the standard administrator. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	60
EDIT_GENERAL_ONE	All editing rights for non system related screens without the bulk change possibility. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	20
EDIT_ONE	Like EDIT_BULK, yet without the possibility for multiple selection.	40
EDIT_PKI	All editing rights for PKI related screens. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	98
EDIT_SYSTEM	All editing rights for system related screens (like Backup/Restore) except: • **Roles and Rights** • **Account Configuration** As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	30
INFO	Right to view and search data in all available masks, no editing right.	10
INFO_GENERAL	Right to view and search all non-system related screens (like Backup/ Restore), no editing rights.	0
INFO_PKI	Right to view and search PKI related screens, no editing rights.	15
INFO_SYSTEM	Right to view and search all system related screens (like Backup/Restore), no editing rights.	5
ROLE_MGM	All existing rights for the **Roles and Rights** area.	99

Role	Rights	Weight
SECURITY_MGM	Right to handle security settings separately. During installation, all security-relevant functions are assigned to this system role; this cannot be changed. This role is assigned to the master admin account. Each account having the both roles ACCOUNT_MGM and SECURITY_MGM can assign the SECURITY_MGM to other accounts. Accounts having only one of the mentioned roles cannot assign SECURITY_MGM to other accounts. Each account having the both roles ROLE_MGM and SECURITY_MGM can assign security relevant functions to non-system roles. Accounts having only one of the mentioned roles cannot do this. Only accounts having the right to execute security relevant functions are able to see these functions in the DLS GUI.	100
TEMPLATE_MGM	Right to edit templates. Valid in all areas in which templates are available. As a rule, this role is not usable in a self-contained way, but must be combined with another role, or serves as a base for defining a new role.	50

To be able to create roles, you need an account that contains the role ROLE_MGM. You can assign a user defined name and a random combination of rights to any new role.

As soon as a role is displayed in the **Roles and Rights** mask, you can copy it by clicking **New**, providing a new name under **Role name** and subsequently clicking on **Save**.

To add roles to accounts or remove roles from accounts, you need an account which contains the role ACCOUNT_MGM.

This area features the following components:

- General Data
- Possible Action Buttons
- "Rights" Tab
- "Policy Settings" Tab

General Data

Role name:

Name of role, to which rights will be assigned.

System defined role

Shows whether this is a system defined role. Such roles cannot be edited or deleted.

Description:

Detailed description of the role.

Displayed in object view only.

Role Weight

If at least one of the roles assigned to the account has password policy settings of its own, the settings of the role with the highest weight are valid and overwrite the equivalent global policy settings for that account. For weight values of system defined roles see the Roles-Weight-Rights table above. These values cannot be changed.

All weights of customer defined roles can be changed by those accounts which have the ROLE_MGM role. The default weight for customer defined roles is **0**.

Displayed in table view only.

Value range: **0** - **100**

Use System Policy

If activated, all specific policy settings for this role are ignored.

Displayed in table view only.

Possible Action Buttons

Search

Searches for all rights that match the search criteria.

When searching for rights, the checkboxes may have following meanings:

 Search for active rights.

 Search for inactive right.

 Right will not be considered when searching.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new account.

Save

Saves the data entered/modified.

Discard

Discards any unsaved changes.

Delete

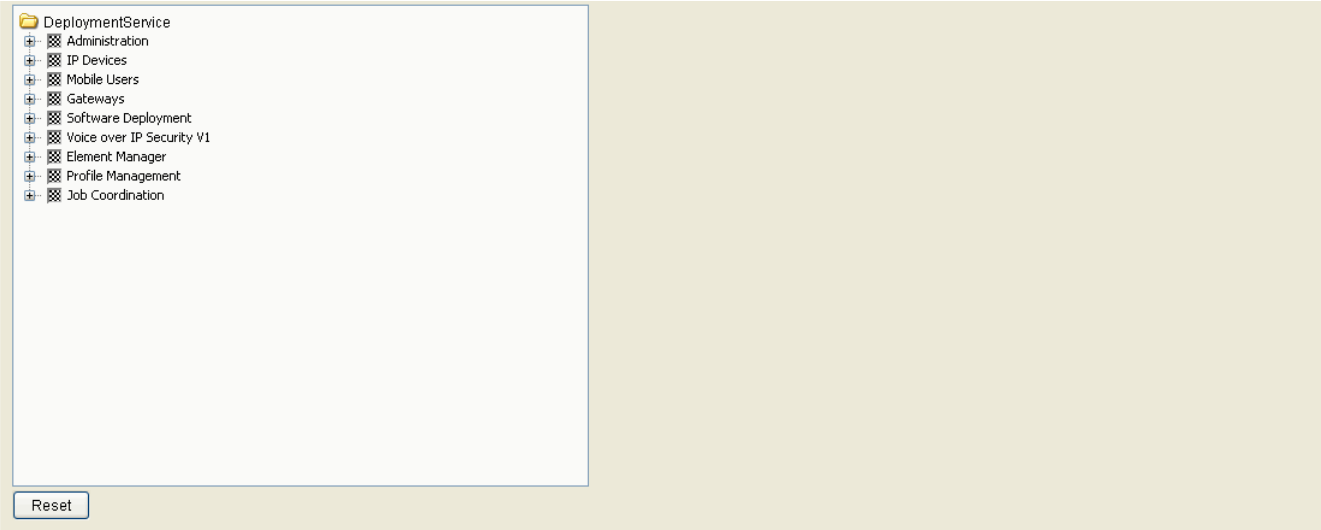
Deletes one or more rights (multiple selections possible in Table view).

Refresh

Refreshes the content of the relevant page.

6.1.3.1 "Rights" Tab

Call: Administration > Account Management > Roles and Rights > "Rights" Tab



Rights:

The rights will be defined on function level.

Possible options:

Area: Right is active for this area. Submenu: Rights is active in all areas of this submenu.

Area: Right is not active for this area. Submenu: Right is not active in any area of this submenu.

Submenu: Right is active in at least one area of this submenu.

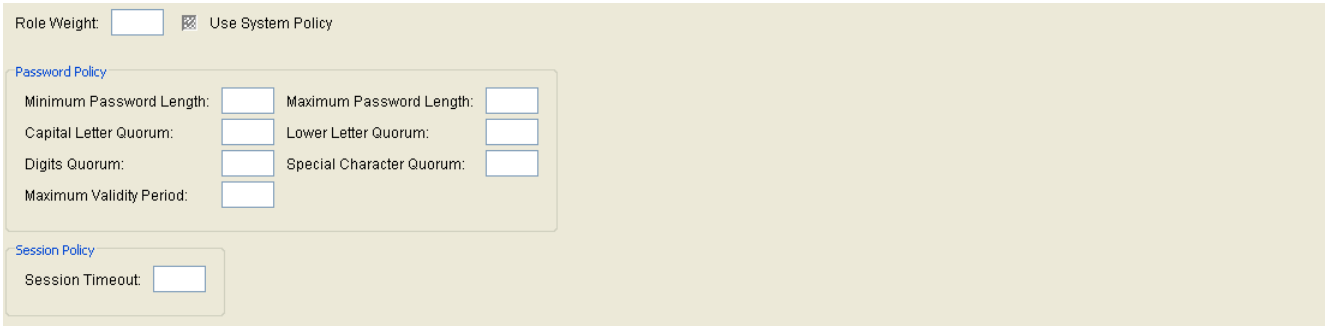
Right is undefined.

Reset

Clicking this button resets all fields to inactive.

6.1.3.2 "Policy Settings" Tab

Call: Administration > Account Management > Roles and Rights > "Policy Settings" Tab



Role Weight

The extensive the rights of a role are, the higher its weight should be. Role dependent settings will be passed on to accounts.

Value range: **1** - **100**

Use System Policy

If activated, the global system policy settings will be used instead of the role specific settings.

Password Policy

Minimum Password Length

Minimum length of a valid password.

Value range: **1** - **20**

Default: **1**

Maximum Password Length

Maximum length of a valid password.

Value range: **1** - **20**

Default: **20**

Capital Letter Quorum

Number of capital letters the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Lower Letter Quorum

Number of lower letters the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Digits Quorum

Number of digits the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Special Character Quorum

Number of special characters the password must contain.

Value range: **0** - **20**

Default: **0** (= no check)

Maximum Validity Period

Maximum validity period of a password in days.

Value range: **0** - **180**

Default: **0** (= no check)

Session Policy

Session Timeout

When there has been no activity for the period (in minutes) specified here, the session will be closed. If the value is 0, there will be no check.

Value range: **5** - **999999**

Default: **1440**

6.2 PKI

This menu item consists of the following areas:

- Plug-In Configuration
- Connector Configuration
- Internal CA
- Renewal

6.2.1 Plug-In Configuration

Call: Administration > PKI > Plug-In Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "General Features" Tab
- "Issuing CAs" Tab
- "Plug-In Properties" Tab

General Data



PKI Connector Plug-In

Name of the PKI connector plug-in configuration.

Description

Description of the PKI connector plug-in configuration

Plug-In Type

The plug-in module used for this configuration

Possible values:

- **DLS Internal Plug-In**
- **DLS Storage Plug-In 1.0**
- **MSCA Connector Plug-In 1.0**

enable Plug-In

Enables this plug-in configuration. A PKI connector license may be required to be able to use an external PKI.

Before plug-in configuration can be enabled, a synchronization with the PKI must be executed via the **Synchronize** Button.

Possible Action Buttons

Synchronize

Synchronization with the PKI must be executed before the plug-in can be enabled. The result of the synchronization will be displayed in the status bar. During synchronization, the data on **"General Features" Tab** and **"Issuing CAs" Tab** will be read out from PKI and written to the DLS database.

Search

Searches the database for PKI plug-in configurations that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Thus, existing entries can be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for PKI plug-in configuration.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

6.2.1.1 "General Features" Tab

Call: Administration > PKI > Plug-In Configuration > "General Features" Tab

The data displayed here have been read out from the PKI and written to the DLS database via the **Synchronize** function. These data cannot be changed.



Revocation supported

Indicates if this plug-in configuration supports revocation requests.

Available Key Algorithms

Available Key Algorithms.

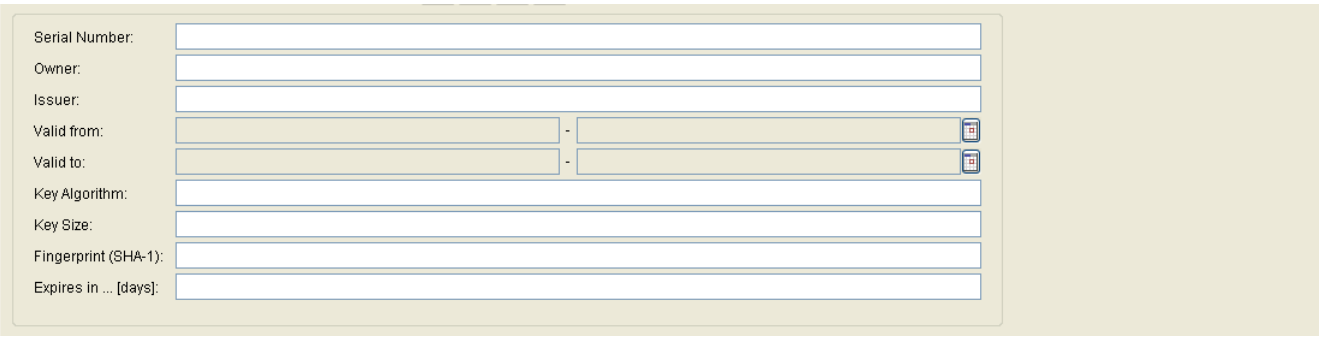
Available Key Sizes

Available Key Sizes.

6.2.1.2 "Issuing CAs" Tab

Call: Administration > PKI > Plug-In Configuration > "Issuing CAs" Tab

The data displayed here have been read out from the PKI and written to the DLS database via the **Synchronize** function. These data cannot be changed.



Serial Number

Serial number of the certificate (display only).

Owner

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm:

Key Algorithm for certificate (display only).

Key Size:

Key Size for certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA1 (160 bits/20 characters) for certificate (display only)

Expires in ... [days]:

Certificate will expire in ... days (display only).

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

6.2.1.3 "Plug-In Properties" Tab

Call: Administration > PKI > Plug-In Configuration > "Plug-In Properties" Tab



Each plug-in must provide a set of property name/value pairs used for its configuration. These parameters are plug-in specific but can be configured using this generic table. Values must be configured with care, as the user interface cannot provide validity checks. A message is displayed after setting wrong values or keys. These messages are plug-in dependent and more information must be obtained from the PKI Basic configuration guide.

For further PKI plug-in properties refer to the **DLS V10 PKI Basic Configuration Guide** under:
http://apps.g-dms.com:8081/techdoc/en/P31003S23A0S101RQ7620/P31003S23A0S101RQ7620.pdf

Property Name

The name of the configuration attribute.

Value

The value of the configuration attribute.

6.2.2 Connector Configuration

Call: Administration > PKI > Connector Configuration

A connector configuration is used to

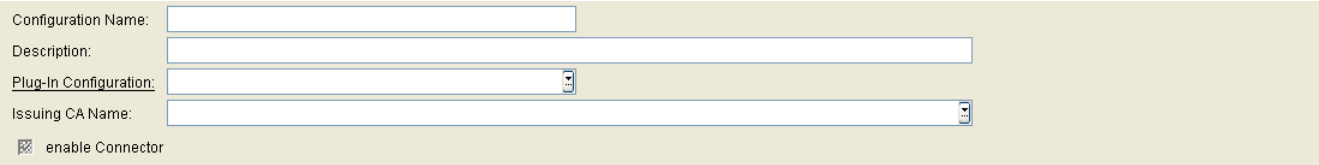
- define the plug-in configuration used to access the external PKI,
- choose an issuing CA to request certificates from and to be able to verify relationship with the configured trust anchor,
- define high level parameters used in the certificate request sent to the CA,
- define and import the trust anchor to be deployed to devices when using this configuration.

A connector configuration can be dedicated to a certificate type (e.g. SPE, 802.1x, WBM …) or can be used as a global configuration for all / some types of certificates to be deployed.

This area features the following components:

- General Data
- Possible Action Buttons
- "Request Parameter" Tab
- "Certificate Renewal" Tab
- "Trust Anchor" Tab
- "User Certificates" Tab

General Data



Configuration Name

Configuration Name.

Description

Description.

Plug-In Configuration

Corresponding plug-in configuration.

Issuing CA Name

Issuing CA Name.

enable Connector

Before enabling the plug-in configuration, synchronization with the PKI must be executed.

Possible Action Buttons

Search

Searches the database for configured PKI connector configurations that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Thus, existing entries can be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for PKI connector configuration.

Save

Saves the field contents to the database.

Discard

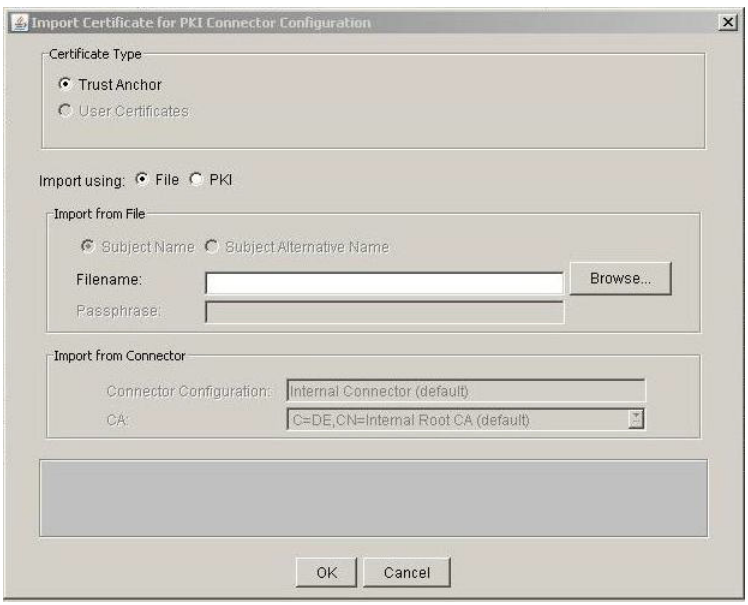
Discards any changes entered.

Refresh

Updates the window using the database.

Import Certificate

Import trust anchor or user certificate into DLS. A dialog window will ask for the current settings.



The Trust Anchor certificate is used when a Server CA certificate is requested from this connector.

At the time user certificates are imported to the connector, the following data are stored in the DLS database:

- The PKI Connector ID

- The Certificate ID. This is the Subject or the Subject Alternative Name of the certificate. The combination of the PKI Connector ID and the Certificate must be unique.Its up to the administer to select at the tome of the import whether the Subject or the subject Alternative Name must be used for Certificate ID
- The Issuer Name
- The Certificate

IMPORTANT: HiPath 4000 oriented Certificates can only be imported for Trust Anchor through a file and not PKI.

For further information on CA certificates please refer to Section 16.5, "Configuring Certificates in DLS".

6.2.2.1 "Request Parameter" Tab

Call: Administration > PKI > Connector Configuration > "Request Parameter" Tab

When a certificate is created for OS phone devices using a PKI Connector with "DNS Name" selected as CN or SAN and the automatic DNS name construction is enabled at device level, the DNS name shall be constructed by DLS using the device attributes without performing a DNS reverse look-up. Otherwise, a DNS look-up shall be performed.



Common Name

Common Name.

Possible values:

- **MAC Address**
- **DNS Name**
- **IP Address**

NOTE: Default & only available **Common Name** value for OpenScape 4000.

Subject Alternative Name

Subject Alternative Name.

Possible values:

- **None**
- **MAC Address**
- **DNS Name**
- **IP Address**

MAC Address Delimiter

Delimiter option for MAC Addresses.

Possible values:

- **Colon**
- **Dash**
- **None**

> ***NOTE:*** MAC address delimiter can be configured only if **Common Name** and **Subject Alternative Name** are set to 'MAC Address'.

Key Algorithm

Key Algorithm.

Possible values:

- **DSA**
- **RSA**

Key Size

Key Size.

Possible values:

- **512**
- **1024**
- **2048**
- **4096**

Validity Offset (days)

Validity Offset (days).

Validity Period (days)

Validity Period (days).

Test

Test the PKI Connector Configuration.

6.2.2.2 "Certificate Renewal" Tab

Call: Administration > PKI > Connector Configuration > "Certificate Renewal" Tab

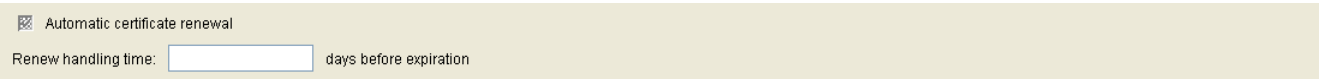
This tab allows settings for renewal of this connector configuration.

If a certificate which has been requested using this configuration, is soon running out, an automatic renewal can be configured.
NOTE: Renewal of certificates will always result in requesting a new certificate. Extending the validity of an already deployed certificate is not supported. .

It is expected that the connector configuration which is used for requesting and deploying the old certificate, is still available for this device. If not, there is no association between a certificate (which will expire soon) and configurations required to request and provide a new certificate.

In such occasions, an alarm will be issued and the certificate deployment must be handled manually if there is no global renewal configuration available.

This configuration may also be used by the global renewal configuration (See also Section 6.2.4, "Renewal").



Automatic Certificate Renewal

Enables automatic renewal for this configuration. If automatic renewal requires another issuer (CA with longer lifetime) or even another PKI, this configuration can be changed accordingly (this may also require a new trust anchor in some situations).

NOTE: A new configuration, identified by its name, will have no association to already deployed certificates and cannot be used for their renewal. In this case,a global renewal configuration is required (see also Section 6.2.4, "Renewal").

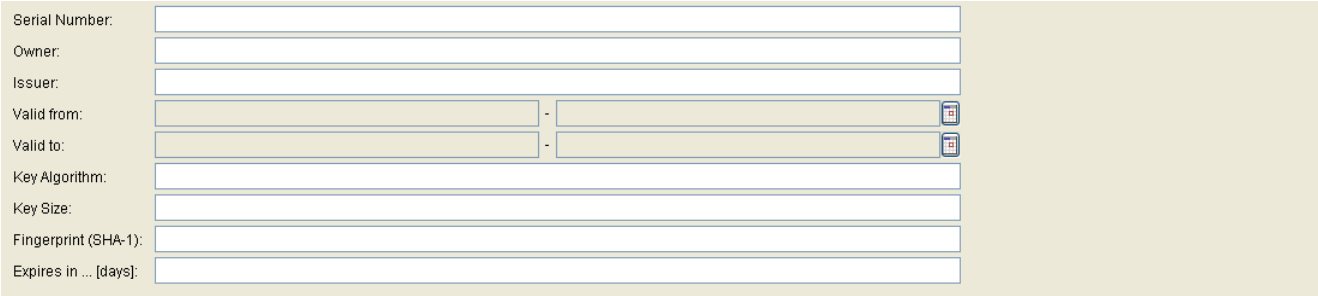
Renew Handling Time

The time interval (in days) at which a renewal will be scheduled before a certificate (issued using this configuration) runs out.

6.2.2.3 "Trust Anchor" Tab

Call: Administration > PKI > Connector Configuration > "Trust Anchor" Tab

For each configuration, a trust anchor must be configured. In most scenarios, this will be the Root CA itself, but can be a subordinate CA as well. If a trust anchor is not available, the configuration cannot be saved!



Serial Number

Serial number of the certificate (display only).

Owner

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm:

Key Algorithm for certificate (display only).

Key Size:

Key Size for certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA1 (160 bits/20 characters) for certificate (display only)

Expires in ... [days]:

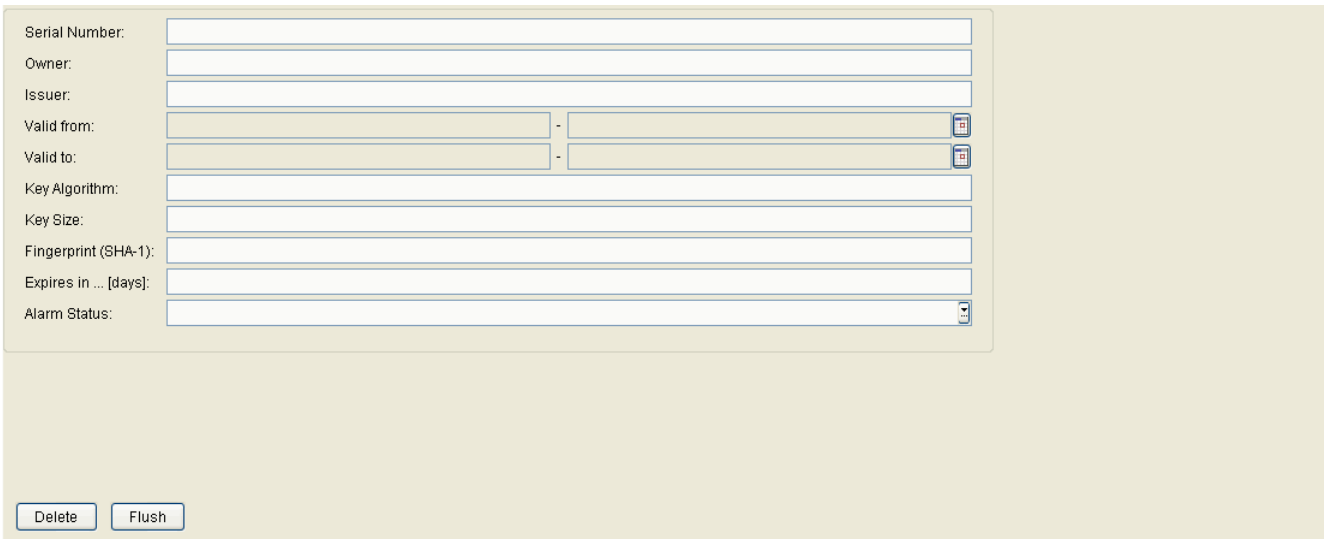
Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

6.2.2.4 "User Certificates" Tab

Call: Administration > PKI > Connector Configuration > "User Certificates" Tab

For each configuration, User Certificates must be configured.



Serial Number

Serial number of the certificate (display only).

Owner

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm:

Key Algorithm for certificate (display only).

Key Size:

Key Size for active certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA1 (160 bits/20 characters) for certificate (display only)

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Alarm Status of the certificate

Possible values:

- **valid**
- **soon running out**
- **expired**

Delete

By clicking this button the certificate will be deleted.

Flush

By clicking this button the certificate will be send.

6.2.3 Internal CA

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

General Data



CA Name

Name of CA.

Description

Description of CA.

enable Internal CA

Switch to enable the internal CA. For this purpose, a CA must have been created, either via **Import CA** or **Create CA**.

Possible Action Buttons

Search

Searches the database for configured PKI connector configurations that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Thus, existing entries can be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for PKI connector configuration.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

Import CA

Import CA from .zip file.

Export CA

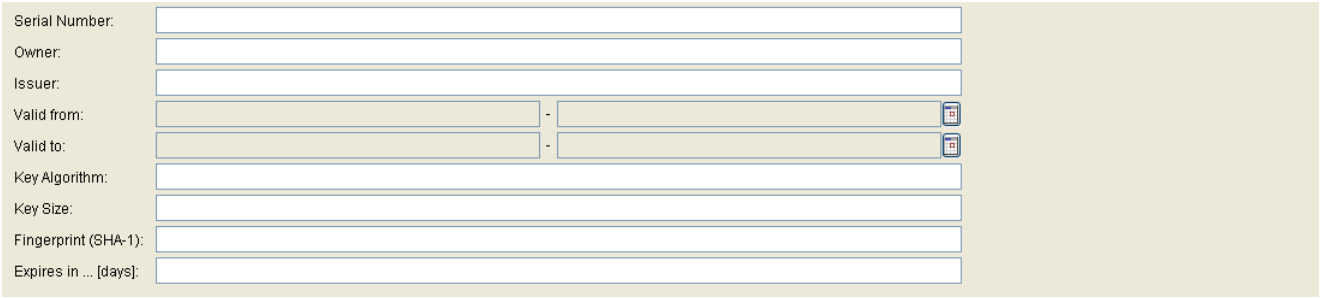
Export CA to a .zip file.

Create CA

Create CA from a DLS data record.

6.2.3.1 "Info" Tab

Call: Administration > PKI > Internal CA > "Info" Tab



Serial Number

Serial number of the certificate (display only).

Owner

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm:

Key Algorithm for certificate (display only).

Key Size:

Key Size for certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA1 (160 bits/20 characters) for certificate (display only)

Expires in ... [days]:

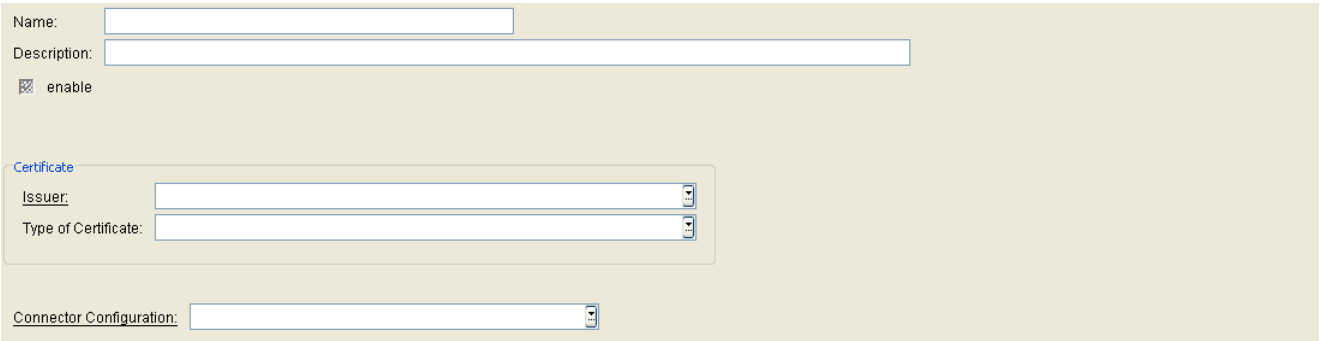
Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

6.2.4 Renewal

Call: Administration > PKI > Renewal

With this function, general renewal settings for all certificates of a type can be made.



Name

Name of renewal configuration.

Description

Description for renewal configuration.

enable

Activates configuration. Enable (disable) all global certificate renewal settings.

Certificate

Issuer:

Issuer of the certificate,required to match.

Type of Certificate

Type of certificate.

Possible values:

- **ALL**
- **Phone Certificate**

- **WBM Server Certificate**
- **SPE Certificate**

In case of ALL the certificate type is not used for matching.

NOTE: The “ALL” option equals “Phone Certificate’’ , “WBM Server Certificate” & “SPE Certificate’’.

Connector Configuration

The connector configuration to be used if issuer and type of certificate matches.

When certificates are reaching their end of lifetime period, a renewal may be initiated automatically. As there may be various connector configurations and external PKIs available to send renewal requests to, it has to be determined which configuration (thus which plug-in and which external PKI) must be used. There are also situations where the origin configuration used to create the present certificate has been lost or cannot be determined.

For such occasions, a global configuration is required to link a certificate by its issuer to a connector configuration used to request a new certificate and replace the old one.

The process uses a predefined order for searching a connector configuration:

1. lookup a connector configuration matching the issuer and the type of certificate using the global certificate renewal configuration, otherwise
2. find and use the original configuration used to request the present certificate, otherwise
3. rise an alarm because no renewal configuration can be found using global alarm settings

The process checking the remaining certificate validity period runs in the interval specified in Alarm ConfigurationSettings Tab (see also Section 6.6.7 "Settings" Tab) .

NOTE: This process is required to run once per day

NOTE: Renewal of certificates will always result in requesting a new certificate. Extending the validity of an already deployed certificate is not supported.

6.3 Server Configuration

This menu item consists of the following areas:

- Tenants
- Location
- P&P Settings
- FTP Server Configuration
- HTTPS Server Configuration
- HTTPS Client Configuration
- Network Drive Configuration
- Infrastructure Policy
- API Notifications
- XML Applications
- Options
- TLS Connector Configuration

6.3.1 Tenants

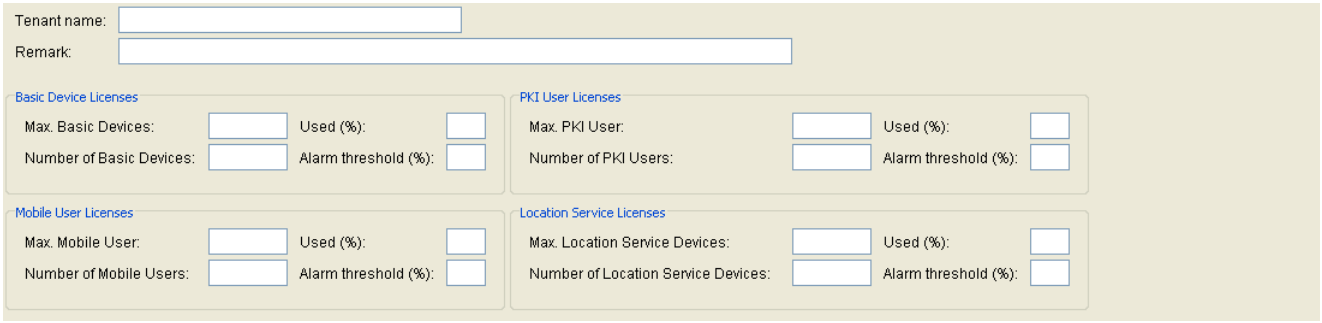
Call: Main Menu > Administration > Server Configuration > Tenants

NOTE: This screen is visible only if multi tenancy is installed4.

This area features the following components:

- General Data
- Possible Action Buttons
- "Locations" Tab

General Data



Tenant Name

Unique name of the tenant.

Remark

Information on the tenant.

Basic Devices Licenses

Max. Basic Devices

Allowed maximum number of basic devices for this tenant.

Number of Basic Devices

Number of registered IP Devices for this tenant

Used (%)

Indicates how many percent of existant basic device licenses are used currently.

Alarm threshold

When this threshold is exceeded, a license alarm will be generated

Mobile User Licenses

Max. Mobile User

Allowed maximum number of Mobile Users for this tenant.

Number of Mobile Users

Number of registered Mobile Users for this tenant.

Used (%)

Indicates how many percent of existant Mobile User licenses are used currently.

Alarm threshold

Specify the percentage of used mobile user licenses that should generate a license alarm.

PKI User Licenses

Max. PKI User

Allowed maximum number of devices for this tenant which are supplied via PKI.

Number of PKI Users

Number configured PKI users.

Used (%)

Percentage of PKI user licenses used.

Alarm threshold (%)

When expiring this threshold, a license alarm will be generated.

Location Service Licenses

Max. Location Service Devices

Allowed maximum number of location service devices for this tenant.

Number of Location Service Devices

Number of IP Devices supplied with IP Infrastructure data by means of Location Service.

Used (%)

Indicates how many percent of existant location service licenses are used currently.

Alarm threshold (%)

Specify the percentage of used location service licenses that should generate a license alarm.

Possible Action Buttons

Search

Searches the database for configured tenants that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Thus, existing entries can be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for a tenant.

Save

Saves the field contents to the database.

Discard

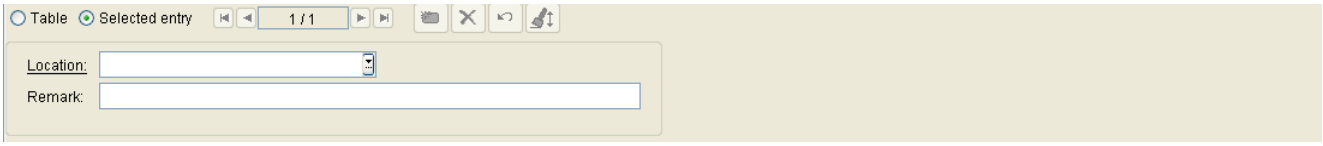
Discards any changes entered.

Refresh

Updates the window using the database.

6.3.1.1 "Locations" Tab

Call: Main Menu > Administration > Server Configuration > Tenants > "Locations" Tab



Location

Name of the location.

Remark

Description of the location.

6.3.2 Location

In this area, you can define locations to group end devices that share common properties, for example, range of IP addresses, registrar addresses, or E.164 number pattern.

IP address ranges are configured via **Administration** > **Server Configuration** > **Location** > **"IP Ranges" Tab**.

IP addresses or host names of systems (PBX/gateway or SIP server) for a location can be specified under **Administration** > **Server Configuration** > **Location** > **"Reg-Addresses" Tab**.

You can find further configuration possibilities under **Administration** > **Server Configuration** > **Location**.

If no location is defined, all location specific parameters are specified in the **Default location**.

To enable the reuse of existing templates or device profiles when client networks are to be divided up into affiliates, hierarchical location definitions are available. For instance, the parent location can be defined by business groups, and divided up into child locations by E.164 patterns. Those standard profiles which are defined for child locations extend or overwrite the data of the parent location's standard profiles.

To check a location or profile configuration, the administrator has the possibility to simulate Plug&Play with location specific data for a device. The determined parameter values are stored temporarily and can be displayed under **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration**.

To prevent overlapping locations, the following restrictions have been devised:

- The property which defines a child location must be different from the property that defines a parent location. Therefore, if a parent location has been defined by a E.164 pattern, the child location must be defined by a different property.
- Per level, only one certain property is allowed for defining a location. Example: All parent locations are defined by registration addresses. The child locations of one certain parent location are defined by business groups, while the child locations of another parent locations are defined by E.164 pattern.
- Overlapping definitions of locations are not allowed.

To establish a child location, create a new location and assign an already existing location as parent location to it. This location may not function as child location by itself.

The properties of the parent location are visible in the child locations; only subsets of the parent location's properties can be configured. However, the restrictions for software and certificate deployment (**"SW Deployment Restrictions" Tab** and **"Certificate Deployment Restrictions" Tab**) in a child location are independent of the settings of the parent location.

Automatic jobs which are started for a parent location affect all end devices residing in this location resp. in a child location of this location. In detail, the following applies:

- With automatic software deployment, rules in child locations take priority over rules in the corresponding parent locations.
- With automatic certificate deployment, the requested certificates are distributed to all IP Devices, both those in the parent locations and those in all child locations.
- With automatic archiving, all IP Devices are archived, both those in parent locations and those in child locations.

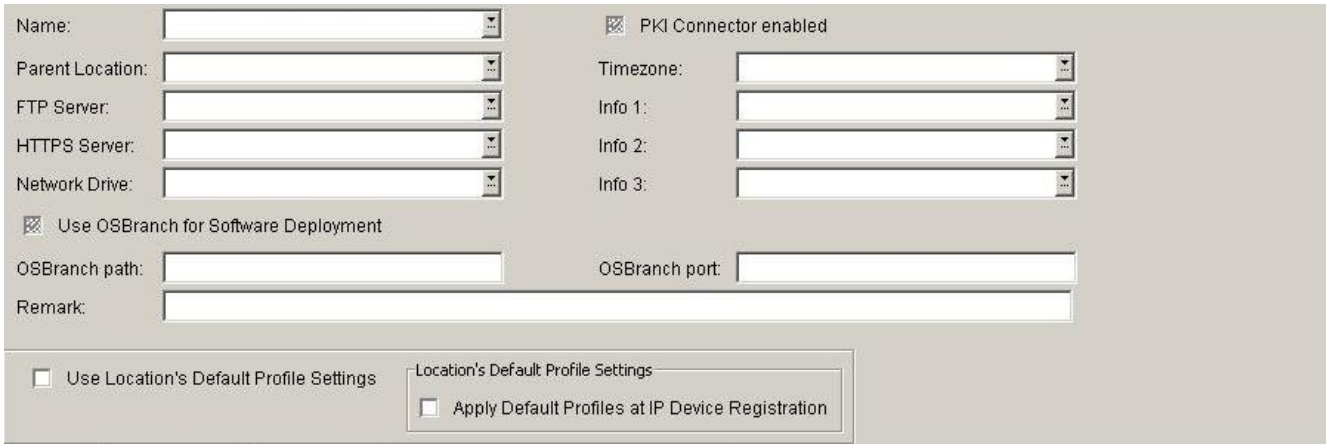
- Automatic Mobile User Logoff: Mobile Users belonging to the parent location including all its sub locations are logged off.
- With Plug&Play, virtual devices within a number pool are assigned to a location appropriate to their E.164 number.
- With Plug&Play and multi tenancy, virtual devices within a number pool are assigned to a tenant appropriate to their E.164 number.

For a location, the following items can be defined: FTP server, temporal software deployment restrictions, and an infrastructure policy.

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Ranges" Tab
- "Reg-Addresses" Tab
- "E.164 Patterns" Tab
- "Business Groups" Tab
- "Infrastructure Policies" Tab
- "P&P Number Pool" Tab
- "SW Deployment Restrictions" Tab
- "Certificate Deployment Restrictions" Tab
- "Tenants" Tab

General Data



Name:

Location name.

Parent Location

Shows the parent location, if existant.

FTP Server:

FTP server for the location.

> ***IMPORTANT:*** If the location of the manage rule does not have any FTP or HTTPS server assigned (in the location mask), then get firmwares from FTP / HTTPS servers that are not assigned to any other location, i.e. not bound to any other location.
> If the location of the manage rule has FTP and/or HTTPS server(s) assigned (in the location mask), then get firmwares only from that FTP and/or HTTPS servers.

HTTPS Server:

HTTPS server for the location.

IMPORTANT: If the location of the manage rule does not have any FTP or HTTPS server assigned (in the location mask), then get firmwares from FTP / HTTPS servers that are not assigned to any other location, i.e. not bound to any other location.
If the location of the manage rule has FTP and/or HTTPS server(s) assigned (in the location mask), then get firmwares only from that FTP and/or HTTPS servers.

Network Drive:

Network drive for the location.

Use OSBranch for Software Deployment:

If this checkbox is active, OSBranch is used for Software Deployment.

OSBranch path:

The path to the directory containing the phone software images provided by the OSBranch.

OSBranch port:

Port number for software deployment communication (phone software images) with the OSBranch.

Remark:

Remark.

Timezone:

Defines timezone for location. For possible values, please consult the choice list.

Info 1:

Additional optional Information of location, e.g. address information.

Info 2:

Additional optional Information of location, e.g. address information.

Info 3:

Additional optional Information of location, e.g. address information.

Location's Default Profile Settings

Use Location's Default Profile Settings:

If this checkbox is activated, the configuration of the '' Apply Default Profiles at IP Device Registration'' at Location level is enabled.

The **Location's Default Profile Settings** apply to all devices of the specific location.

This checkbox is disabled by default.

Apply Default Profiles at IP Device Registration

If this checkbox is activated, the default profile defined in **Profile Management** > **Device Profile** for a particular location is identified and used for each registration.

This checkbox is not applicable (N/A) by default.

> ***NOTE:*** If the "Use Location's Default Profile Settings" checkbox is not activated, the "Apply Default Profiles at IP Device Registration" is not applicable and shall be grayed out.
> If it is activated, the "Apply Default Profiles at IP Device Registration" shall be offered for configuration.

> ***IMPORTANT:*** As of CV441 onwards, the **Apply Default Profiles at IP Device Registration** option also applies to the initial registration of the device even if the device is not P&P configured.

Possible Action Buttons

Search

Searches the database for configured locations that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new data record for a location.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

Export Location

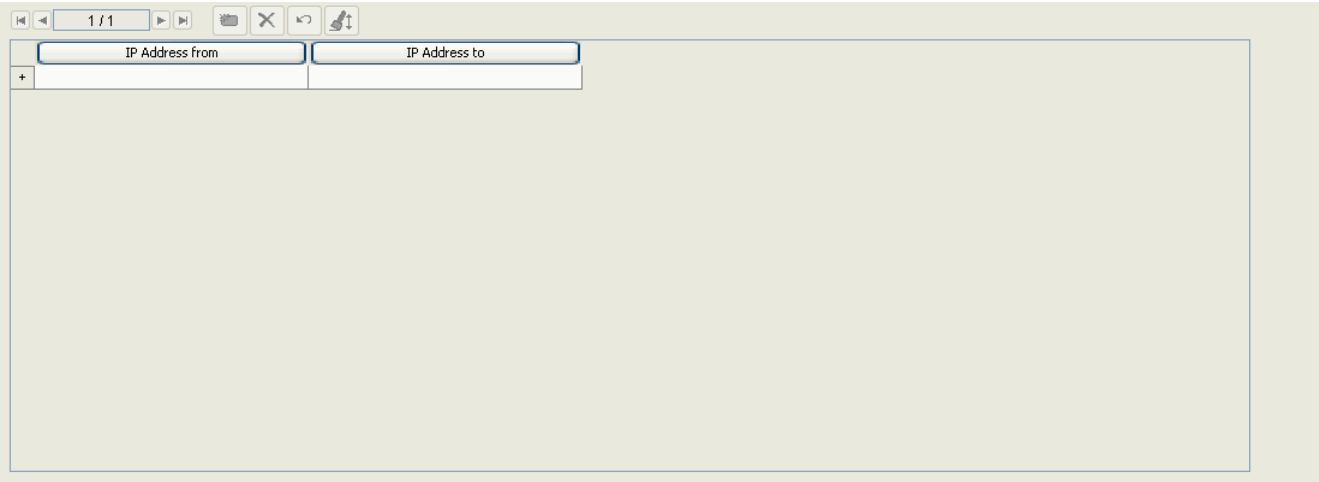
Export the selected locations to a file in .zip format.

Import Location

Import locations from a file in .zip format.

6.3.2.1 "IP Ranges" Tab

Call: Main Menu > Administration > Server Configuration > Location > "IP Ranges" Tab



IP Address from

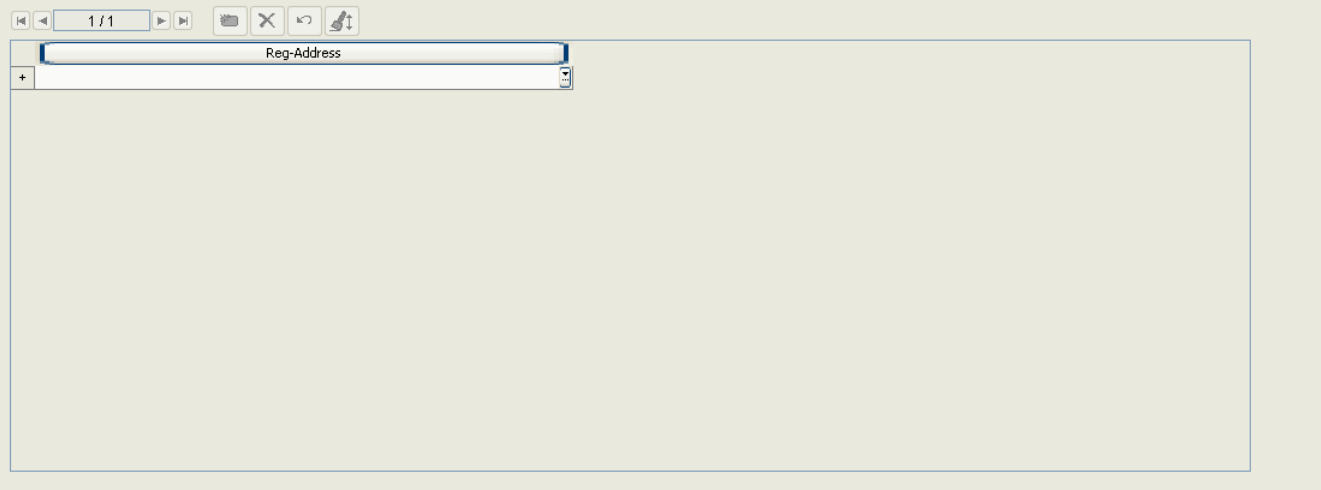
Lowest value for the IP range associated with this location.

IP Address to

Highest value for the IP range associated with this location.

6.3.2.2 "Reg-Addresses" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Reg-Addresses" Tab

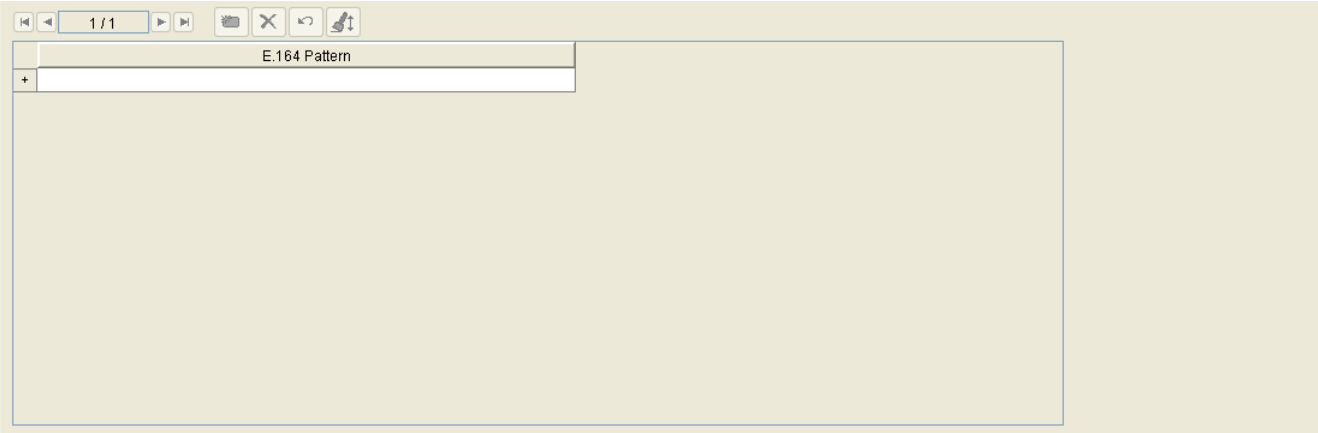


Reg-Address

IP addresses or host names of the PBX, gateway, or SIP server associated with this location.

6.3.2.3 "E.164 Patterns" Tab

Call: Main Menu > Administration > Server Configuration > Location > "E.164 Patterns" Tab



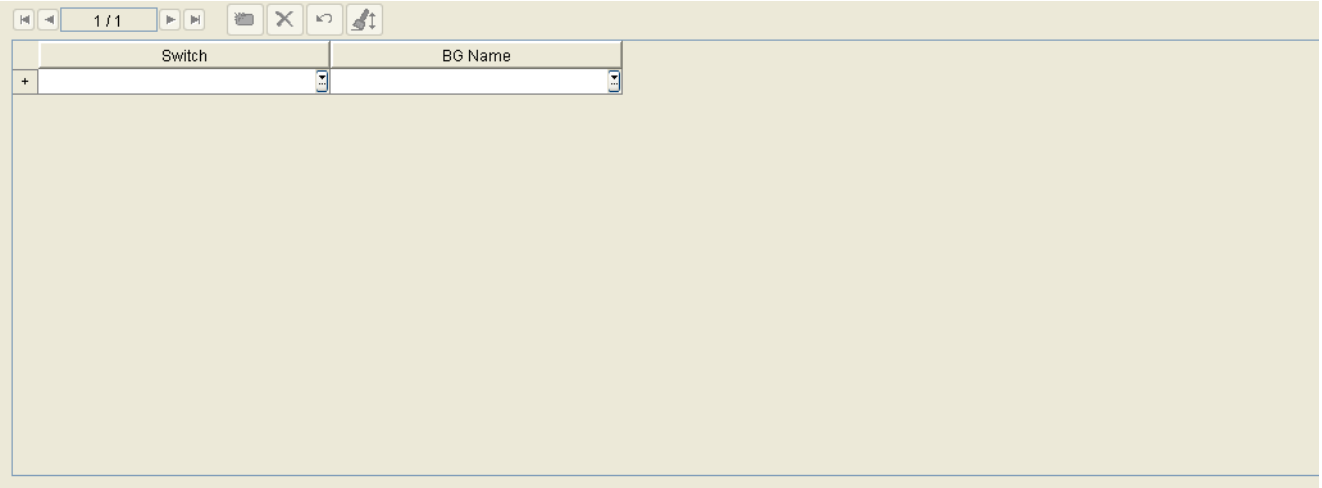
E.164 Pattern

E.164 number pattern corresponding to this location. Regular expressions with the symbol * can be used.

Example: **4989722***.

6.3.2.4 "Business Groups" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Business Groups" Tab



Switch

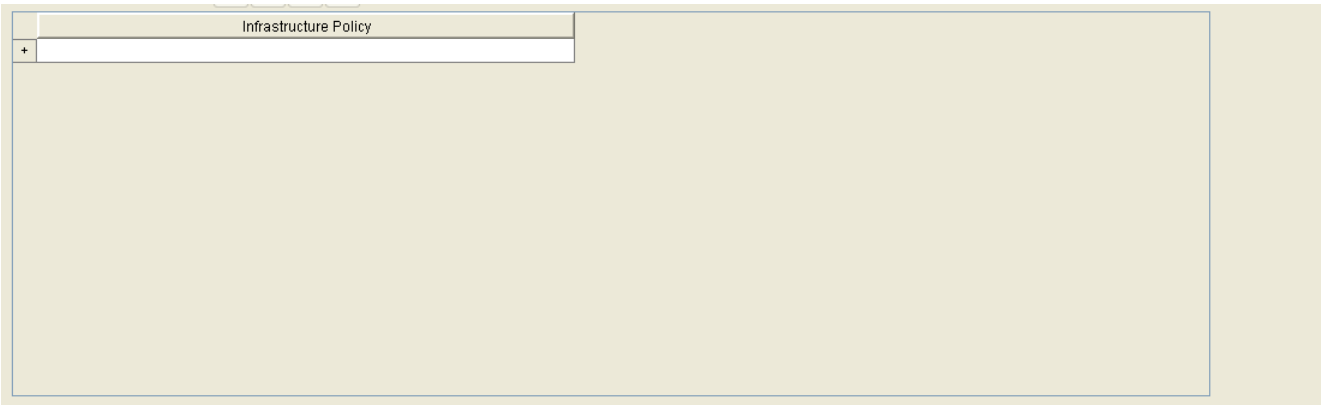
Name of the switch at which the business group is configured.

BG Name

Name of the business group.

6.3.2.5 "Infrastructure Policies" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Infrastructure Policies" Tab



Infrastructure Policy

Location will be considered on infrastructure policy change for a device via DLSAPI or by means of the XML application "Location Services".

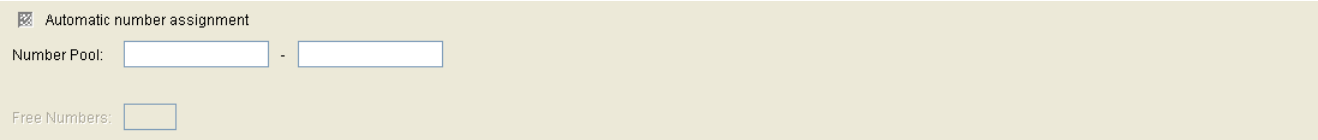
6.3.2.6 "P&P Number Pool" Tab

Call: Main Menu > Administration > Server Configuration > Location > "P&P Number Pool" Tab

In this area, you can configure automatic E.164 number assignment from a number pool to IP Phones during Plug&Play.

If a location specific number pool is required, it must be defined during location configuration. The number pool of the "Default Location" has to be inactive in that case. For automatic number assignment, a location has to be defined via IP range, and it has to be a parent location. This is necessary because otherwise, no location can be assigned to IP Phones which register without E.164 number.

For further information, please see Section 15.8.2, "Setting Up Plug&Play Registration".



Automatic number assignment

If activated, Plug&Play automatically assigns an E.164 call number from the number pool to the IP device.

Number Pool

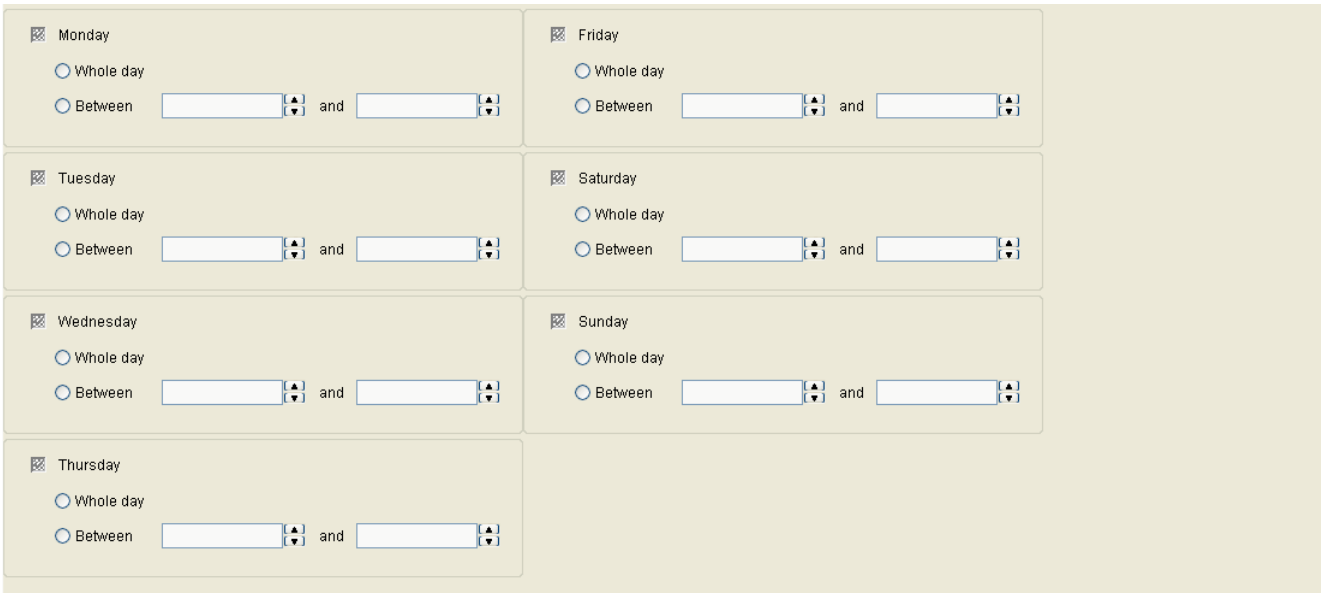
Band of successive fully qualified E.164 numbers, which is defined by entering the first and last number.

Free Numbers

Number of E.164 call numbers from the pool which have not been assigned yet.

6.3.2.7 "SW Deployment Restrictions" Tab

Call: Main Menu > Administration > Server Configuration > Location > "SW Deployment Restrictions" Tab



IMPORTANT: DLS ignores these SW restrictions:

- For the newly registered devices to DLS

- For the existing registered devices in case of E164 change

Monday ... Sunday

Check box for specifying the weekdays on which no or only limited software deployment should be performed.

Whole day

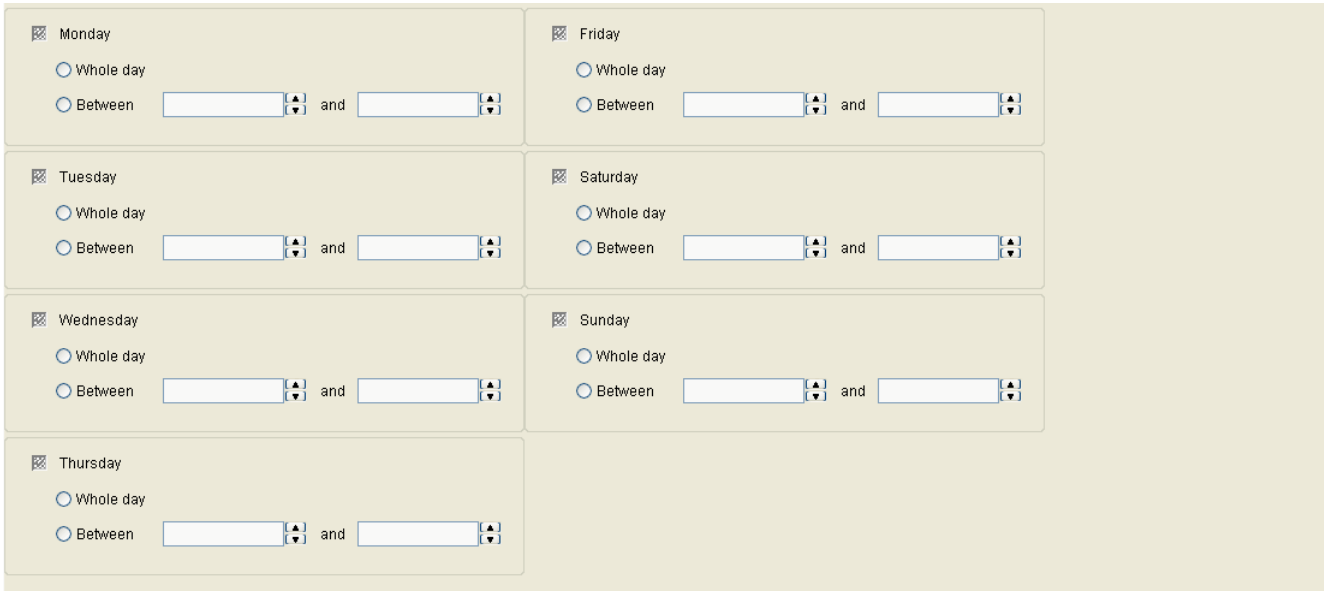
Check box for activating the option to prevent software distribution on the specific day.

Between ... and ...

Check box for activating the option to prevent software distribution during a particular period of time on the specific day. The start and end of the time segment can be defined.

6.3.2.8 "Certificate Deployment Restrictions" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Certificate Deployment Restrictions" Tab

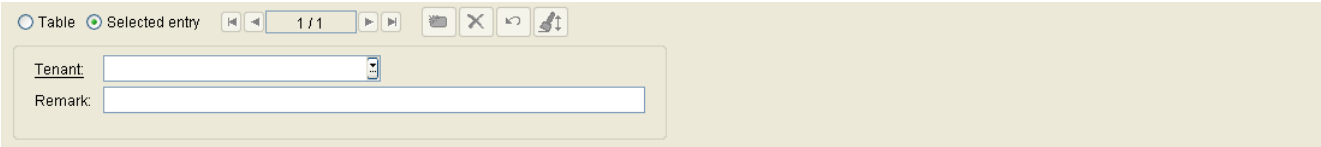


For parameter descriptions, see Section 6.3.2.7, ""SW Deployment Restrictions" Tab".

6.3.2.9 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > Location > "Tenants" Tab

NOTE: This tab is available only if the multi-tenancy function of the DLS is installed.



Tenant

Name of the tenant.

Remark

Information on the tenant.

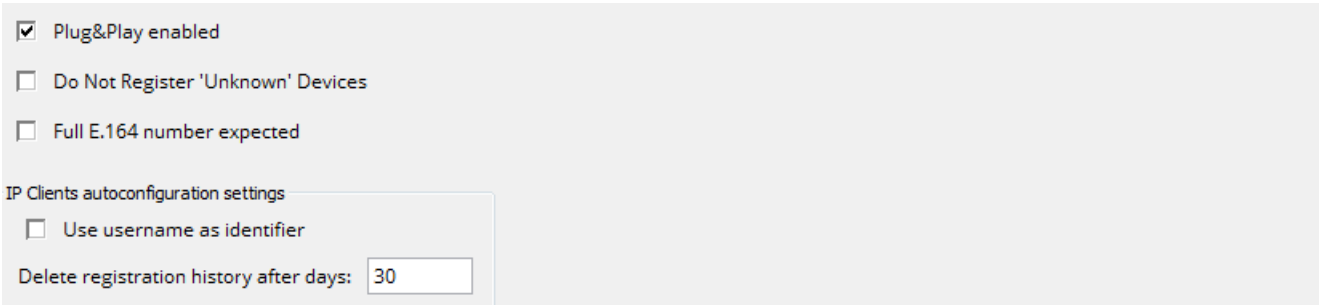
6.3.3 P&P Settings

Call: Main Menu > Administration > Server Configuration > P&P Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "Standard Profile" Tab
- "IP Client Mapping Configuration" Tab

General Data



Plug&Play enabled

When activated, Plug&Play is enabled for all devices.

Do Not Register ’Unknown’ Devices

When activated, you may disable device registration for unknown devices (devices that do not have a P&P entry in the DLS Database)

By enabling this checkbox, you should not be able to register devices that do not have corresponding P&P entry.

Disabled by default (in order to maintain backwards compatibility & not affect existing behavior).

IMPORTANT: This feature is available only when P&P is enabled.

Full E.164 Nummer expected

If this switch is activated, the DLS expects the full E.164 call number of an IP Device for Plug&Play resp. autoconfiguration, in order to find the corresponding virtual device.

IP Clients autoconfiguration settings

Use username as identifier

If checked, DLS shall use the windows username as device identifier. That means that DLS will maintain one IP client entry for every unique windows username.
When enabled:

- Username will be the device identifier
- P&P will be enabled for the IP Clients that have been created with the username as device ID
- History of the last PCs used by this username will be kept

NOTE: For all IP clients that register to the DLS and there is no configured P&P ready device with the received username, DLS will create the corresponding entry using the received username and will keep the received settings as P&P data.

IMPORTANT: Whenever a device contacts the DLS, a P&P takes place.Based on the 'latest PC visited by the windows username',P&P is applied only when the user changes PC.

Delete registration history after days:

Number of days after which registration history is erased.

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the changes.

Refresh

Refreshes the screen contents from the database.

6.3.3.1 "Standard Profile" Tab

Call: Main Menu > Administration > Server Configuration > P&P Settings > "Standard Profile" Tab

Determine how the E.164 number shall be used for autoconfiguration.



Standard Profile available

This check box is active when the standard profile exists.

Create Standard Profile

Creates a standard profile for IP Phones und IP Clients. This profile contains pre-defined templates.

NOTE: When assigning templates to P&P profiles,all P&P profiles MUST have a SW version assigned in order to have the respective masks available.

NOTE: For instance,under **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **IP Routing**> -**"IPv6 Settings" Tab** the “IPv4 / IPv6 Protocol Mode” can only be available in case the Device Type is OpenStage and the SW version is V3 onward (please refer to Section 7.1.2.2, ""IPv6 Settings" Tab")

NOTE: This also applies to all masks that are filtered by SW Version..

Remove Standard Profile

Removes the standard profile.

6.3.3.2 "IP Client Mapping Configuration" Tab

Call: Main Menu > Administration > Server Configuration > P&P Settings > "IP Client Mapping Configuration" Tab



Windows account names are mapped to E.164 numbers to allow windows account / telephony number association. DLS configuration of this mapping should be implemented through manual DLS UI configuration as well as import & export of mapping data through .csv files in order to trigger DLS Plug & Play accordingly.

Import and export mapping data

Import

Mapping data are imported through a .csv formatted file.

Export

Mapping data are exported into a .csv formatted file.

6.3.4 FTP Server Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Tenants" Tab

General Data

Call: Main Menu > Administration > Server Configuration > FTP Server Configuration.

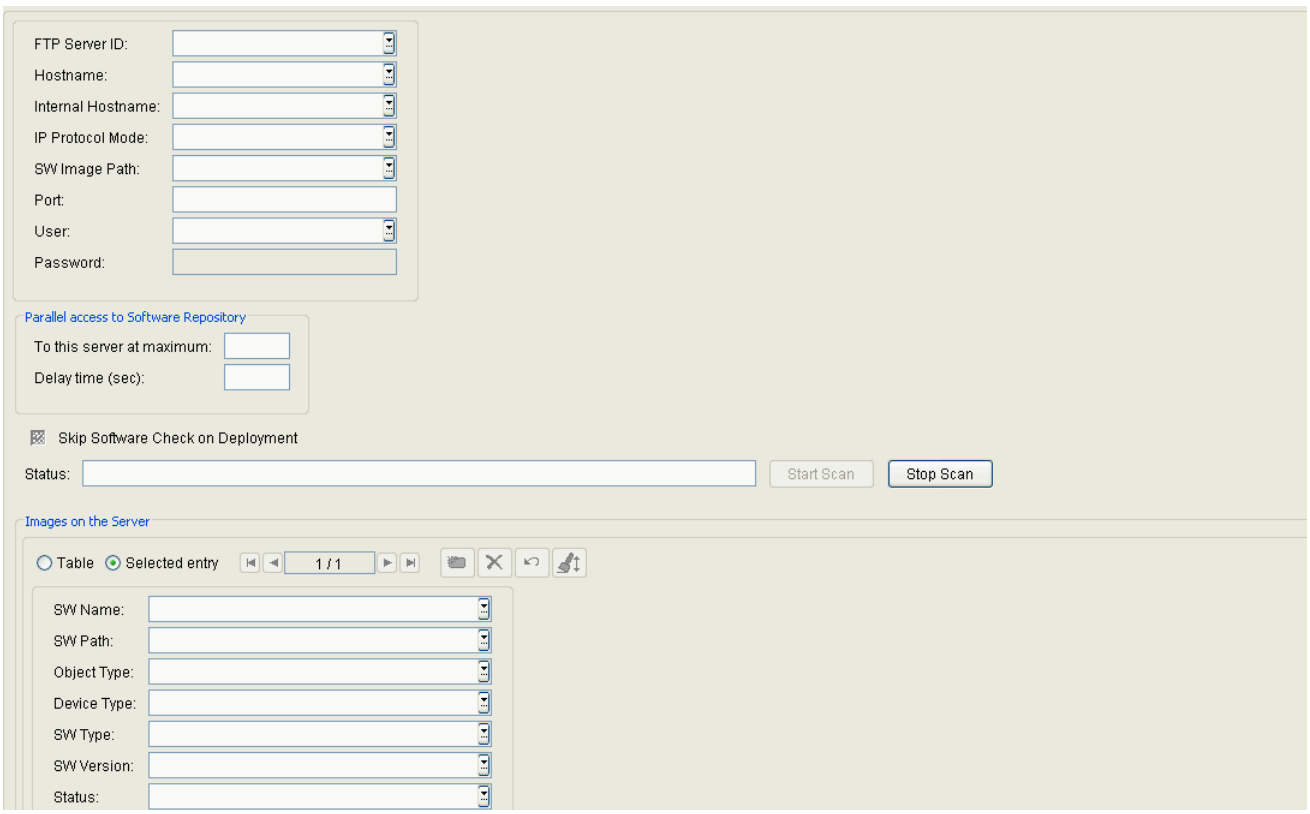
In this area, you can configure access data for one or more FTP servers. All FTP servers detected by the **Search** routine are listed in **Table** view. Moreover, you can read all files which are existant on the FTP server and relevant for IP devices into the DLS database. After this, the data are available for deployment.

For each file on the FTP server, one object per possible usage is created. For instance, a WAV file may be used as ringtone or as hold music. If there is, for instance, a file named "notify.wav", the objects "notify.wav (OpenStage,RINGTONE)" and "notify.wav (OpenStage,MOH)" would be created.

NOTE: The entries depend on the configuration of the FTP server in use at the time.
For more information on configuring FTP servers, see Section 4.12.1, "FTP Server".

An FTP server is necessary to load files to a device - phone software images or on-hold music, for example. You must also configure at least one FTP server for the DLS to register the available phone software images.

NOTE: In contrast to IP phone software and files (which must be present on an FTP server), software and files for IP clients are provided on a network drive and configured as described in **Network Drive Configuration**.



FTP Server ID:

Unique name used to manage and address each FTP server configured.

Hostname:

Host name or IP address of the FTP server (accessible by IP Devices).

Internal Hostname

If specified, this host name or IP address will be used for scan and SW check by the DLS.

Find the configuration files in which IP addresses and workgroup names are assigned to each other in:

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

and add the IP address as well as the Internal Hostname of FTP Server to file (Host).

NOTE: Apply in all nodes of a Multi Node environment.

IP Protocol Mode

The FTP server is supporting this IP protocol version.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

SW Image Path:

Path to the software image relative to the directory root of the FTP server. If the data is located directly in the directory root, enter / (slash).

Port:

The default port number for FTP is 21 and cannot be changed.

User:

User name for read-only access to the FTP server. Read-only access is used by the IP Device to access the software.

Password:

Password for read-only access to the FTP server. This entry is optional.

> ***IMPORTANT:*** In the case where the FTP password is modified under FTP server configuration and there are already template entries that contain a File Deployment record with initial password attribute, due to the fact that the password in these templates will not be updated automatically, then you need to remove and add the specific attribute in the template manually, in order to become updated with the password.

Parallel access to Software Repository

To this server at maximum:

Maximum number of simultaneous accesses to the server. This value corresponds to the number of simultaneous software distribution actions (software deployment jobs) to the devices. The value must be less than the maximum number of simultaneous connections for which the FTP server is configured.

Value range: **1 - 500**.

Default: **10**.

Delay time (sec):

Time between two distribution jobs. The value set should only be increased if the LAN infrastructure is slow (or exceptionally, in the case of a moderately fast connection to the FTP server).

Value range: **1 - 3000** seconds.

Default: **10**.

Skip Software Check on Deployment

When the DLS is scanning the FTP server for files, it examines all phone software files. This includes a header and footer check. If the switch is deactivated, the check will be repeated just before a software file is deployed to a phone. If it is activated, this check will be skipped.

Status:

Status of s server action.

Possible values:

- **Scanning...**

- **Finished**
- **Stopped**

Start Scan

Start a search for software and data files on the FTP server. Entries concerning files which are not available on the server will be deleted in the DLS database.

Stop Scan

Stop scanning the FTP Server for software and data files.

Images on the Server

If a scan has been executed, information on all software and data files found during the scan is displayed here.

SW Name:

Name of the file.

SW Path:

Directory path and file name.

Object Type:

Type of file.

Examples: **Software Image**, **Logo File**, **Screen Saver**.

Device Type:

Device type, for which the file is appropriate.

Examples: **optiPoint 410**, **OpenStage Hi**,**OpenStage Lo, Wave Evolution Lo.**

> ***NOTE:*** OpenStage15 & OpenStage 40 devices are tagged commonly as 'OpenStage Lo'. OpenStage 15 devices use the 'LO' device software category and have common firmware for OS15, OS20 and OS40 devices.

NOTE: OpenScape Desk Phone IP 35G Eco devices are tagged commonly as 'Wave Evolution Lo'.

NOTE: During automatic Software (SW) deployment, DLS finds the matching firmware based on family (HI or LO) and desired SW version. DLS will scan through the FTP list for the first available firmware that meets the criteria and a valid match gets deployed. DLS deploys the correct firmware (as far as OS15 and OS40 belong in the same family and have the same firmaware data) but the shown used filename for the SW update may be misleading.
At manual SW deployment you get prompted to explicitly choose the firmware file to be deployed.

SW Type:

Type of the phone software.

Examples: **Unify HFA**, **Unify SIP**.

SW Version:

Version ot the phone software.

Status:

Status of the phone software.

Example: **version info missing**.

Valid

Activated if the file is valid.

Possible Action Buttons

Search

Searches the database for FTP servers already installed.

Clear Window

Deletes the data entered in the window.

Save

Saves the data entered/modified.

Discard

Discards any changes made.

New

Creates a new FTP server.

Delete

Deletes the FTP server currently listed in Object view.

Test FTP Parameters

Tests the connection to the current FTP server configured. The result is displayed in the status window.

Refresh

Updates the field content using the database.

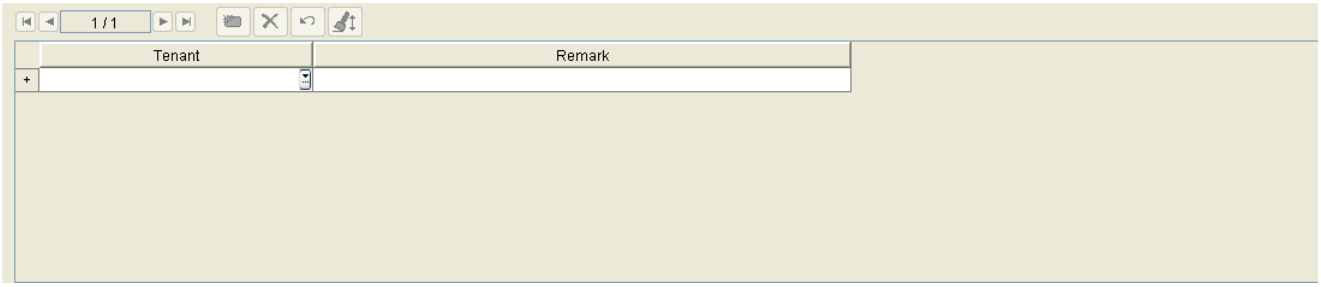
Scan all

All assigned FTP servers will be scanned. A progress bar shows the status of the current server scan. This scan can be cancelled like a single scan by clicking the button **Stop Scan**.

6.3.4.1 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > FTP Server Configuration > "Tenants" Tab

NOTE: This tab is available only if the multi-tenancy function of the DLS is installed.



Tenant

Name of the tenant.

Remark

Information on the tenant.

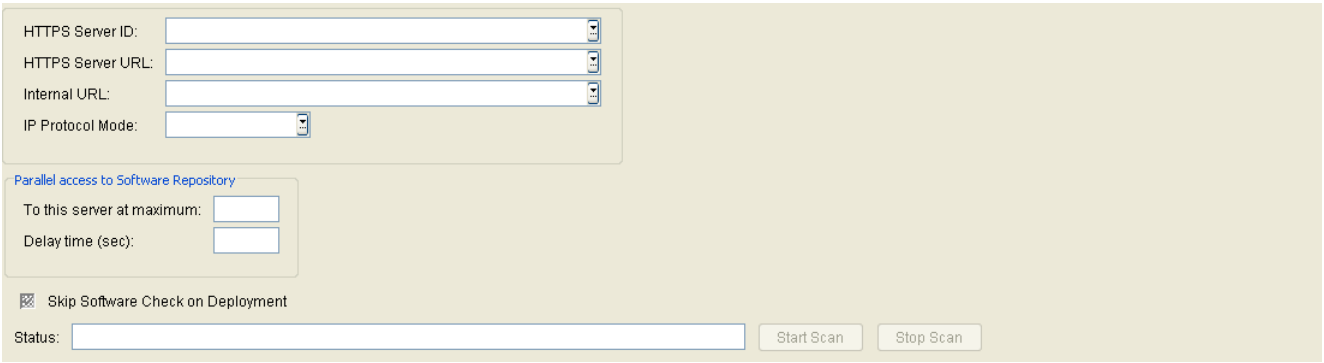
6.3.5 HTTPS Server Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Images on the Server" Tab
- "HTTPS Server CA Certificates" Tab
- "Trust Anchor" Tab
- "Tenants" Tab

General Data

Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration.



NOTE: HTTPS servers can only be used for OpenStage devices.

In this area, you can configure access data for one or more HTTPS servers. All HTTPS servers detected by the search routine are listed in **Table** view.

An HTTPS server can be used instead of an FTP server to load data, such as, on-hold music or phone software images onto an OpenStage device. You must also configure at least one HTTPS server for the DLS to register the available phone software images.

NOTE: The entries depend on the configuration of the HTTPS server in use at a time.

NOTE: In contrast to the IP phone software that must be loaded on an HTTPS server, the software for IP clients is provided on a network drive as described under Windows Network Drive Configuration.

HTTPS Server ID

Unique name used to address each HTTPS server configured.

HTTPS Server URL

URL of the HTTPS server (accessible by IP Devices).

Internal Hostname

If specified, this host name or IP address will be used for scan and SW check by the DLS.

Find the configuration files in which IP addresses and workgroup names are assigned to each other in:

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

and add the IP address as well as the Internal Hostname of FTP Server to file (Host).

NOTE: Apply in all nodes of a Multi Node environment.

IP Protocol Mode

The HTTPS server is supporting this IP protocol version.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Parallel access to Software Repository

To this server at maximum:

Maximum number of simultaneous accesses to the server. This value corresponds to the number of simultaneous software distribution actions (software deployment jobs) to the devices. The value must be less than the maximum number of simultaneous connections for which the HTTPS server is configured.

Value range: **1 - 500**.

Default: **10**.

Delay time (in seconds):

Time between two distribution jobs. The value set should only be increased if the LAN infrastructure is slow (or exceptionally, in the case of a moderately fast connection to the HTTPS server).

Value range: **1 - 3000** seconds.

Default: **10**.

Skip Software Check on Deployment

When the DLS is scanning the HTTPS server for files, it examines all phone software files. This includes a header and footer check. If the switch is deactivated, the check will be repeated just before a software file is deployed to a phone. If it is activated, this check will be skipped.

Status:

Status of s server action.

Possible values:

- **Scanning...**
- **Finished**
- **Stopped**

Start Scan

Start a search for software and data files on the HTTPS server. Entries concerning files which are not available on the server will be deleted in the DLS database.

Stop Scan

Stops scanning the HTTPS Server for software and data files.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Search

Searches the database for HTTPS servers already configured.

Clear Window

Deletes the data entered in the window.

New

Creates a new HTTPS server.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Test

Tests the connection to the current HTTPS server configured. The result is displayed in the status window.

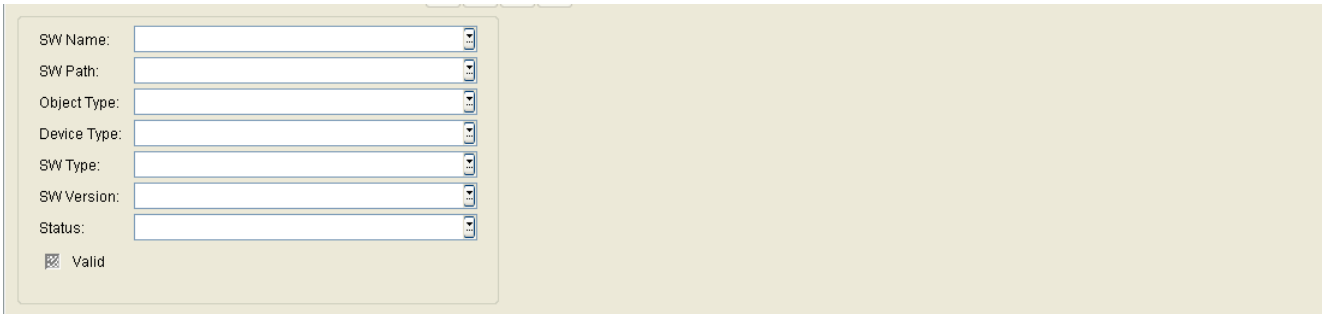
Scan all

All assigned HTTP servers will be scanned. A progress bar shows the status of the current server scan. This scan can be cancelled like a single scan by clicking the button **Stop Scan**.

6.3.5.1 "Images on the Server" Tab

Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration > "Images on the Server" Tab

If a scan has been executed, information on all software and data files found during the scan is displayed here.



SW Name:

Name of the file.

SW Path:

Directory path and file name.

Object Type:

Type of file.

Examples: **Software Image**, **Logo File**, **Screen Saver**.

Device Type:

Device type, for which the file is appropriate.

Examples: **optiPoint 410**, **OpenStage Hi**.

SW Type:

Type of the phone software.

Examples: **Unify HFA**, **Unify SIP**.

SW Version:

Version ot the phone software.

Status:

Status of the phone software.

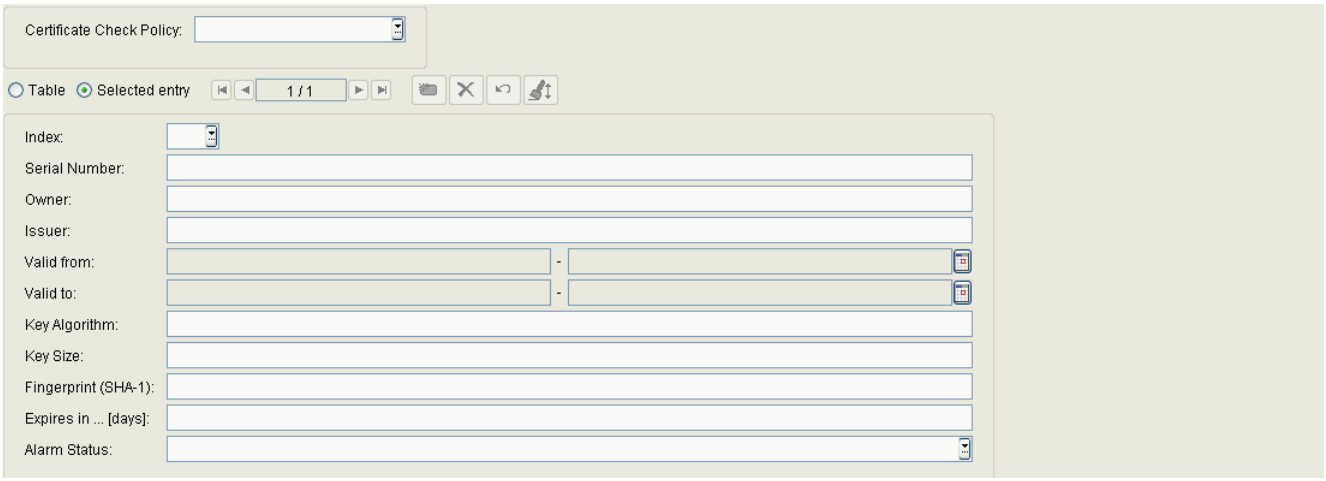
Example: **version info missing**.

Valid

Activated if the file is valid.

6.3.5.2 "HTTPS Server CA Certificates" Tab

Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration > "HTTPS Server CA Certificates" Tab



Certificate Check Policy

Determines if and how the certificate is checked.

Possible values:

- **None**

  No authentification of server. Invalid certificates, which are received before by server or has been loaded by IP Phone, will be ignored. HTTPS connections to server are setup without authentications allways.

- **Trusted**

  Certificates are checked for "expired", "not valid", "signed by trusted CA", and "revoked". Therefore one or two list of "trusted CAs" are required. The same list will be used for "trusted" and "full". As "trusted CAs" may be used RootCAs, temporary created CAs, or even the server-certificate itself. Additional values, such as owner or issuer are not checked. HTTPS connections to server are setup even if some values of the certificate are incorrect.

- **Full**

  Certificates are checked for "expired", "not valid", "signed by trusted CA", "revoked", matching owner and so on. Therefore one or two list of "trusted CAs" are required. The same list will be used for "trusted" and "full". As "trusted CAs" may be used RootCAs, temporary created CAs, or even the server-certificate itself. HTTPS connections to server are setup only, if valid and correct certificates are available.

Index

Index of certicate.

Serial Number:

Serial number of the certificate (display only).

Owner:

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm

Key Algorithm of the certificate (display only).

Key Size

Key Size of the certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) of the certificate (display only).

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status of the certificate (display only).

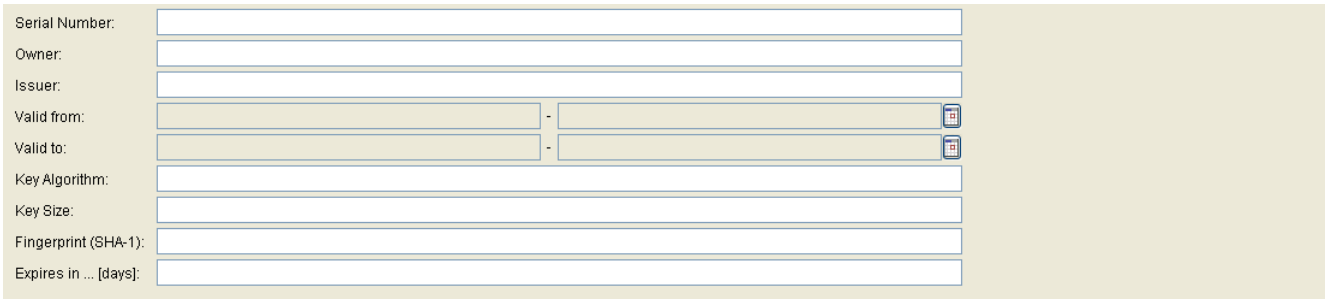
Possible values:

- **valid**
- **soon running out**
- **expired**

6.3.5.3 "Trust Anchor" Tab

Call: Administration > Server Configuration> HTTPS Server Configuration > "Trust Anchor" Tab

For each configuration, a trust anchor must be configured. In most scenarios, this will be the Root CA itself, but can be a subordinate CA as well. If a trust anchor is not available, the configuration cannot be saved!



Serial Number

Serial number of the certificate (display only).

Owner

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm:

Key Algorithm for certificate (display only).

Key Size:

Key Size for certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA1 (160 bits/20 characters) for certificate (display only)

Expires in ... [days]:

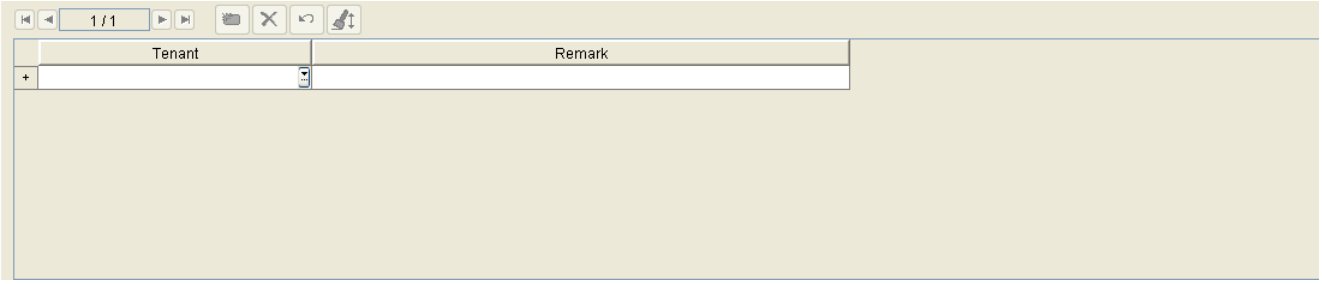
Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

6.3.5.4 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > HTTPS Server Configuration > "Tenants" Tab

NOTE: This tab is available only if the multi-tenancy function of the DLS is installed.



Tenant

Name of the tenant.

Remark

Information on the tenant.

6.3.6 HTTPS Client Configuration

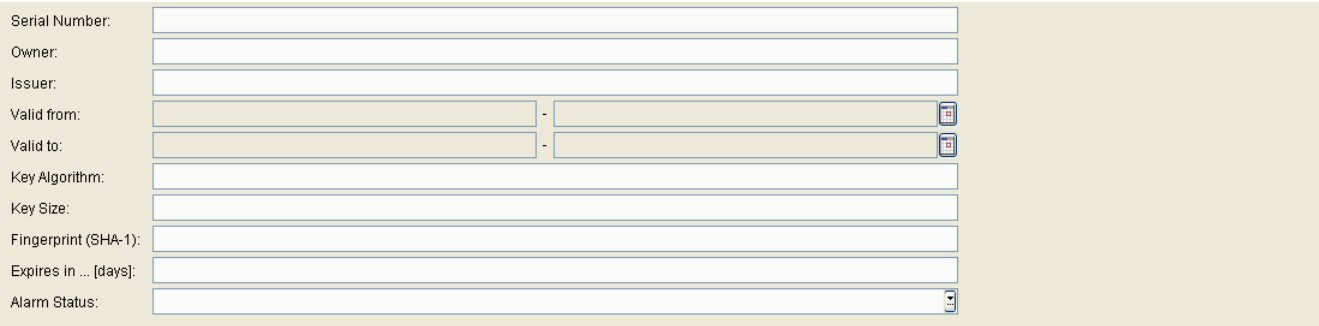
This area features the following components:

- General Data
- Possible Action Buttons

General Data

Call: Main Menu > Administration > Server Configuration > HTTPS Client Configuration.

This item allows to import and display certificates of the HTTPS Client Configuration.



Serial Number:

Serial number of the certificate (display only).

Owner:

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm

Key Algorithm of the certificate (display only).

Key Size

Key Size of the certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) of the certificate (display only).

Expires in ... [days]:

Certificate will expire in ... days of the certificate (display only).

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status of the certificate (display only).

Possible values:

- **valid**
- **soon running out**
- **expired**

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Search

Searches the database for HTTPS servers already configured.

Clear Window

Deletes the data entered in the window.

Import Certificate

Starts the import of HTTPS Client Certificate.

Synchronize Keystore

Starts synchronization of keystore.

6.3.7 Network Drive Configuration

Call: Main Menu > Administration > Server Configuration > Network Drive Configuration.

This area features the following components:

- General Data
- Possible Action Buttons
- "Tenants" Tab

General Data

In this area, you can configure one or more network drives.

NOTE: Deployment via a network drive is not available in the onboard variants of DLS on OpenScape Voice systems.

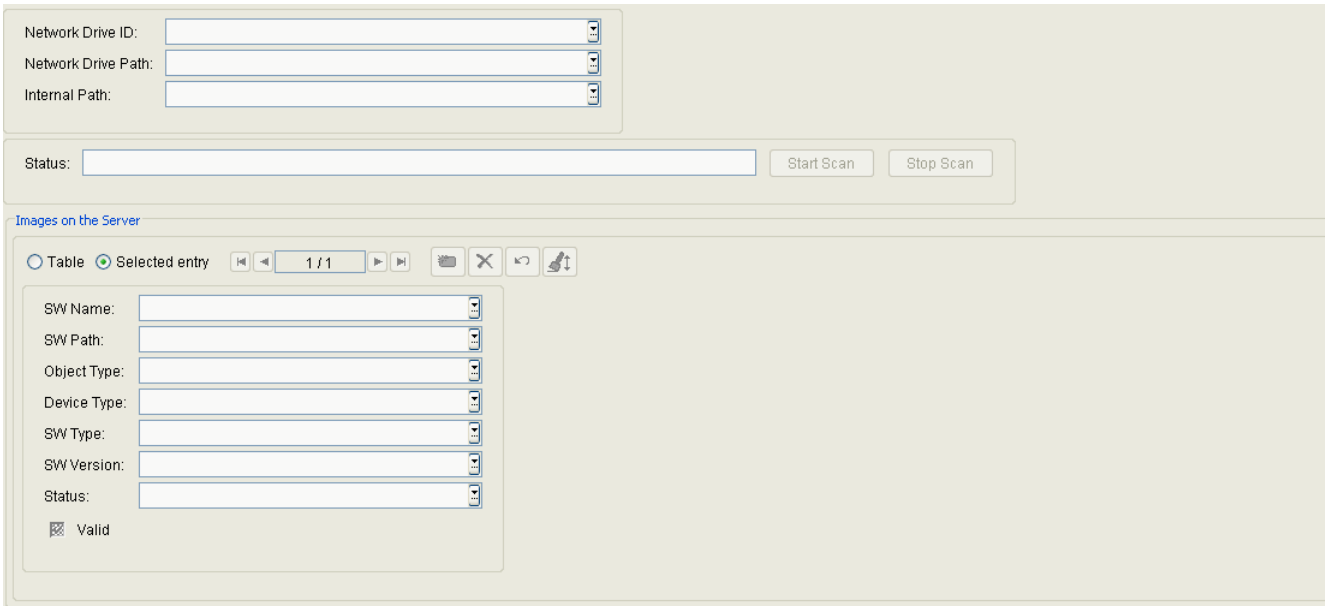
NOTE: The information here is only necessary for the distribution of IP client software. Access to the software for IP phones is via FTP/HTTPS. The server is configured in the **FTP Server Configuration** or **HTTPS Server Configuration** area.

Authorizations for accessing the network release must be set on the *[DLS server name]\system* to guarantee access for the DLS Web server running by default as the service.

If these authorizations cannot be extended or if the authorizations for access to the network releases are limited to a user group, then you must ensure that the DLS runs in the user context that is also included in this user group or that can access this network release.

The user context can be modified as follows (Windows XP, for example):
Start > **Settings** > **Control Panel** > **Administrative Tools** > **Services** > **DeploymentService** > [right-click] **Properties** > **Log On** tab.

Enter the data necessary for the Windows network drive.



Network Drive ID:

Unique name for addressing the network drive configured.

Network Drive Path:

Computer name or IP address where the drive is released and the path of the released directory. The directory must be accessible by IP Clients.

Internal Path

If specified, this path will be used for scan by the DLS.

Status:

Status of s server action.

Possible values:

- **Scanning...**
- **Finished**
- **Stopped**

Start Scan

Start a search for software and data files on the network drive. Entries concerning files which are not available on the server will be deleted in the DLS database.

Stop Scan

Stops scanning the network drive for software and data files.

Images on the Server

If a scan has been executed, information on all software and data files found during the scan is displayed here.

SW Name:

Name of the file.

SW Path:

Directory path and file name.

Object Type:

Type of file.

Examples: **Software Image**, **Logo File**, **Screen Saver**.

Device Type:

Device type, for which the file is appropriate.

Examples: **optiPoint 410**, **OpenStage Hi**.

SW Type:

Type of the phone software.

Examples: **Unify HFA**, **Unify SIP**.

SW Version:

Version ot the phone software.

Status:

Status of the phone software.

Example: **version info missing**.

Valid

Activated if the file is valid.

Possible Action Buttons

Save

Saves the data entered/modified.

Discard

Discards any changes made.

New

Creates a new network drive.

Delete

Deletes the network path currently listed in Object view.

Refresh

Updates the field content using the database.

Scan all

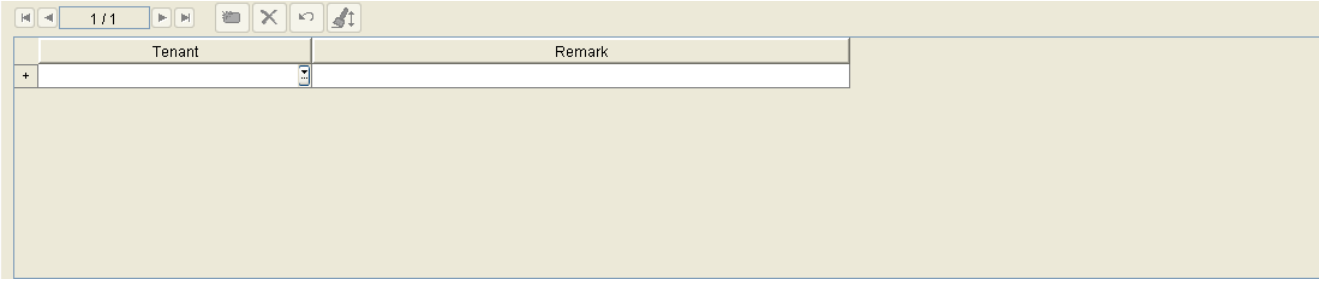
All assigned network drives will be scanned. A progress bar shows the status of the current scan.

This scan can be cancelled like a single scan by clicking the button **Stop Scan**.

6.3.7.1 "Tenants" Tab

Call: Main Menu > Administration > Server Configuration > Network Drive Configuration > "Tenants" Tab

NOTE: This tab is available only if the multi-tenancy function of the DLS is installed.



Tenant

Name of the tenant.

Remark

Information on the tenant.

6.3.8 Infrastructure Policy

Call: Main Menu > Administration > Server Configuration > Infrastructure Policy

This mask supports the mapping to an infrastructure policy according to the switch IP address, the switch port and the network policy. The mapping follows the order of the entries, i. e. the first matching entry will define the resulting infrastructure policy.

It is possible to enter regular expressions for the attributes mapped to the infrastructure policy. An empty mapping attribute means that it is not relevant for the mapping.

To trigger automatic adaptation, the infrastructure policy must be used as criterion for a location (see **Administration** > **Server Configuration** > **Location** >**"Infrastructure Policies" Tab**.

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Infrastructure Policies" Tab
- "Infrastructure Policy Table" Tab

General Data



Infrastructure Policy:

Name of the infrastructure policy.

Description:

Description of the infrastracture policy.

Possible Action Buttons

Depending on the statud of the DLS, various action buttons are available.

Search

Searches the database for configured IP infrastructure policies.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the Search view before new search criteria are entered.

New

Creates a new data record for IP infrastructure policies.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

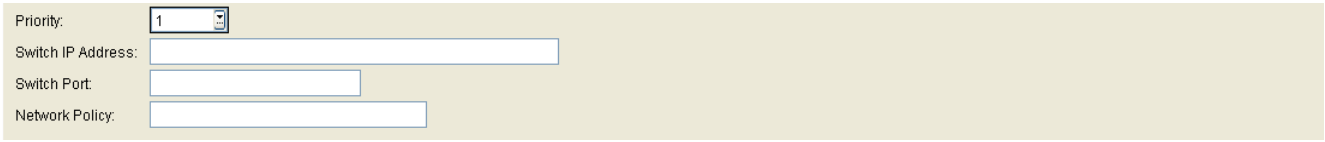
Updates the window using the database.

Apply

Applies IP infrastructure table to already existing IP Devices.

6.3.8.1 "Infrastructure Policy Table" Tab

Call: Main Menu > Administration > Server Configuration > Infrastructure Policy > "Infrastructure Policy Table" Tab



Priority:

The matching policy will be assigned according to the priority entered here.

Switch IP address:

IP address of the switch where the IP Phone is plugged in.

Regular Expressions may be used.

Switch Port:

Port number of the switch where the IP Phone is plugged in.

Regular Expressions may be used.

Network Policy:

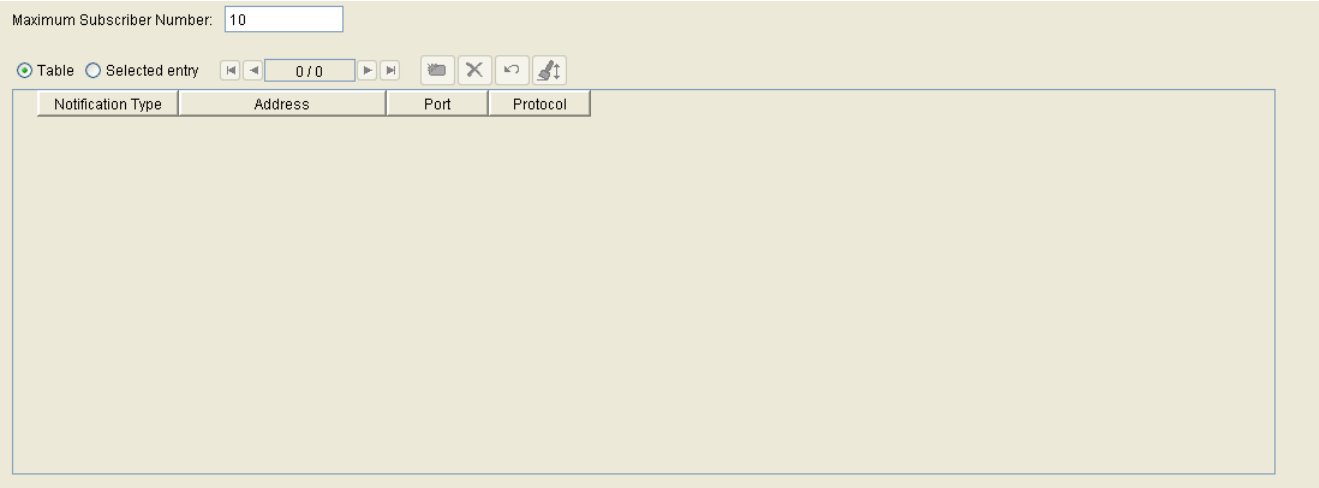
Network Policy assigned to IP Phone.

Regular Expressions may be used.

6.3.9 API Notifications

Call: Main Menu > Administration > Server Configuration > API Notifications

This screen offers an overview on the current subscribers to API notifications. The administrator can restrict the maximum number of subscriptions and also delete entries.



Maximum Subscriber Number:

If this number is reached, the attempt to subscribe to notifications will fail.

Notification Type

Type of notification.

Possible values:

- **inventoryInfo**
  New IP Phones and E.164 changes will be notified.
- **serverStart**
  Notification on DLS server start.

Address

Target IP address for notification.

Port

Target port for notification.

Protocol

Protocol used for notification: UDP.

6.3.10 XML Applications

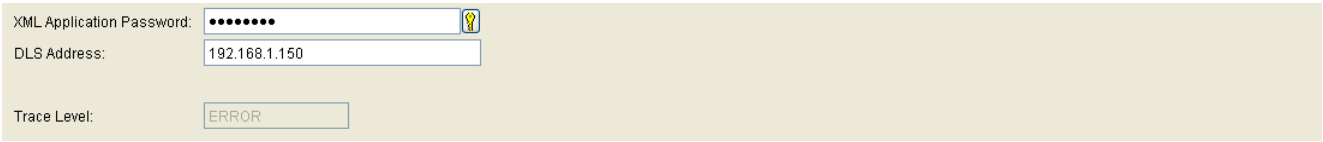
Call: Main Menu > Administration > Server Configuration > XML Applications

XML applications are configured here.

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Deployment Service" Tab
- "Location Service" Tab
- "News Service" Tab
- "MakeCall" Tab

General Data



XML Applications Password

Common password of all password protected XML applications.

DLS Address

IP address of the DLS, or, in a Multinode installation, the IP address of the DLS cluster.

Trace Level

Trace Level for XML Applications which are running as self-contained web applications. The trace data are stored under
`<Installation directory>\Tomcat\webapps\XMLApplications\log\dlsXMLAppsLog.txt`

Possible Options:

- **ERROR**
- **INFO**
- **DEBUG**

Possible Action Buttons

Discard

Discards any changes entered.

Save

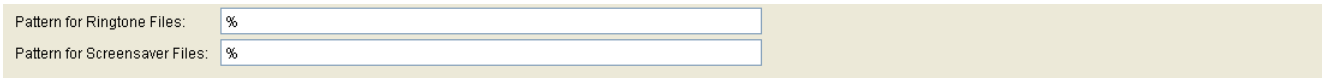
Saves the field contents to the database.

Refresh

Updates the window using the database.

6.3.10.1 "Deployment Service" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "Deployment Service" Tab



Pattern for Ringtone Files

Pattern for the partially qualified selection of ringtone files available from the FTP or HTTPS Server.

Example: ***Unify*New*Devices***

Pattern for Screensaver Files

Pattern for the partially qualified selection of screensaver files available from the FTP or HTTPS Server.

Example: ***Unify*New*Devices***

6.3.10.2 "Location Service" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "Location Service" Tab



Authentication

Select a password to execute this XML application.

Possible options:

- **IP Device User Password**

  NOTE: If the call number of the OpenStage end device is to be changed, this is the password of that virtual device to which the new call number is assigned.

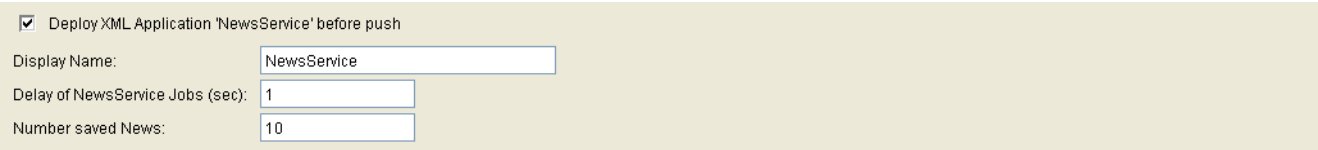
- **XML Applications Password**
- **IP Device User Password or XML Applikations Password**

Factory Reset Password

Password to execute a factory reset on OpenStage end devices. At this, the factory setting are restored.

6.3.10.3 "News Service" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "News Service" Tab



Deploy XML Application ’News Service’ before push

When activated, the XML application ’NewsService’ will be deployed before first execution, if it is not yet configured at the end device.

Display Name:

This name is shown on the end device display for the XML application ’NewsService’ if it has been automatically deployed.

Delay of News Service Jobs (sec):

Delay of jobs in seconds after bulk change operations. This is the minimal time interval between the sending of the same message to two different end devices. Notifications are not delayed.

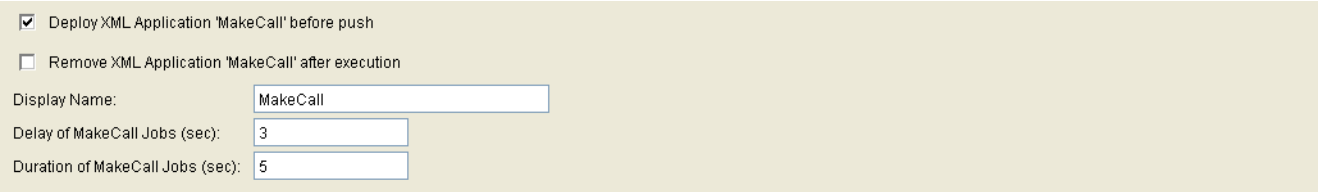
Value range: **1** - **300**

Number saved News:

Number of news which have already been sent via the XML application ’NewsService’, and which have been saved. As soon as the number is exceeded, the oldest news message is deleed.

6.3.10.4 "MakeCall" Tab

Call: Main Menu > Administration > Server Configuration > XML Applications > "MakeCall" Tab



Deploy XML Application ’MakeCall’ before push

Switch to activate the first deployment of the News Service application.

Whe activated, the XML application ’MakeCall’ is deployed before the first execution, if it is not yet configured at the end device.

Remove XML Application ’MakeCall’ after execution

When activated, the XML application ’MakeCall’ is removed from the end device after it has been executed.

Display Name:

This name is shown on the end device display for the XML application ’MakeCall’ if it has been automatically deployed.

Delay of MakeCall Jobs (sec):

Minimal time interval in seconds between the initiating of a call from two different end devices; is needed for bulk changes.

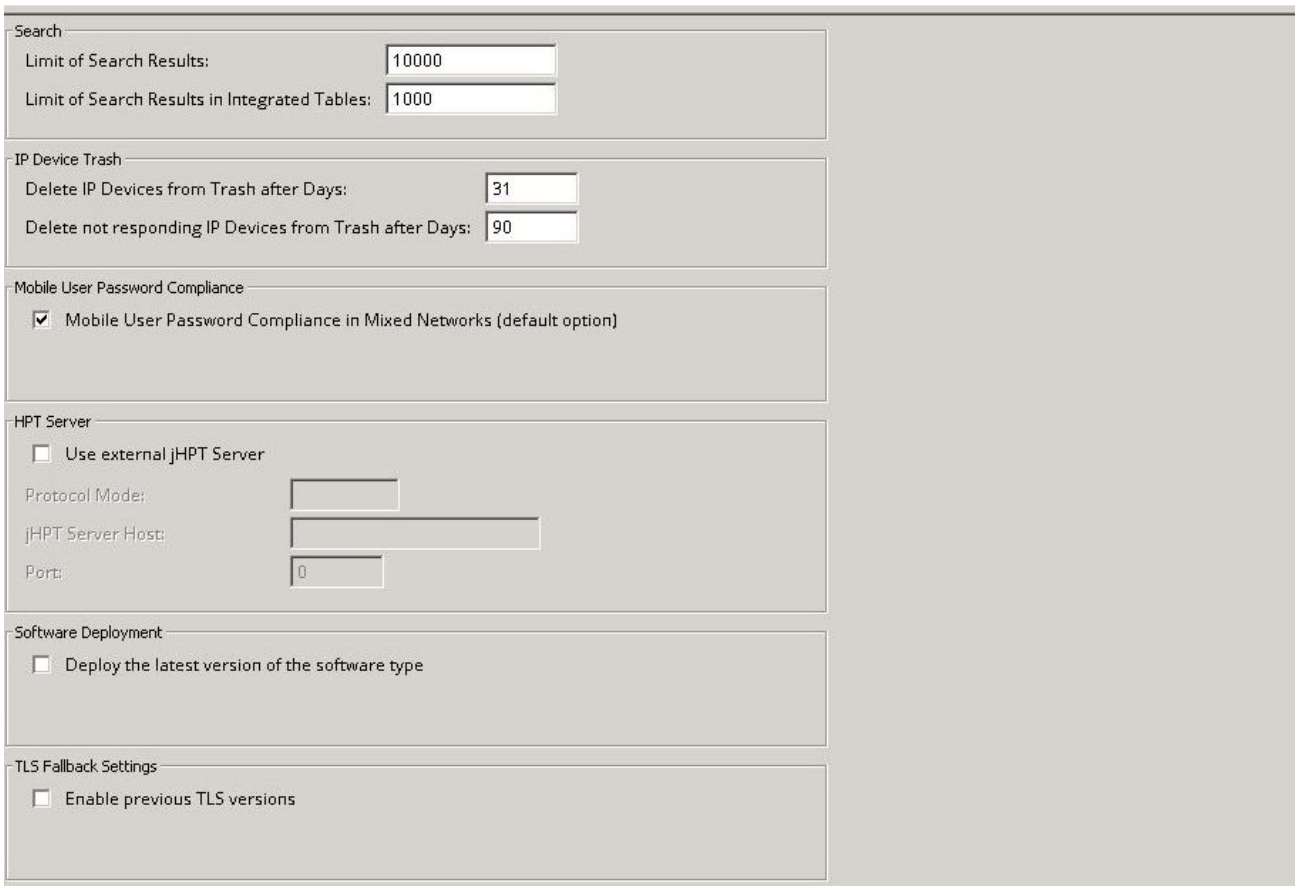
Value range: **1** ... **500**

Duration of MakeCall jobs (sec):

This duration is equivalent to the sum from the time needed for initiating the call and the time needed for the call proper.

6.3.11 Options

Call: Main Menu > Administration > Server Configuration > Options



Search

Limit of Search Results

Maximum number of records displayed when a search is done.

NOTE: Changed values first will be used not until the DLS Client has been restarted.

Limit of Search Results in Integrated Tables

Maximum number of records displayed in integrated tables when a search is done.

NOTE: Changed values first will be used not until the DLS Client has been restarted.

IP Device Trash

Delete IP Devices from Trash after Days

Number of days after which IP Devices marked to be deleted will be deleted completely from the DLS database.

Default value : 31 days

Value range: **1** ... **365**

> ***NOTE:*** If you set it to zero (’’ 0’’), it changes the value to default as soon as you hit the save button or mark another field.

Delete not responding IP Devices from Trash after Days

Number of days after which not responding IP Devices marked to be deleted will be deleted completely from the DLS database.

Default value : 31 days

Possible options: **1** ... **365**

> ***NOTE:*** If you set it to zero (’’ 0’’), it changes the value to default as soon as you hit the save button or mark another field.

Mobile User Password Compliance

Mobile User Password Compliance in Mixed Networks (default option)

If this option is selected and a Mobile User password is changed on an OpenStage V3.0 Phone or higher, the Mobile User also will be able to use it on older phone types or software versions. If not selected, the Mobile User password on older phones or software versions is eventually replaced by the standard password '000000'.

Only available for SIP phones.

> ***IMPORTANT:*** This option is used as a default value for devices connected to DLS for the first time. Please refer to Section 7.1.7.1, ""Passwords" Tab" for enabling this option for specific IP phones (IP Phone Configuration).

> ***NOTE:*** In OpenStage v3 onward, the password for mobile users is send using hash values.Therefore the DLS is not able to display anything in the password field when the Refresh button is used.
> The password is not lost,is just not visible in the DLS graphic user interface.

HPT Server

Use external jHPT Server

Checkbox for enabling/disabling redirection to an external jHPT server and allowing configuration.

Protocol Mode

Possible values:

- **http**
- **https**

> ***IMPORTANT:*** Protocol should be the same as the one used for the access to the DLS GUI or the one configured for an external jHPT.

jHPT Server Host

Example : **https://10.5.12.132:8080/jhptweb**

Port

Port should be the same as the one used for the access to the DLS GUI or the one configured for an external jHPT.

Software Deployment

Deploy the latest version of the software type

Checkbox activating the deployment of the latest available SW version based on the SW type of the device. When enabled, DLS will ignore the configured Manage rules.

> ***NOTE:*** This configuration item applies to both the new P&P and the existing registered devices.

TLS Fallback Settings

Enable fallback to previous versions

Checkbox for enabling/disabling fallback to previous TLS versions (i.e. **TLS V1.0**).

NOTE: By default, DLS Server (Deployment Service) does not negotiate with **TLS v1.0** and **v1.1**. In case a customer requires DLS to fallback to **TLS v1.0** then this checkbox can be enabled.

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the changes.

Refresh

Refreshes the screen contents from the database.

6.3.12 TLS Connector Configuration

Call: Main Menu > Administration > Server Configuration > TLS Connector Configuration

This area features the following components:"Truststore DLS API" Tab

- "DLS Client GUI" Tab
- "Truststore DLS Client GUI" Tab
- "DLS API" Tab
- "Truststore DLS API" Tab

Certificate Check Policy

Certificate Check Policy

Configure the "Certificate Check Policy" for DLS GUI / API.

Possible values:

- **None**
- **Partial**
- **Full**

Possible Action Buttons

Import and activate Certificate

Imports and activates certificate. When clicking the button, a window pops up to select certificate type and import source.

Remove Certificate

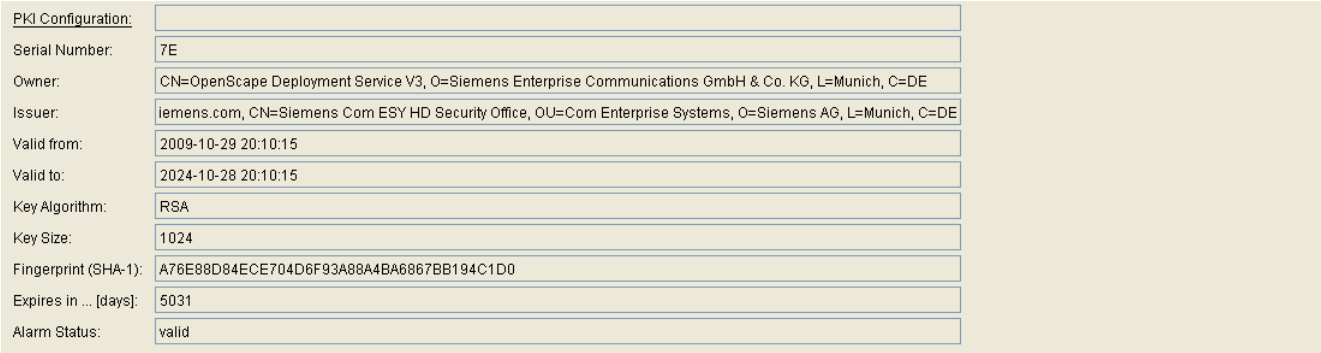
Removes certificate. When clicking the button, a window pops up to select certificate type.

Refresh

Updates the window using the database.

6.3.12.1 "DLS Client GUI" Tab

Call: Main Menu > Administration > Server Configuration > TLS Connector Configuration > "DLS Client GUI" Tab



Serial Number:

Serial number of the certificate (display only).

Owner:

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm

Key Algorithm.

Key Size

Key Size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

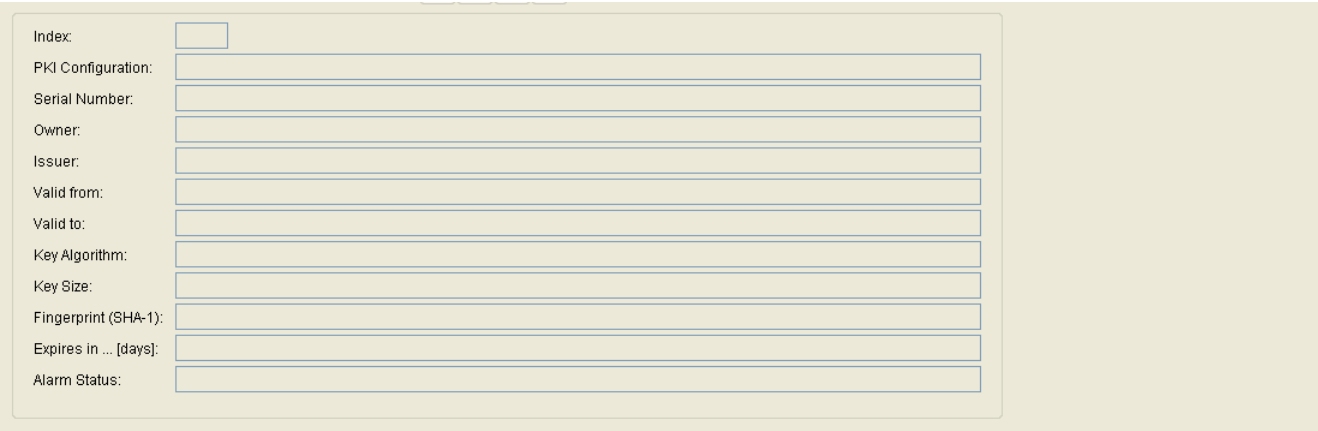
Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

6.3.12.2 "Truststore DLS Client GUI" Tab

Call: Main Menu > Administration > Server Configuration > TLS Connector Configuration > "Truststore DLS Client GUI" Tab



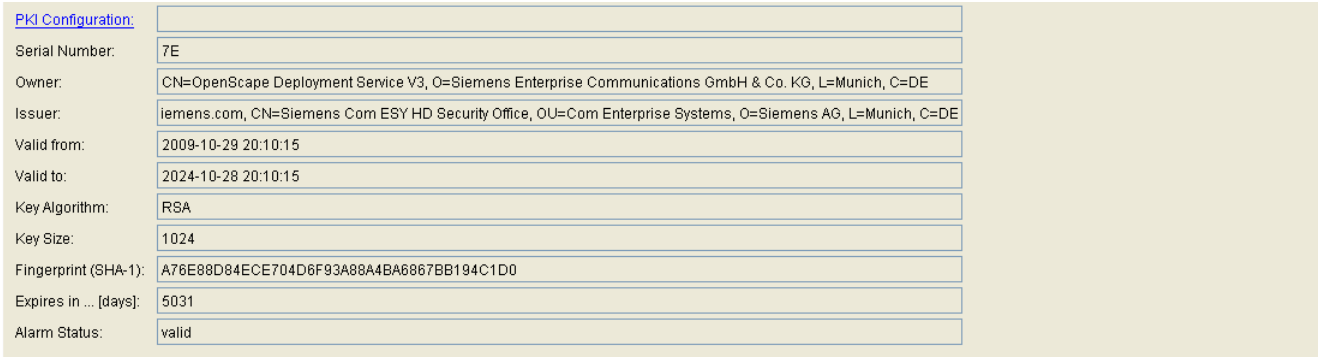
Index

Index of the TLS connector.

For further parameter description, see chapter Section 6.3.12.1, ""DLS Client GUI" Tab".

6.3.12.3 "DLS API" Tab

Call: Main Menu > Administration > Server Configuration > TLS Connector Configuration > "DLS API" Tab

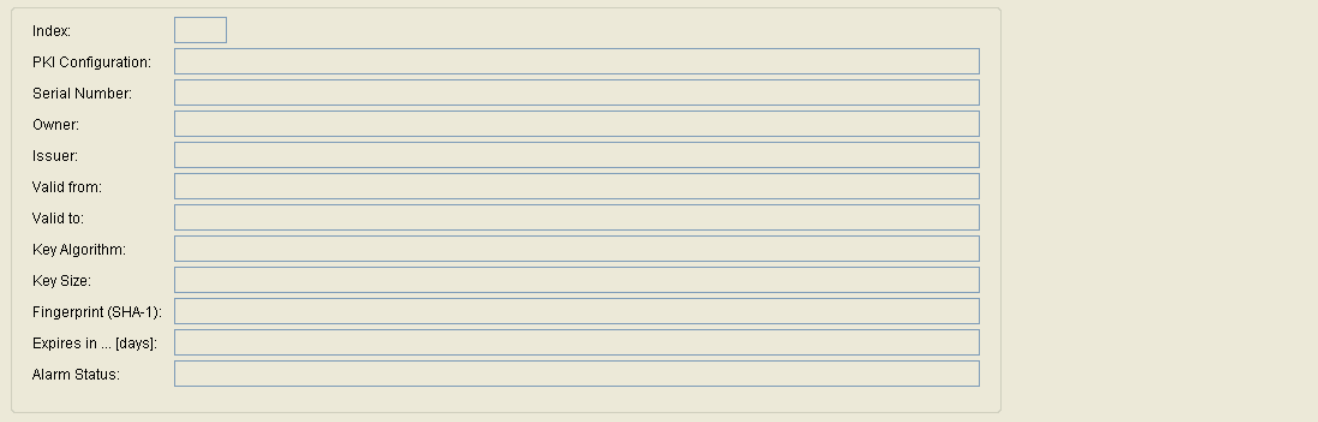


PKI Configuration:	
Serial Number:	7E
Owner:	CN=OpenScape Deployment Service V3, O=Siemens Enterprise Communications GmbH & Co. KG, L=Munich, C=DE
Issuer:	iemens.com, CN=Siemens Com ESY HD Security Office, OU=Com Enterprise Systems, O=Siemens AG, L=Munich, C=DE
Valid from:	2009-10-29 20:10:15
Valid to:	2024-10-28 20:10:15
Key Algorithm:	RSA
Key Size:	1024
Fingerprint (SHA-1):	A76E88D84ECE704D6F93A88A4BA6867BB194C1D0
Expires in ... [days]:	5031
Alarm Status:	valid

For further parameter description, see chapter Section 6.3.12.1, ""DLS Client GUI" Tab".

6.3.12.4 "Truststore DLS API" Tab

Call: Main Menu > Administration > Server Configuration > TLS Connector Configuration > "Truststore DLS API" Tab



Index

Index of TLS Connector.

For further parameter description, see chapter Section 6.3.12.1, ""DLS Client GUI" Tab".

6.4 Cluster Configuration

Call: Main Menu > Administration > Cluster Configuration

This menu item consists of the following areas:

- Deployment Server
- Cluster Settings

6.4.1 Deployment Server

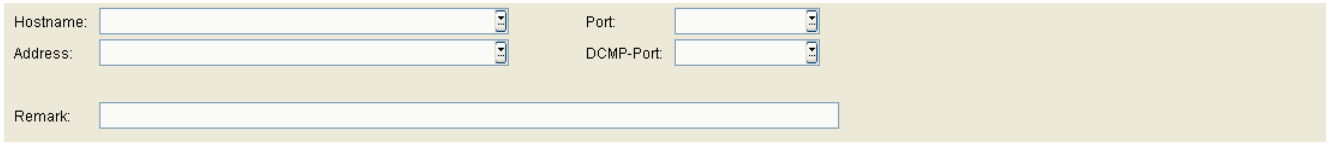
Call: Main Menu > Administration > Cluster Configuration > Deployment Server

This area is used for monitoring and controlling the DLS server installed in the cluster. You can also stop, start or restart the deployment service running on the individual servers here. The requirement for this is that they are registered as cluster nodes in the DLS database. Active nodes log back on at five-minute intervals.

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

General Data



Hostname:

Name of the node within the cluster.

Address:

IP address, domain, or host name of the DLS.

Remark:

Field for general information.

Port:

Port of the DLS.

DCMP-Port:

Port of the DCMP (DLS Communication Management Proxy).

Possible Action Buttons

Search

Searches the database for configured servers that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

New

Creates a new cluster node.

Delete

Deletes one or more nodes (multiple selections possible in Table view).

Deployment Service

Opens a dialog window to start, stop or restart the Deployment Service at the selected node.

6.4.1.1 "Info" Tab

Call: Main Menu > Administration > Cluster Configuration > Deployment Server > "Info" Tab



Last Registration

Last time the node registered at the cluster.

Status

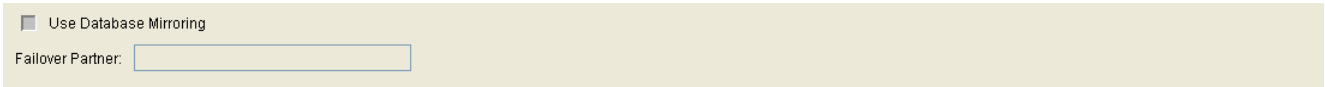
Status of the node within the cluster.

Possible values:

- **Active**
  The node is active.
- **Inactive**
  The node has either logged itself on as inactive or was recognized as inactive by other nodes in the cluster.

6.4.2 Cluster Settings

Call: Main Menu > Administration > Cluster Configuration > Cluster Settings



Use Database Mirroring

Switch on database mirroring. This is helpful only if MS SQL database mirroring has been configured for the DLS database.

Failover Partner

IP address of the mirroring instance for the DLS database.

6.5 Display Logging Data

Call: Main Menu > Administration > Display Logging Data

This menu item consists of the following areas:

- Activity and Error Log
- Audit and Security Log
- P&P Import Protocols
- Alarm Protocol
- Alarm List

6.5.1 Activity and Error Log

Call: Main Menu > Administration > Server Configuration > Display Logging Data > Activity and Error Log

Specify which events should be logged and how long events should be saved.

You can select filters to view a specific range of logged data. The filtered data is displayed in a separate browser window.

This area features the following components:

- Possible Action Buttons
- "Configuration" Tab
- "Protocol" Tab

Possible Action Buttons

Save

Saves all settings made.

Discard

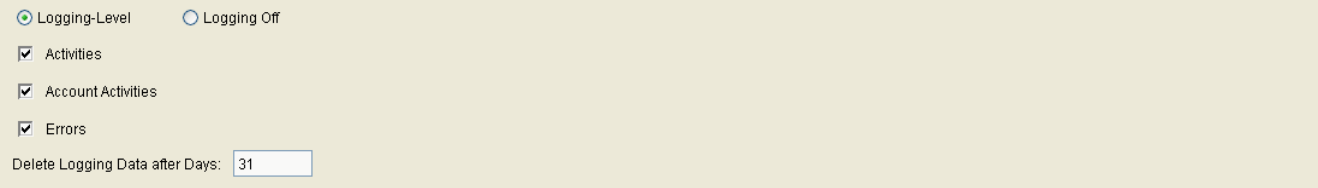
Discards any changes entered.

Refresh

Updates the window using the database.

6.5.1.1 "Configuration" Tab

Call: Main Menu > Administration > Display Logging Data > Activity and Error Log > "Configuration" Tab



Logging-Level

Check box for activating logging.

Logging off

Check box for deactivating logging.

Activities

All DLS activities must be logged in the Activities log.

Account Activities

All account activities must be logged in the Account Activities log.

Errors

The Errors log only records failed actions and internal errors, such as, license violations or SQL database errors.

Delete Logging Data after Days:

Number of days the logged events should remain saved before they are automatically deleted.

Value range: 1 ... 365 days.

Default: 31

6.5.1.2 "Protocol" Tab

Call: Main Menu > Administration > Display Logging Data > Activity and Error Log > "Protocol" Tab



Logging-Level

Activities

All DLS activities must be logged in the Activities log.

Account Activities

All account activities must be logged in the Account Activities log.

Error

The Errors log only records failed actions and internal errors, such as, license violations or SQL database errors.

Date:

Period of time during which the log data should be displayed (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Protocol

Starts outputting logging data. The filtered data is displayed in a separate browser window.

6.5.2 Audit and Security Log

This functionality is available on the GUI depending on the roles and rights of the account.

Call: Main Menu > Administration > Display Logging Data > Audit and Security Log

This area features the following components:

- Possible Action Buttons
- "Configuration" Tab
- "Protocol" Tab

Possible Action Buttons

Discard

Discards any changes entered. Not applicable for the "Protocol" Tab.

Save

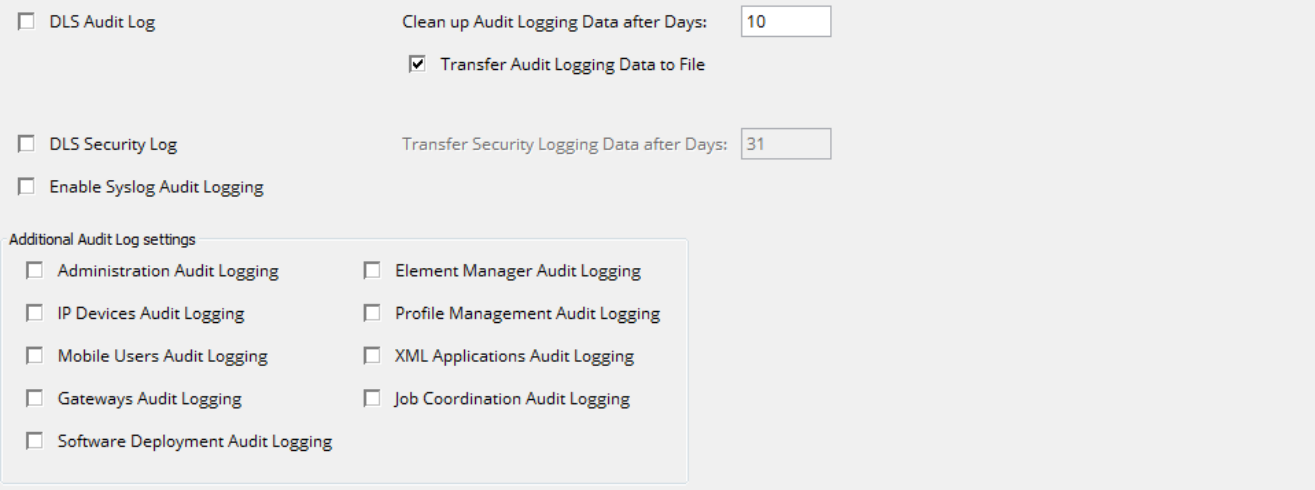
Saves all settings made. Not applicable for the "Protocol" Tab.

Refresh

Updates the window using the database.

6.5.2.1 "Configuration" Tab

Call: Main Menu > Administration > Display Logging Data > Audit and Security Log > "Configuration" Tab



DLS Audit Log

When active, all DLS activities invoked by an account are logged.

Clean up Audit Logging Data after Days

Number of days until the autit related log data is deleted or transferred to a file.

Value range: **1** ... **365**

Transfer Audit Logging Data to File

When active, the audit related logging data will be transferred to a file after the time configured in **Clean up Audit Logging Data after Days**.

DLS Security Log

When active, all security relevant activities are logged.

NOTE: Security logs are a subset of Audit logs.

Transfer Security Logging Data after Days

Number of days until the security related log data is transferred to a file.

Value range: **1** ... **365**

Enable Syslog Audit Logging

When enabled, all DLS event logs (including security logs) are sent to an external syslog server.

> ***IMPORTANT:*** As a prerequisite, syslog server must be configured in DLS.
>
> Refer to Administration > Alarm Configuration > „Syslog“ Tab
>
> Configure:
> Server Address: your Syslog ip address
> Port: Syslog port (default value:**514**)
> Facility: Important only for Alarming (e.g. **local0**)
> Severity: Important only for Alarming (e.g. **alert**)
>
> Press **Save**

> ***NOTE:*** DLS will only report some system related actions in the logs. To select a broader set of events refer to the following Additional Audit Log settings.

Additional Audit Log settings

DLS provides a log reduction capability that supports on-demand reporting. The following audit log areas can be enabled.

Administration Audit Logging

IP Devices Audit Logging

Mobile Users Audit Logging

Gateways Audit Logging

Software Deployment Audit Logging

Element Manager Audit Logging

Profile Management Audit Logging

XML Application Audit Logging

Job Coordination Audit Logging

6.5.2.2 "Protocol" Tab

Call: Main Menu > Administration > Display Logging Data > Audit and Security Log > "Protocol" Tab



Date

Log data that has been created in the time period specified here will be displayed.

Audit Log

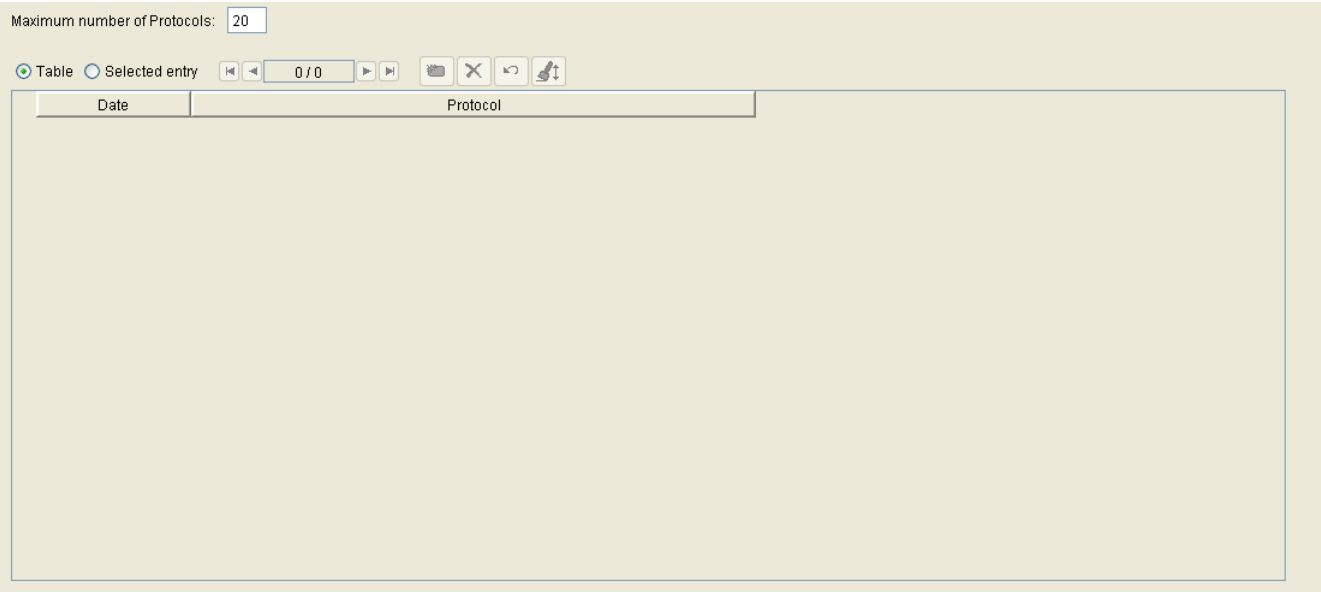
Button to start the display of DLS audit log data.

Security Log

Button to start the display of DLS security log data.

6.5.3 P&P Import Protocols

Call: Main Menu > Administration > Display Logging Data > P&P Import Protocols



For information on general interface operation, see Section 5.4.2, "Work Area".

NOTE: The **Object** view is only available per tennant.Therefore the **ALL** option shall not bring any results.

Maximum number of Protocols:

The maximum number of protocols created when importing Plug&Play data.

Value range: **1** ... **40**.

Date

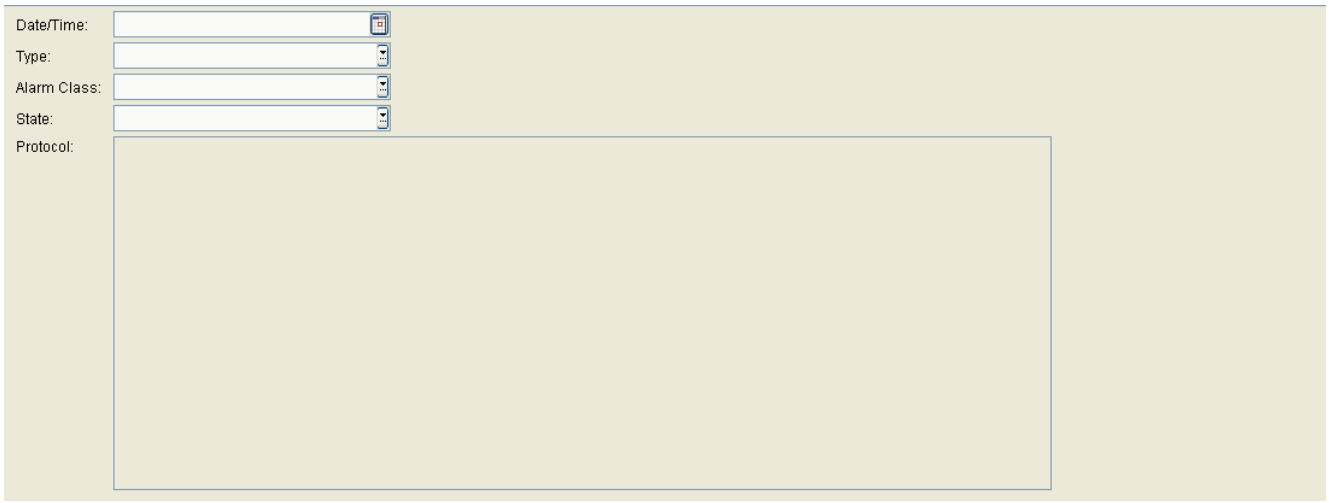
Protocol creation date.

Protocol

Plug&Play import protocol.

6.5.4 Alarm Protocol

Call: Main Menu > Administration > Display Logging Data > Alarm Protocol



Date/Time

Date/Time at which the action has started.

Alarm Class

Alarm class of the alarm.

Type

Type of alarm.

State

State of the action.

Possible Options:

- **running**
- **pending**
- **finished**
- **failed**
- **timeout**

Protocol

Protocol of the execution.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

6.5.5 Alarm List

Call: Main Menu > Administration > Display Logging Data > Alarm List



DLS shall display a list with the DLS alarms that are stored in DLS Database. When an alarm condition occurs (log event), a new entry shall be added in the Database.

Date/Time

Date/Time at which the action has started.

Alarm Class

Alarm class of the alarm.

State

State of the action.

Possible Options:

- **active**

  The state is active when the alarm condition exists.

- **cleared**

  The state is cleared when the alarm condition is disappeared.

Protocol

Protocol of the execution.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Delete

Offers the capability to remove an alarm from the list. DLS shall clear the alarm and then shall remove it from the Database.

Delete all

Offers the capability to remove all the alarms from the list.

Clear Alarm

Offers the capability to change the status of an alarm from ’’ active’’ to ’’cleared’’.

DLS shall update the alarm status in the Database and also send clear trap for this alarm in the configured SNMP destinations.

If an alarm is raised (and displayed) more than once and you press the Clear Alarm option then the Alarm Status should go from ’’active’’ to ’’cleared’’ in all rows.

Refresh

Refreshes the content of the alarm list.

6.6 Alarm Configuration

Call: Main Menu > Administration > Alarm Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Alarm Classes" Tab
- "Notification" Tab
- "SNMP" Tab
- "Batch File" Tab
- "Email" Tab
- „Syslog“ Tab
- "Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data



Notification to DLS Users

When active, logged on DLS users will be notifed of an alarm, depending on the individual settings in the "Alarm Classes" Tab. For this purpose, the DLS users must be selected for notification by means of the "Notification" Tab. The alarm notification is displayed in the title bar of the DLS window.

SNMP Trap

When active, an SMNP trap is sent to the server determined in the "SNMP" Tab, depending on the individual settings in the "Alarm Classes" Tab.

Batch File Execution:

When active, the batch file specified in the "Batch File" Tab is executed, depending on the individual settings in the "Alarm Classes" Tab.

Email:

When active, an Email is sent using data specified in the "Email" Tab, depending on the individual settings in the "Alarm Classes" Tab.

Syslog:

When active, the alarm will be added to systemlog file, depending on the individual settings in the "Alarm Classes" Tab.

Possible Action Buttons

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

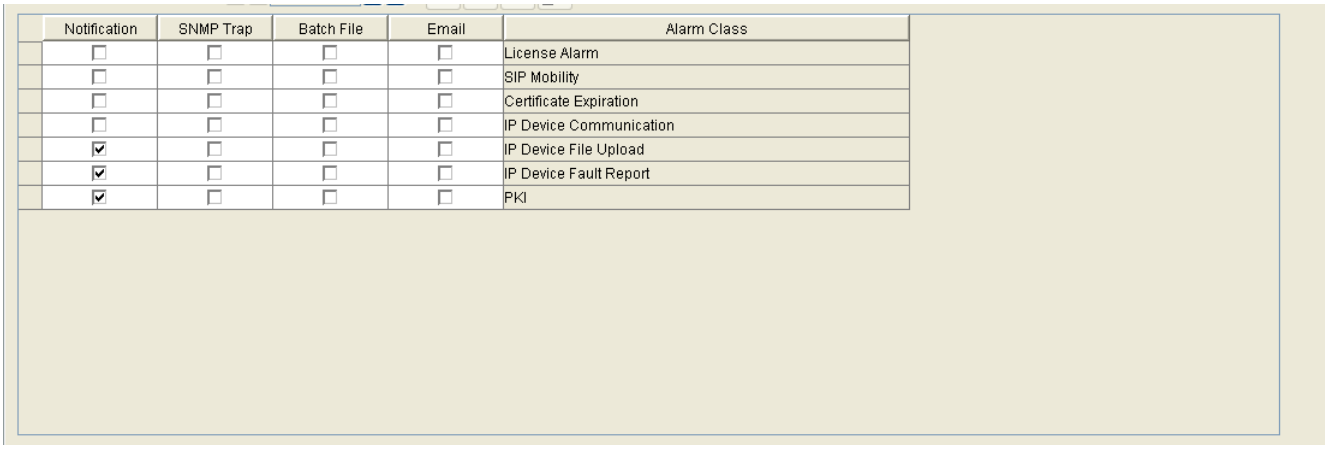
Refresh

Refreshes the content of the relevant page.

6.6.1 "Alarm Classes" Tab

Call: Main Menu > Administration > Alarm Configuration > "Alarm Classes" Tab

Here, the actions for specific alarm classes are selected. The composition of this list depends on the startup settings of the DLS and cannot be modified. The possible actions are user notification, SNMP Trap, execution of a batch file, and the sending of an Email. However, whether the actions are actually executed depends on the check boxes under **General Data**. So, for instance, if **Email** is deactivated under **General Data**, the individual setting in the alarm class table is no longer considered.



Index

Index for the alarm action to be triggered (notification, batch file, SNMP trap, or Email).

Notification

If this check box and the **Notification to DLS Users** check box in the **General Data** area are activated, the DLS users listed in the "Notification" Tab are notified according to this alarm class.

SNMP Trap

If this check box as well as the check box **SNMP Trap** under **General Data** is active, the SNMP trap will be sent to the receiver configured for this alarm class.

Batch File

If this check box and the **Batch file execution** check box in the **General Data** area are activated, the configured command file for this alarm class is executed.

Email

If this check box and the **Email** check box in the **General Data** area are activated, the configured e-mail for this alarm class is executed.

Alarm Class

Functional area within which an alarm shall be triggered in case of an error. The list cannot be modified; it depends on the startup settings of the DLS.

Possible values:

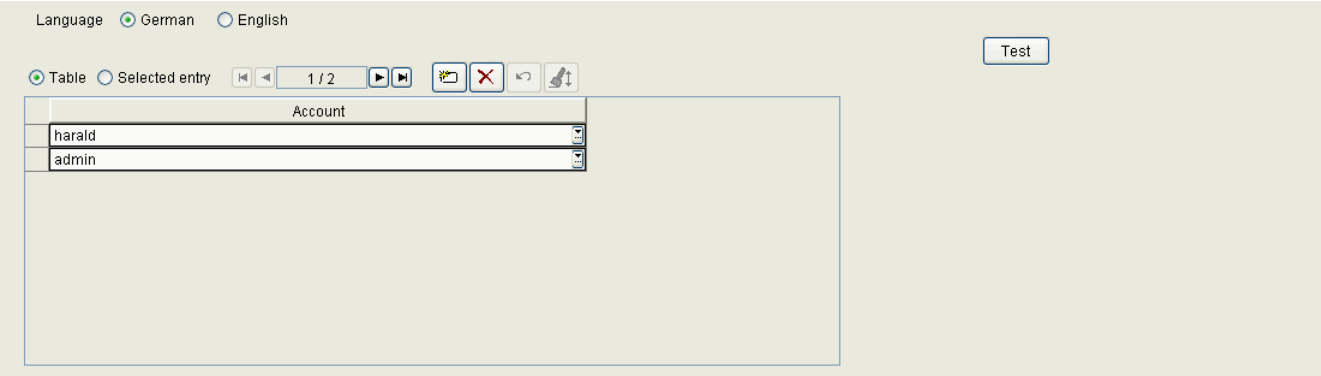
- **DLS Service**
- **DLS Cluster**
- **DLS Communication Error**
  An alarm is triggered when a connectivity failure occurs under Contact Me Notify functionality.
- **License Alarm**
- **SIP Mobility**
- **Element Manager Synchronization**
  An alarm is triggered when an error occurs at some point through registration data transfer from Element Manager to DLS db.
- **Certificate Expiration**
- **Policy Alarm**
  An alarm is triggered when an error occurs in policy settings, please refer to Section 6.1.2, "Policy Settings" .
- **Resource Alarm**
  Corresponds with the threshold **Minimum free space** under **Administration** > **File Server**.
- **DCMP**
  i.e,dcmp configuration error, DLS or phone wise.
- **DLS Cluster**
- **Resource Alarm**
  Corresponds with the threshold **Minimum free space** under **Administration** > **File Server**.
- **IP Device Communication**
  An alarm is triggered when an error occurs in IP Device interaction / management
- **IP Device File Upload**
  i.e, an error alarm is triggered when a timeout occured while executing the deployment job because the time entered for Job Configuration was exceeded (for example, by an IP Device that was unavailable for an extended period of time).
- **IP Device Fault Report**

- **PKI**
  i.e,PKI configuration error.
- **SecurityLog-Upload caused unexpected problems**

  IMPORTANT: This specific alarm remains active even in the case where communication with the device has been re-established.

6.6.2 "Notification" Tab

Call: Main Menu > Administration > Alarm Configuration > "Notification" Tab



Language

The language of the text in the notification alarm.

Possible options:

- **German**
- **English**

Account

The DLS user accounts which shall be notified by the alarms selected in the "Alarm Classes" Tab are entered here.

Test

Tests the notification. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

6.6.3 "SNMP" Tab

Call: Main Menu > Administration > Alarm Configuration > "SNMP" Tab

In case of alarm, a SNMP trap is sent. Not every protocol data unit is supported, especially not GET/SET requests. However, the SNMP partial tree created by the DLS can be read and processed by a trap receiver.

The DLS uses the following part of the MIB to generate 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 }
```

The parameters have the following meanings resp. values:

`hostname`: Host name of the DLS server.

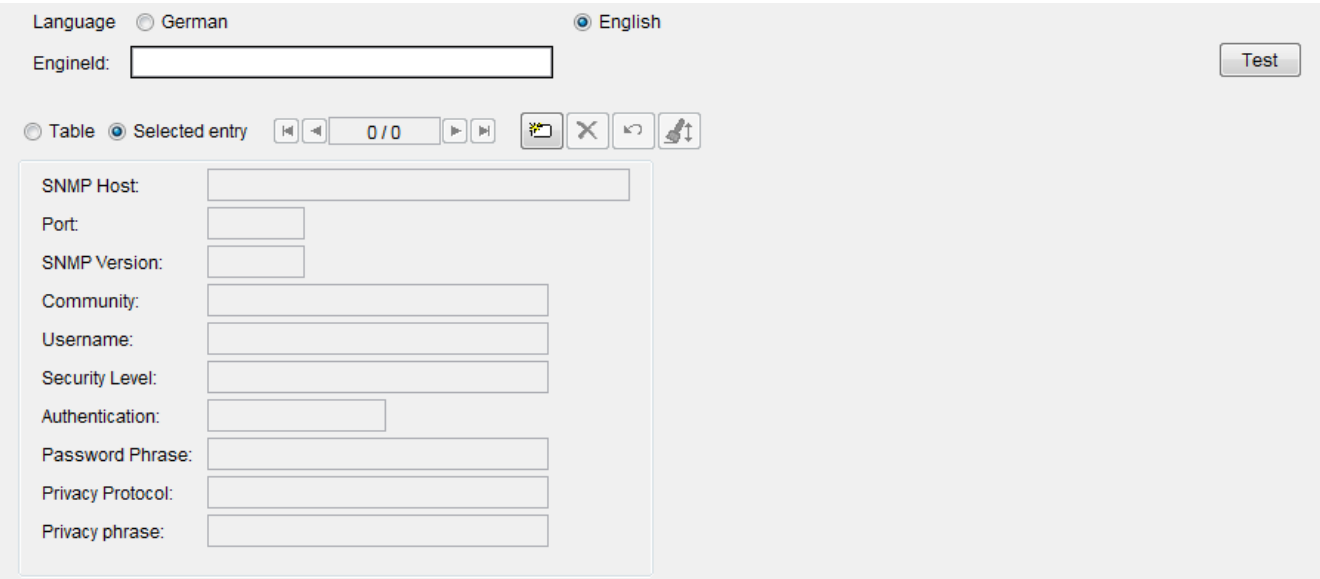
`appName`: "DLS"

`appState`: 3 (= warning)

`evtHistory-Date`: Date of trap occurence.

`evtHistory-Descr`: Description text (as passed by `createHiPathApplicationStatusChange()`).

`hiPathTrapSeverity`: 3 (= warning)



Language

Language of the description text for the SNMP trap.

Possible options:

- **German**
- **English**

EngineId

EngineID is used as an identifier for DLS agent among different agents.

Test

Sends a test SNMP trap. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

SNMP Host

Name of the SNMP Server (manager).

Port

Port of the SNMP server (manager).
Default: **162**

SNMP Version

Possible options:

- **v1/v2c**
- **v3**

Community

Community / password for the SNMP server (manager).

NOTE: Community string is only valid for SNMP **v1/v2c** destinations.

Username

Name of SNMP user.

Security Level

Select the security level of the SNMP user.

- **No Authentication No Privacy**
  No authentication or privacy configured. Username match will be used for authentication.
- **Authentication No Privacy**
  Authentication configured, but no privacy configured. Provides authentication based on the selected authentication algorithm (**MD5** or **SHA**).
- **Authentication Privacy**
  Authentication and privacy configured. Provides authentication based on the selected authentication algorithm (**MD5** or **SHA**). In addition to authentication, provide encryption based on the selected standard (**DES** or **AES**).

Authentication

Applicable only if security level is set to **Authentication No Privacy** or **Authentication Privacy**

Password Phrase

Enter the authentication password of the user.

Privacy Protocol

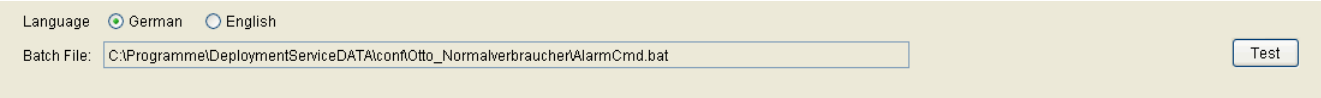
Applicable only if security level is set to **Authentication Privacy**

Privacy phrase

Enter the privacy password of the user.

6.6.4 "Batch File" Tab

Call: Main Menu > Administration > Alarm Configuration > "Batch File" Tab



Language

The language of the alarm message text.

Possible options:

- **German**
- **English**

Batch File:

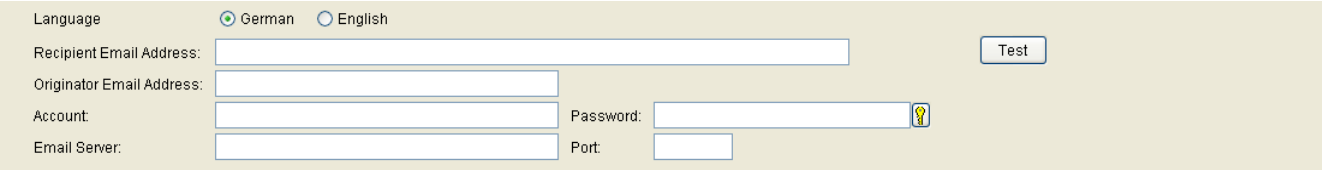
Path and name of the batch file which is executed when an alarm is triggered. After DLS installation, the path and file name reference a sample file which also contains rules for creating a command.

Test

Tests the execution of the batch file. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

6.6.5 "Email" Tab

Call: Main Menu > Administration > Alarm Configuration > "Email" Tab



Language

The language of the alarm message text.

Possible options:

- **German**
- **English**

Recipient Email Address:

Email address of the alarm mail recipient.

Test

Tests the Email send operation using the account data entered. The result of the test can be checked under **Administration** > **Display Logging Data** > **Alarm Protocol**.

Originator Email Address:

Email address(es) that appear as the originator address when the mail is sent. One or more addresses can be entered, up to a maximum of 255 characters, separated by ";" "," or " " (space).

Account:

Name of the Email account.

Password:

Password for this Email account.

Email Server:

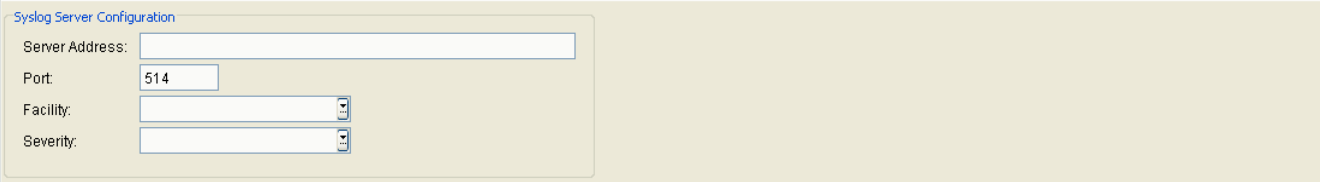
Name of the SMTP server that is to be used for alarm Emails.

Port:

Port number of the SMTP server. If no value is entered, port 25 is used by default.

6.6.6 „Syslog“ Tab

Call: Main Menu > Administration > Alarm Configuration > „Syslog“ Tab



Syslog Server Configuration

Server Address

Address of Syslog Server

Port

Portnumber of Syslog Server

Facility

Possible options:

- **local0**
- **local1**
- **local2**
- **local3**
- **local4**
- **local5**
- **local6**
- **local7**

Severity

Setting of Trace Level

Possible options:

- **emerg**
- **alert**
- **crit**
- **error**
- **warning**
- **notice**
- **info**
- **debug**
- **none**

6.6.7 "Settings" Tab

Call: Main Menu > Administration > Alarm Configuration > "Settings" Tab



Alarm Configuration for Expiring Certificates

Minimum validity period: [days]

An alarm is issued if a certificate expires during this time period.

Value range: **1** - **60**.

Interval: [hours]

The remaining certificate validity period is checked in the interval specified here.

Value range: **1** - **60**.

Default value: **6**

Alarm Configuration for Short of Resources

Interval [mins]

The supply of resources is checked in the interval specified here.

Value range: **1** - **2880 minutes**

Alarm Protocol Settings

Maximum number of Protocols:

Maximum number of lines in the protocol.

Value range: **1** - **100000**

Notification Settings

Alarm Icon:

Choice list of icons for notifying the DLS user of alarms which are not closed yet. The icon is displayed in the title bar of the DLS window.

Notify first new alarm with Popup Window

When active, the first new alarm is signaled by means of a popup window, if all prior alarms have been closed before.

Notify every new alarm with Popup Window

When active, every new alarm is signaled by means of a popup window, if no popup window is not already open.

6.7 Backup/Restore

Call: Main Menu > Administration > Backup/Restore

NOTE: This function is not available in the onboard variants of DLS on OpenScape Voice systems. In this case, the DLS file is backed up using the comprehensive OpenScape Voice Backup/Restore function.

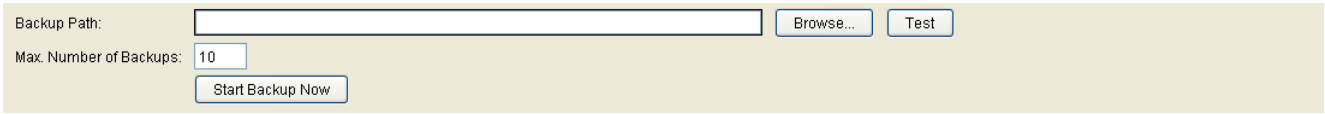
This area features the following components:

- General Data
- Possible Action Buttons
- "Backup" Tab
- "Restore" Tab
- "Protocol" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

Refer to Section 15.11.1, "Automatic Data Backups" for more information on Backup/Restore.

General Data



Backup Path:

File path where the backup is saved on the DLS server. If the DLS uses a remote database for its data, a directory path on the database server must be entered. It must be reachable by the DLS server. The format must also be usable locally on the database server, e. g.
`\\<IP-Address DB Server>\C$\<Backup Pfad on DB Server on drive C>`

NOTE: In a single node deployment with PostgreSQL, the produced backup file is a **.dump file**. In a multi node deployment with MSSQL, the produced backup file is a **.bak file.**

Browse...

Click this button to open a dialog window that you can use to select an existing backup directory. To navigate to the subdirectories of a directory, double click on the directory name. To navigate up to the next higher directory level, double click on "..\". In order to select a directory, highlight it with a single click and, afterwards, click **Open**.

Test

Click Test to verify that the path is valid (accessible).

Max. Number of Backups:

Number of backup files managed. When you create a new backup file, the oldest one is deleted.

Value range: **1** ... **99**.

Start Backup Now

If you click this button, a backup is executed immediately, independently of the automatic, periodic backup setting. This does not use the backup path stored in the database, but the current backup path as it appears in the mask (which may have changed and not yet been saved). This allows you to save an individual backup at a location different from the location where the periodic backups are stored.

> ***NOTE:*** Everytime that you press the backup button, the size of the backup file is different.The reason behind this size flactuation is the .trn files.

NOTE: The .trn files are the backup transaction log files,useful when the recovery transaction model of the database is either full or bulk-logged.The backup of the transaction logs is different than the backup of the database.Transaction logs not only contain all the transaction SQL command requests issued to the database but also differences in data (i.e. tables,indexes).

NOTE: Since the transaction logs contain data changes,it is reasonable to see big differences in the transaction log backup file sizes, even in small time frames.Also,when a transaction log is backed up the backed up transaction log entries are deleted.That is why, if after a transaction log backup you attempt another one,the backup file size will be very small compared to the first one.

Administration
Backup/Restore

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

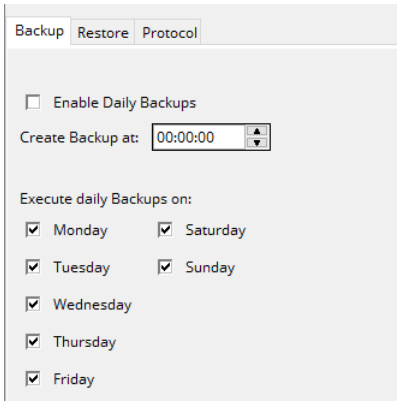
Refresh

Refreshes the content of the relevant page.

6.7.1 "Backup" Tab

Call: Main Menu > Administration > Backup/Restore > "Backup" Tab

For more information, see Section 15.11.1.1, "Configuring Automatic Backups".



Enable Daily Backups

Select to activate a daily backup.

Next Backups on:

Time (date and time) of the next scheduled backup (for information on the calender, see Section 5.4.2.4, "Time field with calendar button").

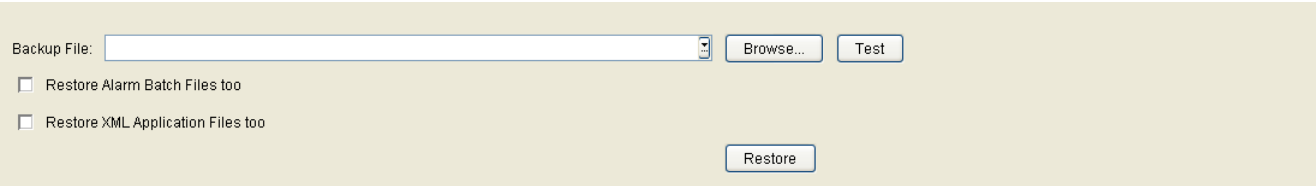
Execute daily Backups on:

If the **Enable Daily Backups** check box is active, use these check boxes to restrict backup to specific days of the week.

6.7.2 "Restore" Tab

Call: Main Menu > Administration > Backup/Restore > "Restore" Tab

For more information, see Section 15.11.1.2, "Restoring Backups".



Backup File:

Path and file name for restoring a backup on the DLS server. If backups have already been successfully restored, you can enter them using the choice list.

NOTE: In a single node deployment with PostgreSQL, the user can choose to restore either a **.zip** or a **.dump** file. In a multi node deployment with MSSQL, the user can restore a **.bak** file.

Restore Alarm Batch Files too:

If switch is activated, the stored alarm batch files will be restored.

Restore XML Application Files too:

If switch is activated, the customer specific XML application files will be restored to the directory `<Installation directory>/XMLApplications/data/custom`

If switch is not activated, the customer specific XML Application Files will be copied to the directory `<Installation directory>/XMLApplications/data/custom_old`

See also Section 16.18, "Data Structures for DLS-hosted XML applications"

Browse...

Click this button to open a window where you can select an existing backup file. The path and file name are entered in **Backup File**.

> ***NOTE:*** In a Multi Node environment,if you press this button and browse for a backup path that is situated locally in Node 1 or Node 2 then the selected path is connected to the IP address of the 1st Ethernet Interface of the DLS server.
> If the 1st interface happens to be that of the external (or frontend network), the DB restore will fail as DLS cannot contact SQL server through that interface.

NOTE: DLS can contact SQL server only through the internal (backend) network interface and this cannot stated explicitly if the path is chosen by the **'Browse...'** button.

Test

Click this button to verify that the backup file is valid (accessible).

Restore

When you click this button, a restore is executed. A dialog window will ask whether Plug&Play is to be switched off after restore or not. If Plug&Play has been switched off, it is possible to switch it on again via **Administration** > **Server Configuration** > **P&P Settings** > **Plug&Play enabled**. Beforehand, it must be ensured that all IP devices are registered in the DLS database.

This does not use the backup file stored in the database, but the current backup file as it appears in the mask (which may have changed and not yet been saved).

NOTE: When database mirroring (see Section 4.6, "SQL Database Mirroring Setup") is active, no restore of backups is possible.

NOTE: There are some basic server configuration data which will never be restored as e.g.
- the base configuration
- the license settings

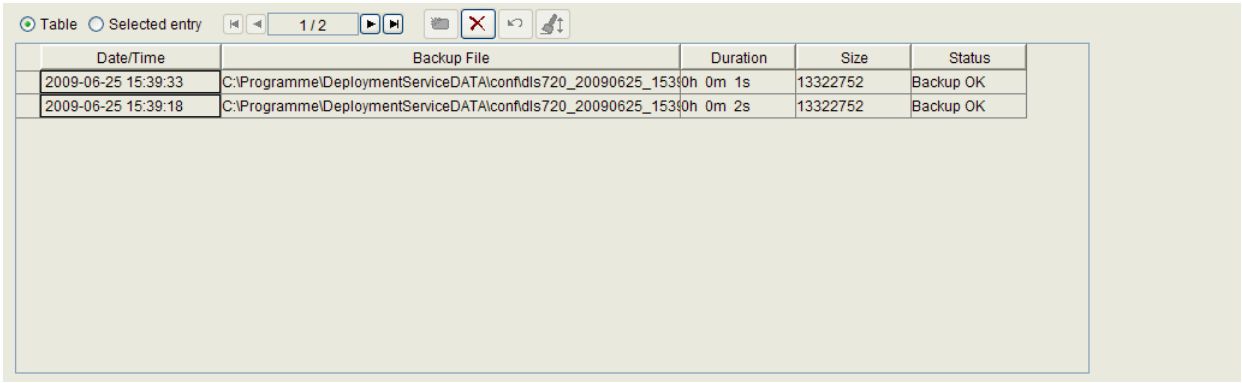
in order to guarantee a proper operation after any restore.

NOTE: During a restore, **all** users are momentarily disconnected from the DLS database as the restore process requires exclusive access to the database. These users must log on again.

6.7.3 "Protocol" Tab

Call: Main Menu > Administration > Backup/Restore > "Protocol" Tab

For more information, see Section 15.11.1.3, "Monitoring Backups".



Date/Time

Backup time.

Backup File

Backup file name.

Duration

Duration of the backup process in hours, minutes, and seconds.

Size

Size of the backup file in bytes.

Status

Status of the backup/restore.

Possible values:

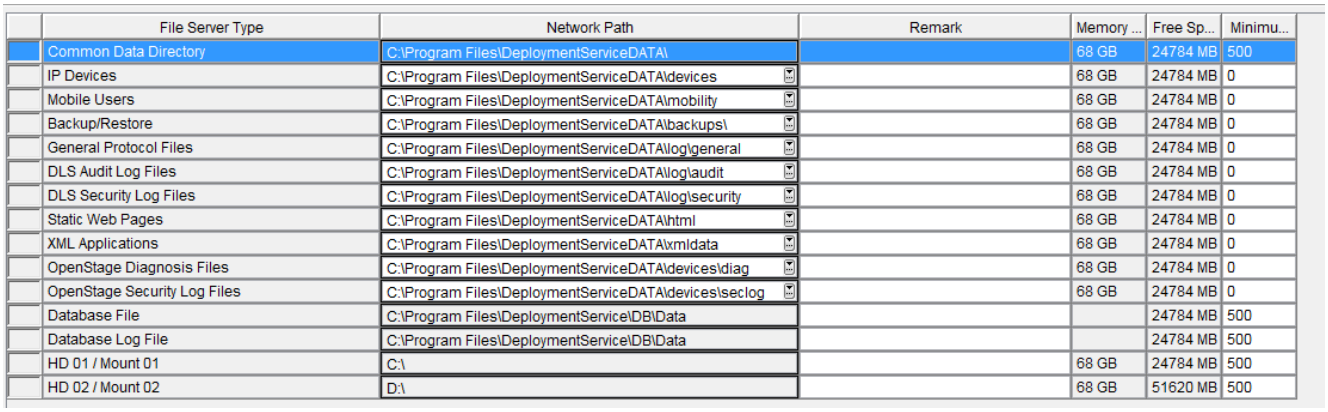
- **Backup OK**
- **Backup failed**

- **deleted**
- **Restore OK**
- **Restore failed**

6.8 File Server

Call: Main Menu > Administration > File Server

You can use this menu item to set the default network drives or local folders for saving DLS data.



File Server Type	Network Path	Remark	Memory ...	Free Sp...	Minimu...
Common Data Directory	C:\Program Files\DeploymentServiceDATA\		68 GB	24784 MB	500
IP Devices	C:\Program Files\DeploymentServiceDATA\devices		68 GB	24784 MB	0
Mobile Users	C:\Program Files\DeploymentServiceDATA\mobility		68 GB	24784 MB	0
Backup/Restore	C:\Program Files\DeploymentServiceDATA\backups\		68 GB	24784 MB	0
General Protocol Files	C:\Program Files\DeploymentServiceDATA\log\general		68 GB	24784 MB	0
DLS Audit Log Files	C:\Program Files\DeploymentServiceDATA\log\audit		68 GB	24784 MB	0
DLS Security Log Files	C:\Program Files\DeploymentServiceDATA\log\security		68 GB	24784 MB	0
Static Web Pages	C:\Program Files\DeploymentServiceDATA\html		68 GB	24784 MB	0
XML Applications	C:\Program Files\DeploymentServiceDATA\xmldata		68 GB	24784 MB	0
OpenStage Diagnosis Files	C:\Program Files\DeploymentServiceDATA\devices\diag		68 GB	24784 MB	0
OpenStage Security Log Files	C:\Program Files\DeploymentServiceDATA\devices\seclog		68 GB	24784 MB	0
Database File	C:\Program Files\DeploymentService\DB\Data			24784 MB	500
Database Log File	C:\Program Files\DeploymentService\DB\Data			24784 MB	500
HD 01 / Mount 01	C:\		68 GB	24784 MB	500
HD 02 / Mount 02	D:\		68 GB	51620 MB	500

File Server Type

Defines which DLS data should be saved on this file server.

Possible values:

- **IP Devices**
- **Mobile Users**
- **Backup/Restore**
- **General Protocol Files**
- **DLS Audit Log Files**
- **DLS Security Log Files**
- **Static Web Pages**
- **XML Applications**
- **OpenStage Diagnosis Files**
- **OpenStage Security Log Files**
- **Database File**
  Shows the path where the DLS database is stored. The network name is relative to the SQL server and cannot be changed by means of this mask. Available only on systems with Microsoft SQL Server as database.
- **Database Log File**
  Shows the path where the transaction log of the DLS database is stored. The network name is relative to the SQL server and cannot be changed by means of this mask. Available only on systems with database type Microsoft SQL Server.

- **HD 01 / Mount 01**
  Shows either necessary devices with system data (on Linux based systems) or all available or mounted devices (on Windows based systems). The network path cannot be changed by means of this mask.
- **HD 02/ Mount 02**
  Shows either necessary devices with system data (on Linux based systems) or all available or mounted devices (on Windows based systems). The network path cannot be changed by means of this mask.

Network Path

Network path or local folder for saving DLS data.
Example: `\\MyFileServer\DlsFiles\Protocols`

Remark

Field for general information.

Memory Capacity

Displays the overall memory capacity of this network drive in gigabytes.

Free Space

Displays the available space on this network drive in megabyte. If this value is lower than the **Minimum Free Space**, this field is marked with a yellow border.

Minimum Free Space

Enter the minimum free space that must remain, in megabytes. If the value of **Free Space** falls below this value, an alarm will be triggered corresponding to the alarm configuration (see Section 6.6, "Alarm Configuration").

Value range: **0** ... **15000**

0 = no check

Acquisition Time

Date and time of acquisition of the additional information about **Memory Capacity [GB]** and **Free Space [MB]**. These values are stored once a week; the entries cannot be deleted.

Only available in object view, cannot be changed or deleted.

Memory Capacity [GB]

Shows the memory capacity at **Acquisition Time**.

Only available in object view, cannot be changed or deleted. The value is stored once a week.

Free Space [MB]

Shows the free space at **Acquisition Time**.

Only available in object view, cannot be changed or deleted. The value is stored once a week.

6.9 Workpoint Interface Configuration

Call: Main Menu > Administration > Workpoint Interface Configuration

This area features the following components:

- Possible Action Buttons
- "Secure mode" Tab
- "DCMP" Tab
- "HTTP-Proxy" Tab
- "Contact Me Notify" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Refresh

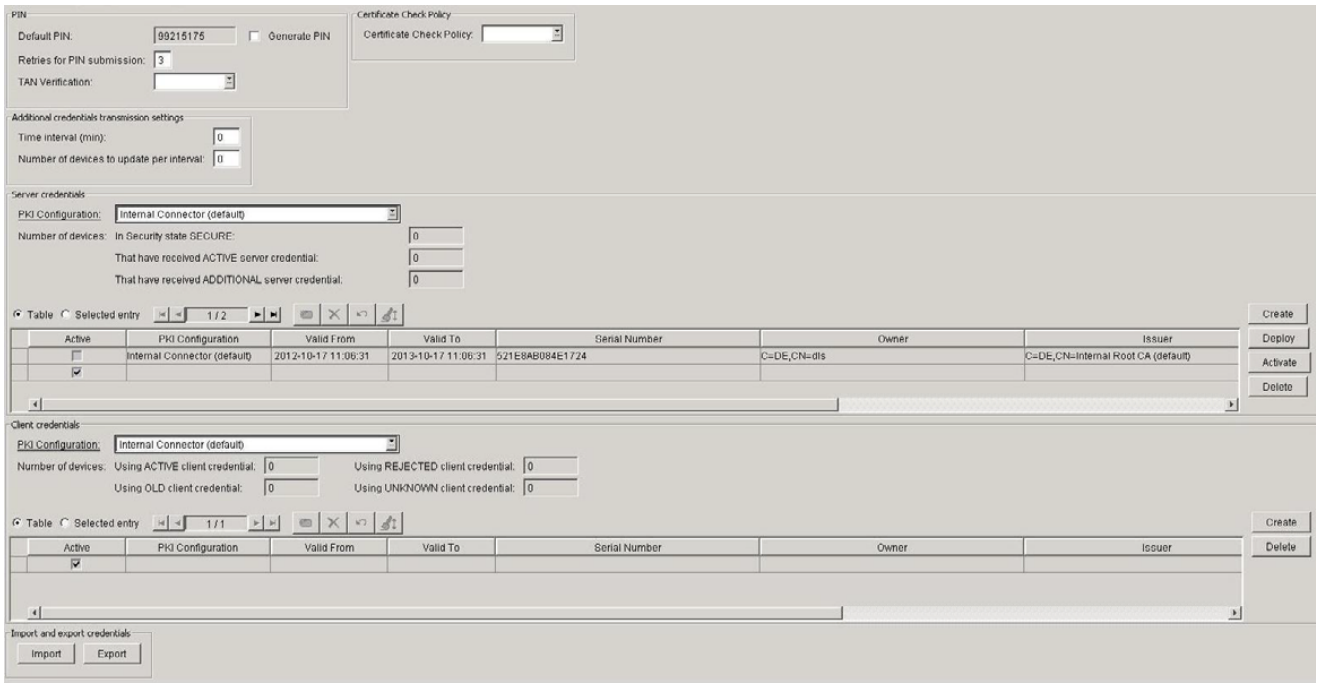
Refreshes the content of the relevant page.

6.9.1 "Secure mode" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "Secure mode" Tab

NOTE: For smooth secure mode operation, please ensure that the time and date on the OpenStage phone conforms with that on the DLS.

NOTE: Factory Reset with Plug&Play data stored is not possible in Secure Mode. The according IP Devices must be revert to Default Mode first.



PIN

Default PIN:

PIN created automatically by DLS to allow encrypted transfer of server credentials to the IP Device. This PIN is used by IP Devices with the "Default PIN" mode.

Generate PIN

If this check box is activated and you click **Save**, DLS creates a new default PIN. This PIN or, optionally, an individual PIN must be entered at the IP Device to decrypt the server credentials delivered by DLS. The PIN is used by IP Devices with **Insecure** security status.

Retries for PIN submission:

Specifies the number of failed attempts permitted when entering the PIN at the IP Device.

TAN Verification:

TAN (Target's Authentication Number) is the last 3 characters of PIN to be used by provisioning service to authenticate the target device in Secure Mode.

Possible Options:

- **False**
- **True**

TAN Verification can only be performed if TAN is required. If the IP Device has sent a TAN, but the current configuration does not require one, then the TAN cannot be verified.

Certificate Check Policy

Certificate Check Policy

The settings are used only for devices in secure mode.

Possible Options:

- **Trusted**
- **Full**

Restriction: When using Free Seating environments, option "Certificate Check Policy" must be set to "Trusted".
Administration > Workpoint Interface Configuration > Secure Mode > Certificate Check
Police = Trusted

NOTICE: When the flag "reset" is marked in DLS, the bootstrapping process is restarted. Its means that the certificates will be exchanged again and if necessary, the PIN code should be inserted.

Additional credentials tranmission settings

Time interval (min)

Time interval (in minutes) where new WPI credentials are sent.

Number of devices to update per interval

Number of devices to which WPI credentials are sent during the time interval.

Server Credentials

PKI Configuration

Selects the PKI Configuration for the server credentials to be activated. See also Section 6.2, "PKI".

> ***NOTE:*** WPI credentials cannot be created if PKI connector defines "Common Name or "Subject Alternative Name" with MAC. This is not supported.

Number of devices:

In Security state SECURE:

Number of devices in the SECURE security status.

That have received ACTIVE server credential:

Number of devices that have received the active server credential.

That have received ADDITIONAL server credential:

Number of devices that have received the ADDITIONAL security credential.

Active

Displays whether a server credential is active or inactive. The DLS always authenticates itself on a device in secure mode using the active server credential.

A maximum of one additional server credential can be created in preparation for exchanging the active server credential.

PKI Configuration

Shows name of the active PKI configuration.

Valid From

Credential start of validity.

Valid To

Credential end of validity.

Serial Number

Corresponding CA certificate serial number.

Owner

Credential's owner.

Issuer

Credential's issuer.

Fingerprint (SHA-1)

This fingerprint (hash value) uniquely identifies the credential (also in different DLS entities).

The fingerprint is part of the name of the export file (see also the **Export** field).

Key Algorithm

Credential's key algorithm.

Key Size

Credential's key size.

Create

Creates an additional (inactive) server credential. Only one additional server credential may be created.

A PKI configuration has to be enabled and selected (an internal connector is by default enabled). If an MS PKI connector shall be used, then an activation of PKI Configuration is needed). After selecting PKI configuration to be used, a new trust anchor is imported from the trust anchor configuration. The DLS will also request a new server certificate for its own TLS connector used for WPI communication.

Deploy

Deploys the additional server credential to all devices already in secure state.

The new trust anchor used by WPI clients to authenticate the DLS, will be deployed to them. One job for each device in secure state will be initiated.

Activate

Activates the additional (inactive) server credential in the DLS (thus the TLS connector may perform a restart using the new additional credential). When activation is complete, DLS queries are denied by all devices to which trust anchor relative to this credential has not yet been sent.

Delete

Deletes the additional (inactive) server credential.

Client credentials

PKI Configuration

Shows the PKI configuration of client credentials.

Number of devices:

Using ACTIVE client credential:

Number of (secure) devices that identify themselves using the active client credential.

Using OLD client credential:

Number of (secure) devices that identify themselves using an outdated client credential.

Using REJECTED client credential:

Number of (secure) devices whose client credential was denied. Credentials not found in the list are denied.

Using UNKNOWN client credential:

Number of (secure) devices in which the client credential used for identification is not known.

Active

Displays whether a client credential is active or outdated.

There is always exactly one active client credential. DLS also accepts devices that authenticate themselves using an outdated client credential. In this case, the device is automatically sent the current active client credential. The next time, it authenticates itself using the active client credential.

PKI Configuration

Shows name of the active PKI configuration.

Valid From

Credential start of validity.

Valid To

Credential end of validity.

Serial Number

Corresponding CA certificate serial number.

Owner

Credential's owner.

Issuer

Credential's issuer.

Fingerprint (SHA-1)

This fingerprint (hash value) uniquely identifies the credential (also in different DLS entities).

The fingerprint is part of the name of the export file (see also the **Export** field).

Key Algorithm

Credential's key algorithm.

Key Size

Credential's key size.

Create

Creates a new client credential. This new client credential is automatically activated and the client credential previously active is deactivated and becomes outdated. When a new client credential is created, it is sent to all devices.

> ***NOTE:*** The ’’ **Create** ’’ button does not trigger a deployment to all devices. Devices in secure state will get new client credentials, as soon as they contact DLS.

> ***IMPORTANT:*** In the case where the phone is unplugged from the network,then if the re-plugging is done quick enough, the job finishes successfully. If the time gap exceeds the job expiration frame (default value is 300 sec), the job for sending the credentials expires. In any case, the phone is deployed with new wpi certificates (as indicated in Section 7.6.4, "IP Device Configuration")
> Even if the job is manually cancelled, the phone will still get the certificate if it gets to contact DLS for other reason (e.g. reboot).

Delete

Deletes all inactive (outdated) client credentials. When the outdated client credentials have been deleted, DLS no longer accepts devices that identify themselves using an outdated client credential.

Import and export credentials

Import

Imports client and server credentials from a password-protected file. This import replaces existing credentials.

Export

Exports client and server credentials to a password-protected file.

> ***NOTE:*** The password is not intended for the zip archive format file but for the files contained in the zip file(WPI credentials).

In the case of manual import of WPI credentials:

- Go to Main Menu > Administration > Workpoint Interface Configuration

  In case you already have at least one Server and one client credential you can export them in order to inspect the naming format. The same format must be used for importing WPI credentials.

  A format example is:

  A zipped file that contains three files! Two files with p12 extension one for server and one for client credential. Note that the client credential is the issuing ca that DLS will use to validate the client certificate sent by the phone during WPI communication. The zipped file also contains a text file that specifies the 'PKI Configuration' name for client and server credentials as it should be displayed in DLS User Interface.

  An example of the three files is:

  ```
  server.act.2016-04-27.4BA0DF38ED790EFA4C0CFD424B92177DF1EC9394.p12
  ```

  PKIConfigurationName.txt

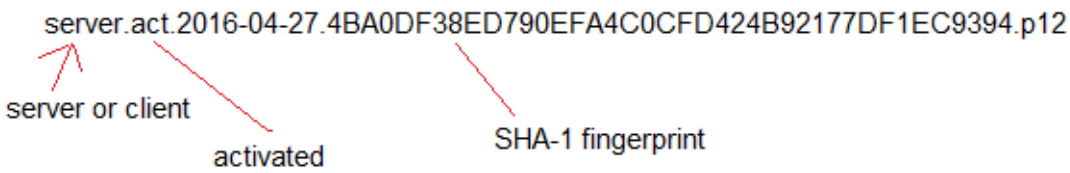
  ```
  client.act.2016-04-27.5DED656CA45E8C35E50D3F4B9DB065BCE17EC1FD.p12
  ```

  Whereas the content of the text file was ('StorageRootConnex' is the PKI connector name):

  ```
  ClientPKIConnectorName=StorageRootConnex
  ServerPKIConnectorName=StorageRootConnex
  ```

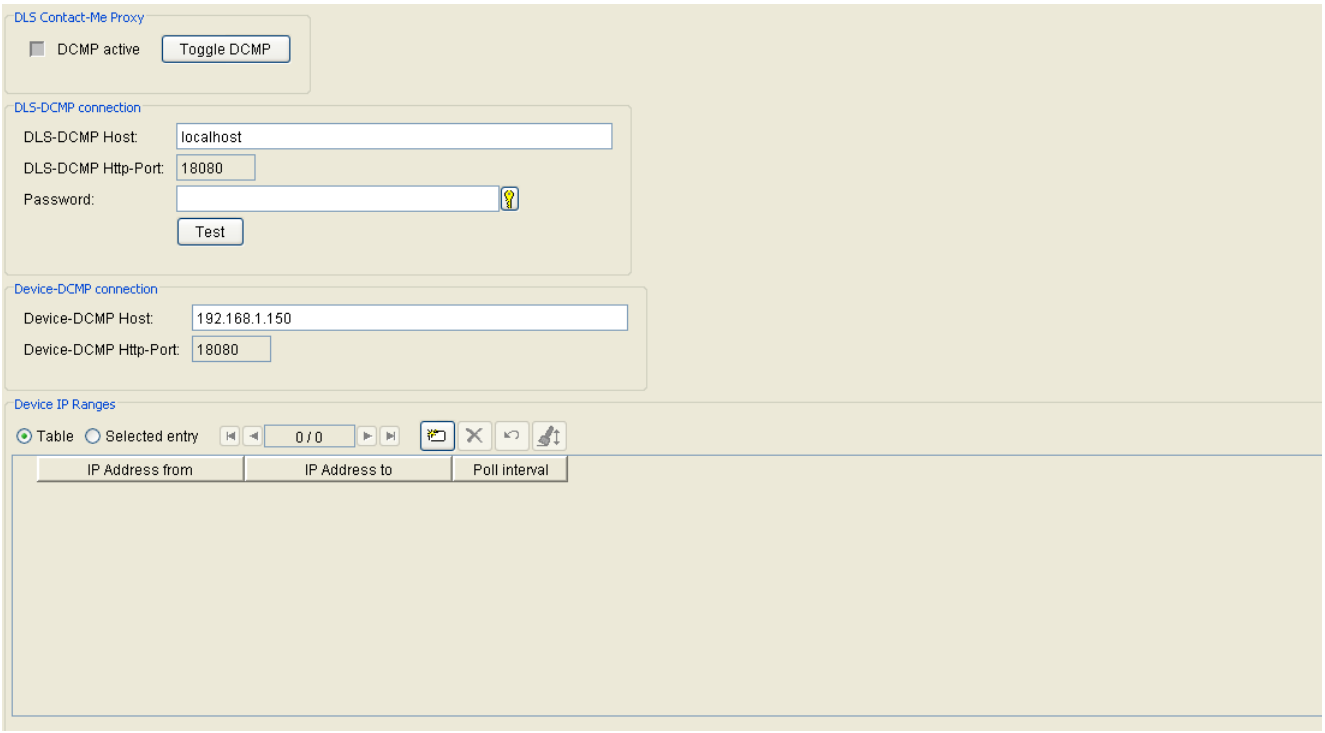
  IMPORTANT: Pay attention to the naming of the p12 files as you will have to follow the same convention for your imports.

  The following picture explains the naming parts.



6.9.2 "DCMP" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "DCMP" Tab



DLS Contact-Me Proxy

DCMP active

Activates DCMP globally. When DCMP is globally deactivated, no devices can be reached via DCMP.

Toggle DCMP

Switches DCMP activation and creates jobs for affected devices.

DLS-DCMP connection

DLS-DCMP Host:

Host name or IP address of the DCMP server. The DCMP server host must be reachable for DLS.

DLS-DCMP HTTP-Port:

DCMP server’s HTTP port for connecting DLS and DCMP.

Password:

Password for DLS access to the DCMP server.

Test

Tests the connection between DLS and the DCMP server using the current values stored for host, port, and password. When you change these values, you must save the changes before testing the DLS connection.

Device-DCMP connection

Device-DCMP Host:

Host name or IP address of the DCMP server. The DCMP server host must be reachable for devices activated by DCMP. In contrast to the DCMP-DLS connection, do not use "localhost" or "127.0.0.1" as the DCMP server host when both are running on the same host.

Device-DCMP HTTP-Port

DCMP server’s HTTP port for connecting telephones and DCMP.

Device IP Ranges

IP Address from:

Lower limit of IP addresses that are administered by DCMP.

IP Address to:

Upper limit of IP addresses that are administered by DCMP

Poll Interval:

The time between two consecutive polls at DCMP (in minutes).

The entered value must be lower than the value for Section 7.5.6.2, "Timeout (sec)"

Possible options:

0 - 1440, default: 60 minutes

6.9.3 "HTTP-Proxy" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "HTTP-Proxy" Tab

The settings made in this tab are necessary if the end devices can be reached by the DLS only via an HTTP proxy.



DLS-Device Connection

HTTP-Proxy active (to send HTTP-Requests to IP Devices)

If this checkbox is active, an HTTP proxy is used to send HTTP requests from the DLS to IP Devices.

Autocorrection of Device-IP

Automatic correction of the devices' IP address with the request address (only if HTTP-Proxy is enabled). In case an HTTP proxy is used, this option is deactivated at first in order to avoid that the IP address of the devices is replaced with the IP address of the HTTP proxy. It is recommended not to activate this switch.

HTTP-Proxy Host

IP address or DNS name of the HTTP proxy to be used for sending HTTP requests from the DLS to the IP Devices.

HTTP-Proxy Port

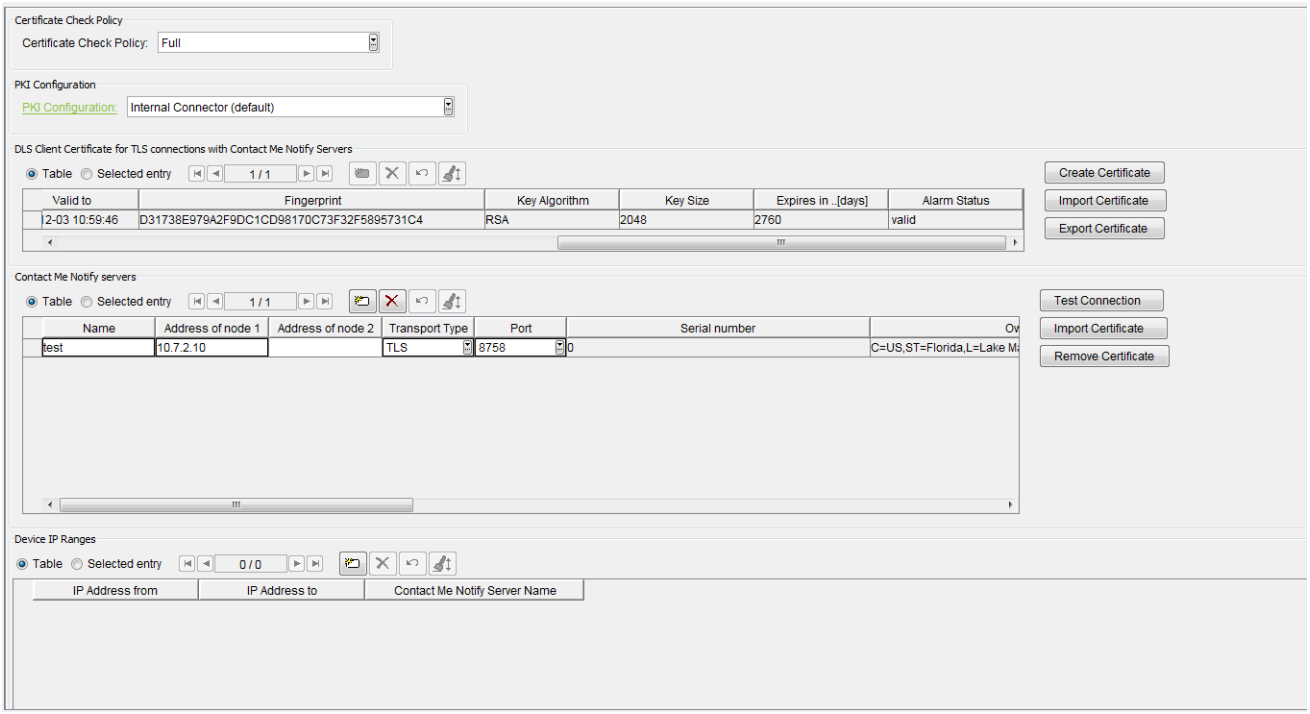
Port of the HTTP proxy used to send HTTP requests from the DLS to IP Devices.

6.9.4 "Contact Me Notify" Tab

Call: Main Menu > Administration > Workpoint Interface Configuration > "Contact Me Notify" Tab

The settings made in this tab are necessary if the end devices can be reached by the DLS only via a Contact Me Notify mechanism.Contact Me Notify replaces the DLS Contact Me Proxy (DCMP) solution for the devices that are registered to an OpenScape Voice server. OSV provides the Contact Me Notify mechanism and serves as the intermediate node between the DLS and the device.

NOTE: It is highly recommended to deploy the V3R1 SW version (or higher) to all the devices before enabling the Contact Me Notify functionality.



Certificate Check Policy

Certificate Check Policy

Possible values :

- **None** (default)- no authentication of the remote entity performed

  The remote entity is not checked at all or any potential errors during the check are ignored

  This is the default value, since both Trusted and Full require administrative steps anyway by configuring the associated (root) CA certificate(s).

IMPORTANT: Even if the Security Check Policy is set to "none",a valid client Certificate generated from the same RootCa should still be uploaded.

- **Partial -** the certificate (including certificate chain) provided by the remote entity is checked.
  a) the chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates, which are preconfigured for that interface on the product
  b) all certificates in the chain are not expired (i.e. current date/time is within the certificate's given validity period)
  c) no certificate in the chain is revoked[1]
- **Full** - the certificate (including certificate chain provided by the remote entity is checked against the same criteria as in Trusted mode, plus :
  a) for correct end entity identity (according to settings in SubjectAlternativeName (SAN) and/or the common name (CN) in the Subject)
  b) for correct use of all critical extensions (e.g. Basic constraints, Key Usage, Extended Key Usage). If an extension is marked critical and is not recognized, the certificate must be rejected.
  c) for correct use of known extensions not marked as critical (e.g. Basic constraints, Key Usage, Extended Key Usage)

PKI Configuration

PKI Configuration

Client certificate can be issued by using a PKI infrastructure or by importing manually a certificate (by default a SEN ROOT signed client certificate is installed with the installation of DLS.

DLS Client Certificate for TLS connections with Contact Me Notify Servers

Serial Number

Serial number of the certificate (display only).

Owner

Owner of the certificate (display only).

1 Revocation checks are done using OCSP (Online Certificate Status Protocol) or based on CRL (Certificate Revocation Lists); Revocation checks are controlled via independent configuration items and apply to both Full and Trusted mode. See more details in the section below.

Issuer

Issuer of the certificate (display only).

Create Certificate

Create automatically a client certificate using the internal root CA of DLS.

Import Certificate

Import a PKCS #12 file that will be used by DLS as client certificate.

Export Certificate

Export the public certificate of the installed client certificate that has to be configured as trusted in OSV.

Contact Me Notify servers

Name

Name of the Contact Me Notify server (32 characters).

The name must be unique..

Address of node 1

IP address or FQDN of the admin interface of the first node.

The IP address must be unique.

Address of node 2

IP address or FQDN of the admin interface of the first node.

The IP address must be unique.

Transport Type

Specify the transport type.

Possible values:

- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

Port

Specify the SOAP server port.

Possible values (Transport Type :**TCP**)

- **8767**
- **8768**
- **8769** (default)
- **8770**

Possible values (Transport Type :**TLS**)

- **8757**
- **8758**
- **8759 (**default)
- **8760**

Serial Number

Serial number of the certificate.

Owner

Owner of the certificate.

Issuer

Issuer of the certificate.

Valid from:

Start of the validity for the certificate.

Valid to:

End of validity for the certificate.

Fingerprint

Test algorithm SHA-1 (160 bits/20 characters) of the certificate.

Key algorithm

Key algorithm of the certificate.

Key size

key size of the certificate.

Expires in...[days]

Certificate will expire in ... days of the certificate.

Alarm Status

Current alarm status of the certificate.

Possible values:

- **Valid**
- **Soon running out**
- **Expired**

Test Connection

Test the connection between DLS and the configured OSV servers.

A Test Connection dialog shall appear via which you will be allowed to select one Contact Me Notify server to test the connection. A simple *GetVersion* request will be sent as a connection test.

Import Certificate

Import a server certificate that will be used by DLS for the server authentication of the OSV during TLS handshake.

> ***NOTE:*** When DLS receives the server certificate from OSV, DLS must validate the server certificate that has been received against the server certificate that has been imported into DLS database as trusted.

Remove Certificate

Remove an installed certificate from a configured Contact Me Notify server. Note that if there is not installed certificate, this operation will fail because there is no installed certificate to remove.

> ***NOTE:*** If there is no installed certificate, the operation will fail.

Device IP Ranges

IP Address from:

Lowest value for the IP range (IPV4 or IPV6) associated with this location.

IP Address to:

Highest value for the IP range (IPV4 or IPV6) associated with this location.

> ***NOTE:*** Any IP devices within the IP ranges defined by **IP Address from** and **IP Address to** will be updated via the associated Contact Me Notify SIP server.

> ***NOTE:*** It shall be allowed to have both **DCMP** and **Contact Me Notify** enabled for the same IP ranges. In this case of overlap, DLS will make the decision of the method that should be used based on the received device type. In other words, for optiPoint or openStage HFA or openStage SIP devices with version lower than V3R1, it will not use the SIP NOTIFY method and make a fallback to **DCMP**. Otherwise, it will use the **Contact Me Notify**.

Contact Me Notify Server Name

The mnemonic name of a configured Contact me Notify server that will be used as intermediate node whenever a changed is made to an IP device within the configured IP range.

6.10 Automatic SPE Configuration

This area enables the automatical configuration of PKI based Signaling and Payload Encryption (SPE). This is especially useful when there is no client PKI.

The DLS supports the generation and deployment of CA Certificates (CA= Certificate Authority) for administered IP Devices (Gateways and end devices). When activating this CA Certificate for each administered gateway, a SPE certificate will be generated and deployed.

Via export and import, it is possible to migrate CA certificates from one DLS to another.

This area features the following components:

- General Data
- Possible Action Buttons
- "CA Administration" Tab
- "Issuer Administration" Tab
- "Settings" Tab

General Data



PKI Configuration

Select PKI configuration.

Possible Options:

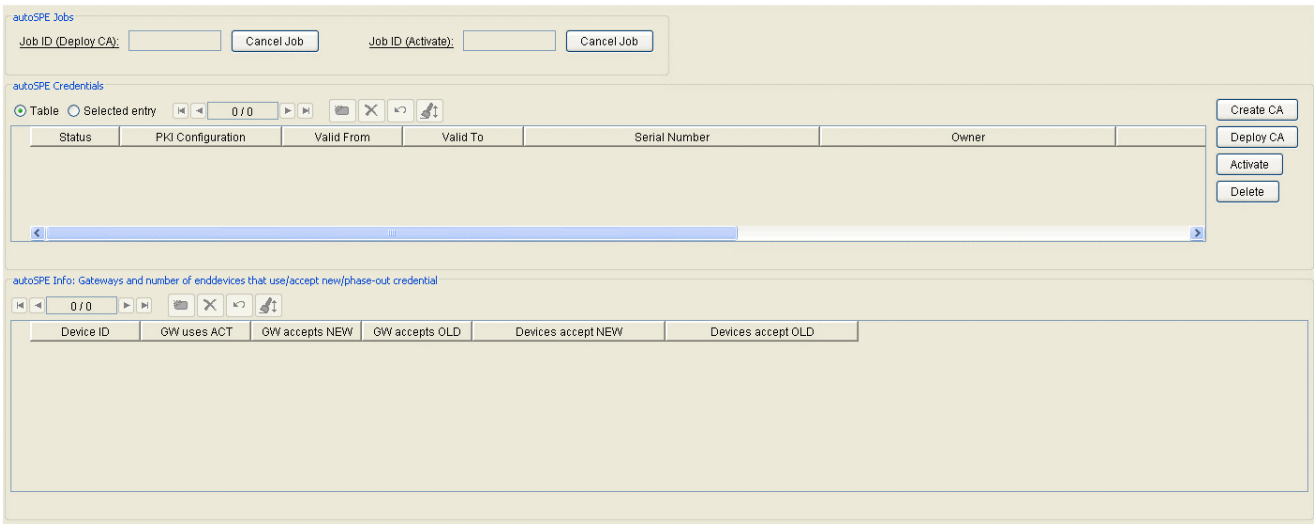
- **Internal Connector (default)**
- **Internal Root CA (default) SHA1**

  Internal Root CA (default) SHA1 s being generated with SHA-1 signature algorithm which is acceptable by HFA phones. The suffix SHA1 occurs in order to differentiate with the default CA with signature algorithm of SHA256.

NOTE: Please refer to Section 16.5.6, "Internal CA Configuration for AutoSPE" for further information on PKI configuration for use by HFA & Automatic SPE.

6.10.1 "CA Administration" Tab

Call: Main Menu > Administration > Automatic SPE Configuration > "CA Administration" Tab



autoSPE Jobs

Job ID (Deploy CA)

For the deployment of CAs, a job is started. A unique job ID is assigned to this job in order to identify it. Via this field, it is possible to jump to the job control (see Section 14.1, "Job Control") to control the status of the job.

Job ID (Activate)

For the activation of CAs, a job is started. A unique job ID is assigned to this job in order to identify it. Via this field, it is possible to jump to the job control (see Section 14.1, "Job Control") to control the status of the job.

Cancel Job

With this button, the particular job can be canceled.

autoSPE Credentials

Status

Displays the status of the credential.

Possible values:

- **created**

- **deployed**
- **activated**
- **phase-out**

PKI Configuration

PKI configuration.

Valid from

Start date of credential validity.

Valid to

Expiry date for new autoSPE credentials (possible maximum duration until 12/31/2037).

Serial number

Serial number for the CA certificate.

Owner

Owner of the credential.

Issuer

Issuer of the credential.

Key Algorithm

Key Algorithm.

Key Size

Key Size.

Fingerprint (SHA-1)

The fingerprint of CA certificate is unique and identifies the credential, also over disparate DLS instances. The fingerprint is also used as a part of the file name for export (see the **Export** button).

Create CA

Creates a new credential for SPE, i. e. first, a new CA certificate, and then, a certificate with this CA signature is created. the status of the new credential is "created".

Deploy CA

Deploys a new credential for SPE, that is, the CA certificate is distributed to the corresponding IP devices. The table is updated, and the status for the credential is changed to "deployed".

Activate

Activates a new credential for SPE, that is, the Ca certificate is distributed to the gateways. The table is update, and the status for the new credential is changed to "acitvated", while the status of the previously active credential is changed to "phase-out".

Delete

Deletes a credential that is no longer necessary, i. e. a credential in "created" or "deployed" status, or or the activated credential (in case only one credential exists) or the phase-out credential (in case more than one credential exist). After this, the table is updated.

autoSPE Info: Gateways and number of enddevices that use/accept new/phase-out credential

Device ID

Displays the device ID of the gateway.

GW uses ACT

Indicates whether the gateway uses the active credential.

Possible values:

- **yes**
- **no**

GW accepts NEW

Indicates whether the gateway accepts the new credential.

Possible values:

- **yes**
- **no**

GW accepts OLD

Indicates whether the gateway accepts the phased-out credential.

Possible values:

- **yes**
- **no**

Devices accept NEW

Shows the number of devices which accept the new credential, as well as the total number of devices connected to the gateway. Furthermore, the coverage in percent is displayed.
Example: 3/5 (=60%) implies that three of five devices connected to the gateway accept the new credential, which is commensurate with 60%.

Devices accept OLD

Shows the number of devices which accept the phased-out credential, as well as the total number of devices connected to the gateway. Furthermore, the coverage in percent is displayed.
Example: 3/5 (=60%) implies that three of five devices connected to the gateway accept the phase-out credential, which is commensurate with 60%.

6.10.2 "Issuer Administration" Tab

Call: Main Menu > Administration > Automatic SPE Configuration > "Issuer Administration" Tab



The data of the certificate issuer are displayed here.

NOTE: It is not possible to change the data of the certificate under "Automatic SPE Configuration" - Issuer Administration.

The user can only apply the default settings pre-defined in the DLS.

Automatic

E=

E-Mail address of the issuer.

Example: **hipath_security_office@unify.com**

CN=

Common Name of the issuer.

Example: **Unify Security Office**.

OU=

Organizational Unit of the issuer.

Example: **Unify Systems**.

O=

Organization of the issuer.

Example: **Unify GmbH & Co. KG**.

L=

Location of the issuer.

Example: **München**.

C=

Country of the issuer.

Example: **DE**.

Valid to

Maximum validity for new autoSPE credentials.

6.10.3 "Settings" Tab

Call: Main Menu > Administration > Automatic SPE Configuration > "Settings" Tab



Allow manual import of certificates besides autoSPE

If the check box is active, a certificate can be imported manually, f. e. if the deployment via autoSPE has failed.

Allow manual removal of certificates besides autoSPE

If the check box is active, a certificate can be removed manually.

NOTE: Certificates that have been removed manually can only be re-imported manually.

Overwrite customer imports with auto SPE credentials

autoSPE handles up to 2 server-side CA certificates (index 0 and 1). However, up to 16 server-side CA certificates (index 0 to 15) can be imported by the user. If autoSPE is activated, it overwrites the indices 0 and 1 with its own CA certificates.

If the check box is active, the indices 2 to 15 are removed during this process. Otherwise, only the indices 0 and 1 are overwritten with autoSPE certificates, while the remaining indices are left untouched.

Delete existing autoSPE credentials during autoSPE import

All existing credentials will be deleted before an import.

Apply autoSPE certificates to new gateways automatically

If activated, new gateways will be provided automatically with existing autoSPE Certificates. Otherwise, gateways will be supported with certificates via **Call: Main Menu > Call: Main Menu >** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **Import Certificate**.

Apply autoSPE certificates to new enddevices automatically

If activated, new enddevices will be provided automatically with existing autoSPE certificates. Otherwise, enddevices will be supported with certificates via **Call: Main Menu > Call: Main Menu >** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **Import Certificate**.

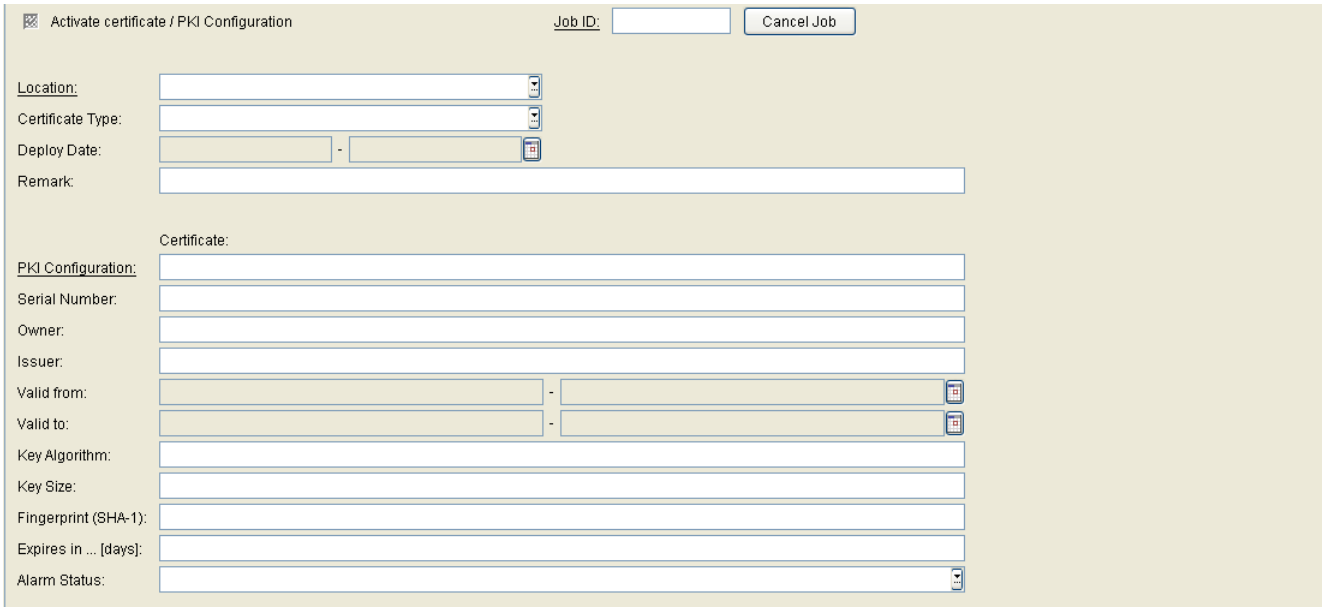
6.11 Automatic Certificate Deployment

Call: Main Menu > Administration > Automatic Certificate Deployment

This area provides the possibility to set up a certificate deployment schedule by assigning certificates to existing locations, i.e. a set of IP phones, and run scheduled jobs to deploy these certificates automatically.

It is possible to prevent autodeployment for an IP phone by enabling the **Automatic Certificate Deployment disabled** checkbox in **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration**.

NOTE: To remove the certificates from all IP phones of a location, deploy an empty certificate.



Activate certificate / PKI Configuration

The certificate will be activated for automatic certificate deployment. After activation, the Jobs corresponding to the devices will be generated. Activated entries cannot be changed.

A certificate deployment task will be stopped/deactivated by unsetting this check box. The jobs already generated but not executed (state: active or running) will not be cancelled. To cancel all jobs belonging to a task, press the **Cancel Job** button. The certificate relating to this task will no longer be deployed to newly registered IP Devices.

Job ID:

For the activation of certificates, a job is started. A unique job ID is assigned to this job in order to identify it. Via this field, it is possible to jump to the job control (see Section 14.1, "Job Control") to control the status of the job.

Cancel Job

With this button, all jobs belonging to this certificate deployment task with active or running status will be cancelled.

Location:

Location where the certificate deployment will be executed. Locations can be assigned as described under Section 6.3.2, "Location".

Certificate Type:

Type of certificate.

Possible options:

- **RADIUS Server CA Certificate 1**
- **RADIUS Server CA Certificate 2**
- **Phone Certificate**
- **WBM Server Certificate (IP Phone)**
- **WBM Server Certificate (IP Gateway: Index 0)**

Deploy Date:

Date when certificate deployment will be started.

Remark:

Remark (free text).

Certificate:

The following certificate parameters are displayed only.

PKI Configuration

PKI configuration.

Serial Number:

Serial number of the certificate.

Owner:

Owner of the certificate.

Issuer:

Issuer of the certificate.

Valid from:

The certificate will be valid from this point in time.

Valid to:

The certificate will be valid until this point in time.

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in [days]:

The certificate expires in ... days.

Alarm Status:

Current alarm status of imported certificate.

Possible values:

- **valid**
- **soon running out**
- **expired**

Possible Action Buttons

Discard

Discards any unsaved changes.

Save

Saves the data entered/modified.

New

Creates a new entry, i.e. a new certificate deployment task.

Delete

Deletes an entry.

Import Certificate

Import either a specific certificate to be automatically deployed to devices or a PKI configuration that will be used to automatically request certificates for all devices.

NOTE: If you don’t proceed with the Import Certificate button,then an empty certificate shall be deployed thus all respective certificates shall be removed

Refresh

Refreshes the content of the relevant page.

6.12 Automatic Archiving

Call: Main Menu > Administration > Automatic Archiving

This feature enables the user to archive the data of selected IP devices in a time-controlled manner. The archived data will be stored in a .zip-file. If the file is not present, it will be created during the 1st archiving of data; if it is already present, the archive data will be added to this existing .zip-archive. For each IP Device that is to be archived, a proper file will be allocated within the .zip archive.

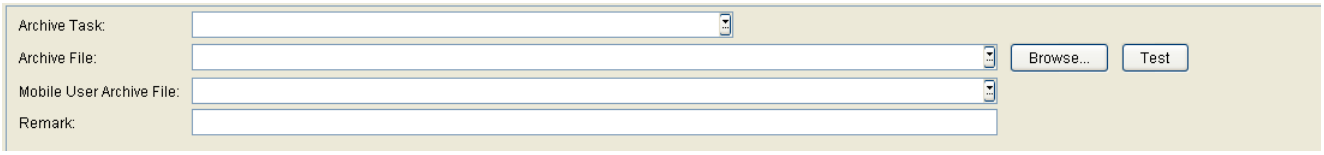
Each new archive entry overwrites an already existing entry for the same IP Device without notification. History data (backups of an already existing file of the .zip archive) will be kept where the maximum number of kept history data can be specified by setting **Maximum Number of Backup Archive Files** within the "Settings" Tab.

The archived data can be retrieved via the screen **Administration** > **Automatic Archiving** > **Action 'Load IP Device from Archive'**.

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "IP Devices to archive" Tab
- "Mobile Users to archive" Tab
- "Protocol" Tab

General Data



Archive Task

Name of the archive task.

Archive File

Filename and directory path for the archive file on the DLS Server. If the file is not present, it will be created during the first archiving of data; if it is already present, the archive data will be added to the existing .zip-archive.

Mobile User Archive file

Filename and directory path for the archive file on the DLS Server. The file name will be derived from **Archive File** and cannot be changed.

Remark

Remark on archive task.

Browse...

Select excisting archive path. Path name and filename will be written to the archive file. Only directories can be searched, not particular files.

Test

Test if the file is accessible.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the Search view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, see Section 15.1,

"First Steps: Changing IP Device Parameters".

Discard

The modifications carried out in the mask are discarded.

Export File

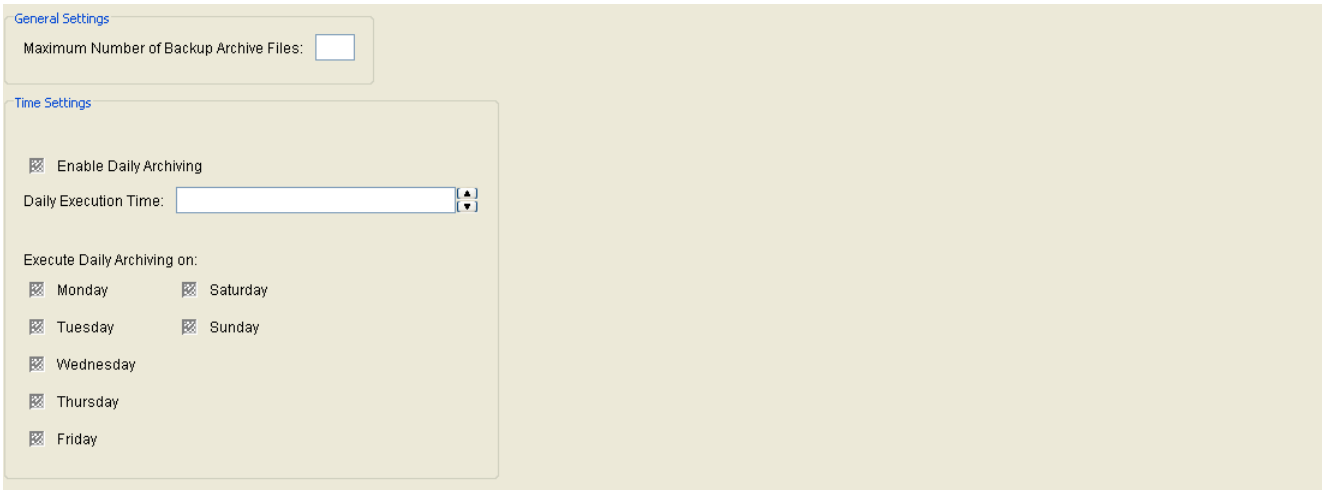
The inventory data are exported into a csv formatted file.

Refresh

Refreshes the window contents from the database.

6.12.1 "Settings" Tab

Call: Main Menu > Administration > Automatic Archiving > "Settings" Tab



General Settings

Maximum Number of Backup Archive Files

Contains the number of backup files to be created for file history, if the original archive file is overwritten.

Time Settings

Enable daily Archiving

Activates daily archiving of IP Devices .

Daily Execution Time

Time of day at which the archiving is started.

NOTE: Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

Execute Daily Archiving on:

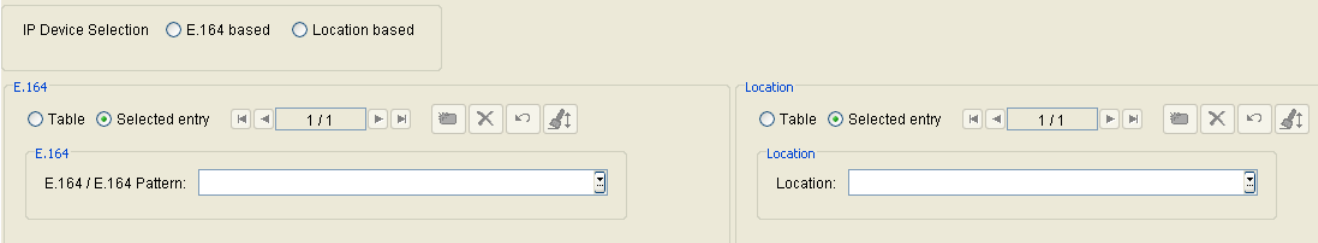
Restricts Archiving to specific days of the week.

Archive now

Starts archiving immediately without any regards to settings for automatic archive. The archive will be saved to the **Archive File** currently displayed.

6.12.2 "IP Devices to archive" Tab

Call: Main Menu > Administration > Automatic Archiving > "IP Devices to archive" Tab



IP Device Selection

E.164 based

Selection of IP Devices to be archived by E.164 number.

Location based

Selection of IP Devices to archive by location.

E.164

E.164 /E.164 Pattern

Entire E.164 number or a range of E.164 numbers partly qualified with '*', e.g. 31* (= all E.164 numbers, starting with 31...).

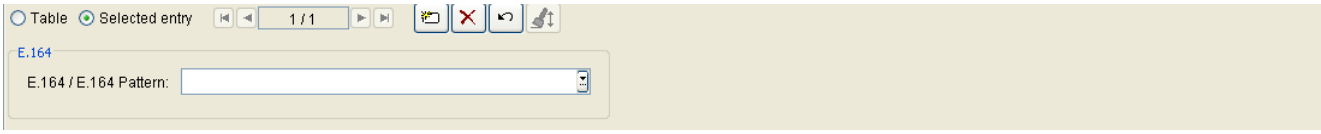
Location

Location

Select a defined location. ’Default Location’ cannot be selected.

6.12.3 "Mobile Users to archive" Tab

Call: Main Menu > Administration > Automatic Archiving > "Mobile Users to archive" Tab



E.164

E.164 / E.164 Pattern:

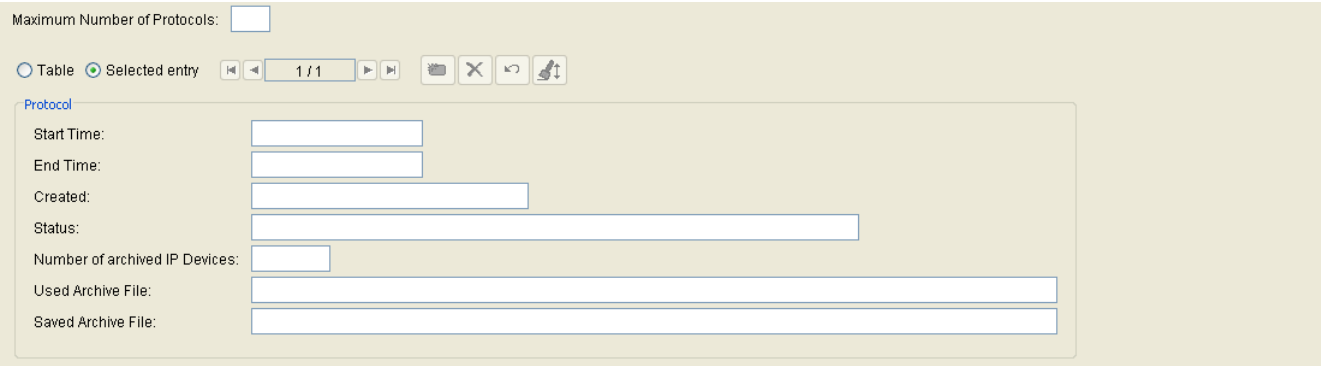
A complete E.164 number or a range of numbers partly qualified with '*' can be entered here.

Example: **31*** = all E.164 numbers that begin with 31.

NOTE: In the case of mobile users, Auto-archiving is enabled and achieved, regardless of their logon/logoff status.

6.12.4 "Protocol" Tab

Call: Main Menu > Administration > Automatic Archiving > "Protocol" Tab



Protocol

Maximum Number of Protocols:

Each protocol entry can be deleted manually or will be deleted automatically according to the number entered here.

Start Time

Start Time of archiving.

End Time

End Time of archiving.

Created

Displays whether it is an automatic or a manual archive task.

- **Manual**
- **Timer triggered**

Status

Status of archiving.

Possible values:

- **Archive Task successful**
- **Archive Task failed**
- **Old Protocol entries automatically deleted**

Number of archived IP Devices

Number of archived IP Devices.

Used Archive File

Filename of the currently used archive file.

Saved Archive File

Filename of the latest saving of the archive file.

6.13 Automatic Upload Diagnosis- and Security Log Files

Call: Main Menu > Administration > Automatic Upload Diagnosis- and Security Log Files

This area enables the user to upload scheduled diagnosis- and security log files of selected IP Devices. The uploaded file will be stored on a network drive. The path is defined in **Main Menu** > **Administration** > **File Server** > **OpenStage Diagnosis Files** or **OpenStage Security Log Files**.

This area features the following components:

- General Data
- Possible Action Buttons
- "Protocol" Tab

General Data



Activate Upload of Diagnosis Files

When active, diagnosis files of selected IP Devices are uploaded.

Upload Interval for Diagnosis Files (min)

Determines the time between two upload jobs (in minutes).

Indicative Options (not restrictive):

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Default value: **60**

Activate Upload of Security Log Files

When active, security log files of selected IP Devices are uploaded.

Upload Interval for Security Log Files (min)

Determines the time interval between two upload jobs (in minutes).

Indicative Options (not restrictive):

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Default value: **60**

Possible Action Buttons

Depending on the selected view and DLS state, various possible action buttons are available.

Save

Saves all settings made.

Discard

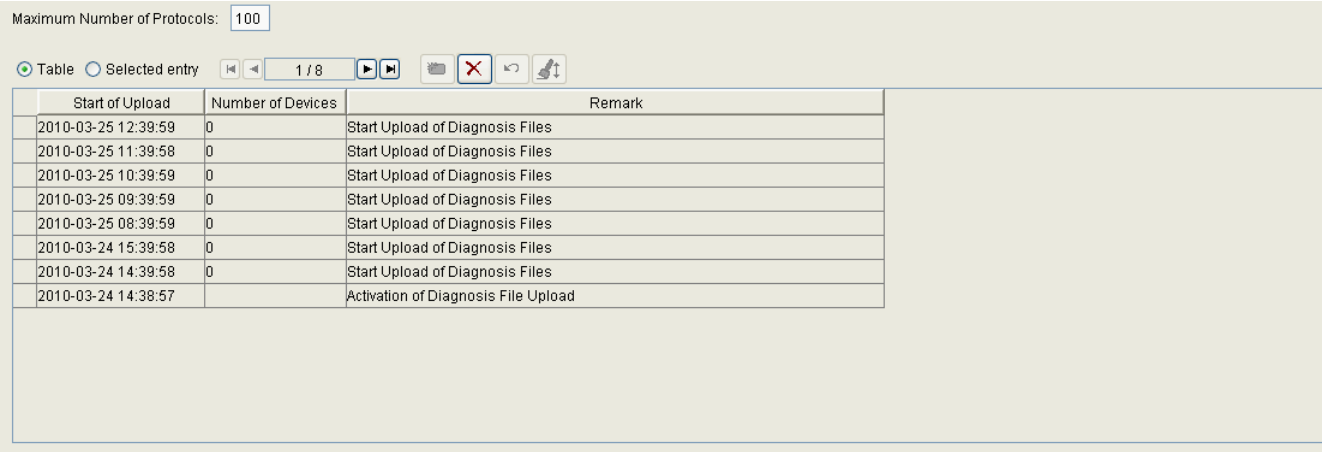
Discards any changes entered.

Refresh

Updates the window using the database.

6.13.1 "Protocol" Tab

Call: Main Menu > Administration > Automatic Upload Diagnosis- and Security Log Files > "Protocol" Tab



Maximum Number of Protocols:

Each protocol entry can be deleted manually or will be deleted automatically according to the number entered here.

Start of Upload

Displays the upload's starting time.

Number of Devices

Displays the number of handled IP Devices.

Remark

Remark on the upload.

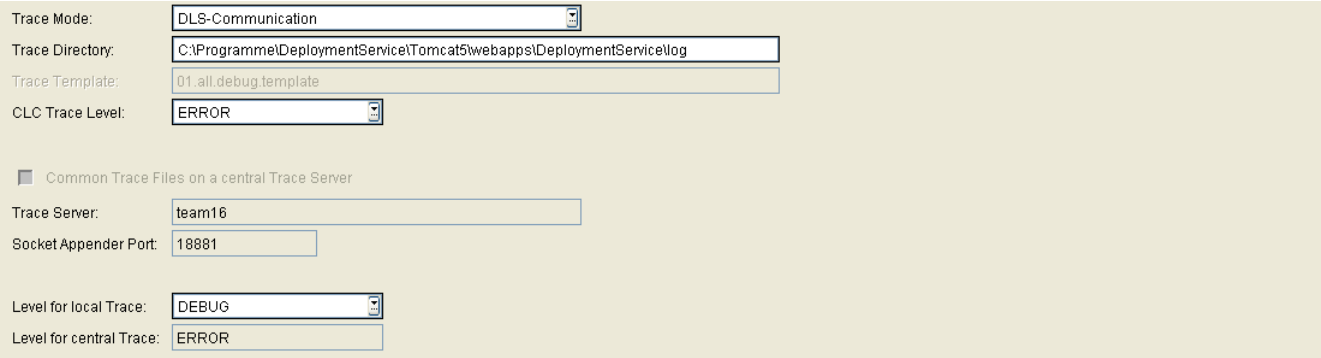
6.14 Trace Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "Additional Settings and Actions" Tab
- "Repeat filter" Tab
- "Message Filter" Tab
- "Filter test" Tab
- "OSVTM Configuration" Tab
- "Thread Monitoring" Tab

General Data

Call: Main Menu > Administration > Trace Configuration



You can use this menu item to configure trace operations. The settings are stored in the DLS database. A timer monitors if there are any new entries in the database. If so, the trace is modified accordingly; where applicable, changes are also transferred to the other servers in a cluster.

NOTE: The changes take effect after approximately two minutes.

NOTE: Individual settings can restrict the options available in the menu **Administration** > **Display Logging Data**.

For information on general interface operation, see Section 5.4.2, "Work Area".

Trace Mode

Option for selecting the trace mode.

Possible values:

- **Off**
  No special traces are performed. All error messages will be written to a default tracefile. This is the default setting after installation.
- **DLS Server**
  The trace is performed in the DLS server with the assigned **Level for local Trace**.
- **DLS Communication**
  Communication between IP devices and DLS server is traced with the assigned **Level for local Trace**. Additionally all error messages will be written to the default tracefile.
- **Log4j Template**
  The trace is performed with the predefined trace template selected under **Trace Template**.

Trace Directory

Directory in which the trace files are stored.

Trace Template

Option for selecting predefined trace settings. The trace templates are stored in the file directory `<drive>:\Program Files\DeploymentService\Tomcat\webapps\DeploymentService\log\templates`.

The settings in the templates are only effective if the **Trace Mode** "Log4j Template" is set.

Possible values:

- **01.all.debug.template**
  Log all DLS activities with DEBUG logging level.

  NOTE: In the case where a SOAP based element manager (H8K, H8K Ass, H4K(WebService)) or a dlsAPI client (H8K Assistant, OSILA) needs to send the payload encryption, they just have to activate the '01.all.debug.template'

- **02.all.info.template**
  Log all DLS activities with INFO logging level.
- **03.default.template**
  Default setting. Log all DLS activities with ERROR logging level.
- **04.gateway.template**
  Log all gateway activities with DEBUG logging level.
- **05.gateway.wpcomm.details.template**
  Log all gateway activities including communication between workpoint and DLS with DEBUG logging level.
- **06.gateway.wpcomm.info.template**
  Log all gateway activities including communication between workpoint and DLS with DEBUG logging level.
- **07.keyexchange.template**
  Log all gateway and key distribution activities with DEBUG logging level.
- **08.keyexchange.wpcomm.details.template**
  Log all gateway and key distribution activities including communication between workpoint and DLS with DEBUG logging level.
- **09.keyexchange.wpcomm.info.template**
  Log all gateway and key distribution activities including communication between workpoint with DEBUG logging level.
- **10.wpcomm.details.template**
  Log communication between workpoint and DLS with DEBUG logging level.
- **11.wpcomm.short.template**
  Log communication between workpoint and DLS with INFO logging level.

- **12.wpscan.wpcomm.details.template**
  Log all workpoint-based scan activities including communication between workpoint and DLS with DEBUG logging level.
- **13.wpscan.wpcomm.short.template**
  Log all workpoint-based scan activities including communication between workpoint and DLS with INFO logging level.
- **14.dlsapi.template**
  Log all DLS API methods with DEBUG logging level.
- **15.auth.debug.template**
  Log all authentication activities including communication between workpoint and DLS with DEBUG logging level.
- **16.nodb.debug.template**
  Log all DLS activities with the exception of database activities including communication between workpoint and DLS with DEBUG logging level.
- **17.pp.em.debug.template**
  Log all Plug&Play and element manager related activities with DEBUG logging level.
- **18.pki.details.template**
  Log all PKI activities with DEBUG logging level.

CLC Trace Level

Trace level for the communication with the Central License Agent (CLA).

Possible values:

- **DEBUG**
  Comprehensive trace of processes.
- **INFO**
  Selected process information.
- **WARN**
  Displays potential problems.
- **ERROR**
  Displays problems that do not cause the deployment service to fail.

Common Trace Files on a central Trace Server

Traces of all nodes in a cluster are written to a file on a central server. The files `dlswpcommunication.*.txt`, `dlslog.*.txt`, and `dlserror.*.txt` are created.

Trace Server

Server where the common trace files are stored.

Socket Appender Port

Number of ports used for sending the common trace data to a node within the cluster.
Default value: **18881**.

Level for local Trace

Trace level setting for local traces in the DLS server. The hierarchy of trace levels is DEBUG < INFO < WARN < ERROR < FATAL, that is, if DEBUG is set, all other levels are also logged. If the diagnostic settings are controlled with a template, the value set there for this parameter has precedence.

Possible values:

- **DEBUG**
  Comprehensive trace of processes.
- **INFO**
  Selected process information.
- **WARN**
  Displays potential problems.
- **ERROR**
  Displays problems that do not cause the deployment service to fail.
- **FATAL**
  Displays problems that cause the deployment service to fail.

Level for central Trace

Trace level for common traces on a trace server within the cluster. If the diagnostic settings are controlled with a template, the value set there for this parameter has precedence.

Possible values:

- **INFO**
  Selected process information.
- **WARN**
  Displays potential problems.
- **ERROR**
  Displays problems that do not cause the deployment service to fail.

- **FATAL**
  Displays problems that cause the deployment service to fail.

Possible Action Buttons

The range of action buttons available depends on the DLS status.

Save

Saves any unsaved changes.

Discard

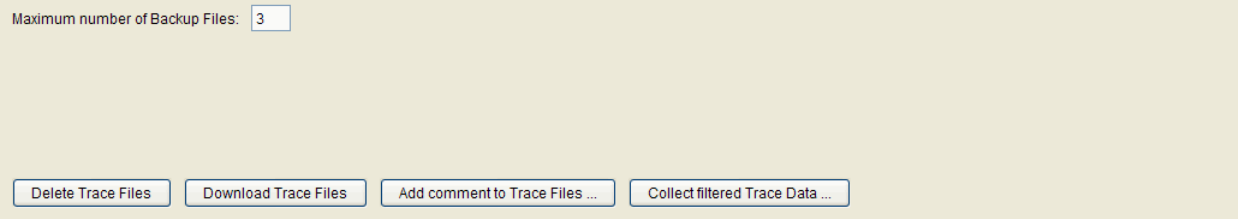
Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

6.14.1 "Additional Settings and Actions" Tab

Call: Main Menu > Administration > Trace Configuration > "Additional Settings and Actions" Tab



Maximum Number of Backup Files

Maximum number of backups per trace files.

Value range: **1** - **999**

Delete Trace Files

Delete all trace files.

Download Trace Files

Download all trace files in a .zip-file to a local path.

NOTE: If you use Microsoft Internet Explorer, **Automatic prompting for file downloads** has to be enabled. To achieve this, go to **Tools** > **Internet Options...** > **Tabsheet "Security"**. Here, select the web content zone the DLS server address belongs to and press **Custom Level**. In the **Security Settings** popup window, under **Downloads**, you can find the option mentioned above.

Add comment to Trace Files ...

Insert a comment in all trace files.

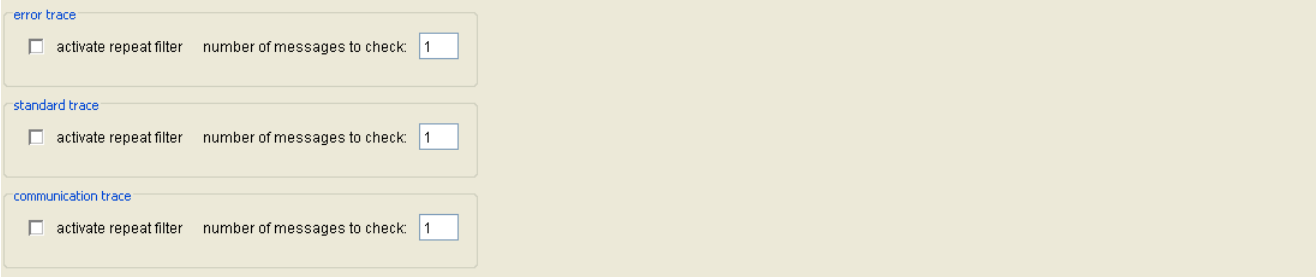
Collect filtered Trace Data ...

This function filters trace files already generated trace files (`dlslog.txt` and `dlsWpCommunication.txt`) according to certain filter criteria: E.164 numbers, IP addresses, or device IDs. A combination of criteria is not possible. These filter criteria are requested in a popup window. Data records which match a filter criterion are stored in an particular trace file. By clicking **Download Trace Files**, the files created are displayed. The generated files receive the following names: `<filter criterion>_FILTERED_dlslog.txt` and `<filter criterion>_FILTERED_dlsWpCommunication.txt`. With **Delete Trace Files**, these files can be deleted.

6.14.2 "Repeat filter" Tab

NOTE: By applying this function, messages which are required for analysis might possibly be lost. Therefore, it should be used with care, preferably only by request of the DLS support team.

Call: Main Menu > Administration > Trace Configuration > "Repeat filter" Tab



Error trace

Activate repeat filter

When activated, repetitions of messages in the error trace are filtered out. The context range, within which repetitions are searched, is specified in the **Number of messages to check** parameter.

Number of messages to check

Size of a block of sequenced messages in the error trace, within which repetitions shall be filtered out.

Standard trace

Activate repeat filter

When activated, repetitions of messages in the standard trace are filtered out. The context range, within which repetitions are searched, is specified in the **Number of messages to check** parameter.

Number of messages to check

Size of a block of sequenced messages in the standard trace, within which repetitions shall be filtered out.

Communication trace

Activate repeat filter

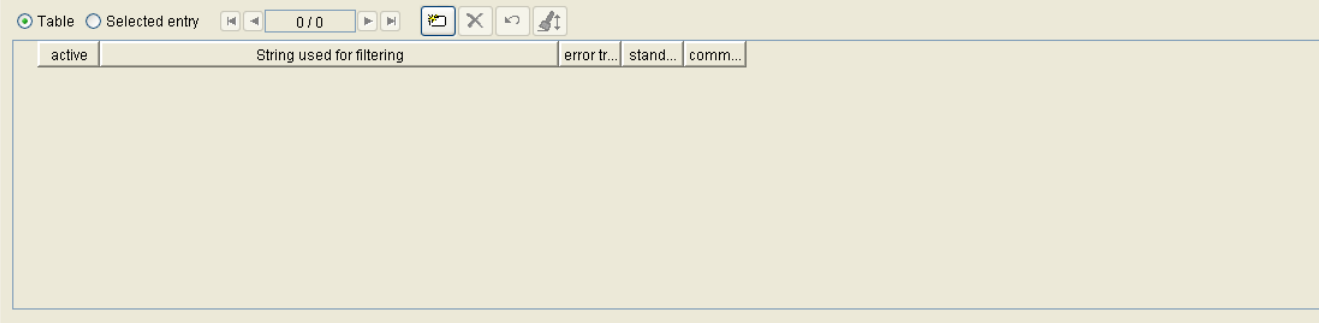
When activated, repetitions of messages in the communication trace are filtered out. The context range, within which repetitions are searched, is specified in the **Number of messages to check** parameter.

Number of messages to check

Size of a block of sequenced messages in the communication trace, within which repetitions shall be filtered out.

6.14.3 "Message Filter" Tab

Call: Main Menu > Administration > Trace Configuration > "Message Filter" Tab



active

Filter is switch off and on.

String used for filtering

Filter according to entered string.

Error trace

If active, this string is valid for error trace filtering.

Standard trace

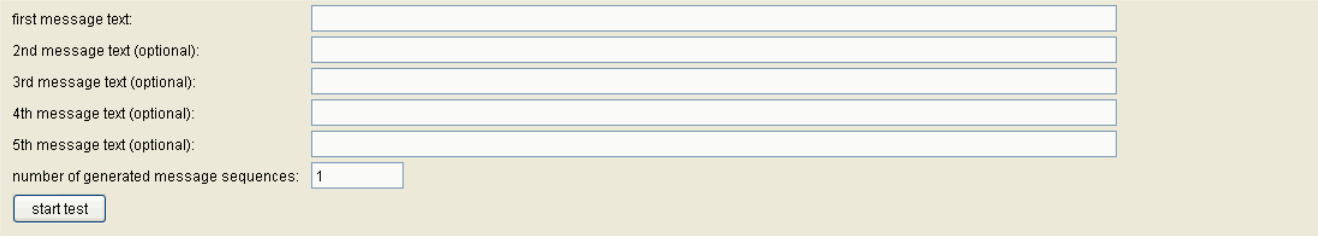
If active, this string is valid for standard trace filtering.

Communication trace

If active, this string is valid for communcation trace filtering.

6.14.4 "Filter test" Tab

Call: Main Menu > Administration > Trace Configuration > "Filter test" Tab



1st message text

String as test message for testing the configured filters.

2nd message text (optional)

Additional string for testing the configured filters; appears as a separate message.

3rd message text (optional)

Additional string for testing the configured filters; appears as a separate message.

4th message text (optional)

Additional string for testing the configured filters; appears as a separate message.

5th message text (optional)

Additional string for testing the configured filters; appears as a separate message.

Number of generated message sequences

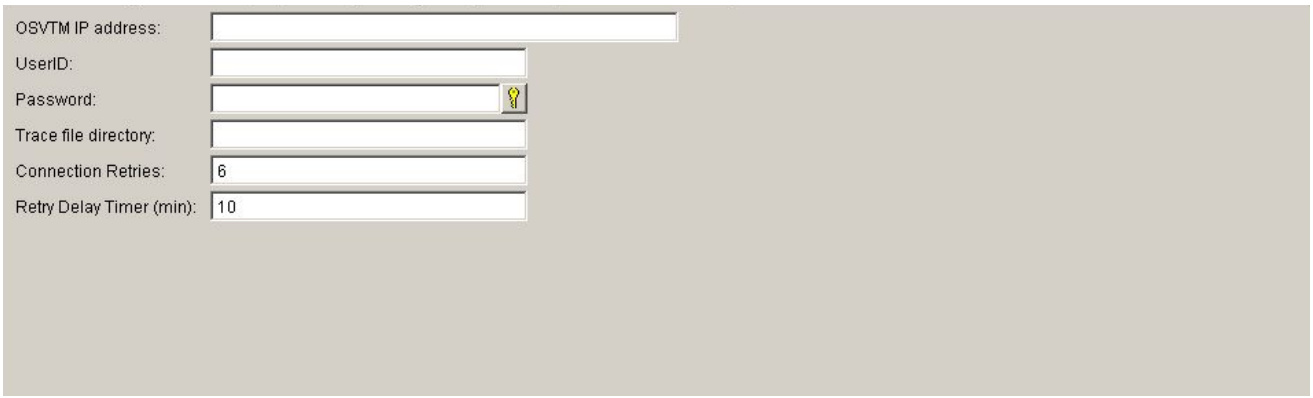
Defines how often the defined test messages shall be generated.

Start Test

The test messages are generated and filtered. The results appear in the traces.

6.14.5 "OSVTM Configuration" Tab

Call: Main Menu > Administration > Trace Configuration > "OSVTM Configuration" Tab



IMPORTANT: OSVTM Configuration is intended to promote phone diagnostics and not DLS-relevant logs.DLS do not forward all phone traces to OSVM but only the diagnostic traces. So if one should enable a diagnostic call then those will be sent to the OSVTM.

OSVTM IP address

Specification of the OSVTM IP address.

User ID

User ID for OSVTM file transfer.

Password

Password for OSVTM file transfer.

Trace file directory

Trace file directory on OSVTM to send trace files.

Connection Retries

If the file transfer fails, the DLS stored trace file is kept for at least a number of Connection Retries.

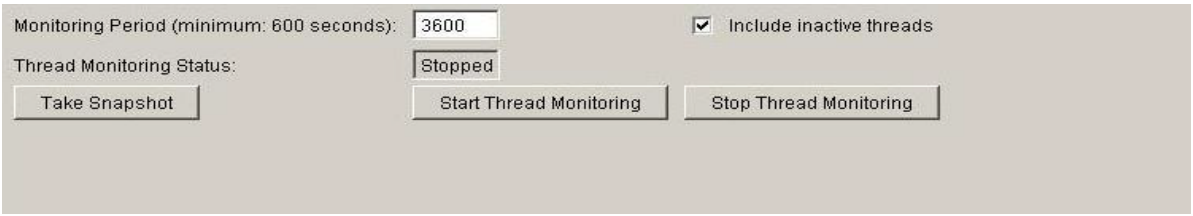
Default value is set to 6.

Retry Delay Timer (min)

Periodical attempts to resend the file.Default value is set to 10 (The file is resent every 10 minutes).

6.14.6 "Thread Monitoring" Tab

Call: Main Menu > Administration > Trace Configuration > "Thread Monitoring" Tab



NOTE: In order to enable Thread Monitoring, you must first set **Trace Mode** to **Log4j Template**. Please refer to Section 6.14, "Trace Configuration".

Monitoring Period (minimum: 600 seconds)

The time period interval in which thread monitoring takes place.

Default value is set to 3600 sec.

Thread Monitoring Status

Include Inactive Threads

Checkbox is active if inactive threads are included.

Take Snapshot

Start Thread Monitoring

Stop Thread Monitoring

6.15 Server Licenses

This area features the following components:

- General Data
- Possible Action Buttons
- "License state" Tab

General Data

Call: Main Menu > Administration > Server Licenses



Licenseagent

IP address or host name of license agent (CLA).

Port

Port number for access to the license server.

License Management

URL of the license server. Press the adjacent **License Management** action button to open the License Management Web interface in a separate window.

Possible Action Buttons

Save

Saves the field contents to the database.

Discard

Discards any changes entered.

Refresh

Updates the window using the database.

Read Licenses

Requests available licenses from license agent.

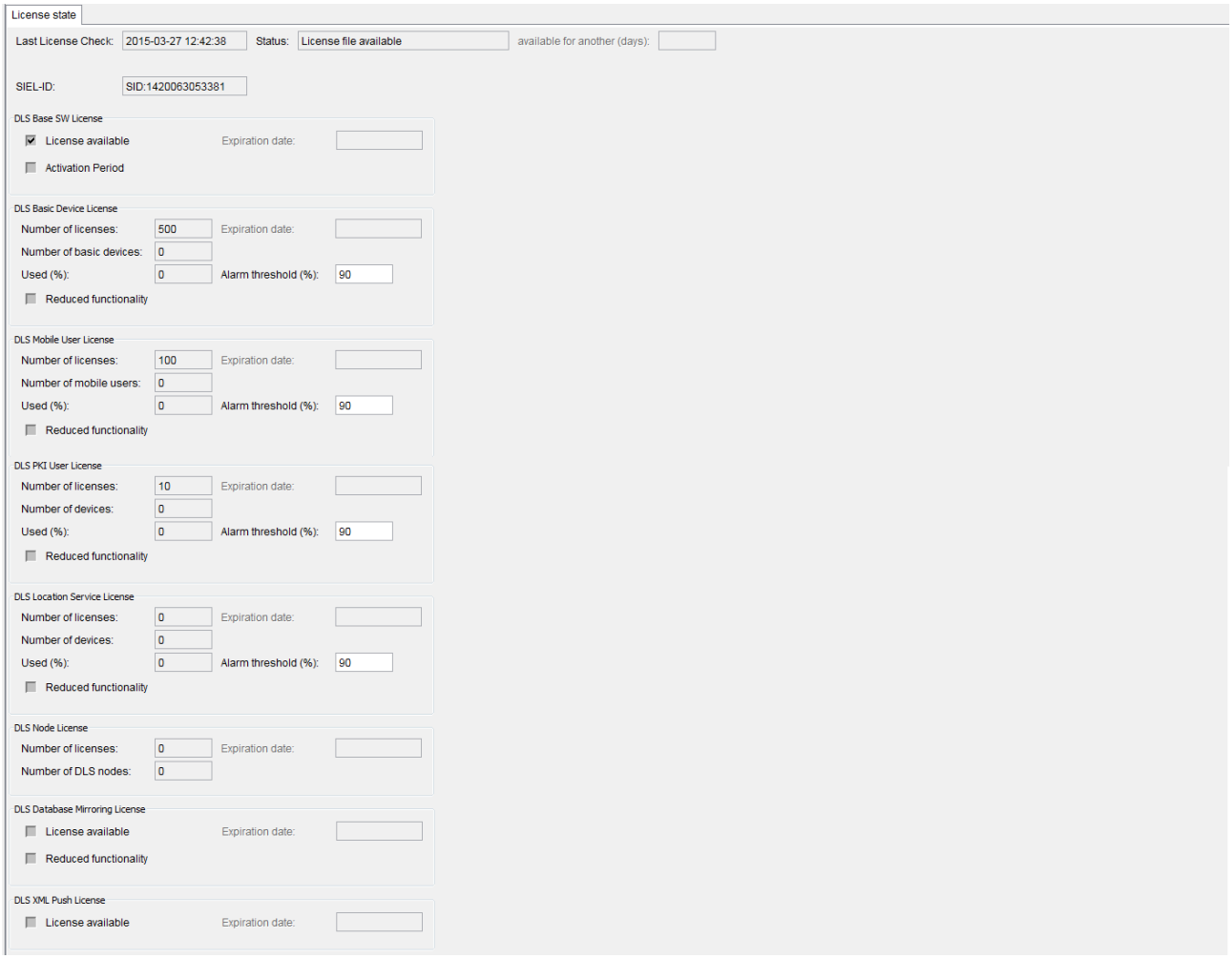
NOTE: Once you install a valid DLS license file at **LinuxCLM** tool, the licenses are not found straightaway from LinuxDLS after you set the corresponding License Agent IP,since DLS :

-(a) periodically checks for license changes (every 4 hours)
-(b) checks license changes when the DLS service starts (you may restart the Deployment Support service manualy from CMP via Dashboard menu)

6.15.1 "License state" Tab

Call: Main Menu > Administration > Server Licenses > "License state" Tab

The current status of various licenses is displayed here.



Last License Check

Date and time of the last license scan at the license agent are displayed.

Status:

Status of the connection to the CLA.

Possible Options:

- **License file available**

- **Activation Period - no license file available**
- **Failover Period - CLA not reachable**

available for another (days)

Number of days the DLS is to be used when CLA is not reachable.

SIEL-ID

Identifier for the Standardized Integrated Equipment Life Cycle

DLS Base SW License

License available

Checkbox is active if a Base SW License is part of the License file.

Expiration date

Date of license expiration. After this date no further DLS logon will be possible. Please contact your license administrator.

Activation Period

If checkbox is active, Base SW and V10 Basic Device Licenses are granted, although they are not part of your licenses. Please, order an upgrade for your license file.

DLS Basic Device License

> ***NOTE:*** In case multi tenancy is installed, configuration of the number of available Basic Device Licenses per tenant has to be done in the tenants screen, as described in Section 6.3.1, "Tenants".

Number of licenses:

Indicates the number of basic devices that can be configured with the current license.

Expiration date

An expiration date is displayed when working with a demo license. A license awarded by the CLA is not limited in time.

Registration of IP Devices is not possible any more after this date. Please contact your license administrator.

Number of basic devices:

Indicates the number of basic devices licenses already in use for mobile users.

Used (%)

Indicates the percentage of licenses already in use.

Alarm threshold (%)

Specify the percentage of used licenses that should generate a license alarm.

Reduced functionality

This check box is automatically selected if the number of licenses has been exceeded. The expiration date is set, and after exceeding the registration of IP Devices is blocked until the surplus IP Devices have been deleted by the administrator.

Please contact your license administrator.

DLS Mobile User License

Number of licenses

Indicates the number of mobile users that can be configured with the current license.

Expiration date

An expiration date is displayed when working with a demo license (activation period). A license awarded by the CLA (license agent) is not limited in time.

No more DLS administration is possible after this date. Please contact your license administrator.

Number of mobile users

Indicates the number of mobile user licenses already in use for mobile users.

Used (%)

Indicates the percentage of licenses already in use.

Alarm threshold (%)

Specify the used-license percentage that should generate a license alarm.

Reduced functionality

This check box is automatically selected if the number of licenses has been exceeded. In this case, the only option available is to delete mobile users.

Please contact your license administrator.

DLS PKI User License

> ***NOTE:*** In case multi tenancy is installed, configuration of the number of available Basic Device Licenses per tenant has to be done in the tenants screen, as described in Section 6.3.1, "Tenants".

Number of licenses:

Indicates the number of IP Devices supplied by PKI service that can be configured with the current license.

Expiration date

An expiration date is displayed when working with a demo license. A license awarded by the CLA (license agent) is not limited in time.

After this date, PKI support is not possible any more. Please contact your license administrator.

Number of devices

Indicates the number of IP Devices supplied by PKI service licenses already in use for IP Devices.

Used (%)

Indicates the number of licenses already in use as a percentage.

Alarm threshold (%)

Specify the used-license percentage that should generate a license alarm.

Reduced functionality

This check box is automatically selected when the number of licenses has been exceeded. After activation period expiry, the PKI service for IP Devices is blocked. Please contact your license administrator.

DLS Location Service License

> ***NOTE:*** This license is necessary to use the function 'Open Communications Solution for Location and Identity Assurance' (OCS LIA).

Number of Licenses

Indicates number of licenses for the Location Service (IP Infrastructure).

Number of devices

Number of IP Devices, supplied with IP Infrastructure data by means of Location Service.

Used (%)

Percentage of used Location Service Licenses.

Alarm threshold (%)

Specifies at which percentage of used licenses an alarm shall be generated.

Expiration date

An expiration date is displayed when working with a demo license (activation period). This is the case, for example, when the CLA (license agent) is not or no longer available. A license awarded by the CLA is not limited in time.

After this date IP Devices will not be supplied with IP Infrastructure data, except emergency Call, by means of Location Service. Please contact you license administrator.

Reduced functionality

This check box is automatically selected if the number of licenses has exceeded. In this case, the only option available is to delete IP Devices.

Please contact your license administrator

DLS Node License

Number of licenses

Indicates the number of DLS Node licenses available in License Agent.

> ***NOTE:*** These licenses are those available in CLA (loaded and activated) not these that DLS requires and uses.

Number of DLS nodes

Indicates the number of additional active DLS Nodes in a cluster. With Single-Node mode, 0 is displayed here. This number indicates the node licenses required.
For a n-node Multi-Node DLS, n-1 node licenses are required.

Expiration date

An expiration date is displayed when working with a demo license (activation period). A license awarded by the CLA (license agent) is not limited in time.

After this date, DLS operation in cluster mode will no longer be possible. Please contact your license administrator.

DLS Database Mirroring License

License available

License for Database Mirroring available

Expiration date

An expiration date is displayed when working with a demo license (activation period). A license awarded by the CLA (license agent) is not limited in time.

After this date, database mirroring will no longer take place. Please contact your license administrator.

Reduced functionality

This check box is automatically selected if the number of licenses has been exceeded. In this case, no database mirroring will be performed.

Please contact your license administrator

DLS XML Push License

> ***IMPORTANT:*** For disabling the **XML Push** feature, please refer to Section 16.19, "Deactivation of XML Push feature on Linux DLS"

License available

XML Push can only be used with a valid license.

Expiration date

An expiration date is displayed when working with a demo license (activation period). A license awarded by the CLA (license agent) is not limited in time.

After this date, XML Push will no longer be available. Please contact you license administrator.

7 IP Devices

Call: Main Menu > Call: Main Menu >

This menu item consists of the following areas:

- IP Phone Configuration
- IP Client Configuration
- IP Gateway Configuration
- IP Device Interaction
- IP Device Management

Use this area to display and change the configuration data of IP devices.

NOTE: If changes are made in data records that have been generated using templates, these changes are not automatically applied to the templates.
These changes must be manually saved to the template (Section 15.7, "Editing Templates").

NOTE: You can enter parameters for both SIP and HFA for every IP client in the **IP Client Configuration** area.

NOTE: An IP device can only be configured at the DLS after its successful registration. For registration, the IP device must be familiar with the relevant DLS address. Registration at the DLS is achieved by:
- reading out IP device data via the DLS, see Section 7.5.6, "Scan IP Devices" and by
- plugging the LAN connector or power supply into the IP device.

7.1 IP Phone Configuration

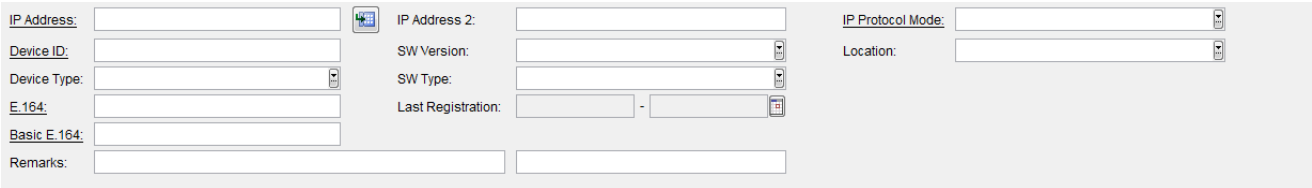
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration

This menu consists of the following submenus:

- Gateway/Server
- IP Routing
- Ports
- Features
- Quality of Service
- QoS Data Collection
- Security Settings
- Telephony
- Small Remote Site Redundancy
- Dialing Properties
- Time Parameters
- Audio Settings
- SNMP Settings
- Applications
- Service Integrations
- User Settings
- SIP Mobility
- HFA Mobility
- Keysets/Keylayout
- WLAN Settings
- Signaling and Payload Encryption (SPE)
- IEEE 802.1x
- Diagnosis
- Miscellaneous
- File Deployment

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view (no changes possible except under **Remarks**).



> ***NOTE:*** The **Search** view fetches only the attributes of the specific mask that is currently displayed for the selected device(s) and not the attributes of all the masks under **IP Phone Configuration** for that device(s) as in previous DLS/phone versions.
> For further information on the **Search** view, please refer to Section 5.5, "Search Functionality".

IP Address:

IP address of the IP phone. For OpenStage, an IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP phone device type. The icon indicates whether this is a virtual device.

All IP phone types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiPoint 410 standard, OpenScape Desk Phone IP 35G, OpenScape Desk Phone IP 35G Eco**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

IP phone software type.

Examples: **Unify HFA**, **Unify SIP**.

> ***IMPORTANT:*** **UF IP SIP** devices need to be registered as **Unify HFA** in the DLS database for proper usage as they are SIP endpoints. However, Element Manager synchronization with OpenScape 4000 Assistant (Webservice) registers the UFIP SIP devices as **Unify HFA** in the DLS database. To have the **UF IP SIP** devices synchronized correctly as **Unify SIP**,please use JDBC synchronization with Element Manager.

Reg-Address

IP address or DNS name of the HFA or SIP server at which the device is registered.

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, **IP Address** contains the IPv4 address, and **IP Address 2** contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Location

Current location of the IP Device. The value is set during registration and is displayed only herein. (For meaning and configuration of the location, see Section 6.3.2, "Location".)

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.7, "Editing Templates".

Discard

Discards any changes made and new entries.

Read

The parameters displayed on the new mask are read in again by the IP device.

Rename

Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

Import Certificate

Imports a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.14, "Security: Administering Certificates".

Remove Certificate

Deletes a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.14, "Security: Administering Certificates".

7.1.1 Gateway/Server

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server

This area features the following components:

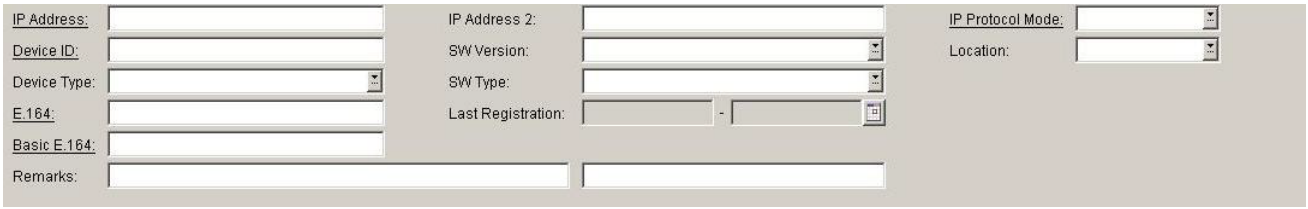
- General Data
- Possible Action Buttons
- "Gateway (HFA) / SIP Server" Tab
- "Gateway (Standby)" Tab
- "SIP Terminal Settings" Tab
- "SIP Registering 1" Tab
- "SIP Registering 2" Tab
- "SIP Survivability" Tab
- "Standard CSTA" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the IP phone. For OpenStage, an IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP phone device type.

All IP phone types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

IP phone software type.

Examples: **Unify HFA**, **Unify SIP**.

> ***IMPORTANT:*** **UF IP SIP** devices need to be registered as **Unify HFA** in the DLS database for proper usage as they are SIP endpoints. However, Element Manager synchronization with OpenScape 4000 Assistant (Webservice) registers the UFIP SIP devices as **Unify HFA** in the DLS database. To have the **UF IP SIP** devices synchronized correctly as **Unify SIP**,please use JDBC synchronization with Element Manager.

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

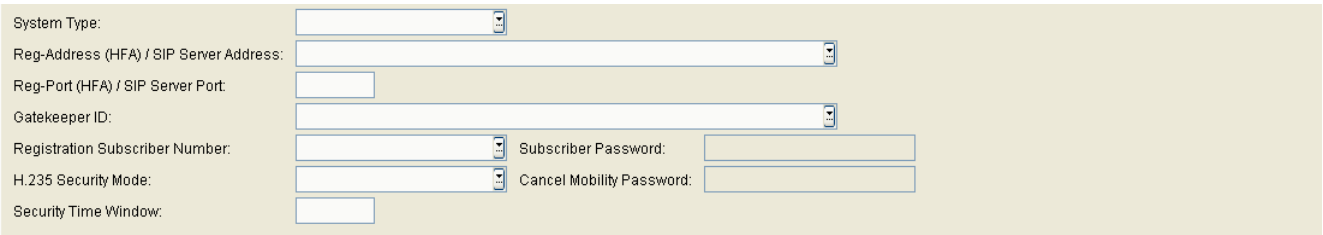
- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Location

Current location of the IP Device. The value is set during registration and is displayed only herein. (For meaning and configuration of the location, see Section 6.3.2, "Location".)

7.1.1.1 "Gateway (HFA) / SIP Server" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "Gateway (HFA) / SIP Server" Tab



System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **Unknown**
- **OpenScape Business V1**
- **OpenScape Business V2**
- **OpenScape Business V3**
- **OpenScape Business V4**
- **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**
- **HiPath 4000 V8.0**
- **HiPath 4000 V9.0**
- **HiPath 4000 V10.0**

Only available in HFA workpoints.

Reg-Address (HFA) / SIP Server Address:

IP address or host name of the PBX or gateway used for operating the workpoint.

Reg-Port (HFA) / SIP Server Port:

Port number of the PBX, gateway or SIP server used for operating the workpoint.

Gatekeeper ID:

ID of the PBX, gateway or gatekeeper used for operating the workpoint.

NOTE: This ID corresponds to the **"**Globid**"** parameter in AMO HFAB for the HiPath 4000 resp. the H.323 ID with the HiPath 3000.

Registration Subscriber Number:

Phone number of the subscriber at the PBX.

Example: **12345**

Only available in HFA workpoints.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only available in HFA workpoints.

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should all run synchronously in H.235.

Only available in HFA workpoints.

Subscriber Password:

Password of the workpoint at the PBX.

Only available in HFA workpoints.

Cancel Mobility Password:

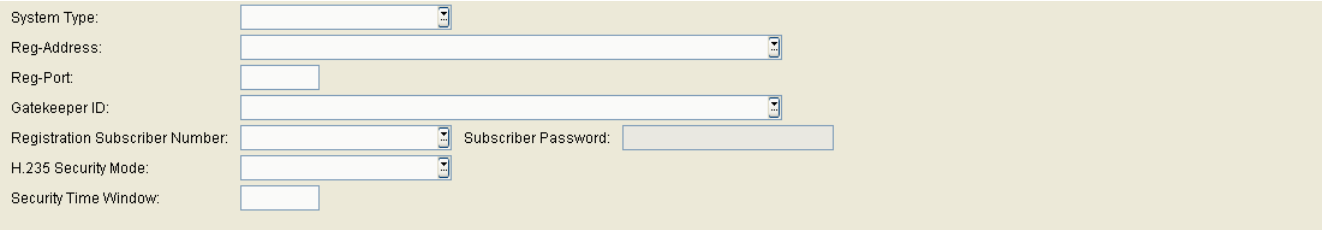
Password to disable the mobility function at the home workpoint.

Only available in HFA workpoints.

7.1.1.2 "Gateway (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "Gateway (Standby)" Tab

NOTE: This "standby" data is used when the "home" data for the "Gateway (HFA) / SIP Server" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **Unknown**
- **OpenScape Business V1**
- **OpenScape Business V2**
- **OpenScape Business V3**
- **OpenScape Business V4**
- **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**
- **HiPath 4000 V8.0**
- **HiPath 4000 V9.0**
- **HiPath 4000 V10.0**

Only available in HFA workpoints.

Reg-Address:

IP address or host name of the PBX or gateway provided as standby for the workpoint.

Reg-Port:

Port number of the PBX or gateway provided as standby for the workpoint.

Gatekeeper ID:

ID of the PBX, gateway or gatekeeper provided as standby for the workpoint.

NOTE: This ID corresponds to the **"**Globid**"** parameter in AMO HFAB for the HiPath 4000 resp. the H.323 ID with the HiPath 3000.

Registration Subscriber Number:

Phone number of the subscriber at the PBX.

Example: **12345**

Only available in HFA workpoints.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.

- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only available in HFA workpoints.

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should all run synchronously in H.235.

Only available in HFA workpoints.

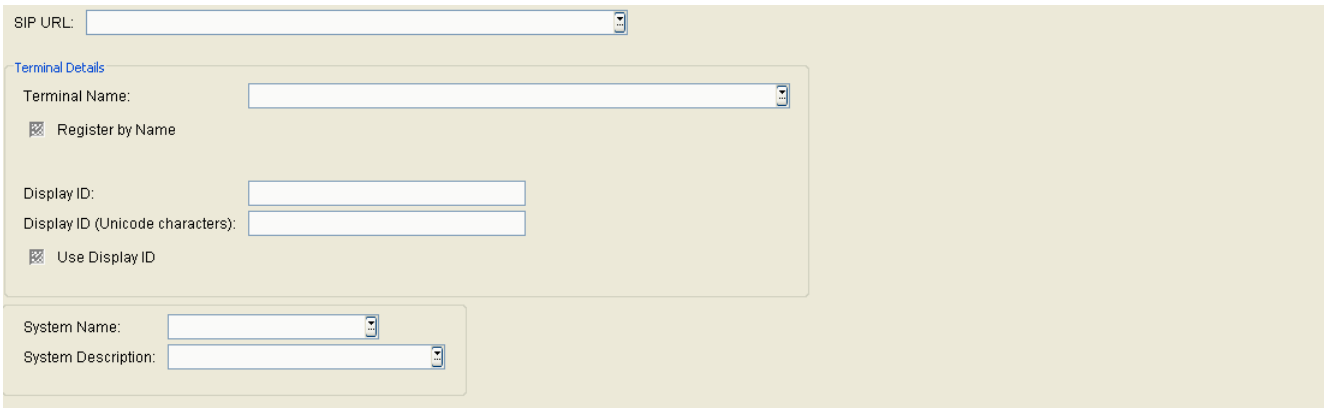
Subscriber Password:

Password of the workpoint at the standby PBX.

Only available in HFA workpoints.

7.1.1.3 "SIP Terminal Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "SIP Terminal Settings" Tab



SIP URL:

SIP address of the IP phone.

Format: **<SIP user ID>@<Domain>**.

Terminal Details

Terminal Name:

Name of the IP phone used as a synonym for the phone number during registration.

Only necessary if the **Register by Name** checkbox is selected and the registrar server is appropriately configured.

Register by Name

If this checkbox is activated, the phone logs on using the **Terminal Name**.

Display ID:

Name of the IP phone, as displayed on the telephone.

Value range: max. 24 alphanumeric characters.

Display ID (Unicode characters):

Name of the IP phone, as displayed on the telephone, in unicode characters.

NOTE: Unicode is only available in the OpenStage family of telephones.

Value range: max. 24 alphanumeric characters.

Use Display ID

If this checkbox is activated, the display ID is displayed on the device's status bar.

System Name:

Random name that appears in the lower right-hand corner of the IP phone's display (in two-line display).

Example: **HiPath**

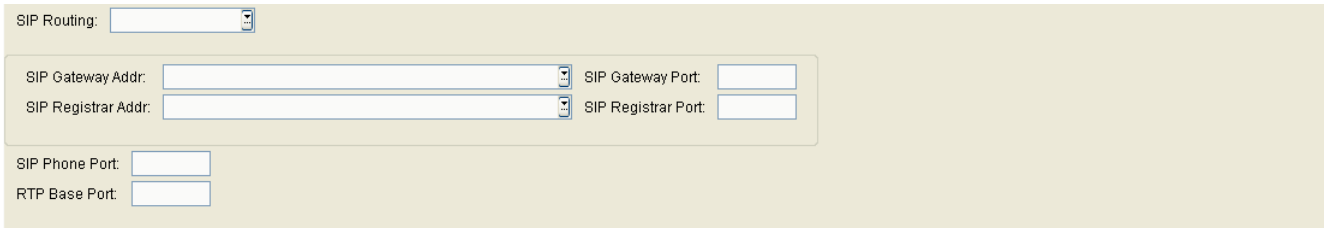
Value range: max. 10 alphanumeric characters.

System Description:

Used to display a system description at the workpoint (for three- or four-line display).

7.1.1.4 "SIP Registering 1" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "SIP Registering 1" Tab



SIP Routing:

Possible options:

- **Direct**
  For test purposes only.
- **Gateway**
  If a gateway is used.
- **Server**
  If an SIP proxy is used.

If Direct or Gateway is selected, no registration messages are sent during registration. Registration messages are sent to the registrar server for the **Server** routing mode.

SIP Gateway Addr:

IP address of the SIP gateway if the routing mode **Gateway** is used.

SIP Gateway Port:

Port number of the SIP gateway if the routing mode **Gateway** is used.

SIP Registrar Addr:

IP address of the SIP registrar.

SIP Registrar Port:

Port number of the SIP registrar.

SIP Phone Port:

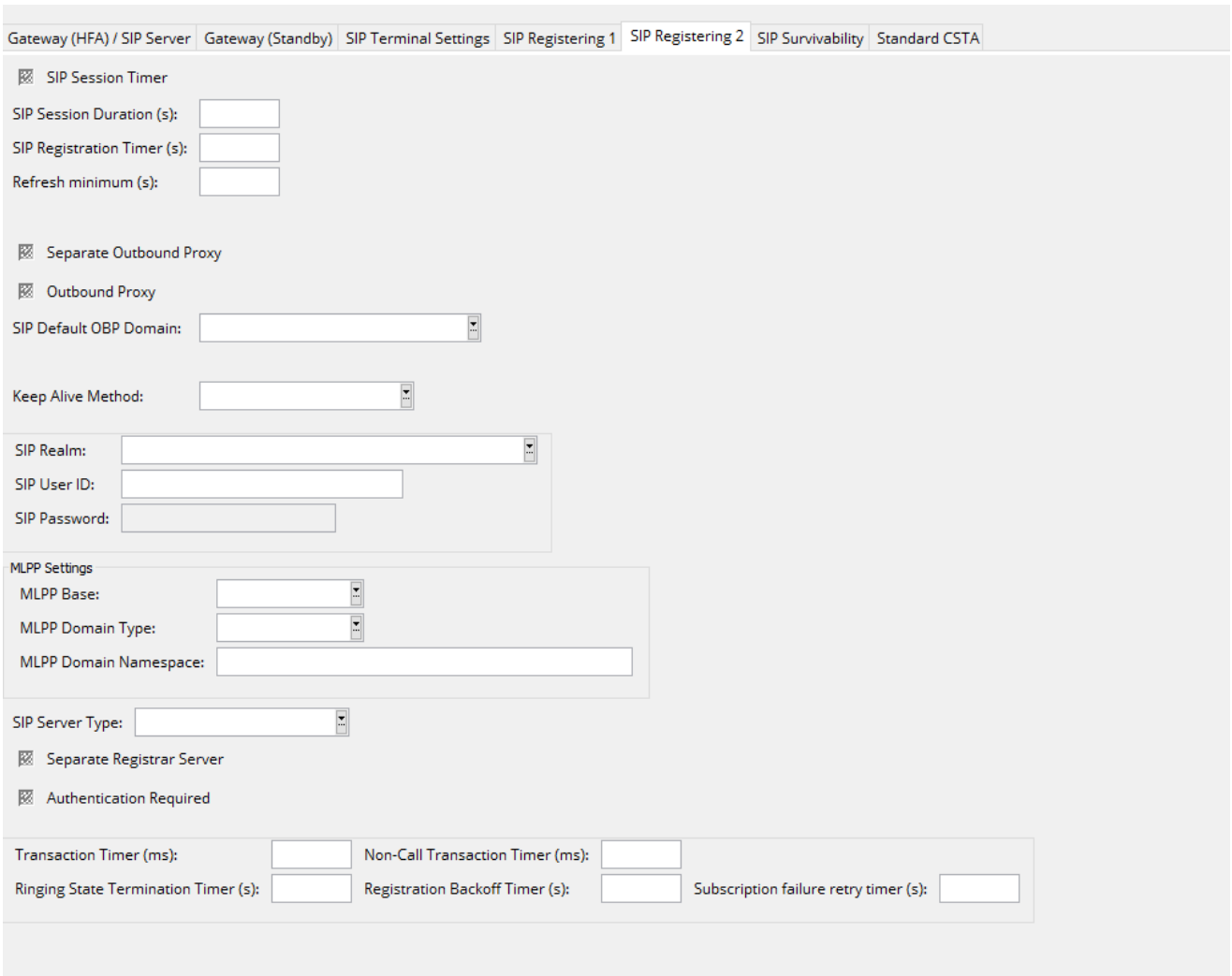
Port number of the IP phone.

RTP Base Port:

Base port number for RTP transport.

7.1.1.5 "SIP Registering 2" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "SIP Registering 2" Tab



SIP Session Timer

Checkbox for activating the SIP session timer. The timer is used to monitor the duration of an SIP session.

SIP Session Duration:

Highest duration in seconds for an SIP session.

Value range: **0** ... **3600** seconds.

SIP Registration Timer (sec):

Time until re-registration at the SIP server. Re-registration ensures that the SIP telephone remains logged on to the SIP server. It can also detect server connectivity problems.

Value range: **0** ... **4320** seconds.

Default value: **0**

Session Refresh Guard Time (sec):

Time interval that triggers a SIP registration / SIP subscription, session to be refreshed before the maximum expiry time provided by the SIP server. The setting value indicates the earliest point before the session expires when the device can consider sending a session refresh message to stop the session from expiring.

Default value: **0**

Value range:**0** ... **3600** seconds.

NOTE: Available only to CP200/205/400/600 devices & of V1R3 version and higher.

Example: if the Expiry header form the SIP server is 600 seconds and the guard time is 15 seconds then the refresh from device will sent between 585 seconds (600-15) and 600 seconds after previous registration.

Separate Outbound Proxy

If this option is activated, a separate outbound proxy is used. This parameter is used with optiPoint WL2 phones to indicate an outbound proxy which is not identical with the SIP proxy.

Outbound Proxy

Checkbox for activating an SIP proxy for outbound calls.

Together with **SIP Default OBP Domain**, this checkbox controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

SIP Default OBP Domain:

Together with **Outbound Proxy** this entry controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

Keep Alive Method:

Selects the keep alive method used between comms and the switch.

Possible options:

- **Sequence**
- **CRLF**

SIP Realm:

Naming range where the user ID and password are valid. This SIP realm must be entered in the system and on the SIP server.

SIP User ID:

The user ID is the first part of the SIP URL. Required, together with the password, to access the SIP server.

SIP Password:

Password associated with the user ID, required to access the SIP server.

MLPP Settings

MLPP Base

Possible options:

- **Local**
- **Server**

MLPP Domain Type

Specifies which resource priority namespace will be accepted from a fixed list.

Possible options:

- **dsn**
  dsn-000000
- **uc**
  uc-000000
- **dsn+uc**
- **Other domain**

MLPP Domain Namespace

Specifies an ASCII string for a single resource priority namespace which will be accepted.

Alphanumerical characters and the following special charakters are allowed: -!%*_+` "~

A "." is not allowed.

SIP Server Type:

Selects the appropriate SIP server type for the IP phone.

Possible options:

- **other**
- **OpenScape Voice**
- **Broadsoft**
- **Sylantro**
- **HiQ 8000**
- **Genesys**
- **Google Voice**
- **Ring Central**
  This option is only available for phones of version SIP V1R8 or later.

Separate Registrar Server

If you log on to a WLAN, you can be contacted at your personal number. A registrar assigns the SIP URI or IP address you are currently logged on under to your personal number. Your SIP provider may offer a separate registrar server.

Activate this checkbox to log on to a separate registrar proxy server. You can enter the server address and port number of the registrar proxy server in the entry fields that then appear.

Only applies to WLAN phones.

Authentication Required

Activate this checkbox if you have to enter your **SIP user ID** in addition to the standard access data to log on to the SIP provider.

Only applies to WLAN phones.

Transaction Timer (ms)

Time in milliseconds that a device will wait for a requested SIP message before the server is categorized as unavailable.

Ringing State Termination Timer (sec)

Time in seconds to terminate an incoming call transaction in ringing state (including alerting and being busy).

When this timer is set to non-zero value, the Ringing state & phone alerting (ringing, visual alert) is stopped by phone after the set period.

When set to 0, the timer is off.

Non-Call Transaction Timer (ms)

Time in milliseconds allowed for non-INVITE (nonCall) based transaction (F timer).

Registration Backoff Timer (sec)

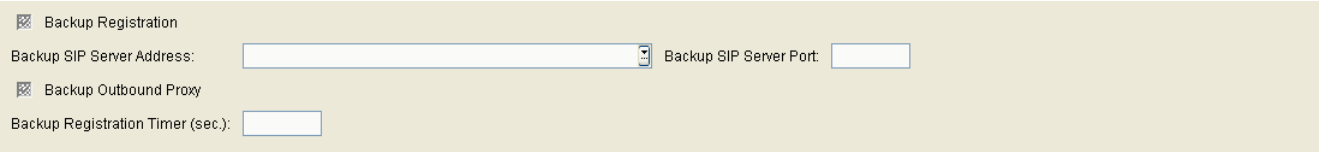
Time in seconds allowed between attempts to reREGISTER after a registration failure.

Subscription failure retry timer (sec)

Time in seconds allowed between attempts to retry after subscription failure.

7.1.1.6 "SIP Survivability" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "SIP Survivability" Tab



Backup Registration

Checkbox for activating the backup registration.

Backup SIP Server Address:

IP address or host name of the backup SIP server.

Backup SIP Server Port:

Port number for communication with the backup SIP server.

Backup Outbound Proxy

Checkbox for activating the SIP Proxy backup for outgoing calls.

For more information, see Chapter 17, "Outbound Proxy".

Backup Registration Time:

Time period before re-registration at the backup SIP server. Re-registration ensures that the SIP telephone remains logged on to the backup SIP server. It can also detect server connectivity problems.

Requirement: An SIP server backup must be used.

Value range: **0** ... **4320** seconds.

Default: **0**.

7.1.1.7 "Standard CSTA" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Gateway/Server > "Standard CSTA" Tab



Server Address:

IP address or host name of the Standard CSTA server.

Server Port:

Port number for communication with the Standard CSTA server.

7.1.2 IP Routing

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IP Routing

This area features the following components:

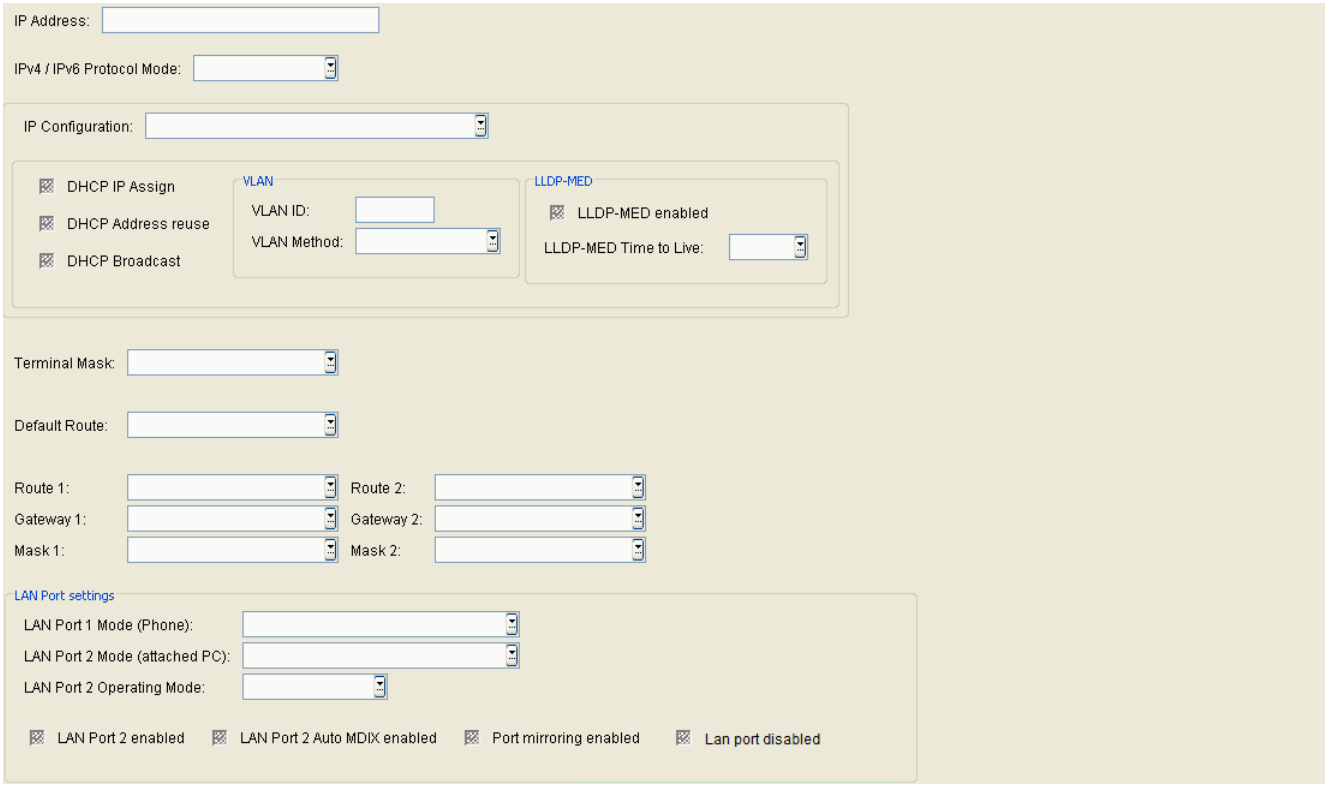
- General Data
- Possible Action Buttons
- "IP Routing" Tab
- "IPv6 Settings" Tab
- "ANAT Settings" Tab
- "ICE Settings" Tab
- "DNS Server" Tab
- "Wi-Fi Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.2.1 "IP Routing" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IP Routing > "IP Routing" Tab



IP Address

IP address of the IP phone.

IPv4 / IPv6 Protocol Mode

Selects the internet protocol to be used by the IP phone.

Possible Options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

IP Configuration

Determines how the IP settings are to be configured; valid from OpenStage version 1.5. With versions < 1.5, this field is greyed out, like the remaining LLDP-MED parameters.

Please note that the writing and reading procedures for this parameter differ from one another. When the DLS user select a particular option (e.g. "LLDP-MED with DHCP Configuration"), the IP configuration parameters are set and sent to the end device. When reading from the device, however, "Please select an option for IP Configuration" is displayed in any case. This is due to the possibility that the parameter may not have been detected unambigously; for instance, the value of the **VLAN method** parameter can depend on whether the VLAN ID has been determined over DHCP or over LLDP-MED.

The field is predefined with 'Please select an option for IP Configuration'.

Possible Values:

- **LLDP-MED with DHCP Configuration**
- **Use DHCP**
- **Manual VLAN with DHCP Configuration**
- **Manual Settings**

DHCP IP Assign

This checkbox can be activated if a DHCP server is present. The workpoint then obtains the IP address data dynamically from the DHCP server.

This checkbox must not be activated if there is no DHCP server available. Instead, the IP address data (**IP Address**, **Terminal Mask** and **Default Route**) must be manually set for this workpoint.

DHCP lease reuse

This checkbox can be activated if a DHCP server is present. If the switch is activated, the DHCP lease will be reused.

DHCP Broadcast

This checkbox can be activated if a DHCP server is present. With this entry the user can change the DHCP protocol element "flags". If the broadcast flag is enabled, the DHCP server will broadcast its responses to the phone's requests; otherwise unicast responses will be used.

DHCP options

When an IP phone is booting, it first obtains an IP address using DHCP. During this process, the DHCP server provides the DMS address and other configuration information to the phone using options 43 and 66. The DMS address is mutually exclusive with a possibly provided DLS address. This is because a phone configures the DMS and DLS addresses as DHCP options, and can only receive one value for each DHCP option.

NOTE: Parse DHCP option 66 and Parse DHCP option 43 are enabled by default on the phone. It is not recommended to disable them, unless it is requested at specific environments.

See below for more information for each of the options:

Parse DHCP option 66

Parse DHCP option 66 can be used in case of a DMS server and is NOT required for getting the DLS address via DHCP.

Parse DHCP option 43

Parse DHCP option 43 (parsing of DHCPv4 option 43 / DHCPv6 option 17) is mandatory for getting the DLS address and port configuration via DHCP.

VLAN

VLAN ID:

VLAN ID when using virtual LANs. Can only be changed if QoS layer 2 is active. The value is read-only if it has been dynamically assigned with DHCP.

Value range: **0** ... **4095**.

VLAN Method:

Determines how the VLAN ID is assigned to the end device. Can only be changed when QoS layer 2 has been activated.

Possible options:

- **Manually**
  The VLAN ID is entered manually.
- **DHCP**
  The VLAN ID supplied by the DHCP server is used.
- **None**
  (For WLAN only)

- **LLDP-MED**
  The VLAN ID supplied by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) is used. Available for OpenStage from V1R5 onwards.

LLDP-MED

LLDP-MED enabled:

Enables sending and receiving LLDP data.

LLDP-MED Time-to-Live

Possible Values:

- **40**
- **60**
- **80**
- **100**
- **120**
- **140**
- **180**
- **240**
- **320**
- **400**

Terminal Mask:

Subnet mask for the IP address.

The value is read-only if it was dynamically assigned with DHCP.

Default Route:

IP address or host name of the default router/gateway.

The value is read-only if it was assigned with DHCP.

Route 1:

IP address or host name of the first static route (optional).

Gateway 1:

IP address or host name of the router/gateway of the first static route (optional).

Mask 1:

Subnet mask of the first static route (optional).

Route 2:

IP address or host name of the second static route (optional).

Gateway 2:

IP address or host name of the router/gateway of the second static route (optional).

Mask 2:

Subnet mask of the second static route (optional).

LAN Port settings

LAN Port 1 Mode (Phone):

Data rate mode for the first Ethernet port on the IP phone. The first port is connected to the LAN. The data rate value depends on the switch or router bandwidth that is supported in the network.

Possible options:

- **10 Mbps half-duplex**
- **10 Mbps full-duplex**
- **100 Mbps half-duplex**
- **100 Mbps full-duplex**
- **Auto**

Default: **Auto**

LAN Port 2 Mode (attached PC):

Data rate mode for the second LAN port on the IP phone. The value depends on the switch or router bandwidth that is supported in the network.

Possible options:

- **10 Mbps half-duplex**
- **10 Mbps full-duplex**
- **100 Mbps half-duplex**
- **100 Mbps full-duplex**
- **Auto**

Default: **Auto**

LAN Port 2 Operating Mode

Choice between three modes of operation for the PC port.

Possible options:

- **Disabled**
  The LAN port is inactive.
- **Enabled**
  The LAN port is active.
- **Mirror**
  All data traffic on LAN port 1 is mirrored to port 2.

LAN Port 2 enabled

Checkbox for enabling LAN port 2.

LAN Port 2 Auto MDIX enabled

Checkbox for enabling LAN Port 2 Auto MDIX. If Auto MDIX is enabled, the LAN port automatically switches between normal MDI and MDI-X (crossover circuit).

Port mirroring enabled

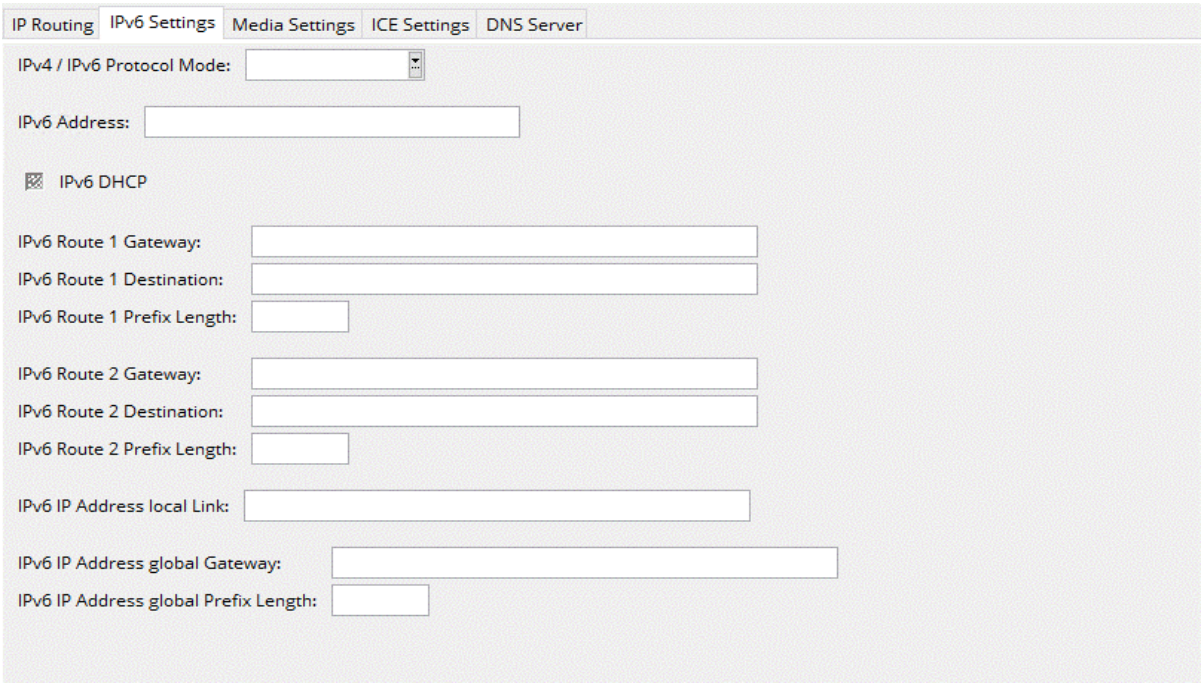
When this checkbox is activated, all data traffic on LAN port 1 can be mirrored to port 2: The operation type for **LAN Port 2 Operating Mode** must be set to **Mirror**.

Lan port disabled

When this checkbox is activated, the LAN port is disabled **but only** when LAN is available.

7.1.2.2 "IPv6 Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IP Routing > "IPv6 Settings" Tab



IPv4 / v6 Protocol Mode

Possible options:

- IPv4
- IPv6
- IPv4 and IPv6

IPv6 Address

IPv6 address of the IP phone.

IPv6 Route 1 Gateway

IPv6 address of the router/gateway for the first static route.

IPv6 Route 1 Destination

Destination address for the first static route.

IPv6 Route 1 Prefix Length

Prefix length for the first static route.

IPv6 Route 2 Gateway

IPv6 address of the router/gateway for the second static route.

IPv6 Route 2 Destination

Destination for the second static route.

IPv6 Route 2 Prefix Length

Prefix length for the second static route.

IPv6 IP Address local Link

Local link address of the IP phone.

IPv6 IP Address global Gateway

IPv6 address of the global router/gateway .

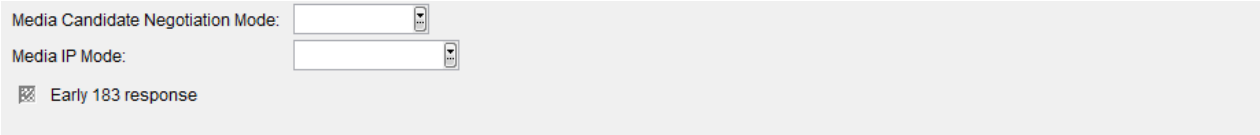
IPv6 IP Address global Prefix Length

Length of the global prefix.

7.1.2.3 "ANAT Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IP Routing > "ANAT Settings" Tab

Alternative Network Adress Type (ANAT) provides a mechanism of IPv4/IPv6 media negotiation on a media stream basis.



Media Candidate Negotiation Mode

Selects the Media Candidate Negotiation Mode.

Possible options:

- **Single IP**
- **ANAT**
- **ICE**

> ***NOTE:*** ICE value is read only and it is set automatically when ICE is enabled under"ICE Settings" Tab.

Media IP Mode

Selects the media IP mode.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 / IPv6**
- **IPv6 / IPv4**

Early 183 response

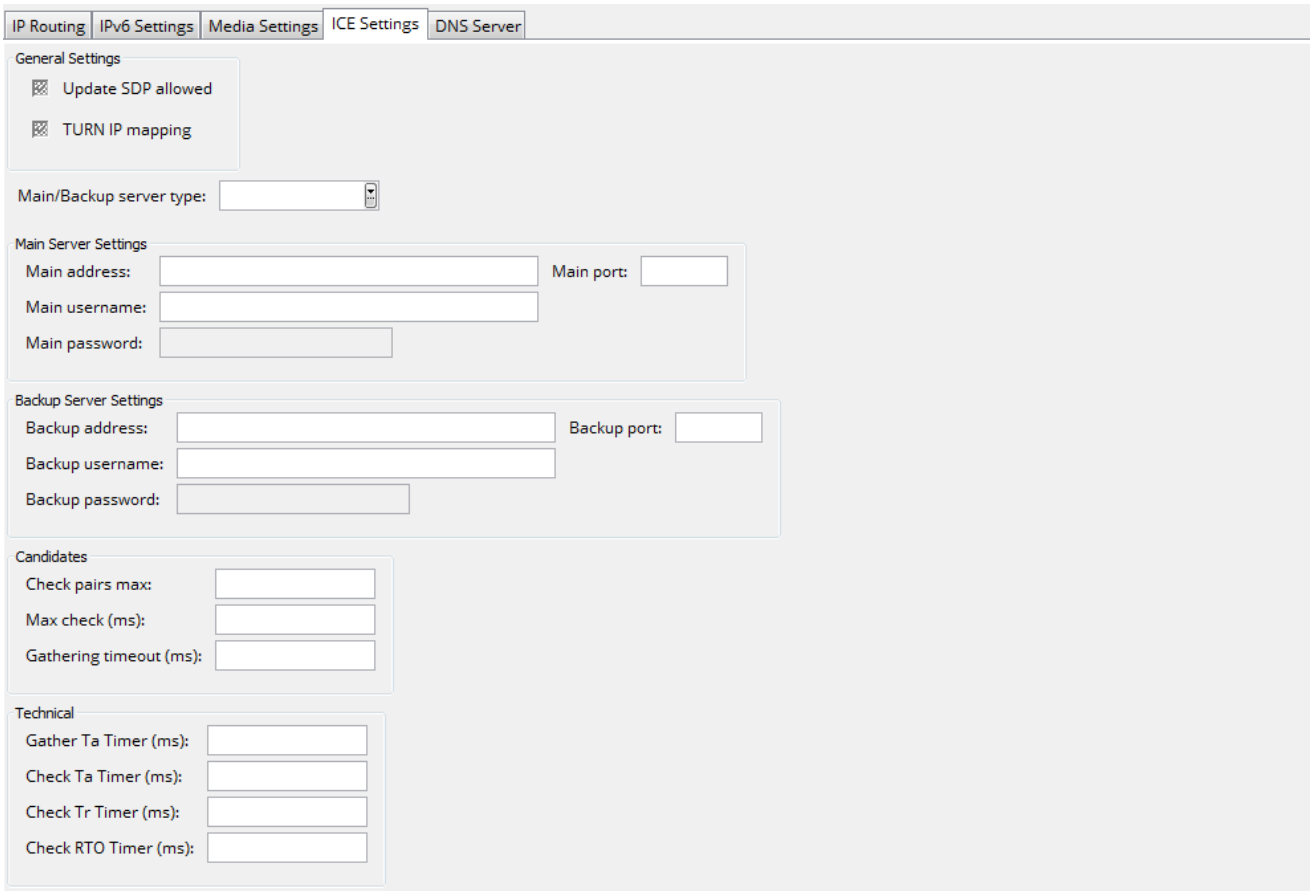
If enabled, the phone will send a SIP 183 response with an SDP answer.

This checkbox is disabled by default.

It is also disabled for all OpenStage /Desk Phone IP devices.

7.1.2.4 "ICE Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IP Routing > "ICE Settings" Tab



General Settings

Update SDP allowed

When enabled, the phone may send an updated SDP offer/answer as required by the ICE standard.

This checkbox is disabled by default.

TURN IP mapping

When enabled, the TURN server will provide an address mapping between IPv4 and IPv6 peer endpoints.Otherwise,only endpoints supporting the locally configured IP family may be addressed.

This checkbox is disabled by default.

Main/Backup server type:

Type of the server providing ICE candidate addresses as an indexed list.

Possible values:

- **None**

The main / backup server is not used.

- **STUN**

The main /backup server is a STUN server that will only return Server reflexive candidates

- **TURN**

The main /backup server is a TURN server that will return Relayed and Server reflexive candidates

> ***NOTE:*** If the Main Server is set to None but the backup server is configured as available and not set to None then the backup server is used instead.If neither the main or the backup server is set to None then both servers may be used to complete gathering candidates.

Main Server Settings

Main Address

Address of the server providing ICE candidate addresses as an indexed list.

Available addresses:

- FQDN
- IP address (IPv4/IPv6)

Main Port

IP port of the server providing ICE candidate addresses as an indexed list.

0 means perform a lookup of an FQDN using DNS-SRV.

Default value is set to 3478.Use the default port if the address is an IP address rather than an FQDN.

Main Username

User name for access to the TURN server as an indexed list.

Main Password

Password for access to the TURN server as an indexed list.

Backup Server Settings

Backup Address

Address of the backup server providing ICE candidate addresses as an indexed list

Available addresses:

- FQDN
- IP address (IPv4/IPv6)

Backup Port

IP port of the backup server providing ICE candidate addresses as an indexed list.

0 means perform a lookup of an FQDN using DNS-SRV.

Default value is set to 3478.Use the default port if the address is an IP address rather than an FQDN.

Backup Username

User name for access to the TURN server as an indexed list.

Backup Password

Password for access to the TURN server as an indexed list.

Candidates

Check pairs max

Maximum number of candidate pairs for connectivity checking.

Default value is set at **50**.

Max check (ms)

Connectivity check duration. Sets the amount of time in milliseconds allowed to perform the connectivity checks.

Default value is set at **15000**.

Gathering timeout (ms)

Timeout value in milliseconds which controls the pacing of the ICE Gathering retransmissions sent on a candidate pair.

Value range: **100-65535**

Default value is set at **5000**.

Technical

Gather Ta Timer (ms)

Value in milliseconds which controls the pacing of the candidates gathering.

Check Ta Timer (ms)

Connectivity check interval. Sets the Ta timer value in milliseconds which controls the pacing of the ICE Connectivity Checks sent on a candidate pairs.

Check Tr Timer (ms)

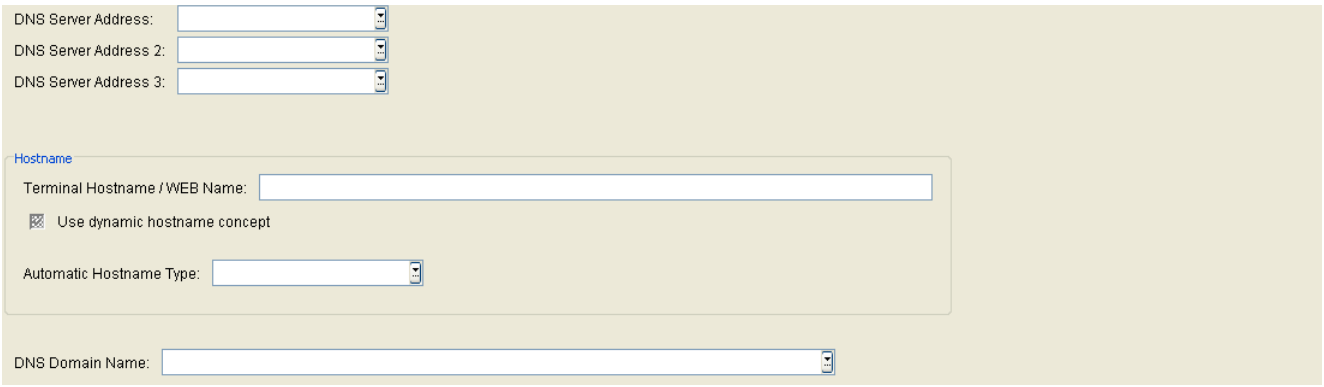
Connectivity check interval. Sets the Tr timer value in milliseconds which controls the pacing of the ICE Connectivity Checks sent on a candidate pairs.

Check RTO Timer (ms)

Connectivity check repeat interval. Sets the RTO timer value in milliseconds which controls the pacing of the ICE Connectivity Check retransmissions sent on a candidate pair.

7.1.2.5 "DNS Server" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IP Routing > "DNS Server" Tab



DNS Server Address:

IP address or host name of the DNS server.

The value is read-only if it was dynamically assigned with DHCP.

DNS Server Address 2:

IP address or host name of the second DNS server (optional).

The value is read-only if it was dynamically assigned with DHCP.

Not available in optiPoint 400.

DNS Server Address 3:

IP address or host name of the third DNS server (optional).

The value is read-only if it was dynamically assigned with DHCP.

Not available in optiPoint 400.

Hostname

Terminal Hostname / WEB Name:

Host name of the terminal.

Permitted characters: letters, digits, hyphens, underscores, and periods; case-sensitive; maximum length: 63 characters.

The value is read-only if it was dynamically assigned with DHCP.

Use dynamic hostname concept

If this checkbox is activated, the E.164 number is used as the DNS host name for IP phones.

Automatic Hostname Type:

Type of automatically generated hostname.

Possible Values:

- **No DDNS Hostname**
- **Only WEB Name**
- **Only Number**
- **Prefix Number**
- **MAC based**

DNS Domain Name:

Domain name of the DNS server.

The value is read-only if it was dynamically assigned with DHCP.

7.1.3 Ports

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Ports

This area features the following components:

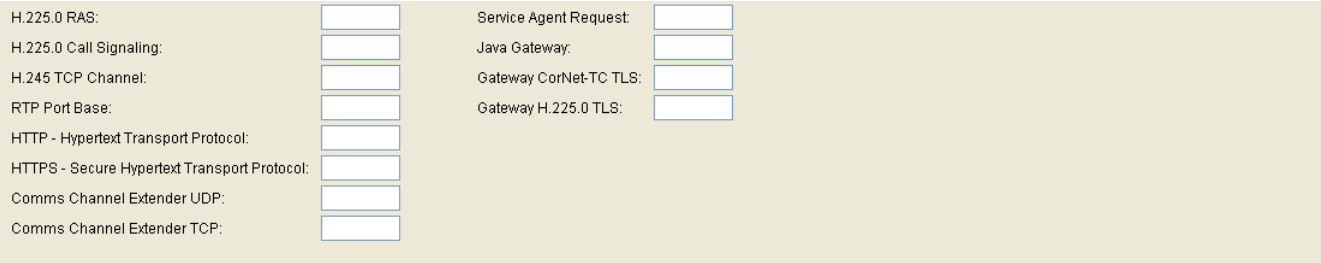
- General Data
- Possible Action Buttons
- "Ports" Tab
- "Ports (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.3.1 "Ports" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Ports > "Ports" Tab



H.225.0 RAS:

Port number for H.225 RAS.

Purpose: Registration and approval in the case of VoIP.

For communication with the following clients: Netmeeting, AP1120.

Port used: **1719**

H.225.0 Call Signaling:

Port number for H.225 call signaling.

Purpose: Connection control in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP1120.

Port used: **1720**

H.245 TCP Channel

Port number for the H.245 TCP channel.

RTP Port Base:

Port number for RTP.

Purpose: Transporting voice packets in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP11xx.

Port range used: **29100** ... **29131**

HTTP - Hypertext Transport Protocol:

Port number for HTTP.

Purpose: Web-based Management.

For communication with the following clients: the workpoint's WBM.

Port used: **8085**

HTTPS - Secure Hypertext Transport Protocol:

Port number for HTTPS.

Purpose: Web-Based Management.

For communication with the following clients: the workpoint's WBM.

Only available in SIP workpoints.

Port used: **443**

Comms Channel Extender UDP Port:

Port range used: **0** ... **65535**

Default: **65530**

Comms Channel Extender TCP Port:

Port range used: **0** ... **65535**

Default: **65531**

Service Agent Request:

Port range used: **0** ... **65535**

JAVA Gateway:

Port number for gateways used by Java applications.

Gateway CorNet-TC TLS

Port used by the HFA gateway for secure communication with the workpoint.

Port range used: **0** ... **65535**

Default: **4061**

Only available in HFA workpoints.

Gateway H.225.0 TLS

Port used for secure signalling with H.255.

Port range used: **0** ... **65535**

Default:**1300**

Only available in HFA workpoints.

7.1.3.2 "Ports (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Ports > "Ports (Standby)" Tab

NOTE: This "standby" data is used when the "home" data for the "Ports" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



H.225.0 RAS:

Port number for H.225 RAS.

Purpose: Registration and approval in the case of VoIP.

For communication with the following clients: Netmeeting, AP1120.

Port used: **1719**

H.225.0 Call Signaling:

Port number for H.225 call signaling.

Purpose: Connection control in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP1120.

Port used: **1720**

H.245 TCP Channel

Port number for the H.245 TCP channel.

For communication with the following clients:

RTP Port Base:

Port number for RTP.

Purpose: Transporting voice packets in the case of VoIP.

For communication with the following clients: HG1500, IP phones, Netmeeting, AP11xx, MEB.

Port range used: **29100** ... **29131**

HTTP - Hypertext Transport Protocol:

Port number for HTTP.

Purpose: Web-based Management.

For communication with the following clients: the workpoint's WBM.

Port used: **8085**

HTTPS - Secure Hypertext Transport Protocol:

Port number for HTTPS (HTTP with SSL encryption).

Purpose: Web-based Management.

For communication with the following clients: the workpoint's WBM.

Only available in SIP workpoints.

Port used: **443**

Service Agent Request:

Port number for service agent request.

JAVA Gateway:

Port number for the Java gatekeeper.

Gateway CorNet-TC TLS

Port used by the standby HFA gateway for secure communication with the workpoint.

Port range used: **0** ... **65535**

Default: **4061**

Only available in HFA workpoints.

Gateway H.225.0 TLS

Port used for secure signalling with H.225 when the workpoint has switched to the standby gateway.

Only available in HFA workpoints.

7.1.4 Features

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features

This area features the following components:

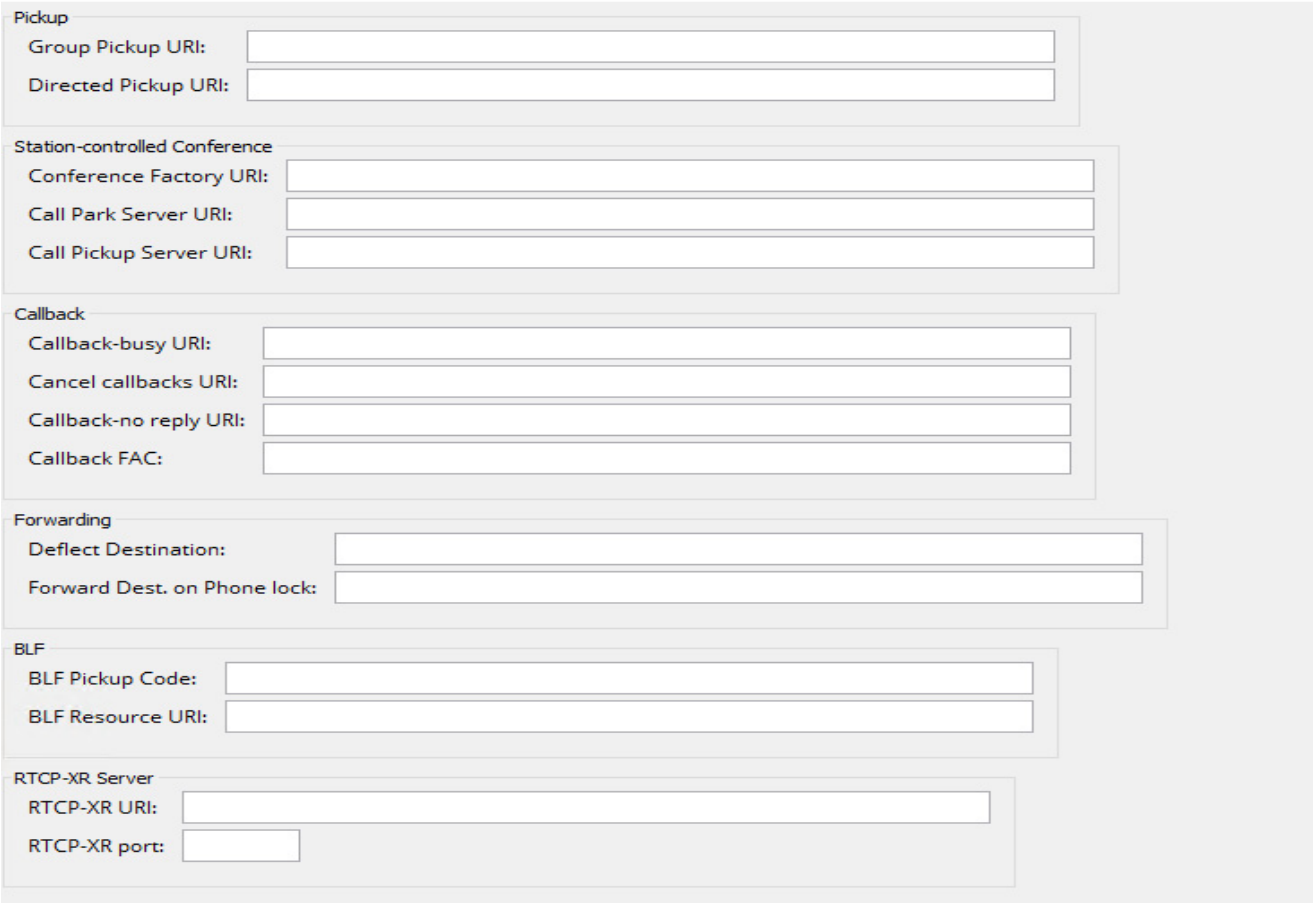
- General Data
- Possible Action Buttons
- "Feature Settings 1" Tab
- "Feature Settings 2" Tab
- "Call related User Settings" Tab
- "Availability" Tab
- "Server based features" Tab
- "Dialplan" Tab
- "Ringer Melody / Tone" Tab
- "Call Forwarding" Tab
- "Direct Video" Tab
- "Door Opener" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.4.1 "Feature Settings 1" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Feature Settings 1" Tab



Group pickup

Group Pickup URI:

URI of the group pickup.

Only available in SIP workpoints.

Directed Pickup URI:

IP address or host name of the server for providing the directed pickup feature.

Only available for non-OpenScape Voice servers.

Station-controlled Conference

Conference Factory URI:

URI for setting up conference calls.

Only available in SIP workpoints.

Call Park Server URI:

URI of the server for parking calls.

Only available in SIP workpoints.

Call Pickup Server URI:

URI of the server for group pickup.

Only available in SIP workpoints.

Callback

Callback-busy URI:

URI of the server that controls the "Callback-busy" feature.

Only available for optiPoint and OpenStage V1 and V2.

Cancel callbacks URI:

URI that prompts the server to delete callback requests.

Callback-no reply URI

URI of the server that controls the "Callback-no reply" feature.

Only available for optiPoint and OpenStage V1 and V2.

Callback FAC

URI to be used for stimulus callback call requests.

Only available for OpenStage V3.0 onwards.

Deflection

Deflect Destination

Destination number for call forwarding.

Forward Dest. on Phone lock:

Destination number for forwarding in the case of a call to a locked workpoint.

BLF

BLF Pickup Code:

Feature code for BLF Pickup Code with Asterisk.

Only available in SIP workpoints.

BLF Resource URI:

Default value is set to NULL.

Available only for CP200/CP400/CP600 SIP phones of V1R2 version and higher.

RTCP-XR Server

RTCP-XR URI:

URI to be used for transmitting voice quality reports after the conclusion of a call.

RTCP-XR port:

Port value of RTCP-XR server.

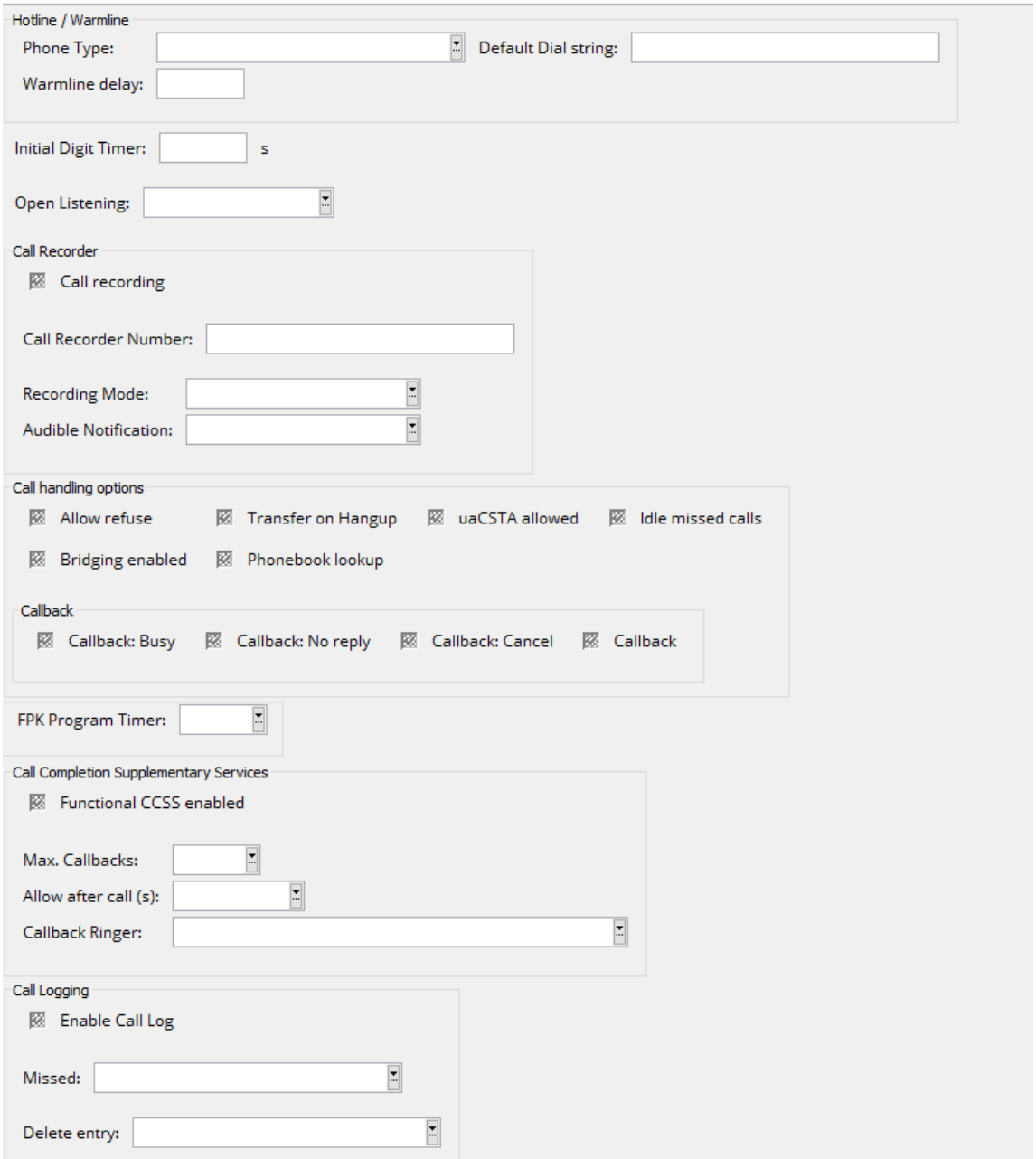
If RTCP-XR port value is not configured or is empty, the RTCP-XR port value will be taken from the SIP server port value.

7.1.4.2 "Feature Settings 2" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Feature Settings 2" Tab

NOTE: When operating SIP IP phones on HiPath 3000 and HiPath 4000 platforms, the following features are not available and should be deactivated so that users cannot see or select them:
- Auto answer
- Callback-busy
- Auto reconnect
- Callback-no reply

See also "Availability" Tab.



Hot Line/Warm Line

Phone Type:

Set device property.

Possible options:

- **Ordinary**

- **Hotline**
- **Warmline**

Only available in SIP workpoints.

Default Dial String:

Destination number for the functions "Hotline" and "Warmline".

Only available in SIP workpoints.

Warm Line delay:

Dialing delay in seconds for the warm line function.

For "Hotline" (emergency call) the value 0 should be entered as the time.

Only available in SIP workpoints.

Initial Digit Timer:

Waiting time in seconds for a dialed digit after the dial tone starts.

Only available in SIP workpoints.

Open Listening

Configures switching to Open Listening mode.

Possible options:

- **Standard Mode**
  To switch to Open Listening mode, the user must press and hold the Open Listening key while returning the handset to the cradle.
- **US Mode**
  To switch to Open Listening mode, the user must press the Open Listening key and then return the handset to the cradle.

Call Recorder

The central voice recorder records the entire voice flow of two or more participants.

Call recording

Switch on/off call recording.

NOTE: The item is selected and grayed out in case of SIP V1R8 (or later) phones. If you want to switch off the call recording feature on these phones, select `Disabled` from the **Recording Mode** drop-down list.

Call Recorder Address:

Address of the call recorder.

The format is similar to an e-mail address: "username@hostname". Therefore, it can accept numbers, symbols and letters.

Recording Mode

Determines the behaviour of the call recording.

Possible options:

- **Manual**
- **Auto Start**
- **All Calls**
- **Disabled**
  Available for SIP V1R8 (or later) phones.
- **One call**
  Available for:
  - OpenScape Desk Phone CP devices version V1R7 or later
  - OpenStage & OpenScape Desk Phone IP phones V3R5 or later.

Audible Notification

Select the tone for audible notification.

Possible options:

- **Off**
- **On / Single Shot**
- **Repeated**

Call handling options

Allow refuse

Checkbox for activating the function for rejecting calls.

Only available in SIP workpoints.

Transfer on Ring

Checkbox for activating the "Transfer on Ring" feature

If this option is activated, you can activate call transfer by replacing the handset even before the called party answers.

Only available in SIP workpoints.

Transfer on Hangup

Checkbox for activating the "Transfer on Hangup" feature.

Only available in SIP workpoints.

Bridging enabled

When active, call bridging is enabled.

Only available in SIP workpoints.

uaCSTA allowed

Checkbox to activate the "uaCSTA" feature.

Only available in SIP workpoints.

Phonebook lookup

Checkbox for activating the "Phonebook lookup" feature.

Idle missed calls

If set, an indication for missed calls will be shown on the display.

Callback

The user can request a callback if the station called is busy or if nobody answers. The user receives a callback when the other party's line becomes free.

Callback: Busy

Checkbox for activating the "Callback-busy" feature.

Only available in SIP workpoints.

Callback: No reply

Checkbox for activating the "Callback-no reply" feature.

Only available in SIP workpoints.

Callback: Cancel

When active, the user can cancel callback requests.

Callback

Activates Callback.

Only available for OpenStage V3 onwards.

FPK Program Timer

When "Off" is selected, the free programmable keys (FPKs) will not change to programming mode on long press.

Possible options:

- **On**
- **Off**

Call Completion Supplementary Service

Functional CCSS enabled

If switch is active, functional mechanisms are used to control & monitor CCSS (Call Completion Supplementary Services). If the switch is inactive, stimulus mechanisms (i.e. FAC) are used to trigger CCSS.

Max. Callbacks

Maximum number of callback requests allowed to be pending at the same time.

Possible values: **1** ... **10**

Allow after call (sec)

Time to retain server provided information required to request a callback after the callback request has failed.

Possible values:

- **unlimited**
- **1**
- **2**
- **3**
- **4**
- **5**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**

Callback Ringer

Sets the ringertone to be used to announce the availability of a callback call.

Call Logging

Enable Call Log

Checkbox that indicates whether Call logging is enabled.

Missed Logging

Indicates whether calls completed elsewhere will be logged on phone.

Possible options:

- **Include answered elsewhere**

  Calls completed elsewhere will be logged on phone.

- **Exclude answered elsewhere**
  Calls completed elsewhere will not be logged on phone.

Delete Entry

Indicates whether calls log entries are deleted in case there is a call to an entry in Missed calls list.

Possible options:

- **Delete manually (**default option)

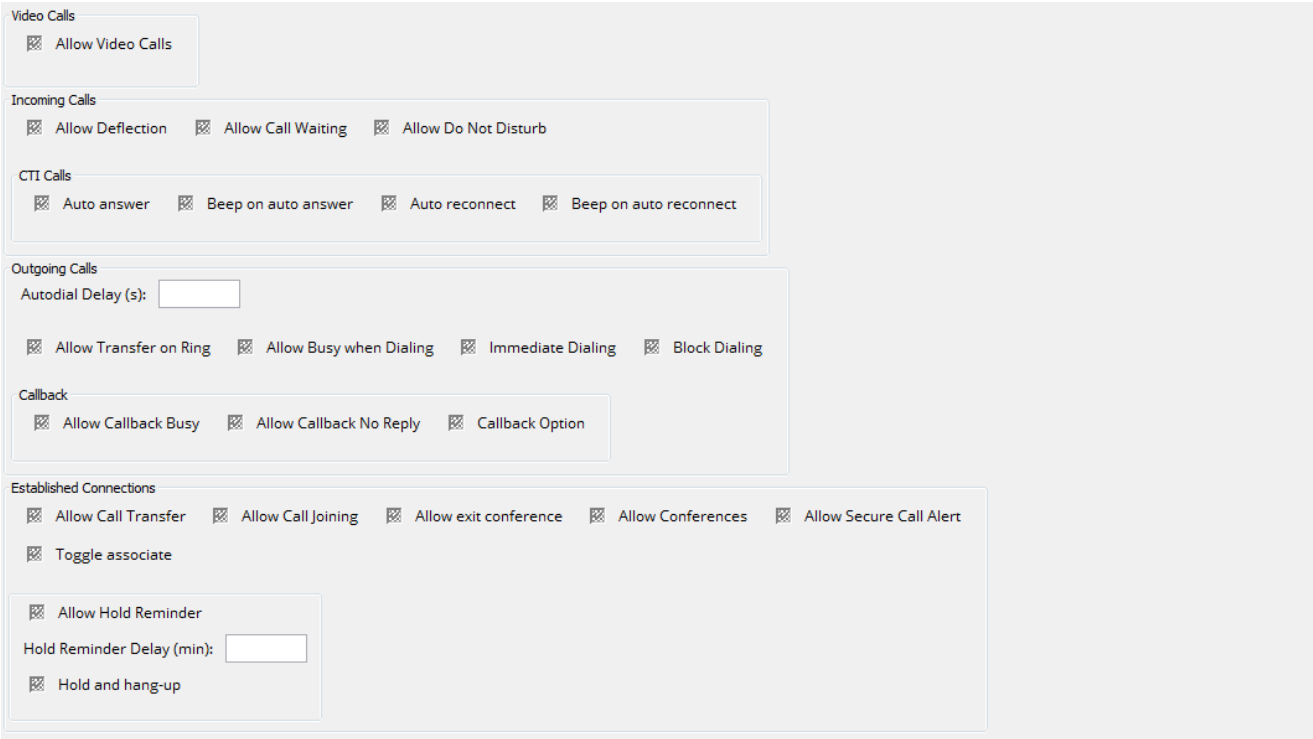
Outgoing calls that are made to entries in Missed calls tab of call log and that are connected will not be deleted from call log.

- **Delete when called**

Outgoing calls that are made to entries in Missed calls tab of call log and that are connected will be deleted from call log.

7.1.4.3 "Call related User Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Call related User Settings" Tab



Video Calls

Allow Video Calls

Checkbox for activating Video Calls.

If the Allow Video Calls checkbox is activated ,then video calls will be allowed.

Incoming Calls

Allow Deflection

Checkbox for activating Call Deflection.

If the user wants to deflect an incoming call, he is prompted to enter a destination phone number if there is none stored.

Allow Call Waiting

Checkbox for activating Call Waiting.

The user can accept a second incoming call in the course of an ongoing call. The caller hears the on-hook signal while the user hears a call-waiting signal tone. The user can reject or accept the second call. Before he accepts the second call, he can end the first call or place it on hold for subsequent retrieval.

Allow Do Not Disturb

Checkbox for activating Do Not Disturb.

If "Do not disturb" is activated, the telephone will not ring. The caller hears the busy signal.

CTI Calls

Auto answer

Checkbox for activating Auto Answer.

Speakerphone mode activates automatically on the phone if a CTI application (such as Outlook) is used to dial a number when Auto Answer is active. If Auto Answer is not active, the phone rings first and the user must press the loudspeaker key or lift the handset to set up the call. This setting also defines whether or not incoming calls are automatically accepted. If the function is active, an alert beep sounds when a call is automatically accepted.

Only available in SIP workpoints.

Beep on auto answer

Checkbox for activating a confirmation beep on Auto Answer.

If the function is active, an alert beep sounds when a call is automatically accepted.

Only available in SIP workpoints.

Auto reconnect

Checkbox for activating automatic reconnection of a parked call.

Only available in SIP workpoints (optiPoint).

Beep on auto reconnect

Checkbox for activating a confirmation beep on reconnection of a parked call.

The user can reconnect a held call both via the CTI application and via the phone. When the function is active, a beep sounds when the user toggles between an active call and a held call.

Only available in SIP workpoints.

Outgoing calls

Autodial delay (sec):

Delay for Automatic Dialing in seconds.

A number is automatically dialed after a set delay starting from the entry of the number's last digit.

Allow Transfer on Ring

Checkbox for activating Transfer on Ring.

If this option is allowed, the user can activate call transfer by replacing the handset even before the called party answers.

Allow Busy when Dialing

Checkbox for activating Busy when Dialing.

If this function is activated, an incoming call received while the user is dialing is rejected. The caller then hears the busy signal.

Immediate Dialing

If this check box is active, immediate dialing is executed as soon as the entered string matches a dial plan entry.

Only available in SIP workpoints.

Block Dialing

This checkbox is only available for CP400 HFA and CP600 HFA phones of V1R0 version and higher.

Block Dialing is enabled by default.

Callback

The user can request a callback if the station called is busy or if nobody answers. He will receive a callback when the other party's line becomes free.

Allow Callback Busy

Checkbox for activating Callback on Busy.

Only available for OpenStage V1 and V2.

Allow Callback No Reply

Checkbox for activating Callback on No Reply.

Only available for OpenStage V1 and V2.

Callback Option

Callback Option.

Only available for OpenStage starting with V3.

Established Connections

Allow Call Transfer

Checkbox for activating Call Transfer.

Allow Call Joining

Checkbox for activating Call Joining.

The user can join the first party with the party he consulted, clearing down his own connection to both parties in the process.

Allow exit conference

Checkbox for activating Exit Conference.

The user is disconnected from the conference call and the other call partners remain connected.

Allow Conferences

Checkbox for activating Conferences.

Allow Secure Call Alert

If the handling of secure calls is enabled on the phone and this check box is activated, a popup window and an alert tone will notify the user when an insecure (unencrypted) call comes in.

Toggle associate

When this feature is activated, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook.

Allow Hold Reminder

Checkbox for activating the Hold Reminder.

With "Hold reminder", the user specifes when he wants to receive an automatic reminder about a held call.

Hold Reminder Delay (min):

Delay for the Hold Reminder in minutes.

The minimum time value is 1, that is, the reminder is output after one minute. The maximum value is 15 minutes.

Hold and Hangup

Checkbox for activating the ” Hold and Hangup ” feature on non-keyset OpenStage phones.

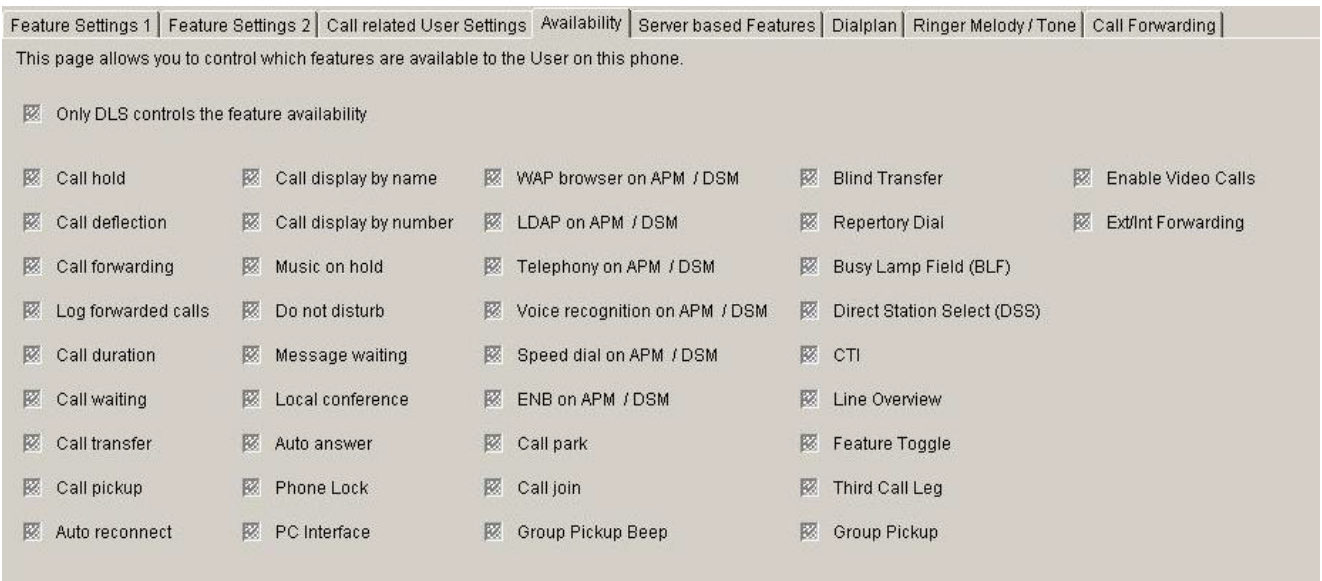
This feature enables the user to temporarily hold and hang up a line without disconnecting your caller. This function in disabled by default.

7.1.4.4 "Availability" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Availability" Tab

NOTE: When operating SIP IP phones on HiPath 3000 and HiPath 4000 platforms, the following features are not available and should be deactivated so that users cannot see or select them:

-Auto answer
-Call deflection
-Call forwarding
-Auto answer
-Call waiting
-Log forwarded calls
-Music on hold
-Call park
-Call transfer
-Local conference
-Message waiting
-Video Call
-
-See also "Feature Settings 2" Tab.



Only DLS controls feature availability

If this checkbox is activated, the availability of features is controlled exclusively by the DLS. The data entered in the "Feature Availability" tab is used. If this checkbox is not activated, the availability can also be controlled on the IP Device.

Only available in SIP workpoints.

Call hold

Checkbox for activating the function for placing calls on hold.

Only available in SIP workpoints.

Call deflection

Checkbox for activating manual forwarding for incoming calls (CD).

Only available in SIP workpoints.

Call forwarding

Checkbox for activating automatic call forwarding (CF).

Only available in SIP workpoints.

Log forwarded calls

Checkbox for activating logging for forwarded calls.

Only available in SIP workpoints.

Call duration

Checkbox for activating the function for displaying the call duration.

Only available in SIP workpoints.

Call waiting

Checkbox for activating visual and/or acoustic alerting for waiting calls (CW).

Only available in SIP workpoints.

Call transfer

Checkbox for activating the function for transferring calls (ECT).

Only available in SIP workpoints.

Call pickup

Checkbox for activating the function for picking up parked calls.

Only available in SIP workpoints.

Auto reconnect

Checkbox for activating the auto reconnect feature.

Only available in SIP workpoints.

Call display by number

Switch for activating call number display at the workpoint.

Only available in SIP workpoints.

Call display by name

Switch for activating caller name display at the workpoint.

Only available in SIP workpoints.

Music on hold

Checkbox for activating music on hold for held and parked calls.

Only available in SIP workpoints.

Do not disturb

Checkbox for activating the do-not-disturb function (optical alerting and ring only).

Only available in SIP workpoints.

Message waiting

Checkbox for activating alerting for waiting messages (MWI).

Only available in SIP workpoints.

Local conference

Checkbox for activating the function for setting up a local conference.

Only available in SIP workpoints.

Auto answer

Checkbox for activating auto answer.

Only available in SIP workpoints.

Phone Lock

Checkbox for activating phone lock function.

Only available in SIP workpoints.

NOTE: The default setting of this function on the OpenStage phone is set to true.
For SW Version< V3,the phone lock function is not available (nor visible),as opposed to versions V3 onwards,where it is possible to control the feature's availability (can also be controlled by WBM).
If the phone lock option is unchecked in the phone's Web Based Management (WBM) it' s impossible to lock the phone.

NOTE: Please refer to Phone lock function at Section 7.1.16.3, ""Locked Local Functions" Tab".Keep in mind the following options:
- If the Phone lock function is enabled at both tabs,the phone lock is not possible and the option is grayed out.
- If both checkboxes are unchecked,the phone lock is not possible nor visible in the menu.
- If the function is enabled for the Mobile user but unchecked at the '' Availability'' tab,the phone lock is not possible nor visible in the menu.
- Finally, the phone lock is possible only if the function is checked solely at the ''Availability tab''.

PC Interface

Checkbox for enabling the interface between the PC and the device.

WAP browser on APM/DSM

Checkbox for activating the WAP browser on the optiPoint application module/display module.

Only available in SIP workpoints.

LDAP on APM/DSM

Checkbox for activating the LDAP function on the optiPoint application module/display module.

Only available in SIP workpoints.

Telephony on APM/DSM

Checkbox for activating the telephony function on the optiPoint application module/display module.

Only available in SIP workpoints.

Voice recognition on APM/DSM

Checkbox for activating the voice recognition function (voice dialing) on the optiPoint application module/display module.

Only available in SIP workpoints.

Speed dial on APM/DSM

Checkbox for activating the speed-dialing function on the optiPoint application module/display module with a Java midlet.

Only available in SIP workpoints.

ENB on APM/DSM

Checkbox for activating the electronic notebook on the optiPoint application module/display module.

Only available in SIP workpoints.

Call park

Checkbox for activating the function for parking calls.

Only available in SIP workpoints.

Call join

Checkbox for activating the function for joining calls.

The user can join the first party with the party he consulted, clearing down his own connection to both parties in the process.

Only available in SIP workpoints.

Group Pickup Beep

If this checkbox is activated, you will hear a beep when a call is waiting for a pickup group.

Blind Transfer

Checkbox for activating the feature "Blind Transfer".

The user can transfer the current call to another party without consultation.

Repertory Dial

Checkbox for activating the feature "Repertory Dial".

The user can select and insert special characters in the dialing sequence for to disconnect the call or activate a consultation hold or insert a pause.

Busy Lamp Flag (BLF)

Checkbox for activating the Busy Lamp Field (BLF).

For displaying the state of other internal phones, the BLF key can be configured. Each BLF key is assigned to the internal phone number of another phone. By means of the LED state, the user can determine whether the other phone is idle, ringing, or busy.

Direct Station Select (DSS)

Checkbox for activating Direct Station Select (DSS).

Apart from line keys, the user can also configure direct station selection (DSS) keys. A DSS key can be used to call an internal station directly, pick up calls for this station or forward calls directly to it.

CTI

Checkbox for activating the CTI interface.

Speakerphone mode activates automatically on the phone if the a CTI application (such as Outlook) is used to dial a number when Auto Answer is active. If Auto Answer is not active, the phone rings first and the user must press the loudspeaker key or lift the handset to set up the call. This setting also defines whether or not incoming calls are automatically accepted.

Line Overview

Checkbox for activating the line Ooverview.

To view the status of the lines, the user must change from the "My phone" tab to the "Overview" tab on the phone screen.

Feature Toggle

Checkbox for activating the feature "Feature Toggle".

The user can pick a programmable sensor key and program it as a feature toggle key for activating the "make line busy" and "stop hunt" functions. He can then use the programmable key to activate or deactivate the relevant OpenScape Voice function on the server for this phone.

Third Call Leg

Checkbox for activating the feature "Third Call Leg".

For Consultation call from second call: If the second call is the active call, the user can initiate a consultation call from it. During a consultation in the second call, the first call is parked and can only be unparked when the consultation or second call ends or these calls were connected.

Group Pickup

Checkbox for activating the feature "Group Pickup".

Enable Video Calls

Checkbox for enabling the feature "Video Call ".

Ext/Int Forwarding

Checkbox for enabling / disabling the External/Internal Forwarding.

7.1.4.5 "Server based features" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Server based features" Tab

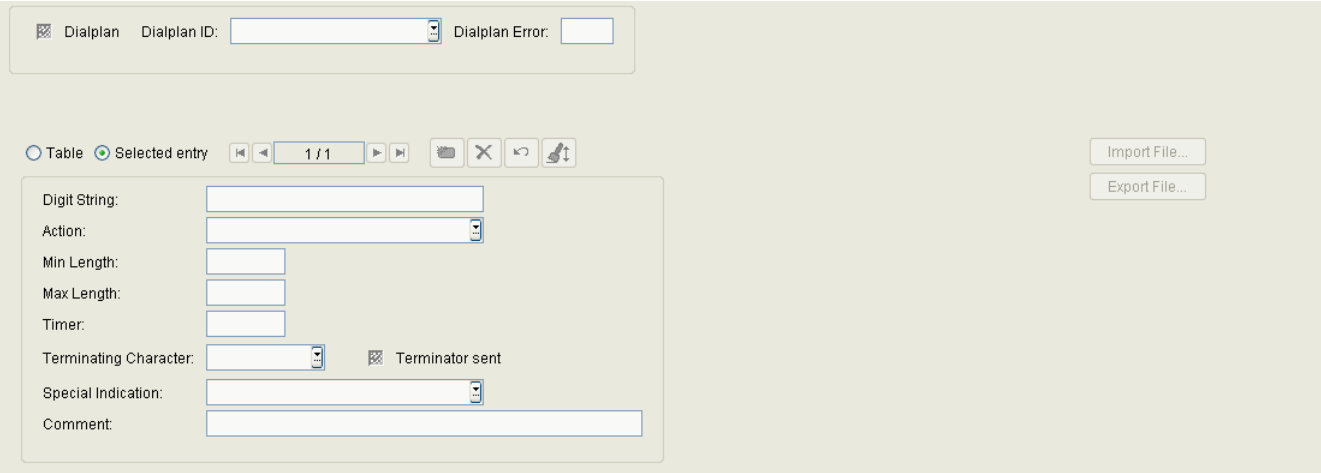


Support of Server based Features

If this checkbox is activated, server-based features on the device are enabled for the user.

7.1.4.6 "Dialplan" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Dialplan" Tab



Dialplan

Checkbox for activating the dial plan. The entries in this tab are interpreted if this checkbox is active.

Only available in SIP workpoints.

Dialplan ID

Name of the dial plan - must begin with a "!".

Value range: max. 14 alphanumeric characters.

Only available in SIP workpoints.

Dialplan Error

Specifies the dial plan entry that is faulty in the event of an error.

Value range: **1** ... **48**

Only available in SIP workpoints.

Digit String

Digit String Digit string for executing this action.

Only available in SIP workpoints.

Action

Action executed for this digit string.

Possible options:

- **-C- Action for digits**
- **-S- Send digits**

Only available in SIP workpoints.

Min Length

Minimum digit string length for digit string interpretation.

Only available in SIP workpoints.

Max Length

Maximum digit string length for digit string interpretation.

Only available in SIP workpoints.

Timer

Delay before the action is performed.

Value range: **1** ... **9** seconds.

Only available in SIP workpoints.

Terminating Character

Character that ends the digit string entered.

Possible options:

- **#**
- *

Only available in SIP workpoints.

Special Indication

Possible options:

- **-E- emergency call**
- **-b- bypass**

Only available in SIP workpoints.

Comment

Field for general information.

Only available in SIP workpoints.

Terminator sent

Displays whether the terminating character is included in the digit string.

Import File

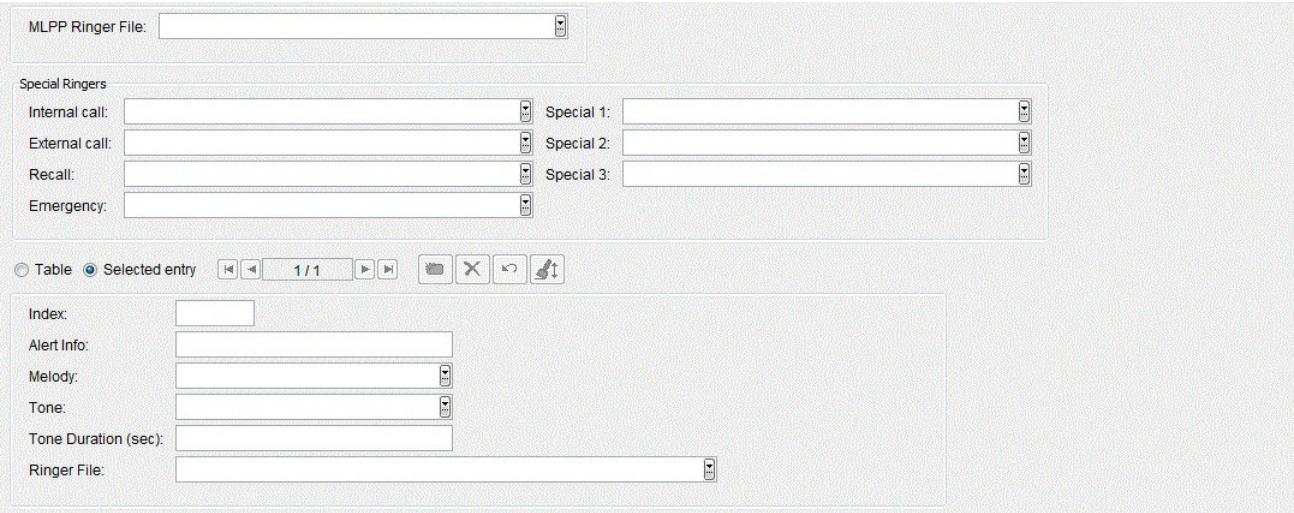
Imports a dialplan from a file in CSV format.

Export File

Exports a dialplan from a file in CSV format.

7.1.4.7 "Ringer Melody / Tone" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Ringer Melody / Tone" Tab



NOTE: A template for **Ringer Melody / Tone** can be created by searching for an IP Device with entries in **Ringer Melody / Tone** (empty entries are allowed as well). Use the action **Copy to Template** to create a template. There must be 15 entries, which may be empty.
This template can be modified, saved, and applied.

MLPP Ringer File

Ringtone file to be used for priority calls.

Special Ringers

Internal call

Default value : Bellcore-dr1

External call

Default value : Bellcore-dr2

Recall

Default value : Bellcore-dr3

Emergency

Default value : alert-emergency

Special 1

Special 2

Special 3

Index

Automatically generated index for the particular distinctive ringtones.

Alert Info

If the string specified here is identical with a special string which is sent to the phone in the SIP alert info header, the corresponding ringtone is used.

Only available in SIP workpoints.

Melody

Type of ring melody.

Possible options: **Melody 1** ... **Melody 8, Melody off**

Only available in SIP workpoints.

Tone

Ringtone sequence.

Possible options:

- **1**
  = 1 sec ON, 4 sec OFF
- **2**
  = 1 sec ON , 2 sec OFF

- **3**
  = 0,7 sec ON, 0,7 sec OFF , 0,7 sec ON, 3 sec OFF

Only available in SIP workpoints.

Tone Duration

Duration of the ringtone.

Value range: **1** ... **300** seconds.

Default: **60** seconds.

Only available in SIP workpoints.

Ringer File

Name of the audio file containing the ringtone.

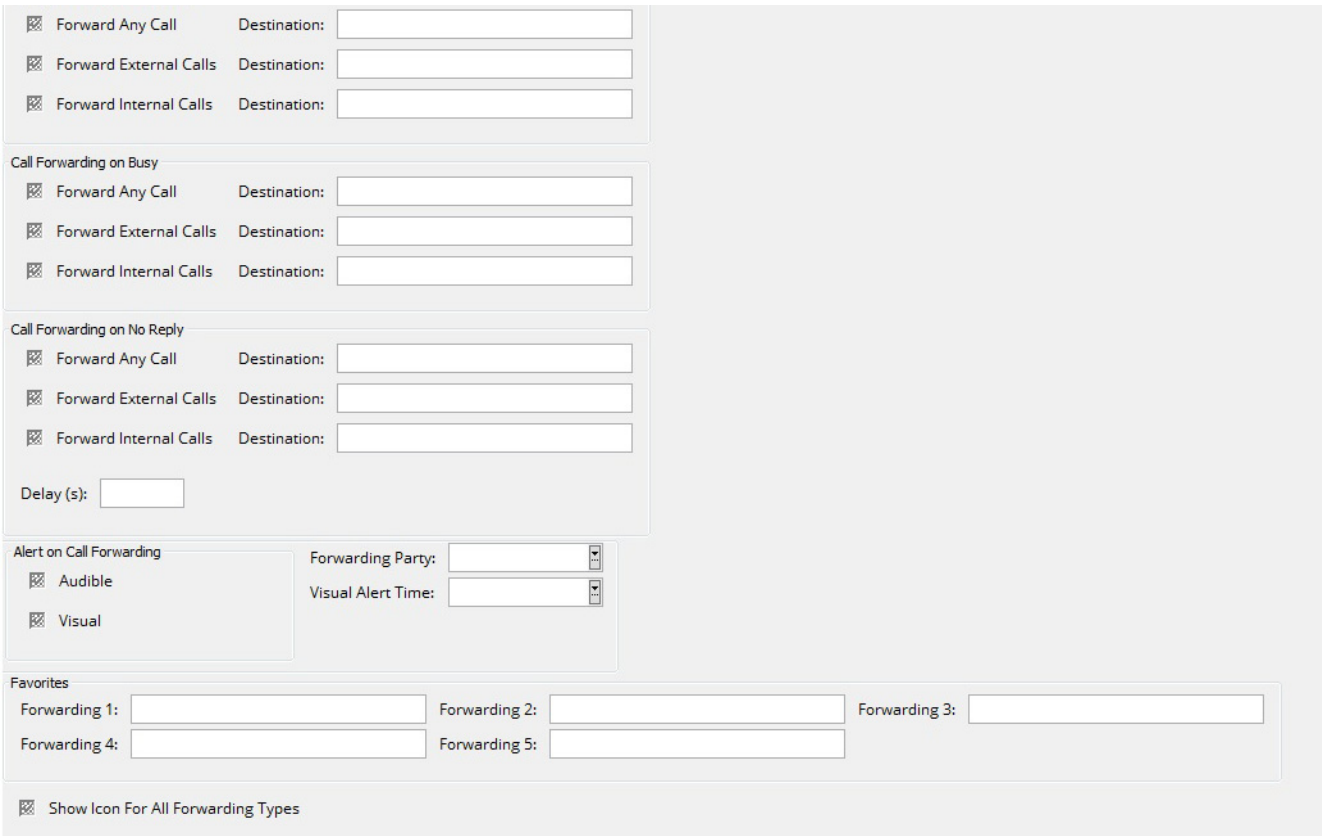
IMPORTANT: In order for a special ringer to be configured, then :

1. it's alert info (e.g. Bellcore-dr1) and
2. it's respective Ringer file (e.g. Harmonize.mp3) should be configured first.

These two configurations (special ringers & ringer melody table) cannot be performed in a single step.A new Alert Info and Special Ringer cannot be added at the same time in the Special Ringers table & the Distinctive Ringers table.Before a Special Ringer is configured, make sure it's Alert Info is already configured,
i.e. first configure Bellcore-dr1 in lower table, press **Save** and then configure this Alert Info in Special Ringers Internal Call & press **Save** again.

7.1.4.8 "Call Forwarding" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Call Forwarding" Tab



NOTE: The additional Call Forwarding settings (for external/internal) shall be available if the option "**Support of Server Based Features**" is enabled under **Call: Main Menu > Call: Main Menu >>IP Phone Configuration** > **Features**> **"Server based features" Tab**.
If that option is enabled, the CFNR delay timer is not configurable (greyed out).

Call Forwarding Unconditional

Forward Any Call

Checkbox for activating unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward External Calls

Checkbox for activating External Call Forwarding.

Destination:

Call number of the External Call Forwarding destination.

Forward Internal Calls

Checkbox for activating Internal Call Forwarding.

Destination:

Call number of the Internal Call Forwarding destination.

Call Forwarding on Busy

Forward Any Call

Checkbox for activating unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward External Calls

Checkbox for activating External Call Forwarding.

Destination:

Call number of the External Call Forwarding destination.

Forward Internal Calls

Checkbox for activating Internal Call Forwarding.

Destination:

Call number of the Internal Call Forwarding destination.

Call Forwarding on No Reply

Forward Any Call

Checkbox for activating Unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward External Calls

Checkbox for activating Unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward Internal Calls

Checkbox for activating Unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Delay (sec):

As soon as this time span has expired without the call being accepted, the call is forwarded.

Alert on Call Forwarding

Audible

Checkbox for activating an audible alert on the forwarding phone.

Visual

Checkbox for activating a visible alert on the forwarding phone.

Forwarding Party:

Select which forwarding party will be displayed when multiple forwarding is active.

Possible options:

- **Display first**
- **Display last**

Visual Alert Time:

When visual alert is active, the toast message is shown on the forwarding phone screen according to the set time. The toast message appears for 5 seconds by default. However, you can configure the visual alert’s appearing time from this field:

Possible values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **11**
- **12**
- **13**

- **14**
- **15**

NOTE: When you set the value to zero, the toast message will not appear at all.

NOTE: On HFA configured phones the toast message is only shown when the phone is configured with OpenScape 4000, not with OpenScape Business.

Favorites

Forwarding 1:

Forwarding 2:

Forwarding 3:

Forwarding 4:

Forwarding 5:

Show Icon For All Forwarding Types:

When enabled, the forwarding icon can be now shown in the main menu of the phone, in case **unconditional** forwarding, forward **on busy** or forward on **no reply** is active.

The user will get a visual indication in the main menu of the phone.

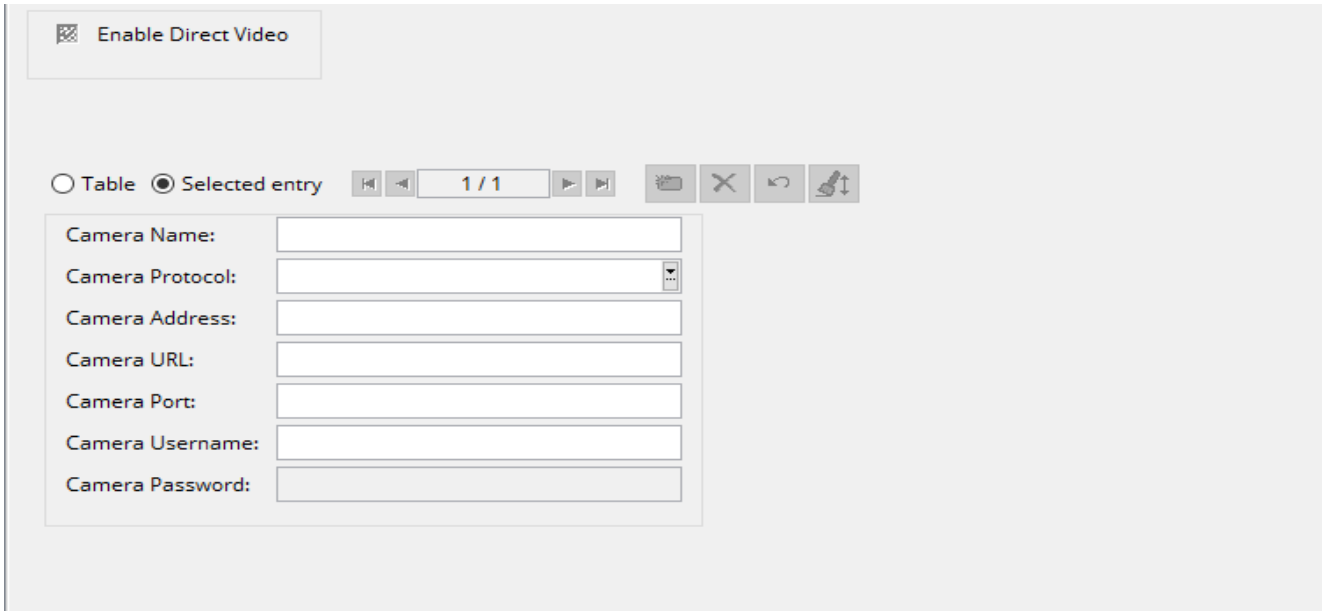
Disabled by default.

NOTE: Forwarding unconditional is not affected. No matter what the setting is, the phone will always display a forwarding icon and make keys LED turn on if call forwarding unconditional is activated.

NOTE: This flag is available only to CP200/205/400/600 HFA devices, SIP V1R3 version and higher.

7.1.4.9 "Direct Video" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Direct Video" Tab.



Enable Direct Video

Checkbox for activating Direct Video

Camera Name:

Freely selectable name for the camera (can be custom name or alphanumeric).

Camera Protocol:

Protocol to transmit video, RTSP and HTTP.

Camera Address:

IP address or DNS name of the video server (e.g. 10.10.10.1 or mycamera.local.net).

Camera URL:

URL path of the camera, e.g. /videoapi/stream/

Camera Port:

Target the port at the server.

Camera Username:

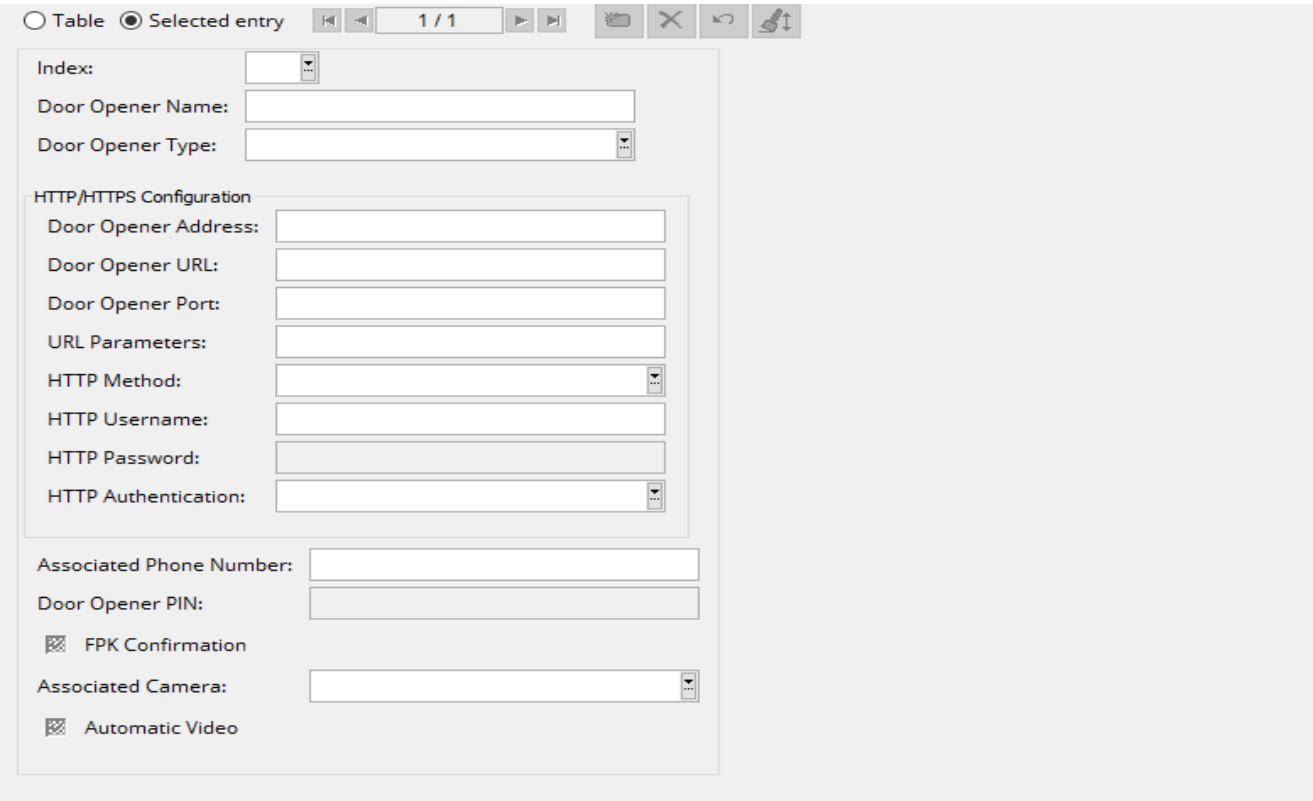
Enter a username for the camera.

Camera Password:

Enter a password for the camera.

7.1.4.10 "Door Opener" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "Door Opener" Tab



Door Opener Name:

Freely selectable name for the door opener (can be custom name or alphanumeric).

Door Opener Type:

Select a control method for the door opener from the drop down list. The available options are:

- **Disabled**
- **Call to open door**
- **HTTP request to open door**
- **HTTPS request to open door**

HTTP/HTTPS Configuration

Door Opener Address:

IP address or DNS name of the door opener server e.g. 10.10.10.1 or mydoor.local.net.

Door Opener URL:

URL path of the door opener, e.g. /door1/opencommand/.

Door Opener Port:

Target the port at the server.

URL Parameters:

Parameters inside the URL path, e.g. user=name&auth=123456.

HTTP Method:

Possible options:

- GET
- POST

HTTP Username:

HTTP Password:

HTTP Authentication:

Possible options:

- Basic
- Digest

Door Opener PIN:

The PIN to open the door, same PIN as the one configured at Door opener device.

FPK Confirmation:

Checkbox for confirming the key to open the door.

Associated Camera:

The name of the associated camera.

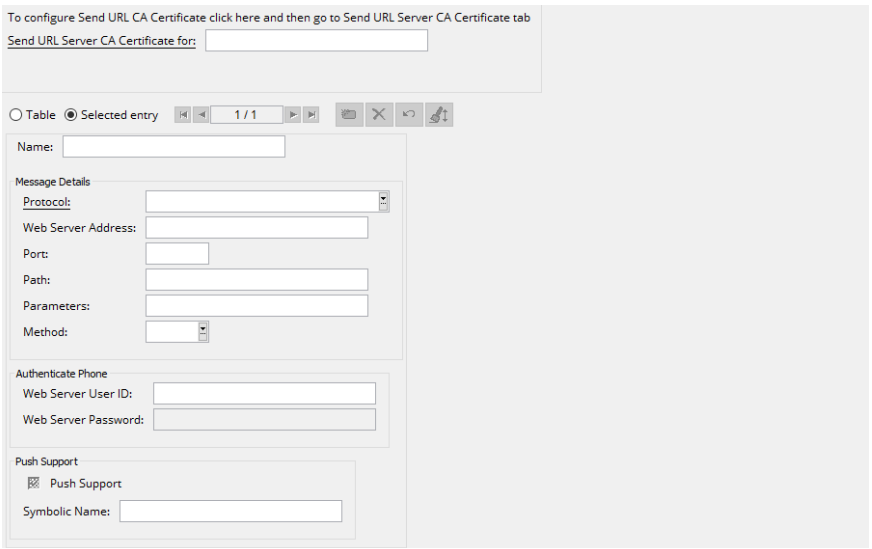
Automatic Video:

When someone rings at the door, the phone rings.

If the call is from door opener with associated camera and the Automatic Door Video option is enabled, the user can see the camera stream before answering the call by pressing "Show video" SRK or related Camera FPK button. Otherwise, video image is shown automatically only after answering the call.
If the call is from door opener with associated camera and the Automatic Door Video option is disabled, the user can see the camera stream either before of after answering the call by pressing "Show video" SRK or related Camera FPK button.

7.1.4.11 "SendURL for HFA" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Features > "SendURL for HFA" Tab



Send URL Server CA Certificate:

Click on the link and then navigate to "Send URL Server CA Certificate" Tab to configure SendURL CA Certificate.

Name:

Freely selectable name used as a key index to store particular configuration in the database. It will be presented to the user during key programming.

Protocol:

Protocol of Web Server.

Possible options:

- **HTTP**
- **HTTPS**

Web ServerAddress:

Host name, domain name, or IP address of Web Server.

Port:

Port number of web server. If the port is null, the fully qualified URL will not include the port element.

Path:

Directory path and name of the program of the web page.

Examples: **servlet/IppGenericServlet** or **webpage/checkin.xml**

The path should have a slash at the beginning and no slash at the end. If the slash at the beginning is missing, a slash will be automatically inserted. If there is an additional slash at the end, it will be automatically removed. The slashes in the path should be forward slashes (’/’). If backslashes (’\’) are used instead, the web server may not find the appropriate program or web page.

Parameters:

Null, one, or more parameter-value pairs in the format “<parameter>=<value>”, with each pair separated by an ampersand (“&”), e. g. **parameter1=value1&parameter2=value2**. A comma (“,”) is not used as a separator because it could be part of the key or value. If the key or value contains an ampersand, it must be replaced by “&”.

The question mark will be automatically added between the path and the parameters. If there is a question mark at the beginning of the parameters, it will be automatically stripped off.

Method:

Method to be used.

Possible options:

- **Get**
- **Post**

Web Server User ID:

User identity known by the server. This information is used for phone authentication by the server.

Web Server Password:

Password known by the server. It is used for phone authentication by the server.

Push Support:

Enables or disables push support.

Symbolic Name:

Symbolic name known by the server. It is used for phone authentication by the server.

7.1.5 Quality of Service

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Quality of Service

This area features the following components:

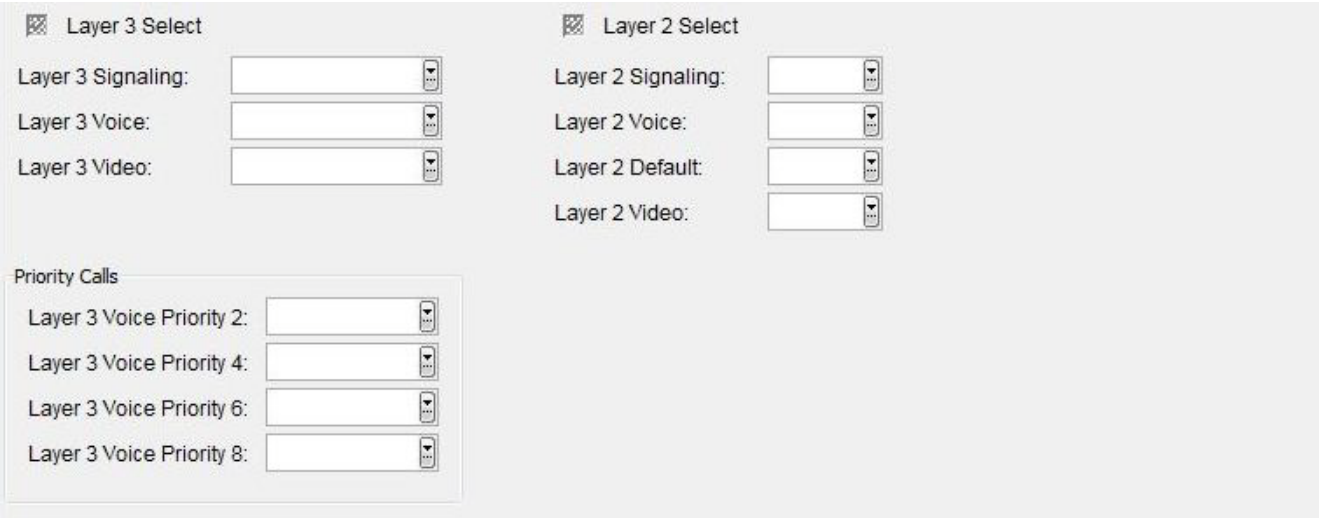
- General Data
- Possible Action Buttons
- "QoS Parameter" Tab
- "QoS Parameter (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.5.1 "QoS Parameter" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Quality of Service > "QoS Parameter" Tab



Layer 3 Select

Checkbox for activating the QoS layer 3 configuration.

Layer 3 Signaling:

Layer 3 value for call signaling.

Value range fo optiPoint HFA workpoints (lower than optiPoint HFA V5R5) and optiPoint SIP workpoints in SIP5 or lower: **0** **63**

Possible values for optiPoint SIP6 or higher and optiPoint HFA V5R5 or higher:

- **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**

Possible values for 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**

Possible values for 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 Voice:

Layer 3 value for voice transmission.

> ***NOTE:*** QoS Layer 3 voice transmission can also be set via LLDP-MED (Link Layer Discovery Protocol). If so, the value can not be changed via DLS.

Value range for optiPoint HFA workpoints (except optiPoint HFA V5R5 and higher) and optiPoint SIP workpoints with SIP5 or lower: **0** **63**

Possible values for optiPoint HFA from V5R5 and optiPoint SIP6 or higher:

- **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**

Possible values for 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**

Values for 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 Video:

Layer 3 value for video.

Possible values

- **0=BE**
- **10=AF11**
- **12=AF12**
- **14=AF13**
- **18=AF21**
- **20=AF22**
- **22=AF23**
- **26=AF31**
- **28=AF32**
- **30=AF33**
- **34=AF41 (Default value)**
- **36=AF42**
- **38=AF43**
- **46=EF**
- **56=CS7**
- **24=CS3**
- **32=CS4**
- **40=CS5**

Layer 2 Select

Checkbox for activating the QoS layer 2 configuration.

Layer 2 Signaling:

Layer 2 value for call signaling.

Value range: **0** ... **7**

Layer 2 Voice:

NOTE: QoS Layer 2 voice transmission can also be set via LLDP-MED (Link Layer Discovery Protocol). If so, the value can not be changed via DLS.

Layer 2 value for voice transmission.

Value range: **0** ... **7**

Layer 2 Default:

Default for the layer 2 value.

Value range: **0** ... **7**

Layer 2 video:

Default for the layer 2 value.

Value range: **0** ... **7**

Priority Calls

Layer 3 Voice Priority 2

Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 4

Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 6

Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 8

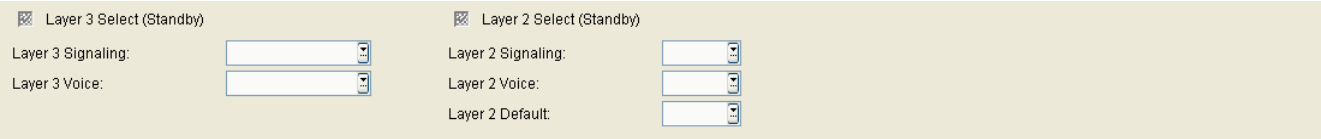
Layer 3 value for voice at priority calls.

Value range: **DSCP00** ... **DSCP63**

7.1.5.2 "QoS Parameter (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Quality of Service > "QoS Parameter (Standby)" Tab

NOTE: This "standby" data is used when the "home" data for the "QoS Parameter" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



Layer 3 Select (Standby)

Checkbox for activating the QoS layer 3 configuration.

Layer 3 Signaling:

Layer 3 value for call signaling.

Value range for optiPoint HFA workpoints (lower than optiPoint HFA V5R5) and optiPoint SIP workpoints in SIP5 or lower: **0** **63**

Possible values for optiPoint SIP6 or higher and optiPoint HFA V5R5 or higher:

- **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 Voice:

NOTE: QoS Layer 3 voice transmission can also be set via LLDP-MED (Link Layer Discovery Protocol). If so, the value can not be changed via DLS.

Layer 3 value for voice transmission.

Value range for HFA workpoints and SIP workpoints in SIP5 or lower: **0** **63**

Possible values for optiPoint SIP6 or higher and optiPoint HFA V5R5 or higher:

- **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**

Possible values for 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 Select (Standby)

Checkbox for activating the QoS layer 2 configuration.

Layer 2 Signaling:

Layer 2 value for call signaling.

Value range: **0** ... **7**

Layer 2 Voice:

NOTE: QoS Layer 2 voice transmission can also be set via LLDP-MED (Link Layer Discovery Protocol). If so, the value can not be changed via DLS.

Layer 2 value for voice transmission.

Value range: **0** ... **7**

Layer 2 Default:

Default for the layer 2 value.

Value range: **0** ... **7**

7.1.6 QoS Data Collection

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > QoS Data Collection

NOTE: This function is not available in the onboard variants of DLS on OpenScape Voice systems.

This area features the following components:

- General Data
- Possible Action Buttons
- "Server Data" Tab
- "Report Settings" Tab
- "Threshold Values" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.6.1 "Server Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > QoS Data Collection > "Server Data" Tab



Send Traps to QCU

Checkbox for activating the function that sends errors to the QCU.

QCU Home Address:

IP address or host name of the server that collects the QDC data.

QCU Host Port Number:

Port number for the server that collects the QDC data.

Send Traps to SNMP Manager

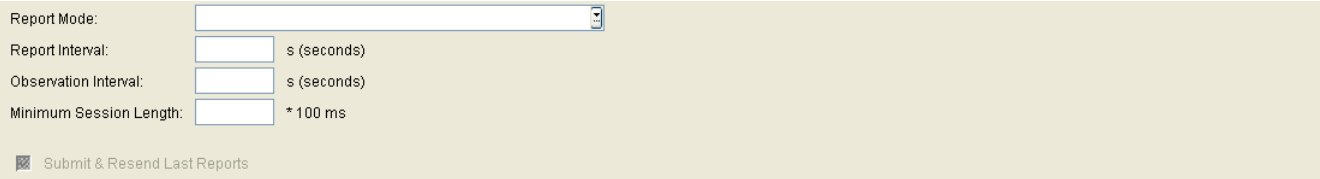
Checkbox for activating the function that sends errors to the SNMP Manager.

QDC Trap Password

Password of the server collecting the QDC traps.

7.1.6.2 "Report Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > QoS Data Collection > "Report Settings" Tab



Report Mode:

Specifies when a report should be generated.

Possible options:

- **EOS Threshold exceeded**
  At the end of the connection that exceeded the threshold.
- **EOR Threshold exceeded**
  At the end of the reporting interval that exceeded the threshold.
- **EOS (End of Session)**
  At the end of the connection.
- **EOR (End or Report Interval)**
  At the end of the reporting interval.

Report Interval:

Time interval in which a QoS report is sent.

Value range: **0** ... **3600** seconds.

Observation Interval:

Time interval in which threshold violation is checked.

Value range: **0** ... **5000** seconds.

Minimum Session Length:

A QoS report is sent if a session (for example, a call) undershoots this minimum.

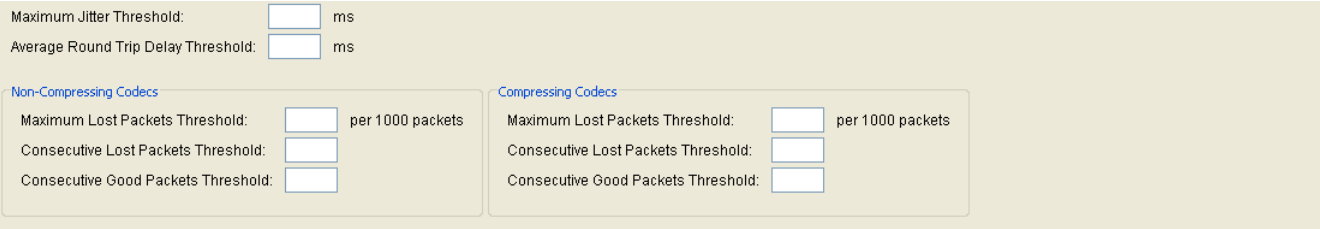
Value range: **0** ... **5000** (x 100 ms).

Submit & Resend Last Reports

When this checkbox is enabled, the workpoint resends the last QoS reports.

7.1.6.3 "Threshold Values" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > QoS Data Collection > "Threshold Values" Tab



Maximum Jitter Threshold:

Maximum threshold in milliseconds for runtime fluctuations during data transmission to trigger a report.

Value range: **0** ... **255** ms.

Default: **15**

Average Round Trip Delay Threshold:

Average response time (in milliseconds) for signal transmission.

Default: **100**

Non-Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during uncompressed transmission.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during uncompressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during uncompressed transmission.

Value range: **0** ... **255**

Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during compressed transmission.

Value range: **0** ... **255**

7.1.7 Security Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings

This area features the following components:

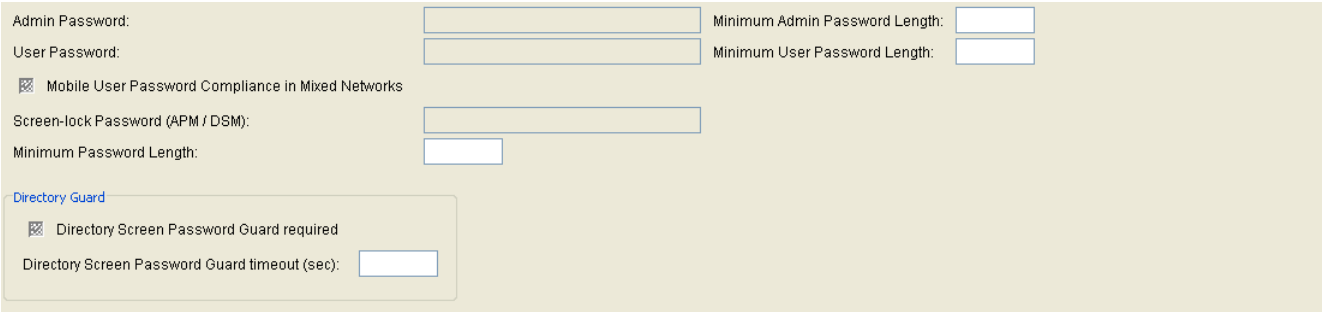
- General Data
- Possible Action Buttons
- "Passwords" Tab
- "Additional Password Policy Settings" Tab
- "Enabled Services (NW Stack)" Tab
- "WBM Server Certificate" Tab
- "HTTPS Server CA Certificates" Tab
- "OCSR 1 Server CA Certificate" Tab
- "OCSR 2 Server CA Certificate" Tab
- "OCSR 1 Signature CA Certificate" Tab
- "OCSR 2 Signature CA Certificate" Tab
- "Authentication Policy" Tab
- "HTTPS Client Certificates" Tab
- "DLS Connectivity" Tab
- "SCEP" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.7.1 "Passwords" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "Passwords" Tab



Admin Password:

Password for access to the workpoint's administration area.

The admin password cannot be read from a device.

> ***NOTE:*** UI does not intend to indicate the existence of the password but only to set it up.
> .When you set it to the device, the device sets it in its database but DLS cannot know that since an error message is displayed when you try to read it for confirmation.
> You can set the admin password but you cannot be aware of the admin password that the device has.

User Password:

Password for access to the workpoint's user area.

The user password for an OpenStage V3.0 or higher,can be forced to be changed by the phone user on its next use.

The user password cannot be read from a device.

> ***NOTE:*** Although it can be managed by DLS there is no possibility to know the user password value or acknowledge password changes realized over WBM pages or directly over the physical device itself.

Mobile User Password Compliance in Mixed Networks

If this option is selected and a mobile user password is changed on an OpenStage V3.0 phone or higher, the password will also be available on older phone types or software versions. If not selected, the mobile user password on prior phones or software versions may be replaced by the standard password "000000".

Only available for SIP phones.

Screen-lock Password (DSM/APM):

Password for canceling the display lock on the optiPoint 410 Application Module/Display Module.

Only applicable if an Application Module/Display Module is used.

Minimum Password Length:

Minimum number of characters that an administration or user password must contain. Only available if the current object is a HFA telephone (old version) because in this case both passwords are the same length.

Minimum Admin Password Length:

Minimum number of characters that an administration password must contain. Only available if the current object is an SIP telephone.

Minimum User Password Length:

Minimum number of characters that a user password must contain. Only available if the current object is an SIP telephone.

Directory Guard

Directory Screen Password Guard required

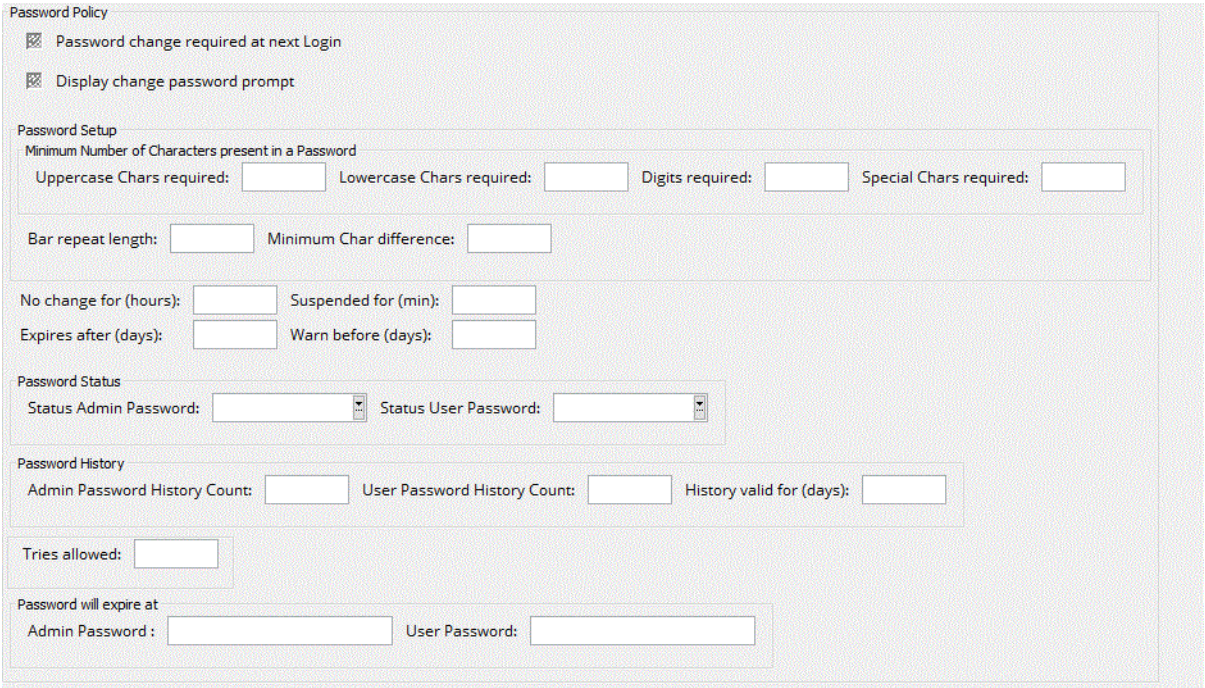
This checkbox activates password protection for the directory screen. To use the screen, you must enter the standard user password.

Directory Screen Password Guard timeout (sec)

Password protection is activated when the length of time specified here expires. After this time, you must enter the password to continue using the screen.

7.1.7.2 "Additional Password Policy Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "Additional Password Policy Settings" Tab



Password Policy

Password change required at next Login

When activated, the user will be required to change the password on its next use in order to access the user menu (including web pages) or to disengage phone lock. The setting will remain as active until the phone user changes the password or the change password request is cancelled.

Display change password prompt

When activated, the user will be prompted to change the password immediately. The prompt can be cleared but it comes back later until the phone user changes the password.

Password Setup

Minimum Number of Characters present in a password

Uppercase Chars required

Number of capital letters the password must contain.

Value range: **0** ... **24**

0 = no check

Lowercase Chars required

Number of lower case letters the password must contain.

Value range: **0** ... **24**

0 = no check

Digits required

Number of digits the password must contain.

Value range: **0** ... **24**

0 = no check

Special Chars required

Number of special characters (`-=[];'#\,./!"£$%^&*()_+{}:@~|<>?) the password must contain.

Value range: **0** ... **24**

0 = no check

Bar repeat length

Maximum number of identical characters the password may contain.

Value range: **0, 2** ... **24**

0 = no check

Minimum Char difference

The number of characters that must change when the password is changed.

Value range: **0** ... **24**

0 = no check

No change for (hours):

Minimum waiting period before an existing password can be updated, in hours.

Suspended for (min):

When the maximum number of retries has been exceeded, the password is suspended for the period specified here, in minutes.

Expires after (days)

Maximum validity period of a password.

Value range: **0** ... **999**

0 = no check.

Warn before (days)

When the password will expire within the number of days specified here, the user is notified.

Value range: **0** ... **999**

0 = no check

Password Status

Status Admin Password

Status of the admin password.

Possible Options:

- **Active**
- **Suspended**
- **Disabled**

Status User Password

Status of the user password.

Possible Options:

- **Active**

- **Suspended**
- **Disabled**

Password History

Admin Password History Count:

Minimum number of admin passwords to store in the history file. New passwords must not match any password in the history file.

Value range: **0** … **99**

User Password History Count:

Minimum number of user passwords to store in the history file. New passwords must not match any password in the history file.

Value range: **0** … **99**

History valid for (days):

Time interval during which a password may not be selected again as a new password by the phone, as it remains in the password history for this time.

Allowed failed logins

Number of attempts a user is given to enter the password before access will be suspended.

Value range: **2** … **5**

Default value: **3**

Password will expire at

Admin Password

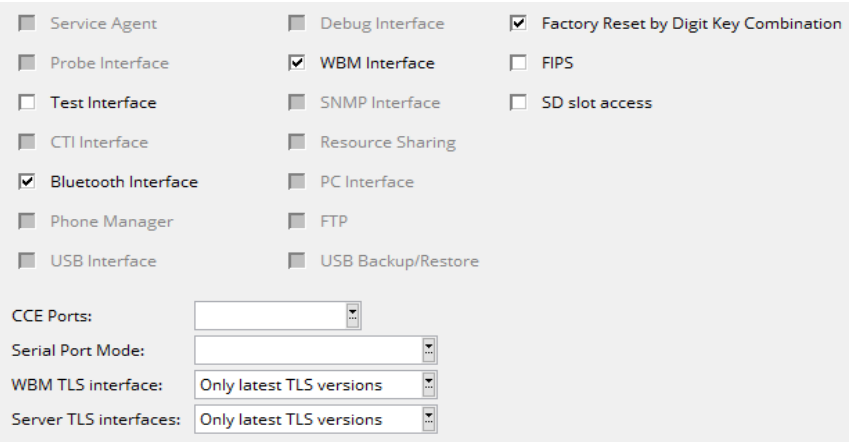
Time and date of admin password expiry.

User Password

Time and date of user password expiry.

7.1.7.3 "Enabled Services (NW Stack)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "Enabled Services (NW Stack)" Tab



Service Agent

Checkbox for activating and deactivating the service agent.

Probe Interface

Checkbox for activating and deactivating the probe interface.

Test Interface

Checkbox for activating and deactivating the test interface.

CTI Interface

Checkbox for activating and deactivating the CTI interface.

Bluetooth Interface

This checkbox is activated if you want to activate the Bluetooth interface on OpenStage telephones.

Phone Manager

This checkbox is activated if you want to enable the interface between OpenStage telephones and Phone Manager.

Phone Manager is a PC application for managing particular phone data.

USB Interface

If this checkbox is activated, the USB interface on the IP device can be accessed (OpenStage 60 and OpenStage 80 only).

Debug Interface

Checkbox for activating and deactivating the debug interface.

WBM Interface

Checkbox for activating and deactivating the WBM interface.

NOTE: Please note that if you deactivate the WBM interface, you can only reactivate it via DLS as the WBM is no longer available for this.

SNMP Interface

Checkbox for activating and deactivating the SNMP interface (network management function).

Resource Sharing

Checkbox for activating and deactivating resource sharing (shared use of mouse and keyboard).

PC Interface

This checkbox is activated if you want to use the PC interface.

FTP

This checkbox is activated if you want to enable the FTP interface on the OpenStage telephone.

USB Backup/Restore

If this checkbox is activated, IP device data (such as, the screensaver) can be backed up/restored over the USB interface. Codec's Backup/Restore feature must be called directly on the relevant IP device (OpenStage 60 and OpenStage 80 only).

Factory Reset by Digit Key Combination

When activated, the factory reset by means of a digit key combination is enabled.

FIPS

Checkbox for enabling / disabling workpoint-booting in FIPS mode.

Checkbox is disabled by default.

NOTE: A phone restart is required.

SD slot access

Controls if the SD card slot is disabled to prevent any use of an SD card.Chekbox for disabling/enabling access to the SD card - added for **WE4** (CP600) phones.

Checkbox is enabled by default.

CEE Ports

Enable or disable the Comms Channel Extender (CCE) ports for both TCP (port 65531) and UDP (port 65530) access.

Possible Options:

- **Disable all**
- **Enable all**
- **TCP only**
- **UDP only**

Serial Port Mode

Shows password protection mode for the serial port.

Possible Options

- **Password required**
- **No Password**
- **Unavailable**

WBM TLS interface:

Possible options:

- **Only latest TLS versions** (default value)
- **All TLS versions**

WBM TLS interface:

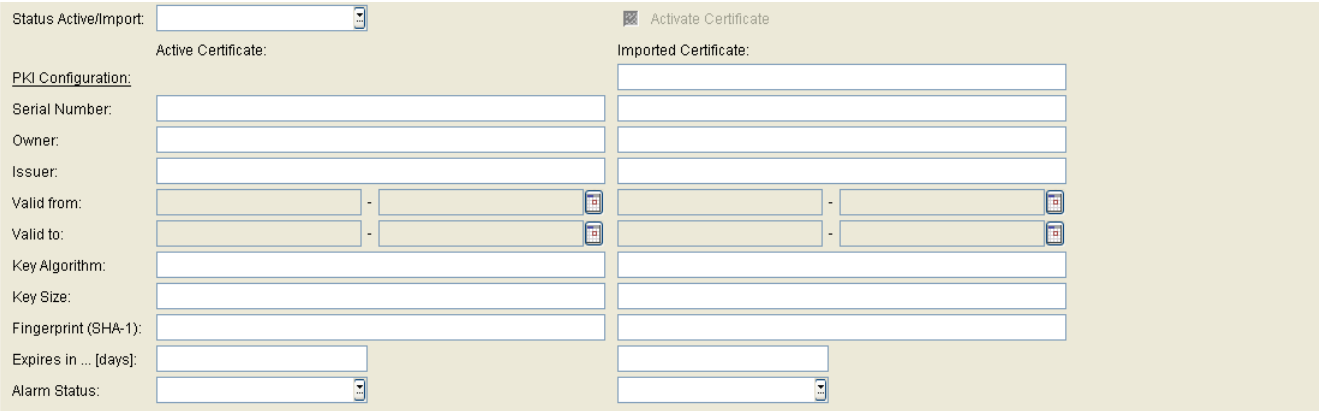
Possible options:

- **Only latest TLS versions** (default value)
- **All TLS versions**

7.1.7.4 "WBM Server Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "WBM Server Certificate" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".



This tab allows to import or remove the Web Based Management (WBM) SSL Server Certificate. This certificate is used for the device WBM interface (e.g. for device administration via a web browser). When no certificate is present, the factory default WBM SSL Certificate is used.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm for the active or imported certificate (display only).

Key Size

Key size for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the active or imported certificate (display only).

Expires in ... [days]

The certificate validity will expire in the number of days specified (display only).

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status for the active or imported certificate (display only).

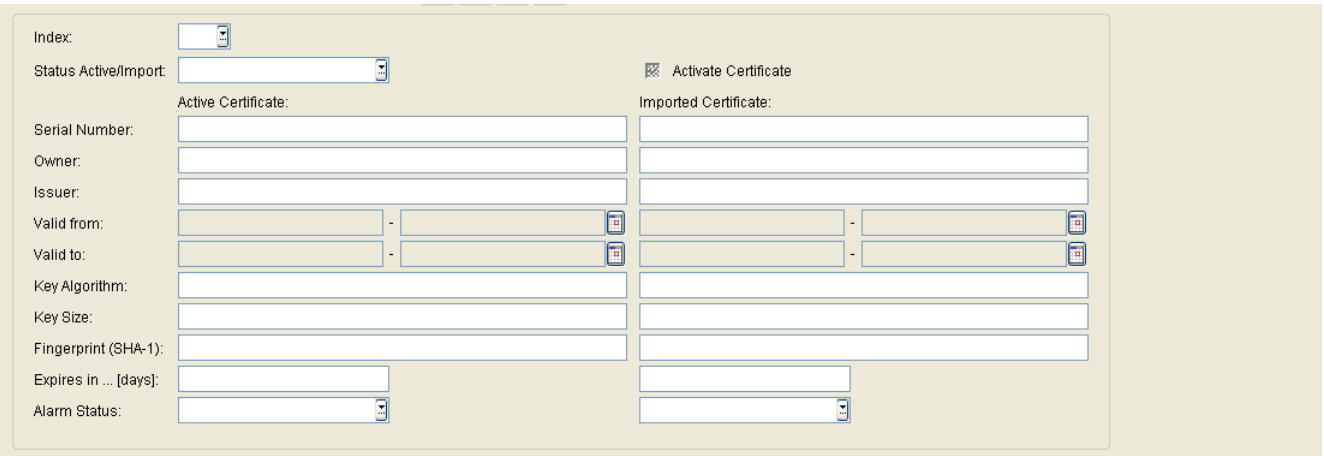
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.7.5 "HTTPS Server CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "HTTPS Server CA Certificates" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".



This tab allows to import or remove server CA (Certificate Authority) Certificates to authenticate the HTTPS server used for file transfer. Up to two certificates can be imported to the device. See Section 6.3.5, "HTTPS Server Configuration". For further configuration, see Section 7.1.7.10, ""Authentication Policy" Tab".

Index

Index of the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm .

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

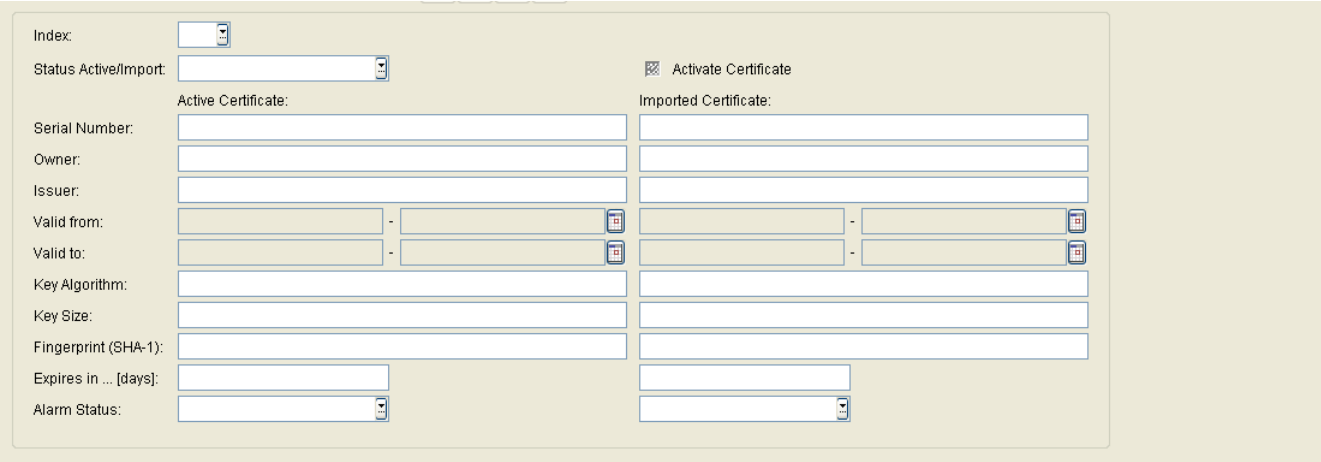
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.7.6 "OCSR 1 Server CA Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "OCSR 1 Server CA Certificate" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

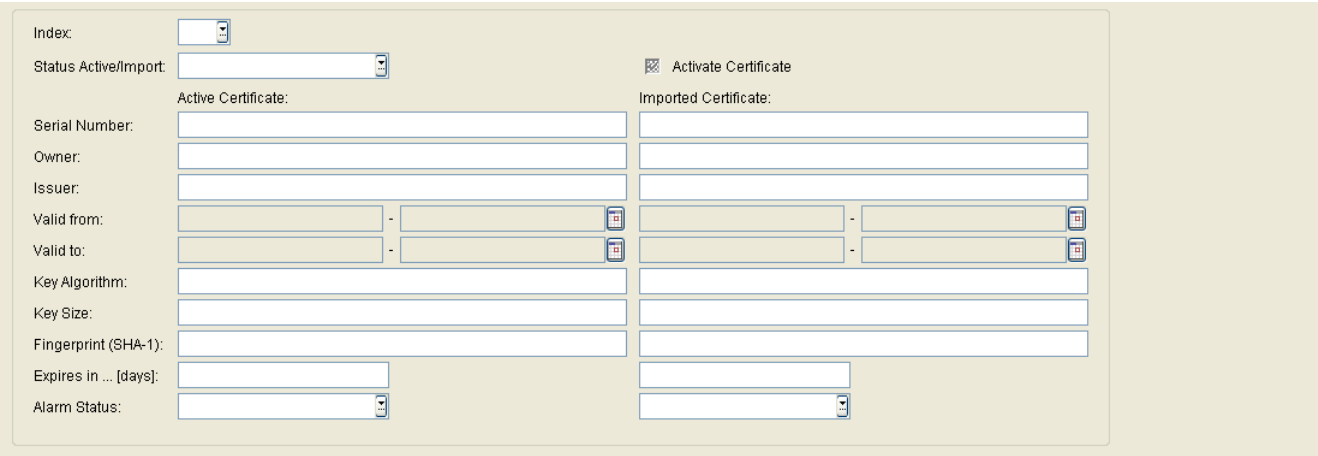


For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab".

7.1.7.7 "OCSR 2 Server CA Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "OCSR 2 Server CA Certificate" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

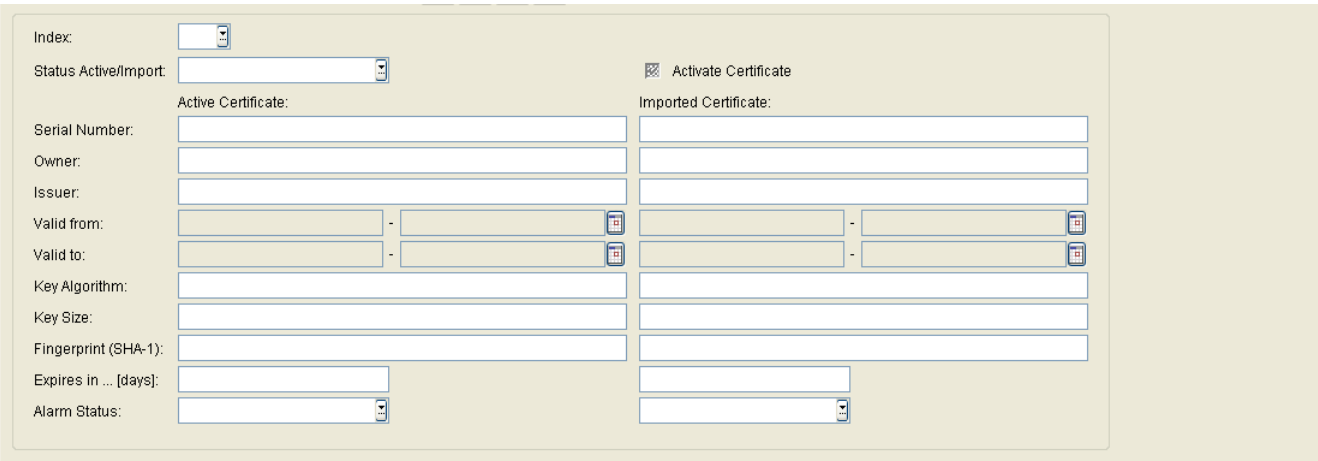


For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab".

7.1.7.8 "OCSR 1 Signature CA Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "OCSR 1 Signature CA Certificate" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

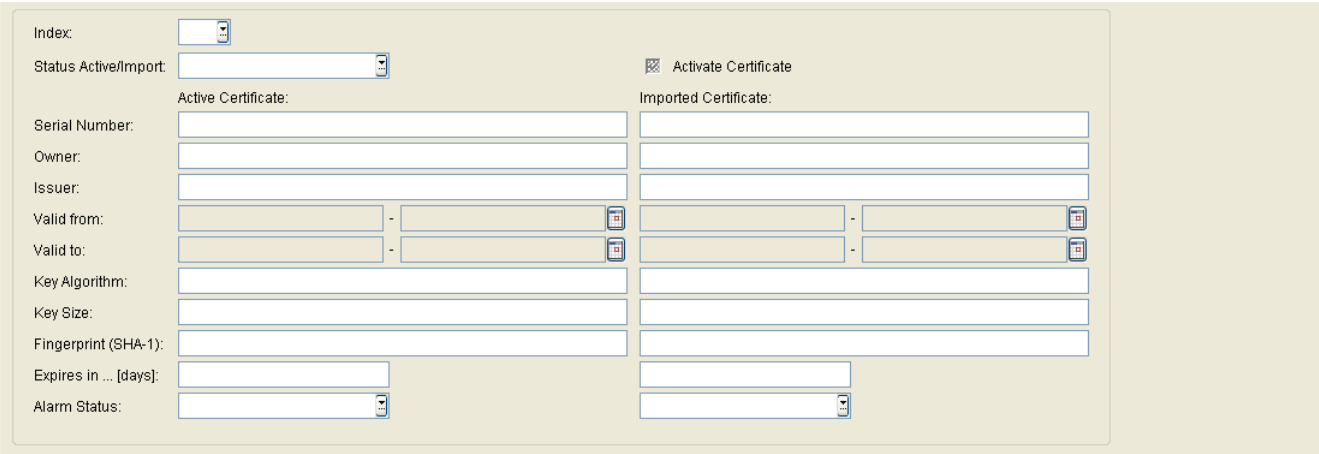


For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab"

7.1.7.9 "OCSR 2 Signature CA Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "OCSR 2 Signature CA Certificate" Tab

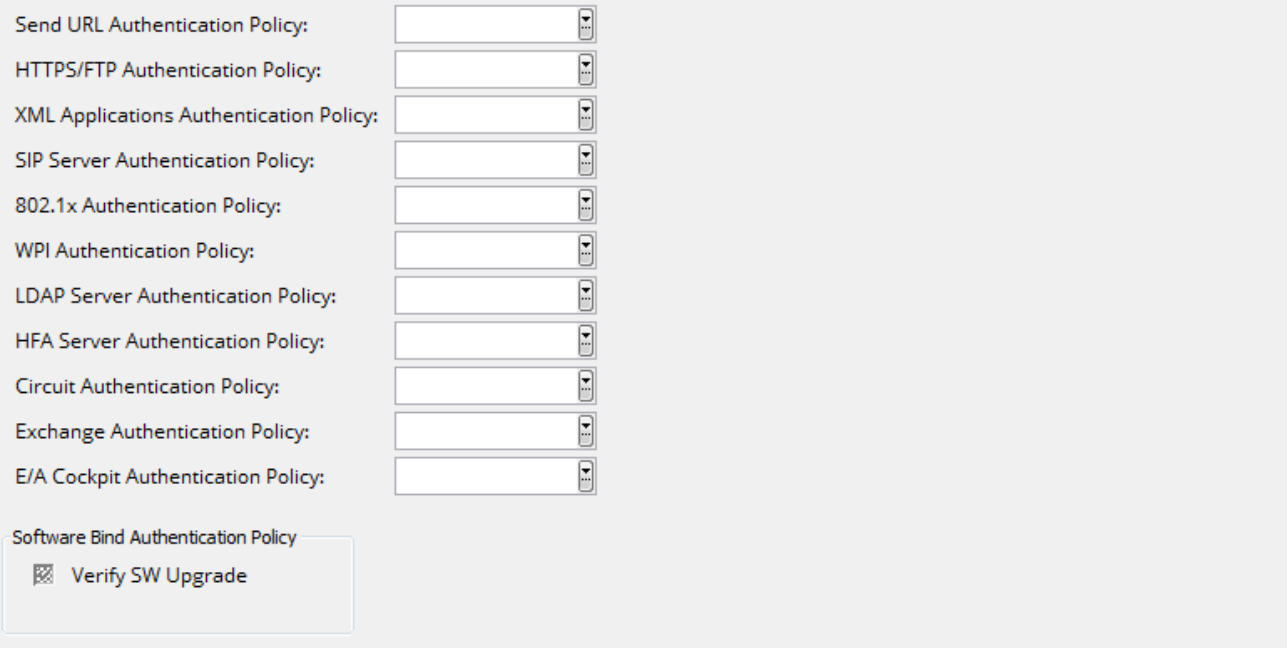
NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".



For parameter descriptions, please see Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab"

7.1.7.10 "Authentication Policy" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "Authentication Policy" Tab



This tab allows to define how secure connections are authenticated by the device.

Send URL Authentication Policy:

Authentication of the Send URL HTTPS Server is defined here, please see Section 7.1.19.3, ""Send URL Server CA Certificate" Tab".

Possible values:

- **None**
- **Trusted**
- **Full**

HTTPS/FTP Authentication Policy

Authentication of the HTTPS Server for file transfer is defined here,please see Section 6.3.5, "HTTPS Server Configuration" and Section 7.1.7.5, ""HTTPS Server CA Certificates" Tab".

Possible values:

- **None**

- **Trusted**
- **Full**

XML Applications Authentication Policy:

Authentication of the XML Application Server is defined here, please see Section 7.1.14.5, ""CA Certificates" Tab".

Possible values:

- **None**
- **Trusted**
- **Full**

SIP Server Authentication Policy

Authentication of the SIP Server (for TLS transport only) is defined here, please see Section 7.1.22, "Signaling and Payload Encryption (SPE)".

Possible values:

- **None**
- **Trusted**
- **Full**

Valid only for OpenStage V3.0 onwards.

802.1x Authentication Policy

Authentication of the 802.1x Server is defined here, please see Section 7.1.23, "IEEE 802.1x".

Possible values:

- **None**
- **Trusted**
- **Full**

Valid for OpenStage V3.0 onwards.

WPI Authentication Policy

Authentication of the DLS Work Point Interface (WPI) is defined here, please see Section 6.9.1, ""Secure mode" Tab".

Possible values:

- **Trusted**
- **Full**

Valid for OpenStage V3.0 onwards.

LDAP Server Authentication Policy

Possible values:

- **None**
- **Trusted**
- **Full**

HFA Server Authentication Policy

Possible values:

- **None**
- **Trusted**
- **Full**

Circuit Authentication Policy

Circuit Authentication Policy is device based in terms of mobility.

Possible values:

- **None (default)**
- **Trusted**
- **Full**

Exchange Authentication Policy

Exchange Authentication Policy is device based in terms of mobility.

Possible values:

- **None**
- **Trusted**
- **Full**

E/A Cockpit Authentication Policy

Allow for root CA upload and authentication policy (device based in terms of mobility) setting to be changeable on the CP phone.

Possible values:

- **None**
- **Trusted**
- **Full**

OpenScape UC Authentication Policy

Allow for root CA upload and authentication policy (device based in terms of mobility) setting to be changeable on the CP phone.

Possible values:

- **None**
- **Trusted**
- **Full**

Software Bind Authentication Policy

Verify SW Upgrade

Checkbox to enable/disable the SW authentication check.This checkbox is enabled by default.

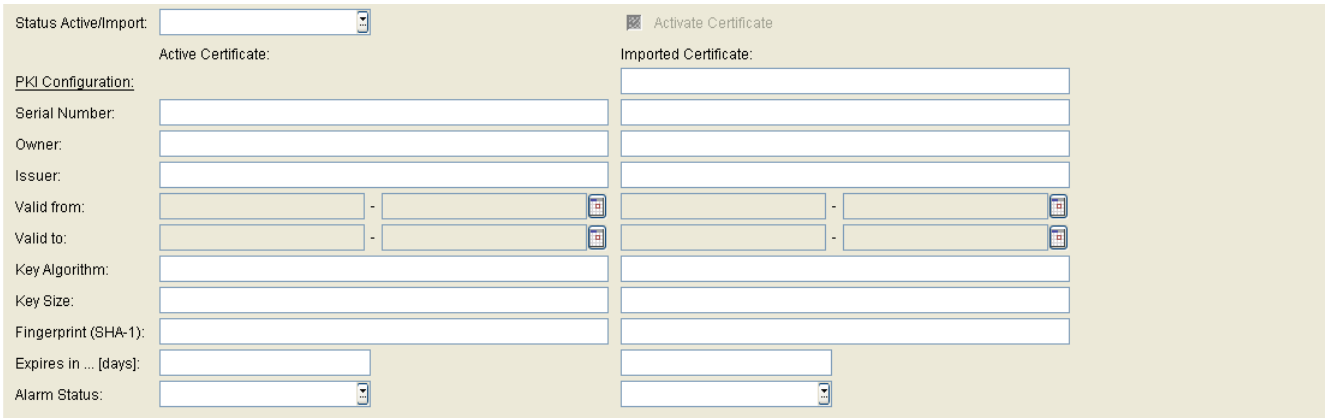
When activated, an authentication check will be done prior to the new bind being burnt to flash and the upgrade being completed.

If not activated, an authentication check will not take place. Regardless of the correct signature, new software can be loaded to the phone.(e.g. downgrade scenarios)

7.1.7.11 "HTTPS Client Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "HTTPS Client Certificates" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".



This tab allows to import or remove one client certificate for authentication of the device against the HTTPS server used for file transfer. This is required if the HTTPS server is configured for mutual authentication.

For parameter descriptions, please see Section 7.1.7.4, ""WBM Server Certificate" Tab"

7.1.7.12 "DLS Connectivity" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > IP Phone Configuration > Security Settings > "DLS Connectivity" Tab



Secure mode required

If this checkbox is activated, mutual authentication is enabled for the DLS and the IP Device.The authentication process (bootstrap) begins the next time the IP Device registers at the DLS or is scanned.

This checkbox is disabled by default.

PIN Mode:

Possible options:

- **No PIN**
  Access data is sent unencrypted to the IP Device.
- **Default PIN**
  A standard PIN is used for several IP Devices. This is generated automatically by the DLS (see Section 6.9.1, ""Secure mode" Tab").
- **Individual PIN**
  An individual PIN is created for the selected IP Device.

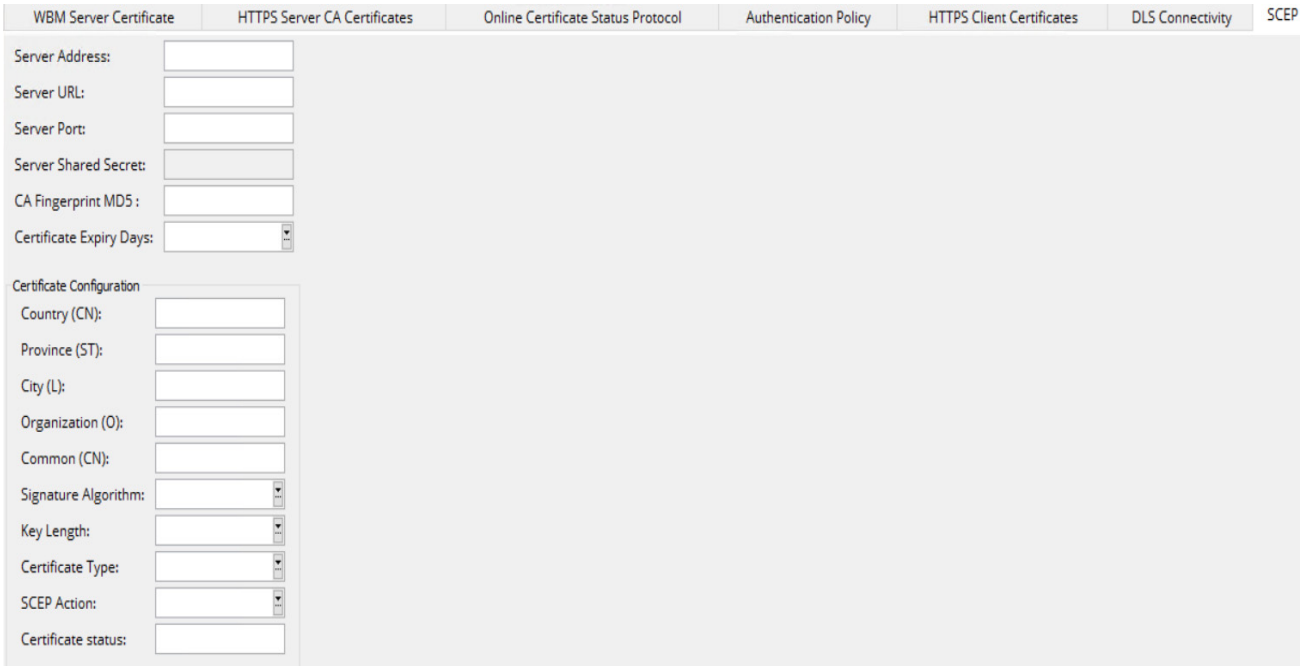
7.1.7.13 "SCEP" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > IP Phone Configuration > Security Settings > "SCEP" Tab

SCEP (Simple Certificate Enrollment Protocol) is a certificate deployment protocol that allows automatic provisioning and renewal of certificates.

NOTE: In case of SCEP server change or replacement, phone certificates deployed by the previous SCEP must be deleted before deployment from the new SCEP server.

NOTE: In case the pending certificate was approved by SCEP admin, phone admin should re-request the certificate enrollment to launch the deployment.



Server Address

IP address of SCEP server.

Server URL

URL of SCEP server.

Server Port

Port of SCEP server.

Server Shared Secret

SCEP shared secret.

CA Fingerprint MD5

CA fingerprint MD5 of SCEP.

Certificate Expiry Days

Number of days before certificate expiry.

Certificate Configuration

Country (CN)

Country of residence.

Province (ST)

Province of residence.

City (L)

City of residence.

Organization (O)

Name of the organization.

Common (CN)

Common name.

Signature Algorithm

sha256 or **sha512**

Key Length

Certificate key length.

Certificate Type

Type of certificate (interface) that should be deployed.

SCEP Action

Type of action that should be performed:

- **None**
- **Enroll**
- **Renew**
- **Delete**
- **Cancel pending**
- **Assign existing cert**

Certificate Status

Status of SCEP certificate.

7.1.8 Telephony

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Telephony

This area features the following components:

- General Data
- Possible Action Buttons
- "Telephony" Tab
- "Phone Location" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.8.1 "Telephony" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Telephony > "Telephony" Tab



Emergency Number:

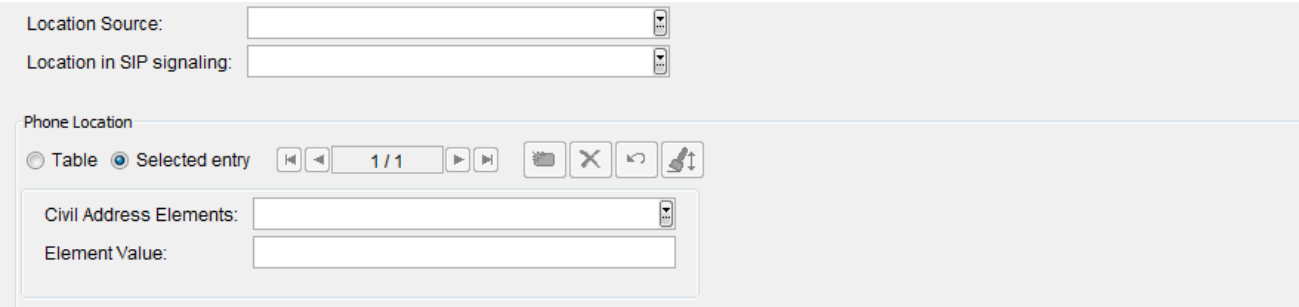
Contains the phone number that can be dialed in an emergency.

Location Identifier Number:

Contains an identification number for unique location identification. This number can be used, for example, to pinpoint the **origin** of an emergency call.

7.1.8.2 "Phone Location" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Telephony > "Phone Location" Tab



DLS manages to import location data to one or more devices by editing manually the location data or applying a location data template to a set of devices.

> ***NOTE:*** The location data configured in device profiles will not be applied to devices which have LLDP-MED location.

Location Source:

Possible options:

- **unknown/not set**
- **LLDP-MED**
- **DLS**

Default value: **unknown/not set**

Location in SIP signaling:

Possible options:

- **Signalled**
  Include location information in appropriate SIP messages
- **Not Signalled**
  Do not include location information in any SIP messages but allow such information to be configured

Default value: **Signalled**

Phone Location

Civil Address Elements:

Possible options:

- **Country**
- **State**
- **County**
- **Incorporated Municipality**
- **Unincorporated Municipality**
- **Neighborhood Community**
- **Street**
- **Leading Street Direction**
- **Trailing Street Direction**
- **Street Type Suffix**
- **Address Number**
- **Address Number Suffix**
- **Landmark Name**
- **Additional Location Information**
- **Business name**
- **Postal Code**
- **Building**
- **Unit**
- **Floor**
- **Room**
- **Place Type**
- **Postal Community name**
- **Post Office Box**
- **Seat**

Element Value:

Appropriate value according to specific civil address elements:

- **Country**
  The name of a country represented by its two-letter ISO 3166-1 English country 536 alpha-2 code elements in capital ASCII letters
  e.g. **US – United States**
- **State**
  The name of a state or state equivalent, represented by the two-letter abbreviation. A state is a primary governmental division of the United States
  e.g. **VA – Virginia**, **WA – Washington**, **GU – Guam**
- **County**
  The name of a country represented by its two-letter ISO 3166-1 English country 536 alpha-2 code elements in capital ASCII letters
  e.g. **US – United States**
- **Incorporated Municipality**
  The name of the incorporated municipality or other general-purpose local governmental unit (if any) where the address is located
  e.g. Haleyville, Chicago, Tamp
- **Unincorporated Municipality**
  The name of an unincorporated community either within an incorporated municipality or in an unincorporated portion of a county, where the address is located. The area must have a definite boundary
  e.g. Manhattan (borough of New York City)
- **Neighborhood Community**
  The name of an unincorporated neighborhood, subdivision or area, either within an incorporated municipality or in an unincorporated portion of a county, where the address is located. The area does not have to have definite boundaries
  e.g. Cypress Meadows Subdivision
- **Street**
  The element of the complete street name that identifies the particular street
  e.g. "Fairfax" in North Fairfax Avenue
- **Leading Street Direction**
  A word preceding the street name that indicates the direction taken by the street from an arbitrary starting point or line, or the sector where it is located
  (e.g. "N" (North) in N Fairfax Drive)
- **Trailing Street Direction**
  A word following the street name that indicates the direction taken by the street from an arbitrary starting point or line, or the sector where it is located
  (e.g. "E" (East) in Seventh St E)

- **Street Type Suffix**
  A word or phrase that follows the street name element and identifies a type of thoroughfare in a complete street name
  (e.g. "Avenue" in North Fairfax Avenue, "Street" in E Street)
- **Address Number**
  The numeric identifier of a location along a thoroughfare or within a defined community
  (e.g. 119 in 119 1/2 Elm)
- **Address Number Suffix**
  An extension of the address number that follows it and further identifies a location along a thoroughfare or within a defined are
  (e.g. "1/2" in 119 1/2 Elm Street)
- **Landmark Name**
  The name by which a prominent feature is publicly known
  (e.g. Empire State Building, Ohio State University)
- **Additional Location Information**
  A part of a building or sub address that is not a building, floor, unit, room, or seat
  (e.g. Concourse B, Corridor 5)
- **Business name**
  Business name (residence and office occupant)
  (e.g. **SEN**)
- **Postal Code**
  A system of 5-digit codes that identifies the individual USPS Post Office or metropolitan area delivery station associated with an address, which may optionally be enhanced by four additional digits that identify a specific range of USPS delivery addresses
  (e.g. 02109 (ZIP Code for Boston, MA))
- **Building**
  One among a group of buildings that have the same address number and street name
  (e.g. "Terminal 3" in John F. Kennedy International Airport)
- **Unit**
  A group or suite of rooms within a building that are under common ownership or tenancy, typically having a common primary entrance
  (e.g. Suite 220)
- **Floor**
  A floor, story, or level within a building
  (e.g. Floor 5)
- **Room**
  A single room within a building
  (e.g. "Room 450F" in 1440 Market St)
- **Place Type**
  The type of place identified by the address
  (e.g. Airport, arena, bank, hospital, hotel)

- **Postal Community name**
  The name of the post office from which mail is delivered to the address, or another city name for that ZIP Code that is recognized in the USPS City State file
  e.g. Stanton (a post office name in KY)
- **Post Office Box**
  Post office box (P.O. box)
  e.g. **U40**
- **Seat**
  A place where a person might sit within a building
  e.g. Desk , workstation, or a cubicle in an open-plan office

7.1.9 Small Remote Site Redundancy

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Small Remote Site Redundancy

This area features the following components:

- General Data
- Possible Action Buttons
- "SRSR Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.9.1 "SRSR Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Small Remote Site Redundancy > "SRSR Settings" Tab



SRSR enabled:

Checkbox for activating small remote site redundancy.

Only available in HFA workpoints.

Automated Switchback:

Checkbox for activating the option for automatic switchback to the main system.

Only available in HFA workpoints.

Switch to Home Retry Count:

Specifies the number of attempts permitted when switching back to the main system.

Value range: **1** ... **255**

Only available in HFA workpoints.

Switch to Home Expiry Timeout:

Timeout for switchover to the main system.

Value range: **1** ... **255** seconds.

Only available in HFA workpoints.

Switch to Standby Retry Count:

Specifies the number of attempts permitted when switching back to the standby system.

Value range: **1** ... **255**

Only available in HFA workpoints.

Switch to Standby Expiry Timeout:

Timeout for switchover to the standby system.

Value range: **1** ... **255** seconds.

Only available in HFA workpoints.

TC_Test

TC_TEST Retry Count:

Specifies the number of positive attempts permitted when switching back to the main system.

Value range: **1** ... **255**

Only available in HFA workpoints.

TC_TEST Expiry Timeout:

Time for a renewed attempt to switch back to the main system.

Value range: **1** ... **255** seconds.

Only available in HFA workpoints.

7.1.10 Dialing Properties

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Dialing Properties

This area features the following components:

- General Data
- Possible Action Buttons
- "Dialing Properties" Tab
- "Canonical Dial Lookup" Tab
- "FAC Prefixes (Phone Log)" Tab

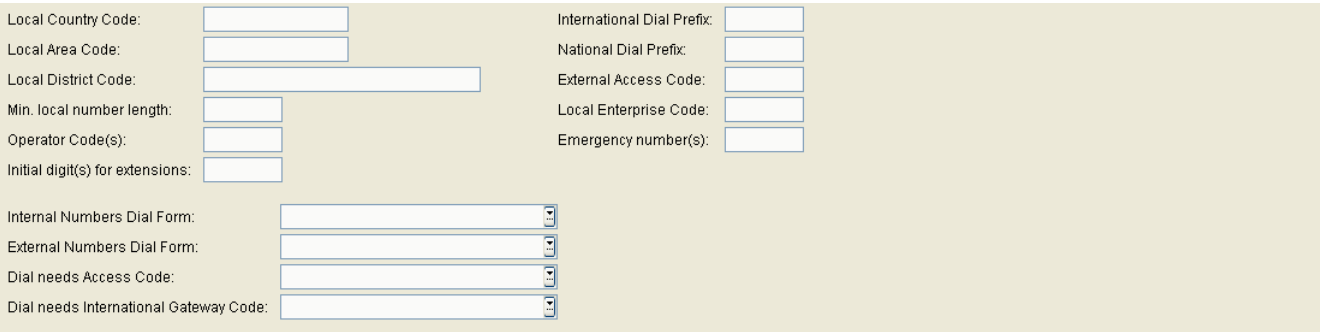
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.10.1 "Dialing Properties" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Dialing Properties > "Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

Local District Code:

Phone number of the company network.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Only available for devices in the optiPoint family.

Min. local number length

Minimum length for a local phone number, that is, within a prefix area.

Example: In Munich (prefix area 089), the minimum length is **6**.

Only available for devices in the OpenStage family.

Operator Code(s):

Number/code for connection to the operator.

Only available for devices in the OpenStage family.

Initial digit(s) for extensions

List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly.

Example: If, the extensions 3000-5999 are configured in the OpenScape Voice, each number will start with 3, 4, or 5. Therefore, the digits to be entered are **3, 4, 5**.

International Dial Prefix:

National prefix.

Format: Up to four digits.

Example: **00** in Germany.

National Dial Prefix:

International prefix.

Format: Up to five digits.

Example: **0** in Germany.

External Access Code:

Number for trunk seizure for an outgoing external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Local Enterprise Node:

Call number of the company network.

Example: **7007** for Unify Munich Hofmannstraße.

Only available for devices in the OpenStage family.

Emergency number(s):

One or more emergency numbers can be entered here.

Only available for devices in the OpenStage family.

Internal Numbers Dial Form:

Possible options:

- **Local Company Format**
- **Always Add Node**
- **Use External Number**

External Numbers Dial Form:

Possible options:

- **Local Public Format**
- **National Public Format**
- **International Public Format**

Dial needs Access Code:

Possible options:

- **Not used**
- **For External Number**

Dial needs International Gateway Code

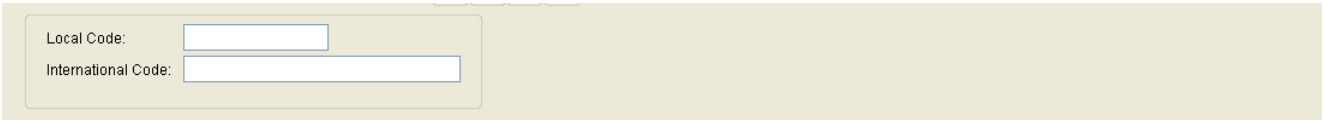
Possible options:

- **Use National Code**
- **Unchanged**

7.1.10.2 "Canonical Dial Lookup" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Dialing Properties > "Canonical Dial Lookup" Tab

This function transforms the entries in the first field ("Local Area Code") on the basis of a particular digit string as specified in the second field ("International Dial Code"). This digit string can be a national or international dial prefix, for example. This allows you to dial frequently used prefixes by entering just one digit.



Local Code

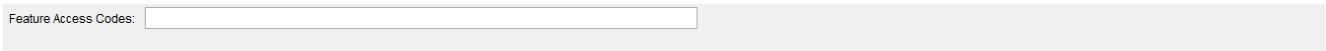
Digit or short digit string for dialing a particular prefix, for example.

International Code

Digit string, such as, a prefix, that is dialed at the beginning of the dialing operation using a particular digit.

7.1.10.3 "FAC Prefixes (Phone Log)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Dialing Properties > "FAC Prefixes (Phone Log)" Tab



Feature Access Codes

A comma separated list of FAC prefix codes considered that represent feature codes configured at the SIP server for abbreviated dialing.

7.1.11 Time Parameters

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Time Parameters

This area features the following components:

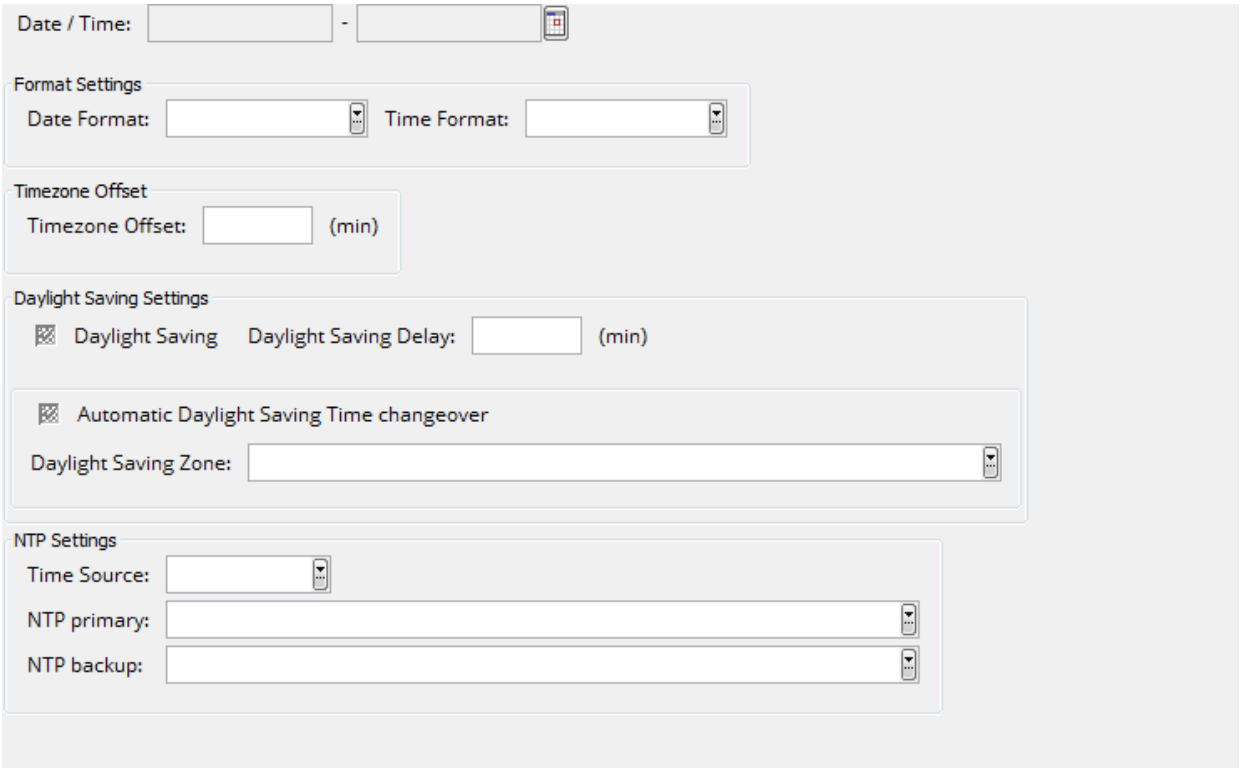
- General Data
- Possible Action Buttons
- "Time" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.11.1 "Time" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Time Parameters > "Time" Tab



NOTE: Available only for CP200/400/600, as well as HFA V1R1 and SIP V1R2 devices.

Date / Time:

Enter current date and time. Manual entry is only necessary if this information is not automatically transmitted (for example, PBX or DHCP server).

Format Settings

Date Format:

Format for date entry.Manual entry is only necessary if this information is not automatically transmitted by the communications system (for example, OpenScape Voice).

Possible options:

- **DD.MM.YY**
  Example: 05.10.06 for 5.10.2006

- **YY-MM-DD**

  Example: 06.10.05 for 5.10.2006

- **MM/DD/YY**

  Example: 10/05/06 for 5.10.2006

- **DD/MM/YY**

  Example: 05/10/06 for 5.10.2006

Time Format:

Time format.

Possible options:

- **24 hours**
- **12 hours**

Timezone Offset

Timezone Offset:

Time offset from UTC (Coordinated Universal Time) in minutes.

Value range: **-720** ... **720**

Examples: **60** (phone residing in Munich); **-480** (phone residing in Los Angeles, USA).

Daylight Saving Settings

Daylight Saving

Checkbox for activating the Daylight Saving function.

> ***NOTE:*** If **Automatic Daylight Saving Time changeover** is deactivated or no SNTP server is in use, you must manually switch between daylight saving and winter time. You must therefore change the status of the **Daylight Saving** checkbox twice a year. Pay particular attention to this when using this parameter in template data.

Daylight Saving Delay:

Difference in minutes to normal or winter time.

Value range: **0** ... **60**

Automatic Daylight Saving Time changeover:

If the checkbox is activated, the daylight saving time is toggled automatically according to the rule of the selecteddaylight saving zone. Start date and end date of daylight saving time are defined hereby.

> ***NOTE:*** With OpenStage phones, the **Daylight Saving** switch must be activated to enable automatic daylight saving time changeover.

Daylight Saving Zone:

Possible options:

- **Not set**
- **Australia 2007 (ACT, South Australia, Tasmania, Victoria)**
- **Australien 2007 (New South Wales)**
- **Australien (Western Australia)**
- **Australien 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)**
- **Brasilia**
- **Canada**
- **Canada (Newfoundland)**
- **Europe (PT, UK)**
- **Europe (AT, BE, HR, DK, FR, DE, HU, IT, LU, NL, NO, PL, SK, ES, SE, CH)**
- **Europe (FI)**
- **Mexico**
- **United States**

NTP Settings

Network devices must use at least two NTP servers to synchronize time.These will be organized as a primary source and a backup source. The primary will normally be used as the sole time source for the phone but in case of a failure of the primary source to provide a valid time then the phone will use the backup source. At start-up, the phone will always attempt to use the primary source and only revert to the backup if there is a failure. A failure of the primary source (or both sources) is to be logged in the security log. Other than that, the phone handles the time form its source as normal.

> ***NOTE:*** This function is only available to CP 200 / 400 / 600, for HFA V1R1 & SIP V1R2 and higher).

Time Source:

Source from where time information is adopted.

Possible options:

- **System**
  The time information is obtained from the communication platform.
- **SNTP**
  The time information comes from the SNTP server (if available).

NTP primary:

NTP primary server.

NTP backup:

NTP backup server.

7.1.12 Audio Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Audio Settings

This area features the following components:

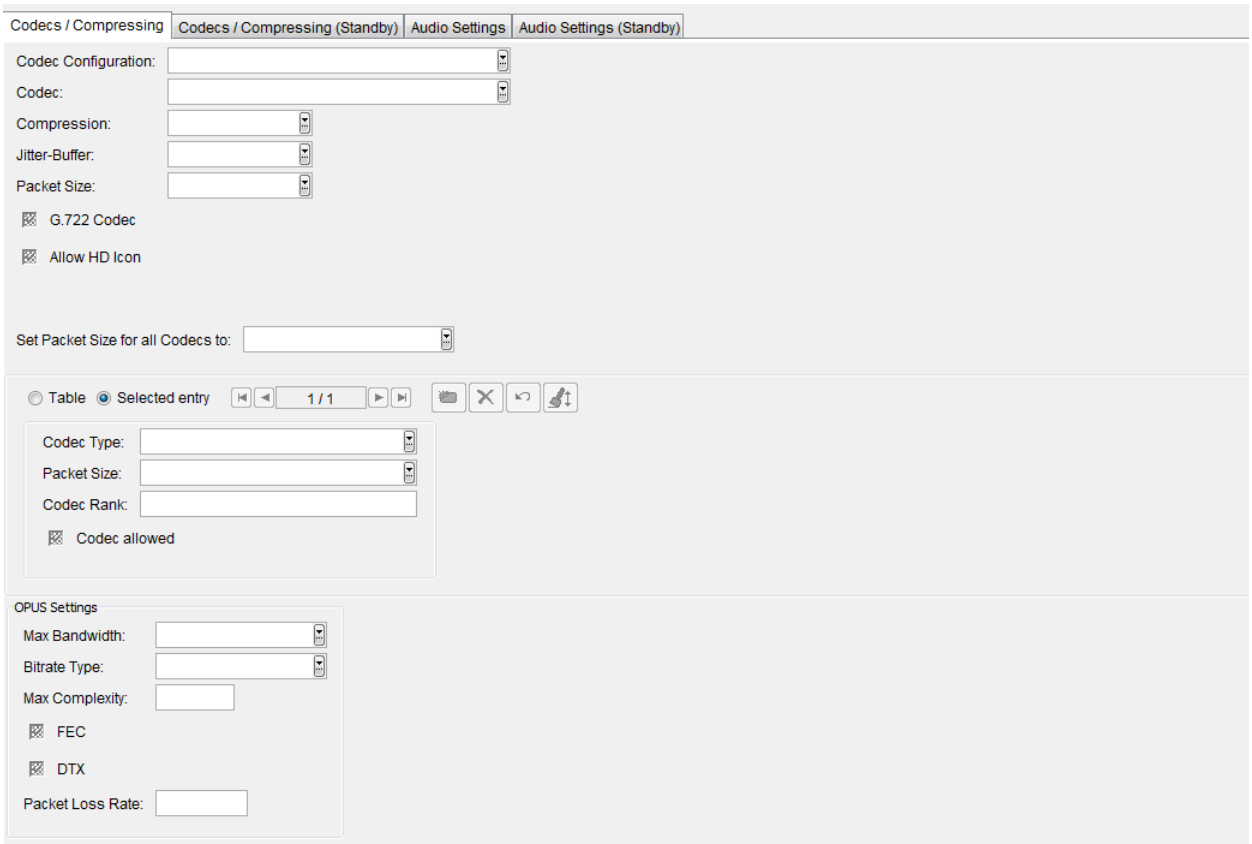
- General Data
- Possible Action Buttons
- "Codecs / Compressing" Tab
- "Codecs / Compressing (Standby)" Tab
- "Audio Settings" Tab
- "Audio Settings (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.12.1 "Codecs / Compressing" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Audio Settings > "Codecs / Compressing" Tab



The settings in the table are made for devices in the OpenStage family because the specification of multiple alternative codecs in these telephones is performed via a list of individual codecs.

Codec Configuration:

Set Codec for WLAN-Phones.

Possible options:

- **G.711 preferred (normal quality)**
- **G.723 preferred (low bandwidth)**
- **G.729 A/B preferred (low bandwidth)**
- **G.723 only (low bandwidth)**
- **G.729 A/B only (low bandwidth)**

Codec:

Audio transmission principle (codec) used.

Possible options:

- **Low bandwidth only**
  For the optiPoint 410/420/600 families.
- **High quality preferred**
  For the optiPoint 410/420/600 families.
- **Low bandwidth preferred**
  For the optiPoint 410/420/600 families.
- **G.711 Preferred**
  For the optiPoint 400 family.
- **G.723 Preferred**
  For the optiPoint 400 family.
- **G.723 Always**
  For the optiPoint 400 family.

Compression:

Compression procedure when the "LoBand" codec is selected.

Possible options:

- **G.723**
- **G.729**

Jitter Buffer:

Buffering duration (number of data packets).

Possible options:

- **Short**
  two packets
- **Long**
  six packets
- **Normal**
  four packets

Packet Size:

Possible options:

- **10mS**
- **20mS**
- **30mS**
- **Automatic**

Allow HD Icon:

Checkbox for activating the HD Audio icon via DLS.

This feature controls the showing of the HD Wideband Audio Icon.This function is enabled by default.

Set Packet Size for all Codecs to:

Set the Packet Size of all codecs to a common value.

Possible options:

- **10 mS**
- **20 mS**
- **30 mS**
- **60 mS**
- **Automatic**

Codec Type

Audio transmission principle (codec) used.

Possible options:

- **G.711**
- **G.729**
- **OPUS**

NOTE: Not supported by OpenStage & OpenScape Desk Phone IP devices.

Packet Size

Size of the packet used to send the audio data packages. The entry is in milliseconds.

- **Automatic**
- **10 ms**
- **20 ms**
- **30 ms**
- **40 ms**
- **60 mS**

Codec Rank

Each available codec is assigned a priority. This is used when negotiating codecs between two devices. Value range: A number between 1 and the number of available codecs.

Codec allowed

Codec usage can be explicitly allowed or denied.

OPUS Settings

NOTE: These settings don’t apply to OpenStage & OpenScape Desk Phone IP devices.

Max Bandwidth

Determines the bandwidth that OPUS encoder should operate on.

Possible values:

- **Narrowband**
- **Wideband**

Default value is set to Wideband.

Bitrate Type

Configures if OPUS encoder should work in VBR or CBR modes.

Possible values:

- **VBR - Variable Bitrate**
- **CBR - Constant Bitrate**

Default value is set to VBR.

Max Complexity

Determines the maximum computational complexity of codec. Lower values indicate worse quality. The complexity level of OPUS encoder can change to a lower value by SW on-the-fly according to CPU usage. It cannot exceed the value of max complexity item.

Possible values: **0...10**

Default value is set to 10.

FEC

Checkbox for including redundant payload data for better quality in lossy networks, but increases computational complexity and bandwidth.

This checkbox is disabled by default.

DTX

Checkbox determining whether to send empty payload frames during silence periods.

This checkbox is disabled by default.

Packet Loss Rate

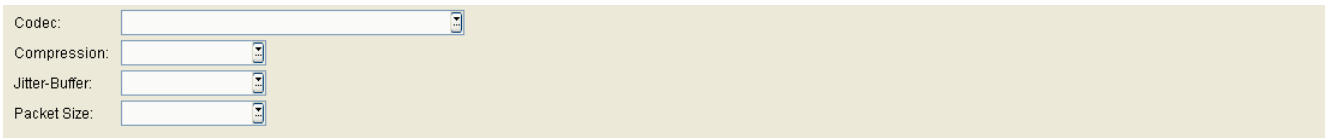
Packet loss percentage of the network as an input to encoder.

Possible values: **0...100**

Default value is set to 0.

7.1.12.2 "Codecs / Compressing (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Audio Settings > "Codecs / Compressing (Standby)" Tab



Codec:

Audio transmission principle (codec) used.

Possible options:

- **Low bandwidth only**
  For the optiPoint 410/420/600 families.
- **High quality preferred**
  For the optiPoint 410/420/600 families.
- **Low bandwidth preferred**
  For the optiPoint 410/420/600 families.
- **G.711 Preferred**
  For the optiPoint 400 family.
- **G.723 Preferred**
  For the optiPoint 400 family.
- **G.723 Always**
  For the optiPoint 400 family.

Compression:

Compression procedure when the "LoBand" codec is selected.

Possible options:

- **G.723**
- **G.729**

Jitter Buffer:

Buffering duration (number of data packets).

Possible options:

- **Short**
  two packets
- **Long**
  six packets
- **Normal**
  four packets

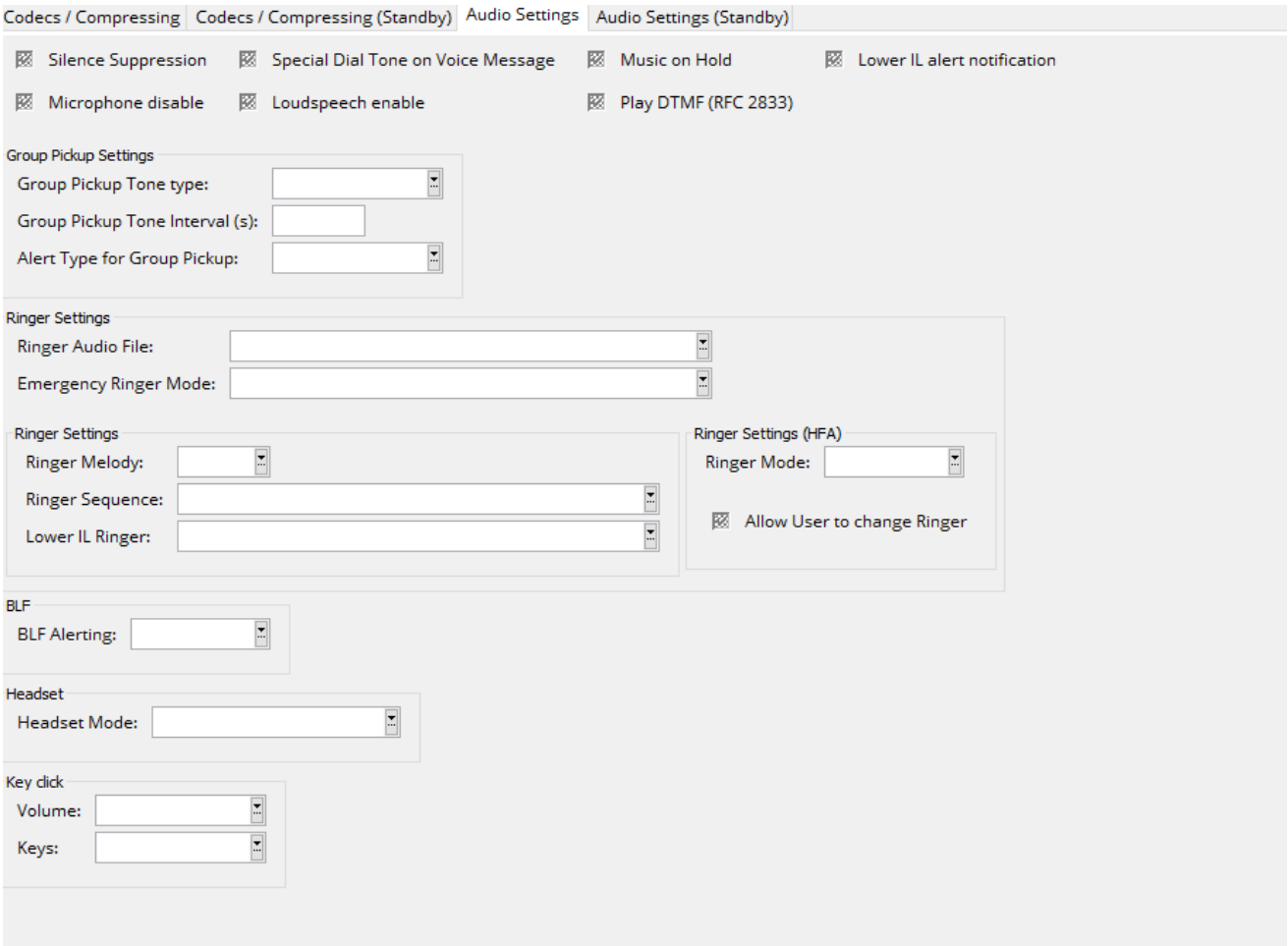
Packet Size:

Possible options:

- **10mS**
- **20mS**
- **30mS**

7.1.12.3 "Audio Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Audio Settings > "Audio Settings" Tab



Silence Suppression

Checkbox for activating silence suppression.

Microphone disable

Checkbox for deactivating the microphone.

Special Dial Tone on Voice Message

If this checkbox is activated, a special dial tone is applied when you lift the handset to inform you that you have a new voice message.

Loudspeech enable

Checkbox for activating the speakerphone function.

Music on Hold

Checkbox to activate Music on Hold.

Play DTMF (RFC 2833)

Checkbox for activating DTMF (RFC 2833) playback. For optiPoint SIP V7 phones only.

Lower IL alert notification

Checkbox for activating an inhibit notification popup / tone when level changes during call (connected or alerting) or when it connects without ringing. This feature is enabled by default.

Group Pickup Settings

Group Pickup Tone type:

Possible options:

- **Off**
- **Beep**
- **Ring burst:** phone plays ringer tone for a few seconds when any of the monitored phones starts ringing.
- **Ring continuous:** phone plays ringer tone whilst any of the monitored phones is ringing**.**

Group Pickup Tone interval (s)

A configurable repeat timer, the group pickup tone is repeated whilst there is a group pickup call available to the phone to pick up.You should be able to configure the interval between playing the Group pickup tone between 0 and 30 seconds, where 0 means the tone is played continuously.

Value range: **0...30** seconds

Default: **15** seconds

> ***NOTE:*** Only applies when the group pickup audio is set to be a tone, not when it is set to be a ringer.This feature is only available to OpenScape Desk Phone CP devices (version V1R4).

Alert type for Group Pickup:

Defines the user action required to accept a pickup call.

Possible Options:

- **Prompt**
  An incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.
- **Notify**
  An incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.
- **FPK only**

  An incoming pickup call is signaled at the corresponding function key only. To accept the call, the user must press the function key.

Ringer Settings

Ringer Melody:

Possible Options:

No.	SIP	HFA	Frequencies (Hz)			Note Length (ms)		
			f1	f2	f3	c1	c2	c3
1	Yes	Yes	457	571	615	45	45	45
2	Yes	Yes	696	762	1067	30	30	30
3	Yes	Yes	400	444	500	35	35	35
4	Yes	Yes	1067	889	696	50	50	50
5	Yes	Yes	762	800	889	30	30	30
6	Yes	Yes	1000	1143	1333	40	40	40
7	Yes	Yes	400	457	593	50	50	50
8	Yes	Yes	533	0	667	90	150	60
9[1]	No	Yes						

1 This option is only available for HFA phones. It is the default option and when selected, ringer melody is taken from the PBX.

Ringer Sequence:

Possible Options:

- **1.0 s ON, 4.0 s OFF**

- **1.0 s ON, 2.0 s OFF**
- **0.7 s ON, 0.7 s OFF, 0.7 s ON, 3.0 s OFF**
- **2.0 s ON, 4.0 s OFF**
- **1.64 s ON, 0.36 s OFF**
- **0.7 s ON, 3.0 s OFF**
- **OpenScape**
  This option is only available for HFA phones. It is the default option and when selected, ringer sequence is taken from the PBX.

Ringer Audio File

Name of the file that contains the ringtone.

Emergency Ringer Mode

Possible Values:

- **Normal** (default view)
- **Always**

Lower IL Ringer

Name of the file that contains the distinctive ringtone to be used in place of the normal ringer for calls from a Lower Impact level.

Ringer Settings (HFA)

The following are distinctive ringer settings for HFA phones.

Ringer Mode

Possible Values:

- **OpenScape** (Default)
- **Local Ringer**

Allow User to change Ringer

If switch is active, the user is allowed to change the ringtone.

BLF

BLF Alerting

Optical alerting by key.

Possible Values:

- **Beep**
- **Ring burst:** phone plays ringer tone for a few seconds when any of the monitored phones starts ringing.
- **Ring continuous:** phone plays ringer tone whilst any of the monitored phones is ringing**.**

Headset

Headset Mode

Connection mode of headset.

Possible Values:

- **Wired Headset**
- **Cordless Headset**
- **Conference Unit**

Key klick

Volume

Defines the volume of key clicks.

Possible Values:

- **Off**
- **Low**
- **Medium**
- **High**

Keys

Defines which keys shall have audible clicks.

Possible Values:

- **Keypad only**
- **All keys**

7.1.12.4 "Audio Settings (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Audio Settings > "Audio Settings (Standby)" Tab

NOTE: This "standby" data is used when the "home" data for the "Audio Settings" Tab is not available. The SRSR functionality must be configured for this, see Section 7.1.9, "Small Remote Site Redundancy".



Silence Suppression (Standby)

Checkbox for activating silence suppression.

7.1.13 SNMP Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SNMP Settings

This area features the following components:

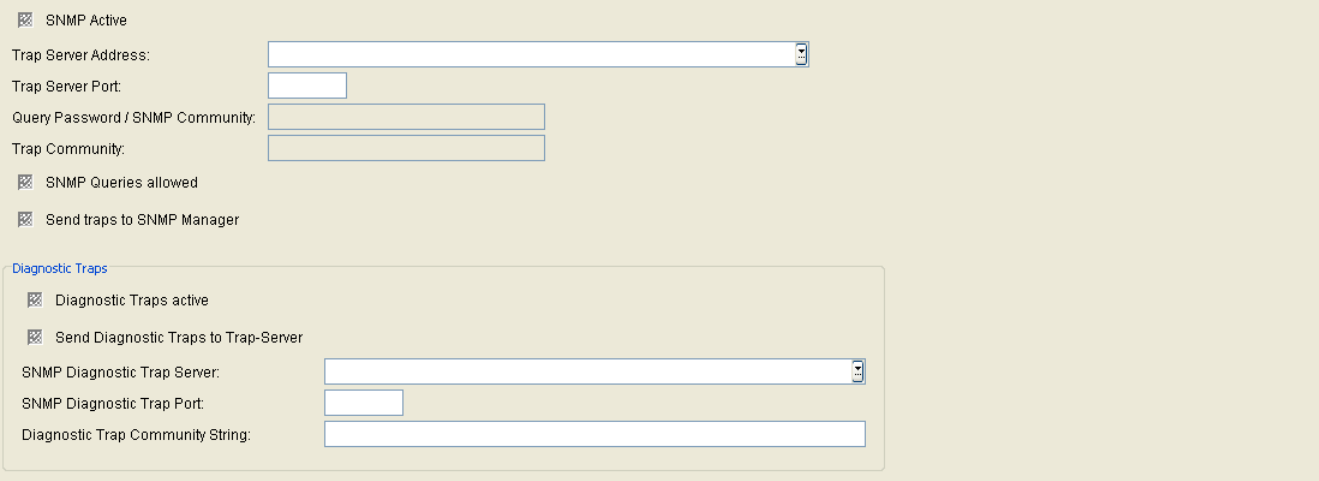
- General Data
- Possible Action Buttons
- "SNMP" Tab
- "Certificate Trap Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.13.1 "SNMP" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SNMP Settings > "SNMP" Tab



SNMP Active

Checkbox for activating the SNMP function (applicable for old HFA optiPoint devices).

Trap Listener Address:

IP address or host name of the SNMP trap server.

Trap Listener Port:

Port number of the SNMP trap server.

Query Password / SNMP Community:

Community string used for authorization on the SNMP server.

Trap Community:

SNMP community string for the SNMP manager receiving trap messages.

SNMP Queries allowed

Checkbox for activating authorization to query QDC data via SNMP.

Send Traps to SNMP Manager

Checkbox for activating the SNMP functionality, that also sends QDC data to an SNMP manager.

Diagnostic Traps

Diagnostic Traps active

If this checkbox is active, diagnostic traps are sent.

Send Diagnostic Traps to Trap Server

If this checkbox is active, the diagnostic traps are sent to the trap server configured.

SNMP Diagnostic Trap Server:

Host name or IP address of the SNMP server that receives diagnostic traps.

SNMP Diagnostic Trap Port:

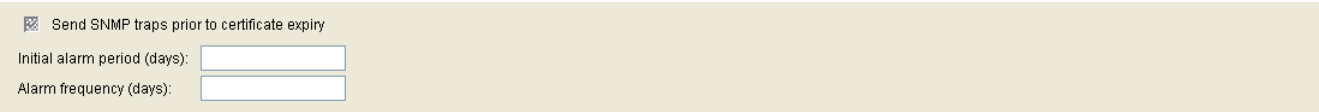
Port used by the SNMP server to receive diagnostic traps.

Diagnostic Trap Community String:

Community string for authentication on the SNMP server that receives diagnostic traps.

7.1.13.2 "Certificate Trap Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SNMP Settings > "Certificate Trap Settings" Tab



Send SNMP traps prior to certificate expiry

If this checkbox is activated, SNMP traps are sent for expired certificates to the address entered under the SNMP settings (see "SNMP" Tab).

Initial alarm period (days):

Number of days before certificate expiry when the SNMP trap is sent.

Alarm frequency (days)

Number of days before an SNMP trap for an expired certificate is resent.

7.1.14 Applications

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications

This area features the following components:

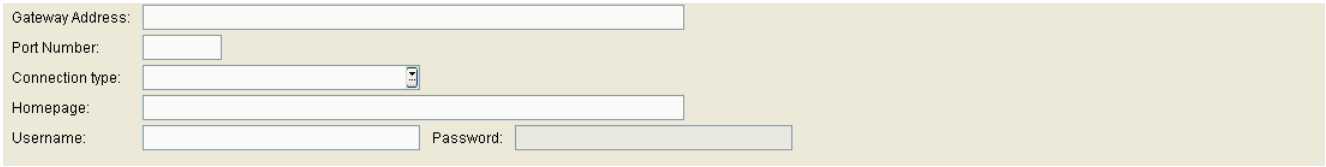
- General Data
- Possible Action Buttons
- "WAP" Tab
- "Java" Tab
- "XML Applications" Tab
- "CA Certificates" Tab
- "Application List" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.14.1 "WAP" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications > "WAP" Tab



Gateway Address:

IP address or host name of the WAP server.

Port Number:

Port number of the WAP server.

Connection type:

Protocol type for connection to the WAP server.

Possible options:

- **HTTP**
- **WSP**

Homepage:

URL of the splash screen where the WAP home page is located.

Username

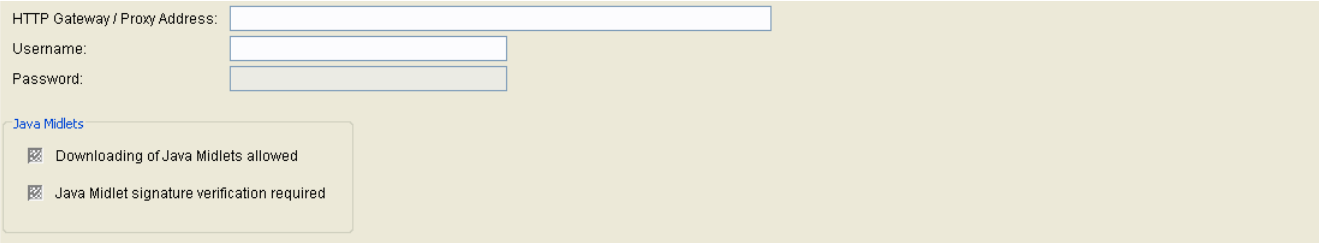
User ID for identification at the WAP server

Password:

Password for the user ID.

7.1.14.2 "Java" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications > "Java" Tab



HTTP Gateway/Proxy Address:

IP address or host name of the HTTP server.

Username:

User ID for identification at the HTTP gateway.

Password:

Password for the user ID.

Java Midlets

Downloading of Java Midlets allowed

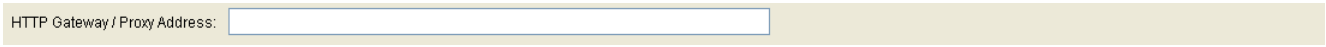
If this checkbox is activated, you can download Java midlets to the workpoint.

Java Midlet signature verification required

If this checkbox is activated, the Java midlet must be verified using a signature.

7.1.14.3 "Java (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications > "Java" Tab

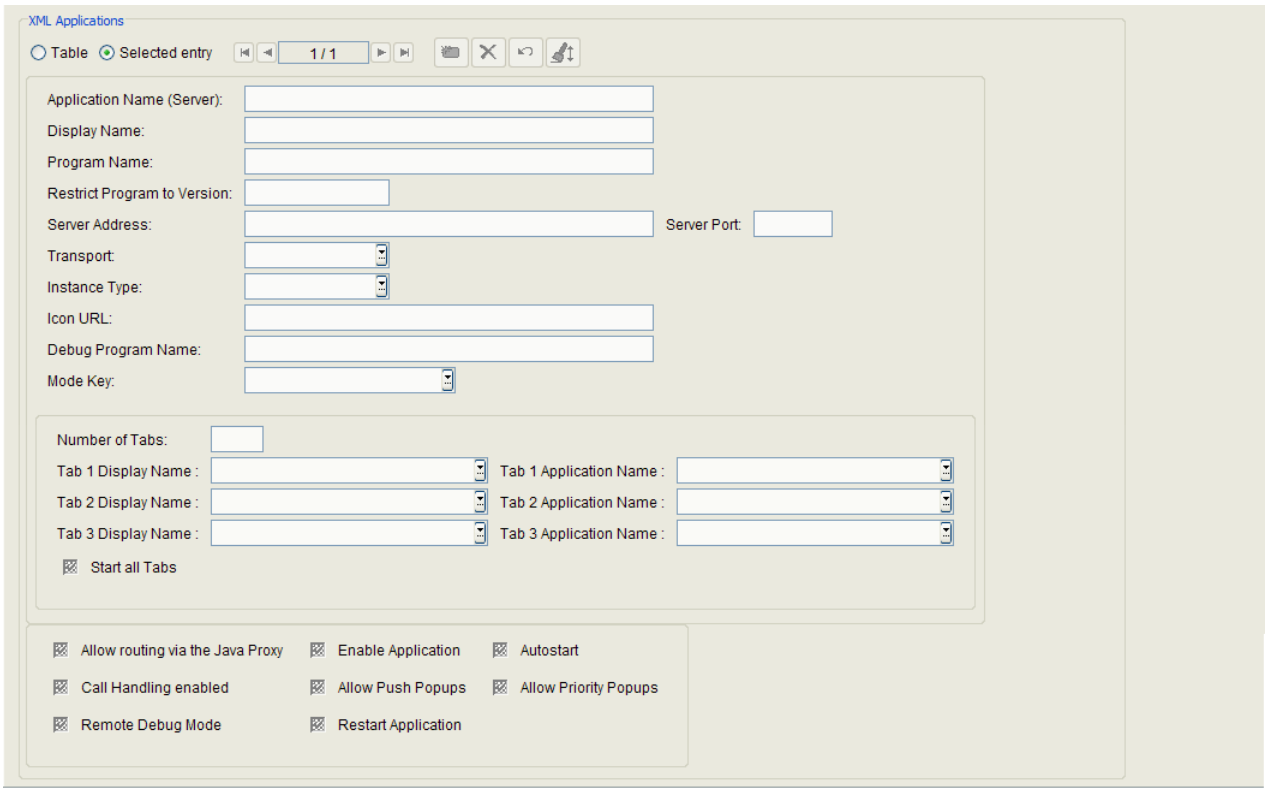


HTTP Gateway/Proxy Address:

IP address or host name of the HTTP server.

7.1.14.4 "XML Applications" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications > "XML Applications" Tab



These are server-side applications which communicate with the phone software via a specially defined XML interface. The Unified Messaging system HiPath Xpressions also uses this interface. The interface enables the workpoint to send user entries, to display data in textual and graphic form, and to control calls.

To set up an XML application on the workpoint, the following specifications are required: a freely selectable user name, communication protocol to be used; server port to be used; start address of the server-side program.

XML applications are only available in OpenStage 60/80.

XML Applications

Application Name (Server):

This is the name of the HTTP servlet, and it is used internally by the workpoint software to identify the application.

For DLS XML applications, the names must be entered unchangend.

Possible values:

- **DeploymentService**
- **LocationService**

- **NewsService**
- **MakeCall**

Display Name:

This name is used for listing the application on the workpoint menu.

Program Name:

Path of the start file of the server-side program, in relation to the server address. For DLS XML applications, enter the WEB application name, followed by the HTTP servlet name.

Restrict Program to Version:

Select a distinct version the application is working with.

Server Address:

IP address of the server on which the program is running. For DLS XML Applications enter the IP address of the DLS Server; for Multinode installation, enter the IP address of the cluster.

Example: **192.168.1.150**

Server Port:

Port used by the server-side program for receiving data from the workpoint.
For DLS XML Applications use port 18080, as only HTTP is supported.
For OSV Assistant XML applications use 7789.

Examples: **80** (Apache default port); **8080** (Tomcat default port).

Transport:

Transport protocol used for transmitting XML data.

Possible options:

- **HTTP**
- **HTTPS**

Instance Type:

Selection of the type of instance.

Possible options:

- **Normal**
- **Xpressions**
- **Phonebook**

Icon URL:

URL of the application icon (not yet implemented).

Debug Program Name:

Name and, where applicable, directory path of the program on the server that receives error messages from the terminal's *.XML application platform.

Mode Key:

Select a mode key to start the application.

Possible options:

- **No Mode Key**
- **Phonebook Mode Key**
- **CallLog Mode Key**
- **Messages Mode Key**
- **Help Mode Key**

Number of Tabs:

The number of embedded tabs within the XML application to be shown on phone display.

Value range: **0** ... **3**

NOTE: For an XML-application with a number of Tabs > 0, one of the entries between **Tab 1 Application Name** and **Tab 3 Application Name** must be set to the same value as the **Application Name (Server)** that it is associated with. When the XML application is started, the tab which has the same name as the XML application is the tab that initially gets focus.

Tab 1 Display Name:

Labeling displayed on the 1st tab header.

Tab 2 Display Name:

Labeling displayed on the 2nd tab header.

Tab 3 Display Name:

Labeling displayed on the 3rd tab header.

Tab 1 Application Name:

The name used by the XML application to identify the application running under the 1st tab. The name must be unique over all XML-applications.

Tab 2 Application Name:

The name used by the XML application to identify the application running under the 2nd tab. The name must be unique over all XML-applications.

Tab 3 Application Name:

The name used by the XML application to identify the application running under the 3rd tab. The name must be unique over all XML-applications.

Start all Tabs

On application start, all tabs will be opened.

Allow routing via the Java Proxy

Switch to allow routing via the Java Proxy.

Enable Application

Switch to enable application.

Autostart

Switch to enable autostart of application.

Call Handling enabled

Switch to enable call handling.

Allow Push Popups

Switch to enable pushing of popups.

Allow Priority Popups

Switch to enable priority popups.

Remote Debug Mode

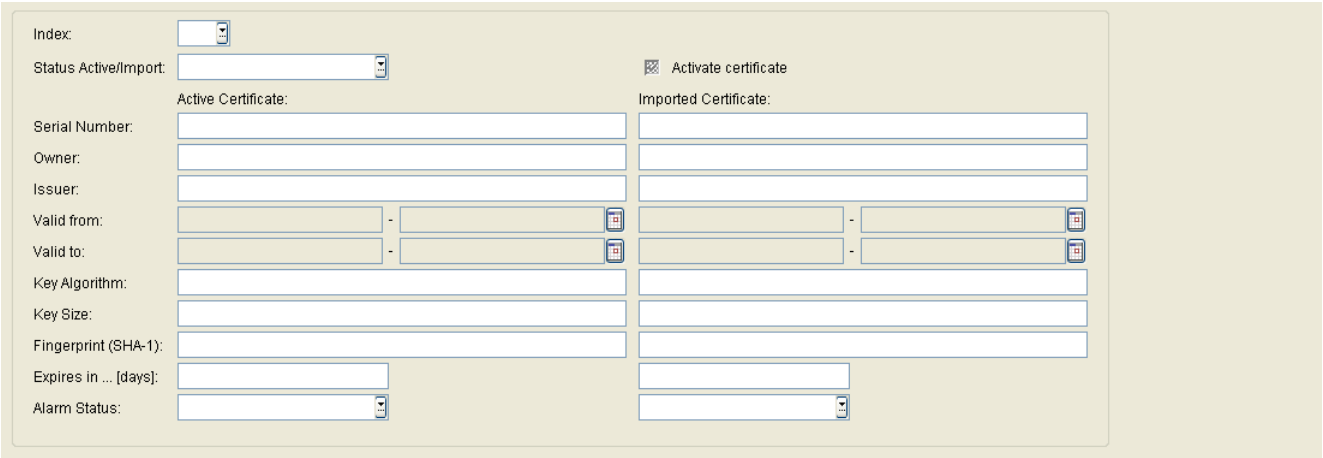
Switch to enable setting of remote debug mode.

Restart Application

Switch to enable restart of application, if it is already running.

7.1.14.5 "CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications > "CA Certificates" Tab



The parameters described below are available once for the currently active certificate and once for the imported certificate.

Index:

Serial number of the CA certificate.

Status Active/Import:

Specifies whether a certificate is registered as imported and/or active on the phone. The five statuses listed below are possible.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Serial Number:

Serial number of the certificate (display only).

Owner:

Owner of the certificate (display only).

Issuer:

Issuer of the certificate (display only).

Valid from:

Start of validity for the certificate (display only).

Valid to:

End of validity for the certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Number of days before the certificate expires.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Displays the duration of validity for certificates when searching for certificates due to expire.

Possible values:

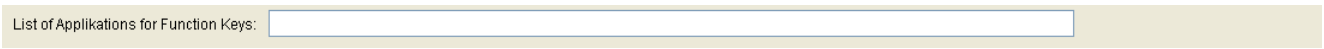
- **valid**
- **soon running out**
- **expired**

Activate certificate

Checkbox for activating the certificate. The active certificate is used to encrypt calls. The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

7.1.14.6 "Application List" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Applications > "Application List" Tab



List of Applications for Function Keys

Comma-separated list of names for applications which can be started by means of Function Keys.

7.1.15 Service Integrations

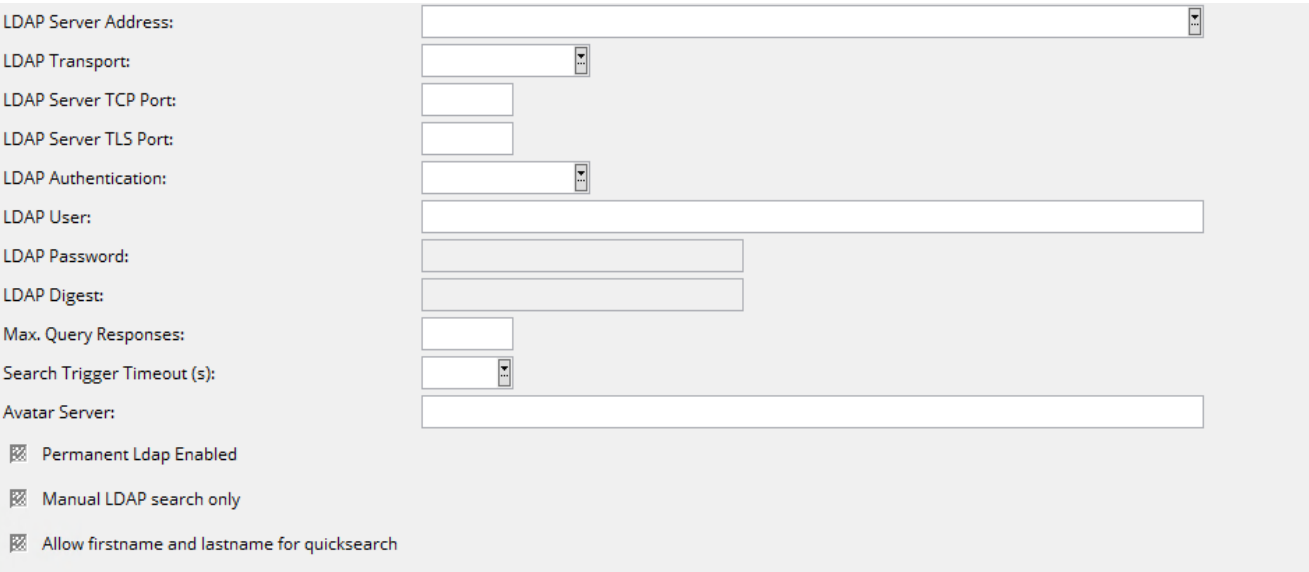
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations

This area features the following components:

- General Data
- Possible Action Buttons
- "LDAP Settings" Tab
- "LDAP Attributes" Tab
- "LDAP CA Certificates" Tab
- "Exchange" Tab
- ’’Exchange CA Certificates’’Tab
- "Circuit" Tab
- ’’Circuit CA Certificates" Tab
- "E/A Cockpit " Tab
- ’’E/A Cockpit CA Certificates" Tab
- ’’WSI(UC)" Tab
- ’’OpenScape UC Connection" Tab
- .’’OpenScape UC Connection CA Certificates" Tab
- ’’Name Update Sources" Tab

7.1.15.1 "LDAP Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > "LDAP Settings" Tab



NOTE: LDAP Server Settings are also applicable for OpenStage 15/20 (SIP only), OpenStage 40 HFA & OpenScape Desk Phone IP 35 G /IP 35 G Eco / 55 G HFA phones.

NOTE: All relevant information regarding the LDAP template file can be found under Section 3.5, "Overview of Software and File Types"

LDAP Server Address:

IP address or host name of the LDAP server.

LDAP Server Port:

Port number of the LDAP server.

LDAP Transport:

Transport protocol used to transmit LDAP data.

Possible options:

- **TCP**

- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

LDAP Authentication:

Option for selecting the LDAP access.

Possible options:

- **Anonymous**
- **Simple**

LDAP User:

User name for authenticated LDAP access.

LDAP Password:

Password for authenticated LDAP access.

LDAP Digest:

Enter LDAP digest.

This item is grayed out.

Max. Query Responses:

Maximum number of results in an LDAP search.

This item is grayed out.

Search Trigger Timeout (sec):

Search Trigger Timeout for LDAP simple search.

Possible options:

- **1**

- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **60**

Avatar Server:

Server name (FQDN ή IP Address).

If the LDAP directory does not include embedded contact pictures then it may use a web-server that can provide a picture for the contact so that this can be displayed as the contacts avatar. The address of the web-server needs to be configured on the phone.

HTTPS is assumed if the string does not start with "HTTP://"

NOTE: This item is supported by CP600 phones SIP V1R2.

Permanent Ldap Enabled:

Enable LDAP server permanently.

Manual LDAP search only:

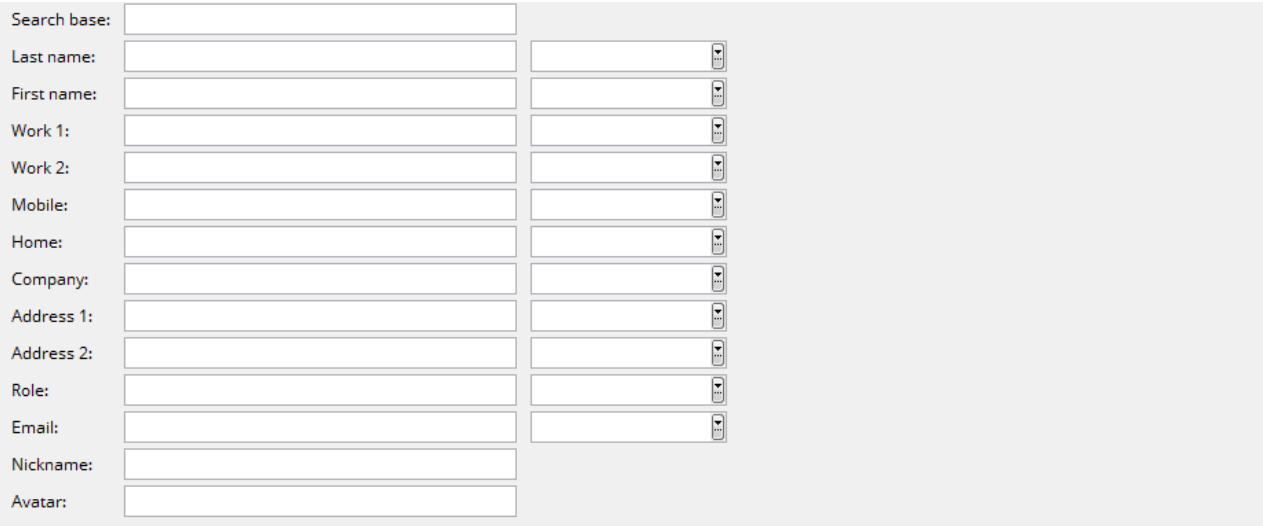
Select this option to allow manual LDAP search on incoming and outgoing calls.

Allow firstname and lastname for quick search:

Search for firstname and lastname.

7.1.15.2 "LDAP Attributes" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > "LDAP Attributes" Tab



Create/edit the LDAP template via WBM or DLS.

IMPORTANT: Available only for CP200/ CP400 / CP600 HFA phones of version V1R1 and higher.

Search Base:

This is the definition of the base point within the LDAP Directory for searches. This is relative to the initial node in the directory at the point of initial connection. For some LDAP servers, this could be an empty string.

Last Name:

Last name contact field.

First Name:

First name contact field.

Work 1:

Business 1 contact field.

Work 2:

Business 2 contact field.

Mobile:

Mobile contact field.

Home:

Sets the Private contact field.

Company:

Sets the Company contact field.

Address 1:

Sets the Address 1 contact field.

Address 2:

Sets the Address 2 contact field.

Role:

Sets the Job function contact field.

Email:

Email contact field.

Nickname:

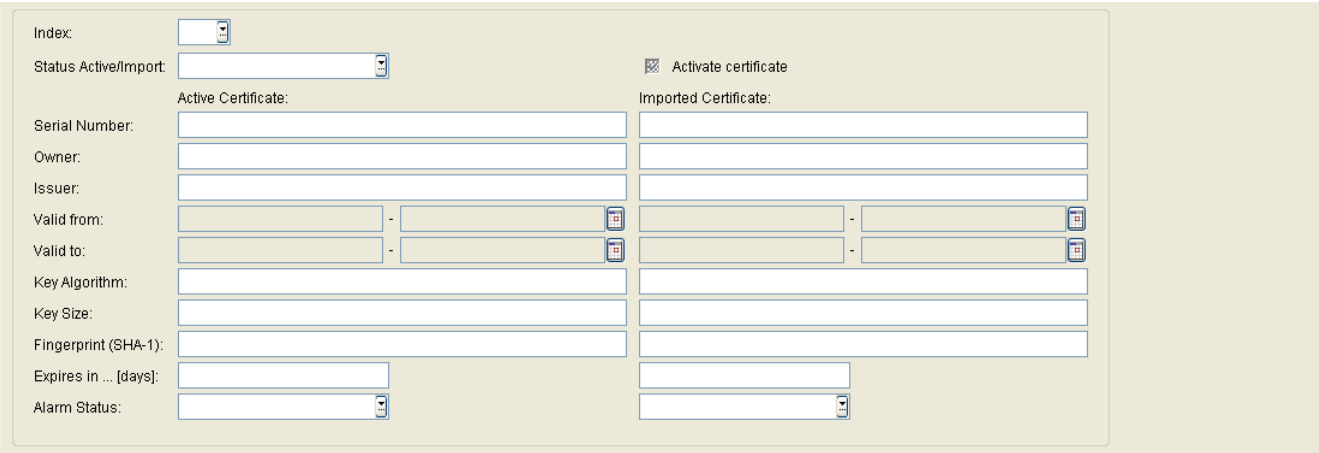
Indicates that Simple search should use nickname mode. The Attribute field does not relate to a contact field and so the field value is not shown by the phone.

Avatar:

Full address of the web-server that holds avatar images.

7.1.15.3 "LDAP CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > "LDAP CA Certificates" Tab



Index

Certificate index number.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

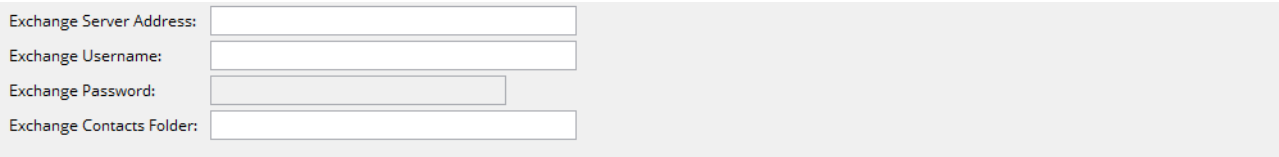
Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.15.4 "Exchange" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > "Exchange" Tab



This tab allows the configuration of **Microsoft Exchange ActiveSync** data for contact synchronization.

IMPORTANT: Available only for CP400 / CP600 HFA V1R1 devices.

Exchange Server Address

Microsoft Exchange server address.

Exchange Username:

Microsoft Exchange username credentials.Username length: max **64** characters.

Exchange Password

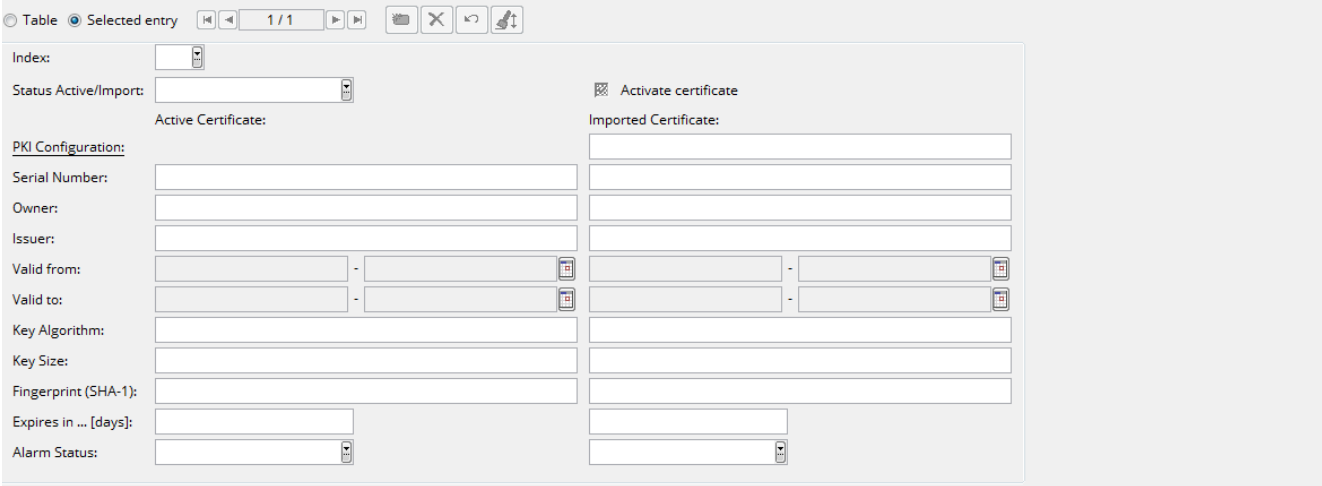
Microsoft Exchange user password.Password length: max **32** characters.

Exchange Contacts Folder

The folder where the User Contacts data resides.

7.1.15.5 ”Exchange CA Certificates”Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > ”Exchange CA Certificates”Tab



The DLS is able to download one or more CA certificates to the phone that can be used to authenticate the Exchange server. The DLS or Admin can specify the certificate policy to be used by the phone when authenticating the Exchange server. When the phone connects to the Exchange server as a TLS client it uses the policy to authenticate the Exchange server against the appropriate certificate.

Certificate handling for the Exchange server will be the same as for a LDAP server

IMPORTANT: This is valid only for CP400 & CP600 SIP phones of V1R2 version and higher, as well as HFA phones of V1R1 version and higher.

IMPORTANT: The phone uses TLS to connect to the Exchange server.

IMPORTANT: The Exchange server provides its certificate as part of the TLS handshake.

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm for the active or imported certificate (display only).

Key Size

Key size for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the active or imported certificate (display only).

Expires in ... [days]

The certificate validity will expire in the number of days specified (display only).

> ***NOTE:*** The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status for the active or imported certificate (display only).

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.15.6 "Circuit" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > "Circuit" Tab



Address

Circuit server address.

Username:

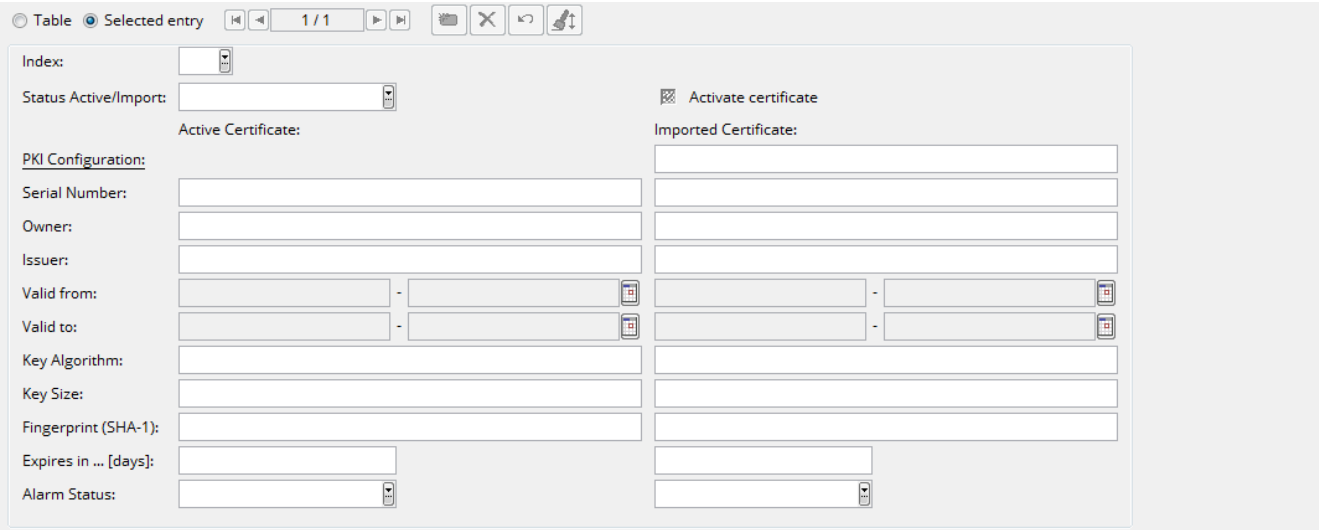
Circuit username credentials.

Password

Circuit user password.

7.1.15.7 ”Circuit CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > ”Circuit CA Certificates" Tab



The DLS is able to download one or more CA certificates to the phone that can be used to authenticate the Circuit server. The DLS or Admin can specify the certificate policy to be used by the phone when authenticating the Circuit server. When the phone connects to the Circuit server as a TLS client it uses the policy to authenticate the Circuit server against the appropriate certificate.

IMPORTANT: This is valid only for CP400 & CP600 SIP phones of V1R2 version and higher, as well as HFA phones of V1R1 version and higher.

IMPORTANT: The phone uses TLS to connect to the Circuit server.

IMPORTANT: The Circuit server provides its certificate as part of the TLS handshake.

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**

- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm for the active or imported certificate (display only).

Key Size

Key size for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the active or imported certificate (display only).

Expires in ... [days]

The certificate validity will expire in the number of days specified (display only).

> ***NOTE:*** The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status for the active or imported certificate (display only).

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.15.8 "E/A Cockpit " Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > IP Routing



E/A Cockpit Server Address:

IP or FQDN (prefixed or not with https://) or IP:port (default https port is 8443)

Allow Server Push:

Allow push requests from the E/A Cockpit Application server.

Mobility logoff action:

This item handles the action taken by the CP phone during SIP Mobile logoff.

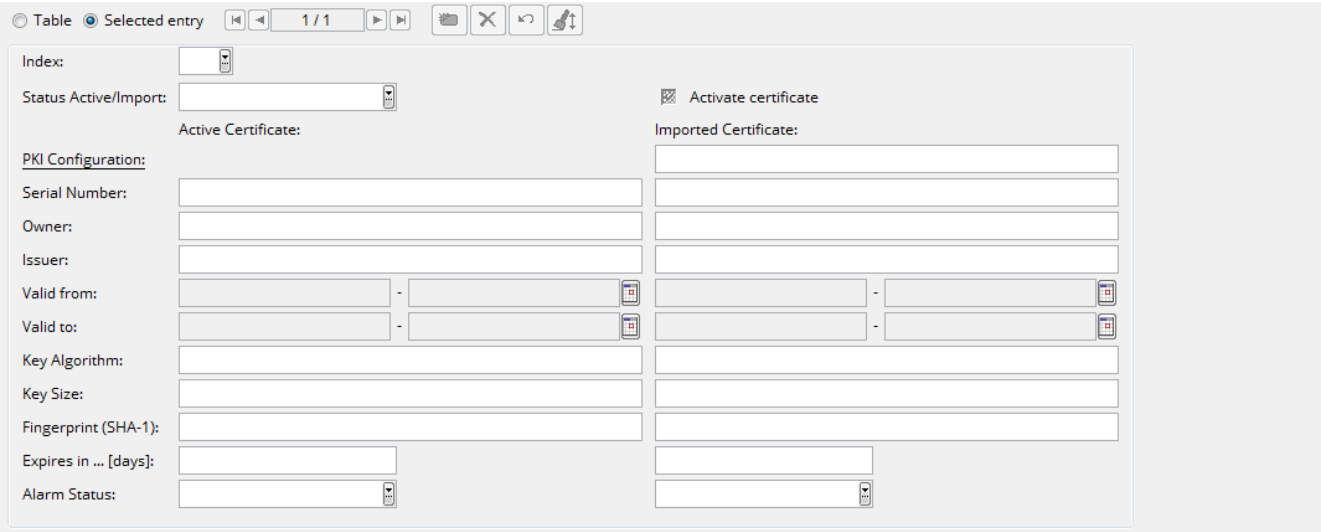
Possible values:

- **None**
  No action is taken.
- **Unavailable**
  An assistant will be set to OFF_DESK, an executive will be set to TO_ASSISTANT_XXX (xxx depends on a different executive related setting)
- **To Voicemail**
  If a voicemail number is configured in the E/A cockpit profile.
- **To Mobile**
  If a mobile number is configured in the E/A cockpit profile.
- **To Number**
  If a to-number is configured.

IMPORTANT: When a SIP mobile user, having E/A cockpit configured, logs off and has the mobility logoff action set to anything except **None**, the E/A cockpit application on the phone will set the state according to **Unavailable**.

7.1.15.9 ”E/A Cockpit CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > ”E/A Cockpit CA Certificates" Tab



The DLS is able to download one or more CA certificates to the phone that can be used to authenticate the E/A (Executive/Assistant) Cockpit server. The DLS or Admin can specify the certificate policy to be used by the phone when authenticating the E/A Cockpit server.

IMPORTANT: This is valid only for CP400 & CP600 SIP phones of V1R2 version and higher, as well as HFA phones of V1R1 version and higher.

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**

- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm for the active or imported certificate (display only).

Key Size

Key size for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the active or imported certificate (display only).

Expires in ... [days]

The certificate validity will expire in the number of days specified (display only).

> ***NOTE:*** The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

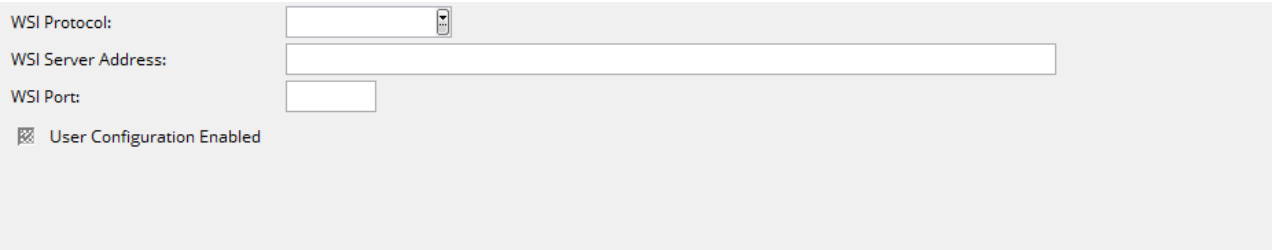
Current alarm status for the active or imported certificate (display only).

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.15.10 ”WSI(UC)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > ”WSI(UC)" Tab



This tab offers WSI interface configuration set up, so that it connects to server and can be used by other services.

IMPORTANT: Available only for CP200/ CP400 / CP600 HFA phones of version V1R1 and higher.

WSI Protocol:

Available options:

- **HTTP**
- **HTTPS (Default)**

WSI Server Address:

If empty, then the system address is used. Hint text in Edit screens if value is empty showing default value (phone number)

WSI Port:

Port range used: **1**... **65535**

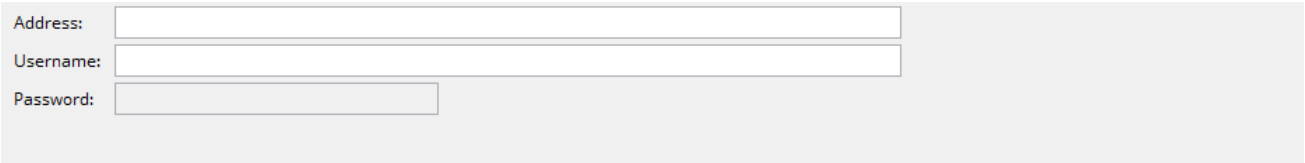
Default: **8802**

User Configuration Enabled:

If this checkbox is activated, configuration changes may be applied.
This flag is enabled by default.

7.1.15.11 ’’OpenScape UC Connection" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > ’’OpenScape UC Connection" Tab



This tab offers OpenScape Desk Phone synchronization with the OpenScape UC Web Client using the OpenScape UC client API.

IMPORTANT: Available only for CP400 / CP600/ CP 600 E HFA phones of version V1R1 and higher.

Address:

UC Server address.

Username:

User name.

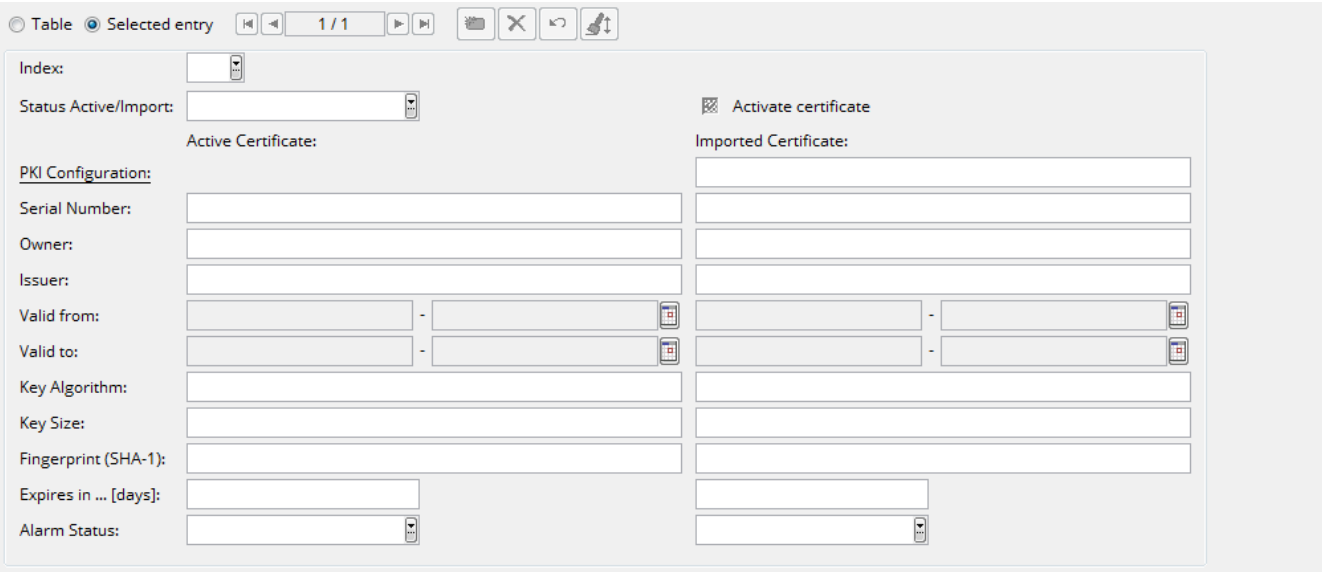
Default: **""**

Password:

UC password.

7.1.15.12 .’’OpenScape UC Connection CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > .’’OpenScape UC Connection CA Certificates" Tab



The DLS is able to download one or more CA certificates to the phone that can be used to authenticate the OpenScape UC Connection server. The DLS or Admin can specify the certificate policy to be used by the phone when authenticating the E/A Cockpit server.

IMPORTANT: This is valid only for CP400 & CP600 SIP phones of V1R2 version and higher, as well as HFA phones of V1R1 version and higher.

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**

- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm for the active or imported certificate (display only).

Key Size

Key size for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the active or imported certificate (display only).

Expires in ... [days]

The certificate validity will expire in the number of days specified (display only).

> ***NOTE:*** The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status for the active or imported certificate (display only).

Possible values:

- **valid**
- **soon running out**
- **expired**

The DLS is able to download one or more CA certificates to the phone that can be used to authenticate the E/A (Executive/Assistant) Cockpit server. The DLS or Admin can specify the certificate policy to be used by the phone when authenticating the E/A Cockpit server.

> ***IMPORTANT:*** This is valid only for CP400 & CP600 SIP phones of V1R2 version and higher, as well as HFA phones of V1R1 version and higher.

> ***NOTE:*** For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm for the active or imported certificate (display only).

Key Size

Key size for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the active or imported certificate (display only).

Expires in ... [days]

The certificate validity will expire in the number of days specified (display only).

> ***NOTE:*** The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status for the active or imported certificate (display only).

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.15.13 ’’Name Update Sources" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Service Integrations > ’’Name Update Sources" Tab



This tab offers an interface where you are able to control if call party names are updated and which source is used to update them.That way, you have full control of name updates in one place.

Name Update sources:

Possible values:

- **No Master Source**
- **LDAP**
- **UC Directory**
- **LDAP and UC Directory**
- **Signalling**
- **LDAP and Signalling**
- **UC Directory and Signalling**
- **LDAP,UC Directory and Signalling**

7.1.16 User Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > User Settings

This area features the following components:

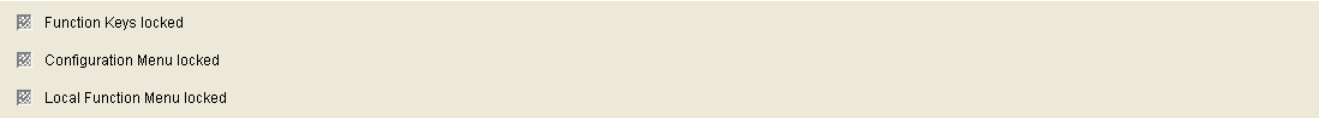
- General Data
- Possible Action Buttons
- "Locks" Tab
- "Locked Configuration Menus" Tab
- "Locked Local Functions" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.16.1 "Locks" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > User Settings > "Locks" Tab



Function Keys locked

Checkbox for locking function keys on the IP Device.

Configuration Menus locked

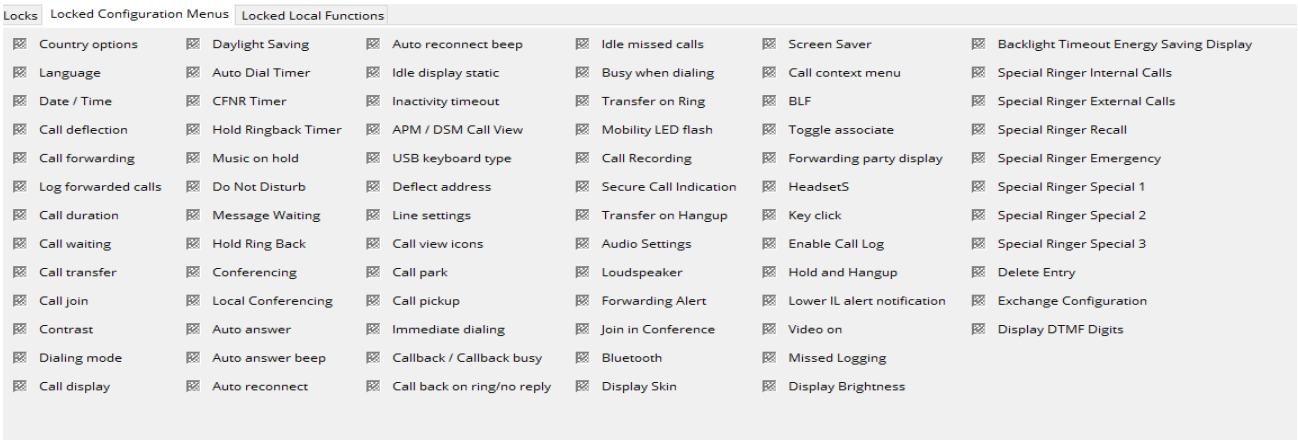
Checkbox for locking configuration menus on the IP Device.

Local Function Menus locked

Checkbox for locking local function menus on the IP Device.

7.1.16.2 "Locked Configuration Menus" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > User Settings > "Locked Configuration Menus" Tab.



NOTE: By clicking on a feature function, the feature shall be grayed out in the phone's WBM menu.

The following functions can be locked in the configuration menus by activating the relevant checkbox:

1-Country options

The user can select a country from a list to adapt the phone to country specific conditions.

2-Language

The user can set the language for the user menu.

3-Date / Time

The user can set the local time, the current date, and the daylight saving time.

4-Call deflection

The user can activate or deactivate call deflection.

5-Call forwarding

The user can activate or deactivate call forwarding.

6-Log forwarded calls

The user can activate or deactivate the logging of forwarded calls.

7-Call duration

The user can determine whether the call duration is indicated on the display.

Only available in optiPoint workpoints.

8-Call waiting

The user can determine whether a second call is allowed during a connected call. If not, the caller hears the busy tone.

9-Call transfer

The user can allow call transfer.

10-Transfer call

The user can enable or disable the posibility to interlink an active and a held call.

11-Contrast

The user can set the contrast for the display.

12-Dialing mode

The user can determine whether a number only or, alternatively, a name can be used for dialing.

Only available in optiPoint workpoints.

13-Call display

The user defines which information about the caller is displayed on an incoming call.

Only available in optiPoint workpoints.

14-Daylight Saving

The user can set the daylight saving time.

15-Auto dial timer

The delay time between the entry of the last call number digit and the start of the dialing process can be set by the user.

16-CFNR timer

The user can set the delay time that passes before a call is forwarded, if Call Forwarding on No Reply is activated.

> ***NOTE:*** if the option "**Support of Server Based Features**" is enabled (under **Call: Main Menu > Call: Main Menu >>IP Phone Configuration** > **Features**> **"Server based features" Tab**) the CFNR delay timer is not configurable (greyed out).

17-Hold ringback timer

The user can set the time delay, after which the workpoints indicates that there us a held call.

18-Music on hold

The user can determine whether the music on hold stored in the phone is used. If music on hold is activated, it is played as soon as the phone is put to hold.

19-Do not disturb

The user can determine whether Do Not Disturb is available on the phone. If Do Not Disturb is active, the phone will not ring on an incoming call, and the caller will hear the busy tone.

20-Message waiting

The user can determine whether new messaes in the mailbox are signaled by a LED.

Only available in optiPoint workpoints.

21-Hold ring back

If this function is active and a participant has been put to hold, a signal sounds after a configurable time to remind that a call is on hold. The user can allow this function and set the delay time for the acoustic signal.

22-Conference

The user can allow system based conferences.

Only available in optPoint workpoints.

23-Local conference

The user can allow local 3-party conferences.

32-Auto answer

The user can determine whether incoming calls are accepted automatically by the CTI application which is connected to the phone.

33-Auto answer beep

The user can determine whether a signal will sound when a call that is accepted automatically by the CTI application connected to the phone.

34-Auto reconnect

The user can determine whether a held call can be reconnected automatically by the CTI application.

35-Auto reconnect beep

The user can determine whether a signal will sound when a held call is reconnected by the CTI application.

36-Idle display static

The user can configure the indication of system messages in idle state.

Only available in optiPoint workpoints.

38-Inactivity timeout

The user can set the delay time between the last entry and the return to the idle state.

39-APM / DSM Call View

The user can activate or deactivate the call view on the optiPoint application module.

40-USB keyboard type

The user can modify the language of the USB keyboard connected to an optiPoint phone.

Only available in optiPoint workpoints.

43-Deflect address

The user can enter resp. modify the target number for call deflection.

44-Line settings

The user can modify the settings of a line key.

45-Call view icons

The user can determine whether messages on the optiPoint display module, like, for instance, the list of missed calls, are displayed as text or symbols.

46-Call park

The user can allow call parking.

47-Call pickup

The user can allow pickup of a parked call.

48-Immediate dialing

The user can allow immediate dialing.

49-Callback / Callback busy

The user can activate the transmission of a callback request to the system. With OpenStage V3 onwards, the callback request can be transmitted in every case; with other end devices, this is only possible in busy case.

50-Call back on ring/no reply

The user can activate the transmission of a callback request to the system in case a call is not replied.

Only available in OpenStage workpoints.

51-Idle missed calls

The user can activate missed calls notifications on the display.

Only available on optiPoint workpoints.

52-Busy when dialing

The user can determine whether incoming calls are refused while a call number is entered.

53-Transfer on Ring

The user can determine whether a call is transferred as soon as the third participant’s phone rings, even if the transferring participant has not hung up.

54-Mobility LED flash

The user can determine whether the mobility key LED flashes during data exchange between phone and DLS, like, for instance, while mobility logon and logoff.

Only available in optiPoint workpoints.

55-Call Recording

The user can activate call recording.

Only available in optiPoint workpoints.

56-Secure Call Indication

The user can determine whether an alert tone shall indicate an insecure speech connection.

57-Transfer on Hangup

The user can determine whether, when one call is active and another call is on hold, the user can connect these calls by hanging up.

60-Audio Settings

The user can modify settings like ringtones and room character.

Only available in OpenStage workpoints.

61-Loudspeaker

The user can activate or deactivate handsfree talking.

Only available in OpenStage workpoints.

62-Forwarding Alert

The user can allow forwarding alert.

63-Join in Conference

The user can determine whether visual or acoustical warning notifications indicate an incoming call while call forwarding is active.

Only available in OpenStage workpoints.

64-Bluetooth

The user can activate or deactivate bluetooth connectivity.

65-Display Skin

The user can choose the display theme.

Only available in OpenStage 60/80 workpoints.

66-Screensaver

The user can activate the phones’s screensaver and set the delay time for starting the screensaver.

Only available in OpenStage 60/80 workpoints.

67-Call context menu

The user can define the displayed menu.

Only available in OpenStage 60/80 workpoints.

68-BLF

The user can define how an incoming call for the phone supervised by the BLF key shall be displayed.

69-Toggle associate

The user can enable or disable the connecting of a first call and a second call by going on-hook. When "Toggle associate" is activated, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook.

Available in all OpenStage workpoints.

70- Forwarding party display

For multiple forwarding, the user can determine whether the first forwarding party or the last forwarding party is displayed.

Available in all OpenStage SIP workpoints.

71- Headset

The user can define the type of headset connected to the phone.

Available for OpenStage 40/60/80 SIP/HFA.

72- Key klick

The user can define the mode of key klick on the phone.

Available for OpenStage 40/60/80 SIP/HFA.

73- Enable Call Log

The user can activate a list of missed,dialed,received or forwarded calls. The call log can be cleared via the WPI.

Available for OpenStage 15/20/20E/40/60/80 SIP.

74- Hold and Hangup

The user can temporarily hold and hang up a line without disconnecting your caller. This function in disabled by default.

Available for OpenStage 40/60/80 SIP/HFA.

75- Lower IL alert notification

The user is informed when an incoming call originated from a lower security zone, or when an outgoing call terminates in a lower security zone.

Available for OpenStage 40/60/80 SIP/HFA.

76- Video On

The user can activate video calls.

Available for OpenStage 60/80 SIP/HFA.

77- Missed Logging

The user can configure whether the calls completed elsewhere will be logged on phone.

Available for OpenStage 15/20/20E/40/60/80 SIP.

78- Display Brightness

79- Backlight Timeout Energy Saving Display

80- Special Ringer Internal Calls

The user can configure special ringers for Internal Calls at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G / 35 G Eco / 55 G (SIP only).

81- Special Ringer External Calls

The user can configure special ringers for External Calls at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

82- Special Ringer Recall

The user can configure special ringers for Recalls at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

83- Special Ringer Emergency

The user can configure special ringers for Emergency at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

84- Special Ringer Special 1

The user can configure his own special ringers (up to 3) at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

85- Special Ringer Special 2

The user can configure his special ringers (up to 3) at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

86- Special Ringer Special 3

The user can configure his own special ringers (up to 3) at device level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

87- Delete Entry

The user can configure whether to delete calls log entries in case there is a call to an entry in Missed calls list.

88- Exchange Configuration

The user can configure whether to setup an Exchange Server.

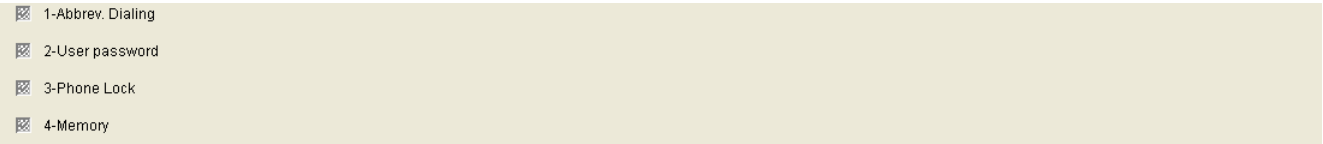
89- Display DTMF Digits

Checkbox for activating the display on the call screen of the DTMF digits pressed during an active call.

Only available in SIP workpoints.

7.1.16.3 "Locked Local Functions" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > User Settings > "Locked Local Functions" Tab



The following functions can be locked in the configuration menus by activating the relevant checkbox:

1-Abbreviated dialing

The user can set up abbreviated dialing numbers.

Only available in optiPoint workpoints.

2-User password

The user can change his password.

3-Phone lock

The user can lock the phone. If the phone is locked, no unauthorized person can call from this phone in a regular manner or modify any settings. Only emergency numbers and pre-defined numbers from the dial plan can be dialed.

> ***NOTE:*** Phone Lock function can only be configured via DLS (not via Web Based Management (WBM) nor locally).
> If the function is locked,the menu is still visible, yet grayed out.

4-Memory

The user can delete all abbreviated dialing numbers and restore the factory settings.

Only available in optiPoint workpoints.

7.1.17 SIP Mobility

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SIP Mobility

This area features the following components:

- General Data
- Possible Action Buttons
- "SIP Mobility" Tab
- "SIP Mobility Logon/Logoff" Tab
- "SIP Mobility Data" Tab

7.1.17.1 "SIP Mobility" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SIP Mobility > "SIP Mobility" Tab



Device available for Mobile User

If the checkbox is active, the device is available for Mobile User log on.

7.1.17.2 "SIP Mobility Logon/Logoff" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SIP Mobility > "SIP Mobility Logon/Logoff" Tab



SNMP Trap on Remote Logoff

If the checkbox is active, a message is sent to the SNMP server each time an unauthorized remote logoff is attempted. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

Mobile User Logoff with Password

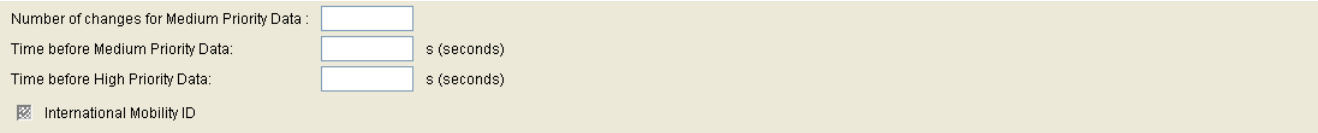
If the checkbox is active, Mobile User logoff is only possible when the password of the currently logged-on Mobile User is entered.

Delay SNMP Trap

Time in seconds until the SNMP trap is sent. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

7.1.17.3 "SIP Mobility Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SIP Mobility > "SIP Mobility Data" Tab



Number of changes for Medium Priority Data:

Defines how many changes to medium priority data may take place in the workpoint before this data is sent to the DLS.

Time before Medium Priority Data:

Defines the interval after which medium priority data that has been changed in the workpoint is sent to the DLS.

Time before High Priority Data:

Defines the interval after which high priority data that has been changed in the workpoint is sent to the DLS.

International Mobility ID

If this checkbox is activated, the device automatically adds the local country code to the extension, in addition to the trunk number and local area code when a mobile user logs on. The international code is configured under **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Dialing Properties** > **"Dialing Properties" Tab** -> **International Dial Prefix**.

Example: The user logs on to the device using the extension/mobility ID "31434". If the checkbox is activated, the device sends the number "498972231434". Otherwise, the device sends the number "8972231434".

7.1.18 HFA Mobility

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > HFA Mobility

This area features the following components:

- General Data
- Possible Action Buttons
- "HFA Mobility" Tab

IMPORTANT: The following **HFA Data Mobility specifications** have to be met:
1.One standalone system has to be used with one DLS
2.Multiple separated standalone systems can't be used against HFA with Data Mobility.
3.Unique numbering has to be used

7.1.18.1 "HFA Mobility" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > HFA Mobility > "HFA Mobility" Tab

NOTE: If the DLS is to store user data like call lists and the phonebook including picture clips, the field **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **HFA Mobility** > **"HFA Mobility" Tab** > **Mobility Mode** must be set to **Data Mobility**. With the values **Data Privacy** and **Basic**, the end device is registered with the DLS, but no further actions are executed in the DLS.



Mobility Mode:

Determines how user data is managed with HFA Mobility. User data falls into two categories :

a) Common User Data (Screensavers,ring tones,volumes,room character,skin)

b) Private Data (Phone Book & associated pictures,Call Log & the user password)

Phones can be configured to support Basic, Data Privacy or Data Mobility modes of operation.

NOTE: **Mobility Mode** configuration is an administrators only option.

Possible options:

- **Basic**

  Default operation where user data is accessible to all users. Users are allowed to log on at any phone.

- **Data Privacy**

  Data Privacy forms an enhancement to the Basic HFA Mobility Mode in such way that Private Data for a previous visitor or the owner of the phone are deleted or hidden whilst a visitor is logged on to a phone.

  NOTE: Administrators are able to set the Mobility Mode from Basic to Data Privacy & vice versa.

- **Data Mobility**

  Data Mobility forms an enhancement to the Data Privacy Mode by supporting the transfer of a limited set of additional user data items between phones that have been used by a user.
  Private Data are made available to users wherever they are logged on, and are securely stored whilst they are logged off. In addition the User Password is transferred along with the user as they move between phones.

  NOTE: If an error is encountered when saving Mobility data, the user is warned & subsequently informed when the problem is cleared.

7.1.19 Keysets/Keylayout

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/Keylayout

This area features the following components:

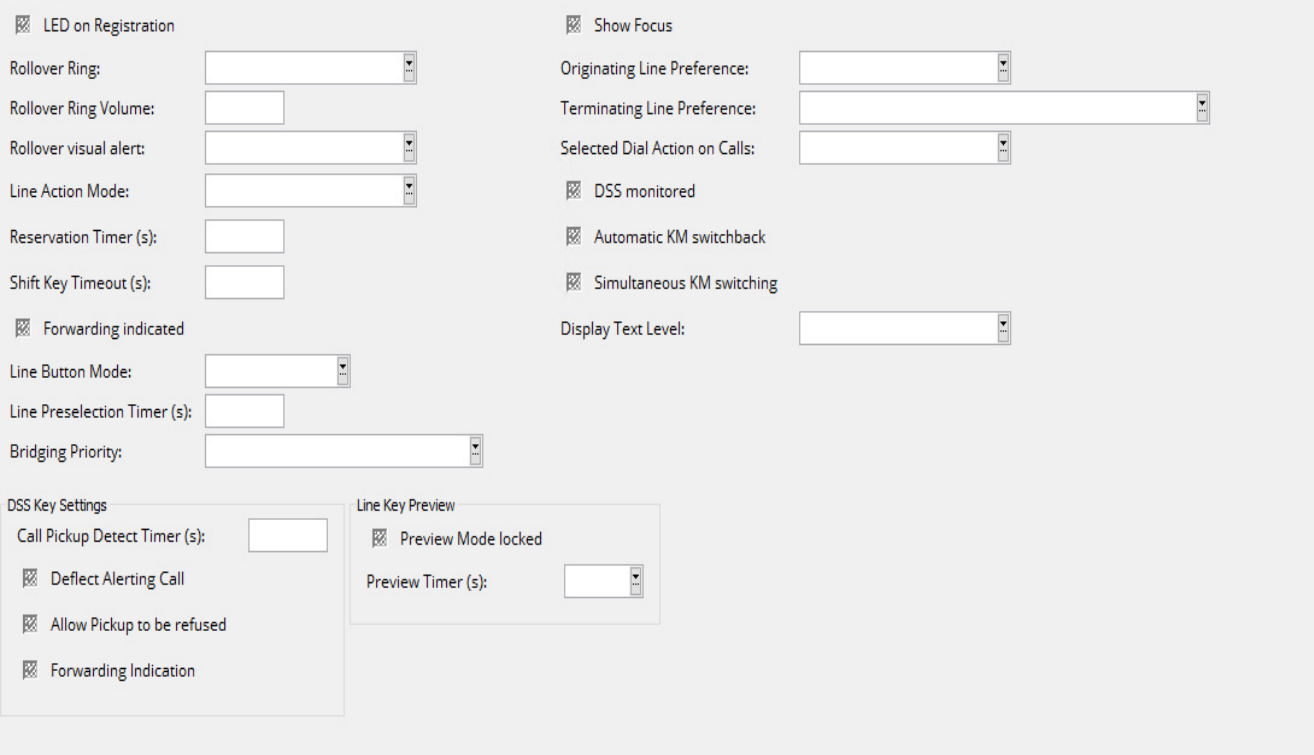
- General Data
- Possible Action Buttons
- "Keysets" Tab
- "Destinations" Tab
- "Send URL Server CA Certificate" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.19.1 "Keysets" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/Keylayout > "Keysets" Tab



LED on Registration

If the checkbox is activated, the successful workpoint registration after a phone restart will be indicated.

Only available in SIP workpoints.

Rollover Ring:

Type of alerting to be used in the case that, during an active call, an incoming call arrives on a different line.

Possible options:

- **No ring**
- **Alert Ring**
- **Standard**
- **Alerting**

Only available in SIP workpoints.

Rollover Ring Volume:

Volume of alerting when busy.

Only available in SIP workpoints.

Rollover visual alert:

Configure the visual alert for any incoming call rollover.

Possible options:

- **no indication**
- **visual alert**

NOTE: Available only for CP600 SIP devices, of version V1R3 and higher.

Line Action Mode:

Defines what should happen to a line (call) when a connection is established over another line.

Possible options:

- **Call hold**
  The original call is put on hold.
- **Release**
  The connection to the original call is cleared down (the call is ended).

Only available in SIP workpoints.

Reservation Timer (sec):

Time in seconds indicating how long a line reservation can be maintained.

Default: **60** s.

Only available in SIP workpoints.

Shift Key Timeout (sec):

Time in seconds indicating how long the Shift key remains active before the keys recover their original level-1 functions.

Forwarding indicated

Checkbox for activating alerting on a line key when call forwarding is active for its destination.

Only available in SIP workpoints.

Line Button Mode

Possible options:

- **Single button**
  The action associated with the line key is executed as soon as the button is pressed, regardless of whether or not the handset is in the cradle.
- **Preselection**
  Press the line key to preselect a line. This line is used the next time you seize a line (by lifting the handset, for example).

Line Preselection Timer (sec):

Specifies the duration of line key preselection.

Bridging Priority:

Possible options:

- **Bridging overrides preview**
- **Preview overrides bridging**

Show Focus

Checkbox for activating the display showing which line is currently active (line has the focus).

Only available in SIP workpoints.

Originating Line Preference:

Defines the preferred line to be used for outbound calls.

Possible options:

- **Idle line preference**
- **Primary line preference**
- **Last line preference**
- **No preference**

Only available in SIP workpoints.

Terminating Line Preference:

Defines the preferred line to be used for incoming calls.

Possible options:

- **Ringing line preference**
- **Calling line preference with prime line preferred**
- **Ringing line preference**
- **Ringing line preference with prime line preferred**
- **No preference**

Only available in SIP workpoints.

Selected Dial Action on Calls:

Defines the action to be performed when a Selected Dialing Free Programmable Key (FPK) is pressed during an active or held call.

Possible options:

- **No Action**
  The default option. No action will be performed.
- **Consult**
  The action will be a consultation transfer to the destination configured in the selected dialing key.
- **Transfer**
  The action will be a blind transfer to the destination configured in the selected dialing key.

Only available for CP600/ CP700 phones of version SIP V1R8 or later.

DSS monitored

Activate this checkbox to allow a DSS key to monitor the non-Keyset phone associated with the DSS key.

Automatic KM switchback

If this checkbox is activated the phone starts a 15 seconds timer, when the user has switched to a shifted level, and then switches to the non shifted level on the attached key modules.

Simultaneous KM switchback

Activate this checkbox to allow switching to the shifted level (or back to normal level) of every attached key module at the same time.

Display Text Level

Defines the preferred text level to be used on the Key Module display.

Possible options:

- **Normal**
  The default Key Module display showing status icons, action icons and alternating text.
- **Max**
  The text will be truncated on boundary and there will be no alternating text, no action icons, nor status icons shown.
- **High**
  The text will be truncated on boundary and there will be no alternating text and no status icons apart from Line and DSS keys. The action icons will be shown only if the key action is not clear from the LED.
- **Medium**
  The text will be alternating and but text scrolling will not be allowed. No status icons will be shown apart from Line and DSS keys. The action icons will be shown only if the key action is not clear from the LED.

Available in SIP and HFA work points.

DSS Key Settings

Call Pickup Detect Timer (sec)

Specifies how long group pickup is signaled by the key.

Deflect Alerting Call

If this checkbox is activated, alert tones can be forwarded by pressing a key.

Allow Pickup to be refused

If this checkbox is activated, you can reject group pickup by pressing a key.

Forwarding Indication

If this checkbox is activated and station forwarding is active for this line, the LED of the line key blinks.

Line Key Preview

Preview Mode locked:

Switch to lock preview mode.

Line Key Preview Duration (sec)

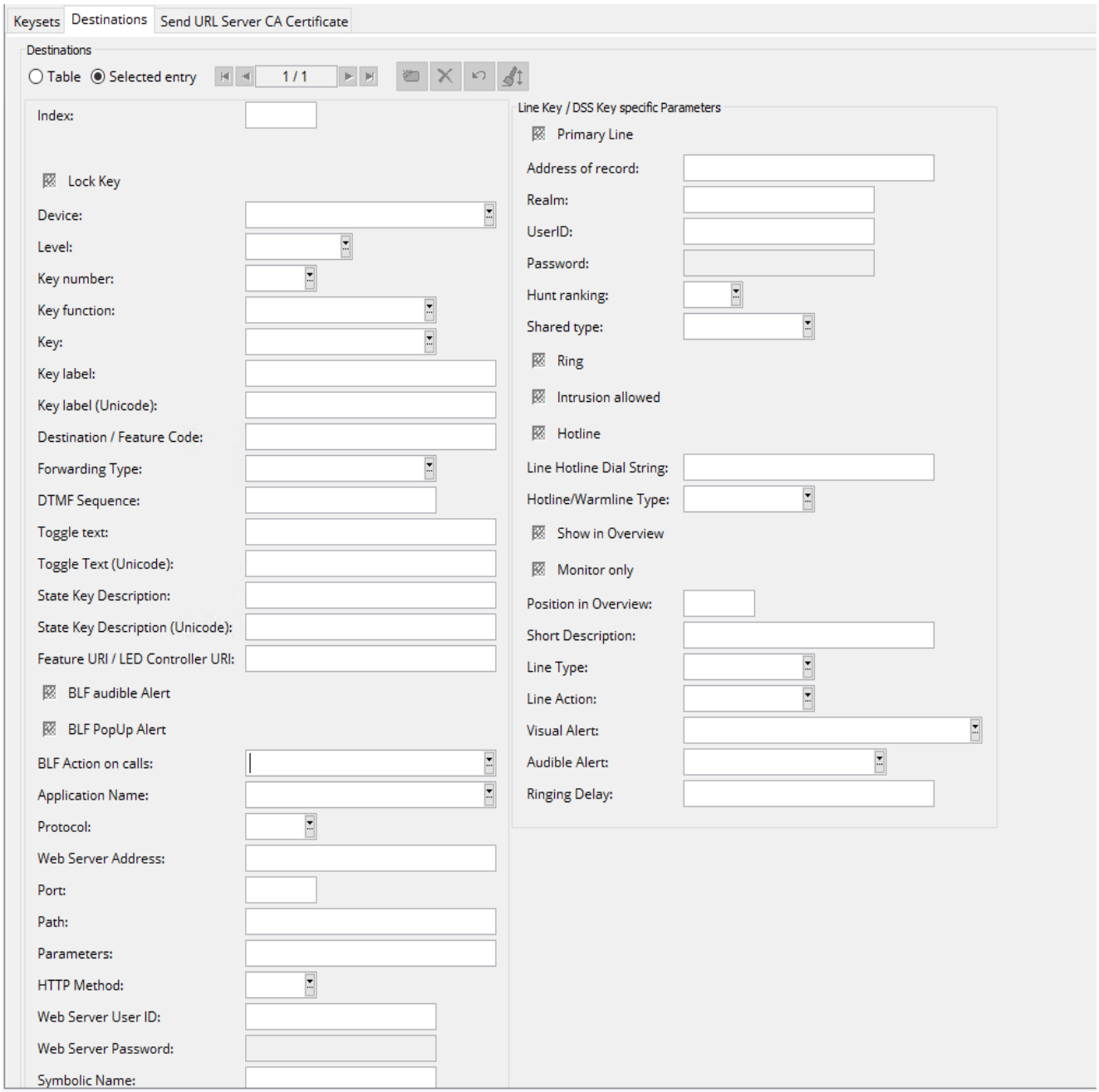
Duration of preview mode in seconds.

Possible options:

- **2**
- **3**
- **4**
- **6**
- **8**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**

7.1.19.2 "Destinations" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/Keylayout > "Destinations" Tab



Index

Name of the key layout function.

Lock Key

Checkbox for locking the function key.

Device

Specifies the device to which the relevant layout applies.

Possible options:

- **Base device**
- **1st Key module**
- **2nd Key module**
- **1st Self Labeling Key module**
- **2nd Self Labeling Key module**
- **OpenStage 15 Key module**

Only available in SIP workpoints.

Level

Key level for the Shift functionality.

Possible options:

- **1. Level**
- **2. Level**
- **3. Level**
- **4. Level**
- **Fixed Keys**
  Fixed Keys are assigned to a fixed key number. They cannot be deleted or created on the IP Device.

Only available in SIP workpoints.

Key number

Number of the key assigned the relevant function.

Only available in SIP workpoints.

Key function:

The following key functions are supported:

- **Key unused**
- **Selected dialing**
- **Abbreviated dialing**
- **Repeat dialing**
- **Missed calls**
- **Voice messages**
- **Forwarding**
- **Loudspeaker**
- **Mute**
- **Ringer off**
- **Hold**
- **Alternate**
- **Blind Transfer**
- **Transfer call (OpenStage) / Join (optiPoint)**
- **Deflect**
- **Setup menu**
- **Room echoing**
- **Room muffled**
- **Shift**
- **Notebook**
- **Settings**
- **Phone lock**
- **Conference**
- **Local Conference**
- **Headset**
- **Do not disturb**

- **Group pickup**
- **Repertory dial**
- **Line**
- **Feature Toggle**
- **Show Phone Screen**
- **Swap screen**
- **Mobility**
- **Call park**
- **Call pickup**
- **Cancel/Release**
- **Ok Confirm**
- **Callback Request**
- **Cancel Callback**
- **Consultation (OpenStage) / Consult/Transfer (optiPoint)**
- **DSS**
- **State Key**
- **Call waiting**
- **Immediate Ring**
- **Preview Key**
- **Call Recording**
- **AICS Zip**
- **Server Feature**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **BLF**
- **Start Application**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **Send URL**
  Sends a configurable HTTP or HTTPS request to a remote server. Assigned to & available for free programmable keys as well as for ’Fixed Keys’.
  The request string contains the **Web server user ID**, **Web server password**, **Parameters**,the phone’s IP address & call number and the **Symbolic Name**

e.g
`userid=jdoe&password=00secret&mode=remote&action=start&ipaddress=192.168.1.244&phonenumber=3338&symbn=key4`

- **Built-in Forwarding**
  Only available for 'Fixed Keys'.
- **Built-in Release**
  Only available for 'Fixed Keys'.
- **Built-in Voice Dial**
  Only available for 'Fixed Keys'.
- **Built-in Redial**
  Only available for 'Fixed Keys'.
- **Personal Directory/Start Phonebook**

NOTE: The Personal Directory/Start PhoneBook function can also be set to the un-shifted /shifted FPK's of OpenStage 15/20/40/60/80 & OpenScape Desk Phone IP 35G / 55 G Eco phones as well as to key modules.
The key label "Start Phonebook" shall be used for the phone version prior to V3R3 and the key label "Personal" for higher phone version.

- **2nd Alert**
- **Corporate Directory**

NOTE: The Corporate Directory function is configured to the V3R3 WP_HI & WP_LO phones.

Key:

Indicates whether this key is a 'Fixed Key'or a freely programmable key.

Key label

A key label can be entered here for every key in the case of Self labeling Keys workpoints (for example, optiPoint 420 standard).

Only available in SIP workpoints.

NOTE: For fixed keys,the key label remains unchanged when the Administration sets a different key function to the default one.

Key label (Unicode)

You can enter the key label in unicode characters for devices in the OpenStage family.

Destination / Feature Code

Destination data to be dialed. This can be a digit string or a URL. Feature codes that need to be sent to external servers (not the SIP server at which the phone is registered) have the following format:

<feature code>@<IP address>

Example: **123@10.2.54.2**

If the destination has been entered for the "Repertory dial" key function, extra control characters can be entered in a digit string:

- **$Q** = clear (CL)
- **$R** = consult (CS)
- **$S** = OK
- **$T** = Pause (PA)

Only available in SIP workpoints.

Forwarding Type

Possible options:

- **on busy**
- **on busy external**
- **on busy internal**
- **on no reply**
- **on no reply external**
- **on no reply internal**
- **unconditionally**
- **unconditionally external**
- **unconditionally internal**

Only available in SIP workpoints.

DTMF Sequence

DTMF Sequence for this target.

Toggle text

Label for the "Feature Toggle" key function.

Only available in SIP workpoints.

Toggle Text (Unicode)

Label for the "Feature Toggle" key function in unicode.

Only available on devices in the OpenStage family (SIP version).

State Key Description

Description text for the state key.

State Key Description (Unicode)

Description text for the state key in unicode. Only available on devices in the OpenStage family (SIP version).

Feature URI / LED Controller URI

URI used to control this feature on the server.

BLF audible Alert

Audible Alert additional to busy lamp field.

BLF PopUp Alert

Additional to busy lamp field a message pops up in display.

BLF Action on Calls:

Possible options:

- **Consult**
- **Transfer**
- **Group pickup**

Application Name:

Name of the XML application to be started with the function key.

Protocol

Protocol of Web Server.

Possible options:

- **HTTP**
- **HTTPS**

Web Server Address

Host name, domain name, or IP address of web server.

Port

Port number of web server: If the port is null, the fully qualified URL will not include the port element.

Path

Directory path and name of the program or web page.

Examples: **servlet/IppGenericServlet** or **webpage/checkin.xml**

The path should have a slash at the beginning and no slash at the end. If the slash at the beginning is missing, a slash will be automatically inserted. If there is an additional slash at the end, it will be automatically removed. The slashes in the path should be forward slashes ('/'). If backslashes ('\') are used instead, the web server may not find the appropriate program or web page.

Parameters

Null, one, or more parameter-value pairs in the format “<parameter>=<value>”, with each pair separated by an ampersand (“&”), e. g. **parameter1=value1&parameter2=value2**. A comma (“,”) is not used as a separator because it could be part of the key or value. If the key or value contains an ampersand, it must be replaced by “&”.

The question mark will be automatically added between the path and the parameters. If there is a question mark at the beginning of the parameters, it will be automatically stripped off.

HTTP Method

HTTP method to be used.

Possible options:

- **Get**
- **Post**

Web Server User ID

User identity known by the server. This information is used for phone authentication by the server.

Web Server Password

Password known by the server. It is used for phone authentication by the server.

Symbolic Name

Symbolic name known by the server. It is used for phone authentication by the server.

Push Support

Enables or disables push support.

Key Functionality

Possible options:

- **Toggle Call Forwarding**
- **Unspecified Call**

- **Unspecified**

ACD

ACD checkbox for the configuration of an AICS zip key function.

NOTE: This flag is enabled only for the key function **AICS Zip** and for specific phones (CP 200 / 400 / 600, for SIP V1R2 and higher).

- If the phone has no AICS Zip keys and you try to add multiple AICS Zip keys, an error message is displayed: **1121: It is not allowed to assign more than one key with the function 'AICS ZIP'.**

- If the phone has one AICS Zip keys and you try to add one or multiple AICS Zip keys, an error message is displayed:
  1121: It is not allowed to assign more than one key with the function 'AICS ZIP'.

- If the phone has 2 or more AICS Zip keys and you try to add one or multiple AICS Zip keys, an error message is displayed:
  1185: It is not allowed to assign more than one key with the function 'AICS ZIP'. Reduce the number of AICS ZIP keys that you already have on the phone from X to 1. , where X is the number of AICS ZIP keys already on the phone.
- If the phone has no AICS Zip keys and you try to add one AICS Zip key,no error message is displayed
- If the phone has any number of AICS Zip keys and you try to add any key or keys (besides AICS Zip), provided that you don’t meet any other restrictions from these keys, no error message is displayed.

Line Key / DSS Key specific Parameters

Primary Line

Specifies whether the line operates as a primary line.

Only available in SIP workpoints.

Address of record

Line’s phone number and address of record.

Only available in SIP workpoints.

Realm

SIP realm for the line’s address of record.

Only available in SIP workpoints.

UserID

Only available in SIP workpoints.

Password

Only available in SIP workpoints.

Ring

Only available in SIP workpoints.

Hunt ranking

Only available in SIP workpoints.

Shared type

Possible options:

- **Private**
- **Shared**
- **Unknown**

Only available in SIP workpoints.

Intrusion allowed

Checkbox for enabling line intrusion.

Only available in SIP workpoints.

Line Hotline Dest. active

Checkbox for activating a line hotline.

Only available in SIP workpoints.

Line Hotline Dial String:

Subscriber number that is used as a destination for the line hotline.

Only available in SIP workpoints.

Hot/Warm Line Type:

Set device property.

- **Ordinary**
- **Hot Line**
- **Warm Line**

Only available in SIP workpoints.

Show in Overview

Checkbox for activating the line display in the line overview.

Only available in SIP workpoints.

Monitor Only

Checkbox for setting the action of the DSS FPK when it is pressed to either Answer or Monitor. Default option is "**False**".

Possible options:

- **True**
- **False**

Only available in SIP workpoints.

Position in Overview

Position of key in Line Overview.

Only available in SIP workpoints.

Short Description

Description of relevant line.

Only available in SIP workpoints.

Line Type

Possible options:

- **Normal**
- **Direct**

Line Action

Possible options:

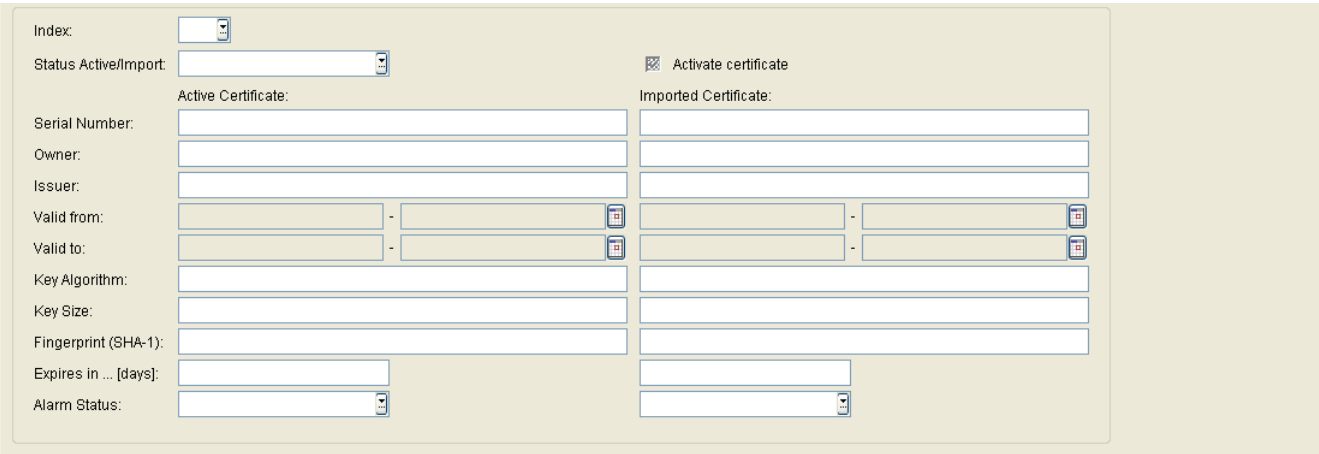
- **Consultation**
- **Transfer**
- **No Action**

Ringing Delay

Time before ringing starts for an alerting call.

7.1.19.3 "Send URL Server CA Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/Keylayout > "Send URL Server CA Certificate" Tab



For a parameter description, please refer to **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Service Integrations** > **"LDAP CA Certificates" Tab**.

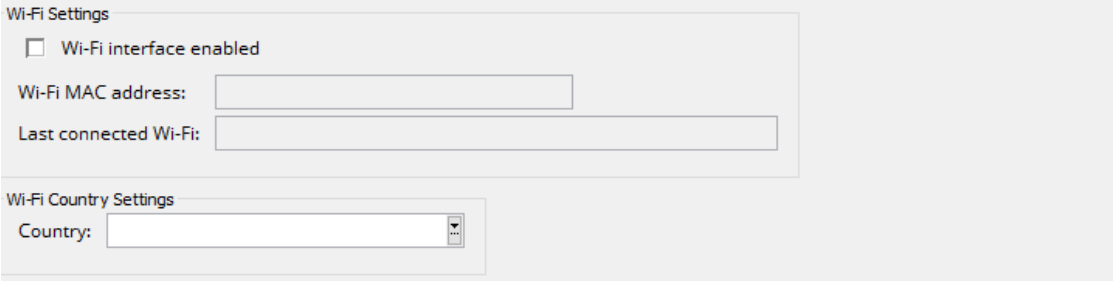
7.1.20 Wi-Fi Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Wi-Fi Settings

This area features the following components:

- "General Items" Tab
- "Network Data" Tab
- WiFi CA Certificates" Tab
- WiFi Client Certificates" Tab
- "WiFi CA Shared Certificates" Tab
- WiFi Client Shared Certificates" Tab

7.1.20.1 "General Items" Tab



Wi-Fi Settings

Wi-Fi interface enabled:

Enables the Wi-Fi interface of the IP phone when the checkbox is selected and disables it otherwise.

Wi-Fi MAC address:

Read only. Shows the media access control address (MAC address) of the phone's Wi-Fi interface. The MAC address is read during boot.

Last connected Wi-Fi:

Read only. Shows the name of the last connected Wi-Fi network.

Wi-Fi Country Settings

Country:

Country where the Wi-Fi device is operated.
Select a country from the drop-down list. The default value is: `GB- United Kingdom`.

7.1.20.2 "Network Data" Tab

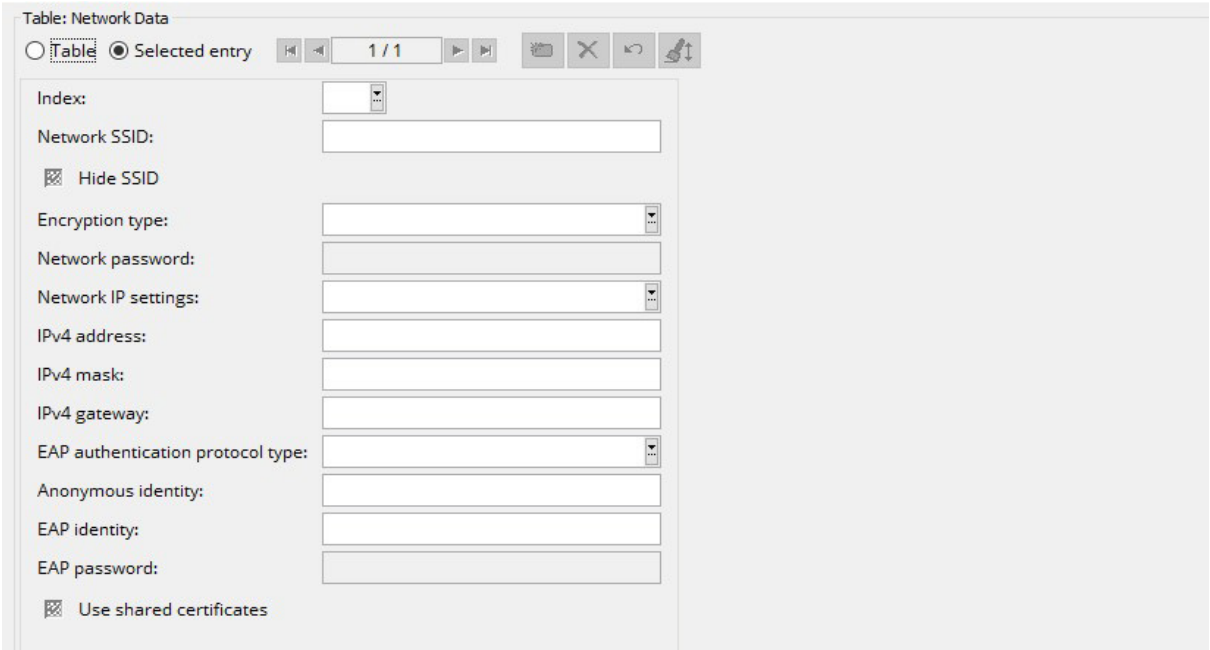


Table: Network Data

Table

Select this option to view Network data in Table Mode.

Selected Entry

This option allows you to view Network data for a selected entry.

Index

Select the index number of the Wi-Fi network.

NOTE: In case you want to configure a certificate connection to a Wi-Fi network, then make sure that the index number of the certificate is the same as the index number of Wi-Fi network.

Network SSID

Enter the name of the Wi-Fi Network.

Hide SSID

Select this option to hide the name of the Wi-Fi Network.

Encryption type:

This field enables you to select the type of key encryption algorithm from a drop-down box with the following choices:

- **ENCRYPTION_NONE**
  Data is not encrypted for transmission in the Wi-Fi.
- **ENCRYPTION_WEP**
  WEP Wi-Fi protected access mode.
- **ENCRYPTION_WPA**
  WPA-PSK encryption.
- **ENCRYPTION_WPA_WPA2**
  WEP encryption.
- **ENCRYPTION_WPA2**
  WPA2 encryption.
- **ENCRYPTION_WPA2_WPA3**
  WPA2 encryption.
- **ENCRYPTION_WPA3**
  WPA2 encryption.
- **ENCRYPTION_WPA_WPA2_EAP**
  WPA2 encryption.
- **ENCRYPTION_WPA2_EAP**
  WPA2 encryption.

Network password:

Enter the password to connect to the Wi-Fi Network.

Network IP Settings:

Click on the drop down menu button to configure IP settings.

A pop-up window is displayed with two options:

- **dhcp** (Dynamic Host Configuration Protocol)

Select this option to enable automatic management of IP addresses on the network.

- **manual**

Select this option to enable manual management of IP addresses on the network.

Click **OK** to save your selection.

IPv4 address:

Enter the adress of IPv4.

IPv4 mask:

Enter the IPv4 mask Wi-Fi number.

IPv4 gateway:

Enter the IPv4 gateway Wi-Fi number.

EAP Authentication protocol type:

Click on the drop down menu button to select an EAP Authentication protocol type.

A pop window is displayed with the following options:

- NONE
- PEAP
- TLS
- LEAP
- FAST

Click **OK** to save your selection.

Anonymous identity:

Enter anonymous identity.

EAP identity:

Enter EAP identity.

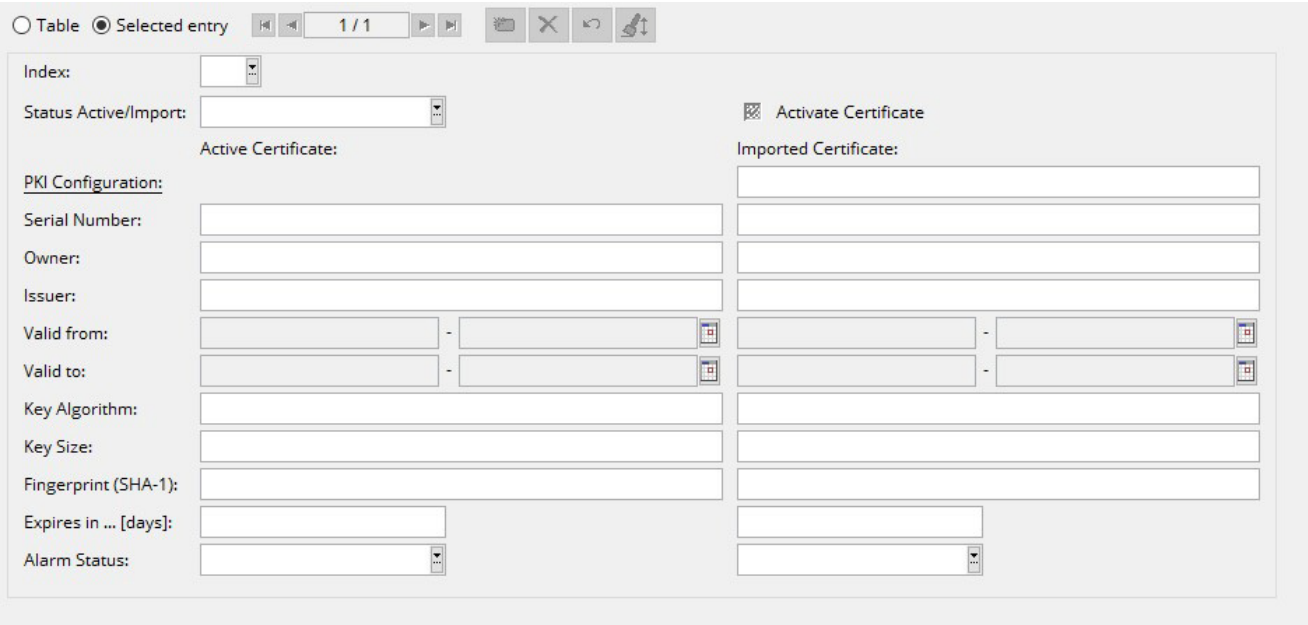
EAP password:

Enter the EAP password number.

Use Shared Certificates:

Select this option to enable use of Shared Certificates.

7.1.20.3 WiFi CA Certificates" Tab



Index

Index number of the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Active Certificate/Imported Certificate:

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity date for the active or imported certificate (display only).

Valid to:

End of validity date for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

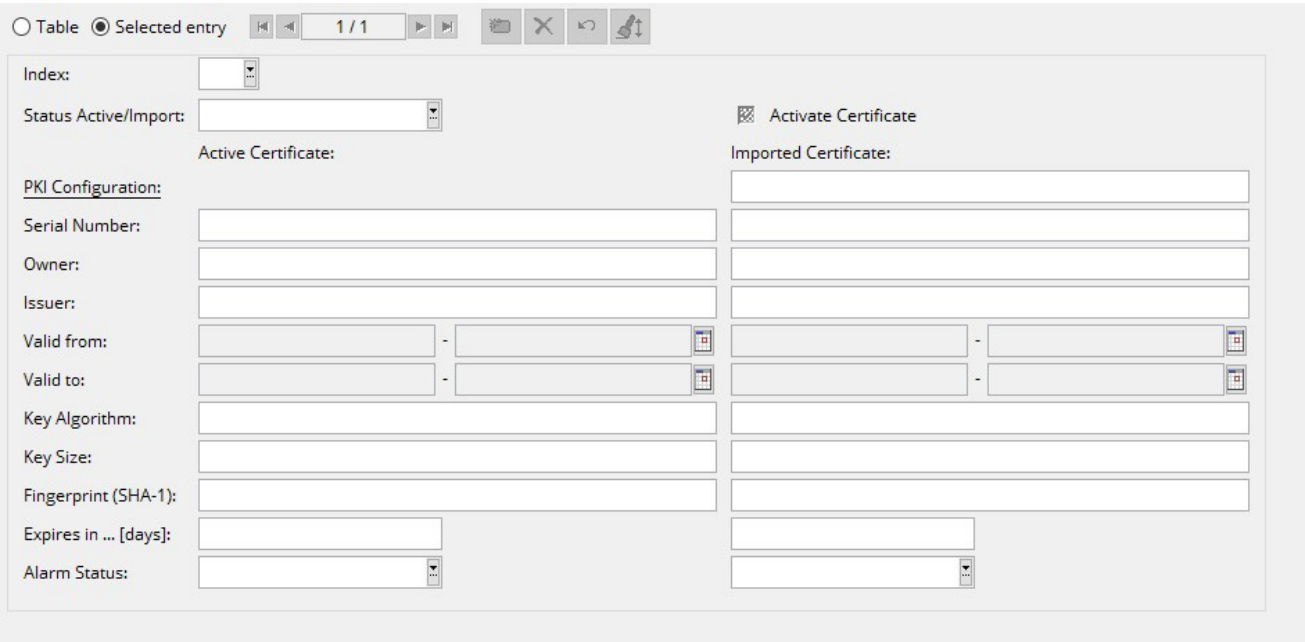
Alarm Status:

Set current alarm status.

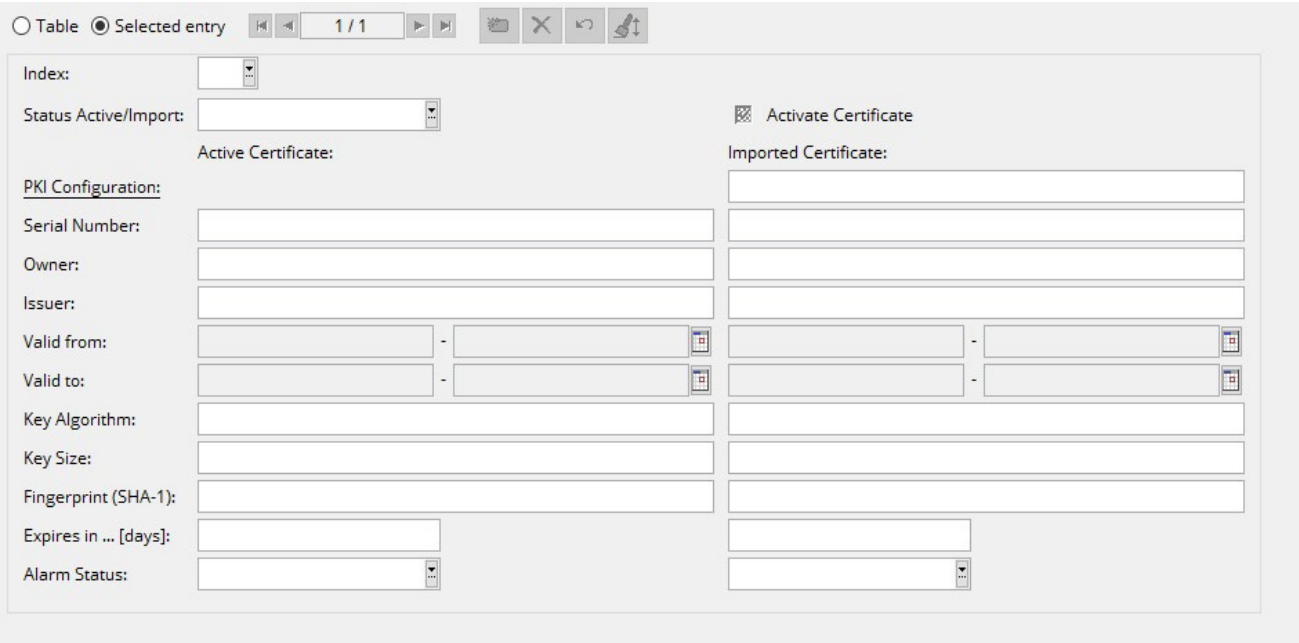
Possible values:

- **valid**
- **soon running out**
- **expired**

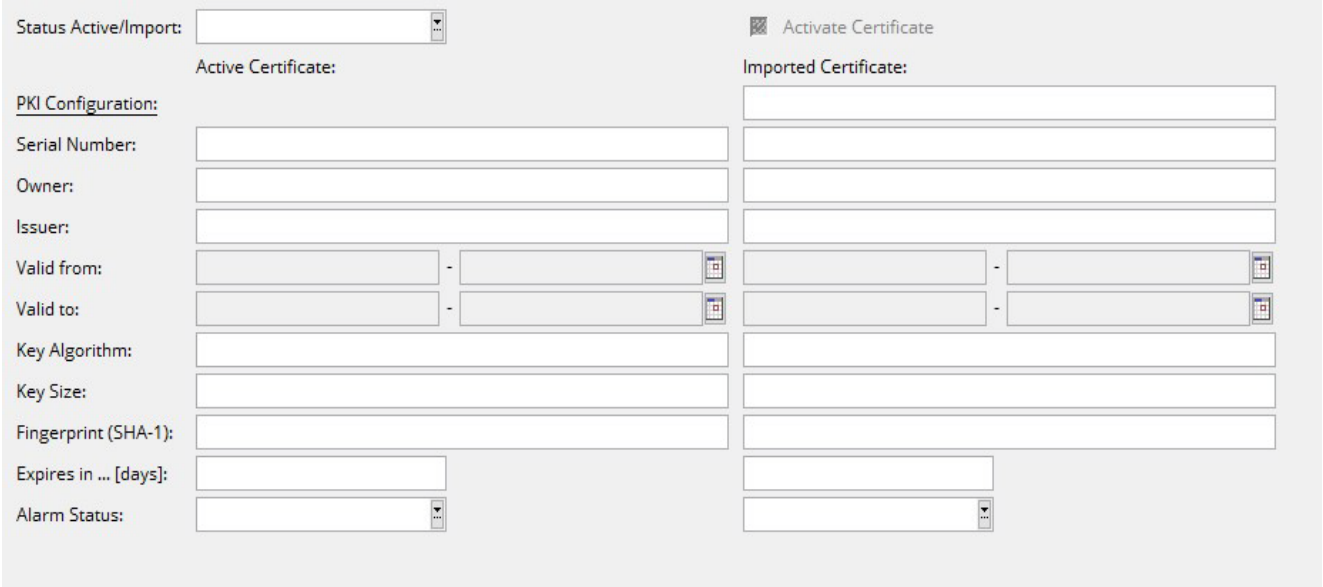
7.1.20.4 WiFi Client Certificates" Tab



7.1.20.5 "WiFi CA Shared Certificates" Tab



7.1.20.6 WiFi Client Shared Certificates" Tab



7.1.21 WLAN Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > WLAN Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "General Data" Tab
- "Security Encryption" Tab
- "Location Server" Tab
- "Advanced Settings" Tab
- "Debug Settings" Tab

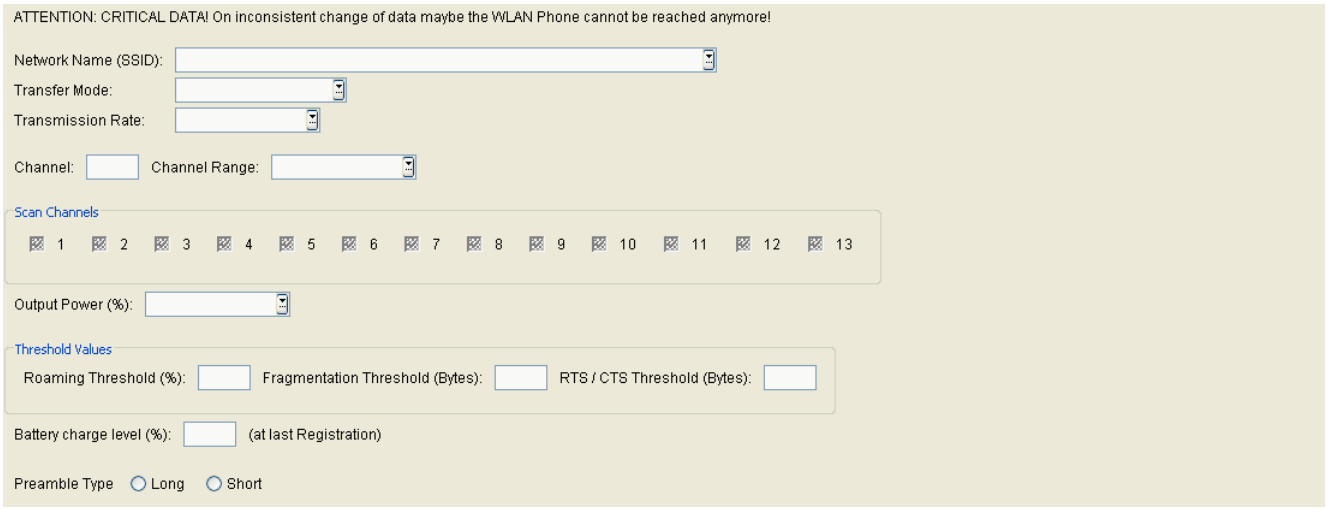
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.21.1 "General Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > WLAN Settings > "General Data" Tab

IMPORTANT: WLAN phone contact may be disrupted if inconsistent data changes are made.



Network Name (SSID)

The SSID is the network name used to identify the WLAN phone. The SSID is defined in the access point (WLAN router).

Transfer Mode:

You can choose the standards IEEE 802.11b (**802.11b only**), or IEEE 802.11b and IEEE 802.11g (**mixed mode**) for data transfer.

The main difference between these standards is the transmission rate. IEEE 802.11g is almost five times faster than the others. If devices in the WLAN use different standards, you must keep the default value (Mixed Mode).

If IEEE 802.11g is entered as a fixed value for transfer mode in the access point or WLAN router, select **Mixed Mode** in this tab.

Possible options:

- **only 802.11b**
- **Mixed Mode**

Transmission Rate:

The transmission rate is the speed in Mbps at which data is transmitted in the WLAN. The transmission rate depends on the transfer mode selected.

Possible options:

- **1.0 Mbps**
- **2.0 Mbps**
- **5.6 Mbps**
- **6.0 Mbps**
- **9.0 Mbps**
- **11.0 Mbps**
- **12.0 Mbps**
- **18.0 Mbps**
- **24.0 Mbps**
- **36.0 Mbps**
- **48.0 Mbps**
- **54.0 Mbps**

Channel:

WLAN radio channel. The channel is configured in the access point or the WLAN router.

Channel Range:

The available channel range in each case can be selected. The restriction is required in some countries due to the fact that the use of channel 12 and 13 is not permitted. Possible values: channel 1-11: for example USA, channel 1-13: for example Germany, channel 1-14: for example Japan.

Scan Channels:

Scan channel selection.

Output Power (%)

Output power that the handset uses to transmit to the access point. Up to 100 mW or 20 dBm (100%) output power is permitted.

Possible options:

- **5 %**
- **10 %**
- **20 %**
- **40 %**
- **100 %**

Threshold Values

Roaming Threshold (%):

Minimum reception strength expressed as a percentage. If the reception strength of the access point currently connected falls below this value, the handset searches for and connects to another access point with better connectivity.

Fragmentation Threshold

Size at which voice packets are fragmented. Fragmenting data packets into smaller packets improves data throughput in a WLAN when the network is running at high capacity.

Value range: **256** ... **2346** bytes.

Default value: **2346** bytes (no fragmenting).

RTS/CTS Threshold:

Minimum packet size in bytes required for transmitting an RTS (Request To Send). Smaller packets are transmitted directly to the access point without an RTS.

Value range: **1** ... **2347** bytes.

Default value: **2347** bytes (RTS/CTS mechanism deactivated).

NOTE: Activating this mechanism may reduce data throughput.

Battery charge level (%): (at last Registration)

Battery charge level in percent of the WLAN phone at the last logon.

Preamble Type

A preamble is set before each data packet is transmitted in a WLAN. It enables the receiver to synchronize with the transmission timing.

A long preamble ensures more stable synchronization. A short preamble enables higher data throughput.

Not all WLAN devices support both preamble types.

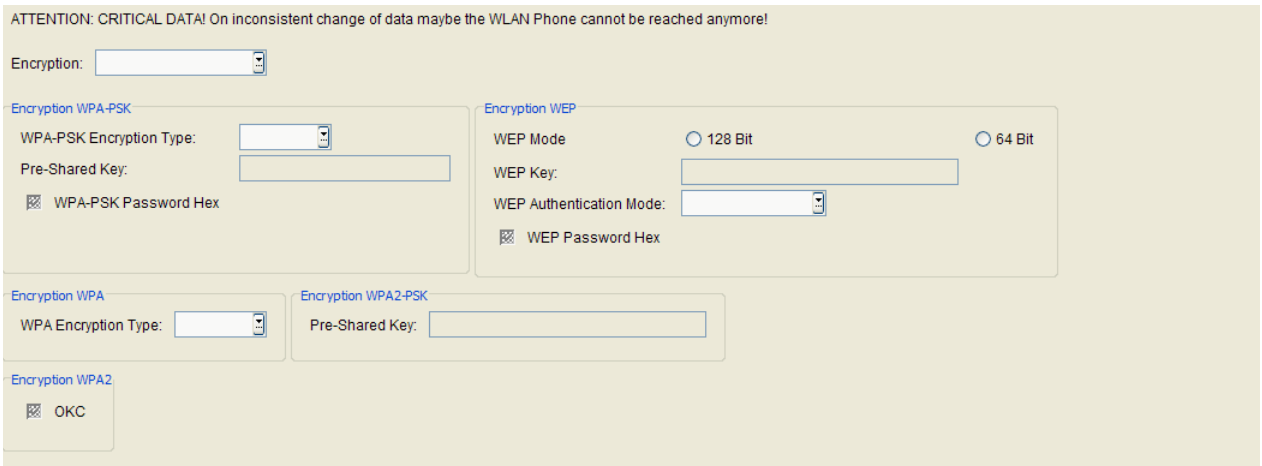
Possible options:

- **Long**
- **Short**

7.1.21.2 "Security Encryption" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > WLAN Settings > "Security Encryption" Tab

IMPORTANT: WLAN phone contact may be disrupted if inconsistent data changes are made.



NOTE: Encryption protects data exchange in the WLAN. It does not protect data exchange with Ethernet networks or the Internet.

Encryption:

This field enables you to select the encryption procedure.

Possible options:

- **None**
  Data is not encrypted for transmission in the WLAN.
- **WPA**
  WPA encryption.
- **WPA-PSK**
  WPA-PSK encryption.
- **WEP**
  WEP encryption.
- **WPA2**
  WPA2 encryption
- **WPA2-PSK (AES)**
  WPA2-PSK encryption

Encryption WPA-PSK

WPA-PSK Encryption Type:

Possible options:

- **TKIP**
  Encryption using the TKIP protocol. Designed for use with WPA-PSK.

Pre-Shared Key:

Entry field for PSK encryption key.

WPA-PSK Password Hex

Checkbox for activating the WPA-PSK password hex.

Encryption WPA2-PSK

Pre-Shared Key:

Entry field for WPA2-PSK encryption key.

Encryption WPA2

OKC:

Checkbox for activating the Opportunistic Key Caching (OKC).

Encryption WEP

WEP Mode

Information on the WEP key length. For 128 bits, the key must consist of 13 ASCII characters or 26 hexadecimal characters. For 64 bits, it must consist of five ASCII characters or 10 hexadecimal characters.

WEP Key:

Entry field for WEP encryption key.

WEP Authentication Mode:

Possible options:

- **Open System**
  The WEP key is only used for data encryption, not for authentication.
- **Shared Key**
  The WEP key is also used for authentication in the WLAN. In other words, the handset can only log on to the WLAN if it transmits the correct key.

WEP Password Hex

Checkbox for activating the WEP password hex.

Encryption WPA

WPA Encryption Type:

Possible options:

- **TKIP**

Encryption using the TKIP protocol. Designed for use with WPA.

Encryption WPA2-PSK

Pre-Shared Key

Entry field for PSK encryption key.

Encryption WPA2

OKC

Switch to activate Opportunistic Key Caching (OKC).

7.1.21.3 "Location Server" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > WLAN Settings > "Location Server" Tab



Location Server

If this checkbox has been enabled, the data for an existing location server is used.

Location Server Address:

IP address or host name of the location server.

Location Server Port:

Port number of the location server.

7.1.21.4 "Advanced Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > WLAN Settings > "Advanced Settings" Tab



U-APSD Support

U-APSD

Activate U-APSD.

Max. Service Period Length (packets)

Maximum length of the service period, expressed as a number of packets.

Possible Options:

- **unlimited max. 15**
- **2**
- **4**
- **6**

Roaming Scan Settings

Max. Number of AP Frames

Maximum number of AP frames.

Min. Channel Duration

Minimum channel duration.

Max. Channel Duration

Maximum channel duration.

Number of Probe Requests

Number of probe requests.

Timeout

Timeout after seconds.

7.1.21.5 "Debug Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > WLAN Settings > "Debug Settings" Tab



Enable Debug Messages

If switch is active, debug messages will be recorded.

7.1.22 Signaling and Payload Encryption (SPE)

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Signaling and Payload Encryption (SPE)

This area features the following components:

- General Data
- Possible Action Buttons
- "SPE Certificate" Tab
- "SPE CA Certificates" Tab
- "SIP Settings" Tab
- "HFA Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

7.1.22.1 "SPE Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "SPE Certificate" Tab

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Number of days before the certificate expires.

> ***NOTE:*** The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

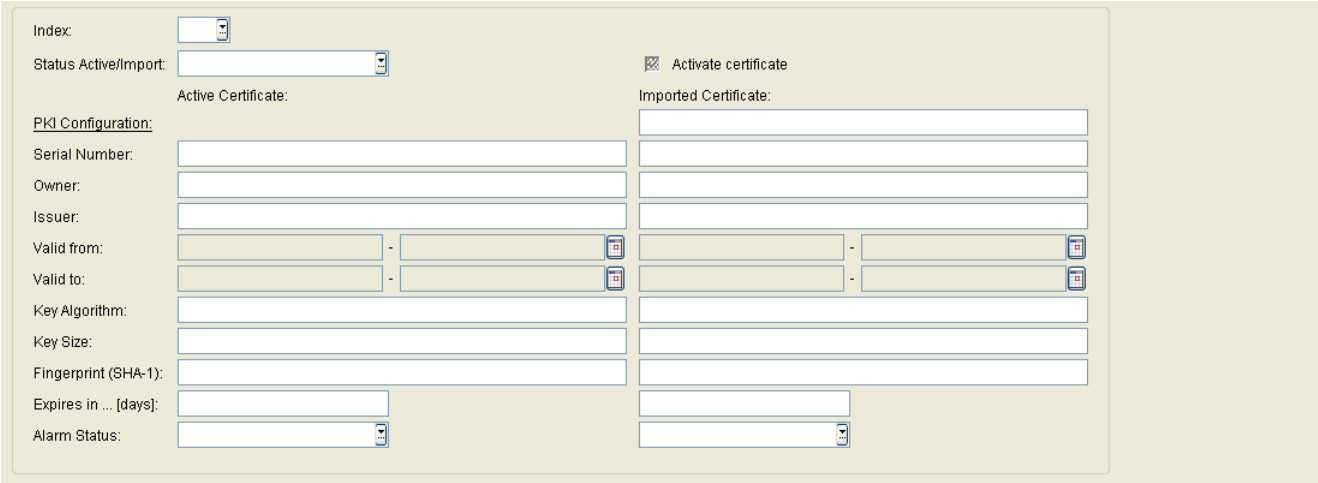
Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.22.2 "SPE CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "SPE CA Certificates" Tab



The parameters described below are available once for the currently active certificate and once for the imported certificate.

Index:

Serial number of the CA certificate.

Status Active/Import:

Specifies whether a certificate is registered as imported and/or active on the phone. The five statuses listed below are possible.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

PKI Configuration

Name of PKI configuration.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Number of days before the certificate expires.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Displays the duration of validity for certificates when searching for certificates due to expire.

Possible values:

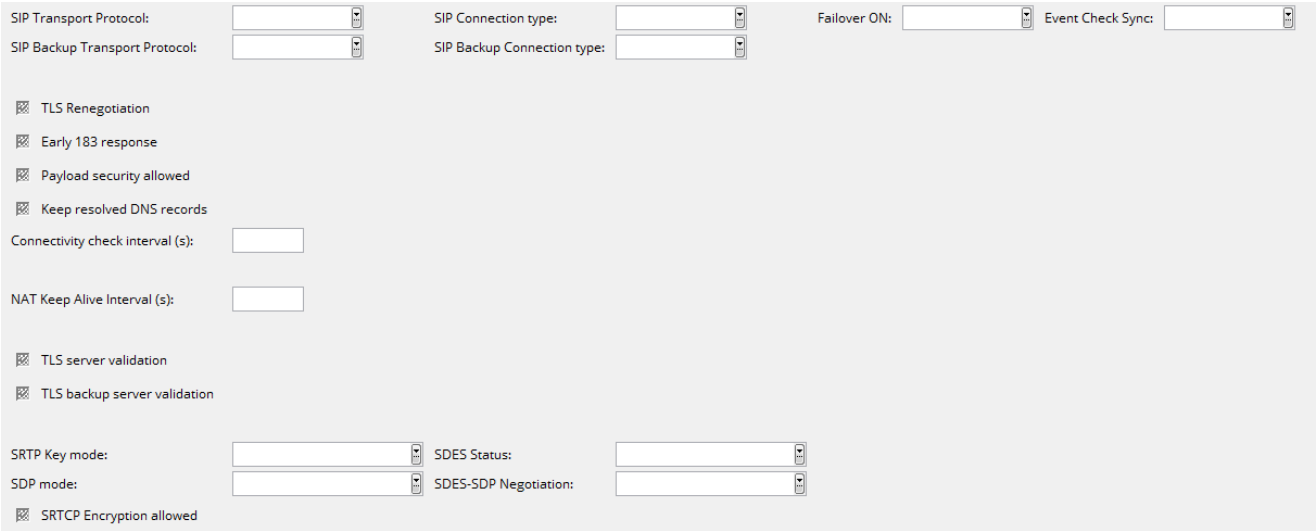
- **valid**
- **soon running out**
- **expired**

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

7.1.22.3 "SIP Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "SIP Settings" Tab



SIP Transport Protocol:

Protocol for SIP signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

SIP Backup Transport Protocol:

Possible options:

- **UDP**
- **TCP**

SIP Connection Type:

Determines the connection type of the phone with main SIP server.

Possible options:

- **Persistent**

  Phone is always acting as connection client, no listening port gets opened to allow incoming connection attempts.

- **Listening**

  Phone opens a listening port on the configured local SIP protocol.

SIP Backup Connection Type:

Determines the connection type of the phone with backup SIP server.

Possible options:

- **Persistent**

  Phone is always acting as connection client, no listening port gets opened to allow incoming connection attempts.

- **Listening**

  Phone opens a listening port on the configured local SIP protocol.

Failover ON:

Determines the phone failover to the next SRV priority IP on 500/503 server responses so that users can continue to use their desk phones on temporary issues.This functionality is available only to CP200 / CP400 / CP600 V1R2 phones and higher.

Possible options:

- **0 (Timeout only)**
- **1 (Timeout and Error)**

Default value: **0 (Timeout only)**

Event Check Sync:

Enumeration value of "Event check-sync"

NOTE: This item is available only for specific phones (CP 200 / 400 / 600, for SIP V1R2 and higher).

Possible options:

- **disabled**
  the phone will reject handling of check-sync events
- **challenge(default)**
  Default value, also current phone behavior. If digest authentication parameters are set, the phone will challenge the server for authentication
- **no challenge**
  the phone will never challenge the server for authentication

TLS Renegotiation

When activated, access is allowed to TLS Servers that don't support secure TLS renegotiation (through RFC 5746).

When disabled, access to servers without secure TLS Renegotiation (according to rfc) is denied.

This checkbox is disabled by default.

Early 183 response

If enabled, the phone will send a SIP 183 response with an SDP answer.

This checkbox is disabled by default.

It is also disabled for all OpenStage /Desk Phone IP devices.

Payload security allowed

When activated, payload security is allowed.

Keep resolved DNS records

When enabled, previously resolved DNS records are kept in case of any DLS issues.In that way, CP phones are able to make emergency calls.

Connectivity check interval

Connectivity check interval in seconds.

NAT Keep Alive Interval (sec):

Timer interval that controls the transfer rate of keep-alive packets. If the value equals **0**, the NAT keep-alive mechanism is switched off.

TLS server validation

When activated, the TLS connection to the SIP server is validated.

For OpenStage < 3.0 only.

TLS backup server validation

If this checkbox is activated, the TLS connection to the backup SIP server is validated.

SRTP Key mode

SRTP type(s) for secure calls. Identifies the type of SRTP that is allowed to be offered or accepted via SDP.

Possible values:

- **MIKEY**
- **SDES**
- **DTLS**
- **DTLS-SDES**

Default value is **DTLS-SDES**

NOTE: These items are disabled for all OpenStage / Desk Phone IP devices.

SDP mode

SDP Negotiation mode for secure calls. Identifies the SDP capability tha configures whether fallback to RTP will be used and which BE-SRTP approach will be used.

Possible values:

- **RTP and SRTP (2mline)**
- **SRTP and RTP (2mline)**
- **SRTP only**
- **SRTP and RTP (1mline)**

Default value is set to **RTP and SRTP (2mline)**

NOTE: These items are disabled for all OpenStage / Desk Phone IP devices.

SDES Status

Select the SDES status.

Possible options:

- **disabled** (MIKEY automatically added as SRTP type)
- **enabled** (SDES added as SRTP type)

SDES-SDP Negotiation

Select the SDP negotiation.

Possible options:

- **SRTP and RTP**
- **SRTP only**
- **Fallback to RTP**

SRCTP Encryption allowed

When activated, SRCTP encryption will be applied.

SRTP Encryption

SRTP Encryption Method

Selects the SRTP encryption method to be used.

Possible options:

- **AES_CM_128_HMAC_SHA1_32**
- **AES_CM_128_HMAC_SHA1_80**
- **AES_CM_256_HMAC_SHA1_80**

SRTP Encryption Rank

Selects the SRTP Encryption Rank.

Possible options:

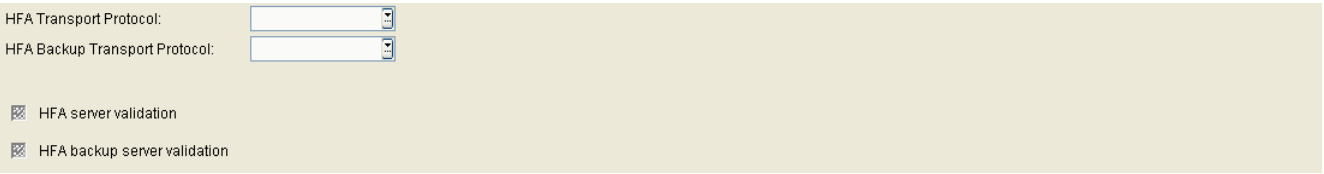
- **Choice 1**
- **Choice 2**
- **Choice 3**

SRTP Encryption allowed

When activated, SRTP will be encrypted.

7.1.22.4 "HFA Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Signaling and Payload Encryption (SPE) > "HFA Settings" Tab



HFA Transport Protocol:

Protocol for HFA alerting.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

HFA Backup Transport Protocol:

Protocol for HFA alerting.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

HFA server validation

If this checkbox is activated, the connection to the HFA server is verified.

HFA backup server validation

If this checkbox is activated, the connection to the HFA backup server is verified.

7.1.23 IEEE 802.1x

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IEEE 802.1x

NOTE: For detailed information on configuring IEE 802.1x, see the "IEE 802.1x Configuration Management" Administration Manual available online at
http://wiki.unify.com/wiki/VoIP_Security#IEEE_802.1X
and
http://wiki.unify.com/images/2/23/IEEE_802.1X_Configuration_Management.pdf

This area features the following components:

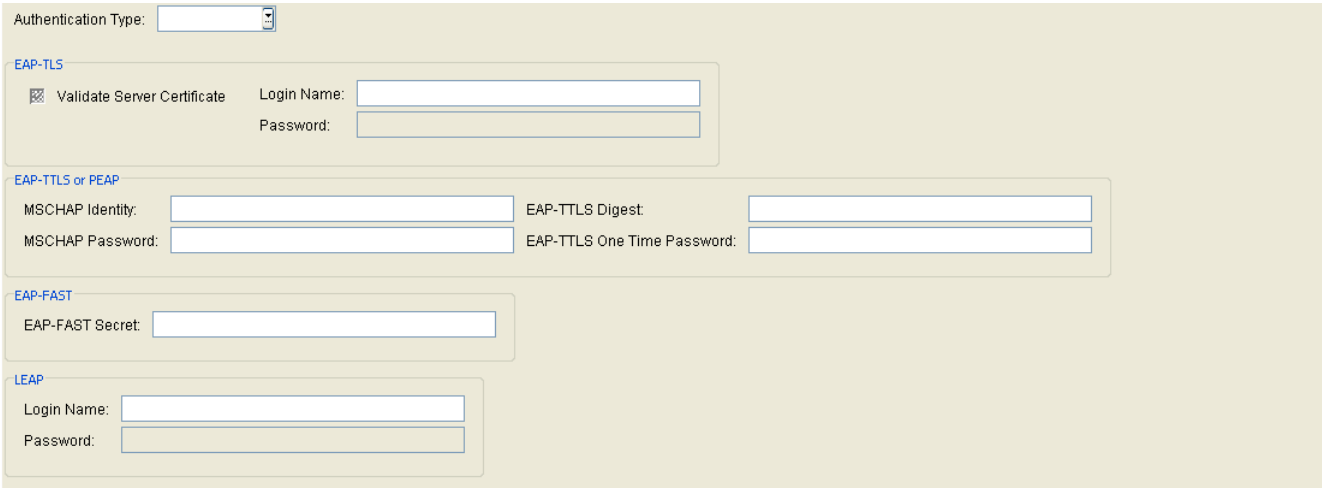
- General Data
- Possible Action Buttons
- "802.1x Settings" Tab
- "Phone Certificate" Tab
- "RADIUS Server CA Certificate 1" Tab
- "RADIUS Server CA Certificate 2" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.23.1 "802.1x Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IEEE 802.1x > "802.1x Settings" Tab



Authentication Type

Possible values:

- **none**
- **EAP-TLS**
- **LEAP**
- **PEAP**

EAP-TLS

Validate Server Certificate

If this checkbox is activated, the telephone checks the validity of the server certificate sent by the access point.

> ***IMPORTANT:*** In the case of OpenStage V3R0 phones (or later) the Server Certificate flag is controlled by **802.1x Authentication Policy** under Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Security Settings > "Authentication Policy" Tab. Therefore, whatever the value of Authentication Type, this checkbox is greyed out, thus not editable
> Please refer to Section 7.1.7.10, ""Authentication Policy" Tab".

Login Name:

Login name for identification.

Password:

Password for identification.

EAP-TTLS or PEAP

Provide support for IEEE 802.1x [802.1x] which is a standard for port-based network access control. 802.1x provides an authentication framework where a user (or device) is authenticated by a central authority (in RADIUS model) and where the user (or device) also authenticates the central authority. With this selection EAP-TTLS or PEAP protocol does the extensible authentication.

MSCHAP Identity:

Device name for MSCHAP-V2 in PEAP or EAP-TTLS.

> ***NOTE:*** If the new value “PEAP” is selected, the attribute “MSCHAP Identity” (Item: mschap-identity) is enabled.

MSCHAP Password:

Password for MSCHAP-V2 in PEAP or EAP-TTLS.
The value is write-only.

> ***NOTE:*** If the new value “PEAP” is selected, the attribute “MSCHAP Password” (Item: mschap-pw) is enabled.

EAP-TTLS Digest

Challenge digest for MD challenge with EAP-TTLS.
The value is write-only.

EAP-TTLS One Time Password

One time password for use with EAP-TTLS.
The value is write-only.

EAP-FAST

EAP-FAST Secret:

Secret for EAP-FAST.
The value is write-only.

LEAP

Login Name:

Login name for identification on the access point/WLAN router.

Password:

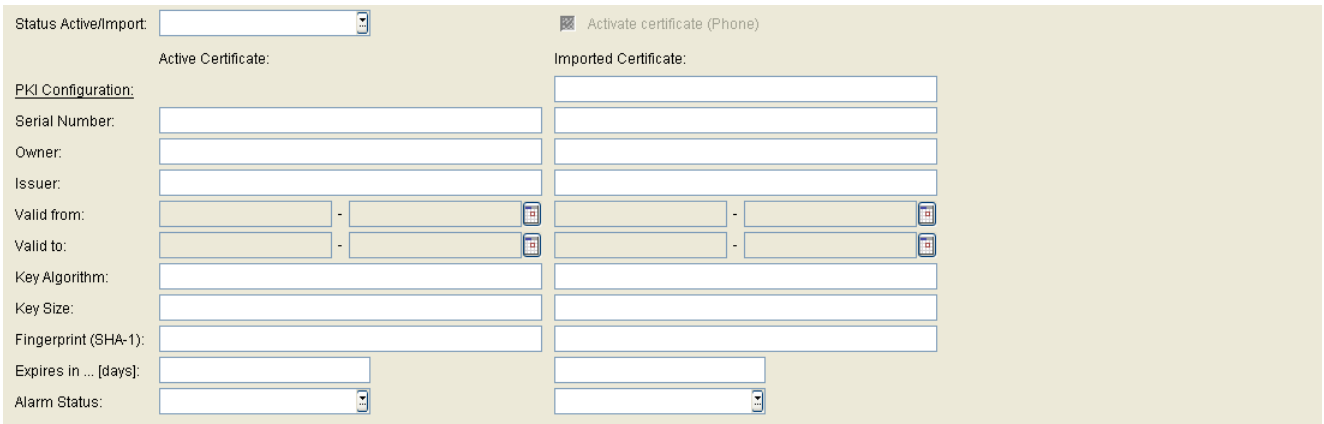
Password for identification on the access point/WLAN router.

7.1.23.2 "Phone Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IEEE 802.1x > "Phone Certificate" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

IMPORTANT: In the case of hardware change via DLS API, from an old device to a new one already registered in DLS, the Phone Certificate will not be replaced to the new device.



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate (Phone)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

PKI Configuration

PKI configuration of the imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

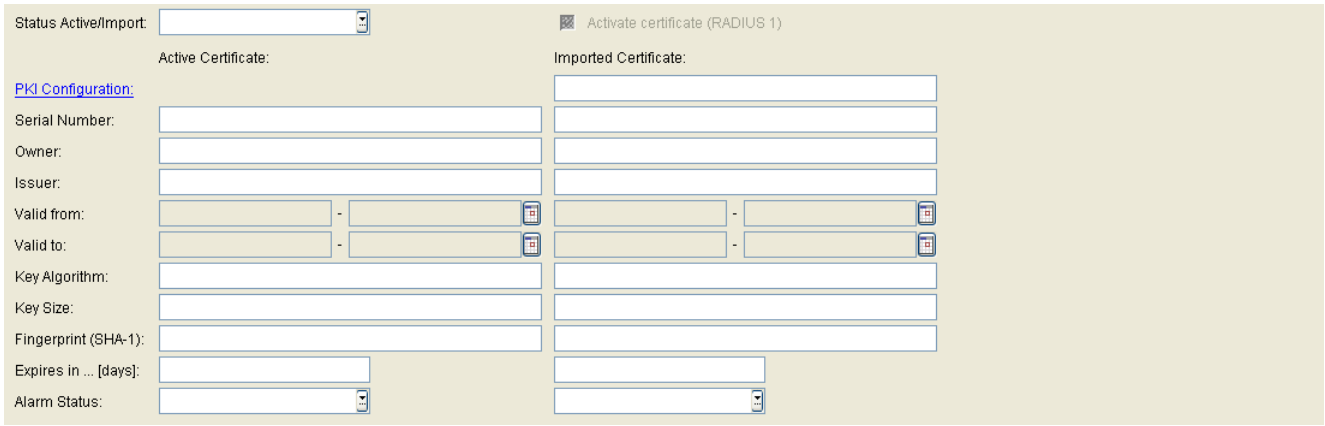
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.23.3 "RADIUS Server CA Certificate 1" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IEEE 802.1x > "RADIUS Server CA Certificate 1" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate (RADIUS 1)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

PKI Configuration

PKI configuration of the imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

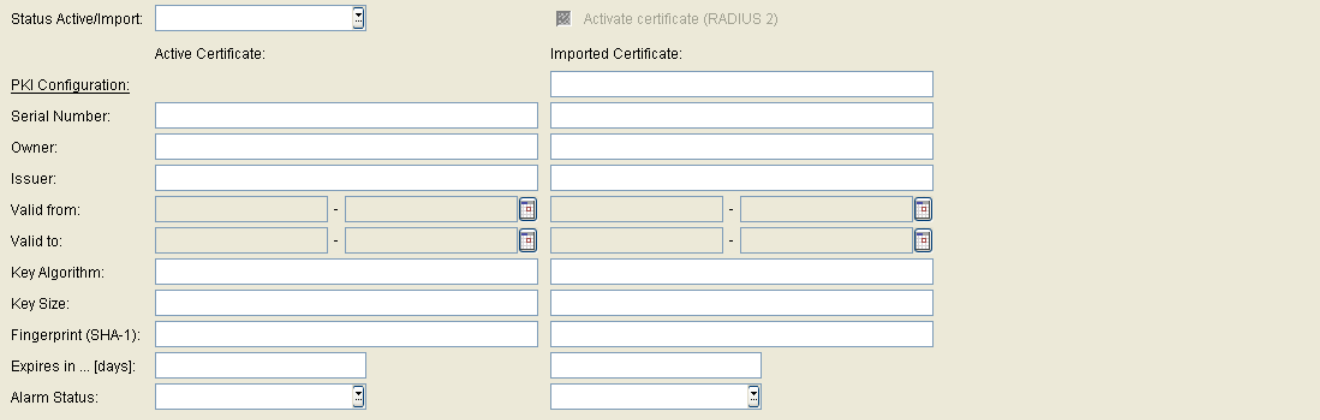
Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.23.4 "RADIUS Server CA Certificate 2" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > IEEE 802.1x > "RADIUS Server CA Certificate 2" Tab

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate (RADIUS 2)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

PKI Configuration

PKI configuration of the imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.24 Diagnosis

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis

This area features the following components:

- General Data
- Possible Action Buttons
- "Diagnostic Settings" Tab
- "File Settings" Tab
- "Secure Shell (SSH) access" Tab
- "Remote Trace Settings" Tab
- "Diagnosis and Security Log Files" Tab
- "Periodical File Upload" Tab
- "Secure Trace Settings" Tab

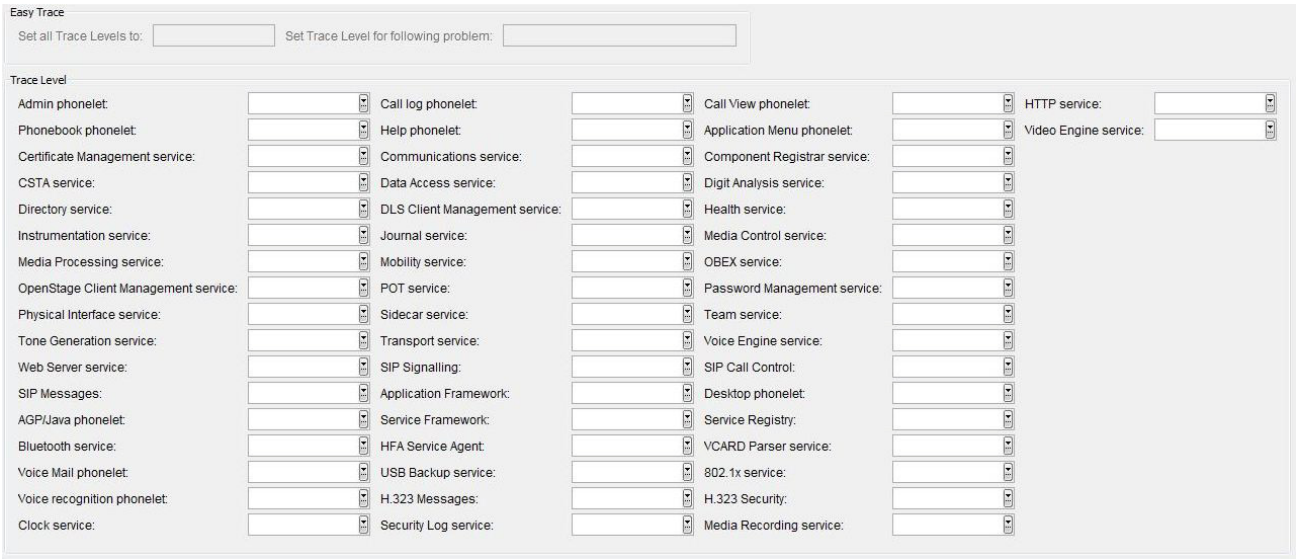
For information on general interface operation, see Section 5.4.2, "Work Area".

7.1.24.1 "Diagnostic Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "Diagnostic Settings" Tab

Error tracing is defined here for the individual telephone components. The trace files are uploaded from the telephone to a server via FTP or HTTPS.

> ***NOTE:*** These settings are also available for OpenStage 15/20 (SIP only) & OpenScape Desk Phone IP 35 G / 35 G Eco phones.



Easy Trace

Pre-defined profiles facilitate the controlling of trace parameters. Common trace levels for all components can be configured, as well as groups of parameters which belong to a specific functional area of the phone.

Set all Trace Levels to:

Activates all trace points in code from OpenStage phones. A different value may be set for each trace level.

Possible Options:

- **Off**
- **Fatal**
- **Error**
- **Warning**
- **Trace**
- **Debug**

Set Trace Level for following problem:

Select a functional area in the phone for which the Easy Trace profile is to be set.

Possible Options:

- **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

Activates particular trace points in code from the OpenStage phones and locates errors. A different value may be set for each trace level.

Admin phonelet:

Possible options:

- **Off**
- **Fatal**
- **Error**
- **Warning**
- **Trace**
- **Debug**

Call log phonelet:

Same options as for Admin phonelet:

Phonebook phonelet:

Same options as for Admin phonelet:

Certificate Management service:

Same options as for Admin phonelet:

CSTA service:

Same options as for Admin phonelet:

Directory service:

Same options as for Admin phonelet:

Instrumentation service:

Same options as for Admin phonelet:

Media Processing service:

Same options as for Admin phonelet:

OpenStage Client Management service:

Same options as for Admin phonelet:

Physical Interface service:

Same options as for Admin phonelet:

Tone generation service:

Same options as for Admin phonelet:

Web Server service:

Same options as for Admin phonelet:

SIP Messages:

Same options as for Admin phonelet:

AGP/Java phonelet:

Same options as for Admin phonelet:

Bluetooth service:

Same options as for Admin phonelet:

Voice Mail phonelet:

Same options as for Admin phonelet:

Voice recognition phonelet:

Same options as for Admin phonelet:

Call Log phonelet:

Same options as for Admin phonelet:

Help phonelet:

Same options as for Admin phonelet:

Communications service:

Same options as for Admin phonelet:

Data Access service:

Same options as for Admin phonelet:

DLS Client Management service:

Same options as for Admin phonelet:

Journal service:

Same options as for Admin phonelet:

Mobility service:

Same options as for Admin phonelet:

Pot service:

Same options as for Admin phonelet:

Sidecar service:

Same options as for Admin phonelet:

Transport service:

Same options as for Admin phonelet:

SIP Signalling:

Same options as for Admin phonelet:

Application Framework:

Same options as for Admin phonelet:

Service Framework:

Same options as for Admin phonelet:

HFA Service Agent:

Same options as for Admin phonelet:

USB Backup service:

Same options as for Admin phonelet:

H.323 Messages:

Same options as for Admin phonelet:

Security Log service:

Same options as for Admin phonelet:

Call View phonelet:

Same options as for Admin phonelet:

Application Menu phonelet:

Same options as for Admin phonelet:

Component Registrar service:

Same options as for Admin phonelet:

Digit Analysis service:

Same options as for Admin phonelet:

Health service:

Same options as for Admin phonelet:

Media Control service:

Same options as for Admin phonelet:

OBEX service:

Same options as for Admin phonelet:

Password Management service:

Same options as for Admin phonelet:

Team service:

Same options as for Admin phonelet:

Voice engine service:

Same options as for Admin phonelet:

SIP Call Control:

Same options as for Admin phonelet:

Desktop phonelet:

Same options as for Admin phonelet:

Service Registry:

Same options as for Admin phonelet:

VCARD Parser service:

Same options as for Admin phonelet:

802.1x service:

Same options as for Admin phonelet:

H.323 Security:

Same options as for Admin phonelet:

Media Recording service:

Same options as for Admin phonelet:

HTTP service:

Same options as for Admin phonelet:

Video Engine service:

Same options as for Admin phonelet:

Ansible service:

Same options as for Admin phonelet:

OpenScape UC service:

Same options as for Admin phonelet:

Exchange service:

Same options as for Admin phonelet:

WSI service:

Same options as for Admin phonelet:

Conversations API:

Same options as for Admin phonelet:

GPAL Audio Framework:

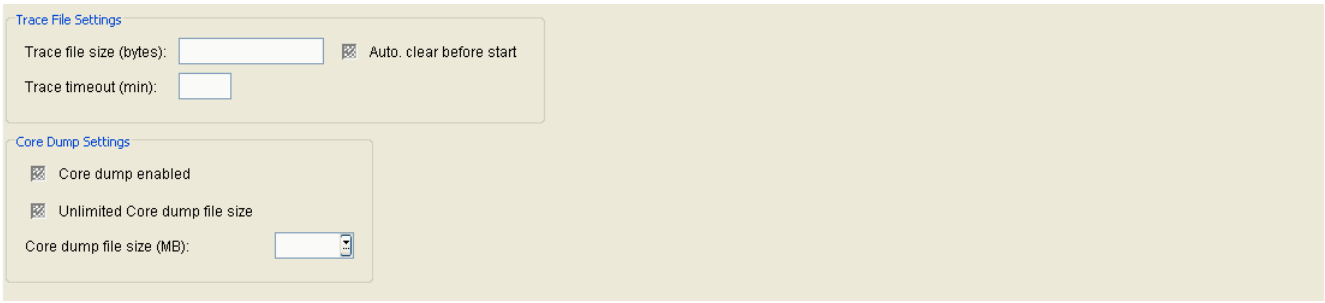
Same options as for Admin phonelet:

GPAL Audio Core:

Same options as for Admin phonelet:

7.1.24.2 "File Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "File Settings" Tab



Trace File Settings

Trace file size (bytes)

Specifies the maximum size of the trace file.

Value range: **65536** ... **4194304** (64KB ... 4MB).

Trace Timeout (min):

Defines the number of minutes after which a timeout for tracing should be activated.

Auto. clear before start

Defines whether the trace memory should be emptied before a new trace is executed.

Core Dump Settings

Core dump enabled

Checkbox for activating the core dump.

Unlimited Core dump file size

If this checkbox is activated, the size of a core dump file is not limited.

Core dump file size (MB)

Specifies the maximum size of the trace file.

Value range: **0** ... **1023**

Default value: **1000**

7.1.24.3 "Secure Shell (SSH) access" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "Secure Shell (SSH) access" Tab



Secure Shell (SSH) access allowed

If this checkbox is active, the phone can be accessed via SSH.

7.1.24.4 "Remote Trace Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "Remote Trace Settings" Tab



Remote Trace

If this checkbox is active, the phones sends its trace data directly to the destination entered in **Remote Trace Destination**.

User Notification

If activated, the phone user will be notified when a trace is performed on the phone.

Remote Trace Destination

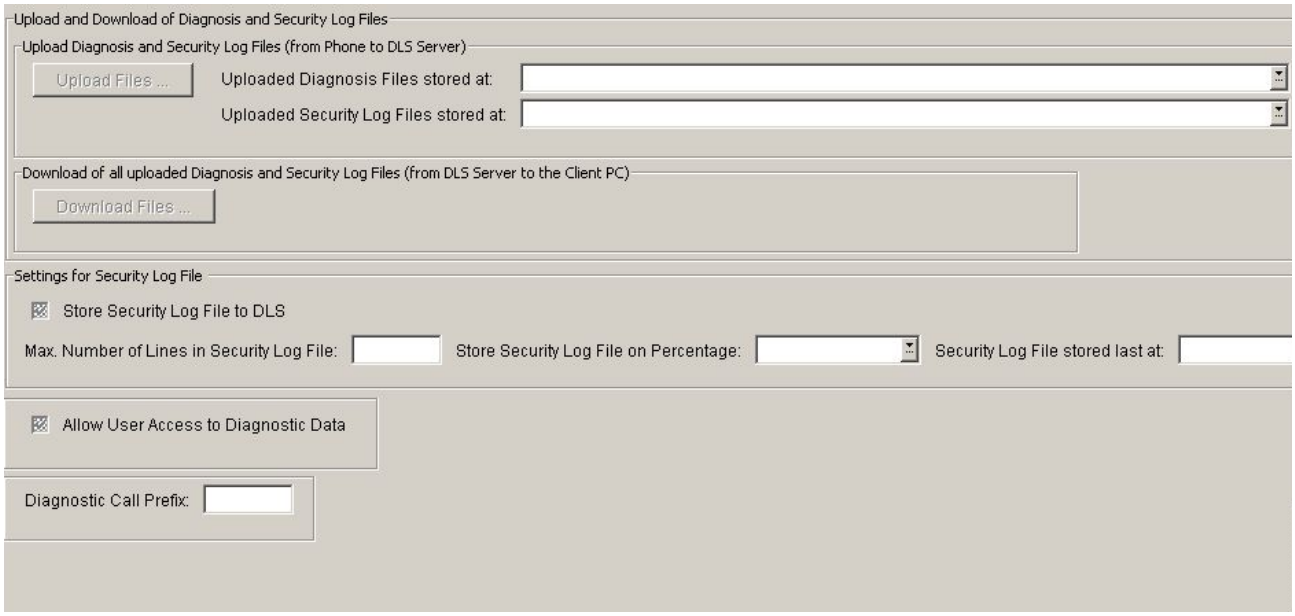
IP address or hostname of the server to which the trace data are sent.

Remote Trace Port

Number of the port at which the server receives the trace data.

7.1.24.5 "Diagnosis and Security Log Files" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "Diagnosis and Security Log Files" Tab



Upload and Download of Diagnosis and Security Log Files

Upload Diagnosis and Security Log Files (from Phone to DLS Server)

Upload Files ...

Starts a single upload of diagnosis- and security log files, independent of the settings for periodical uploads. The files to be uploaded can be selected in a popup window.

Uploaded Diagnosis Files stored at:

Storage path for the diagnosis files that have been uploaded for this device. The path can be set via **Main Menu** > **Administration** > **File Server** > **OpenStage Diagnosis Files**.

Uploaded Security Log Files stored at:

Storage path for the security log files that have been uploaded for this device. The path can be set via **Main Menu** > **Administration** > **File Server** > **OpenStage Security Log Files**.

Download of all Diagnosis and Security Log Files (from DLS Server to Client PC)

Download Files ...

Starts downloading all diagnosis and security log files from phone to DLS Server as a .zip-file.

Settings for Security Log File

Store Security Log File to DLS

When active, the security log file of this IP Device is stored by the DLS.

Max. Number of Lines in Security Log File:

Sets the maximum number of entries that may be contained in the security log file.

Value range: **100** … **1000**

Store Security Log File on Percentage

Determines the percentage of unstored entries. The percentage depends on the value of **Max. Number of Lines in Security Log File**. When the percentage is exceeded, the security log file is sent to the DLS for storing.

Possible Options:

- **save immediately**
- **10%**
- **20%**
- **30%**
- **35%**
- **40%**
- **45%**
- **50%**
- **55%**
- **60%**
- **65%**
- **70%**
- **80%**

- **90%**

Security Log File stored last at

Date at which the security log file has been stored lastly.

Allow User Access to Diagnostic Data

If switch is active, the OpenStage phone user is allowed to access diagnostic data on the phone.

Only available for OpenStage V3R0.

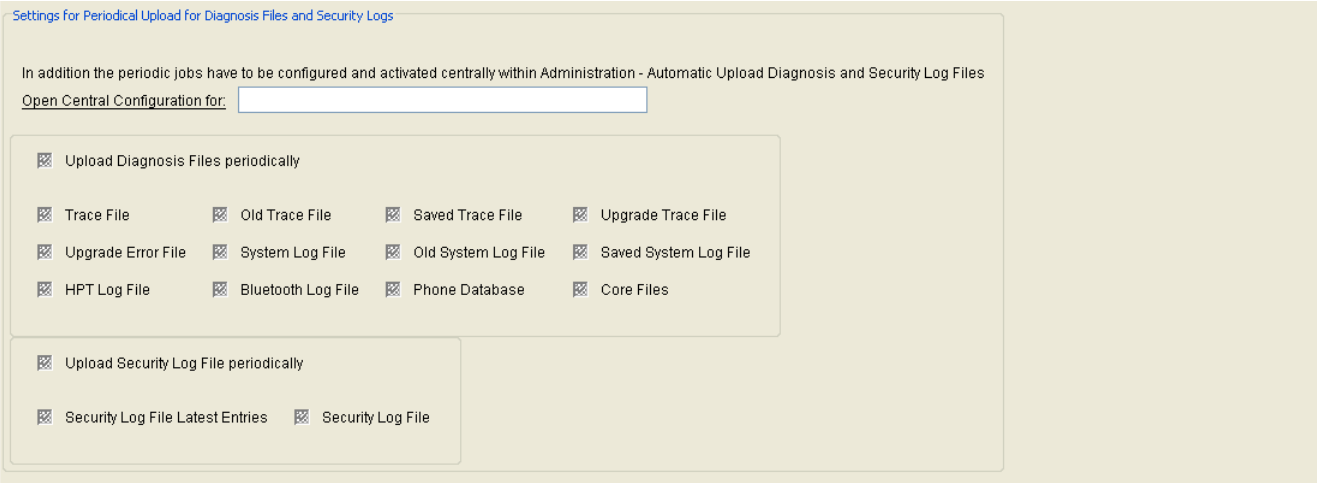
Diagnostic Call Prefix

A diagnostics call can be initiated by dialing the diagnostics call prefix followed by the called party number. The prefix consists of *(0-9)(0-9)(0-9)# .

Maximum length : 5 digits (including * and #)

7.1.24.6 "Periodical File Upload" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "Periodical File Upload" Tab



Settings for Periodical Upload for Diagnosis Files and Security Logs

Open Central Configuration for:

By clicking on the string, the central configuration in **Administration** > **Automatic Upload Diagnosis- and Security Log Files** is opened. The name of the destination mask is displayed in the text field.

Upload Diagnosis Files periodically

When active, diagnosis files of the IP Device are uploaded periodically.

Trace File

When active, the trace file of the IP Device is uploaded periodically.

Old Trace File

If checkbox is active, the old trace file of the IP Device is uploaded periodically.

Saved Trace File

When active, the saved trace file is uploaded periodically.

Upgrade Trace File

When active, the upgrade trace file of the IP Device is uploaded periodically.

Upgrade Error File

When active, the upgrade error file of the IP Device is uploaded periodically.

System Log File

Whens active, the system log file of the IP Device is uploaded periodically.

Old System Log File

When active, the old system log file is uploaded periodically.

Saved System Log File

When active, the saved system log file is uploaded periodically.

HPT Log File

When active, the HPT log file of the IP Device is uploaded periodically.

Bluetooth Log File

When active, the Bluetooth log file of the IP Device is uploaded periodically.

Phone Database

When active, the phone database file is uploaded periodically.

Core Files

When active, the core files of the are IP Device uploaded periodically.

Upload Security Log File periodically

When active, the security log files of the IP Device are uploaded periodically.

Security Log File Last Entries

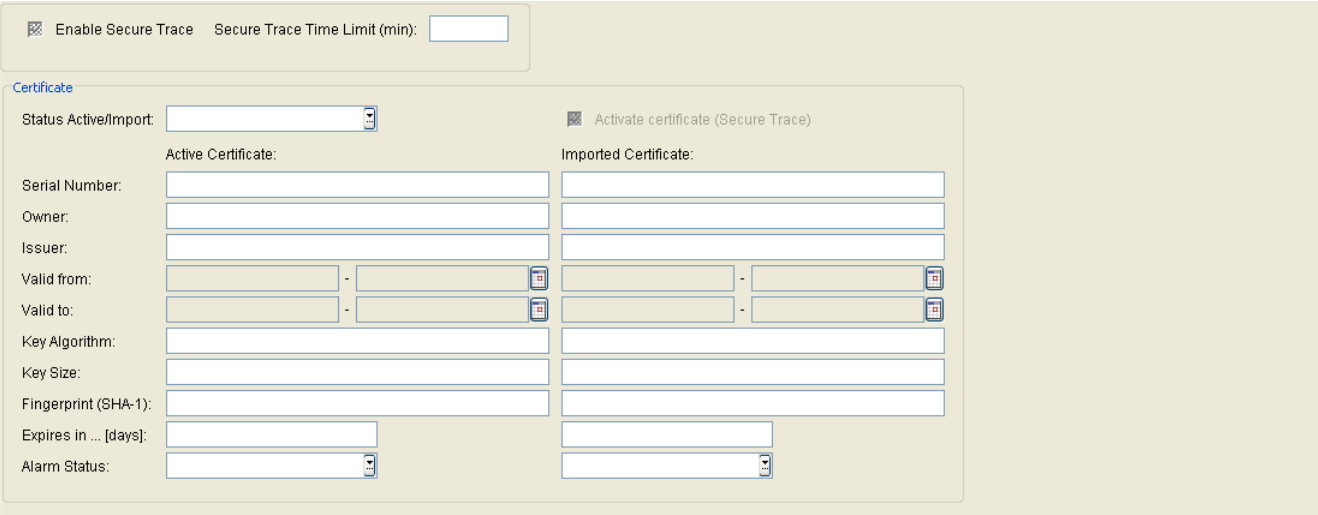
When active, entries in the security log file of the IP Device that have been added since the last storage are uploaded periodically.

Security Log File

When active, the complete security log file of the IP Device is uploaded periodically.

7.1.24.7 "Secure Trace Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Diagnosis > "Secure Trace Settings" Tab



Enable Secure Trace

Enable Secure Trace at the phone.

Secure Trace Time Limit (min)

Defines the time period within which trace data shall be collected.

Maximum value: **43200** (= 30 days)

Certificate

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**

- **no imported certificate**

Activate certificate (Secure Trace)

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Certificate will expire in ... days.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

7.1.25 Miscellaneous

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous

This area features the following components:

- General Data
- Possible Action Buttons
- "Country & Language" Tab
- "Messaging Services" Tab
- "SIP Error Notification" Tab
- "Display / Phone Settings" Tab
- "Help Internet URL" Tab
- "FTP Server" Tab
- "Call Log" Tab
- "Phone Lock" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.1.25.1 "Country & Language" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "Country & Language" Tab



Country:

Country where the workpoint is operated. This parameter corresponds to the country setting on the device.

Possible options:

- **AR - Argentina**
- **AT - Austria**
- **AU - Australia**
- **BE - Belgium**
- **BR - Brazil**
- **CA- Canada**
- **CH- Switzerland**
- **CL - Chile**
- **CN - China**
- **CZ - Czech Republic**
- **DE - Germany**
- **DK - Denmark**
- **EE - Estonia**
- **ES - Spain**
- **FI - Finland**
- **FR - France**
- **GB - United Kingdom**
- **HR - Croatia**
- **HU - Hungary**
- **IE - Ireland**

- **IN - India**
- **IT - Italy**
- **JP - Japan**
- **LT - Lithuania**
- **LU - Luxembourg**
- **LV - Latvia**
- **MX - Mexico**
- **NL - Netherlands**
- **NO - Norway**
- **NZ - New Zealand**
- **PL - Poland**
- **PT - Portugal**
- **RU - Russian Federation**
- **SE - Sweden**
- **SG - Singapore**
- **SK - Slovakia**
- **TH - Thailand**
- **TR- Turkey**
- **US - United States**
- **VN - Vietnam**
- **ZA - South Africa**
- **CY - Wales**

Language:

Language to be used for local applications.

Possible options:

- **bg - bulgarian**
- **ca - catalan**
- **cs - czech**

- **da - danish**
- **de - german**
- **el - greek**
- **en - english**
- **en - english (US)**
- **es - spanish**
- **et - estonian**
- **eu- euskara**
- **fi - finnish**
- **fr - french**
- **hr - croatian**
- **hu - hungarian**
- **id - indonesian**
- **it - italian**
- **ja - japanese**
- **lt - lithuanian**
- **lv - latvian**
- **mk - macedonian**
- **ms - malayan**
- **nl - dutch**
- **no - norwegian**
- **pl - polish**
- **pt - portuguese**
- **pt-Br - brazilian**
- **ro - romanian**
- **ru - russian**
- **sk - slovak**
- **sl - slovenian**
- **sr - serbian (Cyrillic)**
- **sr - serbian (Latin)**

- **sv - swedish**
- **sr - serbian**
- **tr - turkish**
- **zh - chinese**
- **cy- welsh**

USB Keyboard Country:

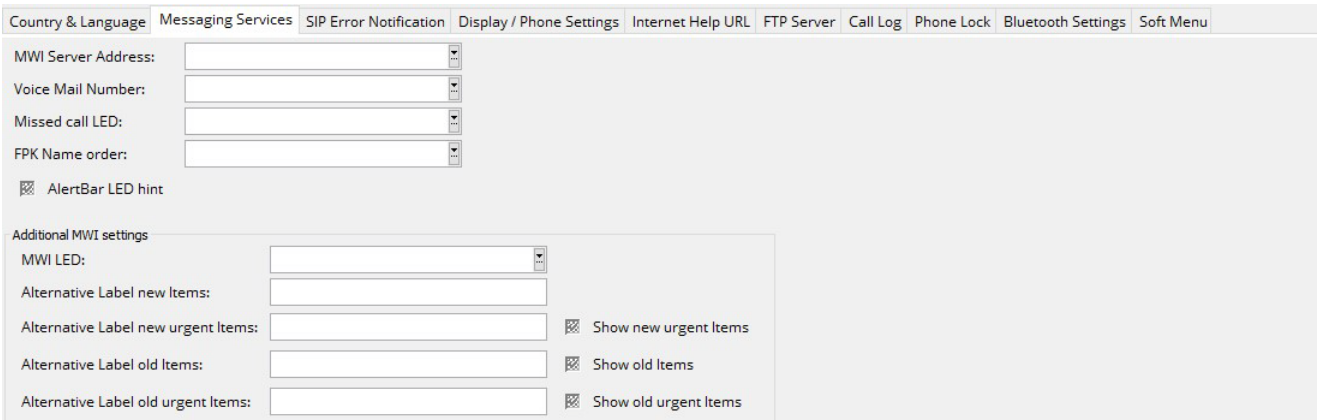
Language-specific keyboard layout when using an external USB keyboard.

Possible options:

- **English**
- **German**
- **French**
- **Spanish**
- **American**
- **Italian**

7.1.25.2 "Messaging Services" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "Messaging Services" Tab



MWI Server Address:

IP address or host name of the MWI server.

Voice Mail Number:

Phone number of the voicemail system (message server).

Missed call LED:

Possible options:

- Key only/Key LED
- Key & AlertBar
- AlertBar LED on
- No LED
- AlertBar LED hint

NOTE: Please note that if you deactivate the WBM interface, you can only reactivate it via DLS as the WBM is no longer available for this.

FPK Name order:

Possible options:

- <lastname>, <firstname>
- <lastname>, <firstname initial>
- <firstname> <lastname>
- <firstname initial> <lastname>
- <lastname>

AlertBar LED hint:

When this checkbox is activated, the red LED indicating new missed calls will be extinguished as soon as the user enters the Conversations menu.

Additional MWI settings

Show new Items

Shows the count of new messages.

Show new urgent Items

Shows the count of new urgent messages.

Show old urgent Items

Shows the count of old messages.

Show old urgent Items

Shows the count of old urgent messages.

Alternative Label new Items

Label for the count of new messages.

Alternative Label new urgent Items

Label for the count of new urgent messages.

Alternative Label old Items

Label for the count of old messages.

Alternative Label old urgent Items

Label for the count of old urgent messages.

7.1.25.3 "SIP Error Notification" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "SIP Error Notification" Tab



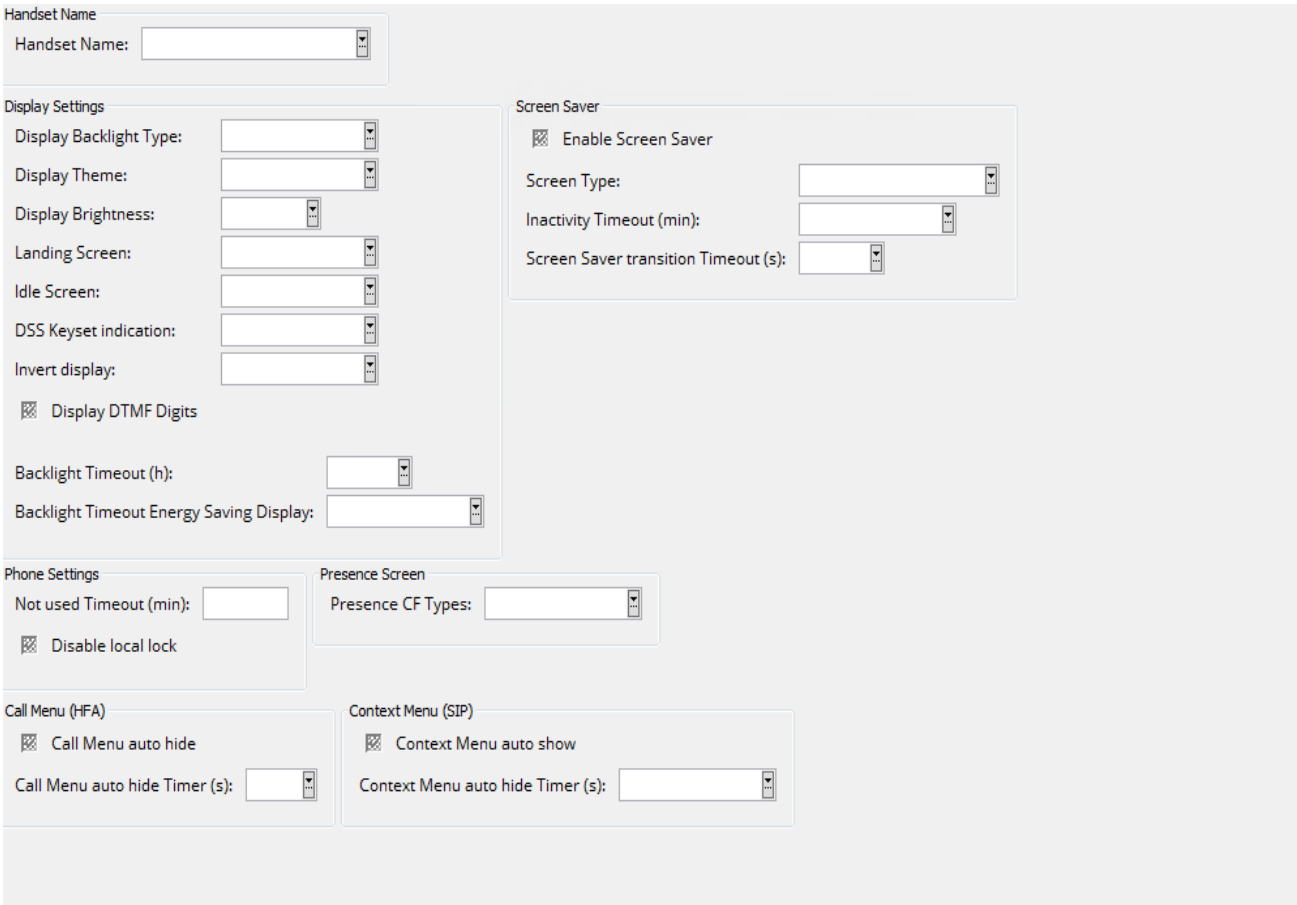
Beep on Error

Checkbox for activating acoustic error signaling during communication with Microsoft RTC.

Only available in SIP workpoints.

7.1.25.4 "Display / Phone Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "Display / Phone Settings" Tab



Handset Name

Handset Name:

Name of the WLAN handset shown on the handset's display.

Value range: max. 16 alphanumeric characters.

Display Settings

Display Backlight Type

Possible options:

- **None**

- **CCFL**
- **LED**

Display Theme

Defines the layout of the graphical user interface on OpenStage phones.

Possible options:

- **Silver Blue**
- **Anthracite Orange**

Display Brightness

Sets the display brightness.

Possible Options:

- **-3**
- **-2**
- **-1**
- **Default**
- **+1**
- **+2**
- **+3**

Landing Screen

Set your Landing Screen.After that, you can easily get back to it, and after a (configurable) period of inactivity and on wake-up from slideshow or energy-saver (as appropriate), your device shows the screen that you find most useful and ultimately suits you most.

NOTE: Available only to CP400/600 devices & of V1R4 version and higher.

Possible Options:

- **Conversations**
- **Favourites/Team**
- **Main Menu**

Idle Screen

Set your Idle Screen Mode.After that, the right side menu of display will become configurable. You may choose if combined menu should be shown, or FPK´s as default, alternated with idle menu. Menu key will switch between menu and FPK´s in this mode.

No other impact to navigation. Screen is still the Idle (menu) screen, only this time,the right side content is different. Under FPK & Idle Menu mode, when navigating from any other screen to Idle screen, FPK´s are shown on the right side.

NOTE: Available only to CP 200/400/600/600 E devices & of V1R4 version and higher.

Possible Options:

- **Menu only**
- **Favourites + Menu**

DSS Keyset indication

Invert display

Change the display to a dark background using color inversion.

Possible Options:

- **Normal Display**
- **Inverted Display**

Display DTMF Digits

When enabled, DTMF digits pressed during an active call are shown on Call screen.

Disabled by default.

Backlight Timeout (h):

When the phone has been in idle state for a timespan longer than this value, the backlight is switched off.

NOTE: Valid only for IP Devices with **Display Backlight Type = Standard**, see Section 7.6.1, "Inventory Data".

Possible options:

- **2**

- **3**
- **4**
- **5**
- **6**
- **7**
- **8**

Backlight Timeout Energy Saving Display

When a phone with energy saving display has been in idle state for a timespan longer than this value, the backlight is switched off.

NOTE: Valid only for IP Devices with **Display Backlight Type = CCFL** or **Display Backlight Type = LED**, see Section 7.6.1, "Inventory Data".

Possible Options:

- **1 min**
- **5 min**
- **30 min**
- **60 min**
- **2 hours**
- **3 hours**
- **4 hours**
- **5 hours**
- **6 hours**
- **7 hours**
- **1min / 5min**
- **5mins / 20 mins**
- **30 mins / 2 hrs**
- **45 mins / 4 hrs**
- **60 mins / 8hrs**

NOTE: The last 4 options apply only for CP400/CP600 V1R2 devices.

Not used Timeout (min):

Time in minutes before the screen is dimmed, if no activities have taken place on the screen until now.

Possible Options:

- **0 (no timeout)**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Screensaver

Enable Screensaver

This checkbox enables the screensaver.

Screen Type

Select the Screen Type.

Possible Options:

- **Menu Screen**
- **Slideshow/ Date screen**

Inactivity Timeout (min):

Possible Options:

- **0(no timeout)**
- **1**
- **5**
- **10**

- **20**
- **30**
- **60**
- **120**

Screensaver transition Timeout (sec)

Time interval in seconds for changing the images.

Possible Options:

- **5**
- **10**
- **20**
- **30**
- **60**

Phone Settings:

Not used Timeout (min):

Defines how long (in minutes) the telephone will remain inactive before its ends a particular status.

Example: Exit the configuration menu after a specified time.

Disable local lock:

Disable local phone lock in environments where only system lock should be used.

This checkbox is disabled by default.

> ***NOTE:*** This flag is available only to CP400/600 HFA phones of V1R1 version and higher.

Presence Screen

Presence CF Types

Allow showing the additional CF types to be configured.

NOTE: Available only to CP400/600 devices of version SIP V1R3 or higher.

Possible Options:

- **Only all calls (default)**
- **All CF types**

Call Menu (HFA)

Call Menu auto hide

If the checkbox is checked, the call menu will be hidden after an adjustable timeout.
2

Call Menu auto hide Timer (sec)

Defines the timeout in seconds, after which the hiding of the call menu starts.

Possible Values:

- **0**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Context Menu (SIP)

Context Menu auto show

When active, the context menu will be shown automatically.

Context Menu auto hide Timer (sec)

The context menu will be hidden after the timeout specified here, in seconds.

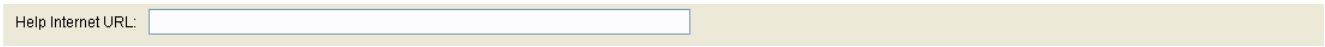
Possible Values:

- **No auto hide**

- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

7.1.25.5 "Help Internet URL" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "Help Internet URL" Tab



Help Internet URL:

URL of the Web help page on the Internet containing information on the telephone.

7.1.25.6 "FTP Server" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "FTP Server" Tab



Use Passive Mode FTP

This checkbox activates the passive mode for connections between the telephone and FTP server. Passive mode is used when the FTP server is unable to set up a connection to the client, for example, because of a firewall.

7.1.25.7 "Call Log" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "Call Log" Tab



Clear Call Log

Deletes the content of the call log.

7.1.25.8 "Phone Lock" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > "Phone Lock" Tab

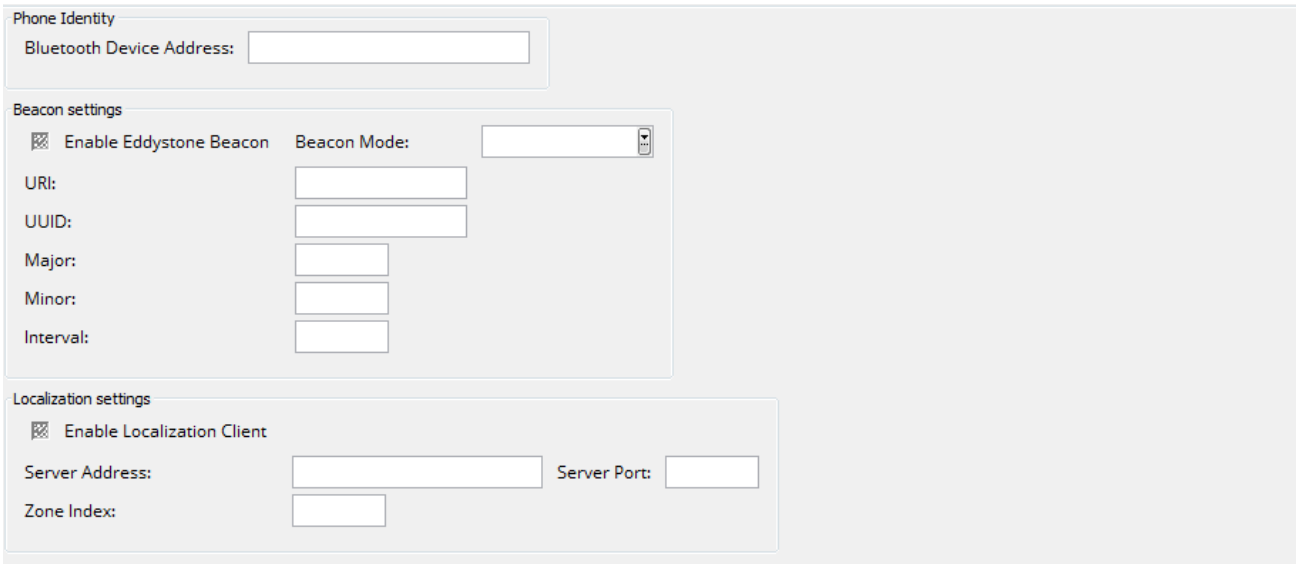


Lock Phone

Locks the phone.

7.1.25.9 Bluetooth Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Miscellaneous > Bluetooth Settings" Tab



NOTE: This is valid only for CP600 SIP phones of V1R2 version and higher.

Phone Identity

Bluetooth Device Address

Bluetooth Device Address

Beacon settings

Bluetooth beacons are hardware transmitters - a class of Bluetooth low energy (LE) devices that broadcast their identifier to nearby portable electronic devices. The technology enables smartphones, tablets and other devices to perform actions when in close proximity to a beacon.

Eddystone is a Bluetooth Low Energy beacon profile released by Google. The Apache 2.0-licensed, cross-platform, and versioned profile contains several frame types, including Eddystone-UID, Eddystone-URL, and Eddystone-TLM.For more info, refer to https://en.wikipedia.org/wiki/Eddystone_(Google)

Enable Eddystone Beacon

This checkbox controls whether the Bluetooth Low Energy mode is switched on or off.

It is disabled by default.

Beacon Mode

Beacon Mode controls whether the Bluetooth Low Energy Advertisement mode is switched on or off.

The **Both** option can be added, once it is verified that the parallel operation works flawlessly.

Disabled by default.

Available options:

- **Disabled**
- **Eddystone**
- **iBeacon**
- **Both**

URI

This defines the content of the Eddystone user data URI.

Default value: **`https://unify.com`**

UUID

This defines the UUID broadcast in the iBeacon frame.

It is a 32 lowercase hexadecimal digits, traditionally displayed in five groups separated by hyphens, in the 8-4-4-4-12 form.

Major

Used by the iBeacon app to identify the beacon.

Values:**0-65535**

Default value: **0**

Minor

Used by the iBeacon app to identify the beacon.

Values:**0-65535**

Default value: **0**

Interval

Interval in which the Bluetooth Low Energy Advertisements are dispatched.

Default value:**1000** ms.

Available options:**20-10240** ms

Localization settings

Under this tab you may configure CP600 phones as localization sensors.

> ***IMPORTANT:*** Bluetooth must be user activated in order for this admin feature to work

Enable Localization Client

This checkbox controls whether the Localization Client is switched on or off.

It is disabled by default.

Server Address

IP address, e.g **10.20.52.132**

Server Port

Default value:**8080**

Zone Index

Possible values: **0...n**

Default value:**0**

7.1.26 File Deployment

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > File Deployment

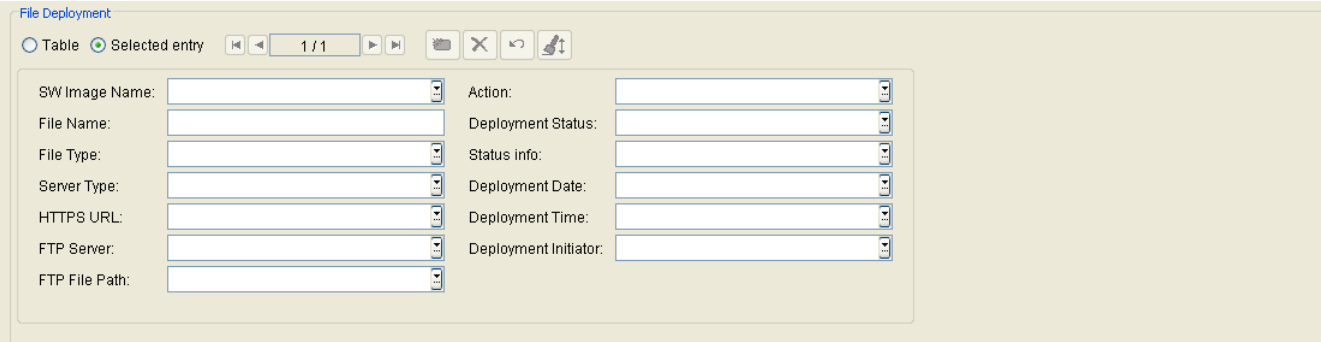
Files which have been read in the DLS database via scan (see Section 6.3.4, "FTP Server Configuration") can be transferred to an IP device. It is possible to transfer multiple files at once. For an overview of all software types supported by the DLS, see Section 3.5, "Overview of Software and File Types".

This area features the following components:

- General Data
- Possible Action Buttons
- "Files" Tab

7.1.26.1 "Files" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > File Deployment > "Files" Tab



NOTE: LDAP Templates are also deployable to OpenStage 15/20 (SIP only) & OpenScape Desk Phone IP 35 G / 35 G Eco phones.

File Deployment

SW Image Name:

Name of the Software Image.

File Name:

Name of the file.

File Type:

Usage of the file.

NOTE: For many file types on the FTP server can be used for multiple purposes. In such cases, there is a table entry for each usage. For instance, a WAV file can be used as a ringtone and as music on hold. Ringtone and music on hold files must not exceed 1MB in size, while screensaver and logo files should not be larger than 300kB.

Example: **LOGO** (OpenStage 40/60/80) , **SCREENSAVER** (OpenStage 40/60/80).

Server Type:

Protocol used by the server which provides the file.

Possible values:

- **FTP**
- **HTTPS**

HTTPS URL:

URL of the software image, if a HTTPS server is used.

FTP Server:

ID of the FTP server that provides the file. This is necessary if a FTP server is used.

FTP File Path:

Path of the file, if a FTP server is used.

Action:

Indicates what is to be done with the file.

Possible values:

- **delete**
- **deploy**

Deployment Status:

Status of the deployment action.

Status info:

Information about the status.

Deployment Date:

Date of the latest file deployment.

Deployment Time:

Time of the latest file deployment.

Deployment Initiator:

Interface over which the deployment has been initiated.

Possible values:

- **DLS**
- **WBM**
- **Local**

7.2 IP Client Configuration

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration

This menu consists of the following submenus:

- CTI Configuration
- Gateway/Server
- Ports
- Quality of Service
- Telephony
- Small Remote Site Redundancy
- Dialing Properties
- Audio/Video Settings
- Directories/Address Books
- Miscellaneous
- Keysets/Keylayout
- Signaling and Payload Encryption (SPE)
- Dialup Site
- OpenScape

IMPORTANT: Some of the settings that are configurable via DLS for IP clients are not applicable for particular clients & versions (e.g. PE, WE or Fusion Clients). Only the settings that are visible in the OpenScape Desktop Client (ODC) menu are the ones configurable by DLS.

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP clients. The base data associated with the IP clients found is displayed in **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the IP client.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device.

Device Type:

Device type of the IP client.

All IP client types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiClient 130**

E.164:

Complete E.164 phone number of the IP client.

Example: **498972212345** (or no input).

For more information, see Chapter 17, "E.164".

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP client registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

Remarks:

Fields for general information.

Location

Current location of the IP Device. The value is set during registration and is displayed only herein. (For meaning and configuration of the location, see Section 6.3.2, "Location".)

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP clients that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Deploy

Starts a job for distributing the configuration changes. For more information, see Section 15.3, "First Steps: Changing IP Device Parameters".

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.7, "Editing Templates".

Rename

Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

7.2.1 CTI Configuration

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration

This menu consists of the following submenus:

- General Data
- Possible Action Buttons
- CTI HFA Provider
- CSTA Service Provider

7.2.1.1 CTI HFA Provider

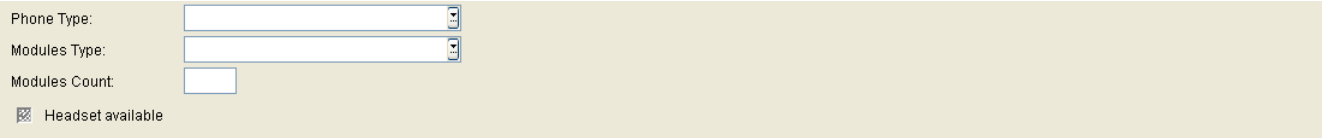
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CTI HFA Provider

This menu consists of the following submenus:

- General Data
- Possible Action Buttons
- "Device" Tab
- "Connection" Tab
- "Dialup" Tab
- "License" Tab

"Device" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CTI HFA Provider > "Device" Tab



Phone Type:

Type of the phone which is to be controlled by the CTI provider.

Possible Options:

- **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**

Modules Type:

Type of the connected module, if present.

Possible Options:

- **optiPoint Key Module**
- **optiPoint Self Labeling Keys Module**
- **optiSet E Key Module**

Modules Count:

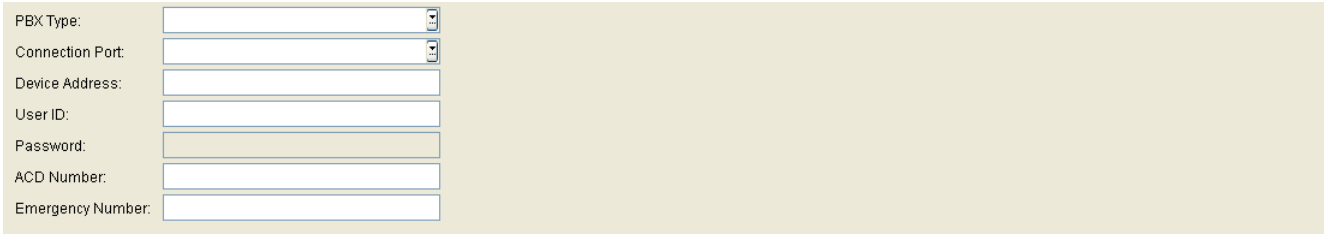
Number of existing modules.

Headset available

Checkbox to determinate whether a headset is connected.

"Connection" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CTI HFA Provider > "Connection" Tab



PBX Type:

Possible Options:

- **HiPath 3000**
  Includes HiPath, OpenScape MX/LX, and OpenOffice EE, too.
- **HiPath 4000**

Connection Port:

Hardware port used for CTI communication with the device. If USB is used, a special driver is necessary, which emulates a COM port. For futher information, see the administrator documentation for optiClient.

Possible Options:

- **LAN**
- **COM1**
- **COM2**
- **COM3**
- **COM4**
- **COM5**
- **COM6**
- **COM7**
- **COM8**
- **COM9**

Device Address:

IP address of the PBX.

User ID:

User address (extension) for the phone.

Password:

Password corresponding to the user ID.

ACD Number:

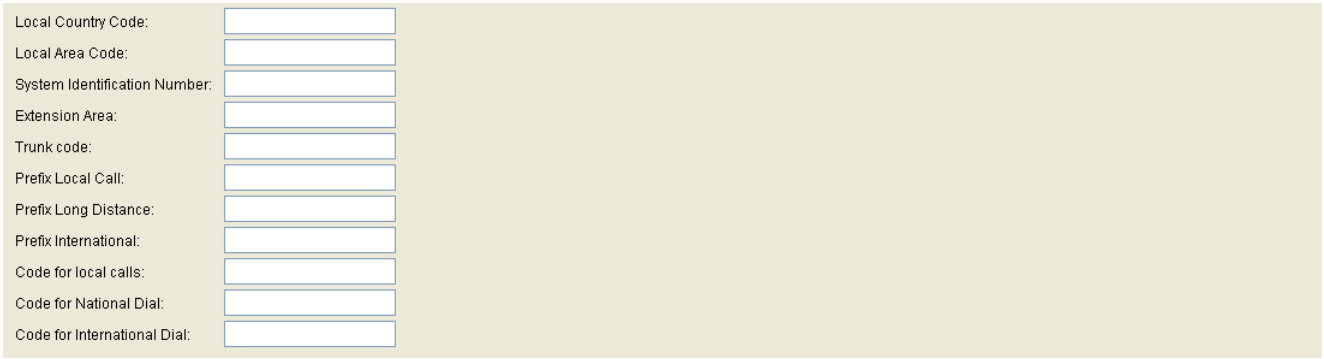
Needed if the user is working as ACD (Automatic Call Distribution) agent.

Emergency Number:

Emergency number configured in the device.

"Dialup" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CTI HFA Provider > "Dialup" Tab



Local Country Code:

E.164 Country code, without leading zero. Maximum length: 4 digits.

Examples: **49** for Germany, **44** for United Kingdom.

Local Area Code:

Local area code / city code, without leading zero. Maximum length: 21 digits.

Examples: **89** for Munich, **20** for London.

System Identification Number:

Number of the company PBX to which the phone is connected. Maximum length: 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Extension area:

This parameter defines a pattern which enables to discern internal extensions. From a workpoint's point of view, extensions are internal if they are assigned to the same PBX. The extension area can be given as a regular expression.

Example: Let 1xxx, 2xxx, 3xxx, 4xxx , 5xxx be (internal) extensions, and let 6xxx, 7xxx, 8xxx, 9xxx be external call numbers. The regular expression ^[12345] defines that call numbers beginning with a digit from 1 to 5 are internal extensions. If, for instance, the system identification number is 667, the call numbers from 6671xxx to 6675xxx are treated as internal extensions.

Trunk Code:

Access code used for dialing out from a PBX to a PSTN. If multiple trunk codes are configured at the communication system connected, enter them in this field using "|" as a separator (0 and 88 in the example). The first value entered is always used to supplement the call number when dialing. Maximum length: 5 digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Prefix for a local call. This data is determined by the network operator, and thus independent of the configuration for the PBX. Maximum length: 21 digits.

Example: **01081**

Prefix Long Distance:

Prefix for a long distance call. This data is determined by the network operator, and thus independent of the configuration for the PBX. Maximum length: 21 digits.

Example: **01081**

Prefix International:

Prefix for an international call. This data is determined by the network operator, and thus independent of the configuration for the PBX. Maximum length: 21 digits.

Example: **01081**

Code for local calls:

This number is designated as call-by-call prefix for local calls. The data is not dependant on the configuration of the provider connected. Maximum length: 21 digits.

Example: **01019**

Code for National Dial:

This number is designated as call-by-call prefix for national calls. The data is not dependant on the configuration of the provider connected. Maximum length: 5 digits.

Example: **01015**

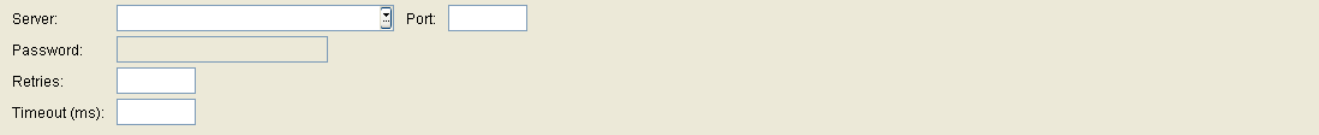
Code for International Dial:

This number is designated as call-by-call prefix for international calls. The data is not dependant on the configuration of the provider connected. Maximum length: 5 digits.

Example: **01015**

"License" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CTI HFA Provider > "License" Tab



Server:

IP address of the server that provides the licenses.

Password:

Password for access to the license.

Retries:

Number of retries to establish a connection to the license server.

Timeout (ms):

Timeout for tries to establish a connection to the license server.

Port:

Number of the port used by the license server for delivering licenses.

7.2.1.2 CSTA Service Provider

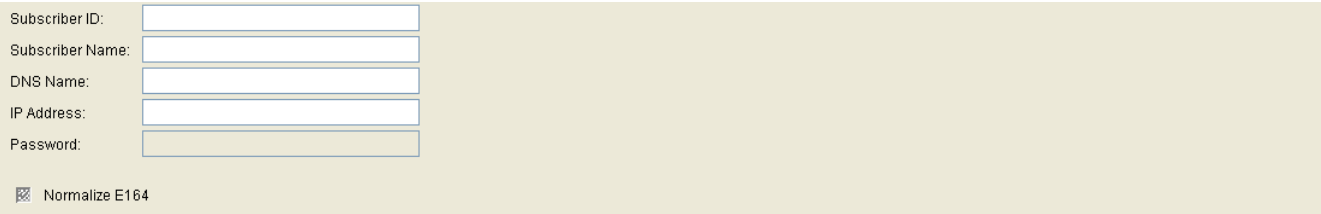
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CSTA Service Provider

This menu consists of the following submenus:

- General Data
- Possible Action Buttons
- "Connection" Tab
- "Dialup" Tab
- "License" Tab

"Connection" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CSTA Service Provider > "Connection" Tab



Subscriber ID:

Subscriber ID resp. extension which is controlled by the CSTA service provider.

Subscriber Name:

Logical name for the extension which is controlled by the CSTA service provider.

DNS Name:

DNS name of the CSTA service provider.

IP Address:

IP address of the CSTA service provider.

Password:

Password required for starting the CSTA service provider.

Normalize E.164:

Activates the normalization of call numbers to E.164 format.

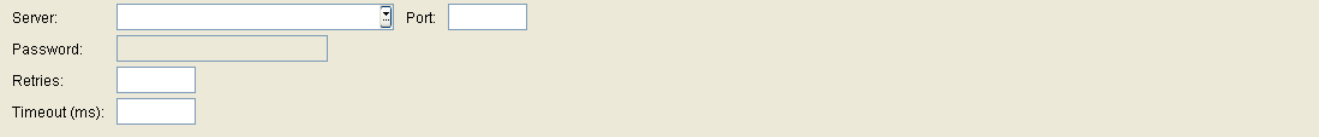
"Dialup" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CSTA Service Provider > "Dialup" Tab

See Section 7.2.8.1, ""HFA Dialing Properties" Tab".

"License" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > CTI Configuration > CSTA Service Provider > "License" Tab



Server:

IP address of the server that provides the licenses.

Password:

Passwort zum Lizenzserver.

Retries:

Number of retries to establish a connection to the license server.

Timeout (ms):

Timeout for triesto establish a connection to the license server.

Port:

Number of the port used by the license server for delivering licenses.

7.2.2 General

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > General

This area features the following components:

- General Data
- Possible Action Buttons
- "Gateway (HFA) / SIP Server" Tab
- "Gateway (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP clients. The base data associated with the IP clients found is displayed in **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the IP client.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device.

Device Type:

Device type of the IP client.

All IP client types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiClient 130**

E.164:

Complete E.164 phone number of the IP client.

Example: **498972212345** (or no input).

For more information, see Chapter 17, "E.164".

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP client registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

Remarks:

Fields for general information.

Location

Current location of the IP Device. The value is set during registration and is displayed only herein. (For meaning and configuration of the location, see Section 6.3.2, "Location".)

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP clients that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Deploy

Starts a job for distributing the configuration changes. For more information, see Section 15.3, "First Steps: Changing IP Device Parameters".

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.7, "Editing Templates".

Rename

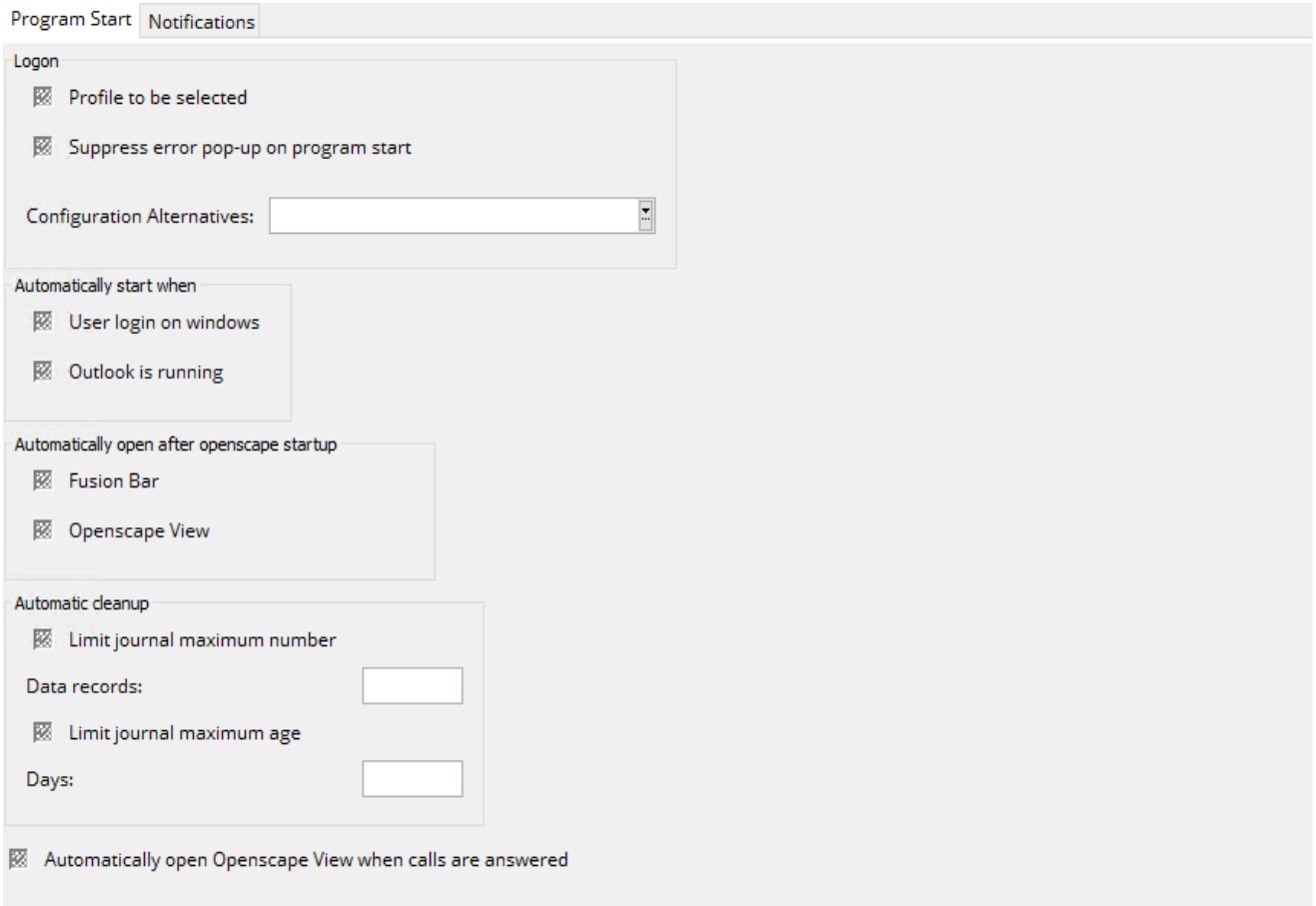
Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

7.2.2.1 "Program Start" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > General > "Program Start" Tab



This tab allows general configurations of Fusion for Office.

NOTE: The Program Start Tab is available only for Fusion for Office V1 R8 or greater.

Logon

Profile to be selected:

Enabled by default.

Suppress error pop-up on program start:

Enabled by default.

Configuration Alternatives:

Possible options:

- Admit settings and profile administration
- Only accept settings
- Hide settings and profile administration

Automatically start when

user login on windows:

Enabled by default.

outlook is running:

Enabled by default.

Automatically open after openscape startup

Fusion Bar:

Disabled by default.

OpenScape View:

Disabled by default.

Automatic cleanup

Limit journal maximun number

Data records:

Default is 300.

Limit journal maximum age

Days:

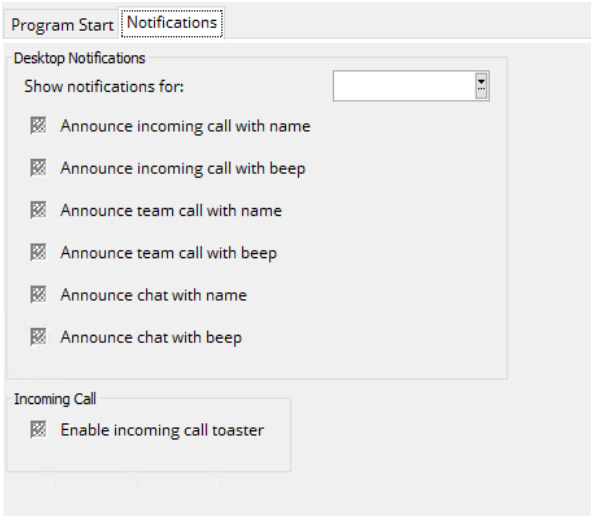
Default is 90.

Automatically open Openscape View when calls are answered:

Disabled by default.

7.2.2.2 " " Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > General > " " Tab



This tab allows general configurations of Fusion for Office.

NOTE: The Program Start Tab is available only for Fusion for Office V1 R8 or greater.

Desktop notifications

Show notifications for:

Indicates the duration of the notifications.

Possible options:

- 5 seconds
- 7 seconds
- 15 seconds
- 30 seconds
- 1 minute
- 5 minutes
- 15 minutes
- 30 minutes
- 1 hour

Announce incoming call with name:

Disabled by default

Announce incoming call with beep:

Disabled by default

Announce team call with name:

Disabled by default

Announce team call with beep:

Disabled by default

Announce chat with name:

Disabled by default

Announce chat with beep:

Disabled by default

Incoming call

Enable incoming call toaster

Check this checkbox if you want to allow incoming call information to be displayed in a toast notification.

7.2.3 Gateway/Server

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server

This area features the following components:

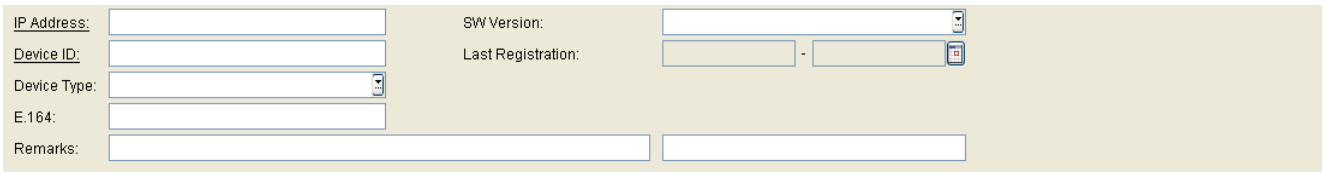
- General Data
- Possible Action Buttons
- "Gateway" Tab
- "Gateway (Standby)" Tab
- "SW Deployment" Tab
- "HFA Settings" Tab
- "SIP Connection" Tab
- "SIP Registrar" Tab
- "SIP Proxy" Tab
- "SIP Gateway" Tab
- "System Services" Tab
- "SIP Survivability" Tab
- "Licenses" Tab
- "VPN Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of IP clients. The base data associated with the IP clients found is displayed in **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the IP client.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device.

Device Type:

Device type of the IP client.

All IP client types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiClient 130**

E.164:

Complete E.164 phone number of the IP client.

Example: **498972212345** (or no input).

For more information, see Chapter 17, "E.164".

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP client registration.

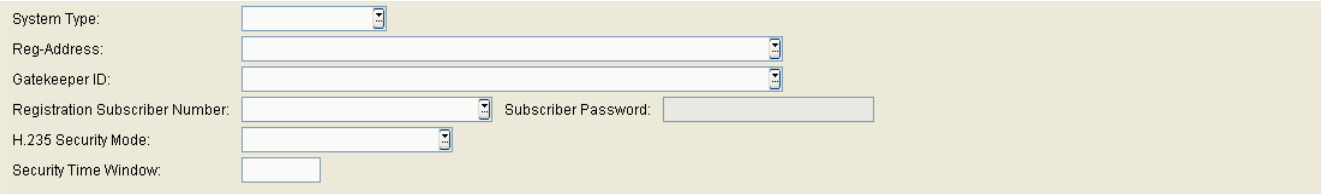
For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

Remarks:

Fields for general information.

7.2.3.1 "Gateway" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "Gateway" Tab



System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **HiPath 3000**
  Includes HiPath, OpenScape Office MX/LX, and OpenOffice EE, too.
- **HiPath 4000**

Only applies to the HFA configuration of the IP client.

Reg-Address:

IP address or host name of the PBX used to operate the workpoint.

Only applies to the HFA configuration of the IP client.

Gatekeeper ID:

Only applies to the HFA configuration of the IP client.

Registration Subscriber Number:

Phone number of the IP client on the PBX.

Only applies to the HFA configuration of the IP client.

Subscriber Password:

Password of the IP client on the PBX.

Only applies to the HFA configuration of the IP client.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only applies to the HFA configuration of the IP client.

Security Time Window:

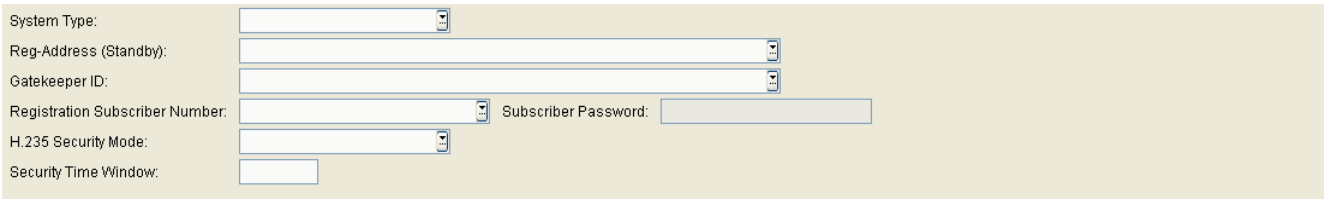
The gateway only accepts messages that arrive during the time window specified here.

Only applies to the HFA configuration of the IP client.

7.2.3.2 "Gateway (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "Gateway (Standby)" Tab

NOTE: This "standby" data is used when the "home" data for the "Gateway" Tab is not available. The SRSR functionality must be configured for this, see Section 7.2.7, "Small Remote Site Redundancy".



System Type:

Type and version of the communication platform at which the workpoint is operated.

Possible options:

- **HiPath 3000**
  Includes HiPath, OpenScape Office MX/LX, and OpenOffice EE, too.
- **HiPath 4000**
- **No standby system**

Only applies to the HFA configuration of the IP client.

Reg-Address (Standby):

IP address or host name of the standby PBX used to operate the workpoint.

Only applies to the HFA configuration of the IP client.

Gatekeeper ID:

Only applies to the HFA configuration of the IP client.

Registration Subscriber Number:

Phone number of the IP client on the (standby) PBX.

Only applies to the HFA configuration of the IP client.

Subscriber Password:

Password of the IP client on the (standby) PBX.

Only applies to the HFA configuration of the IP client.

H.235 Security Mode:

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Only available on HFA IP clients.

Security Time Window:

The gateway only accepts messages that arrive during the time window specified here.

Only applies to the HFA configuration of the IP client.

7.2.3.3 "SW Deployment" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "SW Deployment" Tab



Directory:

Complete path of the directory where the IP client should search for software updates.

SW Update mode

Possible values:

- **None**
  No check.
- **Start**
  Check at program start.
- **Interval**
  Ongoing checks in intervals.

Interval (min):

Interval in minutes for ongoing checks for software updates.

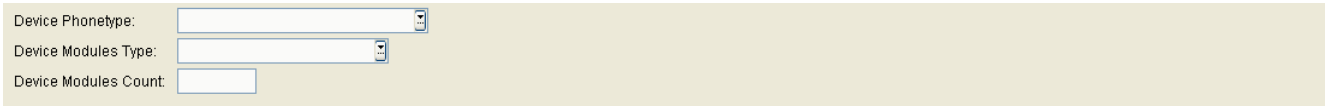
7.2.3.4 "HFA Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "HFA Settings" Tab

The representation of the optiClient 130 telephone is based on the layout of various device phone types.

To display the optiClient 130 telephone and the extended key field, you can choose from a number of different device phone types for telephone and key module.

The telephone and key module type set for optiClient 130 corresponds in terms of display and layout with the relevant desktop devices. Key modules are displayed as columns in optiClient 130's extended key field.



Device Phonetype:

The telephone type defines:

- How many display lines are displayed in optiClient 130's free telephone (always two lines in the main bar in integrated telephones).
- If self labeling keys are available for the optiClients 130 devices
- How many programmable function keys ...
  - are available in optiClient 130.
  - are available in the first column of the extended key field in optiClient 130.

Possible options:

- **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**

Device Modules Type:

Possible options:

- **optiPoint Key Module**
- **optiPoint Self Labeling Key Module**
- **optiSet E Key Module**

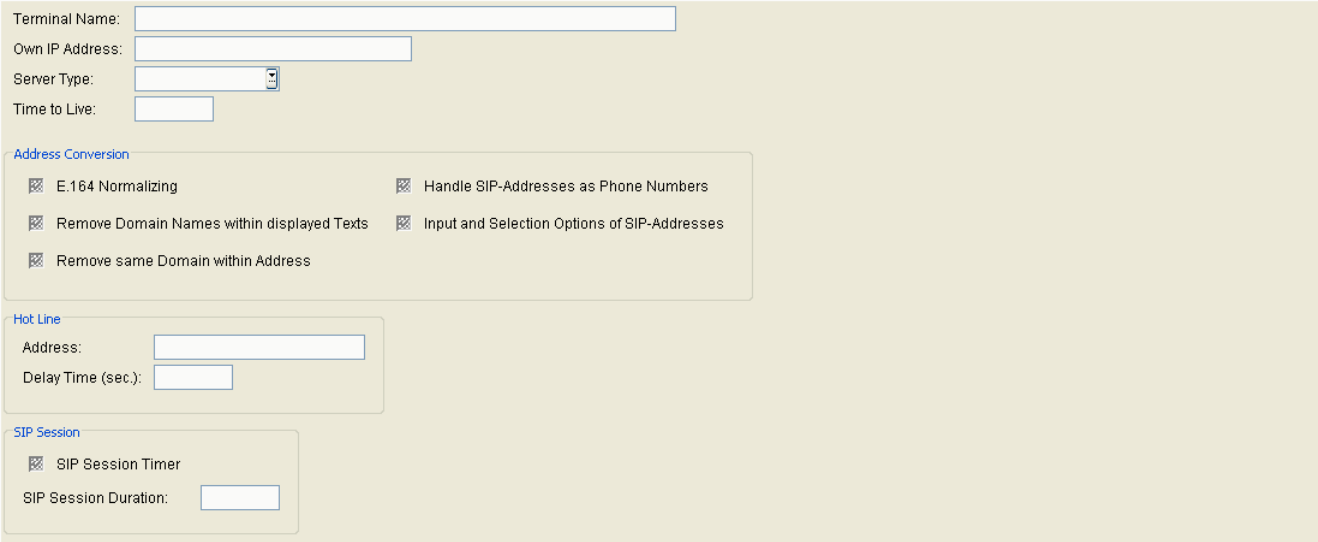
Device Modules Count:

Specifies how many key modules are assigned to the IP client.

Value range: **0** ... **4**

7.2.3.5 "SIP Connection" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "SIP Connection" Tab



Terminal Name

Own IP Address

You can enter the optiClient IP address here. If this field is left empty, the optiClient defines its IP address automatically.

Server Type

Possible options:

- **Standard**
- **OpenScape Voice**
- **hiQ4200**

Time to Live

This value is three times the time taken by the workpoint to register at the gatekeeper to sustain the registration validity. If the value for Time to Live is set to 3 minutes, for example, the workpoint registers every minute.

Value range: **0** ... **4320** minutes.

Address Conversion

E.164 Normalizing

Checkbox for activating phone number normalizing.

Remove Domain Names within displayed Texts

Checkbox for removing the domain name from display texts.

Remove same Domain within Address

Checkbox for removing the domain name from display texts if the called party is located in the same domain.

Handle SIP-Addresses as Phone Numbers

Input and Selection Options of SIP-Addresses

Hot Line

Address:

The address specified here is dialed once the delay time defined for line seizure (for example, on lifting the handset) has elapsed.

Delay Time (sec)

Delay time in seconds for immediate dialing. If the value is 0 the hot line is established without delay.

SIP Session

SIP Session Timer

Checkbox for activating the SIP session timer. The timer is used to monitor the duration of an SIP session.

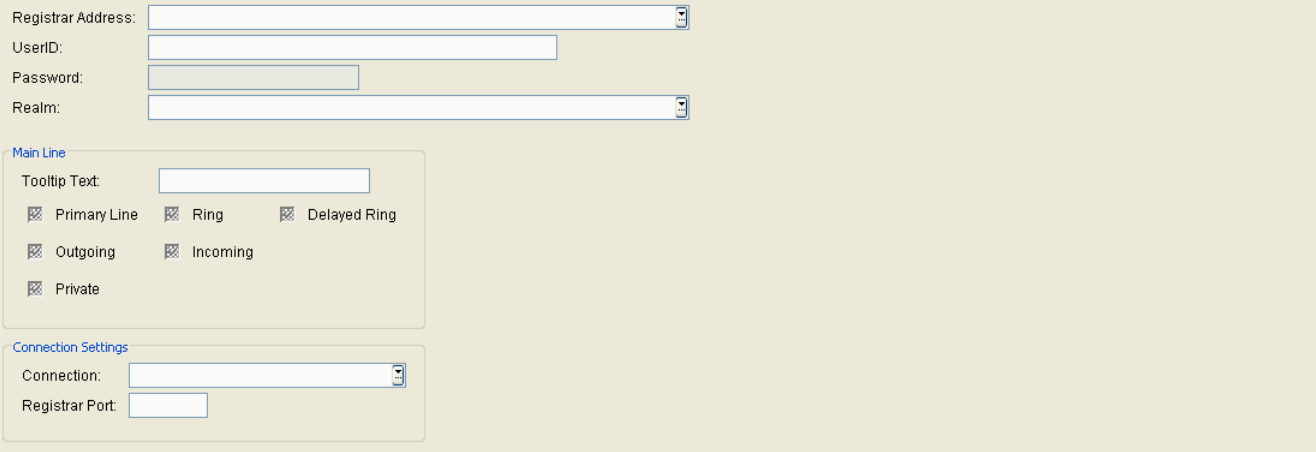
SIP Session Duration:

Highest duration in seconds for an SIP session.

Value range: **0** ... **3600** seconds.

7.2.3.6 "SIP Registrar" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "SIP Registrar" Tab



Registrar Address:

IP address or host name of the SIP registrar.

This setting only applies to the SIP configuration of the IP client.

UserID:

The user ID is the first part of the SIP URL.

Password:

Password required for accessing the SIP server.

Realm:

SIP range in which the workpoint is operated. SIP realm is used to identify the telephone at the SIP server.

Main Line

Tooltip Text:

Defines the display text for the main line.

Primary Line:

Checkbox for marking the main line as a primary line.

Ring

Checkbox for activating the call.

Delayed Ring

Checkbox for activating a delayed call.

Outgoing

Incoming

Private

Connection Settings

Connection

Possible options:

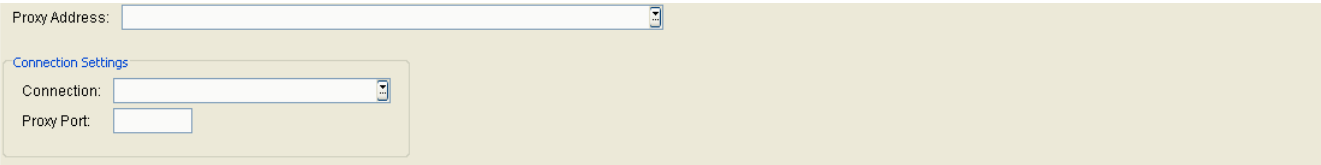
- **Use DNS SRV**
- **Use Standard Port**
- **Use Individual Port**

Registrar Port

Port number of the registrar server.

7.2.3.7 "SIP Proxy" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "SIP Proxy" Tab



Proxy Address

IP address or host name of the SIP proxy.

This setting only applies to the SIP configuration of the IP client.

Connection Settings

Connection

Possible options:

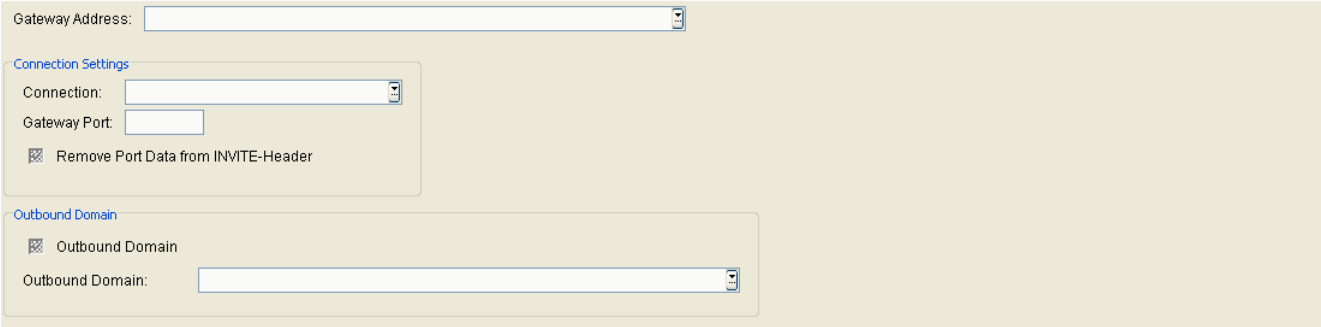
- **Use DNS SRV**
- **Use Standard Port**
- **Use Individual Port**

Proxy Port

Port number of the proxy server.

7.2.3.8 "SIP Gateway" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "SIP Gateway" Tab



Gateway Address:

IP address or host name of the gateway.

This setting only applies to the SIP configuration of the IP client.

Connection Settings

Connection:

Possible options:

- **Use Standard Port**
- **Use Individual Port**

Gateway Port:

Port number of the gateway.

Remove Port Data from INVITE-Header

If this checkbox has been enabled, the port numbers are removed from the INVITE headers.

Outbound Domain

Outbound Domain

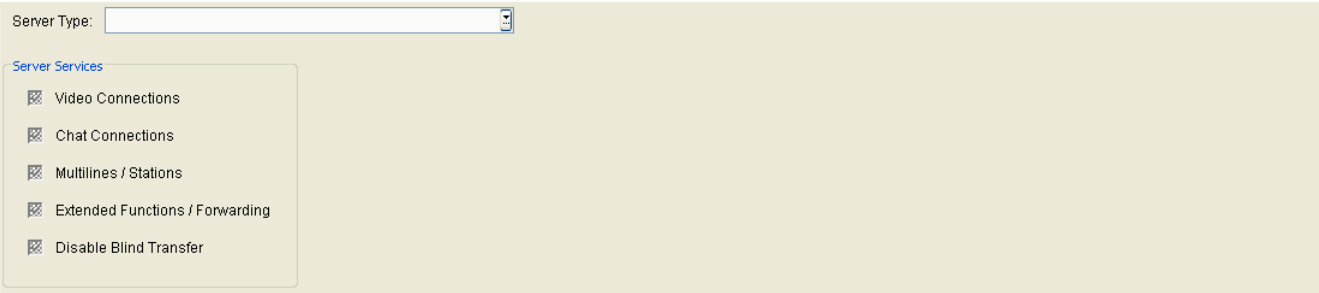
Checkbox for activating the outbound domain.

Outbound Domain:

Name of the outbound domain.

7.2.3.9 "System Services" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "System Services" Tab



Server Type:

Possible options:

- **OpenScape Voice/HQ4200 Chat**
- **OpenScape Voice/HQ4200 Keyset**
- **HiPath 3000/4000/5000 and OpenOffice EE**
- **Standard without Video/Chat**
- **Individual**
- **OpenScape Voice/hiQ4200**
- **OpenScape Voice/hiQ4200 without Video**
- **HiPath 3000 >= V8**
- **HiPath 4000 <= V6**
- **HiPath 4000 V7**
- **HiPath 4000 V8**
- **HiPath 4000 >= V10**

Server Services

Video Connections

Enables connections for exchanging video images.

Chat Connections

Enables connections for exchanging instant messages.

Multilines / Stations

Checkbox for activating additional lines/stations.

Extended Functions / Forwarding

Checkbox for activating enhanced call functions/call forwarding such as Transfer.

Disable Blind Transfer

Switch to disable Blind Transfer

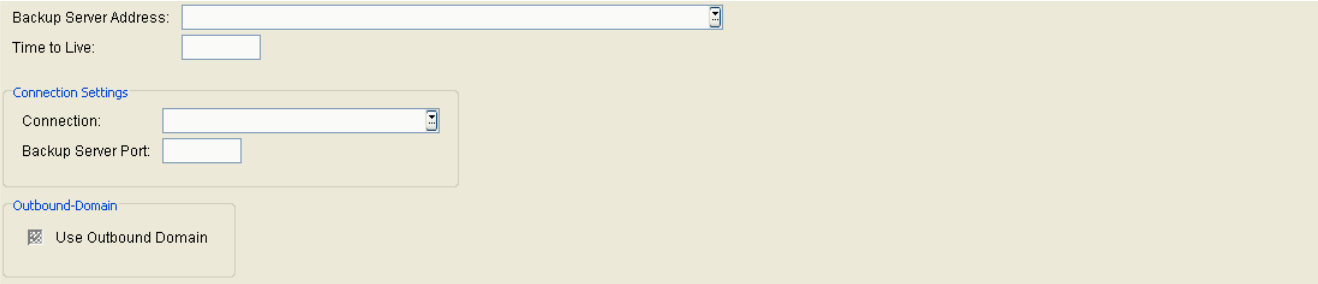
You may determine the number of supported features (server services) by selecting the relevant option under the **Server Type** combo box.The following table shows which features are supported by the available server types:

Server Type	Server Services
OpenScape Voice/ hiQ4200	• Video connections • Additional lines/stations • Extended call functions/call forwardings
OpenScape Voice/ hiQ4200 without Video	• Additional lines/stations • Extended call functions/call forwardings
HiPath 3000/ OpenOffice EE	• The OpenScape Fusion for Microsoft Outlook has not been released for operation at a HiPath 3000.
HiPath 3000 >=V8	The OpenScape Fusion for Microsoft Outlook has not been released for operation at a HiPath 3000.
HiPath 4000 >=V6	• Video connections • Suppress blind transfer
Default without Video/ Instant Messaging	None of the listed services is supported
Custom	You can individually activate the support of the features for the connected communications system (if available)

IMPORTANT: If a listed server service is active, the associated features and elements such as buttons, menu options, module windows, etc. are also active in the OpenScape Fusion for Microsoft Outlook. These controls are unavailable or inactive if the associated server service is not active.

7.2.3.10 "SIP Survivability" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "SIP Survivability" Tab



Backup Server Address:

IP address or host name of the backup server.

Time to Live:

This value is three times the time taken by the workpoint to register at the gatekeeper to sustain the registration validity. If the value for Time to Live is set to 3 minutes, for example, the workpoint registers every minute.

Value range: 0 ... 4320 minutes.

Connection Settings

Connection:

Possible options:

- **Use Standard Port**
- **Use Individual Port**

Backup Server Port:

Port number of the backup server.

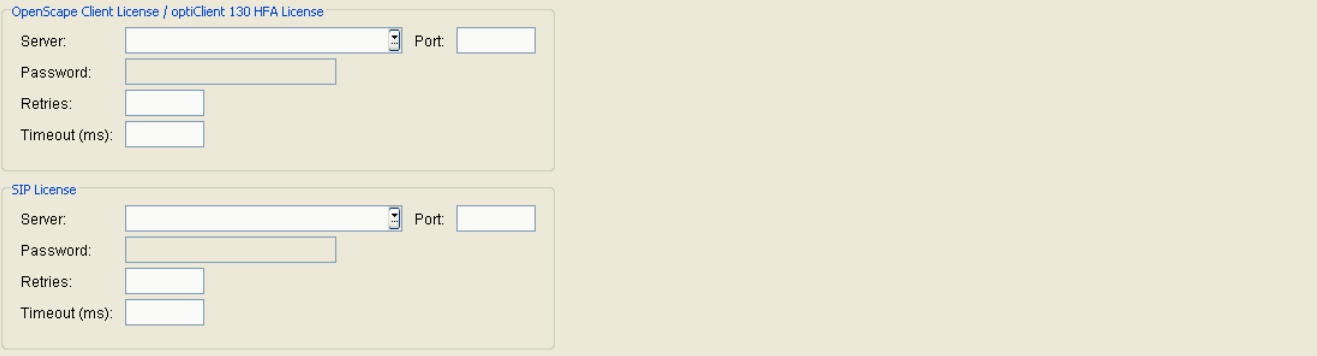
Outbound Domain

Use Outbound Domain

Checkbox for activating use of the outbound domain.

7.2.3.11 "Licenses" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "Licenses" Tab



OpenScape Client License / optiClient 130 HFA License

Server:

IP address or host name of the license server.

Port:

Port number for access to the license server.

Default: **61740**

Password:

Password for access to the license server.

Retries:

Maximum number of connection attempts.

Timeout (ms):

The maximum time (in milliseconds) for the attempt to set up a connection to the license server.

SIP License

Server:

IP address or host name of the license server.

Port:

Port number for access to the license server.

Default: **61740**

Password:

Password for access to the license server.

Retries:

Maximum number of connection attempts.

Timeout (ms):

The maximum time (in milliseconds) for the attempt to set up a connection to the license server.

7.2.3.12 "VPN Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server > "VPN Settings" Tab



VPN Mode:

Possible options:

- **None**
  VPN (Virtual Private Network) is not used.
- **Automatic**
  VPN is used with an automatically determined IP address.
- **Manual**
  VPN is used with the IP address specified in the case of **VPN IP**.

VPN IP:

IP address for the VPN (Virtual Private Network).

7.2.4 Ports

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Ports

This area features the following components:

- General Data
- Possible Action Buttons
- "Ports" Tab
- "SIP Ports" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.4.1 "Ports" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Ports > "Ports" Tab



H.245 Port Range from: ... to:

Port range for H.245.

RTP Port Range from: ... to:

Port range for RTP.

Use Cornet TC Port Range

Checkbox for activating Cornet TC.

Cornet TC Port Range from: ... to:

Port range for Cornet TC.

Use H.225.0 RAS Port

Checkbox for activating Cornet TC.

H.225.0 RAS Port:

For using NetMeeting at the same time as optiClient 130.

Gateway CorNet-TC TLS

Gateway H.225.0 TLS

Gateway CorNet-TC TLS (Standby)

Gateway H.225.0 TLS (Standby)

7.2.4.2 "SIP Ports" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Ports > "SIP Ports" Tab



RTP Port Range from: ... to:

Port range for RTP.

Only applies to the SIP configuration of the IP client.

SIP Signaling Port:

Only applies to the SIP configuration of the IP client.

7.2.5 Quality of Service

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Quality of Service

This area features the following components:

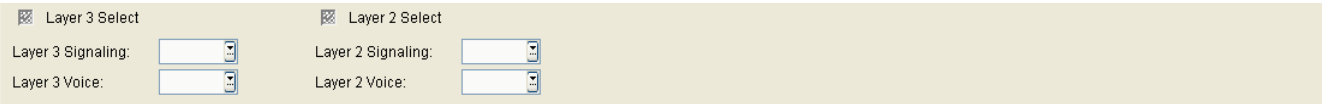
- General Data
- Possible Action Buttons
- "Settings" Tabs
- "Alternate Settings (SIP)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.5.1 "Settings" Tabs

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Quality of Service > "Settings" Tabs



Layer 3 Select

Checkbox for activating layer 3 (network layer).

Layer 3 Signaling:

Priority for layer 3 signaling.

Can only be defined if **Layer 3 Select** is active.

Possible options:

- **Default**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CST**

Layer 3 Voice:

Priority for layer 3 voice.

Can only be defined if **Layer 3 Select** is active.

Same options as for **Layer 3 Signaling**.

Layer 2 Select

Checkbox for activating layer 2 (data link layer).

Layer 2 Signaling:

Priority for layer 2 signaling.

Can only be defined if **Layer 2 Select** is active.

Value range: 0 ... 7.

Layer 2 Voice:

Priority for layer 2 voice.

Can only be defined if **Layer 2 Select** is active.

Same options as for **Layer 2 Signaling**.

7.2.5.2 "Alternate Settings (SIP)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Quality of Service > "Alternate Settings (SIP)" Tab



Layer 2 Select (SIP)

Checkbox for activating layer 2 (data link layer).

Layer 2 Signaling:

Priority for layer 2 signaling.

Can only be defined if **Layer 2 Select** is active.

Value range: **0** ... **7**

Layer 2 Voice:

Priority for layer 2 voice.

Can only be defined if Layer 2 Select is active.

Same options as for Layer 2 Signaling.

Layer 3 Select (SIP)

Checkbox for activating layer 3 (network layer).

Layer 3 Signaling

Can only be defined if **Layer 3 Select (SIP)** is active.

Possible options:

- **Default**
- **AF11**
- **AF12**
- **AF13**

- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CST**

Layer 3 Voice:

Priority for layer 3 voice.

Can only be defined if **Layer 3 Select (SIP)** is active.

Possible options:

- **Default**
- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**

- **EF**
- **CST**

7.2.6 Telephony

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Telephony

This area features the following components:

- General Data
- Possible Action Buttons
- "Telephony" Tab
- "Telephony (Standby)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.6.1 "Telephony" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Telephony > "Telephony" Tab



Emergency Number:

Contains the phone number that can be dialed in an emergency.

ACD Number:

ACD agent number if you are working as an ACD agent.

Location Identifier Number

Contains an identification number for unique location identification. This number can be used, for example, to pinpoint the **origin** of an emergency call.

Available for optiClient 130 V4.0 only.

7.2.6.2 "Telephony (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Telephony > "Telephony (Standby)" Tab

NOTE: This "standby" data is used when the "home" data for the "Telephony" Tab is not available. The SRSR functionality must be configured for this, see Section 7.2.7, "Small Remote Site Redundancy".



Emergency Number:

Contains the phone number that can be dialed in an emergency.

ACD Number:

ACD agent number if you are working as an ACD agent.

7.2.7 Small Remote Site Redundancy

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Small Remote Site Redundancy

This area features the following components:

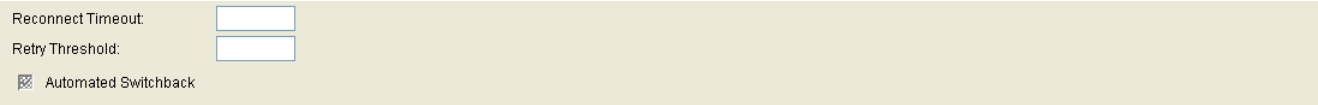
- General Data
- Possible Action Buttons
- "SRSR Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.7.1 "SRSR Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Small Remote Site Redundancy > "SRSR Settings" Tab



Reconnect Timeout:

Timeout for switchover to the main system.

Value range: **1** ... **255** seconds.

Retry Threshold:

Specifies the number of attempts permitted when switching back to the standby system.

Value range: **1** ... **255**

Automated Switchback

Checkbox for activating the option for automatic switchback to the main system.

7.2.8 Dialing Properties

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Dialing Properties

This area features the following components:

- General Data
- Possible Action Buttons
- "HFA Dialing Properties" Tab
- "HFA Dialing Properties (Standby)" Tab
- "SIP Dialing Properties" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.8.1 "HFA Dialing Properties" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Dialing Properties > "HFA Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

System Identification number:

Phone number of the system.

Format: Up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Extension Area:

This parameter defines a pattern for detecting internal extension numbers. From the workpoint's perspective, extension numbers are internal if they are assigned to the same system. The extension area can be specified as a regular expression.

Example: 1xxx, 2xxx, 3xxx, 4xxx, 5xxx are extensions and 6xxx, 7xxx, 8xxx, 9xxx are external phone numbers. The regular expression ^[12345] indicates that phone numbers starting with the digits 1 to 5 are internal extension numbers. If for example the system identification number is 667, all numbers from 6671xxxx to 6675xxx will be used as internal extensions.

Trunk code:

Number for trunk seizure for an outbound external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Format: Up to 21 digits.

Example: **01081**

Prefix Long Distance:

Number for an outbound long distance call.

Format: Up to 21 digits.

Example: **01081**

Prefix International:

Number for an outbound international call.

Format: Up to 21 digits.

Example: **01081**

Code for local calls:

Phone number, for example, of your company.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Code for National Dial:

National prefix.

Format: Up to five digits.

Example: **0** in Germany.

Code for International Dial:

International prefix.

Format: Up to four digits.

Example: **00** in Germany.

7.2.8.2 "HFA Dialing Properties (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Dialing Properties > "HFA Dialing Properties (Standby)" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").

NOTE: This "standby" data is used when the "home" data for the "HFA Dialing Properties" Tab is not available. The SRSR functionality must be configured for this, see Section 7.2.7, "Small Remote Site Redundancy".



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

System Identification number:

Phone number of the system.

Format: Up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Extension Area:

This parameter defines a pattern for detecting internal extension numbers. From the workpoint's perspective, extension numbers are internal if they are assigned to the same system. The extension area can be specified as a regular expression.

Example: 1xxx, 2xxx, 3xxx, 4xxx, 5xxx are extensions and 6xxx, 7xxx, 8xxx, 9xxx are external phone numbers. The regular expression ^[12345] indicates that phone numbers starting with the digits 1 to 5 are internal extension numbers. If for example the system identification number is 667, all numbers from 6671xxxx to 6675xxx will be used as internal extensions.

Trunk code:

Number for trunk seizure for an outbound external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Format: Up to 21 digits.

Example: **01081**

Prefix Long Distance:

Number for an outbound long distance call.

Format: Up to 21 digits.

Example: **01081**

Prefix International:

Number for an outbound international call.

Format: Up to 21 digits.

Example: **01081**

Code for local calls:

Phone number, for example, of your company.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Code for National Dial:

National prefix.

Format: Up to five digits.

Example: **0** in Germany.

Code for International Dial:

International prefix.

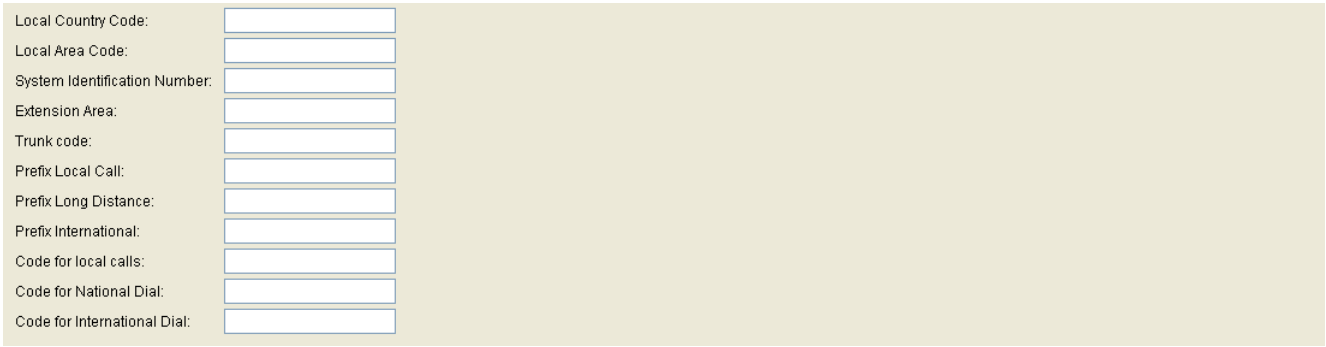
Format: Up to four digits.

Example: **00** in Germany.

7.2.8.3 "SIP Dialing Properties" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Dialing Properties > "SIP Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

System Identification number:

Phone number of the system.

Format: Up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Extension Area:

This parameter defines a pattern for detecting internal extension numbers. From the workpoint's perspective, extension numbers are internal if they are assigned to the same system. The extension area can be specified as a regular expression.

Example: 1xxx, 2xxx, 3xxx, 4xxx, 5xxx are extensions and 6xxx, 7xxx, 8xxx, 9xxx are external phone numbers. The regular expression ^[12345] indicates that phone numbers starting with the digits 1 to 5 are internal extension numbers. If for example the system identification number is 667, all numbers from 6671xxxx to 6675xxx will be used as internal extensions.

Trunk code:

Number for trunk seizure for an outbound external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Prefix Local Call:

Format: Up to 21 digits.

Example: **01081**

Prefix Long Distance:

Number for an outbound long distance call.

Format: Up to 21 digits.

Example: **01081**

Prefix International:

Number for an outbound international call.

Format: Up to 21 digits.

Example: **01081**

Code for local calls:

Phone number, for example, of your company.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Code for National Dial:

National prefix.

Format: Up to five digits.

Example: **0** in Germany.

Code for International Dial:

International prefix.

Format: Up to four digits.

Example: **00** in Germany.

7.2.9 Audio/Video Settings

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings

This area features the following components:

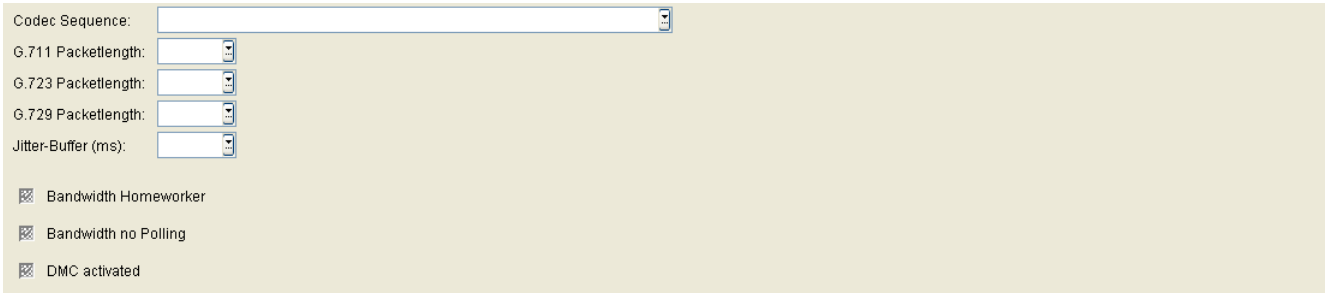
- General Data
- Possible Action Buttons
- "HFA Codec Settings" Tab
- "SIP Codec Settings" Tab
- "Audio Schemes" Tab
- "Available Audio Devices" Tab
- "Video Settings" Tab
- "Available Video Devices"
- "Ring Tones"

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.9.1 "HFA Codec Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "HFA Codec Settings" Tab



Codec Sequence:

Possible options:

- **not compressing Codecs preferred, besides G.723 preferred**
- **not compressing Codecs preferred, besides G.729 preferred**
- **compressing Codecs preferred, G.723 preferred**
- **compressing Codecs preferred, G.729 preferred**
- **only compressing Codecs, G.723 preferred**
- **only compressing Codecs, G.729 preferred**

G.711 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

G.723 Packetlength:

Possible options:

- **30**
- **60**

G.729 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

Jitter-Buffer (ms):

Caching duration:

Possible options (in ms):

Value range: **20** ... **190** milliseconds.

Bandwidth Homeworker

Checkbox for activating the bandwidth for homeworker data transmission.

Bandwidth no polling

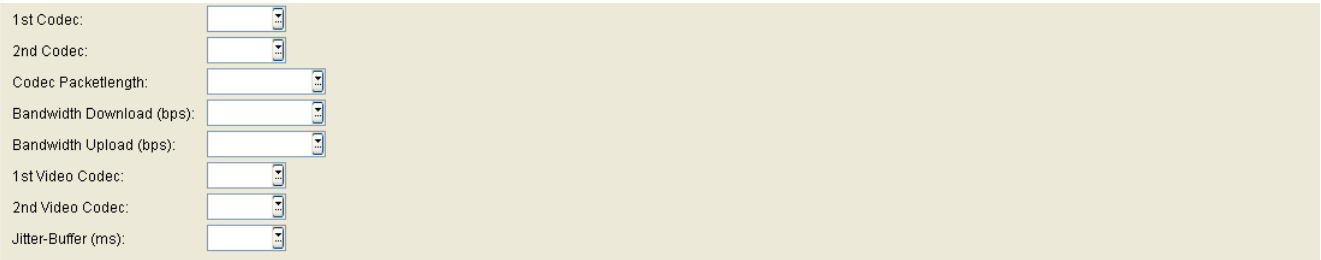
Checkbox for activating the bandwidth with no polling.

DMC activated

Checkbox for activating DMC bandwidth.

7.2.9.2 "SIP Codec Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "SIP Codec Settings" Tab



1st Codec:

First compression job.

Possible options:

- **G.711**
- **G.729**

2nd Codec:

Second compression job.

Possible options:

- **G.711**
- **G.729**
- **None**

3rd Codec:

Third compression job.

Possible options:

- **G.711**
- **G.729**
- **None**

Codec Packetlength:

Possible options:

- **Automatic**
- **10**
- **20**

Bandwidth Download (kbit/s):

Possible options:

- **56**
- **64**
- **128**
- **256**
- **512**
- **1024**
- **2048**
- **3072**
- **6144**
- **10000**
- **12288**
- **24576**
- **100000**
- **1000000**

Bandwidth Upload (kbits):

Possible options:

- **56**
- **64**
- **128**
- **256**

- **512**
- **1024**
- **2048**
- **3072**
- **6144**
- **10000**
- **12288**
- **24576**
- **100000**
- **1000000**

1st Video Codec

Possible options:

- **H.263**
- **H.264**

2nd Video Codec

Possible options:

- **H.263**
- **H.264**
- **None**

Jitter-Buffer (ms)

Possible options:

- **20**
- **30**
- **40**
- **50**
- **60**

- **70**
- **80**
- **90**
- **100**
- **110**
- **120**
- **130**
- **140**
- **150**
- **160**
- **170**
- **180**
- **190**

7.2.9.3 "Audio Schemes" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "Audio Schemes" Tab



These tabs let you define hardware settings for the voice output or ringer devices, for example.

Local Administration of Audio Settings

If this checkbox is activated, the audio settings can be changed only on the optiClient, but not by the DLS. In this case, the fields under **Audio Schemes** are only for display.

If this checkbox is inactive, the audio settings can be changed only by the DLS.

Index

Number of the setting.

Audioscheme

Name of the audioscheme.

Ringer Device

Audio hardware for the ringer device.

Voice Out Device

Audio hardware for the voice out device.

Voice In Device

Audio hardware for the voice in device.

Second Device

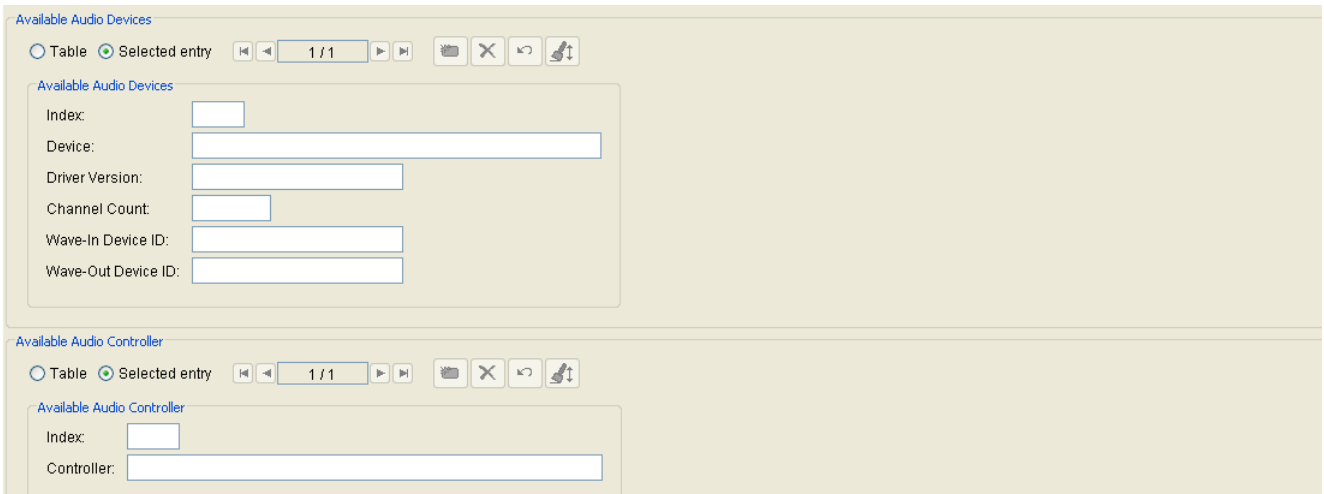
Audio hardware representing a second device. If a second device is selected here and this audioscheme is active, an additional icon appears in the main menu for controlling the second device.

Audio Controller

Additional function for controlling hardware functions.

7.2.9.4 "Available Audio Devices" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "Available Audio Devices" Tab



Available Devices:

Index

Serial number of the audio device.

Device

Name of the audio device for alerting and voice.

Driver Version

Driver version for the audio device.

Channel Count

Number of available audio channels.

Wave-In Device ID

Wave-Out Device ID

Available Audio Controller:

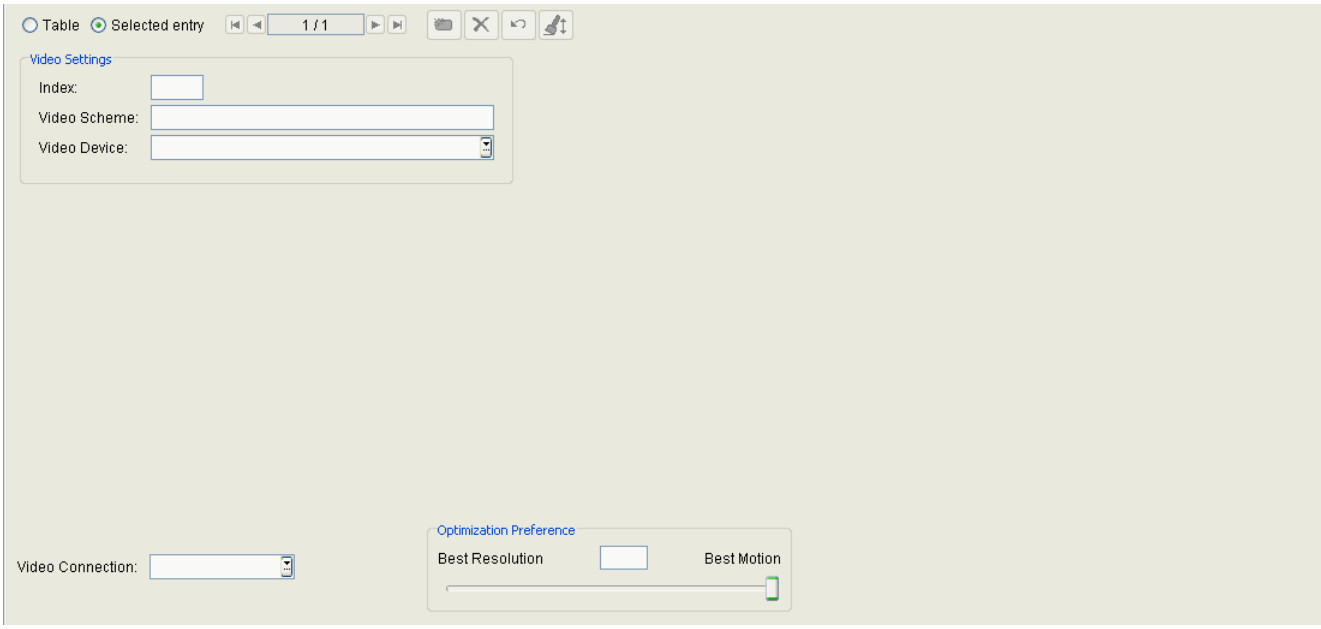
Index

Number of the setting

Controller

7.2.9.5 "Video Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "Video Settings" Tab



Index

Number of the setting.

Video Scheme

Name of the video scheme.

Video Device

Camera for transmitting the picture in video connections.

Video Connection

optiClient 130 allows parties to connect their video pictures providing both parties have an operational video system.

Possible options:

- **Locked**

- **Optional**

Optimization Preference

Best Resolution

Optimization to the highest possible resolution.

Best Motion

Optimization to the best possible reproduction of movement.

7.2.9.6 "Available Video Devices"

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "Available Video Devices"



Index

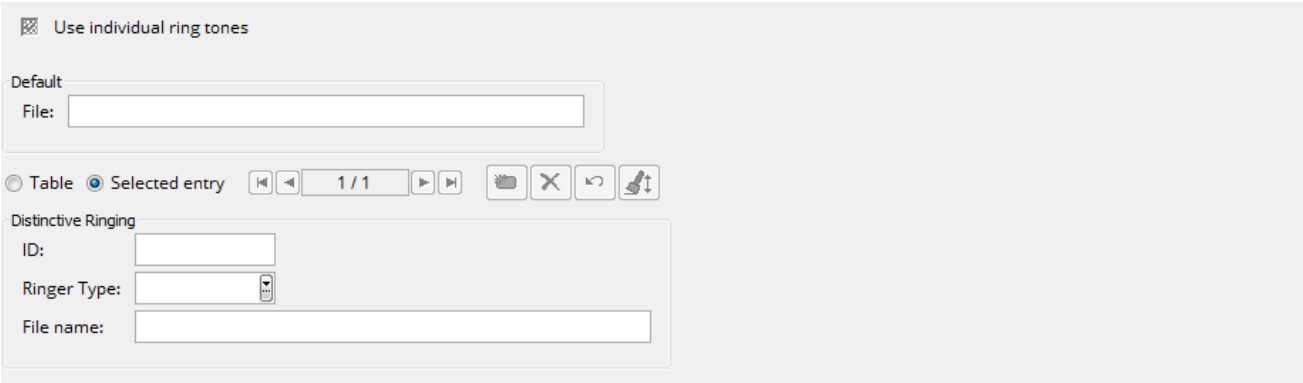
Number of the setting.

Device

All cameras installed on the workstation are listed. Select the camera you wish to use. If no cameras are listed here, your PC is not equipped with a video camera.

7.2.9.7 "Ring Tones"

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Audio/Video Settings > "Ring Tones"



Use Individual ring tones

.Disabled by default.

Default

File:

Individual ringtone file.Type:`String`
No validation needed. This item will be enabled only if the **Use individual ring tones** checkbox is activated.

Distinctive Ringing

ID:

Distinctive ringing ID. Type: `String`.

Ringer Type:

Possible values:

- **Internal**
- **External**
- **Audio File**

File Name:

Distinctive ringing audio file. Type: `String`

> ***NOTE:*** For instance, `C:\Users\Public\Music\Sample Music\Kalimba.mp3`, but no validation is needed on the path, since this path is located in the PC that the clients run.
> Finally this item will be enabled only if the Ringer type has value "**AudioFile**.

7.2.10 Directories/Address Books

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Directories/Address Books

This area features the following components:

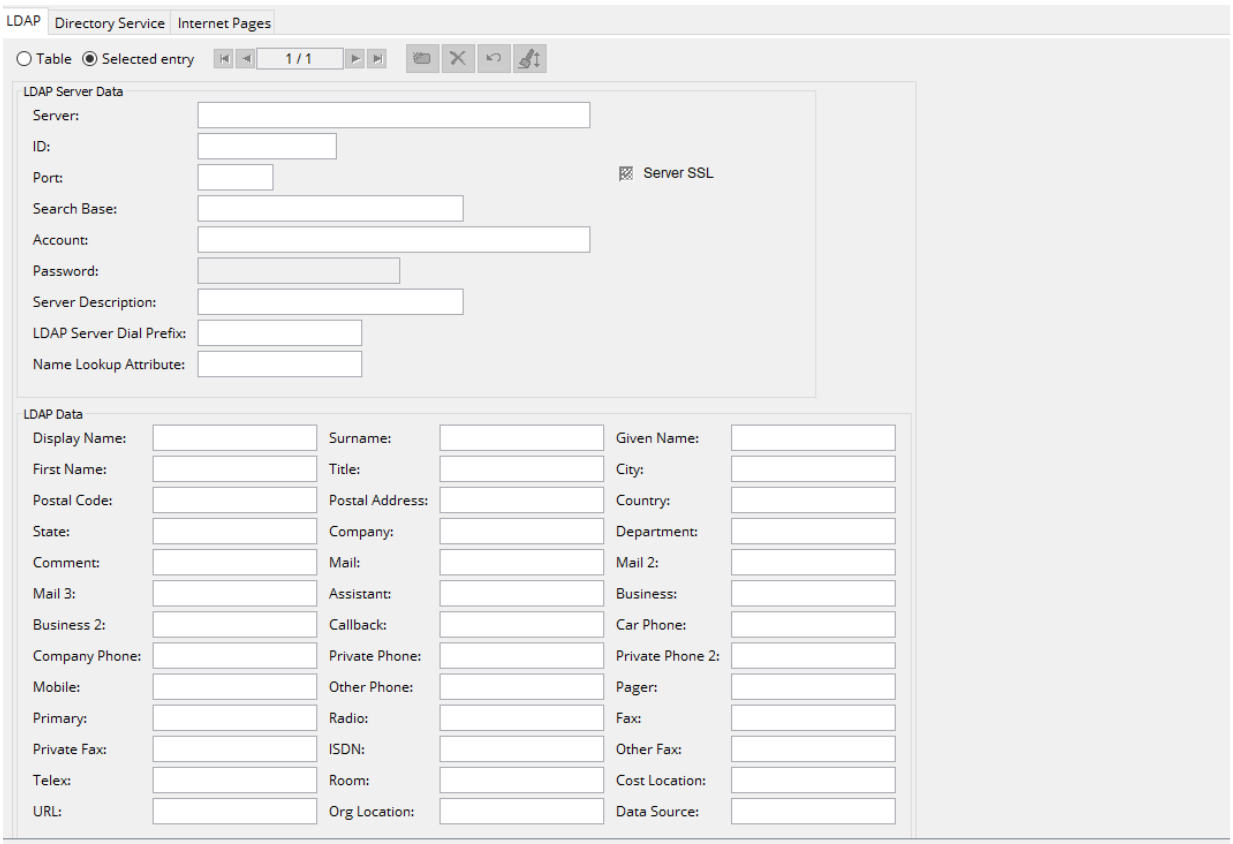
- General Data
- Possible Action Buttons
- "LDAP" Tab
- "Directory Service" Tab
- "Internet Pages" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.10.1 "LDAP" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Directories/Address Books > "LDAP" Tab



You can configure access to any LDAP directories in the network.

Server

IP address or host name of the LDAP server.

ID

Name of the LDAP server.

Port

Port number of the LDAP server.

Server SSL

If this check box is enabled, the Port value changes from 389 to 636.

Account

LDAP server account.

Password

Password for accessing the LDAP server.

Server Description

Descriptive text for the LDAP server.

Searchbase

During LDAP server configuration, this function allows you to specify a base level

which is used as a starting point for searching or displaying optiClient 130 entries in this LDAP directory.

You can use two different formats to define a base level:

`<level 3>=<name>, <level 2>=<name>, <level 1>=<name>` or

`<level 1>=<name>/<level 2>=<name>/<level 3>=<name>`

Example of an LDAP directory with the following elements:

- Level 1: c (for example for "country"), name, for example: US
- Level 2: o (for example, for "organization"), name, for example, Unify
- Level 3: ou (for example for "organization unit"), name, for example, COM

To specify this level as a searchbase, enter the following information in **Searchbase**:

`ou=COM, o=Unify, c=US` or `c=US/o=Unify/ou=COM`.

If you do not restrict the searchbase, the entire LDAP directory is used as the searchbase.

LDAP Server Dial Prefix

If LDAP directory services are generally available in the network and configured in the user settings, these are available under the configured name (for example, "Unify Corporate Directory"). This means you can configure and use several LDAP directories.

Name Lookup Attribute

Searches for an attribute with the name entered in the field (non-numeric values).

Display Name

Activates display name display and the entry of a label for the display name.

Surname

Activates name display and the entry of a label for the name.

Given Name

Activates second name display and the entry of a label for the second name.

First Name

Activates first name display and the entry of a label for the first name.

Title

Activates title display and the entry of a label for the title.

City

Activates city display and the entry of a label for the city.

Postal Code

Activates postal code display and the entry of a label for the postal code.

Postal Address

Activates postal address display and the entry of a label for the postal address.

Country

Activates country display and the entry of a label for the country.

State

Activates state display and the entry of a label for the state.

Company

Activates company display and the entry of a label for the company.

Department

Activates department display and the entry of a label for the department.

Comment

Activates comment display and the entry of a label for the comment.

Mail

Activates mailbox display and the entry of a label for the mailbox.

Mail 2

Activates second mailbox display and the entry of a label for the second mailbox.

Mail 3

Activates third mailbox display and the entry of a label for the third mailbox.

Assistant

Activates assistant display and the entry of a label for the assistant.

Business

Activates business display and the entry of a label for the business area.

Business 2

Activates second business display and the entry of a label for the second business area.

Callback

Activates callback number display and the entry of a label for the callback number.

Car Phone

Activates car phone number display and the entry of a label for the car phone number.

Company Phone

Activates company phone number display and the entry of a label for the company phone number.

Private Phone

Activates private phone number display and the entry of a label for the private phone number.

Private Phone 2

Activates second private phone number display and the entry of a label for the second private phone number.

Mobile

Activates mobile phone number display and the entry of a label for the mobile phone number.

Other Phone

Activates another phone number display and the entry of a label for the other phone number.

Pager

Activates pager number display and the entry of a label for the pager number.

Primary

Radio

Fax

Activates fax number display and the entry of a label for the fax number.

Private Fax

Activates private fax number display and the entry of a label for the private fax number.

ISDN

Activates ISDN number display and the entry of a label for the ISDN number.

Other Fax

Activates another fax number display and the entry of a label for the other fax number.

Telex

Activates telex number display and the entry of a label for the telex number.

Room

Activates room number display and the entry of a label for the room number.

Cost Location

Activates cost location display and the entry of a label for the cost location.

URL

Activates URL display and the entry of a label for the URL.

Location

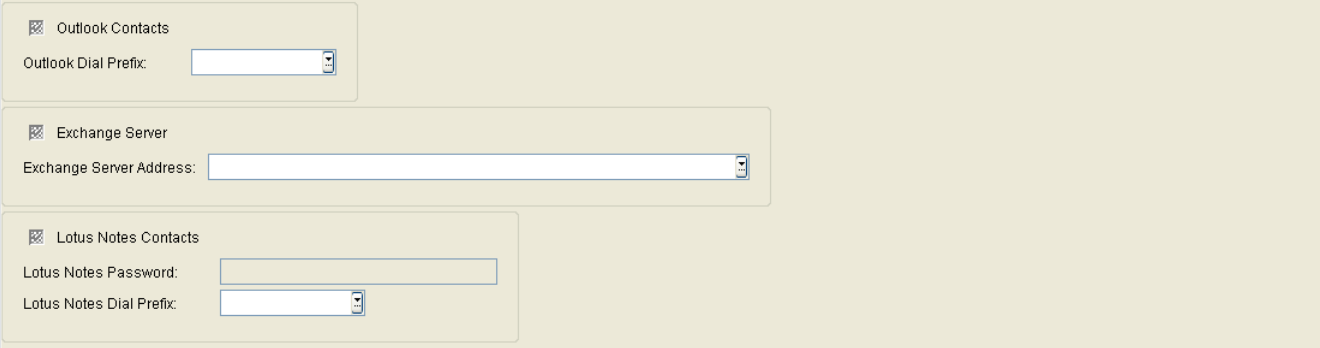
Activates location display and the entry of a label for the location.

Data Source

Activates data source display and the entry of a label for the data source.

7.2.10.2 "Directory Service" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Directories/Address Books > "Directory Service" Tab



You can configure different settings for accessing central and local directories. This access enables you to work with directories and address books in optiClient 130.

Outlook Contacts

This directory contains all entries from the Contacts folder in a local Microsoft Outlook installation. If Outlook is not installed or this directory is not configured for your users, then this directory is not available.

This checkbox creates a directory containing Outlook contact information in the optiClient 130.

Outlook Dial Prefix:

This directory contains all entries from the Contacts folder in a local Microsoft Outlook installation. If Outlook is not installed or this directory is not configured for your users, then this directory is not available.

Exchange Server

This directory contains all entries from the Microsoft Exchange Server Global Address Book (if installed).

This checkbox creates a directory containing Microsoft Exchange Server Information in the optiClient 130.

Exchange Server Address:

IP address or host name of the Microsoft Exchange Server.

Lotus Notes Contacts

This directory contains all entries from the Contacts folder in your local Lotus Notes installation (if installed).

This checkbox creates a directory containing Lotus Notes contact information in the optiClient 130.

Lotus Notes Password:

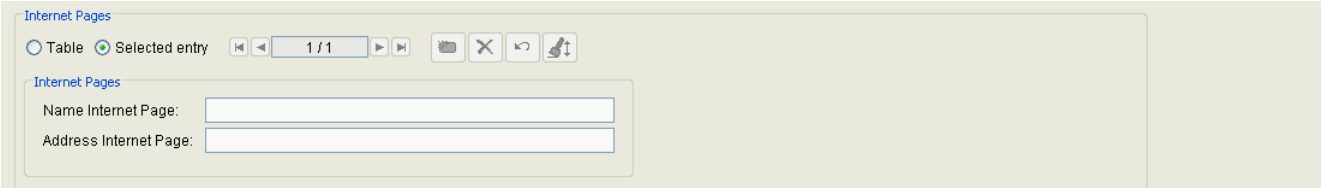
Password for accessing Lotus Notes.

Lotus Notes Dial Prefix:

This directory contains contact entries from your local Lotus Notes installation. If Lotus Notes is not installed or this directory is not configured for your users, then this directory is not available.

7.2.10.3 "Internet Pages" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Directories/Address Books > "Internet Pages" Tab



Name Internet Page:

Random name of the Internet page.

Address Internet Page:

URL of the Internet page.

7.2.11 Miscellaneous

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Miscellaneous

This area features the following components:

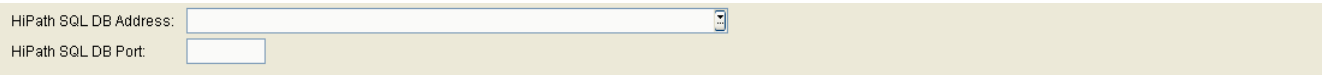
- General Data
- Possible Action Buttons
- "HiPath SQL DB" Tab
- "System Functions" Tab
- "SIP Features" Tab
- "SIP Features 2" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.11.1 "HiPath SQL DB" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Miscellaneous > "HiPath SQL DB" Tab



HiPath SQL DB Address:

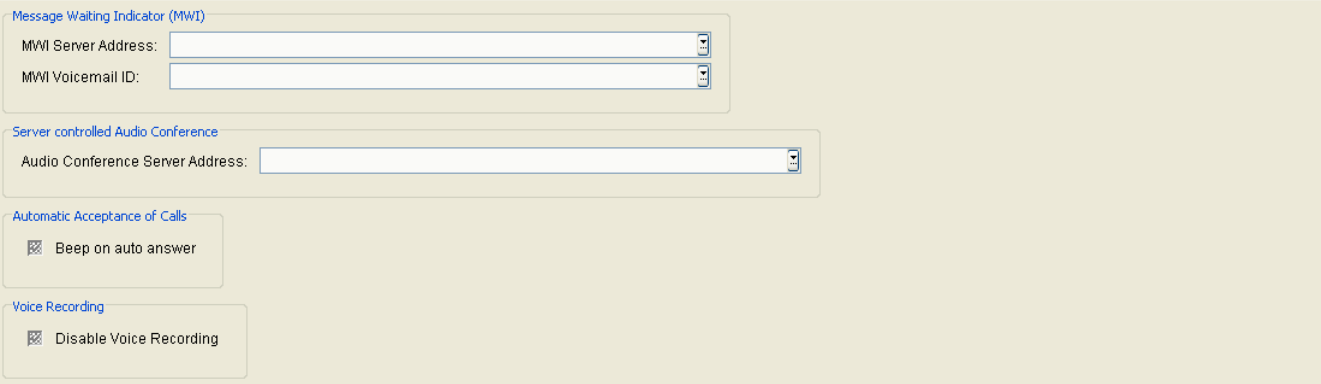
IP address or host name of the HiPath SQL DB.

HiPath SQL DB Port:

Port number for the HiPath SQL DB.

7.2.11.2 "System Functions" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Miscellaneous > "System Functions" Tab



Message Waiting Indicator (MWI)

MWI Server Address:

IP address or host name of the MWI server.

MWI Voicemail ID:

Identification number for accessing the MWI server.

Server Controlled Audio Conference

Audio Conference Server Address:

IP address or host name for the audio conference server.

OSV default Large Conference PAC :1234567890

Automatic Acceptance of Calls

Beep on auto answer

Activates beep on auto answer.

Voice Recording

Disable Voice Recording

Activates or deactivates voice recording.

7.2.11.3 "SIP Features" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Miscellaneous > "SIP Features" Tab



Callback

Activating Code in case of no answer:

Code for controlling the "Callback-no reply" function on the server.

Activating Code in case of busy

Code for controlling the "Callback-busy" function on the server.

Activating Code Clear all Callbacks

Code that deletes all callback jobs on the server.

Call Pickup

Group Pickup Server type:

Possible options:

- **Other**
- **OpenScape Voice**
- **Broadsoft**
- **Sylantro**
- **HiQ8000**

- **Genesys**

Group Pickup URI:

IP address or host name of the server for providing the call pickup feature.

Huntgroup

Function Code for temporary logout from a hunt group

Huntgroup Code for "temporary logout".

OSV PAC default service name : Make Busy Toggle **13

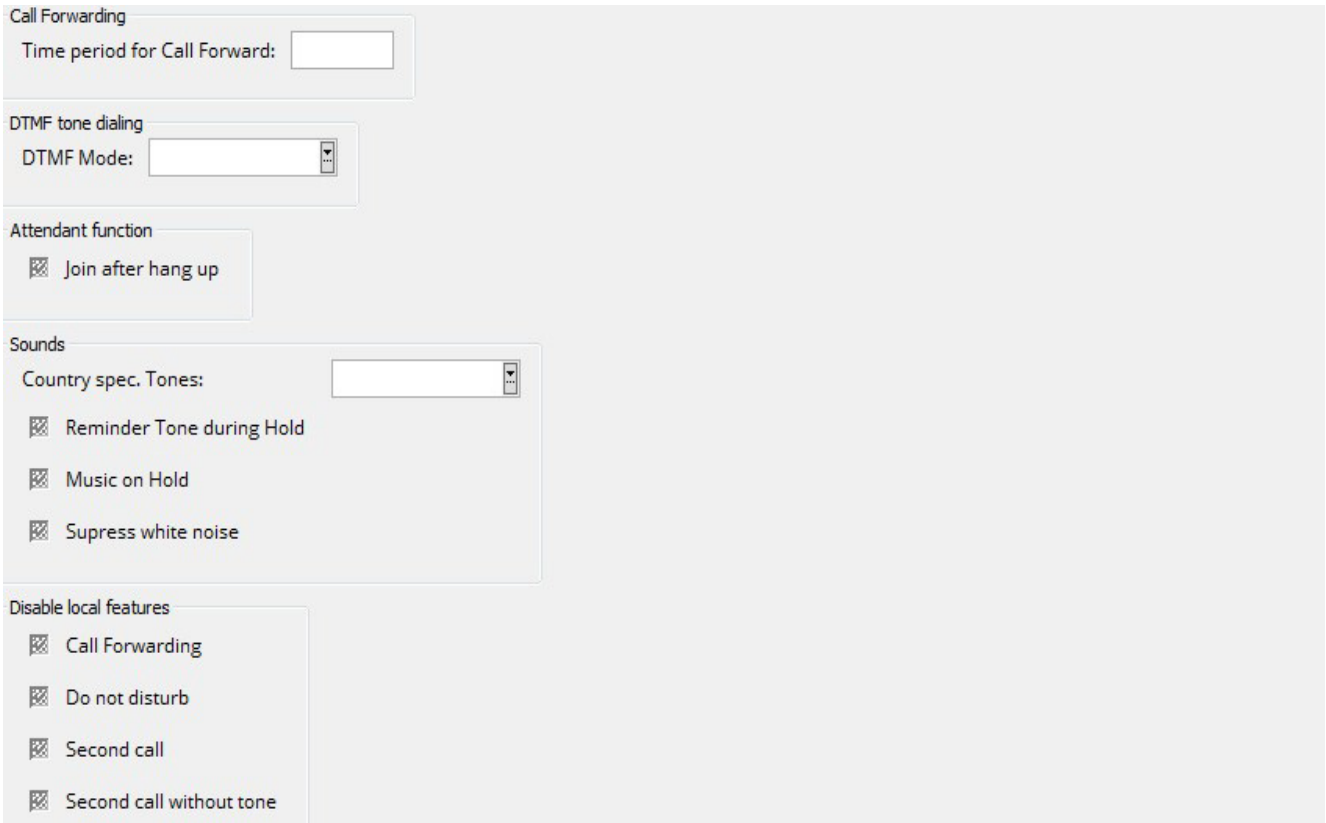
Huntgroup Code for busy signaling

Function code for "busy signaling in a hunt group".

OSV PAC default service name : Stop Hunt Toggle **14

7.2.11.4 "SIP Features 2" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Miscellaneous > "SIP Features 2" Tab



Call Forwarding

Time period for Call Forward

Enter the time after which unanswered calls are forwarded when call forwarding is active.

DTMF tone dialing

DTMF Mode:

Possible options:

- **Automatic**
- **Inband**

Attendant Function

Join after hang up:

Activate this checkbox when you have two active connections (for example, during consultation hold) and then hang up. If the checkbox is active, the two connected parties are connected to each another; if the checkbox is not active, both connections are ended.

Sounds

Country spec. Tones:

Possible options:

- **Brazil**
- **China**
- **Germany**
- **France**
- **Great Britain**
- **International**
- **Italy**
- **Netherlands**
- **Portugal**
- **Spain**
- **USA**

Reminder Tone during Hold:

Activate this checkbox if you want a reminder tone to signal held calls.

Music on Hold:

Activate this checkbox if you want music on hold to be played in certain situations (for example, call forwarding, call hold, consultation).

Suppress white noise:

Activate this checkbox if you want to allow background noise suppression.

Disable local features:

- **Call forwarding**
  Activate this checkbox if you want to disable call redirection to a different phone number.
- **Do not disturb**
  Activate this checkbox if you want to disable the "Do not disturb" mode, where calls and notifications are silenced.
- **Second call**
  Activate this checkbox if you want to disable second call alerting.

Second call without tone

Activate this checkbox if you want to disable the second call alerting without tone.

7.2.12 Keysets/Keylayout

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout

This area features the following components:

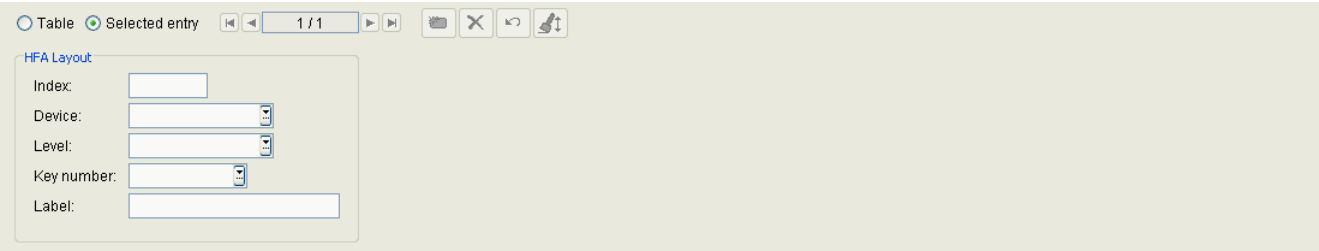
- General Data
- Possible Action Buttons
- "HFA Layout" Tab
- "HFA Layout (Standby)" Tab
- "SIP Keysets" Tab
- "SIP Line Keys" Tab
- "SIP Station Keys (DSS)" Tab
- "SIP Call Forwarding" Tab
- "SIP Keypad" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.12.1 "HFA Layout" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "HFA Layout" Tab



Index

Name of the key layout function.

Device

Device selection for the programmed key.

Possible options:

- **1st Sidecar**
- **2nd Sidecar**
- **3rd Sidecar**
- **4th Sidecar**
- **Base Device**

Level

Level number of the programmed key.

Key number

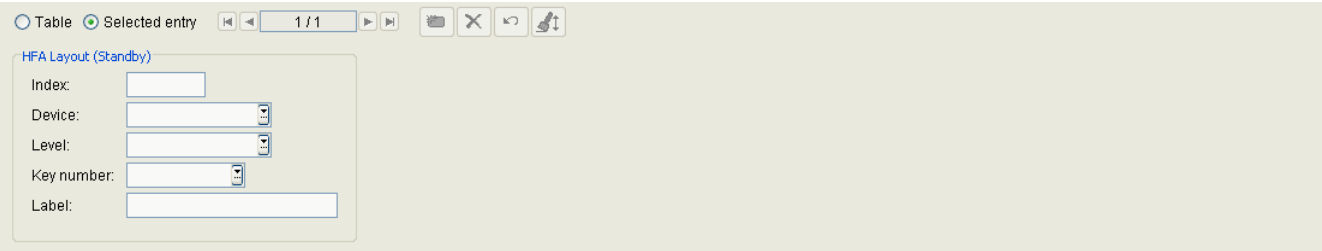
Key number of the programmed key.

Label

Label displayed for the programmed key.

7.2.12.2 "HFA Layout (Standby)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "HFA Layout (Standby)" Tab



Index

Name of the key layout function.

Device

Device selection of the programmed key.

Possible options:

- **1st Sidecar**
- **2nd Sidecar**
- **3rd Sidecar**
- **4th Sidecar**
- **Base Device**

Level

Level number of the programmed key.

Key number

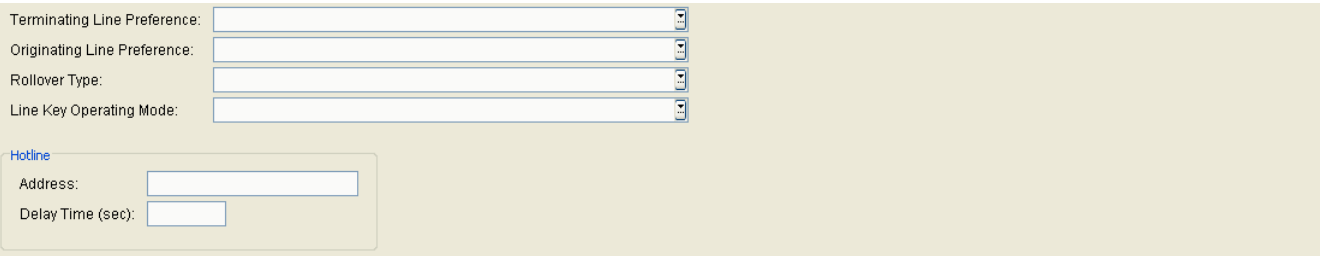
Key number of the programmed key.

Label

Label displayed for the programmed key.

7.2.12.3 "SIP Keysets" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "SIP Keysets" Tab



Terminating Line Preference:

Possible options:

- **Idle line preference**
- **Ringing line preference**

Originating Line Preference:

Possible options:

- **Idle line preference**
- **Primary line preference**

Rollover Type:

Type of alerting to be used in the case that, during an active call, an incoming call arrives on a different line.

Possible options:

- **No tone**
- **Normal beep**
- **Special beep**

Line Key Operating Mode:

Defines what should happen to a line (call) when a connection is established over another line.

Possible options:

- **Hold first call**
- **Clear first call**

Hot Line

Address

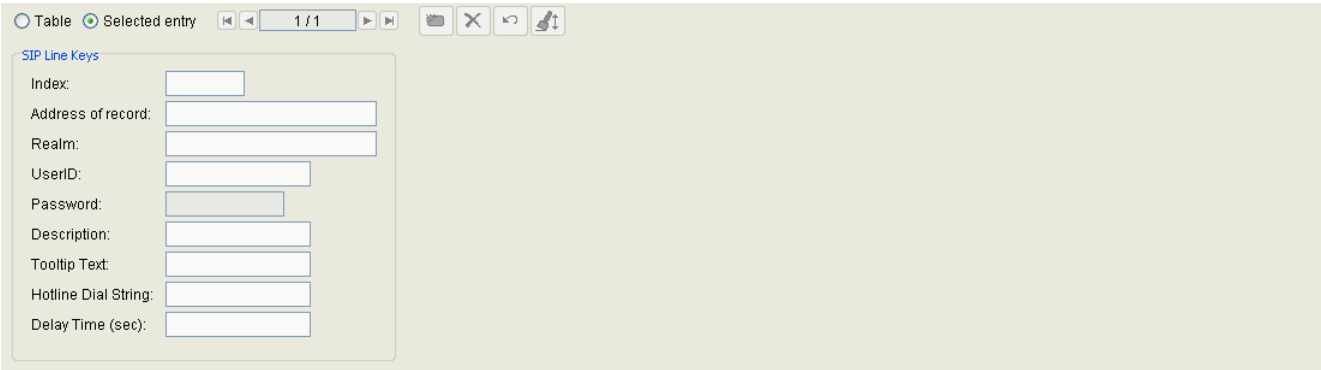
Address resp. call number which is dialed after the line has been activated (e. g. by going off-hook) and the delay time has expired.

Delay Time (sec)

Dialing delay in seconds. If delay time = 0, the connection is established immediately.

7.2.12.4 "SIP Line Keys" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "SIP Line Keys" Tab



Index:

Line key number

Address of record:

Phone number for the line belonging to this line key.

Realm:

SIP realm for the line's address of record

UserID:

SIP user name of the line's address of record

Password:

Password for the SIP user name.

Description:

Description of the line.

Tooltip Text:

Text that appears in the ToolTip for the line.

Hotline Dial String:

Number called if the line is configured as the hotline.

Delay Time (sec):

Delay between line seizure (for example, by lifting the handset) and hotline number dialing.

7.2.12.5 "SIP Station Keys (DSS)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "SIP Station Keys (DSS)" Tab



Index

Index number of the key function.

DSS Address

Phone number of the DSS (Direct Station Select) line.

Realm

SIP realm of the DSS line.

UserID

SIP user name of the DSS line’s address of record.

Password

Password for the SIP user name.

Description

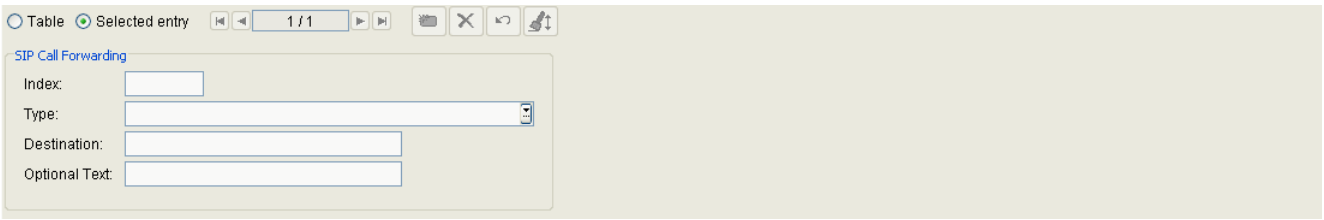
Description of the DSS line.

Tooltip Text

Text entry that appears in the ToolTip for the DSS line key.

7.2.12.6 "SIP Call Forwarding" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "SIP Call Forwarding" Tab



Index

Index number of the call forwarding key.

Type

Selection of conditions, under which call forwarding is executed.

- **All calls**
- **External calls (HiPath 3000)**
- **Internal calls (HiPath 3000)**
- **on busy (SIP, HiPath 4000)**
- **on no answer (SIP, HiPath 4000)**
- **on busy / no answer (HiPath 4000)**
- **on logout (HiPath 3000, HiPath 4000)**

Destination

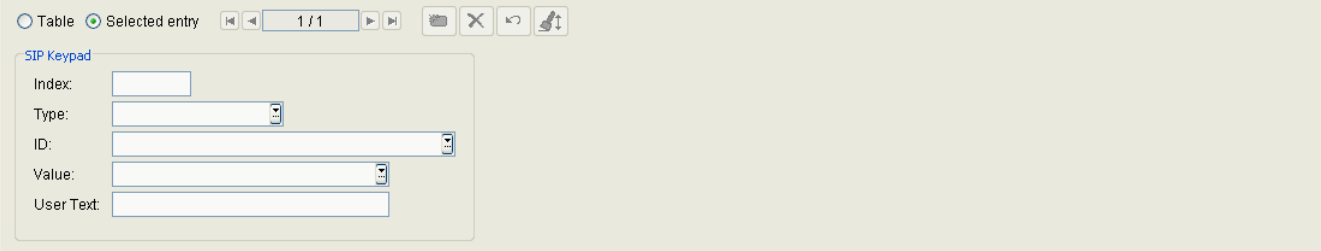
Destination of SIP call forwarding.

Optional Text

Description of the type of SIP call forwarding configured here.

7.2.12.7 "SIP Keypad" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Keysets/Keylayout > "SIP Keypad" Tab



Index

Index number of the key function.

Type

Type of SIP keypad.

ID

SIP keypad ID.

Value

Value of the key.

User Text

Descriptive label for the SIP keypad.

7.2.13 Signaling and Payload Encryption (SPE)

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Signaling and Payload Encryption (SPE)

This area features the following components:

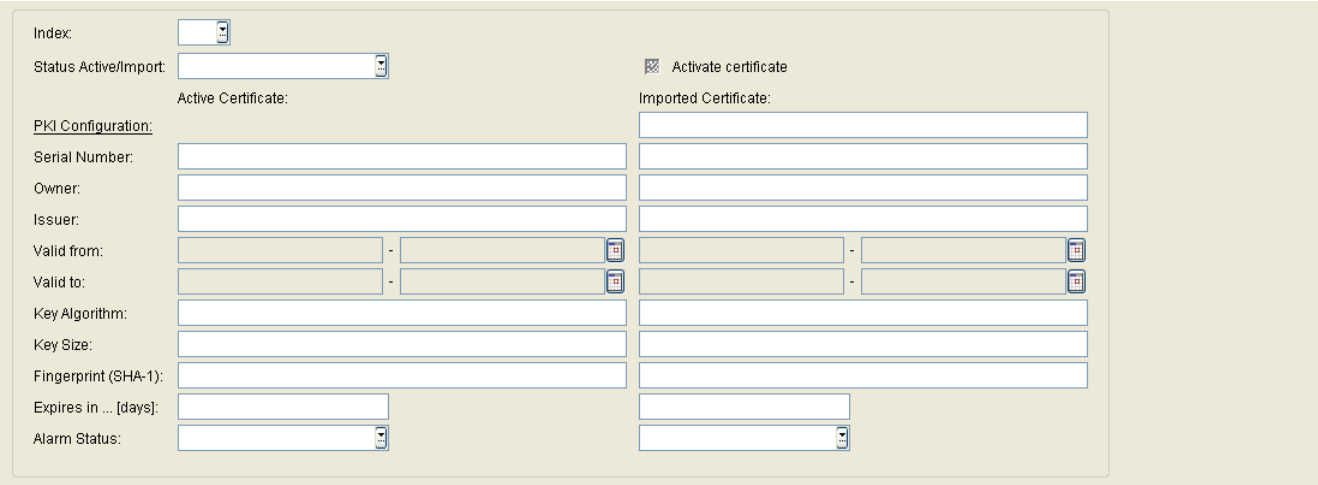
- General Data
- Possible Action Buttons
- "SPE CA Certificates" Tab
- "SIP Settings" Tab
- "HFA Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.2.13.1 "SPE CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Signaling and Payload Encryption (SPE) > "SPE CA Certificates" Tab



The parameters described below are available once for the currently active certificate and once for the imported certificate.

Index

Index number for the certificate.

Status Active/Import:

Specifies whether a certificate is registered as imported and/or active on the phone. The five statuses listed below are possible.

Possible values:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

PKI Configuration

Name of PKI configuration.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key Algorithm.

Key Size

Key Size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

Number of days before the certificate expires.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Displays the duration of validity for certificates when searching for certificates due to expire.

Possible values:

- **valid**
- **soon running out**
- **expired**

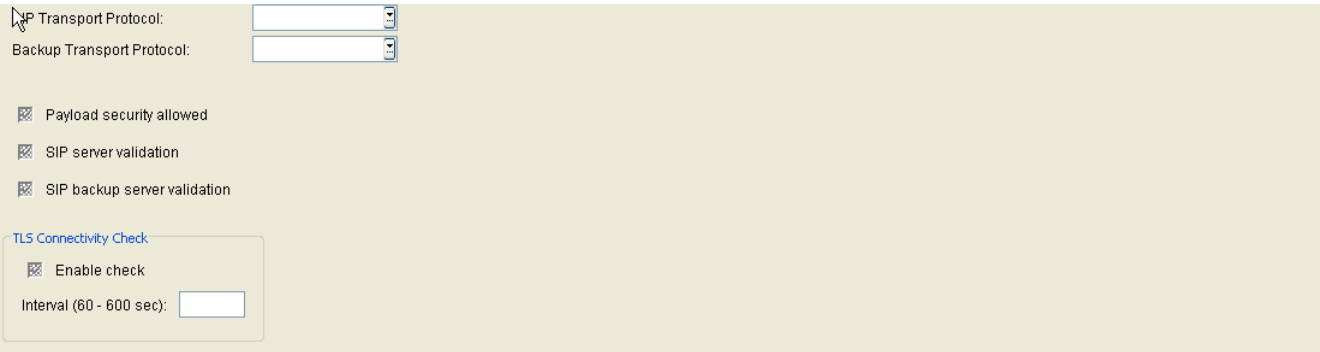
Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted. The active certificate is used to encrypt calls.

> ***IMPORTANT:*** In the case of OpenScape Desktop Clients, there is no impact when changing the TLS certificates .

7.2.13.2 "SIP Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Signaling and Payload Encryption (SPE) > "SIP Settings" Tab



SIP Transport Protocol:

Transport protocol used for SIP signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

Backup Transport Protocol:

Transport protocol used for SIP signaling when the backup SIP server is in use.

Possible options:

- **UDP**
- **TCP**

Payload security allowed

If this checkbox is activated, encryption of voice messages is enabled.

SIP server validation

If this checkbox is activated, the connection to the SIP server is verified.

SIP backup server validation

If this checkbox is activated, the connection to the backup SIP server is verified.

TLS Connectivity Check

Enable check

If checkbox is activated, the TLS connectivity check will be enabled.

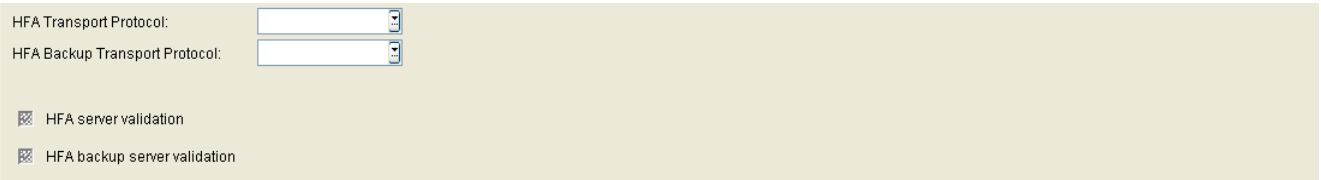
Interval

Time interval in seconds in which the TLS connectivity is checked periodically.

Possible options: **60** - **600**

7.2.13.3 "HFA Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Signaling and Payload Encryption (SPE) > "HFA Settings" Tab



HFA Transport Protocol:

Transport protocol used for HFA signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

HFA Backup Transport Protocol:

Transport protocol used for HFA signaling when the backup HFA server is in use.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

HFA server validation

If this checkbox is activated, the connection to the HFA server is verified.

HFA backup server validation

If this checkbox is activated, the connection to the HFA backup server is verified.

7.2.14 Dialup Site

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Dialup Site

This area features the following components:

- General Data
- Possible Action Buttons
- "Dialup Site Parameters" Tab

7.2.14.1 "Dialup Site Parameters" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Dialup Site > "Dialup Site Parameters" Tab



Dialup Site

The name of the User Profile of IP Client. It is initially created through the Login Dialog of the IP Client.

Quality of Service

Layer 3 Select

Checkbox for activating the QoS configuration on layer 3.

Layer 3 Signaling:

Class of service value for call signaling on layer 3.

Possible options:

- **AF11**
- **AF12**

- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**
- **EF**
- **CS7**
- **Default**

Layer 3 Voice:

Class of service value for voice on layer 3.

Possible options:

- **AF11**
- **AF12**
- **AF13**
- **AF21**
- **AF22**
- **AF23**
- **AF31**
- **AF32**
- **AF33**
- **AF41**
- **AF42**
- **AF43**

- **EF**
- **CS7**
- **Default**

Layer 2 Select

Checkbox for activating the QoS layer 2 configuration.

Layer 2 Signaling:

Class of Service value for call signaling on layer 2.

Value range: **0** ... **7**

Layer 2 Voice:

Class of Service value for voice on layer 2.

Value range: **0** ... **7**

Codec Settings

Codec Settings (SIP)

1st Codec:

First compression method.

Possible options:

- **G.711**
- **G.729**

2nd Codec:

Second compression method.

Possible options:

- **G.711**
- **G.729**

- **None**

3rd Codec:

Third compression method.

Possible options:

- **G.711**
- **G.729**
- **None**

Codec Packetlength:

Possible options:

- **Automatic**
- **10**
- **20**

Jitter-Buffer (ms):

Caching duration:

Possible options (in ms):

Value range: **20** ... **190** milliseconds.

Codec Settings (HFA)

Codec Sequence:

Possible options:

- **not compressing Codecs preferred, besides G.723 preferred**
- **not compressing Codecs preferred, besides G.729 preferred**
- **compressing Codecs preferred, G.723 preferred**
- **compressing Codecs preferred, G.729 preferred**
- **only compressing Codecs, G.723 preferred**
- **only compressing Codecs, G.729 preferred**

G.711 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

G.723 Packetlength:

Possible options:

- **30**
- **60**

G.729 Packetlength:

Possible options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**

Jitter-Buffer (ms):

Cache size.

Possible options (in ms):

Value range: **20** ... **190** milliseconds.

DMC activated

Checkbox for activating DMC bandwidth.

7.2.15 OpenScape

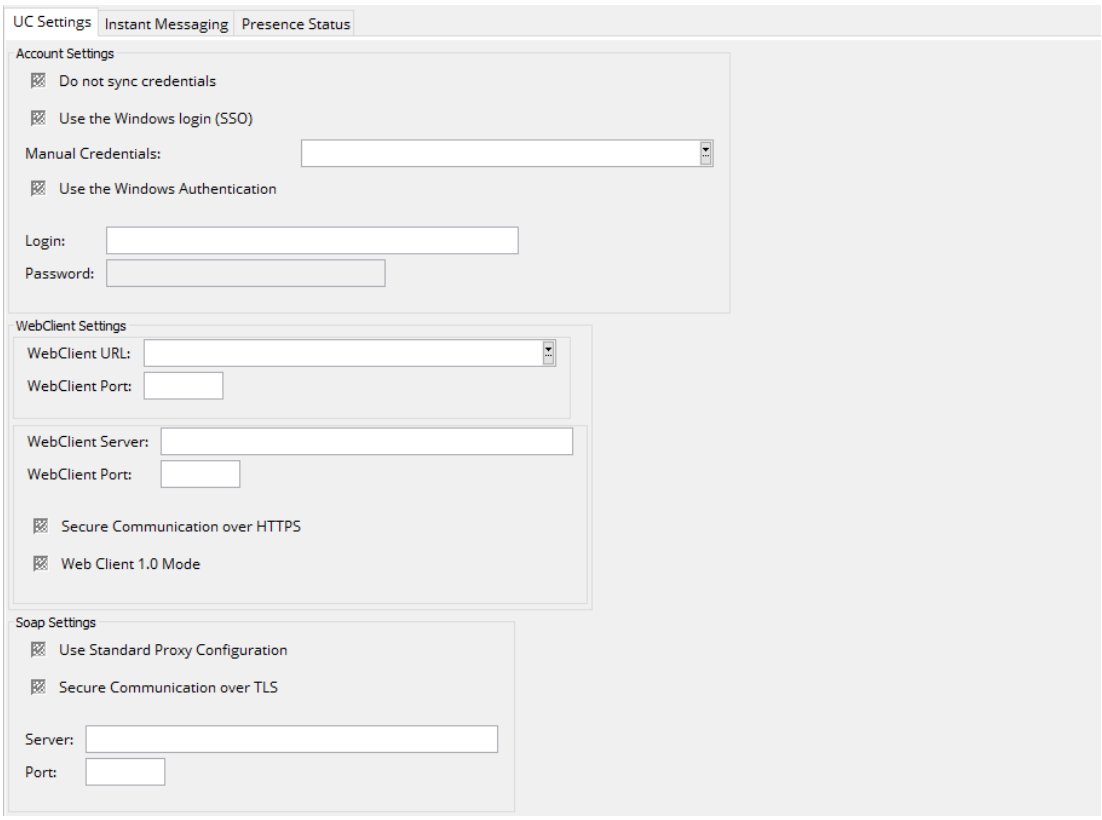
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > OpenScape

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "UC Settings" Tab
- "Instant Messaging (XMP)" Tab

7.2.15.1 "UC Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > OpenScape > "UC Settings" Tab



Account Settings

Do not sync credentials

Checkbox for not synchronizing UC credentials. When this checkbox is enabled, all credential related fields are erased and disabled.

Use the Windows login (SSO):

Checkbox for activating that Single Sign-On is used to login.

Manual Credentials:

Possible options:

- Do not allow

- Allow with cache
- Allow without cache (default option)

NOTE: If the **Use the Windows login (SSO)** checkbox is not activated, the **Manual Credentials** option shall be grayed out.

Login:

User ID for accessing the OpenScape Connection Server.

Password:

Password for accessing the OpenScape Connection Server.

WebClient Settings

WebClient URL:

Rules Configuration for access to WEB server.

WebClient Port:

Port number for access to the WEB server.

IMPORTANT: **WebClient URL** (Rules Configuration) and **WebClient Port** (Rules Port) refer to Fusion Client, whereas the other items to OpenScape Desktop Client-WE.

WebClient Server:

Address of the server for access to WebClient.

WebClient Port:

Port number of the server for access to WebClient.

Secure Communication over HTTPS:

Checkbox for activating secure communication over HTTPS.

Web Client 1.0 Mode:

Checkbox for enabling / disabling the use of existing WebClient interface.

Checkbox is disabled by default, thus implying use of the new WebClient interface.

Soap Settings

Use Standard Proxy Configuration:

If this checkbox is activated, the standard proxy is used.

Secure Communication over TLS:

If this checkbox is activated, TLS is used for secure communication.

Server:

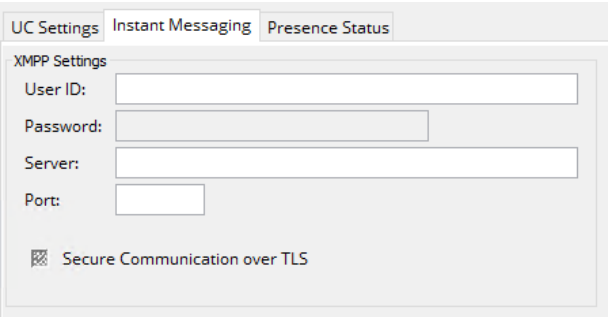
Address of the OpenScape Connection Server.

Port:

Port number of the OpenScape Connection Server.

7.2.15.2 "Instant Messaging (XMP)" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > OpenScape > "Instant Messaging (XMP)" Tab



User ID:

User ID for access to the OpenScape Instant Messaging (XMP) server.

Password:

Password for access to the OpenScape Instant Messaging (XMP) server.

Server:

Address of the server for OpenScape Instant Messaging (XMP).

Port:

Port number of the server for OpenScape Instant Messaging (XMP).

Secure Communication over TLS

Checkbox for activating secure communication over TLS.

7.2.16 HotKeys

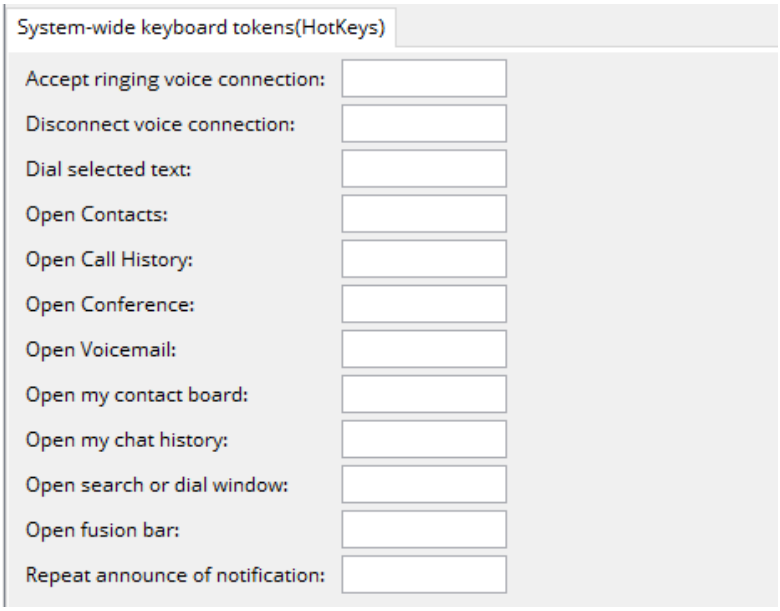
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > HotKeys

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- ’’System-wide keyboard tokens(Hotkeys)’’Tab

7.2.16.1 ”System-wide keyboard tokens(Hotkeys)”Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > HotKeys >”System-wide keyboard tokens(Hotkeys)”Tab



The HotKey configuration for F4O (Fusion for Outlook) is supported. This is the Hotkey (Fusion Client) configuration by DLS.

The values of these items as shown in the graphic User Interface could be any F key, i.e F1, F2, etc., or any combination with Ctrl, Alt, and Shift, i.e. "Ctrl+D" or "Alt+G".The DLS accepts entries under "System-wide keybord tockens (HotKey)" only in case that Hot Key entries are set with capital letters and without any space, e.g the "CTRL + Space" option can be accepted from DLS only in case that is entered as "CTRL+SPACE".

Any combination is upon customer discretion.

Refer to the following table for the possible combinations:

Possible Combinations	Not allowed
F2 to F11	Any combination with F1 and F12
ALT+F2 to F11	ALT+F4
CTRL+F2 to F11	ALT+F8
SHIFT+F2 to F11	CTRL+C (not allowed, except for the "Dial selected text")
ALT+A to Z	More than one modifier key (e.g. ALT+CTRL+Key)

Possible Combinations	Not allowed
ALT+0 to 9	Spaces between KEY selections & small letters is not the proper format for configuring HOTkey entries & will not be accepted from the DLS.
SHIFT+ESC	
ALT+SPACE	
CTRL+SPACE	
SHIFT+SPACE	

IMPORTANT: A specific key combination can be assigned only to one HotKey.

Accept ringing voice connection:

Disconnect voice connection:

Dial selected text:

Open Contacts:

Open Call History:

Open Conference:

Open Voicemail:

Open my contact board:

Open my chat history:

Open search or dial window:

Open fusion bar:

Repeat announce of notification:

7.2.17 Outlook

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Outlook

The HotKey configuration for F4O (Fusion for Outlook) is supported. This is the Hotkey (Fusion Client) configuration by DLS.

7.3 IP Gateway Configuration

This menu item consists of the following areas:

- QoS Data Collection
- Security Settings
- Signaling and Payload Encryption (SPE)
- IPSec/VPN

7.3.1 QoS Data Collection

This area features the following components:

- General Data
- Possible Action Buttons
- "Server Data" Tab
- "Report Settings" Tab
- "Threshold Values" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > QoS Data Collection > General Data



This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP gateways. The base data associated with the IP gateways found is displayed in **Object** view.

The value displayed in the **Remarks** fields can be changed (all other fields are read-only).

IP Address:

IP address of the IP gateway.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID

ID that uniquely identifies this IP gateway.

Device Type:

IP gateway device type.

You can view all IP devices supported by the DLS in Section 3.4, "Area of Application".

Example: **HG3500**

PEN:

Position of the gateway assembly group (plug-in position).

SW Version:

Software version of the IP gateway.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

Last Registration:

Last time the IP gateway logged on to the DLS.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP gateways that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.7, "Editing Templates".

Discard

Discards any changes made and new entries.

Read

The parameters displayed on the new mask are read in again by the IP device.

Rename

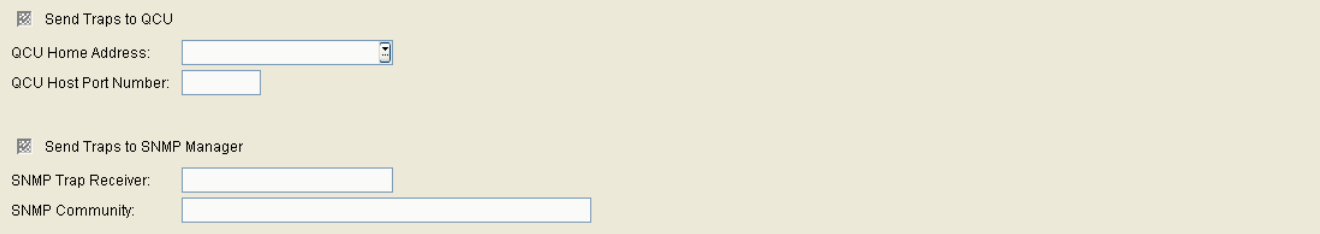
Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

7.3.1.1 "Server Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > QoS Data Collection > "Server Data" Tab



Send Traps to QCU

If this checkbox is activated, messages are sent to QCU in the event of errors.

QCU Home Address:

IP address or host name of the server that collects the QDC data.

QCU Host Port Number:

Port number for the server that collects the QDC data.

Send Traps to SNMP Manager

If this checkbox is activated, messages are sent to SNMP Manager in the event of errors.

SNMP Community:

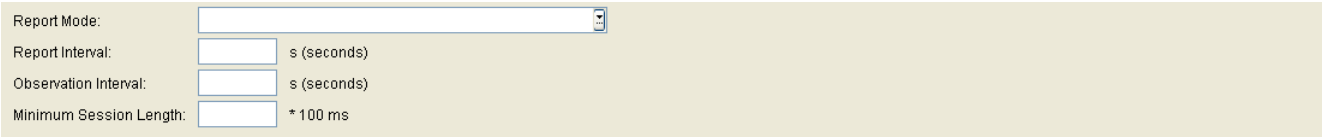
Community string used for authorization on the SNMP server.

SNMP Trap Receiver:

IP address of SNMP Manager.

7.3.1.2 "Report Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > QoS Data Collection > "Report Settings" Tab



Report Mode:

Specifies when a report should be generated.

Possible options:

- **EOS Threshold exceeded**
  At the end of the connection that exceeded the threshold.
- **EOR Threshold exceeded**
  At the end of the reporting interval that exceeded the threshold.
- **EOS (End of Session)**
  At the end of the connection.
- **EOR (End or Report Interval)**
  At the end of the reporting interval.

Report Interval:

Time interval in which a QoS report is sent.

Value range: **0** ... **3600** seconds.

Observation Interval:

Time interval in which threshold violation is checked.

Value range: **0** ... **5000** seconds.

Minimum Session Length:

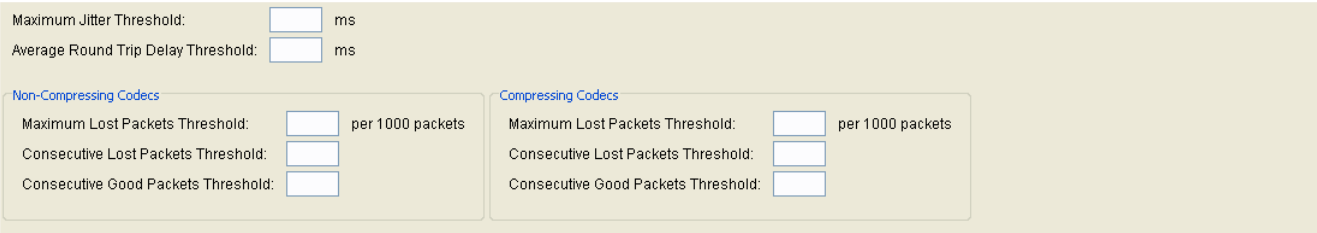
A QoS report is not sent if a session (for example, a call) undershoots this minimum.

Value range: **0** ... **5000** (x 100 ms).

7.3.1.3 "Threshold Values" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > QoS Data Collection > "Threshold Values" Tab

The threshold values that produce a QoS report if exceeded are entered here.



Maximum Jitter Threshold:

Maximum threshold in milliseconds for runtime fluctuations during data transmission.

Value range: **0** ... **255**

Default: **15**

Average Round Trip Delay Threshold:

Average response time in milliseconds for signal transmission. A report is issued if this is exceeded.

Default: **100**

Non-Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during uncompressed transmission. The number is specified in 1000-packet increments.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during uncompressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during uncompressed transmission.

Value range: **0** ... **255**

Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during compressed transmission.

Value range: **0** ... **255**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during compressed transmission.

Value range: **0** ... **255**

7.3.2 Security Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "WBM Server Certificates" Tab

7.3.2.1 "Settings" Tab

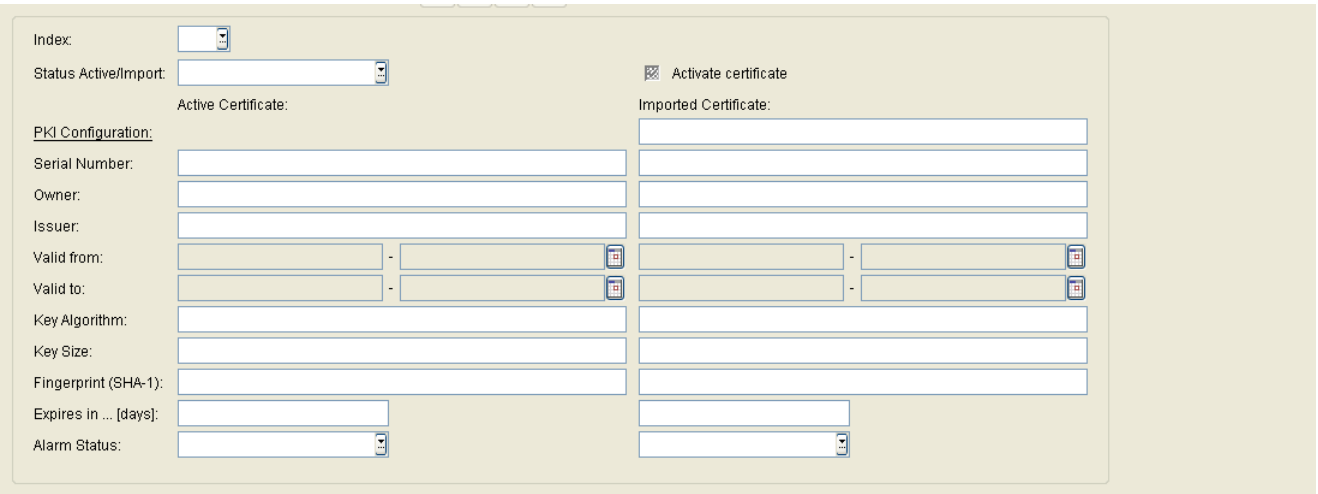
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > Security Settings > "Settings" Tab



No additional security settings are currently required.

7.3.2.2 "WBM Server Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > Security Settings > "WBM Server Certificates" Tab



Index

Indec number for the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key Algorithm.

Key Size

Key Size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

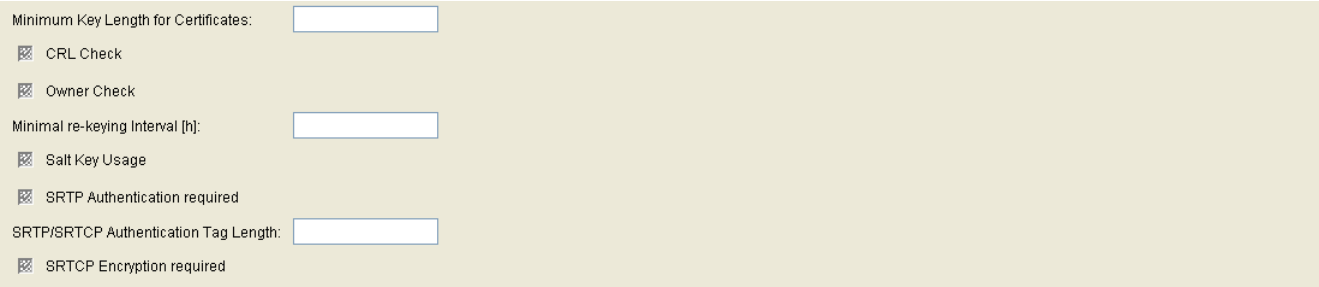
7.3.3 Signaling and Payload Encryption (SPE)

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "SPE Certificate" Tab
- "SPE CA Certificates" Tab
- "CRL Distribution Points" Tab

7.3.3.1 "Settings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "Settings" Tab



Minimum Key Length for Certificates

Minimum key length for certificates.

CRL Check

If this checkbox is activated, the Certificate Revocation List (CRL) in which invalid certificates can be entered is verified.

Owner Check

If this checkbox is activated, the owner’s name is verified (Subjectname check).

Maximum re-keying Interval

Maximum re-keying interval in hours.

Salt Key Usage

If this checkbox is activated, salt key usage is necessary.

SRTP Authentication required

If this checkbox is activated, secure RTP authentication is necessary.

SRTP/SRTCP Authentication Tag Length

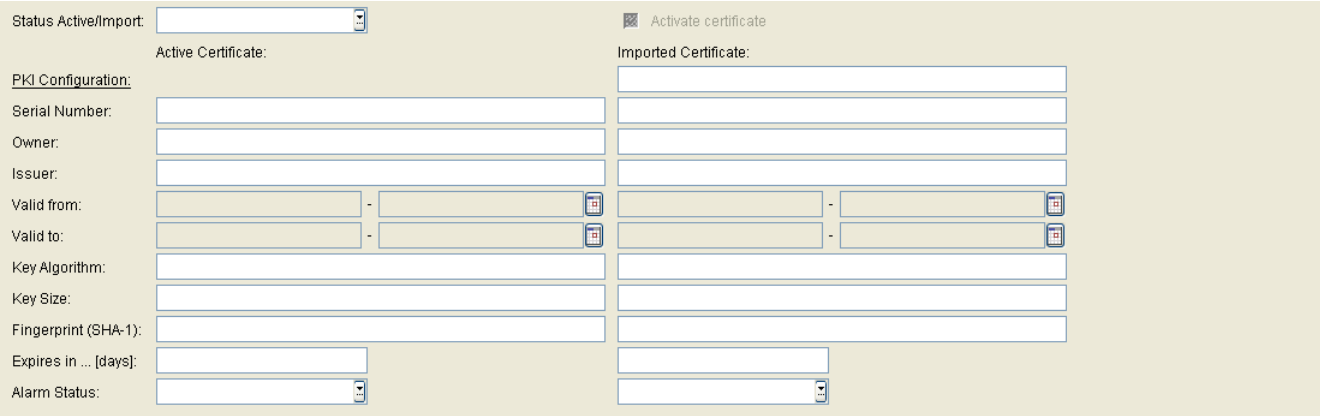
Length of the authentication key.

SRTCP Encryption required

If this checkbox is activated, SRTCP encryption is necessary.

7.3.3.2 "SPE Certificate" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "SPE Certificate" Tab



Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

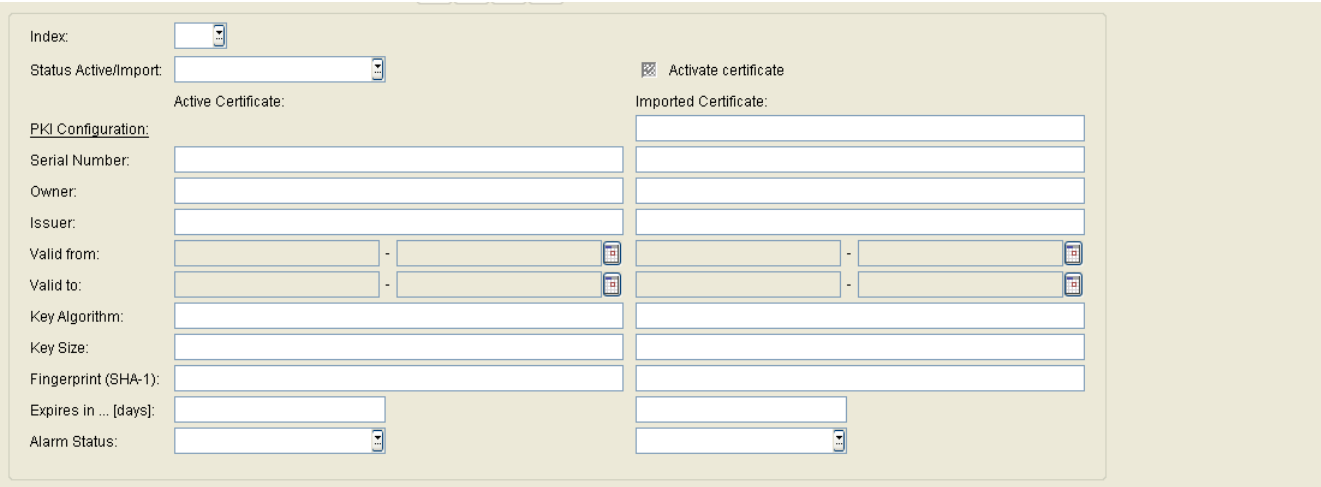
Possible values:

- **valid**
- **soon running out**
- **expired**

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

7.3.3.3 "SPE CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "SPE CA Certificates" Tab



Index

Index for identifying the SPE CA certificates.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

PKI Configuration

Shows PKI configuration of imported certificate.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

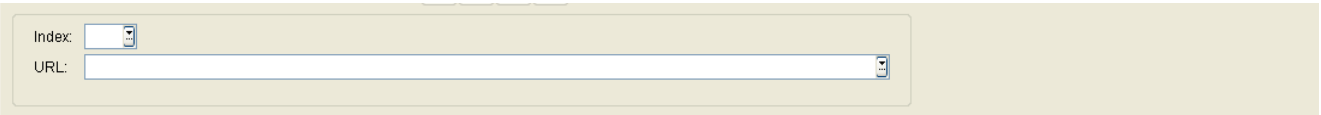
Possible values:

- **valid**
- **soon running out**
- **expired**

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

7.3.3.4 "CRL Distribution Points" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > Signaling and Payload Encryption (SPE) > "CRL Distribution Points" Tab



Index

Index for identifying the CRL distribution points.

URL

URL of the CRL distribution point, for example, http://.... or ldap://...

7.3.4 IPSec/VPN

This area features the following components:

- General Data
- Possible Action Buttons
- "Settings" Tab
- "Peer Credentials" Tab
- "CA Certificates" Tab
- "CRL Files" Tab

7.3.4.1 "Settings" Tab

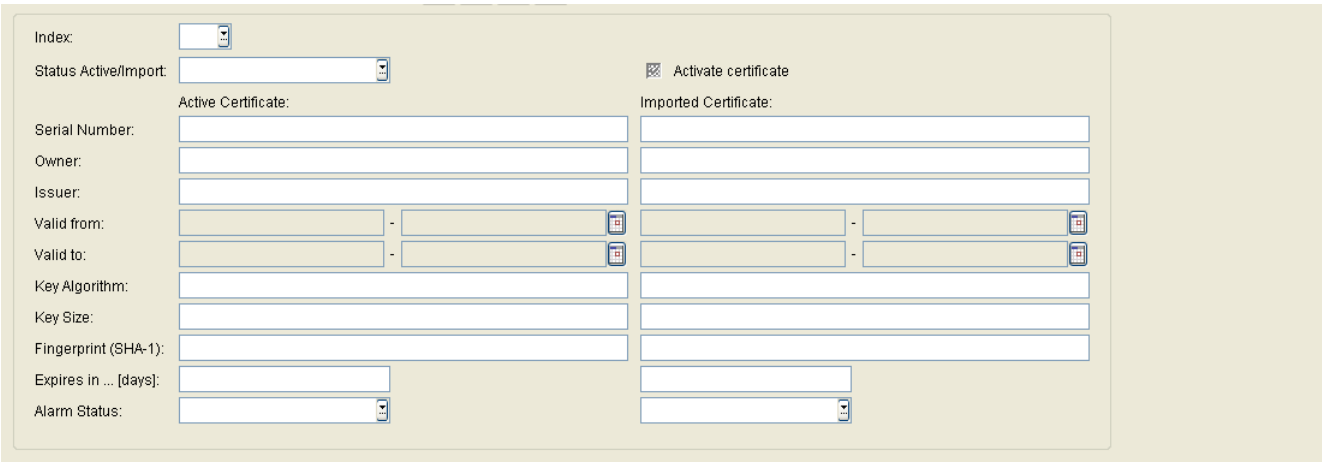
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > IPSec/VPN > "Settings" Tab



No additional IPSec/VPN settings are currently required.

7.3.4.2 "Peer Credentials" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > IPSec/VPN > "Peer Credentials" Tab



Index

Index number for the certificate.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

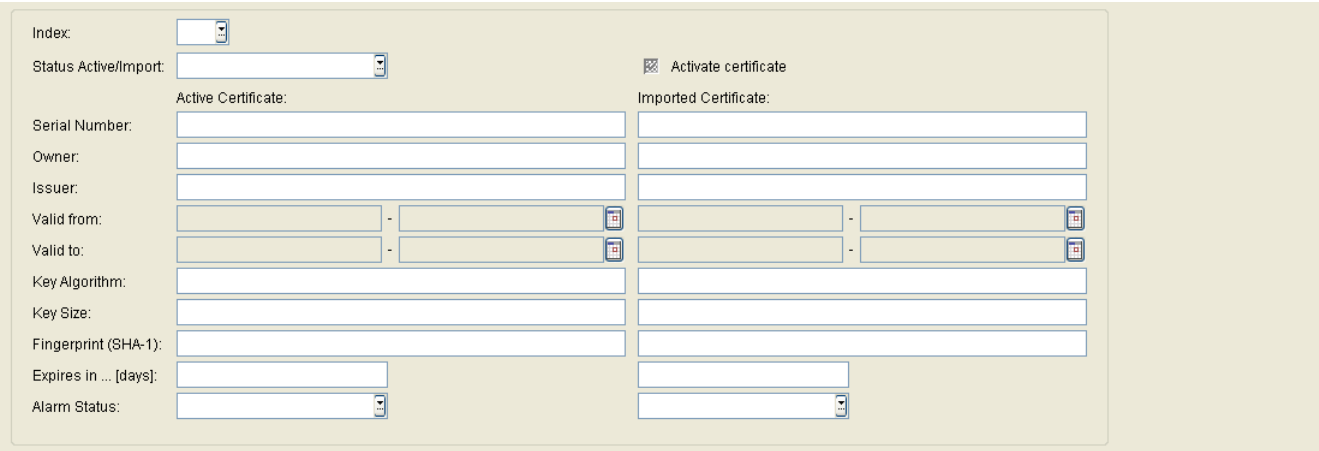
Possible values:

- **valid**
- **soon running out**
- **expired**

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

7.3.4.3 "CA Certificates" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > IPSec/VPN > "CA Certificates" Tab



Index

Index for identifying the CA certificates.

Status Active/Import:

Content is automatically specified after import depending on whether active and/or imported certificates exist and whether these are different or identical.

Possible options:

- **no certificate**
- **different**
- **equal**
- **no active certificate**
- **no imported certificate**

Activate certificate

The imported certificate is automatically activated.

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm SHA-1 (160 bits/20 characters) for the security certificate

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

NOTE: For further information on importing and activating certificates, see Section 16.14, "Security: Administering Certificates".

7.3.4.4 "CRL Files" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Gateway Configuration > IPSec/VPN > "CRL Files" Tab



Index

Index for identifying the CRL files.

CRL Files

Directory path for CRL files.

7.4 Mediatrix Gateway Configuration

Call: Main Menu > Call: Main Menu > Call: Main Menu > > Mediatrix Gateway Configuration

This menu consists of the following area:

- Configuration

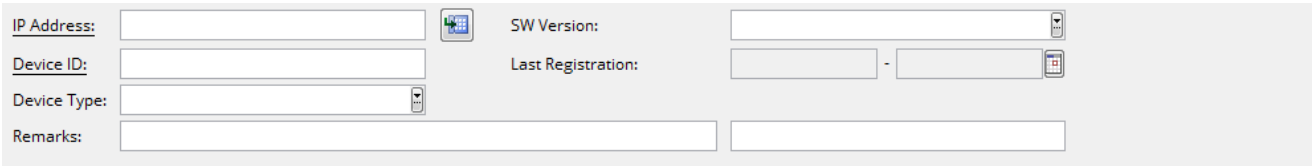
7.4.1 Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- Configuration
- "Configuration Scripts"Tab

General Data

Call: Main Menu > Call: Main Menu > Call: Main Menu > > Mediatrix Gateway Configuration > Configuration > General Data



This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP gateways. The base data associated with the IP gateways found is displayed in **Object** view.

The value displayed in the **Remarks** fields can be changed (all other fields are read-only).

IP Address:

IP address of the IP gateway.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID

ID that uniquely identifies this IP gateway.

Device Type:

IP gateway device type.

You can view all IP devices supported by the DLS in Section 3.4, "Area of Application".

Example: **Mediatrix S7**

SW Version:

Software version of the IP gateway.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

Last Registration:

Last time the IP gateway logged on to the DLS.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP gateways that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.7, "Editing Templates".

Discard

Discards any changes made and new entries.

Read

The parameters displayed on the new mask are read in again by the IP device.

Rename

Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

Import Certificate

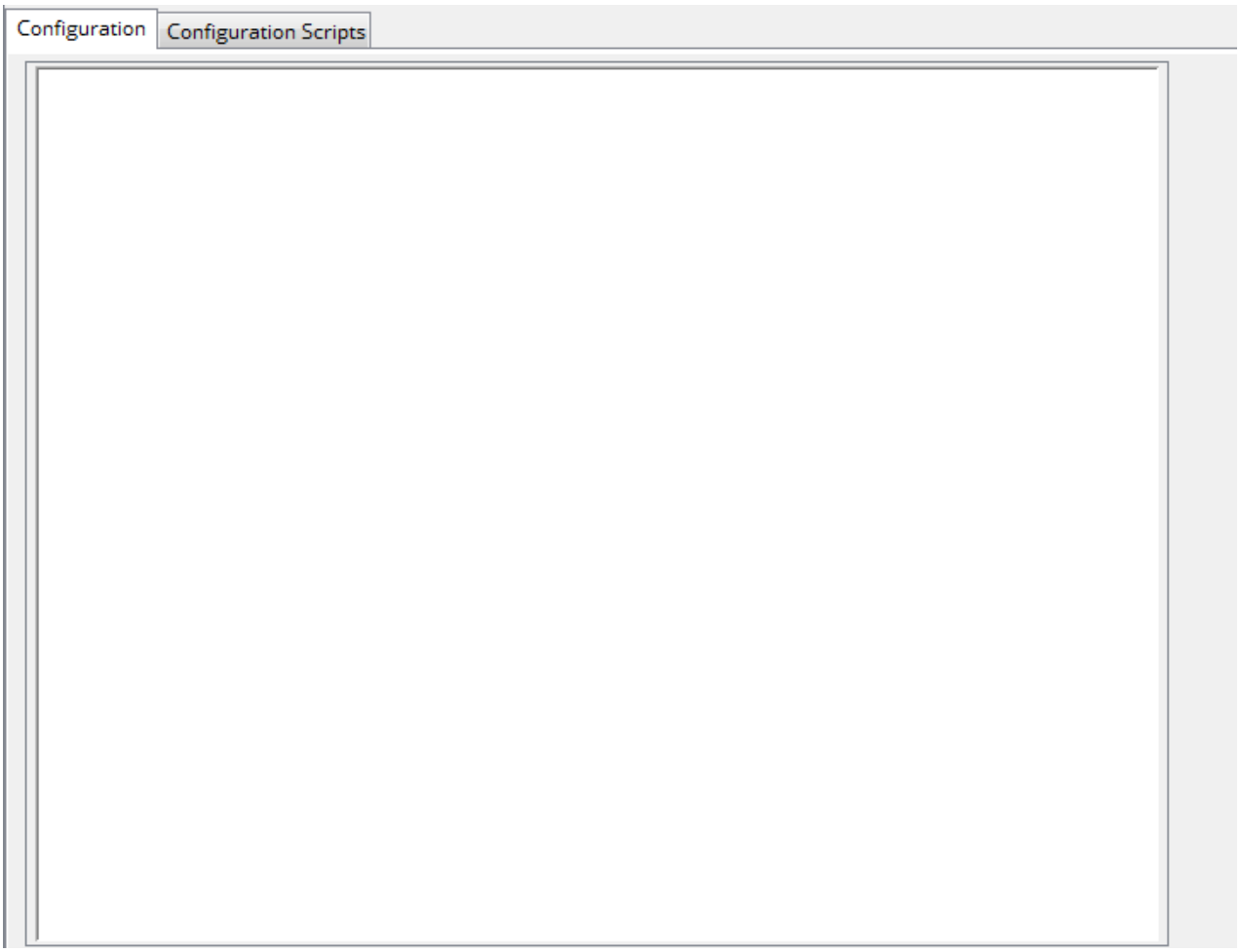
Imports a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.14, "Security: Administering Certificates".

Remove Certificate

Deletes a certificate for the selected IP device (only available in Certificate Management). For more information, see Section 16.14, "Security: Administering Certificates".

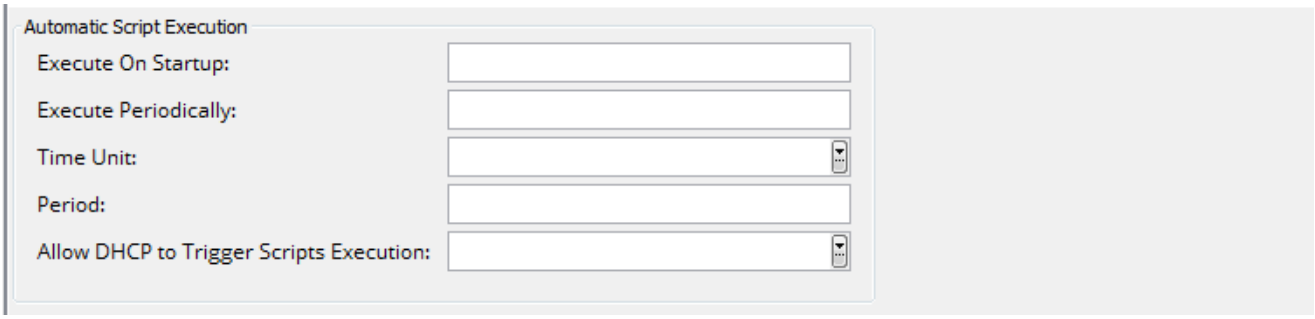
7.4.1.1 "Configuration"Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > Mediatrix Gateway Configuration> "Configuration"Tab



7.4.1.2 "Configuration Scripts"Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > Mediatrix Gateway Configuration> "Configuration Scripts"Tab



The auto-provisioning feature on the Mediatrix units can fetch two types of files:

- **Generic configuration script**
  For the auto-provisioning via DLS, generic configuration script has to be used using the MAC address macro. MAC address will be used as device identifier
- **Specific configuration script**
  The Specific configuration script contains parameters that are specific to each Mediatrix unit (i.e, specific parameters are SIP username and SIP authentication parameters)

It is allowed to configure the mediatrix unit to check for new script periodically. If you have enabled the periodic update, you can configure the frequency.

NOTE: The mediatrix unit with gather any configuration change that has been performed by DLS admin after the initial device registration, at the next periodic check for updates. That means that all jobs will remain in status '**running**' until the next periodic check.

IMPORTANT: For further info on Mediatrix,refer to the corresponding **Unify Experts Wiki** page under:
http://wiki.unify.com/wiki/How_to_setup_Mediatrix

Automatic Script Execution

Execute On Startup:

Execute Periodically:

Time Unit:

Possible values:

- **Hours**
- **Minutes**

Period:

Allow DHCP to Trigger Scripts Execution:

By using DHCP option, it is possible to have the Mediatrix units automatically execute a configuration script. Mediatrix units, by default, send DHCP requests to acquire an IP address.

Possible values:

- **Disable**
- **Enable**

7.5 IP Device Interaction

You can use the **IP Device Interaction** area to transfer data from the IP Device to the DLS and to activate a restart at the IP Devices.

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction

This menu consists of the following submenus:

- Read IP Device Data
- Reset IP Devices
- IP Device Revoke Certificates
- IP Device Response Test
- Ping IP Devices
- Scan IP Devices

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

7.5.1 Read IP Device Data

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Read IP Device Data

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

You can use this function to read out information from the IP Device. Only registered IP Devices will be considered.

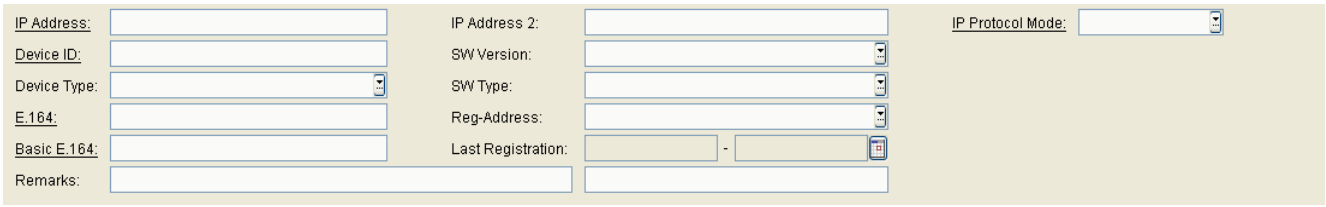
In this case, the data is synchronized between the IP Device and DLS database. The data is read without IP Devices being reset (see Section 7.5.2, "Reset IP Devices"). In other words, no further actions or interventions are performed at the workpoint.

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is identical for the **Read IP Device Data** and **Reset IP Devices** interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP Devices. The base data associated with the IP Devices found is displayed in the **Object** view (no changes possible).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the IP Device. For OpenStage, in IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint device types supported by DLS can be found in Section 3.4, "Area of Application".

Examples: **optiPoint 410 standard**, **optiClient 130**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the IP Device.

Example for IP phones and IP clients: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

Software type used by the IP Device.

Examples: **Unify HFA**, **Unify SIP**.

Reg-Address:

IP address of the gateway or the gatekeeper where the IP Device must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Remarks:

Fields for general informations.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP Device that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Reset IP Device

Restarts/resets the device.

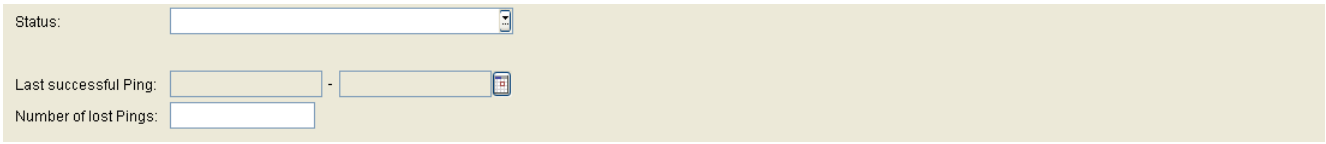
Restore Factory Setting

Restarts/resets the device and restores factory settings. When you press this button, you will be asked to enter the reset password.

Available for OpenStage, optiPoint410, and optiPoint420.

7.5.1.1 "Info" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Read IP Device Data > "Info" Tab



Status:

Possible options:

- **in Service**
  IP phone that is currently in service.
- **license expired**
  IP phone with an expired license.
- **invalid license token**
  Unlicensed IP phone.
- **invalid SW signature**
  IP phone with an invalid software signature.

Last successful Ping

Displays the last successful PING.

The value is read-only.

See also Section 7.5.5, "Ping IP Devices".

Number of lost Pings

Total number of unsuccessful PINGs.

The value is read-only.

See also Section 7.5.5, "Ping IP Devices".

7.5.2 Reset IP Devices

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Reset IP Devices

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

You can perform a reboot, a factory reset, and revoke all PSE-certificates used by this IP Device. No CA certificates will be revoked.

For information on general interface operation, see Section 5.4.2, "Work Area".

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

IP Device Revoke Certificates

When clicking the button, a window pops up to select the certificates to revoke.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Reset IP Device

Restarts/resets the device.

Restore Factory Setting

Restarts/resets the device and restores factory settings. When you press this button, a window pops up where you will be asked to:

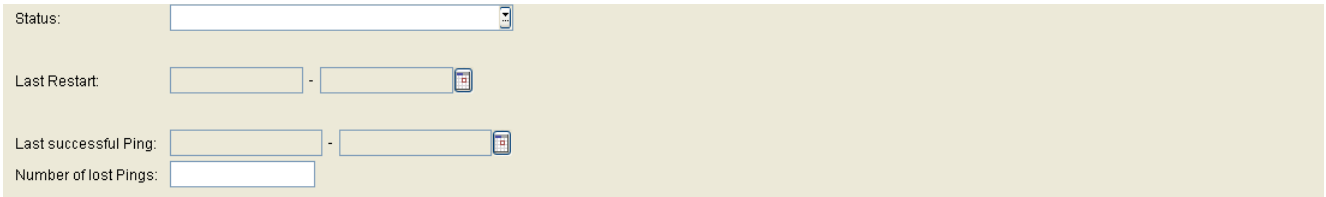
- enter the reset password.
- select the option **Revoke all Certificates** or not**.**

IMPORTANT: No CA certificates will be revoked.

Available for OpenStage, optiPoint410, and optiPoint420.

7.5.2.1 "Info" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Reset IP Devices > "Info" Tab



Status:

IP phone status.

Possible options:

- **in Service**
  IP phone that is currently in service.
- **license expired**
  IP phone with an expired license.
- **invalid license token**
  Unlicensed IP phone.
- **invalid SW signature**
  IP phone with an invalid software signature.

Last Restart:

Displays date/time of last restart.

Last successful Ping

Displays the last successful PING.

The value is read-only.

See also Section 7.5.5, "Ping IP Devices".

Number of lost Pings

Total number of unsuccessful PINGs.

The value is read-only.

See also Section 7.5.5, "Ping IP Devices".

7.5.3 IP Device Revoke Certificates

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > IP Device Revoke Certificates

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

Possible Action Buttons

IP Device Revoke Certificates

When clicking the button, a window pops up to select the certificates to revoke.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, Section 15.3, "First Steps: Changing IP Device Parameters".

Discard

The modifications carried out in the mask are discarded.

Refresh

Updates the window using the database.

7.5.3.1 "Info" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > IP Device Revoke Certificates > "Info" Tab



State

Shows the state of the certificate.

Possible Options:

- **in Service**
- **license expired**
- **invalid license token**
- **invalid SW signature**

7.5.4 IP Device Response Test

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > IP Device Response Test

With this function, not responding IP Devices can be moved to trash automatically. Not responding IP Devices are determined by the ping mechanism. When the count defined in **Maximum Number of lost Pings** is exceeded, the IP Device will be moved to trash. IP Devices in trash will not be pinged any more. They can be either recovered, or deleted manually or automatically.

When an IP Device residing in trash registers again, it will be recovered automatically

This function is available for IP Phones (optiPoint, OpenStage, WLAN phones), but not for IP Clients and IP Gateways.

For further information, please see chapter Section 7.6.2, "Trash".

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

Possible Action Buttons

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, Section 15.3, "First Steps: Changing IP Device Parameters".

Discard

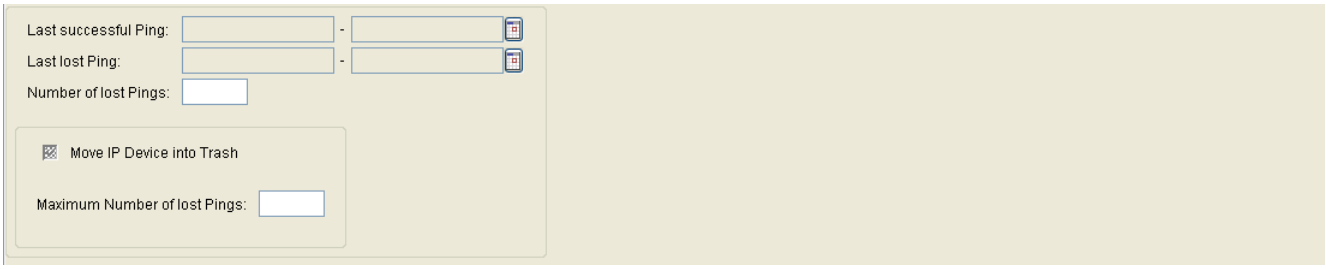
The modifications carried out in the mask are discarded.

Refresh

Updates the window using the database.

7.5.4.1 "Info" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > IP Device Response Test > "Info" Tab



Last successful Ping

Shows date and time of the last successful ping.

Last lost Ping

Shows date and time of the last lost ping.

Number of lost Pings

Shows the total number of lost pings.

Move IP Device into Trash

If checked, the IP Device will be moved into trash when exceeding the **Maximum Number of lost Pings**.

> ***NOTE:*** The **Move IP Device into Trash** checkbox is grayed out in the case of DCMP-enabled devices.

Maximum Number of lost Pings

When exceeding this count, the IP Device will be moved into the trash. These IP Devices will not be pinged any more. They can be either recovered or deleted.

For further information, see chapter Section 7.6.2, "Trash".

> ***NOTE:*** The **Maximum Number of lost Pings** checkbox is grayed out in the case of DCMP-enabled devices.

7.5.5 Ping IP Devices

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Ping IP Devices

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Phones" Tab
- "IP Clients" Tab
- "IP Gateways" Tab

This function enables you to use PINGs to check IP Device response, in other words , to check if they are still contactable.

The following DLS areas contain information on successful or unsuccessful pings:

- Call: Main Menu > Call: Main Menu > > IP Device Management > Inventory Data > "Pings" Tab
- IP Device Interaction > Read IP Device Data > "Info" Tab
- IP Device Interaction > Reset IP Devices > "Info" Tab

General Data



Enable IP Device Pings

Checkbox for activating IP device PING settings.

Possible Action Buttons

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

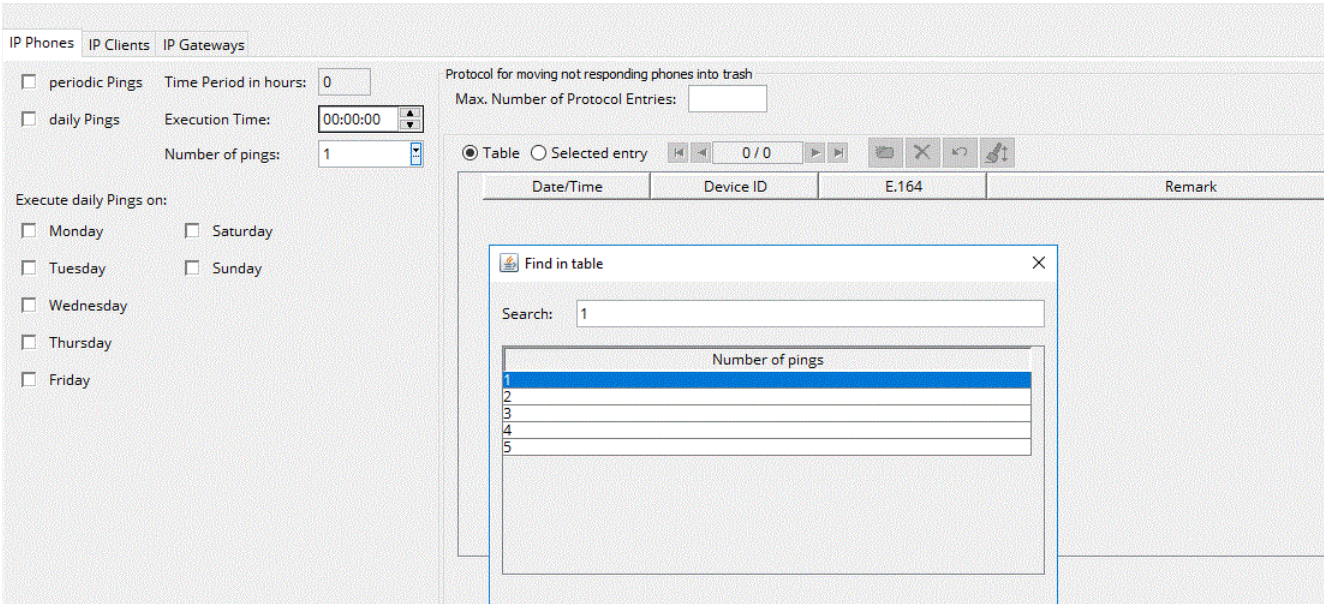
Refresh

Refreshes the content of the relevant page.

7.5.5.1 "IP Phones" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Ping IP Devices > "IP Phones" Tab

You can define the chronological order of PING requests for IP phones in this tab.



periodic Pings

Checkbox for activating periodic PINGs.

Time Period in hours

Time between two periodic pings. Only applies if "periodically Pings" is active.

Value range: **1** ... **23** hours.

daily Pings

Checkbox for activating daily pings.

Execution Time:

Time for daily pings (for a calendar, see Section 5.4.2.4, "Content Area").

Only applies if "daily Pings" is active.

Number of pings:

DLS, by default, sends one ping at a time.

With this configuration you can set the maximum number of pings that DLS will execute before marking the attempt as failed.

You can select **Number of pings** to be between 1 to 5.

Execute daily Pings on:

This function enables you to restrict pings to individual weekdays.

Options available (several options possible):

- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**
- **Sunday**

Only applies if "daily Pings" is active.

Protocol of moving not responding phones into trash

Max. Number of Protocol Entries

Maximum number of protocol entries.

Date/Time

Date/Time at which the action has started.

Device ID

Device ID of the IP Device.

E.164

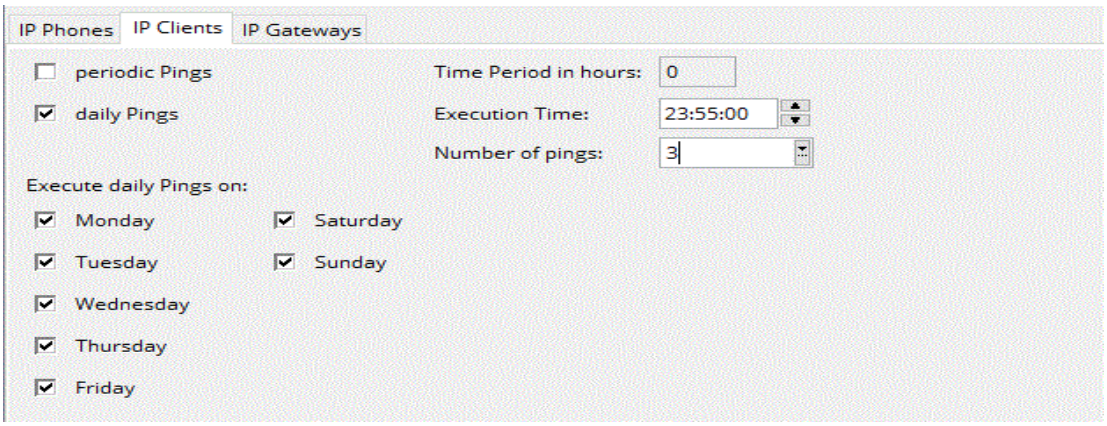
E.164 number of the IP Device.

Remark

Remark on the IP Device.

7.5.5.2 "IP Clients" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Ping IP Devices > "IP Clients" Tab

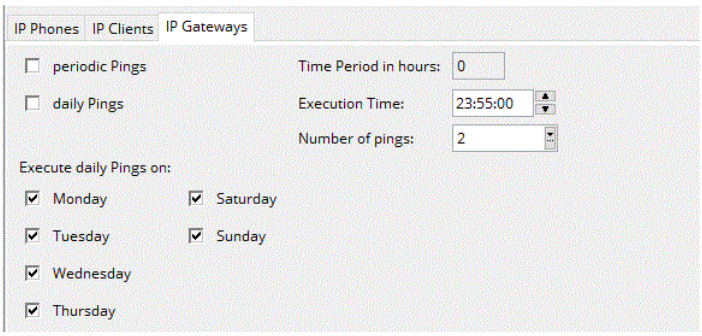


You can define the chronological order of PING requests for IP clients in this tab.

For a description of the interface, see Section 7.5.5.1, ""IP Phones" Tab".

7.5.5.3 "IP Gateways" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Ping IP Devices > "IP Gateways" Tab



You can define the chronological order of PING requests for IP clients in this tab.

For a description of the interface, see Section 7.5.5.1, ""IP Phones" Tab".

7.5.6 Scan IP Devices

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Scan IP Devices

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Ranges" Tab
- "Configuration" Tab
- "Scan Results" Tab

This function lets a DLS user with an TAP, for example, create a DLS database of all IP Devices in the network for processing purposes.

During a scan, the DLS sends a ContactMe request consisting of a short HTML message to every IP address in the specified range. The DLS then waits to see if the relevant device sends a callback. If the ICMP ping is activated for the scan (see "Configuration" Tab), an ICMP ping is sent before a ContactMe request to find out if the IP address is assigned to a device.

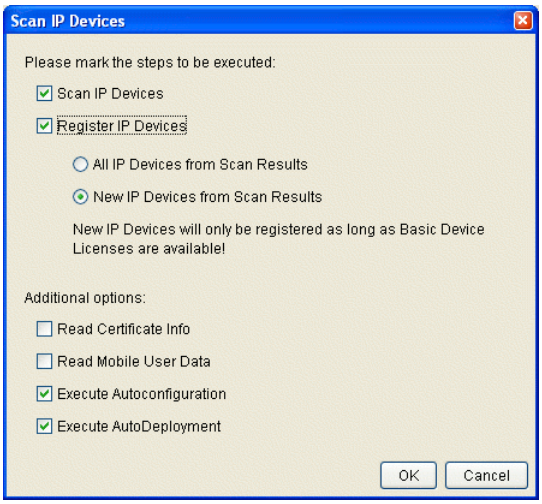
Configuring an IP scanner

If you have not done so already, you must now create an IP scanner, that is, a configuration that indicates the IP areas to be scanned and how the scan should proceed. To do this, proceed as follows:

1. Create a new IP scanner by clicking **New**.
2. Enter a name and a description for the IP scanner in the General Data area.
3. Enter the address range that should be scanned and the port where the devices can be reached for the DLS in the **"IP Ranges" Tab** area.
4. If necessary, specify additional parameters in **"Configuration" Tab**.

Start scanning

A selection window is displayed when you click **Scan IP Devices**:



The administrator can decide whether the workpoint scan should take place first or at the same time as registration:

- **Scan IP Devices**
  The IP devices are scanned.
- **Register IP Devices**
  The IP devices are registered.

Registration is necessary to record the workpoints in the inventory database.

The whole procedure can also take place in two steps, with scanning as the first step and registration as the second. Registration differentiates between the registration of all scanned IP devices and the registration of only those IP devices that are not yet contained in the inventory database:

- **All IP devices from Scan Results**
  This registers all IP Devices contained in the scan results, including those already registered.
- **New IP Devices from Scan Results**
  Only unregistered IP devices are registered.

If the administrator does not wish to allow all IP devices recognized by the scan to be registered, he or she must delete the corresponding entries from the scan results.

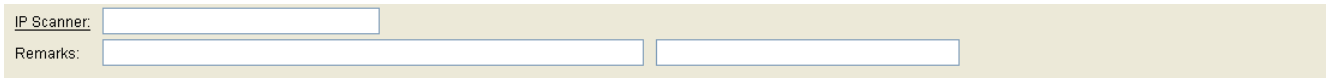
NOTE: If you are using TAP to scan IP devices for the first time at a customer facility, (for example, to record the inventory), ensure that **Perform AutoDeployment** is deactivated using deployment rules. This prevents unwanted deployment in the customer network during operating hours.

If individual devices are not found during the scan, increase the timeout (see **Timeout (sec)**) and run a new scan. If some of the workpoints are still not reached during scanning, a second scan operation is started for the affected IP devices. This takes **at least five minutes**. During this time, the progress bar indicates 99%; the IP devices identified during the first run can now be administered.
An entry is stored in the activity log for every IP device that was not reached during the second scan (see Section 14.1, "Job Control").

NOTE: When scanning IP devices, a valid DLS server address is transferred to the scanned IP device so that the device can contact the DLS server independently later.
This does not happen, however, if the IP device already received a DLS server address from a DHCP server. In this case, the DLS address delivered by the DHCP server is maintained.

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data



IP Scanner:

Name of the IP scanner.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all scanners that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

New

Creates a new IP scanner.

Delete

Deletes one or more IP scanners (multiple selections possible in table view).

Scan Workpoints

Starts the IP scanner displayed in **Object** view.

Refresh

Refreshes the content of the relevant page.

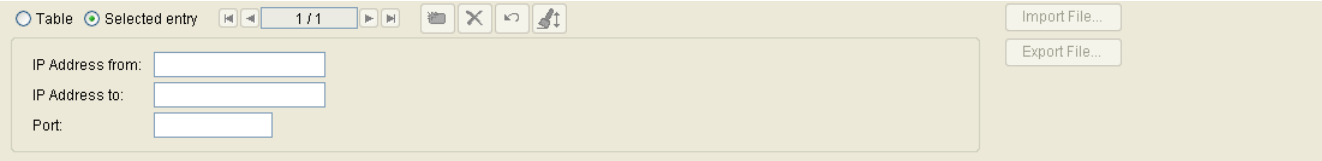
7.5.6.1 "IP Ranges" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Scan IP Devices > "IP Ranges" Tab

Use this tab to specify an IP address range/port number combination for the IP Devices to be scanned. You can add another combination in the **New** and **Object** view with the button and delete it with the button.

In addition, you can import a CSV file containing IP/port combinations and export this data in CSV format.

> ***NOTE:*** To avoid heavy network load, the IP address range should be selected so that where possible only one workpoint is scanned.
>
> If the IP range specified contains other IP clients (not workpoints), malfunctions can sometimes occur at the devices.



IP Address from

IP address for the lower limit of the IP range to be scanned.

Format: **000.000.000.000**, 000 = value between 000 and 255.

IP Address to

IP address for the upper limit of the IP range to be scanned.

Format: **000.000.000.000**, 000 = value between 000 and 255.

> ***NOTE:*** The **IP Address from** and **IP Address to** appropriate value pair has to be identical. Administrators are able to configure not only IP adresses,but DNS names as well.

Port

Port number for the IP addresses to be scanned.

The following default ports are used by the various workpoint types and should be entered here:

- IP phone: **8085**
- IP Gateways: **8084**
- IP client: **8082**

- WLAN phone: **80**

Format: Up to five digits.

Import File...

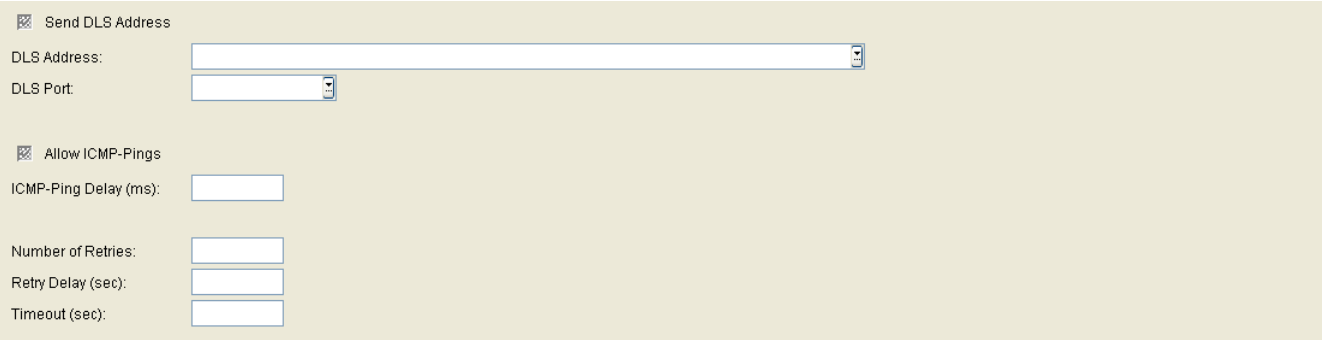
Loads a file in CSV format with existing IP ranges and port numbers into the IP range table.

Export File...

Saves the IP ranges and port numbers from the IP range table to a file in CSV format.

7.5.6.2 "Configuration" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Scan IP Devices > "Configuration" Tab



Send DLS Address

Use the DLS on an TAP to activate the **Send DLS Address** checkbox and identify the DLS address and the DLS port number on the EWS. During scanning, the workpoints are informed of the address data of the DLS that serves them.

NOTE: The Send DLS Address option must not be used if there is a permanent DLS server in the network.

DLS Address:S

IP address of the DLS server on the EWS.

Format: **000.000.000.000** (000 = value between 000 and 255).

DLS Port:

Port number of the DLS server on the EWS.

Value range: Up to five digits.

Allow ICMP-Pings:

If the checkbox is activated, ICMP pings are used when scanning. This speeds up IP device scans because ContactMe requests are only sent to IP addresses where the ICMP ping was successful.

NOTE: This checkbox must be deactivated if the network does not support ICMP pings as otherwise the IP device scan is unable to deliver a result.

ICMP-Delay (ms):

Interval between ICMP pings to ensure that the ICMP pings are not blocked by the operating system.

Number of Retries:

Maximum number of retries for a scan. The value is evaluated for each IP address.

Default: **1**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries. The value is evaluated for each IP address.

Default: **10**

Timeout (sec)

The maximum amount of time that may elapse between a Contact-Me request from the DLS and registration of the IP Devices involved.

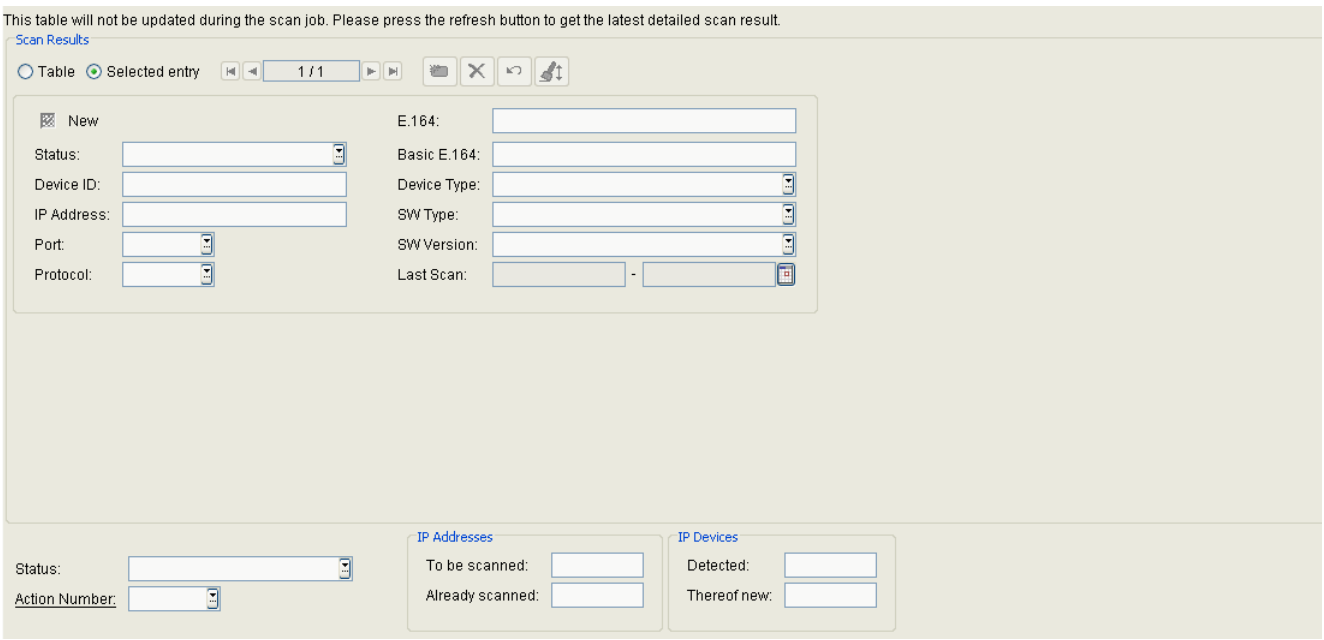
The entered value must be greater than the value Section 6.9.2, ""DCMP" Tab"

Possible Options:

0 - 3600, default: **60** seconds

7.5.6.3 "Scan Results" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Interaction > Scan IP Devices > "Scan Results" Tab



New

An IP Device that is reregistered during a scan is indicated by a checkmark.

Status

Displays the status of the scan for each individual IP Device.

Possible values:

- **running**
- **confirmed**
- **finished**
- **failed**

Device ID

Displays the device ID of the scanned IP Device. This is used for unique identification of the IP device. In IP phones, this is generally identical to the MAC address.

IP Address

Displays the IP address of the scanned IP Device.

Port

Displays the port that the scanned IP Device uses to communicate with the DLS.

Protocol

Displays the protocol that the scanned IP Device uses to communicate with the DLS.

E.164

Displays the E.164 number of the scanned IP Device.

Basic E.164

Displays the basic E.164 number of the scanned IP Device.

Device Type

Displays the phone type of the scanned IP Device.

Example: **optiPoint 410 advance**

Software Type:

Displays the software type of the scanned IP Device.

Example: **Unify HFA**, **Unify SIP**.

SW Version

Displays the software version installed on the scanned IP Device.

Example: **6.0.53**

Last Scan

Displays the data and time of the last scan.

Status:

Displays the current scan status.

Example: **running**, **finished**

Action Number:

Displays the action number for the current scan.

IP Addresses

To be scanned:

Displays how many IP addressed within the IP range are yet to be scanned.

Already scanned:

Displays how many IP addressed within the IP range are already scanned.

Workpoints

Detected:

Displays how many workpoints have been found by the scan.

Thereof new:

Displays how many of the workpoints found by the scan are not yet registered.

7.6 IP Device Management

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management

This menu item consists of the following areas:

- Inventory Data
- Trash
- IP Infrastructure
- IP Device Configuration

7.6.1 Inventory Data

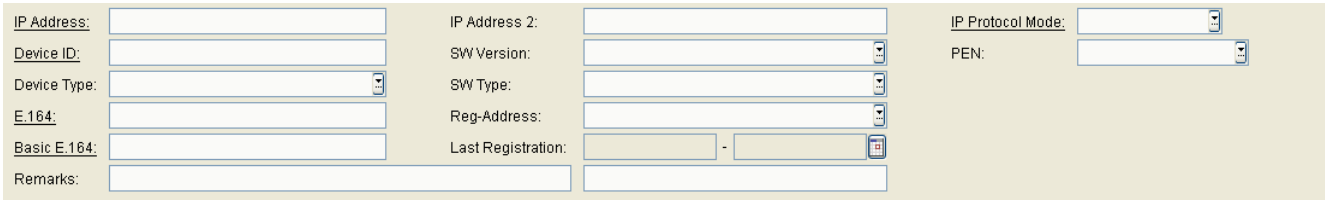
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Inventory Data

This area features the following components:

- General Data
- Possible Action Buttons
- "Inventory Data" Tab
- "Information" Tab
- "Accounting" Tab
- "Pings" Tab

General Data

This part of the content area is used for entering parameters in **Search** view to find a specific group of workpoints. The base data associated with the workpoints found is displayed in the **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the workpoint. For OpenStage, in IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the workpoint.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

Software type used by the workpoint.

Examples: **Unify HFA**, **Unify SIP**.

PEN:

Position of the gateway assembly group (plug-in position).

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last workpoint registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, see Section 15.3, "First Steps: Changing IP Device Parameters".

Discard

The modifications carried out in the mask are discarded.

Export File

The inventory data are exported into a csv formatted file.

Refresh

Refreshes the window contents from the database.

Clear Trash

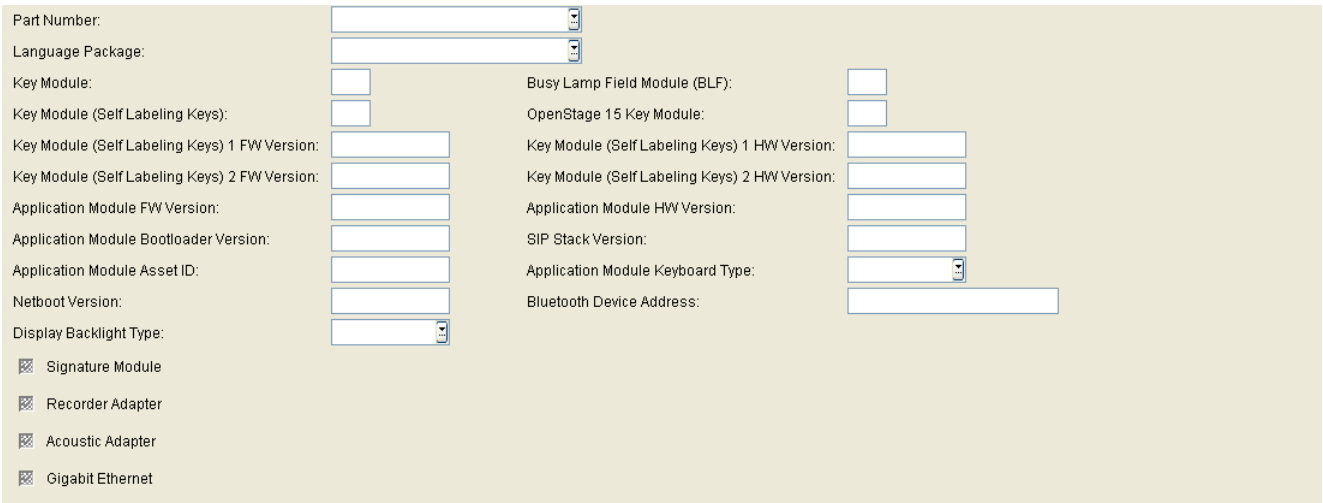
Deletes completely all IP Devices marked to be deleted from the DLS.

Restore IP Device

Moves IP Device out of trash. Afterwards the IP Phone can be administered by DLS.

7.6.1.1 "Inventory Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Inventory Data > "Inventory Data" Tab



Part Number:

Part number of the workpoint; this number identifies the relevant hardware.

The value is read-only.

Language Package:

Name of installed Language Package.

The value is read-only.

Key Module:

Number of Self Labeling Keys Modules connected.

The value is read-only.

Key Module (Self Labeling Keys):

Number of Self Labeling Keys Modules connected.

The value is read-only.

Key Module (Self Labeling Keys) 1 FW Version:

Firmware version of the first Self Labeling Keys Module.

The value is read-only.

Key Module (Self Labeling Keys) 2 FW Version:

Firmware version of the second Self Labeling Keys Module.

The value is read-only.

Application Module FW Version:

Firmware version of the optiPoint Application Module.

The value is read-only.

Application Module Bootloader Version:

Bootloader version of the optiPoint Application Module.

The value is read-only.

Application Module Asset ID:

You can use the asset ID for the unique identification of an optiPoint Application Module.

Coding:

Byte 1	Byte 2	Byte 3	Byte 4
yyyywwww	wwdddlll	aasssss	ssssttt

Definition:

Section	Length	Meaning	Example
yyyy	4 bits	Last digit of the year	0001 = 2001
w...w	6 bits	Calendar week	000001 = Week 1
ddd	3 bits	Day	001 = Monday, 111 = Sunday
lll	3 bits	Design Line	000 = Unify, else : reserved
aa	2 bits	Tester Group	0 - 3, factory setting
s...s	11 bits	Serial Number	0 ... 2047
ttt	3 bits	Tester Number	0.1 ... 6.7

The value is read-only.

Netboot Version:

Version of Netboot.

The value is read-only.

Display Backlight Type

Shows the backlight type of display.

Possible options:

- **None**
- **CCFL**
- **LED**

Signature module

Active when an optiPoint signature module is connected.

The value is read-only.

Recorder Adapter

Active when an optiPoint recorder module is connected.

The value is read-only.

Acoustic Adapter

Active when an optiPoint acoustic module is connected.

The value is read-only.

Gigabit Ethernet

Indicates whether the device has a gigabit LAN interface.

Busy Lamp Field Module (BLF):

Display showing the BLFs connected.

The value is read-only.

OpenStage 15 Key Module:

Hardware version of the OpenStage 15 Key Module.

Key Module 1 HW Version:

Hardware version of the first Self Labeling Key module.

The value is read-only.

Key Module 2 HW Version:

Hardware version of the second Self Labeling Key module.

The value is read-only.

Application Module HW Version:

Hardware version of the optiPoint Application Module.

The value is read-only.

SIP Stack Version:

Version of the SIP stack.

The value is read-only.

Application Module Keyboard Type:

Keyboard layout of the optiPoint application module connected.

Possible options:

- **QWERTZ**
  (German layout)

- **QWERTY**
  (American layout)

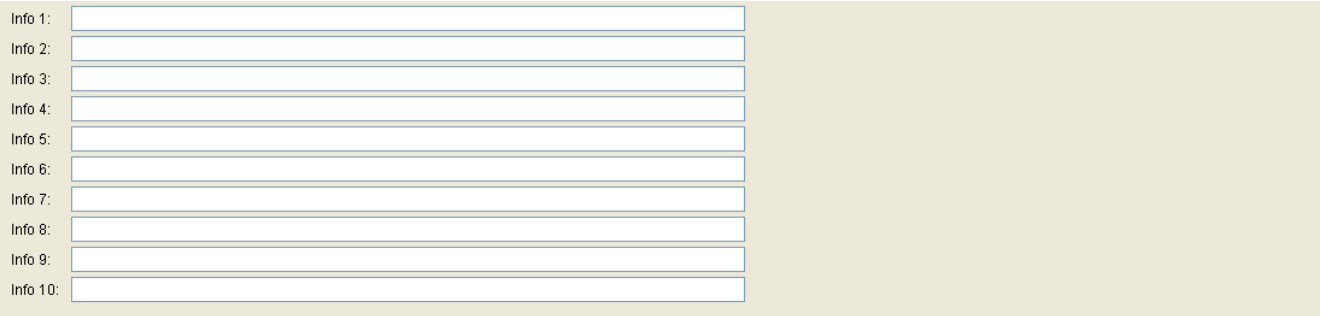
The value is read-only.

Bluetooth Device Address

Bluetooth address of the device.

7.6.1.2 "Information" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Inventory Data > "Information" Tab



Info 1 ... Info 10:

Additional information on the workpoint, such as, billing data, etc., can be saved in these fields. This information is only stored in the DLS database. Administration is not performed at the workpoint.

7.6.1.3 "Accounting" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Inventory Data > "Accounting" Tab



Department:

Defined department of the associated Business Group subscriber.

Accounting ID:

Accounting ID of the subscriber.

Account ID is by default subscriber (Subscriber ID).

Retailer ID:

Retailer ID of the subscriber.

Retailer ID is by default subscriber (Subscriber ID).

Billing ID:

Billing ID of the subscriber.

Billing ID is by default subscriber (Subscriber ID).

7.6.1.4 "Pings" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Inventory Data > "Pings" Tab



For information on PING, see Section 7.5.5, "Ping IP Devices".

Last successful Ping

Displays the last successful PING.

The value is read-only.

Number of lost Pings

Total number of unsuccessful PINGs.

The value is read-only.

7.6.2 Trash

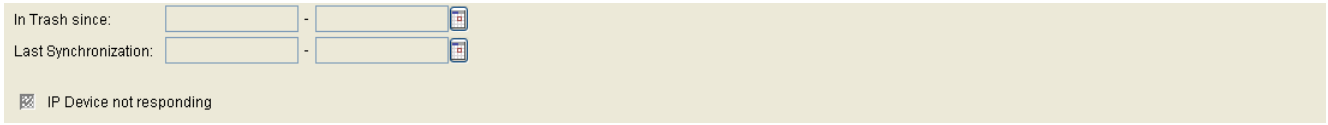
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Trash

This area features the following components:

- General Data
- Possible Action Buttons
- "Information" Tab

7.6.2.1 "Information" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > Trash > "Information" Tab



In Trash since:

Date at which the IP Device has been put into trash.

Last Synchronization:

Date of last element manager synchronization for this E.164 number.

IP Device not responding

Switch is set if IP Device is in trash because of not responding PING requests.

7.6.3 IP Infrastructure

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Infrastructure

In this screen, the administrator can view the IP infrastructure data sent by an application to the DLS. The infrastructure policy is used for automatic adaptation: A default device profile is searched to which that location is assigned for which this infrastructure policy is defined. This profile will be applied to the IP Phone.

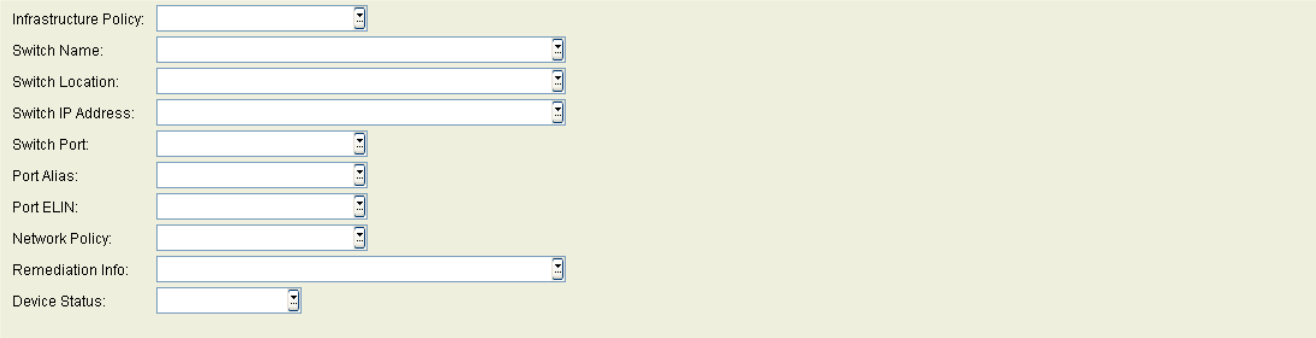
The infrastructure policy is not part of the API interface, though it will be mapped from the switch IP address, the switch port and the Network Policy. The mapping has to be configured by the administrator in the screen **Administration** > **Server Configuration** > **Infrastructure Policy**.

This area features the following components:

- General Data
- Possible Action Buttons
- "IP Switch Data" Tab

7.6.3.1 "IP Switch Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Infrastructure > "IP Switch Data" Tab



Infrastructure Policy:

Currently enabled policy, mapped from **Switch IP Address**, **Switch Port** and **Network Policy**.

Switch Name

Name of the edge switch device is currently plugged in.

Switch Location

Location of the edge switch device is currently plugged in.

Switch IP Address

IP address of the edge switch device is currently plugged in

Switch Port

Port of the edge switch device is currently plugged in.

Port Alias

Port Alias

Port ELIN

Port ELIN

Network Policy

Currently enabled network policy for this device.

Remediation Info

Long description of Network Policy.

Device Status

Connection status of device

Possible options:

- **plugged in**
- **plugged off**
- **unknown**

7.6.4 IP Device Configuration

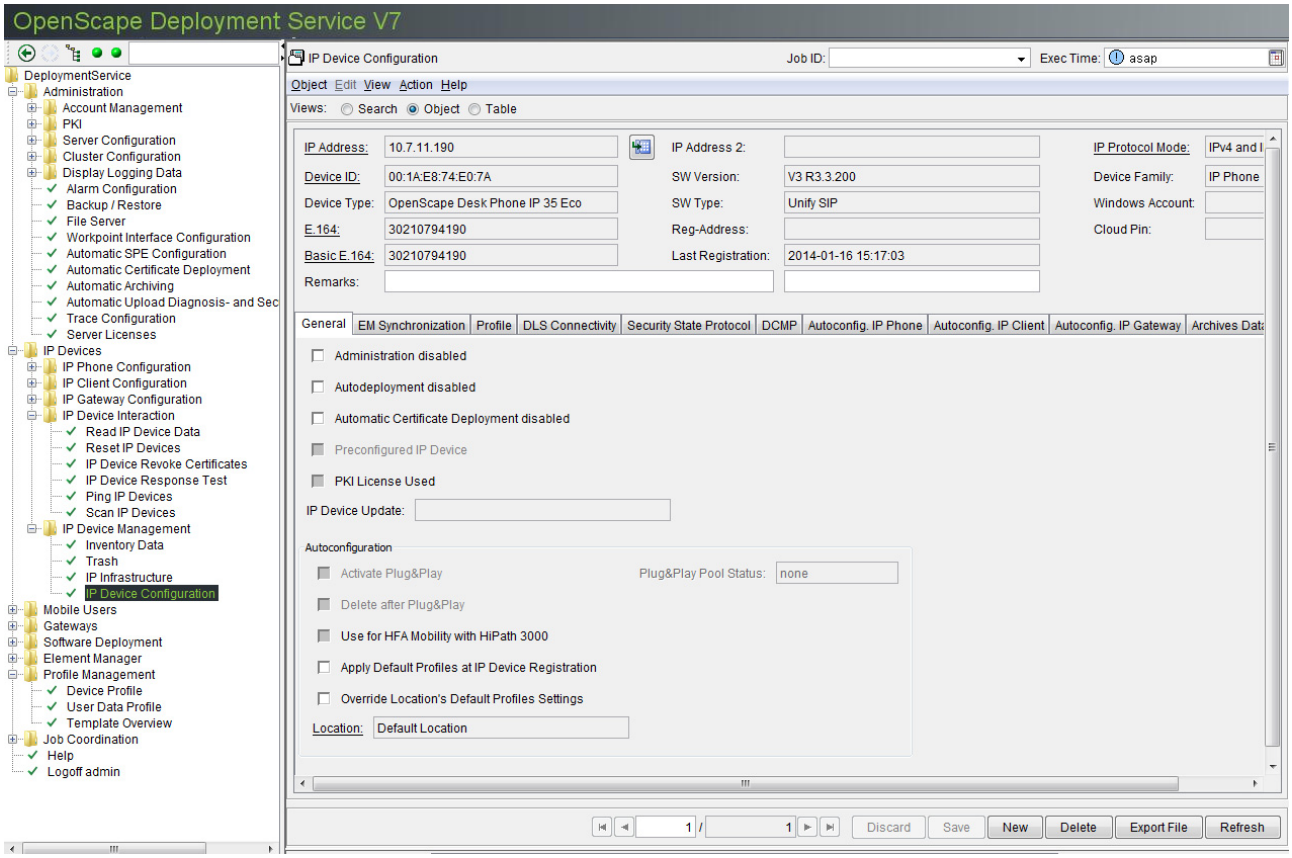
Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration

This area features the following components:

- General Data
- Possible Action Buttons
- "General" Tab
- "EM Synchronization" Tab
- "Profile" Tab
- "DLS Connectivity" Tab
- "Security State Protocol" Tab
- "DCMP" Tab
- "Autoconfig. IP Phone" Tab
- "Autoconfig. IP Client" Tab
- "Autoconfig. IP Gateway" Tab
- "Archives Data" Tab
- "IP Client Registration History" Tab

General Data

This part of the content area is used for entering parameters in **Search** view to find a specific group of IP Devices. The base data associated with the IP Devices found is displayed in the **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the IP Device.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

NOTE: The **Remote Control** button next to the IP address field launches a new browser window with the URL of the jHPT application and the needed devices specific parameters so that the user is redirected to the HPT page for selected device.For further info on icons beside entry fields please refer to Section 5.4.2.4, "Content Area"

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP Device type.

All IP Device types supported by DLS can be found in Section 3.4, "Area of Application".

Example: **optiPoint 410 standard**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the IP Device.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

Software type used by the IP Devices.

Examples: **Unify HFA**, **Unify SIP**.

Reg-Address:

IP address of the gateway or the gatekeeper where the IP Device must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of the last IP Device registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Content Area".

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Device Family:

Type of device.

Possible options:

- **IP Phone**
- **IP Client**
- **IP Gateway**

Windows Account :

The respective domain \ Windows Account of the client. If the device is a client the field contains a value, else it is void.

Cloud Pin:

The cloud pin string consists only of numeric digits. A redirect code is extracted from the pin entered by the phone user, as part of the cloud deployment process.

The cloud pin is added as a new optional item in all workpoint messages initiating a connection with DLS and is used by DLS for device identification with precedence over the E.164 number. The cloud-pin-value is sent by the phone in SHA-256 hashed format.

> ***NOTE:*** If DLS is unable to configure the phone based on the mac-addr inventory item alone, the DLS will look at cloud-pin-value. If DLS is able to match the client-pin-value unambiguously, it will configure the phone accordingly. This includes writing a new value for the e164 item (if a corresponding e.164-phone number could be determined by DLS). If the cloud-pin value is not included in the inventory items or is empty, the DLS will look at the E.164 inventory item for device identification.

> ***NOTE:*** The value that should be entered in 'Cloud Pin' textbox is the same string assigned to the phone after its factory reset. Cloud Pin contains the redirect code,hence the longer string.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP Devices that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for distributing the configuration changes. For more information, see Section 15.3, "First Steps: Changing IP Device Parameters".

Discard

The modifications carried out in the mask are discarded.

Refresh

Refreshes the window contents from the database.

Reset

Allows clearing of the IP Switch data.

New

Creates a new configuration.

Delete

Deletes the record of the current selected IP Device from DLS database.

Export File

The configuration data are exported into a csv formatted file.

Import File

The configuration data are imported from a csv formatted file. Section 15.14, "Importing and Exporting Plug&Play Data"describes the format.

Copy IP Device

Copy data of an IP Device, see also Section 16.6, "Replacing an IP Device",Section 16.7, "Copy a Registered Device to a Virtual Device" Section 16.9, "Replacing HFA with SIP Software and Vice Versa with Identical Device IDs", and Section 16.14.7, "Replace IP Phone".

Save Selected IP Device to Archive

Selected IP Devices are written into .zip archive.

Load IP Device from Archive

Loads data of IP Devices from .zip archive.

Generate all Templates

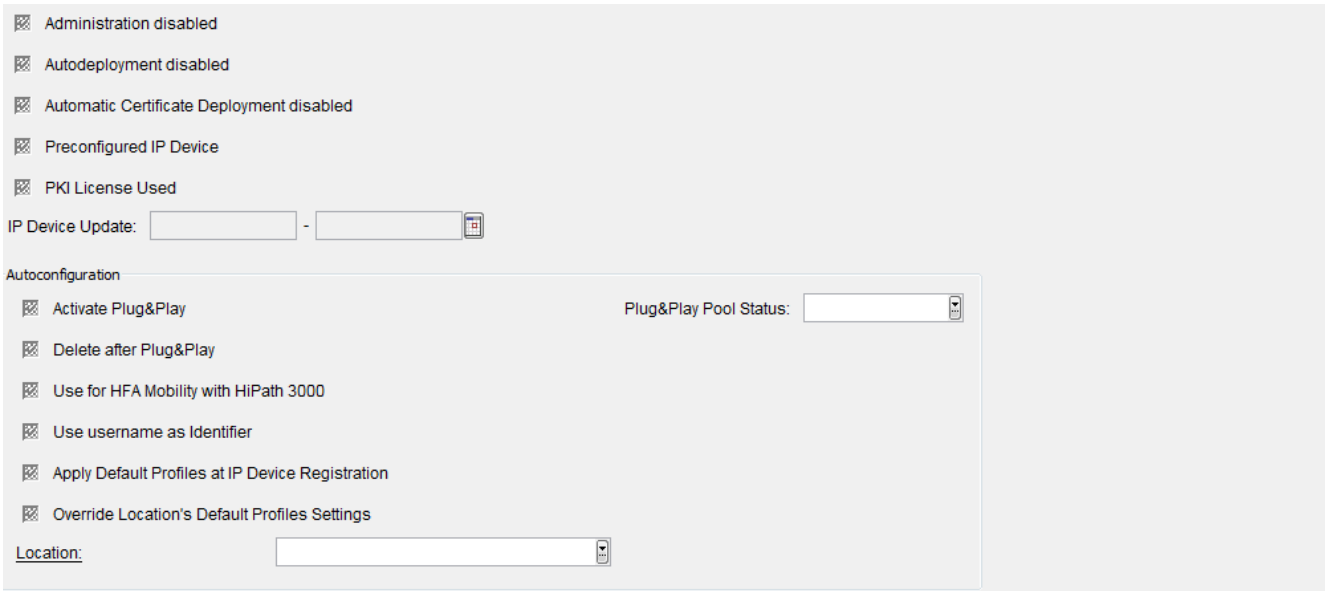
Templates are generated for all objects or masks associated with the selected IP Device type.

Simulate Plug&Play

Test of location and default profile configuration. Location data are entered and after clicking "Simulate Plug&Play", the data sent to the phone which might register with the DLS, can be checked.

7.6.4.1 "General" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "General" Tab



Administration disabled

If this checkbox is activated, IP Device administration via DLS is disabled. This temporary block prevents accidental changes on the IP Device.

Autodeployment disabled

If this checkbox is activated, autodeployment (see Section 15.9.2, "Automatic Deployment") is disabled for the IP Device.

Automatic Certificate Deployment disabled

If this checkbox is activated, automatic deployment of certificates (see Section 6.11, "Automatic Certificate Deployment") is disabled for this IP Device.

Preconfigured IP Device

If this checkbox is automatically activated, the IP device is preconfigured.

PKI License Used

If this checkbox is activated, a PKI license is used by the IP device and a new certificate is issued by a PKI connector which is based on the MS PKI plugin.
If not, the IP device is not in secure mode or the PKI connector used for secure mode is not based on the MS PKI plugin, and also no device interfaces remain associated with a PKI connector based on the MS PKI plugin.

This checkbox facilitates the counting of PKI licenses on an IP device basis.

IP Device Update:

Specifies when the last IP Device update was performed.

Autoconfiguration

Activate Plug&Play

If this checkbox is activated, all data in this data record is assigned to the IP Device at the next registration.

Delete after Plug&Play

If this checkbox is activated, the virtual device changes to the real, registered device. The virtual device no longer exists after plug&play. Otherwise, the data record is copied and the virtual device remains.

> ***NOTE:*** Regardless of the case where the virtual device shall be used for the creation of a mobile user, this virtual device will be deleted if this checkbox is activated.

Use for HFA Mobility with HiPath 3000

If active, this data record will be used in order to provide gateway registration data for HFA mobility with HiPath 3000.

Use username as Identifier

This item is read only and will be checked only for all IP clients that use username as device ID. P&P will always be enabled for these IP clients that use the windows username as device ID (refer to Section 6.3.3, "P&P Settings")

Apply Default Profiles at IP Device Registration

If this checkbox is activated, the default profile defined in **Profile Management** > **Device Profile** for a particular location is identified and used for each registration. (For meaning and configuration of the location, see Section 6.3.2, "Location".)

> ***NOTE:*** The case where the checkbox is activated and an 802.1x certificate is part of a Profile's Template, could lead to a phone reboot loop.It is highly recommended to use the Automatic Certificate Deployment functionality of DLS instead.

Override Location's Default Profiles Settings

If this checkbox is activated, the "Apply Default Profiles at IP Device Registration" is not applicable and shall be grayed out.

This checkbox is disabled by default.

> ***NOTE:*** In order to override the location settings for a specific device this checkbox must be checked.

Location

Current location of the IP Device. The value is set during registration and is displayed only herein. (For meaning and configuration of the location, see Section 6.3.2, "Location".)

Plug&Play Pool Status

Indicates whether this dataset is used for automatic number assignment with Plug&Play.

Possible options:

- **none**
- **free**
- **in use**
- **multiple use**

7.6.4.2 "EM Synchronization" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "EM Synchronization" Tab



Element Manager ID:

ID of the Element Manager assigned to the IP Device.

System Type:

Type of Element Manager assigned to the IP Device.

Possible values:

- **HiPath 4000**
- **HiPath DXWeb Pro**
- **HiPath 3000/5000**
- **Other**
- **OpenScape Voice**
- **Imported**
- **OpenOffice EE**
- **OpenScape Business**
- **OpenScape Office MX/LX**

Switch:

Switch Name (For OpenScape Voice Assistant with Multiple Switch Support only).

Business Group:

Business Group Name (For OpenScape Voice Assistant).

Referenced Element Manager

If an Element Manager is entered here, the data record is only changed at EM synchronization if the data comes from the Element Manager specified here. For more information, see Section 15.4, "Changing the Element Manager Configuration and Creating Jobs".

Last Synchronization:

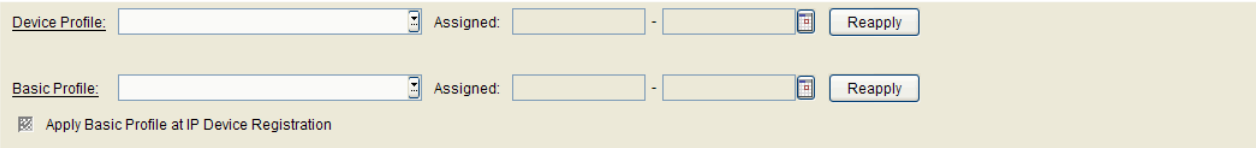
Time of the last synchronization with the system.

Last Update:

Time of the last change to these settings.

7.6.4.3 "Profile" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Profile" Tab



NOTE: "Profile" Tab includes the info of the last deployed Profile. It does not specify nor bounds that subscriber record to the Profile assigned since the profile parameters are a one-time only propagation of data. As such, if an administrator modifies the name (or contents) of a Profile that won't be reflected back in this UI section. Name will still depict the last Profile deployed and not the newly adjustable profile name.

NOTE: Since there is no direct linkage after the initial Profile deployment has taken place, if those fields are used as a search criteria by administrators, it should be first manually validated for any changes in the configuration since new adaptations might not reflect properly anymore. Profile Management of DLS will exclusively notify on the UI if Profile contained data have been altered and those Profiles are already assigned on subscribers that changes won't take immediate effect unless a Profile gets re-applied first.

Device Profile:

Selection of standard device configurations defined in **Profile Management > Device Profile** to be sent to the IP Device. This sets all existing parameters in the profile and any values previously set are overwritten. The parameters that are not replaced by the profile retain their values.

NOTE: When assigning a profile over a Virtual Device under **IP Device Configuration**,the list of offered Profiles is filtered and matched to that of the "Supported Devices of IP Device" Tab for profiles.

Assigned:

Time and date when the device profile was last assigned to the IP Device.

Reapply:

Apply the **Device Profile** to the IP Device again.

Basic Profile:

Selection of a standard user configuration defined in **Profile Management > User Data Profile** to be sent to the IP Device. This resets all parameters. The parameters that are not set by the profile are assigned default values.

Assigned:

Time when the **Basic Profile** was last assigned to the IP Device.

Reapply:

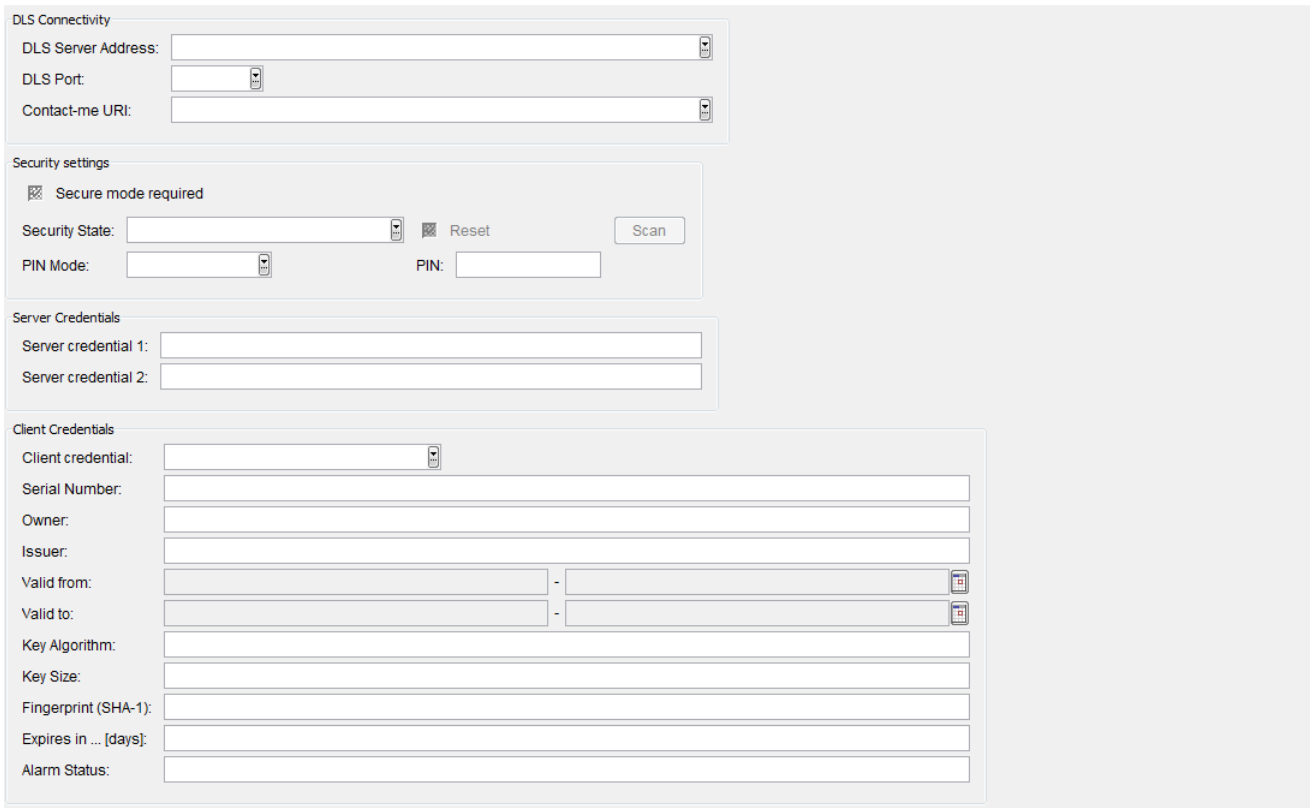
Apply the **Basic Profile** to the IP Device again.

Apply Basic Profile at IP Device Registration

If this checkbox is active, the IP Device is assigned the selected **Basic Profile** at registration.

7.6.4.4 "DLS Connectivity" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "DLS Connectivity" Tab



DLS Connectivity

DLS Server Address:

IP address or host name of the DLS server. This value is automatically entered in the IP Device if a DHCP server is available and appropriately configured (refer tot he **Unify Experts Wiki Portal** under http://wiki.unify.com/wiki/Configuring_the_DHCP_Server_for_DLS

DLS Port:

Port number of the DLS server. This value is automatically entered in the IP Device if a DHCP server is available and appropriately configured (refer to the **Unify Experts Wiki Portal** under http://wiki.unify.com/wiki/Configuring_the_DHCP_Server_for_DLS

Default: **18443**

Contact-me URI:

This field is for display purposes and contains the complete URL used by the IP Device to set up a connection to the DLS.

Security Settings

Secure mode required

If this checkbox is activated, mutual authentication is enabled for the DLS and the IP Device. The authentication process (bootstrap) begins the next time the IP Device registers at the DLS or is scanned.

Security State:

Display the security mode for communication between the DLS and the IP Device.

Possible options:

- **Standard**
  In this mode, the DLS is authenticated using a standard certificate which is the same for all DLS installations.
- **Insecure**
  The previous "Default" mode is considered unsecure once the checkbox "Secure mode required" is activated.
- **Secure**
  This status is displayed once mutual authentication has been carried out between the DLS and the IP Device.
- **Pending**
  The credentials have been transferred to the device, the device has responded but a secure connection between the DLS and the device is not yet complete.
- **Credential transmitted**
  The credentials have been transferred to the device but the device has not yet responded.
- **Credential refused**
  The device rejects secure authentication (for example, because it is not technically ready).
- **Tan failed**
  In standard or individual PIN mode, both the device and the DLS must verify part of the PIN. If the number of failed verification attempts on the DLS side exceeds the threshold set, the security status is set to "Tan failed".
- **Blocked**
  This security status is not currently in use.
- **Go to Default**
  This security state is displayed when the security mode has been changed, but the IP Device does not respond.

PIN Mode:

Possible options:

- **No PIN**
  Access data is sent unencrypted to the IP Device.
- **Default PIN**
  A standard PIN is used for several IP Devices. This is generated automatically by the DLS (see Section 6.9.1, ""Secure mode" Tab").
- **Individual PIN**
  An individual PIN is created for the selected IP Device.
- **Unknown**
  This PIN mode is only available when the DLS interface is in **Search** mode. When moving the DLS to another server, the PIN mode cannot be retrieved. Therefore, the PIN mode is set to "unknown". This has no influence on the functionality.

Reset

If this checkbox is activated, the security mode can be reset to "Insecure" by clicking **Save**. The DLS must then send a new security configuration to the IP Device, that is, the bootstrap operation must be repeated (see also **Secure mode required**).

PIN:

This is entered locally at the IP Device and used to encrypt access data that was sent by the DLS and is required for the transfer to secure mode.The PIN may be preconfigured in the local administration menu.

Scan

Starts the scan for IP Devices (only with Device Family - IP Gateway). In the process of scanning, the Bootstrapping process is executed. Bootstrapping is the process used to raise the interface security between an IP Device and DLS from Default Mode to Secure Mode.

> ***NOTE:*** If you select "Scan" for a device other than IP Gateway (ie. IP Phone or IP Client) the action is finished with error :"1355: Server is not able to create a job: Device is not a IP Gateway".

Server Credentials

Server Credential 1

Fingerprint of trust anchor relative to credential 1, deployed to IP Device and used to authenticate the DLS.

Server Credential 2

Fingerprint of trust anchor relative to credential 2, deployed to IP Device and used to authenticate the DLS.

NOTE: Any DLS that presents either credential 1 or credential 2 is accepted by the IP Device.

Client Credentials

Client Credential

The device uses these credentials to authenticate itself at the DLS.

Possible options:

- **Active**
  The device last authenticated itself using the active client credentials.
- **Old**
  The device last authenticated itself using old client credentials.
- **Unknown**
  In the DLS, it is currently unknown whether the device possesses active, old or invalid client credentials (for example, when new client credentials have been created or client credentials have been imported).
- **Rejected**
  The device last attempted to authenticate itself using invalid client credentials.

Serial Number:

Serial number of the active certificate (display only).

Owner:

Owner of the active certificate (display only).

Issuer:

Issuer of the active certificate (display only).

Valid from:

Start of validity for the active certificate (display only).

Valid to:

End of validity for the active certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]

The certificate validity will expire in the number of days specified.

Alarm Status:

Current alarm status.

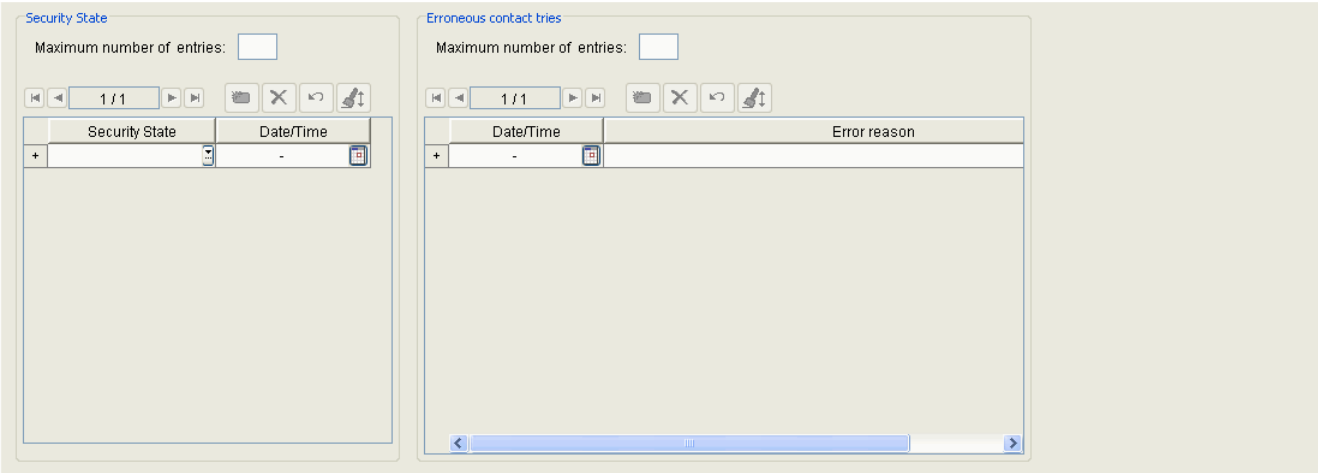
Possible values:

- **valid**
- **soon running out**
- **expired**

7.6.4.5 "Security State Protocol" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Security State Protocol" Tab

Changes to the security mode are logged here for the selected IP Devices.



Security State

Maximum number of entries:

Maximum number of security log entries to be displayed.

Security State

Shows the security state of the IP Device at a given time.

Date/Time

Displays the time at which the IP Device had a particular security state.

Erroneous contact tries

Maximum number of entries:

Maximum number of security log entries to be displayed.

Value range: **0** - **100** for devices in default mode, **1** - **100** for devices in secure mode.

Date/Time

Displays the time of the contact try.

Error reason

Error message.

Possible messages:

Error Message	Description
DLS internal authentication failure (no transition)	During the bootstrapping process, the DLS recognized an unknown sequence of messages (e. g. an unexpected message, deviating from the expected one) and cancelled the contact attempt for security reasons.
Workpoint with given id could not be found.	The IP device is not known to the DLS. Possibly an internal DLS error (database or configuration problem).
Encountered invalid PIN	The bootstrapping PIN contains illegal characters or exceeds the defined length.
TAN Verification can only be performed if TAN is required.	The IP Device has sent a TAN, but the current configuration does not require one, thus the TAN cannot be verified.
Verification of DlsObjWorkpointBase failed.	Internal DLS error.
Error while updating DlsObjWorkpointBase.	Internal DLS error.
Invalid security state.	The message traffic does not conform to the current DLS security state (e. g. wrong sequence of messages, modified configuration or error).
Invalid security transition.	The message traffic does not conform to the current DLS security state (e. g. wrong sequence of messages, modified configuration or error).
Error while generating new client certificate.	Internal DLS error during the creation and distribution of e new client certificate.
Fatal server error. See log file for additional information.	Fatal internal DLS error. **Troubleshooting:** For further information, see `..\DeploymentService\Tomcat\webapps\DeploymentService\log\dlslog.txt`
An active dls server ca could not be found.	Internal DLS error because of a missing CA certificate.
Active server ca is corrupt.	Internal DLS error because of a wrong or corrput CA certificate.
An additional dls server ca could not be found.	Internal DLS error because of a missing second CA certificate.
An additional dls server ca already exists.	Internal DLS configuration error.
Additional server ca is corrupt.	Internal DLS error because of a wrong or corrupt second CA certificate.

Error Message	Description
An item with name mac-addr is missing in item list.	IP Device message contains no device ID (attribute name: mac-addr).
AES encoding failed due to an internal error.	Evaluation of the message by AES failed due to a DLS internal error.
Client must provide a certificate.	The IP Device must provide a client certificate.
Client certificate with invalid signature.	The IP Device has sent an invalid or corrupt certificate.
Client certificate invalid.	The IP Device certificate is invalid due to unknown causes (e. g. expired etc.).
Client ca not found or corrupt.	Internal DLS error because of a missing or corrupt client CA certificate.
DLS internal authentication failure.	Internal DLS error due to problems with the authentification (e. g. invalid or corrupt certificate key, internal certificate problems).
Export of CAs could not be performed.	Internal DLS configuration error: export of the CA certificate could not be executed.
Import of CAs could not be performed.	Internal DLS configuration error: import of the CA certificate could not be executed.
Client cert state is invalid.	Internal DLS configuration error: client certificate status is invalid.
String is not a X509 PEM.	Internal DLS configuration error: characters do not comply to the X509 rules.
DCMP URI is not valid.	Internal DLS configuration error: DCMP URI is invalid.
Invalid dcmp state.	Internal DLS configuration error: DCMP state is invalid.
Invalid dcmp transition.	Internal DLS configuration error: DCMP transition is invalid.
client certificate not accepted by device	The IP Device has not accepted the new client certificate sent by the DLS.
device is blocked	Any communication with this IP Device is blocked for security reasons.
device must use secure port	The IP Device must use the secure port (e. g. 18444) instead of the standard port (e. g. 18443.
wrong TAN from device	A TAN has been requested from the IP Device once or multiple times, but even after a defined number of repetitions no valid TAN has been sent. For security reasons, the IP Device is blocked.
No DLS license	No DLS license exists.
licenses exceeded	The number of DLS licenses is exceeded.
unexpected solicited message from workpoint	An (accidental) request message has been sent from the IP Device to the DLS, but was not expected there (no preceding contact-me from the DLS).
empty items list but items expected	The message list is empty, though the DLS expects multiple items.
timeout during read items	Timeout during reading data from a IP Device.
synchronisation exception	Internal DLS synchronisation error.

Error Message	Description
missing e164	The E.164 has been expected by the DLS, but the IP Device has not sent it.
missing items	The expected items are not contained in the message list.
try later	HFA mobility logoff.
mobility save disabled	HFA mobility.

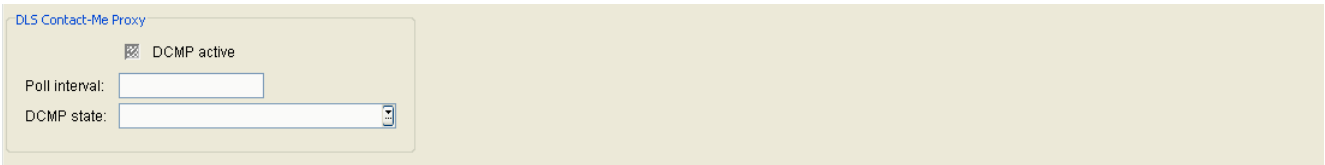
7.6.4.6 "DCMP" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "DCMP" Tab

The DLS Contact-Me Proxy (DCMP) can communicate with the DLS over a firewall or NAT (Network Address Translation) and, if necessary, can perform routing between devices and a DLS in front of the firewall. The devices poll the DCMP regularly. If there are messages on the DLS, the DCMP creates a connection between the device and the DLS.

A DCMP proxy can be assigned as specific location and, therefore, a specific IP address range; see Section 6.9.2, ""DCMP" Tab".

The values in this mask are for display only and cannot be modified.



DLS Contact-Me Proxy

DCMP active

If this checkbox is activated, the device uses the DCMP to communicate with the DLS and polls it regularly. This requires global DCMP activation, see **Administration** > **Workpoint Interface Configuration** > **"DCMP" Tab**.

Poll Interval:

Specifies the intervals at which the device polls the DCMP.

DCMP state:

Provides information about the communication between the device and the DCMP.

Possible values:

- **Enabled**
  The device is in DCMP mode, that is, the DLS contacts the device via the DCMP server.
- **Disabled**
  The device is not in DCMP mode, that is, the DLS contacts the device directly.
- **Refused**
  The device denies DCMP mode (for example, when it is technically unable to operate in DCMP mode).
- **Outdated**
  DCMP data on the DLS has changed and must be communicated to the device.

- **Disable in progress**
  DCMP for this device is deactivated in the DLS and the modified configuration must be communicated to the device.

7.6.4.7 "Autoconfig. IP Phone" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Autoconfig. IP Phone" Tab

This displays the attributes that must be sent to the IP Device for autoconfiguration (Plug&Play) on devices not yet connected (= virtual devices). The individual checkmarks are automatically set once an attribute is configured and/or a profile is entered. But also possible the administrator can check individual checkmarks; if so, default values for the checked parameters are sent to the IP Device.



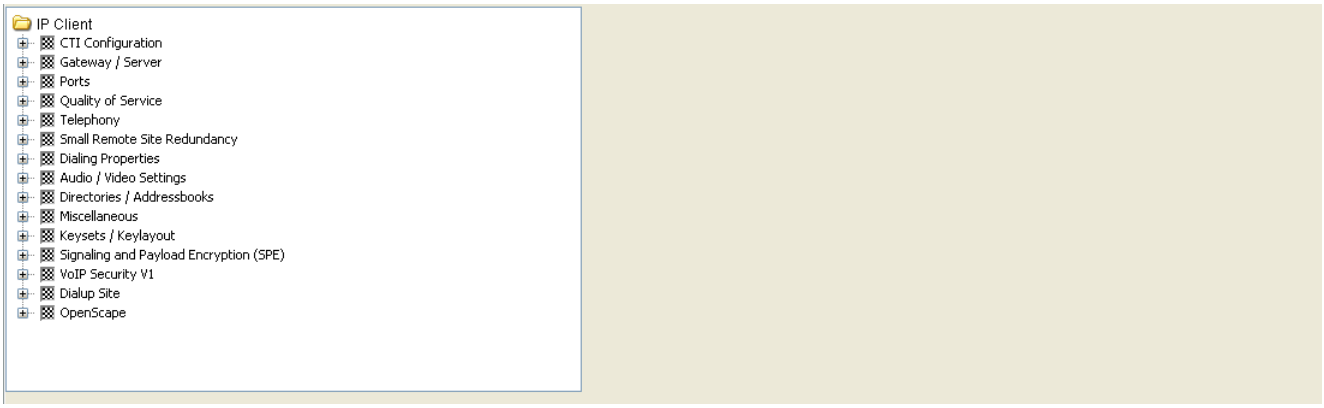
Reset

Resets all fields to inactive.

7.6.4.8 "Autoconfig. IP Client" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Autoconfig. IP Client" Tab

This displays the attributes that must be sent to the IP Device for autoconfiguration (Plug&Play) on IP clients not yet connected (= virtual devices). The individual checkmarks are automatically set once an attribute is configured and/or a profile is entered. But also possible the administrator can check individual checkmarks; if so, default values for the checked parameters are sent to the IP Device.



Reset

Resets all fields to inactive.

7.6.4.9 "Autoconfig. IP Gateway" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Autoconfig. IP Gateway" Tab

This displays the attributes that must be sent to the IP device for autoconfiguration (Plug&Play) on IP gateways not yet connected (= virtual devices). The individual checkmarks are automatically set once an attribute is configured and/or a profile is entered. But also possible the administrator can check individual checkmarks; if so, default values for the checked parameters are sent to the IP Device.



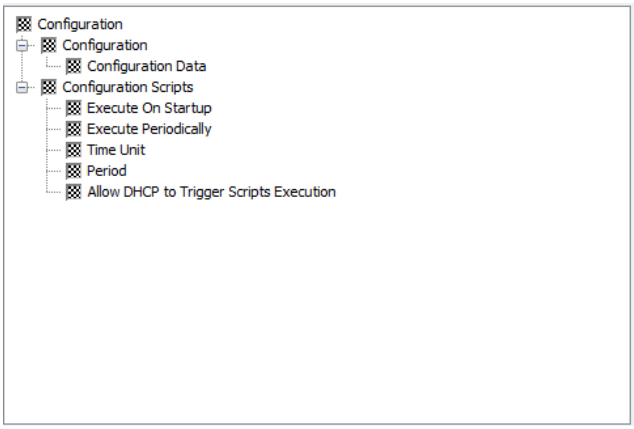
Reset

Resets all fields to inactive.

7.6.4.10 "Autoconfig. Mediatrix Gateway" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Autoconfig. Mediatrix Gateway" Tab

This displays the attributes that must be sent to the IP device for autoconfiguration (Plug&Play) on Mediatrix gateways not yet connected (= virtual devices).

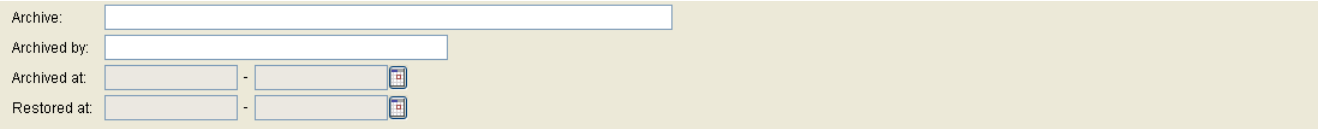


Reset

Resets all fields to inactive.

7.6.4.11 "Archives Data" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Archives Data" Tab



Archive:

Path for the ZIP archive file on the DLS system.

Archived by

Name of the DLS user who created the archive.

Archived at

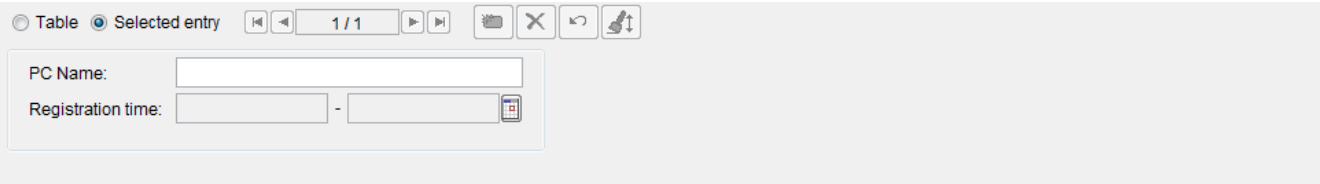
Date and time of the archive.

Restored at

Date and time of the archive restore.

7.6.4.12 "IP Client Registration History" Tab

Call: Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "IP Client Registration History" Tab



Administrators shall be allowed to view the history of the last PCs visited by the windows username. This information will be available for all the devices that have the windows username as device ID.

PC Name:

PC visited by the windows username.

Registration time:

The time PC visited by the user.

8 Mobile Users

Call: Main Menu > Mobile Users

This menu item consists of the following areas:

- SIP Mobile User Configuration
- SIP Mobile User Interaction
- User Data Administration
- Mobility Statistics
- Mobility Statistics Configuration

The **Mobile Users** area is for displaying and modifying Mobile User parameters. For an introduction to mobility, see Section 3.8, "DLS Mobility - General Information".

IMPORTANT: Changes to data in workpoint configuration masks created with templates are not automatically applied to these templates.
These changes must be manually saved to the template (Section 15.7, "Editing Templates").

NOTE: A workpoint can only be configured after successful registration at the DLS. The workpoint must be aware of the corresponding DLS IP address for registration. Registration at the DLS is achieved by:

- reading out workpoint data via the DLS, see Section 7.5.6, "Scan IP Devices" and by
- plugging the LAN connector or power supply into the workpoint.

8.1 SIP Mobile User Configuration

Call: Main Menu > Mobile Users > SIP Mobile User Configuration

This menu consists of the following submenus:

- Gateway/Server
- IP Routing
- Features
- Quality of Service
- Security Settings
- Telephony
- Dialing Properties
- Time Parameters
- Audio Settings
- Applications
- Service Integrations
- User Settings
- SIP Mobility
- Keysets/Keylayout
- Signaling and Payload Encryption (SPE)
- Miscellaneous

General Data

This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

E.164:

Complete E.164 phone number (Mobility ID or basic user phone number).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IMPORTANT: While attempting the related jump, you shall be redirected to the SIP Mobile User Configuration menu options available.

User Type:

Displays the type of data used.

Possible options:

- **Mobility enabled Device**
  Mobility Phone data.
- **Mobile User**
  Mobile User data.

For more information on mobility, see Section 3.8, "DLS Mobility - General Information".

Status:

Displays mobility status.

Possible options:

- **Mobile User logged on**
  Mobile User data: a Mobile User is logged on.
- **Mobile User logged off**
  Mobile User data: no Mobile User is logged on.
- **Device available for Mobile User**
  data: no Mobility Phone Mobile User is logged on to the Mobility Phone.
- **Device used by Mobile User**
  data: a Mobility Phone Mobile User is logged on to the Mobility Phone.

For more information on mobility, see Section 3.8, "DLS Mobility - General Information".

IP Address:

IP address of the IP phone.

Example: **192.117.1.193**

The value is read-only at this location.

> ***IMPORTANT:*** While attempting the related jump, you shall be redirected to the IP Phone Configuration menu options available.

Device ID:

Physical MAC address of the IP phone.

Example: **00:0E:A6:85:71:80**

> ***IMPORTANT:*** While attempting the related jump, you shall be redirected to the IP Phone Configuration menu options available.

Device Type:

Device type of the IP phone.

You can view all IP phone types supported by the DLS in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

This is a read only value.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Starts a job for transmitting configuration changes to the selected object. For more information, see Section 15.3, "First Steps: Changing IP Device Parameters". In Templates view, parameters are saved in the selected templates. For more information, see Section 15.7, "Editing Templates".

Discard

The modifications made are not transmitted to the selected object and are deleted from the input mask.

Refresh

The parameters are reloaded from the database.

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Rename

Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

8.1.1 Gateway/Server

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server

This area features the following components:

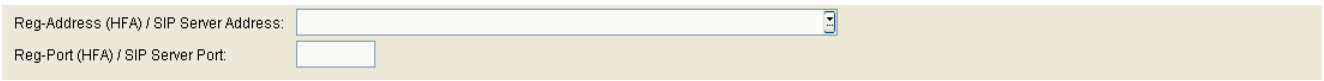
- General Data
- Possible Action Buttons
- "Gateway (HFA) / SIP Server" Tab
- "SIP Terminal Settings" Tab
- "SIP Registering 1" Tab
- "SIP Registering 2" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.1.1 "Gateway (HFA) / SIP Server" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "Gateway (HFA) / SIP Server" Tab



Reg-Address (HFA) / SIP Server Address:

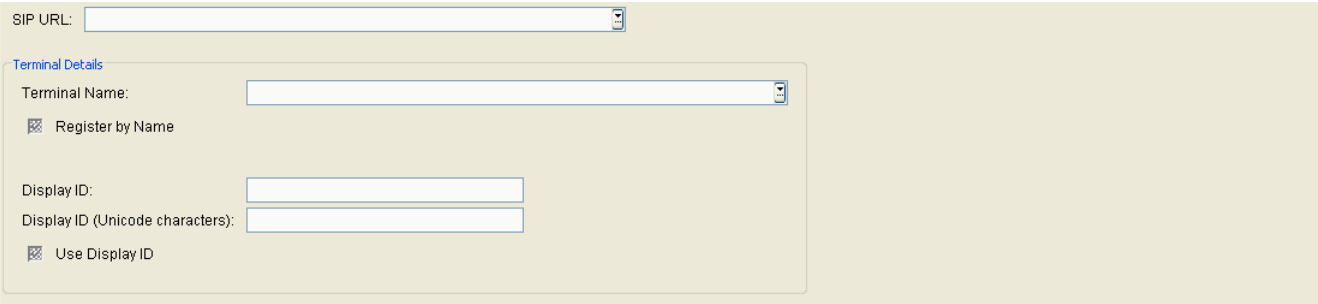
IP address or host name of the PBX, gateway or SIP server used for operating the workpoint.

Reg-Port (HFA) / SIP Server Port:

Port number of the PBX, gateway or SIP server used for operating the workpoint.

8.1.1.2 "SIP Terminal Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "SIP Terminal Settings" Tab



SIP URL:

SIP address of the IP phone.

Format: **<SIP user ID>@<Domain>**.

Terminal Details

Terminal Name:

Name of the IP phone used as a synonym for the phone number during registration.

Only necessary if the **Register by Name** check box is selected and the registrar server is appropriately configured.

Register by Name

Check box for activating the function that sends the contents of the **Terminal Name** field as part of registration.

If the check box is not active, the contents of the **E.164 number** field are also sent in the course of registration.

Display ID:

Name of the IP phone as shown on the workpoint display.

Value range: max. 24 alphanumeric characters.

NOTE: Please refer to Section 15.15.1, "Macro Command Syntax" in case you need to use macro commands, otherwise the DLS will not save the proper Display ID.

Display ID (Unicode characters):

Name of the IP phone in unicode characters as shown on the workpoint display.

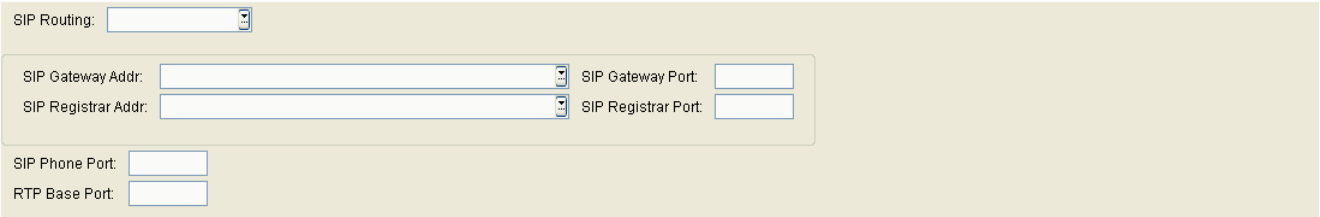
This option is only supported by OpenStage devices.

Use Display ID

If this check box is activated, the Display ID is shown on the workpoint.

8.1.1.3 "SIP Registering 1" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "SIP Registering 1" Tab



SIP Routing:

Possible options:

- **Gateway**
  A gateway is used for SIP routing.
- **Server**
  An SIP proxy is used for SIP routing.
- **Direct**

If **Direct** or **Gateway** is selected, no registration messages are sent. Registration messages are sent to the registrar server for the **Server** routing mode.

SIP Gateway Addr.

IP address of the gateway. This parameter is used when the **Gateway** mode is selected for SIP routing.

SIP Gateway Port:

Port number of the gateway. This parameter is used when the **Gateway** mode is selected for SIP routing.

SIP Registrar Addr:

IP address of the SIP registrar.

SIP Registrar Port:

Port number of the SIP Registrar.

SIP Phone Port:

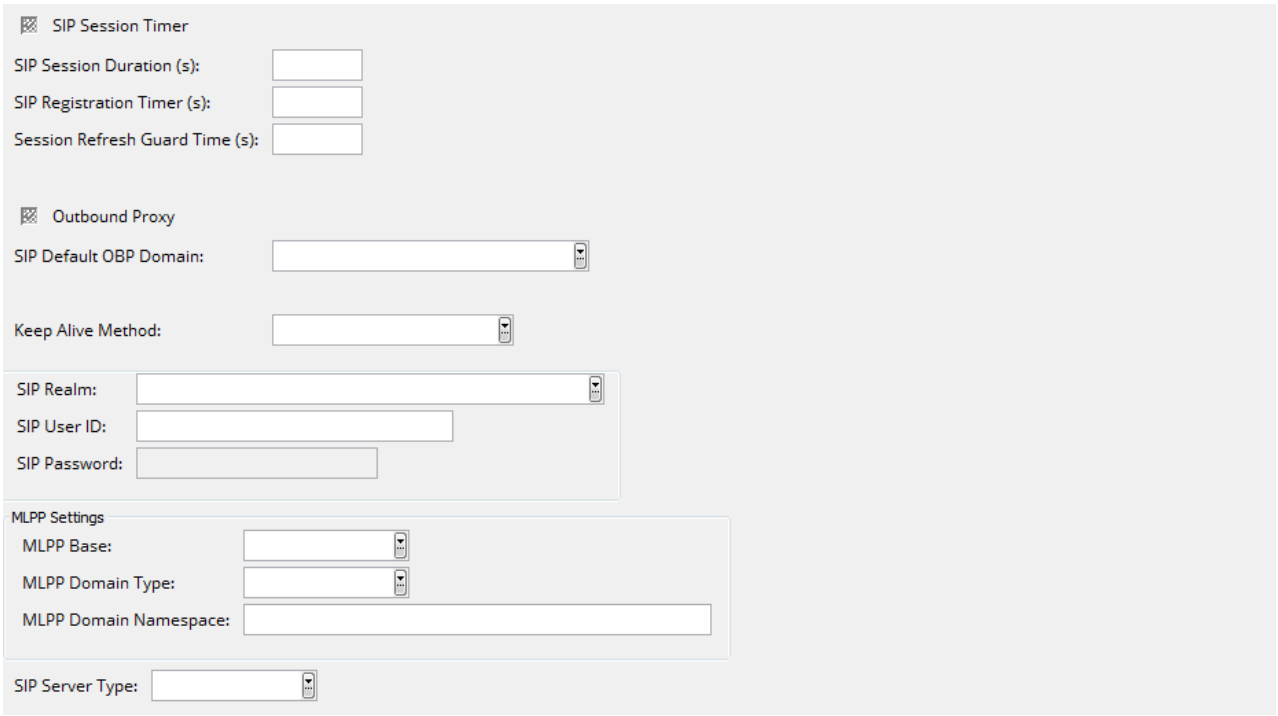
Port number of the IP phone.

RTP Base Port:

Base port number for RTP transport.

8.1.1.4 "SIP Registering 2" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Gateway/Server > "SIP Registering 2" Tab



SIP Session Timer

Check box for activating the SIP session timer. The timer is used to monitor the duration of an SIP session.

SIP Session Duration:

Highest duration in seconds for an SIP session.

Value range: **0** ... **3600** seconds.

SIP Registration Timer:

Time period for re-registration at the SIP server. Re-registration ensures that the SIP telephone remains logged on to the SIP server. It can also detect server connectivity problems.

Value range: **0** ... **4320** seconds.

Default: **0**

Session Refresh Guard Time (sec):

Time interval that triggers a SIP registration / SIP subscription, session to be refreshed before the maximum expiry time provided by the SIP server. The setting value indicates the earliest point before the session expires when the device can consider sending a session refresh message to stop the session from expiring.

Default value:**0**

Value range:**0** ... **3600** seconds.

NOTE: Available only to CP200/205/400/600 devices & of V1R3 version and higher.

Example: if the Expiry header form the SIP server is 600 seconds and the guard time is 15 seconds then the refresh from device will sent between 585 seconds (600-15) and 600 seconds after previous registration.

Outbound Proxy

Check box for activating an SIP proxy for outbound calls.

Together with **SIP Default OBP Domain** this check box controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

SIP Default OBP Domain:

Together with **Outbound Proxy** this entry controls outbound call routing on the basis of the number dialed or the user ID.

For more information, see Chapter 17, "Outbound Proxy".

Keep Alive Method:

Possible options:

- **Sequence**
- **CRLF**

SIP Realm:

SIP range in which the workpoint is operated. SIP realm is used to identify the telephone at the SIP server.

SIP User ID:

The user ID is the first part of the SIP URL.

SIP Password:

Password required for accessing the SIP server.

MLPP Settings

MLPP Base

Possible options:

- **Local**
- **Server**

MLPP Domain Type

Specifies which resource priority namespace will be accepted from a fixed list.

Possible options:

- **dsn**
  dsn-000000
- **uc**
  uc-000000
- **dsn+uc**
- **Other domain**

MLPP Domain Namespace

Specifies an ASCII string for a single resource priority namespace which will be accepted.

Alphanumerical characters and the following special charakters are allowed: -!%*_+` "~

A "." is not allowed.

SIP Server Type:

Possible options:

- **other**
- **OpenScape Voice**
- **Broadsoft**
- **Sylantro**
- **HiQ8000**
- **Genesys**
- **Google Voice**

8.1.2 IP Routing

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > IP Routing

This area features the following components:

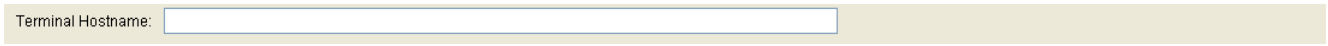
- General Data
- Possible Action Buttons
- "DNS Server" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.2.1 "DNS Server" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > IP Routing > "DNS Server" Tab



Terminal Hostname:

Host name of the terminal.

Permitted characters: letters, digits, hyphens, underscores, and periods; case-sensitive; maximum length: 63 characters.

The value is read-only if it was dynamically assigned with DHCP.

8.1.3 Features

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features

This area features the following components:

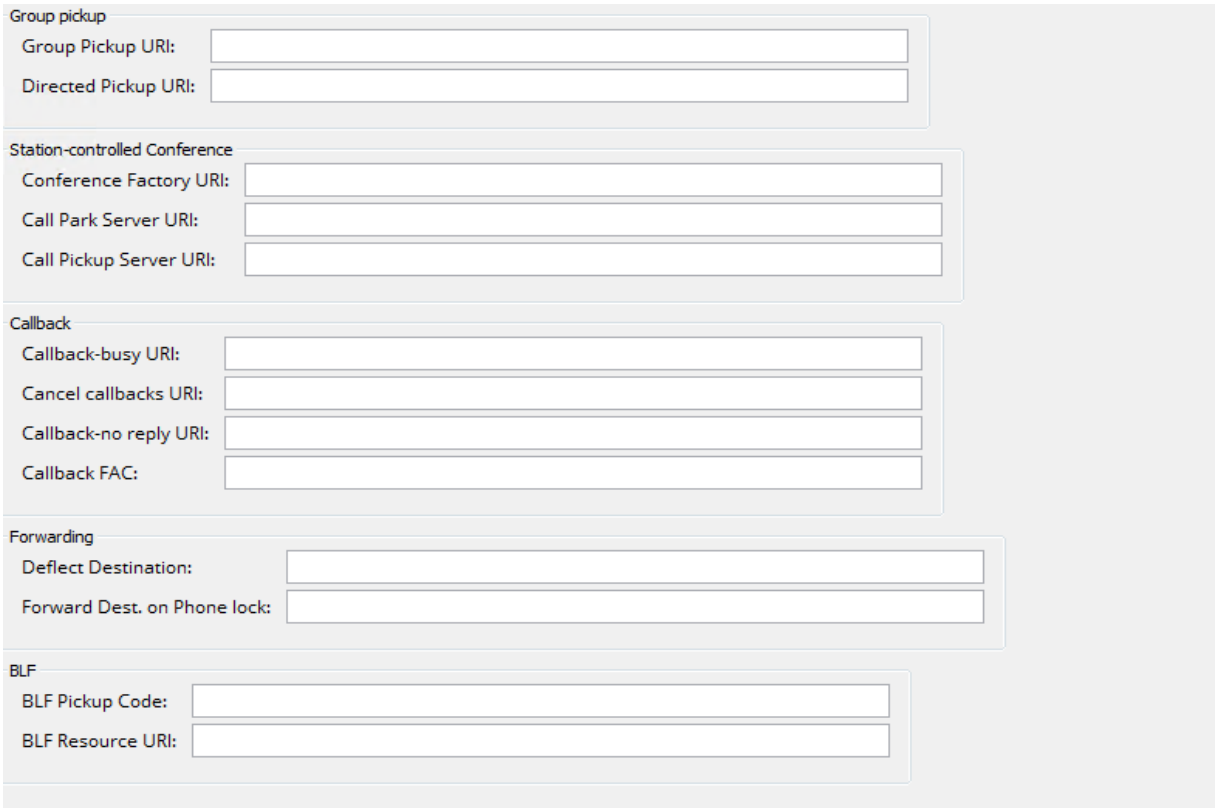
- General Data
- Possible Action Buttons
- "Feature Settings 1" Tab
- "Feature Settings 2" Tab
- "Call related User Settings" Tab
- "Availability" Tab
- "Server based Features" Tab
- "Dialplan" Tab
- "Ringer Melody / Tone" Tab
- "Call Forwarding" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.3.1 "Feature Settings 1" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Feature Settings 1" Tab



Group pick-up

Group Pickup URI:

URI of the group pickup.

Only available in SIP workpoints.

Directed Pickup URI:

IP address or host name of the server for providing the directed pickup feature.

Only available for non-OpenScape Voice servers.

Station-controlled Conference

Conference Factory URI:

URI for setting up conference calls.

Only available in SIP workpoints.

Call Park Server URI:

URI of the server for parking calls.

Only available in SIP workpoints.

Call Pickup Server URI:

URI of the server for group pickup.

Only available in SIP workpoints.

Callback

Callback-busy

URI of the server that controls the "Callback-busy" feature.

Only available for optiPoint and OpenStage up to V2.

Cancel callbacks URI:

URI of the server that controls the "Cancel callbacks" feature.

Callback-no reply URI

URI of the server that controls the "Callback-no reply" feature.

Only available for optiPoint and OpenStage up to V2.

Callback FAC

URI to be used for stimulus callback call requests.

Only available for OpenStage V3.0 onwards.

Deflection

Deflect Destination:

Destination number for call forwarding.

Only available in SIP workpoints.

Forward Dest. on Phone lock:

Destination number for forwarding in the case of a call to a locked workpoint.

BLF

BLF Pickup Code:

BLF Pickup Code.

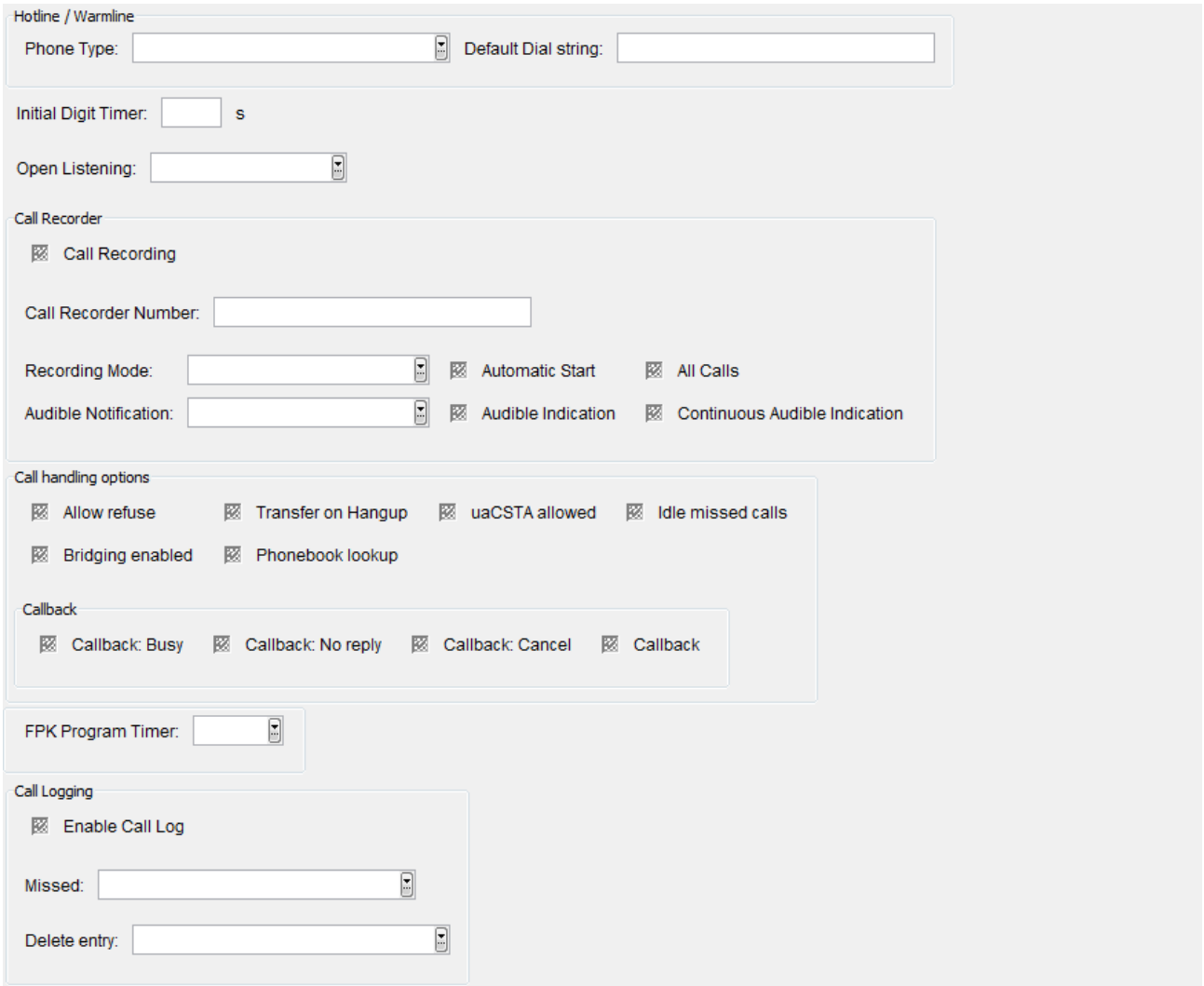
BLF Resource URI:

Default value is set to NULL.

Available only for CP200/CP400/CP600 SIP phones of V1R2 version and higher.

8.1.3.2 "Feature Settings 2" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Feature Settings 2" Tab



Hot Line/Warm Line

Phone Type:

Time delay for the functions "Hotline" and "Warmline"

Possible options:

- **Ordinary**
- **Hot Line**
- **Warm Line**

Only available in SIP workpoints.

Default Dial String:

Destination number for the functions "Hotline" and "Warmline".

Only available in SIP workpoints.

Initial Digit Timer:

Waiting time in seconds for a dialed digit after the dial tone starts.

Only available in SIP workpoints.

Open Listening

Open Listening settings.

Possible options:

- **Standard Mode**
  To switch to Open Listening mode, the user must press and hold the Open Listening key while returning the handset to the cradle.
- **US Mode**
  To switch to Open Listening mode, the user must first press the Open Listening key and then return the handset to the cradle.

Call Recorder

Call recording

Check box for activating call recording.

Call Recorder Number

Phone number of the call recorder.

Recording Mode

Determines the behaviour of the call recording.

Possible options:

- **Manual:**
- **Auto Start**
- **All Calls**
- **One Call**

Audible Notification

Select the tone for audible notification.

Possible options:

- **Off**
- **On / Single Shot**
- **Repeated**

Automatic Start

When activated, call recording is started automatically, with incoming calls and outgoing calls. The user can switch the recording on or off during a conversation.

The checkbox is effective only if voice recording is activated on the phone.

All Calls

When activated, call recording is started automatically, with incoming calls and outgoing calls. The user can not control the recording.

The checkbox is effective only if voice recording is activated on the phone.

Audible Indication

A beep signals to the called party that the phone call is being recorded.

Continuous Audible Indication

A continuous audible indication signals to the called party that the phone call is being recorded.

The checkbox is effective only when **Audible Indication** is activated.

Call handling options

Allow refuse

Checkbox for activating the function for rejecting calls.

Only available in SIP workpoints.

Transfer on Ring

Checkbox for activating the "Transfer on Ring" feature

Only available in SIP workpoints.

Transfer on Hangup

Checkbox for activating the "Transfer on Hangup" feature.

Only available in SIP workpoints.

Bridging enabled

When active, call bridging is enabled.

Only available in SIP workpoints.

uaCSTA allowed

Checkbox to activate the "uaCSTA" feature.

Only available in SIP workpoints.

Phonebook lookup

Checkbox for activating the "Phonebook lookup" feature.

Idle missed calls

If set, an indication for missed calls will be shown on the display.

Callback

Callback: Busy

Checkbox for activating the "Callback-busy" feature.

Only available in SIP workpoints.

Callback: No reply

Checkbox for activating the "Callback-no reply" feature.

Only available in SIP workpoints.

Callback: Cancel

When active, the user can cancel callback requests.

Callback

Activates Callback.

Only available for OpenStage V3 onwards.

FPK Program Timer

When "Off" is selected, the free programmable keys (FPKs) will not change to programming mode on long press.

Possible options:

- **On**
- **Off**

Call Logging

Enable Call Log

Checkbox that indicates whether Call logging is enabled.

Missed Logging

Indicates whether calls completed elsewhere will be logged on phone.

Possible options:

- **Include answered elsewhere**
  Calls completed elsewhere will be logged on phone.
- **Exclude answered elsewhere**
  Calls completed elsewhere will not be logged on phone.

Delete Entry

Indicates whether calls log entries are deleted in case there is a call to an entry in Missed calls list.

Possible options:

- **Delete manually (**default option)

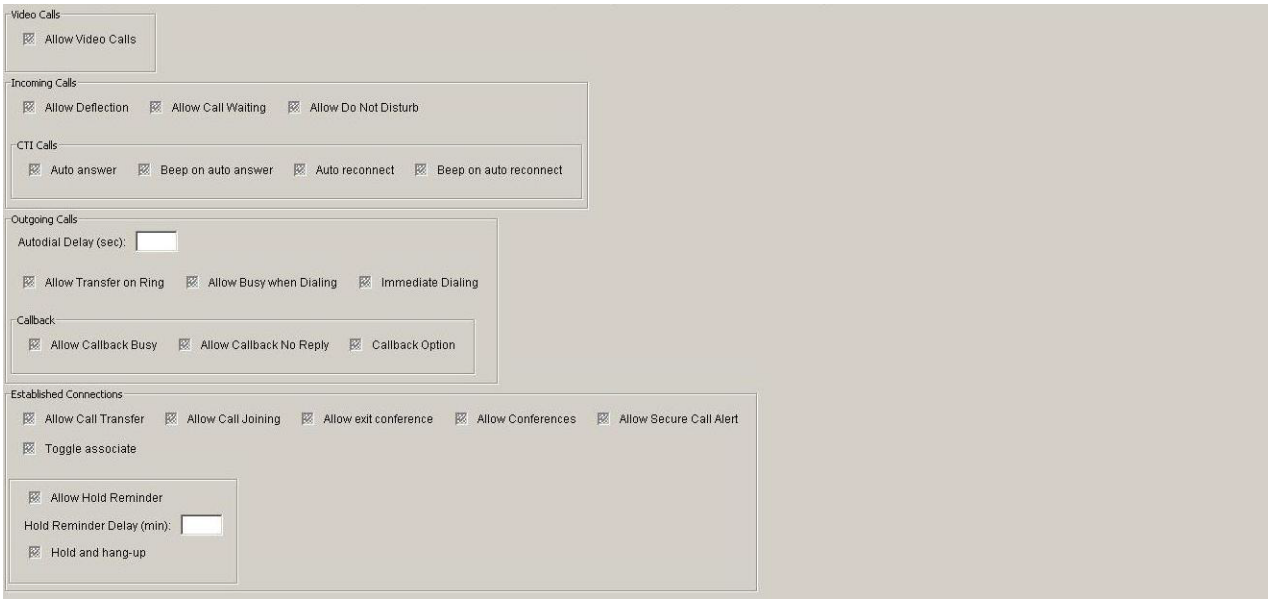
Outgoing calls that are made to entries in Missed calls tab of call log and that are connected will not be deleted from call log.

- **Delete when called**

Outgoing calls that are made to entries in Missed calls tab of call log and that are connected will be deleted from call log.

8.1.3.3 "Call related User Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Call related User Settings" Tab



Video Calls

Allow Video Calls

Checkbox for activating Video Calls.

If the Allow Video Calls checkbox is activated , then video calls will be allowed.

Incoming Calls

Allow Deflection

Check box for activating Call Deflection.

Allow Call Waiting

Check box for activating Call Waiting.

Allow Do Not Disturb

Check box for activating Do Not Disturb.

CTI Calls

Auto answer

Check box for activating Auto Answer.

Only available in SIP workpoints.

Beep on auto answer

Check box for activating a confirmation beep on Auto Answer.

Only available in SIP workpoints.

Auto reconnect

Check box for activating automatic reconnection of a parked call.

Only available in SIP workpoints.

Beep on auto reconnect

Check box for activating a confirmation beep on reconnection of a parked call.

Only available in SIP workpoints.

Immediate Dialing

If this check box is active, immediate dialing is executed as soon as the entered string matches a dial plan entry.

Only available in SIP workpoints.

Outgoing calls

Autodialing delay (sec):

Delay for Automatic Dialing in seconds.

Allow Transfer on Ring

Check box for activating Transfer on Ring.

Allow Busy when Dialing

Check box for activating Busy when Dialing.

Allow Immediate Dialing

Check box for activating the **Hot Keypad Dialing** feature.

Callback

Allow Callback Busy

Checkbox for activating Callback on Busy.

Only available for OpenStage V1 and V2.

Allow Callback No Reply

Checkbox for activating Callback on No Reply.

Only available for OpenStage V1 and V2.

Callback Option

Callback Option.

Only available for OpenStage starting with V3.

Established Connections

Allow Call Transfer

Check box for activating Call Transfer.

Allow Call Joining

Check box for activating Call Joining.

Allow exit conference

Check box for activating Exit Conference.

Allow Conferences

Check box for activating Conferences.

Allow Secure Call Alert

If the handling of secure calls is enabled on the phone and this check box is activated, a popup window and an alert tone will notify the user when an insecure (unencrypted) call comes in.

Toggle associate

Checkbox for activating associated toggle.

Allow Hold Reminder

Check box for activating the Hold Reminder.

Hold Reminder Delay (min):

Delay for the Hold Reminder in minutes.

Hold and Hangup

Checkbox for activating the ’’ Hold and Hangup ’’ feature on non-keyset OpenStage phones.

This feature enables the user to temporarily hold and hang up a line without disconnecting your caller. This function in disabled by default.

8.1.3.4 "Availability" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Availability" Tab



Call Hold

Check box for activating the function for placing calls on hold.

Area of validity: Only applies to SIP workpoints.

Call deflection

Check box for activating manual forwarding for incoming calls (CD).

Only available in SIP workpoints.

Call forwarding

Check box for activating automatic call forwarding (CF).

Only available in SIP workpoints.

Log forwarded calls

Check box for activating logging for forwarded calls.

Only available in SIP workpoints.

Call duration

Check box for activating the function for displaying the call duration.

Only available in SIP workpoints.

Call waiting

Check box for activating visual and/or acoustic alerting for waiting calls (CW).

Only available in SIP workpoints.

Call transfer

Check box for activating the function for transferring calls (ECT).

Only available in SIP workpoints.

Call pickup

Check box for activating the function for picking up parked calls.

Only available in SIP workpoints.

Auto reconnect

Check box for activating the auto reconnect feature.

Only available in SIP workpoints.

Call display by number

Switch for activating call number display at the workpoint.

Only available in SIP workpoints.

Call display by name

Switch for activating caller name display at the workpoint.

Only available in SIP workpoints.

Music on hold

Check box for activating music on hold for held and parked calls.

Only available in SIP workpoints.

Do not disturb

Check box for activating the do-not-disturb function (optical alerting and ring only).

Only available in SIP workpoints.

Message waiting

Check box for activating alerting for waiting messages (MWI).

Only available in SIP workpoints.

Local conference

Check box for activating the function for setting up a local conference.

Only available in SIP workpoints.

Auto answer

Check box for activating auto answer.

Only available in SIP workpoints.

PC Interface

Check box for activating the PC interface.

WAP browser on APM/DSM

Check box for activating the WAP browser on the optiPoint application module/display module.

Only available in SIP workpoints.

LDAP on APM/DSM

Check box for activating the LDAP function on the optiPoint application module/display module.

Only available in SIP workpoints.

Telephony on APM/DSM

Check box for activating the telephony function on the optiPoint application module/display module.

Only available in SIP workpoints.

Voice recognition on APM/DSM

Check box for activating the voice recognition function (voice dialing) on the optiPoint application module/display module.

Only available in SIP workpoints.

Speed dial on APM/DSM

Check box for activating the speed-dialing function on the optiPoint application module/display module with a Java midlet.

Only available in SIP workpoints.

ENB on APM/DSM

Check box for activating the electronic notebook on the optiPoint application module/display module.

Only available in SIP workpoints.

Call park

Check box for activating the function for parking calls.

Only available in SIP workpoints.

Call join

Check box for activating the function for joining calls.

Only available in SIP workpoints.

Group Pickup Beep

Check box for activating the "Group Pickup Beep" feature.

Blind Transfer

Checkbox for activating the feature "Blind Transfer".

Repertory Dial

Checkbox for activating the feature "Repertory Dial".

Busy Lamp Flag (BLF)

Checkbox for activating the Busy Lamp Field (BLF).

Direct Station Select (DSS)

Checkbox for activating Direct Station Select (DSS).

CTI

Checkbox for activating CTI.

Line Overview

Checkbox for activating the "Line Overview"

Feature Toggle

Checkbox for activating the feature "Feature Toggle".

Third Call Leg

Checkbox for activating the feature "Third Call Leg".

Group Pickup

Checkbox for activating the feature "Group Pickup".

Video Call

Checkbox for enabling the feature " Video Call ".

Ext/Int Forwarding

Checkbox for enabling / disabling the External/Internal Forwarding.

8.1.3.5 "Server based Features" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Server based Features" Tab

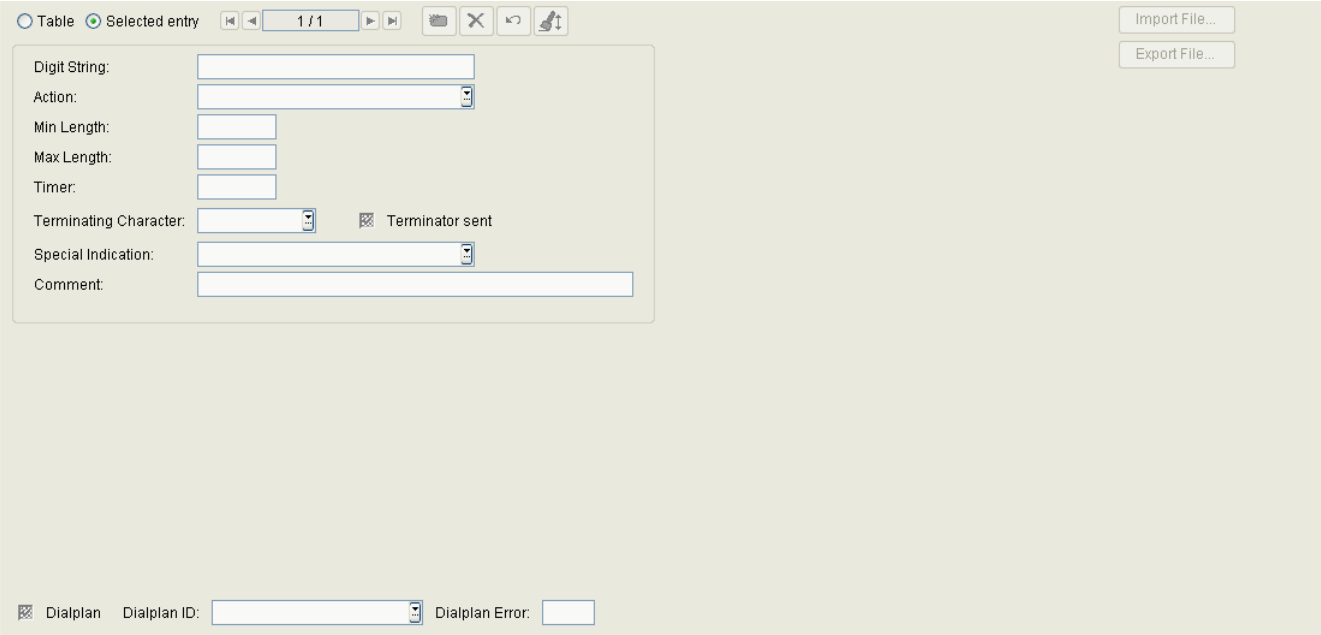


Support of Server based Features

If this check box is activated, server-based features on the device are enabled for the user.

8.1.3.6 "Dialplan" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Dialplan" Tab



Digit String

Digit String Digit string for executing this action.

Only available in SIP workpoints.

Action

Action executed for this digit string.

Possible options:

- **-C- Action for digits**
- **-CD1- Action for digits, dial tone**
- **-D1- Dial tone**
- **-S- Send digits**
- **SD1- Send digits, dial tone**

Only available in SIP workpoints.

Min Length

Minimum digit string length for digit string interpretation.

Only available in SIP workpoints.

Max Length

Maximum digit string length for digit string interpretation.

Only available in SIP workpoints.

Timer

Delay before the action is performed.

Value range: 1 ... 9 seconds.

Only available in SIP workpoints.

Terminating Character

Character that ends the digit string entered.

Possible options:

- **#**
- *****

Only available in SIP workpoints.

Special Indication

Possible options:

- **-E- emergency call**
- **-b- bypass**

Only available in SIP workpoints.

Terminator sent

Displays whether the terminating character is included in the digit string.

Dial Plan

Check box for activating the dial plan. The entries in the "Dialplan" Tab are interpreted if this check box is active.

Only available in SIP workpoints.

Dial Plan ID:

Name of the dial plan - must begin with a "!".

Value range: max. 14 alphanumeric characters.

Only available in SIP workpoints.

Dial Plan Error:

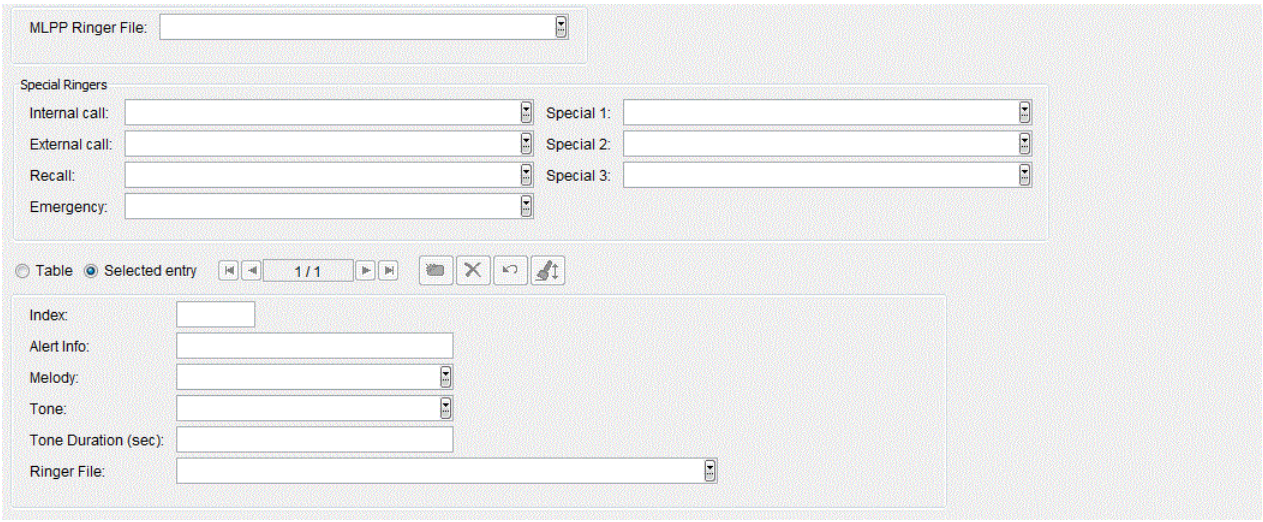
Specifies the dial plan entry that is faulty in the event of an error.

Value range: **1** ... **48**

Only available in SIP workpoints.

8.1.3.7 "Ringer Melody / Tone" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Ringer Melody / Tone" Tab



NOTE: A template for **Ringer Melody / Tone** can be created by searching for an IP Device with entries in **Ringer Melody / Tone** (empty entries are allowed as well). Use the action **Copy to Template** to create a template. There must be 15 entries, which may be empty.
This template can be modified, saved, and applied.

MLPP Ringer File

Precedence ringer for priority calls.

Special Ringers

Internal call

Default value : Bellcore-dr1

External call

Default value : Bellcore-dr2

Recall

Default value : Bellcore-dr3

Emergency

Default value : alert-emergency

Special 1

Special 2

Special 3

Index

Specifies the sequence of the signaling entries.

This is automatically set. The field is provided for display only.

Alert Info

If the string specified here is identical with a special string which is sent to the phone in the SIP alert info header, the corresponding ringtone is used

Only available in SIP workpoints.

Melody

Type of ring melody.

Possible options: **Melody 1** ... **8**, **Melody off**.

Only available in SIP workpoints.

Tone

Ringtone sequence.

Possible options:

- **1**
  = 1 sec ON, 4 sec OFF
- **2**
  = 1 sec ON, 2 sec OFF

- **3**
  = 0,7 sec ON, 0,7 sec OFF, 0,7 sec ON, 3 sec OFF

Only available in SIP workpoints.

Tone Duration

Duration of the ringtone.

Value range: **1** ... **300** seconds.

Default: **60** seconds.

Only available in SIP workpoints.

Ringer File

Name of the audio file containing the ringtone.

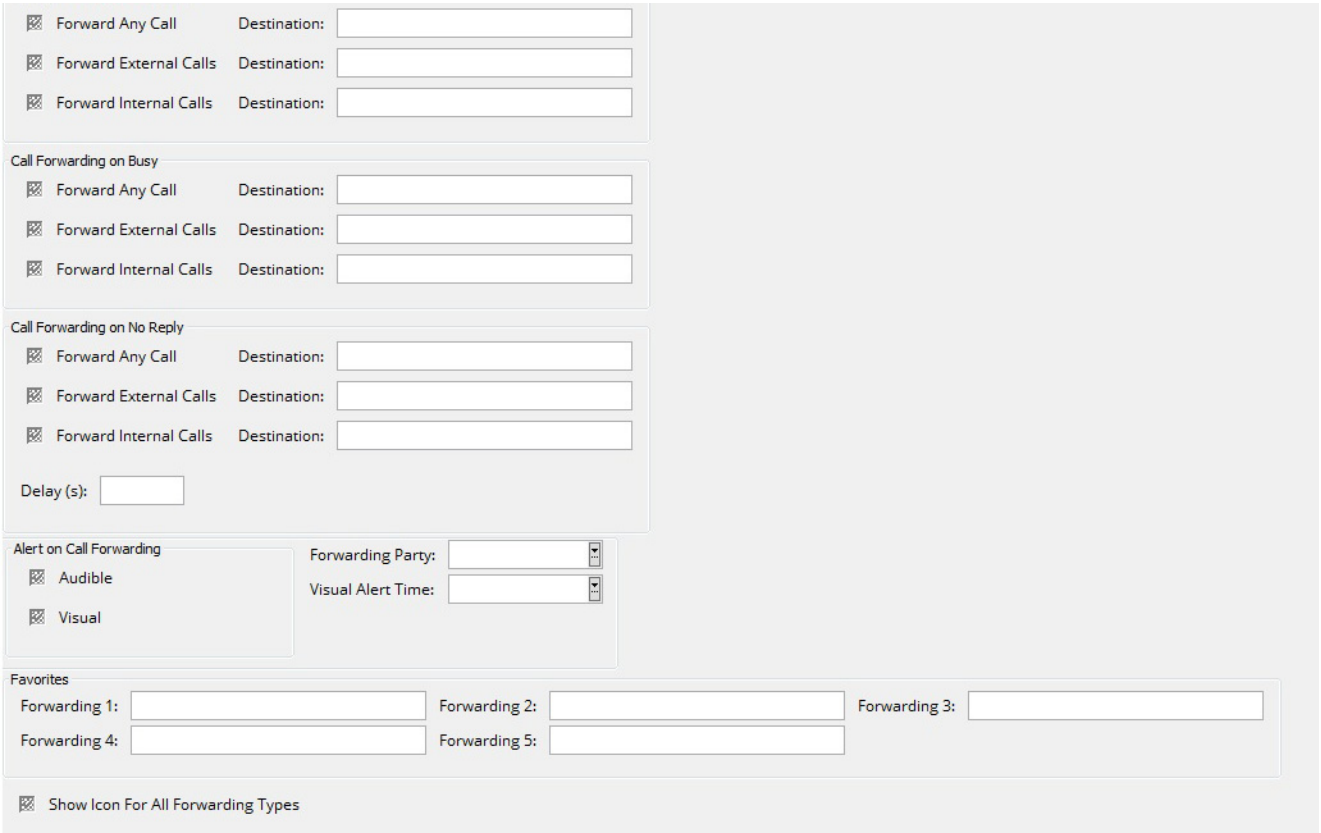
IMPORTANT: In order for a special ringer to be configured, then :

1. it's alert info (e.g. Bellcore-dr1) and
2. it's respective Ringer file (e.g. Harmonize.mp3) should be configured first.

These two configurations (special ringers & ringer melody table) cannot be performed in a single step.A new Alert Info and Special Ringer cannot be added at the same time in the Special Ringers table & the Distinctive Ringers table.Before a Special Ringer is configured, make sure it's Alert Info is already configured,
i.e. first configure Bellcore-dr1 in lower table, press **Save** and then configure this Alert Info in Special Ringers Internal Call & press **Save** again.

8.1.3.8 "Call Forwarding" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Features > "Call Forwarding" Tab



NOTE: The additional Call Forwarding settings (for external/internal) shall be available if the option "**Support of Server Based Features**" is enabled under **Mobile Users**> **SIP Mobile User Configuration**> **Features**> **"Server based Features" Tab**.

Call Forwarding Unconditional

Forward Any Call

Checkbox for activating unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward External Calls

Checkbox for activating External Call Forwarding.

Destination:

Call number of the External Call Forwarding destination.

Forward Internal Calls

Checkbox for activating Internal Call Forwarding.

Destination:

Call number of the Internal Call Forwarding destination.

Call Forwarding on Busy

Call Forwarding on Busy

Forward Any Call

Checkbox for activating unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward External Calls

Checkbox for activating External Call Forwarding.

Destination:

Call number of the External Call Forwarding destination.

Forward Internal Calls

Checkbox for activating Internal Call Forwarding.

Destination:

Call number of the Internal Call Forwarding destination.

Call Forwarding on No Reply

Forward Any Call

Checkbox for activating unconditional Call Forwarding.

Destination:

Call number of the Call Forwarding destination.

Forward External Calls

Checkbox for activating External Call Forwarding.

Destination:

Call number of the External Call Forwarding destination.

Forward Internal Calls

Checkbox for activating Internal Call Forwarding.

Destination:

Call number of the Internal Call Forwarding destination.

Delay (sec):

As soon as this time span has expired without the call being accepted, the call is forwarded.

Alert on Call Forwarding

Audible

Check box for activating an audible alert on the forwarding phone.

Visual

Check box for activating a visible alert on the forwarding phone.

Forwarding Party:

Select which forwarding party will be displayed when multiple forwarding is active.

Possible options:

- **Display first**
- **Display last**

Visual Alert Time:

When visual alert is active, the toast message is shown on the forwarding phone screen according to the set time. The toast message appears for 5 seconds by default. However, you can configure the visual alert’s appearing time from this field:

Possible values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

- **8**
- **9**
- **10**
- **11**
- **12**
- **13**
- **14**
- **15**

NOTE: When you set the value to zero, the toast message will not appear at all.

NOTE: On HFA configured phones the toast message is only shown when the phone is configured with OpenScape 4000, not with OpenScape Business.

Favorites

Forwarding 1:

Forwarding 2:

Forwarding 3:

Forwarding 4:

Forwarding 5:

Show Icon For All Forwarding Types:

When enabled, the forwarding icon can be now shown in the main menu of the phone, in case **unconditional** forwarding, forward **on busy** or forward on **no reply** is active.

The user will get a visual indication in the main menu of the phone.

Disabled by default.

> ***NOTE:*** Forwarding unconditional is not affected. No matter what the setting is, the phone will always display a forwarding icon and make keys LED turn on if call forwarding unconditional is activated.

> ***NOTE:*** This flag is available only to CP200/205/400/600 HFA devices, SIP V1R3 version and higher.

8.1.4 Quality of Service

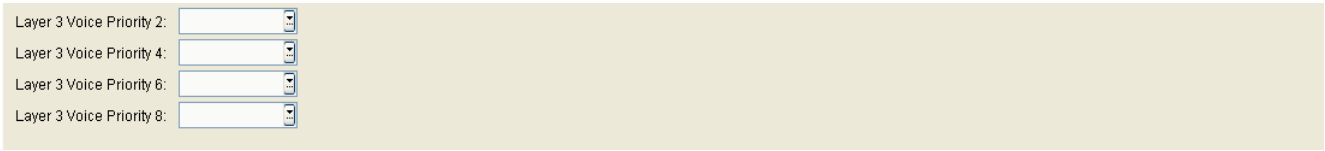
Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Quality of Service

This area features the following components:

- General Data
- Possible Action Buttons
- "QoS Parameter" Tab

8.1.4.1 "QoS Parameter" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Quality of Service > "QoS Parameter" Tab



Layer 3 Voice Priority 2

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 4

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 6

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

Layer 3 Voice Priority 8

Layer 3 value for voice priority calls.

Value range: **DSCP00** ... **DSCP63**

8.1.5 Security Settings

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Security Settings

This area features the following components:

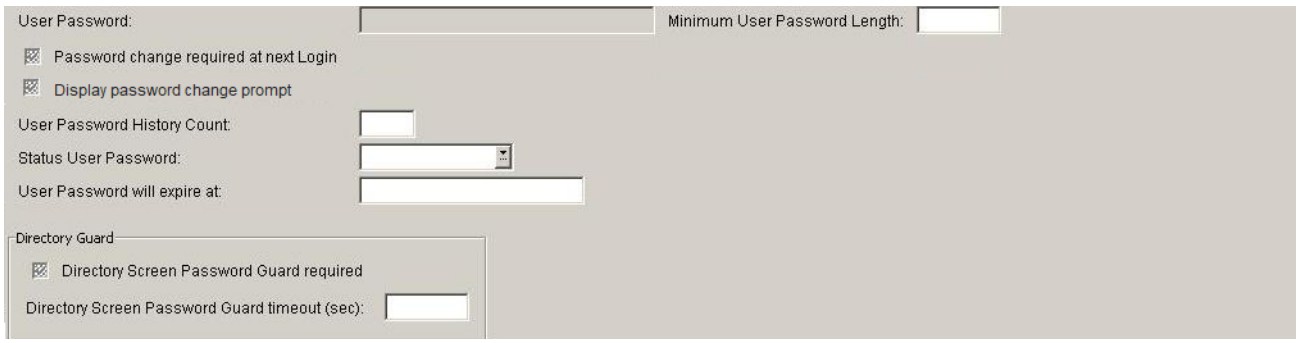
- General Data
- Possible Action Buttons
- "Passwords" Tab
- "Enabled Services (NW Stack)" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.5.1 "Passwords" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Security Settings > "Passwords" Tab



User Password:

Password for access to the workpoint's user area.

> ***NOTE:*** When a mobile user is logged on, User Password stands as Mobility Password (as described in Section 8.2.1.1, ""Mobile / Basic User" Tab").
> When the mobile user logs off, the User Password reverts back to the password of the basic user.

Minimum User Password Length:

Minimum number of characters that a password must contain.

Password change required at next Login

If this checkbox is activated, the user will be prompted to change the password.

Display change password prompt

If this checkbox is activated, the user will be prompted upon logging in to change the password immediately.

User Password History Count:

Shows the count of password changes.

Status User Password:

Status of the user password.

Possible Options:

- Active
- Suspended
- Disabled

User Password will expire at:

Time & Date of the User Password expiration

Directory Guard

Directory Screen Password Guard required

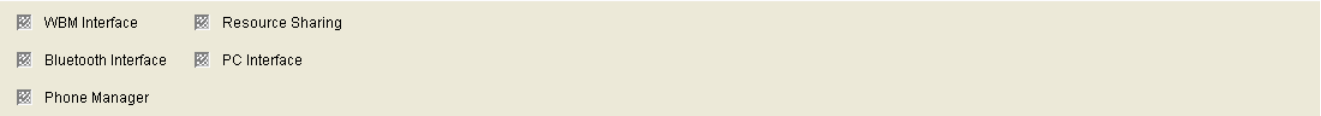
This check box activates password protection on the directory screen. To use the screen, you must enter the standard user password.

Directory Screen Password Guard timeout (sec)

Password protection is activated when the length of time specified here expires. After this time, you must enter the password to continue using the directory screen.

8.1.5.2 "Enabled Services (NW Stack)" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Security Settings > "Enabled Services (NW Stack)" Tab



WBM Interface

Check box for activating the WBM interface.

Resource Sharing

Check box for activating resource sharing (shared use of mouse and keyboard).

Bluetooth Interface

Check box for activating the Bluetooth interface.

Phone Manager

Check box for activating the Phone Manager.

PC Interface

Check box for activating the interface between the PC and the device.

8.1.6 Telephony

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Telephony

This area features the following components:

- General Data
- Possible Action Buttons
- "Telephony" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.6.1 "Telephony" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Telephony > "Telephony" Tab



Emergency Number:

Contains the phone number that can be dialed in an emergency.

8.1.7 Dialing Properties

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Dialing Properties

This area features the following components:

- General Data
- Possible Action Buttons
- "Dialing Properties" Tab
- "Canonical Dial Lookup" Tab

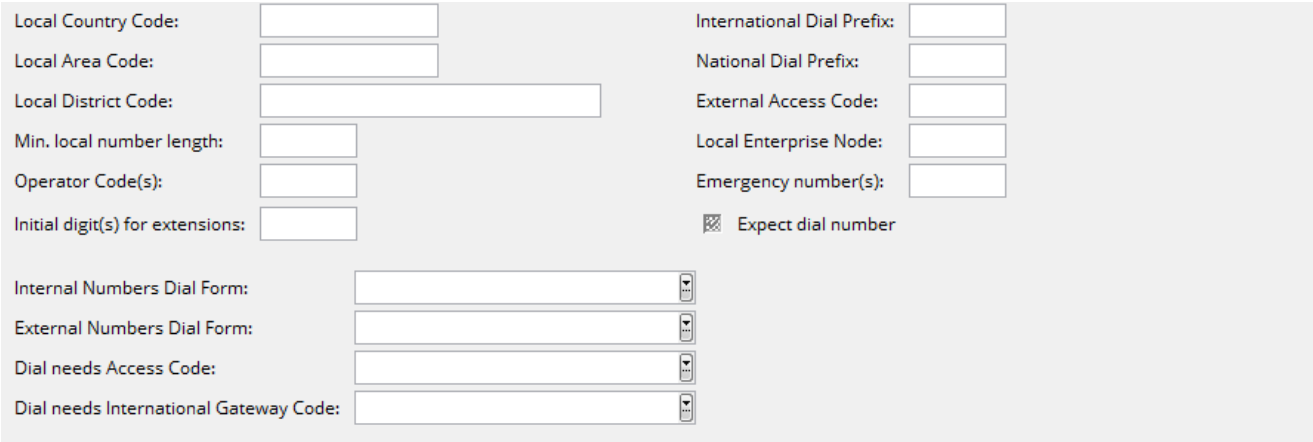
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.7.1 "Dialing Properties" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Dialing Properties > "Dialing Properties" Tab

The dialing properties are required for the correct resolution of phone numbers in canonical format (see Chapter 17, "Canonical format").



Local Country Code:

Format: No leading zeros, up to four digits.

Example: **49** for Germany.

Local Area Code:

Format: No leading zeros, up to 21 digits.

Example: **89** for Munich.

Local District Code:

Phone number of the company network.

Format: No leading zeros and no extension numbers, up to 21 digits.

Example: **7007** for Unify Munich Hofmannstraße.

Only available for devices in the optiPoint family.

Min. local number length

Minimum length of the local number.

Operator Code(s)

The operator number. You may enter multiple numbers separated by commas.

Initial digit(s) for extensions

List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly.

Example: If, the extensions 3000-5999 are configured in OpenScape Voice, each number will start with 3, 4, or 5. Therefore, the digits to be entered are **3, 4, 5**.

International Dial Prefix:

National prefix.

Format: Up to four digits.

Example: **00** in Germany.

National Dial Prefix:

International prefix.

Format: Up to five digits.

Example: **0** in Germany.

External Access Code:

Number for trunk seizure for an outgoing external call.

Format: Up to five digits.

Examples: **0**, **74**, **9** (USA).

Local Enterprise Node:

Call number of the company network.

Example: **7007** for Unify Munich Hofmannstraße.

Only available for devices in the OpenStage family.

Emergency number(s)

You may enter multiple emergency numbers separated by commas.

Expect Dial Number

When enabled, you’re allowed to dial frequently used prefixes by entering just one digit.

Disabled by default.

Internal Numbers Dial Form

Possible options:

- **Local Company Format**
- **Always Add Node**
- **Use External Number**

External Numbers Dial Form

Possible options:

- **Local Public Format**
- **National Public Format**
- **International Public Format**

Dial needs Access Code

Possible options:

- **Not used**
- **For External Number**

Dial needs International Gateway Code

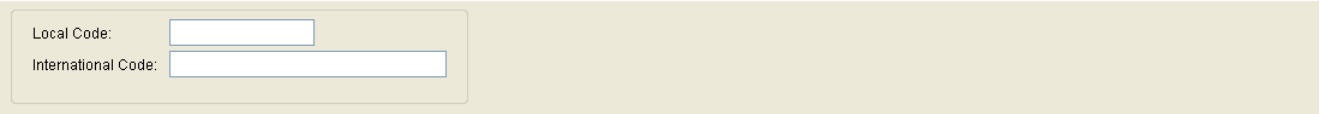
Possible options:

- **Use National Code**
- **Unchanged**

8.1.7.2 "Canonical Dial Lookup" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Dialing Properties > "Canonical Dial Lookup" Tab

This function transforms the entries in the first field ("Local Area Code") on the basis of a particular digit string as specified in the second field ("International Dial Code"). This digit string can be a national or international dial prefix, for example. This allows you to dial frequently used prefixes by entering just one digit.



Local Code

Digit or short digit string which can be used for dialing a particular prefix, for example.

International Code

Digit string, such as, a prefix, that is dialed at the beginning of the dialing operation using a particular digit.

8.1.8 Time Parameters

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Time Parameters

This area features the following components:

- General Data
- Possible Action Buttons
- "Time" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.1.8.1 "Time" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Time Parameters > "Time" Tab



Date format:

Format for date entry. Manual entry is only necessary if this information is not automatically transmitted (for example, PBX or DHCP server).

Possible options:

- **DD.MM.YY**
  Example: 05.10.06 for 5.10.2006
- **YY-MM-DD**

  Example: 06.10.05 for 5.10.2006
- **MM/DD/YY**

  Example: 10/05/06 for 5.10.2006
- **DD/MM/YY**

  Example: 05/10/06 for 5.10.2006

Time Format:

Time format.

Possible options:

- **12 hour**
- **24 hour**

8.1.9 Audio Settings

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Audio Settings

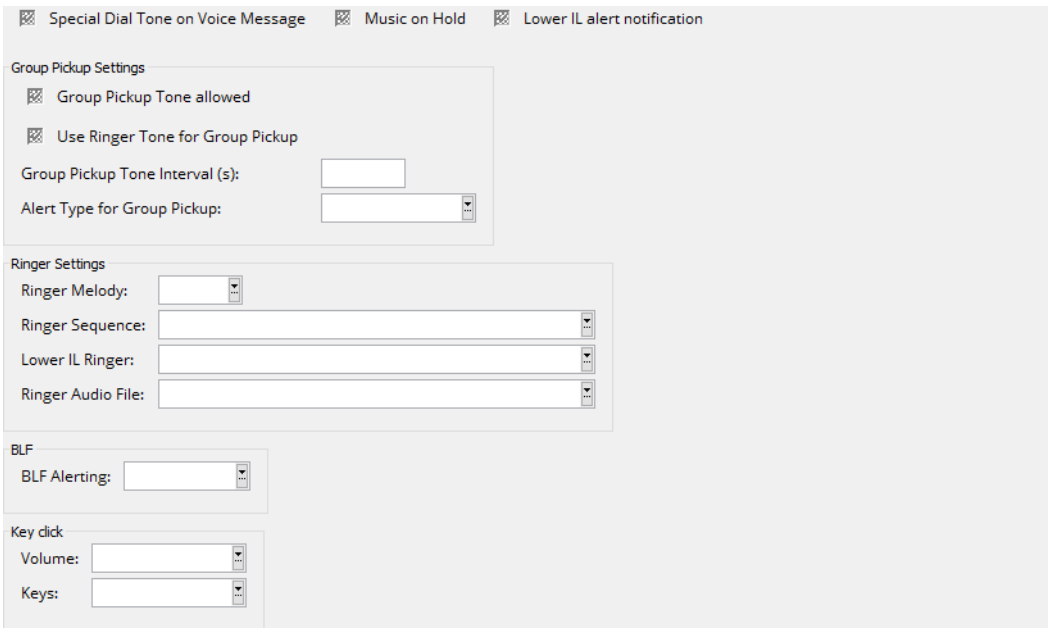
This area features the following components:

- General Data
- Possible Action Buttons
- "Audio Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.1.9.1 "Audio Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Audio Settings > "Audio Settings" Tab



Special Dial Tone on Voice Message

Check box for activating a special dial tone if a voice message is received.

Music on Hold

If this checkbox is activated, the phone will play music to a caller when he is put on hold.

Group Pickup Settings

Group Pickup Tone allowed

Activates or deactivates the generation of an acoustic signal for incoming pickup group calls.

Use Ringer Tone for Group Pickup

If this is checked, a pickup group call will be signaled by a short standard ringtone. If unchecked, a pickup group call will be signaled by an alert tone.

Group Pickup Tone interval (s)

A configurable repeat timer, the group pickup tone is repeated whilst there is a group pickup call available to the phone to pick up.You should be able to configure the interval between playing the Group pickup tone between 0 and 30 seconds, where 0 means the tone is played continuously.

Value range: **0...30** seconds

Default: **15** seconds

> ***NOTE:*** Only applies when the group pickup audio is set to be a tone, not when it is set to be a ringer.This feature is only available to OpenScape Desk Phone CP devices (version V1R4).

Alert type for Group Pickup:

Defines the user action required to accept a pickup call.

Possible Options:

- **Prompt**
  An incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.
- **Notify**
  An incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.
- **FPK only**

  An incoming pickup call is signaled at the corresponding function key only. To accept the call, the user must press the function key.

Ringer Settings

Ringer Melody:

Possible Options: see Section 7.1.12.3, "Ringer Melody:"

Ringer Sequence:

Possible Options: see Section 7.1.12.3, "Ringer Sequence:"

Lower IL Ringer:

Name of the file that contains the distinctive ringtone to be used in place of the normal ringer for calls from a Lower Impact level.

Ringer Audio File

Name of the file that contains the ringtone.

BLF Alerting

- **Beep**
- **Ring burst:** phone plays ringer tone for a few seconds when any of the monitored phones starts ringing.
- **Ring continuous:** phone plays ringer tone whilst any of the monitored phones is ringing**.**

Key click

Volume

Defines the volume of key clicks.

Possible Values:

- **Off**
- **Low**
- **Medium**
- **High**

Keys

Defines which keys shall have audible clicks.

Possible Values:

- **Keypad only**
- **All keys**

8.1.10 Applications

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications

This area features the following components:

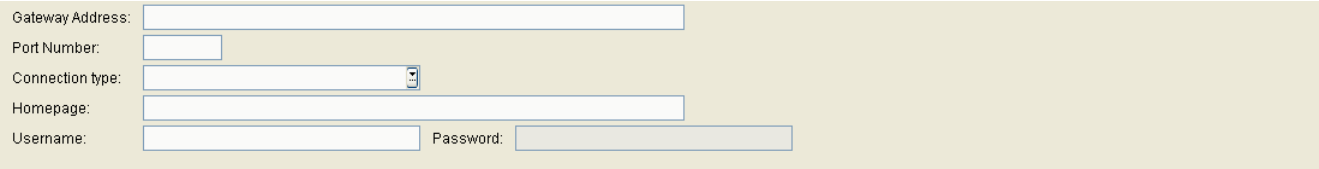
- General Data
- Possible Action Buttons
- "WAP" Tab
- "Java" Tab
- "XML Applications" Tab
- "Application List" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.10.1 "WAP" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "WAP" Tab



Gateway Address:

IP address or host name of the WAP server.

Port Number:

Port number of the WAP server.

Connection type:

Protocol type for connection to the WAP server.

Possible options:

- **HTTP**
- **WSP**

Homepage:

URL of the welcome page where the WAP homepage is located.

Username

User ID for identification at the WAP server.

Password:

Password for the user ID.

8.1.10.2 "Java" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "Java" Tab



Java Midlets

Downloading of Java Midlets allowed

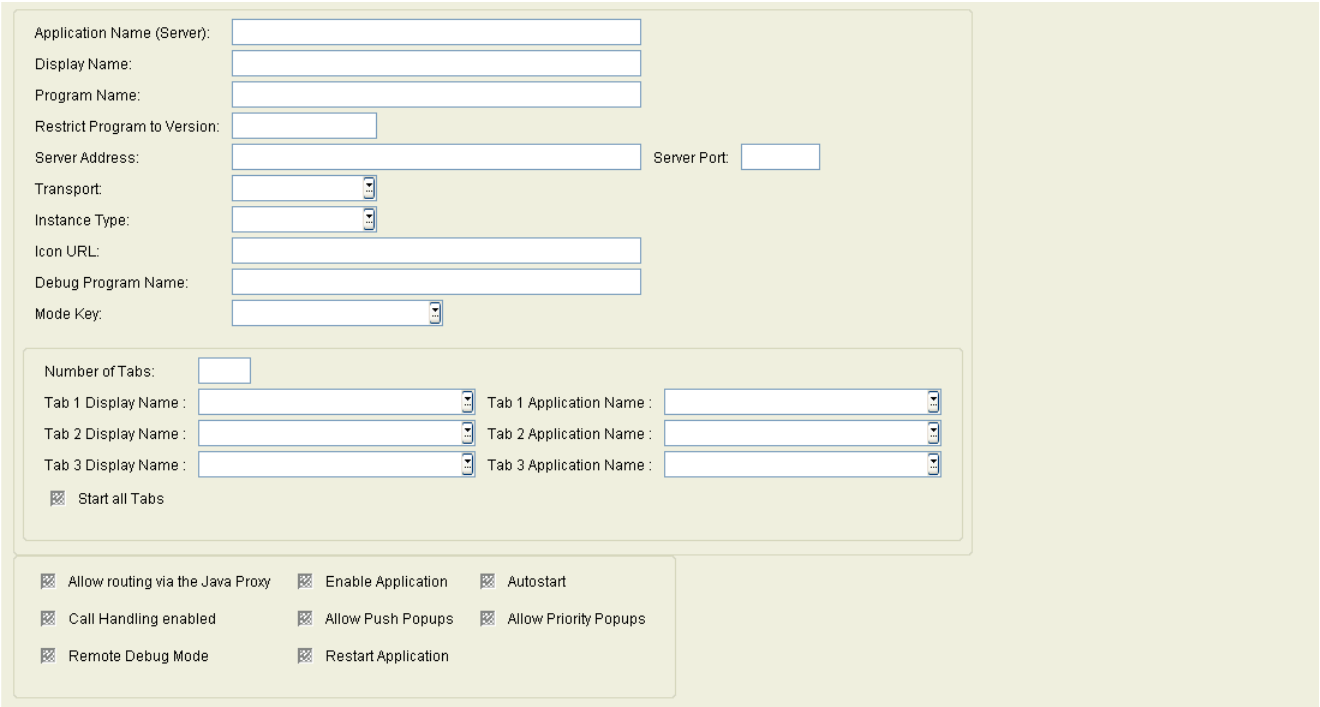
If this check box is activated, you can download Java midlets to the workpoint.

Java Midlet signature verification required

If this check box is activated, Java midlets must be verified using a signature.

8.1.10.3 "XML Applications" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "XML Applications" Tab



For information on XML applications, please refer to Section 7.1.14.4, ""XML Applications" Tab"

XML Applications

Application Name (Server):

This name is used internally by the workpoint software to identify the application.

Display Name:

This name is used for listing the application on the workpoint menu.

Program Name:

Path of the start file of the server-side program, relativ to the server address.

Restrict Program to Version:

Select a distinct version the application is working with.

Server Address:

IP address of the server, on which the program is running.

Example: **192.168.1.150**

Server Port:

Port used by the server-side program for receiving data from the workpoint.

Examples: **80** (Apache default port); **8080** (Tomcat default port).

Transport:

Transport protocol used for transmitting XML data.

Possible options:

- **HTTP**
- **HTTPS**

Instance Type:

Selection of the type of instance.

Possible options:

- **Normal**
- **Xpressions**
- **Phonebook**

Icon URL:

URL of the application icon (not yet implemented).

Debug Program Name:

Name and, where applicable, directory path of the program on the server that receives error messages from the terminal's *.XML application platform.

Mode Key:

Select a mode key to start the application.

Possible options:

- **No Mode Key**
- **Phonebook Mode Key**
- **CallLog Mode Key**
- **Messages Mode Key**
- **Help Mode Key**

Number of Tabs:

The number of embedded tabs within the XML application to be shown on phone display.

Value range: **0** ... **3**

NOTE: For an XML-application with a number of Tabs > 0, one of the entries between **Tab 1 Application Name** and **Tab 3 Application Name** must be set to the same value as the **Application Name (Server)** that it is associated with. When the XML application is started, the tab which has the same name as the XML application is the tab that initially gets focus.

Tab 1 Display Name:

Labeling displayed on the 1st tab header.

Tab 2 Display Name:

Labeling displayed on the 2nd tab header.

Tab 3 Display Name:

Labeling displayed on the 3rd tab header.

Tab 1 Application Name:

The name used by the XML application to identify the application running under the 1st tab. The name must be unique over all XML-applications.

Tab 2 Application Name:

The name used by the XML application to identify the application running under the 2nd tab. The name must be unique over all XML-applications.

Tab 3 Application Name:

The name used by the XML application to identify the application running under the 3rd tab. The name must be unique over all XML-applications.

Start all Tabs

On application start, all tabs will be opened.

Allow routing via the Java Proxy

Switch to allow routing via the Java Proxy.

Enable Application

Switch to enable application.

Autostart

Switch to enable autostart of application.

Call Handling enabled

Switch to enable call handling.

Allow Push Popups

Switch to enable pushing of popups.

Allow Priority Popups

Switch to enable priority popups.

Remote Debug Mode

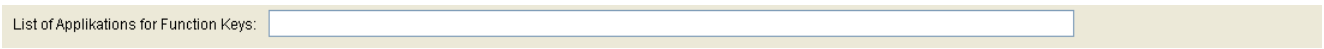
Switch to enable setting of remote debug mode.

Restart Application

Restart Application, if it is already running.

8.1.10.4 "Application List" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Applications > "Application List" Tab



List of Applications for Function Keys

Comma-separated list of names for applications, which can be started by means of Function Keys.

8.1.11 Service Integrations

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations

This area features the following components:

- General Data
- Possible Action Buttons
- "LDAP Settings" Tab
- "LDAP Attributes" Tab
- "Exchange" Tab
- "Circuit" Tab

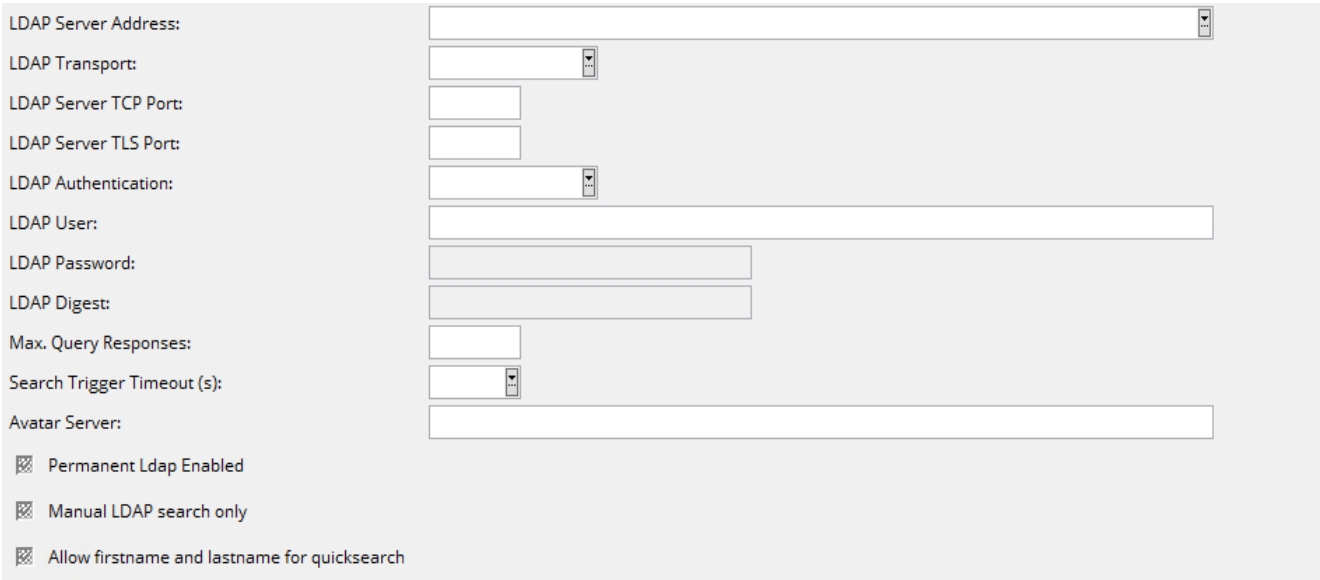
For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination")

> ***IMPORTANT:*** In order to employ LDAP data (or any other File Deployment contents,e.g logo,ringtone,screensaver) the mobile user must be logged on.

8.1.11.1 "LDAP Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > "LDAP Settings" Tab



LDAP Server Address:

IP address or host name of the LDAP server.

LDAP Server Port:

Port number of the LDAP server.

LDAP Transport:

Transport protocol used to transmit LDAP data.

Possible options:

- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

LDAP Authentication:

Option for selecting the LDAP access.

Possible options:

- **Anonymous**
- **Simple**

LDAP User:

User name for authenticated LDAP access.

LDAP Password:

Password for authenticated LDAP access.

LDAP Digest:

Enter LDAP Digest

Search Trigger Timeout (sec):

Search Trigger Timeout for LDAP simple search.

Possible options:

- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **60**

Avatar Server:

Server name (FQDN ή IP Address).

This is valid for mobile users that logon to CP200/CP400/CP600 phones of V1R2 version and higher.

Permanent Ldap Enabled:

Enable LDAP server permanently.

Manual LDAP search only:

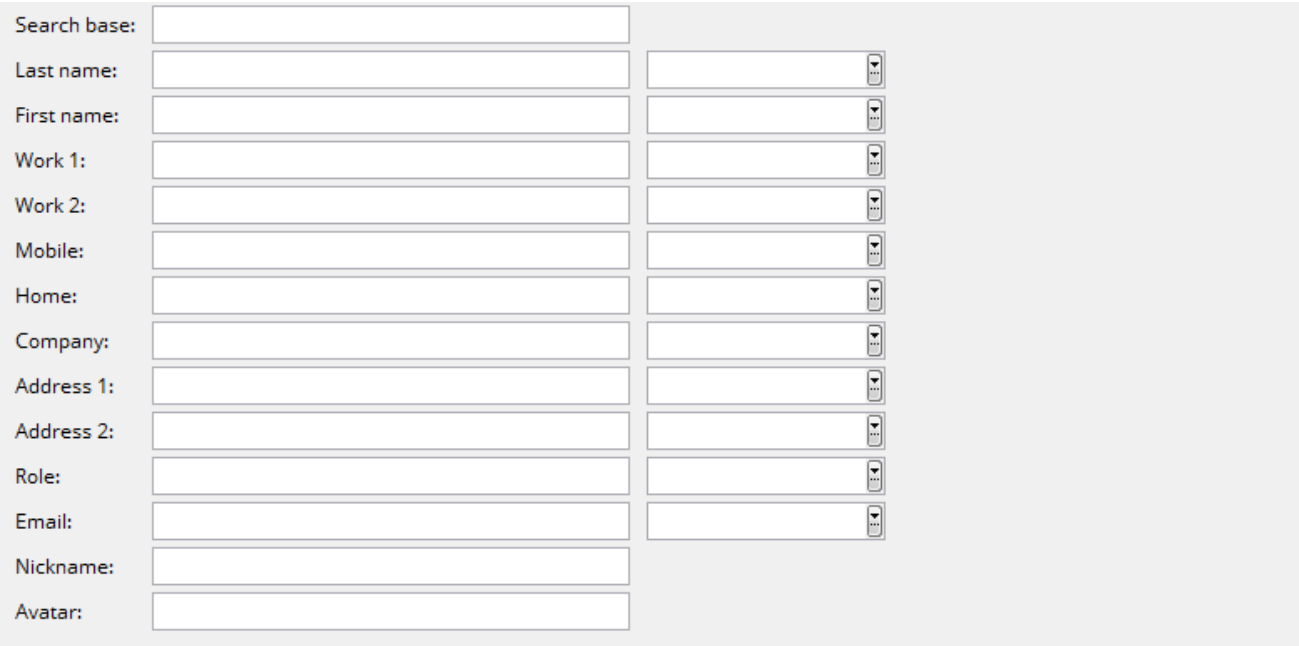
Select this option to allow manual LDAP search on incoming and outgoing calls.

Allow firstname and lastname for quick search:

Search for firstname and lastname.

8.1.11.2 "LDAP Attributes" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > "LDAP Attributes" Tab



NOTE: This is valid for mobile users that logon to CP200/CP400/CP600 phones of V1R2 version and higher.

Search Base:

This is the definition of the base point within the LDAP Directory for searches. This is relative to the initial node in the directory at the point of initial connection. For some LDAP servers, this could be an empty string.

Last Name:

Last name contact field.

First Name:

First name contact field.

Work 1:

Business 1 contact field.

Work 2:

Business 2 contact field.

Mobile:

Mobile contact field.

Home:

Sets the Private contact field.

Company:

Sets the Company contact field.

Address 1:

Sets the Address 1 contact field.

Address 2:

Sets the Address 2 contact field.

Role:

Sets the Job function contact field.

Email:

Email contact field.

Nickname:

Indicates that Simple search should use nickname mode. The Attribute field does not relate to a contact field and so the field value is not shown by the phone.

Avatar:

Full address of the web-server that holds avatar images.

8.1.11.3 "Exchange" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > "Exchange" Tab



Address

Microsoft Exchange server address.

Username:

Microsoft Exchange username credentials.

Password

Microsoft Exchange user password.

8.1.11.4 "Circuit" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > "Circuit" Tab



Address

Microsoft Exchange server address.

Username:

Microsoft Exchange username credentials.

Password

Microsoft Exchange user password.

8.1.11.5 E/A Cockpit " Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > E/A Cockpit " Tab



E/A Cockpit Server Address:

IP or FQDN (prefixed or not with https://) or IP:port (default https port is 8443)

Allow Server Push:

Allow push requests from the E/A Cockpit Application server.

Mobility logoff action:

This item handles the action taken by the CP phone during SIP Mobile logoff.

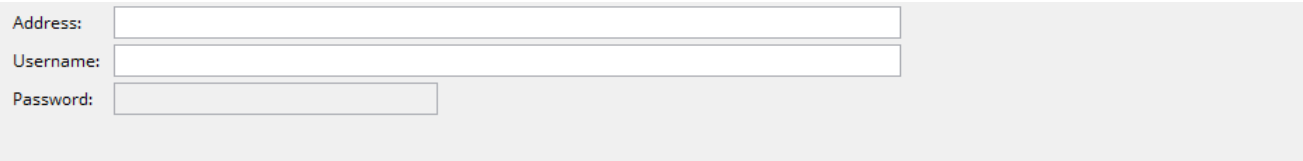
Possible values:

- **None**
  No action is taken**.**
- **Unavailable**
  An assistant will be set to OFF_DESK, an executive will be set to TO_ASSISTANT_XXX (xxx depends on a different executive related setting)
- **To Voicemail**
  If a voicemail number is configured in the E/A cockpit profile.
- **To Mobile**
  If a mobile number is configured in the E/A cockpit profile.
- **To Number**
  If a to-number is configured.

> ***IMPORTANT:*** When a SIP mobile user, having E/A cockpit configured, logs off and has the mobility logoff action set to anything except **None**, the E/A cockpit application on the phone will set the state according to **Unavailable**.

8.1.11.6 ’’OpenScape UC Connection" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > ’’OpenScape UC Connection" Tab



This tab offers OpenScape Desk Phone synchronization with the OpenScape UC Web Client using the OpenScape UC client API.

> ***IMPORTANT:*** Available only for CP400 / CP600/ CP 600 E HFA phones of version V1R1 and higher.

Address:

UC Server address.

Username:

User name.

Default: **""**

Password:

UC password.

8.1.11.7 ’’Name Update Sources" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Service Integrations > ’’Name Update Sources" Tab



This tab offers an interface where you are able to control if call party names are updated and which source is used to update them.That way, you have full control of name updates in one place.

Name Update sources:

Possible values:

- **No Master Source**
- **LDAP**
- **UC Directory**
- **LDAP and UC Directory**
- **Signalling**
- **LDAP and Signalling**
- **UC Directory and Signalling**
- **LDAP,UC Directory and Signalling**

8.1.12 User Settings

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings

This area features the following components:

- General Data
- Possible Action Buttons
- "Locks" Tab
- "Locked Configuration Menus" Tab
- "Locked Local Functions" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.12.1 "Locks" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings > "Locks" Tab



Function Keys locked

Check box for locking function keys on the Mobility Phone for a Mobile User.

Configuration Menus locked

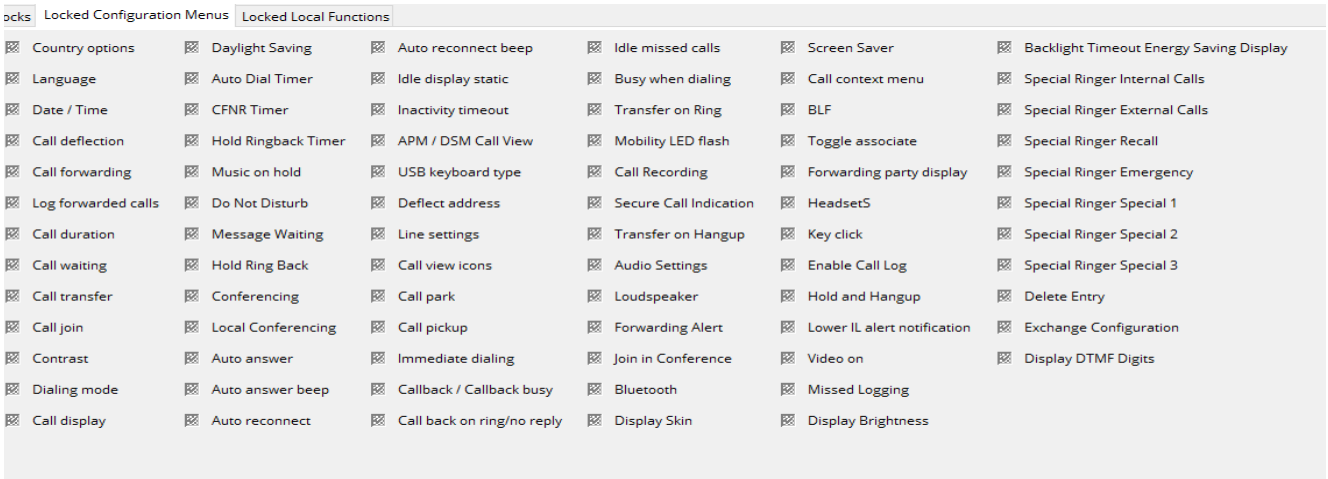
Check box for locking configuration menus on the Mobility Phone for a Mobile User.

Local Function Menus locked

Check box for locking local function menus on the Mobility Phone for a Mobile User.

8.1.12.2 "Locked Configuration Menus" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings > "Locked Configuration Menus" Tab



The following functions can be locked for the Mobile User in the configuration menus by activating the relevant check box:

1-Country options

The user can select a country from a list to adapt the phone to country specific conditions.

2-Language

The user can set the language for the administration and user menu.

3-Date / Time

The user can set the local time, the current date, and the daylight saving time.

4-Call deflection

The user can activate or deactivate call deflection.

5-Call forwarding

The user can activate or deactivate call forwarding.

6-Log forwarded calls

The user can activate or deactivate the logging of forwarded calls.

7-Call duration

The user can determine whether the call duration is indicated on the display.

Only available in optiPoint workpoints.

8-Call waiting

The user can determine whether a second call is allowed during a connected call. If not, the caller hears the busy tone.

9-Call transfer

The user can allow call transfer.

10-Transfer call

The user can enable or disable the posibility to interlink an active and a held call.

11-Contrast

The user can set the contrast for the display.

12-Dialing mode

The user can determine whether a number only or, alternatively, a name can be used for dialing.

Only available in optiPoint workpoints.

13-Call display

The user defines which information about the caller is displayed on an incoming call.

Only available in optiPoint workpoints.

14-Daylight Saving

The user can set the daylight saving time.

15-Auto dial timer

The delay time between the entry of the last call number digit and the start of the dialing process can be set by the user.

16-CFNR timer

The user can set the delay time that passes before a call is forwarded, if Call Forwarding on No Reply is activated.

17-Hold ringback timer

The user can set the time delay, after which the workpoints indicates that there us a held call.

18-Music on hold

The user can determine whether the music on hold stored in the phone is used. If music on hold is activated, it is played as soon as the phone is put to hold.

19-Do not disturb

The user can determine whether Do Not Disturb is available on the phone. If Do Not Disturb is active, the phone will not ring on an incoming call, and the caller will hear the busy tone.

20-Message waiting

The user can determine whether new messaes in the mailbox are signaled by a LED.

Only available in optiPoint workpoints.

21-Hold ring back

If this function is active and a participant has been put to hold, a signal sounds after a configurable time to remind that a call is on hold. The user can allow this function and set the delay time for the acoustic signal.

22-Conference

The user can allow system based conferences.

Only available in optPoint workpoints.

23-Local conference

The user can allow local 3-party conferences.

32-Auto answer

The user can determine whether incoming calls are accepted automatically by the CTI application which is connected to the phone.

33-Auto answer beep

The user can determine whether a signal will sound when a call that is accepted automatically by the CTI application connected to the phone.

34-Auto reconnect

The user can determine whether a held call can be reconnected automatically by the CTI application.

35-Auto reconnect beep

The user can determine whether a signal will sound when a held call is reconnected by the CTI application.

36-Idle display static

The user can configure the indication of system messages in idle state.

Only available in optiPoint workpoints.

38-Inactivity timeout

The user can set the delay time between the last entry and the return to the idle state.

39-APM / DSM Call View

The user can activate or deactivate the call view on the optiPoint application module.

40-USB keyboard type

The user can modify the language of the USB keyboard connected to an optiPoint phone.

Only available in optiPoint workpoints.

43-Deflect address

The user can enter resp. modify the target number for call deflection.

44-Line settings

The user can modify the settings of a line key.

45-Call view icons

The user can determine whether messages on the optiPoint display module, like, for instance, the list of missed calls, are displayed as text or symbols.

46-Call park

The user can allow call parking.

47-Call pickup

The user can allow pickup of a parked call.

48-Immediate dialing

The user can allow immediate dialing.

49-Callback / Callback busy

The user can activate the transmission of a callback request to the system. With OpenStage V3 onwards, the callback request can be transmitted in every case; with other end devices, this is only possible in busy case.

50-Call back on ring/no reply

The user can activate the transmission of a callback request to the system in case a call is not replied.

Only available in OpenStage workpoints.

51-Idle missed calls

The user can activate missed calls notifications on the display.

Only available on optiPoint workpoints.

52-Busy when dialing

The user can determine whether incoming calls are refused while a call number is entered.

53-Transfer on Ring

The user can determine whether a call is transferred as soon as the third participant’s phone rings, even if the transferring participant has not hung up.

54-Mobility LED flash

The user can determine whether the mobility key LED flashes during data exchange between phone and DLS, like, for instance, while mobility logon and logoff.

Only available in optiPoint workpoints.

55-Call Recording

The user can activate call recording.

Only available in optiPoint workpoints.

56-Secure Call Indication

The user can determine whether an alert tone shall indicate an insecure speech connection.

57-Transfer on Hangup

The user can determine whether, when one call is active and another call is on hold, the user can connect these calls by hanging up.

60-Audio Settings

The user can modify settings like ringtones and room character.

Only available in OpenStage workpoints.

61-Loudspeaker

The user can activate or deactivate handsfree talking.

Only available in OpenStage workpoints.

62-Forwarding Alert

The user can allow forwarding alert.

63-Join in Conference

The user can determine whether visual or acoustical warning notifications indicate an incoming call while call forwarding is active.

Only available in OpenStage workpoints.

64-Bluetooth

The user can activate or deactivate bluetooth connectivity.

65-Display Skin

The user can choose the display theme.

Only available in OpenStage 60/80 workpoints.

66-Screensaver

The user can activate the phones’s screensaver and set the delay time for starting the screensaver.

Only available in OpenStage 60/80 workpoints.

67-Call context menu

The user can define the displayed menu.

Only available in OpenStage 60/80 workpoints.

68-BLF

The user can define how an incoming call for the phone supervised by the BLF key shall be displayed.

69-Toggle associate

The user can enable or disable the connecting of a first call and a second call by going on-hook. When "Toggle associate" is activated, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook.

Available in all OpenStage workpoints.

70- Forwarding party display

For multiple forwarding, the user can determine whether the first forwarding party or the last forwarding party is displayed.

Available in all OpenStage SIP workpoints.

71- Headset

The user can define the type of headset connected to the phone.

Available for OpenStage 40/60/80 SIP/HFA.

72- Key klick

The user can define the mode of key klick on the phone.

Available for OpenStage 40/60/80 SIP/HFA.

73- Enable Call Log

The user can activate a list of missed,dialed,received or forwarded calls. The call log can be cleared via the WPI. Available for OpenStage 15/20/20E/40/60/80 SIP/HFA.

74- Hold and Hangup

Checkbox for activating the ’’ Hold and Hangup ’’ feature on non-keyset OpenStage phones.

This feature enables the user to temporarily hold and hang up a line without disconnecting your caller. This function in disabled by default.

75- Lower IL alert notification

The user is informed when an incoming call originated from a lower security zone, or when an outgoing call terminates in a lower security zone.

Available for OpenStage 40/60/80 SIP/HFA.

76- Video on

Checkbox for activating the ’’ Video Call ’’ feature on non-keyset OpenStage phones.

This feature enables the user to make video calls.

Available for OpenStage 60/80 SIP/HFA.

77- Missed Logging

The user can configure whether the calls completed elsewhere will be logged on phone.

Available for OpenStage 15/20/20E/60/80 SIP/HFA.

78- Display Brightness

79- Backlight Timeout Energy Saving Display

80- Special Ringer Internal Calls

The user can configure special ringers for Internal Calls at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

81- Special Ringer External Calls

The user can configure special ringers for External Calls at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

82- Special Ringer Recall

The user can configure special ringers for Recalls at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

83- Special Ringer Emergency

The user can configure special ringers for Emergency at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

84- Special Ringer Special 1

The user can configure his own special ringers (up to 3) at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

85- Special Ringer Special 2

The user can configure his special ringers (up to 3) at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

86- Special Ringer Special 3

The user can configure his own special ringers (up to 3) at mobile user level.

Available for OpenStage 15/20/20E/40/41/60/80 & OpenScape Desk Phones 35 G/ 35 G Eco / 55 G (SIP only).

87- Delete Entry

The user can configure whether to delete calls log entries in case there is a call to an entry in Missed calls list.

88- Exhange Configuration

The user can configure whether to setup an Exchange Server.

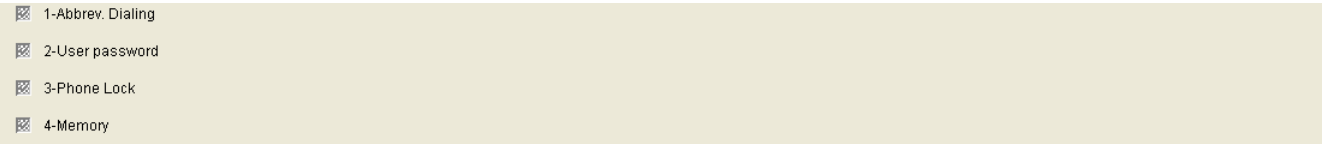
89- Display DTMF Digits

Checkbox for activating the display on the call screen of the DTMF digits pressed during an active call.

Only available in SIP workpoints.

8.1.12.3 "Locked Local Functions" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > User Settings > "Locked Local Functions" Tab



The following functions can be locked for the Mobile User in the configuration menus by activating the relevant checkbox:

1-Abbreviated dialing

The user can set up abbreviated dialing numbers.

Only available in optiPoint workpoints.

2-User password

The user can change his password.

3-Phone lock

The user can lock the phone. If the phone is locked, no unauthorized person can call from this phone in a regular manner or modify any settings. Only emergency numbers and pre-defined numbers from the dial plan can be dialed.

4-Memory

The user can delete all abbreviated dialing numbers and restore the factory settings.

Only available in optiPoint workpoints.

8.1.13 SIP Mobility

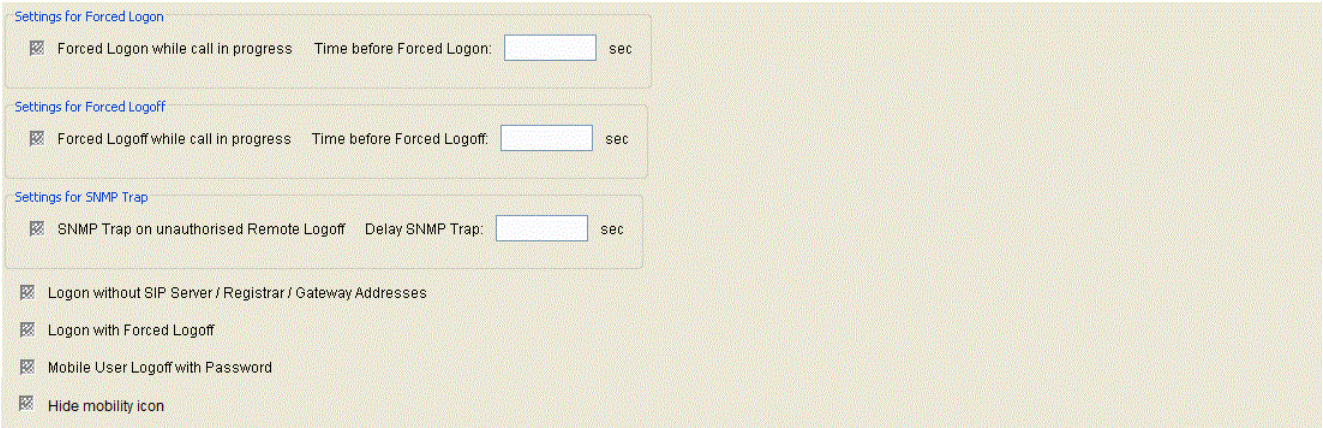
Call: Main Menu > Mobile Users > SIP Mobile User Configuration > SIP Mobility

This area features the following components:

- General Data
- Possible Action Buttons
- "Mobility Logon/Logoff" Tab
- "Mobility Data" Tab

8.1.13.1 "Mobility Logon/Logoff" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > SIP Mobility > "Mobility Logon/Logoff" Tab



Settings for Forced Logon

If the check box is active, the mobile user can be logged on to the device during the call. Logon is performed once the time entered in the field **Time before Forced Logon** has expired. If the check box is not active, attempted logon during the call is not forced even when the call has been completed. Forced logon must then be restarted.

Settings for Forced Logoff

If the check box is active, the Mobile User can be logged off from the device during the call. Logoff is performed once the time specified in the field **Time before Forced Logoff** has elapsed. If the check box is not active, attempted logoff during the call is not forced even when the call has been completed. Forced logoff must then be restarted.

Settings for SNMP Trap

If the check box is active, a message is sent to the SNMP server each time an unauthorized remote logoff is attempted. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

Logon without SIP Server / Registrar / Gateway Addresses

If this check box is active, the following data is not sent to the device when a mobile user logs on: SIP server address/port, SIP registrar address/port, SIP gateway address/port.

Logon with Forced Logoff

If this check box is active, Mobile User logoff is forced as soon as another user logs on to the device.

Mobile User Logoff with Password

If the check box is active, Mobile User logoff is only possible when the password of the currently logged-on Mobile User is entered.

Hide mobility icon

If the check box is active, mobility related icons in the status bar and menus will not be shown.

Time before Forced Logon

Time in seconds until forced logon takes place. This information is only relevant if the option **Forced Logon while call in progress** is activated. A value from 0 to 180 can be entered.

Time before Forced Logoff

Time in seconds until forced logoff takes place. This information is only relevant if the option "Forced Logoff while call in progress" is activated. A value from 0 to 180 can be entered.

Delay SNMP Trap

Time in seconds until the SNMP trap is sent. For information on entering SNMP server data, see Section 7.1.13.1, ""SNMP" Tab".

8.1.13.2 "Mobility Data" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > SIP Mobility > "Mobility Data" Tab



Number of changes for Medium Priority Data:

Defines how many changes to medium priority data may take place in the workpoint before this data is sent to the DLS.

Time before Medium Priority Data:

Defines the interval after which medium priority data that has been changed in the workpoint is sent to the DLS.

Time before High Priority Data:

Defines the interval after which high priority data that has been changed in the workpoint is sent to the DLS.

International Mobility ID

If this check box is activated, the device automatically adds the local country code to the extension, in addition to the trunk number and local area code when a mobile user logs on. The international code is configured under **Mobile Users** > **SIP Mobile User Configuration** > **Dialing Properties** > **"Dialing Properties" Tab** -> **International Dial Prefix**.

Example: The user logs on to the device using the extension/mobility ID "31434". If the check box is activated, the device sends the number "498972231434". Otherwise, the device sends the number "8972231434".

8.1.14 Keysets/Keylayout

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout

This area features the following components:

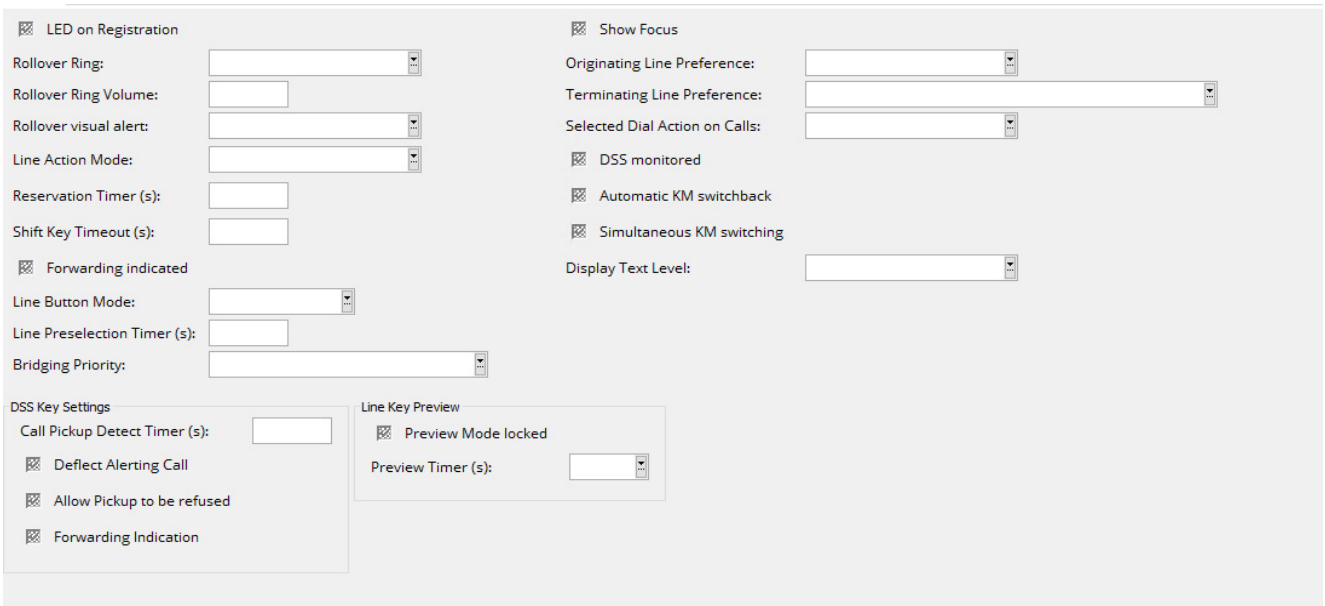
- General Data
- Possible Action Buttons
- "Keysets" Tab
- "Destinations" Tab
- "Send URL Server CA Certificate" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.14.1 "Keysets" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout > "Keysets" Tab



LED on Registration

Check box for activating the display when restarting the IP phone indicating whether the workpoint was registered successfully.

Only available in SIP workpoints.

Rollover Ring:

Type of alerting when busy.

Possible options:

- **No ring**
- **Alert Ring**
- **Standard**
- **Alerting**

Only available in SIP workpoints.

Rollover Ring Volume:

Volume of alerting when busy.

Only available in SIP workpoints.

Rollover visual alert:

Configure the visual alert for any incoming call rollover.

Possible options:

- **no indication**
- **visual alert**

NOTE: Available only for CP600 SIP devices, of version V1R3 and higher.

Line Action Mode:

Defines what should happen to a line (call) when a connection is established over another line.

Possible options:

- **Call hold**
  The original call is put on hold.
- **Release**
  The connection to the original call is cleared down (the call is ended).

Only available in SIP workpoints.

Reservation Timer:

Time in seconds indicating how long a line reservation can be maintained.

Default: 60 s.

Only available in SIP workpoints.

Shift Key Timeout (sec)

Duration of Shift key mode in seconds.

Forwarding indicated

Check box for activating alerting on a line key when call forwarding is active for its destination.

Only available in SIP workpoints.

Line Button Mode

Line Button functionality.

Possible options:

- **Single button**
  The action associated with the line key is executed as soon as the button is pressed, regardless of whether or not the handset is in the cradle.
- **Preselection**
  Press the line key to preselect a line. This line is used the next time you seize a line (by lifting the handset, for example).

Line Preselection Timer (sec)

Duration of line preselection in seconds.

Bridging Priority

Possible options:

- **Bridging overrides preview**
- **Preview overrides bridging**

Show Focus

Check box for activating the display showing which line is currently active (line has the focus).

Only available in SIP workpoints.

Originating Line Preference:

Defines the preferred line to be used for outgoing calls.

Possible options:

- **Idle line preference**

- **Primary line preference**
- **Last line preference**
- **No preference**

Only available in SIP workpoints.

Terminating Line Preference:

Defines the preferred line to be used for incoming calls.

Possible options:

- **Ringing line preference**
- **Calling line preference with prime line preferred**
- **Ringing line preference**
- **Ringing line preference with prime line preferred**
- **No preference**

Only available in SIP workpoints.

Selected Dial Action on Calls:

Defines the action to be performed when a Selected Dialing Free Programmable Key (FPK) is pressed during an active or held call.

Possible options:

- **No Action**
  The default option. No action will be performed.
- **Consult**
  The action will be a consultation transfer to the destination configured in the selected dialing key.
- **Transfer**
  The action will be a blind transfer to the destination configured in the selected dialing key.

Only available for CP600/ CP700 phones of version SIP V1R8 or later.

DSS monitored

Activate this checkbox to allow a DSS key to monitor the non-Keyset phone associated with the DSS key.

Automatic KM switchback

If this checkbox is activated the phone starts a 15 seconds timer, when the user has switched to a shifted level, and then switches to the non shifted level on the attached key modules.

Simultaneous KM switchback

Activate this checkbox to allow switch to the shifted level (or back to normal level) on every attached key module at the same time.

DSS Key Settings

Deflect Alerting Call

Check box for activating the "Deflect Alerting Call" feature.

Allow Pickup to be refused

Check box for activating the "Reject Group Pickup" feature.

Forwarding Indication

Checkbox for activating the forwarding indication.

Line Key Preview

Preview Mode locked:

Switch to lock preview mode

Preview Timer (sec)

Duration of preview mode in seconds.

Possible options:

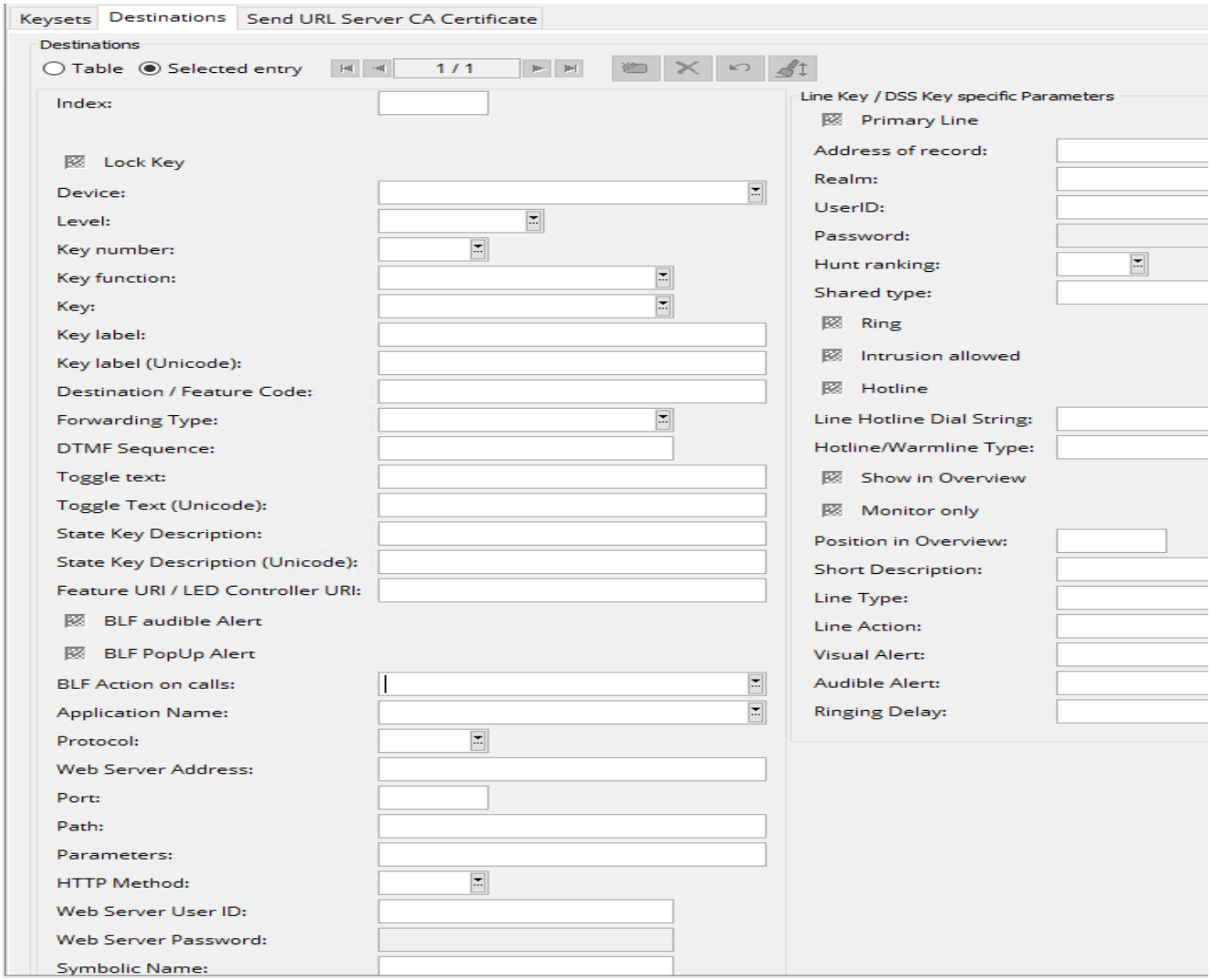
- **2**
- **3**
- **4**
- **6**

- **8**
- **10**
- **15**
- **20**
- **30**
- **40**
- **50**
- **60**

8.1.14.2 "Destinations" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout > "Destinations" Tab

NOTE: When creating a key layout, make sure that the key used by a mobile user for the primary line is available on all device types.
If the primary line is assigned to a key that does not exist on the device to which the mobile user is logged on, then there is no primary line key available to the mobile user. This can be avoided by entering the appropriate settings in the **SIP Mobile User Interaction** > **SIP User Keylayout** mask.



Index:

Name of the key layout function.

Lock Key

Locks the key for the user.

Device:

Specifies the device to which the relevant layout applies.

Possible options:

- **Base device**
- **1st Key module**
- **2nd Key module**
- **1st Self Labeling Key module**
- **2nd Self Labeling Key module**
- **OpenStage 15 Key module**

Only available in SIP workpoints.

Level:

Key level for the Shift functionality.

Possible options:

- **1. Level**
- **2. Level**
- **3. Level**
- **4. Level**
- **Fixed Keys**
  Fixed Keys are assigned to a fixed key number. They cannot be deleted or created on the IP Device.

Only available in SIP workpoints.

Key number:

Number of the key assigned the relevant function.

If **Level** "Fixed Keys" is selected, the following key numbers are fixed:

1 Fixed Keys - release

2 Fixed Keys - forwarding

3 Fixed Keys - voice dial

9 Fixed Keys - redial

Depending on the selected key number, **Key function** shows a selection of possible values.

Only available in SIP workpoints.

Key function:

The following key functions are supported:

- **Key unused**
- **Selected dialing**
- **Abbreviated dialing**
- **Repeat dialing**
- **Missed calls**
- **Voice messages**
- **Forwarding**
- **Loudspeaker**
- **Mute**
- **Ringer off**
- **Hold**
- **Alternate**
- **Blind Transfer**
- **Transfer call (OpenStage) / Join (optiPoint)**
- **Deflect**
- **Setup menu**
- **Room echoing**
- **Room muffled**
- **Shift**
- **Notebook**
- **Settings**

- **Phone lock**
- **Conference**
- **Local Conference**
- **Headset**
- **Do not disturb**
- **Group pickup**
- **Repertory dial**
- **Line**
- **Feature Toggle**
- **Show Phone Screen**
- **Swap screen**
- **Mobility**
- **Call park**
- **Call pickup**
- **Cancel/Release**
- **Ok Confirm**
- **Callback Request**
- **Cancel Callback**
- **Consultation (OpenStage) / Consult/Transfer (optiPoint)**
- **DSS**
- **State Key**
- **Call waiting**
- **Immediate Ring**
- **Preview Key**
- **Call Recording**
- **AICS Zip**
- **Server Feature**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **BLF**
- **Start Application**
  Available for free programmable keys as well as for ’Fixed Keys’.

- **Send URL**
  Available for free programmable keys as well as for ’Fixed Keys’.
- **Built-in Forwarding**
  Only available for ’Fixed Keys’.
- **Built-in Release**
  Only available for ’Fixed Keys’.
- **Built-in Voice Dial**
  Only available for ’Fixed Keys’.
- **Built-in Redial**
  Only available for ’Fixed Keys’.
- **Personal Directory/Start Phonebook**

  NOTE: The Personal Directory/Start PhoneBook function can also be set to the un-shifted /shifted FPK’s of OpenStage 15/20/40/60/80 & OpenScape Desk Phone IP 35G / 55 G Eco phones as well as to key modules.
  The key label “Start Phonebook” shall be used for the phone version prior to V3R3 and the key label “Personal” for higher phone version.
- **2nd Alert**
- **Corporate Directory**

  NOTE: The Corporate Directory function is configured to the V3R3 WP_HI & WP_LO phones.

Key:

Indicates whether this key is a ’Fixed Key’or a freely programmable key.

Key label:

A key label can be entered here for every function key in the case of Self labeling Keys workpoints (for example, optiPoint 420 standard).

Only available in SIP workpoints.

Key label (Unicode characters):

You can enter the key label in unicode characters for devices in the OpenStage family.

Destination / Feature Code:

Destination data to be dialed. This can be a digit string or a URL. Feature codes that need to be sent to external servers (not the SIP server at which the phone is registerd) have the following format:

<feature code>@<IP address>

Example: **123@10.2.54.2**

If the destination has been entered for the "Repertory dial" key function, extra control characters can be entered in a digit string:

- **$Q** = clear (CL)
- **$R** = consult (CS)
- **$S** = OK
- **$T** = Pause (PA)

Only available in SIP workpoints.

Forwarding Type:

Selection of situations when forwarding should be enabled.

Possible options:

- **on busy**
- **on busy external**
- **on busy internal**
- **on no reply**
- **on no reply external**
- **on no reply internal**
- **unconditionally**
- **unconditionally external**
- **unnconditionally internal**

Only available in SIP workpoints.

DTMF Sequence

DTMF Sequence for this target.

Toggle Text:

Text describing the server function selected with Feature Toggle.

Only available in SIP workpoints.

Toggle Text (Unicode characters):

Text in unicode describing the server function selected with Feature Toggle.

Only available on OpenStage devices.

State Key Description:

Description text for the state key.

State Key Description (Unicode characters):

Description text for the state key in unicode. Only available on devices in the OpenStage family (SIP version).

Feature URI / LED Controller URI

URI used to control this feature on the server.

BLF audible Alert

Audible Alert additional to busy lamp field.

BLF PopUp Alert

Additional to busy lamp field a message pops up in display.

Application Name:

Name of the application to be started with the function key.

Protocol

Protocol of Web Server.

Possible options:

- **HTTP**
- **HTTPS**

Web Server Address

Host name, domain name, or IP address of web server.

Port

Port number of web server: If the port is null, the fully qualified URL will not include the port element.

Path

Directory path and name of the program or web page.

Examples: **servlet/IppGenericServlet** or **webpage/checkin.xml**

The path should have a slash at the beginning and no slash at the end. If the slash at the beginning is missing, a slash will be automatically inserted. If there is an additional slash at the end, it will be automatically removed. The slashes in the path should be forward slashes (’/’). If backslashes (’\’) are used instead, the web server may not find the appropriate program or web page.

Parameters

Null, one, or more parameter-value pairs in the format “<parameter>=<value>”, with each pair separated by an ampersand (“&”), e. g. **parameter1=value1&parameter2=value2**. A comma (“,”) is not used as a separator because it could be part of the key or value. If the key or value contains an ampersand, it must be replaced by “&”.

The question mark will be automatically added between the path and the parameters. If there is a question mark at the beginning of the parameters, it will be automatically stripped off.

HTTP Method

HTTP method to be used.

Possible options:

- **Get**
- **Post**

Web Server User ID

User identity known by the server. This information is used for phone authentication by the server.

Web Server Password

Password known by the server. It is used for phone authentication by the server.

Symbolic Name

Symbolic name.

Push Support

Enables or disables push support.

Key Functionality

Possible options:

- **Toggle Call Forwarding**
- **Unspecified Call**
- **Unspecified**

ACD

ACD checkbox for the configuration of an AICS zip key function.

> ***NOTE:*** This flag is enabled only for the key function **AICS Zip** and for specific phones (CP 200 / 400 / 600, for SIP V1R2 and higher).

- If the phone has no AICS Zip keys and you try to add multiple AICS Zip keys, an error message is displayed:
  1121: It is not allowed to assign more than one key with the function 'AICS ZIP'.

- If the phone has one AICS Zip keys and you try to add one or multiple AICS Zip keys, an error message is displayed:
  1121: It is not allowed to assign more than one key with the function 'AICS ZIP'.

- If the phone has 2 or more AICS Zip keys and you try to add one or multiple AICS Zip keys, an error message is displayed:
  1185: It is not allowed to assign more than one key with the function 'AICS ZIP'. Reduce the number of AICS ZIP keys that you already have on the phone from X to 1. , where X is the number of AICS ZIP keys already on the phone.
- If the phone has no AICS Zip keys and you try to add one AICS Zip key,no error message is displayed
- If the phone has any number of AICS Zip keys and you try to add any key or keys (besides AICS Zip), provided that you don’t meet any other restrictions from these keys, no error message is displayed.

Line Key / DSS key specific Parameters

Primary line

Only available in SIP workpoints.

Address of record:

Only available in SIP workpoints.

Realm:

Entry of the SIP realm.

Only available in SIP workpoints.

UserID:

Only available in SIP workpoints.

Password:

Only available in SIP workpoints.

Hunt ranking:

Only available in SIP workpoints.

Shared type:

Possible options:

- **Private**
- **Shared**
- **Unknown**

Only available in SIP workpoints.

Ring

Only available in SIP workpoints.

Intrusion allowed

Check box for allowing intrusion.

Only available in SIP workpoints.

Hotline

Line Hotline Dial String:

Destination for the line hotline.

Only available in SIP workpoints.

Hot/Warm Line Type:

Possible options:

- **Ordinary**
- **Hot Line**
- **Warm Line**

Only available in SIP workpoints.

Show in Overview

Checkbox for activating the line display in the line overview.

Only available in SIP workpoints.

Monitor Only

Checkbox for setting the action of the DSS FPK when it is pressed to either Answer or Monitor. Default option is "**False**".

Possible options:

- **True**
- **False**

Only available in SIP workpoints.

Position in Overview

Position of key in Line Overview.

Only available in SIP workpoints.

Short Description:

Description of relevant line.

Only available on OpenStage devices.

Line Type:

Possible options:

- **normal**
- **direct**

Line Action:

Possible options:

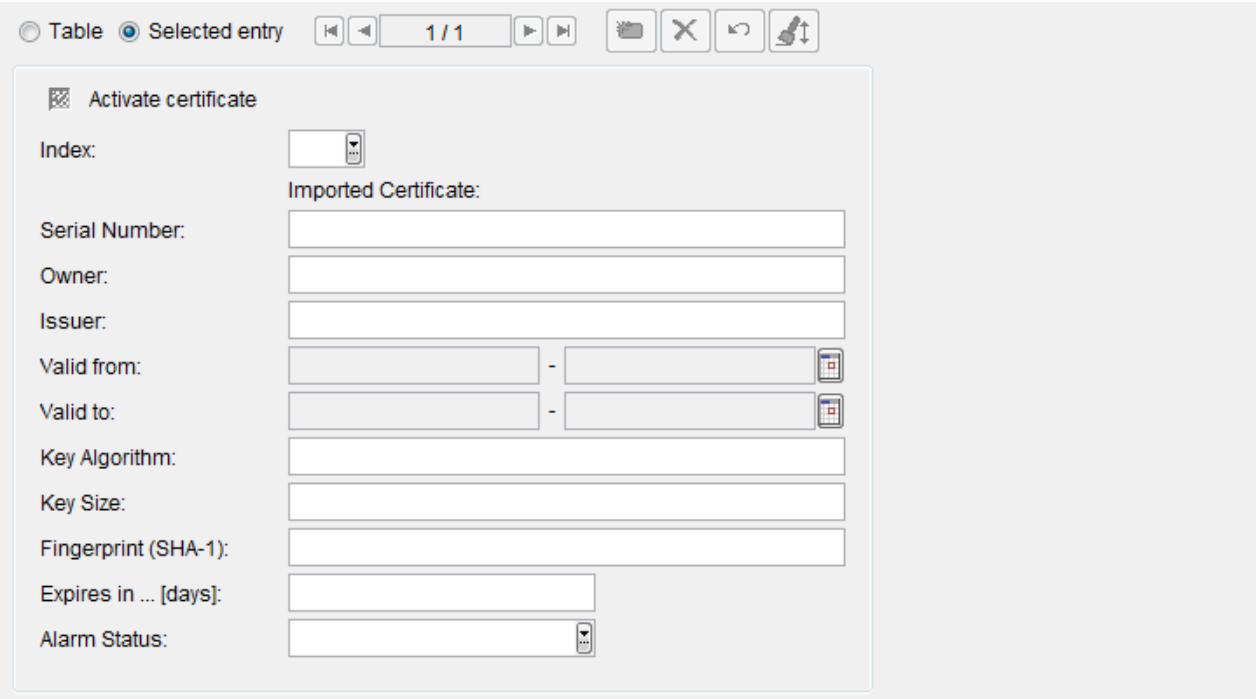
- **Consult**
- **Transfer**
- **No Action**

Ringing Delay:

Time before ringing starts for an alerting call.

8.1.14.3 "Send URL Server CA Certificate" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Keysets/Keylayout > "Send URL Server CA Certificate" Tab



Please refer also to **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Service Integrations** > **"LDAP CA Certificates" Tab**.

Activate certificate

The imported certificate will be activated with the next saving. By activating an empty certificate, the certificate at the end device will be deleted.

> ***IMPORTANT:*** This checkbox is an action checkbox and not an indication. This means that it does not show any current state. That is why it is sometimes grayed out or unchecked.

Index

Certificate index number.

Imported Certificate

Serial Number:

Serial number of the active or imported certificate (display only).

Owner:

Owner of the active or imported certificate (display only).

Issuer:

Issuer of the active or imported certificate (display only).

Valid from:

Start of validity for the active or imported certificate (display only).

Valid to:

End of validity for the active or imported certificate (display only).

Key Algorithm

Key algorithm.

Key Size

Key size.

Fingerprint (SHA-1):

Test algorithm **SHA-1** (160 bits/20 characters) for the security certificate.

Expires in ... [days]:

The certificate validity will expire in the number of days specified.

NOTE: The value of the imported certificate is updated periodically dependent on the settings in **Administration** > **Alarm Configuration** > **"Settings" Tab** > **Alarm Configuration for Expiring Certificates** > **Interval**. Therefore it might be greater than the value of the active certificate until the next update.

Alarm Status:

Current alarm status.

Possible values:

- **valid**
- **soon running out**
- **expired**

8.1.15 Signaling and Payload Encryption (SPE)

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Signaling and Payload Encryption (SPE)

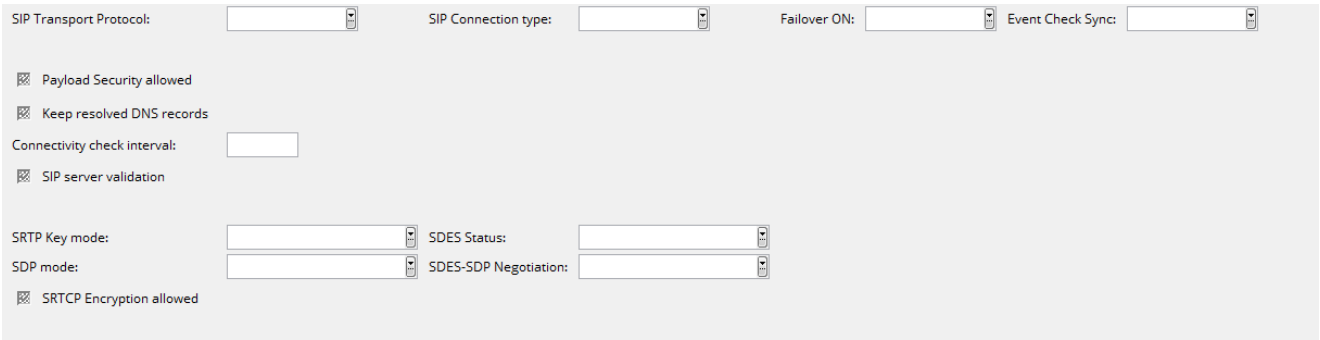
This area features the following components:

- General Data
- Possible Action Buttons
- "SIP Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.1.15.1 "SIP Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Signaling and Payload Encryption (SPE) > "SIP Settings" Tab



SIP Transport Protocol:

Protocol for SIP signaling.

Possible options:

- **UDP**
- **TCP**
- **TLS**

NOTE: **TLS** versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported.

SIP Connection Type:

Determines the connection type of the phone with main SIP server.

Possible options:

- **Persistent**

  Phone is always acting as connection client, no listening port gets opened to allow incoming connection attempts.

- **Listening**

Phone opens a listening port on the configured local SIP protocol.

Failover ON:

Determines the phone failover to the next SRV priority IP on 500/503 server responses so that users can continue to use their mobile phones on temporary issues.This functionality is available only to CP200 / CP400 / CP600 V1R2 devices and higher.

Possible options:

- **0 (Timeout only)**
- **1 (Timeout and Error)**

Default value: **0 (Timeout only)**.

Event Check Sync:

Enumeration value of "Event check-sync"

> ***NOTE:*** This item is available only for specific phones (CP 200 / 400 / 600/ 600 E, for SIP V1R2 and higher).

Possible options:

- **disabled**
  the phone will reject handling of check-sync events
- **challenge(default)**
  Default value, also current phone behavior. If digest authentication parameters are set, the phone will challenge the server for authentication
- **no challenge**
  the phone will never challenge the server for authentication

Payload security allowed

When activated, payload security is allowed.

Keep resolved DNS records

When enabled, previously resolved DNS records are kept in case of any DNS issues.

Connectivity check interval

Connectivity check interval in seconds.

SIP server validation

When activated, the TLS connection to the SIP server is validated.

SRTP Key mode

SRTP type(s) for secure calls. Identifies the type of SRTP that is allowed to be offered or accepted via SDP.

Possible values:

- **MIKEY**
- **SDES**
- **DTLS**
- **DTLS-SDES**

Default value is **DTLS-SDES**

SDP mode

SDP Negotiation mode for secure calls. Identifies the SDP capability tha configures whether fallback to RTP will be used and which BE-SRTP approach will be used.

Possible values:

- **RTP and SRTP (2mline)**
- **SRTP and RTP (2mline)**
- **SRTP only**
- **SRTP and RTP (1mline)**

Default value is set to **RTP and SRTP (2mline)**

SDES Status

Select the SDES status.

Possible options:

- **Disabled**
- **Enabled**

SDES-SDP Negotiation

Select the SDES-SDP negotiation.

Possible options:

- **SRTP and RTP**
- **SRTP only**
- **RTP and SRTP**

SRCTP Encryption allowed

When activated, SRCTP encryption will be applied.

8.1.16 Miscellaneous

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous

This area features the following components:

- General Data
- Possible Action Buttons
- "Country & Language" Tab
- "Messaging Services" Tab
- "SIP Error Notification" Tab
- "Display/Phone Settings" Tab
- "Help Internet URL" Tab
- "Phone Lock" Tab
- "Bluetooth Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

8.1.16.1 "Country & Language" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Country & Language" Tab



Country:

Country where the workpoint is operated.

Possible options:

- **AE - United Arab Emirates**
- **AF - Afghanistan**
- **AL - Albania**
- **AM - Armenia**
- **AR - Argentina**
- **AT - Austria**
- **AU - Australia**
- **AZ - Azerbaijan**
- **BA - Bosnia and Herzegovina**
- **BD - Bangladesh**
- **BE - Belgium**
- **BG - Bulgaria**
- **BO - Bolivia**
- **BR - Brazil**
- **BY - Belarus**
- **CH - Switzerland**
- **CI - Ivory Coast**
- **CL - Chile**
- **CM - Cameroon**
- **CN - China**
- **CO - Columbia**

- **CR - Costa Rica**
- **CR - Serbia**
- **CY - Cyprus**
- **CZ - Czech Republic**
- **DE - Germany**
- **DZ - Algeria**
- **DK - Denmark**
- **EC - Ecuador**
- **EE - Estonia**
- **EG - Egypt**
- **ES - Spain**
- **FI - Finland**
- **FR - France**
- **GB - Great Britain**
- **GE - Georgia**
- **GR - Greece**
- **GT - Guatemala**
- **HN - Honduras**
- **HK - Hong Kong**
- **HR - Croatia**
- **HU - Hungary**
- **ID - Indonesia**
- **IE - Ireland**
- **IL - Israel**
- **IN - India**
- **IR - Iran**
- **IT - Italy**
- **JO - Jordan**
- **JP - Japan**
- **KE - Kenya**

- **KG - Kyrgyzstan**
- **KR - Korea**
- **KW - Kuwait**
- **KZ - Kazakhstan**
- **LB - Lebanon**
- **LK - Sri Lanka**
- **LT - Lithuania**
- **LU - Luxembourg**
- **LV - Latvia**
- **MA - Morocco**
- **MD - Moldova**
- **MK - Macedonia**
- **MV - Maldives**
- **MX - Mexico**
- **MY - Malaysia**
- **NA - Namibia**
- **NG - Nigeria**
- **NI - Nicaragua**
- **NL - Netherlands**
- **NO - Norway**
- **NP - Nepal**
- **NZ - New Zealand**
- **OM - Oman**
- **PA - Panama**
- **PE - Peru**
- **PH - Philippines**
- **PK - Pakistan**
- **PL - Poland**
- **PT - Portugal**
- **PY - Paraguay**

- **RO - Romania**
- **RU - Russia**
- **SA - Saudi Arabia**
- **SE - Sweden**
- **SG - Singapore**
- **SI - Slovenia**
- **SK - Slovakia**
- **SV - El Salvador**
- **TH - Thailand**
- **TJ - Tajikistan**
- **TN - Tunisia**
- **TR- Turkey**
- **TM - Turkmenistan**
- **TZ - Tanzania**
- **UA - Ukraine**
- **US - United States of America**
- **UY - Uruguay**
- **UZ - Uzbekistan**
- **VE - Venezuela**
- **VN - Vietnam**
- **ZA - South Africa**
- **ZW - Zimbabwe**

Language:

Language to be used for local applications.

Possible options:

- **bg - bulgarian**
- **ca - catalan**
- **cs - czech**

- **da - danish**
- **de - german**
- **el - greek**
- **en_GB - english (GB)**
- **en_US - english (US)**
- **en - english**
- **es - spanish**
- **et - estonian**
- **eu- euskara**
- **fi - finnish**
- **fr - french**
- **hr - croatian**
- **hu - hungarian**
- **it - italian**
- **ja - japanese**

  NOTE: The Japanese language is valid only for CP400 & CP600 SIP phones of V1R2 version and higher.

- **lv - latvian**
- **mk - macedonian**
- **ms - malayan**
- **nl - dutch**
- **no - norwegian**
- **pl - polish**
- **pt - portuguese**
- **pt_Br - brazilian**
- **ro - romanian**
- **ru - russian**
- **sk - slovak**
- **sl - slovanian**

- **sr - serbian (cyrillic)**
- **sr_Latn - serbian (Latin)**
- **sv - swedish**
- **tr - turkish**
- **zh - chinese**

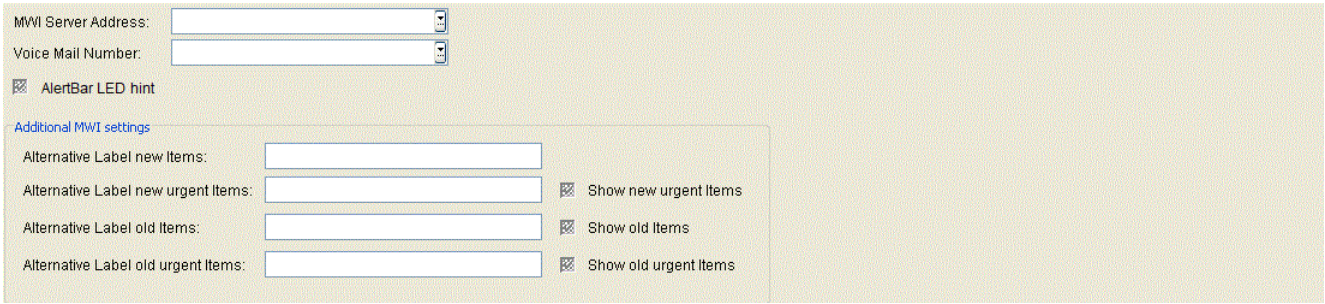
  NOTE: The Chinese language is valid only for CP400 & CP600 SIP phones of V1R2 version and higher.

- **ko- korean**

  NOTE: The Korean language is valid only for CP400 & CP600 SIP phones of V1R2 version and higher.

8.1.16.2 "Messaging Services" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Messaging Services" Tab



MWI Server Address:

IP address or host name of the MWI server.

Voice Mail Number:

Phone number of the voicemail system (message server).

AlertBar LED hint:

When this checkbox is activated, the red LED indicating new missed calls will be extinguished as soon as the user enters the Conversations menu.

Additional MWI settings

Show new urgent Items

Shows the count of new urgent messages.

Show old Items

Shows the count of old messages.

Show old urgent Items

Shows the count of old urgent messages.

Alternative Label new Items

Label for the count of new messages.

Alternative Label new urgent Items

Label for the count of new urgent messages.

Alternative Label old Items

Label for the count of old messages.

Alternative Label old urgent Items

Label for the count of old urgent messages.

8.1.16.3 "SIP Error Notification" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "SIP Error Notification" Tab



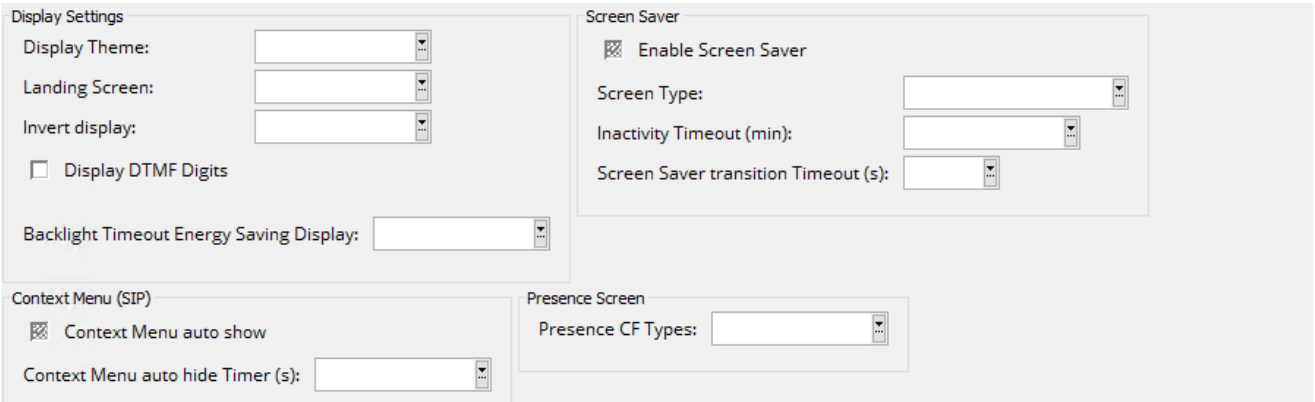
Beep on Error

Check box for activating acoustic error signaling during communication with Microsoft RTC.

Only available in SIP workpoints.

8.1.16.4 "Display/Phone Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Display/Phone Settings" Tab



Display Settings

Display Theme

Defines the layout of the graphical user interface on OpenStage phones.

Possible options:

- **Silver Blue**
- **Anthracite Orange**

Landing Screen

Set your Landing Screen.After that, you can easily get back to it, and after a (configurable) period of inactivity and on wake-up from slideshow or energy-saver (as appropriate), your phone shows the screen that you find most useful and ultimately suits you most.

NOTE: Available only to CP400/600 phones & of V1R4 version and higher.

Possible Options:

- **Conversations**
- **Favourites/Team**
- **Main Menu**

Invert display

Change the display to a dark background using color inversion.

Possible Options:

- **Normal Display**
- **Inverted Display**

Backlight Timeout Energy Saving Display

When a phone with energy saving display has been in idle state for a timespan longer than this value, the backlight is switched off.

NOTE: Valid only for IP Devices with **Display Backlight Type = CCFL** or **Display Backlight Type = LED**, see Section 7.6.1, "Inventory Data".

Possible Options:

- **1 min**
- **5 min**
- **30 min**
- **60 min**
- **2 hours**
- **3 hours**
- **4 hours**
- **5 hours**
- **6 hours**
- **7 hours**
- **8 hours**

Screensaver

Enable Screensaver

This check box enables the screensaver.

Screen Type

Select the Screen Type.

Possible Options:

- **Menu Screen**
- **Slideshow/ Date screen**

Inactivity Timeout (min):

Possible Options:

- **0(no timeout)**
- **1**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Screensaver transition Timeout (sec)

Time interval in seconds for changing the images.

Possible Options:

- **5**
- **10**
- **20**
- **30**
- **60**

Context Menu (SIP)

Context Menu auto show

When active, the context menu will be shown automatically.

Context Menu auto hide Timer (sec)

The context menu will be hidden after the timeout specified here, in seconds.

Possible Values:

- **No auto hide**
- **5**
- **10**
- **20**
- **30**
- **60**
- **120**

Presence Screen

Presence CF types

Allow showing the additional CF types to be configured by the phone user.

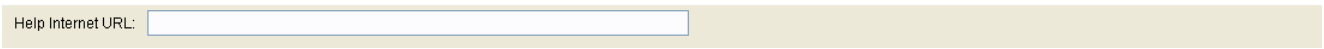
NOTE: Available only to CP400/600 devices of SIP V1R3 version and higher.

Possible Options:

- **Only all calls (default)**
- **All CF types**

8.1.16.5 "Help Internet URL" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Help Internet URL" Tab



Help Internet URL:

URL of the Web help page on the Internet containing information on the telephone.

8.1.16.6 "Phone Lock" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Phone Lock" Tab

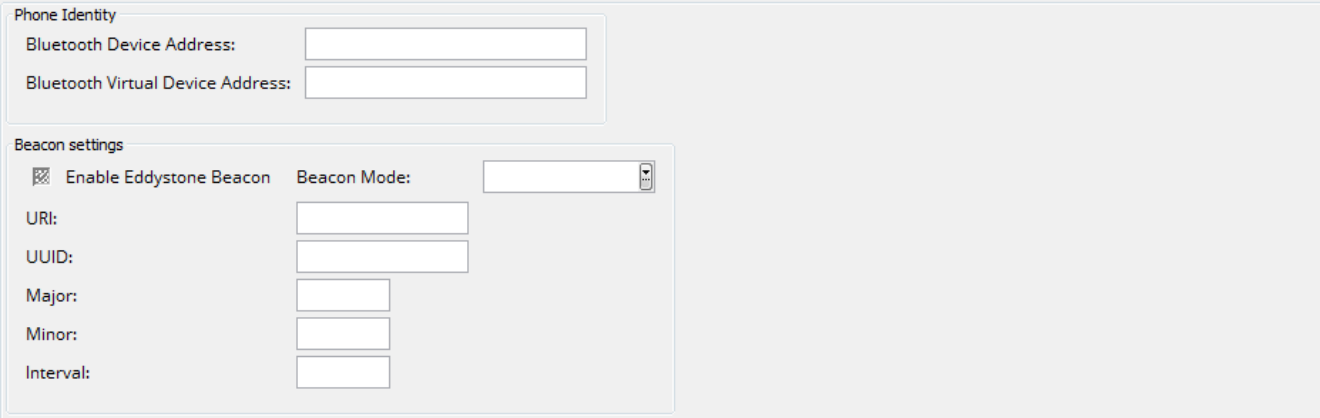


Lock Phone

Locks the phone.

8.1.16.7 "Bluetooth Settings" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > Miscellaneous > "Bluetooth Settings" Tab



NOTE: This is valid only for CP600 SIP phones of V1R2 version and higher.

Phone Identity

Bluetooth Device Address

Bluetooth Device Address

Bluetooth Virtual Device Address

Bluetooth Virtual Device Address

Beacon settings

Bluetooth beacons are hardware transmitters - a class of Bluetooth low energy (LE) devices that broadcast their identifier to nearby portable electronic devices. The technology enables smartphones, tablets and other devices to perform actions when in close proximity to a beacon.

Eddystone is a Bluetooth Low Energy beacon profile released by Google. The Apache 2.0-licensed, cross-platform, and versioned profile contains several frame types, including Eddystone-UID, Eddystone-URL, and Eddystone-TLM.For more info, refer to https://en.wikipedia.org/wiki/Eddystone_(Google)

Enable Eddystone Beacon

This checkbox controls whether the Bluetooth Low Energy mode is switched on or off.

It is disabled by default.

Beacon Mode

Beacon Mode controls whether the Bluetooth Low Energy Advertisement mode is switched on or off.

The **Both** option can be added, once it is verified that the parallel operation works flawlessly.

Disabled by default.

Available options:

- **Disabled**
- **Eddystone**

  NOTE: **Eddystone** will disable UUID, Major, and Minor configuration items
- **iBeacon**

  NOTE: **iBeacon** will disable URI and Interval configuration items
- **Both**

URI

This defines the content of the Eddystone user data URI.

Default value: **`https://unify.com`**

UUID

This defines the UUID broadcast in the iBeacon frame.

It is a 32 lowercase hexadecimal digits, traditionally displayed in five groups separated by hyphens, in the 8-4-4-4-12 form.

Major

Used by the iBeacon app to identify the beacon.

Values:**0-65535**

Default value: **0**

Minor

Used by the iBeacon app to identify the beacon.

Values:**0-65535**

Default value: **0**

Interval

Interval in which the Bluetooth Low Energy Advertisements are dispatched.

Default value:**1000** ms.

Available options:**20-10240** ms

8.1.17 File Deployment

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > File Deployment

This area features the following components:

- General Data
- Possible Action Buttons
- "Files" Tab

DLS supports the deployment of files such as LDAP Template, logos, ringtones and screensavers to mobile users automatically at the time of logon.

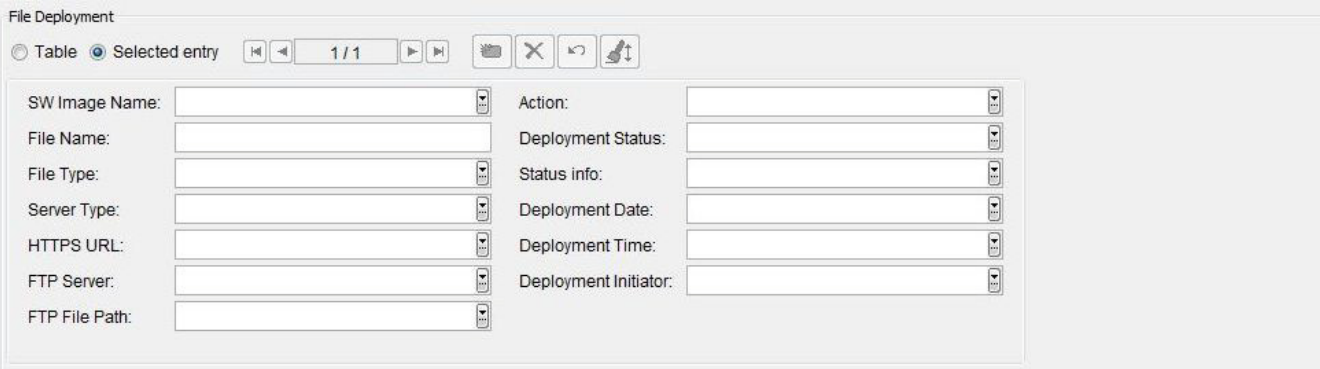
For each file deployment configuration the data stored includes all the information needed by DLS in order to make a file deployment request to a device (such as the file server address, the file name etc) as well as DLS specific data such as the result of file deployment request (initially empty).

After a mobile user logs on, DLS looks up into the new table in the DB - based on the E164 number of the mobile user - to see if there is any file deployment configured for this mobile user which has not been successfully completed already. If there is a pending file deployment (i.e. not already successfully completed in previous logons), DLS starts a new job to deploy the files and updates the result when file deployment finished in order to avoid deploying the same file again at the next logon.

> ***NOTE:*** When a mobile user is deleted, all the configured file deployment data and history data are deleted as well.

8.1.17.1 "Files" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Configuration > File Deployment > "Files" Tab



NOTE: LDAP Templates are also deployable to OpenStage 15/20 (SIP only) & OpenScape Desk Phone IP 35 G / 35 G Eco phones.

File Deployment

SW Image Name:

Name of the Software Image.

File Name:

Name of the file.

File Type:

Usage of the file.

NOTE: For many file types on the FTP server can be used for multiple purposes. In such cases, there is a table entry for each usage. For instance, a WAV file can be used as a ringtone and as music on hold. Ringtone and music on hold files must not exceed 1MB in size, while screensaver and logo files should not be larger than 300kB.

Example: **LOGO** (OpenStage 40/60/80) , **SCREENSAVER** (OpenStage 40/60/80).

Server Type:

Protocol used by the server which provides the file.

Possible values:

- **FTP**
- **HTTPS**

HTTPS URL:

URL of the software image, if a HTTPS server is used.

FTP Server:

ID of the FTP server that provides the file. This is necessary if a FTP server is used.

FTP File Path:

Path of the file, if a FTP server is used.

Action:

Indicates what is to be done with the file.

Possible values:

- **delete**
- **deploy**

Deployment Status:

Status of the deployment action.

Status info:

Information about the status.

Deployment Date:

Date of the latest file deployment.

Deployment Time:

Time of the latest file deployment.

Deployment Initiator:

Interface over which the deployment has been initiated.

Possible values:

- **DLS**
- **WBM**
- **Local**

> ***NOTE:*** The data for file deployment (but not the files themselves) are saved in the DLS DB as part of the mobile user data and deployed to the device with the first 'start-up' after logon.
> If the deployment is successful, DLS marks the file(s) as 'successfully deployed' in order not to deploy the same file again at the next logon. DLS shall support a history of up to 20 deployed files per mobile user including the date/time of deployment. Once a new file beyond the 20th is deployed, the oldest deployed file is removed from the list. if file deployment is unsuccessful, another attempt is made at the next user logon.

8.2 SIP Mobile User Interaction

In this area, you can configure, modify or delete mobile users. You can also log off mobile users, obtain information about logons and logoffs, create user data profiles, and define defaults for key layouts.

> ***NOTE:*** DLS also enables you to delete mobile users that are left in a forgotten log-on state (on a mobility enabled device) as well as logoff mobility enabled devices for which the mobile user has been deleted.

Call: Main Menu > Mobile Users > SIP Mobile User Interaction

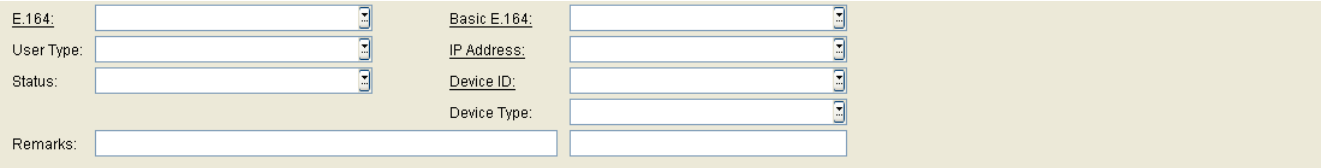
This menu consists of the following submenus:

- SIP Mobile User
- Logon/Logoff
- Automatic Logoff
- SIP User Keylayout
- Mobile User Response Test Settings

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is identical for the **SIP Mobile User** and **Logon/Logoff** interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of workpoints. The base data associated with the workpoints found is displayed in the **Object** view (no changes possible).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

E.164:

Complete E.164 phone number (Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

User Type:

Displays which type of data the remainder of the fields contain.

Possible options:

- **Mobility enabled Device**
  Mobility Phone data.
- **Mobile User**
  Mobile User data.

For more information on mobility, see Section 3.8, "DLS Mobility - General Information".

Status:

Displays mobility status.

Possible options:

- **Mobile User logged on**
  Mobile User data: a Mobile User is logged on.

- **Mobile User logged off**
  Mobile User data: no Mobile User is logged on.
- **Mobility enabled Device**
  Mobility Phone data: no Mobile User is logged on to the Mobility Phone.
- **Device used by Mobile User**
  Mobility Phone data: a Mobile User is logged on to the Mobility Phone.

For more information on mobility, see Section 3.8, "DLS Mobility - General Information".

Basic E.164:

E.164-Rufnummer des Mobility -Telefons.

Beispiel: **498972212345**

IP Address:

IP address of the workpoint.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

Physical MAC address of the workpoint.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for an entry in the database.

Clear Window

Deletes the contents of all fields in the **Search** view. This deletes all previous search criteria so you can enter new criteria.

Save

Saves the changes.

Discard

Discards any changes made.

Logon Mobile User

Logs a mobile user on to a mobility terminal.

If you click this button, a dialog window appears. The terminal’s E.164 phone number must be specified if a mobile user is selected in the general part of the mask. The mobile user’s mobility ID is entered if a terminal is specified in the general part.

Logoff Mobile User

Logs a mobile user off a terminal.

If a mobile user is selected in the general part of the mask, it will be logged off the terminal. If a terminal is selected, the mobile user logged on to it is logged off.

Reset Mobile User

To be used in case the end device cannot be reached by the DLS. The mobile user and the phone he is currently logged onto are set to "logged off" in the DLS database.

New

Creates a new Mobile User or a default Mobile User.

Migration to Mobile User

Migrate a Basic User to a Mobile User. See also Section 16.16.4.2, "Creating Mobile Users via Migration".

Migration to Device

Migrate a logged on Mobile User to a Basic User.

Refresh

Refreshes the window contents from the database.

Delete

Delete an object.

8.2.1 SIP Mobile User

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User

This area features the following components:

- General Data
- Possible Action Buttons
- "Mobile / Basic User" Tab
- "Archives Data" Tab
- "Response Test Settings" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

8.2.1.1 "Mobile / Basic User" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User > "Mobile / Basic User" Tab

NOTE: For an introduction to mobility, see Section 3.8, "DLS Mobility - General Information".

For information on mobility administration, see Section 16.16, "Configuring and Administrating Mobility".

For information on IP Client Mobility, see Section 16.16.13, "IP Client Mobility".



New Mobile User IDs:

E.164 call numbers of all Mobility phones for which a Mobile User is to be created. If there is more than one Mobility phone, the E.164 call numbers are entered comma-separated.

On clicking the button , a list of all available call numbers is displayed. From this table, you can select the desired numbers, similar to the multile selection in table view (see Section 5.4.2.4).

Mobile User Profile:

Selection of a Mobile User Configuration defined in **Profile Management** > **User Data Profile**.

NOTE: In the case where a device is contacting DLS with a user logged in already AND the user does not exist at the time the device contacts DLS, DLS creates the user automatically.
In that case an **@#####** profile name is assigned to the user (the mobile user call number is automatically entered with the prefix ''@'') .

Reapply:

Apply the Mobile User profile to the Mobile User again. On starting this function, the DLS user will be asked whether this should be done as a merge of the data or by replacing all user data by profile/ default data. If the merge option is chosen (click on "Yes"), those user parameters which are also configured in the profile are overwritten by the profile data. That user data which is not contained in the profile will not be touched. If, for instance, the profile contains additional keys, they will be added to the keys currently configured on the mobile user's phone; but in case of concurrent key definitions, the key definitions of the profile will overwrite those currently set on the phone.

If the replace option (click on "No") is chosen instead of the merge option, those user parameters which are also configured in the profile are overwritten by the profile data. That user data which is not contained in the profile will be overwritten with default values.

Mobile User Password:

With this password, the user can log on to the phone, both at the device itself and via the WBM (Web Based Manager).

Mobile User Home Phone

Allow automatic Logon at Home Phone

If this check box is activated, the Mobile User is logged on automatically to that Home Phone whose E.164 call number has been entered under **Home Phone**.

Allow Logon at Home Phone for all Mobile Users

If actived, all Mobile Users are allowed to log on at that home phone whose E.164 number has been entered under **Home Phone**.

Home Phone

E.164 number of the Home Phone assigned to this Mobile User.

Home Phone Status

Displays the current status of the Mobile User at the Home Phone.

Possible values:

- **Mobile User logged on at Home Phone**
- **Mobile User logged off from Home Phone**

Get SIP Registration Data from Virtual Devices

If this check box is activated, data for SIP access is taken from the corresponding plug&play configuration, that is, from the virtual device which has the same E.164 number as the newly created mobile user. The access data for the SIP server is located at **IP Phone Configuration** > **Gateway/Server**.

Get Keyset Data from Virtual Devices

This checkbox determines whether Keyset configuration of the respective virtual device will be inherited by the mobile user or not.If this check box is activated, data for Keyset attributes is taken from the corresponding plug&play configuration, that is, from the virtual device which has the same E.164 number as the newly created mobile user.

Tenant

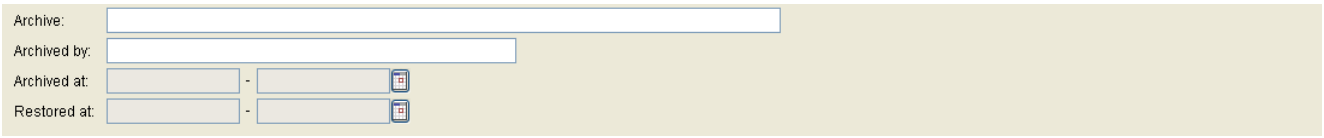
Name of the tenant the Mobile User belongs to.

8.2.1.2 "Archives Data" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User > "Archives Data" Tab

NOTE: For an introduction to mobility, see Section 3.8, "DLS Mobility - General Information".

For information on mobility administration, see Section 16.16, "Configuring and Administrating Mobility".



Archive:

Path for the ZIP archive file from the DLS system.

Archived by:

Name of the DLS user who created the archive.

Archived at:

Indicates the date and time of the archive.

Restored at:

Displays the date and time of the archive restore.

8.2.1.3 "Response Test Settings" Tab

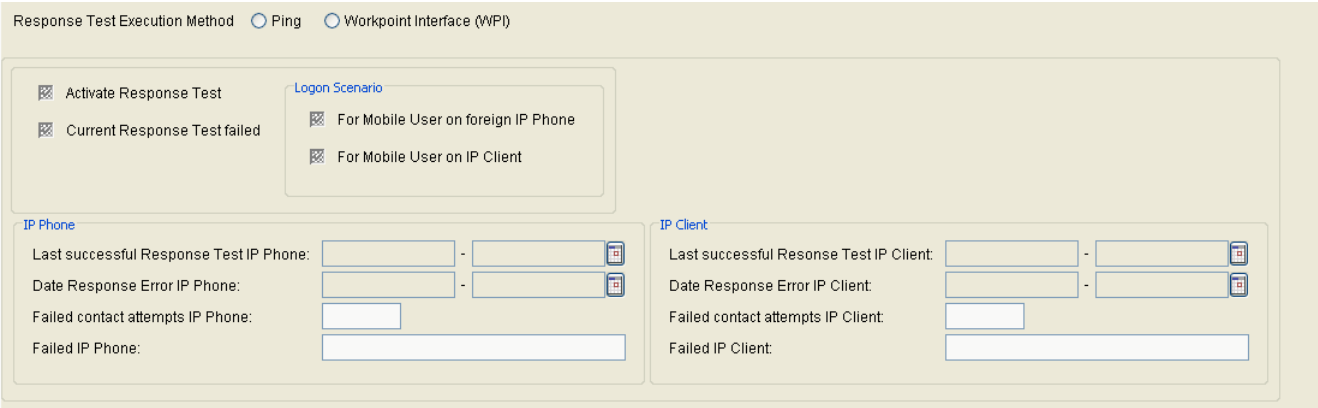
Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP Mobile User > "Response Test Settings" Tab

This functions checks if an IP Phone or IP Client to which a Mobile User is logged on is reachable by the DLS.

If the IP Phone or IP Client is unreachable according to the settings (see Section 8.2.5, "Mobile User Response Test Settings") and a Home Phone is assigned to the Mobile User, the Mobile User will be logged off from the current IP Phone or IP Client and logged on to the assigned Home Phone. This prevents the Mobile User from becoming unreachable.

A failled attempt means that within 10 minutes no conntact has been established. The Response Test failed, if the number of 'Failed contact attempt IP Phone' or 'Failed contatct attempt IP Client' is higher then the number of 'Response Test Retries' on mask 'Mobile User Response Test Settings'.

A contact attempt is considered to be failed when no contact could be established within 10 seconds. The respond test has failed when the counter **Failed contact attempts IP Phone** or **Failed contact attempts IP Client** is greater than the value of **Response Test Retries** in the mask **Mobile Users** > **SIP Mobile User Interaction** > **Mobile User Response Test Settings**.



Response Test Execution Method

- **Ping**
  The DLS tries to reach the IP Phone or IP Client via ping.
- **Workpoint Interface (WPI)**
  The DLS tries to reach the IP Phone or the IP Client via its workpoint interface by means of a ContactMe request. If the IP Phone or the IP Client sends a corresponding message, in which with the "ReasonForContact" parameter has the value "solicited", the test was successful. Otherwise, the test is considered failed.

Activate Response Test

Activates or deactivates the response test for this mobile user.

Current Response Test failed

If no contact could be established after 10 seconds, the error counter is incremented.

Logon Scenario

For Mobile User on foreign IP Phone

If activated, response tests are executed for a Mobile User at a foreign IP Phone, that is, at a phone which is not the Home Phone of this Mobile User.

For Mobile User on IP Client

If activated, response tests are executed for a Mobile User at an IP Client, that is, at an IP Client which is not the Home Phone of this Mobile User.

IP Phone

Last successful Response Test IP Phone

Date of the last successful response test for this IP Phone.

Time Response Test Error IP Phone

Date of the last failed response test for dieses IP Phone.

Failed contact attempts IP Phone

Number of failed contact attempts for this IP Phone.

Failed IP Phone

IP Address of the IP Phone that could not be reached.

IP Client

Last successful Response Test IP Client

Date of the last successful response test for this IP Client.

Time Response Test Error IP Client

Date of the last failed response test for this IP Client.

Failed contact attempts IP Client

Number of failed contact attempts for this IP Client.

Failed IP Client

IP address of the IP Client that could not be reached.

8.2.2 Logon/Logoff

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Logon/Logoff

This area features the following components:

- General Data
- Possible Action Buttons
- "History" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

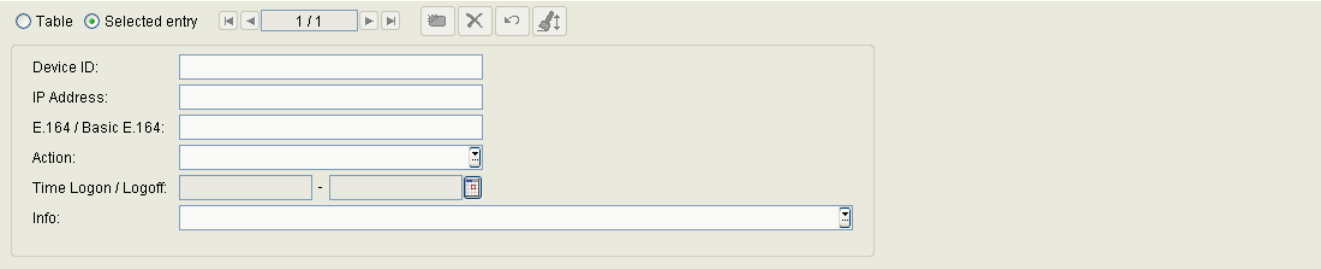
8.2.2.1 "History" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Logon/Logoff > "History" Tab

All successfull or failed actions concerning mobile users are logged here.

NOTE: For an introduction to mobility, see Section 3.8, "DLS Mobility - General Information".

For information on mobility administration, see Section 16.16, "Configuring and Administrating Mobility".



Device ID

Device ID of the Mobility Phone with which the action logged here has proceeded (display only).

IP Address

IP address of the Mobility Phone with which the action logged here has proceeded (display only).

E.164 / Basic E.164

E.164 and Basic E.164 of the Mobility Phone with which the action logged here has proceeded (display only).

Action

Type of action that took place (display only).

Possible entries:

- **Logon**
- **Logoff**

Time Logon/Logoff

Time of the logon, logoff or the failed attempt (display only).

Info

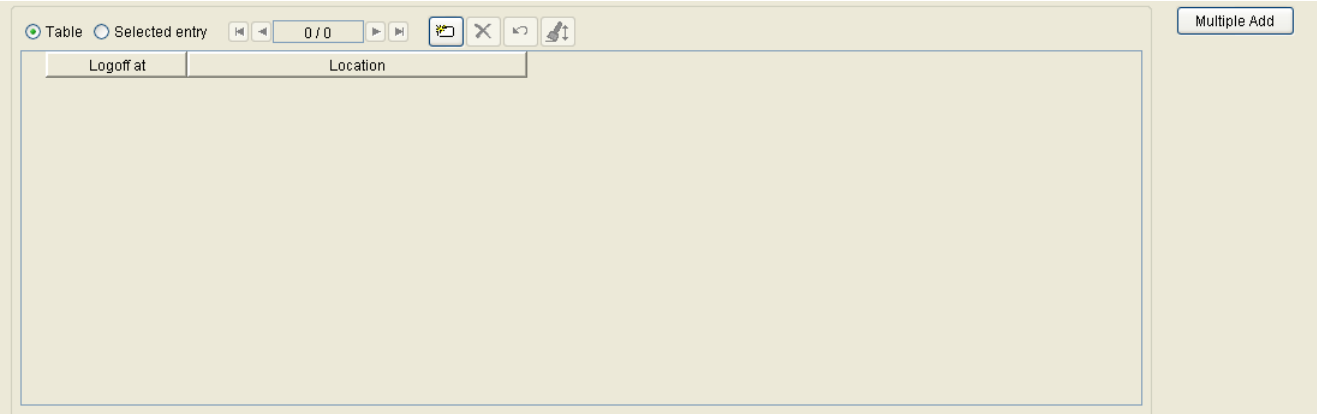
Additional information on the logon, logoff or the failed attempt (display only).

Possible entries:

- **Password or E.164 invalid**
- **Internal Error**
- **User logged in on another phone**
- **Second logon not permitted**
- **Forced logoff**
- **Forced logoff failed**
- **Forced logoff because of second logon**
- **Successful Logon**
- **Successful Logoff**
- **Forced logoff refused (phone busy)**

8.2.3 Automatic Logoff

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Automatic Logoff



This function enables the user to schedule a daily automatic logoff of all SIP mobile users for selected locations. This ensures e.g. that all devices are logged at start of work, and thus are available for SIP mobile users.

NOTE: Automatic Logoff is not allowed for Mobile Users logged on at their Home Phones.
Only when a mobile user is logged on at another device (besides its home phone) will be able to automatically log it off in order to return back to its home phone and by that ensure it will always be possible to contact.

NOTE: For affected Mobile Users considered as part of an Automatic Logoff **Location**, no individual jobs will be generated under **Job Control** while Automatic Logoff is executed.
Administrators will need to point under Mobile Users > SIP Mobile User Interaction > Logon/Logoff User Interface to look for the successful logoff completion state and time.

Logoff at:

Next daily logoff is scheduled on this time. The current time of the timezone defined for this location will be used.

NOTE: Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

Location

Location where automatic logoff will happen at entered time. Locations are entered as described under Section 6.3.2, "Location".

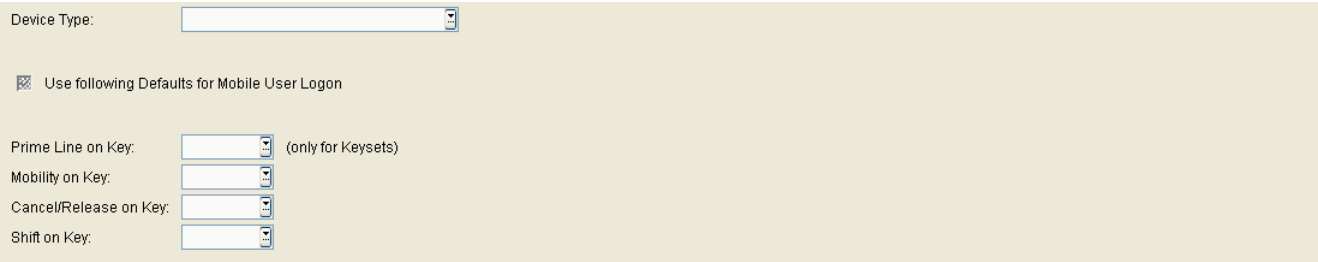
Multiple Add

Add multiple locations to one logoff time.

8.2.4 SIP User Keylayout

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > SIP User Keylayout

NOTE: The default key layout defined here can not be overridden instantly by changing a template and reapplying the relevant user data profile while the mobile user is logged on. However, the changes will be made after the mobile user has logged off and on again.



Device Type:

Select the device type for key layout.

Possible options:

- **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**

Use following Defaults for Mobile User Logon

Check box for activating the default setting specified below.

Prime Line on Key

Key number of the primary line key (only for phones on which the mobile user profile already has a primary line key).

Value range: **1 ... 19** or none.

Default: **5**

For OS60, the default key layout defines that position 5 is reserved for Prime Line. So, any change concerning that key will not be sent to the phone. It will be sent to the phone only when logging off and logging on again. Any change to other key or adding a new key on other position it will work successfully.

In order to overcome this issue, change the position of the Prime Line on the default key layout to position null.

Mobility on Key:

Number of the key where Mobility should be programmed.

Value range: **1** ... **19** or none.

Default: **10**

Release on Key:

Configure Cancel/Release key on key

Value range: **1 ... 19** or none.

Defaults:
optiPoint 410/420 economy/economy plus/standard: **11**
optiPoint 410 advance: **18**
optiPoint 420 advance: **17**

Shift on Key:

Number of the key where Shift should be programmed.

Value range: **1** ... **19** or none.

Defaults:
optiPoint 410/420 economy/economy plus/standard: **12**
optiPoint 410 advance: **19**
optiPoint 420 advance: **18**

Possible Action Buttons

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Refresh

Refreshes the content of the relevant page.

8.2.5 Mobile User Response Test Settings

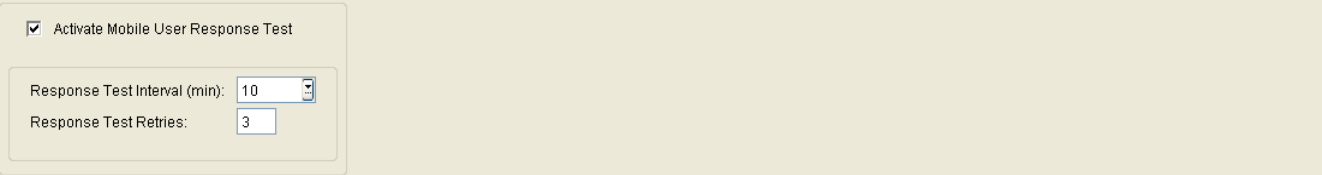
Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Mobile User Response Test Settings

Here, response tests for logged on Mobile Users can be displayed and managed. (See also Section 8.2.1.3, ""Response Test Settings" Tab")

This area features the following components:

- General Data
- Possible Action Buttons
- "Protocol" Tab

General Data



Activate Mobile User Response Test:

Central switch for activating or deactivating the Mobile User response tests.

Response Test Interval (min):

Interval in which the response tests will be performed, in minutes.

Possible Options:

- **10**
- **20**
- **30**
- **40**
- **50**
- **60**
- **90**
- **120**
- **240**

Default value: **30**

Response Test Retries:

Number of response test retries when no connection could be established.

Value range: **0** ... **9**

Default value: **5**

Mobile Users
SIP Mobile User Interaction

Possible Action Buttons

Save

Saves the changes.

Discard

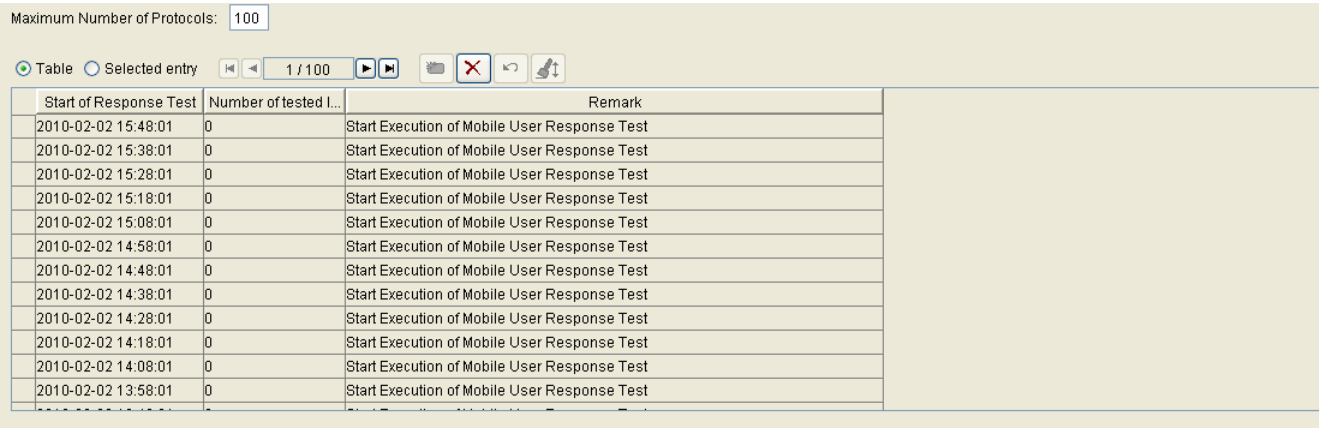
Discards any changes made.

Refresh

Refreshes the screen contents from the database.

8.2.5.1 "Protocol" Tab

Call: Main Menu > Mobile Users > SIP Mobile User Interaction > Mobile User Response Test Settings > "Protocol" Tab



Maximum Number of Protocols

At most as many protocol entries as specified here are created.

Start of Response Test

Date and time of response test start

Number of tested IP Devices

Number of IP Phones or IP Clients that have been tested.

Remark

Annotation about the particular protocol entry.

8.3 User Data Administration

In this area, Mobile User data are displayed and managed. These data are not modifiable via DLS, e. g. phonebook entries. The data are sent to the DLS for storage when a Mobile User is logging off; when a Mobile User is logging on, they are sent to the end device by the DLS.

The memory requirements for each Mobile User is displayed, as well as date, device ID, and IP address of the end device. Furthermore, the total amount of used memory can be determined.

The displayed user data can be deleted. This should only be done with deleted Mobile Users.

> ***NOTE:*** Export functionality on Mobility Users is not offered due to security / exposure reasons. Mobility User Data (e.g. call log) are not accesible by the DLS Administrator. They are stored/encrypted in the DLS Database.

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "Statistics" Tab

General Data

This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of IP phones. The base data associated with the IP phones found is displayed in **Object** view.



E.164:

Complete E.164 phone number (Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all registered IP phones that match the search criteria.

Clear Window

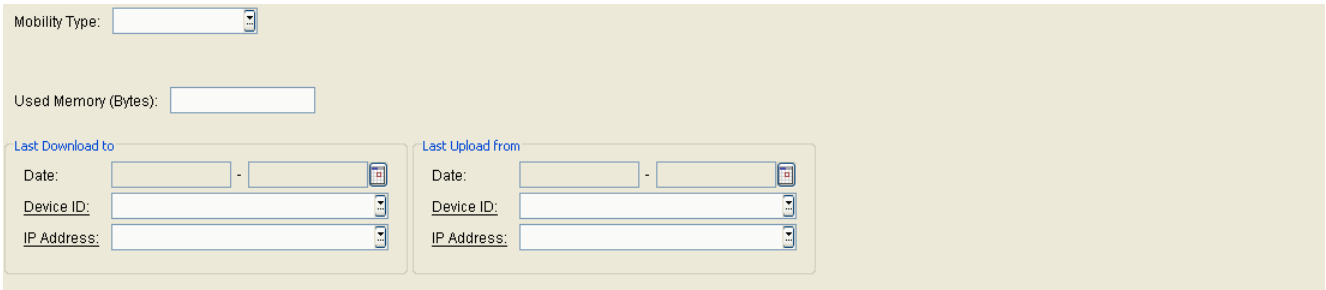
Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Determine overall Memory usage

By clicking this button, the total memory use of the user data stored in all workpoints can be determined.

8.3.1 "Statistics" Tab

Call: Main Menu > Mobile Users > User Data Administration > "Statistics" Tab



Mobility Type

Shows the mobility type (SIP or HFA Mobility).

Used Memory (Bytes):

Memory in bytes used by user data of this IP Device.

Last Download to

Date:

Date and time of the last sending of user data to the IP Device.

Device ID:

ID of the IP Device to which the user data have been sent.

IP Address:

IP address of the workpoint to which the user data have been sent.

Last Upload from

Date:

Date and time of the last saving of user data sent by the IP Device.

Device ID:

ID of the IP Device whose user data have been saved.

IP Address:

IP address of the IP Device whose user data have been saved.

8.4 Mobility Statistics

This area displays the mobility statistics. With its help, the administrator can overview all mobile users withinin a defined space of time. That way, e. g. periods of peak occupancy can be determined. For this purpose, the mobile user logon/logoff history is analyzed (see Main Menu > Mobile Users > SIP Mobile User Interaction > Logon/Logoff).

This menu item consists of the following areas:

- General Data
- Possible Action Buttons
- "SIP Mobility" Tab

General Data

This part of the contents area is identical for all interfaces associated with this menu. In **Search** view, it is used for entering parameters to find a specific group of statistics. In **Object** view, the base data associated with the statistics found is displayed, or the base data for a new statistics are defined.



Statistics:

Name of the statistics.

Begin:

Begin of the time interval in which actions are observed. If **Daily Statistics** is active, this field is read-only.

End:

End of the time interval in which actions are observed. If **Daily Statistics** is active, this field is read-only.

Last Update:

Creation date of the statistics currently displayed.

Periods:

Sets the period during the observation time interval. After the expiration of each period, an entry in the table is created.

Possible Options:

- **1 min**
- **2 min**
- **3 min**
- **4 min**
- **5 min**

- **10 min**
- **15 min**
- **20 min**
- **30 min**
- **1 h**
- **2 h**
- **3 h**
- **4 h**
- **6 h**
- **24 h**

Daily Statistics

The checkbox indicates whether the statistics currently displayed is a **Daily Statistics**.

Possible Action Buttons

Search

Searches for all statistics that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the Search view before new search criteria are entered.

Delete

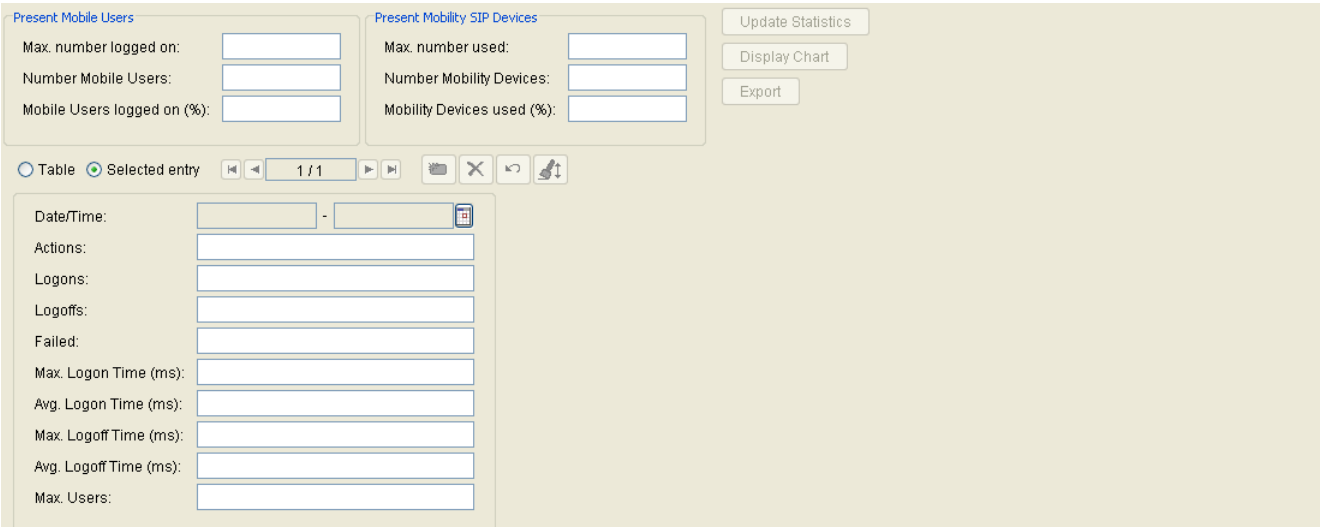
Delete the statistics currently displayed.

New

Creates new statistics.

8.4.1 "SIP Mobility" Tab

Call: Main Menu > Mobile Users > Mobility Statistics > "SIP Mobility" Tab



Present Mobile Users

Max. number logged on:

Maximum number of mobile users logged on at the same time within the observation time interval.

Number Mobile Users:

Number of mobile users extant within the observation time interval.

Mobile Users logged on (%)

Indicates the percentage of extant mobile users which have been logged on within the time interval.

Present Mobility SIP Devices

Max. number used:

Maximum number of mobility enabled SIP devices at which mobile users have been logged on within the observation time interval.

Number Mobility Devices:

Number of mobility enabled DIP devices extant at the end of the observation time interval.

Mobility Devices used (%):

Indicates the percentage of mobility enabled devices at which mobile users have been logged on within the observation time interval.

Update Statistics

If the date of **End** (of the observation time interval) is later than the date of **Last Update**, the statistics can be updated using this button. The button is inactive if the date of **Begin** and **End** are in the past.

Display Chart

Via this button, the content of the current statistics is displayed graphically.

Export

Via this button, the content of the current statistics is stored in a file in csv format. The file name will be requested in a dialog window.

Date/Time:

Time stamp with date and time at the beginning of the observation period. if, f. e., the period is set to 5 min, all successive values, actions etc. will be determined and entered in the table. At this, they are provided with the appropriate time stamp.

Actions:

Total number of actions within the period indicated.

Logons:

Number of logons within the period indicated.

Logoffs:

Number of logons within the period indicated.

Failed:

Number of failed actions within the period indicated.

Max. Logon Time (ms):

Maximum processing time for a logon within the period indicated in milliseconds.

Avg. Logon Time (ms):

Average processing time for a logon within the period indicated, in milliseconds.

Max. Logoff Time (ms):

Maximum processing time for a logoff within the period indicated, in milliseconds.

Avg. Logoff Time (ms):

Average processing time for a logoff within the period indicated, in milliseconds.

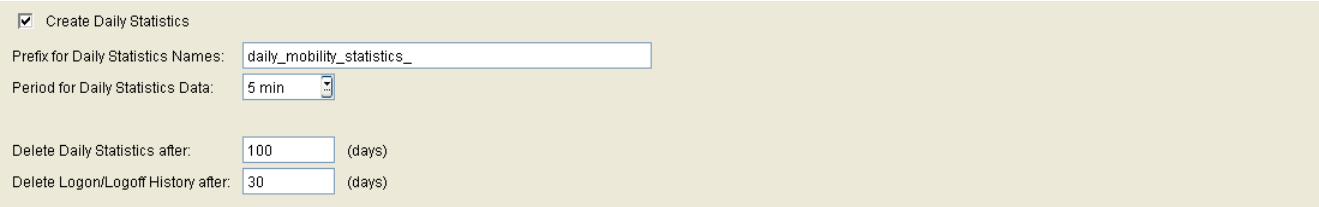
Max. Users:

Maximum number of mobile users logged on at the same time within the period indicated.

8.5 Mobility Statistics Configuration

Call: Main Menu > Mobile Users > Mobility Statistics Configuration

With this area, the daily mobility statistics (see Mobility Statistics) can be configured. The daily statistics are usually generated short after midnight. This is the time configuration changes get valid.



Create Daily Statistics

If this checkbox is active, a statistics according to the further parameters is created daily.

Prefix for Daily Statistics Names:

Name prefix for automatically created statistics.

Period for Daily Statistics Data:

Sets the period for the daily statistics. For each period, an entry is created in the table.

Possible Options:

- **1 min**
- **2 min**
- **3 min**
- **4 min**
- **5 min**
- **10 min**
- **15 min**
- **20 min**
- **30 min**
- **1 h**
- **2 h**

- **3 h**
- **4 h**
- **6 h**
- **24 h**

Delete Daily Statistics after:

Delete daily statistics after the number of days entered here. If 0 is entered, there will be no automatic deletion.

Delete Logon/Logoff History after:

Delete entries in the logon/logoff history after the number of days entered here. If **0** is entered, there will be no automatic deletion.

Possible Action Buttons

Save

Saves the configuration.

Discard

Discards previously unsaved modificationes in the configuration.

Refresh

Updates the display of the configuration from the database.

9 Gateways

Call: Main Menu > Gateways

This menu item consists of the following area:

- Gateway Configuration
- QoS Data Collection

9.1 Gateway Configuration

Call: Main Menu > Gateways > Gateway Configuration

This area features the following components:

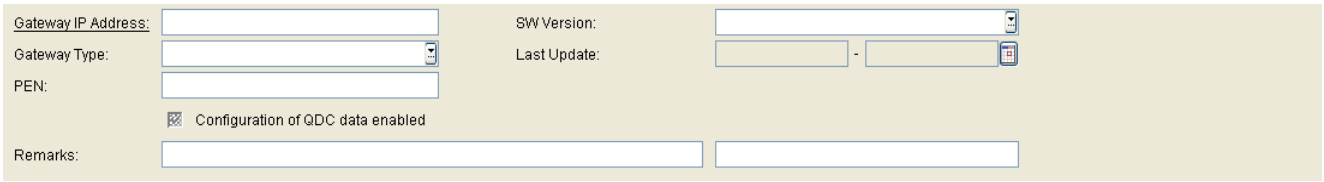
- General Data
- Possible Action Buttons
- "Gateway Connection" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area only applies to the **Gateway Configuration**. It is used for entering parameters in **Search** view to find a specific group of gateways. The base data associated with the gateways found is displayed in the **Object** view (no changes possible).



> ***NOTE:*** For further information about the **Search** view, please see Section 5.5, "Search Functionality".

Gateway IP Address:

IP address of the gateway.

Example: **192.117.1.193**

Gateway Type:

Type of the gateway.

Possible options:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

PEN:

Position of the gateway board (slot).

Example: **1-17-3**

SW Version:

Gateway software version. This value is read-only in search results.

Last Update:

Time when the gateway was last updated. This value is read-only in search results.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Configuration of QDC data enabled

Check box indicating whether the gateway is capable of processing QDC data. The check box is set while reading the gateway data and can only be read.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all gateways that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new gateway.

Save

Saves the changes made to configuration entries.

Discard

Discards any unsaved changes.

Delete

Deletes all selected objects.

Read Gateway Data

Reads the data for all selected gateways. The gateway is entered in the DLS and can be modified using the DLS.
Gateway Data consists of PEN (number that corresponds to a specific slot number of a gateway board),Software Version & MAC Address.

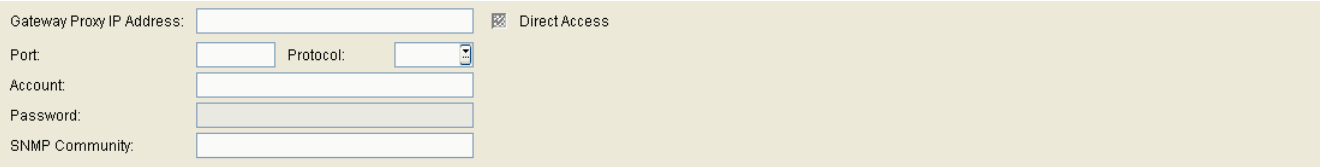
Refresh

Refreshes the content of the relevant page.

9.1.1 "Gateway Connection" Tab

Call: Main Menu > Gateways > Gateway Configuration > "Gateway Connection" Tab

NOTE: Different configuration parameters are assigned default values or deactivated (if not relevant), depending on gateway type.
For information on configuration, see Section 16.4, "Configuring a Gateway in DLS".



Gateway Proxy IP Address:

Proxy IP address of the gateway.

Direct Access

If this check box is activated, the connection between HiPath 4000/HG 3550 and the DLS is via direct access and not via the Assistant.

Port:

Proxy port of the gateway.

Protocol:

Protocol used for communicating between the DLS and the gateway.

Possible options:

- **http**
- **https**

Account

User name for accessing the gateway proxy. The user ID is the first part of the URL.

Password:

Password necessary for accessing the gateway proxy.

SNMP Community:

Community string used for authentication on the SNMP server.

9.2 QoS Data Collection

Call: Main Menu > Gateways > QoS Data Collection

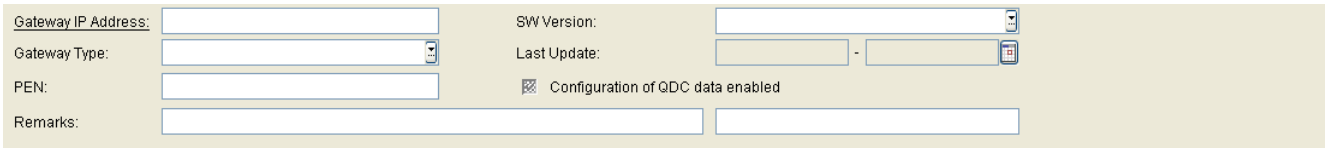
This area features the following components:

- General Data
- Possible Action Buttons
- "Server Data" Tab
- "Report Settings" Tab
- "Threshold Values" Tab

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is used for entering parameters in **Search** view to find a specific group of gateways. The base data associated with the gateways found is displayed in the **Object** view (no changes possible except under **Remarks**).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

Gateway IP Address:

IP address of the gateway.

Example: **192.117.1.193**

Gateway Type:

Type of the gateway.

Possible options:

- **HG1500**
- **HG3530**
- **HG3540**
- **HG3550**
- **HG3570**
- **HG3575**
- **RG2700**

PEN:

Position of the gateway board (slot).

Example: **1-17-3**

SW Version:

Gateway software version. This value is read-only in search results.

Last Update:

Time when the gateway was last updated. This value is read-only in search results.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Configuration of QDC data enabled

Check box indicating whether the gateway is capable of processing QDC data. The check box is set while reading the gateway data and can only be read.

Remarks:

Fields for general information.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all gateways that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Get

Loads a template that has already been saved. For more information, see Section 15.7, "Editing Templates".

Save

Saves configuration entries as a template. For more information, see Section 15.7, "Editing Templates".

Rename

Changes the name of a saved template. For more information, see Section 15.7, "Editing Templates".

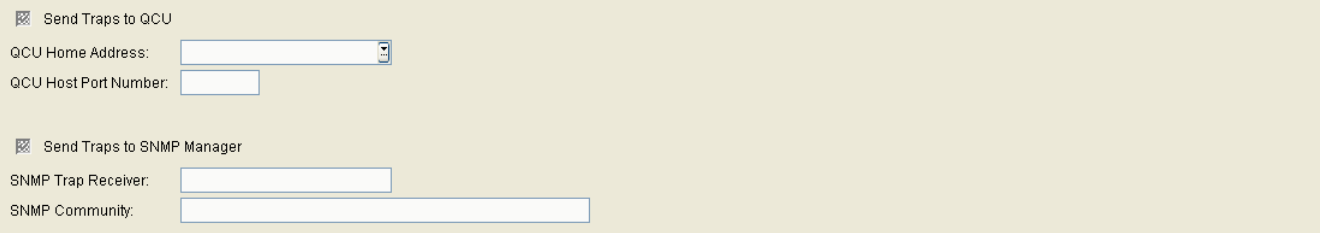
Delete

Deletes a saved template. For more information, see Section 15.7, "Editing Templates".

9.2.1 "Server Data" Tab

Call: Main Menu > Gateways > QoS Data Collection > "Server Data" Tab

More information on QDC can be found in the QDC Interface Description (P31003-H1000-X104-*-7618) and the QDC Service Manual (P31003-H1000-S104-*-7620).



Send Traps to QCU

Check box for sending traps to the QCU.

QCU Home Address:

IP address or host name of the server that logs the QDC data. Corresponds to the value entered in the gateway under **Explorer - Payload - QDC**.

QCU Host Port Number:

Port number for the server that logs the QDC data. Corresponds to the value entered in the gateway under **Explorer - Payload - QDC**.

Send Traps to SNMP Manager

Check box for sending traps to the SNMP Manager.

SNMP Trap Receiver:

Check box for activating the function that sends errors to the SNMP Manager. Matches the value entered in the gateway under **Maintenance - SNMP - Communities - Trap Communities**.

SNMP Community:

Name of the SNMP community. Matches the value entered in the gateway under **Maintenance - SNMP - Communities - Trap Communities**.

Default: **public**

9.2.2 "Report Settings" Tab

Call: Main Menu > Gateways > QoS Data Collection > "Report Settings" Tab

More information on QDC can be found in the QDC Interface Description (P31003-H1000-X104-*-7618) and the QDC Service Manual (P31003-H1000-S104-*-7620).



Report Mode:

Possible options:

- **Off**
  No report.
- **EOS Threshold exceeded**
  Send report at the end of the connection and when the threshold is exceeded.
- **EOR Threshold exceeded**
  Send report at the end of the reporting interval and when the threshold is exceeded.
- **EOS (End of Session)**
  Send report at the end of the connection.
- **EOR (End or Report Interval)**
  Send report at the end of the reporting interval.

Report Interval:

Value range: **0** ... **3600** seconds.

Default: **60** seconds.

Observation Interval:

Value range: **0** ... **3600** seconds.

Default: **10** seconds.

Minimum Session Length:

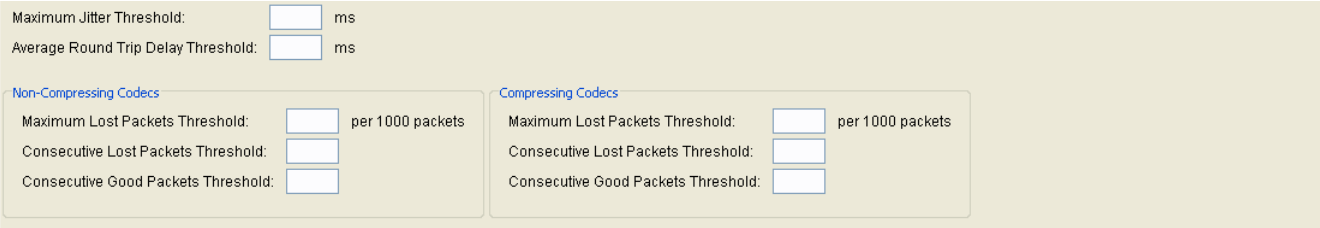
Value range: **0** ... **5000** (x 100 ms)

Default: **20** (= 2 seconds)

9.2.3 "Threshold Values" Tab

Call: Main Menu > Gateways > QoS Data Collection > "Threshold Values" Tab

More information on QDC can be found in the QDC Interface Description (P31003-H1000-X104-*-7618) and the QDC Service Manual (P31003-H1000-S104-*-7620).



Maximum Jitter Threshold:

Maximum threshold in milliseconds for runtime fluctuations during data transmission to trigger a report.

Value range: **0** ... **255** ms.

Default: **15**

Average Round Trip Delay Threshold:

Average response time (in milliseconds) for signal transmission.

Default: **100**

Non-Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during uncompressed transmission.

Value range: **0** ... **255** (per 1000 packets).

Default: **10**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during uncompressed transmission.

Value range: **0** ... **255**

Default: **2**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during uncompressed transmission.

Value range: **0** ... **255**

Default: **8**

Compressing Codecs

Maximum Lost Packets Threshold:

Maximum number of total packets lost during compressed transmission.

Value range: **0** ... **255** (per 1000 packets).

Default: **10**

Consecutive Lost Packets Threshold:

Maximum number of consecutive packets lost during compressed transmission.

Value range: **0** ... **255**

Default: **2**

Consecutive Good Packets Threshold:

Minimum number of consecutive inbound packets lost during compressed transmission.

Value range: **0** ... **255**

Default: **8**

10 Software Deployment

Call: Main Menu > Software Deployment

This menu consists of the following submenus:

- Workpoint Deployment
- Manage Rules

The **Software Deployment** area is used for the user-friendly distribution of software images and other workpoint software.

NOTE: Note the difference between **Software Deployment** and **File Deployment** in the DLS interface (see Section 10.1.1 and Section 10.1.2).

Software deployment refers to the distribution of workpoint software (IP phones and IP clients). **File deployment**, on the other hand, refers to the distribution of any binary or ASCII files that perform a certain task in the workpoint.

Both functions are combined in the DLS main menu under **Software Deployment**.

For information on general interface operation, see Section 5.4.2, "Work Area".

NOTE: When distributing software for optiPoint WL2 professional workpoints, ensure that the workpoints have sufficient battery capacity. If not, it may not be possible to operate the software successfully.

10.1 Workpoint Deployment

Call: Main Menu > Software Deployment > Workpoint Deployment

The distribution of software (firmware) and other data to individual IP clients and IP phones can be controlled using the DLS.

For this to work, both the files to be distributed and the required workpoints must be registered at the DLS. The FTP server and network drives must also be registered at the DLS as these supply the data to the workpoints (see Section 6.3.4, "FTP Server Configuration" and Section 6.3.7, "Network Drive Configuration").

NOTE: Deployment via a network drive is not available in the onboard variants of the DLS on OpenScape Voice.

This area can be split into the following groups:

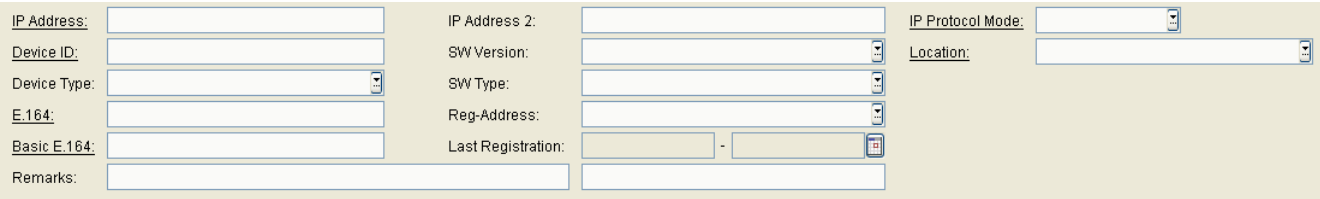
- General Data
- Possible Action Buttons
- Software and File Deployment
  consisting of:
  - "Software Deployment" Tab
  - "File Deployment" Tab
- Display of Inventory Data
  consisting of:
  - "Software Inventory" Tab
  - "LDAP Inventory" Tab
  - "MOH Inventory" Tab
  - "INCA Inventory" Tab
  - "Java Midlet Inventory" Tab
  - "Logo File Inventory" Tab
  - "SYSTEM/RINGTONE Inventory" Tab
  - "APM Inventory" Tab
  - "NETBOOT Inventory" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

If you need this function frequently, you can automate it simply and conveniently with deployment jobs (see Chapter 14, "Job Coordination").

General Data

This part of the contents area is identical for all interfaces associated with this menu. It is used for entering parameters in **Search** view to find a specific group of workpoints. The base data associated with the workpoints found is displayed in **Object** view (no changes possible except under **Remarks**).



Some areas do not contain all of the fields described.

NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of the workpoint. For OpenStage, an IPv4 or IPv6 address is displayed here. See also the description of the **IP Protocol Mode** parameter.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

Physical MAC address of the workpoint.

Example: **00:0E:A6:85:71:80**

Device Type:

Workpoint device type.

All workpoint types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Examples: **optiPoint 410 standard**, **optiClient 130**.

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

IP Address 2:

Second IP address of the IP phone, if it has an IPv6 address.

Available for OpenStage only.

SW Version:

Software version used by the workpoint.

Example for IP phones and IP clients: **5.0.12**.

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

Software type used by the workpoint.

Examples: **Unify HFA**, **Unify SIP**.

Reg-Address:

IP address of the gateway or the gatekeeper where the workpoint must register. In HiPath 3000, this is the IP address of the HG 1500, in HiPath 4000 it is the HG 3530 or the STMI board.

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Location:

Current location of the IP Device.

Remarks:

Fields for general information.

IP Protocol Mode

Indicates which IP version is used by the phone. If both versions are used, IP address contains the IPv4 address, and IP address 2 contains the IPv6 address.

Only available for openStage.

Possible options:

- **IPv4**
- **IPv6**
- **IPv4 and IPv6**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

A search is performed in the **Search** view for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Deploy

A software or file deployment job is started in the **Object** and **Table** views. For more information, see Section 15.9, "Distribution of Workpoint Software".

10.1.1 "Software Deployment" Tab

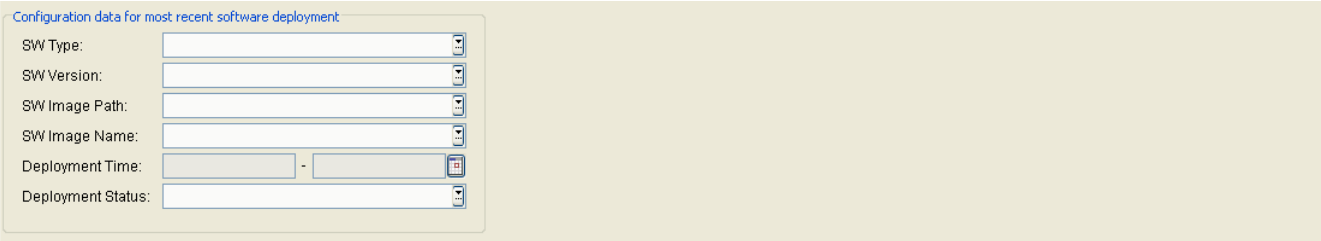
Call: Main Menu > Software Deployment > Workpoint Deployment > "Software Deployment" Tab

This tab shows the data entered for the last software deployment job that was performed for workpoints with the DLS.

"Software" is always used to refer to application software for a specific type of workpoint (for example, optiPoint 410 standard). This software is generally provided as a software image (mostly a file with the extension *.app*) that can be distributed ("deployed") to workpoints.

NOTE: All software images provided with and after the introduction of DLS contain a DLS interface for communication with the DLS (new software format). This interface is not available in any existing and previously available software images (old software format).

For an overview of all software types supported by the DLS, see Section 3.5, "Overview of Software and File Types".



Configuration data for most recent software deployment

SW Type:

Software type used by the workpoint.

Example: **Unify HFA**, **Unify SIP**.

SW Version:

Software version used by the workpoint.

Example for IP phones and IP clients: **5.0.12**

SW Image Path:

Path name of the directories in which the file is saved with the software image.

Examples: **/Directory1/Subdirectory2** for IP phone files, **\Directory1\Subdirectory2** for IP client files.

SW Image Name:

File name of the software image.

Examples: **vxworks.app**, **op410std-unify-hfa-V5.0.12-L12345678.app**

Deployment Time:

Time when the last software deployment job was started (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Deployment Status:

Result (status) of the last software deployment job.

Possible options:

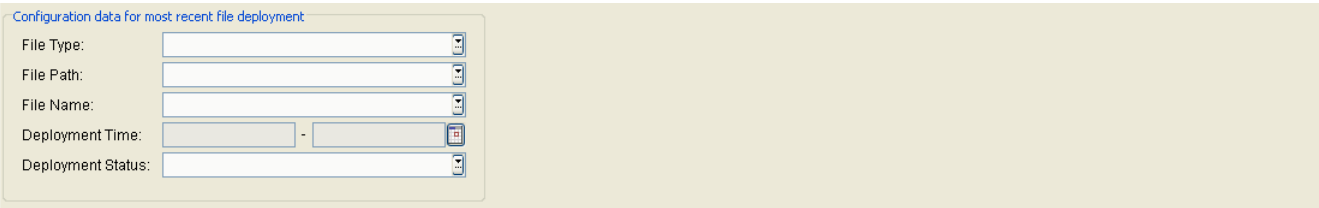
- **Deployment rejected**:
  Deployment could not be started. Possible reason: Configuration settings only permit deployment to be performed when the workpoint is idle; this was not the case.
- **Deployment initiated**:
  Deployment was started but is not yet complete.
- **Deployment finished**:
  Deployment was successfully completed.
- **Deployment failed**:
  An error occurred in the course of deployment.

10.1.2 "File Deployment" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "File Deployment" Tab

This tab shows the data (file type) entered for the last file deployment job that was performed for workpoints with the DLS.

For an overview of all file types supported by the DLS, see Section 3.5, "Overview of Software and File Types".



Configuration data for most recent file deployment

File Type:

Type of file (see Section 3.5, "Overview of Software and File Types").

Example: **Java Midlet** when the last action of a Java application was distributed to the IP phone.

File Path:

Path name of the directory in which the appropriate file type is saved.

Examples: **/Directory1/Subdirectory2** for IP phone files, **\Directory1\Subdirectory2** for IP client files.

File Name:

Name of the distributed file.

Deployment Time:

Time when the last software deployment job was started (for a calendar, see Section 5.4.2.4, "Time field with calendar button").

Deployment Status:

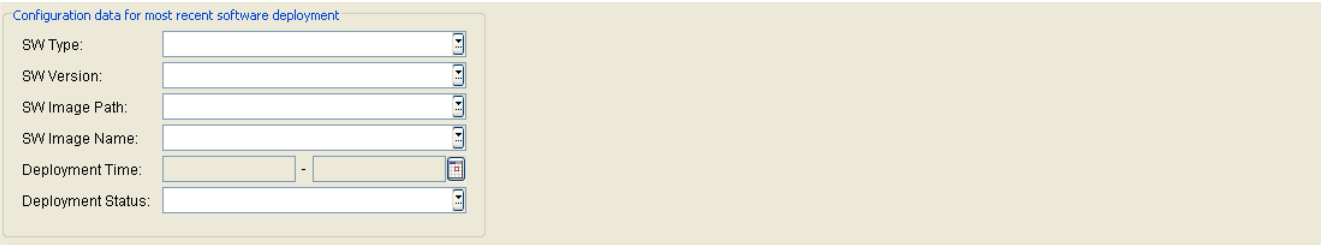
The result (status) of the last software deployment job is displayed.

Possible status:

- **Deployment rejected**:
  Deployment could not be started.
- **Deployment initiated**:
  Deployment was started but is not yet complete.
- **Deployment finished**:
  Deployment was successfully completed.
- **Deployment failed**:
  An error occurred in the course of deployment.

10.1.3 "Software Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "Software Inventory" Tab



Inventory/Status data for software installation

SW Repository:

Address of the FTP server (for IP phones) or network computer (for IP clients) from which the software was downloaded. The address can be either an IP address or a host name.

SW Image Name:

The file name of the software downloaded.

Installation Date:

Date when the last software was downloaded or installed.

Installation Status:

The status of software installation is displayed here.

Language Package:

Shows the installed language package.

10.1.4 "LDAP Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "LDAP Inventory" Tab



NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.5 "MOH Inventory" Tab

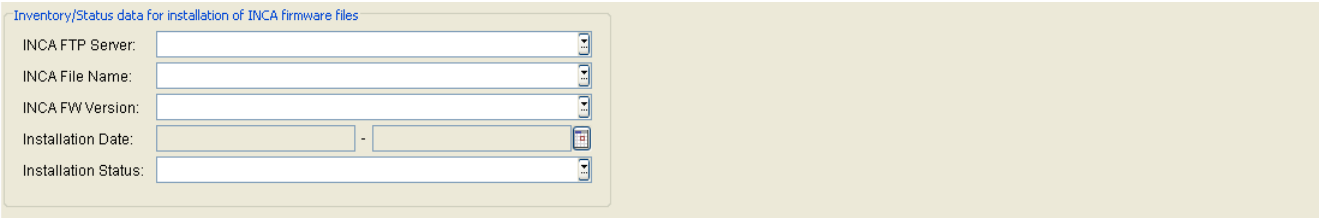
Call: Main Menu > Software Deployment > Workpoint Deployment > "MOH Inventory" Tab



NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.6 "INCA Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "INCA Inventory" Tab



NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

INCA FW Version:

Version of INCA Firmware.

10.1.7 "Java Midlet Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "Java Midlet Inventory" Tab



NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.8 "Logo File Inventory" Tab

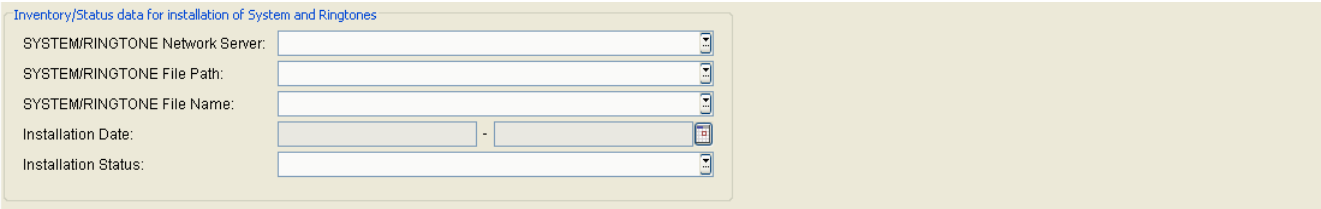
Call: Main Menu > Software Deployment > Workpoint Deployment > "Logo File Inventory" Tab



NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

10.1.9 "SYSTEM/RINGTONE Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "SYSTEM/RINGTONE Inventory" Tab



SYSTEM/RINGTONE Network Server:

Address of the network computer from which the ringtones were downloaded. The address can be either an IP address or a host name.

SYSTEM/RINGTONE File Path:

Directory on the network computer from which the ringtones were downloaded, starting from the network path released.

SYSTEM/RINGTONE File Name:

Name of the file with ringtones that were downloaded.

Installation Date:

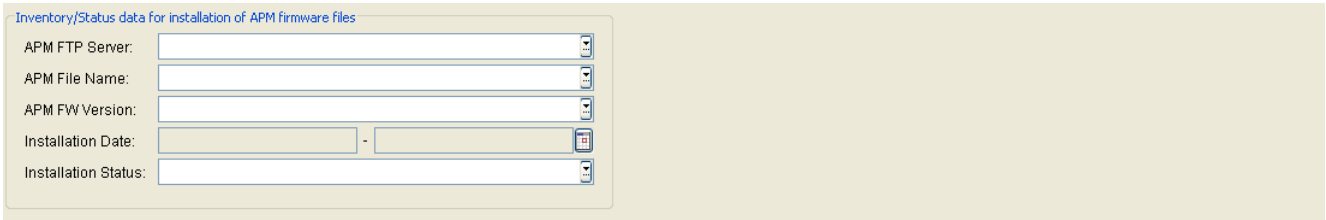
Date on which the last ringtones were downloaded or installed.

Installation Status:

The status of ringtone installation is displayed here.

10.1.10 "APM Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "APM Inventory" Tab



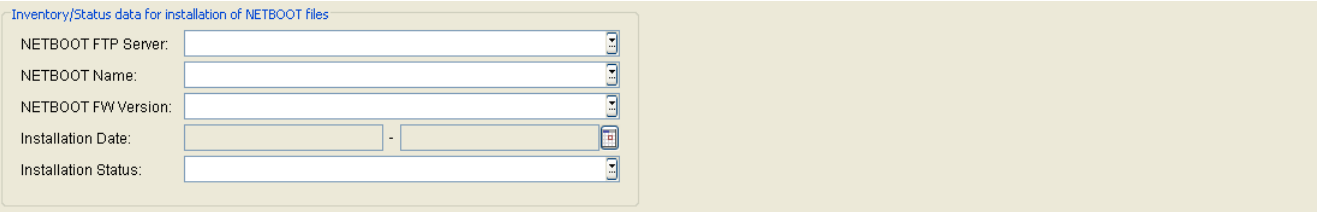
NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

APM FW Version:

Version of APM Firmware.

10.1.11 "NETBOOT Inventory" Tab

Call: Main Menu > Software Deployment > Workpoint Deployment > "NETBOOT Inventory" Tab



NOTE: The description provided in Section 10.1.3, ""Software Inventory" Tab" applies to all fields in this tab.

NETBOOT FW Version:

Version of NETBOOT Firmware.

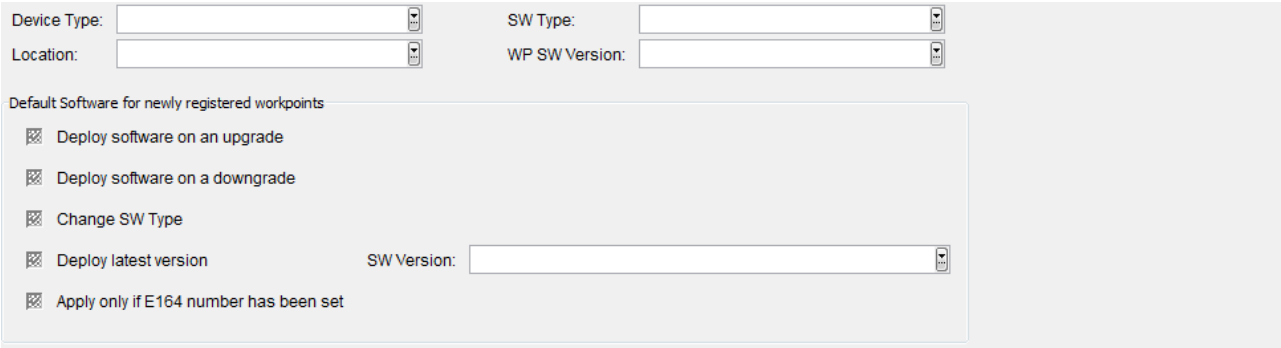
10.2 Manage Rules

Call: Main Menu > Software Deployment > Manage Rules

You can use deployment rules to control the distribution of software and limit the resulting transmission traffic.

If automatic software distribution is initiated for a workpoint, this workpoint checks first if there is a rule for the workpoint device type. If there is no rule or if the rule has been deactivated, no software is distributed to this workpoint.

For information on using deployment rules, see Section 15.9.2, "Automatic Deployment".



Device Type:

Device type of the workpoints to which the rule should apply.

Examples: **optiPoint 410 standard**, **optiClient 130**.

> ***NOTE:*** In the case where you want to apply a SW to all devices regardless of the current location that they are, create a default location with a device type equal to **ALL**. However, the devices MUST not conform to any other individual manage rule per location.

> ***NOTE:*** For Mediatrix device types, before configuring manage rules, please refer to the following Wiki page in order to comply with correct versioning:
> http://wiki.unify.com/wiki/How_to_setup_Mediatrix

SW Type:

Type of software type which is currently installed on the workpoints to which the rule should apply.

Examples: **Unify HFA**, **Unify SIP**.

WP SW Version:

Version of the software which is currently installed on the workpoints to which the rule should apply.

Location

Location name (IP range and gatekeeper) to which the deployment rules are assigned.

> ***IMPORTANT:*** Manage rules that are assigned to the "**Default location**" are executed for all locations without assigned Manage rules.

Default Software for newly registered workpoints

Deploy software on an upgrade

Check box for activating the deployment function in the case of an upgrade.
This means that deployment is performed if the software at the workpoint is **older** than the newest software or the software generally selected.

> ***NOTE:*** If you want to deactivate (but not delete) the rule, deactivate this and the following option.

Deploy software on a downgrade

Check box for activating the deployment function in the case of a downgrade.
This means that deployment is performed if the version number of the software at the workpoint is higher than the version of the software generally selected.

> ***NOTE:*** If you want to deactivate (but not delete) the rule, deactivate this and the previous option.

Change SW Type:

When switch is activated, the workpoint's software type is replaced by the one of the selected software image.

Deploy latest version

Check box for activating the deployment function with the latest version of a software type.
This means that during an update (downgrade), the latest software is transmitted to all workpoints that do not yet have this software version.

SW Version:

Drop down list containing all available software images respective to Device Type and SW Type as those are defined.

> ***NOTE:*** SW Version drop down list returns Software Images located on the FTP server assigned to the location selected. If no FTP server is assigned to location then an error message "**Choice list not available**" will be displayed.

Example for optiPoint and optiClient: **5.0.12**.

Apply only if E164 number has been set

if ithis checkbox is activated, DLS will not trigger any automatic SW deployment by applying this rule if E164 has not been set on the device.

This checkbox is disabled by default.

Possible Action Buttons

Search

Searches for configured deployment rules on the basis of the criteria specified.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Adds a new deployment rule.

Save

Saves the changes. A newly created rule is immediately effective.

Discard

Discards any changes made.

Delete

Deletes an existing deployment rule.

Apply

Starts the automatic software distribution.

11 Element Manager

Call: Main Menu > Element Manager

Information on the relevant system types are managed here.

This menu consists of the following submenus:

- Element Manager Configuration
- Element Manager Security

To use plug&play functionality, you must adjust a number of configurations here.

For background information on plug&play, see Section 15.8, "Workpoint Autoconfiguration (Plug&Play)".

For information on configuring the DHCP server for full plug&play, see Section 4.12.4, "DHCP Server in a Windows Environment" and Section 4.12.5, "DHCP Server in a Linux/Unix Environment".

For information on general interface operation, see Section 5.4.2, "Work Area".

11.1 Element Manager Configuration

Call: Main Menu > Element Manager > Element Manager Configuration.

Information on the different system types is entered in separate tabs in Element Manager.

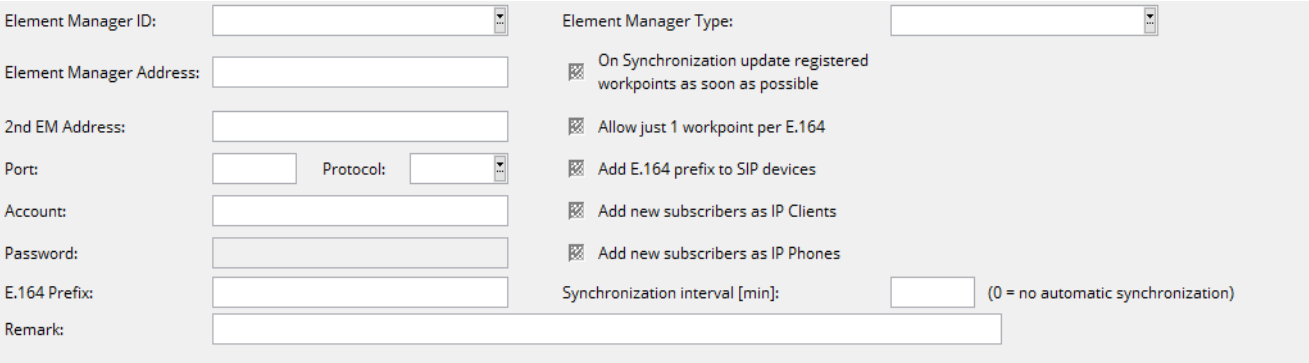
This area features the following components:

- General Data
- Possible Action Buttons
- "OpenScape Voice" Tab
- "OpenScape Voice Assistant" Tab
- "HiPath 4000 Assistant" Tab
- "HiPath 3000/5000" Tab
- "Protocol" Tab

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of Element Managers. The base data associated with the Element Managers found is displayed in the Object view (no changes possible except under Remark).

For more information on modifying the configuration, see Section 15.4, "Changing the Element Manager Configuration and Creating Jobs".



Element Manager ID

Freely preset ID (mandatory). Uniquely identifies the Element Manager that supplies data to the workpoints when necessary.

Element Manager Address

Host name or IP address of the Element Manager.

2nd EM Address

Hostname or IP address of the 2nd node.

NOTE: This parameter is only relevant for geographically separated OpenScape Voice clusters.

Port

Port used by the Element Manager for communication with the DLS. The following list specifies the ports used by the individual Element Managers for different protocols:

- OpenOffice EE: **443** (HTTPS)
- HiPath 3000 / 5000: **8085** (HTTP) or **443** (HTTPS)
- HiPath 4000 (Web service): **443** (HTTPS)

- HiPath 4000 (JDBC): **1527**

  NOTE: This port is locked & cannot be modified / checked as opposed to the rest EM options.

- OpenScape Voice: **8769** (HTTP)
- OpenScape Voice Assistant: **443** (HTTPS)
- OpenScape Office MX/LX: **443** (HTTPS)

Protocol

Protocol used for exchanging data with the Element Manager.

Possible options:

- **http**
- **https**

E.164 Prefix

Prefix for the E.164 number. Used for workpoints on OpenScape Voice, HiPath 3000/5000, OpenOffice EE, and HiPath DXWebPro. With Hipath 3000/5000 Version < V7, this is used only for HFA phones. If nothing is entered, the call number of the workpoint must be unique in the net. In other DLS menus, only the call number has to be entered for E.164. This field is not used for HiPath 4000; instead, the corresponding values should be entered in the **Virtual Node IDs (HFA)** table in the "HiPath 4000 Assistant" tab. If nothing is entered here, the phone number of the IP phone or IP client must be unique in the network. In other DLS interfaces, you only have to enter the phone number for E.164 fields.

Example: **4989722** (or no input).

Account

The access code is needed for HiPath 4000 Assistant and for OpenScape Voice Assistant. The "uas_read" account is needed for HiPath 4000 JDBC Assistant; this must be activated there.

For example, JDBC ID in HiPath 4000.

Password

Password required for Element Manager access. The entry is made by clicking the key icon in a dialog window.

For example, JDBC password in HiPath 4000.

Element Manager type

Select the Element Manager type. You may only enter data in the corresponding tab.

Possible options:

- **HiPath 4000 (JDBC)** (see **"HiPath 4000 Assistant" Tab**)
- **OpenScape Voice Assistant** (see **"OpenScape Voice Assistant" Tab**)

  NOTE: In that option,OpenScape Voice Tab is disabled.

  IMPORTANT: In the case of multiple element manager ID's, DLS Element Manager only supports multiple OSV's with non overlapping provisioning.
- **HiPath 3000/5000** (see **"HiPath 3000/5000" Tab**)
- **OpenScape Voice** (see **"OpenScape Voice" Tab**)
- **HiPath 4000 (Webservice)** (see **"HiPath 4000 Assistant" Tab**)
- **OpenScape Business**
- **OpenScape Office MX/LX**

On Synchronization update registered workpoints as soon as possible

If this check box is activated, jobs are immediately executed during element manager synchronization.

Allow just 1 workpoint per E.164 number

If this check box is activated, only those workpoints will be updated which have been updated before by the same Element Manager or are assigned to it (**Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"EM Synchronization" Tab** > **Referenced Element Manager**). Thereby, the security risk of sending registration data automatically to IP Devices with manipulated E.164 numbers is avoided, in case multiple workpoints are registered with the same E.164.

Add E.164 prefix to SIP (UFIP) devices

If this checkbox is activated, the e164 prefix defined in the Virtual Node IDs table is added also for the SIP (UFIP) stations.

Add new subscribers as IP Clients

If this check box is activated, new IP clients are created for stations (that is, E.164 numbers) transmitted during synchronization with the telephone system but not yet present in the DLS.

Add new subscribers as IP Phones

If this check box is activated, new IP phones are created for stations (that is, E.164 numbers) transmitted during synchronization with the telephone system but not yet present in the DLS. This check box is activated by default.

Synchronization Interval [min]

Defines the intervals for periodic synchronization between the telephone systems configured in the Element Manager and the DLS.

Value range: **60 ... 1440** minutes or **0** for no automatic synchronization.

Default: **0**

> ***NOTE:*** For default value **0**, OpenScape Voice Tab is disabled.

> ***IMPORTANT:*** Do not allow the synchronization interval to be set to lower than **60** min.
> Although **0** is allowed,during upgrade all Element Managers with synchronization interval < **60** min must be updated to the new minimum value of 60 minutes.

Remark

Field for general information.

Possible Action Buttons

Search

Searches for all Element Managers already entered in the DLS and that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new Element Manager configuration.

Save

Saves the Element Manager configuration.

Discard

Discards any changes made and new entries.

Delete

Deletes the Element Manager configuration.

Synchronize

Synchronization transfers registration data from the Element Manager to the DLS database. This operation runs in the background. A protocol file is created after synchronization, which can take a few minutes. Synchronization generates or modifies workpoints; it can also result in job generation. These jobs are generated without consultation.

> ***NOTE:*** An error message is issued if you try to start a synchronization session on the Element Manager where a session is already in progress.
>
> ***NOTE:*** A new Element Manager synchronization should not be triggered unless the previous one has completed (regardless of being successful or not).

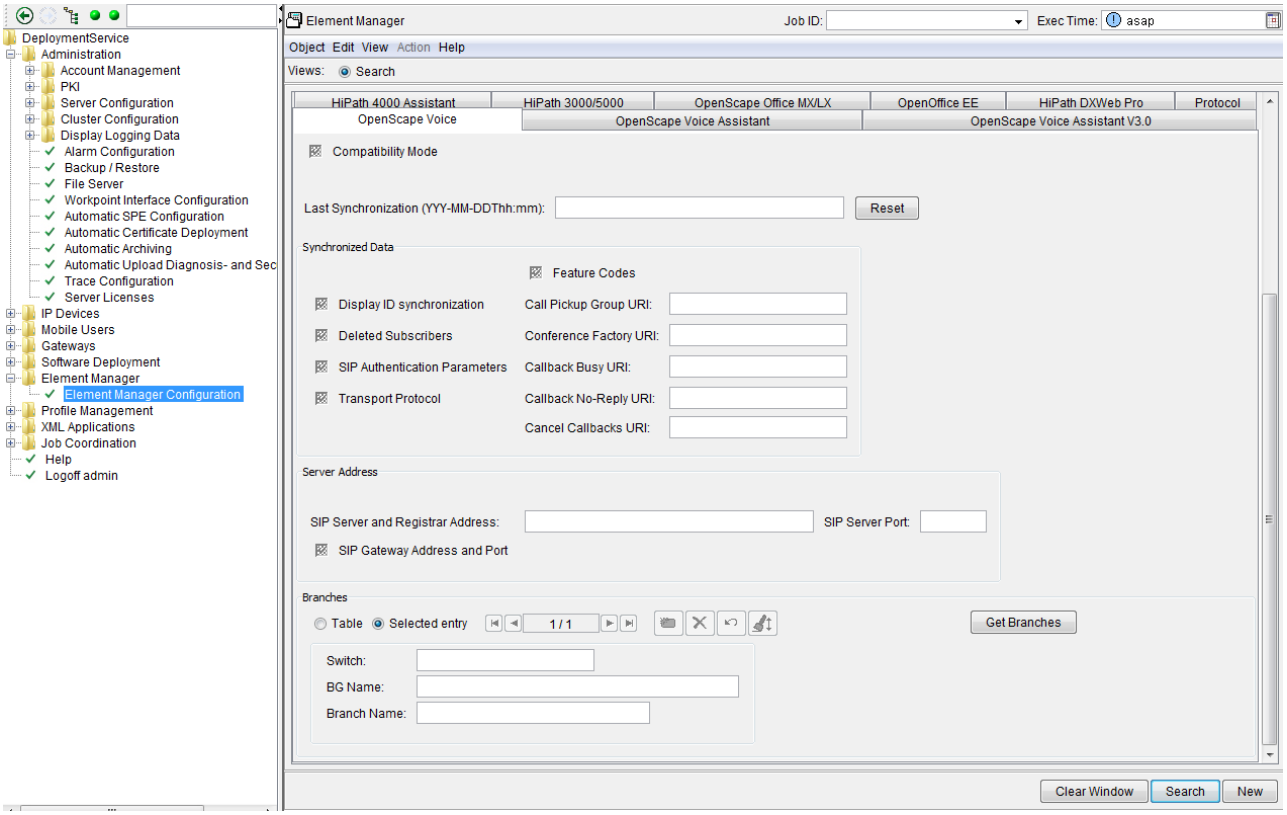
Refresh

Refreshes the contents of the current mask from the database.

11.1.1 "OpenScape Voice" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "OpenScape Voice" Tab.

For more information on modifying the configuration, see Section 15.4, "Changing the Element Manager Configuration and Creating Jobs".



NOTE: In order to synchronize with OpenScape Voice,you need to create the necessary appropriate packet filter rule* to OpenScape Voice for local port 8769 and allow TCP Incoming Connection from the remote Windows DLS server IP.
* firewall rule via OpenScape Voice Assistant

Compatibility Mode

Checkbox for configuration of the Compatibility Mode. If checked, then the last synch was in compatibility mode. If unchecked, the last synch was in normal mode.

Last Synchronization

Time & date of the last synch. Read only Text with the following format :

YYYY-MM-DDThh:mm

Example: 2011-05-29T19:00

The defaullt value is set to void.

Reset

Clicking this button enables the option to clear/reset the last synchronization field value.

Synchronized Data

Display ID Synchronization

Checkbox for activating the synchronization of the display ID.

Deleted Subscribers

Check Box for activating the deletion of OSV Subscribers. If checked, then devices and line/DSS keys with Address of Record that corresponds to non-existing (or deleted) OSV subscribers are deleted permanently from the database.

If unchecked, then devices and line/DSS keys that correspond to non-existing (or deleted) OSV subscribers are kept in DLS DB.

This box is unchecked by default.

SIP Authentication Parameters

Checkbox for configuration of the SIP Authentication Parameters. If checked,then for all devices and line/DSS keys that are created/updated during synchronization the SIP Realm, Username and Password shall be set the same with the SIP Realm Username and Password of the respective OSV subscriber line.

If unchecked, the OSV subscriber SIP Realm, Username and Password are ignored during synchronization with OSV.

This box is unchecked by default.

Transport Protocol

Checkbox for configuration of the Transport Protocol. If checked, the Transport Protocol will be set to the same value as the respective OSV subscriber for all devices that are created / updated during synchronization.

If unchecked, the transport protocol is set to the devices in DLS without taking into account the transport protocol of the OSV subscribers although it could be set to the DLS device by CMP after a device modification (that happens out of the synchronization context). However it is still taken into account for the proper setting of the SIP gateway port (if enabled).

This box is unchecked by default.

Feature Codes

Checkbox for configuration of Feature Codes. If checked, Feature Access Codes will be set as configured at the respective OSV Element Manager attributes for all Devices that are created/updated via synchronization.

If unchecked, Feature Access Codes will not be set.

This box is unchecked by default.

Call Pickup Group URI

Textbox for configuration of the Call Pickup Group URI.

Maximum of 15 characters (0-9,*,#) is allowed.

Default value is set to *7.

Conference Factory URI

Textbox for configuration of the Conference Factory URI.

Maximum of 15 characters (0-9,*,#) is allowed.

Default value is set to 1234567890.

Callback Busy URI

Textbox for configuration of the Callback Busy URI.

Maximum of 15 characters (0-9,*,#) is allowed.

Default value is set to *6.

Callback No-Reply URI

Textbox for configuration of the Callback No-Reply URI.

Maximum of 15 characters (0-9,*,#) is allowed.

Default value is set to *6.

Cancel Callbacks URI

Textbox for configuration of the Cancel Callbacks URI.

Maximum of 15 characters (0-9,*,#) is allowed.

Default value is set to #6.

Server Address

SIP Server and Registrar Address

IP address of the SIP server and the SIP registrar. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Server Port

Port number of the SIP server. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Gateway Address and Port

Checkbox for configuration of SIP Gateway Address and Port. If checked, the address (IP of FQDN) of the associated endpoint of the subscriber as retrieved from the OSV SOAP request will be set as the Gateway IP address of the devices that are created/updated during synchronization. The Gateway port number is set according to the Transport protocol of the synchronized subscriber to 5060 (for TCP/UCP) or 5061 (for TLS).

If unchecked, the gateway address and port is not set for the devices that are created/updated during synchronization

This box is unchecked by default.

Branches

Switch

Name of the switch where the OSBranch is administered.

BG Name

Name of the Business Goup.

Branch Name

Name of the Branch.

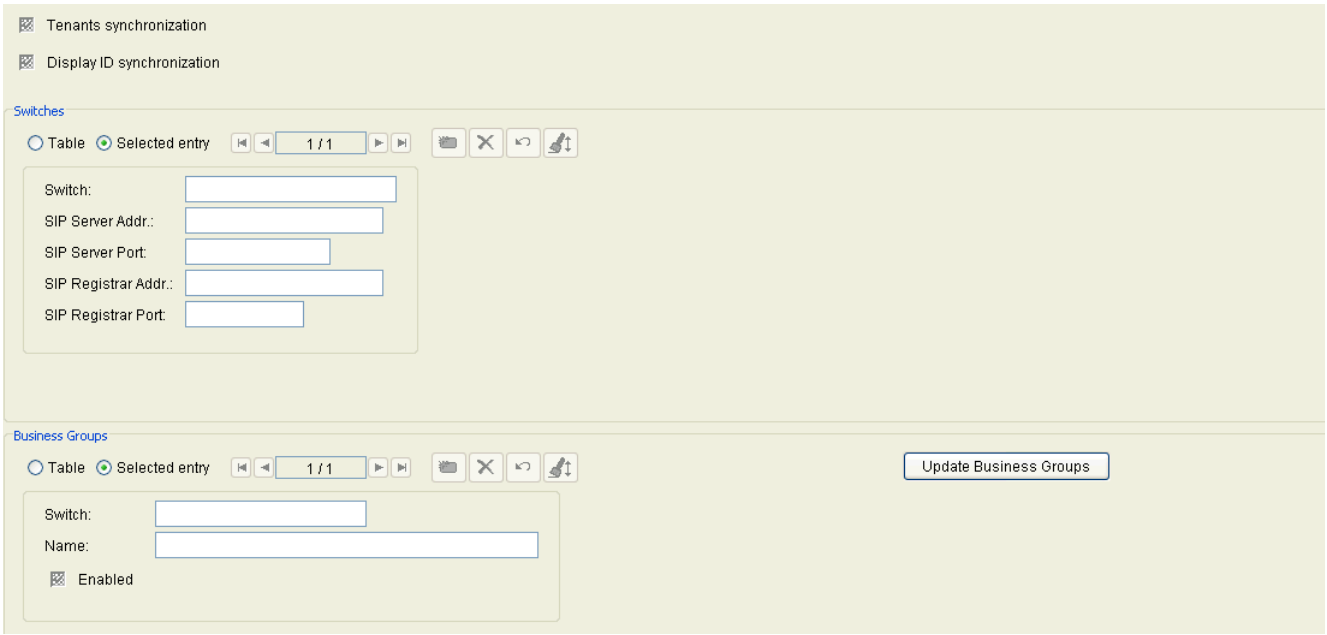
Get Branches

Starts update of Branches and the tenants will be synchronized. The refresh is performed in the background; the protocol file is only created at the end. It may take a few minutes to provide this file.

> ***NOTE:*** When the selected Element Manager Type is OpenScape Voice Assistant ,you won’t be able to run Get Branches.

11.1.2 "OpenScape Voice Assistant" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "OpenScape Voice Assistant" Tab.



> ***IMPORTANT:*** The OSV Element Manager is enhanced to cover all the functionality offered by the OSV Assistant EM (synchronization per BG and secure connection).Therefore the OSV Assistant EM becomes obsolete and given the fact that it does not support Delta synchronization, it is strongly recommended that any configured OSV Assistant EM in DLS should be replaced with OSV EM(s). Please refer to Section 15.5, "How to replace OSV Assistant Manager with OSV Element Manager".

Tenants synchronization

When activated, the tenants will be synchronized as well when **Update Business Groups** is executed.

Display ID synchronization

Checkbox for activating the synchronization of the display ID.

Switches

Switch

Switch name of the administrated switch. The entry is optional. When clicking **Update Business Groups**, it will be set by OpenScape Voice Assistant. The switch name is case-sensitive and must match to that one defined inside the OpenScape Voice Assistant.

SIP Server Addr:

IP address or hostname of the SIP server. This value is not supplied by OpenScape Voice, it must be configured manually.

SIP Server Port:

Port number of the SIP server. This value is not supplied by OpenScape Voice, hence it must be configured manually.

SIP Registrar Addr:

IP address or hostname of the SIP registrar. This value is not supplied by OpenScape Voice, hence it must be configured manually.

SIP Registrar Port:

Port number of the SIP registrar. This value is not supplied by OpenScape Voice, hence it must be configured manually.

Business Groups

Name

Name of Business Group.

Enabled

Only enabled Business Groups will be synchronized.

Update Business Groups

Stations are sorted into business groups. Before you start a synchronization session, you must first find out which business groups are available and then activate the relevant check boxes. If **Tenants synchronization** is activated, the tenants will be synchronized as well. The refresh is performed in the background; the protocol file is only created at the end. It may take a few minutes to provide this file.

NOTE: Synchronization cannot be started while business groups are being refreshed. If you try, however, an appropriate advisory message appears.

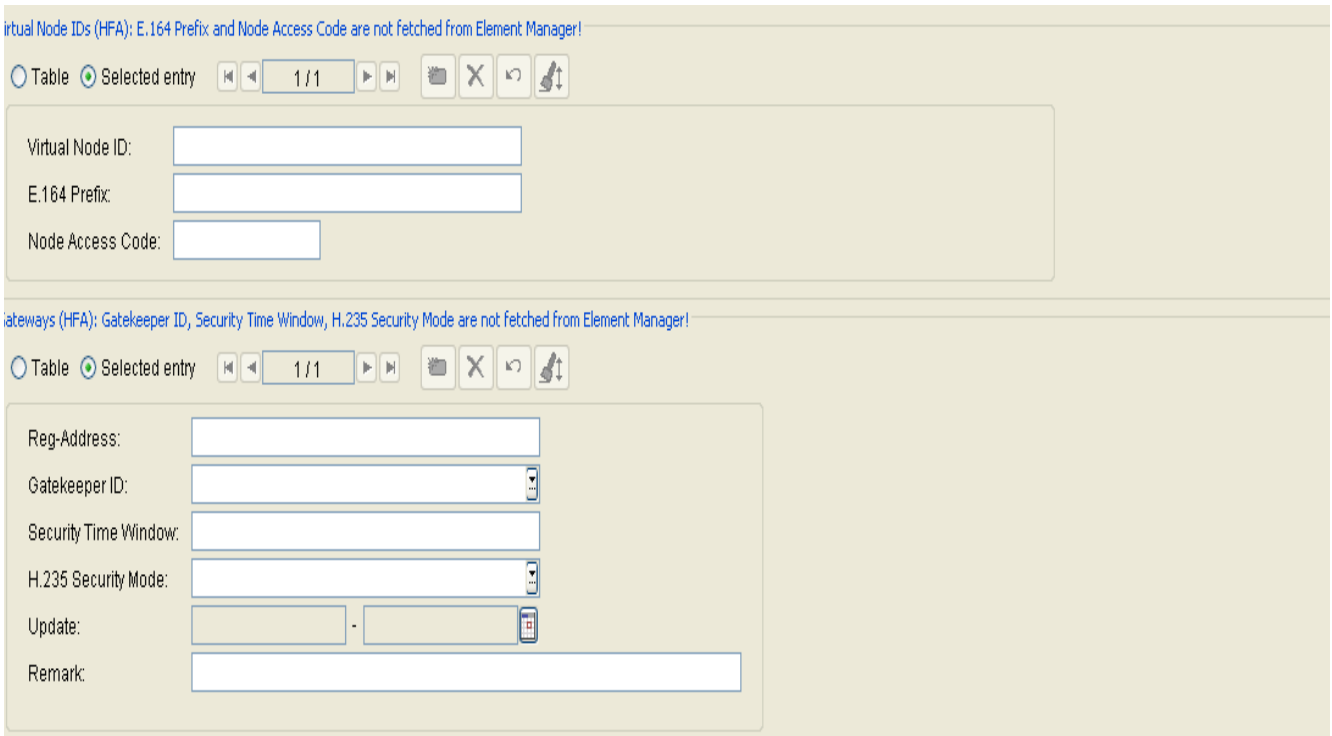
11.1.3 "HiPath 4000 Assistant" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "HiPath 4000 Assistant" Tab.

> ***NOTE:*** The synchronization of DLS Element manager data with those of HiPath 4000 Assistant (H4K Assistant) is possible only if the data within the H4K Assistant are synchronized. That is, the upload status found in H4K Assistant under **Configuration Management** > **Network** > **System** > **Basic Data** must be SYNCHRONOUS. Otherwise, the synchronization of the data within the H4K Assistant by means of AMO UPLOA must be started first by the H4K Assistant action "Upload".

> ***NOTE:*** The settings of this tab are also valid for HiPath 4000 V6.

For more information on modifying the configuration, see Section 15.4, "Changing the Element Manager Configuration and Creating Jobs".



Virtual Node IDs (HFA): E.164 Prefix and Node Access Code are not fetched from Element Manager!

> ***IMPORTANT:*** After the first synchronization you need to import information on Hi Path 4000 Assistant tab on Virtual Node IDs with valid data exported from HP4K regarding E164 prefix and Node Access code on each mentioned Virtual Node ID entry that came from first synchronization.
> Then, you need to re-synchronize and check the virtual Device entries that are generated.

Virtual Node ID

ID of the virtual node if a HiPath 4000 is distributed across several virtual nodes and different CO accesses are used within the node. With this solution, you can generate unique E.164 numbers for all nodes by creating different subscriber phone number/node number combinations. This value is supplied by HiPath 4000.

If entries are not available for either **Virtual Node ID** or **E.164 Prefix**, no HFA workpoints are transferred. If entries are not available for **Virtual Node ID**, but there is an entry for **E.164 Prefix**, all HFA workpoints as assigned this prefix.

E.164 Prefix

Prefix for the E.164 number. This value is not supplied by HiPath 4000 - it must be configured.

If the table is empty or a **virtual node ID** is entered without an **E.164 prefix**, no workpoints are created. If a line is present containing just one **E.164 prefix** and no **virtual node ID**, all HFA workpoints are assigned this prefix (default prefix). If there are other entries, however, with one **virtual node ID** and one **E.164 prefix** each, the corresponding prefix is used for each one. The default prefix is used for lines for which only the **virtual node ID** is set without an assigned **E.164 prefix**.

If the E.164 prefix is modified and there are workpoint entries for it, then all associated E.164 numbers are immediately adapted (the E.164 is composed of the extension and the E.164 prefix). Depending on the number or workpoints, this process can take a few minutes but runs in the background. Synchronization cannot be performed during this time. If you try, however, an appropriate error message appears.

Node Access Code

Node Access Code for numbering plan.

Gateways (HFA): Gatekeeper ID, Security Time Window, H.235 Security Mode are not fetched from Element Manager!

Reg-Address:

Host name or the gateway server address. This value is supplied by HiPath 4000.

Gatekeeper ID

Unique gatekeeper ID. This value is not supplied by HiPath 4000, it must be configured manually.

Security Time Window:

Indicates the maximum time difference permitted between the individual devices that should run synchronously in H.235. This value is not supplied by HiPath 4000, it must be configured manually.

H.235 Security Mode:

Voice encryption setting. This value is not supplied by HiPath 4000, it must be configured manually.

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Update

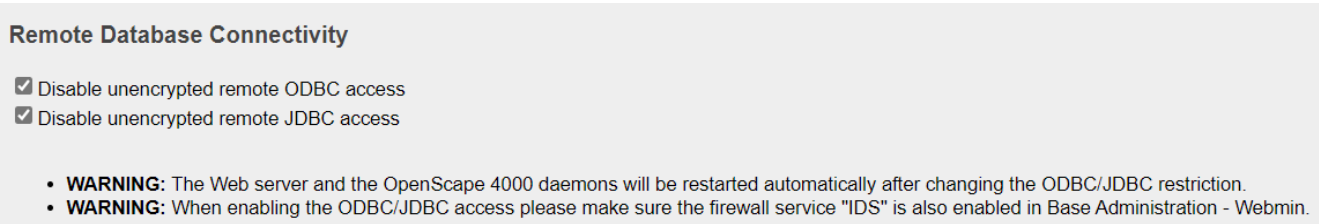
Time of the last PBX or gateway server update.

Remark

Field for general information.

Remote database connectivity

Unencrypted remote ODBC and JDBC access is by default disabled in OpenScape4000 Assistant. It can be enabled using Assistant > Access Management > Security Mode Configuration > Remote Data Base Connectivity



Uas_read user account is available by default in OpenScape 4000 Assistant > Access Management > System Account Administration and it is created for the Remote ODBC access connection. This user will be used in the DLS when Element Manager is configured with JDBC.

11.1.4 "HiPath 3000/5000" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "HiPath 3000/5000" Tab.

For more information on modifying the configuration, see Section 15.4, "Changing the Element Manager Configuration and Creating Jobs".



H.235 Security Mode:

Voice encryption setting. This value is not supplied by HiPath 3000/5000, it must be configured manually.

Possible options:

- **None**
  No voice encryption.
- **Reduced**
  One-way voice encryption (gatekeeper data not sent in encrypted form).
- **Full**
  Voice encryption both ways (workpoint and gatekeeper data both sent in encrypted form).

Security Time Window:

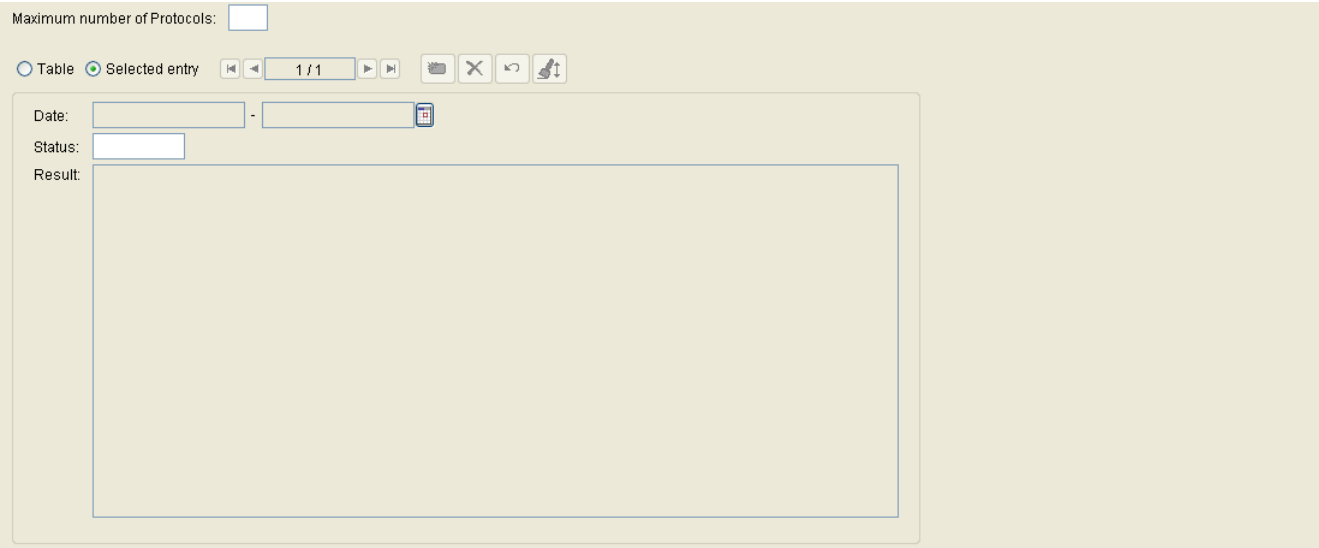
Indicates the maximum time difference permitted between the individual devices that should all run synchronously in H.235. This value is not supplied by HiPath 3000/5000, it must be configured manually.

Gatekeeper ID:

Gatekeeper ID. This value is not supplied by HiPath 3000/5000, it must be configured manually.

11.1.5 "Protocol" Tab

Call: Main Menu > Element Manager > Element Manager Configuration > "Protocol" Tab



Maximum number of Protocols

Maximum number of protocol files.

Value range: 1 ... 20.

Date

Time of synchronization with the Element Manager identified in the **Element Manager ID** column.

Status

Identification status. This column may contain one of the following values:

- **OK**
- **Not OK**
- **Cancelled**
- **OK (partially failed)**

Result

Contents of the protocol file.

Possible Action Buttons

Logfile

Click this button to view the log file.

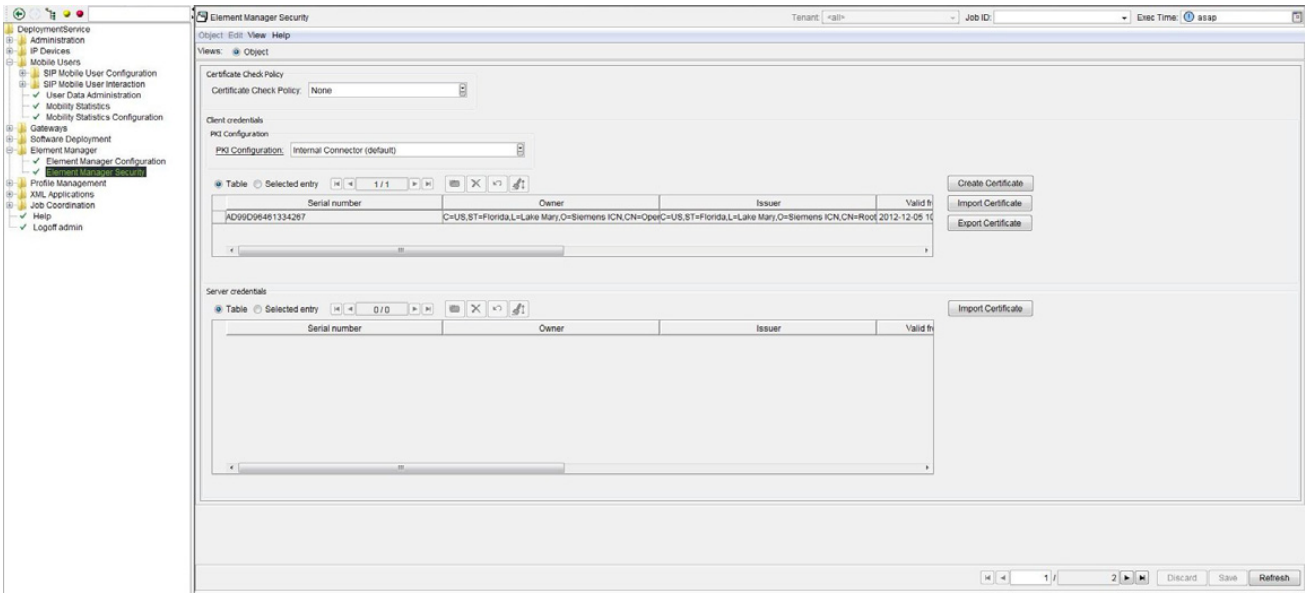
NOTE: In the case where no content is shown in the Protocol tab,you should clear the IE cache. To achieve this,proceed with the following instructions :

1. In the Windows Start Menu,open **Start** > **Settings** > **Control Panel**.
2. Double-click **Internet Options**.
3. Click on the **General Tab**.
4. Click the **Delete** button under the **Browsing History** section.
5. In the **Delete Browsing History** click **Delete** by ensuring that only **Temporary Internet files** and **Cookies** are checked.
6. Click **OK**,then **Close**.
7. Relaunch your browser.

11.2 Element Manager Security

Call: Main Menu > Element Manager > Element Manager Security.

This area is used to configure the 802.x Certificates that are employed for the Client & Server HTTPS/TLS connections with the Element Manager servers. The administrators are also able to configure the Certificate Check Policy.



Certificate Check Policy

Certificate Check Policy

Possible values :

- **None** (default)- no authentication of the remote entity performed

  The remote entity is not checked at all or any potential errors during the check are ignored

  This is the default value, since both Trusted and Full require administrative steps anyway by configuring the associated (root) CA certificate(s).

  IMPORTANT: Even if the Security Check Policy is set to "none",a valid client Certificate generated from the same RootCa should still be uploaded.

- **Partial -** the certificate (including certificate chain) provided by the remote entity is checked.

a) the chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates, which are preconfigured for that interface on the product

b) all certificates in the chain are not expired (i.e. current date/time is within the certificate's given validity period)

c) no certificate in the chain is revoked[1]

- **Full** - the certificate (including certificate chain provided by the remote entity is checked against the same criteria as in Trusted mode, plus :

a) for correct end entity identity (according to settings in SubjectAlternativeName (SAN) and/or the common name (CN) in the Subject)

b) for correct use of all critical extensions (e.g. Basic constraints, Key Usage, Extended Key Usage). If an extension is marked critical and is not recognized, the certificate must be rejected.

c) for correct use of known extensions not marked as critical (e.g. Basic constraints, Key Usage, Extended Key Usage)

Client Credentials

The Client certificate is the one that is sent to the H8K during SSL handshake.The Client certificate can be issued by the DLS PKI infrastructure or imported to the DLS(by default a SEN ROOT signed client certificate is installed with the installation of DLS.)

The Client Certificate should be trusted by the H8K (this means that H8K’s truststore should be configured properly).

1 Revocation checks are done using OCSP (Online Certificate Status Protocol) or based on CRL (Certificate Revocation Lists); Revocation checks are controlled via independent configuration items and apply to both Full and Trusted mode. See more details in the section below.

12 Profile Management

Call: Main Menu > Profile Management

This menu consists of the following submenus:

- Device Profile
- User Data Profile
- Template Overview

12.1 Device Profile

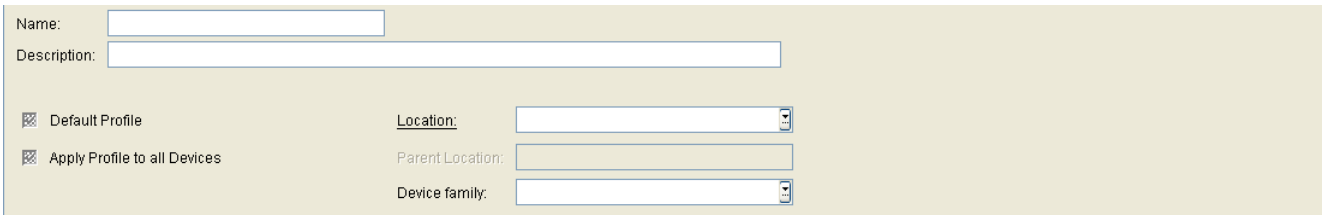
Call: Main Menu > Profile Management > Device Profile

This area features the following components:

- General Data
- Possible Action Buttons
- "Templates" Tab
- "Supported Devices of IP Device" Tab
- "Tenants" Tab
- "Parent Profiles" Tab

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of profiles, and for entering parameters which are valid for all tabs. The base data associated with the profiles found is displayed in the Object view.



Name:

Profile name.

Description:

Brief description of the profile.

Default Profile

If this check box is activated, the profile is also used during Plug & Play registration on new that have not entered this profile under **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"Profile" Tab** > **Device Profile**. In order to use the default profile during Plug & Play, the following checkbox must be enabled :

- **Default Profile** checkbox under **Profile Management** > **Device Profile**

The profile can only be used if the location and device type for the profile and the IP device match - unless the switch **Apply Profile to all Devices** is active. This profile is also used when registering a IP device for which the **Apply Default Profiles at IP Device Registration** check box is activated (**Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"General" Tab**).

IMPORTANT: As of **CV323** onwards, devices/subscribers that do not belong to the Default Location (as seen under IP Device Configuration > "General" Tab > field: Location), will not be deployed by a Default Profile belonging to the Default Location.
Only devices that have not met the criteria of other specific Locations and can be considered as left-out from exclusive Location conditions will get the Default Location assignment. Only then and only for those "left-out" devices (in the context of Location definition) can receive a Default Profile that has been configured to point to a Default Location.
This negates to the old behavior (**CV322** backwards), where a Default Profile pointing to the Default Location was intended to be deployable to all devices irrespectively of the exclusive Location those devices could have been assigned.

To use Location Service IP Infrastructure, a default device profile has to be defined and assigned to the IP Infrastructure location.

Apply Profile to all Devices

If this check box is activated, the current default is assigned to all devices that are not entered in the **Supported Devices** list.

Location

Location where the selected profile should apply as the default profile.

Parent Location

If available, also the templates of the parent location’s default profiles are displayed.

Device Family

The profile is valid for the device family specified here.

Possible options:

- **IP Phone**
- **IP Client**
- **IP Gateway**
- **Mediatrix Gateway**

Possible Action Buttons

Search

Searches for Device Profiles that meet the search criteria.

Clear Window

Deletes the content of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new Device Profile.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Export Profile

Export the selected Device Profiles to a file in zip format.

Import Profile

Import a Device Profile from a file in zip format.

12.1.1 "Templates" Tab

Call: Main Menu > Profile Management > Device Profile > "Templates" Tab

You can define an appropriate template here. You can add another template in the **New** and **Object** view with the button and delete it with the button.



Template Name

Name of the selected template.

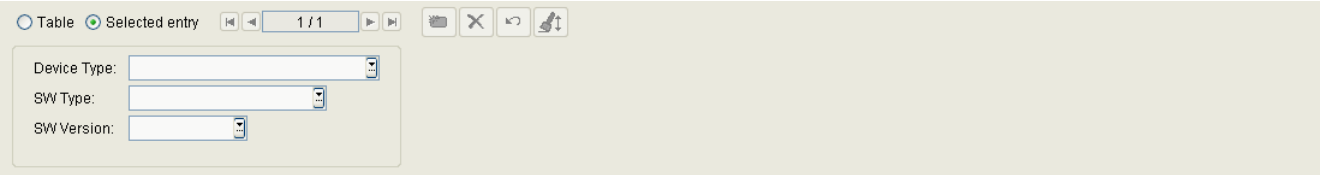
Multiple Add

Adds multiple templates to one Device Profile.

12.1.2 "Supported Devices of IP Device" Tab

Call: Main Menu > Profile Management > Device Profile > "Supported Devices of IP Device" Tab

You can define the IP Devices that should be supported by the profile here. You can add another device in the **New** and **Object** view with the button and delete it with the button.



Device Type

IP Device type.
All IP Devices supported by DLS can be found in Section 3.4, "Area of Application".

Examples: **optiPoint 410 standard**, **optiClient 130**, **Mediatrix3xxx**, **Mediatrix41xx**, **Mediatrix44xx**

SW Type:

Type of software for the device.

Examples: **Unify HFA**, **Unify SIP**.

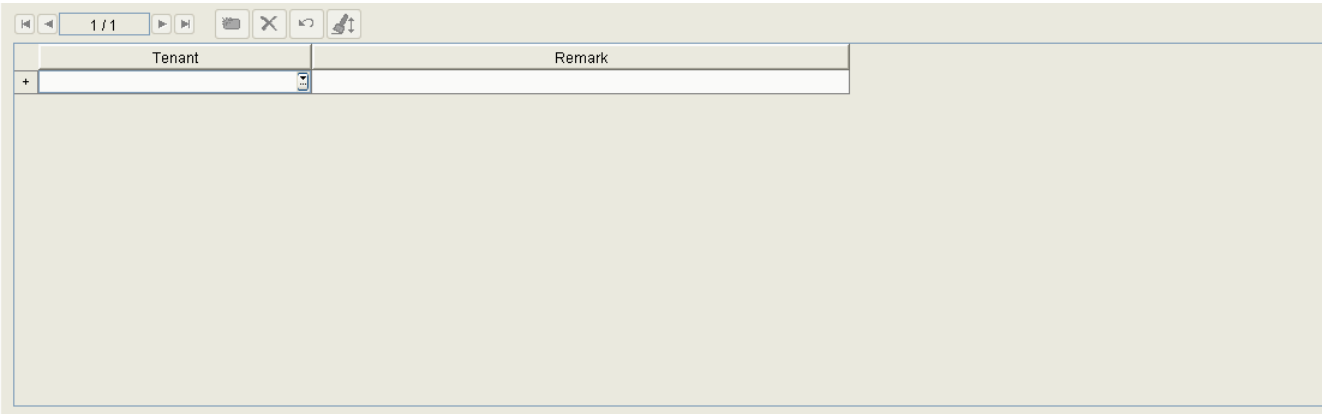
SW Version

Example for optiPoint and optiClient: **5.0.12**.

12.1.3 "Tenants" Tab

Call: Main Menu > Profile Management > Device Profile > "Tenants" Tab

NOTE: This tab is available only if the Multi-Tenancy function of the DLS is installed.



Tenant

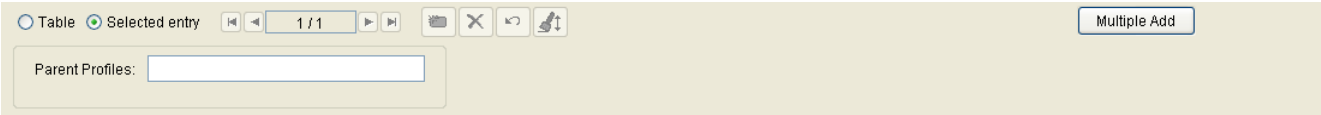
Name of the tenant.

Remark

Information on the tenant.

12.1.4 "Parent Profiles" Tab

Call: Main Menu > Profile Management > Device Profile > "Parent Profiles" Tab



Parent Profiles

Name of parent location’s profiles.

Multiple Add

Add multiple templates to one profile.

12.2 User Data Profile

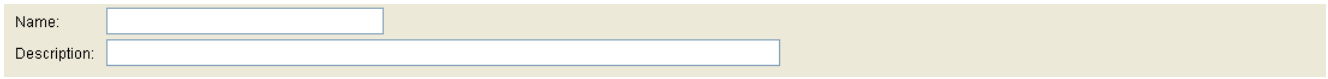
Call: Main Menu > Profile Management > User Data Profile

This area features the following components:

- General Data
- Possible Action Buttons
- "Templates" Tab
- "Tenants" Tab

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of profiles, and for entering a description. The base data associated with the profiles found is displayed in the Object view.



Name:

Profile name. The defined profiles may be eighter used as Mobile User Profile in **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User** > „**"Mobile / Basic User" Tab** or as Basic Profile in **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"Profile" Tab**.

Description:

Brief description of the profile.

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all User Data Profiles that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

New

Creates a new User Data Profile.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Export Profile

Export selected User Data Profiles into a zip file.

Import Profile

Import User Data Profiles from a zip file.

12.2.1 "Templates" Tab

Call: Main Menu > Profile Management > User Data Profile > "Templates" Tab

You can define one or more templates for the user data profile here. You can add another template in the **New** and **Object** view with the button and delete it with the button.



Template Name

Name of the template.

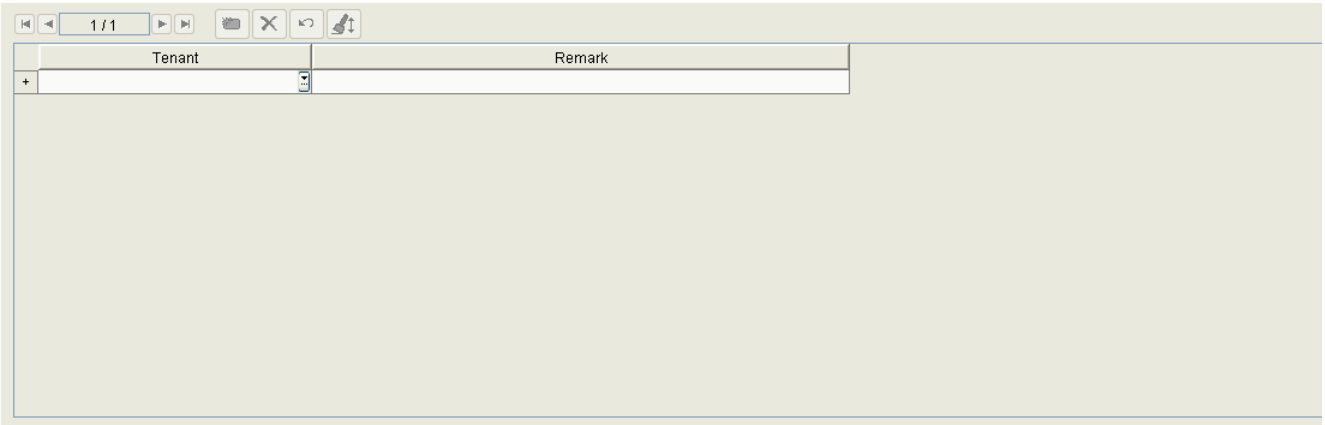
Multiple Add

Adds multiple templates to one User Data Profile.

12.2.2 "Tenants" Tab

Call: Main Menu > Profile Management > User Data Profile > "Tenants" Tab

NOTE: This tab is available only if the DLS multi tenancy function is installed.



Tenant

Name of the tenant.

Remark

Information on the tenant.

12.3 Template Overview

Call: Main Menu > Profile Management > Template Overview

Use this area to

- search for existing templates,
- change the name and the description of templates,
- delete templates, and
- export all templates in XML format into a .zip file or import them from a .zip file. Single templates can be imported from a .zip file as well.

Changes to template attributes and attribute values are not possible here. For more information, see Section 15.7, "Editing Templates".

IMPORTANT: If data changes are made in configuration forms that have been generated using templates, these changes are not automatically applied to the templates.
These changes must be manually saved to the template (Section 15.7, "Editing Templates").

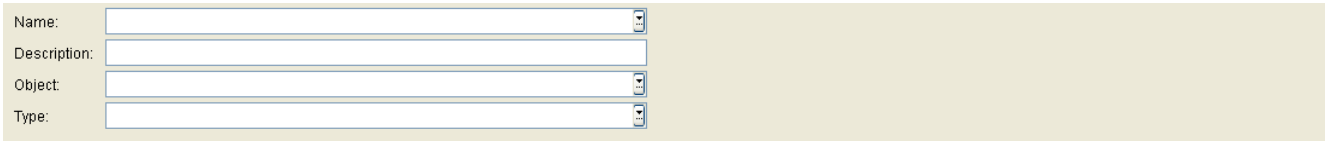
This area features the following components:

- General Data
- Possible Action Buttons
- "Template data" Tab
- "Profiles" Tab
- "Tenants" Tab

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the content area is used for entering parameters in **Search** view to find a specific group of templates, and for importing and exporting template data. The base data associated with the templates found is displayed in the **Object** view (no changes possible).



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

Name:

Name of the template.

Description:

Description of the template.

Object:

Template object type.

Example: **IP Phone SNMP Settings**

Type:

Specifies the type of parameters stored in the template.

Possible entries:

- **IP client**
- **IP phone**
- **User Data**

Possible Action Buttons

The range of action buttons available depends on the selected view and DLS status.

Search

Searches for all template that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves any unsaved changes.

Discard

Discards any unsaved changes.

Delete

Deletes one or more templates (multiple selections possible in table view).

Refresh

Refreshes the content of the relevant page.

Import Template

Import templates in XML format from a zip file. Single templates can be imported from a .zip file as well. They are selected by name in a popup window.

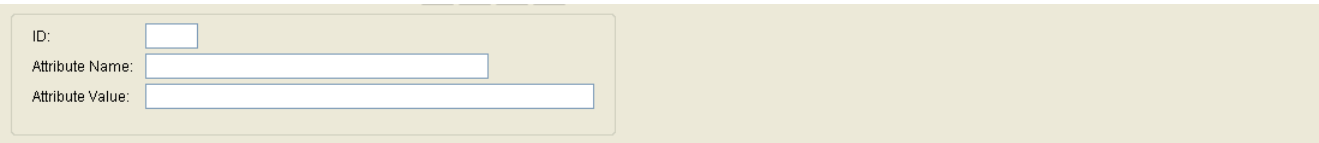
NOTE: Existing templates with the same name are overwritten during an import.

Export Template

Export the selected templates in XML format to a .zip file. Multiple template selection is possible in table view. A pop-up window prompts you to enter the file path.

12.3.1 "Template data" Tab

Call: Main Menu > Profile Management > Template Overview > "Template data" Tab



ID

ID for improved sorting (for example, for key assignments).

Attribute Name

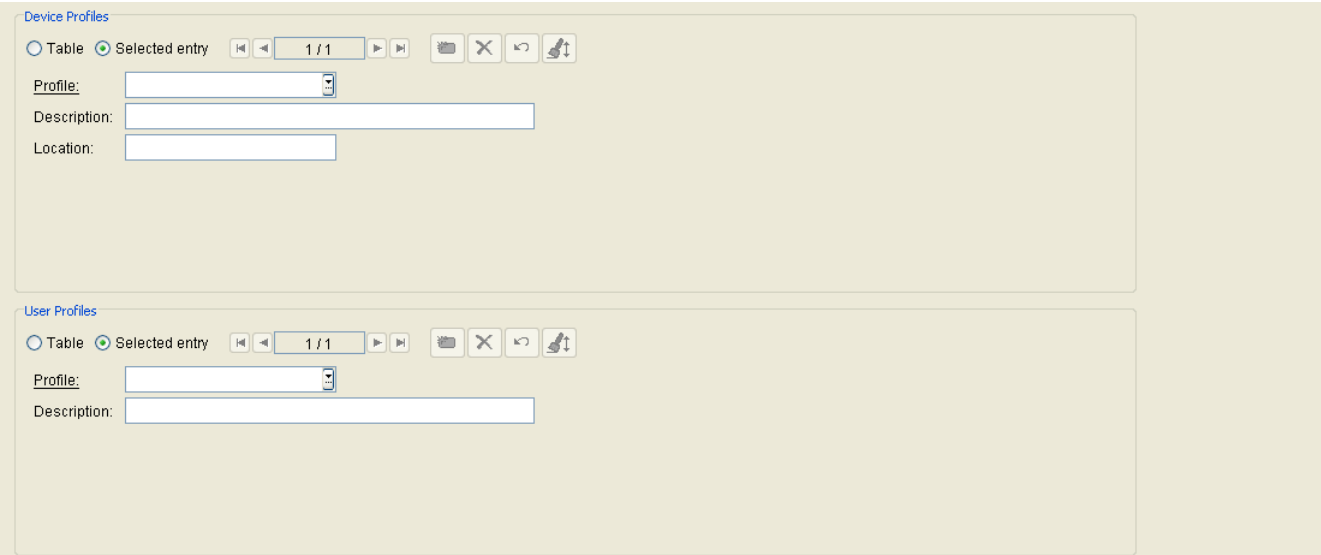
Name of the attribute defined in the template.

Attribute Value

Value of the relevant attribute name.

12.3.2 "Profiles" Tab

Call: Main Menu > Profile Management > Template Overview > "Profiles" Tab



Device Profiles

Profile

Name of Device Profile.

Description

Description of Device Profile.

Location

Location of Device Profile.

User Data Profiles

Profile

Name of User Data Profile.

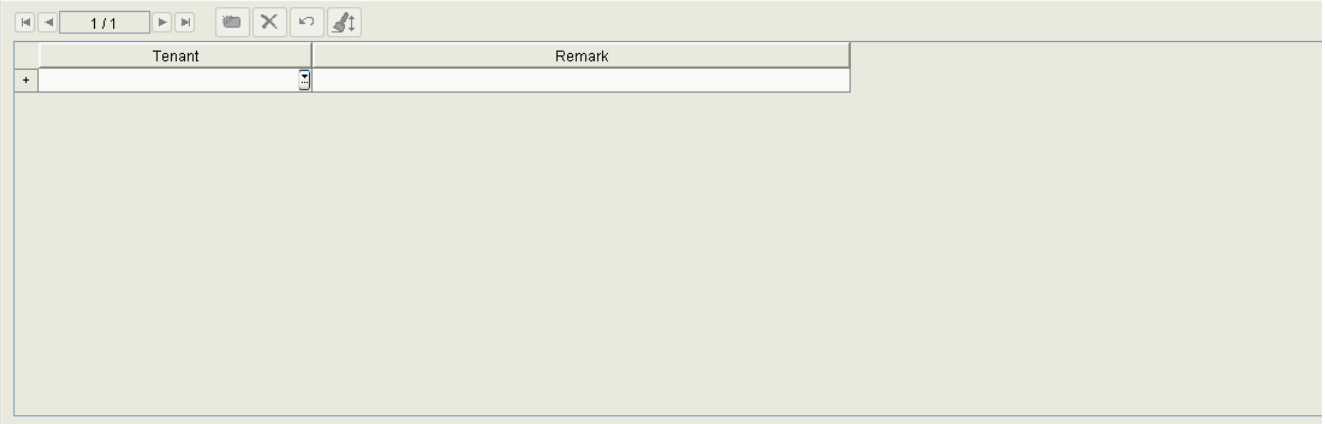
Description

Description of User Data Profile.

12.3.3 "Tenants" Tab

Call: Main Menu > Profile Management > Template Overview > "Tenants" Tab

NOTE: This tab is available only if the Multi-Tenancy function of the DLS is installed.



Tenant

Name of the tenant.

Remark

Information on the tenant.

13 XML Applications

Call: Main Menu > XML Applications

The DLS can be used not only for installing and configuring XML applications, but also as application server itself.

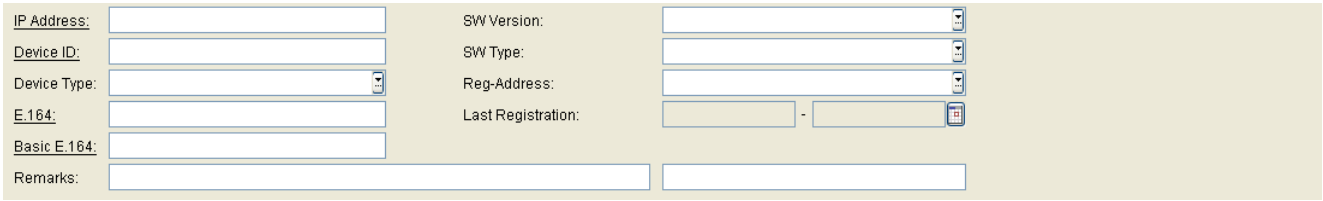
NOTE: XML applications are available only for OpenStage 60 and OpenStage80 with firmware versions SIP V1, SIP V2, and HFA V2.

This menu item consists of the following areas:

- MakeCall
- NewsService
- NewsService Archive

General Data

This part of the contents area is identical for the applications **MakeCall** and **NewsService**. It is used for entering parameters in **Search** view to find a specific group of IP phones for configuring and executing XML applications. If **Object** view is selected, the base data associated with the IP phones found is displayed.



IP Address:

IP address of the IP phone. For OpenStage, an IPv4 or IPv6 address is displayed here.

Example: **192.117.1.193**

The value is read-only if it was dynamically assigned with DHCP.

Device ID:

ID for unique identification of the IP device. In IP phones, this is generally the MAC address.

Example: **00:0E:A6:85:71:80**

Device Type:

IP phone device type. The icon indicates whether this is a virtual device.

All IP phone types supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **OpenStage 60**

E.164:

Complete E.164 subscriber number (Basic Profile or Mobile Profile).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

Basic E.164:

Complete E.164 phone number (Mobility Phone).

Example: **498972212345**

For information on the meaning of the E.164 station number in relation to mobility, see Section 3.8.3, "Mobility ID".

SW Version:

Software version of the IP phone.

Example: **5.0.12**

Information on the difference between the software and license version can be found in Section 15.9, "Distribution of Workpoint Software".

SW Type:

IP phone software type.

Examples: **Unify HFA**, **Unify SIP**.

Reg-Address

IP address or DNS name of the HFA or SIP server at which the device is registered.

Last Registration:

Time of last IP phone registration.

For information on selecting a time segment for a search, see Section 5.4.2.4, "Time field with calendar button".

Remarks:

Fields for general information.

13.1 MakeCall

Call: Main Menu > XML Applications > MakeCall

This mask enables the start (=push) of the XML application 'MakeCall'. This application initiates calls from selected end devices to a target end device. After this, it is possible to check in the call log whether all calls have been executed. This check makes sense after a software update, for instance. The application can only be started from the DLS only, not from the end devices.

To start the function, press the **MakeCall** action button. Then, a dialog window will request the target call number.

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

Possible Action Buttons

The range of action buttons available depends on the selected view, the selected XML application, and the DLS status.

Search

Searches for all registered workpoints that match the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

MakeCall

Pushes the XML application ’MakeCall’. A subsequent dialog window asks the **MakeCall Destinationnumber**.

Send Info Alert

Pushes the XML Application ‚NewsService'. A subsequent dialog window asks for the **Header** and **Text** of the message.

Send Text-/Picture-File

Pushes the XML Application ’NewsService’. A subsequent dialog window asks for the name of the **Text-/Picture-File**.

Delete

Deletes the saved news.

Refresh

Refreshes the window contents from the database.

13.1.1 "Info" Tab

Call: Main Menu > XML Applications > MakeCall > "Info" Tab



MakeCall Destinationnumber

Displays the destination number for the last automatic call initiated by the XML Application ’MakeCall’.

13.2 NewsService

Call: Main Menu > XML Applications > NewsService

This screen enables the start (=push) of the XML application 'NewsService'. This application sends messages to selected end devices. These can be text or picture files. There is a distinction between an info alert message and a file message. On an info alert, the message is displayed on the end device along with an 'INFO' symbol, until it is confirmed by a button press. File messages are displayed on the end device within the application tab 'NewsService'.

The messages are created and sent by means of the DLS. Stored messages can be read again at the end device. To send a message, press **Send Info Alert** or **Send Text-/Picture File**. Then, a dialog window will ask for the **Header** and **Text** of the message, or for the name of the **Text-/Picture-File**.

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab

13.2.1 "Info" Tab

Call: Main Menu > XML Applications > NewsService > "Info" Tab



Info Alert Header

Header of the last Info Alert sent to IP Device by means of XML Application 'NewsService'.

Info Alert Text

Text of the last Info Alert sent to IP Device by means of XML Application 'NewsService'.

Text-/Picture File

Name of last Text- (.txt) or Picture-File (.jpg, .bmp, .gif, .png) sent to IP Device by means of XML Application 'NewsService'.

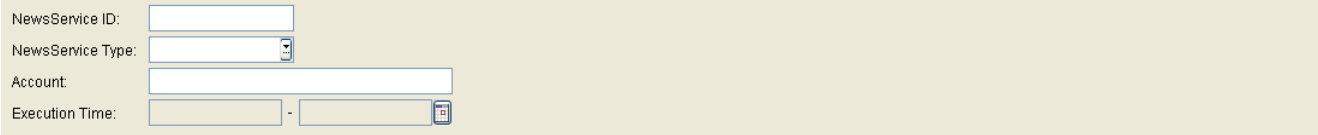
13.3 NewsService Archive

Call: Main Menu > XML Applications > NewsService Archive

This area features the following components:

- General Data
- Possible Action Buttons
- "Info" Tab
- "IP Devices" Tab

General Data



NewsService ID

Continuous numbering

NewsServiceType

Type of message.

Possible Values:

- **Info Alert**
- **Picture File**
- **Text File**

Account

Account name of the user who issued the message.

Execution Time

Execution time of the message sending job.

13.3.1 "Info" Tab

Call: Main Menu > XML Applications > NewsService Archive > "Info" Tab



Info Alert Header

Header of info alert sent to IP Device.

Info Alert Text

Text of info alert sent to IP Device.

Text File

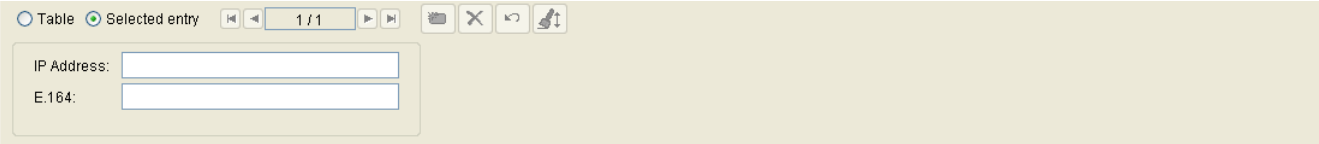
Name of text file sent to IP Device.

Picture File

Name of picture file sent to IP Device.

13.3.2 "IP Devices" Tab

Call: Main Menu > XML Applications > NewsService Archive > "IP Devices" Tab



IP Address

IP Address of IP Device the news is sent to.

E.164

Complete E.164 subscriber number of IP Device the news is sent to.

14 Job Coordination

Call: Main Menu > Job Coordination

This menu consists of the following submenus:

- Job Control
- Daily Status
- Job Configuration

More complex deployment tasks are performed in the **Job Coordination** area. This area is used for configuring, performing, and logging deployment jobs (see also the operating sequence in Section 15.10).

14.1 Job Control

Call: Main Menu > Job Coordination > Job Control

This area features the following components:

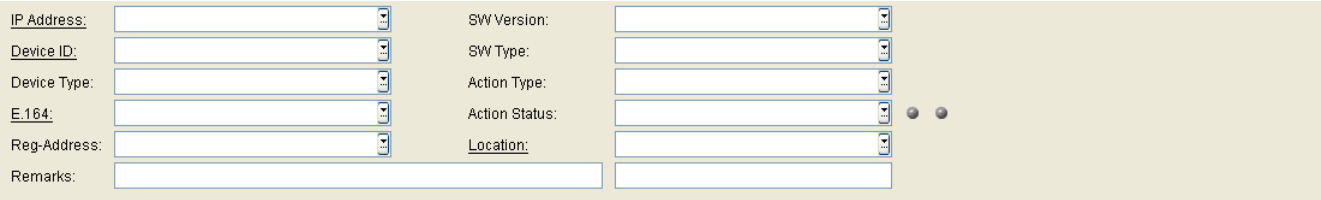
- General Data
- Possible Action Buttons
- "Basic Data" Tab
- "Deployment Data" Tab
- "Configuration Data" Tab
- "XML Application Data" Tab

This function lets you view a large volume of information on the individual jobs and discard, delete, or reactivate existing jobs. New jobs are not created here but rather by defining the activities to be performed in the job (for an example, see Section 15.10, "Using Job Coordination").

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of jobs. The base data associated with the jobs found is displayed in the Object view.



NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

IP Address:

IP address of a IP Device or an address range.

In the case of jobs for IP ranges, **000.000.000.000** is displayed here in the **Search** view.

Format: **000.000.000.000**, 000 = value between 000 and 255.

Device ID:

Device ID of an IP Device or address range.

In the case of jobs for device ID areas, **00:00:00:00:00:00** is displayed here in the **Search** view.

Format: XX:XX:XX:XX:XX:XX, XX = Hex value between 00 and FF.

Device Type:

IP Device type.

In the case of jobs for different device types, nothing is displayed here in the **Search** view.

Format: Up to 30 characters.

All IP Devices supported by DLS can be found in Section 3.4, "IP Devices / versions supported".

Example: **optiPoint 410 standard**, **optiClient 130**

E.164:

Complete phone number of an IP Device.

In the case of jobs for different phone numbers, nothing is displayed here in the **Search** view.

Job Coordination
Job Control

Format: Up to 15 characters.

See also Section 17.1, "E.164".

Reg-Address

IP address or host name of the registry server where the IP Device is registered.

SW Version:

Software version of an IP device.

In the case of jobs for different version numbers, nothing is displayed here in the **Search** view.

Example for optiPoint and optiClient: **5.0.12**.

SW Type:

Type of Software to be downloaded.

In the case of jobs for different software types, nothing is displayed here in the **Search** view.

Examples: **Unify HFA**, **Unify SIP**.

Action Type:

Possible options:

- **IP Device Configuration**
- **IP Device Notification**
- **Mobile User Configuration**
- **Mobile User Migration**
- **Software Deployment**
- **Music on Hold File Deployment**
- **LDAP Template File Deployment**
- **INCA Firmware Deployment**
- **Java Midlet Deployment**
- **Logo File Deployment**
- **Application and Systemtone Deployment**

- **System and Ringtone Deployment**
- **APM Firmware Deployment**
- **Netboot Deployment**
- **IP Device Notification**
- **Screensaver Deployment**
- **File Deployment**
- **Scan IP Devices**
- **Read IP Device Data**
- **Read specific IP Device Data**
- **Reset IP Device**
- **Restore Factory Setting**
- **Gateway Configuration**
- **Read Gateway Data**
- **Gateway Probe**
- **Mobile User Logon**
- **Mobile User Logoff**
- **Push XML Application**
- **File Upload**

Action Status:

Possible action status:

- **expired**
  A timeout occurred when executing the deployment job because the time entered for **Job Configuration** was exceeded, for example, by an IP Device that was unavailable for an extended period of time. The job can be cancelled and deleted with the result that no more actions are performed for the job.
- **cancelled**
  The deployment job was cancelled. In the case of cancelled jobs, only the time of execution is modified (to re-start the job at a future time). The job can be deleted.
- **active**
  The deployment job was entered in the job table but has not started running because the execution time, for example, has not yet been reached. The job can be cancelled and deleted with the result that no more actions are performed for the job.

- **confirmed**
  The deployment job was accepted by the IP Device and waits until the status of the IP Device permits processing. The job can be cancelled and deleted with the result that the job execution is no longer interrupted.
- **failed**
  The deployment job was started but could not be executed. The job can be cancelled and deleted.
- **finished**
  The deployment job was executed correctly. The job can be cancelled and deleted.
- **running**
  The deployment job is currently being executed. The job can be cancelled and deleted with the result that the job execution is no longer interrupted.
- **waiting**
  The deployment job is queued, it was entered in the job table but has not started running because the IP Device is busy.The job status can turn to **active** if the amount of time that the job has been in **waiting** status exceeds a configurable upper limit.

NOTE: The **waiting** status option is only supported in Openstage V3R3 phones.

Status Indicator for Jobs

The status indicator for a job can be reset over a pop-up menu by clicking **Reset Status** (see Section 5.4.1, "Main Menu").

Left hand indicator ball:
Job is not running.
Job is waiting.
Job is running.

Right hand indicator ball:
Job has been executed without errors.
Job has been cancelled with errors.

Location:

Current location of the IP Device.

Remarks:

Fields for general information, remarks (e.g.comments) for each job.

These fields are editable for all job types and all job statuses.

NOTE: Editable fields under Job Control that reflect values carried over from an initial action (e.g. a Remark note over a subscriber), are considered editable only in the context of Job parameters and will not reflect back the changes to the initial record from which the job itself has been originated.

Possible Action Buttons

Search

Searches for all deployment jobs that correspond to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

Save

Saves changes to the existing deployment job. The Save option is only available after a change to an interrupted job.

Discard

Discards changes to the existing deployment job. The Discard option is only available after a change to an interrupted job.

Delete

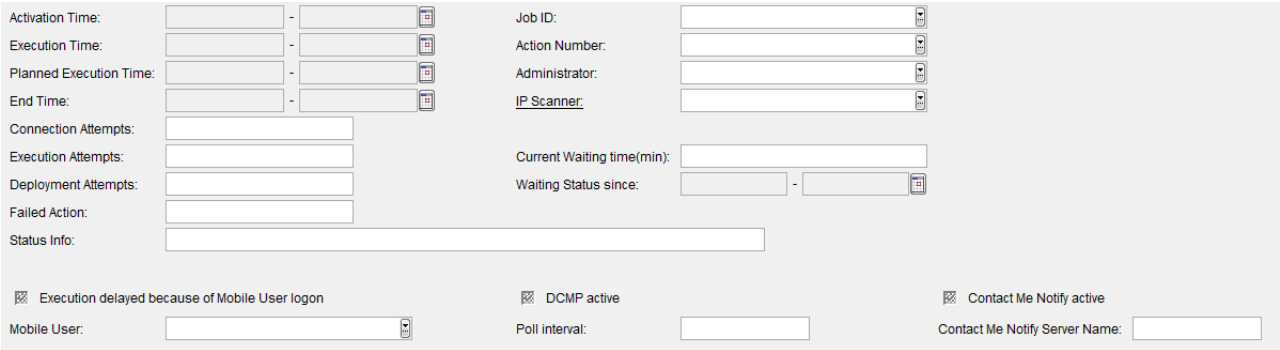
Deletes the deployment job displayed in the **Object** view.

Cancel Job

Interrupts the deployment job displayed in the **Object** view.

14.1.1 "Basic Data" Tab

Call: Main Menu > Job Coordination > Job Control > "Basic Data" Tab



Activation Time:

Time for the activation of the deployment job (see Section 5.4.2.4, "Time field with calendar button").

Execution Time:

Time for the execution of the deployment job (see Section 5.4.2.4, "Time field with calendar button").

> ***NOTE:*** Interrupted deployment jobs can be reactivated by entering a future point in time.
> For all other job statuses, the time displayed here indicates the time of execution, irrespective of whether it is in the past or the future.

Planned Execution Time:

Time when the deployment job will be started.

> ***NOTE:*** For devices running in different timezones, device local time +/- timeshift related to the timezone is displayed.

End Time:

Time for ending the deployment job (see Section 5.4.2.4, "Time field with calendar button").

> ***NOTE:*** For deployment jobs that were already executed, the time at which these job were ended is displayed here.

Connection Attempts:

Number of retries needed to perform the job (**0** means not yet executed).

Execution Attempts:

Number of execution retries needed to perform the job (**0** means not yet executed).

Deploy Attempts:

Number of deployment retries needed to perform the job (**0** means not yet executed, only for deployment jobs).

Failed Action:

In the job table, this is the number of the action that could not be successfully completed and caused DLS to automatically generate and execute a **Read IP Device Data**.

The field only contains one value for jobs of the type **Read IP Device Data** generated by the DLS. The administrator is shown as **@DLS** for these jobs.

Status Info:

Messages can indicate the successful completion of a deployment job as well as to a fault. The following status messages are output (sorted in alphabetical order based on the **Status Info**):

Status Info	Description	Trigger
action type not implemented[1]	-	neutral
equal item names	Identical entry names.	IP phone
failed	Failed.	IP phone
file-not-found	Error, for example, when opening stored templates or when opening the deployment file.	IP client
ignored - dial plan error	Error in the numbering plan.	IP phone
image path not contactable	Removed image path is not available.	IP client
initiated	The job was initiated but not yet finished.	neutral
internal ERROR[1]	-	neutral
invalid data	Invalid data.	IP phone
invalid format	Invalid format.	IP phone
invalid function key	Invalid function key.	IP phone
invalid Index	Invalid Index.	IP phone
invalid item name	Invalid item name.	IP phone

Status Info	Description	Trigger
local deployment path not specified	Item "dls-deployment-local-path" is not set.	IP client
local deployment path not writable	Local deployment path not writable.	IP client
missing item content	Missing item content.	IP phone
missing item name	Missing item name.	IP phone
nonce not valid[1]	-	neutral
not a Feature Toggle key	Not a Feature Toggle key.	IP phone
not a line key	Not a line key.	IP phone
not a repertory dialing key	Not a Repertory Dialing key.	IP phone
not a selected dialing key	Not a selected dialing key.	IP phone
not implemented	Not implemented.	IP phone
not readable	Not readable.	IP phone
not supported	Not supported.	IP phone
OK	Deployment was successful.	neutral
read only	Read-only.	IP phone
server-not-contactable	The remote server is not available.	IP client
Self Labeling Key Sidecar not available	The optiPoint Self Labeling Key Module is not available.	IP phone
unknown item	Unknown item.	IP phone
not a DSS key	Not a DSS key.	IP phone

1 For internal debugging only; Not relevant for the DLS user.

Job ID:

ID of the jobs. The Job ID is the name that was entered when the job was created (see Section 5.4.2.1, "Toolbar"). If a name was not entered, the action number is used for the job ID.

The job ID for jobs that distribute and activate a PSS (Pre-Shared Secret) are prefixed with PSS.

Action Number:

Action number of the job. This sequential number is automatically generated for every action in every deployment job (one for each IP address edited).

Administrator:

User names for this job. The name corresponds to the user who defined the action. Enter **@DLS** as the name for automatically generated actions.

NOTE: This field corresponds to which DLS account has performed an action for which a job has been created inside DLS's Job Control list.

NOTE: The Administration user **@DBUpdateVirtualDevices** is an alias for the admin user used for the Element Manager related scheduled tasks.

IP Scanner:

IP scanner for this job. The name is set when the IP scanner is configured, see Section 7.5.6, "Scan IP Devices".

Execution delayed because of Mobile User logon

The job is delayed because of Mobile User logon.

Mobile User:

Mobile User currently logged on.

DCMP active

If this check box is activated, the device periodically checks for DLS jobs on the DCMP (DLS Contact-Me Proxy).

Poll Interval

Interval (in minutes) between two polls from the device to the DCMP.

Contact Me Notify active

If this check box is enabled, the Contact Me Notify functionality is activated.

Contact Me Notify Server Name

The name of the unique Contact Me Notify Server (32 characters).

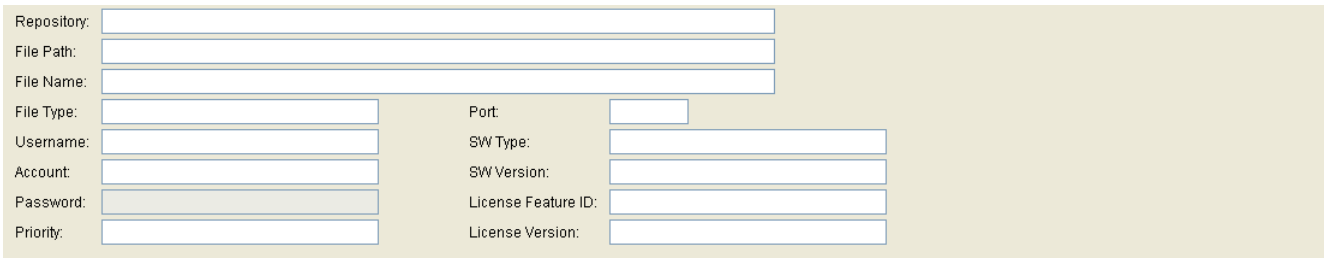
14.1.2 "Deployment Data" Tab

Call: Main Menu > Job Coordination > Job Control > "Deployment Data" Tab

The software deployment data is displayed here for jobs with the following action types.

- **INCA Firmware Deployment**
- **Java Midlet Deployment**
- **LDAP Template File Deployment**
- **Logo File Deployment**
- **System and Ringtone Deployment**
- **Software Deployment**
- **Music on Hold File Deployment**

Data for a job may be available in either the "Deployment Data" Tab or the "Configuration Data" Tab.



Repository:

IP address or host name of the FTP server (for IP phones) or network computer (for IP clients) from which the software is downloaded.

File Path:

Directory on the FTP server (for IP phones) or on the network computer (for IP clients) from which the software is downloaded. In the case of IP phone software, the path begins with the configured "virtual" root directory. For IP client software, it begins with the shared network path.

File Name:

The file name of the software downloaded.

File Type:

Deployment type of the file downloaded.

Examples:
INCA (INCA firmware deployment)
MIDLET (Java midlet deployment)
LDAP (LDAP template file deployment)
LOGO (Logo file deployment)
RINGTONE (System and ringtone deployment)
APP (Software deployment)
MOH (Hold music file deployment)

Username:

Username ("login") of the FTP access to the server from which the software is downloaded.

Account

Not currently used in DLS.

Password:

Password of the FTP access to the server from which the software is downloaded.

Priority:

Signals whether deployment should pause when a IP Device is busy and wait until it frees up (**normal**) or if deployment should be performed at the set time irrespective of the IP Device status (**high**).

Port:

Port used for the FTP server from which the software is downloaded. Permanently set to port 21.

SW Type:

Software type of the software that is downloaded (for software deployment).

Examples: **Unify HFA**, **Unify SIP**.

SW Version:

Software version of the IP Device.

Example for optiPoint: **5.0.12**.

License Feature ID:

If the downloaded software requires a license, then this field contains the product ID (HLM terminology) used for registering the software in HiPath License Management (for software deployment).

Example for optiPoint 410 standard HFA: **OPTI410STDHFA**.

License Version:

If the downloaded software requires a license, then this field contains the product version (HLM terminology) used for registering the software in HiPath License Management (for software deployment).

Example for optiPoint only: **6.0.0**

14.1.3 "Configuration Data" Tab

Call: Main Menu > Job Coordination > Job Control > "Configuration Data" Tab

Configuration data for jobs with the **IP Device Configuration** action type is displayed here.

All configuration data for this job is displayed in tabular form.

Data for a job may be available in either the "Deployment Data" Tab or the "Configuration Data" Tab.



Parameter

Name of the parameter used to perform modifications in this job.

Index

Index within the parameter you want to change (if available).
If a IP Device parameter can accept more values (value list), an index is created for each value. The field remains empty if there is only one value.

Old Setting

Value of the parameter before the change. Only wildcards are displayed here if the parameter is a password.

New Setting

Value of the parameter after the change. Only wildcards are displayed here if the parameter is a password.

User Data

If this check box is active, user-specific data was sent to the IP device instead of device-specific data (display only).

Finished

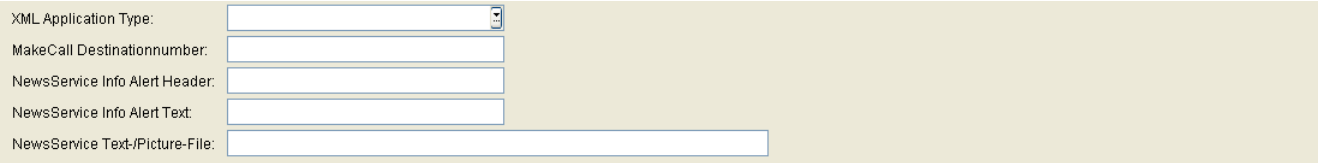
Indicates if the parameter has already been changed.

Status Info

Information on the job status.

14.1.4 "XML Application Data" Tab

Call: Main Menu > Job Coordination > Job Control > "XML Application Data" Tab



XML Application Type:

Type of XML application that has been started with this job.

Possible Options:

- **MakeCall**
- **NewsService File Display**
- **NewsService Info Alert**

MakeCall Destinationnumber:

Dialing number of the end device to which an automatic call has been initiated by the XML application 'MakeCall'.

NewsService Info Alert Header:

Header of the latest info alert message that has been sent to the end device by means of the XML application ’NewsService’.

NewsService Info Alert Text:

Text of the latest info alert message that has been sent to the end device by means of the XML application ’NewsService’

NewsService Text-/Picture File:

File name of the latest text (.txt) or picture file (.jpg, .bmp, .gif, .png) that has been sent to the end device by means of the XML application ’NewService’:

14.2 Daily Status

Call: Main Menu > Job Coordination > Daily Status

This area features the following components:

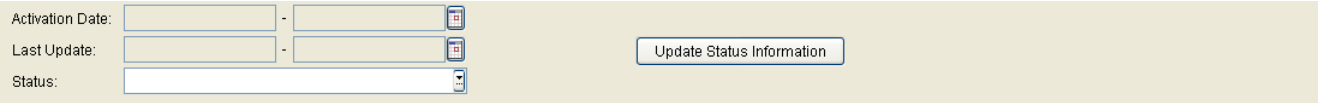
- General Data
- Possible Action Buttons
- "Status Information" Tab

This function gives you a clear display of all jobs in a table. Additionally, you may search for Job Status or Job ID. In addition to the job found according to the requested Job Status, all jobs belonging to the same day will be displayed. In object view, you can switch between entire table view or individual table entries. The table can be sorted by Job ID, Job Status, Activation Time, or End Time.

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the contents area is used for entering parameters in Search view to find a specific group of jobs. The data associated with the jobs found is displayed in the Object view.



Activation Date:

Time for the activation of the deployment job (see Section 5.4.2.4, "Time field with calendar button").

Last Update

Date of the last status information update.

Status:

Possible action status:

- **active**
  The deployment job was entered in the job table but has not started running because the execution time, for example, has not yet been reached.
- **failed**
  The deployment job was started but could not be executed.
- **finished**
  The deployment job was executed correctly.
- **running**
  The deployment job is currently being executed.

Update Status Information

Set status information to the current state, including all jobs that have been created on the current day.

> ***NOTE:*** When pressing this button, the database is updated accordingly.
> By pressing the **Refresh** button, the updated info is displayed on the **Status Information Tab**.Please refer to Section 14.2.1, ""Status Information" Tab"

Possible Action Buttons

Search

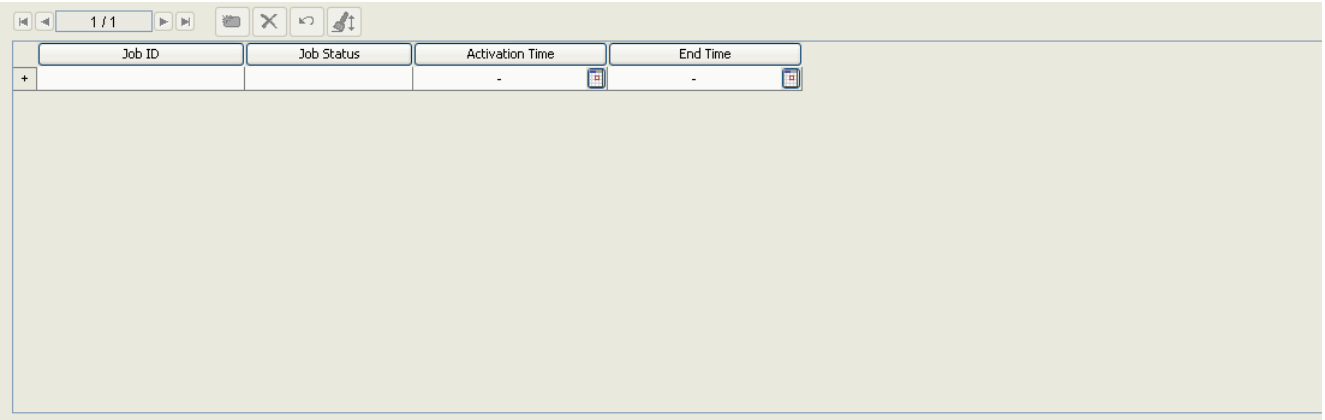
Searches for all statistical data that corresponds to the search criteria.

Clear Window

Deletes the contents of all fields in this view. Existing entries can therefore be deleted in the **Search** view before new search criteria are entered.

14.2.1 "Status Information" Tab

Call: Main Menu > Job Coordination > Daily Status > "Status Information" Tab



Job ID

Job ID (or the action number) of the deployment job.

Job Status

Status of the deployment job.

Activation Time

Time of activation for the deployment job.

End Time

For jobs with the status **finished**: time of end of execution.

14.3 Job Configuration

Call: Main Menu > Job Coordination > Job Configuration

This area features the following components:

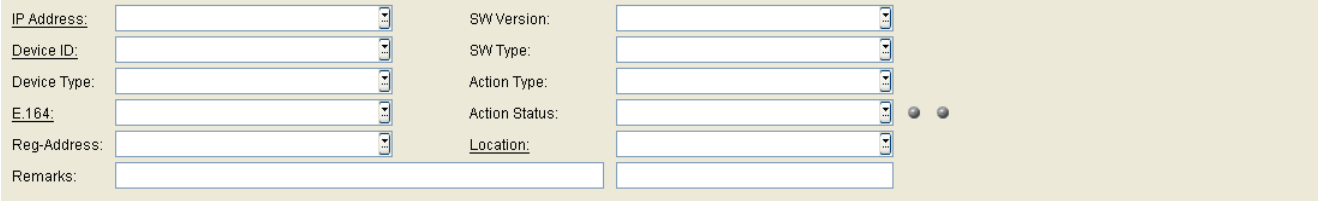
- General Data
- Possible Action Buttons
- "IP Phones" Tab
- "IP Clients" Tab
- "IP Gateways" Tab
- "Gateways" Tab

This function can be used to influence the behavior of a job. Some configuration data can be entered differently for IP phones and IP clients.

For information on general interface operation, see Section 5.4.2, "Work Area".

General Data

This part of the contents area is used for entering parameters which are valid for all tabs.



Limit of concurrent Jobs:

Maximum number of deployment jobs that can be performed simultaneously. If the number of jobs to be started according to the execution time is greater than number of jobs entered, retries would automatically be started for all jobs involved.

Default: 100.

Delete Finished Jobs after Days:

Number of days after which ended jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 10.

Delete Cancelled Jobs after Days:

Number of days after which interrupted jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 10.

Delete Expired Jobs after Days:

Number of days after which expired jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 10.

Delete Failed Jobs after Days:

Number of days after which interrupted jobs should be deleted. Jobs with other statuses are not affected by this.

Default: 99999 (failed jobs are not deleted).

Default Job Execution Option:

Default value for the time of job execution.

Possible options:

- **Immediately**
  The job is started immediately.
- **Immediately or after registration**
  The job is started immediately. If it should fail, another attempt will be made on registration of the device.
- **After registration**
  The job is started on registration of the device.

Save Finished Jobs

Check box for activating the option that allows jobs to be left in the job table and displayed in the job statistics.

Default: **activated**

Possible Action Buttons

Save

Saves the changes you made under **Job Configuration**.

Discard

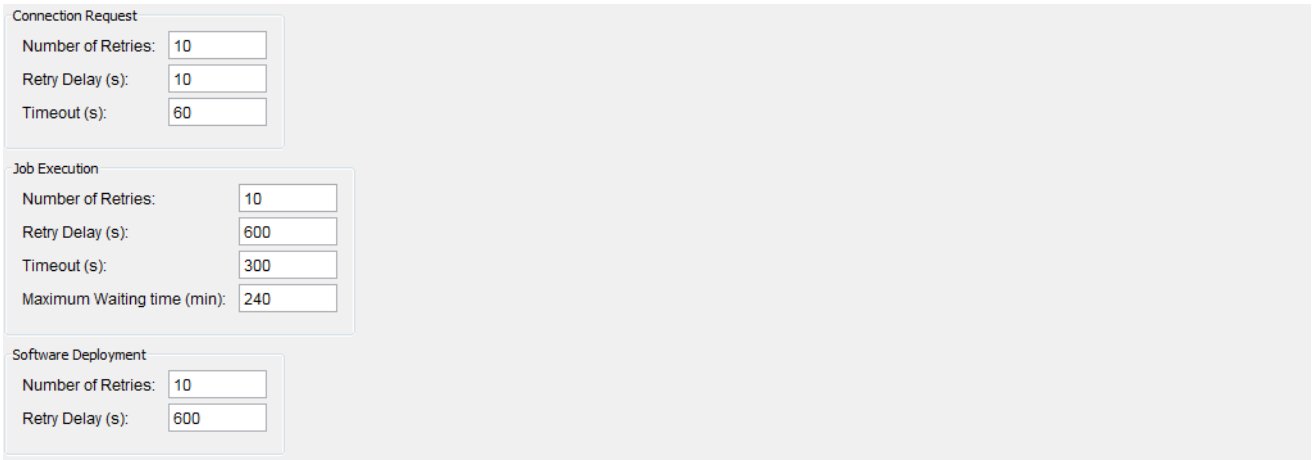
Discards the changes you made under **Job Configuration**.

Refresh

Refreshes the content of the relevant page.

14.3.1 "IP Phones" Tab

Call: Main Menu > Job Coordination > Job Configuration > "IP Phones" Tab



Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be cancelled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Default: **10** Value range: **1** - **3600**

Timeout (sec):

Time in seconds that the DLS waits for an IP phone answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Coordination

Job Configuration

Job Execution

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be cancelled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

Time limit for complete job execution, including all retries.

Value range: **30** - **3600**

Default: **300**

Maximum Waiting time (min):

Total amount of time in minutes that a job can remain in **Waiting** status.

Value range: **30**- **720**

Default: **240**

NOTE: Waiting time is increased every time a job enters the 'Waiting' state and reset on each new job execution attempt.

NOTE: Waiting time does not count in the job execution timer.

Software Deployment

Number of Retries:

Number of retries permitted before the software deployment for IP phones should be cancelled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two software deployment retries for IP phones.

Value range: **1** - **3600**

Default: **600**

14.3.2 "IP Clients" Tab

Call: Main Menu > Job Coordination > Job Configuration > "IP Clients" Tab



Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Value range: **1** - **3600**

Default: **10**

Timeout (sec):

Time in seconds that the DLS waits for an IP phone answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Number of Retries:

Number of retries permitted before the execution of a job for IP phones should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP phones.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

Time limit for complete job execution, including all retries.

Value range: **30** - **3600**

Default: **300**

14.3.3 "IP Gateways" Tab

Call: Main Menu > Job Coordination > Job Configuration > "IP Gateways" Tab



Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for IP gateways should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP gateways.

Value range: **1** - **3600**

Default: **10**

Timeout (sec):

Time in seconds that the DLS waits for an IP gateway answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Number of Retries:

Number of retries permitted before the execution of a job for IP gateways should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **100**

Default: **10**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for IP gateways.

Value range: **1** - **3600**

Default: **600**

Timeout (sec):

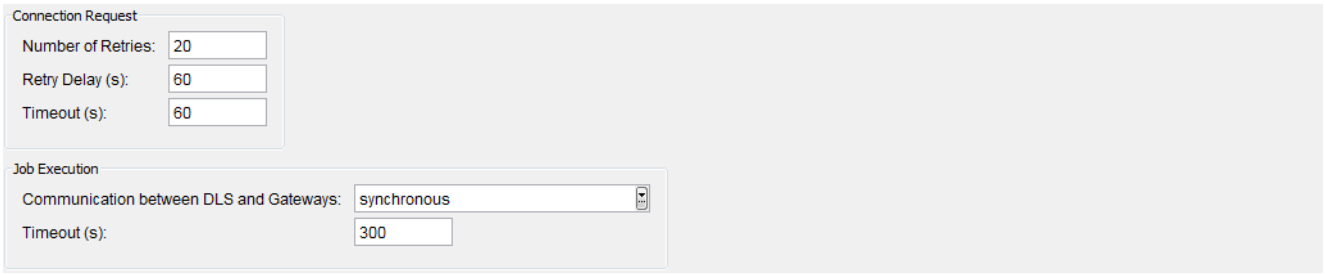
Time limit for complete job execution, including all retries.

Value range: **30** - **3600**

Default: **300**

14.3.4 "Gateways" Tab

Call: Main Menu > Job Coordination > Job Configuration > "Gateways" Tab



Connection Request

Number of Retries:

Number of retries permitted before the execution of a job for gateways should be canceled after a set number of automatic retries with the status **cancelled**.

Value range: **1** - **200**

Default: **20**

Retry Delay (sec):

Time in seconds that should elapse between two automatic job retries for gateways.

Value range: **10** - **3600**

Default: **60**

Timeout (sec):

Time in seconds that the DLS waits for a gateway answer for each attempt if a job is performed.

Value range: **1** - **3600**

Default: **60**

Job Execution

Communication between DLS and Gateways:

Possible options:

- **synchronous**
  The jobs are executed synchronously. The display on the DLS stops responding (the hourglass appears) until these actions are fully complete. Clicking **Refresh** always results in the current data record.
- **asynchronous**
  The jobs are executed in the background allowing you to continue working in parallel. To see the result, you must wait a little and then click **Refresh**. If you refresh too soon, the old data record is returned as a result.

Timeout (sec):

Time limit for complete job execution, including all retries.

Value range: **1** - **3600**

Default: **300**

15 Operating Sequences

This chapter contains the following practical sequences:

- Configure a user account that never expires
- Bulk deletion of default device files
- First Steps: Changing IP Device Parameters

  NOTE: This section provides fundamental operating information - also helpful for performing other functions.

- Changing the Element Manager Configuration and Creating Jobs
- Registering Workpoint Software and Files
- Editing Templates
- Workpoint Autoconfiguration (Plug&Play)
- Distribution of Workpoint Software
- Using Job Coordination
- Backup/Restore
- Automatic Restore on Upgrade Failure
- Importing and Exporting Plug&Play Data
- Copy Macro for P&P and Templates

For information on general interface operation, see Section 5.4.2, "Work Area".

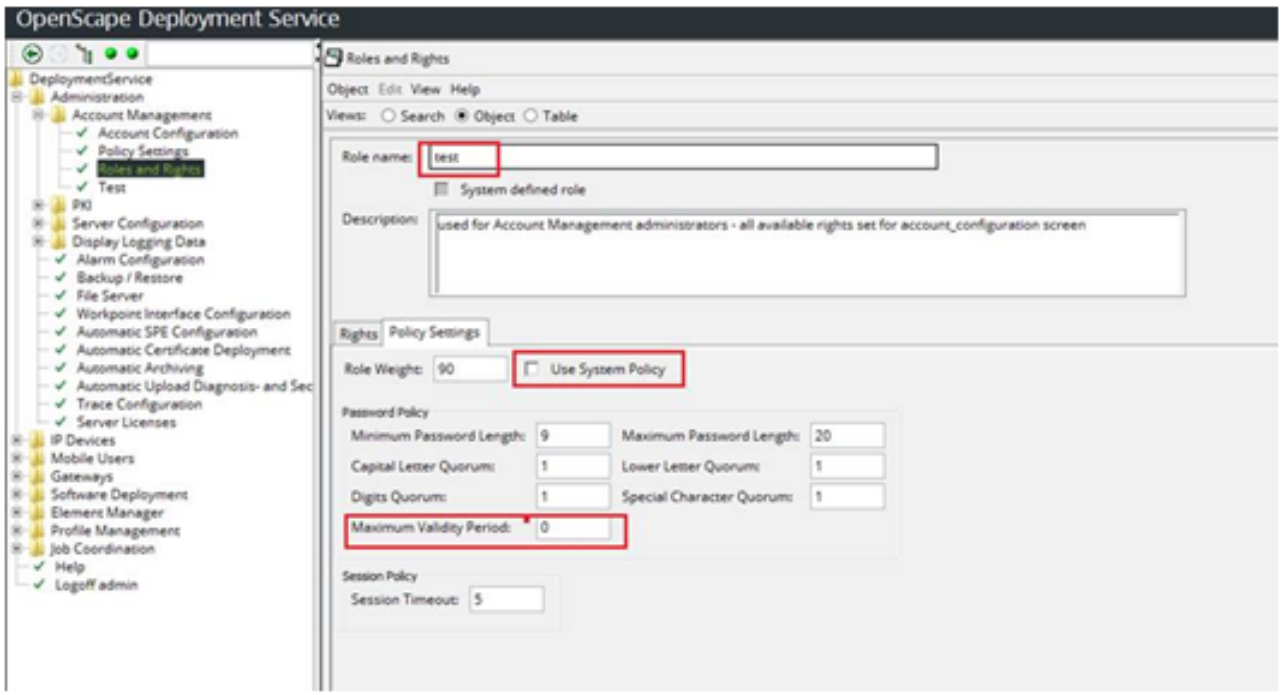
NOTE: The sequence descriptions provided here are intended as examples. The actual sequence may vary from the description, depending on the particular DLS configuration, the servers or IP Devices used, and the ongoing development of the DLS.

15.1 Configure a user account that never expires

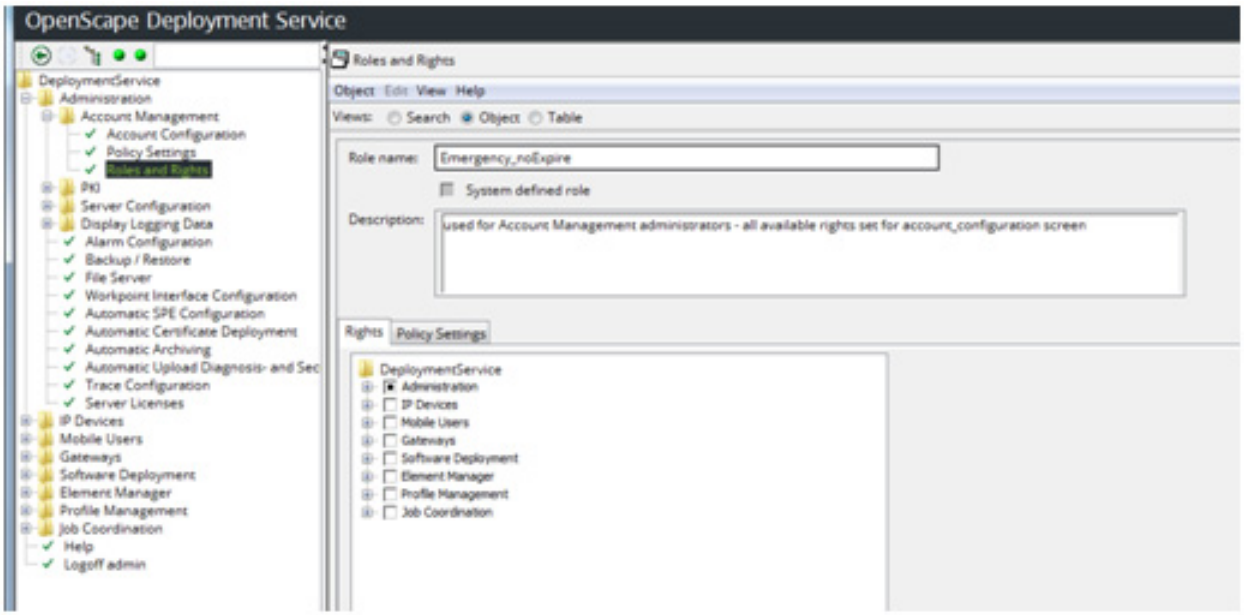
In case you want to configure a DLS user whose password never expires without altering other user settings (remaining users may have passwords that will expire) then refer to the following process:

You may use an existing account or create a new one and assign to that account a custom role where you have configured **Maximum Validity Period** set to zero. In that role disable **Use System Policy**. Then configure remaining parameters (lengths and quorums) as required not to be overriden by defaults.

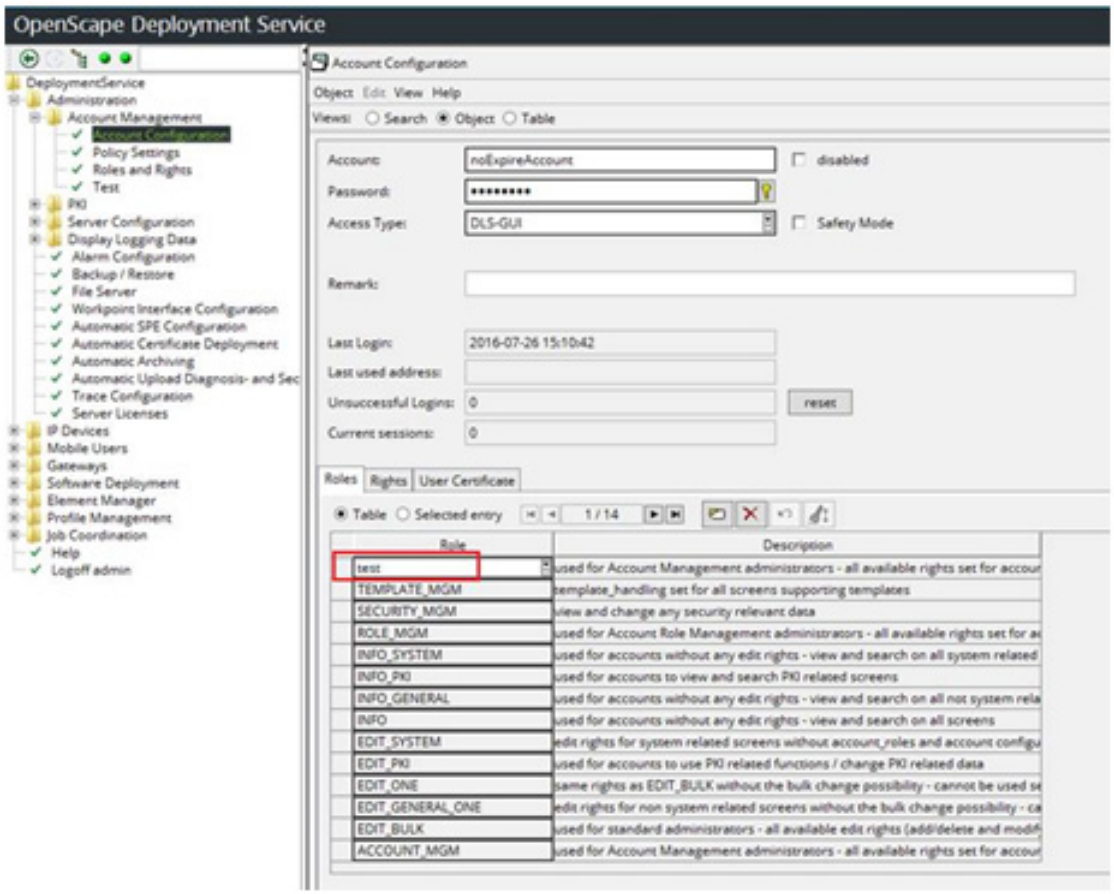
1. Create custom role with the required Rights and Policy Settings with **Maximum Validity Period** configured to zero. Also disable **Use System Policy**.



2. Give administration rights to the role.



3. Assign this role to a new or existing account.



15.2 Bulk deletion of default device files

It could be observed that a mass deletion of default files contained within devices is only successful for the actively selected device inside the DLS when performing the bulk action and not for the whole selected list. The above restriction is not applicable for the files that have been previously deployed by the DLS. Please, follow the workaround below for a bulk deletion of default ringtones, logos and screensavers :

12. Place those default files contained with the involved devices inside an FTP server configured for DLS use.
13. Execute a full Scan of the involved FTP server(s) from within the DLS GUI.
14. Point under Main Menu > Call: Main Menu > Call: Main Menu > > IP Phone Configuration > File Deployment, and in **Table** view select all the devices that have the default files needed to be deleted. Press the **Read** button.
15. After the procedure is finished (jobs are completed), the **SW Image Name** field is not empty anymore and now DLS can perform bulk deletions.
16. Under the same GUI, select again the devices and the file or files to be deleted and press **Save**. This time the bulk procedure will be successful for the whole selection of devices.

15.3 First Steps: Changing IP Device Parameters

In many areas of the DLS (for example, **Call: Main Menu > Call: Main Menu >**), you can use the database running in the DLS to select all or a subset of the total number of IP Devices available for subsequent administration. This takes place in the working area using **Search** view (see Section 5.4.2.3).

Requirements for this example: the DLS, the servers and IP Devices are operational.

1. In the main menu, select an area where you would like to change something under **Call: Main Menu > Call: Main Menu >**.
2. Select **Search** view (see Section 5.4.2.3) if it is not yet shown.
3. Indicate the IP Devices you want to select.
   Do this by choosing an entry in the selection list field, for example, beside **Device Type** (see Section 5.4.2.4) or enter an IP address range.

   NOTE: For further information about the **Search** view, please see Section 5.5, "Search Functionality".

   If you want to search through all available IP Devices, do not enter any information in the fields in Search view.
4. Click **Search** (see Section 5.4.2).
5. If no matching data was found, a message appears in the message window (see Section 5.4.2.6).

   If the search was successful, the display changes to **Object** view, which always shows the data for a single IP Device. You can use the navigation buttons (see Section 5.4.2.5) to scroll through all IP Device data that corresponds to the search filter.

6. Click **Table** in the view bar to change to List view. Click a column header to sort the entire table according to the value specified in the header (alternating between ascending and descending).

   Click between two column headers and drag the mouse right or left to change the width of the left-hand column.

   Click a column header and drag the mouse right or left to change the order of the columns.

7. Now you can change any fields that have not been dimmed. This is possible in both **Object** view and **Table** view.

8. To transmit the changes to a single IP Device, click **Save**. This sends the data directly to the IP Device.

   NOTE: If you would like to transmit the changes to multiple IP Devices simultaneously, change to **Table** view before you save the changes and mark additional IP Device entries in the list (see Section 5.4.2.4, "Multiple selection and data transfer in Table view" for information on how to do this).

   Click **Save**. This sends the data directly to the selected IP Devices.

15.4 Changing the Element Manager Configuration and Creating Jobs

Changes made in the Element Manager configuration under **Element Manager** > **Element Manager Configuration** (for example, E.164 prefix, gatekeeper ID, SIP server address, etc.) are forwarded to the relevant workpoints. The ID of this Element Manager is entered in the **Element Manager ID** field on these workpoints under **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"EM Synchronization" Tab**. However, if a different Element Manager (or Element Manager ID) is entered under Referenced Element Manager, this one is valid.[1]A modification (of the E.164 prefix, for example) can take several minutes, depending on the number of workpoints.

Jobs are created for registered workpoints in the Element Manager configuration during modification. A dialog appears before the modifications are implemented, displaying the number of jobs and requesting confirmation of the action. You can save the configuration changes here without immediately creating jobs. The jobs are then automatically created (no confirmation required) during the next automatic or manual synchronization.

A synchronization that has been started but is not yet finished prevents the initiation of other synchronization operations for this Element Manager or Element Manager ID. A corresponding message appears in the window. The same message appears if you try to modify the Element Manager configuration while an (automatic) synchronization is running.

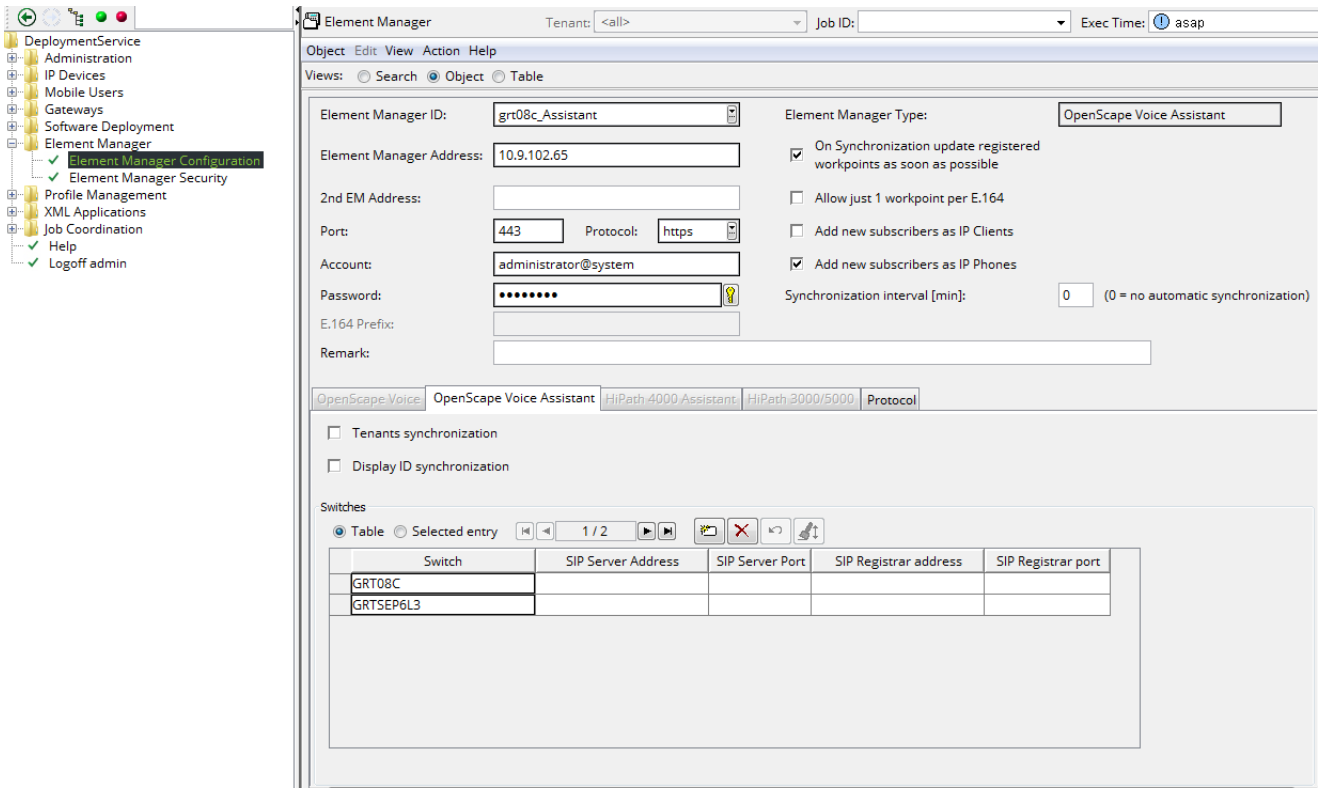
1 This parameter is used when preparing to relocate a station to another system. Two data records exist during this operation with the same E.164 number and different device IDs. One of the data records is assigned to system A, the other to system B. The parameter defined here ensures that during synchronization between both systems, only the data record belonging to a particular system is updated.

15.5 How to replace OSV Assistant Manager with OSV Element Manager

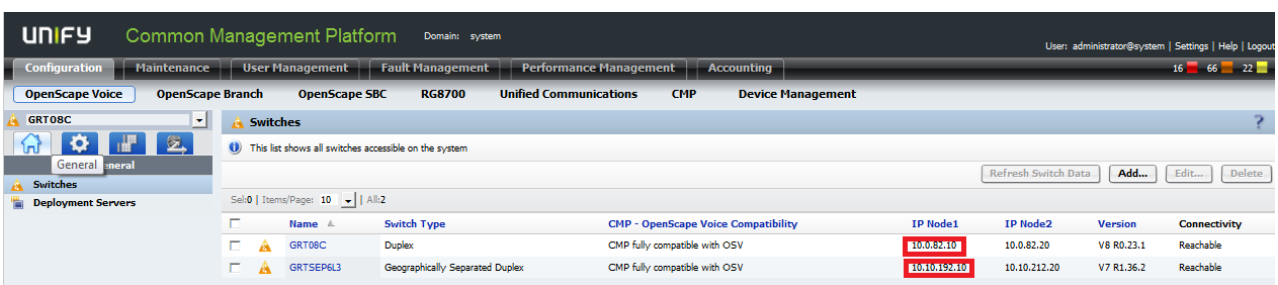
The OSV Element Manager is enhanced to cover all the functionality offered by the OSV Assistant EM (synchronization per BG and secure connection).Therefore the OSV Assistant EM becomes obsolete and given the fact that it does not support Delta synchronization, it is strongly recommended that any configured OSV Assistant EM in DLS should be replaced with OSV EM(s).

Please refer to the following detailed steps for this procedure:

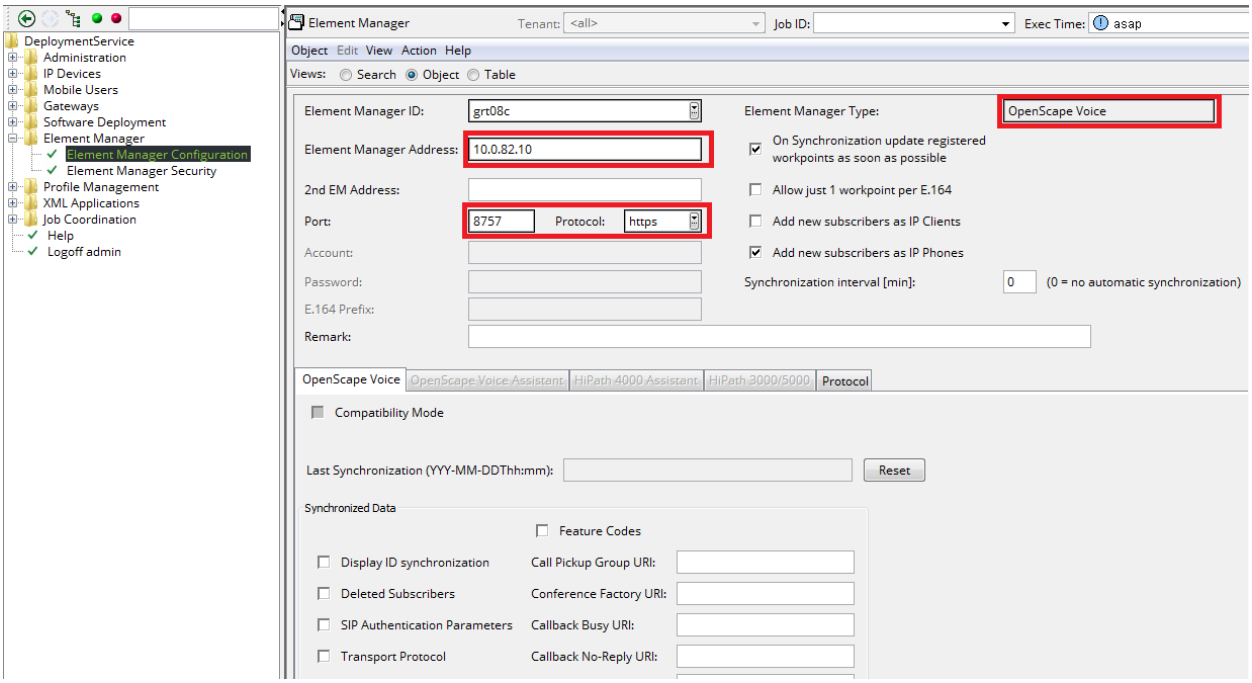
1. Go to Main Menu > Element Manager > Element Manager Configuration and search for any OSV Assistant EM entries:



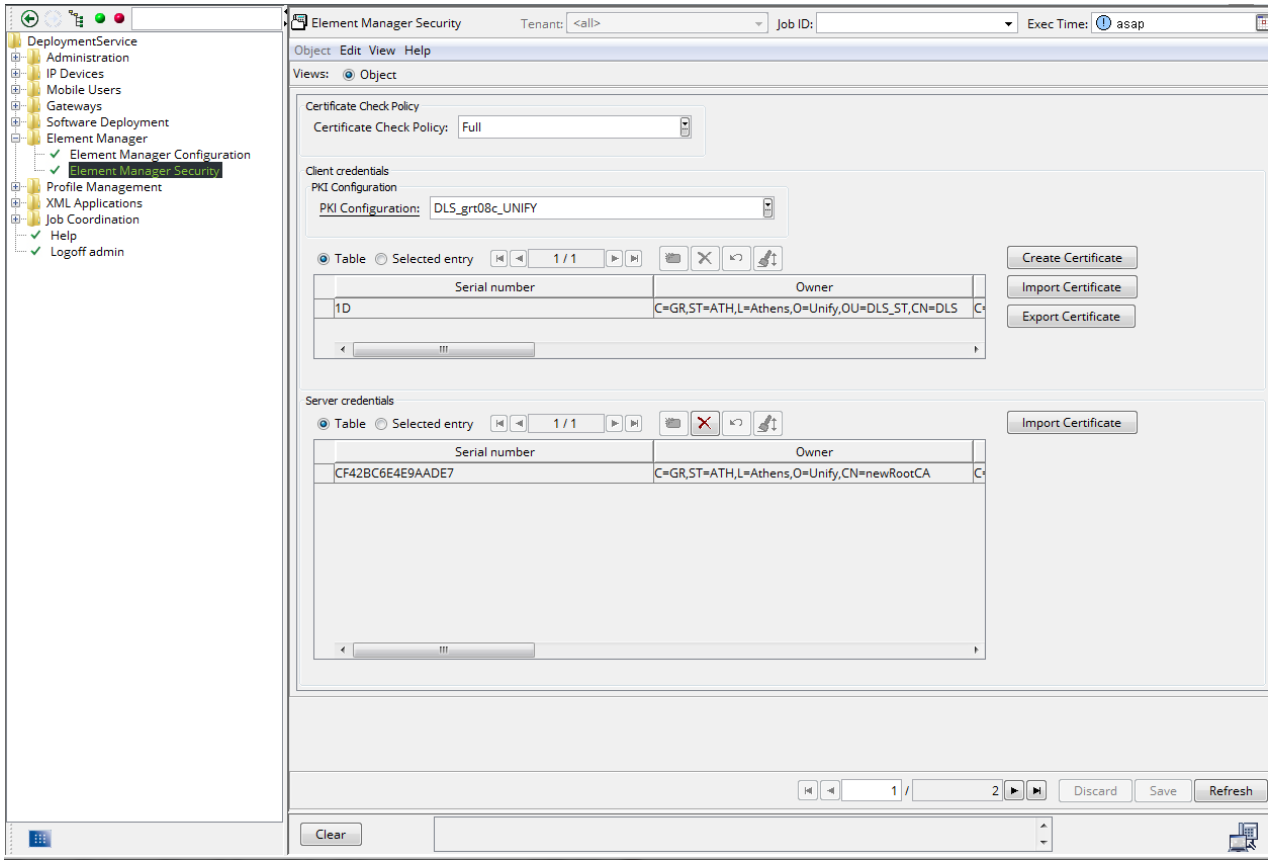
2. Get the Element Manager Address (**10.9.102.65** according to the example) and connect to the CMP portal. Under Configuration > OpenScape Voice > Switches, all the configured OSV switches are displayed:



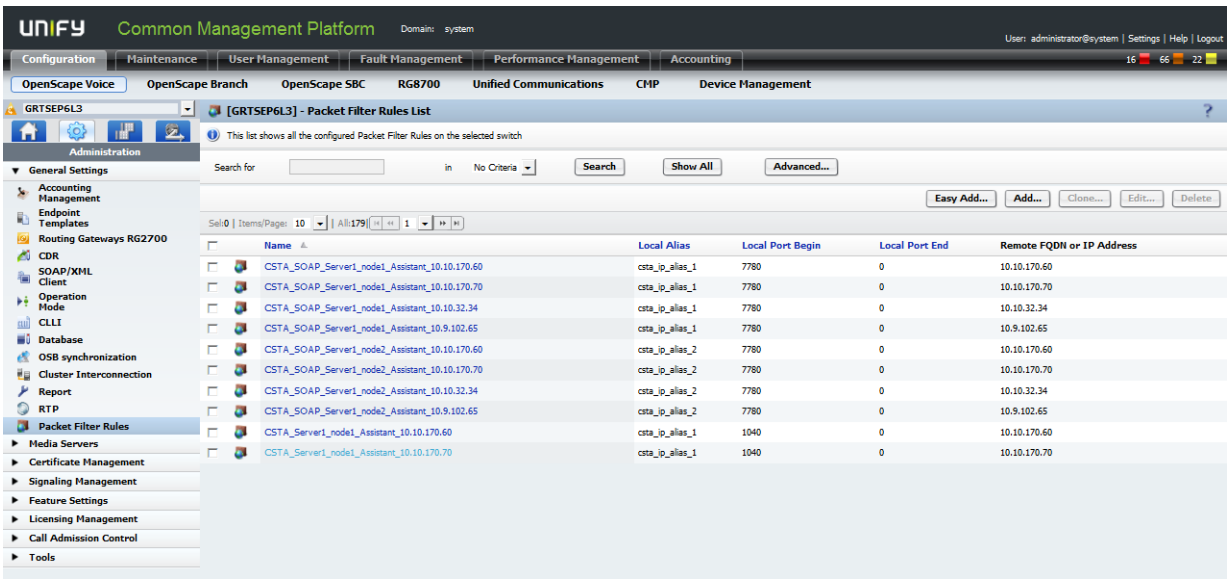
3. For every OSV switch listed above, create a new Element Manager in DLS as shown below:

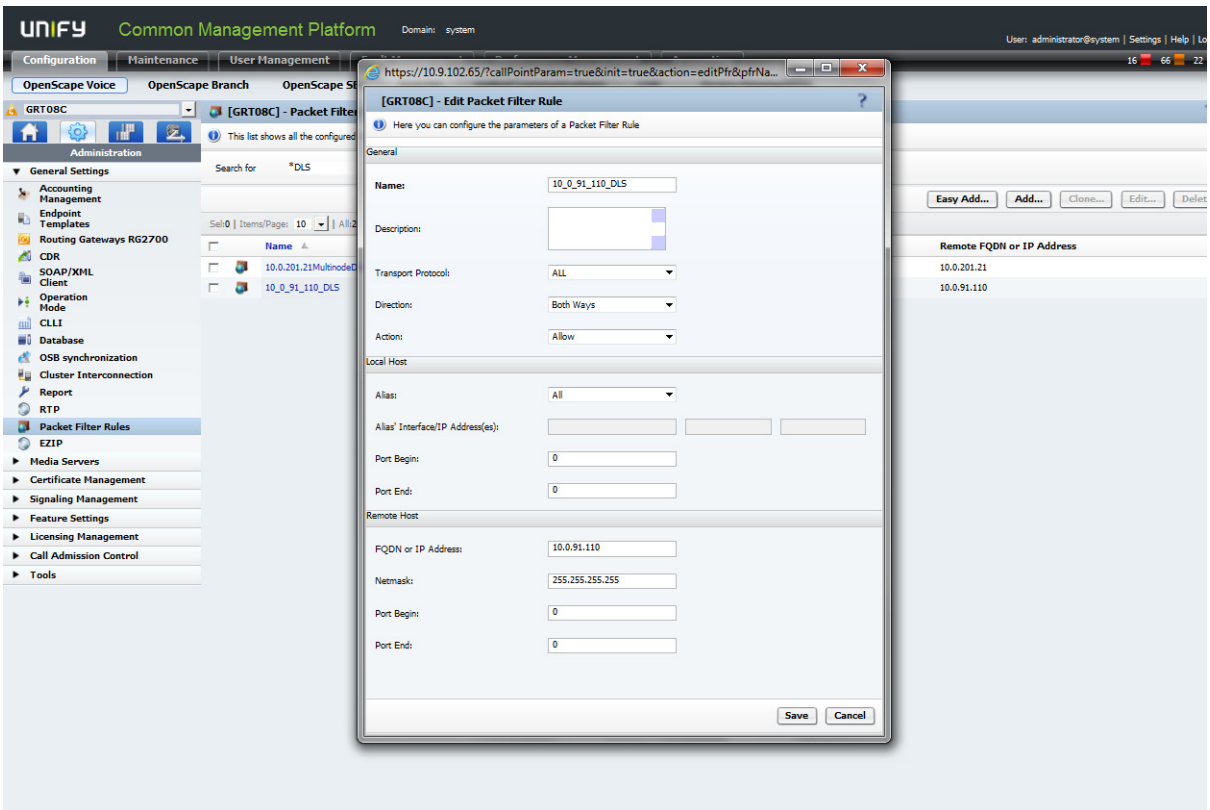


By default the protocol is set to “http”, but it is recommended to be set to “https”. For the secure mode to work, the correct information (certificates) should be set in the Element Manager Security mask (see below and also refer to DLS Admin manual for more information):


DeploymentService
Administration
IP Devices
Mobile Users
Gateways
Software Deployment
Element Manager
Element Manager Configuration
Element Manager Security
Profile Management
XML Applications
Job Coordination
Help
Logoff admin
Element Manager Security
Tenant: <all>
Job ID:
Exec Time: asap
Object Edit View Help
Views: Object
Certificate Check Policy
Certificate Check Policy: Full
Client credentials
PKI Configuration
PKI Configuration: DLS_grt08c_UNIFY
Table Selected entry
1 / 1
Serial number
Owner
1D
C=GR,ST=ATH,L=Athens,O=Unify,OU=DLS_ST,CN=DLS
Create Certificate
Import Certificate
Export Certificate
Server credentials
Table Selected entry
1 / 1
Serial number
Owner
CF42BC6E4E9AADE7
C=GR,ST=ATH,L=Athens,O=Unify,CN=newRootCA
Import Certificate
1 / 2
Discard
Save
Refresh
Clear

4. Before performing any synchronization between DLS and the OSV, the corresponding PFR (packet filter rules) should be set by the OSV administrator, so that DLS access is granted by OSV (see below):



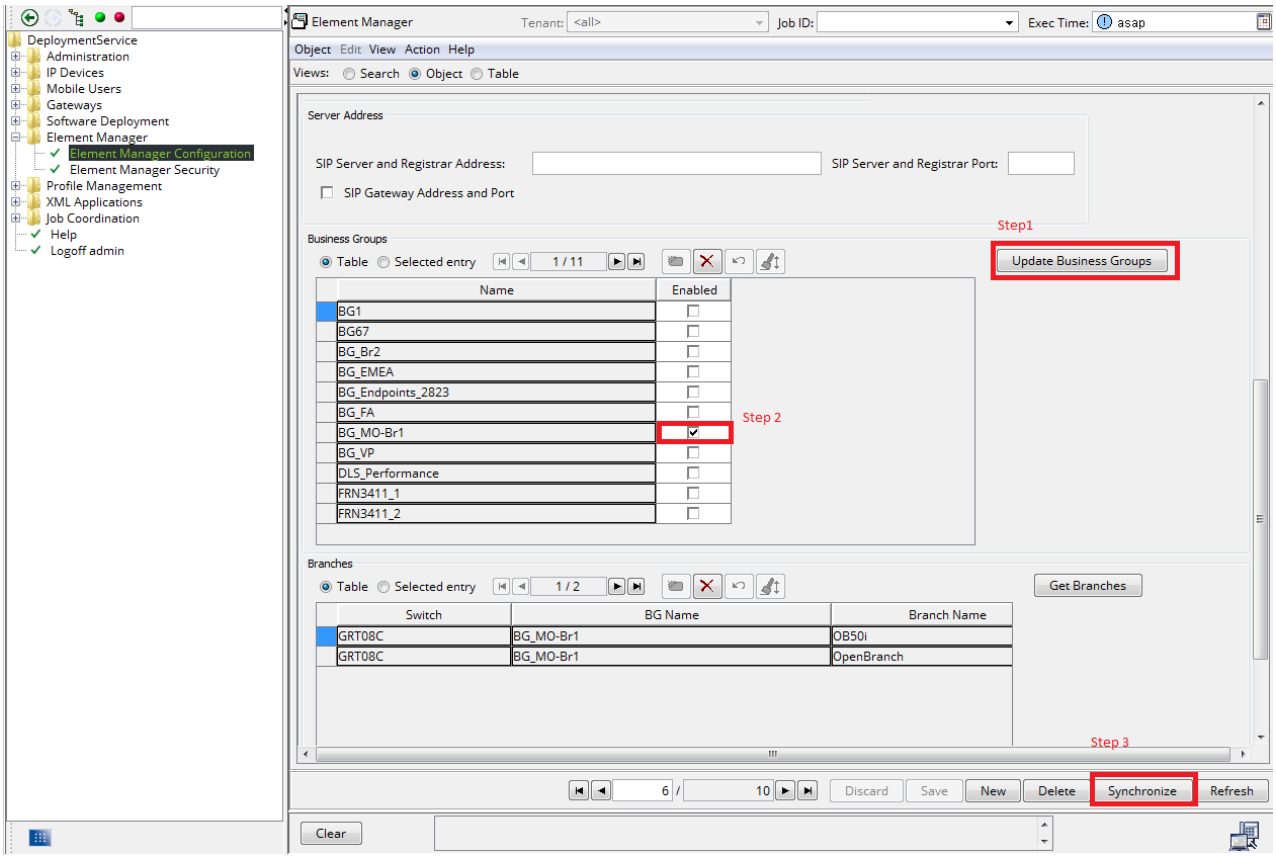


5. Go back to Main Menu > Element Manager > Element Manager Configuration, fetch the OSV EM that has just created above and (see also the example below):

   a) Press the **Update Business Groups** button. This will bring all the available BG's of the corresponding OSV.

   b) Select any BG (that needs to be synchronized). This step is optional. If no BG is selected DLS will synchronize all the subscribers of the switch.

   c) Press the **Synchronize** button, in order to bring the subscribers / devices to DLS. Check the **Protocol** tab to verify that the synchronization is successful.



15.6 Registering Workpoint Software and Files

This section explains how you can register software and files in the DLS so that the DLS can use them for the deployment.

The functions can be found under **Main Menu** > **Administration** > **Server Configuration** > **FTP Server Configuration**, ..> **HTTPS Server Configuration**, ... > **Network Drive Configuration**.

NOTE: The file that is to be registered is examined during registration.
The following checks are made:
- Whether the file exists at the source storage location.
- If so and if this file contains software, whether the SPA is unknown, old, or new.
- Any additional data available in the new format, such as, the **SW type** (HFA or SIP), **SW version**, etc. is read out.

This process can take some time, depending on the network.

For an overview of all object types supported by the DLS, see Section 3.5, "Overview of Software and File Types".

For an overview of all IP Devices and platforms supported by the DLS, see Section 3.4, "Area of Application".

NOTE: You must also register IP client software installations in the DLS, but no license check is performed for IP client software in the DLS because this is done while it is running (at software startup).

Requirements

- A configured FTP server for IP phone software images or a configured Windows network drive for IP client software (see Section 6.3.4 or Section 6.3.7).
- The suitable files are available in the source storage location.

15.6.1 Automatic Registration

The only difference between the automatic registration of IP phone software and IP client installations involves the type of source storage location.

1. To register software and data on an FTP server, select an FTP server from the choice list under **Administration** > **Server Configuration** > **FTP Server Configuration** by means of the **Search** button. Then, click on **Start scan** to start the registration.

   To register an installation for IP Clients, use **Administration** > **Server Configuration** > **Network Drive Configuration** > **Scan Server**.

   To register softare and data on an HTTPS server, use **Administration** > **Server Configuration** > **Network Drive Configuration** > **Scan Server**.

   To configure FTP servers and network drives, see Section 6.3.4 or Section 6.3.7.

2. Click **Start**. Automatic registration starts and updates the status, and information is entered in the dialog window.

   NOTE: You can go ahead and close the dialog window during this process. Automatic registration runs in the background without being affected.

15.6.2 Understanding License Information for IP Phone Software

NOTE: Licensed IP phone software is not yet available. This means that as far as licensing is concerned, only data entered here for unlicensed software applies to IP phones.

When you register IP phone software, information is also read out of the software image's "license trailer".

The license trailer information consists of the following possible values:

- Device type (contains the device type designation)
- Software version (contains the software version number)
- Software type (contains the software type designation)
- License feature ID (contains the identification of the license feature)
- Licensed SW version (contains the software license version number)
- Expiry Date (contains the software expiration date)

15.7 Editing Templates

The DLS can create templates for all parameters in the **Call: Main Menu > Call: Main Menu >** area. This provides a quick and easy option for reusing configurations that are frequently deployed.

You can also combine existing templates in profiles, which greatly simplifies the use of extensive workpoint configurations.

You can create a template for each interface in the contents area (see Section 5.4.2, "Work Area") and save it to use later. You can use buttons in addition to export and import all stored templates into an ZIP file (see Section 12.3, "Template Overview").

IMPORTANT: If data changes are made in configuration forms that have been generated using templates, these changes are not automatically applied to the templates.
In order to be applied, the changes must be saved manually in the template; see below.

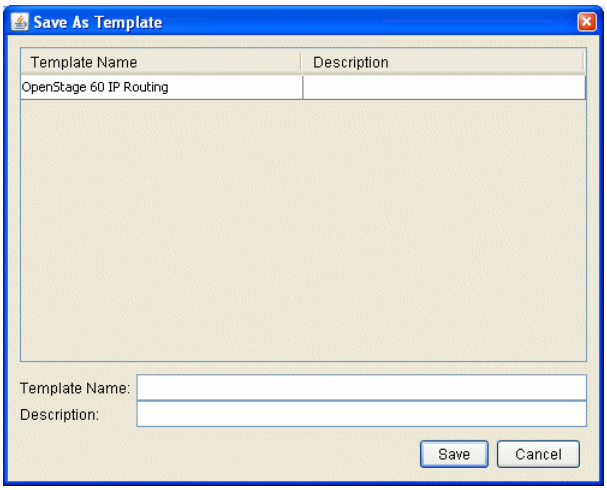
15.7.1 Creating a Template Manually

1. Select an area for which you want to create the template in the main menu under **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** or **IP Client Configuration**.
2. Select **Template** view (see Section 5.4.2.3, "View Bar").
3. Enter all the required data.

   A template always includes the contents of an interface under **Call: Main Menu > Call: Main Menu >**, with all available tabs.

   NOTE: In many cases, it is useful to select the scope of a template so that it is not too large. For example, it may be advisable to create two separate templates instead of one for WAP and LDAP so that you can assign them more flexibly, that is, separately from one another, to different profiles.
4. Click **Save**.

5. The dialog window for saving the template appears.



   Enter a meaningful name under **Template Name**, such as, "QoS Configuration 1". Under **Description**, enter a text that explains this template.

6. Click **Save**.

   The name of the current template now appears after **Template** in the view bar.

You can also save multiple different templates for an area by using different template names.

You can export templates that you have saved (see Section 12.3, "Template Overview").

15.7.2 Creating a Template From an Existing Configuration

You can take configuration data that already exists in **Object** view and include it in a template.

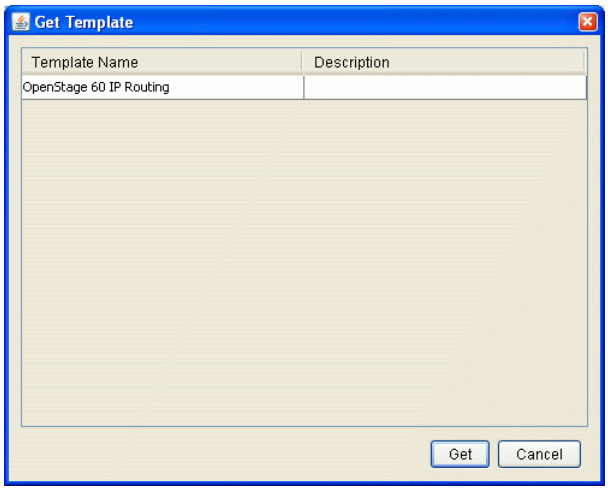
1. In the main menu under **Call: Main Menu > Call: Main Menu >**, select an area in **Object** view from which you want to copy the data into a template.
2. In the menu bar, select **Copy to template** under **Action**. **Template** view appears with the data that you copied.

Save the template for later use as described above (see "Creating a Template From an Existing Configuration", starting with step 4).

15.7.3 Loading the Template

To change a template that has already been saved or to use such a template manually, you first have to load it into **Template** view.

1. Select the **Template** view for which you want to load a template that has already been saved in the area and click **Get**.
2. If there is at least one template for this area, the dialog for loading a template appears.



3. Select a template from the list and click **Get**.
4. The template contents are displayed in **Template** view and the template name appears in the view bar.

   To use the data for configuration or as a search criterion, select the appropriate view (**Object** or **Search**) and select the **Use template** entry under **Action** in the menu bar.

   NOTE: When you use a template, only the contents defined in the template are applied. Empty or grayed out fields or check boxes do not overwrite or delete any current values in the configuration.

   Use **Profile Management** > **Template Overview** to check which individual attributes are currently configured.

15.7.4 Additional Functions

By clicking **Rename Template** in **Template** view, you can rename a template that has already been saved and change the description of the template. With **Delete Template**, you can delete one or more saved templates.

15.8 Workpoint Autoconfiguration (Plug&Play)

The goal of Plug&Play in DLS is to automatically provide the workpoints supported with the parameters needed for registering at a gatekeeper or SIP server. This should always be done as soon as a workpoint is switched on or connected.

There are different types of Plug&Play:

- **Full Plug&Play**
  - Provision of the workpoint with IP base data and DLS address data using the DHCP server.
- **Limited Plug&Play**
  - Manual entry of IP base data and DLS address data at the workpoint.

NOTE: We recommend that you use a DHCP server in the DLS environment to :

-support full plug&play and
-ensure the authenticity of the DLS server

For more information on how to configure a DHCP server, refer to refer to the **Unify Experts Wiki portal** under http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment or Section 4.12.5, "DHCP Server in a Linux/Unix Environment".

NOTE: Factory Reset with Plug&Play data stored is not possible in Secure Mode. The according IP Devices must be revert to Default Mode first.

15.8.1 Requirements

Requirements for full Plug&Play

- Functional DHCP infrastructure. Depending on the network topology, this consists of at least one DHCP server and, where applicable, multiple DHCP relay agents.

The IP base data and the DLS address data is entered on the DHCP server so that it can be distributed automatically to the terminals. For information on configuring the DHCP server, refer to the **Unify Experts Wiki portal** under http://wiki.unify.com/wiki/Configuring_the_DHCP_Server_for_DLS (Windows) or Section 4.12.5 (Linux/Unix).

This ensures that an IP phone with factory settings receives its initial IP configuration when it is booted.

Requirements for limited Plug&Play

- Manual storage of the complete IP base data (IP address, subnet mask, default IP gatekeeper, DNS server, DNS domain suffix, etc.) and DLS address data on the IP phone.

This guarantees Plug&Play operation, albeit in a restricted form, in networks without DHCP infrastructure.

NOTE: For IP clients, full plug&play looks a little bit different.

As IP clients usually run on a host with proper IP configuration, the IP client can be provided with missing DLS address data either using a "DHCP Inform" or with a "DNS Text Resource Request".

Both ways are considered full plug&play because in contrast to the exclusive use of a DNS with IP phones, manual configuration is not necessary.

15.8.2 Setting Up Plug&Play Registration

15.8.2.1 Assignment Procedure

There are three different procedures for Plug&Play registration. These differ in terms of the manner in which a workpoint's Plug&Play data is assigned to a physical workpoint.

- **Assignment using Device ID**

  A specific device ID is entered here for an existing data record, that is, a virtual device (see Section 15.8.2.2, "Creating Plug&Play Data"). The DLS uses the device ID to identify which Plug&Play data it should send to the workpoint.

- **Assignment using E.164**

  Alternatively, the data record can be assigned to an E.164 number which must be entered manually at the workpoint. The DLS then checks all familiar Plug&Play data sources based on phone numbers one after the other (for example, configured HiPath 4000 Assistant databases or HiPath 3000/5000) to see whether the phone number can be uniquely assigned to a system.

  If the workpoint responds during DLS installation, the DLS can use the E.164 number to identify which Plug&Play data it should send to the workpoint.

- **Assignment using number pool**

  If a number pool is configured and enabled, each IP phone registering at the DLS without an E.164 receives a dummy E.164 number from the pool. A prerequisite is that at least one free number must exist in the pool. The virtual device associated with the particular E.164 number is assigned to the IP phone by changing its device ID to "@ <IP Phone's MAC address>" and by setting its status to "in use". After this, Plug&Play will be executed using this virtual device. Before Plug&Play, a software upgrade is possibly executed.

  The E.164 number assigned to the IP phone is not available by the number pool until the IP phone has received its final number, either by the administrator, an application using the DlsAPI or the user via WBM or locally at the IP phone, or the IP phone is deleted from the DLS.

As soon as the E.164 is considered free again, the virtual device gets a new **Device ID**, the **Plug&Play active** flag is enabled again and its Plug&Play pool status reset to “free”. Now the virtual device is available again in the number pool again. See also chapter Section 6.3.2.6, ""P&P Number Pool" Tab".

15.8.2.2 Creating Plug&Play Data

The are a number of different procedures for creating Plug&Play data:

- **Creation by synchronization with an Element Manager**
  Synchronizing DLS with an Element Manager creates a new data record for each station that is stored in the Element Manager but not yet in the DLS. For more information about connecting the Element Manager and the DLS, see **Element Manager** > **Element Manager Configuration**.
- **Plug&Play data import**
  You can import Plug&Play data from a file via **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration**.
- **Manual configuration of a station in the DLS**

  You can use the **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** area to create a new station data record in the DLS as a virtual device.
- **Configuration via a provisioning tool using the DLS API**

15.8.3 Registration

1. Connect the workpoint(s) (see the workpoint installation or administration manuals). If all requirements for full Plug&Play are met, the workpoint will receive the DLS address data from DHCP.

   The workpoint registers at the DLS with this data.

2. If the DLS can identify the unique Plug&Play data required by the workpoint performing registration, it automatically sends it to the workpoint.

   The DLS basically has three ways to determine Plug&Play data. For more information, see Section 15.8.2.1, "Assignment Procedure".

   - **Assignment using Device ID**

     In the first alternative, the DLS checks whether it can determine a set of Plug&Play data records from the device ID presented by the workpoint. However, this option currently requires that the device ID and Plug&Play data be linked manually.

   - **Assignment using E.164**

     Using the E.164 number that is manually entered at the workpoint, the DLS checks whether it can determine a corresponding data record.
     Example of a complete E.164 number: **498972212345**.

   - **Assignment using number pool**

     If a number pool is configured and enabled, each IP phone registering at the DLS without an E.164 receives a dummy E.164 number from the pool. A prerequisite is that at least one free number must exist in the pool.

3. If configuration templates have been defined (see Section 15.7) and grouped as the standard template, data from the templates is transferred to the workpoint.

4. The Plug&Play sequence is completed when all assigned data has been sent successfully.

15.9 Distribution of Workpoint Software

This section explains how to perform manual software or file deployment and which configurations are necessary for automatic deployment.

NOTE: Note the difference between **Software Deployment** and **File Deployment** in the DLS interface (see Section 10.1.1 and Section 10.1.2).

Software deployment refers to the distribution of workpoint software (IP phones and IP clients). In contrast, **file deployment** means the distribution of any binary or ASCII files that perform a certain task in the workpoint.

Both functions are combined in the DLS main menu under **Software Deployment**.

For automatic deployment, see Section 15.9.2, "Automatic Deployment".

NOTE: A single software deployment operation can take place for each workpoint at the same time as a file deployment operation, but it is not possible for multiple software deployment operations or multiple file deployment operations to take place simultaneously.

If you want to update workpoint software using a netboot server, and the update is not possible with a crosslink cable (crossed LAN cable), the workpoint must be connected to the Netboot server via a hub.

NOTE: When distributing software for optiPoint WL2 professional workpoints, ensure that the workpoints have sufficient battery capacity. If not, it may not be possible to operate the software successfully.

Software image properties

A distinction between software images can be made on the basis of the following properties:

- Type of hardware supported (device type, such as optiPoint 410 Standard).
- Software type (such as, Unify HFA).
- Software version (such as, CLA, DHCP, DNS, and FTP servers).5.1.3).
- Integrated DLS interface
  (yes = new, no = old SPA).
- Requiring a license (yes or no).

  NOTE: Licensed IP phone software is not yet available. The IP phone software that is currently on offer does not require a license.

15.9.1 Manual Deployment

In principle, you can define the following parameters during manual deployment:

- Which workpoints should be provided with the software.
- Which software should be used for the distribution.
- When the distribution should occur.

Requirements

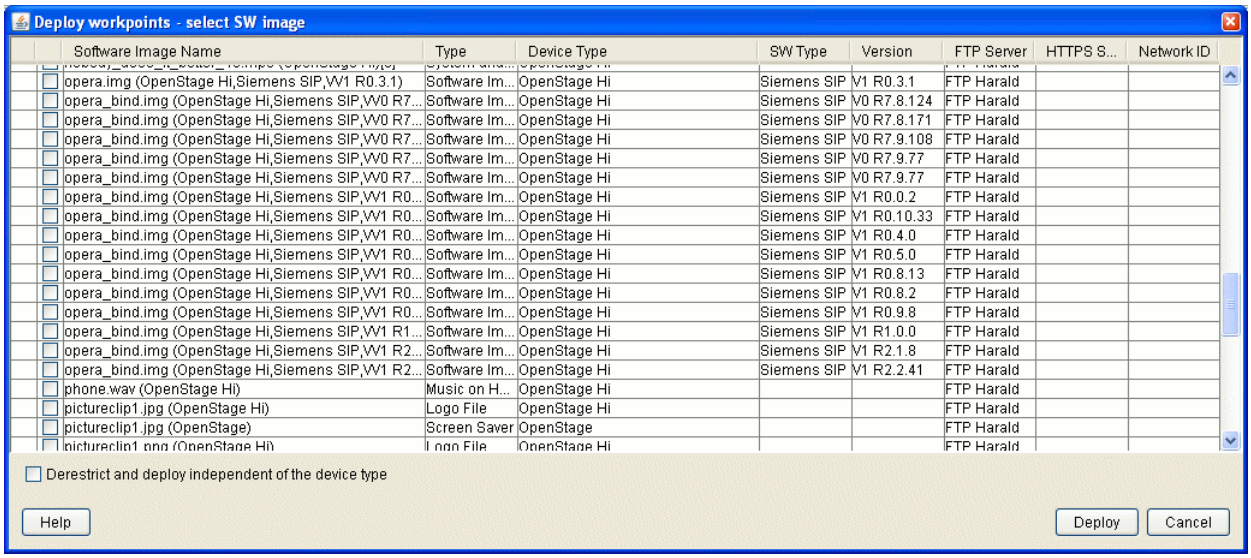
- A working DLS infrastructure (such as
- The workpoints to be supplied have automatically registered at the DLS or were found by the DLS during a manual scan (see Section 7.5.6, "Scan IP Devices").
- The software to be distributed was either automatically or manually registered at the DLS (see Section 15.6, "Registering Workpoint Software and Files").

Performing distribution

1. First decide which workpoints you want to provide with the software.
   Do this by choosing the **Software Deployment** > **Deploy Workpoints** area and, if necessary, enter search criteria in **Search** view. Click **Search** to start the search.
2. If one or more workpoints were found, the first entry is shown in **Object** view.
   To select multiple workpoints, change to **Table** view and hold down the <CTRL> key to select a number of individual workpoints or hold down the <SHIFT> key to select workpoint ranges.
3. Click **Deploy**.

   NOTE: When you click **Deploy**, the system checks whether suitable software is available, that is, registered, for the selected workpoints.
   If this is not the case, an appropriate message is displayed. This is also true if you have selected both IP clients and different IP phones (optiPoint, OpenStage) in a multiple selection.

If suitable software was found, the following dialog appears (example):



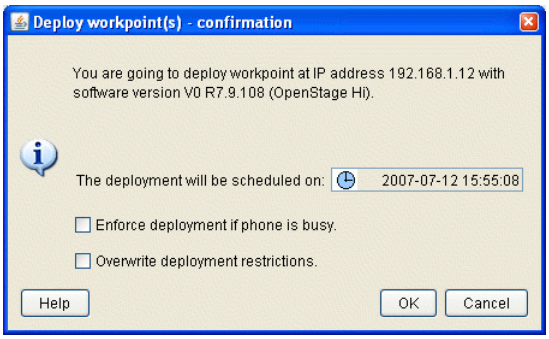
If a software image is not suitable for this workpoint type, the entry is displayed with a yellow triangle and dimmed. If you hover the mouse pointer over this icon, a ToolTip appears with the reason for this.
For example, the ToolTip "Software not applicable for this device type" states that a specific registered HFA software package cannot be distributed on Unify HFA workpoints.

> ***IMPORTANT:*** You can use the check box **Derestrict and deploy independent of the device type** to perform software deployment even for a workpoint that does not match the other workpoints because of the software license information (see Section 15.6.2, "Understanding License Information for IP Phone Software").
> In general, this is only necessary if you want to perform deployment for a new device type unknown to the DLS.
> The result can involve the loss of the entire workpoint functionality.
> If this check box is selected, all entries in the list (including ones that were previously dimmed) are available for selection.

4. Select an **Execution Time** in the toolbar. To do this, click the calendar symbol  and select one of the time options and the conditions for the deployment. For more information on the calendar button, see Section 5.4.2.4, "Time field with calendar button".

5. Choose the entry that you want and click **Deploy** to stipulate the performance time.

6. A dialog window where you can start software distribution appears. By default, the software is set on the basis of the configured restrictions (see Section 6.3.2.7, ""SW Deployment Restrictions" Tab"). If you activate **Overwrite deployment restrictions**, these restrictions are ignored.



7. Activating **Force deployment if device is busy** forces the deployment procedure to be carried out without delay even if a workpoint is busy (active call). You should only use this option in exceptional cases because it interrupts a telephone connection on the workpoint.
8. Activating **Overwrite deployment restrictions** forces deployment regardless of any restrictions that may be configured.
9. Click **OK**. If the license check was successful, individual jobs are generated for distribution to the selected workpoints and carried out at the specified time. A progress bar shows job generation progress (see Section 5.4.2.6, "Message Windows").

For more information on job coordination, see Section 15.10, "Using Job Coordination".

15.9.2 Automatic Deployment

As the name suggests, in addition to manual distribution (see Section 15.9.1, "Manual Deployment"), you can also distribute workpoint software automatically, that is, without user intervention.

If a workpoint is registered at the DLS, either during a manual scan (see Section 7.5.6, "Scan IP Devices") or as a result of first-time registration of a workpoint with software in the new format (with DLS interface), a deployment procedure will be initiated on the DLS that complies with the deployment rules.

The following describes how to configure the rules that control this procedure.

Requirements

- A working DLS infrastructure (such as CLA, DHCP, DNS and FTP servers).
- The workpoints to be supplied have automatically registered at the DLS or were found by the DLS during a manual scan (see Section 7.5.6, "Scan IP Devices").
- The software to be distributed was registered at the DLS (see Section 15.6, "Registering Workpoint Software and Files").

Reconfiguring deployment rules

1. Select the **Software Deployment** > **Manage Rules** area and click **New**.
2. In the **Device Type** field, select the workpoint type to which the rule should apply.

   NOTE: You can only configure one rule per combination of location, device type, software type, and software version.
3. In the **Location** field, select the location to which the rule should apply.
4. In the **Software Type** field, select the type of software type which is currently installed on the workpoints to which the rule should apply.
5. In the **WP SW Version** field, select the version of the software which is currently installed on the workpoints to which the rule should apply.
6. If applicable, activate **Deploy Newest SW Version** if only you want software deployment to be performed when there is a version available for distribution that is newer than the version installed at the time. Example: Version 5.1.9 is distributed to workpoints with version 5.1.1, while version 5.2.0 is left on the workpoint.
7. To distribute a very specific software version, you must deactivate **Deploy Newest SW Version**. You must make this setting to force a change in the workpoint software type.
   In this case, go to the **SW Image** and **Software Version** fields and select the required software image in the available software version from the lists or enter the image and version.
8. Click **Save** to save the new rule.
9. Click **Apply** to obtain a listing of all workpoints to which the rule applies. A dialog window opens up in which you can select the workpoints to which the rule shall apply effectively. After this, confirm by pressing **Apply** in the dialog window.

Repeat the procedure for each rule that you want to set up.

Automatic distribution sequence

Automatic software distribution is always initiated at the workpoint.

When registering a workpoint, the DLS first checks if there is a rule for the workpoint device type. If there is no rule or if the rule has been deactivated by deselecting **Deploy Default Software**, no further processing takes place.

If the distribution of the newest software is activated across the board, the newest software (software with the highest software version number) is distributed to all workpoints with the same software type. Workpoints with other software types do not receive new software.

If **Deploy newest version** is deactivated, each workpoint receives the software entered, without taking the software type into consideration.

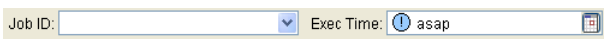
15.10 Using Job Coordination

In the DLS, all tasks are planned, processed, and logged with the help of jobs. Individual jobs can consist of a number of actions.

You can set up jobs in the following areas:

- Location
- Workpoint Interface Configuration
- Automatic SPE Configuration
- IP Phone Configuration
- IP Client Configuration
- IP Gateway Configuration
- IP Device Interaction
- SIP Mobile User Configuration
- SIP Mobile User Interaction
- Gateways
- Software Deployment

You can assign specific configuration, deployment, and interaction tasks to particular jobs in these areas by entering a name with **Job ID** and stipulating the execution time and execution option in the toolbar (see Section 5.4.2.4, "Time field with calendar button").



If a name was defined before the object was saved, this then appears later in **Job Control** in addition to the action number. You can group individual actions into jobs to achieve greater clarity by manually entering a **Job ID**.

NOTE: Switching from daylight saving time to regular time (one hour back) will not lead to a second execution of a job that has been started in the time interval hereby doubled. When switching from regular time to daylight saving time (one hour advance), a job which is scheduled for this skipped time will not be executed.

You can configure properties for executing and logging jobs (see Section 14.3, "Job Configuration").

15.10.1 Defining a Job

A job is defined by entering a **Job ID** in the tool bar. You can enter a time in the future to the right of **Job ID**. In this case, the required action (such as, changes to IP Device parameters) is performed at the specified time instead of immediately.

To avoid assigning further actions to the specified job, simply select the empty entry from the selection list under **Job ID**. You can remove a defined time in the calendar dialog by clicking **Delete**.

15.10.2 Viewing Job Properties and Status

There are two tools available for checking and logging jobs.

Job Control

This function lets you view a large volume of information on the individual jobs and discard, delete, or reactivate existing jobs.

1. Click the **Job Coordination** > **Job Control** area.
2. If necessary, enter filter criteria to narrow the search to only jobs with certain properties. For example, this lets you search for jobs that are currently active, that is, they have not been processed yet.
3. Click **Search** to start the search.

   The search result shows all relevant data on each job or action that was found (see Section 14.1, "Job Control").
4. You can delete (completely remove) selected jobs or actions in **Object** and **Table** views. You can do this either before or after the job has executed.

   You can use **Discard job** to prevent a job from executing. This job remains in the list of all jobs, however, and is also still shown under **Daily Status**.

   NOTE: You can discard any job regardless of its status. If the job's status is **done**, you can discard it and enter a new execution time. This allows you to reactivate jobs, that is, you can execute them again.

Daily Status

This function gives you a clear display of all jobs in a table and lets you filter them according to time frame and job status. You can also delete the jobs that are displayed here.

1. Click the area **Job Coordination** > **Daily Status**.
2. If necessary, restrict the statistics by entering an activation date and job status so that the search includes only jobs with these properties.
3. Click **Search** to start the search.

   The search results shows a table containing the job ID, job status, activation time and end time (see Section 14.2, "Daily Status").

   If several actions have been combined into one job ID and if at least one action has the status **time exceeded**, **discarded**, or **failed**, this status is shown for the entire job.
4. Click **Delete** to remove the job completely. If several actions have been combined into one job ID, all of these actions are deleted.

15.11 Backup/Restore

The DLS client interface provides enhanced options for automatically saving DLS data and restoring backups.

15.11.1 Automatic Data Backups

You can create and restore automatic backups of the entire DLS database. You can also view backup logs.

15.11.1.1 Configuring Automatic Backups

1. Click the **Administration** > **Backup/Restore** > **"Backup" Tab** area.
2. If you have not already done so, enter the path for saving the backup (without the file name) under **Backup Path** or select a suitable path by clicking **Browse**. Click **Test** once to check the availability of this path.
3. If necessary, change the maximum number of backup file types that should be backed up under **Max. Number of Backups**. The oldest backup file is deleted once this value is exceeded.
4. You can perform the following types of backups:
   – A single backup performed immediately.
   Click **Start Backup Now**.
   – A single backup performed at a specific time in the future.
      1. Enter a time in **Start Backups at** (for a calendar, see Section 5.4.2.4, "Time field with calendar button").
      2. Click **Save**.
   – A backup performed periodically on one, multiple or all weekdays.
      1. Enter a time in **Start Backups at** (for a calendar, see Section 5.4.2.4, "Time field with calendar button").
      2. Activate **Enable Daily Backups** .
      3. Activate or deactivate **Execute daily Backups on,** depending on your requirements.
      4. Click **Save**.

The backup file is created with the name `DLS_YYYYMMDD_HHMMSS.bak` in the directory you selected.

15.11.1.2 Restoring Backups

NOTE: A DLS database restore assumes that a database backup already exists, see Section 15.11.1.1, "Configuring Automatic Backups".
If the database to be restored is older (modified database definition), please perform a migration instead of a restore (see Section 15.11.2.3, "Migrating DLS Database Data"). A migration should also be performed if you are not sure if the database backup is still compatible.
There are some basic server configuration data which will never be restored as e.g.
- the account the Deployment Service is running with
- the license settings
in order to guarantee a proper working after any restore.

1. Click the **Administration** > **Backup/Restore** > **"Restore" Tab** area.
2. Enter the name of the backup you want to restore under **Backup File** or select a suitable file by clicking **Browse**. Click **Test** to check the availability of this file.
3. Click **Restore** to start backup recovery.
4. A dialog window asks if Plug&Play shall be disabled after restore. When Plug&Play has been disabled, it can be enabled again via **Administration** > **Server Configuration** > **P&P Settings** > **Plug&Play enabled**. For this, it must be ensured that all IP Devices are registered in the DLS database.

15.11.1.3 Monitoring Backups

1. Click the **Administration** > **Backup/Restore**> **"Protocol" Tab** area.
2. Click **Refresh** to display the backup log. The log provides information on the time the backups and recoveries were created and their statuses, as well as the backup files used.
   Possible values for the backup/recovery status: **Backup OK**, **Backup failed**, **Deleted**, **Restore OK**, **Restore failed**.

15.11.2 Manual Database Manipulation

This section explains how you can manually manipulate data in the DLS SQL database. The data is stored on the PC on which the deployment service is also running (the DLS server).

> ***NOTE:*** We strongly urge you to use the automatic DLS Backup/Restore function as this is a simpler and more secure procedure (see Section 15.11.1, "Automatic Data Backups").

You can:

- perform a backup of all data, see Section 15.11.2.1,
- restore saved data, see Section 15.11.2.2,
- migrate a database backup with a current database definition (combine), see Section 15.11.2.3,
- reset the database (delete all database data), see Section 15.11.2.4.

> ***NOTE:*** In order to execute the scripts `import/export/migrate.bat` commands, you should run the Command Prompt as administrator (UAC windows feature).

> ***NOTE:*** For cluster deployment, no migration of backups or resetting DLS DB is possible when mirroring is active.

> ***NOTE:*** For import/migrate scenarios, all data is wiped out on the target DLS installation if present, except:
> a) configuration of license server (this is to avoid consuming all licenses on the license server when a second DLS with same data is started)
> b) configuration of localized data which needs to be adopted to the current installation, e.g. trace file directories.

15.11.2.1 Backing Up DLS Database Data

To back up the DLS server SQL database, proceed as follows:

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. Save the directory **[installation path]\DeploymentService\DB** with all subdirectories by executing the following command:

```
[Installation path]\DeploymentService\Tomcat\webapps\
DeploymentService\database\dbexport.bat <filename>.zip
```

4. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.11.2.2 Restoring DLS Database Data

NOTE: A DLS database restore assumes that a database backup already exists, see Section 15.11.2.1, "Backing Up DLS Database Data".

If the database to be restored is older (modified database definition), please perform a migration instead of a restore (see Section 15.11.2.3, "Migrating DLS Database Data"). A migration should also be performed if you are not sure if the database backup is still compatible.

NOTE: There are some basic server configuration data which will never be restored as e.g.

- the account the Deployment Service is running with
- the license settings

in order to guarantee a proper working after any restore.

The procedure for restoring a saved database is similar to the one already described for a backup.

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. Restore the the DLS data by executing the following command:

```
[Installation path]\DeploymentService\Tomcat\webapps\
DeploymentService\database\dbimport.bat <filename>.zip
```

4. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.11.2.3 Migrating DLS Database Data

"Migration" here means that you can restore a saved database even if the database definition has been changed in the meanwhile. The database definition can change over time, for example, if IP Device configuration parameters are added .

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. To migrate the DLS data, execute the following command:

```
[Installation path]\DeploymentService\Tomcat\webapps\
DeploymentService\database\migrate.bat <exportfilename>.zip
```

The file `<exportfilename>` must be created by a backup of DLS data (see Section 15.11.2.1, "Backing Up DLS Database Data").

4. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.11.2.4 Resetting the DLS Database

You can reset the DLS database, which means that you can delete all data. As far as the data in the database is concerned, this produces the same result as the uninstallation (see Section 4.13, "Uninstalling the Deployment Service") and renewed installation of the complete DLS application.

IMPORTANT: A reset deletes all data in the DLS database.
To avoid data loss, create a backup of the database before you carry out the reset (see Section 15.11.2.1, "Backing Up DLS Database Data").

1. Close all browser windows connected to the DLS.
2. End *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. Delete the database by executing the following commands:
   - `cd[Installation path]\DeploymentService\Tomcat\webapps\ DeploymentService\database`
   - `dbinstall.bat delete`

   NOTE: With database deletion, a backup of the DLS configuration, collected only during DLS setup and held in the database, is saved under `Tomcat\bin` folder (in `dls_config.properties` file), in order for the database creationto use the last known configuration.

   IMPORTANT: In case or an error (e.g. you don't have permissions to write on `Tomcat\bin` folder) the file may fail to be created & the configuration may not be backed up & the last configuration may be lost. For that reason, the database reset action should be executed by an authorized user. The user will be notified about the process outcome in any case..

4. Create a new database by executing the following commands:
   - `cd[Installation path]\DeploymentService\Tomcat\webapps\ DeploymentService\database`
   - `dbinstall.bat create <password>`
     `<password>` defines the password for the user "admin".

NOTE: When the DLS database is created, the `dls_config.properties` file is used to restore the last known setup configuration. If the file is not found (e.g. in case of an error, failed to create) a Single Node installation with the default data (`C:\Program Files\DeploymentServiceDATA`) is assumed and this path will be set in the new DLS configuration.

NOTE: Before creating DLS database, you may open the `dls_config.properties` file and modify the `CommonData` path value in order to set a new value, pointing to the required path if desired (e.g. useful in the case of manually migrating common data path).

5. Start *DeploymentService* on the DLS server. Do this by clicking **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

15.11.2.5 Troubleshooting: License agent is unreachable

If the DLS cannot be called due to a deficient connection to the license agent, a different license agent can be entered in the DLS database. This is accomplished by the following steps:

1. Close all browser windows that are connected to the DLS.
2. On the DLS server, terminate the service "Deployment service" by clicking on **Programs** > **Deployment Service** > **Stop Service** in the Windows start menu.
3. Execute the command that is appropriate for the desired action:

   - to change the license agent:
     `[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\dbinstall.bat setcla <hostname> <port>`
   - to change the license manager:
     `[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\dbinstall.bat setclm <hostname> <port>`
   - if multiple DLS share one license agent:
     `[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\dbinstall.bat setmaxbasicdevices <Number of Devices>`
     `[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\dbinstall.bat setmaxmobileusers <Number of Mobile Users>`
   - to setup CLA/CLM values:
     `[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\dlslicense.bat setclm <IP of CLM> <CLM port> setcla <IP of CLA> <CLA port>`
     `e.g.`
     `dlslicense.bat setclm 10.6.25.11 8819 setcla 10.6.25.15 61740`

     NOTE: In case that CLM/CLA setup via the above command is not working, please reapply the same command for CLA and CLM seperately i.e.,
     - `dlslicense.bat setclm 10.6.25.11 8819`
     - `dlslicense.bat setcla 10.6.25.15 61740`

4. Start the service "Deployment service" on the DLS server by clicking on **Programs** > **Deployment Service** > **Start Service** in the Windows start menu.

15.11.3 DLS Restore Point

Whenever you want to keep the DLS software and database state and have the ability later to revert back to that state, you can do so by creating a DLS Restore Point. The functionality of DLS Restore Point includes only one (1) restore point and the process includes software, database and registry backup & restore when needed.

How to create a DLS Restore Point :

1. Go to `C:<Program Files>\DeploymentService\tools` and run `DlsSync.bat`. This command will backup the current state of both DLS software and database. For Multi-Node deployments you need also to provide a database backup directory (usually a network share) as the first parameter before running `DlsSync.bat`.

How to revert back to a DLS Restore Point :

1. Go to `C:<Program Files>\DeploymentService\tools` and run `DlsRestore.bat`. This command will restore the DLS software and database to the state taken from a previously created restore point. For Multi-Node deployments you need also to provide the database backup directory (usually a network share) as the first parameter before running `DlsSync.bat`.

NOTE: You can have only one (1) DLS restore point. If you try to create a DLS restore point and an old restore point already exists ,the old restore point will be deleted and the new will be created.

NOTE: When you initiate a DLS upgrade the installer will automatically create a DLS Restore Point, thus, deleting any previously taken restore point.

NOTE: In order to improve upgrade speed and lower data duplication, administrators should clear the DLS trace (or move/maintain outside the DLS path if a copy is required), and also from within <`DLS installation path>\Tomcat\bin` to copy outside any possibly generated heapdump-related files (heapdump.<data>.<id>.phd, javacore.<data>.<id>.txt, Snap.<data>.<id>.trc).

An increased number of such data is the security logs of devices being stored under: `..\DeploymentServiceDATA\devices\seclog\`

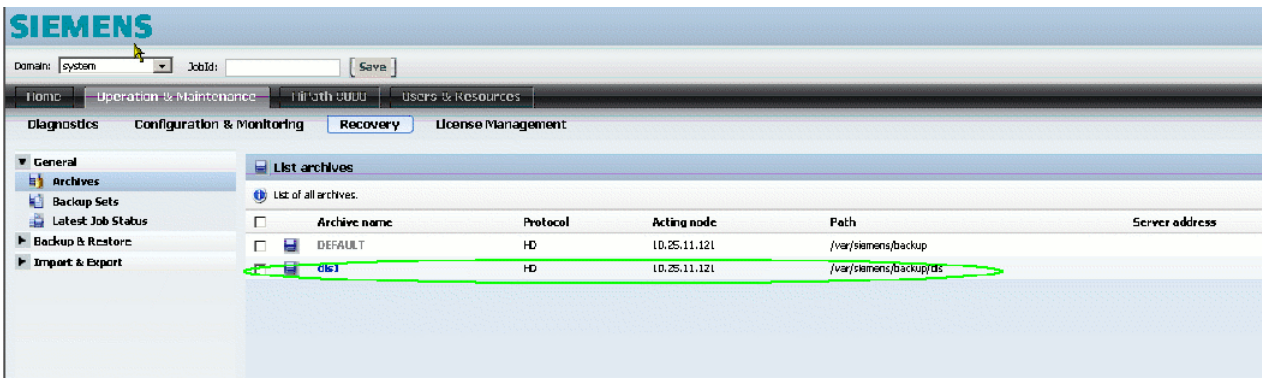
NOTE: Due to Microsoft SQL Server restrictions,in the case of deployments with active database mirroring, no restore procedures can be performed.
In such cases,when an upgrade is performed in Multi-Node deployments, a popup window will be displayed at the beginning of the upgrade requesting to either remove the mirroring and retry (**retry**), abort (**abort**) or continue (**ignore**) without the rollback feature.
At this point if the mirroring is active then the restore procedure cannot be executed.

15.12 Backup & Restore On OpenScape Voice Integrated and Linux Standalone Installations

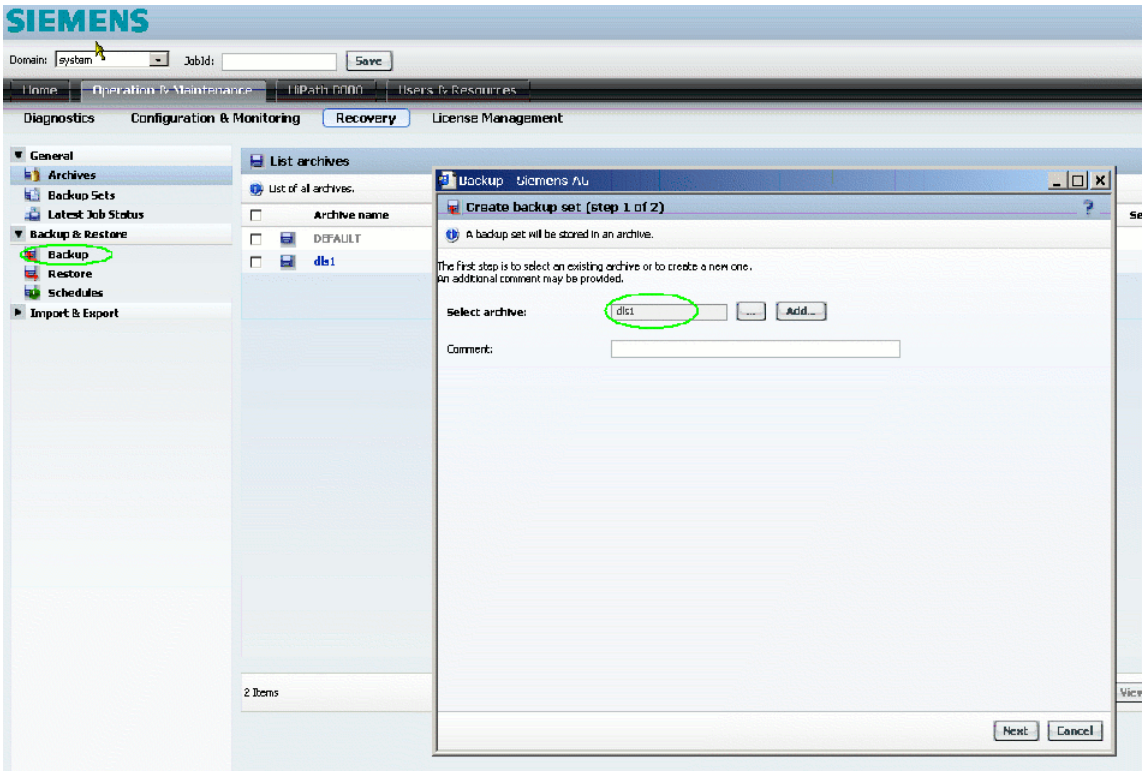
This chapter describes DSL database backup and recovery for the OpenScape Voice onboard version and the Linux Standalone version.

15.12.1 Backup

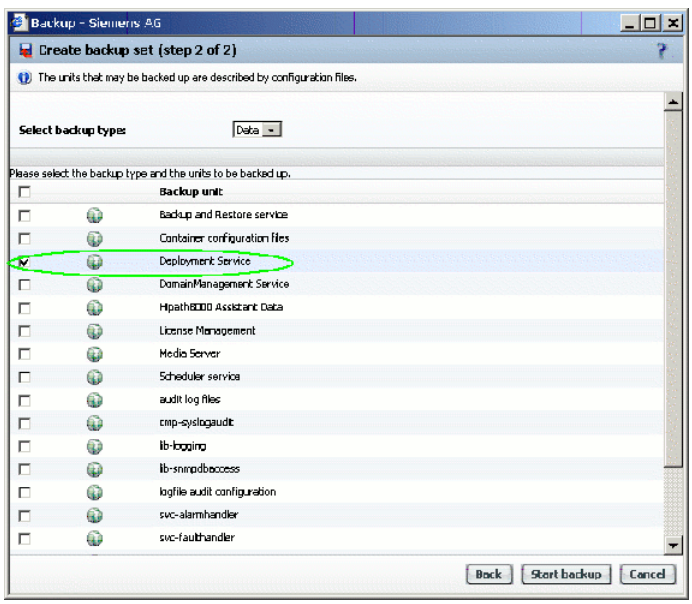
1. Log on at the **Common Management Platform**. The management platform is reached under `https://<IP of server>`
2. Navigate to **Operation & Mainentance** > **"Recovery" Tab**. Create an archive for DLS backups, e. g. in `/var/siemens/backup/dls`.



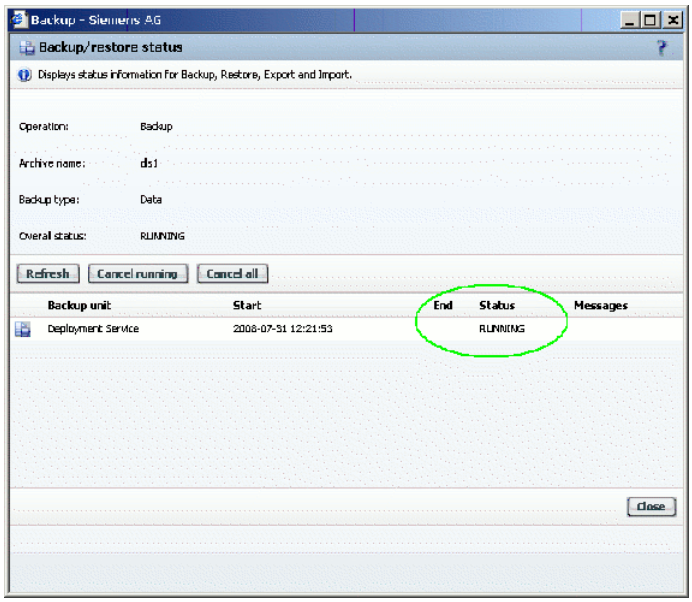
3. To create a backup, firstly open the folder **Backup & Restore** and click **Backup**. In the **Backup** window, in the **Select archive** field, select the newly created archive.



4. As **Backup unit**, select **Deployment Service**. Afterwards, click **Start backup**.

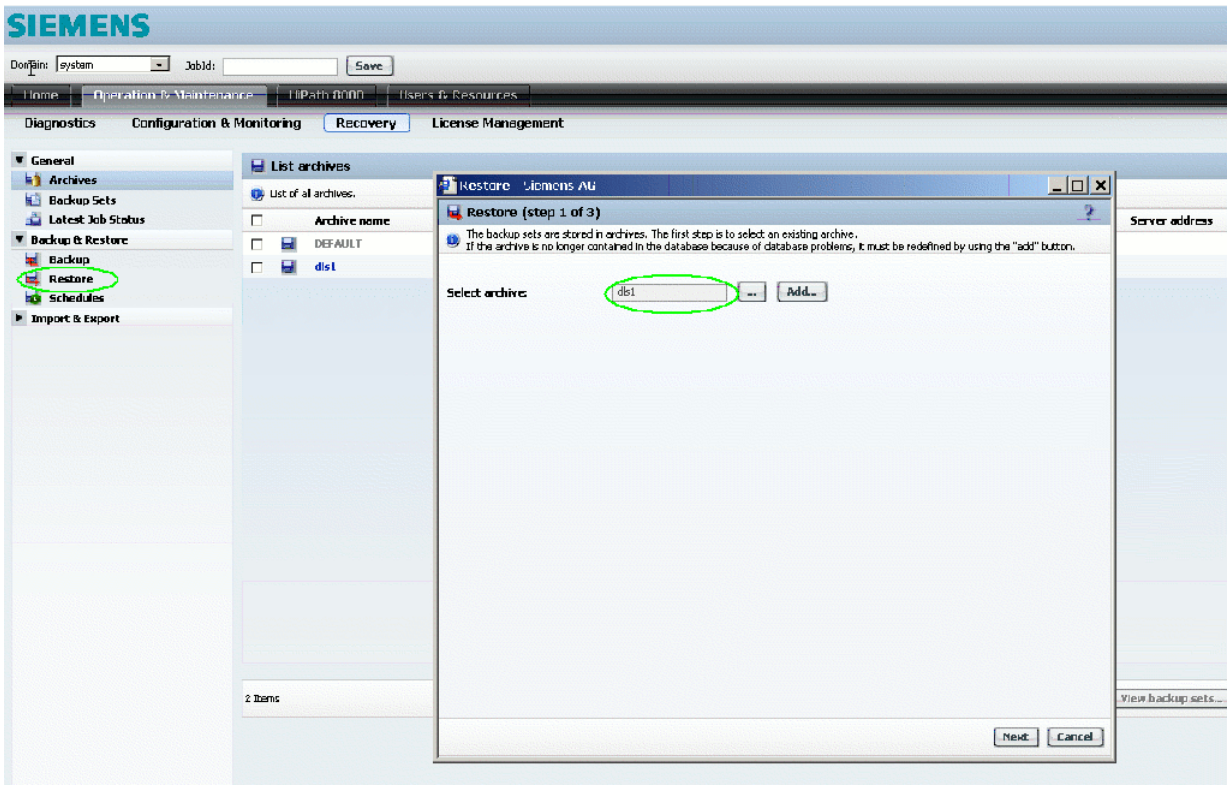


5. Wait until **Status** changes from **RUNNING** to **OK** (this screen refreshes automatically).

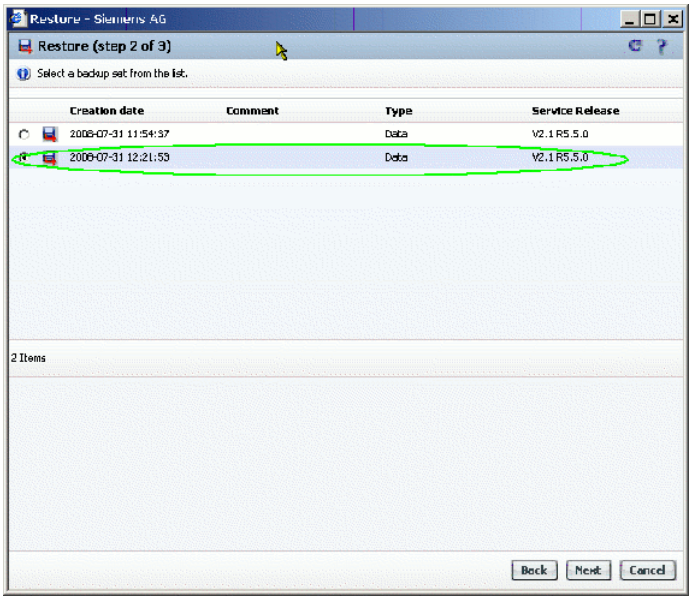


15.12.2 Restore

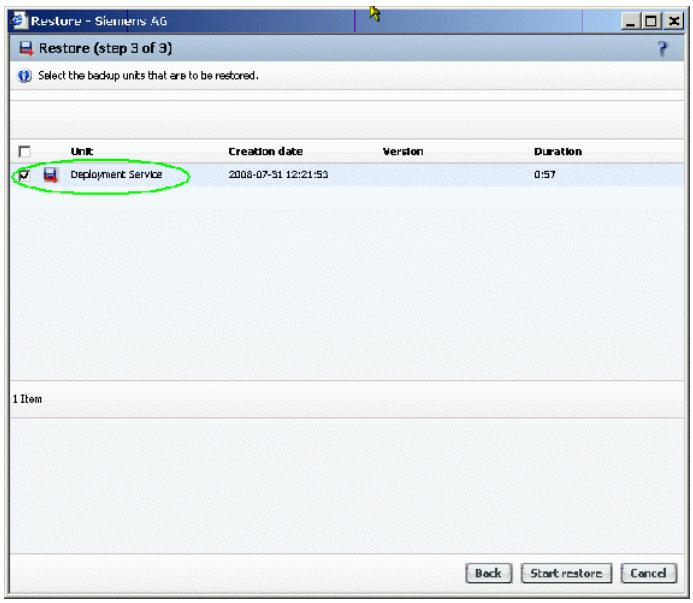
1. To restore a database, firstly open the folder **Backup & Restore** and click **Restore**. In the **Restore** window, in the **Select archive** field, select the archive containing the desired backup, and click **Next**.



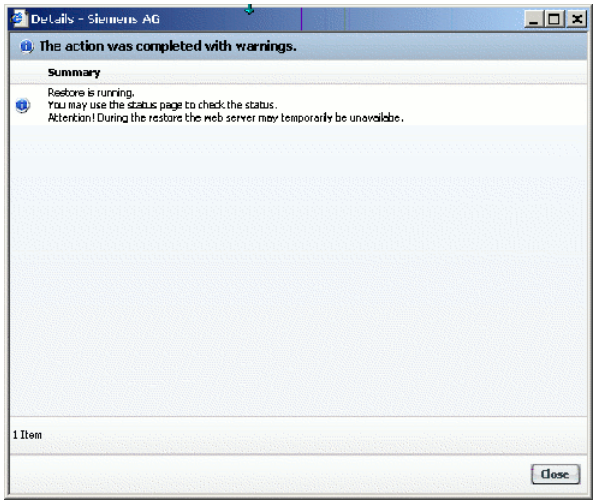
2. Select the desired backup from the list. The backups are identified by a time stamp or optional comment. Click **Next**.



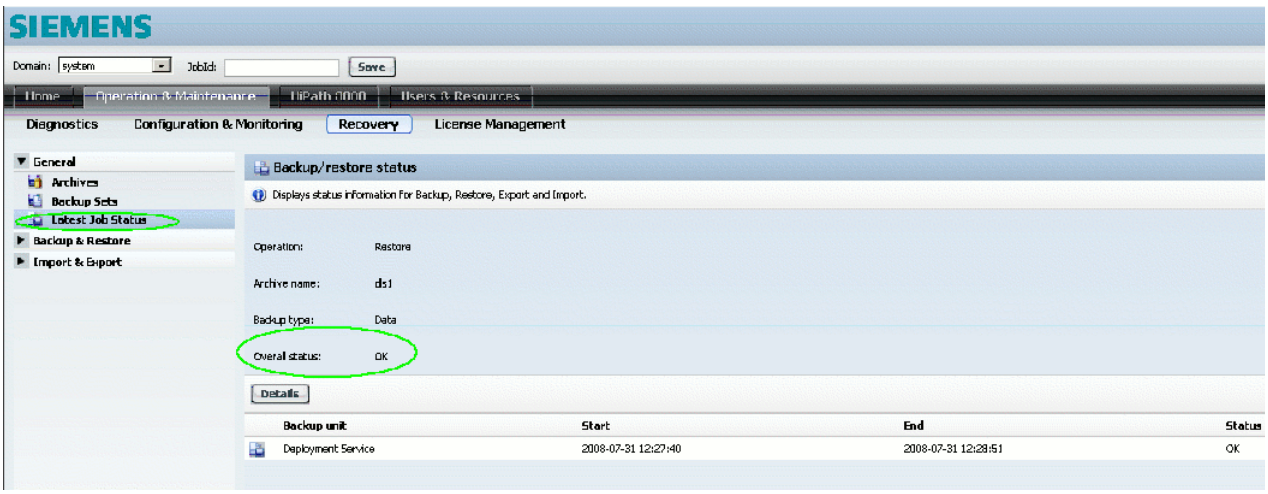
3. As backup **Unit**, select **Deployment Service**, and click **Start restore**.



4. You will be presented with a confirmation window. As this window will not refresh automa-tically, you can close it any time.



5. To check the state of the restore process, use the **Latest Job Status** screen.



15.12.3 Post-Restore Procedures

After the database has been restored successfully, the following manual steps must be performed, using shell commands on the server.

1. Log in as root at the Linux server or OpenScape Voice (for OpenScape Voice cluster: at both nodes).
2. Stop DeploymentService:
   ```
   sh /etc/init.d/symphoniad stop TomcatServletContainer
   ```
   On OpenScape Voice Cluster: Perform this step at both nodes.
3. Adopt the DLS database to the current layout. The command paths vary according to the platform.

   On Linux Standalone:

   ```
   cd /opt/siemens/share/tomcat/webapps/DeploymentService/database
   sh dbinstall.sh update
   ```

   On OpenScape Voice:

   ```
   cd /enterprise/share/tomcat/webapps/DeploymentService/database
   sh dbinstall.sh update
   ```

   On a OpenScape Voice cluster, you need to perform this step only on that node where the PRIMARY database is located. You can check the result with the following command:

   ```
   su - srx -c "RtpSolid -l"
   ```

4. Start DeploymentService:

   ```
   sh /etc/init.d/symphoniad start TomcatServletContainer
   ```

   On OpenScape Voice cluster, perform this step on both nodes.

15.13 Automatic Restore on Upgrade Failure

Due to the nature of DLS and the number of different deployment scenarios as well as the freedom of the customer to modify the underlying operating system,the upgrade of the software is a high-risk administrative task. Until recently, in case of a failed upgrade, the customer was left with a dysfunctional system and in order to revert back to an operational state, manual intervention was required having to re-install DLS as well as to restore the database from a previous backup.

Now the DLS installer can automatically revert back to the operational system state prior to upgrading in case of an upgrade failure. This functionality is available only for Microsoft Windows DLS deployments. For Linux, DLS deployment is not available due to the dependency on the Symphonia framework and the DVD delivery mechanism.

NOTE: In case the restore process fails, the installer will notify the user and it will exit. The system will be in an undefined state and you will have to contact support in order to resolve the issue.

NOTE: After a successful restore, the software and database backup are not deleted so as the customer to have the ability to revert back in case there is a need for that (please refer to Section 15.11.3, "DLS Restore Point").

IMPORTANT: Manual downgrade is not supported.

15.14 Importing and Exporting Plug&Play Data

The following section describes how to import and export workpoint Plug&Play data as files in CSV format.

15.14.1 Exporting Plug&Play Data

The following steps explain how to store Plug&Play data from a particular workpoint as a CSV file on the DLS server.

NOTE: A file that already exists with the name you enter will be overwritten.

1. Click the **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** area.
2. Locate and select the workpoints from which you want to export Plug&Play data and click **Export File**.
3. In the subsequent dialog, enter the name of the export file on the server and click **Save**.
4. A window appears confirming that the export was successful or displaying an error message.

15.14.2 Importing Plug&Play Data

The following steps explain how to import Plug&Play data from a CSV file on the DLS server. Detailed import results documenting which workpoints were newly created, which were modified and on which errors occurred, for instance, can be found in the log file. It is displayed under **Administration** > **Display Logging Data** > **P&P Import Protocols**.

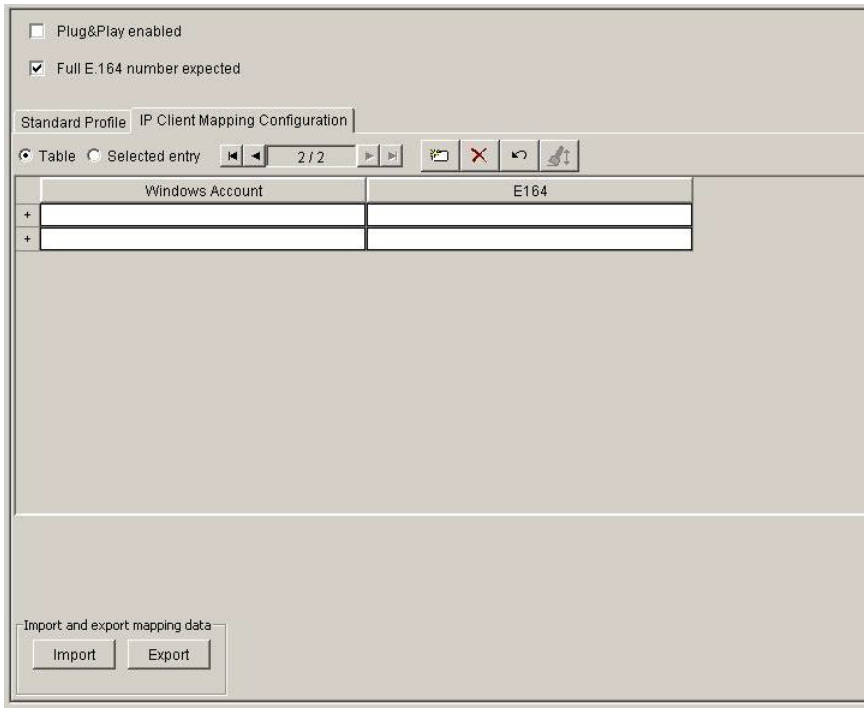
1. Click the **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** area.
2. Click **Import File** in Search view.
3. Enter the name of the CSV file you wish to import in the next dialog. In this dialog, you can also specify whether workpoints created during the import should be created as IP phones and/or IP clients. Confirm the next dialog by clicking **Open**.
4. A window appears on the client confirming that import was executed and giving the location of the log file containing the import results.

15.14.3 Plug&Play Data over OpenScape Desktop Clients

OpenScape Desktop Clients must be setup in relation to DLS Virtual Device records in order to make use of the DLS IP address in order to be able to establish a connection to DLS.

The following steps describe how to promote Plug & Play Data by the DLS when the OpenScape Client is running.

1. Go to **Administration** > **Server Configuration** > **P&P Settings** > **"IP Client Mapping Configuration" Tab**
2. Prepare a .csv file by clicking the **Add Entry**  icon.



NOTE: Click the icon to delete the entry at your will.

NOTE: Click the icon to add entries one-by-one.

3. Use the **Selected Entry** view to import mapping data for a Windows PE / WE client.
4. In the Windows Account textbox enter the respective domain / Windows Account of the client.
5. In the ’E.164’ textbox enter the number for this client.
6. In the **Import and Export mapping data** field press **Import**. Select the previously edited .csv file.
7. Press **Save**.
8. In **Table** view verify that the import was successful.
9. Login to the PE (OpenScape Desktop Client Personal Edition) / WE (Web Embedded) client with the Windows Account given by the previous mapping.

NOTE: The subscriber should acquire the specified ’E.164’.

15.14.4 Syntax of the .csv Files

The .csv file used for import and export has following format:

- 1st row: Description of content of columns
- 2nd and following rows: command and parameters

Empty lines and lines starting with a '#' will be ignored.

If a virtual ID is used (no MAC address), a second trial is ignored, and will be documented in the protocol file. As long as different MAC addresses are in use, it is possible to create multiple devices with a common E.164 number.

NOTE: Prior to changing keys or keysets, a device must be created.

NOTE: This format is supported by DLS version V2R2 onwards. Older formats are supported further on; in such cases, all devices are imported als IP phones. If IP clients are to be imported, a conversion to the previously described format is necessary.

You can find a list of parameters under Section 15.14.4.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

15.14.4.1 Create a SIP Phone (CreateSIPPhone)

Command syntax for creating a SIP phone:

```
CreateSIPPhone;<DeviceID>;<e164 number>;<IP Phone Type>;<Software Type>;<Software Version>;<Device Profile>;<Remark>;<Basic Profile>;<Restore Basic Profile after Workpoint Reset>;<Remark2>;<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>;<Secure Mode Required>;<PIN Mode>;<Remark2>
```

You can find a parameter list under section Section 15.14.4.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateSIPPhone;00:1A:E8:34:4F:BE;302109998062;OpenStage 80;Unify SIP;V3 R0.61.0;;;;false;302109998062;302109998062;;;;10.11.221.54;5060;10.11.221.54;5060;0;;5060;;true; Individual PIN;
```

15.14.4.2 Create an HFA Phone (CreateHFAPhone)

Command syntax for creating a HFA phone:

```
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)>;<Remark2>
```

You can find a parameter list under section Section 15.14.4.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateHFAPhone;00:01:E3:25:E2:19;498972221456;OpenStage 80;Unify HFA;V1
R0.0.93;;;;false;21456;218.1.16.211;;;;;
```

15.14.4.3 Create a SIP Client (CreateSIPClient)

Command syntax for creating a SIP phone:

```
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>;
```

You can find a parameter list under section Section 15.14.4.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateSIPClient;00:19:99:03:5B:0E;498972221458;Unify OpenScape Desktop Client;
Unify oC-Bundle;5.1.182.0000;;;;;;;;;218.1.16.211;218.1.16.211;5060
;;5060;;
```

15.14.4.4 Create an HFA Client (CreateHFAClient)

Command syntax for creating an HFA Client:

```
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)>
```

You can find a parameter list under section Section 15.14.4.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateHFAClient;00:19:99:03:5B:0E;498972221458;Unify OpenScape Desktop Client;
Unify oC-Bundle;5.1.182.0000;;;;;21458;;;;;;
```

15.14.4.5 Create an IP Gateway (CreateIpGateway)

Command syntax for creating an IP Gateway:

```
CreateIpGateway;<DeviceID>;<IP Gateway Type>;<Software Type>;
<Software Version>;<Device Profile>;<Remark>
```

You can find a parameter list under section Section 15.14.4.10, "Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway".

Example:

```
CreateIpGateway;139.21.93.205;HG1500;Unify CGW;HXG_V7_R0.215.4;;;
```

15.14.4.6 Modify Key

This command enables enables to create or change the configuration of a particular device key. You can set any device key, depending on the type, software and version of the IP phone. With the reset parameter, all key functions can be deleted before setting them newly. If this field is empty, the existing keys remain unchanged.

Syntax:

```
ModifyKey;<reset>;<e164 number>|deviceId=<deviceId>;
<key function>;<level>;<module>;<key-number>[;<name>=<value>]+
```

NOTE: The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

You can find a list of parameters under Section 15.14.4.11, "Parameter Description for ModifyKey, ModifyKeyset".

Examples

1. An OptiPoint 410 advance shall be equipped with a control key for a headset:
   `ModifyKey;false;218116231;024;001;0;1;locked-function-keys=false;`
   As an alternative, the UI term "headset" can be used for defining the key function, instead of the function number (here: 024).

2. For setting up a direct station select (DSS) key, 2 steps are required:
   1. Set up a primary line
   `ModifyKey;false;218116230;line;000;0;1;`
   `line-sip-uri=49897223500;line-primary=true;`
   2. Set up the direct station select key
   `ModifyKey;false;218116230;dss;000;0;3;line-sip-uri=498972233439`
3. To delete a function key, set the key function to "Key Unused". In this example, key #3 is deleted:
   `ModifyKey;false;218116232;Key Unused;0;0;3`

15.14.4.7 Modify Keyset

The values of a keyset can be modified. With the reset parameter, all key functions can be deleted before setting them newly. If the field is empty, the existing keyset vaues remain unchanged.

Syntax:

`ModifyKeyset;<reset>;<e164 number>|deviceId=<deviceId>[;<attribute-name>=`
`<attribute-value>]+`

NOTE: The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

You can find a parameter list in Section 15.14.4.11, "Parameter Description for ModifyKey, ModifyKeyset".

Example

In the following example, multiple parameters are set:

1. Rollover volume is set to 2 (line-rollover-volume).
2. Show focus is reset (keyset-use-focus => 0; true/false can also be used for activating/deactivating.
3. LED on registration is set (line-registration-leds, 0/1 can be used as well).

```
ModifyKeyset;false;218116230;line-rollover-volume=2;
keyset-use-focus=0;line-registration-leds=true;
```

15.14.4.8 Modify Device Attributes (ModifyDevice)

This command enables to create or change device attributes, dependent on type, software and version of the IP phone. The allowed device attributes are described under:

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_Device_EN.html
```

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_SIPRegistration_EN.html
```

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_HFARegistration_EN.html
```

Syntax:

```
ModifyDevice;<e164>|deviceId=<deviceId>[;<attribute-name>=<attribute-value>]+
```

NOTE: The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

You can find a parameter list under Section 15.14.4.12, "Parameter Description for ModifyDevice".

Example:

```
ModifyDevice;218116230;remark=Testdeviceconfiguration;
display-id=6230;display-id-unicode=6230;
```

15.14.4.9 Modify OpenScape Data (ModifyOpenScape)

This command enables modification of OpenScape Data.

The allowed attributes and their values are described under:

```
...\DeploymentService\api\doc\v200\dlsapi\
device\index_OpenScapeParam_EN.html
```

Syntax:

```
ModifyOpenScape;<reset>;<e164 number>|<deviceId=anyDeviceId>
[;<attribute-name>=<attribute-value>]+
```

NOTE: The default value is `e164`. If a device ID is to be used, `deviceId=<deviceId>` must be written.

Example:

```
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;
```

15.14.4.10 Parameter Description for Create SIP/HFA Phone, Create SIP/HFA Client, Create IP Gateway

Unless otherwise stated, it is about parameters in the menu Call: Main Menu > Call: Main Menu >> IP Phone Configuration > Gateway/Server.

Parameter	optional/required	DLS Parameter	Description
Device ID	optional	Device ID	MAC address. If not specified, a virtual ID is created by the DLS.
e164 number	required	E.164	Unique E.164 number, max. 24 characters.
IP Phone Type, IP Client Type, IP Gateway Type	optional	Device Type	Device type or virtual device. Alphanumeric, max. 50 characters. Possible values: IP Phone Type: "Possible Values for IP PhoneType". IP Client Type: Possible Values for IP Client Type: IP Gateway: Possible Values for IP Gateway Type:
Software Type	optional	SW Type	Alphanumeric, max. 30 characters.

Table 10

Parameter	optional/required	DLS Parameter	Description
Software Version	optional	SW Version	Alphanumeric, max. 30 characters.
Device Profile	optional	Device Profile	Alphanumeric, max. 30 characters.
Remark	optional	Remark	Alphanumeric, max. 256 characters.
Basic Profile	optional	Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration > "Profile" Tab > Basic Profile	Alphanumeric, max. 40 characters.
Restore Basic Profil after Workpoint Reset	optional	Apply Basic Profile at IP Device Registration	Possible values: true / false or 1/ 0
Terminal Name	optional	Terminal Name	Alphanumeric, max. 255 characters.
Display ID	optional	Display ID	Alphanumeric, max. 24 characters
SIP User ID	optional	UserID	1st part of SIP URL, alphanumeric, max. 20 characters
SIP Password	optional	Password	Password, max. 25 characters
SIP Realm	optional	SIP Realm	Alphanumeric, max. 93 characters.
SIP Server Addr	optional	Reg-Adr	IP Address, max. 25 characters
SIP Server Port	optional	Reg-Port	Port number, numeric, max. 5 Zeichen, default: 5060.
SIP Registrar Addr	optional	SIP Registrar Adr	IP Address, alphanumeric, max. 255 characters
SIP Registrar Port	optional	SIP Registrar Port	Portnumber, numeric, max. 5 characters
SIP Routing	optional	SIP Routing	Poss. Values: Server, Gateway, Direct
SIP Gateway Addr	optional	SIP Gateway Addr	IP Address, alphanumeric, max. 255 characters
SIP Gateway Port	optional	SIP Gateway Port	Portnumber, numeric, max. 5 characters, default: 5060
Subscriber Number	optional	Registration Subscriber Number	HFA parameter, E.164 number, max. 24 characters
Gatekeeper	optional	Gatekeeper ID	HFA parameter, domain-ID, max. 255 characters

Table 10

Parameter	optional/required	DLS Parameter	Description
Gatekeeper Password	optional	Subscriber Password	HFA parameter, password, max. 24 characters
Subscriber Number (Standby)	optional	Registration Subscriber Number (Standby)	HFA parameter, E.164 number, max. 24 characters
Gatekeeper (Standby)	optional	Gatekeeper ID (Standby)	HFA parameter, domain ID, max. 255 characters
Gatekeeper Password (Standby)	optional	Subscriber Password (Standby)	HFA parameter, password, max. 24 characters

Table 10

15.14.4.11 Parameter Description for ModifyKey, ModifyKeyset

Parameter	optional/required	DLS Parameter	Description
Device ID	optional	Device ID	MAC address. If not specified, a virtual ID is created by the DLS.
e164 number	required	E.164	Unique E.164 number, max. 24 characters.
key function	optional	Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/ Keylayout > "Destinations" Tab > Key function	For possible values, see table "Possible Values for Key Function".
level	optional	Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/ Keylayout > "Destinations" Tab > Level	Poss. Values: 0 = 1st Level,1= 2nd Level, 2 = 3rd Level, 3 = 4th Level
module	optional	Module	Poss. Values: 0 ... 4
key-number	optional	Call: Main Menu > Call: Main Menu > > IP Phone Configuration > Keysets/ Keylayout > "Destinations" Tab > Key number	Numeric. For possible values, please see table "Possible Values of name for ModifyKey".
attribute-name	optional	----	For possible values, please see table "Possible Values of name for ModifyKey".
name	optional	----	For possible values, please see table "Possible Values of name for ModifyKey".
reset	optional	No DLS parameter	Poss. values: true/false, 1/ 0

15.14.4.12 Parameter Description for ModifyDevice

Parameter	optional/required	DLS Parameter	Description
Device ID	optional	Device ID	MAC address. If not specified, a virtual ID is created by the DLS.
e164 number	required	E.164	Unique E.164 number, max. 24 characters.
attribute-name	optional	----	For possible values, see the table "Possible Values for attribute-name in ModifyDevice".

Possible Values for attribute-name in ModifyDevice

- `...\DeploymentService\api\doc\v200\dlsapi\device\index_Device_EN.html`
- `...\DeploymentService\api\doc\v200\dlsapi\device\index_SIPRegistration_EN.html`
- `...\DeploymentService\api\doc\v200\dlsapi\device\index_HFARegistration_EN.html`

Possible Values for IP PhoneType

- 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

Possible Values for IP Client Type

- optiPoint 130
- Unify OpenScape Desktop Client
- AC-Win 2Q IP
- AC-Win MQ IP

Possible Values for IP Gateway Type

- HG1500
- HG3500
- HG3575
- HOOEE
- HOOME V1
- HP2K V2.0

Possible Values for Key Function

Function	Code
Key Unused	000
Selected Dialing	001
Abbreviated Dialing	002
Repeat Dialing	003
Missed Calls	004
Voice Messages	005
Forwarding	006
Loudspeaker	007
Mute	008
Ringer Off	009
Hold	010
Alternate	011
Blind Transfer	012
Join (optiPoint)	013
Transfer Call (OpenStage)	013
Deflect	014

Table 11

Function	Code
Setup Menu	015
Room Echoing	016
Room Muffled	017
Shift	018
Notebook	019
Settings	020
Phone Lock	021
Conference	022
Local Conference	023
Headset	024
Do Not Disturb	025
Group Pickup	029
Repertory Dial	030
Line	031
Feature Toggle	032
Show Phone Screen	033
Swap Screen	041
Mobility	042
Call Park	044
Call Pickup	045
Cancel/Release	046
Ok Confirm	047
Callback Request	048
Cancel Callback	049
consultation transfer	050
DSS	051
State Key	052
Call Waiting Toggle	053
Immediate Ring	054
Preview Key	055
Call Recording	056
AICS Zip	057
Server Feature Key	058
BLF	059
start application	060
send url	063
built-in forwarding	064

Table 11

Function	Code
built-in release	065
built-in voice dial	066
built-in redial	067
start phonebook	068
2nd alert	069

Table 11

Possible Values of name for ModifyKey

Name	DLS Parameter	DLS description	Type
key-destination	Destination	Destination data to be dialed. This can be a digit string or a URL.	Alphanumeric, max. 255 characters
state-key-uri	Feature-URI	URI used to control this feature on the server.	Alphanumeric, max. 48 chars
line-primary	Primary Line	Specifies whether the line operates as a primary line.	Poss. values: true/false
line-sip-uri	Address of record	Line’s phone number and address of record.	E.164 number
line-sip-realm	Realm	SIP realm for the line's address of record.	Alphanumeric, max. 48 characters
line-sip-user-id	UserID	User ID	Alphanumeric, max. 48 characters
line-sip-pwd	Password	Password	Alphanumeric, max. 48 characters
line-ring	Ring	Ring	Poss. values: true/false
line-hunt-sequence	Hunt Ranking	Hunt Ranking	0 ... 10
line-shared-type	Shared type	Shared type	Poss. Values: • Private • Shared • Unknown
feature-toggle-description	Toggle text	Label for the "Feature Toggle" key function.	Alphanumeric, max. 24 characters
feature-toggle-code-description-unicode	Toggle text (Unicode)	Label for the "Feature Toggle" key function in unicode.	Alphanumeric, max. 24 characters
state-key-description-text	State Key Description	Description text for the state key.	Alphanumeric, max. 22 characters
state-key-description-text-unicode	State Key Description (Unicode)	Description text for the state key in unicode.	Alphanumeric, max. 22 characters

Table 12

Name	DLS Parameter	DLS description	Type
key-label	Key Label	A key label can be entered here for every key in the case of Self labeling Keys workpoints (for example, optiPoint 420 standard).	Alphanumeric, max. 24 characters
key-label-unicode	Key label (Unicode)	You can enter the key label in unicode characters for devices in the OpenStage family.	Alphanumeric, max. 24 characters
line-hidden	Show on APM/DSM	Check box for activating the line display on the optiPoint Application Module/Display Module	Poss. values: true/false
line-int-allow	Line intrusion allowed	Check box for enabling line intrusion	Poss. values: true/false
line-hld-active	Line Hotline Dest. active	Check box for activating a line hotline.	Poss. values: true/false
line-hld	Line Hotline Destination	Subscriber number that is used as a destination for the line hotline.	Alphanumeric, max. 60 characters
line-mlo-pos	Overview Position on APM/ DSM	Overview Position on APM / DSM	Number, length 2
line-short-desc	Line Description	Description of Line	Alphanumeric, max. 10 characters
line-hot-line-warm-line	Hot/Warm Line Type		Poss. Values: • Normal • Hot Line • Warm Line
line-ring-delay	Ringing Delay	Time before ringing starts for an alerting call.	Number, length: 5
forwarding-type	Forwarding Type	Forwarding Type	Poss. Values: • on busy • on no reply • unconditionally
locked-function-keys	Lock Key	Check box for locking the function key	Poss. values: true/false
dss-sip-line-type	Line Type	Line Type	Poss. values: • normal • direct

Table 12

Name	DLS Parameter	DLS description	Type
dss-sip-line-action	Line Action	Line Action	Poss. Values: • Consultation • Transfer • No Action

Table 12

Possible Values of name for ModifyKeyset

Internal name	DLS display label	DLS description	Type
dss-sip-deflect	Deflect Alerting Call	active: Deflect Alerting Call by pressing key	Poss. values: true/false
dss-sip-detect-timer	Call Pickup Detect Timer (sec)	Specifies how long group pickup is signaled by the key	Number
dss-sip-refuse	Allow Pickup to be refused	active: Allow Pickup to be refused by pressing key	Poss. values: true/false
line-key-operating-mode	Line Key Operating Mode	Defines what should happen to a line (call) when a connection is established over another line. Call hold: The original call is put on hold. Release: The connection to the original call is cleared	Poss. Values: • Call hold • Release
originating-line-preference	Originating Line Preference	Defines the preferred line to be used for outgoing calls	Poss. Values: • Idle line preference • Primary line preference • Last line preference • No preference
line-registration-leds	Registration LEDs	Activates display when restarting the IP phone indicating whether the IP Device was registered successfully	Poss. values: true/false
keyset-remote-forward-ind	Remote Forward Indication	Activates alerting on a line key when call forwarding is active for its destination	Poss. values: true/false
keyset-reservation-timer	Reservation Timer	Time in seconds indicating how long a line reservation can be maintained	Number

Table 13

Internal name	DLS display label	DLS description	Type
line-rollover-type	Rollover Type	Type of alerting when busy	Poss. Values: • No ring • Alert Ring • Standard • Alerting
line-rollover-volume	Rollover Ring Volume	Volume of alerting when busy	Number
terminating-line-preference	Terminating Line Preference	Defines the preferred line to be used for incoming calls	Poss. Values: • Ringing line preference • Calling line preference with prime line preferred • Ringing line preference • Ringing line preference with prime line preferred • No preference
keyset-use-focus	Show Focus	Activates display showing which line is currently active (line has the focus)	Poss. values: true/false
line-button-mode	Line Button Mode	Mode of line button	Poss. Values: • Single button • Preselection
line-preselection-timer	Line Preselection Timer (sec)	Time in seconds before Line Preselection is cancelled	Number
line-preview-period	Line Key Preview Period	Time in seconds before preview mode is cancelled	Number
shift-key-timeout	Shift Key Timeout	Time in seconds before shift mode is cancelled	Number
stimulus-dtmf-sequence	DTMF Sequence	DTMF Sequence	Alphanumeric, max. 255 chars
blf-audible	BLF audible alert	BLF audible alert	Poss. values: true/false
blf-popup	BLF popup alert	BLF popup alert	Poss. values: true/false
fpk-app-name	Application name	Application name	Alphanumeric, max. 48 chars
send-url-address	Web server address	Host name, domain name, or IP address of web server	Alphanumeric, max. 255 chars

Table 13

Internal name	DLS display label	DLS description	Type
send-url-protocol	Protocol	Protocol	Poss. values: 0: HTTP 1: HTTPS
send-url-port	Port	Port number of web server	Number
send-url-path	Path	Directory path and name of the program or web page. Examples: "servlet/IppGenericServlet" or "webpage/checkin.html"	Alphanumeric, max. 255 chars
send-url-query	Parameters	Parameters (e.g.: parameter1=value1&parameter2=value2)	Alphanumeric, max. 255 chars
send-url-method	HTTP method	HTTP method	Poss. values: 0: Get 1: Post
send-url-user-id	Web server user ID	User identity known by web server	Alphanumeric, max. 48 chars
send-url-passwd	Web server password	Password known by web server	Alphanumeric, max. 48 chars
key-functionality	Key functionality	Key functionality	Poss. Values: 0: Toggle call forwarding 1: Unspecified call forwarding 2: Unspecified

Table 13

15.15 Copy Macro for P&P and Templates

This function enables copying field values to another field automatically. For example, copy registration data for HFA phones to standby configuration by means of a macro command.

To copy a value or parts of it from one field to another, provides a template containing the macro command.

As an example, you can define a template to use the registration subscriber number of the main gateway to be copied to the registration subscriber number (standby): In order to do this, enter the following string in the **Standby Reg** field: `%reg-number%`

When the template is applied, the macro command will be executed and the result will be written to the field and sent to the device.

It is also possible to enter a macro command for a virtual device directly. It will be executed when P&P is applied. For an already registered device, the macro command will be executed immediately via a job.

15.15.1 Macro Command Syntax

The syntax of the macro command

`%<item name >[begin index, end index]%`

consists of the following parts:

- `%` marks the begin and the end of the macro command.
- `item name` names the field whose values are to be copied.
- `begin index` to `end index` (optional): only parts of the value are copied. `$` represents the last index.

  Example: Macro command `%e164%` copies the whole E.164 number; `%e164[1,5]%` copies the first 5 digits of the E.164; `%e164[$-4,$]%` copies the last 5 digits of the E.164.

15.15.2 Available <item name>s

The feature is available for dedicated fields only. The source item `<item name>` has to be part of the same screen as the destination item.

The following fields are supported:

Screen	Field	Item name
IP Devices > IP Phone Configuration > Gateway / Server	E.164	`e164`
	Reg address	`reg-addr`
	Registration Subscriber Number	`reg-number`
	Subscriber Password	`reg-password`
	Gatekeeper ID	`reg-id`
	H.235 Security Mode	`h235securitymode`
IP Devices > IP Client Configuration > Gateway / Server	System Type	`hfa-pbx-type`
	E.164	`e164`
	Reg address	`reg-addr`
	Registration Subscriber Number	`registration-phone-no`
	Gatekeeper ID	`gatekeeper-id`
	H.235 Security Mode	`h235securitymode`

Table 14

15.15.3 Available Destination fields

Screen	Field
IP Devices > IP Phone Configuration > Gateway / Server	E.164
IP Devices > IP Phone Configuration > Gateway / Server > Gateway (HFA) / SIP Server Tab	Registration Subscriber Number
	Subscriber Number
IP Devices > IP Phone Configuration > Gateway / Server > Gateway (Standby) Tab	Reg address
	Registration Subscriber Number
	Subscriber Number
	Gatekeeper ID
	H.235 Security Mode
IP Devices > IP Phone Configuration > Gateway / Server > SIP Terminal Settings Tab	Display ID
	Display ID (Unicode characters)
	Terminal Name
IP Devices > IP Phone Configuration > Gateway / Server > SIP Registering 2	SIP UserID

Table 15

Screen	Field
IP Devices > IP Phone Configuration > Gateway / Server > SIP Registrar	UserID
IP Devices > IP Phone Configuration > Miscellaneous > Display/Phone Settings Tab	Handset Name
IP Devices > IP Phone Configuration > IP Routing > DNS Server Tab	Terminal Hostname
IP Devices > IP Client Configuration > Gateway / Server	E.164
IP Devices > IP Client Configuration > Gateway / Server > Gateway (HFA) / SIP Server Tab	Registration Subscriber Number
IP Devices > IP Client Configuration > Gateway / Server > Gateway (Standby) Tab	System Type
	Reg address
	Registration Subscriber Number
	Gatekeeper ID
	H.235 Security Mode
IP Devices > IP Client Configuration > Gateway / Server > SIP Connection Tab	Terminal Name
IP Devices > IP Phone Configuration > Keyset / Keylayout> " Destinations " Tab	Address of record
	UserID
	Key label
	Key label (Unicode)
Mobile Users> SIP Mobile User Configuration > Keyset / Keylayout> " Destinations" Tab	Address of record
	UserID
	Key label
	Key label (Unicode)

Table 15

16 Administration Scenarios

This chapter contains the following administration scenarios:

- Overload Protection with HiPath 4000
- Workpoint Reinstallation with HiPath 4000
- Workpoint Reinstallation with HiPath 3000
- Configuring a Gateway in DLS
- Replacing an IP Device
- Replacing an Old Workpoint (TDM) with a New One (IP)
- Replacing HFA with SIP Software and Vice Versa with Identical Device IDs
- Configuring an IP Client in DLS
- Changing the IP Address and/or Port Number of the DLS
- Using an EWS with DLS in a Customer Network Without Permanent DLS
- Operating the DLS via the Program Interface (DlsAPI)
- Security: Administering Certificates
- Configuring and Administrating Mobility
- HFA Mobility with HiPath 3000
- Data Structures for DLS-hosted XML applications
- Migration Scenarios
- Syslog Configuration for Event (and security) logging
- Automatic certificate renewal

NOTE: The sequence descriptions provided here are intended as examples. The actual sequence may vary from the description, depending on the particular DLS configuration, the servers or IP Devices used, and the ongoing development of the DLS.

16.1 Overload Protection with HiPath 4000

Certain actions should be followed in order to enable the new DLS overload protection.

> ***NOTE:*** This overload protection mechanism is only meant to support high load situations caused by HFA devices .The minimum load for HFA devices to work with this mechanism is **V2.R0.97**.

Proceed with the following steps :

1. Stop DLS Service.
2. Open [`InstallationPath]\DeploymentService\Tomcat\conf\server.xml`
3. Edit the file as follows:

```
<!-- DLS - Workpoint Interface, default (bootstrapping) port -->
  <Connector port="18443" maxThreads="100" backlog="50000" maxQueueSize="50000"
acceptCount="20000" enableLookups="false" connectionTimeout="150000" maxPostSize="1048576"
      redirectPort="-1" scheme="https" SSLEnabled="true" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA"
clientAuth="false" algorithm="IbmX509"
      keystoreType="PKCS12" truststoreType="PKCS12" protocols="TLSv1"

SSLImplementation="de.siemens.icn.hipath.dls.connector.jsse.bsafe.BSAFEJSSE_WPI_Implementation"
/>

<!-- DLS - Workpoint Interface, secure port -->
  <Connector port="18444" maxThreads="100" backlog="50000" maxQueueSize="50000"
acceptCount="20000" enableLookups="false" connectionTimeout="150000" maxPostSize="1048576"
      redirectPort="-1" scheme="https" SSLEnabled="true" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA"
clientAuth="want" algorithm="IbmX509"
      keystoreType="PKCS12" truststoreType="PKCS12" protocols="TLSv1"

SSLImplementation="de.siemens.icn.hipath.dls.connector.jsse.bsafe.BSAFEJSSE_WPI_Secure_Implement
ation"
  />
```

4. Open `[InstallationPath]\DeploymentService\Tomcat\webapps\DeploymentService\WEB-INF\filterContext.xml`
5. Edit the file as follows :

   <bean id="WPIFilter" class="de.siemens.icn.hipath.dls.wpi.v2.servlet.WPIServletFilter">

   <property name="enabled" value="true"/>

   <**property name="maximumThreads" value="600"/>**

   <property name="wpiEngine">

   <ref bean="wpi-engine"/>

   </property>

   </bean>
6. Start DLS Service.

16.2 Workpoint Reinstallation with HiPath 4000

Requirements

- A working DLS infrastructure (such as, DHCP and DNS server).
- A HiPath 4000 Assistant with deactivated access block[1] configured in the DLS (see Section 11.1.3).

Performing reinstallation

1. Configure the stations in the system, for example, with the help of HiPath 4000 Manager or AMOs. For more information refer to the relevant documentation.
2. Select the **Element Manager** > **Element Manager Configuration** > **"HiPath 4000 Assistant" Tab** area.
3. Click **Synchronize**. This transmits all data for the stations configured in the system to the DLS.
4. Click the area **IP Device Management** > **IP Device Configuration**.
   Click **Search** to find all configured workpoints. The first of the workpoints found is displayed in **Object** view.
5. Change to **Table** view and sort the table by **E.164**.
6. Select the desired, pre-configured virtual device from the table. The **device ID** generated by the DLS for a virtual device is prefixed by "@".
7. Enter the **Device ID** of the workpoint.
8. Click **Save**.
9. Connect the workpoint.

This completes reinstallation.

1 To deactivate the access block, select **Access Management** > **Password Management** > **System Password Management** > Password **uas_read** in the HiPath 4000 Assistant and deactivate the option **Block password**. Enter the password and save your changes.

16.3 Workpoint Reinstallation with HiPath 3000

Requirements

- A working DLS infrastructure (such as DHCP- and DNS server).
- A HiPath 3000/5000 configured in the DLS (see Section 11.1.4).

Performing reinstallation

1. Configure the stations in the system. For more information refer to the relevant documentation.
2. Select the **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** area to create an station, that is, a virtual device, in the DLS. Instead of a device ID, the virtual device receives a placeholder generated by the DLS beginning with "@".
3. Enter the **E.164** of the new station.
4. Click the **Element Manager** > **Element Manager Configuration** > **"HiPath 3000/5000" Tab** area.
5. Click **Synchronize**. If the E.164 already exists in one of the configured HiPath 3000/ 5000 DB Feature Servers, the relevant gatekeeper address is added to the data record.
6. Enter the device ID of the workpoint in **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration**.
7. Click **Save**.
8. Connect the workpoint.

This completes reinstallation.

16.4 Configuring a Gateway in DLS

Requirements

- A working DLS infrastructure.
- A configured gateway (HG1500, HG3530, HG3550, HG3570, HG3575 or RG2700).

16.4.1 Adding Gateways

1. Click the **Gateways** > **Gateway Configuration** area.
2. Click **New**.
3. Select the gateway you want under Gateway Type. Once you have made this selection, all unnecessary fields are deactivated (dimmed).

   NOTE: If a gateway of the same category is already configured, you can copy the data from this and modify it to meet your requirements. Find the gateway you want to copy data from and select **New**.
4. If necessary, add a description of this gateway under **Remark**.
5. Enter the necessary data in the "Gateway Connection" Tab. The following is a list of entries required for the various gateway types.

   - **HG1500** (for HiPath 3000/5000, direct connection), **RG2700**

     Gateway IP Address: IP address of the gateway.

     Account: Gateway access ID (as configured in the gateway, default ID: **31994**).

     Password: Password for accessing the gateway (configured on the gateway as described above for the account).

   - **HG3550** (for HiPath 4000, connection via the HiPath 4000 Assistant)

     Gateway IP Address: IP address of the gateway.

     Gateway Proxy IP Address: IP address of the relevant HiPath 4000 Assistant.

     Gateway Proxy Port: 443.

     Account: Access ID for HiPath 4000 Assistant (as configured on the Assistant). You must use an ID in the HiPath 4000 Assistant that contains user rights for HG3550Mgr.
     For information on creating IDs and assigning rights with this tool, refer to "Access Management" in the HiPath 4000 Assistant online help.

     Password: Password for accessing HiPath 4000 Assistant (configured on HiPath 4000 Assistant as described above for the account).

   - **HG3530**, **HG3570**, **HG3575** (for HiPath 4000, connection via SNMP proxy - an integral part of the DLS server)

     Gateway IP Address: IP address of the gateway.

SNMP Community: Community string (for authenticating SNMP communication to the gateway). Default community string: **nbcs**.
The community string must be set to the same value as the relevant gateway in HiPath 4000 (AMO HFAB: TYP=SNMP, parameter: CS2).

NOTE: During DLS installation, the SNMP proxy is also installed at the same time and automatically started as a local service on the DLS server PC. You can stop and start the SNMP proxy manually on this PC.
To access this service, select: Start > Settings > Control Panel > Administrative Tools > Services > DeploymentServiceSNMPProxy

6. Click **Save** to apply the entries.

16.4.2 Release Information (QDC and 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 (may still "officially" be V2.0)
- HG3530: V3.0 (may still "officially" be V2.0)
- HG3570: No VoIP security
- HG3575: No VoIP security
- RG2700: No VoIP security

16.5 Configuring Certificates in DLS

In order to support distribution of mass certificates to phones and clients the OpenScape Deployment Service (DLS) supports its own internal public key infrastructure (PKI).The purpose is to secure communication between

- DLS and phones / clients
- DLS and OpenScape Voice Assistant, and the
- DLS and web browsers.

This internal PKI operates like most other PKI's. It can create its own CA, create certificates signed by this CA, and even automatically distribute these certificates. On top of this it can also maintain more than one internal PKI to allow for certificate management of different functions within the phone.

NOTE: Certificate format: PKCS#12 formatted keystore or use of the Deployment Service's internal PKI infrastructure.

Figures 1 and 2 illustrate examples of certificate and PKI hierarchies.

In figure 1 the Deployment Service's public facing interfaces employ a certificate from the customers CA while the phones' certificates are managed by the Deployment Service's internal PKI. The Deployment Service can maintain more than one PKI to manage different phones functions requiring certificates. A single internal PKI can also be used.

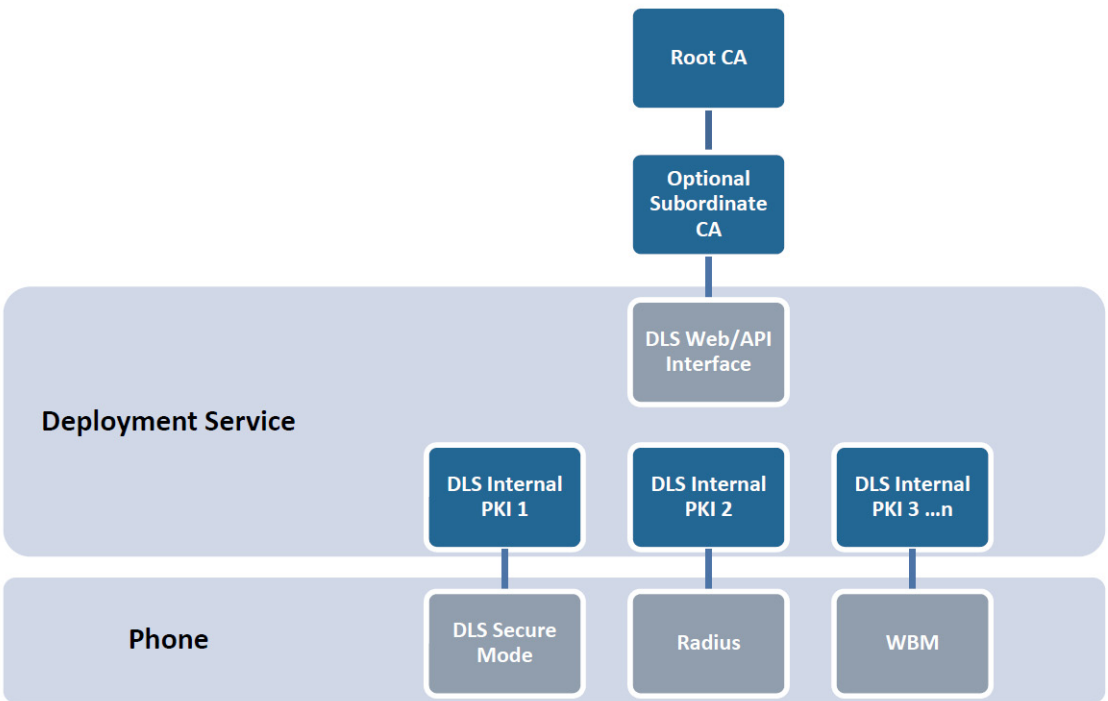


Figure 1 Deployment Service Certificate hierarchy example

The OpenScape Deployment Service also supports integration with an external Microsoft certificate authority. In this case the Deployment Service PKI depends on the Microsoft CA to manage and create certificates while the DLS handles the distribution aspect. Use of the Microsoft CA is not discussed in this document. Instead please refer to the OpenScape Deployment Service PKI Basic Configuration guide.
Figure 2 shows an example certificate hierarchy using a Microsoft certificate authority. The Deployment Service uses a single internal PKI to manage both public facing Deployment Service interfaces and all phone functions requiring certificates.

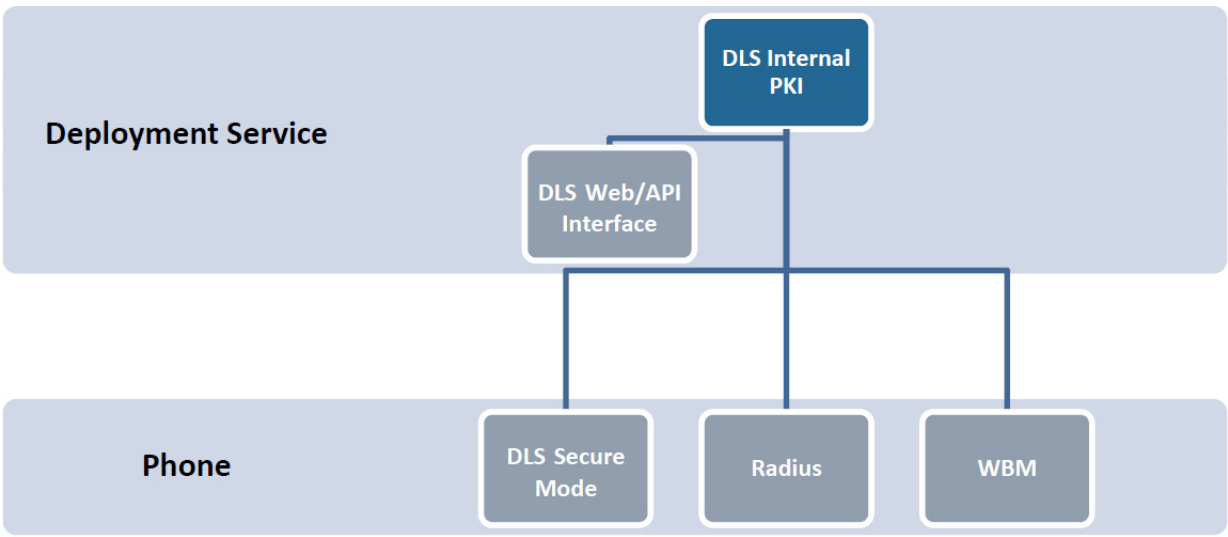


Figure 2 Deployment Service Certidficate hierarchy example 2

16.5.1 Creating a New PKI

It is possible to create more than one PKI. Different PKI's can be used for different purposes.For instance,one PKI could manage all WBM Certificates while another could manage RADIUS server certificate distribution.Or ,one PKI could manage all certificates.

Creation of a new PKI follows three (3) basic steps. Together they create a new PKI.

Proceed with the following steps :

1. Create a new Internal CA
2. Create a new Plug-in Configuration
3. Create a new Connector Configuration

16.5.1.1 Create a new Internal CA

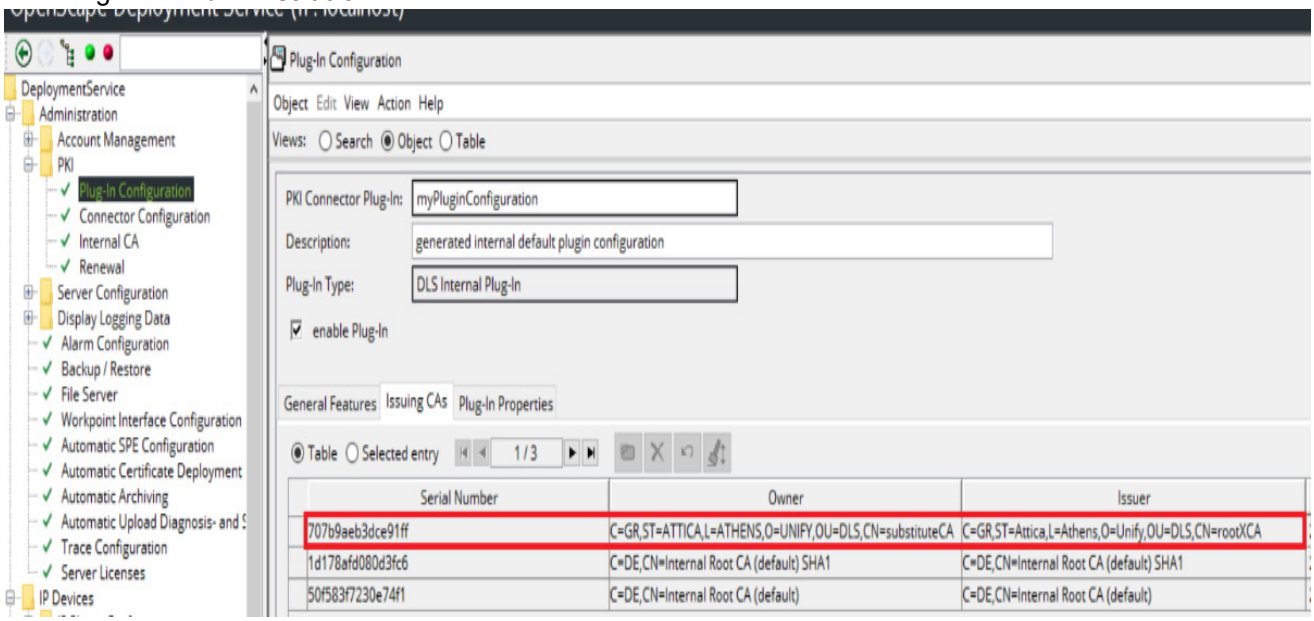
1. Log into the Deployment Service and navigate to **Administration** >**PKI** >**Internal CA**.
2. Click on **New** and enter a **CA Name** and **CA Description**. Click on **Save**.
3. Click **Create CA**. Enter **Subject/Issuer DN** information. This step defines the identity information of the CA and will also be seen in any certificate created by this CA.

   Certificates should at least include country, state or province, organization, organizational unit, and common name information.

   Example: C=US,ST=FL,L=Boca Raton,O=Unify,OU=Sales,CN=MyNewCA
4. Alternate to step 3). It is also possible to create a new internal CA using a predefined CA. This CA certificate can be imported into the Internal CA. Click on **Import CA**.**Browse** for the CA keystore. The keystore must be in a PKCS#12 format. Enter the keystore **Passphrase** and click on **OK**.
5. Set **Key Algorithm** to RSA. Set **Key Size** to 2048. 1024 and 4096 are also possible.
6. Set **Valid from** and **Valid to** dates. Default lifetime is 1 year time. Set this to a more acceptable lifetime for a CA, such as 10 years.
7. Click **OK**. The new CA is created and this information can now be seen.
8. Finally, check **Enable Internal CA** and then **Save**.

16.5.1.2 Create a new Plug-In Configuration

1. Create a new Internal CA as mentioned in Section 16.5.1.1, "Create a new Internal CA".
2. Navigate to **Administration** >**PKI** >.



3. Click on New and provide a name and description in the **PKI Connector Plug-In** and **Description** fields. Click on **Save**.
4. Navigate to the **Plug-In Properties** tab and select the **Table** view radio button.
5. There are two product-embedded (hard-coded) certificate values that should be changed,**internal.default.validity.days** and **internal.x509name.template**. These certificates are embedded in the product build, cannot be replaced or modified via the DLS UI in affected versions, and are updated only through product releases. After certificate expiry there is no functional impact on already operational systems: TLS encryption remains active, Secure Mode communication (port 18444) is unaffected, and existing installations continue to operate without restriction. However, upgrading to DLS V10 R3.20 is recommended for security hygiene and compliance, and becomes necessary if new UC/OSILA connections must be created or modified, or if new devices are to be onboarded using Secure Mode.
6. Select **internal.default.validity.days**. This field defines the number of days certificates created by the Deployment Service are valid for. A typical length is 3 years. Click on **Save**.
7. Select **internal.x509name.template**. This field defines the subject information for certificates the Deployment Service will create. This field acts as a template. Most information is filled, except for the common name (CN). When issuing a certificate the Deployment Service will automatically input the CN based on the end points IP address or FQDN. This allows for easy point and click or automated certificate deployment. This template should match the issuer name information supplied for the root CA in step 1,except for the CN field. The CN field MUST contain a '?'. Click on **Save**.

Example: C=US,ST=FL,L=Boca Raton,O=Unify,OU=Sales,CN=?

8. Click on the **Issuing CAs** tab. Click **Synchronize**. This will pull in all of the enabled internal CA's. We will only used the internal CA we created in step 1). This will be seen in the next steps.
9. Finally, check **Enable Plug-In** and click on **Save**.

16.5.1.3 Create a new Connector Configuration

1. Create a new Internal CA and Plug-In Configuration as mentioned in Section 16.5.1.1, "Create a new Internal CA" and Section 16.5.1.2, "Create a new Plug-In Configuration".
2. Navigate to **Administration** >**PKI** >**Connector Configuration**.
3. Click on **New** and provide a name and description in the **Configuration Name** and **Description** fields. Click **Save**.
4. Select **Plug-In Configuration**. Select the name of the Plug-In Configuration created in Section 16.5.1.2, "Create a new Plug-In Configuration",click on **OK** and then **Save**.
5. Select **Issuing CA Name**. Select the name of Issuing CA created in Section 16.5.1.1, "Create a new Internal CA",click on **OK** and then **Save**.
6. Select the **Trust-Anchor** tab click on **Import Certificate**. Select the **PKI** radio button and under **Import from Connector** select the name of the issuing CA created in Section 16.5.1.1, "Create a new Internal CA". Click **OK** and **OK** again. The CA defined in Section 16.5.1.1, "Create a new Internal CA" is now the trust anchor (root CA) for this PKI. The trust anchor fields should now show this.
7. Navigate to the **Request Parameter** tab. The default settings should be acceptable.Click on **Test**. The Deployment Service will internally create and sign a new certificate to ensure proper operation. A success message should be returned.

   Example: C=US,ST=FL,L=Boca Raton,O=Unify,OU=Sales,CN=?
8. Finally, check **Enable Connector** and then **Save**. At this point a new internal PKI has been created for the DLS. This new PKI can be used to create and deploy certificates to phones and clients.

16.5.2 Deploying the Signaling and Payload Encryption (SPE) Certificate

The signaling and payload encryption (SPE) certificate is simply the CA certificate (or chain of CA certificates) used to sign the OpenScape Voice certificate. When this CA certificate is placed on the phones it allows the phones to identify and verify the OpenScape Voice based on the certificate received from the OpenScape Voice. By default, phones perform no certificate verification. Phones can still connect to the OpenScape voice via TLS and place secure calls.

Before enabling certificate verification for all phones it is advised to manually place the CA certificate on a couple of phones and enable certificate verification. If the test fails the phone will fail to register against the OpenScape Voice. If the test succeeds then automatic certificate deployment can be used to distribute the CA certificate to all phones.

16.5.2.1 Manual Deployment

NOTE: A PKI does not need to be created in order to execute this section.

1. Navigate to **Call: Main Menu > Call: Main Menu >** >**IP Phone Configuration** >**Signaling and Payload Encryption (SPE)** >**"SPE CA Certificates" Tab**.
2. Click on **Import Certificate**.
3. Check **Import certificates to DLS and activate on device (1-step)**. Select **Import using:File**.
   Click on **Browse** and locate the file containing the CA certificates.
4. Finally, click **OK**. The certificate will be imported and a new entry will appear containing the CA certificate information.
5. You can now enable certificate verification. Please refer to Section 16.5.2.2, "How to Enable SPE Certificate Verification".

16.5.2.2 How to Enable SPE Certificate Verification

The phones support three levels of certificate verification, none, full, and trusted. Each level performs more stringent checks. If a check fails on either the trusted or full levels the phone will not be able to register against the OpenScape Voice.

- **None**:
  The default option. No checking of the received certificate is performed. The received certificate is only used to provide an encrypted connection.
- **Trusted**:
  The phone checks the expiration date and signature of the received certificate.
- **Full**:
  The phone checks the expiration date, signature, and certificate usage fields of the received certificate.

To enable verification perform the following steps:

> ***NOTE:*** OpenStage phones running firmware version V3 or later will perform step 1). Older firmware versions and OptiPoint phones will perform step 2).

1. Navigate to **Call: Main Menu > Call: Main Menu > >IP Phone Configuration >Security Settings >"Authentication Policy" Tab**. Under **SIP Server Authentication Policy** choose a verification level. Click **Save**.
2. Navigate to **IP Devices >IP Phone Configuration >Signaling and Payload Encryption>SIP Settings** tab.Check **TLS server validation**.

16.5.3 Deploying new Web Based Management (WBM) certificates to phones

Unify phones are administrable via a secure web based management interface and all phones ship with a product-embedded (hard-coded) certificate. Certificates for the WBM interface can be deployed manually or automatically by the Deployment Service.This certificate is embedded in the product build, cannot be replaced or modified via the DLS UI in affected versions, and are updated only through product releases. After certificate expiry there is no functional impact on already operational systems: TLS encryption remains active, Secure Mode communication (port 18444) is unaffected, and existing installations continue to operate without restriction. However, upgrading to DLS V10 R3.20 is recommended for security hygiene and compliance, and becomes necessary if new UC/OSILA connections must be created or modified, or if new devices are to be onboarded using Secure Mode.

16.5.3.1 Manual Deployment

1. Navigate to **Call: Main Menu > Call: Main Menu > >IP Phone Configuration >Security Settings>"WBM Server Certificate" Tab**.
2. Click on **Import Certificate**. For **Certificate Type** select **WBM Server Certificate**. Check **Import Certificate to DLS and activate on device (1-step)**. Check **Import Using: PKI**. Under **Import from PKI** select the PKI you wish to use. Finally, click **OK**.
3. The certificate will be generated by the DLS and deployed to the phone automatically. Wait a few seconds then click on **Refresh**. You should now see the Imported and Active Certificate fields contain new certificate information. If only the Imported Certificate fields contains information then its possible the activate on device option was not selected in step 2). In this case check **Activate Certificate** and click on **Save**. This will activate the certificate on the phone.

16.5.3.2 Automatic Deployment

1. Navigate to **Administration >Automatic Certificate Deployment**.
2. Click on **New**.Under **Location** select a location. Under **Certificate Type** select **WBM Server Certificate (IP Phone)**. Click **Save**.

NOTE: All phones defined by this location will receive new WBM certificates. Locations can be defined under **Administration** >**Server Configuration** >**Location**.

3. Click **Import Certificate**. Check **Import using: PKI**. Under **Import from PKI** select your PKI. Click **OK**.
4. Under **Deploy Date** select a date and time to deploy the certificates. Click **Save**.
5. Check the **Activate Certificate / PKI Configuration** checkbox. Click **Save**.

Once you click **Save** ,the Deployment Service will automatically create jobs to deploy new WBM certificates to all phones defined by this location. Job completion can be monitored under **Job Coordination** > **Job Control**. Once the job is complete new certificate information can be viewed by navigating to **Call: Main Menu > Call: Main Menu > >IP Phone Configuration** >**Security Settings** >**"WBM Server Certificates" Tab**.

A certificate deployed using automatic methods will only be visible under the active certificate field and not the imported certificate field. The imported certificate field is used for manual deployments. If you have deployed certificates in the past using the manual method then an older certificate may still be present. This does not impact the currently active certificate.

16.5.4 Phone Secure Mode Operation

By default, phones communicate with the Deployment Service using a standard TLS connection.However, if greater security is desired, phones can be set to communicate with the Deployment Service in secure mode. In secure mode communication takes place via mutual TLS (MTLS).

MTLS offers the benefit of a mutually authenticated connection, meaning the Deployment Service verifies the phone and the phone verifies the Deployment Service. If either side cannot verify the other then the connection fails. This method provides an extra layer of protection for the phone as it will not allow another Deployment Service to connect it and manage the phone.

16.5.4.1 Set the Workpoint Interface Configuration PKI

This section changes the PKI used for secure mode operation of phones.

1. Create a new PKI or use an existing one,as described in Section 16.5.1, "Creating a New PKI".
2. Navigate to **Administration** > **Workpoint Interface Configuration**.
3. In the **Secure Mode** tab, under **Server Credentials**, select **PKI Configuration**. Select your PKI, click **OK** and then **Save**.
4. Click **Create**. This creates a new server credential for the Deployment Service based on the PKI chosen in step 1. A new entry will appear in the table. It should be active by default. If it is not, click on it and click **Activate**.
5. Repeat steps 2 and 3 for **Client Credentials**.
6. After the new PKI has been activated you can safely delete the default credentials.

16.5.4.2 Set the Phones to Secure Mode

1. Create the PKI in the Workpoint Interface Configuration as mentioned in section Section 16.5.4.1, "Set the Workpoint Interface Configuration PKI".
2. To place phones in secure mode, navigate to **Call: Main Menu > Call: Main Menu >>IP Device Management**> **IP Device Configuration** >**"DLS Connectivity" Tab**
3. Under **Security Settings** check **Secure mode required**. For **PIN Mode** you can choose between No PIN, Default PIN, or Individual PIN. A PIN encrypts the phones certificate information as it is being transferred to the phone. The default option is Default PIN. This uses the PIN generated by the DLS. This can be found under the Workpoint Interface Configuration screen. If a PIN is used then the PIN must be entered on the phone before secure mode operation is complete.
4. Click **Save**. The Deployment Service will communicate new certificate information to the phone. If a PIN was used then the PIN must be manually entered on the phone to complete the secure mode setup. On an OpenStage phone login as admin and navigate to **Admin** >**Network** >**Update Service (DLS)**. The **Security Status** is in Awaiting PIN state. Enter the PIN in the **Security PIN** field. Once the PIN is entered, press **Save & Exit**. Secure mode setup is now complete.
5. Transition from insecure to secure mode can be monitored under the **Security State Protocol** tab. A phone can be removed from secure mode by un-checking the Secure mode required checkbox.

> ***NOTE:*** If a phone is in secure mode and is unable to communicate with a DLS, it is possible to manually take the phone out of secure mode. On an OpenStage phone login as admin and navigate to **Admin** >**Network** >**Update Service (DLS)** >**Options** and select **Default Security**. This will reset the phone it its default security mode. The phone will now be able to communicate with any Deployment Service. If the phone is to communicate again with the existing Deployment Service then the Deployment Service must also take the phone out of secure mode.

16.5.5 Replacing the DLS Web Interface & API Certificates

The Deployment Service contains a web and API interface. These interfaces are used to communicate with a web browser or the OpenScape Voice Assistant. For this reason it may be desirable to have these interfaces participate in the customer's PKI rather than the Deployment Service's internal PKI.

1. Navigate to **Administration**>**Server Configuration**>**TLS Connector Configuration**.
2. Click **Import and Activate Certificate**. Select **DLS Client GUI**. Select **Import using:File** and then **Browse** for the PKCS#12 formatted keystore. Click **OK**. The certificate is imported and activated.
3. Repeat step 2) for the DLS API. Use the same PKCS#12 keystore.

16.5.6 Internal CA Configuration for AutoSPE

Internal CAs

In order to view the default DLS internal CAs :

Under Administration > PKI > Internal CA, enable the CA or CAs that your configuration requires.

The Internal Plugin, which is the DLS default internal CA generator, has 2 root CAs:

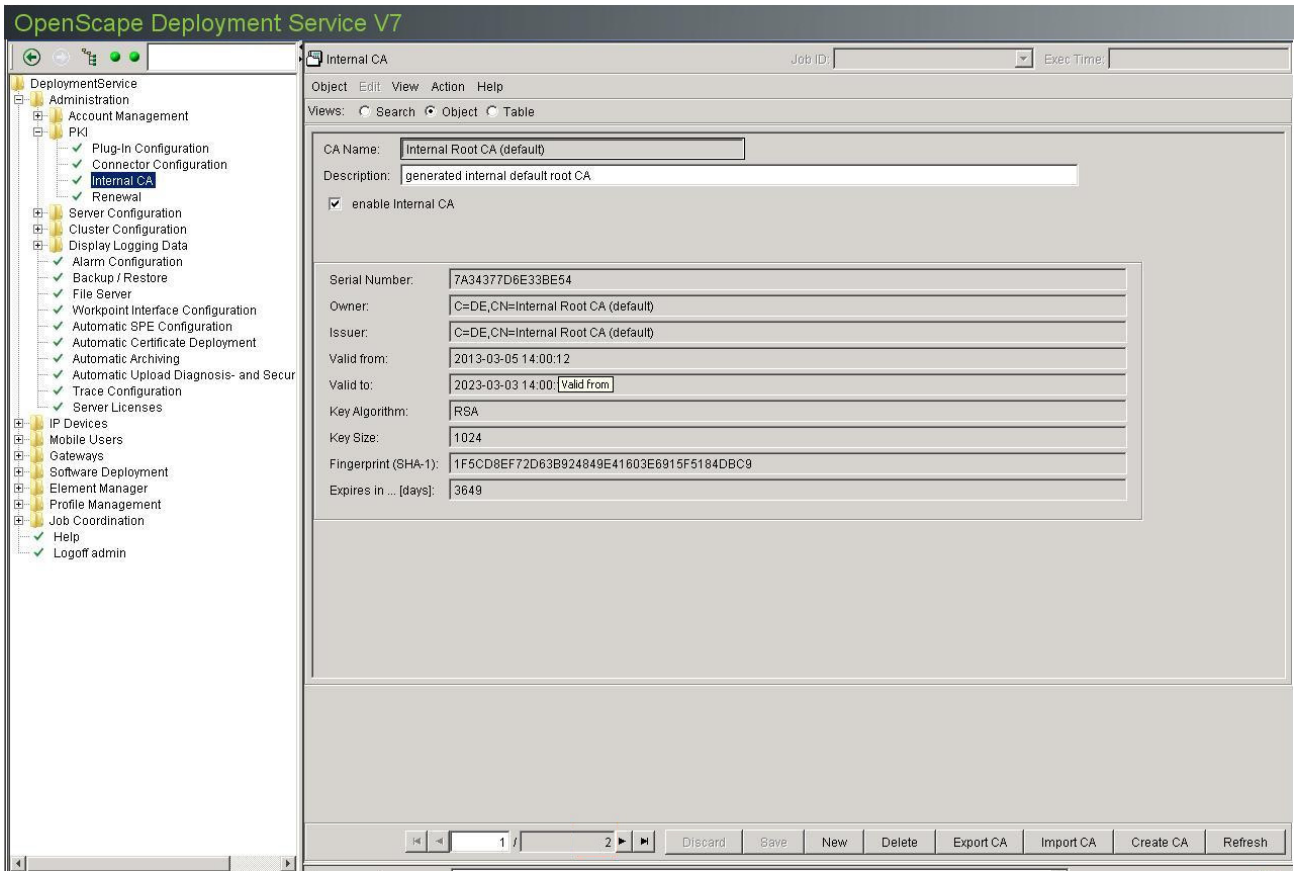
- **Internal Root CA (default)**

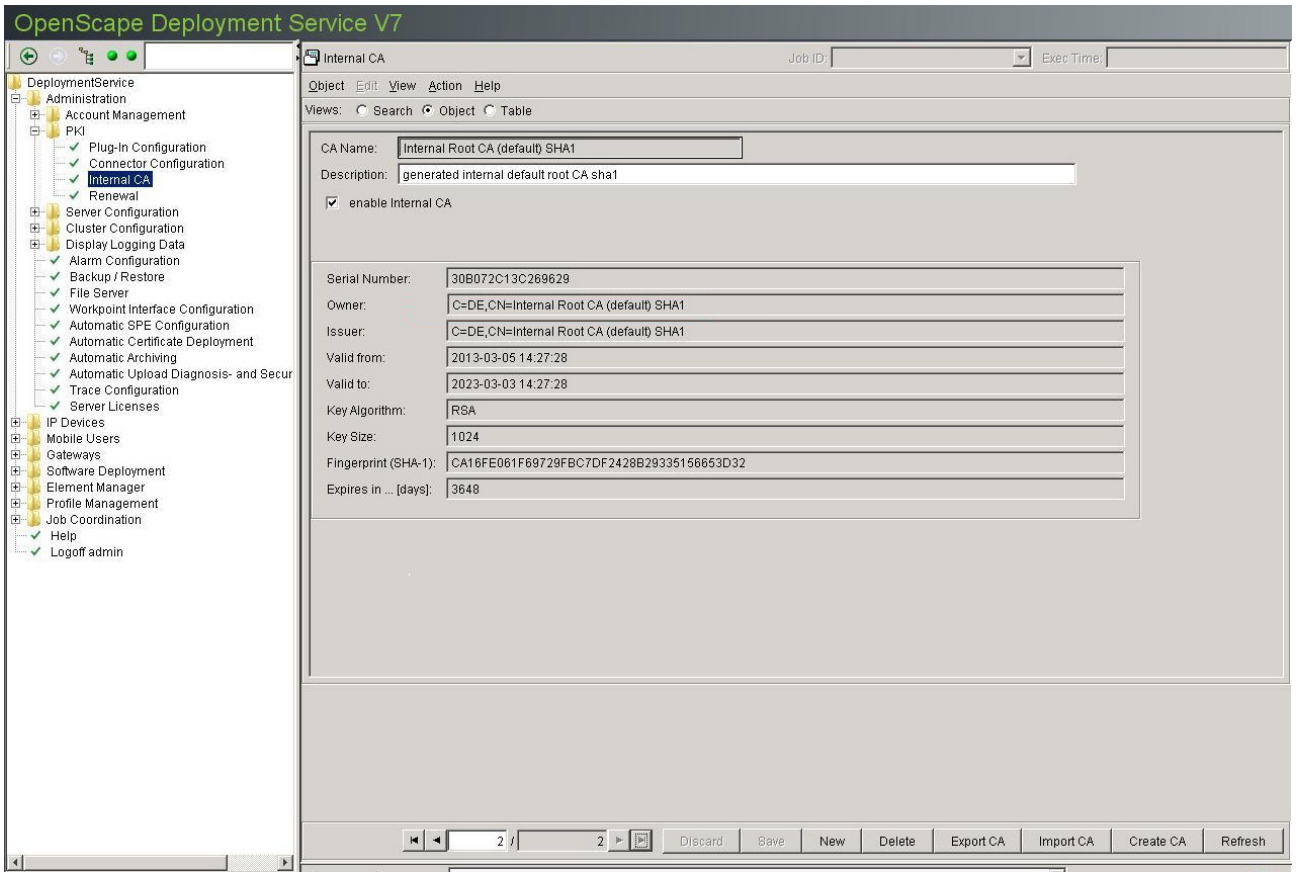
  This is the default internal root CA with SHA-256 as signature algorithm. This CA signs with a more secure algorithm in comparison to that of SHA-1 that is going to be deprecated.

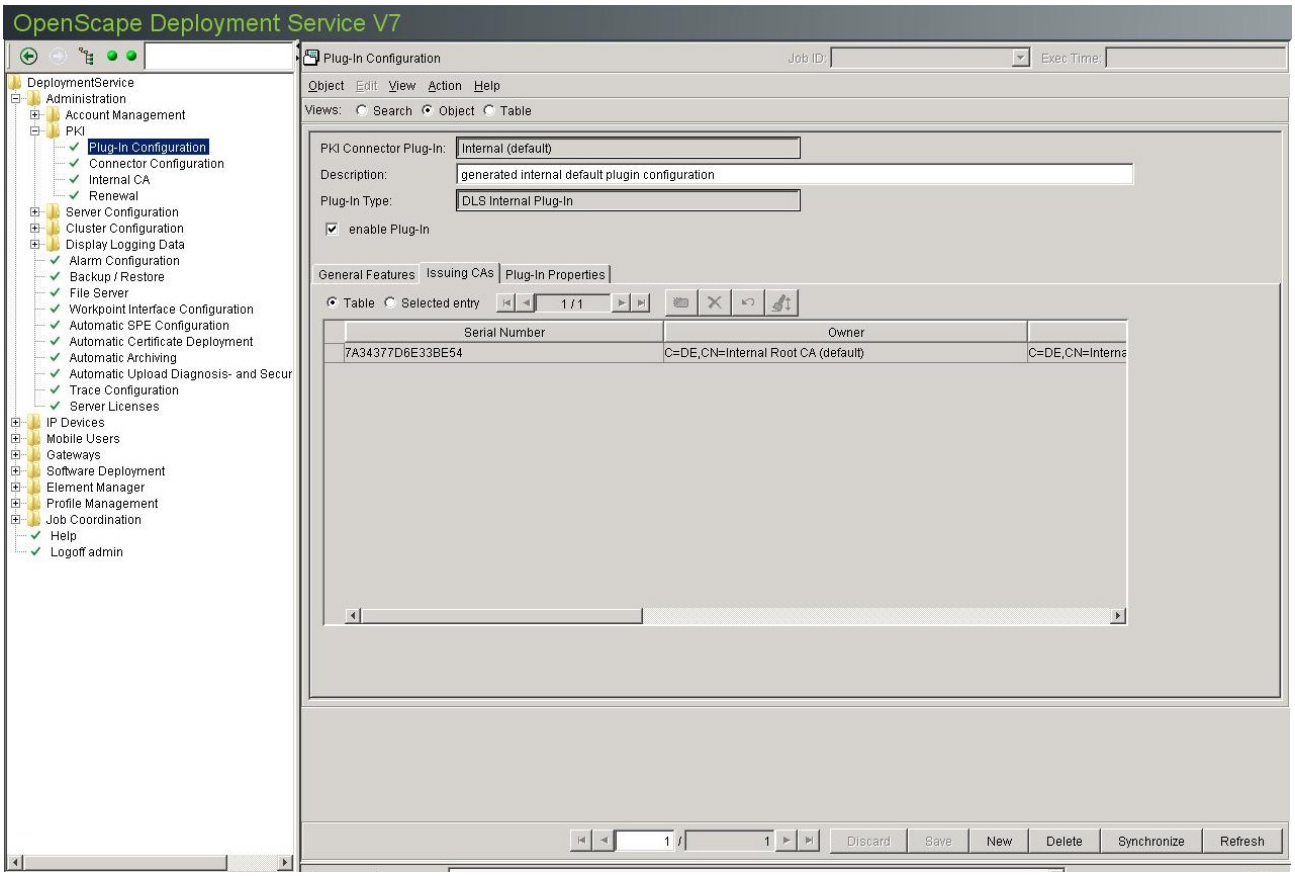
- **Internal Root CA (default) SHA1**

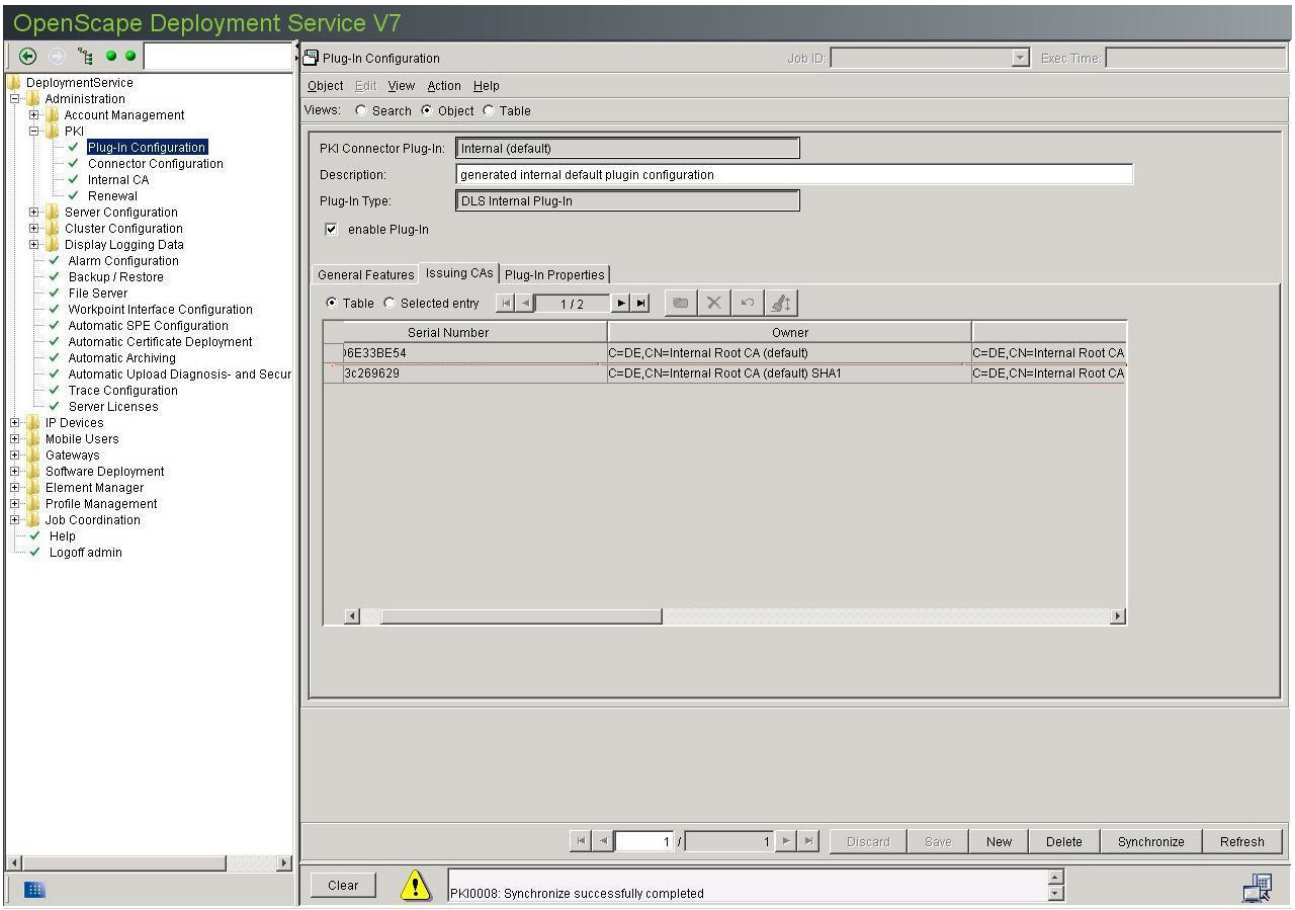
  Internal Root CA (default) SHA1 is being generated with SHA-1 signature. The suffix SHA1 denotes that this is not the default CA with signature algorithm of SHA256. This less secure CA could be used where the additional equipment (devices, switch) do not support the more secure SHA-256 yet.

IMPORTANT: The usage of SHA1 or SHA2 depends on the customer's environment and what the rest of the components (devices, switch) support. This information should be found in the appropriate release notes for the phones and switches.


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
Internal CA
Job ID:
Exec Time:
Object Edit View Action Help
Views: Search Object Table
CA Name: Internal Root CA (default)
Description: generated internal default root CA
enable Internal CA
Serial Number: 7A34377D6E33BE54
Owner: C=DE,CN=Internal Root CA (default)
Issuer: C=DE,CN=Internal Root CA (default)
Valid from: 2013-03-05 14:00:12
Valid to: 2023-03-03 14:00:
Valid from
Key Algorithm: RSA
Key Size: 1024
Fingerprint (SHA-1): 1F5CD8EF72D63B924849E41603E6915F5184DBC9
Expires in ... [days]: 3649
1 / 2
Discard
Save
New
Delete
Export CA
Import CA
Create CA
Refresh


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
Internal CA
Job ID:
Exec Time:
Object Edit View Action Help
Views: Search Object Table
CA Name: Internal Root CA (default) SHA1
Description: generated internal default root CA sha1
enable Internal CA
Serial Number: 30B072C13C269629
Owner: C=DE,CN=Internal Root CA (default) SHA1
Issuer: C=DE,CN=Internal Root CA (default) SHA1
Valid from: 2013-03-05 14:27:28
Valid to: 2023-03-03 14:27:28
Key Algorithm: RSA
Key Size: 1024
Fingerprint (SHA-1): CA16FE061F69729FBC7DF2428B29335156653D32
Expires in ... [days]: 3648
Discard
Save
New
Delete
Export CA
Import CA
Create CA
Refresh


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

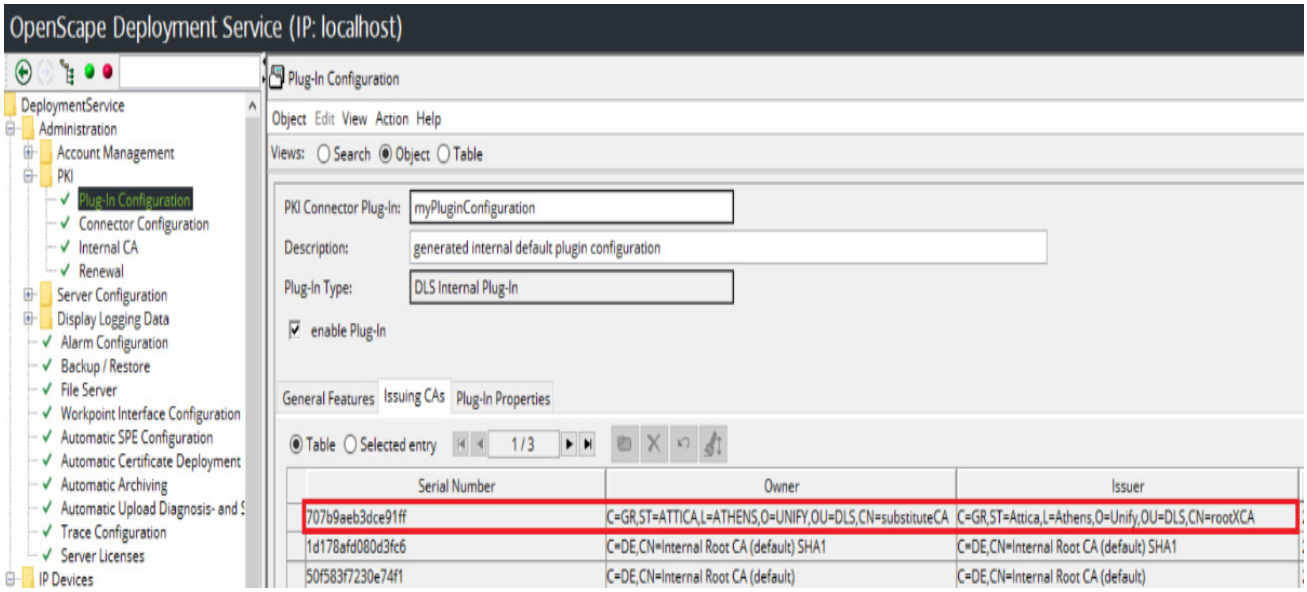


16.5.6.1 Create PKI configuration for use with AutoSPE

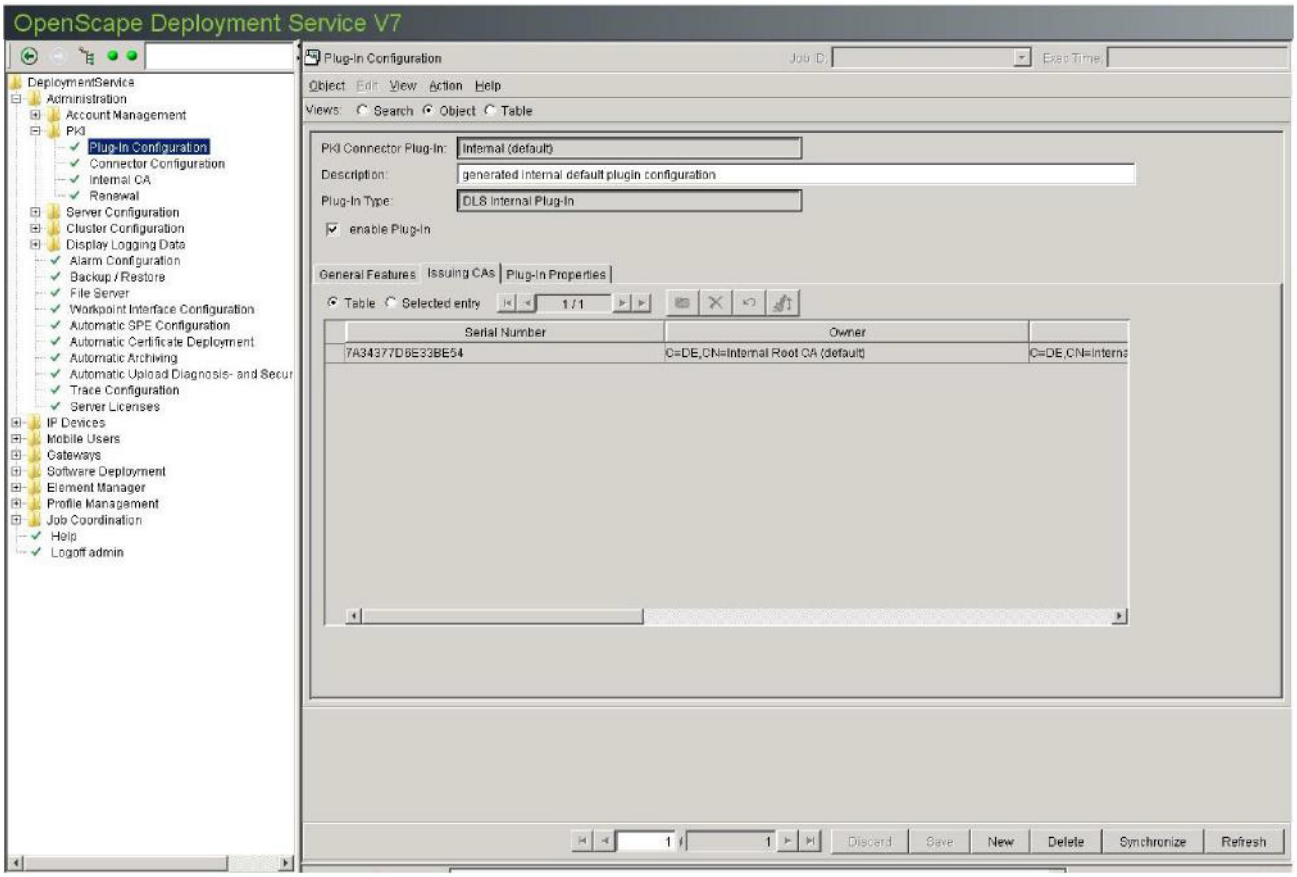
In order to configure the PKI configuration for AutoSPE, proceed with the following steps:

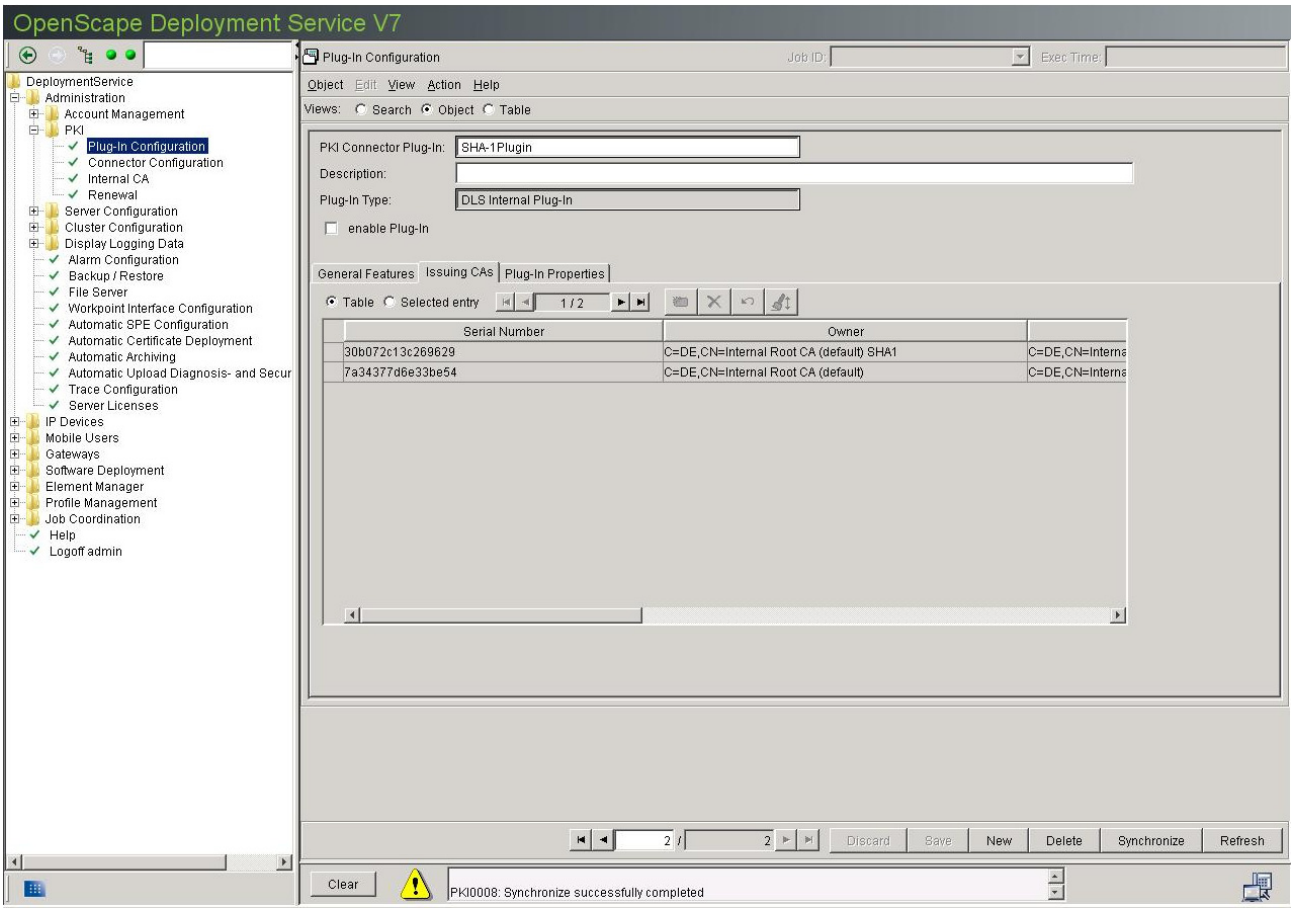
1. Create new Plug-in configuration

   Go to Administration > PKI >



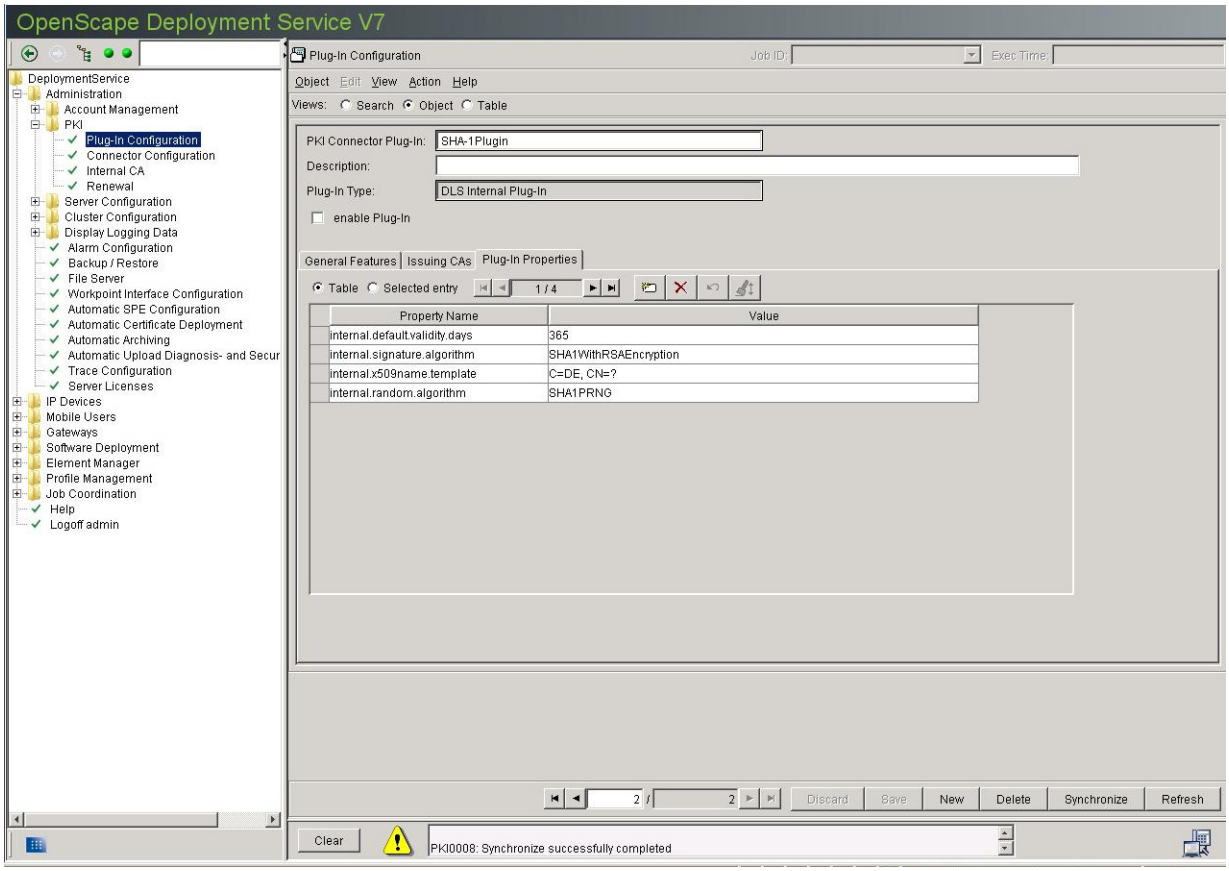
   In a default DLS installation you should see the ‘Internal (default)’ Plug-in. Under the "Issuing CAs" Tab you shall see one certificate. This should be the root certificate of the ’Internal Root CA (default)’ that has SHA-256 as signature algorithm.

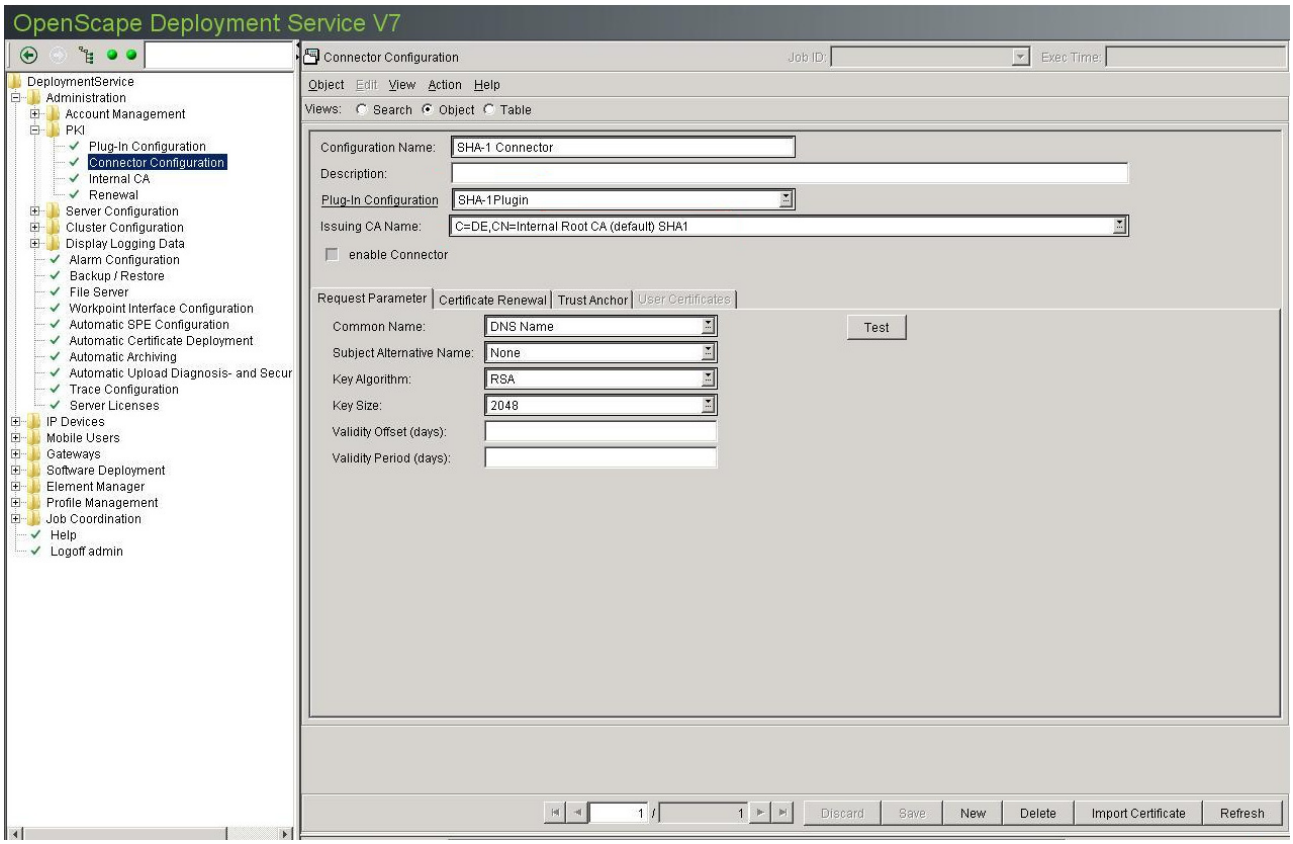

OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Configuration
Connector Configuration
Internal CA
Renewal
Server Configuration
Cluster Configuration
Display Logging Data
Alarm Configuration
Backup / Restore
File Server
Workpoint Interface Configuration
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
7A34377D8E33BE54
C=DE,CN=Internal Root CA (default)
C=DE,CN=Interna
1 / 1
Discard Save New Delete Synchronize Refresh

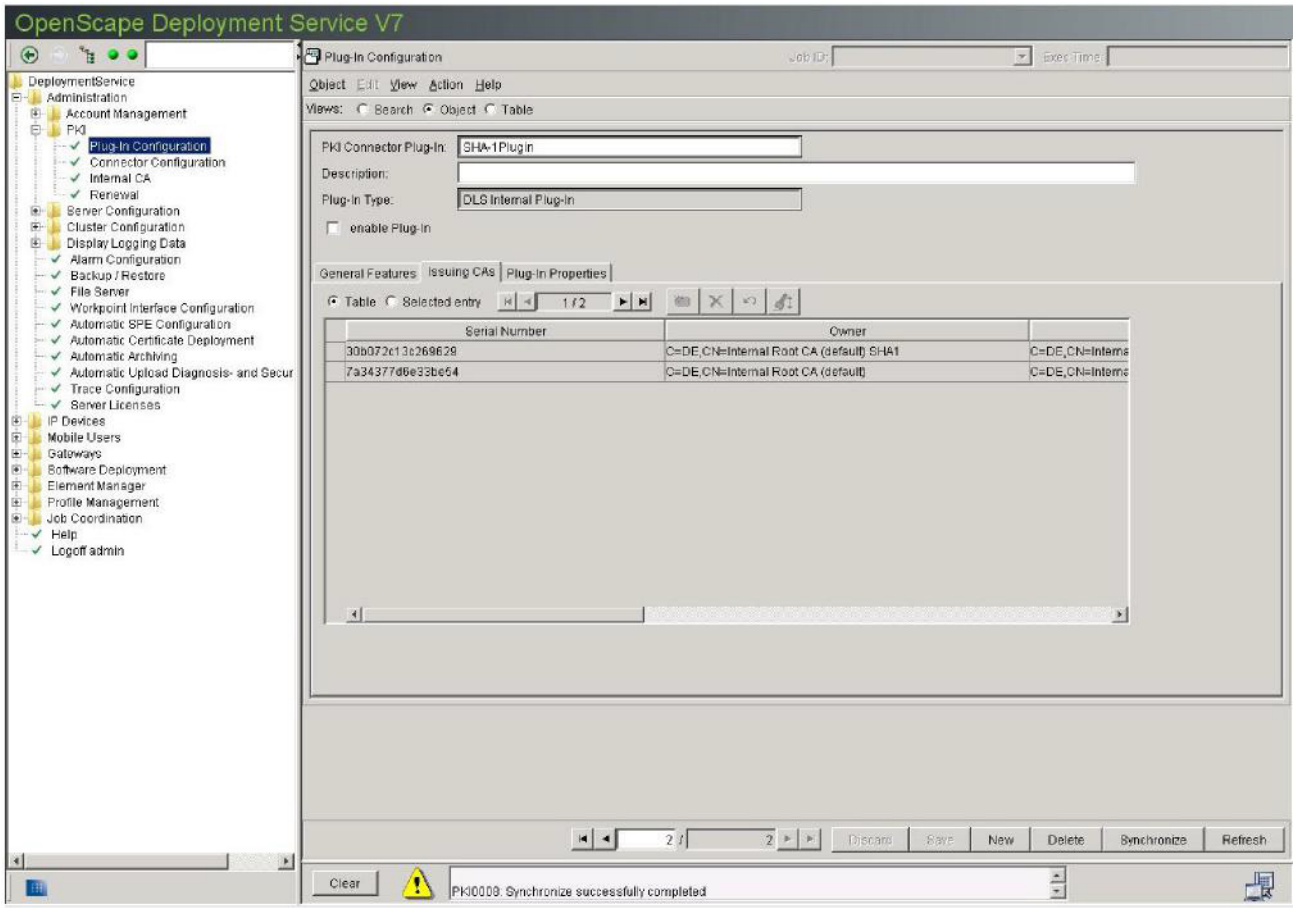


In case your equipment does not support SHA-256 yet, you can create a SHA-1 plugin that will use the SHA-1 CA to sign the certificates.

- Enable SHA-1 CA under Internal CA.
- Under Plug-In Configurationmenu select **New**, give the name (e.g. SHA-1Plugin), '`DLS Internal Plug-In`' as Plug-in Type and press **Save**.
- Under Plug-In Configuration> "Plug-In Properties" Tab set '`SHA1WithRSAEncryption`' as internal.signature.algorithm
- Press the **Synchronize** button. Two root CA certificates shall appear under Issuing CAs. The second shall be the root CA certificate of 'Internal Root CA (default) SHA1' that signs with the less secure SHA-1.
- Enable plugin from it's checkbox


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: SHA-1Plugin
Description:
Plug-In Type: DLS Internal Plug-In
enable Plug-In
General Features
Issuing CAs
Plug-In Properties
Table Selected entry
1 / 4
Property Name
Value
internal.default.validity.days
365
internal.signature.algorithm
SHA1WithRSAEncryption
internal.x509name.template
C=DE, CN=?
internal.random.algorithm
SHA1PRNG
2 / 2
Discard
Save
New
Delete
Synchronize
Refresh
Clear
PKI0008: Synchronize successfully completed


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 Object Table
Configuration Name: SHA-1 Connector
Description:
Plug-In Configuration SHA-1Plugin
Issuing CA Name: C=DE,CN=Internal Root CA (default) SHA1
enable Connector
Request Parameter
Certificate Renewal
Trust Anchor
User Certificates
Common Name: DNS Name
Subject Alternative Name: None
Key Algorithm: RSA
Key Size: 2048
Validity Offset (days):
Validity Period (days):
Test
Discard
Save
New
Delete
Import Certificate
Refresh



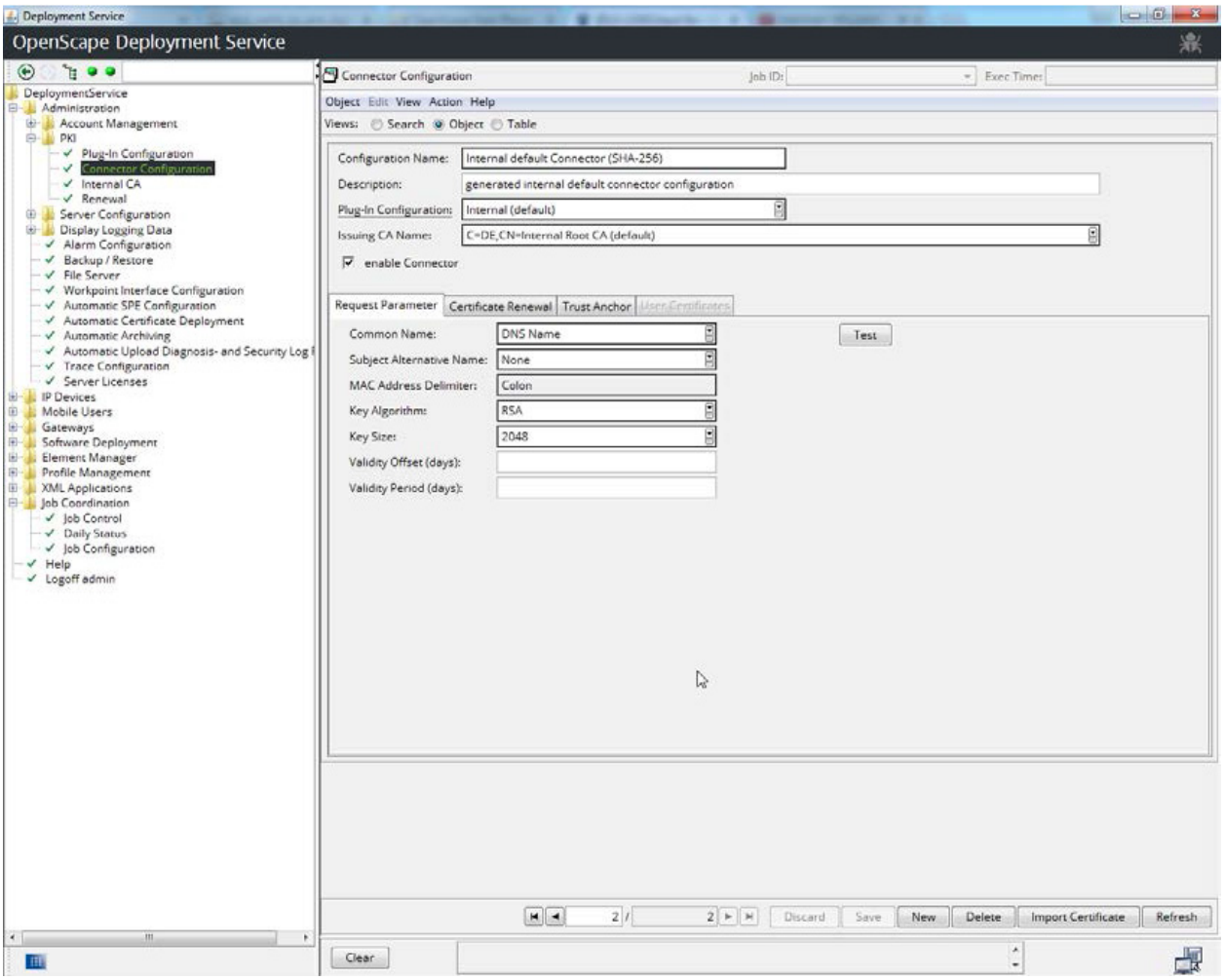
2. Create new Connector Configuration

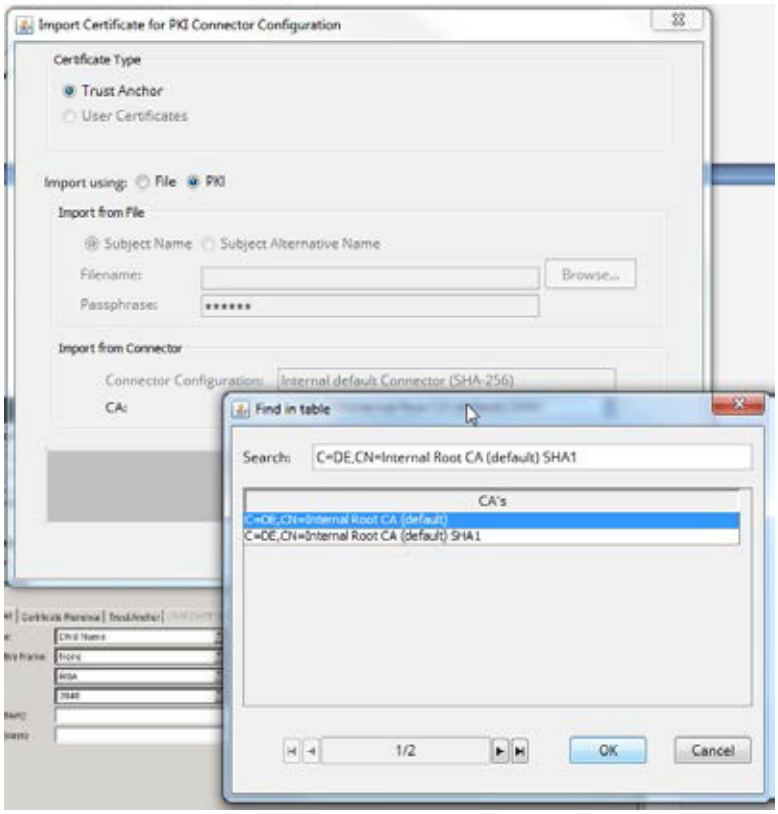
   Under Administration > PKI > Connector Configuration,create a new connector

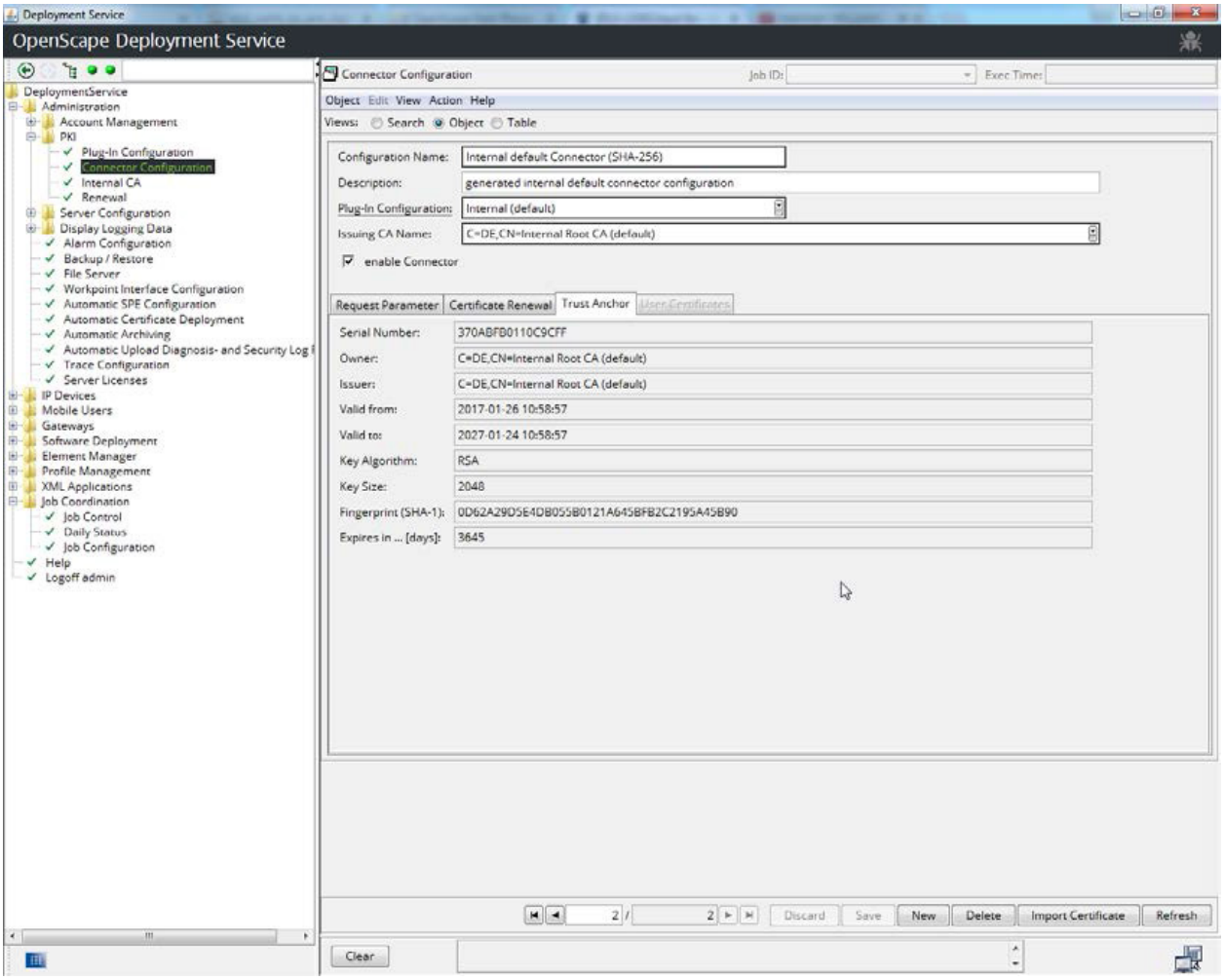
   If your equipment supports SHA-2 (recommended as more secure) then link this connector to the Internal default (SHA-256) plugin.

   Under the **Trust Anchor** tab, import the corresponding CA certificate (the one signed by SHA-256 in this case).

   Then enable connector by its checkbox.

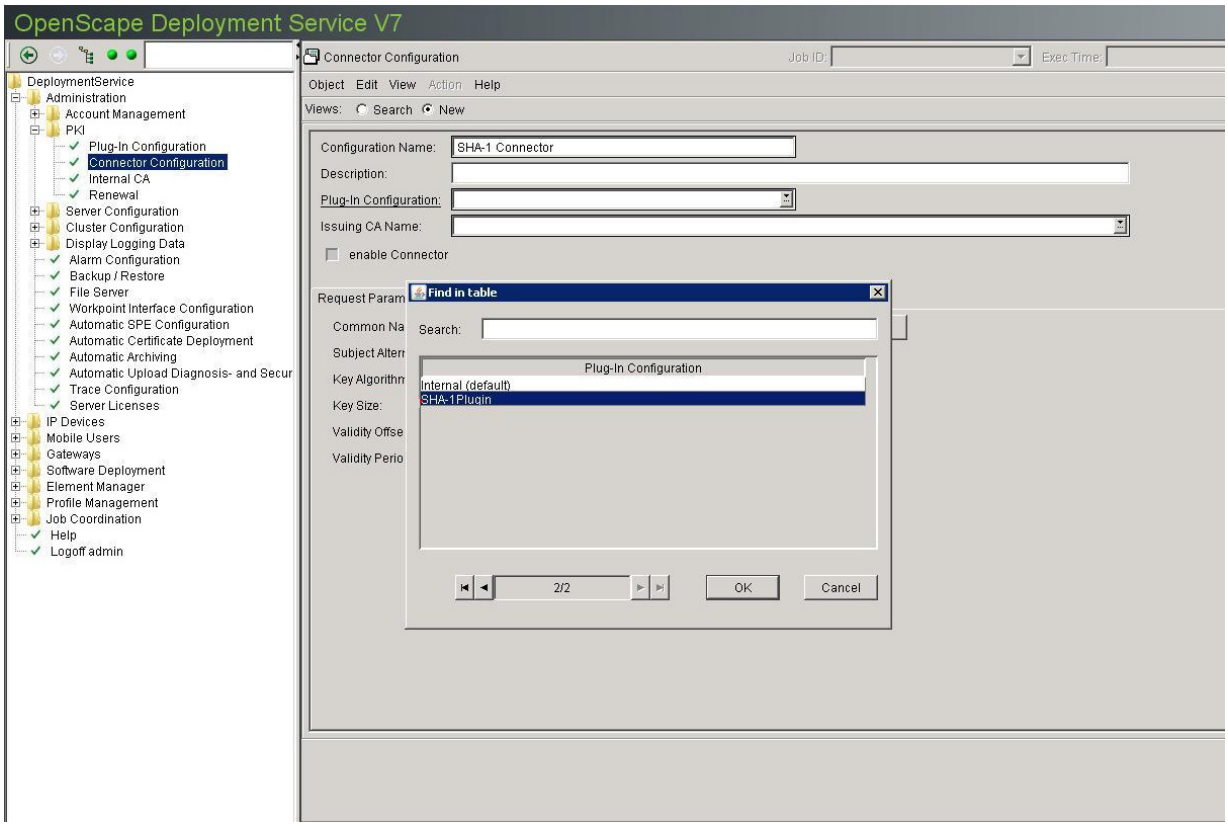

Deployment Service
OpenScape Deployment Service
DeploymentService
Administration
Account Management
PKI
Plug-In Configuration
Connector Configuration
Internal CA
Renewal
Server Configuration
Display Logging Data
Alarm Configuration
Backup / Restore
File Server
Workpoint Interface Configuration
Automatic SPE Configuration
Automatic Certificate Deployment
Automatic Archiving
Automatic Upload Diagnosis- and Security Log
Trace Configuration
Server Licenses
IP Devices
Mobile Users
Gateways
Software Deployment
Element Manager
Profile Management
XML Applications
Job Coordination
Job Control
Daily Status
Job Configuration
Help
Logoff admin
Connector Configuration
Job ID:
Exec Time:
Object Edit View Action Help
Views: Search Object Table
Configuration Name: Internal default Connector (SHA-256)
Description: generated internal default connector configuration
Plug-In Configuration: Internal (default)
Issuing CA Name: C=DE,CN=Internal Root CA (default)
enable Connector
Request Parameter
Certificate Renewal
Trust Anchor
User Certificates
Common Name: DNS Name
Test
Subject Alternative Name: None
MAC Address Delimiter: Colon
Key Algorithm: RSA
Key Size: 2048
Validity Offset (days):
Validity Period (days):
2 / 2
Discard
Save
New
Delete
Import Certificate
Refresh
Clear

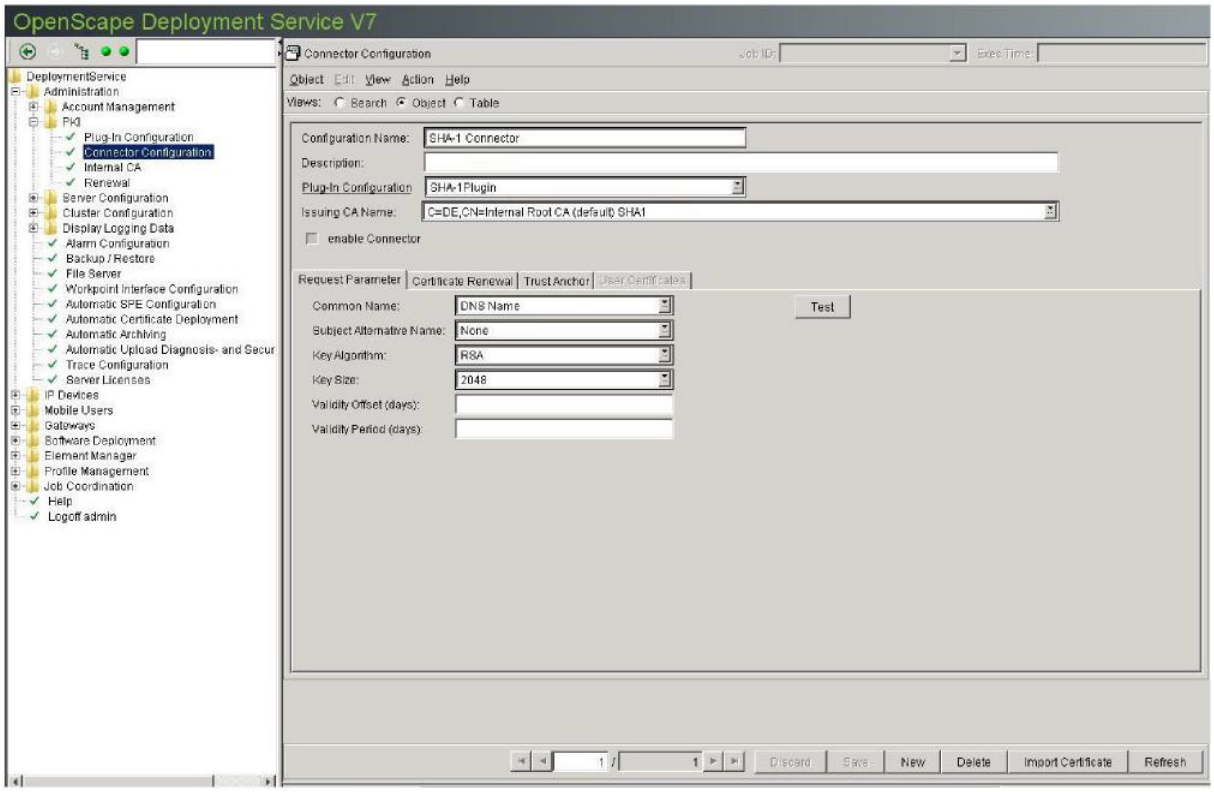

Import Certificate for PKI Connector Configuration
Certificate Type
Trust Anchor
User Certificates
Import using:
File
PKI
Import from File
Subject Name
Subject Alternative Name
Filename:
Browse...
Passphrase:
Import from Connector
Connector Configuration:
Internal default Connector (SHA-256)
CA:
Find in table
Search:
C=DE,CN=Internal Root CA (default) SHA1
CA's
C=DE,CN=Internal Root CA (default)
C=DE,CN=Internal Root CA (default) SHA1
1/2
OK
Cancel



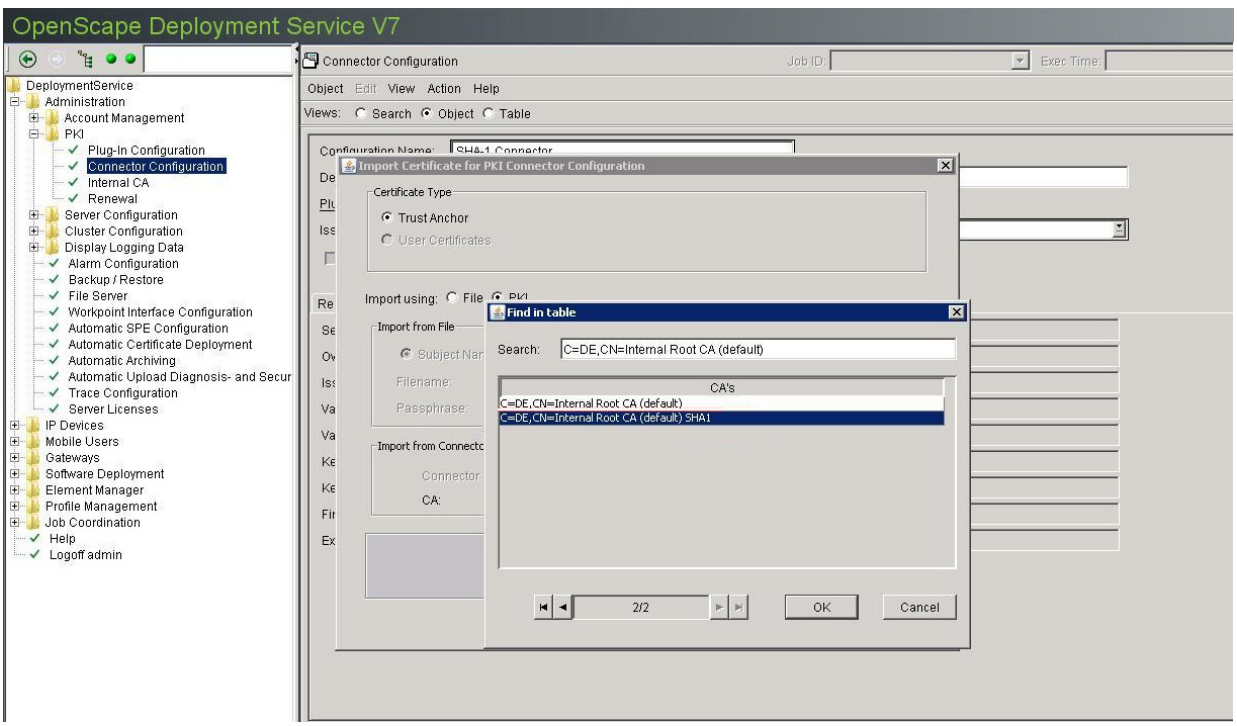
IMPORTANT: It is crucial to select the correct Issuing CA both as a Trust Anchor and as the connector's configuration Issuing CA which MUST be the SHA1 / SHA 2 certificate.

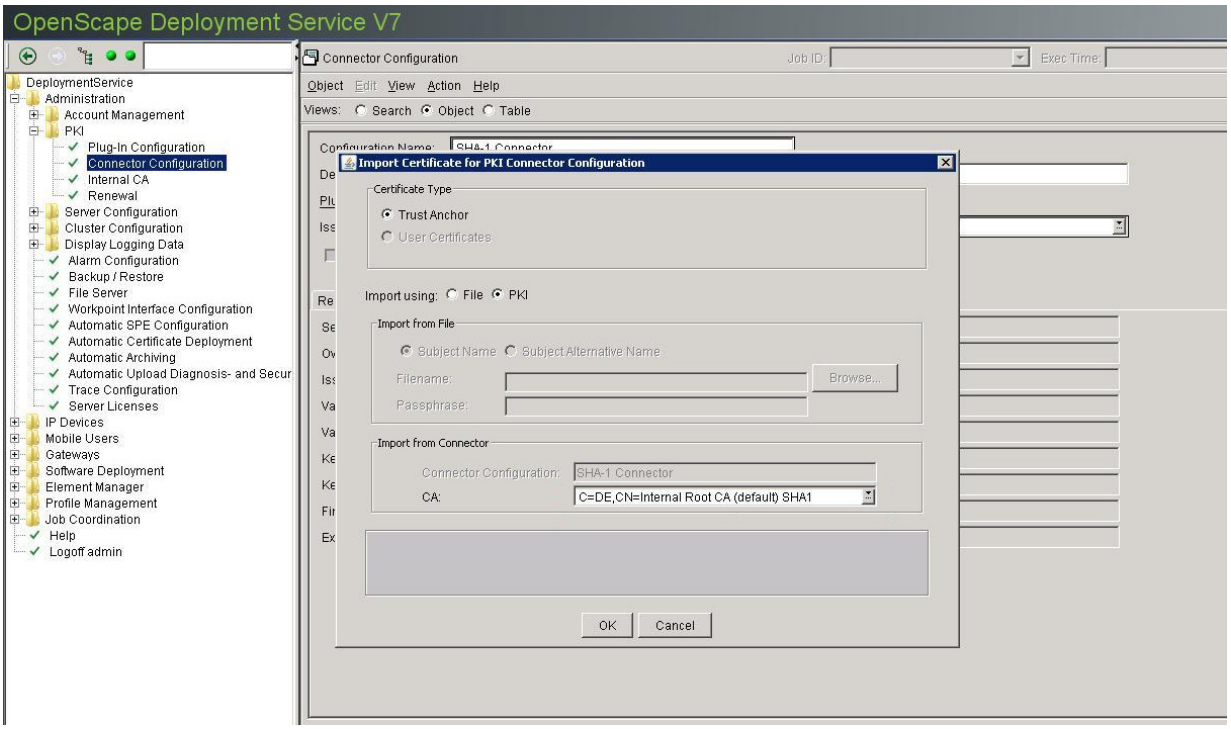
In case your equipment does not support SHA-2 signing algorithms then proceed as following to create a connector based to the SHA-1 plugin created previously.

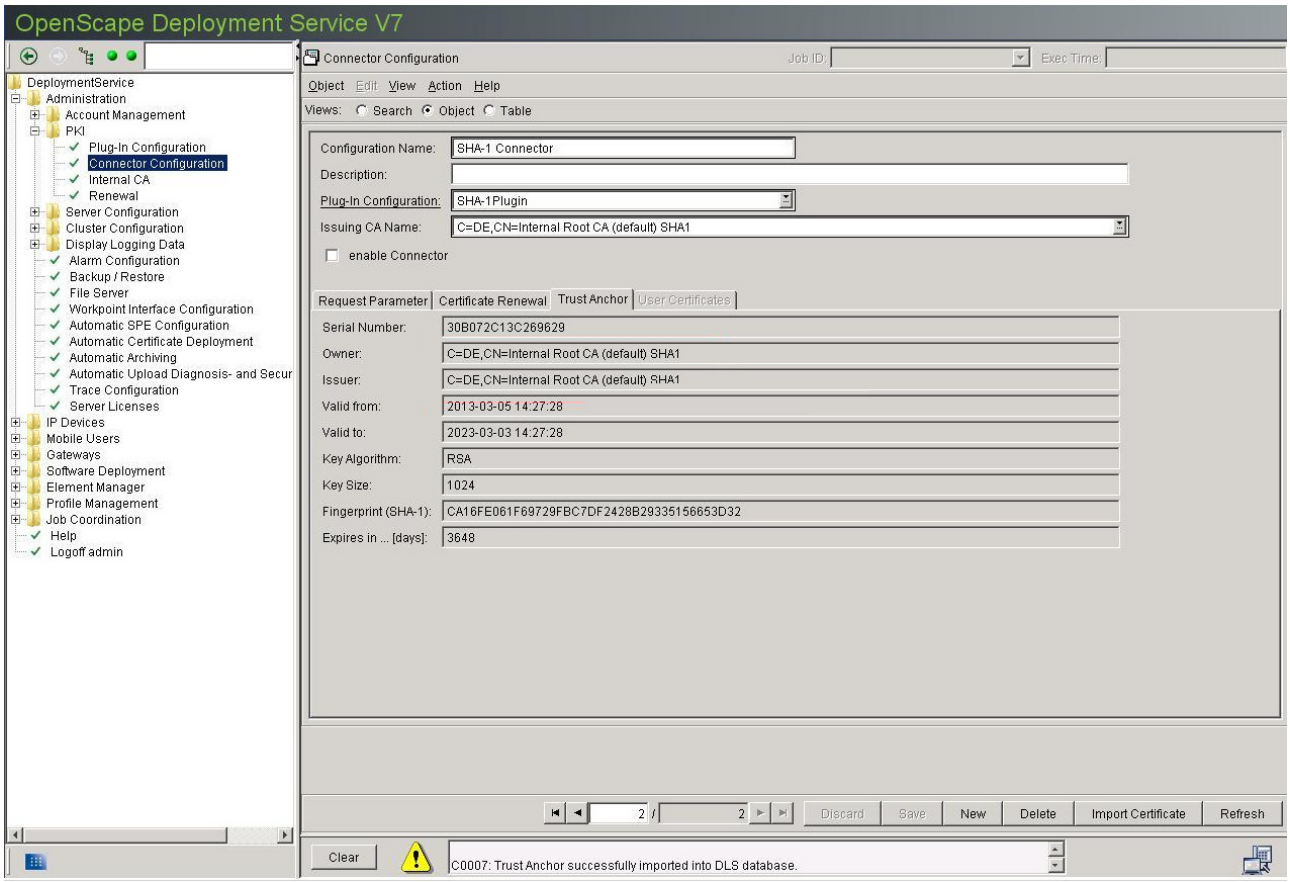

OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Configuration
Connector Configuration
Internal CA
Renewal
Server Configuration
Cluster Configuration
Display Logging Data
Alarm Configuration
Backup / Restore
File Server
Workpoint Interface Configuration
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

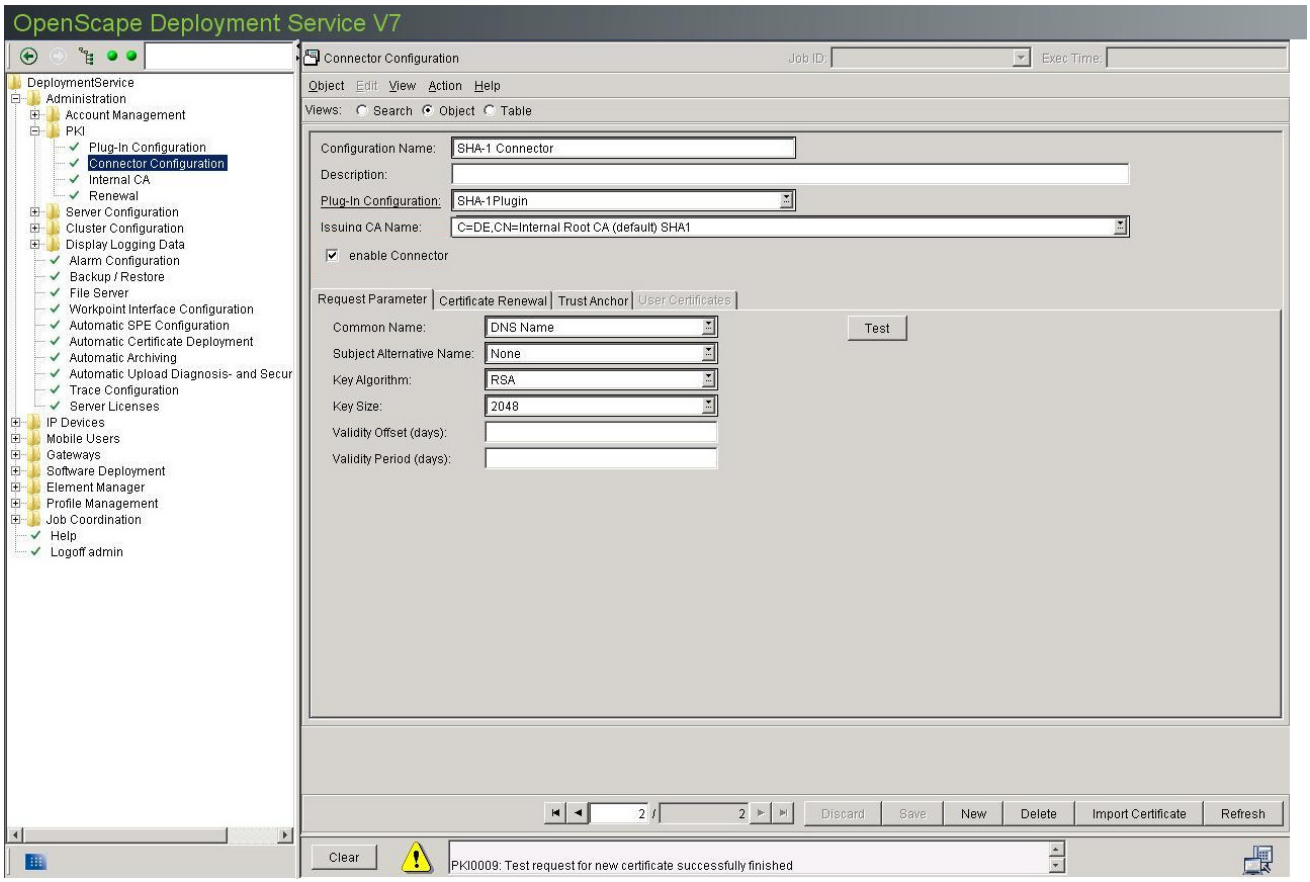


3. Import the Trust Anchor for this configuration




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 Object Table
Import Certificate for PKI Connector Configuration
Certificate Type
Trust Anchor
User Certificates
Import using: File PKI
Import from File
Subject Name Subject Alternative Name
Filename:
Browse...
Passphrase:
Import from Connector
Connector Configuration: SHA-1 Connector
CA: C=DE,CN=Internal Root CA (default) SHA1
OK
Cancel

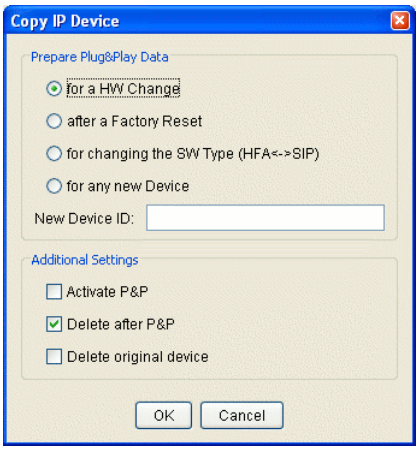

OpenScape Deployment Service V7
DeploymentService
Administration
Account Management
PKI
Plug-In Configuration
Connector Configuration
Internal CA
Renewal
Server Configuration
Cluster Configuration
Display Logging Data
Alarm Configuration
Backup / Restore
File Server
Workpoint Interface Configuration
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 Object Table
Configuration Name: SHA-1 Connector
Description:
Plug-In Configuration: SHA-1Plugin
Issuing CA Name: C=DE,CN=Internal Root CA (default) SHA1
enable Connector
Request Parameter
Certificate Renewal
Trust Anchor
User Certificates
Serial Number: 30B072C13C269629
Owner: C=DE,CN=Internal Root CA (default) SHA1
Issuer: C=DE,CN=Internal Root CA (default) SHA1
Valid from: 2013-03-05 14:27:28
Valid to: 2023-03-03 14:27:28
Key Algorithm: RSA
Key Size: 1024
Fingerprint (SHA-1): CA16FE061F69729FBC7DF2428B29335156653D32
Expires in ... [days]: 3648
2 / 2
Discard
Save
New
Delete
Import Certificate
Refresh
Clear
C0007: Trust Anchor successfully imported into DLS database.



The procedure is complete. The connector can now be used for AutoSPE

16.6 Replacing an IP Device

1. Click the **IP Device Management** > **IP Device Configuration** area. Click **Action** in the menu bar and select **Copy IP Device**.
2. The following dialog window opens:



Select **for a HW Change** under **Prepare Plug&Play Data**.

If you wish to leave configuration data as it is, select **Activate P&P**. The data record is then released for transfer to the workpoint.

3. Disconnect the defective workpoint and connect the replacement workpoint.
4. If full Plug&Play is supported for the workpoint, the replacement workpoint is automatically registered and configured (as in the case of reinstallation, Section 16.2 or Section 16.3).

   If Plug&Play is not supported, workpoint registration must be performed manually in the DLS. Registration depends on the presence of a DHCP server:

   - If a **DHCP server is not present**:

     The following data must be configured on the workpoint in the *Configuration* menu:

     1. DHCP must be set to *off*.
     2. The IP address of the workpoint must be entered.
     3. The network mask of the workpoint subnet must be entered.
     4. The IP address of the default router must be entered.
     5. The *Fully qualified Subscriber Number* must be entered.

     After saving changes and restarting the IP phone, DLS can be used to perform a scan to register the IP phone in the DLS (see Section 7.5.6, "Scan IP Devices"). The DLS address must also be sent when performing scanning.

   - If a **DHCP server is present**:

If the DHCP does not send DLS address data to the workpoint, start the workpoint scan. In the scanning dialog box, activate **Register IP Devices** and **New IP Devices from Scan Results** (see Section 7.5.6, "Scan IP Devices") to register the new workpoint in the DLS.

If the DLS address data is sent automatically from the DHCP to the workpoint, registration in the DLS is automatic.

For information on configuring a DHCP server to transfer DLS access data to the workpoints, refer to the **Unify Experts Wiki portal** under http://wiki.unify.com/wiki/Configuring_the_DHCP_Server_for_DLS

NOTE: You should not delete the old workpoint data from the DLS database until after the new workpoint is functioning.

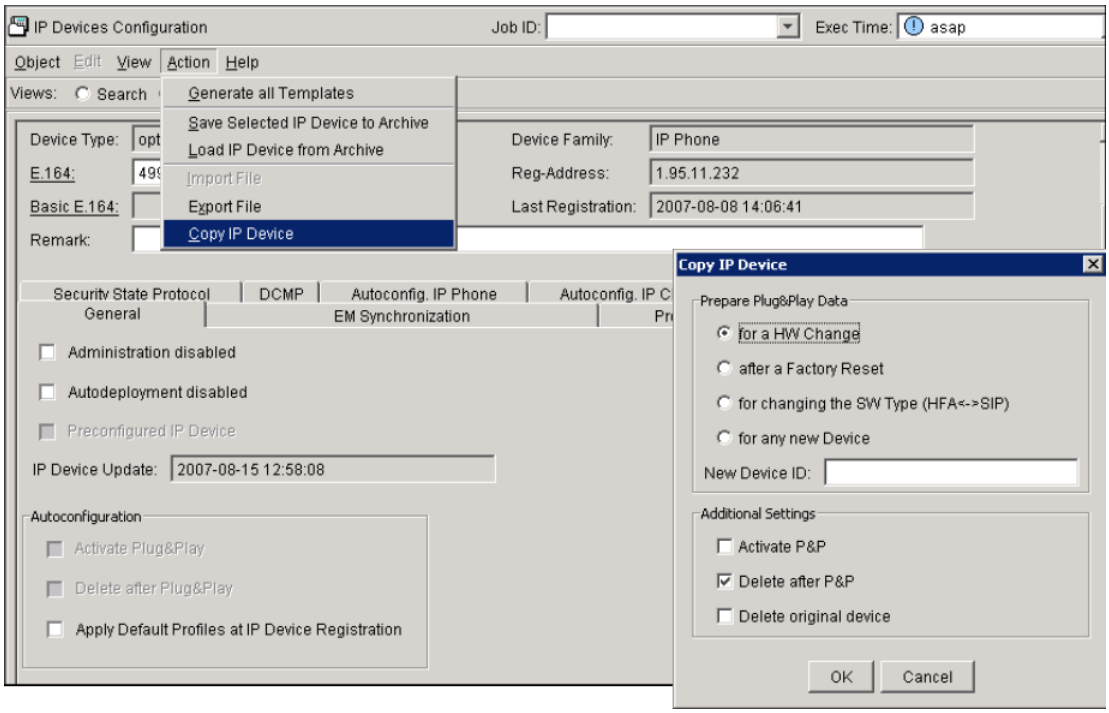
This completes the replacement.

5. Alternatively, you may select **for any new Device** under **Prepare Plug&Play Data**, only now, **Activate P&P** and **Delete original Device** checkboxes are not editable (and disabled by default).

   Once the virtual device is created by selecting f**or any new Device**, you can edit **Activate P&P** via **General** tab under **IP Device Configuration**.By selecting **for any new Device**, the only difference is that the original device is not deleted after **Plug&Play** by the DLS.

16.7 Copy a Registered Device to a Virtual Device

Auto configuration is based on Virtual Devices. If no Virtual Device exists for a Registered Device because it has been deleted (default), you can copy the data back from the Registered Device into a Virtual Device.



Prepare the Plug&Play data under **IP Device Configuration** via **Copy IP Device**.

- **for a HW Change**: transfers all data of the device, including the device type of specific parameters.

  If no new MAC address is entered, the DLS deploys a virtual MAC.

- **after a Factory Reset**: incorporates all data of the device, including MAC address.The virtual device receives an @ before the MAC address.The registered device entry is retained because the option to start a factory reset of the device via the DLS only exists for a registered device.If the device registers, the @ character in the MAC address field is ignored an the device is assigned.

- **for changing the SW type (HFA<->SIP)**: incorporates the data of the device and switches the entry masks to the other device type.Further required parameters musty be manually assigned.

- **for any new Device**: incorporates the current data of the registered device.If no new MAC address is entered, the DLS deploys a virtual MAC.

- **Activate P&P**: immediately activates the virtual device for the autoconfiguration.This option is only available for a hardware change or after a factory reset.

- **Delete after P&P**: deletes the virtual device after the autoconfiguration.

- **Delete original device**: is only available for hardware replacement and deletes the original device after the copy has been created as a virtual device.

16.8 Replacing an Old Workpoint (TDM) with a New One (IP)

Requirements

- A working DLS infrastructure (such as CLA, DHCP, DNS and FTP servers).

Performing the replacement

1. Reconfigure the stations in the system by deleting them and then recreating them, for example, with the help of the HiPath 4000 Manager or AMOs. For more information refer to the relevant documentation.
2. For the remaining procedure, follow the instructions for the reinstallation of a workpoint (see Section 16.2, "Workpoint Reinstallation with HiPath 4000").

This completes replacement.

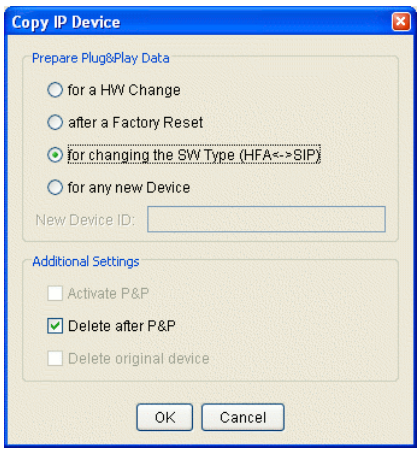
16.9 Replacing HFA with SIP Software and Vice Versa with Identical Device IDs

Requirements

- A working DLS infrastructure (such as CLA, DHCP, DNS and FTP servers).

16.9.1 Replacing HFA with SIP Software

1. Prepare the SIP software in the DLS (see Section 15.6, "Registering Workpoint Software and Files").
2. Click **Action** in the menu bar and select **Copy IP Device**.
3. The following dialog window opens:



   Select **changing the SW Type (HFA<->SIP)** under **Prepare Plug&Play Data**.

   If you wish to leave the configuration data unchanged, select **Activate P&P**. The data record is then released for transfer to the workpoint.

4. Define the required registration data. This configuration is dependant on the SIP server used. In the case of OpenScape Voice, this is for a minimum configuration:

   Call: Main Menu > Call: Main Menu > > IP Phone Configuration > **Gateway/Server**

   – **"Gateway (HFA) / SIP Server" Tab**:
   Reg-Addr., **Reg-Port**.

   – **"SIP Registering 1" Tab**:
   SIP Routing, SIP Registrar Addr., **SIP Registrar Port**, **SIP Phone Port**, **RTP Base Port**.

   We recommend managing configuration data using templates. For more information, see Section 15.7.1, "Creating a Template Manually".

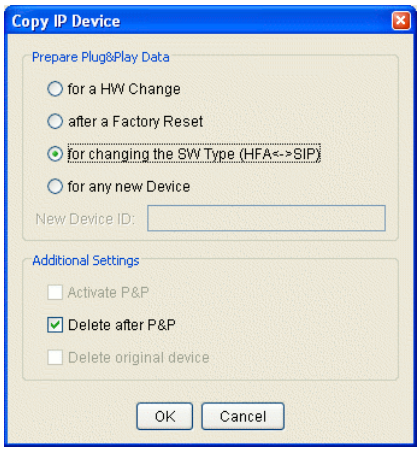
   If necessary, you can also transfer registration data via synchronization with the system. For more information, see Section 11.1, "Element Manager Configuration".

5. Start software deployment (see Section 15.9.1, "Manual Deployment").

The workpoint is restarted once the software is loaded to the phone. This completes the software replacement operation.

16.9.2 Replacing SIP with HFA Software

1. Prepare the HFA software in the DLS (see Section 15.6, "Registering Workpoint Software and Files").
2. Click **Action** In the menu bar and select **Copy IP Device**.
3. The following dialog window opens:



Select **changing the SW Type (HFA<->SIP)** under **Prepare Plug&Play Data**.

If you wish to leave the configuration data unchanged, select **Activate P&P**. The data record is then released for transfer to the workpoint.

4. Define the access data for the gateway.

   You can also use templates to manage configuration data. For more information, see Section 15.7.1, "Creating a Template Manually".

   If necessary, you can also transfer access data via synchronization with the system. For more information, see Section 11.1, "Element Manager Configuration".

5. Start software deployment (see Section 15.9.1, "Manual Deployment").

   The workpoint is restarted once the software is loaded to the phone. This completes the software replacement operation.

16.10 Configuring an IP Client in DLS

16.10.1 Configuring an IP Client 130 in the DLS

The following describes how to configure an optiClient 130 V5.0 as a HFA client in a HiPath 4000 environment.

Requirements

- A live DLS infrastructure (including existing connection to the HiPath 4000).

Procedure

1. Creating Templates
2. Settings at the optiClient 130

The following describes how to configure an optiClient 130 V5.0 as a HFA client in a HiPath 4000 environment.

16.10.1.1 Creating Templates

Template: Gateway/Server

The data for system type (including standby), program update, telephone type, and licensing are entered in this template.

1. Click the **Call: Main Menu > Call: Main Menu >** > **IP Client Configuration** > **Gateway/Server** > **"Gateway" Tab** area.
2. In the view bar (see Section 5.4.2.3, "View Bar"), select **Template**.
3. Select **HiPath 4000** in the **System Type** list.
4. Switch to the **"Gateway (Standby)" Tab.**
5. Select **No standby system** in the **System Type** list.
6. Switch to the **"SW Deployment" Tab**.
7. Select the **DLS Deployment** check box and enter the **Directory** and the **SW Update Mode**.

   The meaning of the entries in **SW Update Mode** are as follows:

   – **Start**: the system checks for a new version when starting optiClient 130.

   – **Interval**: the system checks for a new version every X minutes based on the value set under **Update Mechanism Interval.**
8. Switch to the **"HFA Settings" Tab**.
9. Select the telephone (including add-on devices) used to represent the optiClient 130 from the **Device Phonetype** list. For example: **Device Phonetype:** optiPoint 420 standard, **Device Modules Type:** optiPoint 420 Key Module and **Device Modules Count:** 2.

10. Switch to the **"Licenses" Tab**.
11. Enter the IP address and the port number of the license server under **Server** and **Port** in the **HFA License** tab.
12. Click **Save** and define the name for the template, for example, **oC130 Gateway/DLS HP4000**.
13. Click the **Call: Main Menu > Call: Main Menu >** > **IP Client Configuration** > **Dialing Properties** > **"HFA Dialing Properties" Tab** area.
14. Select **Template** in the view bar and set the template name.
15. Enter the necessary data here for the main network access, for example, **49** for the local country code.
16. Click **Save** and define the name for the template, for example, **oC130 dialing properties HP4000**.
17. Create more templates as needed, for example, if an LDAP server is available, the relevant data is in the **LDAP** section.

16.10.1.2 Creating a Profile from the Template

1. Click the > **Device Profile** area.
2. Click **New** in the view bar to create a new profile.
3. Enter a suitable name for your profile, such as, **oC 130 device** in the **Name** field and enter a brief description in the **Description** field.
4. If you wish the profile to be the default profile for a particular **Location** (see Section 6.3.2, "Location"), activate **Default Profile**.

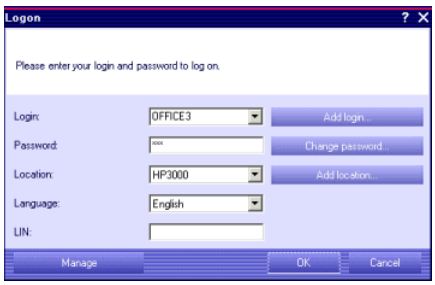
Group the templates that you wish to use to form the profile under > **Device Profile** > **"Templates" Tab**. To do this, click  for each template you wish to add and then select a template from the choice list.

5. Enter the correct **Device Type**, **SW Type**, and **SW Version** under > **Device Profile** > **"Templates" Tab**.
6. Click Save to save the profile.

16.10.1.3 Settings at the optiClient 130

Certain additional data must be entered at the optiClient 130 so that the optiClient 130 can operate with the DLS.

Login (same as for the optiClient 130 extension), Password, and Location:



Under **Settings...** the data for the DLS server:



NOTE: For more information on configuring the optiClient 130, refer to the online help or the optiClient 130 Administration Manual.

16.10.1.4 OptiClient in Call Centers

n call centers, it is necessary that optiClient users are enabled to work with their own call number. With every first login at a specific PC, P&P is executed. For this purpose, the Activate Plug&Play flag must be set.

1. Configure the optiClient for the first time, using the E.164 relevant to the user (e. g. 497224711), and the corresponding profile.

   Please ensure that the DLS address is defined in the optiClient, and that the data is stored in the home drive within the network.

2. Now create a corresponding participant, that is, a virtual device, in the DLS. For this purpose, select **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** und click on the action button **New**.

3. Enter the E.164 number.

4. Enter the E.164 number once again, as **Device ID**, and end with a '.' (dot; e. g. '497224711.').

5. Click on **Save**.

16.10.2 Configuring an ODC Client in DLS

Plug & Play (P&P) is a part of the feature Easy Client installation. This feature permits that ODC is installed and configured without any user intervention. With P&P ODC will search by his database in DLS on first initialization.

In order to configure this feature, refer to the following steps:

1. Make sure that the subscriber does not exist in DLS. Go to Main Menu > Call: Main Menu > Call: Main Menu > > IP Device Management > IP Device Configuration. Make a search and verify if the subscriber exists. If so, delete it.
2. In order to create the new subscriber, change the visualization to **search** (to be sure that this subscriber will not inherit anything from an existing subscriber). Create the new subscriber in button **New**. Fill the E164 parameter with E164 number of this subscriber (the same number of subscriber in OSV). Mark the fields **Active Plug&Play** and **Delete after Plug&Play**.
3. Now this device can be configured as any other in DLS. Set the mandatory parameters in **Gateway**, under Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Gateway/Server

   Mandatory:

   – SIP Registrar TAB
   – Registrar Address
   – User ID (if digest enabled)
   – Password (if digest enabled)
   – Realm (if digest enabled)
   – License TAB
   – Server under OpenScape Client License / Opticlient 130 HFA License (yes, it is a bug)
4. If the protocol in OSV is not UDP, it must to be changed under Main Menu > Call: Main Menu > Call: Main Menu > > IP Client Configuration > Signaling and Payload Encryption (SPE)
5. This step is necessary only to P&P works with the name resolution. If P&P will work with E164, it is not necessary and you can refer to the next step. Configure the association between domain \ account and E164 number used in step 2. Go to Administration > Server Configuration > P&P Settings > "IP Client Mapping Configuration" Tab.
6. On the DLS side, the job is finished. Now, let's configure the ODC. Make sure that there is no database to this ODC. Erase the entire folder OpenScape, under `%appdata%\Siemens`. (or `%appdata\Roaming\Siemens` in Win7)
7. Set the ODC to search the Database in DLS via registry (if you are installing the ODC, you can set this step via installer)

   Set the keys:

   - DLSServer (IP address of DLS)
   - UseDLS (1 to use DLS)

- DLSE164Mode (1 to P&P works with E164 number, otherwise, P&P will works with domains\windows account)

8. Start the ODC and fill the requested parameters. Profile name is anyone you want. Call Number is the number that you set in step 2. If in the step 7 you left the DLSE164Mode empty, ODC will not ask by Call Number.
9. Load the ODC. If all configurations are OK, ODC will search by database in DLS and will load with this information.

16.11 Changing the IP Address and/or Port Number of the DLS

If you need to change the address data (IP address and port number) of the DLS while it is running, for example, because you want to move it to an alternative computer, you must perform all changes in a specific sequence.

The current DLS installation is called "old" and the DLS with the modified data is called "new" in the following.

1. First put the new DLS into operation. Do this by installing all necessary components and starting the new DLS.

   The new DLS is now already running with a new IP address and port number, but the workpoints are not yet using it.

2. You must change the DLS IP address data in the workpoints so that the workpoints can contact the new DLS. How you change this data depends on how the workpoints are supplied with the DLS IP address and port number.

   - With DHCP (full Plug&Play):

     Change the data in the DHCP server's "vendor class" (refer to the **Unify Experts Wiki portal** under http://wiki.unify.com/wiki/Configuring_the_DHCP_Server_for_DLS).

   - Without DHCP (limited Plug&Play):

     a) In the DLS, select the **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"DLS Connectivity" Tab** area with all available workpoints (see also Section 15.3, "First Steps: Changing IP Device Parameters").

     b) Enter the IP address data of the new DLS under **DLS Server Address** and **DLS Port** and apply it to all workpoints (see Section 5.4.2.4, "Multiple selection and data transfer in Table view").

     c) Send the DLS IP address data to the workpoints by clicking **Save**.

3. Restart all relevant workpoints (**Call: Main Menu > Call: Main Menu >** > **IP Device Interaction** > **Reset IP Devices**).

   NOTE: Note that the workpoints will communicate only with the new DLS after a restart. This means that there is no message indicating whether this action was successfully executed for the old DLS.

   The workpoints register with the new DLS.

4. Deactivate the old DLS (to uninstall the DLS, see Section 4.13, "Uninstalling the Deployment Service").

16.12 Using an EWS with DLS in a Customer Network Without Permanent DLS

Requirements

- DLS CV45 and higher.
- An FTP server installed on the TAP. For information on installation, see Section 4.12.1, "FTP Server".
- The workpoint software to be deployed must be located on the EWS and registered in the DLS (see Section 6.3.4, "FTP Server Configuration", Section 6.3.5, "HTTPS Server Configuration" or Section 6.3.7, "Network Drive Configuration").
- The EWS must be connected to the customer LAN and assigned a free IP address from the customer LAN. The IP address can be modified using the IP changer.

Restriction

DHCP can be activated or deactivated at the workpoint (*DHCP=ON* or *DHCP=OFF*). However, no DLS info may be sent from the DHCP to the workpoint. "Vendor Class" must not be configured in the DHCP as described under http://wiki.unify.com/wiki/Configuring_the_DHCP_Server_for_DLS

If the workpoint has already received the DLS info from the DHCP, this value can only be reset with a *Factory Reset*.

16.12.1 Installation and Initial Configuration of DLS on the EWS

1. Install Java 2 Runtime Environment 1.6.0_13
2. Install the current version of DLS.
3. Perform initial configuration on the DLS (see Section 4.10, "Initial Configuration"). You must configure the data for the FTP server(s) here.
4. The IP address range containing the workpoint must be configured before the workpoint can be transferred from the customer network to the DLS (**Call: Main Menu > Call: Main Menu >** > **IP Device Interaction**> **Scan IP Devices** > **"IP Ranges" Tab**).

   In addition, the current IP address of the EWS must be entered as the **DLS Address** (the current IP address is displayed, for example, by entering *ipconfig/all* in the DOS shell). The **Send DLS Address** option must be activated (**Call: Main Menu > Call: Main Menu >** > **IP Device Interaction**> **Scan IP Devices** > **"Configuration" Tab**). This IP address range is then scanned with **Scan Workpoints**.

16.12.2 Manipulating the DLS Database for Using the TAP at Different Customer Facilities

The database used by the DLS must be modified to facilitate working with multiple databases on the TAP.

16.12.2.1 Configuring a Database at a new Customer Facility

1. If the DLS database already contains data, save it on the EWS. See Section 15.11.1, "Automatic Data Backups".
2. Create a new database on the EWS. See Section 15.11.2.4, "Resetting the DLS Database".

16.12.2.2 Database Change Between Customers A and B

1. Save the currently active database associated with **customer A** on the EWS. See Section 15.11.1, "Automatic Data Backups".
2. Restore the saved DLS database associated with **customer B**. See Section 15.11.1, "Automatic Data Backups".

16.13 Operating the DLS via the Program Interface (DlsAPI)

In addition to standard GUI-based operation, the DLS can also be operated by external applications over a web service interface. An account with authorization to access the Dls API must first be configured for this (see Section 6.1, "Account Management").

DLS V2 provides both DlsAPI v100 (as released with DLS V1) and new methods as part of DlsAPI v200. While DlsAPI v100 methods support IP Phones only, DlsAPI v200 methods also support IP Clients and IP Gateways.

16.13.1 DLS API Web Service Interface

The DLS API is included in the DLS installation and is stored in the following directory:

```
<DLS installation directory>\Programs\DeploymentService\api
```

The following data is included:

1. `dlsapiv100.wsdl`
   Describes the DlsAPI v100 in WSDL (Web Services Description Language).
2. `dlsapiv100.jar`
   Generated by WSDL2JAVA. This JAR file contains Client Stubs and the Service Locator and may be used by JAVA clients as an interface to the DlsAPI v100.
3. `dlsapiv200.wsdl`
   Describes the DlsAPI v200 in WSDL (Web Services Description Language).
4. `dlsapiv200.jar`
   Generated by WSDL2JAVA. This JAR file contains Client Stubs and the Service Locator and may be used by JAVA clients as an interface to the DlsAPI v200.
5. `doc`
   This subdirectory contains a description of the DLS API interface in Javadoc format.

The WSDL descriptions are stored on the DLS server at the following URLs:

```
https://<DLS server>:10444/DeploymentService/services/
DlsAPIv100?wsdl
```

```
https://<DLS-Server>:10444/DeploymentService/services/
DlsAPIv200?wsdl
```

Online documentation for the DLS API is stored at the following URL:

```
https://<DLS server>:10443/DeploymentService/dlsapidoc
```

NOTE: If the DLS HTTP port is not deactivated, it can be used as an alternative to the HTTPS port.
In this case, the URLs will change:
`https://<DLS server>:10443/DeploymentService/...`

A PHP test script is available for the DLS API. Among other things, this enables you to monitor SOAP communication, query particular IP phones in the DLS database, and modify configuration parameters for a selected IP phone. For more information, please refer to the DLS Release Notes.

16.14 Security: Administering Certificates

Certificates are used for secure authentication between the server and clients. A certificate is comparable to a digital ID card issued by an authorized body - the Certification Authority (CA).

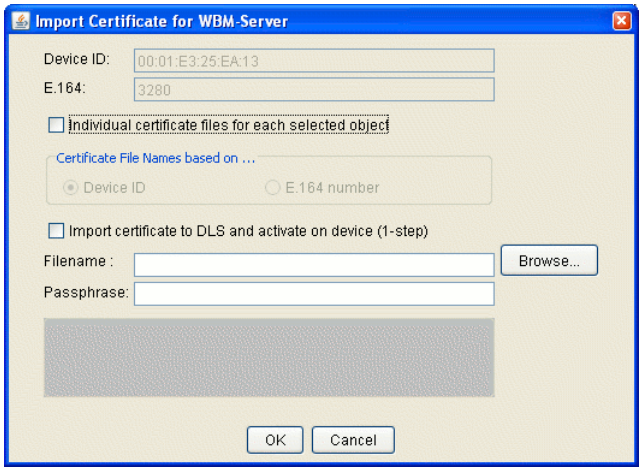
You can administer certificates in the DLS for the following server/client configurations:

- **Server**: WBM server in the IP phone
  Client: Web browser for administering IP phones (see Section 16.14.1, "Importing WBM Server Certificates")
  For an interface description, see Section 7.1.7.4, ""WBM Server Certificate" Tab".
- **Server**: RADIUS server
  Client: IP phone (see Section 16.14.2, "Importing Phone and RADIUS Certificates")
  For an interface description, see Section 7.1.23.2, ""Phone Certificate" Tab".
- **Server**: RADIUS server
  Client: IP phone (see Section 16.14.2, "Importing Phone and RADIUS Certificates")
  For an interface description, see Section 7.1.23.3, ""RADIUS Server CA Certificate 1" Tab" and Section 7.1.23.4, ""RADIUS Server CA Certificate 2" Tab".
- **Server**: SIP server
  Client: IP phone (see Section 16.14.3, "Importing SPE CA Certificates for IP Phones")
  For an interface description, see Section 7.1.22.2, ""SPE CA Certificates" Tab".
- **Server**: SIP server
  Client: IP client (see Section 16.14.4, "Importing SPE CA Certificates for IP Clients")
  For an interface description, see Section 7.2.13.1, ""SPE CA Certificates" Tab".
- **Server**: SIP Server
  Client: IP Gateway (see Section 16.14.5, "Importing SPE Certificates and SPE CA Certificates for IP Gateways")
  For an interface description, see Section 7.3.3.3, ""SPE CA Certificates" Tab".

  NOTE: Certificates can only be administered via DLS and not via the deployment tool, the WBM or directly at a telephone.

16.14.1 Importing WBM Server Certificates

1. Select **Call: Main Menu > Call: Main Menu > > IP Phone Configuration** > **Security Settings** > **"WBM Server Certificate" Tab**. Search for and select the IP phone that you want to import a certificate for to enable communication with the WBM client (Web browser).
2. Click **Import Certificate**. An import dialog appears:



   This dialog contains the device ID of the IP phone you have selected.
3. In the **File name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.

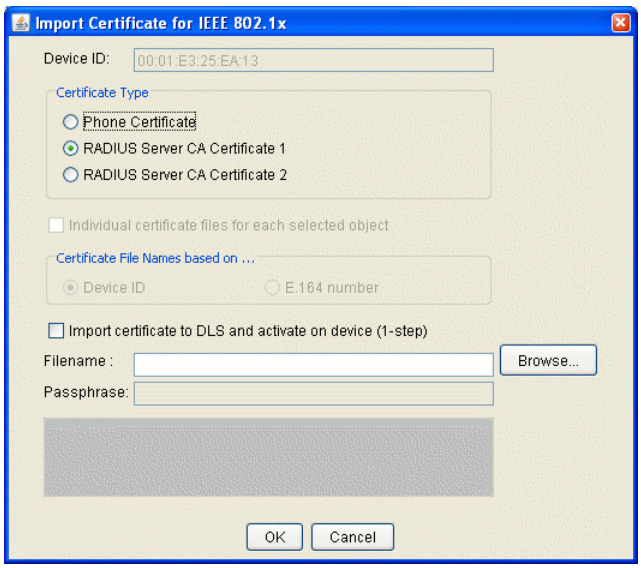
   The certificate should be in `PKCS#12` format.
4. Enter the key used to encrypt the PKCS#12 file you want to import in the **Passphrase** field.
5. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.
6. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
7. For activating the imported certificate, click **Activate** certificate and **Save** afterwards, if **Import certificate to DLS and activate on device (1-step)** is not activated.

NOTE: Certificates should be deployed to devices when respective template (with PKI Connector saved) is applied through Plug & Play

NOTE: Certificates won't be deployed to already registered devices even if a template with PKI Connector saved, is applied.

16.14.2 Importing Phone and RADIUS Certificates

1. Click the **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **IEEE 802.1x** area.
2. Select the tab for the relevant certificate **"Phone Certificate" Tab, "RADIUS Server CA Certificate 1" Tab** or **"RADIUS Server CA Certificate 2" Tab**. Search for and select the IP phone that you want to import the certificate for.
3. Click **Import Certificate**. An import dialog appears:



This dialog contains the device ID of the IP phone you have selected.

4. Select the relevant certificate in the **Certificate Type** field. The option that corresponds to the tab is already selected.
5. Activate the check box **Individual certificate files for each selected object** to import an individual certificate for every IP phone (for more information, see step 6).
6. In the **File Name** entry field (or **Directory** if the check box in step 5 is activated), enter the entire local path including the certificate name (without the name if the check box in step 5 is activated) or click **Browse** to enter the path via the browser.

   NOTE: If you decided to import individual certificated for each IP phone in step 5, these certificates must already be available as follows:
   All certificate file names must be based on:
   - The device IDs of the telephones or
   - The phones' E.164 numbers

   Select the appropriate option in **Certificate File Names based on ...**.

   Phone certificates should be in `PKCS#12` format and RADIUS certificates in `.pem` format.

7. For phone certificates only: Enter the key used to encrypt the PKCS#12 file you want to import in the **Passphrase** field (not necessary for RADIUS certificates).
8. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.
9. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
10. For activating the imported certificate, click **Activate certificate** and **Save** afterwards, when **Import certificate to DLS and activate on device (1-step)** is not activated.

NOTE: Certificates should be deployed to devices when respective template (with PKI Connector saved) is applied through Plug & Play

NOTE: Certificates won't be deployed to already registered devices even if a template with PKI Connector saved, is applied.

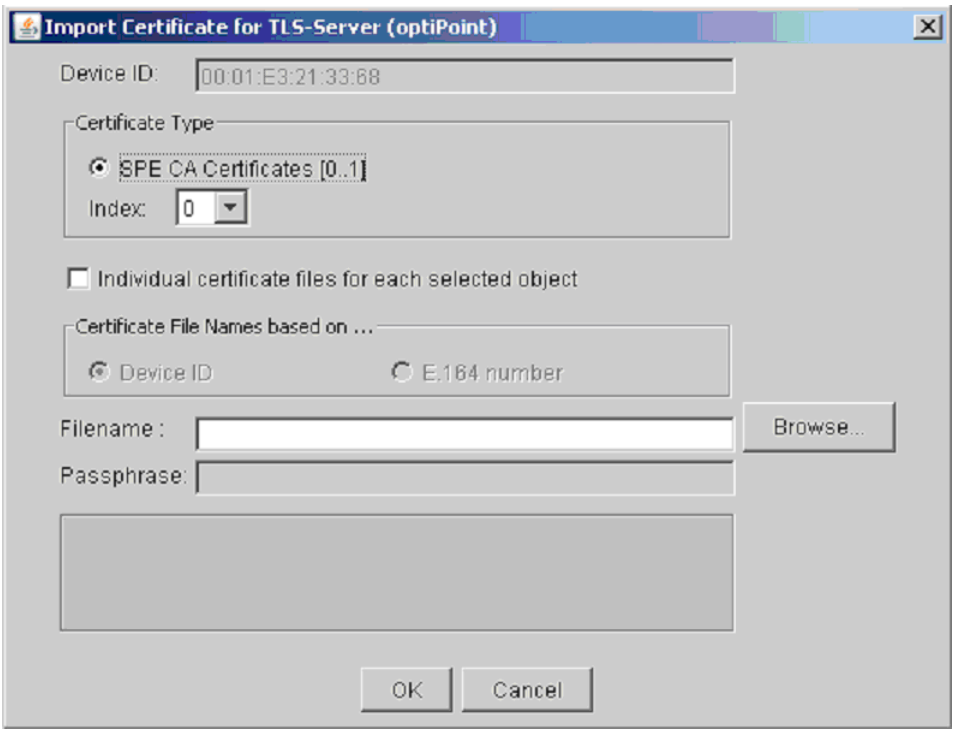
IMPORTANT: In order for a phone running IEEE 802.1x to successfully authenticate with a Radius server, it is essential that the IEEE 802.1x settings on the phone are complete, correct, and consistent with those on the Radius server.t is essential that all of the information is sent from the DLS to the phone in a single operation.For instance, when setting PEAP, a RADIUS Server CA Certificate must have been imported into the DLS and the **Activate certificate** on the relevant tab ticked, as well as the Authentication Type (PEAP), MSCHAP Identity and MSCHAP Password should all be set before pressing **Save**.

IMPORTANT: If there are multiple certificates and the Authentication Type has to be set to EAP-TLS, the **Import certificate to DLS and activate on device (1-step)** checkbox MUST NOT be checked. It MUST be left blank.Instead, when all certificates have been imported into the DLS, the **Activate certifica**te on the relevant tabs is ticked, and the **Authentication Type** MUST be set to EAP-TLS before **Save** is pressed.

IMPORTANT: If the phone does not have complete and correct settings for the Radius server, it will fail to authenticate and dependent upon the switch settings may not be assigned to a network. If this happens, the phone must be connected to an unauthenticated network that has DLS access to correct and complete the IEEE 802.1x information on the phone before further authentication attempts to the Radius server. When the Radius server is set up for mutual authentication, the phone MUST have a client certificate and a RADIUS server CA certificate. If the RADIUS server is not set up for mutually authentication, the phone only requires a RADIUS server CA certificate. (edited)

16.14.3 Importing SPE CA Certificates for IP Phones

1. Select **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**. Search for and select the IP phone that you want to import a certificate for to enable communication with the SIP server.
2. Click **Import Certificate**. An import dialog appears:



   This dialog contains the device ID of the IP phone you have selected.
3. You must enter the according **Index**, because the CA certificate is indexed.
4. In the **File name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.

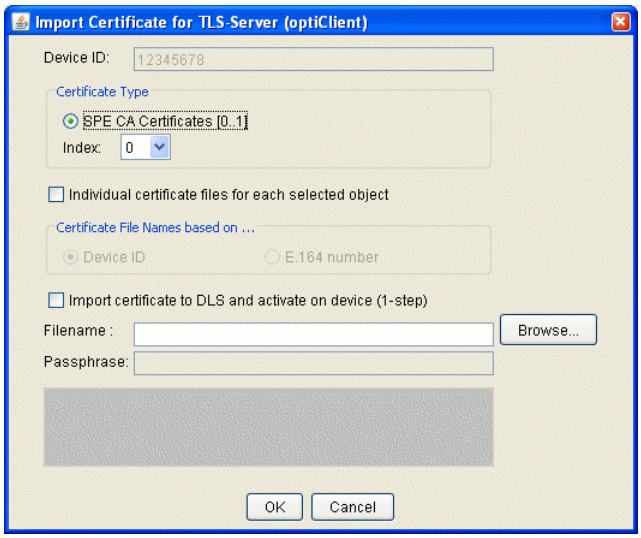
   The certificate should be in `.pem` format.
5. Enter the key used to encrypt the PKCS#12 file you want to import in the **Passphrase** field.
6. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
7. For activating the imported certificate. click **Activate certificate** and **Save** afterwards.
8. To import a second certificate, proceed as described for the first certificate.

NOTE: Certificates should be deployed to devices when respective template (with PKI Connector saved) is applied through Plug & Play

NOTE: Certificates won't be deployed to already registered devices even if a template with PKI Connector saved, is applied.

16.14.4 Importing SPE CA Certificates for IP Clients

1. Select **Call: Main Menu > Call: Main Menu >** > **IP Client Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE CA Certificates" Tab**. Search for and select the IP client that you want to import a certificate for to enable communication with the SIP server.
2. Click **Import Certificate**. An import dialog appears:



   This dialog contains the device ID of the IP phone you have selected.
3. In the **File Name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.

   The certificate should be in `.pem` format.
4. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.
5. Click **OK** to import the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
6. For activating the imported certificate, click **Activate certificate** and **Save** afterwards, if **Import certificate to DLS and activate on device (1-step)** is not activated..
7. To import a second certificate, proceed as described for the first certificate.

NOTE: Certificates should be deployed to devices when respective template (with PKI Connector saved) is applied through Plug & Play

NOTE: Certificates won't be deployed to already registered devices even if a template with PKI Connector saved, is applied.

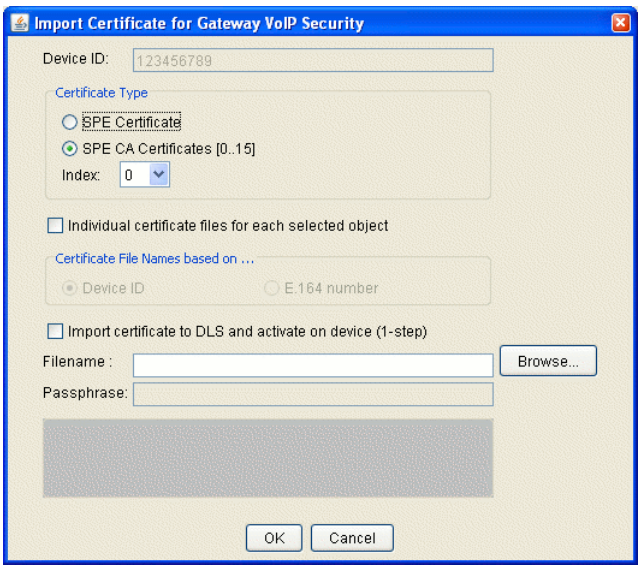
16.14.5 Importing SPE Certificates and SPE CA Certificates for IP Gateways

If Signaling and Payload (SPE) certificates are to be used, the IP phones must be connected to an IP gateway. The IP gateway has to be be pre-configured as virtual device.

1. Select **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration**. Enter the IP address of the IP Gateway in the **Device ID** field and select "IP Gateway" in the **Device Family** field.
2. When configuring IP Gateways for the first time, enter the **DLS Server Address** and the **DLS Port** (Default: 18443) in the tab **DLS Connectivity**. If you want to configure further IP Gateways, these values will be used internally by the DLS.
3. **Secure mode required** is activated automatically, because IP Gateways may operate in this mode only. Select **PIN Mode**.

   NOTE: If **Default PIN** has been chosen, this PIN might be administered by means of **Administration** > **Workpoint Interface Configuration**.

   The PIN must be declared to the IP Gateway board before the registration. This is done by the CLI interface (activate dls pin <pin>)
4. When pressing the **Scan** button, the registration including bootstrapping will be executed.
5. Switch to **Call: Main Menu > Call: Main Menu >** > **IP Gateway Configuration** > **Signaling and Payload Encryption (SPE)** > **"SPE Certificate" Tab** and click on **Import Certificate**. An import dialog appears:



NOTE: The imported certificates must be created by means of a customer PKI.

It is recommended to deploy an individual certificate for each gateway to which the own IP address is assigned in **Owner field (CN)**. This is absolutely neccessary if **Owner check** is activated. If DNS is used, the host name of the gateway may be entered instead of its IP address.

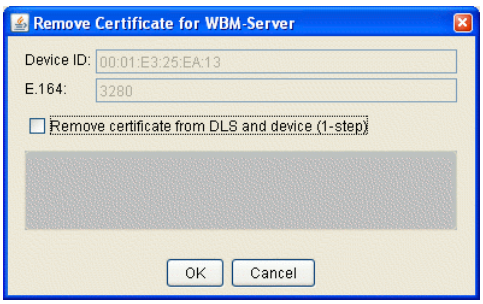
6. Choose whether you want to import a SPE certificate or a SPE CA certificate. For SPE CA certificates, you must enter the according **Index**, because this certificate is indexed.
7. In the **File name** entry field, enter the entire local path including the name of the certificate or click **Browse** to enter the path via the browser.
   The SPE certificate should be in PKCS#12 format, and the SPE CA certificate should be in `.pem` format.
8. For SPE certificate only: In the **Passphrase** field, enter the key used to encrypt the PKCS#12 file you want to import.
9. Activate **Import certificate to DLS and activate on device (1-step)**, if the certificate should be activated immediately.
10. Click **OK** to import the certificate. If you have selected several objects (see Section 5.4.2.4, "Multiple selection and data transfer in Table view"), select **Apply to All** to import certificates for all of these objects. The additional question due to security reasons must be answered with **Apply to All**.
11. For activating the imported certificate, click **Activate certificate** and **Save** afterwards, if **Import certificate to DLS and activate on device (1-step)** is not activated.
12. SPE Certificate as well as SPE CA certificate for IP Gateway must be imported.
13. Afterwards, the SPE Certificates for IP Phones / IP Clients must be imported as described in chapter Section 16.14.3, "Importing SPE CA Certificates for IP Phones" / Section 16.14.4, "Importing SPE CA Certificates for IP Clients".
14. Switch to **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** > **Signaling and Payload Encryption (SPE)** > **"SIP Settings" Tab** or **"HFA Settings" Tab** and set "TLS" in the entry fields **SIP Transport Protocol** resp. **HFA Transport Protocol**. For IP Clients the values have to be entered the same way.

NOTE: Certificates should be deployed to devices when respective template (with PKI Connector saved) is applied through Plug & Play

NOTE: Certificates won't be deployed to already registered devices even if a template with PKI Connector saved, is applied.

16.14.6 Remove Certificate (IEEE 802.1x Phone as an example)

1. Select the area you require under **Call: Main Menu > Call: Main Menu >** > **IP Phone Configuration** (see Section 16.14.1 to Section 16.14.5).
2. Search and select the IP phone whose certificate you want to remove or switch to **Template** view to delete a certificate from a template.
3. Click **Remove Certificate**. A dialog appears (see the following example):



4. For IEEE 802.1x certificates, select the certificate to be removed (if applicable). The option that corresponds to the tab is already selected.
5. Activate **Remove certificate from DLS and device (1-step)**, if the certificate should be remoced immediately.
6. Click **OK** to remove the certificate.
   If you have selected several objects (see Section 5.4.2.4), select **Apply to All** to remove certificates for all of these objects.
7. Click **Activate certificate** and **Save** to delete the certificate on the phone, if **Remove certificate from DLS and device (1-step)** is not activated.

16.14.7 Replace IP Phone

1. Click the **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** area. Click **Action** in the menu bar and select **Copy IP Device** (see Section 16.6, "Replacing an IP Device").
2. Please check if the copy contains all certificates as imported certificates, or the certificates are part of a default profile. If only activated certificates are available, they are not used any more with Plug&Play.

16.15 How to remove browser's Certificate Error message when logging in to DLS

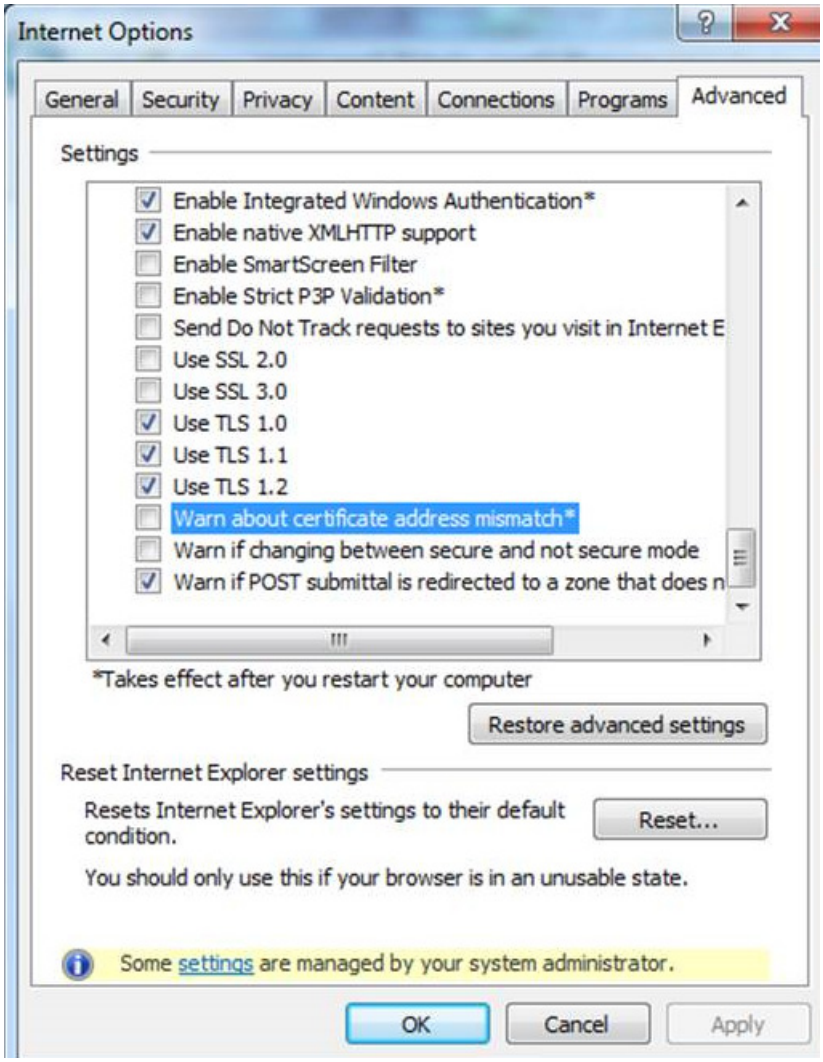
While trying to access DLS using it's hostname or IP address, e.g. `10.0.201.151`, DLS sends back a server certificate that has as common name (of it's subject) not that hostname or ip but the following:

Your browser expects the CN of DLS certificate to be `10.0.201.151` (say) but instead of that receives CN=OpenScape Deployment Service. Your browser shows this warning about mismatched address between the URL you are trying to access and the CN of the presented certificate. It doesn't complain about untrusted certificate as the DLS product-embedded (hard-coded) certificate has been installed in Windows Trustore already (you can install it).

> ***IMPORTANT:*** It is advised to import to DLS server a more appropriate certificate and not the self signed one that ships with the product. This product-embedded (hard-coded) certificate is not issued to the specific customer's CN which is customer's DLS FQDN, hostname or IP. It is a generic certificate issued to some DLS server with CN= OpenScape Deployment Service. You can trust it's issuer but you cannot fully verify it's CN.
>
> ***IMPORTANT:*** Another proper solution would be to import to DLS (for GUI access) a server certificate issued to the FQDN or ip of customer's DLS.

Another workaround is to disable '**Warn about certificate address mismatch**' in Internet Explorer (as in the screenshot, PC restart is not necessary). Then you won't get the warning anymore.

NOTE: This certificate is embedded in the product build, cannot be replaced or modified via the DLS UI in affected versions, and is updated only through product releases. After certificate expiry there is no functional impact on already operational systems: TLS encryption remains active, Secure Mode communication (port 18444) is unaffected, and existing installations continue to operate without restriction. However, upgrading to DLS V10 R3.20 is recommended for security hygiene and compliance, and becomes necessary if new UC/OSILA connections must be created or modified, or if new devices are to be onboarded using Secure Mode.


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Enable Integrated Windows Authentication*
Enable native XMLHTTP support
Enable SmartScreen Filter
Enable Strict P3P Validation*
Send Do Not Track requests to sites you visit in Internet E
Use SSL 2.0
Use SSL 3.0
Use TLS 1.0
Use TLS 1.1
Use TLS 1.2
Warn about certificate address mismatch*
Warn if changing between secure and not secure mode
Warn if POST submittal is redirected to a zone that does n
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
Some settings are managed by your system administrator.
OK
Cancel
Apply

16.16 Configuring and Administrating Mobility

With the Mobility function, call numbers can be assigned to specific persons instead of devices. In addition to their call numbers, a user's settings, such as, the key layout, can be transferred from one device to another. To enable this, users must log on to the device in question with their call number and a password. Once the user has logged off, the previous device used is reassigned its basic profile, and as a result, a different call number to that of the mobile user.

NOTE: For basic information on mobility in DLS, see Section 3.8, "DLS Mobility - General Information".

16.16.1 Configuring the Mobility Function on the Device

Select the **Mobility** tab in the area **Call: Main Menu > Call: Main Menu > > IP Phone Configuration > SIP Mobility** and activate the option **Device available for Mobile User**.

16.16.2 Programming the "Mobility" Button

Configure a template with a key layout that provides a mobility key:

1. Select **Template** view in the area **Call: Main Menu > Call: Main Menu > >** IP Phone Configuration > Keysets/ Keylayout and click the  icon in the **Destinations** tab. A new line is displayed in the table, in which you can make the required entries.
2. As the key function **Mobility** is on the first level, select "1. Level" in the **Level** column.
3. In the **Key number** column, select the key to which the new function should be assigned. For more information, see Section 7.1.19.2, ""Destinations" Tab".
4. Select "Mobility" in the **Key function** column.
5. You can now enter a key label in the final column. This is only displayed with optiPoint 420 telephones that provide LCD key labeling.
6. If you click **Save**, a dialog window opens where you can enter a name and a description for the template. Save the template by clicking **Save**.

   For more information on creating templates, see Section 15.7.1, "Creating a Template Manually".
7. Assign the template to a profile and load this profile to the required workpoint.

16.16.3 Creating a Mobile User Profile

1. Create templates containing the required mobile user configurations. Select the **Templates** view in the area to be configured, for example in **Mobile Users** > **SIP Mobile User Configuration** > **Miscellaneous**.
2. If you click **Save**, a dialog window opens where you can enter a name and a description for the template. Save the template by clicking **Save**.
3. Click **New** in the area > **User Data Profile** to create a new profile. Click the icon  . In the choice list that now opens, select the required template.
4. In the **Name** field, enter the name for the new profile. In the **Description** field, enter a short description of the profile if required.
5. Click **Save** to save the profile.

16.16.4 Creating Mobile Users

Requirements

- A working DLS infrastructure.
- The Mobile Users must already be configured in OpenScape Voice.

16.16.4.1 Adding New Mobility Users

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User > "Mobile / Basic User" Tab**.
2. Click **New**.

   Click the  button to the right of the **New Mobile User IDs** field. A dialog window appears. The list shows all call numbers registered in the telephone system that are still available, i.e. that have not yet been assigned to a workpoint or mobile use. Clicking **OK** applies the data. In addition to the choice list, you also have the option of entering the call number of the mobile user into the field by hand. Multiple numbers must be comma-separated.
3. Under **Mobile User Password**, enter the password for the Mobile User accessing the Mobility Phone.

   NOTE: In OpenStage v3 onward, the password for mobile users is send using hash values.Therefore the DLS is not able to display anything in the password field when the Refresh button is used.
   The password is not lost,is just not visible in the DLS graphic user interface.
4. Under **Mobile User Profile**, select the profile (see Section 16.16.3, "Creating a Mobile User Profile") that should be applied for the Mobile User to be created.
5. If necessary, activate the **Get SIP Data from Virtual Devices** to automatically apply the SIP data entered in the device profile (**Profile Management** > **Device Profile**) for the Mobile User.
6. Click **Save**.

16.16.4.2 Creating Mobile Users via Migration

1. Go to **Mobile User > Mobile User Interaction > Mobile User**. If you select "Mobility enabled Device" in the **User Type** field and then click **Search**, a list of all devices available for a mobile user is shown in the **Table** view.
2. Click **Migration to Mobile User**. A dialog window opens.
3. Enter a new E.164 for use as the basic E.164 number for the mobility-enabled device. That is, the E.164 number used by the device when no user is logged-on the device.
4. Enter a mobile user profile for use by the mobility enabled device when no user is logged-on the device.
5. Enter the mobile user password for the newly created basic user.
6. Start the migration.

NOTE: During migration, the user data of the mobility enabled device are used for the creation of a new mobile user. New E.164 number and new user data are copied to the mobility enabled device for use when no user is logged on the device.

NOTE: As soon as migration has been completed, the previous basic user is migrated to mobile user. The default password for new mobile user is "000000" .

16.16.5 Create a Home Phone

A home phone is an end device assigned to a SIP mobile user. The mobile user is logged on to the home phone by default. Setting up of a home phone is optional. However, when a home phone has been set up, the mobile user is automatically logged on to it after having been logged off from another phone, and thus, he is accessible. When the mobile user logs off from the home phone, he is not accessible any more.

1. Navigate to **Mobile Users > SIP Mobile User Interaction > SIP Mobile User**. If you choose "Mobility enabled Device" in the field **User Type** and click on **Search** afterwards, you get a list in **table** view that contains all end devices which are available to a mobile user. For mobile users with status "Mobile User Logged Off", the fields under **Mobile User Home Phone** are available.
2. Activate **Allow automatic Logon at Home Phone**, so that logging on the mobile user at the home phone is activated immediately.
3. For **Home Phone**, choose the call number of the end device from the selection list. The Home **Phone Status** field shows the status of the home phone selected.
4. Finally, confirm by **Save**.

16.16.6 Logging On Mobile Users (Forced Logon)

A mobile user can be logged on not only at the device but also via DLS.

1. In the area **Mobile Users > SIP Mobile User Interaction > Logon/Logoff** use **Search** > **Table** view **> Object** view to find the mobile user you want to log on. Alternatively, you can also select the device where you want to log the mobile user on.
2. Click **Logon Mobile User**.
3. A dialog window opens. If you had already selected a mobile user, enter the Basic E.164 number now for the device where you want to log the mobile user on. If you have selected a device, you must enter the mobile user's mobility ID.

16.16.7 Logging Off Mobile Users (Forced Logoff)

Using the DLS, the administrator can implement a forced logoff for a Mobile User that is logged on to a workpoint. This interrupts ongoing calls.

1. In the area **Mobile Users > SIP Mobile User Interaction > Logon/Logoff** use **Search** > **Table** view **> Object** view to find the mobile user that you wish to log off. Alternatively, you can also select the device where the mobile user is logged on.
2. You can use **Logoff Mobile User** to log the Mobile User off the relevant device.

16.16.8 Troubleshooting for Mobile User Logon/Logoff

The **History** tab in the area **Mobile Users > SIP Mobile User Interaction > Logon/Logoff** contains information regarding actions. This information is available for the Mobile User and for devices that are available for the Mobile User.

You can find a survey of all mobile user related actions in the **Mobile Users** > **Mobility Statistics**.

A multitude of reasons can lead to a situation where a mobile user is logged on at two phones (A and B) simultaneously. This will not cause an error in OpenScape Voice. However, the DLS provides a special error handling which tries to clear this situation by logging off the mobile user at phone A, as soon as it is reachable again.

Possible reasons for unsuccessful logoff:

1. Phone A is not available, is restarting, is plugged off, has a broken network, or a hardware problem. These are the most probable reasons.
2. Phone A has a software problem and cannot complete the protocol for executing the logoff. In most of these cases, the DLS is able to tell the phone to start a logoff, but the phone does not execute it.
3. Phone A is DCMP-enabled. SIP Mobility and DCMP do not work together. Therefore, DCMP has to be disabled when using SIP Mobility.

4. Phone A is not accepted by the DLS, because it is in Secure Mode, but does not have a valid certificate of this DLS.
5. Phone A does not have the correct DLS-Address.
6. Phone A is in a phone call (see time before doing a Logoff while a Phone Call is ongoing: **Main Menu** > **Mobile Users** > **SIP Mobile User Configuration** > **SIP Mobility** > **"Mobility Logon/Logoff" Tab**).

16.16.9 Default Setting for the Key Layout in Mobility Telephones

For each device type, default key layouts can be defined for the four basic key functions "Prime Line", "Mobility", "Cancel" and "Shift". These defaults overwrite the key layout defined in each Mobile User's profile.

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP User Keylayout**.
2. Select the required **Device Type**.
3. Activate **Use following Defaults for Mobile User Logon**.

16.16.9.1 FFK/FPK settings in Mobility Telephones

DLS maintains a properties file with the default FFK/FPK settings (key function/label) for all different phone types. This file shall be read by DLS during the service startup.

The following tables illustrate the default FFK/FPK settings per phone type. These tables shall be used internally by DLS to detect if the received FPK's / FFK's have different values than the default.

Key Index	OpenStage 40	OpenStage 40 US	OpenStage 60 / 80	Desk Phone IP 35	Desk Phone IP 55
4001	Release icon	Conference icon	Release icon	Conference icon	Conference icon
4002	Forward icon	Hold icon	Forward icon	Hold icon	Hold icon
4003	(Key not present)	(Key not present)	Voice Dial icon	(Key not present)	(Key not present)
4009	Redial icon	Transfer icon	(Key not present)	Transfer icon	Transfer icon
4010	(Key not present)	(Key not present)	(Key not present)	(Key not present)	Forward icon

Key Index	OS 40	OS 40 US	OS 60	OS 80	Desk Phone IP 35	Desk Phone IP 55
1	Key icon / no imprinted label	Shift icon / no imprinted label	Key icon / no imprinted label	Key icon / no imprinted label	Forward icon	Shift icon
2	Key icon / no imprinted label	Phonebook icon / no imprinted label	Key icon / no imprinted label	Key icon / no imprinted label	Pickup icon	Key icon / no imprinted label
3	Key icon / no imprinted label	Pickup icon / no imprinted label	Key icon / no imprinted label	Key icon / no imprinted label	DND icon	Key icon / no imprinted label
4	Key icon / no imprinted label	Forward icon / no imprinted label	Key icon / no imprinted label	Key icon / no imprinted label	(Key not present)	Key icon / no imprinted label
5	Key icon / no imprinted label	DND icon / no imprinted label	Key icon / no imprinted label	Key icon / no imprinted label	(Key not present)	Key icon / no imprinted label
6	Key icon / no imprinted label	Phone Screen icon / no imprinted label	Key icon / no imprinted label	Key icon / no imprinted label	(Key not present)	Key icon / no imprinted label
7	(Key not present)	(Key not present)	Key icon / no imprinted label	Key icon / no imprinted label	(Key not present)	Key icon / no imprinted label
8	(Key not present)	(Key not present)	Key icon / no imprinted label	Key icon / no imprinted label	(Key not present)	Key icon / no imprinted label
9	(Key not present)	(Key not present)	(Key not present)	Key icon / no imprinted label	(Key not present)	(Key not present)

Whilst a mobile user is logged on, if DLS receives FPK's / FFK's as part of local changes, DLS shall compare the received FFK's / FFK's with the default FPK's / FFK's of the phone (for the keys that are not locked) and then, it shall perform the following handling:

a) If the received key has different key function:

- Search the mobile user keys based on the received key index
- If there is configured mobile user key, update it
- Otherwise (no configured mobile user key), add a new mobile user key

b) If the received key has the default key function, but different key label:

- Search the table with the custom key labels based on the received key function
- if there is configured custom key label, update it

- Otherwise (no configured custom key label), add a new custom key label for the received key function

c) If the received key has the default key function and label:

- Search the mobile user keys based on the received key index and if there is configured mobile user key, delete it
- Search the table with the custom key labels based on the received key function and if there is configured custom key label, delete it
- Otherwise (no configured mobile user key or custom key label), nothing to do

NOTE: In the same manner, the "migrate to mobile user" functionality shall be enhanced to NOT move the basic user FFK's / FPK's that have the default key functions and labels of the basic user device type.

16.16.10 Data Backup to a .zip Archive

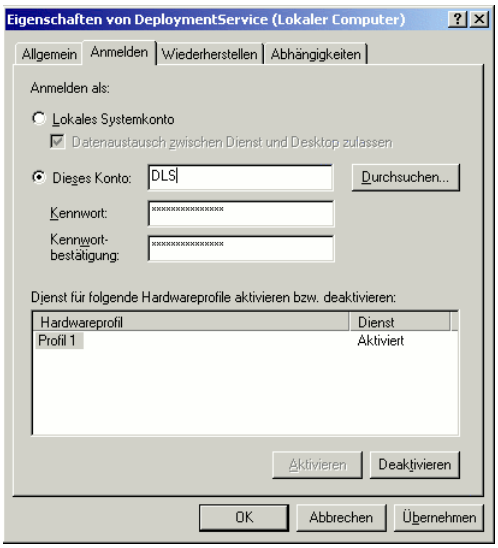
All mobile user data can be saved in a .zip archive. The data within the .zip archive is saved in XML format which is the format used for data exchange between workpoints and DLS.

16.16.10.1 Preparation

Data backup should normally be performed on a network drive. Only one specific directory should be released for mobile user data storage. The following steps are required for this:

1. Stop the DeploymentService, that is the DLS Web service. To do this, click **Programs** > **DeploymentService** > **Stop Service** in the Windows Start menu.
2. As the DeploymentService runs after installation with the localadmin account for which no drives are normally mapped, it can only access local drives at first. You should therefore assign the DeploymentService an account which contains privileges for the network drive to be mapped.
   IMPORTANT: Make sure that the DeploymentService account has administrator rights. Restrictions can lead to problems with DLS.

   To assign a new account to the DeploymentService, select **Settings** > **Administrative Tools** > **Services** or **Settings** > **Control Panel** > **Administrative Tools** > **Services** in the Windows Start menu. Double-click the **DeploymentService** entry to open a window where you can change the properties of the service. Now activate the **This account** check box in the **Log On** tab and click **Browse** to select the relevant user account.



3. Rename the following files in the folder `"C:\Program Files\DeploymentService\Tomcat\bin"`:

   `initdlsservice.template` > `initdlsservice.bat`

   `releasedlsservice.template` > `releasedlsservice.bat`

4. Enter the network drive connection or release command as described in the files `"initdlsservice.bat"` and `"releasedlsservice.bat"`.

5. Select **Programs** > **DeploymentService** > **Start Service** to restart the service.

16.16.10.2 Saving Mobile User Data

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User**.
2. Click **Search** to find all available mobile users.
3. Select the option **Table** under **Views**. Mark the mobile user whose data you want to save.
4. Now, select the entry **Save Selected Mobile User to Archive** in the menu bar under **Action**. A dialog window opens where you can select the storage location.

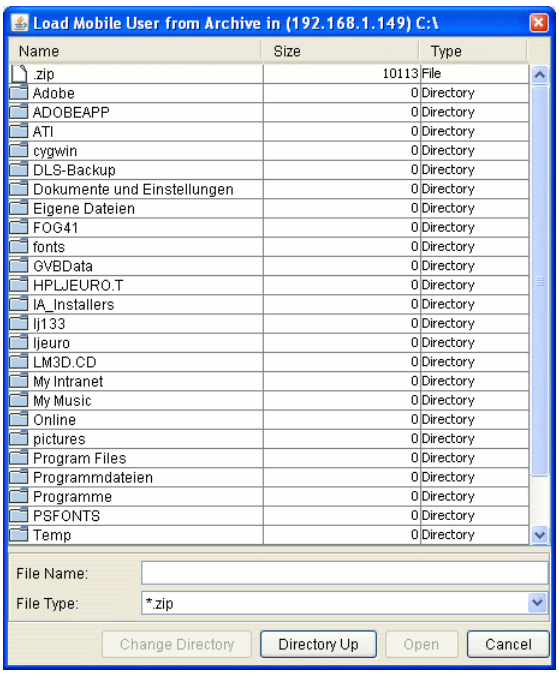


5. The contents of the drive where the DLS is installed are displayed by default. Mark a directory name and then click **Directory Change** or double-click the directory name to select the required destination directory. Click **Directory Up** to move to a higher directory level.
6. Enter a file name for the ZIP archive and confirm with **Save**. Alternatively, you can mark an existing archive in the list with a simple click and then press **Save**. In the ensuing selection window, you can choose if you want to save the mobile user data to the existing archive (**Write Data to existing Archive**) or overwrite the existing archive (**Create new Archive**).

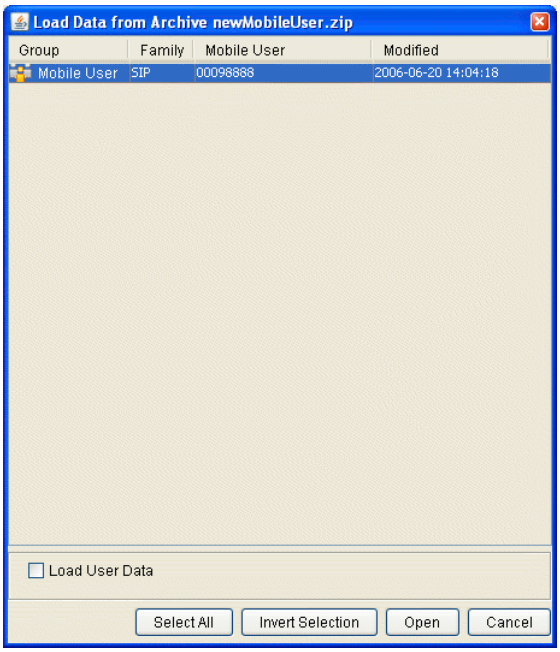
16.16.10.3 Loading Mobile User Data

NOTE: You can only load mobile user data if the relevant mobile users are logged off. Data associated with a mobile user who is logged on will not be overwritten.

1. Select the area **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User**.
2. Now, select the entry **Import Mobile User** in the menu bar under **Action**. A dialog window opens for selecting the directory path. Mark a directory name and then click **Directory Change** or double-click the directory name to select the required destination directory. Click **Directory Up** to move to a higher directory level.



3. Mark a .zip archive in the list and click **Open**. A list of all mobile user data records saved in this archive is displayed.



4. Mark the data records you want or, where applicable, click **Select All**. You can also select **Reset selection**. Use the **Load User Data** check box to specify whether or not non-configurable user data, such as, call lists or phone book data, should be loaded to the DLS database.

   NOTE: Call lists and phone book data must be saved in encrypted format.

5. If you click **Open** now, the selected mobile user data is loaded to the DLS database.

   NOTE: It may take some time to load all user data depending on the data volume.
   The size of the non-configurable user data can be requested over **Mobile Users** > **User Data Administration**

16.16.11 Import Mobile User Data

It is possible to import a manually created csv file with Mobile User Data. An export of Mobile User Data is not allowed due to data security reasons.

The file must have following format:

1. row: Description of columns content:

<E.164>	Required ,valid E.164 number
<Mobile User Password>	Required
<Mobile User Profile>	Required
<Get SIP Registration Data from Virtual Devices>	optional
<Home Phone>	optional
<Allow automatic Logon at Home Phone>	Required, possible values: true, false
Get Keyset Configuration from Virtual Device	Optional

Table 16

2. and following rows: Columns content separated by ';'

Import-File example:

```
12345;000000;@profile;;;false
33333;000000;@profile;;;false
4411594311111;000000;MobUser;;;false
4411594312334566789;000000;MobUser;;12345;true
```

Example of data that have to be imported for the creation of Mobile User with SIP registration and KeyStet Data are as follows:

1.Import of a Virtual device with the needed SIP registration data and Keyset configuration :

##CreateSIPPhone <ID> <e164> <type>...<SIP Server Addr.><SIP Server Port><SIP Reg Addr.><SIP Reg Port>…

CreateSIPPhone 302108189656 OpenStage 80... 10.7.1.54 5060 10.7.1.54 5060…

Keysets

ModifyKeyset<reset><e164 number><attribute-name>=<attribute-value>]+

ModifyKeysetFALSE302108189656line-registration-leds=true...

Keys

ModifyKey<reset><e164 number><key function><level><module>...

ModifyKeyFALSE302108189656hold00...

ModifyKeyFALSE302108189656do not disturb00...

ModifyKeyFALSE302108189656conference00...

ModifyKeyFALSE302108189656headset00...

ModifyKeyFALSE302108189656mobility00...

ModifyKeyFALSE3021081896567010...

ModifyKeyFALSE302108189656built-in release40...

ModifyKeyFALSE302108189656built-in forwarding40...

ModifyKeyFALSE302108189656built-in voice dial40...

2.Import of the mobile user :

302108189656;000000;temp;true;;false;true

To import a file with mobile user data, proceed as follows:

1. Switch to **Mobile Users** > **SIP Mobile User Interaction** > **SIP Mobile User** and click **Import Mobile User**. An import dialog appears, brows for valid filename.
2. Click on **Save** to save the imported mobile user.

16.16.12 Mobility between optiPoint and OpenStage

Mobility between optiPoint and OpenStage is possible, but with restrictions only. For additional information see http://wiki.unify.com/images/7/72/SIP_Mobility_User_-_optiPoint_and_OpenStage_Regression_Test.pdf

16.16.13 IP Client Mobility

Requirements

- A created device as described in Section 16.10.2, "Configuring an ODC Client in DLS".
- A mobile user with the E164 number of the IP client. Mobile user has to be configured with the mandatory parameters for the user to log on phone.

NOTE: Mobile user can be logged on one device at a time (phone or client). During mobile user log-on, DLS forces the user log off from the second device.

16.17 HFA Mobility with HiPath 3000

This feature allows the HiPath 3000 IP Mobility feature to be used in a networked (TDM or IP trunks) environment with a closed numbering range.

> ***NOTE:*** Technically, only a matching HiPath 3000 LCR dial plan entry is required for the IP Clients on other nodes, while LCR routing is irrelevant. Without a matching LCR dial plan entry, it will only be possible to enter local E.164 subscriber numbers when using the feature. The network trunks are not used for this feature.

On HiPath 3000 systems, the DLS is responsible for sending the correct registration information to IP Clients that are not logging-on at their home location.

HFA Mobility with HiPath 3000 systems works as follows: A subscriber from a different HiPath 3000 system logs on at an IP Phone, which results in the phone being unable to communicate with the gateway because of modified registration data. The IP Phone contacts the DLS, which thereupon looks up the virtual device that belongs to the subscriber's E.164 number. The registration data of this virtual device are now sent to the IP Phone, thus enabling it to register.

For further settings, see Section 7.1.18, "HFA Mobility".

16.17.1 HiPath 3000 Configuration Prerequisites

IP mobility is configured and working on each HiPath 3000 node as described in the HiPath 3000/5000 feature description.

16.17.2 DLS Configuration for Network-wide HFA Mobility

Only the extra DLS configuration required for HFA Mobility with HiPath 3000 will be considered here:

- Import the configuration from each node into the DLS using "Element Manager" (including the mobile IP Clients). The mobile IP Clients are virtual devices on the DLS.
- In **Call: Main Menu > Call: Main Menu >** > **IP Device Management** > **IP Device Configuration** > **"General" Tab** activate the **Use for HFA Mobility with HiPath 3000** switch for each mobile IP Client in each node.

16.17.3 Operating procedure

1. Activate (Mobile user logon) with this entry:
   *9419 + E.164 subscriber number + password (password optional if not configured)
2. The IP Phone will try to logon at the current HiPath 3000 node using the E.164 subscriber number that has been entered. The message "Logging On To Home" will be displayed briefly. The logon will fail because the mobile IP Client is not configured at this HiPath 3000 node. The message "Mobile Log On Failed" will appear on the top line of the display, with "Contacting DLS" on the bottom line of the display.

The IP Phone will then send a "mobility-configuration-request" message to the DLS. The DLS will then send the correct registration information that will allow this mobile IP Client to log-on at the correct home node.

3. Deactivate (Mobile user logoff) by entering #9419.

16.18 Data Structures for DLS-hosted XML applications

In the following, the storage locations for data to be used by DLS-hosted XML applications are described. This enables customizing the applications by the user resp. administrator.

16.18.1 Directory Structure

- Texts and default pictures are searched under `<DLS installation path>/DeploymentService/Tomcat/webapps/XMLApplications/data/default`
- For customization by means of customer texts and pictures, it is possible to create a directory `<DLS installation path>/DeploymentService/Tomcat/webapps/XMLApplications/data/custom` which will then serve as search path for the texts and pictures.

  NOTE: It is recommended to copy the directory `.../XMLApplications/data/default` to `.../XMLApplications/data/custom` and then make the intended changes there.
- Under `.../XMLApplications/data/DeploymentService`, `.../XMLApplications/data/LocationService`, `.../XMLApplications/data/MakeCall`, `.../XMLApplications/data/NewsService` the texts for the respective XML applications are stored. These directories may not be changed by the user.

16.18.2 Directories at Upgrade Installations

With regard to upgrade installations, please consider the following:

- The `.../XMLApplications/data/default` directory is updated.
- The `.../XMLApplications/data/custom` is renamed to `.../XMLApplications/custom_old`

  NOTE: If customizations have been made, these must be redone. For this, copy `.../XMLApplications/data/default` to `.../XMLApplications/data/custom` again or rename `.../XMLApplications/data/custom_old` to `.../XMLApplications/data/custom`
- The directories `.../XMLApplications/data/DeploymentService`, `.../XMLApplications/data/LocationService`, `.../XMLApplications/data/MakeCall`, `.../XMLApplications/data/NewsService` remain unchanged.

16.18.3 Directories at Backup/Restore

With regard to a restore, please consider the following:

- The directory `.../XMLApplications/data/default` is not saved.
- The directory `.../XMLApplications/data/custom` is saved and will either be restored or copied to `.../XMLApplications/data/custom_<old Version>`, dependent on the setting of **Administration** > **Backup/Restore** > **"Restore" Tab** > **Restore XML Application File too**.

  NOTE: If customizations have been made, these must be redone. For this, copy `.../XMLApplications/data/default` to `.../XMLApplications/data/custom` again or rename `.../XMLApplications/data/custom_old` to `.../XMLApplications/data/custom`
- The directories `.../XMLApplications/data/DeploymentService`, `.../XMLApplications/data/LocationService`, `.../XMLApplications/data/MakeCall`, `.../XMLApplications/data/NewsService` are saved and restored. These directories may not be changed by the user.

16.19 Deactivation of XML Push feature on Linux DLS

By default, Linux installation comes with **XML Push** enabled. However, if you want to disable this feature, you should follow these steps:

Go to:

1. Go to:

   ```
   /enterprise/share/tomcat/webapps/DeploymentService/database/
   ```

2. Run the following command:

   ```
   ./dlsconfig.sh set xml_apps_available 0
   ```

3. Restart Symphonia framework:

   ```
   /etc/init.d/symphoniad restart
   ```

This way, the **XML Push** feature will be deactivated.

16.20 Migration Scenarios

Migration scenarios include deployment change as opposed to Upgrade scenarios who refer to an installation of a new DLS version over a previous one by using the same deployment.

OpenScape Deployment Service supports the following scenarios :

- **Upgrade scenarios**

From	To
Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/ V7R3	Onboard DLS in Integrated Simplex V10
Windows DLS Single Node V6R1/V7R1/V7R2/V7R3	Windows DLS Single Node V10
Windows DLS Multi Node V6R1/V7R1/V7R2/V7R3	Windows DLS Multi Node V10

- **Migration scenarios**

  Starting with **CV438**, DLS V10 currently supports the following:

From	To
Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/ V7R3	Windows DLS Single Node V10
Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/ V7R3	Windows DLS Multi Node V10
Windows DLS Single Node V6R1/V7R1/V7R2/V7R32	Windows DLS Multi Node V10

16.20.1 Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/V7R3 to Windows DLS Single-Node V10

Backing Up DLS Database Data for Onboard DLS in Integrated Simplex

1. Close all browser windows connected to the DLS.
2. End DeploymentService on the Onboard DLS in Integrated Simplex by executing the command "`./` symphoniad stop" under `/etc/init.d/ directory`
3. Execute the command “sh dbexport.sh /tmp/filename.zip” under `/enterprise/share/tomcat/webapps/DeploymentService/database.`

   This will export the DLS dB under `/tmp` directory path or choose another directory path and archive it in the “filename.zip” file.
4. Start Deployment Service on the Onboard DLS in Integrated Simplex by executing the command "./ symphoniad start" under `/etc/init.d/ directory.`

Migrating the DLS Database Data to the Windows DLS Single-Node

1. Fresh install Windows DLS V10 Single-Node.
2. Copy the file “filename.zip” to the folder:
   `[Installation path]\DeploymentService\Tomcat\webapps\DeploymentService\database\`
3. Close all browser windows connected to the DLS.
4. End DeploymentService on the DLS server by clicking **Start** > **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
5. In order to migrate the DLS data, execute the following command on Command Prompt (run as administrator) :

   ```
   [Installationpath]\DeploymentService\Tomcat\webapps\DeploymentService\database\
   migrate.bat filename.zip
   ```

6. Start Deployment Service on the DLS server. Do this by clicking **Start** >**Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

16.20.2 Onboard DLS in Integrated Simplex V6R1/V7R1/V7R2/V7R3 to Windows DLS Multi-Node V10

Backing Up DLS Database Data for the Onboard DLS in Integrated Simplex

1. Close all browser windows connected to the DLS.
2. End DeploymentService on the Onboard DLS in Integrated Simplex by executing the command "./symphoniad stop" under `/etc/init.d/ directory`
3. Execute the command “sh dbexport.sh /tmp/filename.zip” under `/enterprise/share/tomcat/webapps/DeploymentService/database`

   This will export the DLS dB under `/tmp` directory path or choose another directory path and archive it in the “filename.zip” file.
4. Start Deployment Service on the Onboard DLS in Integrated Simplex by executing the following command "./symphoniad start" under `/etc/init.d/ directory`

Migrating DLS Database Data for the Windows DLS Multi-Node

The following example demonstrates the migration of a Multi Node with two (2) DLS Nodes:

1. Fresh install Windows DLS V10 Multi-Node system.
2. Copy the file “filename.zip” to the first DLS node under the folder:
   `[Installationpath]\DeploymentService\Tomcat\webapps\DeploymentService\database\`
3. Close all browser windows connected to the DLS.
4. End Deployment Service on DLS server for both Nodes by clicking **Start** > **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.

5. To migrate the DLS data, execute the following command on Command Prompt (run as administrator) for the first DLS Node :

   ```
   [Installationpath\DeploymentService\Tomcat\webapps\DeploymentService\database\
   migrate.bat filename.zip
   ```

6. Start Deployment Service on DLS server for both Nodes by clicking **Start** > **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

16.20.3 Windows DLS Single-Node V6R1/V7R1/V7R2/V7R3 to Windows DLS Multi- Node V10

Backing Up DLS Database Data for the Windows DLS Single-Node

1. Close all browser windows connected to the DLS.
2. End DeploymentService on DLS server by clicking **Start** > **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
3. In order to backup the DLS data, execute the following command on Command Prompt (run as administrator) for the DLS Single Node :
   ```
   [Installationpath\DeploymentService\Tomcat\webapps\DeploymentService\database\
   dbexport.bat filename.zip
   ```
   This will export the DLS dB and archive it in the filename.zip file.
4. Start Deployment Service on DLS server by clicking **Start** > **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

Migrating DLS Database Data for the Windows DLS Multi-Node

The following example demonstrates the migration of a Multi Node with two (2) DLS Nodes:

1. Fresh install Windows DLS V10 Multi-Node system.
2. Copy the file “filename.zip” to the first DLS node under the folder:
   ```
   [Installationpath]\DeploymentService\Tomcat\webapps\DeploymentService\database\
   ```
3. Close all browser windows connected to the DLS.
4. End DeploymentService on DLS server for both Nodes by clicking **Start** > **Programs** > **Deployment Service** > **Stop Service** in the Windows Start menu.
5. To migrate the DLS data, execute the following command on Command Prompt (run as administrator) for the first DLS Node :
   ```
   [Installationpath]\DeploymentService\Tomcat\webapps\DeploymentService\database\
   migrate.bat filename.zip
   ```
6. Start Deployment Service on DLS server for both Nodes by clicking **Start** > **Programs** > **Deployment Service** > **Start Service** in the Windows Start menu.

NOTE: When database mirroring is active for a Windows DLS Multi-Node, no migration of backups is possible.

NOTE: In order to execute the "migrate.bat" command you should run the Command Prompt as administrator (UAC windows feature).

NOTE: Nearly all data is wiped out on the target DLS installation if present.
Only the following data is conserved when data is migrated on the target load:
- configuration of license server (this is to avoid consuming all licenses on the license server when a second DLS with same data is started)
- configuration of localized data which needs to be adopted to the current installation, e.g. trace file directories.

NOTE: Due to enhancement changes in V6R1, from **CV111.00** onwards the database representation of the languages for the batch file, snmp and e-mail alarms has been swapped.
Therefore, in a migration attempt from any DLS (either Linux or Windows) **CV110.00** or earlier to a **CV111.00** or later, expect the above mentioned alarm language configuration to be swapped (i.e. German will be English and English will be German).

An IP adaptation must follow for a successful migration since the newly introduced DLS server will now hold a new IP address. The procedure is described in the following paragraph:

16.20.3.1 Subsequent IP adaptation

DLS uses all enabled LAN interface cards of the server it is installed on. When changing the IP address of a LAN card (or replacing DLS server hardware), or applying a migration procedure, the following actions must take place:

1. DLS must be restarted.
2. All DLS objects using the old IP address must be adapted, which includes DLS address in SCAN objects and FTP Server address in case an FTP Server is installed on DLS host.
3. All devices and applications which communicate with DLS must be reconfigured:
   - **Phones configured via DHCP**: adapt DHCP server, the phones will use the new DLS address after DHCP lease timed out. Since the lease may never time out, this may be a time-consuming action, it is therefore recommended to:
     – *restart all phones* (outside business hours) - this will take some time and when all jobs are finished, check failed jobs and/or search for all phones which are still configured for the old DLS IP address. Either retry or resolve manually the problem, i.e. in case the phone is switched off.
   - **Phones not configured via DHCP**: manually set the new IP address using DLS **before** the IP is changed or scan these phones using the new IP address.

- **Gateways, HiPath 4000 Manager, HiPath 8000 Assistant, HiPath QoS**: manual reconfiguration of DLS address using the individual mechanisms of these products. As an example, reconfigure the DLS parameters inside CMP to reflect the new IP address of the DLS Server.

16.20.4 DLS Multi-Node Systems with Database Mirroring Operating System Upgrade/Migration Procedure

This process is designed so that the upgrade/migration of the operating system is executed within the minimum possible downtime for the DLS service.

Requirements

Make sure of the following :

- All devices, browsers and API clients are configured to use the Cluster IP and not the DLS Node IP's
- No administrative tasks are allowed during the time that this procedure lasts. The functionality that is guaranteed to work – with the exception of the outage period, where the service is stopped – is mobility and device registration. Administrative tasks that are automatically triggered should also be disabled (e.g. Element Manager Synchronization, Plug &Play)
- All scheduled jobs must be deleted or cancelled before starting this process
- All GUI browser sessions are logged off
- If DCMP is installed on the DLS nodes, each node must have a DCMP instance configured in cluster mode, as the DLS Admin Guide describes (see Section 4.4.2,Step 3). If the DCMP is on an external system, it will not be affected.
- Have the DLS Admin Guide in handy. All installation and configuration steps below should be done according to the OpenScape Deployment Service Admin Guide.

Abbreviations about the involved machines

Front End 1 (FE1): This is the computer designated as DLS Node 1 of the DLS Cluster.

Front End 2 (FE2): This is the computer designated as DLS Node 2 of the DLS Cluster.

Back End 1 (BE1) : This is the computer designated as Database Server having the Principal Role which is configured during the installation of the system. If any fail-over has occurred since the installation of the system, **BE1** might have changed to the Mirror Role. **BE1** is the system that was intended to be the Database Server with the Principal Role during the initial installation of the system.

Back End 2 (BE2) : This is the computer designated as Database Server having the Mirror Role. Look above (**BE1**) for clarifications.

Back End 3 (BE3): This is the computer designated as the Database Witness Server.

For abbreviations and additional information,you can also refer to Section 17.1, "Abbreviations and Technical Terms"

Prerequisites

- A DLS Multi-Node environment in a working state.
- The DLS Common Data folder to be located on an external computer (not in **FEx** or **BEx**).

- The CLA to be located on an external computer (not in **FEx** or **BEx**).

Proceed with the following steps :

1. Preparation of database servers
   a) Check if **BE2** has the Principal Role - if yes skip to step d.
   b) Perform manual database failover using SQL Server Management Studio (the mirror database server will become the principal database server and the principal database server will become the mirror database server)
   c) Verify that **FE2** is in functional state. Try to login directly to **FE2** GUI (not virtual IP) and check if login process completed successfully.
   d) Disable the Database Mirroring using the Microsoft SQL Management Studio
2. Shutdown of **FE1** & **BE1**& **BE3**
   NOTE: **BE3** (Witness Server) is optional; therefore it is not used by all configurations.In the case where the **BE3** does not exist, skip instructions targeting **BE3**.
   a) Shutdown **FE1**, **BE1** & **BE3**
   b) Verify that **FE2** has gained master role and the DLS service is operational by logging in using the Virtual Cluster IP
   c) Remove **FE1** from Load Balancer's network configuration
   - For Microsoft NLB: NLB is automatically disabled when the DLS service is stopped (already done in step a). Verify in the NLB Management Console from **FE2** that **FE1** appears in red and **FE2** remains converged.
   - For external Load Balancer: Configure the external Load Balancer as appropriate.

   NOTE: At this point the DLS Cluster does not support High Availability nor Load Balancing, however, the DLS service is still available from **FE2** and **BE2**.
3. Installation of Windows Server 2008 R2
   a) Installation of Windows Server 2008 R2 + Service Packs on **FE1**, **BE1** and **BE3**.
   b) Network configuration of **FE1**, **BE1** and **BE3**.
   c) Installation of the Microsoft NLB (if an external Load Balancer is used,skip this step).
   - Install the Microsoft NLB on **FE1** by adding it as a feature from the Server Manager.

   IMPORTANT: DO NOT proceed with the NLB configuration to create a cluster.
   d) Install and configure the Windows FTP Server on **FE1** as appropriate (skip this step if Windows FTP Server is not used).
   e) Installation of SQL Server Native Client 2008 R2.

4. Installation of SQL Server 2008 R2 on **BE1** & **BE3**
5. Installation of DLS on **FE1**

    a) Create a new Common DLS Data folder

    NOTE: The folder should be granted with respective permissions. Do NOT use Common DLS Data folder of previous installation.

    - The Common DLS Data folder is recommended to be located on **BE3** or on an external computer and certainly NOT in the computer where CLA is installed.

    b) Installation of DLS on **FE1**

    - Use the exact same configuration as the old system. If DCMP was installed, install DCMP on this new system as well.
    - Do NOT install a hotfix directly. Instead first install the base version of the hotfix and then upgrade to the hotfix (e.g. the base version of **V6 R1 127.05** is the **V6 R1 127.00**).

    c) Stop the DLS service on **FE1**

6. Database Migration

    a) Backup the DLS database from **BE2** – Through DLS GUI proceed with backup. Verify that backup file is saved on a network path accessible from **FE1** – **BE1**. (e.g. on **BE3**)

    NOTE: From the time when the backup procedure is started and after, all actions – requests sent to DLS will NOT be restored to the new installation.

    IMPORTANT: From this point the DLS service will be unavailable

    b) Stop the DLS service on **FE2** – If Microsoft NLB is used,then check on NLB Management that the Console host for **FE2** is stopped. If not ,then stop host manually on NLB.

    - Remove **FE2** from Load Balancer's network configuration.
    - For Microsoft NLB: NLB is automatically disabled when the DLS service is stopped (already done in step b).
    - For external Load Balancer: Configure the external Load Balancer as appropriate

    c) Uninstall, Re-Install CLA and then activate licenses for DLS.

    NOTE: In case there are other products which use the same CLA then it is mandatory to additionally activate licenses for these products

    d) Restore the DLS database to **BE1**. Through DLS GUI proceed with restore. Verify that the backup file is saved on a network path accessible from **FE1** and **BE1**

7. NLB Configuration and start of the new cluster

    a) Configure Load Balancer's network configuration for **FE1**.

    - Create the Cluster using the same IP and configuration as in the old system.
    - For Microsoft NLB: Add **FE1** to the Cluster. Using NLB Manager Console, select "Create New Cluster" and proceed with the new Cluster with Host 1 = **FE1** and Cluster IP = Virtual IP.

- For external Load Balancer: Configure the external Load Balancer as appropriate.

b) Start DLS on **FE1**

c) Verify that the new DLS installation is operational by logging in using the Virtual IP of the system.

NOTE: From this point on the DLS service will be available again, serving from the newly installed Windows Server 2008 R2 system.

8. Installation of Windows Server 2008 R2

   a) Installation of Windows Server 2008 R2 on **FE2** and **BE2**

   b) Network configuration of **FE2** and **BE2**.

   c) Installation of the Microsoft NLB (if an external Load Balancer is used,skip this step).

   - Install the Microsoft NLB on **FE1** by adding it as a feature from the Server Manager.

   IMPORTANT: DO NOT proceed with the NLB configuration to create a cluster.

   d) If a FTP server used for file deployment was installed on **FE2**, install, configure & test the FTP service on Windows.

9. Installation of SQL Server 2008 R2 on **BE2**
10. Setup Database mirroring between **BE1**, **BE2** and **BE3** according to the Admin Guide
11. Installation of DLS on **FE2**

    a) Use the exact same configuration as the previous system. If DCMP was installed, install DCMP on this new system as well.

    b) Do NOT install a hotfix directly.Instead, install the base version of the hotfix first,and then upgrade to the hotfix (e.g. the base version of **V6 R1 127.05** is the **V6 R1 127.00**).

    c) Verify that DLS login is possible using the **FE2** IP (not the Cluster IP).

    d) Configure Load Balancer's network configuration for **FE2**.

    - For Microsoft NLB: Add **FE2** to the Cluster. Using NLB Manager Console, connect to the existing cluster and then add **FE2** as host on the Cluster.
    - For external Load Balancer: Configure the external Load Balancer as appropriate.

12. Verify that DLS login is possible using the Virtual IP of the cluster.

    a) Enable any automated administrative tasks that were disabled before the migration procedure (e.g. Element Manager Synchronization, P&P)

    b) Activate any scheduled jobs that were cancelled before the migration procedure

The upgrade/migration is complete. The DLS Cluster should be operational again, without any data loss.

The IP and MAC assignments of the computers as well as the DLS Node’s order within the Cluster and the Database Mirroring should be unaffected.

16.21 Syslog Configuration for Event (and security) logging

Refer to the following steps:

1. Navigate to Main Menu > Administration > Alarm Configuration.Enable the **Syslog** checkbox.
2. Under Alarm Configuration > „Syslog“ Tab, provide the Syslog server IP, port (default is 514), facility (e.g. local0), Severity (e.g. alert) values.
3. Under Alarm Configuration > "Alarm Classes" Tab, enable the required alarm classes in column 'Syslog' (optional, depends on requirements)
4. Navigate to Main Menu > Administration > Display Logging Data > Audit and Security Log > "Configuration" Tab. At minimum enable **Syslog Audit Logging** checkbox.
5. Enable **DLS Audit Log** and '**DLS Security Log** checkboxes.
6. Depending on your requirements select logging areas of interest of field **Additional Audit Log settings** under Main Menu > Administration > Display Logging Data > Audit and Security Log > "Configuration" Tab.

16.22 Automatic certificate renewal

The '*PKI Configuration Connector*' can be configured to automatic renew the certificates, which has been requested using this connector and are soon running out.

Before you configure an automatic certification renewal, make sure that the connector configuration used for requesting and deploying the old certificate is available for this device.

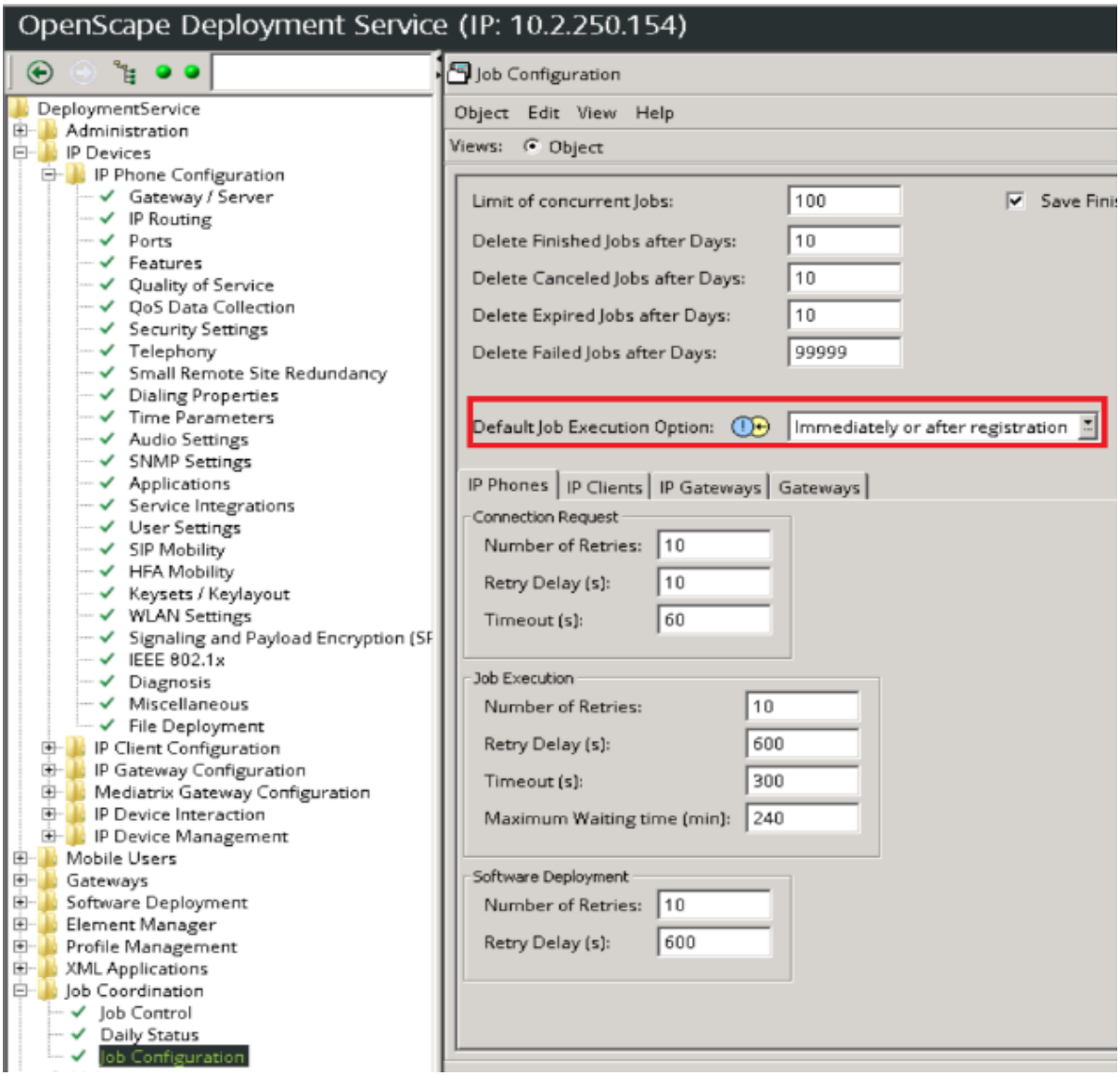
If not, you will not be able to configure the necessary settings to request a new certificate. In this case, and if there is no global renewal configuration available, an alarm will notify you to configure the certificate renewal manually.

NOTE: Automatic renewal is supported for the following certificates:

- Phone Certificate
- WBM Certificate
- SPE Certificate
- 802.1x Certificate
- Client WPI Certificate (in secure communication)
- DLS Server WPI Certificate (in secure communication)

16.22.1 How to set up an automatic certification renewal

1. Configure **Default Job Execution Option** (optional)
   a) Call: Main Menu > Job Coordination > Job Configuration



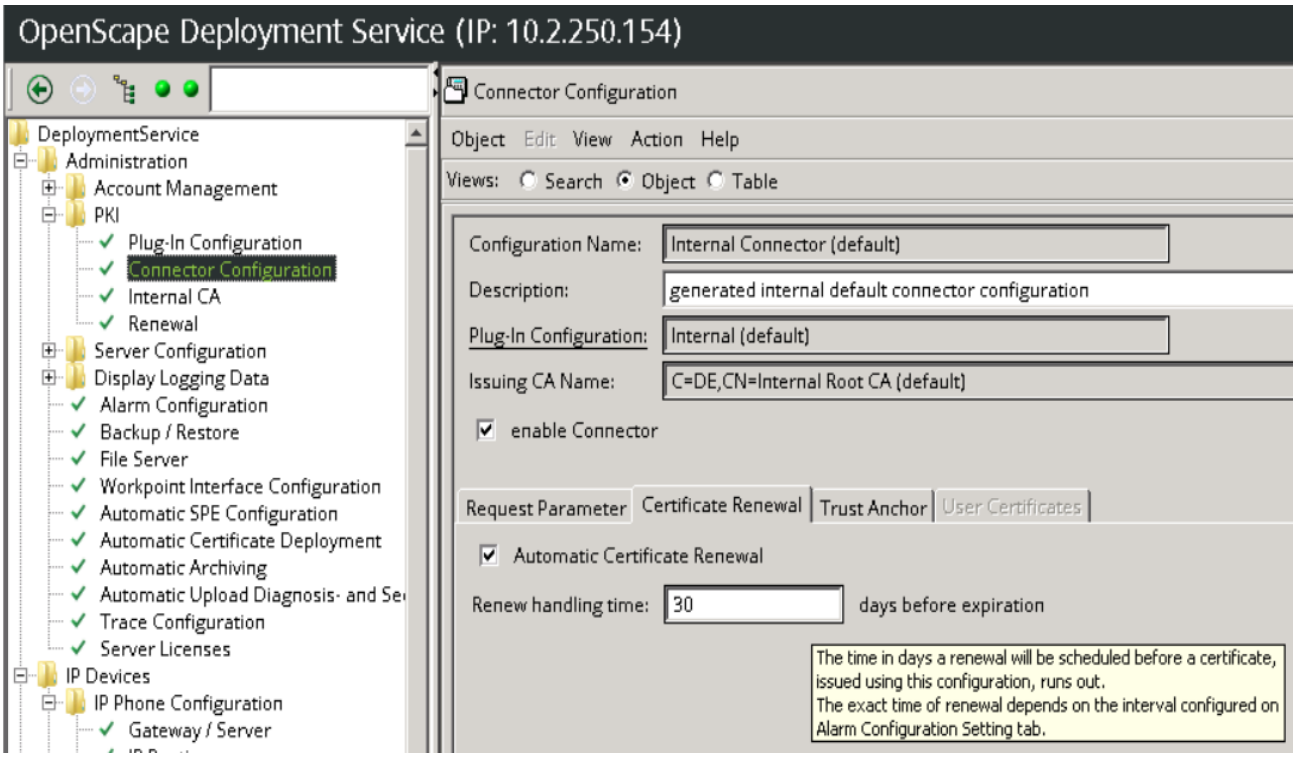
By default the **Default Job Execution Option** is set to **Immediately**. The jobs that are created are executed immediately.

In case the device is unreachable, the job will eventually expire and the configuration change will never be sent to the device.

b) To prevent job expirations, it is suggested to configure the **Default Job Execution Option** to **Immediately or after registration**. As a result, in case the connection to the device cannot be established, the configuration change will be sent to the device after the next registration.

2. Activate **Automatic Certificate Renewal**

   a) **Call:** Main Menu > Administration > PKI > Connector Configuration > "Certificate Renewal" Tab

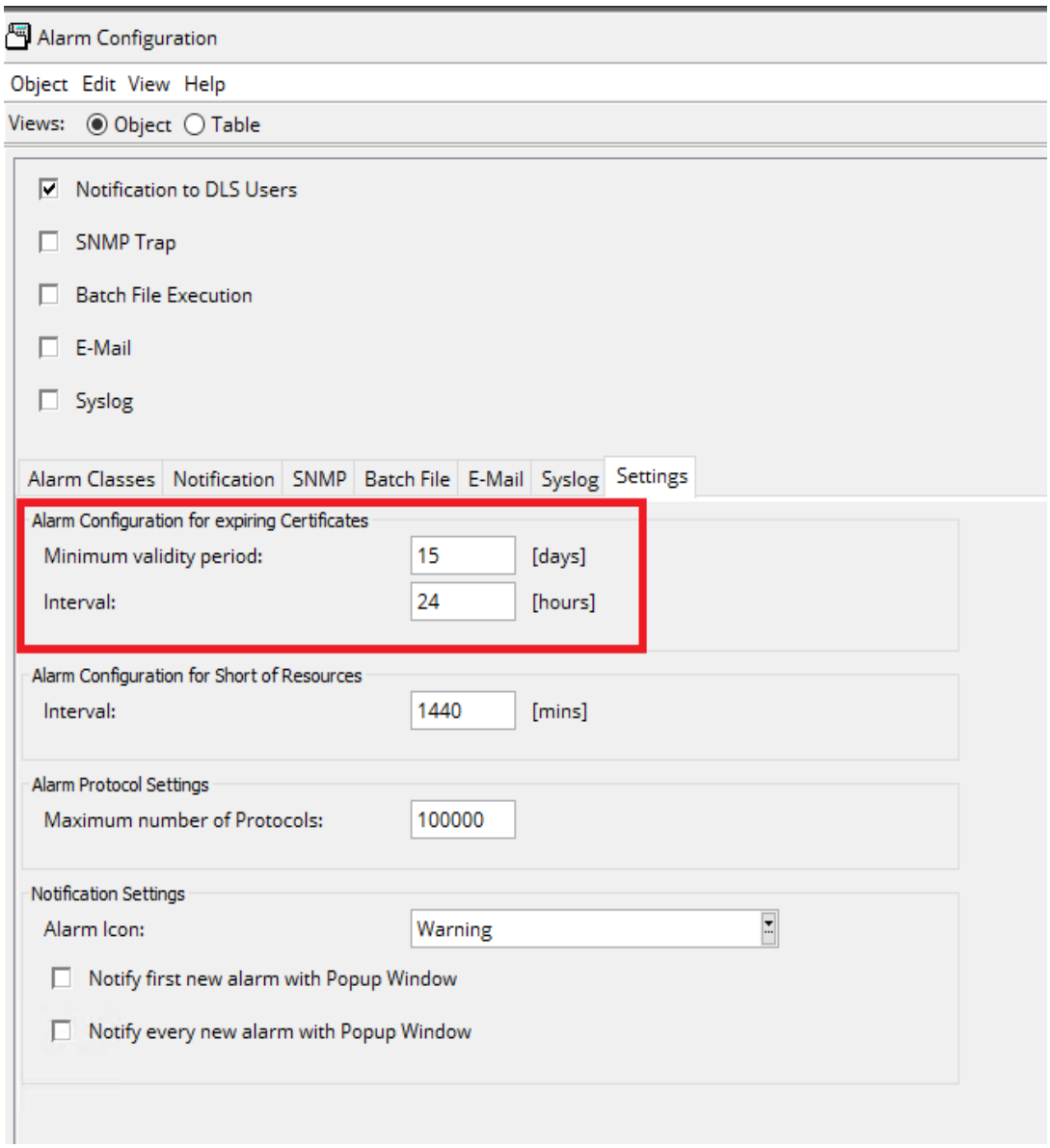


   b) Check the **Automatic Certificate Renewal** checkbox.

   c) In the **Renew handling time** field**,** enter the time in days a renewal will be scheduled before a certificate expiration. As an example, in the above image it is shown that a certificate renewal is scheduled 30 days before its expiration.

3. Set up the **Alarm configuration** (optional)

   a) **Call:** Main Menu > Administration > Alarm Configuration > Settings



Alarm Configuration for expiring Certificates

   b) In the **Minimum validity period** field, enter the time in days an alarm will be raised before a certificate expiration. As an example, a **Minimum Validity Period** of 15 days ensures that an alarm will be raised if the certificate has not been renewed 15 days before the expiration.

c) In the **Interval** field, enter the time in hours to configure the interval between two subsequent certificate expiration checks. As an example, an **Interval** of 24 hours ensures that the server is set to check the certificate renewals once per day. The default check runs once per 6 hours.

NOTE: Renewing certificates before the expiry date is important. Therefore, it is suggested to set the **Renew handling time** earlier than the **Minimum validity Period**.

In case an automatic renewal fails, the alarm notifies the administrator to configure a certification renewal manually.

16.22.2 Scenarios

This section presents scenarios which are based on the server configuration described in Section 16.22.1, "How to set up an automatic certification renewal".

16.22.2.1 Client WPI certificate renewal (in secure communication)

Normally, no manual action is needed to renew the **Client WPI certificate:**

1. Device is in secure mode.

2. Device’s certificate is soon running out.

3. According to the **Activate automatic renewal** configuration, a certificate renewal job will be created 30 days before the certificate expiration.

4. The **Default Job Execution Option** is set to **Immediately or after registration;** that means that the server will try to execute the job immediately. If the connection to the device cannot be established, the configuration change will be sent to the device after the next registration.

5. In case the certificate renewal fails, an alarm will be raised 15 days before the certificate expiration. In that case the administrator needs to renew the certificate manually, before the certificate expiry date.

16.22.2.2 Server WPI certificate renewal (in secure communication)

Normally, no manual action is needed to renew the **Server WPI certificate**:

1. Server’s certificate is soon running out.

2. According to the **Activate automatic renewal** configuration, the server's certificate will automatically be renewed 30 days before the certificate expiration.

NOTE: Device's should not be informed for that change.The new server certificate can still be validated by the certificate authority (CA) that had been sent to devices during bootstrap.

In case the certificate renewal fails, an alarm will be raised 15 days before the certificate expiration. In that case, the administrator needs to renew the certificate manually, before the certificate expiry date.

16.22.2.3 Phone/WBM/SPE/802.1x certificate renewal

Normally, no manual action is needed to renew the **Phone/WBM/SPE/802.1x** certificate**:**

1. The corresponding certificate is soon running out.

2. According to the **Activate automatic renewal** configuration, a certificate renewal job will be created 30 days before the certificate expiration.

3. The **Default Job Execution Option** is set to **Immediately or after registration.** That means the server will try to execute the job immediately. In case the connection to the device cannot be established, the configuration change will be sent to the device after next registration.

4. In case the certificate renewal has not succeeded, an alarm will be raised 15 days before the certificate expiration. In that case, the administrator needs to renew the certificate manually, before the certificate expiry date.

16.22.2.4 How to configure Issuing Certificate Authority (CA) replacement

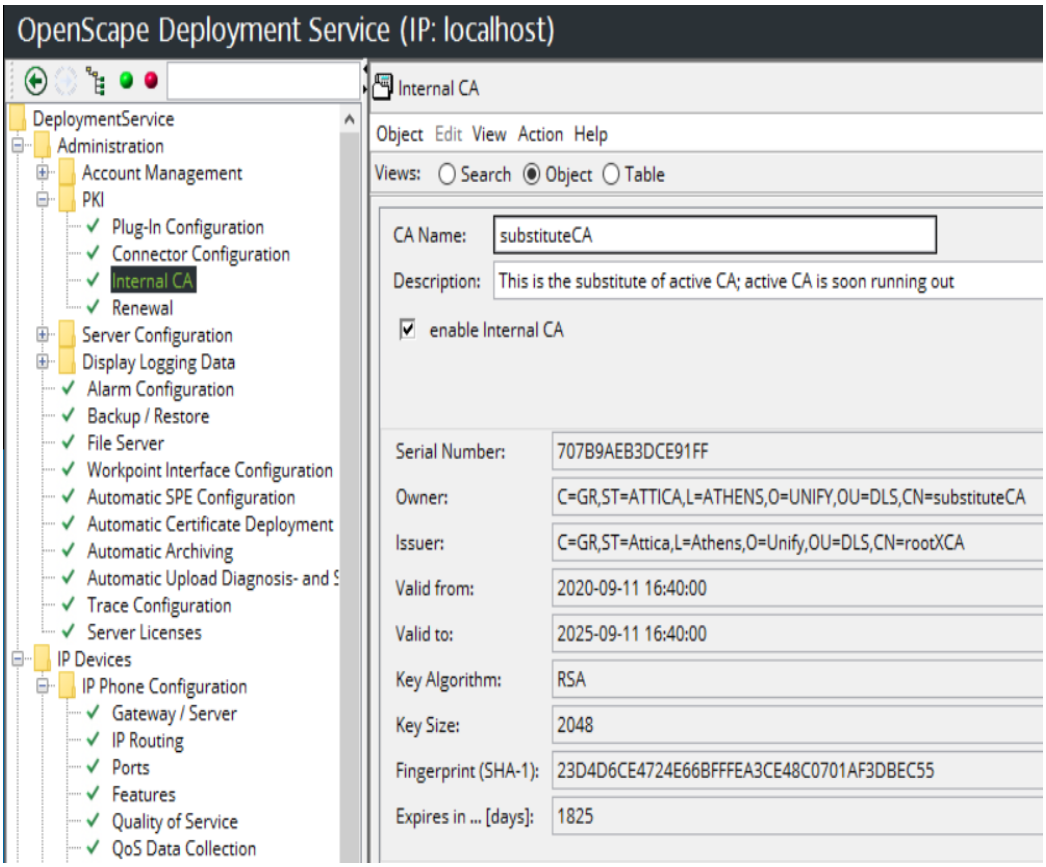
This section describes how to configure an **Issuing Certificate Authority replacement** manually, in case it needs to be replaced (e.g. is soon running out[1], is compromised etc.).

Set up PKI Configuration

1. Import the substitute CA to the server.

1 Renewing certificates before the expiry date is important in order to ensure that the certificate replacement will be completed on time.

a) **Call:** Main Menu > Administration > PKI > Internal CA



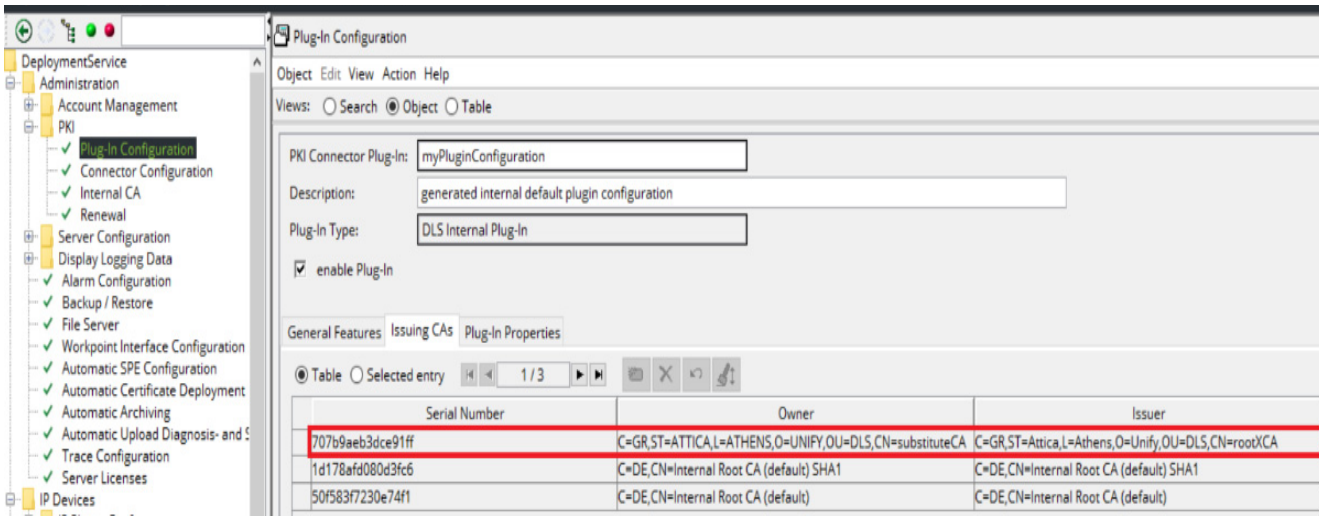
b) Edit the **CA Name** field to create a new entry (e.g. substituteCA).

c) Import the **substituteCA** from its PKCS#12 file.

d) Check the **enable Internal CA** box to activate it.

2. Synchronize the Plug-in Configuration.

a) **Call:** Main Menu > Administration > PKI > Plug-In Configuration

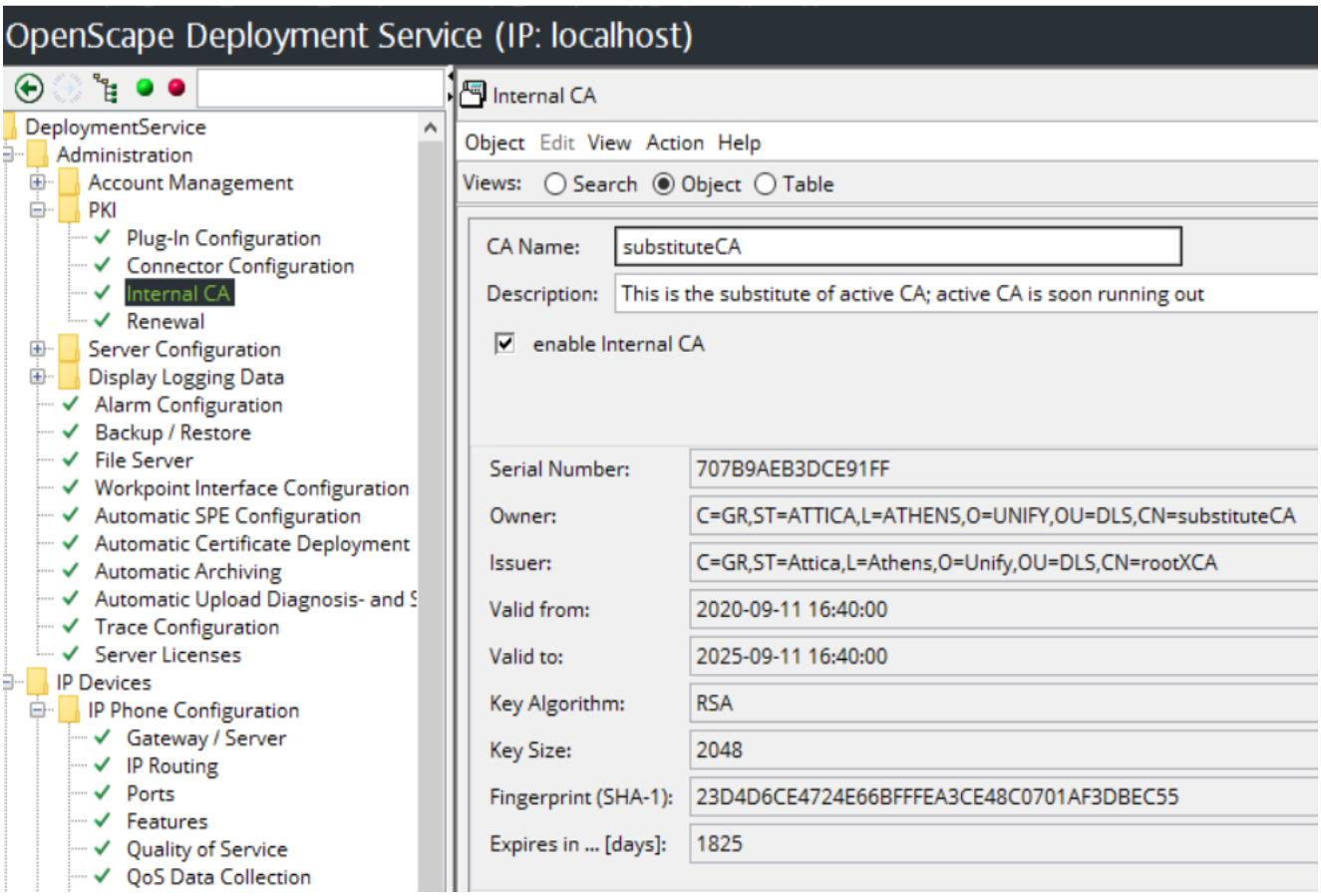


b) Select the **Plug-in Configuration** of the Connector Configuration of the CA to be replaced and press **Synchronize.**

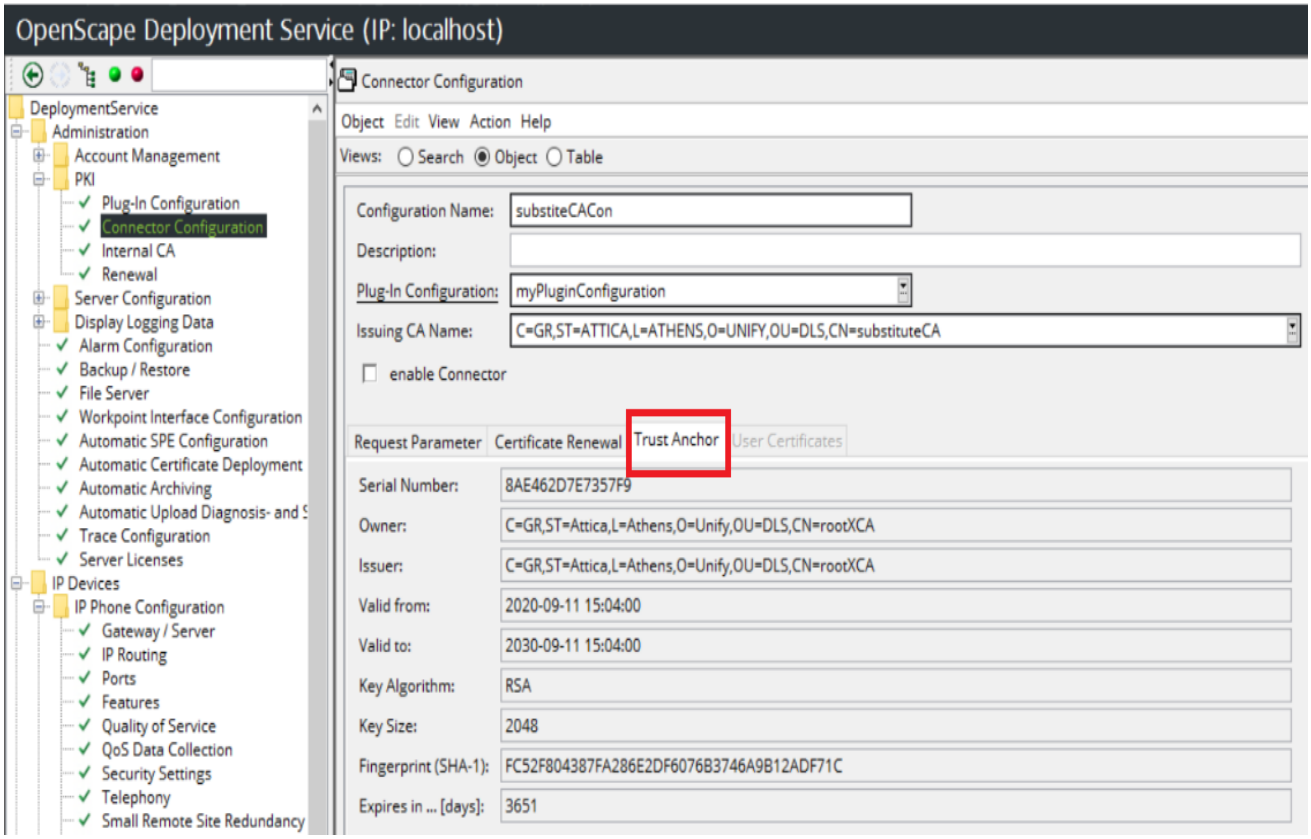
c) The new **Internal CA** should be added to the **Issuing CAs** tab.

3. **Create and activate a new Connector Configuration.**

a) **Call:** Main Menu > Administration > PKI > Internal CA



b) Enter the substitute CA in the **CA Name** field.



c) Use as Trust Anchor, the issuer of the substitute CA.

16.22.2.5 PKI Activation/Replacement.

The replacement of the existing PKI Connector is ready to be used. The administrator needs to activate it to various interfaces.

Client WPI Credentials

Call: Main Menu > Administration > Workpoint Interface Configuration

- In the **Client credentials** section:
  - Update the **PKI Configuration** with the replacement connector and **Save** the change.
  - Click **Create** to create an additional client certificate. After creation, each device contacting DLS using an old client credential will be sent a new one.

NOTE: In order for DLS server to be able to trust a contacting device with an old certificate, the ‘old’ issuing CA should not be deleted. The ‘old’ issuing CA can be deleted only after all the devices have been updated with the new client credentials. Otherwise, DLS will reject the device’s request.

Server WPI Credentials

Call: Main Menu > Administration > Workpoint Interface Configuration

- In the **Server credentials** section:
  - Update the **PKI Configuration** with the replacement connector and **Save** the change.
  - Click **Create** to create, but not activate yet, an additional server certificate.This certificate will be issued from the replacement connector enabled in the previous step.
  - Click **Deploy** to send the server credentials to the devices which are in secure mode. At that step DLS creates one job [1] for each device to deploy the new server credentials [2].
  - Click **Activate** to enable the additional server certificate. After activation, the devices which have not yet acquired the server’s credentials, will reject DLS requests [1].

1 Before the **Activate** action, the administrator must ensure that all the devices have the server’s credentials and that the jobs have been successfully completed.
2 During that job execution DLS sends to the devices the **Trust Anchor** of the Server Certificate Issuing CA. As a result, the device can trust the updated server certificate.

17 Appendix

The appendix contains abbreviations and additional information.

17.1 Abbreviations and Technical Terms

For more information on network technology and Voice over IP (VoIP), refer to the relevant reference material.

> ***NOTE:*** For definitions of the terminology related to the mobility feature, see Section 3.8.1, „Mobility Definitions“.

EA

Abbreviation for "**E**xternal **A**ccess".
If appropriately configured, the external access must precede a phone number if this number is an external phone number. See also Canonical format.

AMO

Abbreviation for "**A**dministration and **M**aintenance **O**rder".
An order which directly provides the CBX (**C**omputerized **B**ranch **E**xchange) with administration or maintenance information. An AMO is transmitted via EMML (Extended Machine Maintenance Language).

ANAT

Abbreviation for "**A**lternative **N**etwork **A**ddress **T**ype" in SIP.

ASCII code

Standardized character set for representing and processing text in computers and communication systems (see ASCII tables on the following pages).

ASCII Table (Standard)

Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)
	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 Table (Enhanced)

Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)	Character	ASCII (hex)	ASCII (dec)
_	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	Ð	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

PU

Abbreviation for "Call **P**ick**u**p".
If you have one workpoint in an office and another in a lab and want your contacts to be able to reach you at a single subscriber number, you can create a pickup group containing both workpoints. The workpoint called rings. The call can be accepted. The "call pickup" LED also flashes on the other workpoint. You can answer the call by simply pressing the appropriate button.

BE1

Abbreviation for "**B**ack **E**nd **1**".
This is the computer designated as Database Server having the Principal Role which is configured during the installation of the system. If any fail-over has occurred since the installation of the system, BE1 might have changed to the Mirror Role. BE1 is the system that was intended to be the Database Server with the Principal Role during the initial installation of the system.

BE2

Abbreviation for "**B**ack **E**nd **2**".
This is the computer designated as Database Server having the Mirror Role. Look above (BE1) for clarifications.

BE3

Abbreviation for "**B**ack **E**nd **3**".
This is the computer designated as the Database Witness Server.

C-SWS

Abbreviation for "**C**entral **S**oft**w**are **S**upply Server".
Name of the central software supply server in Brussels.

CA

Abbreviation for "**C**ertification **A**uthority".

CAP

Abbreviation for "**C**ommon **A**pplication **P**latform".

CAT NetInstall

In Germany, you can use CAT NetInstall for installation on ⑦ TAP.

CD

Abbreviation for "**C**all **D**eflection".
ISDN feature for call deflection in ringing state.

CF

Abbreviation for "**C**all **F**orwarding".
ISDN feature for automatic call forwarding.

The following types of call forwarding exist:

- **CFU**
  Call **F**orwarding **U**nconditional (immediate call forwarding)
- **CFNR**
  Call **F**orwarding **N**o **R**eply (forward call if no reply)
- **CFB**
  Call **F**orwarding **B**usy (forward call if busy)

CLA

Abbreviation for "**C**ustomer **L**icense **A**gent".
The HLM component that encrypts the licenses for the product and assigns them to the relevant products.

CLI

Abbreviation for "**C**ommand **L**ine **I**nterface".
Operating network devices by entering data in a command line. This interface is usually password-protected and is reached via Telnet.

CLM

Abbreviation for "**C**ustomer **L**icense **M**anager".
The HLM component that administers HiPath product licenses for the customer.

CSV

Abbreviation for "**C**omma-**S**eparated **V**alues".
File with tabular data. In some cases, the column labels are entered in the first line. In general, a column is set off by a semicolon or comma, and a line change is indicated by the start of a new line. Can be imported with Microsoft Excel, for example.

CTI

Abbreviation for "**C**omputer **T**elephony **I**ntegration".
CTI uses computer technology to support telephone services. It not only supports the varied attendant functions associated with service features but also system management and accounting.

CTS

Abbreviation for "**C**lear **T**o **S**end".
Clear to send is an interface function signal. It is part of modem control in handshake mode and is also used for access authorization in the CSMA/CA procedure. In this procedure (which is also used in WLANs with 802.11), a station that wants to send data transmits an RTS (Ready To Send) packet. If the transmission route to the receiver is clear, the station receives a CTS packet.

CW

Abbreviation for "**C**all **W**aiting".
ISDN feature for signaling the arrival of more calls during a call.

DBFS

Abbreviation for "**D**ata**b**ase **F**eature **S**erver".
Manager for the HiPath 3000/5000 communication platform.

Default Route

A default route is a route that is suitable for each target address. This means that the route can be used for all target addresses. The default route has the lowest priority and is only used if no other routes match. A route essentially determines which path the packets should or can take for transport in the network – if no path is prescribed or known, the default route is used.

DCMP

Abbreviation for "**D**LS-**C**ontact-**M**e-**P**roxy". The DCMP acts as a proxy for routing between the DLS and devices when a firewall or NAT prevents the DLS from sending Contact-Me messages to the devices. The DCMP can communicate with the DLS over the firewall or NAT and is polled regularly by the devices for messages from the DLS. If messages are present, the DCMP creates a connection between the device and the DLS. The DLS can then send control and configuration data to the device.

DHCP

Abbreviation for "**D**ynamic **H**ost **C**onfiguration **P**rotocol".
Dynamic assignment of IP addresses for stations in an IP network using a central DHCP server.

DLS

Abbreviation for "**O**penScape **D**eployment **S**ervice".
The DLS is an OpenScape Management application for administering IP devices (IP phones, IP client installations, and IP gateways) in HiPath and non-HiPath networks.

DMC

Abbreviation for "**D**irect **M**edia **C**onnection".
Workpoints that use signaling to establish connections via a switching element (for example, a gateway) also usually transmit reference data via this switching element. If both workpoints use the same signaling protocol and the same type of reference data transmission, switching via the gateway can be used to directly exchange reference data between the two workpoints. This direct exchange of reference data is referred to as "**D**irect **M**edia **C**onnection".

DNS

Abbreviation for "**D**omain **N**ame **S**ervice".
The DNS service converts an alphanumeric name query (such as www.unify.com/us/) into an IP address.

The large primary name servers at InterNIC and the national registration agencies (such as, en-NIC for Germany) have database servers for this to assign the IP addresses to the host names.

Domain

A domain is a logical network of computers and can also be split up into subdomains. DNS servers are used for resolving domain names. An example of a domain name is www.microsoft.com, for example. In this case, the "." (period) stands for the ROOT of the DNS server, ".com" stands for the commercial top-level domain, ".microsoft" stands for the company and "www" stands for the computer. Domain names are resolved from right to left.

Downgrade

Installation of software with a version number that is lower than the one currently in use.

DSM

Abbreviation for "optiPoint **DIs**play **M**odule".
A key module for optiPoint workpoints which features a touchscreen and enhanced functions, such as phone book, browser, and Java programs.

DTMF

Abbreviation for "**D**ual-**T**one **M**ulti**f**requency".
This dual-tone procedure is used in phone systems for dialing. DTMF replaced the pulse-tone procedure used in older rotary-dial telephones and establishes connections quickly in communications networks. The DTMF signal consists of two tones which are generated by pressing the keys on a phone and transmitted to the switching center. These two tones are taken from a set of eight different tones. They are assigned to the lines (1, 4, 7, star) and rows (1, 2, 3) on a telephone keypad. The DTMF procedure can also be used to access menu-driven services (for example, answering machines, mailboxes) directly via a telephone keypad.

E.164

Standardized phone number according to the ITU's international numbering plan with a maximum of 15 digits. Normally composed of three parts: CC, **(C**ountry **C**ode), NDC (**N**ational **D**estination **C**ode) and SN (**S**ubscriber **N**umber).

EAP
Abbreviation for "**E**xtensible **A**uthentication **P**rotocol".

ECT

Abbreviation for "**E**xplicit **C**all **T**ransfer".
ISDN feature for call transfer during the call.

ENB

Abbreviation for "**E**lectronic **N**ote **B**ook".
A personal phone book in a display or application module.

EOR

Abbreviation for "**E**nd **O**f **R**ecord".
Describes the end of a data record or reporting interval.

EOS

Abbreviation for "**E**nd **O**f **S**ession".
Describes the end of a connection.

FE1

Abbreviation for "**F**ront **E**nd **1**".
This is the computer designated as DLS Node 1 of the DLS Cluster.

FE2

Abbreviation for "**F**ront **E**nd **2**".
This is the computer designated as DLS Node 2 of the DLS Cluster.

FTP

Abbreviation for "**F**ile **T**ransfer **P**rotocol".
Used for transferring files in networks, for example, for updating telephone software.

G.711

Audio protocol for uncompressed voice transmission based on the Pulse Code Modulation (PCM) procedure. Requires a bandwidth of 64 Kbps ("ISDN quality").

G.723

Audio protocol for compressed voice transmission. The quality is inferior to G.711 and G.729. Requires a bandwidth of approximately 6 Kbps.

G.729

Audio protocol for compressed voice transmission. The quality is inferior to G.711 and superior to G.723. Requires a bandwidth of approximately 8 Kbps.

Gatekeeper

A gatekeeper is a logical component of the H.323 standard that can be implemented as Windows or UNIX software, as a router option, or as a part of an MCU or a Gateway.

Gateway

A system (computer or module) that transmits data between different networks. Where necessary, gateways coordinate different protocols with each other, for example, IP network and ISDN network protocols. A gateway can also simultaneously comprise a Router.

H.323 standard

The standard consists of at least three of the following components:

- Terminals
- Gateways
- Gatekeeper
- Multipoint Control Units (MCUs)

HFA

Abbreviation for "**H**icom **F**eature **A**ccess" or "**H**iPath **F**eature **A**ccess".
Produces the connection using a gateway (for example, HG 1500 or HG 3530) between IP telephony and a PBX.

HLM

Abbreviation for "**H**iPath **L**icense **M**anagement".

HTTP

Abbreviation for "**H**yper**t**ext **T**ransfer **P**rotocol".
Protocol for transmitting data in IP networks.

INCA

Abbreviation for "**I**nterleaved **N**ative **C**ompiled **A**rchitecture".
Part of the software and hardware architecture of a workpoint.

IP

Abbreviation for "**I**nternet **P**rotocol".

IP address

Also called "IP" for short. Unambiguous address of a telephone in the network; both IPv4 and IPv6 can be used.

An IPv4 address consists of 4 number blocks, each between 0 and 255, separated by ".". Example:
1.222.44.123

An IPv6 address consists of 8 hexadecimal number blocks, separated by ":". Example:
2001:0db8:85a3:08d3:1319:8a2e:0370:7347
or, if not all blocks are used:
2000:1::3

IPSec

Abbreviation for "**I**nternet **P**rotocol **S**ecurity".

Jitter

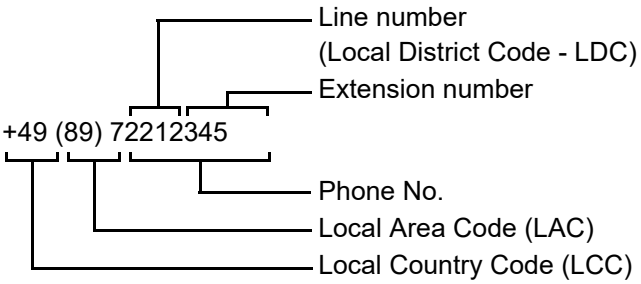
Runtime fluctuations during data transmission in IP networks.

JDBC

Abbreviation for "**J**ava **D**ata**b**ase **C**onnectivity".
JDBC is an interface that establishes a connection between a Java program and a database.

Canonical format

Example of a phone number in canonical format:



To dial phone numbers saved in canonical format, these must be made "dialable" using output rules or dialing properties. The various codes are recognized here as part of the phone number and, where applicable, replaced with the corresponding dial prefixes (see DP) or the external access code (see EA).

Examples of number resolution:

Phone number saved in canonical format:	LCC/IDP	LAC/NDP	LDC/EA	Phone number dialed
+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

Table 1 Examples of number resolution:

KDC

Abbreviation for "**K**ey **D**istribution **C**enter".

LAN

Abbreviation for "**L**ocal **A**rea **N**etwork".

Layer 2

Second layer (data link layer) in the seven-layer OSI model for describing data transmission interfaces.

The "network access protocol" in the LAN is found in layer 2. The layer contains the access mechanism (for example, CSMA/CD in the case of Ethernet) and MAC addresses.

Layer 3

Third layer (network layer) in the seven-layer OSI model for description of data transmission interfaces.

The network protocol, for example, IP (Internet Protocol) is found on layer 3. This can unambiguously transmit data packets based on the address. Devices that perform this task are called routers.

LDAP

Abbreviation for "**L**ightweight **D**irectory **A**ccess **P**rotocol".
Simplified protocol for access to standardized directory systems, such as, a company telephone book.

LCD

Abbreviation for "**L**iquid **C**rystal **D**isplay".
Display of numbers, text, or graphics, using liquid crystal technology.

LEAP

Abbreviation for "**L**ightweight **E**xtensible **A**uthentication **P**rotocol".

LED

Abbreviation for "**L**ight **E**mitting **D**iode".
Cold-light lamp with low energy consumption and various colors.

LLDP-MED

Abbreviation for "**L**ink **L**ayer **D**iscovery **P**rotocol - **M**edia **E**ndpoint **D**iscovery".

LOGO

A graphically designed image.

Mask

The subnet mask classifies networks into A, B, and C networks. Each class has a subnet mask that masks out the relevant bits. 255.0.0.0 for class A, 255.255.0.0 for class B, and 255.255.255.0 for class C. For example, 254 ⑦ IP addresses are available in a class C network.

MAC

Abbreviation for "**M**edium **A**ccess **C**ontrol **A**ddress".
A 48-bit address with which each terminal (for example, ⑦ IP telephone or network card) unambiguously identifies itself globally in a network.

MCU

An MCU (**M**ultipoint **C**ontrol **U**nit) makes conferences possible between three or more geographically discrete stations. The MCU acts as a kind of "star distributor", which connects the telephones (known as "commercial systems") to one another.

MD5

Abbreviation for "**M**essage **D**igest". The **5** stands for a new variant of the MD algorithm. MD5 is a pure hash algorithm and generates a unique checksum comprising 128 bits (16 characters) from any data length.

MDIX

Abbreviation for "**M**ultiple **D**ocument **I**nterface".
Allows users to display one or more documents in different views within a window.

MDI-X

Abbreviation for **M**edia **D**ependent **I**nterface crossover. Allows two network devices to be connected without using a crossover cable. If auto MDI-X is available, the MDI can automatically switch between normal connection assignment and crossover assignment, depending on the connected device.

MEB

Abbreviation for "**M**edia **E**xtension **B**ridge".

MIB

Abbreviation for "**M**anagement **I**Information **B**ase".
Database that contains descriptions and error messages for devices and functions in a network.

MoH

The file contains **M**usic **o**n **H**old (waiting melody).

MWI

Abbreviation for "**M**essage **W**aiting **I**ndicator".
Signals a new message, meaning one that has not yet been read or heard.

NAT

Abbreviation for "**N**etwork **A**ddress **T**ranslation".
The source NAT (source address) and/or the destination NAT are replaced by other addresses via a router, firewall or another network component. This translation usually occurs between two networks, for example between the local network and the Internet.

OCK

A fast roaming technology made possible by 802.11i is also referred to as "**O**pportunistic **K**ey **C**aching" or "Proactive Key Caching".
If multiple Access Points share PMKs (Pairwise Master Keys), it is possible that an IP Phone changes over to an access point it has not visited before without having performed pre-authentication. The PMK that has been used with the last access point is reused thereby.

Outbound Proxy

SIP proxy (=representative) that decides in the case of a dialed SIP-URI where the outgoing call is routed.

In the following example, the registrar server is in *dom1.com* and is resolved as the IP address *w.x.y.z*; *dom2.com* is resolved as *a.b.c.d*.

Dialed URI (before proxy)	Outbound Proxy			

Payload

That percentage of the IP data or of an IP data package that contains the user data, such as, the voice data in the VoIP .

PBX

Abbreviation for "**P**rivate **B**ranch E**X**change".
Private telephone system that connects different internal devices to the ISDN network.

PING

Abbreviation for "**P**acket **In**ternet **G**roper".
Program for testing whether a connection can be set up to a defined IP destination. During the test, data is sent to the destination and back again. The result that is output is the success or failure of the transmission and, if applicable, additional information, such as transmission time.

Port

Ports are used to allow multiple communication connections at one time in IP networks. Different services often have different port numbers.

Proxy

A proxy server is interim memory that saves information locally.

PSK

Abbreviation for "**P**re-**S**hared **K**ey".
A passphrase that is distributed and used for authenticating encrypted communication.

PSE

Abbreviation for "**P**ersonal **S**ecurity **E**nvironment".

That covers e.g. phone certificate, WPI client certificate etc.

PSS

Abbreviation for "**P**re-**S**hared **S**ecret".
Password for authentication in VoIP Security.

PSTN

Abbreviation for "**P**ublic **S**witched **T**elephone **N**etwork", analog telephone network or analog connections to digital network nodes, also public international telephone network.

QCU

Abbreviation for "**Q**uality **C**ontrol **U**nit".

QDC

Abbreviation for "**Q**uality **D**ata **C**ollection".
Concept for centrally collecting data on the quality of voice connections via IP networks.

QoS

Abbreviation for "**Q**uality **o**f **S**ervice".
Describes the subjectively detectable quality of a voice connection over IP networks. QoS properties are packet loss rate, packet delay, delay variation, reserved bandwidth, type of bit rate (variable, constant, or unspecified bit rate), and the bit rate.

RADIUS

Abbreviation for "**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice".
Protocol or software for user authentication via dial-up lines.

RAM

Abbreviation for "**R**andom **A**ccess **M**emory".
Memory with read/write access.

RCC

Abbreviation for "**R**outing **C**ontrol **C**enter".
If central routing is used in a network, individual network nodes transmit local route information to the RCC in regular intervals. The RCC saves this information and uses its global network knowledge to calculate the best routes between nodes.

Regular expression

Character string that uses specific syntactic rules to describe a set or subset of character strings. Regular expressions are firstly a type of text-based filter criterion that compares the expression in the form of a pattern with the text. For instance, it lets your find all character strings starting with 1 or 2, without having to enter any subsequent digits. Secondly, you can use regular expressions as a type of template for generating sets of digit combinations without having to specify each individual digit combination.

ROM

Abbreviation for "**R**ead **O**nly **M**emory".
Memory with read-only access.

Router

Routers set up connections to gateways and have access to several subnets and other routers. Using the IP address, a router determines the subnet or other router to which it should send data. It decides which path is the most favorable for the data at a given time.

RSM

Abbreviation for "**R**ealtime **S**ervice **M**anager".

RTC

Abbreviation for "**R**eal-**T**ime **C**ommunications Server" from Microsoft.

RTS

Abbreviation for "**R**eady **T**o **S**end).
This transmission request is part of modem control and is also used in the collision-free access procedure CSMA/CA (as implemented in 802.11). In modem control, the RTS signal is used in handshake mode as a control signal between a modem and a digital device that initiates data transmission via the transmission line.

SDLP

Abbreviation for "**S**tandard **D**evice **L**evel **P**rotocol".

SHA-1

Abbreviation for "**S**ecure **H**ash **A**lgorithm". The **1** indicates a newer version. SHA-1 is a hash algorithm and generates a checksum of 160 bits (20 characters) out of data lengths under 264 bits.

SIP

Abbreviation for "**S**ession **I**nitiation **P**rotocol".
Protocol standard for initializing calls in IP networks.

SNMP

Abbreviation for "**S**imple **N**etwork **M**anagement **P**rotocol".
The protocol is used for communicating with servers that take on network management functions. For example, this includes logging errors that occur on network components (SNMP trap).

SNTP

Abbreviation for "**S**imple **N**etwork **T**ime **P**rotocol".
The protocol is used between time servers and telephones in a network in order to synchronize the time on the telephones.

SPA

Abbreviation for "**S**oftware **P**roduct **A**ssurance".

SQL

Abbreviation for Structured Query Language. This is programming language that was developed by IBM to retrieve information from relational databases (for example, Microsoft Access).
Particular emphasis was placed on client/server environments (a client sends a request, the server provides the relevant information) during development.

SRSR

Abbreviation for "**S**mall **R**emote **S**ide **R**edundancy".
Indicates that a redundancy system is available.

SRTP

Abbreviation for "**S**ecure **R**ealtime **T**ransport **P**rotocol".
Protocol for the secure transmission of multimedia data via symmetrical encryption.

SSID

Abbreviation for "**S**ervice **S**et **ID**entifier".
Network name in a WLAN.

SSL

Abbreviation for "**S**ecure **S**ocket **L**ayer".
Technology for encrypted data transmission between client and server using authentication.

SSSO

Abbreviation for "**S**ecure **S**ingle **S**ign **O**n".
Access to the DLS is password-protected. The SSSO and all information in the DLS are transmitted in encrypted form using SSL.

Switch

Switching center in a star-shaped network, for example, HiPath 4000 system.

TAP

Abbreviation for "**T**echniker **A**rbeits**P**latz" (EWS - Engineering Workstation).

TCP

Abbreviation for "**T**ransmission **C**ontrol **P**rotocol".
Along with IP, this is the main protocol on the Internet. It provides a reliable, connection-oriented, full duplex service in the form of a data flow.

TKIP

Abbreviation for "**T**emporal **K**ey **I**ntegrity **P**rotocol".
Algorithm for encryption in WLANs.

TLS

Abbreviation for "**T**ransport **L**ayer **S**ecurity".
Standard protocol for performing computer authentication using certificates and encryption.

TLS versions **v1.0** & **TLS v1.1**, in addition to **TLS v1.2**, are supported at the web server interface.

TTL

Abbreviation for "**T**ime **T**o **L**ive".
This value specifies the lifespan of an IP data packet. Data packets transferred in IP networks can take different routes to reach their destination. Every time the data packet moves to a new network it passes a router which decrements the packet's TTL value by one. The packet is discarded when the value reaches 0. This ensures that packets that are unable to find their destination despite lengthy searches do not drift around the Internet ad infinitum. The higher the original TTL value of a data packet, therefore, the longer the packet can try to reach its destination.

UDP

Abbreviation for "**U**ser **D**atagram **P**rotocol".
Can be used as an alternative to TCP if there are no requirements in terms of reliability. UDP does not guarantee to deliver packets or supply them in a particular sequence.

URI/URL

Abbreviations for "**U**niform **R**esource **I**dentifier" and "**U**niform **R**esource **L**ocator".
These are the address of a file or a directory. The most common form of a URI is a URL. A typical URI indicates:

- the mechanism for accessing the contents (for example, a protocol such as http, ftp, or file).
- the computer where the contents can be found, and

- the specific name of the contents on this computer (usually a file name).

The parts are optional with the result that a file name is in itself a URL (even a relative one).

DP

Abbreviation for "**D**ial **P**refix".
A distinction is made between the national DP (NDP or National Dial Prefix) and the international DP (IDP or International Dial Prefix). For example, the national DP for Munich is the "0" in "**0**89". See also Canonical format.

VLAN

Abbreviation for "**V**irtual **L**ocal **A**rea **N**etwork".
Subdivision of an IP network into autonomous administration groups (domains). An option for identifying VLAN membership is by using a VLAN ID.

VLAN is, therefore, a network structure with all the properties of a conventional LAN but without any physical connections. In contrast to LANs where the distances between stations are subject to restriction, VLANs allows nodes that are further apart to be combined into a virtual local network.

VoIP

Abbreviation for "**V**oice **o**ver **IP**".
This refers to voice transmission using IP technology.

VoIP Security

Abbreviation for "**V**oice **o**ver **IP S**ecurity".
This describes measures for secure VoIP voice transmission.

VPN

Abbreviation for "**V**irtual **P**rivate **N**etwork".
A VPN connects two networks, a computer, and a network or two computers via public connections (for example, the Internet).
A tunneling protocol encrypts and decodes transmitted data to ensure that it cannot be accessed by unauthorized parties.
This technology was developed to cut costs as it is considerably cheaper for field workers to send data to headquarters via public lines than to create individual networks.

WAP

Abbreviation for "**W**ireless **A**pplication **P**rotocol".
This also refers to graphic applications on mobile telephones, organizers, and other suitable terminals that are transmitted using the protocol of the same name.

WBM

Abbreviation for "**W**eb-**B**ased **M**anagement".
A Web-based workpoint (IP phone) interface for administering configurations and modifying user settings via remote access.

WEP

Abbreviation for "**W**ired **E**quivalent **P**rivacy".
Standard encryption for WLANs. All stations in a WLAN and the access point or WLAN router use the same key for encrypting and decoding data. WEP distinguishes between 64- and 128-bit encryption.

See also WPA, WPA-PSK.

WLAN

Abbreviation for "**W**ireless **L**ocal **A**rea **N**etwork".

Workpoint

Workpoint is a term for both IP telephones, such as, optiPoint 410 standard, and soft clients, such as optiClient 130.

WPA

Abbreviation for "**W**I-FI **P**rotected **A**ccess".
WPA provides security in WLANs by using dynamic keys for encryption. When a connection or session is set up, dynamic keys are exchanged via the Extensible Authentication Protocol (EAP).

See also WEP, WPA-PSK.

WPA-PSK

Abbreviation for "**W**I-FI **P**rotected **A**ccess with **P**re-**S**hared **K**ey".
An encryption procedure for WLANs. This procedure uses station-specific keys made up of a pre-shared key and the MAC address of each device. These keys are automatically updated at regular intervals (rekeying intervals)

See also WEP, WPA.

WSP

Abbreviation for "**W**ireless **S**ession **P**rotocol".
Protocol for transmitting data on WAP-compatible telephones.

Index

’’Autoconfig. Mediatrix Gateway" Tab 1085
’’Bluetooth Settings’’ Tab 802
"E/A Cockpit " Tab 465
"Standard CSTA" Tab 464

802.1x Settings 746

A

Accessing help 147
Action Buttons 165, 177, 397
Activity and Error Log 318, 320
Administering Certificates 1552
Alarm Classes 337
Alarm Configuration 334, 1596
Alarm List 332
Alarm Protocol 329, 332
ANAT Settings 475
API Notifications 291
APM Inventory 1326
Application interface 147
Application List 635, 1169
Archives Data 1086, 1087, 1261
Archiving automatic 398
Area of DLS application 44
Audio
    Schemes 894
    Settings 612
Audio Devices available 896
Audio Settings 1157
Audit and Security Log 322, 324
Authentication Policy 574
Autoconfiguration 32
    IP Client 1083
    IP Gateway 1084, 1085
    IP Phone 1082
Availability 507, 1122

B

Backing up the DLS database 1459, 1461
Backup 355
Backup/Restore 351
Basic Data 1399
Basic E.164 37
Batch File 344
Before the Activate action, the administrator must ensure that all the devices have the server’s credentials and that the jobs have been successfully completed 1607
Business Groups 244
Buttons 165

C

CA Administration 385
CA Certificates 640, 643, 646, 650, 1177
    IPSec / VPN 989
CA CertificatesCertificates
    CA 632
CA intern 221
Calender button 156
Call Forwarding 522, 528, 933, 1135
Call Log 800
Canonical Dial Lookup 597, 1154
Capacity limits of the DLS 53
Certificate
    phone certificate 749
    RADIUS server CA certificate 752, 755
Certificate Deployment automatic 393
Certificate Deployment Restrictions 248
Certificate Renewal 216
Certificate Trap Settings 622
Certificates 39
    administering certificates 1552
    CA 640, 643, 646, 650, 1177
    WBM server certificate 564, 578, 579
Changing parameters (first steps) 1432
Changing workpoint parameters (first steps) 1432
Check box 156
Circuit 650, 1178
Circuit CA Certificates 651
Cluster Configuration 311
Cluster Settings 316
Codecs/Compressing 605
Configuration 1033
    Activity and Error Log 320
    Audit and Security Log 324
Configuration Data 1406
Configuration Menus locked 669, 1185
Configuration templates 1443
Contact Me Notify 377
Context-sensitive help 147
Copy a Registered Device to a Virtual Device 1538

Copy Macro for P&P 1495
Country 782
Country & Language 1230
CRL Distribution Points 983
CRL Files 992
CSTA Service Provider 823
CTI Configuration 813
CTI HFA Provider 814

D

Daylight Saving 601
DCMP 373, 1080
Deactivation of XML Push feature on Linux DLS 1585
Debug WLAN 730
Deployment Data 1403
Deployment Server 312
Deployment Service 296
Destinations 694, 1208
Device Attributes modify 1482
Device Profile 1358
DHCP 41
Diagnosis and Security 772
Diagnosis Files upload automatic 407
Diagnostic 759
Dialing Properties 593, 1149, 1150
  Canonical Dial Lookup 597
Dialplan 516, 1129
Dialup Site 944
Directories Address Books 903
Directory Service 911
Display Logging Data 317
Display/Phone 790
Display/Phone Settings 1239
DLS advantages 51
DLS API 175, 309
DLS client
  ending 146
  starting 145
  starting on the server/client 113
DLS Client GUI 306
DLS database
  backup 1459, 1461
  migration 1462
  reset 1463
  restore 1460, 1462
DLS Database manipulating 1549
DLS on the EWS 1548
DlsAPI Program Interface 1550
DLS-Device Connection 376
DLS-GUI 175
DNS Server 1107
DNS server 477, 481
DSS 931

E

E.164 Patterns 243
E/A Cockpit CA Certificates" Tab 656
Element 156
Element Manager 1334, 1355
  Protocol 1353
Element Manager Configuration 1333
Element Manager Security 1355
EM Synchronization 1067
Enabled Services 1146
Exchange 646, 650, 1177, 1178
Exchange CA Certificates 647
Exporting Plug&Play Data 1475

F

FAC Prefixes (Phone Log) 598
Feature
  Settings 1 491, 1109
  Settings 2 494, 1112
Features 51
  Server based 515
Field name in the wizard
  Configure FTP Server 255
  Configure Logging 250
File Deployment 806, 1248, 1317
File Server 360
File Settings 768
File Types 47
Files
  difference to software 1309
  registering in the DLS 1440
Filter test 422, 423, 425
Format update of the DLS database (migration) 1462
FTP configuration 32
FTP Server 799
FTP server configuration 256

G

Gateway 831, 834, 839, 852
  Configuration 1292
  Connection 1297
  QoS Data Collection 1299
  Report Settings 1305
  Server Data 1303
  Threshold Values 1307
Gateway (HFA) / SIP Server 448
Gateway (HFA)/SIP Server 1097
Gateway (Standby) 451
Gateway/Server 444, 827, 1096
Gateways 1424

General Features 205

H

Header 151
Help 147
Help function 147
Help Internet URL 798, 1243
HFA
  Codec Settings 888
  Dialing Properties 878
  Layout 924
  Mobility 686
  Mobility with HiPath 3000 1581
  Settings 743, 844
  Settings SPE 941
HFA Client create 1479
HFA Phone create 1479
HiPath 3000/5000 1352
HiPath 4000 Assistant 1349
HiPath SQL DB 915
History 1266
History of Changes 13
Hot Line 1112
HotKeys 955
How to replace OSV Assistant Manager with OSV Element Manager (steps) 1435
HTTP-Proxy 376, 377
HTTPS configuration 32
HTTPS Server CA Certificates 271, 567
HTTPS Server Configuration 265

I

IEEE
  802.11b (Transfer Mode) 720
  802.1x (import certificate) 1554
  802.1x (remove certificate) 1561
  802.1x phone/RADIUS certificates 745
IEEE 802.1x 1554
Images on the Server 269
Import Mobile User Data 1577
Importing Plug&Play Data 1475
Importing WBM Server Certificates 1553
INCA Inventory 1322
Info
  Deployment Server 315
  Internal CA 224
  IP Device Response Test 1018
  IP Device Revoke Certificates 1015
  Read IP Device Data 1008
  Reset IP Devices 1011
Infrastructure Policies 245
Infrastructure Policy 287
Infrastructure Policy Table 290
Installation
  DHCP server 129
  DNS server (configuration) 132
  FTP server 125
Instant Messaging (XMP) 954
Interaction 1252
Interface of the DLS 147
Internal CA 221
Internet Pages 913
Inventory Data 1044
  management 52
  Pings 1051
  tab 1044
IP Address changing 1547
IP Client Configuration 809
IP Client Logon/Logoff History 1087
IP Client Registration History 1087
IP Clients 1420
IP clients 1024
IP Device
  Interaction 993, 999, 1000, 1002
  Pinging 1019
IP Device Configuration 1064, 1536
  DCMP 1080
  DSL Connectivity 1071
  Profile 1069
IP Devices 1390
  Scanning 35
  To archive 403
IP Gateway create 1480
IP Gateways 1025, 1422
IP Phone Configuration 438
IP Phones 1417
IP Ranges 241
  Scan IP Devices 1031
IP Routing 465, 1106
IP Switch Data 1055
IPSec/VPN
  Settings 985
IPv6 Settings 473
Issuer Administration 389
Issuing CAs 206

J

Java 625, 1163
Java Midlet Inventory 1323
Job
  Configuration (interface) 1413
  Control (interface) 1392
  entering in the toolbar 151
  using job coordination 1457

Job Configuration 1413
Job Control 1392

K

Keylayout 687, 1201
Keysets 687, 688
    Destinations 694

L

Language 782
LDAP 904, 1170
LDAP Inventory 1320
LDAP Settings 637
License information 1442
License state 429
Licenses 859
Licensing 28
Line Keys 929
List of ports in use 53
Local Functions locked 680, 1196
Location 235
Location configuration 31
Location Server 727
Location Service 297
Locations 234
Locks 1184
Logging On/Off Mobile Users 1569
Login Policy 189
Login window 145
Logo File Inventor 1324
Logoff automatic 1268
Logon/Logoff 1265

M

Macro Command Syntax 1495
Main menu 148
MakeCall 299
Manage Rules 1328
Mediatrix Gateway Configuration 993, 999, 1002
Menu
    tree view 148
Menu line 152
Message Filter 421
Message window 166
Messaging Services 786, 1236
Migration
    DLS database 1462
Migration Scenarios 1499
Mobile
    Users 1089
Mobile Users
    Application List 1169
    Archives Data 1261
    Audio Settings 1157
    Availability 1122
    Call Forwarding 1135
    Canonical Dial Lookup 1154
    Configuration Menus locked 1185
    Country & Language 1230
    Data saving 1574
    Destinations 1208
    Dialing Properties 1149, 1150
    Dialplan 1129
    Display/Phone Settings 1239
    DNS Server 1107
    Enabled Services 1146
    Feature Settings 1 1109
    Feature Settings 2 1112
    Gateway (HFA)/SIP Server 1097
    Gateway/Server 1096
    Help Internet URL 1243
    History 1266
    Hot Line 1112
    Interaction 1252
    IP Routing 1106
    Java 1163
    Keylayout 1201
    LDAP 1170
    Lggin on/off 1569
    Local Functions locked 1196
    Locks 1184
    Logoff automatic 1268
    Logon/Logoff 1265
    Messaging Services 1236
    Mobile/Basis User 1258
    Mobility Data 1200
    Mobility Logon/Logoff 1198
    Passwords 1144
    Phone Lock 1244, 1245
    Profile 1566
    Protocol 1277
    QoS Parameter 1142
    Quality of Service 1141
    Response Test Settings 1262, 1274
    Ringer Melody 1132
    Security Settings 1143
    Send URL Server CA Certificate 1221
    Server based Features 1128
    SIP Error Notification 1238
    SIP Mobility 1286
    SIP Registering 1 1100
    SIP Registering 2 1102
    SIP Settings 1225
    SIP Terminal Settings 1098

Statistics 1280, 1289
Telephony 1148
Time 1155
Time parameters 1155
User Keylayout 1270
User Settings 1183
Call related 1118
WAP 1162
Warm Line 1112
XML Applications 1164
Mobile Users to archive 404
Mobile/Basis User 1258
Mobility 682, 686
Adminstrating 1565
Configuring 1565
configuring (overview) 57
configuring a function 1565
definitions 55
Function 37
Logon/Logoff 1198
overview 55
profile concept 58
subscriber number 57
Mobility Data 1200
Modify Key 1480
Modify Keyset 1481
Modify OpenScape Data 1483
Modifying passwords 30
MOH Inventory 1321

N

Name Update Sources 666, 1182
NETBOOT Inventory 1327
Network Drive Configuration 281
News Service 298
Notification 340

O

OCSR 1 Server CA Certificate 570
OCSR 1 Signature CA Certificate 572
OCSR 2 Signature CA Certificate 573
OpenScape UC Connection 660, 1181
OpenScape UC Connection CA Certificates 661
OpenScape Voice 1341, 1467
Operating Sequences 1427
OptiClient in Call Centers 1545
Options 300
Options field 156
Outlook 959

P

P&P Import Protocols 328
P&P Number Pool 246
Parent Profiles 1365
Password Change 187
Password Policy 184
Password Policy Settings dditional 556
Passwords 554, 1144
Passwords modifying 30
Peer Credentials 986
Periodical File Upload 775
Phone Certificate 749
Phone Location 584
Phone Lock 801, 1244, 1245
Ping IP Devices 1021, 1024
Pinging IP Device 1019
Platform 46
Plug&Play
function overview 52
registering workpoints 1446
Plug-In Properties 208
Policy Settings 182
Port list 53
Port Number changing 1547
Ports 484, 863
Standby 487
Profile Management
Parent Profiles 1365
Templates 1362, 1369
Tenants 1364, 1370, 1378
Program Interface DlsAPI 1550
Protocol 1277
Activity and Error Log 321
Audit and Security Log 327
Automatic Archiving 405
Backup/Restore 358
Upload Diagnosis- and Security Log Files 410
Proxy 851

Q

QoS Data Collection 1299
QoS Parameter 537, 1142
Standby 544
Quality of Service 867, 1141

R

RADIUS Certificates 1554
RADIUS Server CA Certificate 752
Reg-Addresses 242
Registering
by scanning workpoints 1026
workpoints by reading data 1003
Registrar 849
Registration

software, automatic 1441
Remote Trace 771
Renewal 226
Repeat filter 419
Replacing an Old Workpoint 1539
Replacing HFA with SIP Software 1540
Replacing SIP with HFA Software 1541
Report
Settings 549, 966, 1305
Request Parameter 213
Requirements
personnel 71
technical 69
Reset
DLS database 1463
workpoints 1009, 1013, 1016
Response Test Settings 1262, 1274
Restore 356
DLS database 1460, 1462
Restrictions of the DLS 53
Rights
Account Configuration 179
Roles and Rights 197
Ring Tones 901
Ringer Melody 519, 1132
Roles 178
Roles and Rights 193
Routing 465
Rules, managing (deployment) 1328

S

Safety Mode 176
Saving the DLS database 1459, 1461
Scan IP Devices 35, 1033
Scan Results 1035
Search Functionality 170
Section 6.6.7 "Settings" Tab 227
Secure mode 365
Secure Shell (SSH) access 770
Secure Trace 778
Security EncryptionWLAN
Security Encryption 724
Security Log Files upload automatic 407
Security Settings 970, 1143
Security State Protocol 1076
Selecting views 155
Selection list field 156
Send URL Server CA Certificate 707, 1221
Server based Features 1128
Server Configuration 228
Server Data 548, 965, 1303
Server Licenses 426
Service Integrations 636
Service Interface 1550
Services (NW Stack) enabled 560
Services nabled 1146
Session Policy 192
Settings
802.1x 746
Alarm Configuration 349
ANAT 475
Audio 612
Automatic Archiving 401
Automatic SPE Configuration 391
Codecs 605
Daylight Saving 601
Diagnostic 759
Display/Phone 790
HFA 743, 844
IPSec/VPN 985
IPv6 473
Remote Trace 771
Report 549
Secure Trace 778
SIP 737
SPE 975
SRSR 590, 876
Time 600
Trace Configuration 417
Video 898
Signaling and Payload Encryption (SPE) 731, 936, 975
SIP
Call Forwarding 933
Codec Settings 890
Connection 846
Dialing Properties 884
Error Notification 789, 1238
Features 918
Gateway 852
Keypad 934
Keysets 927
Line Keys 929
Mobile User Configuration 1090
Mobility 682, 1286
Ports 865
Proxy 851
Registering 1 456, 1100
Registering 2 458, 1102
Registrar 849
Settings 737, 1225
Settings SPE 939
Station Keys (DSS) 931
Survivability 463, 857
Terminal Settings 454, 1098

User Keylayout 1270
SIP Client create 1479
SIP Phone create 1478
SIP phones on HiPath 3000/4000 (feature availability) 494, 507
SNMP 341
Settings 620
Software
deployment, different sequences 1451
difference to files 1309
Images 33
license information 1442
registering in the DLS 1440
Software Deployment 1315
Software Inventory 1319
SPE CA Certificates 732, 734, 936, 980, 1556
SPE Certificate 732, 977
SPE Configuration 383
SQL DB 915
SRSR
Settings 876
SRSR Settings 590
SSH 770
Standard Profile 253, 254
Statistics 1280, 1289
Status Area 167
Status Information 1412
Supported Devices of IP Device 1363
Survivability 857
SW Deployment 843
SW Deployment Restrictions 247
Syslog 347
System
Functions 916
Requirements 22
Services 854
SYSTEM/RINGTONE Inventory 1325
System-wide keyboard tokens(Hotkeys) 956

T

Tab
Standard Profile 253, 254
Syslog 347
Tabs
displaying 156
Inventory Data 1044
Telephony 583, 584, 873, 1148
Templates 1362, 1369, 1443
Tenants 229
Account Configuration 180
FTP Server Configuration 263
HTTPS Server Configuration 276
Location 249
Network Drive Configuration 286
Profile Management 1364, 1370, 1378
Text field 156
Threshold Values 551, 967, 1307
Time 600, 1155
Time parameters 599, 1155
TLS Connector Configuration 190, 304
Trace Configuration 411, 417
Trash 1053
Tree menu 148
Trust Anchor 217, 218
Truststore DLS API 310
Truststore DLS Client GUI 308

U

Uninstalling the DLS server 143
Update 843
Upgrading from SQL Server 2008 to SQL Server 2012 73
User Data Profile 1366
User Keylayout 1270
User Settings 667, 1183
Call related 502, 1118
Using the DLS 41

V

Video Devices available 900
Video Settings 898
View bar 155
VPN Settings 861

W

WAP 624, 1162
Warm Line 1112
WBM Importing Server Certificates 1553
WBM Server Certificate 564
WBM Server Certificates 971
Web Service Interface 1550
Windows for messages 166
WLAN
Debug 730
Location Server 727
Settings 720
Workpoint Firmware Installation 33
Workpoint Interface Configuration 363, 372
workpoint_hotkeys_oc 956
WSI(UC) 659

X

XML Application Data 1408
XML Applications 293, 627, 1164, 1379, 1384, 1583
Info 1384

IP Devices 1390

© 2026 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.